

Cisco

企业网快速构建 与排错手册

闫志刚 编著

www.net527.cn

小牛

 人民邮电出版社
POSTS & TELECOM PRESS

Cisco

企业网快速构建 与排错手册

www.net527.cn 小牛

封面设计：张群胆

ISBN 7-115-13068-X



9 787115 130686 >

人民邮电出版社网址 www.ptpress.com.cn

ISBN7-115-13068-X/TN·2419
定价：55.00 元

Cisco 企业网快速构建与排错手册

闫志刚 编著

www.net527.cn 小牛

人民邮电出版社

图书在版编目 (CIP) 数据

Cisco 企业网快速构建与排错手册/闫志刚编著. 北京: 人民邮电出版社, 2005.4
ISBN 7-115-13068-X

I.C... II.闫... III.计算机网络—技术手册 IV.TP393-62

中国版本图书馆 CIP 数据核字 (2005) 第 012631 号

内 容 提 要

本书是一本专门介绍 Cisco 网络构建方面的技术图书。本书首先介绍了网络的基本技术及 Cisco 的网络产品, 并采用案例的形式介绍了如何选购 Cisco 的网络设备来构建不同的企业网络。然后, 分别对构成企业网络的 Cisco 的主要网络设备进行了有针对性的讲解, 这里主要采用案例的形式介绍如何有效地配置 Cisco 的交换机、路由器和防火墙产品, 接着通过具体的案例介绍了如何快速的构建一个典型的企业网络。接下来是对企业网络的管理和安全作了简要的介绍, 并通过一些例子来介绍企业网络安全方面的一些具体的配置。最后对在企业网络中如何进行故障排除作了简要的介绍。

本书包括了许多典型的案例, 涵盖了中小企业乃至大型企业常见的一些网络架构和详细的配置文档, 同时对国内常用的通信线路进行了相应的介绍。非常适合于负责企业网络建设的网络工程技术人员, 以及负责网络管理的管理人员使用。

Cisco 企业网快速构建与排错手册

- ◆ 编 著 闫志
责任编辑 王晓明
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线: 010-67129258
北京密云春雷印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本 787×1092 1/16
印张 29.5
字数 721 千字 2005 年 4 月第 1 版
印数 1—3 500 册 2005 年 4 月北京第 1 次印刷

ISBN 7-115-13068-X/TN·2419

定价: 55.00 元

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

前 言

信息技术在过去的十几年里的发展是非常惊人的，曾经被认为是昂贵且复杂的许多网络设备，而今已被企业广泛采用，比如路由器、交换机、防火墙等，曾经被认为是大公司的专利，现如今几乎到处可见。所有这些都源于人们越来越意识到了网络的重要性，这也使得对熟练掌握配置、管理、诊断网络设备的人员的需求与日俱增。

虽然目前已有一些介绍网络技术及 Cisco 产品的比较优秀的书籍和培训资料，但这些书籍或培训资料多为“应试”型的教材，主要针对各种网络方面的认证（包括 Cisco 公司的职业和专业认证），书中许多配置也是根据美国的网络状况给出的，而针对国内具体的网络现状的书籍还很缺少，这就导致虽然有些人已经通过了 CCNA、CCNP 乃至 CCIE 认证，但在实际工作中调试一个简单的帧中继线路都会出问题，并不是他不具备这方面的知识，而是他获得的这些知识没有针对性。相比这些书籍，本书包括了许多典型的案例，涵盖了中小企业乃至大型企业常见的一些网络架构和详细的配置文档，同时对国内常用的通信线路进行了相应的介绍。相信对初涉网络行业以及在这个行业中工作的人会有很大的帮助，希望本书能够成为网络工程师的工作手册。

在本书的撰写过程中，我们始终采用任务驱动的方式来进行教学，也可以称为目标驱动的方式，因为我们在认知一个新事物时，往往是在遵循着一定的规律，也可以称为逻辑顺序，即“what-why-how”，那么我们就根据这一顺序来学习有关企业网的知识，首先我们解释什么是网络、网络通信的机制从而引出对企业网的解释以及企业网络的构成模块，然后我们介绍如何来构建一个成熟的企业网络，最后我们来学习如何管理一个企业网络，以及出现问题后如何来快速的处理。

作 者

2004 12 于北京

目 录

第 1 章 网络技术基础	1
1.1 简介	1
1.2 网络互联基础	3
1.3 OSI 和 TCP/IP 参考模型	5
1.3.1 为何要将通信协议进行分层	6
1.3.2 OSI 参考模型	6
1.3.3 TCP/IP 参考模型	10
1.4 局域网基础知识	12
1.5 广域网基础知识	13
1.6 小结	15
第 2 章 网络设备选购指南	16
2.1 交换机选购指南	16
2.2 路由器选购指南	19
2.3 防火墙选购指南	25
2.4 Cisco 交换机产品	28
2.4.1 Catalyst 2950 系列交换机	29
2.4.2 Catalyst 3550 系列交换机	31
2.4.3 Catalyst 3750 系列交换机	32
2.4.4 Catalyst 4500 系列交换机	35
2.4.5 Catalyst 6500 系列交换机	37
2.5 Cisco 路由器产品	41
2.5.1 Cisco 1700 系列路由器	41
2.5.2 Cisco 2600 系列路由器	44
2.5.3 Cisco 3600 系列路由器	46
2.5.4 Cisco 3700 系列路由器	48
2.5.5 Cisco 7200 系列路由器	50
2.5.6 Cisco 7500 系列路由器	57
2.5.7 Cisco 7600 系列路由器	60
2.5.8 Cisco 12000 系列路由器	61
2.6 Cisco 防火墙产品	61
2.6.1 Cisco PIX501 系列防火墙	62

2.6.2	Cisco PIX506E 系列防火墙	64
2.6.3	Cisco PIX515E 系列防火墙	65
2.6.4	Cisco PIX525 系列防火墙	66
2.6.5	Cisco PIX535 系列防火墙	68
2.7	小结	68
第 3 章	企业网组建	70
3.1	简介	70
3.2	典型企业网构成	70
3.3	企业内部局域网模块	71
3.3.1	超小型局域网	71
3.3.2	小型局域网	73
3.3.3	中大型局域网	75
3.4	企业广域网互联模块	80
3.5	企业 Internet 出口模块	90
3.6	小结	94
第 4 章	Cisco 交换机配置	95
4.1	概述	95
4.2	Cisco 交换机基础	95
4.3	Cisco 交换机配置	101
4.3.1	基本设置方式	101
4.3.2	IOS 和 SET 命令集介绍	104
4.3.3	IOS 命令状态	106
4.3.4	IOS 文件管理	107
4.3.5	IOS 常用命令	107
4.3.6	交换机基本配置模板	110
4.3.7	端口配置	111
4.3.8	VLAN 配置	117
4.4	Cisco 交换机经典配置案例	125
4.4.1	案例 1	125
4.4.2	案例 2	131
4.5	小结	142
第 5 章	Cisco 路由器配置	143
5.1	简介	143
5.2	Cisco 路由器基础	143
5.2.1	Cisco 路由器基本构成	144
5.2.2	基本设置方式	146
5.2.3	IOS 命令状态	150
5.2.4	IOS 文件管理	150
5.2.5	IOS 常用命令	151

5.2.6 路由器基本配置模板	153
5.3 广域网互联设置	154
5.3.1 电信网简介	154
5.3.2 数字数据网 (DDN)	157
5.3.3 帧中继 (Frame Relay)	168
5.3.4 数字电路	179
5.3.5 ISDN	197
5.3.6 PSTN	208
5.3.7 ADSL	218
5.4 路由协议设置	229
5.4.1 静态路由	232
5.4.2 RIP 协议	234
5.4.3 EIGRP 协议	235
5.4.4 OSPF 协议	236
5.4.5 BGP 协议	240
5.4.6 重新分配路由	240
5.5 访问控制和地址转换	242
5.5.1 访问控制	242
5.5.2 地址转换	246
5.6 Cisco 路由器经典配置案例	251
5.7 小结	269
第 6 章 Cisco 防火墙配置	270
6.1 简介	270
6.2 Cisco 防火墙基础	271
6.2.1 Cisco 防火墙基本构成	273
6.2.2 基本设置方式	274
6.2.3 PIX 命令状态	276
6.2.4 PIX 文件管理	276
6.2.5 PIX 常用配置命令	276
6.2.6 防火墙基本配置模板	279
6.3 Cisco 防火墙经典配置案例	282
6.4 小结	285
第 7 章 典型企业网构建案例	286
7.1 简介	286
7.2 小企业网络构建案例	286
7.2.1 案例 1	286
7.2.2 案例 2	291
7.3 中型企业网络构建案例	305
7.4 大型企业网络构建案例	336

7.5 小结	337
第 8 章 企业网维护管理	338
8.1 简介	338
8.1.1 网络管理的概念	338
8.1.2 网络管理的内容	339
8.2 文档管理	340
8.3 设备管理	341
8.4 Cisco 设备软件升级	341
8.4.1 Cisco 路由器软件升级或恢复	342
8.4.2 Cisco 交换机软件升级	358
8.4.3 Cisco 防火墙软件升级	367
8.5 Cisco 设备口令恢复	369
8.5.1 Cisco 路由器口令恢复	369
8.5.2 Cisco 交换机口令恢复	372
8.5.3 Cisco 防火墙口令恢复	374
8.6 SNMP 网管协议	375
8.7 小结	379
第 9 章 企业网安全配置	380
9.1 简介	380
9.2 企业网络安全风险分析	380
9.3 企业网络安全的部署	385
9.3.1 局域网模块	386
9.3.2 广域网模块	387
9.3.3 Internet 接入模块	388
9.4 企业网安全部署案例	389
9.4.1 网络设备通用安全设置	389
9.4.2 局域网模块	395
9.4.3 广域网模块	397
9.4.4 Internet 接入模块	399
9.5 小结	401
第 10 章 企业网故障诊断与排除	402
10.1 简介	402
10.2 系统化排错方法	402
10.3 分层排错思想	404
10.4 IP 排错工具	406
10.5 TCP/IP 连通性排错	413
10.6 链路层排错	415
10.6.1 局域网排错	415
10.6.2 广域网链路排错	417

10.7 网络层排错	428
10.8 Cisco 故障诊断和排除资源	429
10.9 企业网排错案例	435
10.10 小结	438
附录 A Cisco IOS 命名规范	439
附录 B 常用线缆介绍	444
附录 C Cisco 常用工具和链接	445
附录 D 通过 LED 灯查看 Cisco 交换机负载	460

第1章 网络技术基础

本章将涵盖下列有关网络基础方面的关键主题：

- 网络互连基础
- OSI/TCP/IP 参考模型
- 局域网基础知识
- 广域网基础知识

希望读者通过对本章的学习，能够对网络的一些基础知识有所了解，这些基础知识主要包括以下内容：

- (1) 什么是网络；
- (2) 常见的网络类型有哪些；
- (3) 常用的网络介质有哪些；
- (4) 为什么会对网络通信分层；
- (5) OSI 网络参考模型各层的主要功能；
- (6) TCP/IP 网络参考模型和 OSI 模型的对比；
- (7) TCP/IP 网络参考模型各层包括的主要协议（V.24、V.35、HDLC、PPP、IP、UDP、TCP、RPC、NFS、JPEG、FTP、HTTP、Telnet）；
- (8) 常见网络设备在 OSI 模型中的位置（网卡、集线器、交换机、路由器）；
- (9) 什么是局域网；
- (10) 局域网的设备有哪些；
- (11) 什么是广域网；
- (12) 广域网的设备有哪些。

1.1 简介

1. 什么是计算机网络

计算机网络是指将地理位置不同，具有独立功能的多个计算机系统用通信设备和线路连模起来，并借功能完善的网络软件（网络协议、网络操作系统等）实现资源共享的系统。计算机网络是现代通信技术与计算机技术相结合的产物。计算机网络的发展大致经历了具有通信功能的单机系统、具有通信功能的多机系统和计算机网络这 3 个阶段。

2. 计算机网络的分类

对于网络，有局域网、广域网、校园网、企业网、宽带网、无线网等很多种类，以下我们就对计算机网络的分类进行一个较为全面的介绍，以便对网络有一个整体上的认识。

(1) 按地理范围分类, 可以分为局域网、广域网和城域网。

① 局域网 (Local Area Network, 简称 LAN): 局域网一般在几十米到几公里范围内, 一个局域网可以容纳几台至几千台计算机。局域网具有如下特性:

a. 局域网分布于比较小的地理范围内。因为采用了不同传输能力的传输媒介, 因此局域网的传输距离也不同。

b. 局域网往往用于某一群体, 比如一个公司、一个单位、某一幢楼、某一学校等。

② 广域网 (Wide Area Network, 简称 WAN): 广域网是将分布在各地的局域网络连接起来的网络, 是“网间网”(网络之间的网络)。广域网具有如下特性:

a. 广域网的范围非常大, 可以跨越国界、洲界, 遍布全球范围。

b. 广域网是网络的公共部分, 在我国广域网一般需租用电信部门的线路搭建而成。

③ 城域网 (Metropolis Area Network, 简称 MAN): 城域网是规模局限在一座城市的范围内的区域性网络。城域网的速度比广域网快, 符合宽带趋势, 因此现在发展很快。与局域网相比, 城域网具有分布地理范围广的特点, 一般来说, 城域网的覆盖范围介于 10~100km 之间。

(2) 按网络拓扑结构分类, 可以分为星形网络、环形网络和总线形网络结构。

网络的拓扑 (Topology) 结构是指网络中通信线路和节点 (计算机或设备) 的相互连接的几何形式。按照拓扑结构的不同, 可以将网络分为星形网络、环形网络、总线形网络 3 种基本类型。在这 3 种类型的网络结构基础上, 可以组合出树形网、网状网等其他类型拓扑结构的网络。

① 星形网络结构: 在星形网络结构中各个计算机使用各自的线缆连接到网络中, 因此如果一个节点出了问题, 不会影响整个网络的运行, 但相比其他两种结构, 星形网络结构所消耗的传输介质的数量最大。星形网络结构是现在最常用的网络拓扑结构, 其结构如图 1-1 所示。

② 环形网络结构: 环形网络结构的各节点通过通信介质连成一个封闭的环形。环形网络容易安装和监控, 但容量有限, 网络建成后, 难以增加新的站点。因此, 现在组建局域网已经基本上不使用环形网络结构了。在电信的城域传输网中多采用环形结构, 其结构图如图 1-2 所示。

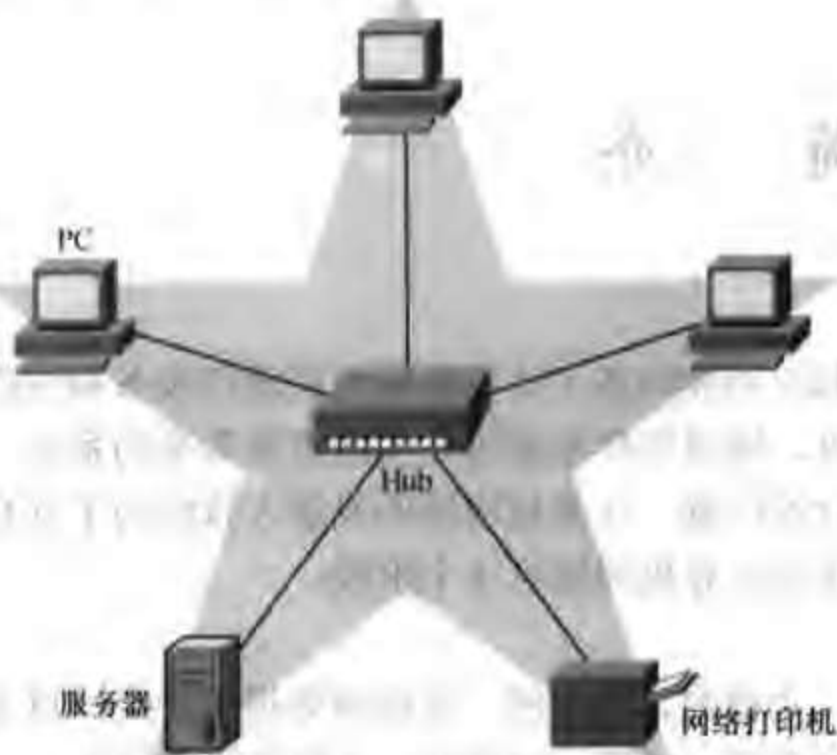


图 1-1 星形拓扑



图 1-2 环形拓扑

③ 总线形网络结构：在总线形网络结构中所有的站点共享一条数据通道。总线形网络安装简单方便，需要铺设的电缆最短，成本低，某个站点的故障一般不会影响整个网络，但介质的故障会导致网络瘫痪。总线形网络安全性低，监控比较困难，增加新站点也不如星形网络容易。所以，总线形网络结构现在基本上已经被淘汰了。图 1-3 显示了总线形拓扑结构。

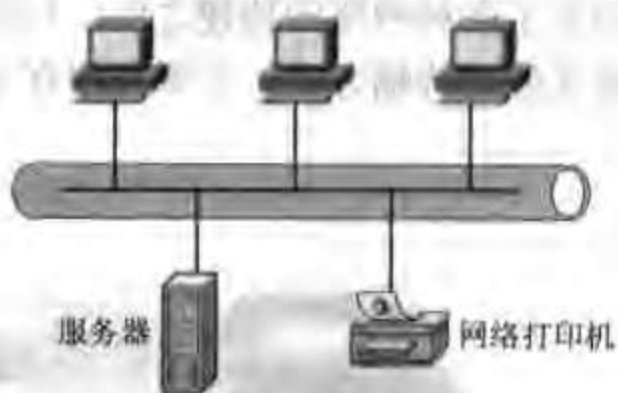


图 1-3 总线形拓扑

(3) 按传输介质分类，可以分为有线网络（同轴电缆、双绞线、光纤等）、无线网络（微波、红外线、无线电等电磁波）。

(4) 按服务对象分类，可以分为企业网、校园网等。

1.2 网络互联基础

一个网络是由各种各样的设备通过一定的规则组织而成，这一节我们首先来直观地认识一下这些设备，下一节我们再来介绍互连的规则（OSI 和 TCP/IP 模型）。

建设一个计算机网络，首先需要使用一些传输介质来传输数据。这些介质可以是铜线、光纤、微波及红外光束等。传输介质是网络中发送方与接收方之间的物理通路，它对网络数据通信的质量有很大的影响。常用的网络传输介质包括：双绞线、同轴电缆、光缆（光导纤维）和微波，如图 1-4~1-7 所示。



图 1-4 双绞线



图 1-5 同轴电缆



那么在建设网时我们应该如何来选择传输介质呢？

对于局域网来说，铜线是使用最多的网络传输介质。其中 5 类非屏蔽双绞线使用最为广泛；同轴电缆主要用在总线型的拓扑结构，目前基本已淘汰。光纤主要用在对传输速率和传输距离有较高要求的电信传输网络上，但随着计算机技术的飞速发展，新型的应用对传输速

率的要求越来越高，同时随着技术的进步，光纤的价格也逐渐走低，这样，光纤越来越广地应用在了各种网络的构建之中，目前大多数企业网络的主干都采用的是光纤连接。微波采用的是无线的传输方式，主要应用在不便布线的石油、地质、水利等行业中。



图 1-6 光纤

选择传输介质需要考虑的因素主要包括：传输带宽、传输距离、抗电磁干扰能力、抗衰减能力以及非常重要的价格。双绞线和光纤两种介质的对比见表 1-1。

表 1-1 介质对比

	双 绞 线	光 纤
传输带宽	10、100、1000Mbit/s	10Mbit/s~几百 Gbit/s
最大传输距离	100m	几百米~几十公里
抗电磁干扰能力	弱	强
抗衰减能力	弱	强
价格	低	高

选择传输介质之后，在计算机上需要一个设备来将计算机上的数据转换为可在网络上传输的数据，这个重新组织数据的设备就是网卡（NIC）。网卡通常插在主机的总线扩展槽上，网络电缆同网卡相连，网卡实物如图 1-8 所示。

网卡提供了计算机与网络传输介质（铜线与光纤等）之间的连接。计算机总线上的数据是并行传输的，而网络介质上的数据是串行传输的，网卡来实现将数据从并行转换为串行或从串行转换为并行。

网卡有一个惟一的地址（MAC 地址），它驻留在每块网卡的 ROM 芯片里，这个地址用来惟一地识别此节点，交换机根据 MAC 地址进行数据转发，有关交换机的知识我们会在以后的章节进行介绍。



图 1-7 微波



图 1-8 网卡

在选择好传输介质和在计算机上安装了相应的网卡之后,还需要通过一些连接设备来将网络中的节点连接起来,并能扩展网络中的节点。在局域网络中最常用的连接设备是集线器(Hub)和交换机,如图1-9和1-10所示。低端的交换机和集线器外观没有太大区别,集线器属于物理层(OSI和TCP/IP模型)的设备,它只是将电缆进行组织,并将信号中继到所有的连接设备上,所以又称为多端口中继。集线器所有端口连接的设备同处于一个碰撞域和广播域;而交换机是属于数据链路层(OSI和TCP/IP模型)的设备,它是根据节点的MAC地址进行数据的交换,交换机的所有端口连接的设备同处于一个广播域,但每个端口属于一个碰撞域。



图 1-9 Hub



图 1-10 交换机

采用上面介绍的设备我们就可以组成一个局域网了。但随着微型计算机的普及以及网络应用的快速发展,在更大范围内实现相互通信和资源共享已成为必然,下面我们就来介绍广域网互联所必需的路由器设备,其实物图如图1-12所示。路由器是用来在多个网络和介质之间实现网络互联的一种设备,是一种比交换机更复杂的网络互联设备。它的主要功能可以拆分成“路由”部分和“交换”部分,“路由”部分负责为数据包进行选路(静态路由和动态路由),“交换”部分负责将数据包进行转发。路由器的每一端口都是一个单独的子网,每个端口属于一个广播域,因此路由器可以对广播进行隔离。



图 1-11 网络互连



图 1-12 路由器

1.3 OSI 和 TCP/IP 参考模型

在现实生活中人与人之间的交流(通信)需要语言(协议),只有说同样语言的人才能正常交流。在网络世界中,计算机之间的通信也是一样,它们必须遵守一些约定即通信协议,

只有采用相同协议的节点才可以相互通信。

由于节点之间的联系可能是很复杂的，因此，在制定协议时，一般是把复杂成分分解成一些简单的成分，再将它们复合起来。最常用的复合方式是层次方式，即上一层可以调用下一层，而与再下一层不发生关系。通信协议的分层是这样规定的：把用户应用程序作为最高层，把物理通信线路作为最低层，将其间的协议处理分为若干层，规定每层处理的任务，也规定每层的接口标准。

1.3.1 为何要将通信协议进行分层

将通信协议分层使得整个通信协议被分为许多相对独立的模块，这样有利于实现标准化，从而降低开发和学习的复杂性，同时也有利于通信的排错。这就好比制造业的生产线一样，比如汽车的生产非常复杂，如果我们不对其进行模块（工序）划分，生产汽车那将非常困难，效率也会非常低，但现在的一条汽车生产线往往划分为非常多的工序，每道工序只承担非常单一的任务（比如上螺丝），这样每道工序需要的技能比较单一，效率可以大幅度地提高，同时如果出错也很容易定位和解决。

1.3.2 OSI 参考模型

由于世界各大型计算机厂商推出各自的网络体系结构，因而国际标准化组织 ISO 于 1978 年提出“开放系统互连参考模型”，即著名的 OSI（Open System Interconnection）参考模型。它将计算机网络体系结构的通信协议规定为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层共七层，这受到计算机界和通信业的极大关注。1984 年该模型成为了网络通信的国际标准，作为解释网络上数据从一个节点传递到另一节点的概念模型。

OSI 模型是一种从概念上分层的模型，用于讨论和理解实际网络中所使用的协议栈。目前应用最广的协议栈 TCP/IP 以及 AppleTalk 和 IPX/SPX 都可以和 OSI 模型栈中的各层协议相参照，这样有助于了解它们的工作机制。

OSI 模型对网络通信中许多非常重要的事件提出了规范，对各种网络处理过程概括出了基本规则：

（1）数据如何翻译成与网络结构相适应的格式。当我们发一封电子邮件或一个文件给另一台计算机时，其实是在与电子邮件客户端或 FTP 客户端之类的应用程序打交道。通过这种应用程序所传送的数据必须以一种更一般的格式才能送到网络上并到达接收者。

（2）PC 以及其他网络设备如何建立彼此通信。从 PC 上发送数据时，必须有一种机制能在发送方与接收方之间建立通信，这和我们拿起电话打电话很相似。

（3）数据在设备之间如何发送以及如何排序和错误检测。当计算机之间建立起了会话通信后，必须有相应规则来控制如何在它们之间传递数据。

（4）信息包的逻辑地址如何转化为网络提供的实际物理地址。计算机网络会使用诸如 IP 地址之类的逻辑地址，而这些地址必须转化为网卡中的实际硬件地址（MAC 地址）。

OSI 模型提供了上述所讨论的各种机制和规则。理解 OSI 模型的各层不仅有助于洞察各种实际的网络协议，也可以通过各种概念化的框架更好地理解诸如调制解调器、交换机以及路由器等各种复杂的网络设备。

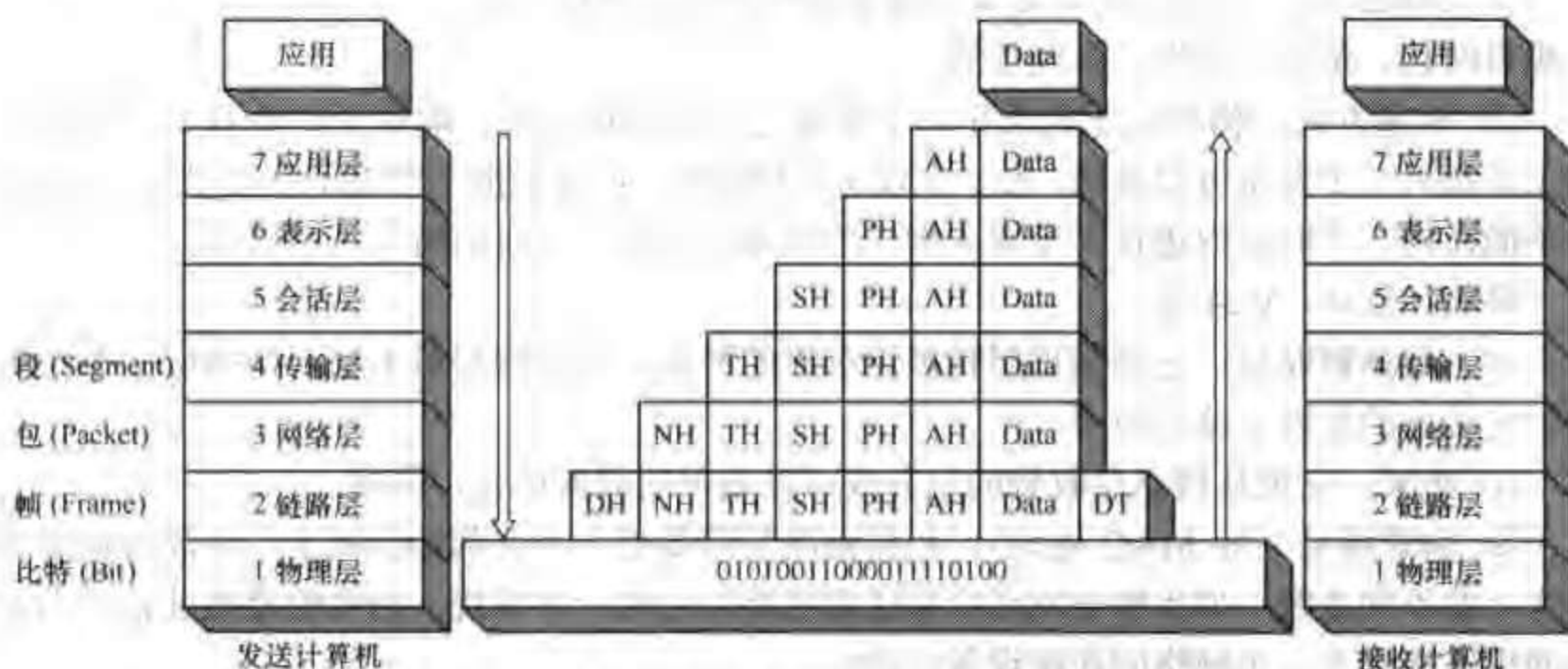
在我们讨论协议栈中的每一层之前，我们有必要来看一看数据在 OSI 模型中运动时到底

发生了什么事情, 比如, 一个用户准备将一封电子邮件发给网络上的另一个用户。发邮件的用户首先要利用电子邮件的客户端程序 (比如 Outlook 或 Foxmail) 作为编辑邮件信息并发送的界面工具, 这项工作发生在应用层。当数据离开应用层后 (此层会将一个头信息附加到数据包上), 它将穿过 OSI 协议栈的各层, 每层会分别提供一部分与建立通信链接相关的信息, 并对数据进行一定的格式加工。

无论每层的功能如何, 它都会将头信息附加在数据上 (物理层除外), 即在第 6、5、4、3、2 层要给数据加上首部, 尾部则在第 2 层才加上。数据最终到达发送方计算机的物理层 (即真正连接计算机的网络介质, 如双绞线和光纤等), 并在物理介质上传输到其终点, 即接收方的计算机上。

接收方计算机的物理层首先接收到数据, 然后以和发送方相反的顺序遍历 OSI 协议栈, 数据每经过一层, 相应层的头信息和尾部就被从数据上剥掉, 当数据最终到达应用层时, 接收方将用他的电子邮件客户端程序 (如 Outlook 或 Foxmail) 来阅读发来的邮件信息。

OSI 对等通信模型如图 1-13 所示。



注: AH、PH、SH、TH、NH、DH: 分别表示应用层、表示层、会话层、传输层、网络层、数据链路层的数据包头。
DT表示数据链路层的包尾。

图 1-13 OSI 对等通信模型

在发送设备和接收设备中数据和信息通过各层向上传送之所以是可能的, 是因为在各层每二个相邻层之间有一个接口。每一个接口定义了一个层必须向其上层提供什么信息和服务。定义清楚的接口和层功能使得网络可以模块化。

下面我们就对 OSI 模型 (如图 1-14 所示) 中的各层进行详细的介绍。

第 1~3 层可视为网络支持层, 其功能是在物理方面将数据从一个设备传送到另一个设备。第 5~7 层可以看成是用户支持层, 这些层使得一些相关的软件系统有了互操作性, 它是用软件来实现的。第 4 层是传输层, 它将上面两个组链接起来, 使得低层所发送的是高层可使用的形式。在七层参考模型中的各个层之间的关系为服务关系, 每一层均接收来自与其相邻的下一层的服务, 同时为与其相邻的上一层提供服务功能。大量的数据通过分割和各层的封装 (在上一层的数据单元上加上本层的数据包头或尾), 在传输层形成段 (Segment), 在网络层形成包 (Packet)、在数据链路层形成帧 (Frame)、在物理层以二进制位 (Bit) 传输。

(1) 物理层：最重要的一点，在物理媒体中传送的是比特流，物理层规定的是以下内容。

① 接口和媒体的物理特性：定义在设备与传输媒体之间接口的特性，它还定义传输媒体的类型。

② 比特的表示：数据由比特组成（0 和 1 的序列），比特必须经过编码变成信号（电或光），物理层定义编码的类型，即 0 和 1 怎样变成信号。

③ 数据速率：传输速率（即每秒发送的比特数）也在物理层定义。

④ 比特的同步：发送器和接收器不仅要使用同样的比特速率，而且还要在比特级进行同步，即二者的时钟必须是同步的。

⑤ 线路配置：在点对点配置中，二个设备通过专用链路连接在一起，在多点配置中，若干个设备共享一条链路。

⑥ 物理拓扑：物理拓扑是定义设备是如何连接到网络上的。一般有网状、星形、环形、总线形等。

⑦ 传输方式：物理层还定义在二个设备之间的传输方式，即单工、半双工、全双工。单工是指只有一个设备可以发送，另一个设备只能接收。半双工指二个设备都可以发送和接收，但不能在同一个时间内进行。全双工指二个设备可在同一个时间内发送和接收。

举例：V.35、V.24 等。

(2) 数据链路层：它将物理层转换为可靠的链路，使物理层对上层（网络层）不产生差错。它关心的是以下内容。

① 组帧：它把从网络层收到的包分成可以处理的数据单元，即帧。

② 物理编址（如 MAC 地址）：数据链路层需要把一个首部加到帧上，才能将帧发送给网络上的不同系统。如果帧是发送给发送器网络以外的一个系统，则接收器地址就应当是将本网络连接到的下一个网络的连接设备的地址。

③ 流控制：如果接收器接收数据的速率小于发送器产生数据的速率，那么数据链路层就应该使用流控制预防接收器超负荷运转。

④ 差错控制：此层增加了一些措施来检测和重传受损伤的帧或丢失的帧，它还有防止出现重复帧的机制，差错控制通常是在帧的最后加一个尾部来实现的。

⑤ 接入控制：当 2 个或更多个设备连接到同一条链路时，数据链路层就必须在任意指定的时刻决定哪一个设备对链路有控制权。

举例：HDLC、PPP 等。

(3) 网络层：该层负责将一个分组从源站发送到目的站，这可能要跨越多个网络。数据链路层监督在同一个链路（网络）上的两个系统之间分组的交付，而网络层则是确保每一个分组能够从其起点到达目的地。它关心的是以下内容。

① 逻辑编址（如 IP 地址）：由数据链路层实现的物理编址在本地处理寻址问题，当穿越两个以上网络时，就需要对从上层来的分组增加一个首部，来帮助我们区分源系统和目的系统，其中包括发送器和接收器的逻辑地址。

② 路由选择：当许多独立的网络或链路互连在一起组成互联网络时，这些连接设备（叫做

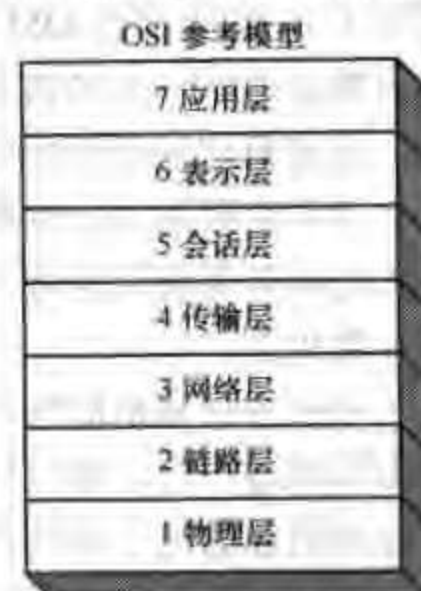


图 1-14 OSI 模型

路由器或三层交换机)就要使用所选择的路由或交换方法,将分组数据送交到它们的目的站点。

举例:IP、IPX等。

(4) 传输层:负责将完整的报文进行从源到目的的交付,网络层监督单个分组的端到端交付,不考虑分组之间的关系,将每一个分组视为一个独立的报文来处理,而运输层要确保整个的报文原封不动地按序到达,并负责监督从源到目的这一级的差错控制和流控制。它关心的是以下这些内容。

① 服务点编址(PORT):在传输层给分组加上一种类型的地址,叫服务点地址(或叫端口地址)。网络层将每一个分组送到指定的计算机,传输层则将完整的报文送到该计算机的相应程序上。

② 分段与重装:一个报文要划分成若干个可传输的报文段,每个报文段包括一个序号,这些序号使传输层能够将报文在它到达目的地时重装起来,能够识别在传输时丢失的分组并替换为正确的分组。

③ 连接控制:传输层可以是无连接的(如UTP),也可以是面向连接的(TCP)。无连接的传输层将每个报文段看成是独立的数据报,并将此报文交付给目的机器上的传输层;面向连接的传输层在发送分组前,先要和目的机器建立一条连接,当全部数据传送完后,再释放连接(注:无连接可类比邮件,面向连接可类比打电话)。

④ 流控制:在传输层的流控制是在端到端的意义上实现的,而不是在一条链路上实现的(区别于数据链路层的流控制)。

⑤ 差错控制:发送端的传输层必须保证整个的报文到达接收端的传输层是没有差错的,纠错通常是通过重传来完成,在传输层的差错控制是在端到端的意义上实现的,而不是在一条链路上实现的(区别于数据链路层的差错控制)。

举例:TCP、UDP等。

(5) 会话层:它建立和维持通信系统之间的交换,并使这些通信系统同步,它是网络的对话控制器。它关心的是以下这些内容。

① 对话控制:会话层允许两个系统进入对话状态,它允许两个进程之间的通信按半双工、全双工方式进行。

② 同步:会话层允许进程将若干个检查点插入到一个数据流中。比如,如果某系统要发送一个2000页的文件,那么可以在每100页后面插入一个检查点,这样,假如在传输到756页时,计算机死机了,那么系统恢复后重传的只是701~756页,第756~2000页还是照常继续传送。

举例:RPC、NFS等。

(6) 表示层:表示层考虑的问题是两个系统所交换信息的语法和语义。它关心的是以下这些内容。

① 转换:由于不同的计算机使用不同的编码系统,所以表示层的责任就是在这些不同的编码方法之间提供互操作性,在发送器的表示层将信息从与发送器有关的格式转换为一种公共的格式,在接收的机器上的表示层将此公共格式转换为与接收器有关的格式。

② 加密:加密就是发送器将原始信息转换为另一种形式,然后将得到的这种形式的报文发送到网络上。

③ 压缩:数据压缩减少了信息中所包含的比特数。

举例：JPEG、ASCII 等。

(7) 应用层：使用户接入到网络，应用层给用户提供了接口，也提供了对许多种服务的支持。它关心的是以下这些内容。

① 网络虚拟终端：这是一个物理终端的软件版本，这个应用程序创建一个软件对远程主机的终端进行仿真。用户的计算机先与这个软件终端交谈，然后此软件终端再和主机交谈，远程主机相信它正在和它自己的终端交谈，因此就允许你进行注册。

② 文件传送、存取和管理：允许用户在一个远程计算机中存取文件，将文件从远程计算机读取到本地计算机来使用。

③ 邮件服务。

④ 名录服务：提供分布式数据库源，以及对各种对象和服务的共用信息的存取。

举例：FTP、E-mail 等。

1.3.3 TCP/IP 参考模型

TCP/IP (Transmission Control Protocol/Internet Protocol) 中译名为传输控制协议/国际协议，协议起初是为美国 ARPA net 设计的，目的是使不同厂家生产的计算机能在共同网络环境下运行。它涉及异构网通信问题，后发展成为 DARPA net (Internet)，要求 Internet 上的计算机均采用 TCP/IP 协议。目前 TCP/IP 实际上已经成为互联网网间通信的标准，作为 Internet 上的传输协议，它使得全球数以百万计的计算机能够相互通信。应用最广的 Windows 和 UNIX 操作系统都已把 TCP/IP 作为它的核心组成部分。正因为如此，我们有必要对 TCP/IP 进行一下全面的了解。

TCP/IP 是在 20 世纪 70 年代开发的，早于 OSI 模型 (20 世纪 80 年代)，所以 OSI 模型比 TCP/I 模型划分得更细，但它们之间还是有许多相似的地方，我们可以将这两个模型进行如图 1-15 所示的对应。



图 1-15 OSI 模型和 TCP/IP 模型的对应

1. 应用层

应用层协议提供了访问网络的各种协议及应用的用户接口。TCP/IP 协议栈中的协议处理文件传输、远程节点登录、电子邮件以及网络监控等。此层包括以下一些协议。

FTP (文件传输协议)：提供了计算机之间进行文件传输的功能。

TFTP (Trivial FTP)：是 FTP 的精简版。它不用认证 (用户名和密码) 即可进行文件的传输。在对网络设备进行操作系统的升级以及对操作系统和配置文件进行备份时，我们会用到 TFTP。

SMTP (简单邮件传输协议)：提供了计算机之间进行邮件传递的功能。电子邮件客户端 (如 outlook) 支持 SMTP 可用于发送电子邮件。

SNMP (简单网络管理协议)：它是一个与网络管理相关的协议，能通过 SNMP 代理 (一种对网络进程进行监控的软件) 来收集与网络相关的数据。许多网络管理软件都支持 SNMP 协议，如 Ciscoworks2000、HPOpenview 等。

Telnet: 它是一个终端仿真的协议, 允许本地计算机与远程计算机或其他网络设备(如路由器、交换机等)连接起来, 本地作为一个虚拟的终端, 可以对远程的计算机或其他设备进行配置。

2. 传输层

传输层协议提供了数据在收发计算机之间传输时的流量控制和连接的可靠性。此层从应用层获得数据, 并着手准备数据在网上的传输。此层包括以下两个协议。

TCP (传输控制协议): 它是一个面向连接的协议, 提供收发计算机上用户应用程序间的虚链路(类似电话连接)。TCP 从应用层协议取得数据, 将其分段, 并确保其在接收方的正确组合。TCP 要求收发计算机之间建立同步连接, 这就使得在数据包中必须添加相应的序号和同步控制位, 因此 TCP 会增加网络的额外负载。

UDP (用户数据报协议): 它是一个无连接的传输协议, 提供了应用层协议间的连接, 但不要求像 TCP 那样的应答和同步机制。UDP 和邮件的传输很相似(发送方写上接收方的地址, 然后发送, 但不保证一定收到)。TFTP 和 SNMP 协议是用 UDP 来传输的。

TCP 和 UDP 都采用端口号来把信息传到上层的不同应用协议, 端口号用来识别同一时间内通过网络的不同会话。TCP 和 UDP 都保留一些端口, 应用程序不能随便使用, 如图 1-16 所示。端口号的指定范围是:

- 低于 255 的端口号用于公共应用;
- 255~1023 的端口号被指定给各个公司;
- 高于 1023 的端口号未做规定。

3. 网络层

网络层负责逻辑网络间数据的路由, 并向上层提供地址系统。此层还定义了数据在网络上传输的数据包格式。网络层一个最重要的协议就是众所周知的 IP 协议。此层的其他协议基本都是为 IP 地址系统服务的。网络层另外的一个重要工作就是将逻辑地址解析为实际的硬件地址(将 IP 地址解析为 MAC 地址)。此层包括以下一些协议。

IP (Internet Protocol): 它从上层获得数据, 然后将它们分割为数据包, 对每一个包都标识上接收方设备的 IP 地址, IP 在接收方将数据包重新组合起来, 送到上一层协议去处理。IP 是无连接的协议, 它对数据包的内容不感兴趣, 它惟一的愿望就是对数据包进行编址并将它送到目的地。

ARP (Address Resolution Protocol, 地址解析协议): 当 IP 准备好数据包时, 它已知道收、发计算机的 IP 地址(它从上层协议中, 比如 Telnet 或 SMTP, 获得这些信息); 为了将数据包发送出去, IP 还必须知道接收方的 MAC 地址, 因为它必须向网络访问层协议(如以太网协议)提供这些信息。ARP 的作用就是提供了将 IP 地址解析为实际的硬件地址(MAC)的机制。ARP 发出带有接收方计算机 IP 地址的广播, 并要求该计算机以硬件地址予以回答。ARP 的工作原理如图 1-17 所示。

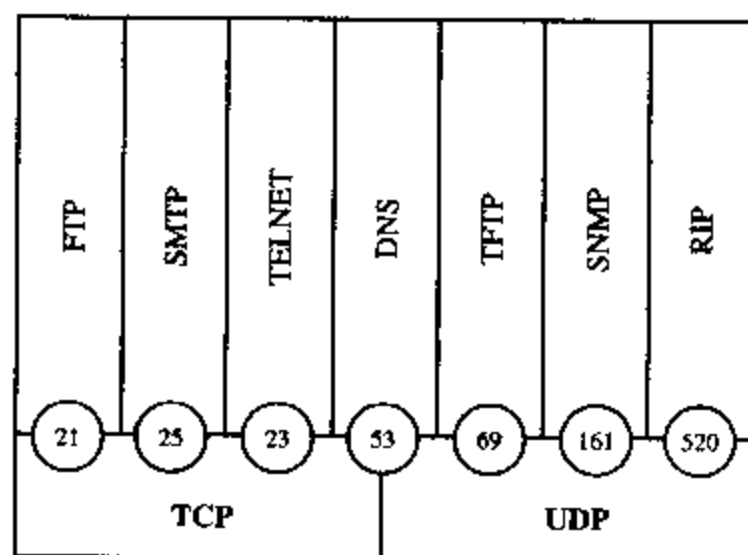


图 1-16 常用 TCP 和 UDP 端口号

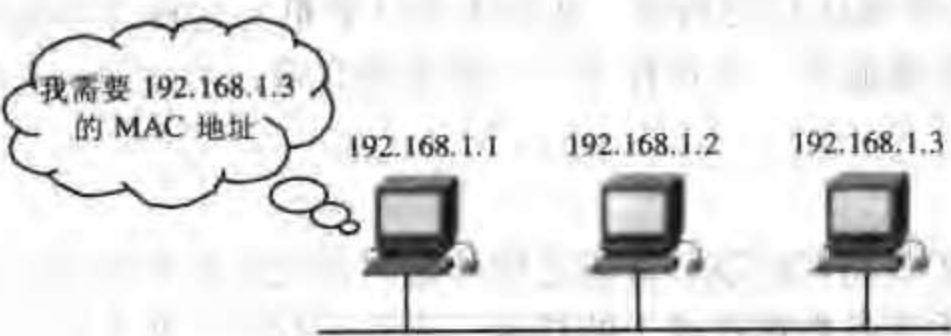


图 1-17 ARP 工作原理

ICMP (Internet Control Message Protocol)，中译名为因特网控制报文协议，此协议是用来对报文提供差错和控制消息的。例如，如图 1-18~1-19 所示，我们经常用 ping 来检测网络是否通畅，用 traceroute 来对数据包进行跟踪，它们采用的都是 ICMP 协议。



图 1-18 ICMP 目的不可达

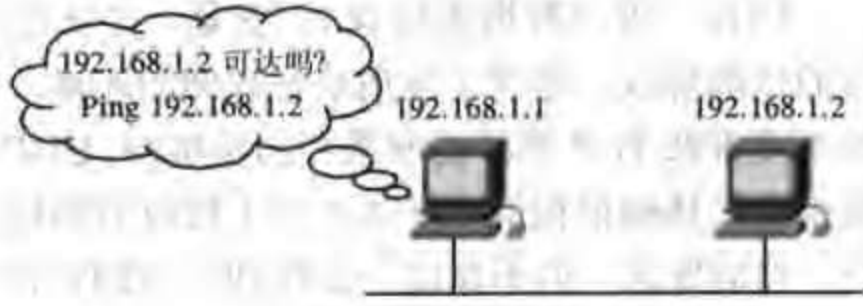


图 1-19 ping 的工作原理

4. 网络接入层

网络接入层协议从网络层获得数据包，并将数据以特定的帧格式包装，以比特流方式交给物理传输介质。

1.4 局域网基础知识

1. 什么是局域网

局域网 (Local Area Network，简称 LAN)：一般在几十米到几公里范围内，一个局域网可以容纳几台至几千台计算机，如图 1-20 所示。局域网具有如下特性：



图 1-20 传统局域网技术

- (1) 局域网分布于比较小的地理范围内。因为采用了不同传输能力的传输媒介，所以局域网的传输距离也不同。
- (2) 局域网往往用于某一群体，比如一个公司、一个单位、某一幢楼、某一学校等。

按照网络的拓扑结构和传输介质,局域网有以太网(Ethernet)、令牌环网(Token Ring)、光纤分布式数据接口(FDDI)、异步传输模式(ATM)等多种,其中最常用的是以太网。

2. 以太网和 IEEE 802.3 标准

以太网(Ethernet)是世界上用的最多的网络结构,它采用 CSMA/CD(带冲突检测的载波侦听多路访问)的方法访问网络。这种网络访问策略的基本思想是:网络上的每个节点(计算机)侦听网络,当网络空闲时,节点才能将信息发送到网上去,如果有多个节点侦听到网络是空闲的而同时发送信息,就会产生冲突,一旦检测到冲突,所有节点都停止发送,直到再次侦听到网络是空闲的才再次发送,为了减少再次发生冲突的机率,不同节点在重传前会等待一个不同的退避时间(Backoff Time),最终一个节点将获得传送机会,从而实现其信息的传递。

以太网通常采用总线形或星形拓扑结构,早期的同轴电缆构建的多为总线形网络,目前已基本淘汰。现在流行的以太网是用非屏蔽双绞线和交换机构建的星形网络。

电子与电气工程师协会(IEEE)制定了以太网体系的规范,即 IEEE 802.3 规范。

3. 局域网常用设备

集线器(Hub):主要指共享式集线器。它处于 OSI 模型的物理层,相当于一个多端口的中继器。集线器实物图如图 1-21 所示。

交换机(Switch):指交换式集线器,其实物图如图 1-22 所示。它处于 OSI 模型的数据链路层,因此它可以识别 MAC 地址,通过 MAC 地址来进行数据的交换。随着交换机技术的不断发展,现在出现了带路由功能的交换机(三层交换机),它不但可以实现网络分段(VLAN 划分)用以隔离广播,而且可以像路由器一样,识别 IP 地址,完成不同网段之间的互通,甚至可以运行各种路由协议(RIP、EIGRP、OSPF 等)。



图 1-21 集线器



图 1-22 交换机

1.5 广域网基础知识

1. 什么是广域网

广域网(WAN, Wide Area Network):广域网是将分布在各地的局域网络连接起来的网络,是“网间网”(网络之间的网络)。广域网具有如下特性:

- (1) 广域网的范围非常大,可以跨越国界、洲界,甚至全球范围。
- (2) 广域网是网络的公共部分,在我国广域网一般需租用电信部门的线路搭建而成。

2. 我国主要的广域网链路

公用交换电话网(PSTN, Public Switched Telephone Network):速度 9600bit/s~56kbit/s,需要异步 Modem 和电话线,投资少,安装调试容易,常常用作拨号访问方式。现在随着网络的发展,和人们对网络带宽的要求越来越高,PSTN 更多的是被应用到了作为主要链路的

备份链路。当然，由于 PSTN 是分布最为广泛的网络，目前还有大量的用户采用 PSTN 拨号的方式访问 Internet（比如 163、169 等）。

综合业务数字网（ISDN, Integrated Service Digital Network）：128kbit/s 的基本接口，使用普通电话线但需要电信提供 ISDN 业务，数字传输，来电显示，拨通时间短（3s），费用比 PSTN 高，同时许多地方没有开通 ISDN 业务。

非对称数字用户环路（ADSL, Asymmetrical Digital Subscriber Loop）：ADSL 技术是运行在原有普通电话线上的一种新的高速宽带技术，它利用现有的一对电话铜线，为用户提供上、下行非对称的传输速率（带宽）。非对称主要体现在上行速率（最高 640kbit/s）和下行速率（最高 8Mbit/s）的非对称性上。上行（从用户到网络）为低速的传输，可达 640kbit/s；下行（从网络到用户）为高速传输，可达 8Mbit/s。它最初主要是针对视频点播业务开发的，随着技术的发展，逐步成为了一种较方便的宽带接入技术，为电信部门所重视。

DDN 专线（Leased Line）：速度为 64kbit/s~2.048Mbit/s（E1 标准），需要配同步 Modem，有 EIA/TIA 232（V.24）和 V.35 两种标准；点对点的连接方式，结构不够灵活。广泛应用在企业广域网和 Internet 接入上，在我国的使用非常普遍。

X.25 网：速度为 9600bit/s~64kbit/s，比较古老的方式，主要用在早些年的银行和电信网络，现在应用越来越少；采用冗余校验纠错，可靠性高，但速度慢，延迟大。

帧中继（Frame Relay）：替代 X.25，减少了冗余校验纠错，速度为 64kbit/s~2.048Mbit/s（E1 标准）；一点对多点的连接方式，分组交换；独特的 **Bursty** 技术（在传输信息量大的情况下可以超越传输线速度）；目前大多数城市都开通了 Frame Relay 服务。

数字电路：数字电路业务是一种直接在电信传输网上进行数字信号传送的业务，是基于准同步数字传输网络（PDH）、同步数字传输网络（SDH）等先进光纤数字传输技术组建的宽带核心传送网络，利用各种新的传输技术进行高速数字信号传送的业务。该业务可向用户提供 2 Mbit/s 至 2.5Gbit/s 各种传输速率的全透明电路，为客户提供高效的信息传送通路。数字电路接入是指直接通过电信传输网络进行数字传输的。数字电路为用户提供端到端的全透明高速数字信号传送服务，通信速率可根据需要进行选择，有 2Mbit/s、8Mbit/s、34Mbit/s、155Mbit/s、622Mbit/s、2.5Gbit/s 等速率；数字电路是一种全透明的物理通道，支持数据、语音、图像等多种业务，对客户通信协议没有任何要求，客户可自由选择网络设备及通信协议；数字电路传输质量高，网络时延小，实时性强；数字电路技术成熟，拥有完善网络管理监控性能和各种网络保护机制，具有很高的安全可靠性能；数字电路传输网络（PDH、SDH）覆盖面广、可通达国内主要城市；数字电路价格低，性能价格比优。

异步传输模式（ATM, Asynchronous Transfer Mode）：异步传递方式是 ITU-T 定义的一种网络技术，它采用固定长度的信元，按照面向连接的方式进行工作。连接是指虚连接，传输时的数据形式是固定长度的短信元，数据按照统计复用的方式传输，因而传输效率更高。通常，速率范围从 2Mbit/s 到 622Mbit/s。主要的应用包括高速局域网互联、高质量的电视会议、远程教学、远程医疗、远程协同工作、多媒体通信和视频点播等各种业务。ATM 的应用与它所能提供的 QoS 密切相关。

3. 广域网常用设备

路由器（Router）：广域网的通信过程与邮局中信件传递的过程类似，都是根据地址来寻找到达目的的路径，这个过程在广域网中称为“路由（Routing）”。路由器负责不同广域网中

各局域网之间的地址查找(建立路由),信息包翻译和交换,实现计算机网络设备与电信设备电气连接和信息传递。因此路由器通常具有广域网和局域网两种网络通信接口。路由器实物图如图1-23所示。

调制解调器(Modem):作为网络设备与电信通信线路的接口,用来在电话线上传递数字信息。分为同步和异步两种,分别用来与路由器的同步和异步串口相连接。Modem的实物图如图1-24所示。



图 1-23 路由器



图 1-24 基带猫

广域网中的电信通信服务由电信局提供,路由器只提供相应的接口。路由器的广域网通信接口分为两大类,即同步串口(SyncSerial Port)和异步串口(AsyncSerial Port);Leased Line、Frame Relay、X.25 使用路由器的同步串口(Serial Port),ISDN 使用路由器的 ISDN BRI(属同步口),PSTN 使用路由器的异步串口。

1.6 小 结

本章我们简要地介绍了一下有关网络基础方面的一些知识,包括网络互连的基础、OSI 和 TCP/IP 的参考模型以及有关局域网和广域网的一些基础知识。下面我们做一下简单的总结。

计算机网络是指将地理位置不同,具有独立功能的多个计算机系统用通信设备和线路连接起来,并借功能完善的网络软件(网络协议、网络操作系统等)实现资源共享的系统。计算机网络有多种分类方式,例如按地理位置可分为局域网、广域网和城域网;按网络拓扑结构可分为星型网络、环型网络和总线型网络结构,按传输介质可分为有线网络(同轴电缆、双绞线、光纤等)、无线网络(微波、红外线、无线电等电磁波),按服务对象可分为企业网、校园网等。网络传输的介质主要包括同轴电缆、双绞线、光纤和无线。为了简化网络通信的过程,我们将整个通信的过程进行分层,协议分层使得整个通信协议被分为许多相对独立的模块,这样有利于实现标准化,从而降低开发和学习的复杂性,同时也有利于网络的排错。我们在学习网络的过程中,接触最多的有两个通信协议分层的参考模型,一个是 OSI 模型,另一个是 TCP/IP 参考模型。应该说 OSI 更像一种概念上的模型,但具体工作中我们接触最多的应该是 TCP/IP 协议栈的参考模型,因为它涵盖了在我们许多工作和学习中会用到的具体的通信协议,因此更具有实际的意义。参考模型的各层都定义了相互独立功能,我们应该清楚地了解这些功能,同时我们应该清楚构成网络的主要组件在通信模型中的位置,如集线器位于物理层,交换机位于链路层,路由器位于网络层等;同时我们应该对 TCP/IP 协议栈中的一些具体协议有所了解,尤其是 TCP、UDP、ICMP、ARP,因为掌握这些协议对我们理解网络通信和将来对网络进行排错有至关重要的帮助。

第2章 网络设备选购指南

本章将涵盖下列有关网络设备选购方面的关键主题：

- 交换机选购指南
- 路由器选购指南
- 防火墙选购指南
- Cisco 交换机产品
- Cisco 路由器产品
- Cisco 防火墙产品
- Cisco 网络产品配置案例

通过对本章的学习，希望大家能对以下一些方面有所了解：

- (1) 交换机包括哪些指标参数，如何选购交换机；
- (2) 路由器包括哪些指标参数，如何选购路由器；
- (3) 防火墙包括哪些指标参数，如何选购防火墙；
- (4) Cisco 公司的交换机产品有哪些；
- (5) Cisco 公司的路由器产品有哪些；
- (6) Cisco 公司的防火墙产品有哪些；
- (7) 如何根据用户的需求，合理地进行产品选型。

2.1 交换机选购指南

在选购交换机之前，用户首先要明确自己的业务需求和未来的发展规划，找到一个适合自己的评判准则，也就是说在名目繁多的各种指标和参数之中要有一个衡量的尺度。总体上看，下述指标是用户进行选购时要参考的一些基本指标。

1. 设备基本指标

(1) 网络接口类型

网络接口提供不同网络设备之间的互连，作为骨干以太网交换机，对 10M/100M/1000Mbit/s 端口的支持是必需的，10 吉比特以太网可以作为一个选项，根据网络的业务和未来发展规划来确定是否必备。目前的骨干以太网交换机大都支持一些广域网端口，如 ATM、POS 等，并提供城域网网络连接。由于骨干交换机在城域网的作用越来越重要，对 CWDM 技术的支持也成为设备选型时的重要参考。通常，网络的核心交换机需要具有吉比特端口，接入层交换机往往是 100Mbit/s 以太网端口加上 1~2 个吉比特上连端口。

(2) 用户可用槽数

该指标指模块化交换机中除引擎等必要系统板及/或系统板专用槽位外,用户可以使用的插槽数。根据该指标以及用户板端口密度,可以计算出该交换机所支持的最大端口数。

(3) 端口密度

该指标体现交换机制作的集成度。由于交换机体积不同,该指标应当折合成机架内每英寸端口数。但是考虑应直观和使用方便,通常可以使用交换机对每种端口支持的最大数量来替代。

2. 功能指标

(1) VLAN 划分

支持的 VLAN 数量有多少。

(2) 堆叠

是否支持堆叠,最多可以堆叠几台交换机。一般在选择接入交换机时会考察此指标。

(3) 单播和组播协议支持

核心交换机往往须具备路由功能,支持包括单播路由协议和多路广播路由协议。目前存在很多路由协议,选择适合自己的网络协议非常必要。作为核心交换机应该支持的路由协议包括 RIPv1、RIPv2、OSPF,这些路由协议应用比较广泛,几乎所有的厂商都支持这几种协议,并且能够很好地互通。其他路由协议根据具体的需求来确定是否必需。组播路由协议包括 IGMP、DVMRP、PIM-SM、PIM-DM 等,较为流行的是 DVMRP、PIM-SM。

(4) 可网管

可网管交换机是指能够通过软件手段(如浏览器)进行诸如查看交换机的工作状态、开通或封闭某些端口等管理操作的交换机。

对一个小型局域网来说,一般不必采用可网管的交换机,因为网络管理的任务相对简单。对一个大中型局域网来说,能够远程监视和控制交换机尤其是中心交换机,对于保障网络的安全具有重要的实用价值。

3. 性能指标

(1) 背板带宽(吞吐量)

交换机实际上是一台特殊用途的计算机,内部也有 CPU、内存和主板,只不过这些部件是专门为数据交换设计的。背板带宽类似于电脑主板上的总线,是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。一台交换机的背板带宽越高,处理数据的能力就越强,同时价格也越高。背板带宽的单位是比特每秒(bit/s)。

(2) 包转发率

交换机的包转发率充分地反映了该设备转发数据包的能力,是交换机三层性能的主要衡量参数。包转发率的单位是包每秒(Packet/s)。

(3) 支持的 MAC 地址数量

交换机能够记住连接在端口的计算机网卡的 MAC 地址,但是有一定的数量限制。现在的中小型交换机都能支持到 2×2^{10} 个以上的 MAC 地址,也就是说,这个交换机最多可以通过 Hub 扩展端口连接 2024 台电脑。但是能够达到这个规模的局域网,已经是大型局域网,肯定不会只用一台交换机的。因此现在一般交换机支持的 MAC 地址数量足以满足实际的需要。

(4) 服务质量保证

服务质量保证是解决网络拥塞时确保高优先级的流量获得带宽的技术。由于网络的关键

应用越来越多，尤其是多媒体应用的大量涌现，服务质量保证技术的应用显得非常必要，并且要求交换机支持硬件优先级队列的数量越来越多，目前业界达到的最多的硬件队列是 8 个。仅支持 2~3 个硬件优先级队列的产品已不能满足用户和业务的需求。

说明：目前很多人对交换机的背板、吞吐量和线速交换的概念理解得不是很清楚，对它们之间的关系也缺乏了解，而这 3 个名词又频繁出现，所以下面我们就对它们进行一下解释。

背板带宽，是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。一台交换机的背板带宽越高，所能处理数据的能力就越强，但同时设计成本也会上去。在选购交换机时，我们如何去考察一个交换机的背板带宽是否够用呢？显然，通过估算的方法是没有用的，我认为应该从两个方面来考虑。

① 所有单端口容量×端口数量之和的 2 倍应该小于背板带宽，才可实现全双工无阻塞交换，证明交换机具有发挥最大数据交换性能的条件。

比如 Cisco 公司的 Catalyst2950G-48，它有 48 个 100Mbit/s 端口和 2 个吉比特端口，它的背板带宽应该不小于 13.6Gbit/s，才能满足线速交换的要求。

$$(2 \times 1000 + 48 \times 100) \times 2 \text{ (Mbit/s)} = 13.6 \text{ (Gbit/s)}$$

② 满配置吞吐量 (MPacket/s) = 满配置 GE 端口数 × 1.488MPacket/s，其中 1 个吉比特端口在包长为 64Byte 时的理论吞吐量为 1.488MPacket/s。例如，一台最多可以提供 64 个吉比特端口的交换机，其满配置吞吐量应达到 $64 \times 1.488 \text{MPacket/s} = 95.2 \text{MPacket/s}$ ，才能够确保在所有端口均线速工作时，提供无阻塞的包交换。如果宣称的吞吐量达不到 95.2MPacket/s，那么用户有理由认为该交换机采用的是有阻塞的结构设计。

当我们选择交换机时，一般会通过厂商提供的背板带宽和吞吐量结合该交换机的端口数量，来计算一下，看看它是否满足线速交换的要求，对于核心交换设备来说，线速交换是非常重要的。例如，Cisco 公司的 Catalyst4506，配置 IV 代引擎 (WS-X4515)，其宣称的背板带宽为 64Gbit/s，满配置时的吉比特端口为 32 个，根据其宣称的背板带宽 64Gbit/s 以及它满配置时的端口数量 32，我们可以得出为了确保其所有端口均能满足线速交换的要求，它的吞吐量不能低于 47.616MPacket/s ($32 \times 1.488 = 47.616$)。Cisco 宣称的吞吐量为 48MPacket/s，因此 Catalyst4506 配置 IV 代引擎能够满足线速交换的要求。

(补充一下 1.488 的由来：具体的数据包在传输过程中会在每个包的前面加上 64 个 Preamble (前导符)，然后在每个包之间会有长 96bit 的 IFG (帧间隙)，也就是原本传输一个 64Byte 的数据包，虽只有 512 (64×8) bit，但在传输过程中实际上会有 $512 + 64 + 96 = 672 \text{bit}$ ，也就是说，这时一个数据包的长度实际上是 672bit。吉比特端口线速包转发率 = $1000 \text{Mbit/s} / 672 = 1.488095 \text{MPacket/s}$ ，约等于 1.4881MPacket/s，百兆端口线速包转发率 = $100 \text{Mbit/s} / 672 = 0.1488095 \text{MPacket/s}$ ，约等于 0.14881MPacket/s。)

4. 可靠性指标

以太网交换机的可靠性基本可以从下面几个方面来评判：

- (1) 核心交换机是否支持关键模块的冗余，即电源、风扇、交换矩阵、引擎。
- (2) 链路层是否具备弹性恢复的功能，如 Spanning Tree 协议，多种形式的链路捆绑等。
- (3) 在网络层是否支持动态路由协议，是否支持等价多路由功能，是否支持网关冗余协议 (VRRP、HSRP) 等。

以上包括了所有交换机的一些通用指标，在品目繁多的指标中，我们往往只须根据几个

指标来进行选择,其中,最重要的指标就是背板带宽、包转发率和端口数量。下面我们针对企业网中不同层次的交换机做一个简单介绍。

(1) 核心层交换机

企业核心层交换机的背板带宽基本上在几十 Gbit/s 以上,包转发速率在几十 MPacket/s 以上,可扩展百兆比特端口为 300 个左右,可扩展吉比特端口 100 左右。交换层数最好是 2/3/4 层以上,一般 2/3 层是必备的,另外我们还要考查各交换机提供的接口模块型号是否较为丰富。核心层交换机的典型代表是 Cisco 公司的 Catalyst6500 系列交换机,它的背板带宽可达 720G,包转发率 400MPacket/s (配置 SUP720 引擎)。

(2) 汇聚层交换机

汇聚层交换机的背板带宽基本上在几十 Gbit/s 以上,包转发速率在几十 MPacket/s 以上,总体指标应比核心层略低。汇聚层交换机较为重要的性能还包括:要有三层以上交换功能和较多的 VLAN 数。汇聚层交换机的典型代表是 Cisco 公司的 Catalyst4500 系列交换机,它的背板带宽可达 64G,包转发率 48MPacket/s (配置 4 代引擎)。

(3) 接入层交换机

接入层交换机的背板带宽基本上为几个 Gbit/s,包转发速率为几个 MPacket/s。接入层交换机一般支持 VLAN 的划分,但不支持第三层功能,VLAN 之间的互通需要通过汇聚层或核心层交换机来实现。如今的接入层交换机一般具有吉比特铜缆或吉比特光纤向上级联扩展端口,以便能在接入层与核心层或与汇聚层之间实现吉比特互联。接入层交换机的典型代表是 Cisco 公司的 Catalyst2950 系列交换机,它的背板带宽根据具体型号的不同可从 8~13.6Gbit/s,包转发率从 6.6~10.1MPacket/s。

说明:以上的分层主要是针对中大型企业网,对于小型企业而言,可能核心层、汇聚层和接入层的功能都集中到一台设备上。

注意,考核一个骨干交换机不能简单地从几个数字上便得到结论,企业应当明确网络应用、业务,分析对网络的需求,有针对性地考核网络设备,从而建设一个稳定、高性能、易管理的网络。

2.2 路由器选购指南

和选购交换机一样,在选购路由器的时候,用户首先也要明确自己的业务需求和未来的发展规划,找到一个适合自己的评判准则,只有在对自己的需求非常明确的前提下,对各种参数的对比才更有针对性。下面,我们就对路由器的一些常用的参数进行一下介绍。

1. 设备基本指标

(1) 网络接口类型

列举路由器能支持的接口种类。这主要是体现路由器的通用性。常见的接口种类有:通用串行接口,10、100、1000Mbit/s 以太网接口,ATM 接口(2、25、155、633Mbit/s 等),POS 接口(155Mbit/s、622Mbit/s 等),令牌环接口,FDDI 接口,E1/T1 接口,E3/T3 接口,ISDN 接口等。

(2) 用户可用槽数

该指标指模块化路由器中除 CPU 板、时钟板等必要系统板及/或系统板专用槽位外，用户可以使用的插槽数。根据该指标以及用户板端口密度可以计算该路由器所支持的最大端口数。

(3) 端口密度

该指标体现路由器制作的集成度。由于路由器体积不同，该指标应当折合成机架内每英寸端口数。但是出于直观和方便，通常可以使用路由器对每种端口支持的最大数量来替代。

2. 功能指标

(1) 路由协议支持

对各种路由协议的支持体现了一款路由器的兼容能力，它是路由器很重要的一项功能指标。常用的路由协议根据其算法的不同，分为以下两类：

① 基于距离矢量算法的路由协议：RIP、RIPv2、IGRP、EIGRP、BGP

② 基于链路状态算法的路由协议：OSPF、IS-IS

(2) 源地址路由支持，透明桥接

地址路由指路由器为数据包选择路由时不根据 IP 包的目的地地址（通常情况根据目的地地址），而根据 IP 包的源地址选路。源地址路由是情略路由的一种，一般路由器应当支持它。透明桥接是指路由器端口以透明网桥的方式工作，执行网桥的功能。不对数据包作路由检查转发，只作 MAC 情桥接。

(3) 策略路由方式

路由器除将目的地址作为选路的依据以外，还可以根据 TOS 字段、源和目的端口号（高层应用协议）来为数据包选择路径。策略路由可以在一定程度上实现流量工程，使不同服务质量的流或者不同性质的数据（语音、FTP）走不同的路径。

(4) PPP、MLPPP

PPP 是互联网协议中一个重要协议：早期的网络是通过路由器使用 PPP 点到点连接起来的，并且大多数用户采用 PPP 接入。所以凡是具有串口的路由器都应当支持 PPP 并作为首选。MLPPP 是指将多个 PPP 链路捆绑使用。

(5) PPPOE 支持

PPPOE (PPP Over Ethernet) 是一种情型的协议用于解决对以太网接入用户的认证和计费问题。与 PPPOE 类似的是 PPPOA (PPP Over ATM) 协议，使用该协议的路由器设备可以终结接入业务。当前 PPPOE 与 PPPOA 协议存在的问题是容量问题。大多数支持该协议的路由器只能处理数千个活动的会话。

(6) 组播支持

① 因特网组管理协议 (IGMP)

IGMP (Internet Group Management Protocol) 是 IP 主机用作向相邻多目路由器报告多目组成员。多目路由器是支持组播的路由器，向本地网络发送 IGMP 查询。主机通过发送 IGMP 报告来应答查询。组播路由器负责将组播包转发到所有网络中的组播成员。

② 距高矢量组播路由协议 (DVMRP)

DVMRP 是基于距离矢量的组播路由协议，基本上基于 RIP 开发。DVMRP 利用 IGMP 与邻居路由器交换数据包。

③ 协议无关组播协议 (PIM)

PIM 是一种组播传输协议,能在现存 IP 网上传输组播数据。PIM 是一种独立于路由协议的组播协议,可以工作于两种模式:密集模式和疏松模式。在 PIM 密集模式下,报文分组缺省向所有端口转发,直到发生裁减和切除。在密集模式下假设所有端口上的设备都是组播成员,可能使用组播包。疏松模式与密集模式相反,只向有请求的端口发送组播数据。

(7) VPN 支持

可能使用的协议有 L2TP、GRE、IPSec 等,并且应当关注支持 VPN 的能力。

(8) 加密方式

路由器可能在 VPN 实现中或其他条件下使用加密机制来保证安全。路由播使用 CPU 执行软件算法通常会影响转发他率。部分路由器在设计中采用硬件加密方式来提高转发效率。

(9) MPLS

MPLS 中除包括标记交换外还包括快速重路由、VPN、流量工程等高级应用。由于 MPLS 标准尚未成熟,对 MPLS 互通也应当关注。

3. 性能指标

(1) 全双工线速转发能力

路由器最基本且最重要的功能是数据包转发。在同样端口速率下转发小包是对路由器包转发能力最大的考验。全双工线速转发能力是指以最小包长(以太网 64Byte、PGS 口 40Byte)和最小包间隔(符合协议规定)在路由器端口上双向传输同时不引起丢包。该指标是衡量路由器性能的重要指标。

(2) 设备吞吐量

设备吞吐量指设备他机包转发能力,是设备性能的重要指标。路由器的工作在于根据 IP 包头或者 MPLS 标记选路,所以性播指标是每秒转发包的数量。设备吞吐量通常小于路由器所有端口吞吐量之和。

(3) 端口吞吐量

端口吞吐量是指端口包转发能力,通常使用包每秒(Packet/s)来衡量,它是路由器在某端口上的包转发能力。通常采用两个相同速率接口进行测试。但是测试接口可能与接口位置及关系相关。例如同一个插卡上端口间测试的吞吐量可能与不同插卡上端口间吞吐量值不同。

(4) 背靠背帧数

背靠背帧数是指以最小播间隔发送最多数据包不引起丢包时的数据包数量。该指标用于测试路由器缓存能力。有线速全双工转发能力的路由播该播标他无限大。

(5) 路由表能力

路由播通常依靠所建立及维护的路由表来决定如何转发。路由表能力是指路由表内所容纳路由表项数量的极限。由于 Internet 上执行 BGP 的路由播通常拥有数十万条路由表项,所以该项目也是路由器能力的重要体现。

(6) 背板能力

背板能力是路由器的内部实现。背板能力能够体现在路由器吞吐量上:背板能力通常大于依播吞吐量和测试包场所计算的值。但是背板能力只能在设计中体现,一般无法测试。

(7) 丢包率

丢包率是指测试中所丢失数据包数量占所发送数播包的比率,通常在吞吐量范围内测

试。丢包率与数据包长度以及包发送频率相关。在一些环境下可以加上路由抖动、大量路由后测试。

(8) 时延

时延是指数据包第一个比特进入路由器到最后一比特从路由器输出的时间间隔。在测试中通常使用测试仪表发出测试包到收到数据包的时间间隔。时延与数据包长相关，通常在路由器端口吞吐量范围内测试，超过吞吐量测试该指标没有意义。

(9) 时延抖动

时延抖动是指时延变化。数据业务对时延抖动不敏感，所以该指标没有出现在 Benchmarking 测试中。由于 IP 网支持多种业务，包括语音、视频业务的出现，该指标才有测试的必要性。

(10) VPN 支持能力

通常路由器都能支持 VPN，其性能差别一般体现在所支持 VPN 数量上。专用路由器一般支持 VPN 数量较多。

(11) 无故障工作时间

该指标按照统计方式指出设备无故障工作的时间。一般无法测试，可以通过主要器件的无故障工作时间计算或者大量相同设备的工作情况计算。

(12) 内部时钟精度

拥有 ATM 端口做电路仿真或者 POS 口的路由器互连通常需要同步，如使用内部时钟则其精度会影响误码率。内部时钟精度级别定义以及测试方法可参见相应同步标准。

(13) QoS 能力

① 队列管理机制

队列管理控制机制通常指路由器拥塞管理机制以及队列调度算法，常见的方法有 RED、WRED、WRR、DRR、WFQ、WF2Q 等。

② 端口硬件队列数

通常路由器中所支持的优先级由端口硬件队列来保证，每个队列中的优先级由队列调度算法控制。

③ QoS 分类方式

指路由器可以区分 QoS 所依据的信息，最简单的 QoS 分类可以基于端口。同样路由器也可以依据链路层优先级（802.1Q 中规定）、上层内容（TOS 字段、源地址、目的地址、源端口、目的端口等信息）来区分包优先级。

④ 分类业务带宽保证

该指标体现路由器是否能对各种业务等级作带宽保证，可以由队列调度算法等方式实现。

⑤ RSVP

RSVP 中文名为资源预留协议，用于端到端路径上资源的预留。使用软状态刷新，是流驱动工作方式。该协议一般不能在大规模全国范围网络上运行。但是通常的路由器都支持该协议，一些著名厂商使用该协议用于 MPLS。

⑥ IP DiffServ

区分服务是对 IP 服务质量分级，是对 QoS 的一种简化。

⑦ CAR 支持

CAR 中文名是承诺接入速率，是一种接入控制。CAR 按照与用户签订的协议，对超出承诺速率的数据包做不同处理：丢弃或标记，又称为标记颜色。

4. 可靠性指标

(1) 冗余

冗余可以包括接口冗余、插卡冗余、电源冗余、系统板冗余、时钟板冗余和设备冗余等。冗余用于保证设备的可靠性与可用性。冗余量的设计应当在设备可靠性要求与投资间折衷。

(2) 热插拔组件

由于路由器通常要求 24 小时工作，所以更换部件不应影响路由器工作。部件热插拔是路由器 24 小时工作的保障。

(3) 路由器冗余协议

路由器可以通过 VRRP 等协议来保证路由器的冗余。

5. 网管指标

网管是指网络管理员通过网络管理程序对网络上资源进行集中化管理的操作，包括配置管理、记账管理、性能管理、差错管理和安全管理。设备所支持的网管程度体现设备的可管理性与可维护性。

(1) 基于 Web 的管理

体现设备是否能够通过 Web 进行管理。通过 Web 管理比较方便，但是安全性较差，通常允许通过 Web 浏览，不允许通过 Web 作更改。

(2) 网管类型

指示网络管理所支持的类型，通常使用 SNMP 管理。

(3) 带外网管支持

带外网管的支持表示路由器能否通过带外信道管理。

(4) 网管粒度

指示路由器管理的精细程度，包括管理到端口、到网段、到 IP 地址、到 MAC 地址等粒度。管理粒度可能会影响路由器转发能力。

(5) 计费能力/协议

随着路由器进入运营商网络，计费成为必不可少的一部分。路由器必须能够支持某种计费能力和协议来计费。

6. 分组语音能力

(1) 分组语音支持方式

在企业中，路由器分组语音承载能力非常重类。在远程办公室与总部间，支持分组语音的路由器可以使电话通信和数据通信一体化，有效地节省长途话费。

当前技术环境下，分组语音可以分为 3 种：使用 IP 承载分组语音、使用 ATM 承载语音以及使用帧中继承载语音。使用 ATM 承载语音时可以分 AAL1 和 AAL2 两种。AAL1 即电路仿真，技术非常成熟但是相对成本较高；AAL2 技术较先进，但是当前 ATM 接口通常不支持。帧中继承载语音也比较成熟，相对成本较低。IP 承载语音当前较流行，在上述技术中其成本最低，但是当前 IP 网络 QoS 保证困难，通话质量较难保证。

(2) 协议支持

在 IP 承载语音中，H.323 是 ITU 标准，是当前 IP 电话网络最常用的协议栈。SIP 是 IETF

标准，其目的是将网络设备简单化，将复杂功能做到用户终端中。从 IP 网本质来看，路由器与所承载业务无关，但是路由器端口对 IP 电话协议的支持可以节约成本。

（3）语音压缩能力

语音压缩是 IP 电话节约成本的关键之一，通常可以使用 G.723 和 G.729。G.723 在 ITU-T 建议 G.723.1(1996)，语音编码器在 5.3 和 6.3kbit/s 多媒体通信传输双率语音编码器中规定。相对压缩比较高，压缩时延较大。G.729 在 ITU-T 建议 G.729 (1996)、8kbit/s 共轭结构代数码激励线形预测 (CS-ACELP) 语音编码中规定，其压缩比较低，通话质量较好。

（4）端口密度

指路由器支持 IP 电话的能力，通常以 E1 计算，一般一个 E1 支持 30 路电话。

（5）信令支持

路由器 E1 端口上可能支持多种信令：ISUP、TUP、中国 1 号信令以及 DSS1。支持 ISUP、TUP 或者 DSS1 信令的路由器可以有效地减少接续时间。在电信级的 IP 电话网络设备中通常要求支持 7 号信令。但是作为中低端路由器，通常只支持 DSS1 和中国 1 号信令。

以上包括了所有路由器的一些通用指标，在品目繁多的指标中，我们往往只须根据几个指标来进行选择，其中，最重要的指标就是网络接口类型、设备吞吐量、支持的路由协议及路由表的大小。下面我们针对企业网中不同层次的路由器做一个简单介绍。

根据性能和价格，路由器还可分为低端、中端和高端三类。

高端路由器的包转发速率在几百 kPacket/s 以上，可支持各种高速端口 (OC3、OC12 等)。高端路由器的典型代表是 Cisco 公司的 Cisco7200、Cisco7500、Cisco7600、Cisco12000 系列路由器。

中端路由器的包转发速率在几十至 200kPacket/s 之间，可支持的最高速端口为 OC3。中端路由器的典型代表是 Cisco 公司的 Cisco3600、Cisco3700 系列路由器。

低端路由器的包转发速率在几十 kPacket/s 左右，可支持的最高速端口为 E3。低端路由器的典型代表是 Cisco 公司的 Cisco1700、Cisco2600 系列路由器。

我们在选择路由器的时候，首先要满足的是企业建网的功能需求，即首先我们的选择必须能够符合具体线路（广域和局域线路）的要求，能够把网络搭建起来，这就要求我们选择的路由器支持具体线路所要求的端口类型，比如一个企业网要通过帧中继互联，那么就要求路由器必须拥有串行端口（比如 Cisco2600 系列路由器支持 WIC-1T 模块拥有 1 个同步串口）；其次，我们应该满足网络的性能需求，即我们在满足功能需求的基础上，同时必须满足性能的需求，比如同样是采用帧中继线路进行互联，一个是分支节点较少，传输数据量很小的企业，也许只需选择 Cisco1700 系列的路由器即可满足要求（如图 2-1 所示），而另一个是传输数据量较大的企业，我们也许必须选择 Cisco2600 系列的路由器才能满足要求（如图 2-1 所示）。

除了以上两点以外，我们往往还会从设备的可靠性（是否支持冗余协议，比如 VRRP、HSRP）、安全性、可管理性以及价格方面进行综合的考察，最终选出满足需求的性价比最好的设备。

注意，当我们选购路由器的时候，不能简单地从几个数字上便得到结论，企业应当明确网络应用、业务，分析对网络的需求，有针对性地考核网络设备，从而建设一个稳定、高性能、易管理的网络。

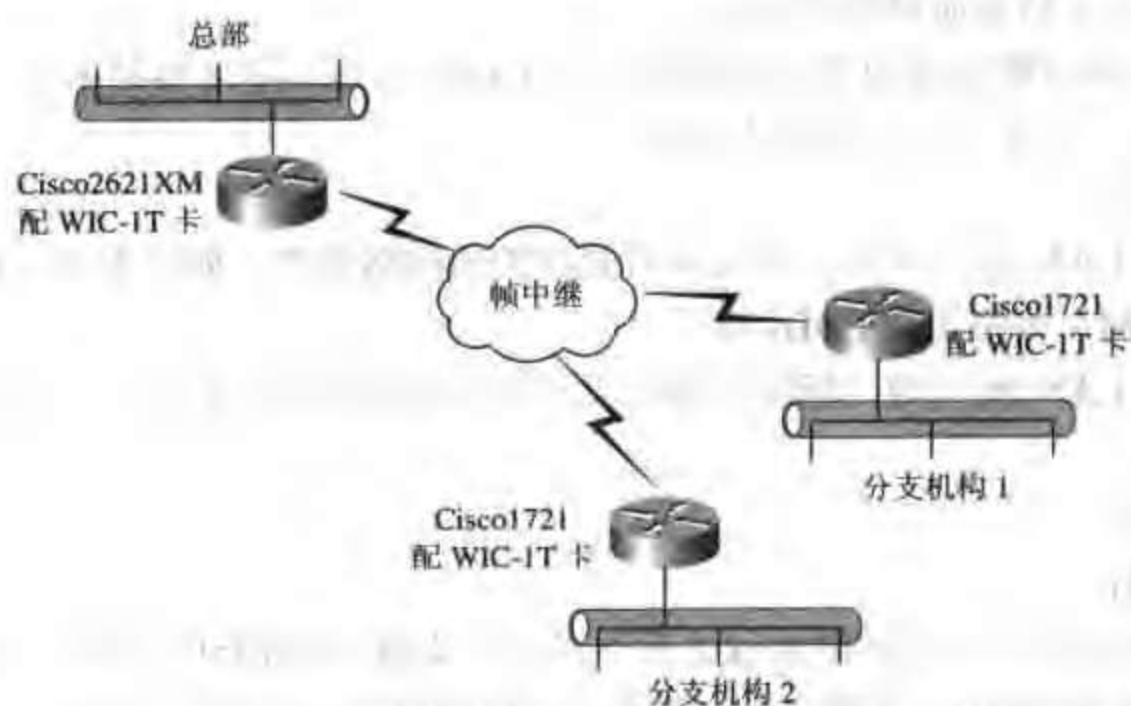


图 2-1 采用 Cisco1700 系列路由器的组网

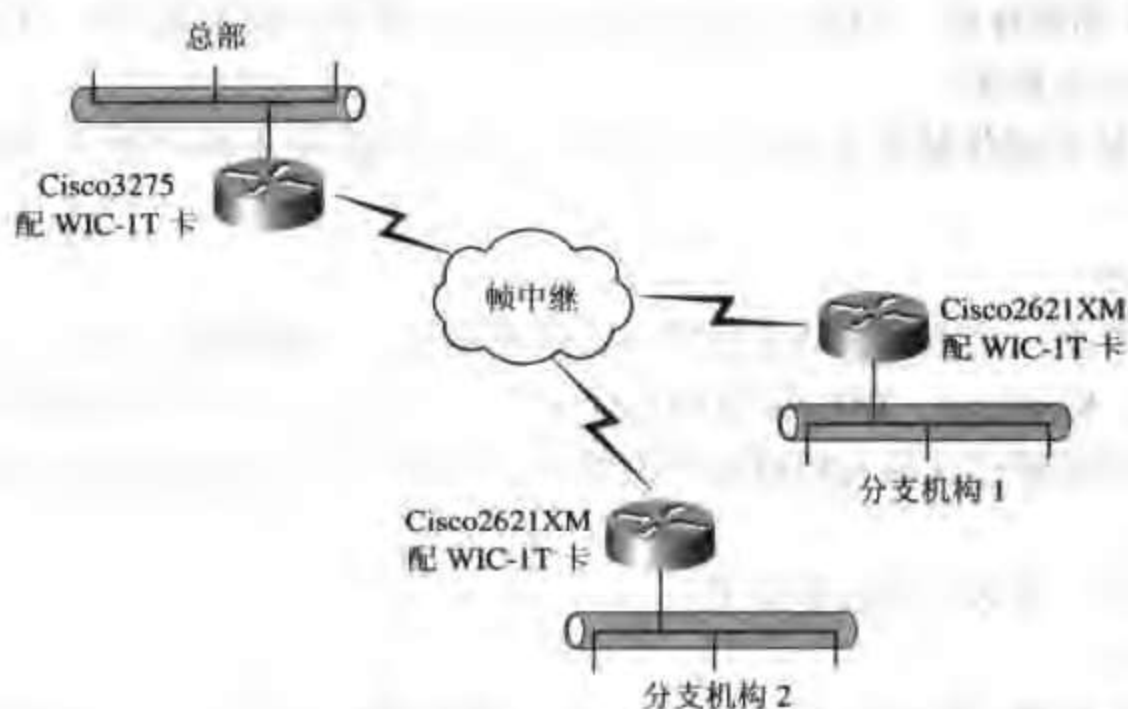


图 2-2 采用 Cisco2600 系列路由器和组网

2.3 防火墙选购指南

和交换机及路由器的选购一样，在选购防火墙的时候，用户首先也要明确自己的业务需求和未来的发展规划，找到一个适合自己的评判准则。只有在对自己的需求非常明确的前提下，对各种参数的对比才更有针对性。下面，我们就对防火墙的一些常用的参数进行一下介绍。

1. 设备基本指标

(1) 产品类型

防火墙产品根据其采用技术的不同一般分为 3 种类型：基于包过滤技术的防火墙、基于

代理的防火墙、基于状态监测的防火墙。

Cisco 的路由器可配置成为包过滤的防火墙, Cisco 的 PIX 防火墙是采用其自有技术 ASA (自适应安全算法) 基于状态监测的防火墙。

(2) LAN 接口

列出支持的 LAN 接口类型: 防火墙所能保护的网路类型, 如以太网、快速以太网、吉比特以太网、ATM、令牌环及 FDDI 等。

支持的最大 LAN 接口数: 指防火墙所支持的局域网络接口数目, 也是其能够保护的不同内网数目。

2. 功能指标

(1) 协议支持

支持的非 IP 协议: 除支持 IP 协议之外, 是否还支持 AppleTalk、IPX 等协议。

建立 VPN 通道的协议: 构建 VPN 通道所使用的协议, 如密钥分配等, 主要有 IPSec, PPTP、专用协议等。

(2) 加密支持

支持的 VPN 加密标准: VPN 中支持的加密算法, 例如数据加密标准 DES、3DES、RC4 以及其他专用的加密算法。

硬件加密: 是否提供硬件加密方法, 硬件加密可以提供更快的加密速度和更高的加密强度。

(3) 认证支持

支持的认证类型: 是指防火墙支持的身份认证协议, 一般情况下具有一个或多个认证方案, 如 RADIUS、Kerberos、TACACS/TACACS+、口令方式、数字证书等。防火墙能够为本地或远程用户提供经过认证与授权的对网络资源的访问, 防火墙管理员必须决定客户以何种方式通过认证。

支持数字证书: 是否支持数字证书。

(4) NAT 支持

支持网络地址转换 (NAT): NAT 指将一个 IP 地址域映射到另一个 IP 地址域, 从而为终端主机提供透明路由的方法。NAT 常用于私有地址域与公有地址域的转换以解决 IP 地址匮乏问题。在防火墙上实现 NAT 后, 可以隐藏受保护网络的内部结构, 在一定程度上提高了网络的安全性。

(5) 防御功能

提供内容过滤: 是否支持内容过滤, 信息内容过滤指防火墙在 HTTP、FTP、SMTP 等协议层, 根据过滤条件, 对信息流进行控制。防火墙控制的结果是: 允许通过、修改后允许通过、禁止通过、记录日志、报警等。过滤内容主要指 URL、HTTP 携带的信息: Java Applet、JavaScript、ActiveX 和电子邮件中的 Subject、To、From 域等。

能防御的 DoS 攻击类型: 拒绝服务 (DoS) 攻击就是攻击者过多地占用共享资源, 导致服务器超载或系统资源耗尽, 而使其他用户无法享有服务或没有资源可用。防火墙通过控制、检测与报警等机制, 可在一定程度上防止或减轻 DoS 黑客攻击。

阻止 ActiveX、Java、Cookies、JavaScript 侵入: 属于 HTTP 内容过滤, 防火墙应该能够从 HTTP 页面剥离 Java Applet、ActiveX 等小程序及从 Script、PHP 和 ASP 等代码检测出危

险代码或病毒，并向浏览器用户报警。同时，能够过滤用户上传的 CGI、ASP 等程序，当发现危险代码时，向服务器报警。

(6) 管理功能

防火墙管理是指对防火墙具有管理权限的管理员通过对防火墙进行身份鉴别，编写防火墙的安全规则，配置防火墙的安全参数，查看防火墙的日志的行为。防火墙的管理一般分为本地管理、远程管理和集中管理等。

提供基于时间的访问控制：是否提供基于时间的访问控制。

支持 SNMP（简单网络管理协议）协议：支持 SNMP 监视和配置。

本地管理：是指管理员通过防火墙的 Console 口或防火墙提供的键盘和显示器对防火墙进行配置管理。

远程管理：是指管理员通过以太网或防火墙提供的广域网接口对防火墙进行管理，管理的通信协议可以基于 FTP、TELNET、HTTP 等。

集中管理：通过集成策略集中管理多个防火墙。

失败恢复特性（Failover）：指支持容错技术，如双机热备份、故障恢复和双电源备份等。

(7) 记录和报表功能

防火墙处理日志的方法：防火墙规定了对于符合条件的报文做日志，应该提供日志信息管理和存储方法。

提供自动日志扫描：指防火墙是否具有日志的自动分析和扫描功能，这可以获得更详细的统计结果，达到事后分析、亡羊补牢的目的。

提供自动报表、日志报告书写器：防火墙实现的一种输出方式，提供自动报表和日志报告功能。

警告通知机制：防火墙应提供告警机制，在检测到入侵网络以及设备运转异常情况时，通过告警来通知管理员采取必要的措施，包括 E-mail、呼机、手机等。

提供简要报表（按照用户 ID 或 IP 地址）：防火墙实现的一种输出方式，按要求提供报表分类打印。

提供实时统计：防火墙实现的一种输出方式，日志分析后所获得的警能统计结果，一般是图表显示。

3. 性能指标

(1) 并发连接数

支持的最大同时连接数。

(2) 吞吐量

明文吞吐量：在不加密的情况下，数据最大的转发率。

密文吞吐量：在加密的情况下，数据最大的转发率。

机据性能指标的不同，防火墙可分为低端、中端和高端，低端的代表是 Cisco 的 PIX501 和 PIX506，中端的代表是 Cisco 的 PIX515 和 PIX525，高端的代表是 Cisco 的 PIX535。

4. 其他指标

列出获得的国内有关部门许可证类别及号码，这是防火墙合格与销售的关键要素之一。其中主要的证书包括：公安部的销售许可证、国家信息安全测评中心的认证证书、总参的国防通信入网证和国家保密局的推警证明等。

以上包括了防火墙的一些通用指标,在众多的指标中,我们往往只需几个指标来进行选择,其中,最重要的指标就是网络接口类型、设备吞吐量和并发连接数。下面我们针对企业网中防火墙的选购做一个简单介绍:

在具体选购防火墙时,我们首先应该对自己的网络进行一下安全的评估,了解一下如果网络遭到入侵,受到的损失能有多大。这一点将直接影响我们对防火墙的选择。

防火墙作为网络安全体系的基础设备,其作用是切断受控网络的通信主干线,对通过受控主干线的任何通信进行安全处理。既然要切断通信的主干线,那么防火墙的吞吐量就显得非常重要,否则防火墙就会成为整个网络的瓶颈。目前防火墙主要有包过滤、应用代理和状态检测等几种类型。从技术上看状态检测型防火墙比包过滤型防火墙性能上更具优势,因此,基于状态检测的防火墙将具有更大的发展空间。

中小企业的防火墙主要用于网络的边界,往往置于接入路由器和内网交换机之间,如图 2-3 所示。

中小企业接入 Internet 的目的是方便内部用户浏览 Web、收发 E-mail 以及发布主页等。这类用户在选购防火墙时,要注意考虑防火墙能够保护内部数据的安全,安全性是放在第一位的,其次是设备的吞吐量和并发数要满足具体的需求,对服务协议的多样性等可以不作特殊要求。

大型企业往往会在多个地点布置防火墙,通常会在 Internet 接入的地方布置边界防火墙,在各个应用系统前面布置专有的防火墙。对于边界防火墙的选购和中小企业防火墙的选择没有太大的差别,而对于内部专有的防火墙,往往需要根据具体的应用来进行选择,但吞吐量通常会必须考虑的因素之一。

总结:以上我们分别对交换机、路由器和防火墙产品的选购作了一个简单的介绍,需要说明的是,我们这里只是从技术角度来分析,当然我们在选择这些网络产品的时候,除了技术层面的因素外,我们还会从品牌、服务和价格等方面进行综合的考察。

下面我们将针对 Cisco 公司的产品进行详细的介绍。



图 2-3 中小企业的防火墙所处位置

2.4 Cisco 交换机产品

Cisco 的交换机产品以“Catalyst”为商标,包含 2950、3550、3750、4500、6500 等 10 多个系列,各产品的比较如图 2-2 所示。1900、2900、3500、4000、5000、6000 系列交换机已经停产。总的来说,这些交换机可以分为如下两类:

(1) 一类是固定配置交换机,包括 3750 及以下的大部分型号,比如 2950G-48 是 48 口 100Mbit/s 以太交换机,带两个 1000Mbit/s GBIC 插槽。除了可进行有限的软件升级之外,这些交换机不能扩展。

(2) 另一类是模块化交换机,主要指 4000 及以上的机型,网络设计者可以根据网络需求,选择不同数目和型号的接口板、电源模块及相应的软件。

目前,网络集成项目中常见的 Cisco 交换机有以下几个系列,2950 系列、3550 系列、3750 系列、4500 系列和 6500 系列,如图 2-4 所示。通常我们将 2950 和 3550 系列称为低端交换机,它们往往被放置于网络的接入层;将 3750 和 4500 系列称为中端交换机,它们往往被放置于网络的汇聚层;将 6500 系列称为高端交换机,它们往往被放置于网络的核心层;下面分别介绍一下这几个系列的产品。

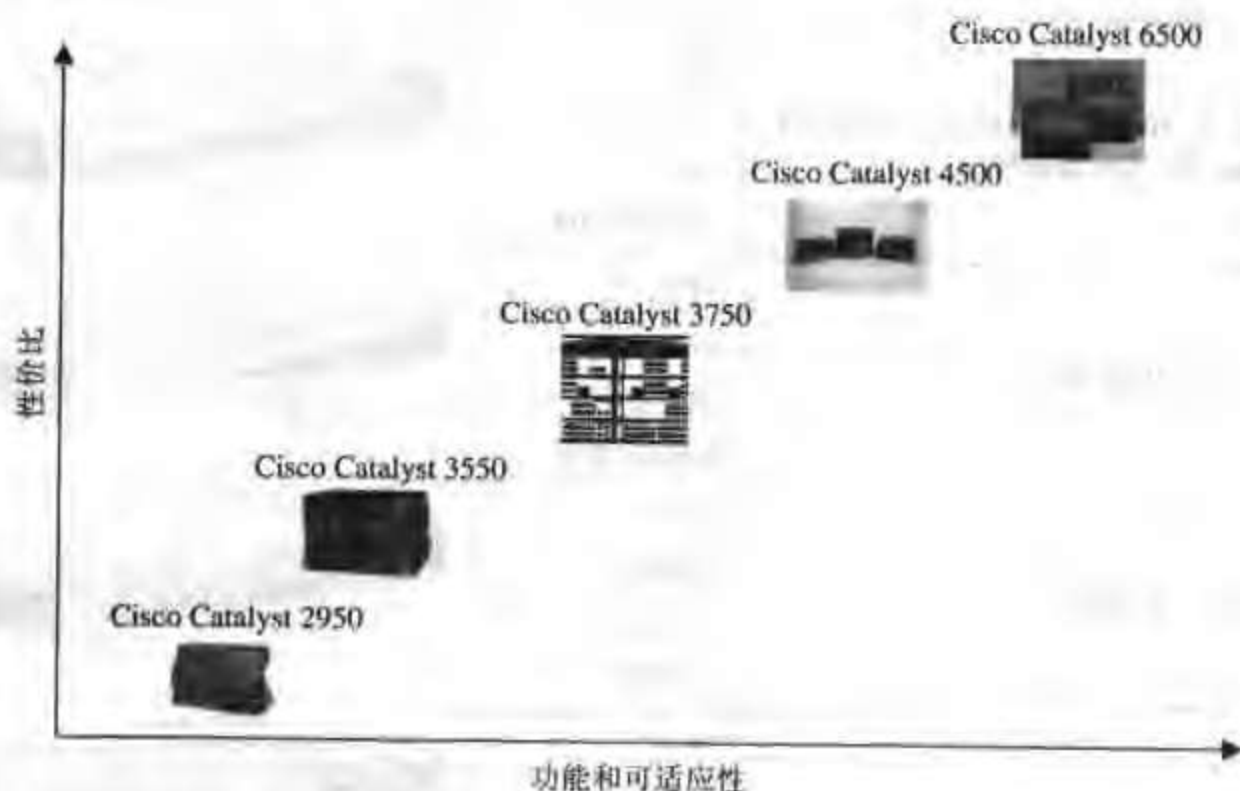


图 2-4 Cisco 交换机产品线

2.4.1 Catalyst 2950 系列交换机

Catalyst 2950 系列智能以太网交换机是一个固定配置、可堆叠的独立设备系列,提供了线速快速以太网和吉比特以太网连接,其实物图如图 2-5 所示。这是一款最廉价的 Cisco 交换产品系列,为中型网络和城域网接入应用提供了智能服务。作为 Cisco 最为廉价的交换产品系列,Catalyst 2950 系列在中型网络或城域网接入边缘实现了智能服务。

固定安装的线速快速以太网桌面交换机 Catalyst 2950 系列,可以为局域网(LAN)提供极佳的性能和功能。这些独立的、10/100 自适应交换机能够提供增强的服务质量(QoS)和组播管理特性,所有的这些都由易用、基于 Web 的 Cisco 集群管理套件(CMS)和集成 Cisco IOS 软件来进行管理。带有 10/100/1000 Base-T 上行链路的 Cisco Catalyst 2950 吉比特铜线,可为中等规模的公司和企业分支机构办公室提供理想的解决方案,以使它们能够利用现有的 5 类铜线从快速以太网升级到更高性能的吉比特以太网主干。

Catalyst 2950 系列包括如表 2-1 所列出的一些具体型号。



图 2-5 Catalyst 2950 系列交换机

表 2-1 Catalyst 2950 系列交换机一览表

项 目	描 述	性 能	图 片
C2950T-24	24 个 10/100 端口和 2 个固定 10/100/1000 Base-T 上行链路端口	背板: 13.6Gbit/s 包转发率: 10.1MPacket/s	
C2950C-24	24 个 10/100 端口和 2 个固定 100 Base-FX 上行链路端口	背板: 13.6Gbit/s 包转发率: 10.1MPacket/s	
C2950-12	12 个 10/100 端口	背板: 8Gbit/s 包转发率: 6.6MPacket/s	
C2950-24	24 个 10/100 端口	背板: 8Gbit/s 包转发率: 6.6MPacket/s	
C2950G-12	12 个 10/100 端口和 2 个 GBIC 插槽	背板: 13.6Gbit/s 包转发率: 10.1MPacket/s	
C2950G-24	24 个 10/100 端口和 2 个 GBIC 插槽	背板: 13.6Gbit/s 包转发率: 10.1MPacket/s	
C2950G-48	48 个 10/100 端口和 2 个 GBIC 插槽	背板: 13.6Gbit/s 包转发率: 10.1MPacket/s	

交换机中的吉比特接口转换器如图 2-6 所示，具体性能列于表 2-2 中。



图 2-6 GBIC

表 2-2

GBIC 性能

GBIC	波长 (nm)	光纤类型	内芯规格 (μm)	模态带宽 (MHz/km)	布线距离
WS-G5484 SX1	850	多模光纤	62.5	160	220m (722 英尺)
			62.5	200	275m (902 英尺)
			50.0	400	500m (1640 英尺)
			50.0	500	550m (1804 英尺)
WS-G5486 LX/LH	1300	多模光纤 ²	62.5	500	550m (1804 英尺)
		单模光纤	50.0	400	550m (1804 英尺)
		(LX/LH)	50.0	500	550m (1804 英尺)
			9/10	-	10km (32810 英尺)
WS-G5487 ZX	1550	单模光纤	无此条件	N/A	70~100km

交换机中使用的堆叠模块如图 2-7 所示。

如果想进一步了解 Catalyst 2950 系列交换机，请访问下面网址：

<http://www.cisco.com/global/CN/products/si/casi/ca2950/index.shtml>

2.4.2 Catalyst 3550 系列交换机

Catalyst 3550 系列智能以太网交换机是一个可堆叠多层交换机系列，可通过高可用性、服务质量 (QoS) 和安全性来改进网络运行，其实物图如图 2-8 所示。凭借一系列快速以太网和吉比特以太网配置，Catalyst 3550 系列堪称一款适用于企业和城域接入应用的强大选择。使您能利用传统 LAN 交换的简洁性来部署网络智能服务，它将 Cisco IOS 软件中的一套第二到四层功能——IP 路由、QoS、限速、访问控制列表 (ACL) 和多播服务扩展到边缘，凭借内置 Cisco 集群管理套件 (CMS) 来简化接入层和小型骨干网的部署。同时它用全套吉比特接口转换器 (GBIC) 设备提供强大的吉比特以太网连接。Catalyst 3550 系列交换机具体情况见表 2-3。



图 2-7 堆叠模块









图 2-8 Catalyst 3550 系列交换机

表 2-3

Catalyst 3550 系列交换机一览表

项 目	描 述	性 能	图 片
C3550-12T	10 个 10/100/1000 Base-T 端口和 2 个 GBIC 插槽	背板： 24Gbit/s 包转发率： 17MPacket/s	<p>10/100/1000 端口 GBIC module 插槽</p>

续表

项 目	描 述	性 能	图 片
C3550-12G	10 个 GBIC 插槽和 2 个 10/100/1000 Base-T 端口	背板: 24Gbit/s 包转发率: 17MPacket/s	
C3550-24-SMI	24 个 10/100 端口和 2 个 GBIC 插槽 (SMI 代表标准版)	背板: 8.8Gbit/s 包转发率: 6.6MPacket/s	
C3550-24-EMI	24 个 10/100 端口和 2 个 GBIC 插槽 (EMI 代表加强版)	背板: 8.8Gbit/s 包转发率: 6.6MPacket/s	
C3550-48-SMI	48 个 10/100 端口和 2 个 GBIC 插槽 (SMI 代表标准版)	背板: 13.6Gbit/s 包转发率: 10.1MPacket/s	
C3550-48-EMI	48 个 10/100 端口和 2 个 GBIC 插槽 (EMI 代表加强版)	背板: 13.6Gbit/s 包转发率: 10.1MPacket/s	
C3550G-24-FX-SMI	24 个 100Base-FX 端口和 2 个 GBIC 插槽	背板: 8.8Gbit/s 包转发率: 6.6MPacket/s	

注意 SMI（标准多层软件镜像）和 EMI（增强多层软件镜像）的区别如下：SMI 也支持路由功能但只支持静态路由和动态的 RIP 协议，EMI 支持静态路由和所有的动态路由协议（RIP、EIGRP、ISIS、OSPF、BGP 等）。

如果想进一步了解 Catalyst 3550 系列交换机，请访问下面网址：
<http://www.cisco.com/global/CN/products/si/casi/ca3550/index.shtml>

2.4.3 Catalyst 3750 系列交换机

Cisco 新推出的 Catalyst 3750 系列交换机是一个创新的产品系列，它结合业界领先的易用性和最高的冗余性，里程碑地提升了堆叠式交换机在局域网中的工作效率，其实物图如图 2-9 和 2-10 所示。这个新的产品系列采用了最新的 Cisco StackWise 技术，不但实现高达 32Gbit/s 的堆叠互联，还从物理上到逻辑上使若干独立交换机在堆叠时集成在一起，便于用户建立一个统一、高度灵活的交换系统，就好像是一整台交换机一样。这代表了堆叠式交换机新的工业技术水平和标准。







图 2-9 Catalyst 3750 系列交换机



图 2-10 Catalyst 3750 系列交换机堆叠

对于中型组织和企业分支机构而言，Catalyst 3750 系列可以通过提供配置灵活性，支持融合网络模式，以自动配置智能化网络服务，降低融合应用的部署难度，适应不断变化的业务需求。此外，Catalyst 3750 系列针对高密度吉比特以太网部署进行了专门的优化，其中包含多种可以满足接入、汇聚或者小型网络骨干网连接需求的交换机。Catalyst 3750 系列交换机具体情况见表 2-4。

表 2-4 Catalyst 3750 系列交换机一览表

项 目	描 述	性 能	图 片
C3750G-24TS	24 个以太网 10/100/1000 端口和 4 条 SFP 上行链路	背板： 32Gbit/s 包转发率： 38.7MPacket/s	
C3750G-24T	24 个以太网 10/100/1000 端口	背板： 32Gbit/s 包转发率： 35.7MPacket/s	
C3550-24-TS	24 个以太网 10/100 端口和 4 条 SFP 上行链路	背板： 32Gbit/s 包转发率： 6.5MPacket/s	
C3550-48-TS	48 个以太网 10/100 端口和 2 条小型可插拔 (SFP) 上行链路	背板： 32Gbit/s 包转发率： 13.1MPacket/s	

注意：Catalyst 3750 系列可以使用 SMI 或者 EMI。SMI 功能集包括先进的服务质量(QoS)、速率限制、访问控制列表 (ACL) 和基本的静态和路由信息协议 (RIP) 路由功能。EMI 可以提供一组更加丰富的企业级功能，包括先进的、基于硬件的 IP 单播和组播路由。

1. SFP 模块介绍



图 2-11 SFP 模块

SFP 模块实物图如图 2-11 所示。

(1) Cisco 1000Base-SX SFP

GLC-SX-MM, 1000Base-SX SFP 使用多模光纤, 最大传输 550 m。

(2) Cisco 1000Base-LX/LH SFP

GLC-LH-SM, 1000Base-LX/LH SFP 使用单模光纤, 最大传输 10km。

(3) Cisco 1000Base-ZX SFP

GLC-ZX-SM, 1000BaseZX SFP 使用单模光纤, 最大传输 70 km~100 km。

2. Cisco StackWise 技术介绍

Cisco StackWise 技术是一种针对吉比特以太网优化的、先进的堆叠架构。该技术的设计目的是及时地对设备添加、移除和重新部署做出反应, 同时保持稳定的性能。

利用特殊的堆叠互连电缆和堆叠软件, Cisco StackWise 技术最多可以将 9 台单独的 Catalyst 3750 交换机连接到一个统一的逻辑单元中。堆叠相当于一个单一的交换单元, 由一个从成员交换机中选出的主交换机管理。主交换机可以自动地创建和升级所有的交换信息和可选的路由表。一个工作中的堆叠可以在不中断服务的情况下, 添加新的成员或者移除旧的成员。

(1) 主要特性和优点

① 可用性——不中断的第二层和第三层性能

Catalyst 3750 系列可以提高可堆叠交换机的可用性。每个交换机可以充当主控制器和转发处理器。堆叠中的每台交换机都可以充当一个主交换机, 从而为网络控制创建了一种 1:N 的可用性机制。在某个单元发生故障时(尽管发生这种情况的可能性很小), 所有其他单元都可以继续转发流量和保持正常运行。

② 便于使用——“即插即用”配置

一个工作中的堆叠可以自行管理和配置。在用户添加或者移除交换机时, 主交换机会自动地更新所有的路由表, 及时地反应堆叠结构的变化。升级信息将同时发送给堆叠的所有成员。

③ 可扩展性——快速以太网到吉比特以太网

Catalyst 3750 系列最多可以将 9 个交换机堆叠在一起, 构成一个统一的逻辑单元, 其中总共包含 468 个以太网 10/100Mbit/s 端口或者 252 个以太网 10/100/1000Mbit/s 端口。各个 10/100Mbit/s 和 10/100/1000Mbit/s 单元可以根据网络的需要任意组合。

④ 混和搭配的交换机类型——根据用户扩建网络的速度支付相应的费用

堆叠可以由 Cisco Catalyst 3750 交换机的任意组合构成。需要混用 10/100 和 10/100/1000 端口的客户可以逐步地发展接入环境, 即只为他们需要的功能付费。

⑤ 智能组播——将融合网络的效率提高到一个新的水平

利用 Cisco StackWise 技术, Catalyst 3750 系列可以为组播应用(例如视频)提供更高的效率。每个数据分组只需要在堆叠互连上发送一次, 从而可以为更多的数据流提供更加有效的支持。

⑥ 出色的服务质量——覆盖堆栈和线速

Catalyst 3750 系列可以提供吉比特以太网速度和智能化的服务, 从而可以保持所有数据的平稳传输, 即使在 10 倍于正常网络速度时。业界领先的标记、分类和调度机制可以为数据、语音和视频流量提供业界最佳的性能——全部都以线速提供。

⑦ 安全性——对接入环境的精确控制

Catalyst 3750 系列支持一组针对连接性和接入控制、全面的安全功能,其中包括 ACL、身份认证、端口级安全和基于身份识别的、支持 802.1x 及其扩展的网络服务。

⑧ 单一 IP 管理——多台交换机共享一个 IP 地址

每个 Catalyst 3750 系列堆叠都作为一个统一的对象进行管理,拥有一个单一的 IP 地址。单一 IP 管理可以支持故障检测、虚拟 LAN 创建和更改、安全和 QoS 控制等功能。

⑨ 大型帧——为要求很高的应用提供支持

Catalyst 3750 系列可以在 10/100/1000Mbit/s 配置上支持大型帧,为那些需要使用很大数据帧的高级数据和视频应用提供支持。

⑩ 支持 IPv6——为将来做好准备

Catalyst 3750 可以通过基于硬件的 IPv6 路由技术,获得最大限度的性能。随着网络设备的增长和对于更大的地址空间和更高的安全性的需求变得日益迫切, Catalyst 3750 将可以满足人们的需求。

(2) 管理选项

Catalyst 3750 系列可以提供一个用于精确配置、出色的命令行界面 (CLI) 和用于根据预设模板进行快速配置的思科集群管理套件 (CMS) 软件,这是一种基于 Web 的工具。此外, CiscoWorks 也可以在整个网络范围内对 Cisco Catalyst 3750 系列进行管理。

如果想进一步了解 Catalyst 3750 系列交换机,请访问下面网址:

<http://www.cisco.com/global/CN/products/si/casi/ca3750/index.shtml>

2.4.4 Catalyst 4500 系列交换机

Catalyst 4500 系列能够为无阻碍的第 2/3/4 层交换提供集成式弹性,因而能进一步加强对融合网络的控制,其实物图如图 2-12 所示。可用性高的融合语音/视频/数据网络能够为正在部署基于互联网企业应用的企业和城域以太网客户提供业务弹性。






图 2-12 Catalyst 4500 系列交换机

作为新一代 Catalyst 4000 系列平台, Catalyst 4500 系列包括 3 种新型 Catalyst 机箱: Catalyst 4507R (7 个插槽)、Catalyst 4506 (6 个插槽) 和 Catalyst 4503 (3 个插槽)。Catalyst

4500 系列中提供的集成式弹性增强包括 1+1 超级引擎冗余（只对 Catalyst 4507R）、集成式 IP 电话电源、基于软件的容错以及 1+1 电源冗余。硬件和软件中的集成式冗余性能能够缩短停机时间，从而提高生产率、利润率和客户成功率。

作为 Cisco AVVID（集成语音、视频和融合数据体系结构）的关键组件，Catalyst 4500 能够通过智能网络服务将控制扩展到网络边缘，包括高级服务质量（QoS）、可预测性能、高级安全性、全面管理和集成式弹性。由于 Catalyst 4500 系列提供与 Catalyst 4000 系列线卡和超级引擎的兼容性，因而能够在融合网络中延长 Catalyst 4000 系列的部署窗口。由于这种方式能减少重复运作开支，降低拥有成本，因而能提高投资回报率（ROI）。Catalyst 4500 系列交换机具体情况见表 2-5。

表 2-5 Catalyst 4500 系列交换机一览表

特 征 \ 型 号	Catalyst 4503	Catalyst 4506	Catalyst 4507R
总槽数	3	6	7
引擎槽数	1	1	2
是否支持引擎冗余	否	否	是
所支持的引擎	SUPII、SUPIII、SUPIV	SUPII、SUPIII、SUPIV	SUPIV
背板带宽	28Gbit/s	64Gbit/s	64Gbit/s
图片			

- 说明：
- （1）Catalyst 4503 和 Catalyst 4506 的第 1 槽用于引擎，其他槽位用于各种线卡，Catalyst 4507R 的第 1 和 2 槽用于引擎，其他槽位用于各种线卡（注意 1、2 槽即使不插引擎，也不能插线卡）。
 - （2）SUPII、SUPIII、SUPIV 分别代表 2、3、4 代引擎。
- Catalyst 4500 系列引擎的具体情况见表 2-6。

表 2-6 Catalyst 4500 系列引擎一览表

特 征 \ 型 号	Supervisor II (WS-X4013)	Supervisor III (WS-X4014)	Supervisor IV (WS-X4515)
操作系统	CATOS	IOS	IOS
路由实现方式	通过路由模块	引擎自带	引擎自带
所支持的机箱	C4006、C4503、C4506	C4006、C4503、C4506	C4006、C4503、C4506、C4507R
包转发率	18MPacket/s	48MPacket/s	48MPacket/s
图片			

Catalyst4500 系列交换机的选配包括机箱、电源、引擎、模块和相应软件的选择，下面我们通过如表 2-7 所示的案例来解释一下：

WS-C4506 是 4506 的机箱它包括风扇但不带电源；

PWR-C45-1000AC 是选配的 1kW 的电源，这要根据具体的负载来定；

CAB-7KACA 是电源线；

WS-X4515 是所选的引擎；

S4KL3-12120EW 是所选的 IOS 软件，这要根据具体需求来定；

WS-X4306-GB 是所选的 6 口吉比特光纤模块，它上面只有 6 个 GBIC 的插槽，必须插 GBIC 卡，才能用；

WS-X4148-RJ 是所选的 48 口 RJ45 以太接口模块，用以连接普通的终端；

WS-G5484 是所选的 GBIC 卡。

表 2-7 Catalyst4506 配置案例

项目名称	描 述	数 量
WS-C4506	Catalyst 4500 Chassis (6-插槽),风扇,无 p/s	1
PWR-C45-1000AC	Catalyst 4500 1000W AC 电源 (仅用于数据)	1
CAB-7KACA	AC 电源线	1
WS-X4515	Catalyst 4500 监视器 IV (2 GE),控制台(RJ-45)	1
S4KL3-12120EW	Cisco IOS BASIC L3 Cat4500 SUP 2+/3/4(RIP,St 路由器,IPX,AT)	1
WS-X4306-GB	Catalyst 4500 吉比特以太网模块, 6 端口 (GBIC)	1
WS-X4148-RJ	Catalyst 4500 10/100 自动槽块, 48 端口 (RJ-45)	1
WS-G5484	1000BASE-SX 短波长 GBIC (仅用于多模)	6

如果想进一步了解 Catalyst 4500 系列交换机，请访问下面网址：

<http://www.cisco.com/global/CN/products/si/casi/ca4500/index.shtml>

2.4.5 Catalyst 6500 系列交换机

由 Catalyst 6500 系列（如图 2-13 所示）和 Catalyst 6000 系列产品组成的 Catalyst 6500 家族为企业网络和服务供应商网络提供了一系列高性能、多层交换解决方案。Catalyst 6500 家族是专为满足对吉比特密度、数据和语音集成、LAN/WAN/MAN 集中、可扩展性、高可用性，以及主干/分布、服务器接合和服务供应商环模中智模多层交换的不端增长的需求而设计的，是 Catalyst 4000 和 5000 系列以及思科 8500 系列交换机的补充和完善，这些产品将继续提供相应的主要配线柜和 ATM 网络核心解决方案。这些 Cisco 家族产品共同提供了广泛的智能交换解决方案，使公司内部网和 Internet 能够支持多媒体、共模任务数据和语音应用。

Catalyst 6500 系列交换机提供 3 插槽、6 插槽、9 插槽和 13 插槽的机箱，以及多种集成式服务模块，包括数吉比特网络安全、内容交换、语音和网络分析模块。Catalyst 6500 系列中的所有型号都使用了统一的模块和操作系统软件，形成了能够适应未来发展的体系结构，由于能提供操作一致性，因而能提高 IT 基础设施的利用率，并增加投资回报。从 48 端口到

576 端口的 10/100/1000M 以太网布线室到能够支持 192 个 1Gbit/s 或 32 个 10Gbit/s 骨干端口, 提供每秒数亿个数据包处理能力的网络核心, Catalyst 6500 系列能够借助冗余路由与转发引擎之间的故障切换功能提高网络正常运行时间。



图 2-13 Catalyst 6500 系列交换机

Catalyst 6500 系列具有许多业界领先的功能, 获得了许多“业界第一”称号。它同时支持三代模块, 这些模块不但能不断提升 Catalyst 6500 系列的用户价值, 也同时体现出思科对于创新的关注。思科的新一代 Catalyst 6500 系列模块和交换引擎 Supervisor Engine 720 包含思科新开发的 11 种应用专用集成电路 (ASIC), 它不但扩展了 Cisco 在网络界的领先地位, 还能提供无与伦比的投资保护。

Catalyst 6500 系列不但能为企业和电信运营商提供市场领先的服务、性能、端口密度和可用性, 还能提供无与伦比的投资保护能力, 包括:

(1) 最长的网络正常运行时间。利用平台、电源、控制引擎、交换矩阵和集成网络服务冗余性提供 1~3s 的状态故障切换, 提供应用和服务连续性统一在一起的融合网络环境, 减少关键业务数据和服务的中断。

(2) 全面的网络安全性。将切实可行的数吉比特级 Cisco 安全解决方案集成到现有网络中, 包括入侵检测、防火墙、VPN 和 SSL。

(3) 可扩展性能。利用分布式转发体系结构提供高达 400MPacket/s 的转发性能。

(4) 能够适应未来发展并保护投资的体系结构。在同一种机箱中支持三代可互换、可热插拔的模块, 以提高 IT 基础设施利用率, 增大投资回报, 并降低总体拥有成本。

(5) 操作一致性。3 插槽、6 插槽、9 插槽和 13 插槽机箱配置使用相同的模块、Cisco IOS Software、Catalyst Operating System Software 以及可以部署在网络任意地方的网络管理工具。

(6) 卓越的服务集成和灵活性。将安全和内容等高级服务与融合网络集成在一起, 提供从 10/100Mbit/s 和 10/100/1000Mbit/s 以太网到 10 吉比特以太网, 从 DS0 到 OC-48 的各种接口和密度, 并能够在任何部署项目中端到端地执行。

Catalyst 6000 系列交换机为园区网提供了高性能、多层交换的解决方案, 专门为需要吉比特扩展、可用性高、多层交换的应用环境设计, 主要面向园区骨干连接等场合。Catalyst 6500 系列交换机见表 2-8, 各交换机实物图如图 2-14~2-17 所示。

表 2-8 Catalyst 6500 系列交换机一览表

型号	Catalyst 6503	Catalyst 6506	Catalyst 6509	Catalyst 6513
特征				
总槽数	3	6	9	13
是否支持引擎冗余	是	是	是	是
所支持的引擎	SUP1、SUP2、SUP720	SUP1、SUP2、SUP720	SUP1、SUP2、SUP720	SUP1、SUP2、SUP720

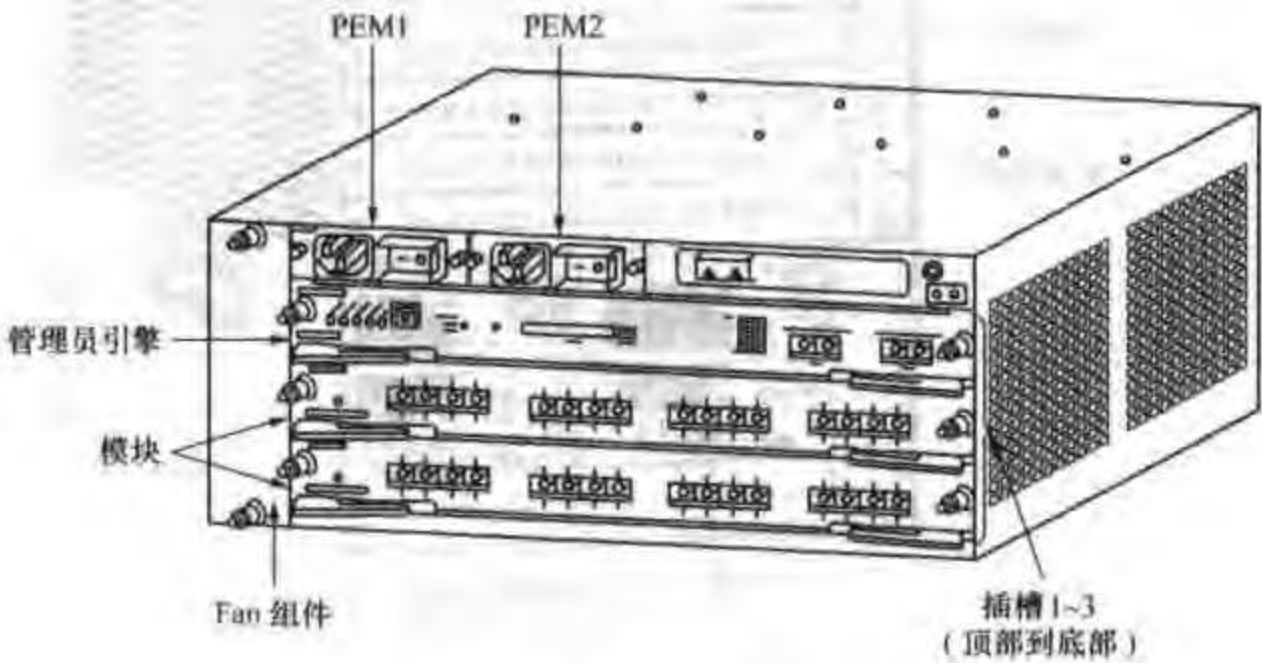


图 2-14 Catalyst 6503

说明：对所有的引擎，Catalyst 6503 的槽位 1、2 用于插引擎，当 2 槽不插引擎时可插其他的线卡，3 槽用于插各种线卡。

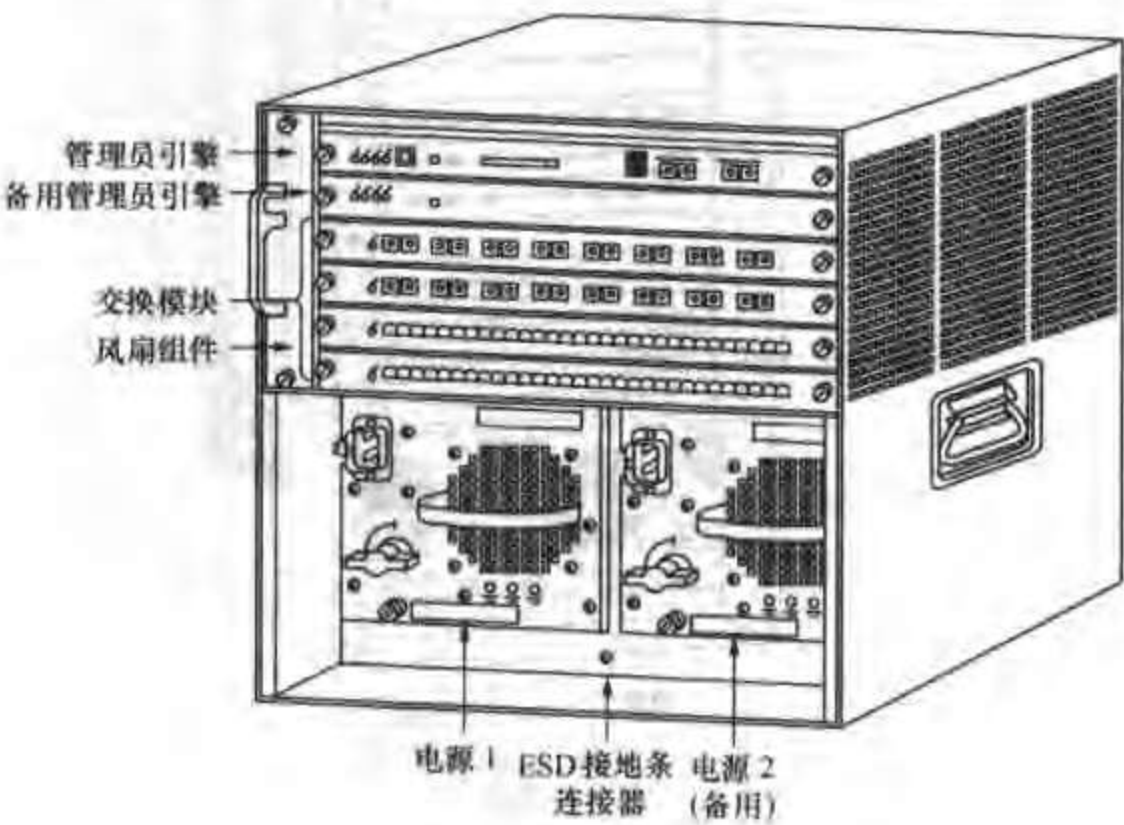


图 2-15 Catalyst 6506

说明：Catalyst 6506 的槽位 1、2 用于插引擎，当 2 槽不插引擎时可插其他的线卡，3~6 槽用于插各种线卡。

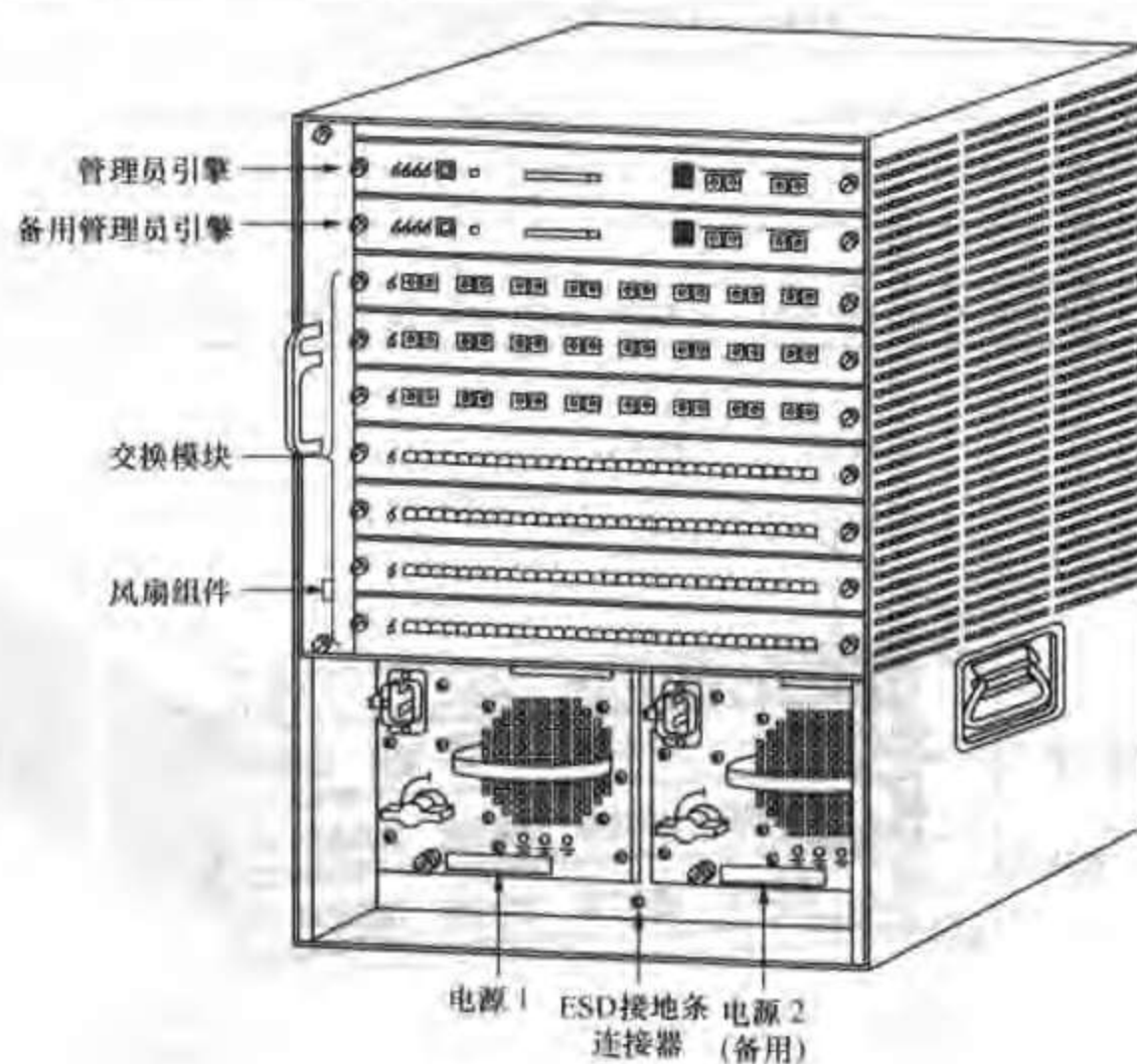


图 2-16 Catalyst 6509

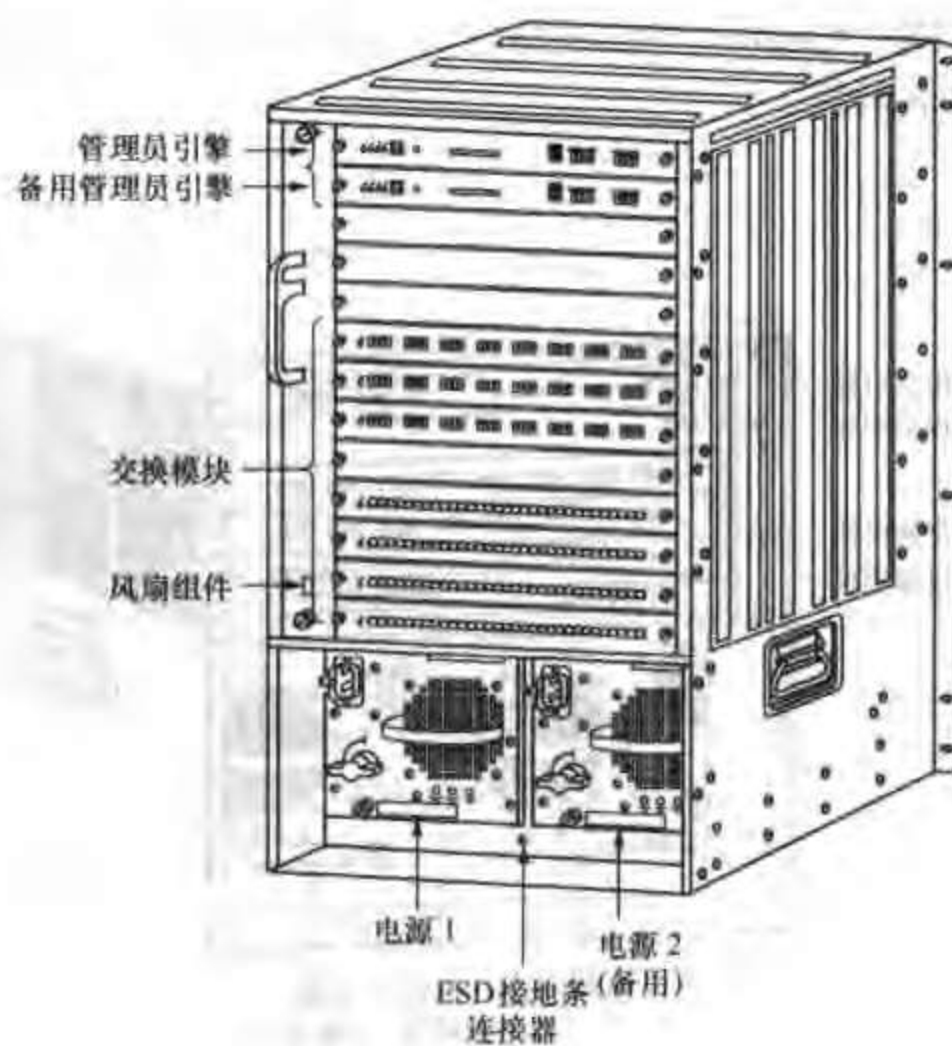


图 2-17 Catalyst 6513

说明：

(1) 当采用 1、2 代引擎时，Catalyst 6513 的槽位 1、2 用于插引擎，其他槽位可插各种

线卡，当只插一块引擎时，另一引擎的槽位可用来插线卡。

(2) 当采用 720 引擎时，Catalyst 6513 的槽位 7、8 用于插引擎，其他槽位可插各种线卡，当只插一块引擎时，另一引擎的槽位可用来插线卡。

Catalyst 6500 系列引擎的具体情况见表 2-9。

表 2-9 Catalyst 6500 系列引擎一览表

型号	Supervisor 1	Supervisor 2	Supervisor 720
特征			
操作系统	Hybrid IOS	Hybrid IOS	Native IOS
路由实现方式	通过在引擎上添加 MSFC 模块来实现	通过在引擎上添加 MSFC 模块来实现	引擎自带
所支持的机箱	C6503、C6506、C6509、C6513	C6503、C6506、C6509、C6513	C6503、C6506、C6509、C6513
背板带宽	32Gbit/s	256Gbit/s	720Gbit/s
包转发率	15MPacket/s	210MPacket/s	400MPacket/s
图片			

说明：

(1) Hybrid IOS 指，引擎是采用的 CatOS，但 MSFC 采用的是 IOS。

(2) Supervisor 2 需要添加 SFM 矩阵模块才能达到背板带宽 256Gbit/s，否则它的背板只能是 32Gbit/s；Supervisor 720 自带矩阵模块，不用外加，因此它可以节约一个槽位。

如果想进一步了解 Catalyst 6500 系列交换机，请访问下面网址：

<http://www.cisco.com/global/CN/products/si/casi/ca6000/index.shtml>

2.5 Cisco 路由器产品

Cisco 的路由器产品以“Cisco”为商标，包含 800、1700、2600、3600、3700、7200、7300、7400、7500、7600、12000 等 10 多个系列，如图 2-18 所示。目前，网络集成项目中常见的 Cisco 路由器有以下几个系列，1700 系列、2600 系列、3600 系列、3700 系列、7200 系列和 7500 系列。通常我们将 1700 和 2600 系列称为低端路由器，将 3600 系列和 3700 系列称为中端路由器，将 7200、7500 和 12000 系列称为高端路由器，下面分别介绍一下这几个系列的产品。

2.5.1 Cisco 1700 系列路由器

Cisco 1700 系列模块化访问路由器为中小型企业 and 小型分支机构提供灵活、安全的访问解决方案，其实物图如图 2-19 所示。Cisco 1700 系列的模块化体系结构能使用户定制一个满足其目前访问要求的安全访问解决方案，能使他们经济有效地实施新应用，包括虚拟专用网（VPN）访问、多服务语音/数据集成和宽带服务。集成的网络功能包括 1 个可选的防火墙、CSU/DSU 和 VPN 特性，减少了部署及管理时间和工作量。



图 2-18 Cisco 路由器产品线

Cisco 1721 支持传统的数据访问应用以及目前和未来的新广域网服务，包括 VPN 和宽带技术。

除数据应用之外，Cisco 1751 还支持集成的多服务语音/传真/数据应用。企业可以从一个稳健的数据访问解决方案开始，然后在准备就绪时经济有效地集成语音和传真。



图 2-19 Cisco 1700 系列路由器

Cisco 1760 模块化接入路由器为中小企业和小型企业个体分支机构提供多服务电子商务功能。Cisco 系统公司隆重推出了 Cisco 1760 模块化接入路由器，这种路由器是中小企业和小型企业个体分支机构的理想接入解决方案。Cisco 1760 属于四插槽模块化接入路由器，安装在 19 英寸机架中，不但能提供安全的因特网和内部网接入，还能在同一个平台上实施多种电子商务和语音应用。这些服务包括 IP 语音（VoIP）、安全的虚拟专用网（VPN）接入和集成式防火墙，以及企业级数字用户线（DSL）接入，该产品适用于许多行业和企业。借助 Cisco 1760，客户能够进行安全的数据联网开始，并在需要时移植到 VoIP 和 IP 电话服务。有了这种灵活性，除基本的因特网和内部网接入外，还能销售增值服务，从而成为客户的战备联网合作伙伴。由于能引入新应用，并在平台上修改或添加 WAN 和语音接口，因而能根据客户的需求添加服务并获得更多收入。Cisco 1760 使用的 Cisco IOS 软件、WAN 和语音接口卡与 Cisco 1700、Cisco 2600 和 Cisco 3600 路由器相同，不但降低了存储和支持要求，还能充分利用您在销售和支持思科系统公司接入解决方案方面积累的丰富经验。

Cisco 1700 系列模块化接入路由器使您可以通过一个集成化的平台，为中小型企业 and 小型分支机构提供灵活的、安全的接入解决方案。Cisco 1700 系列可以提供可更换的 WAN 接口和强大的性能，帮助用户定制一个符合客户现在的网络和业务需求的安全接入解决方案，并能够经济有效地部署新型应用，其中包括虚拟专用网（VPN）、多服务语音/传真/数据集成，

以及宽带数字用户线路（DSL）和有线电视服务。

表 2-10

Cisco1700 系列路由器一览表

项 目	描 述	性 能
Cisco1710	2 个以太网口（1 个 10Base-T, 1 个 10/100Base-T）的安全路由器 （带 VPN/FW/IDS 功能）	进程交换: 1300Packet/s 快速交换: 14000Packet/s
Cisco1720	1 个 10/100Base-T 以太网口, 2 个 WIC 插槽	进程交换: 1400Packet/s 快速交换: 8500Packet/s
Cisco1721	1 个 10/100Base-T 以太网口, 2 个 WIC 插槽	进程交换: 1700Packet/s 快速交换: 12000Packet/s
Cisco1751	1 个 10/100Base-T 以太网口, 3 个 WIC 插槽	进程交换: 1500Packet/s 快速交换: 15000Packet/s
Cisco1760	1 个 10/100Base-T 以太网口, 2 个 WIC/VIC 插槽, 2 个 VIC 插槽	进程交换: 1700Packet/s 快速交换: 16000Packet/s

上述产品的图片如图 2-20~2-23 所示。

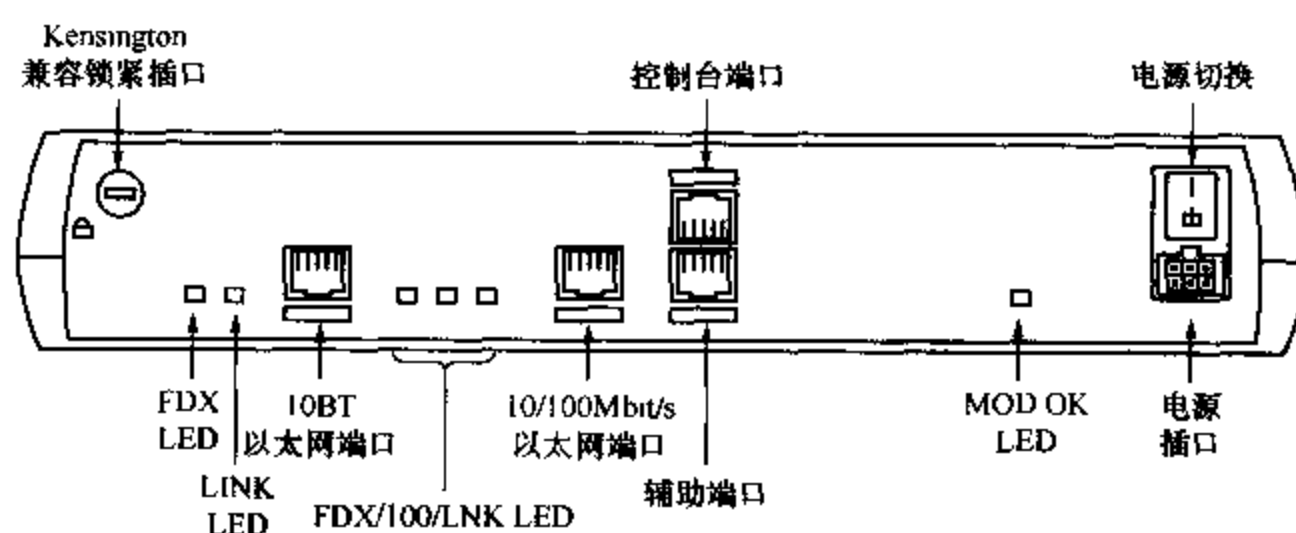


图 2-20 Cisco1710

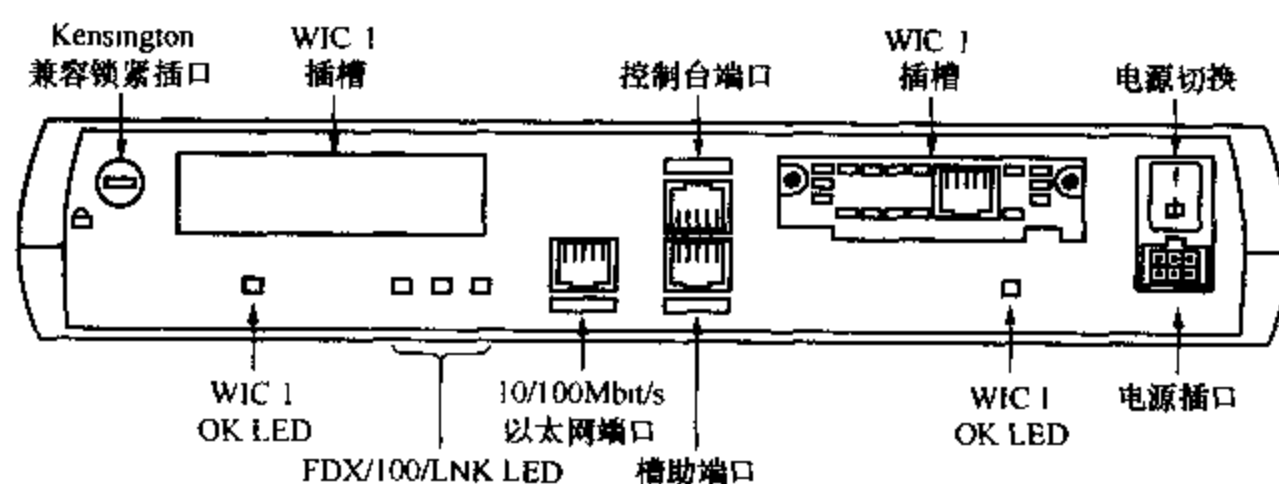


图 2-21 Cisco1720

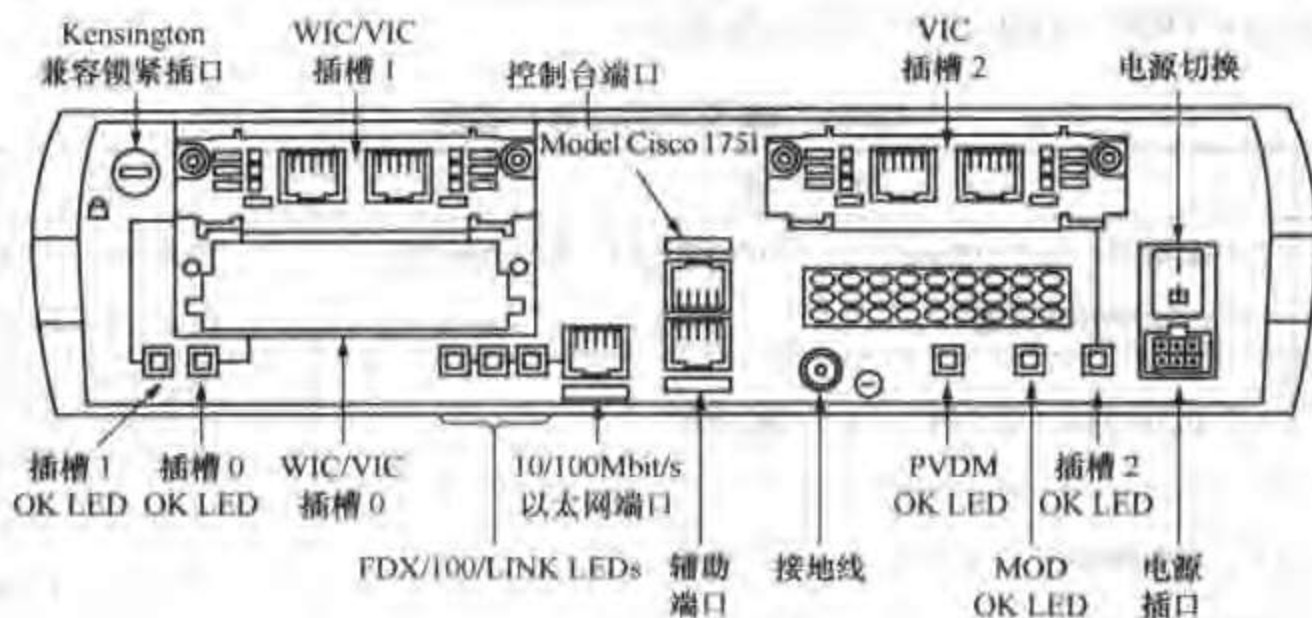


图 2-22 Cisco1751



图 2-23 Cisco1760

如果想进一步了解 Cisco1700 系列路由器，请访问下面网址：

<http://www.cisco.com/global/CN/products/rt/1700/index.shtml>

2.5.2 Cisco 2600 系列路由器

Cisco Systems 通过 Cisco 2600 系列（如图 2-24 所示）将企业级的通用性、集成和功能扩展到了创建以机构。随着新服务和应用的面市，Cisco 2600 系列的模块化体系结构能够提供适应网络技术变化所需的通用性。Cisco 2600 系列配置了强大的 RISC 处理器，能够支持当今不断发展的网络中所需的高级服务质量（QoS）、安全和网络集成特性。通过将多个独立设备的功能集成到一个单元之中，Cisco 2600 系列降低了管理远程网络的复杂性。Cisco 2600 系列与 Cisco 1600、1700 和 3600 系列共享模块化接口，为 Internet、内部网访问、多服务语音/数据集成、模拟和数字拨号访问服务、VPN 访问、ATM 访问集中、VLAN 以及路由带宽管理等应用提供经济有效的解决方案。

新的 Cisco 2610XM、2611XM、2620XM、2621XM、2650XM 和 2651XM 路由器分别应当部署于过去使用 Cisco 2610、2611、2620、2621、2650 和 2651 路由器的（Cisco 2610、2611、2620、2621、2650 和 2651 路由器已停产）场合。新的 XM 系列产品可

可以在不增加成本的前提下，提供更高的性能以及更大的缺省内存和最大内存。Cisco 2600 系列路由器见表 2-11。



图 2-24 Cisco 2600 系列路由器

表 2-11

Cisco2600 系列路由器一览表

项 目	描 述	性 能
Cisco2610XM	1 个 10/100Base-T 以太网口, 2 个 WIC 插槽, 1 个 NM 插槽	进程交换: 1500Packet/s 快速交换: 20000Packet/s
Cisco2611XM	2 个 10/100Base-T 以太网口, 2 个 WIC 插槽, 1 个 NM 插槽	进程交换: 1500Packet/s 快速交换: 20000Packet/s
Cisco2620XM	1 个 10/100Base-T 以太网口, 2 个 WIC 插槽, 1 个 NM 插槽	进程交换: 1500Packet/s 快速交换: 30000Packet/s
Cisco2621XM	2 个 10/100Base-T 以太网口, 2 个 WIC 插槽, 1 个 NM 插槽	进程交换: 1500Packet/s 快速交换: 30000Packet/s
Cisco2650XM	1 个 10/100Base-T 以太网口, 2 个 WIC 插槽, 1 个 NM 插槽	进程交换: 2000Packet/s 快速交换: 40000Packet/s
Cisco2651XM	2 个 10/100Base-T 以太网口, 2 个 WIC 插槽, 1 个 NM 插槽	进程交换: 2000Packet/s 快速交换: 40000Packet/s
Cisco2691	2 个 10/100Base-T 以太网口, 3 个 WIC 插槽, 1 个 NM 插槽	进程交换: 7400Packet/s 快速交换: 70000Packet/s

上述产品的图片如图 2-25~2-31 所示。

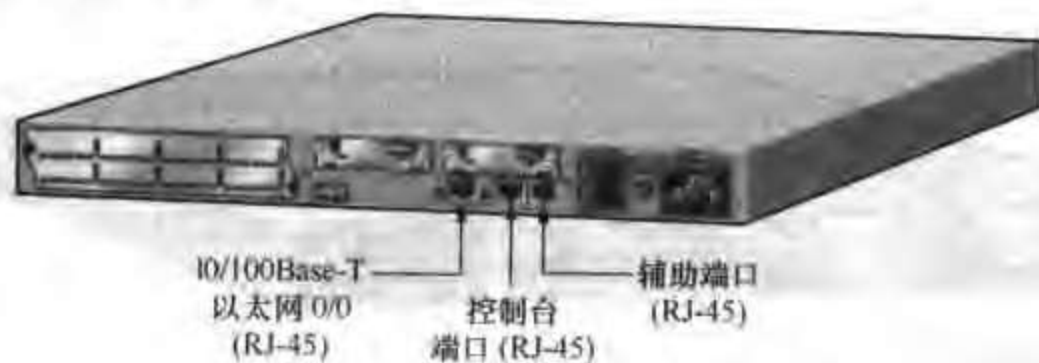


图 2-25 Cisco2610XM

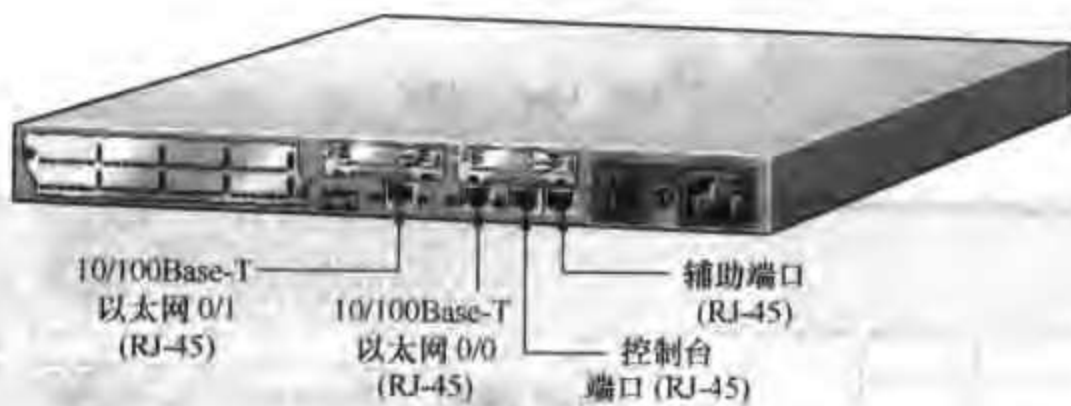


图 2-26 Cisco2611XM

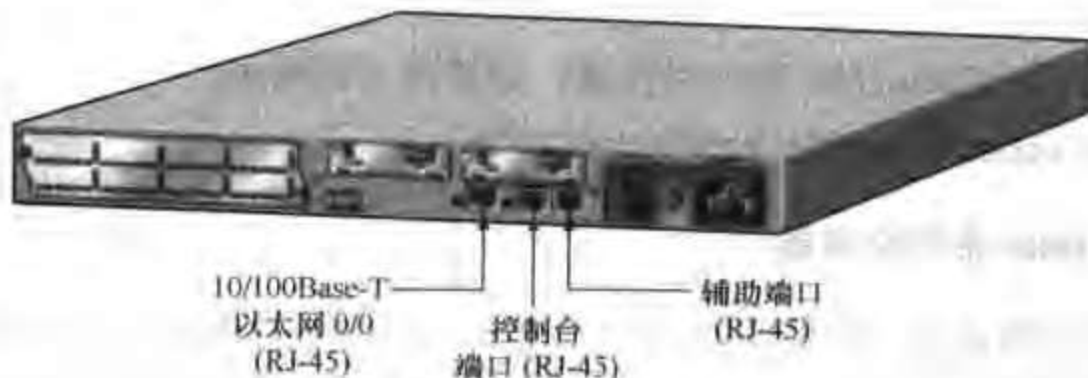


图 2-27 Cisco2620XM

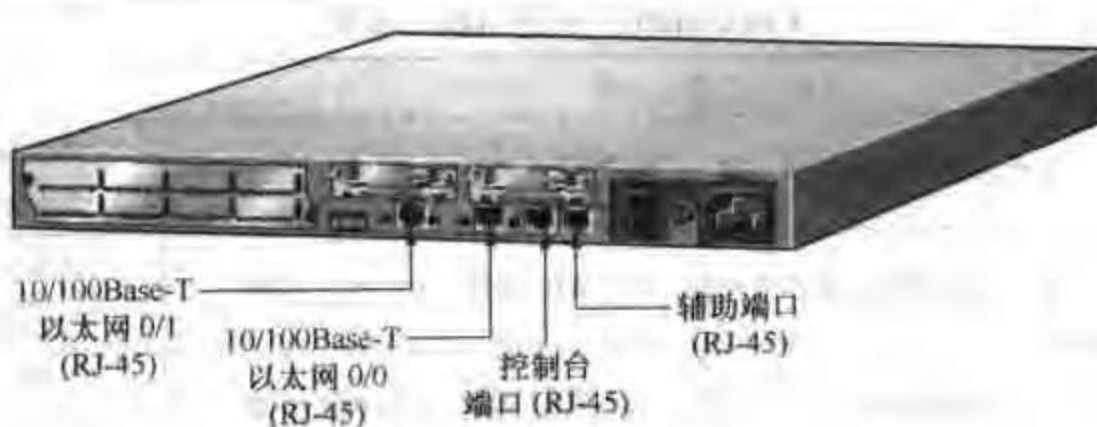


图 2-28 Cisco2621XM



图 2-29 Cisco2650XM

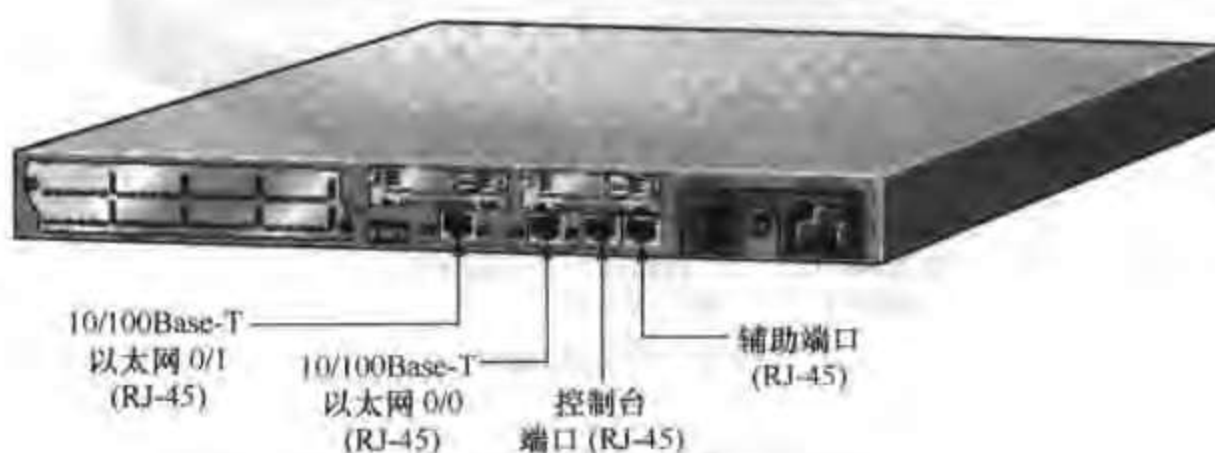


图 2-30 Cisco2651XM



图 2-31 Cisco2691

如果想进一步了解 Cisco2600 系列路由器，请访问下面网址：

<http://www.cisco.com/global/CN/products/rt/2600/index.shtml>

2.5.3 Cisco 3600 系列路由器

Cisco 3600 系列路由器（如图 2-32 所示）是一个适合大中型企业 Internet 服务供应商的模块化、多功能访问平台家族。Cisco 3600 系列拥有 70 多个模块化接口选项，提供语音/数据集成、虚拟专网（VPN）、拨号访问和多协议数据路由解决方案。通过利用 Cisco 的语音/

传真网络模块, Cisco 3600 系列允许客户在单个网络上合并语音、传真和数据流量。高性能的模块化体系结构保护了客户的网络技术投资, 并将多个设备的功能集成到一个可管理的解决方案之中。

Cisco 3600 是世界第一个真正的多功能应用支持平台, 在单独一个服务器上广泛支持分支机构/企业拨号访问应用, LAN 到 LAN 或者路由选择应用以及多服务应用。它提供前所未有的模块化选项, 可使用多种不同的网络模块, 它还具有强大的灵活性, 可针对客户的不同应用环境, 提供各种配置选项, 而且最重要的是, 它具有支持所有这些应用的优质运行性能。



图 2-32 Cisco 3600 系列路由器

高度模块化的 Cisco 3600 系列访问服务器具有惊人的多功能性, 可以单一机箱内支持分支机构/企业拨号访问应用, 局域网到局域网 (LAN to LAN) 或路由选择应用以及多服务应用。这些独有的特性使 Cisco 3600 系列成为大型分支机构理想的平台。Cisco 将继续为 Cisco 3600 系列开发新的解决方案, 以助你保持领先的地位。Cisco 提供前所未有的模块化选项, 可以使用多种网络模块, 还有巨大的灵活性, 配有各种适合客户专用应用环境的可配置选择, 而且最重要的是, Cisco 具有支持所有这些应用的优质运行性能。Cisco 3600 系列路由器见表 2-12。

表 2-12

Cisco3600 系列路由器一览表

项 目	描 述	性 能
Cisco3620	2 个 NM 插槽	进程交换: 2000Packet/s 快速交换: 20000~40000Packet/s
Cisco3640	4 个 NM 插槽	进程交换: 4000Packet/s 快速交换: 50000~70000Packet/s
Cisco3662	2 个 10/100Base-T 以太网口, 6 个 NM 插槽	进程交换: 12000Packet/s 快速交换: 100000~120000Packet/s

说明:

目前 Cisco3600 系列路由器已经只剩下 3662 一款路由器了, 其他型号都已停产, 替代产品是性价比更高的 3700 系列路由器, 我们将在下面进行介绍。

上述产品的图片如 2-33~2-35 所示。

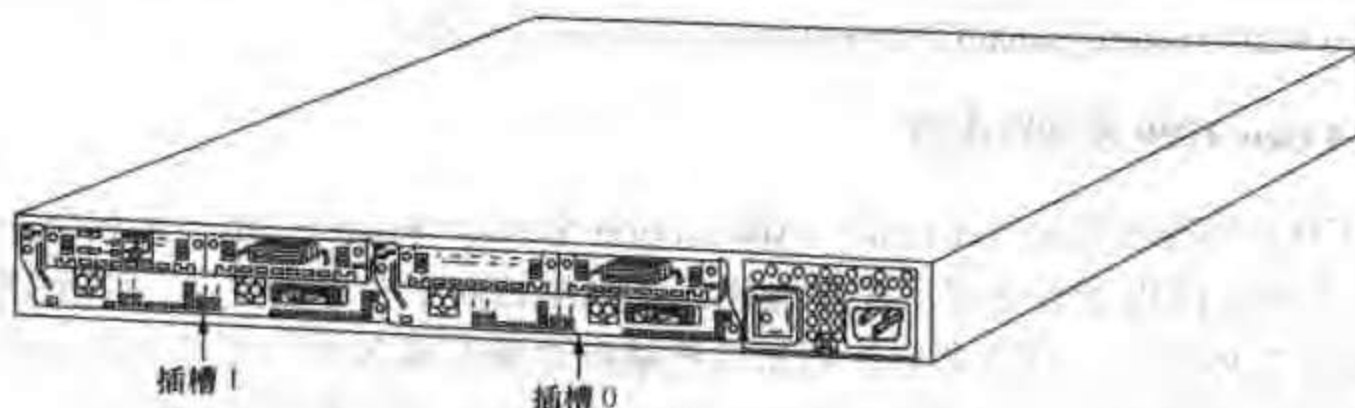


图 2-33 Cisco3620

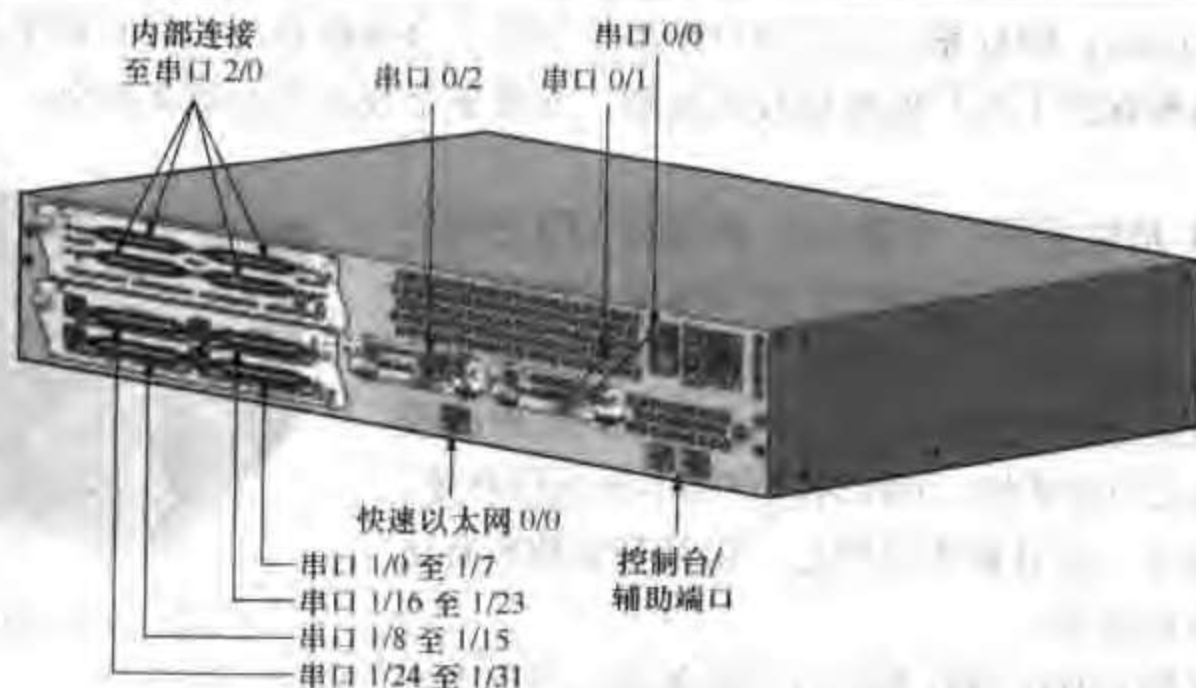


图 2-34 Cisco3640

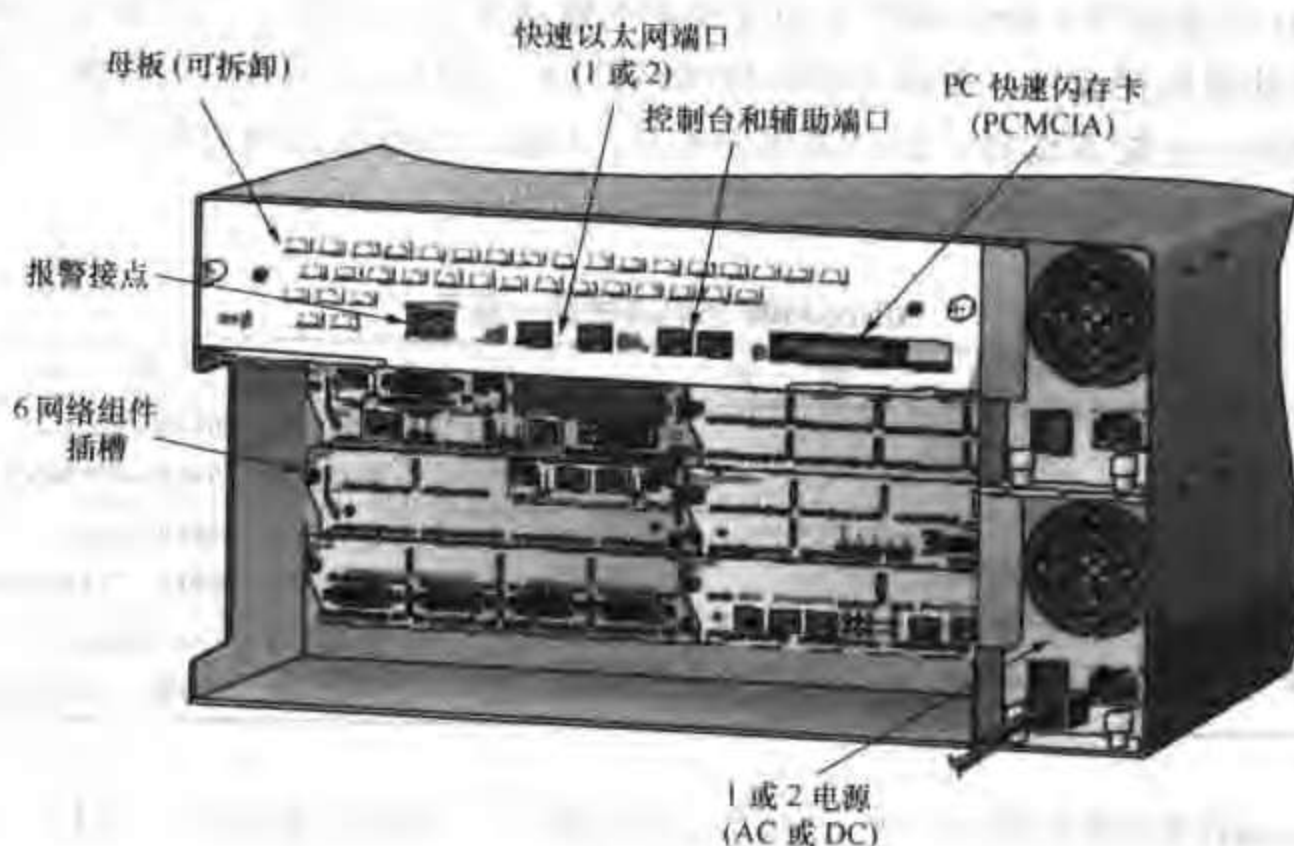


图 2-35 Cisco3662

如果想进一步了解 Cisco3600 系列路由器，请访问下面的网址：

<http://www.cisco.com/global/CN/products/rt/3600/index.shtml>

2.5.4 Cisco 3700 系列路由器

Cisco 3700 系列应用服务路由器 (Application Service Router) 是一系列全新的模块化路由器，可实现新的电子商务应用在集成化分支机构访问平台中的灵活、可扩展的部署，其实物图如图 2-36 所示。对于那些计划从传统基础设施对服务进行升级并将新的应用从核心网络分布到企业边缘的客户而言，Cisco 3700 系列为远程交换局访问提供了一套新的功能强大的解决方案。Cisco 3700 系列的部署可帮助客户更快地降低电子商务应用的成本并从中受益，降低客户基础设施的总拥有成本，并可改进网络利用率和增强网络的竞争能力。

Cisco 3700 系列支持 Cisco AVVID (语音、视频和集成数据体系结构), 而 Cisco AVVID 则是一种覆盖整个企业的、基于各种标准的网络体系结构, 它可为将各种商业和技术战略组合成一个聚合模型奠定基础。

模块化 Cisco 3700 系列应用服务路由器充分利用了 Cisco 1700、2600 和 3600 系列路由器针对 WAN 访问、语音网关和拨号应用等而配备的可选的网络模块 (NM)、WAN 接口卡 (WIG) 和高级集成模块 (AIM)。

此外, Cisco 3725 和 Cisco 3745 这 2 个 Cisco 3700 平台引进一种新的、可提供更广泛接口的高密度服务模块 (HDSM)。配备 4 个 NM 插槽的 Cisco 3745 路由器取消了在每一对相邻 NM 插槽之间的中心导轨, 因此可以采用 2 个 HDSM, 而不是 4 个 NM。配备 2 个 NM 插槽的 Cisco 3725 路由器可在它所配备的 2 个 NM 插槽之一中采用一个 HDSM, 并仍可在剩余的 NM 插槽内采用一个 NM。采用新的 HDSM 之后, Cisco 3700 系列路由器就能够集成更高端口密度和新的性能服务了。Cisco 3700 系列路由器具体情况见表 2-13。



图 2-36 Cisco 3700 系列路由器

表 2-13

Cisco3700 系列路由器一览表

项 目	描 述	性 能
Cisco3725	2 个 NM 插槽	进程交换: 8000Packet/s 快速交换: 100000~120000Packet/s
Cisco3745	4 个 NM 插槽	进程交换: 20000Packet/s 快速交换: 225000~250000Packet/s

说明: Cisco3700 系列路由器是原来 3600 系列路由器的升级产品。

上述产品的图片如图 2-37 和 2-38 所示。

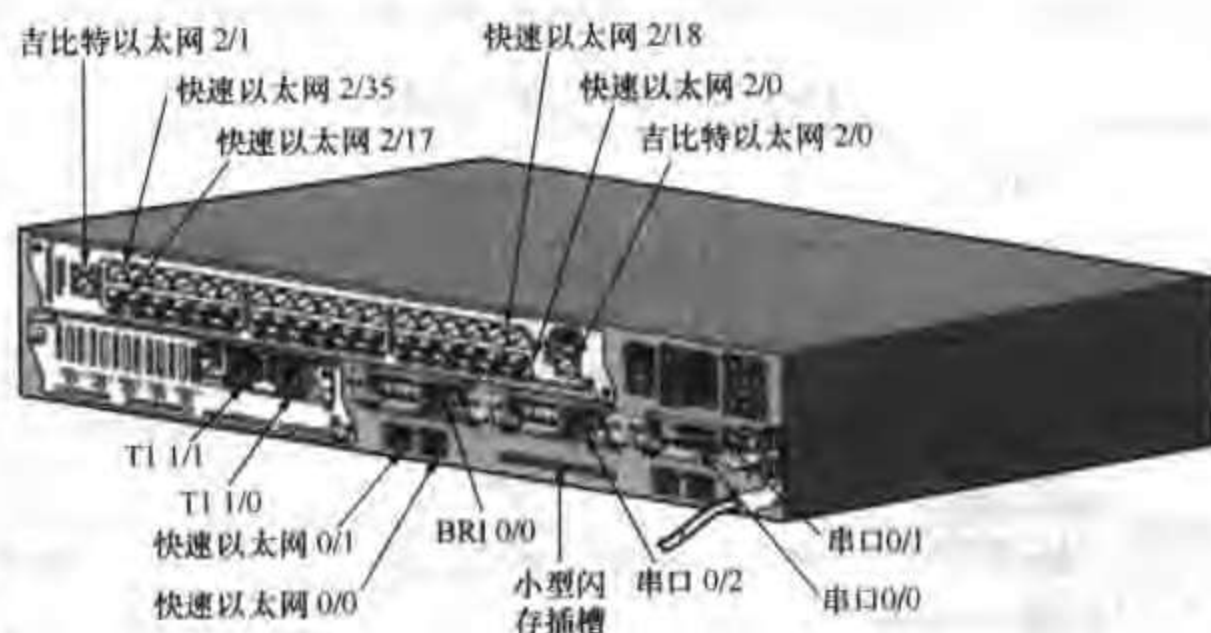


图 2-37 Cisco3725

如果想进一步了解 Cisco3700 系列路由器, 请访问下面地网址:

<http://www.cisco.com/global/CN/products/rt/3700/index.shtml>

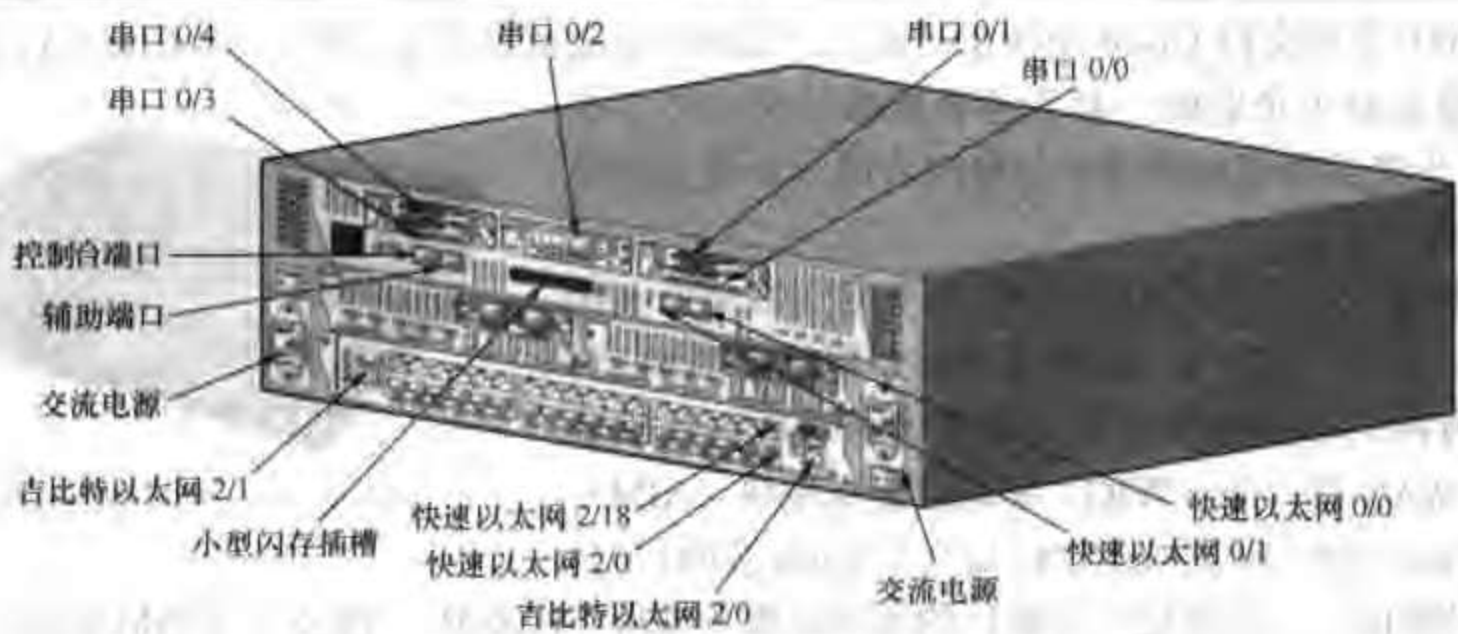


图 2-38 Cisco3745

2.5.5 Cisco 7200 系列路由器




Cisco 7200 系列路由器（如图 2-39 所示）提供优异的性价比，可以满足下列需求：需要广域网和 Internet 网关连接的地区办事处和分公司；企业和服务供应商的远程站点集合，通过一个中心站点将多个分散站点连接起来；需要 IBM 数据中心连接的站点；需要结合上述所有特性多方面功能的站点，以便支持多服务语音、视频和数据流量。



图 2-39 Cisco 7200 系列路由器

拥有出色性价比的 Cisco 7200 系列路由器可以提供很多网络服务加速解决方案，如通过网关连接到 WAN 和 Internet 的地区和分支办公室，企业和服务供应商的远地集中（多个分散地点通过一个中央地点实现互连），要求 IBM 数据中心连接的地点，要求能够将以上所有功能结合起来实现多服务语音，视频和数据的多功能能力的地点。Cisco 7200 系列路由器具体情况见表 2-14。

表 2-14 Cisco 7200 系列引擎一览表

型号	NPE-225	NPE-400	NPE-G1
特征			
所支持的机箱	Cisco7204vvr、 Cisco7206vvr	Cisco7204vvr、 Cisco7206vvr	Cisco7204vvr、 Cisco7206vvr
包转发率	进程交换：13kPacket/s 快速交换：233kPacket/s	进程交换：20kPacket/s 快速交换：420kPacket/s	进程交换：79kPacket/s 快速交换：1MPacket/s
图片			

说明：Cisco7200 系列路由器由以下几部分组成：机箱、电源、引擎、接口控制器和接口板，如图 2-40 所示。因此我们在购买 7200 系列路由器是就要为其选择相应的机箱、电源、引擎、接口控制器和接口板。最新的引擎 NPE-G1 不需配置接口控制器。



图 2-40 Cisco 7200 系列路由器的组成

如图 2-41 所示，从体系机构上看，Cisco7200 系列路由器的 1、3、5 和 I/O 插槽共用一条 PCI 总线，2、4、6 插槽共用一条 PCI 总线。共用一条总线的设备相互之间会产生竞争，为了使所选的设备不至于负载过重，Cisco 为 Cisco7200 系列路由器设置了一个“点数”规则，它为每一个接口卡和接口控制器根据其速率的高低分配了相应的点数，而机箱的 1、3、5 槽所插的接口卡和 I/O 控制器插槽所插 I/O 控制器点数之和以及 2、4、6 槽所插的接口卡点数之和都不能超过一定的点数。规定的点数根据所采用的引擎的不同有所不同，下面对不同的引擎分别进行介绍。

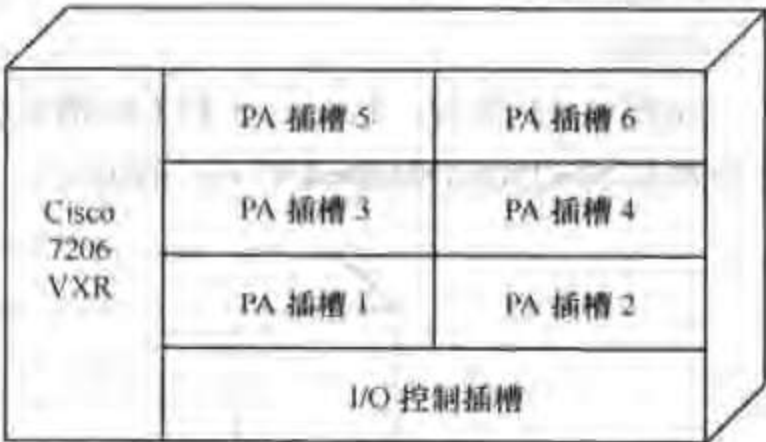


图 2-41 Cisco 7200 系列路由器的体系结构

1. NPE-G1

对于引擎 NPE-G1，它为每一个接口卡和接口控制器根据其速率的高低分配为相应的点数，具体点数如表 2-15 所示。

表 2-15 对于引擎 NPE-G1，各路由器的点数

Product ID	Points	Product ID	Points	Product ID	Points
PA-A2-4E1XC-E3ATM	90	PA-MC-2T3+	180	PA-1C-E	100
PA-A2-4E1XC-OC3SM	300	PA-MC-E3	90	PA-1C-P	0
PA-A2-4T1C-OC3SM	300	PA-MC-T3	90	PA-POS-OC3MM	300
PA-A2-4T1C-T3ATM	90	PA-SRP-OC12MM	300	PA-POS-OC3SMI	300
PA-A3-8E1IMA	34	PA-SRP-OC12SMI	300	PA-POS-OC3SML	300
PA-A3-8T1IMA	24	PA-SRP-OC12SML	300	PA-4E1G/120	0
PA-A3-E3	90	PA-SRP-OC12SMX	300	PA-4E1G/75	0
PA-A3-OC3MM	300	PA-4E	40	PA-4T+	0
PA-A3-OC3SMI	300	PA-5EFL	50	PA-8T-232	0
PA-A3-OC3SML	300	PA-8E	80	PA-8T-V35	0
PA-A3-T3	90	PA-2FE-TX	400	PA-8T-X21	0
PA-MC-2E1/120	0	PA-2FE-FX	400	SA-ISA	200
PA-MC-2T1	0	PA-2FEISL-FX	400	SA-VAM	300
PA-MC-4T1	0	PA-2FEISL-TX	400	PA-2T3	180
PA-MC-8E1/120	0	PA-FE-FX	200	PA-2T3+	180

续表					
Product ID	Points	Product ID	Points	Product ID	Points
PA-MC-8T1	0	PA FE-TX	200	PA-T3	90
PA-MCX-2TE1	32	PA-GE	400	PA-T3+	90
PA-MCX-4TE1	32	PA-2E3	180	PA-4R-DTR	120
PA-MCX-8TE1	36	PA-2H	200	PA-VXB-2TE1+	14
PA-MCX-8TE1+	0	PA-E3	90	PA-VXC-2TE1+	24
PA-MC-STM-1SMI	250	PA-H	100	C7200-I/O-2FE/E	0
PA-MC-STM-1MM	250			C7200-I/O-GE+E	0

规则:

PA Slot1+3+5+I/O≤600

PA Slot2+4+6≤600

例如:

如图 2-42 所示, 1、3、5 和 I/O 槽的点数总和=250+180+0=430 点≤600 点; 2、4、6 槽的点数总和=250+180+0=430 点≤600 点, 故满足要求。

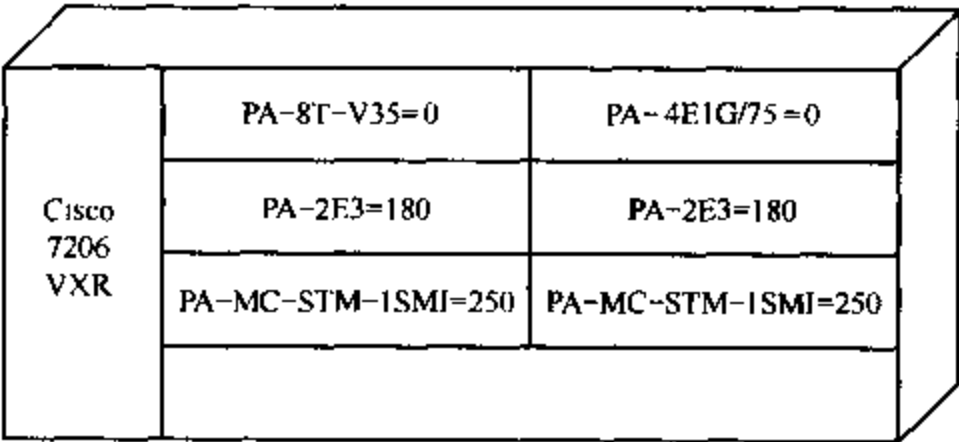


图 2-42 NPE-G1 分配点数

2. NPE-400

对于引擎 NPE-400, 它为每一个接口卡和槽口控制器槽槽其速率的高低分配为相应的点数, 具体点数如表 2-16 所示。

表 2-16 对于引擎 NPE-400, 各路由器的点数

Product ID	Points	Product ID	Points	Product ID	Points
PA-A2-4E1XC-E3ATM	90	PA-MC-2T3+	180	PA-1C-E	100
PA-A2-4E1XC-OC3SM	300	PA-MC-E3	90	PA-1C-P	0
PA-A2-4T1C-OC3SM	300	PA-MC-T3	90	PA-POS-OC3MM	300
PA-A2-4T1C-T3ATM	90	PA-SRP-OC12MM	300	PA-POS-OC3SMI	300
PA-A3-8E1IMA	34	PA-SRP-OC12SMI	300	PA-POS-OC3SML	300
PA-A3-8T1IMA	24	PA-SRP-OC12SML	300	PA-4E1G/120	0
PA-A3-E3	90	PA-SRP-OC12SMX	300	PA-4E1G/75	0
PA-A3-OC3MM	300	PA-4E	40	PA-4T+	0
PA-A3-OC3SMI	300	PA 5EFL	50	PA-8T-232	0
PA-A3-OC3SML	300	PA-8E	80	PA-8T-V35	0
PA-A3-T3	90	PA-2FE-TX	400	PA-8T-X21	0
PA-MC-2E1/120	0	PA-2FE-FX	400	SA-ISA	200

续表

Product ID	Points	Product ID	Points	Product ID	Points
PA-MC-2T1	0	PA-2FEISL-FX	400	SA-VAM	300
PA-MC-4T1	0	PA-2FEISL-TX	400	PA-2T3	180
PA-MC-8E1/120	0	PA-FE-FX	200	PA-2T3+	180
PA-MC-8T1	0	PA-FE-TX	200	PA-T3	90
PA-MCX-2TE1	32	PA-GE	400	PA-T3+	90
PA-MCX-4TE1	32	PA-2E3	180	PA-4R-DTR	120
PA-MCX-8TE1	36	PA-2H	200	PA-VXB-2TE1+	14
PA-MCX-8TE1+	0	PA-E3	90	PA-VXC-2TE1+	24
PA-MC-STM-1SMI	250	PA-H	100	C7200-I/O-2FE/E	0
PA-MC-STM-1MM	250			C7200-I/O-GE+E	0

规则:

PA Slot1+3+5+I/O≤600

PA Slot2+4+6≤600

例如:

如图 2-43 所示, 1、3、5 和 I/O 槽的点数总和=400+180+0=580 点≤600 点; 2、4、6 槽的点数总和=250+180+0=430 点≤600 点, 故满足要求。

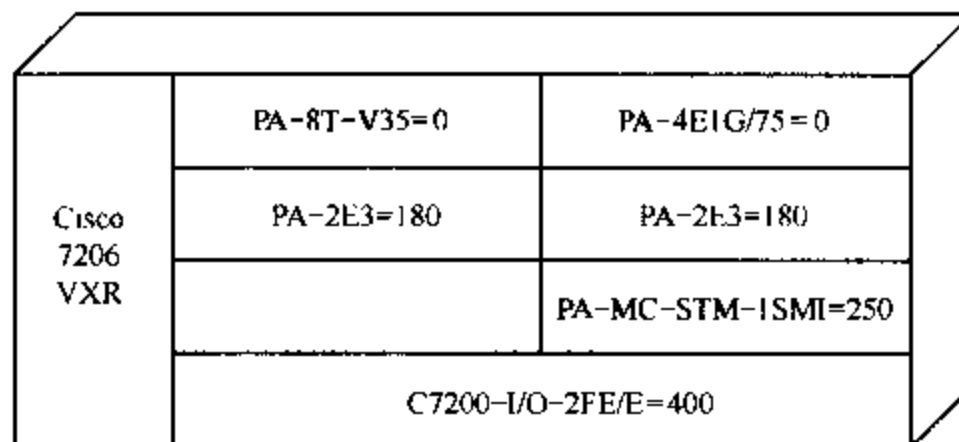


图 2-43 NPE-400 分配点数

3. NPE-225

对于引擎 NPE-225, 它为每一个接口卡和接口控制器根据其速率的高低分配为“high”、“medium”、“low”3 个不同的分值, 见表 2-17。

表 2-17 对于引擎 NPE-225, 各路由器的点数

Product ID	Bandwidth	Product ID	Bandwidth	Product ID	Bandwidth
PA-A2-4E1XC-E3ATM	High	PA-MC-2T3+	High	PA-1C-E	High
PA-A2-4E1XC-OC3SM	High	PA-MC-E3	High	PA-1C-P	Low
PA-A2-4T1C-OC3SM	High	PA-MC-T3	High	PA-POS-OC3MM	High
PA-A2-4T1C-T3ATM	High	PA-SRP-OC12MM	High	PA-POS-OC3SMI	High
PA-A3-8E1IMA	Low	PA-SRP-OC12SMI	High	PA-POS-OC3SML	High
PA-A3-8T1IMA	Low	PA-SRP-OC12SML	High	PA-4E1G/120	Low
PA-A3-E3	High	PA-SRP-OC12SMX	High	PA-4E1G/75	Low
PA-A3-OC3MM	High	PA-4E	Medium	PA-4T+	Low
PA-A3-OC3SMI	High	PA-5EFL	Medium	PA-8T-232	Low

续表

Product ID	Bandwidth	Product ID	Bandwidth	Product ID	Bandwidth
PA-A3-OC3SML	High	PA-8E	Medium	PA-8T-V35	Low
PA-A3-T3	High	PA-2FE-TX	High	PA-8T-X21	Low
PA-MC-2E1/120	Low	PA-2FE-FX	High	SA-ISA	High
PA-MC-2T1	Low	PA-2FEISL-FX	High	SA-VAM	High
PA-MC-4T1	Low	PA-2FEISL-TX	High	PA-2T3	High
PA-MC-8E1/120	Low	PA-FE-FX	High	PA-2T3+	High
PA-MC-8T1	Low	PA-FE-TX	High	PA-T3	High
PA-MCX-2TE1	Low	PA-2E3	High	PA-T3+	High
PA-MCX-4TE1	Low	PA 2H	High	PA-4R-DTR	High
PA-MCX-8TE1	Low	PA-E3	High	PA-VXB-2TE1+	Low
PA-MC-8TE1+	Low	PA-H	High	PA-VXC-2TE1+	Low
PA-MC-STM-1SMI	High			C7200-I/O-2FE/E	High
PA-MC-STM-1MM	High				

规则:

PA Slot1+3+5+I/O 加 PA Slot2+4+6≤3 “high”

并且 PA Slot1+3+5+I/O 加 PA Slot2+4+6≤5 “medium” +1 “high”

并且 PA Slot1+3+5+I/O 加 PA Slot2+4+6 的点数≤800 点（点数值参考 NPE-400 的点数）

例如:

如图 2-44 所示，PA Slot1+3+5+I/O 加 PA Slot2+4+6=2 “high” +2 “low”，且总点数为 580，符合规则要求。

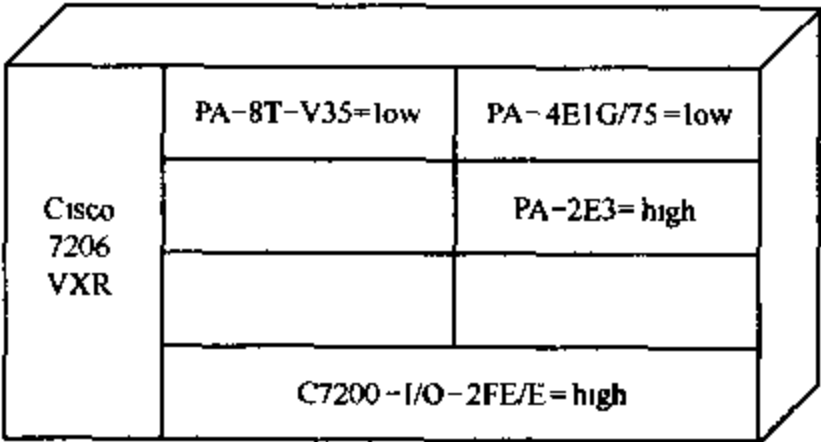


图 2-44 NPE-225 分配点数

注意:

- (1) 如果 7200 发现一条总线已经过载了，它会发出警告，但会试图正常地转发数据，这样的结果会导致路由器的不稳定，也许会产生不可预知的结果；
- (2) NPE-G1 不需要 I/O 控制器，它自带的 3 个 10/100/1000Mbit 自适应以太网端口，并不占用任何点数；
- (3) 当 PA 处于 “administratively shutdown” 状态时，它仍然占用点数；
- (4) 为了使 7200 能有最佳的性能，我们应将最高速的 PA 模块插在 2 槽，然后模速率由高到低的顺序依次插入 1、4、3、6、5 槽。

上述介绍的各路由器和引擎的结构如图 2-45~2-52 所示。

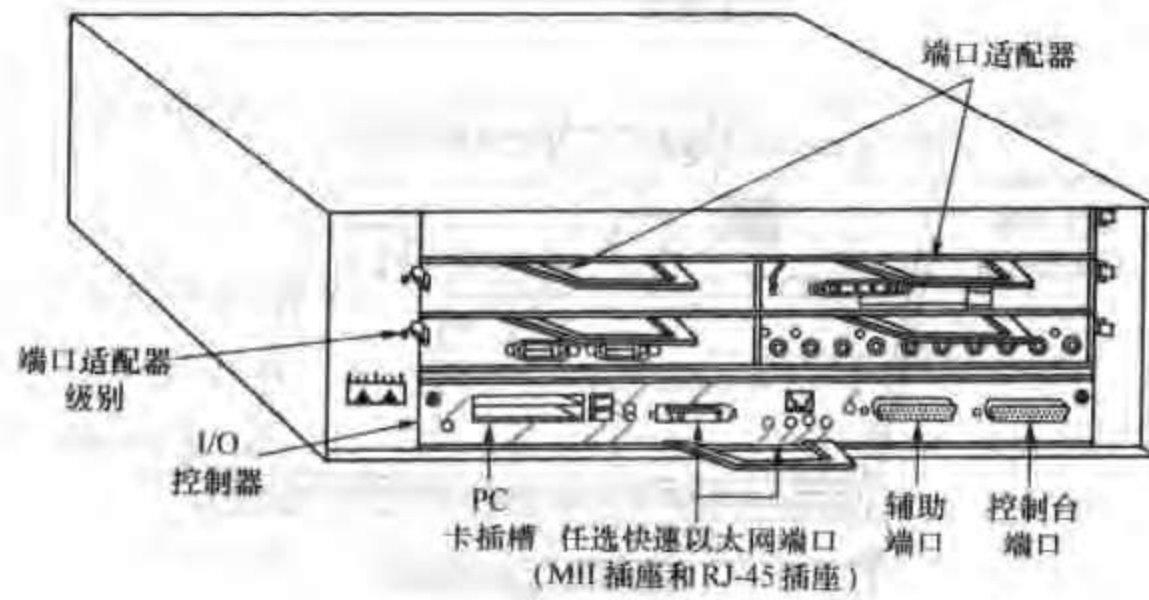


图 2-45 Cisco7204VXR

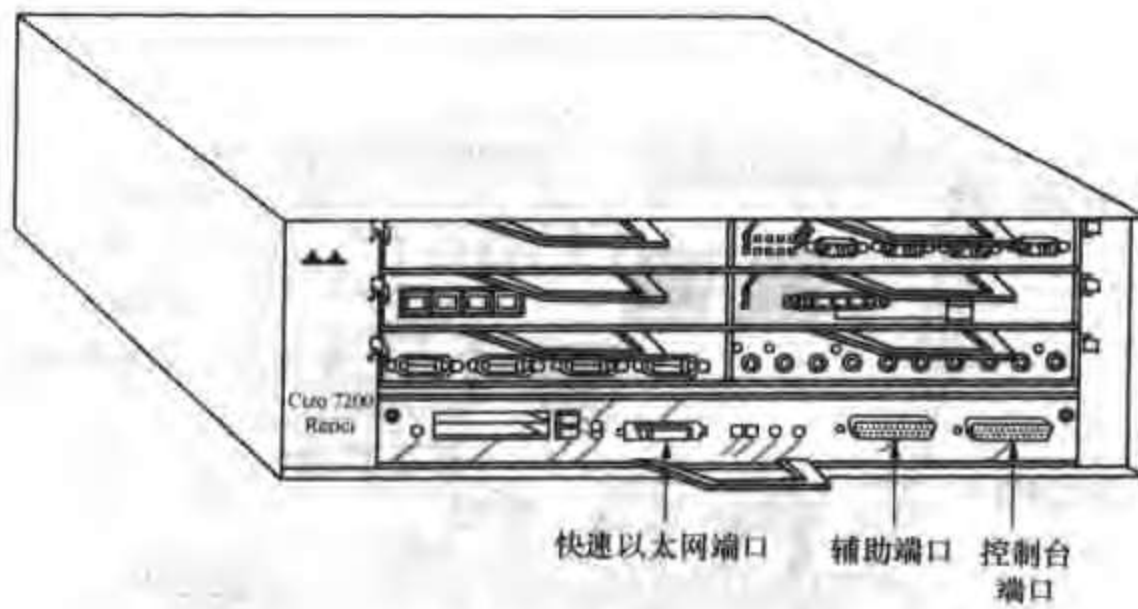


图 2-46 Cisco7206VXR

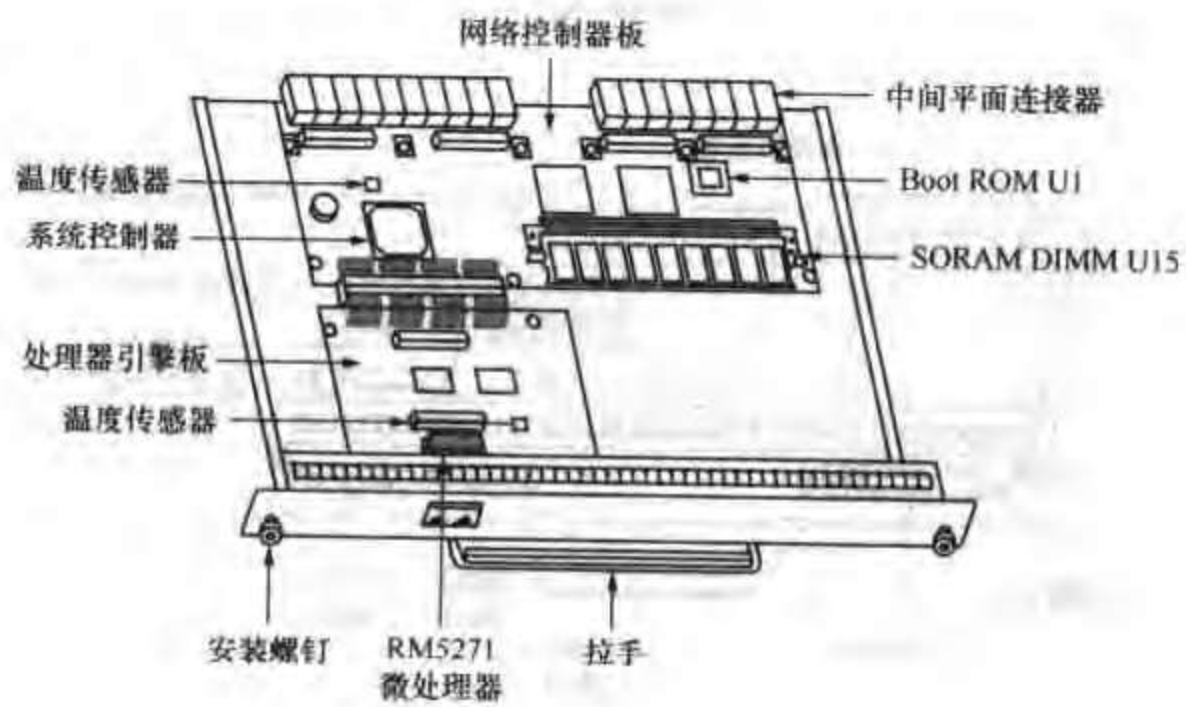


图 2-47 NPE-225

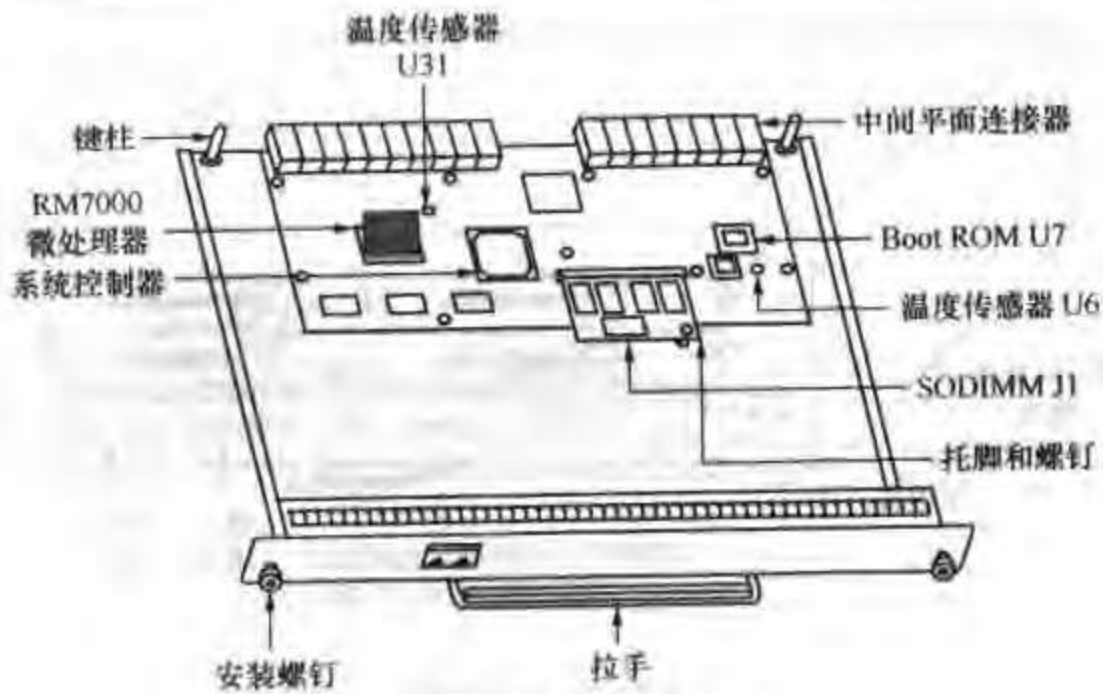


图 2-48 NPE-400

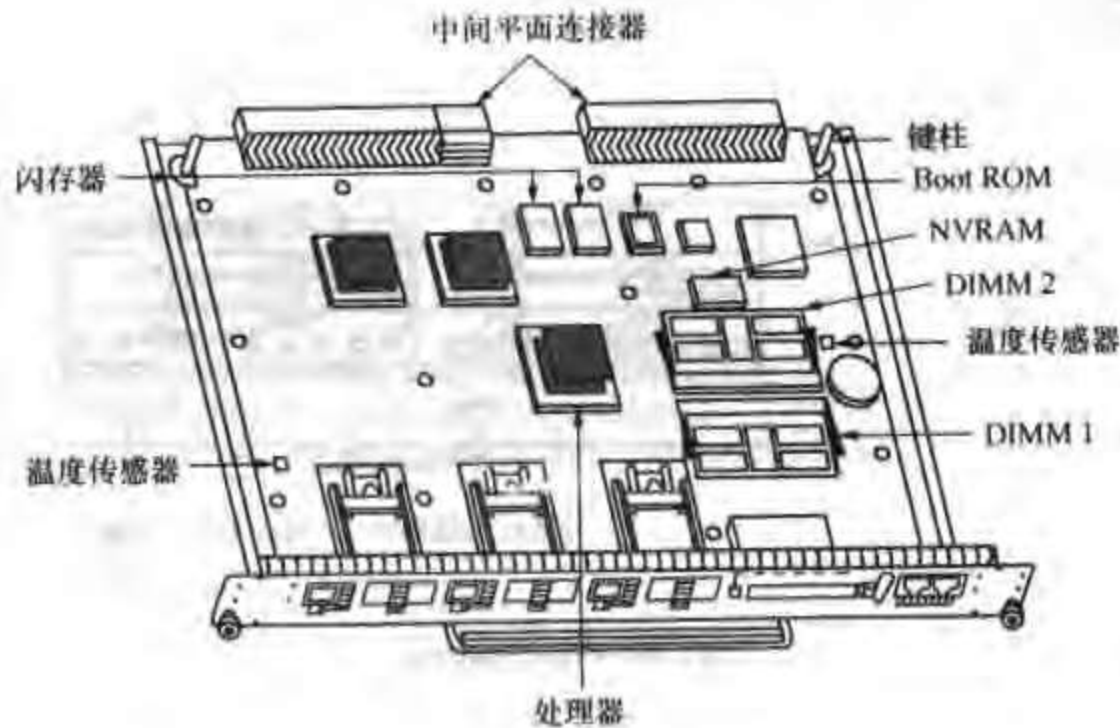


图 2-49 NPE-G1

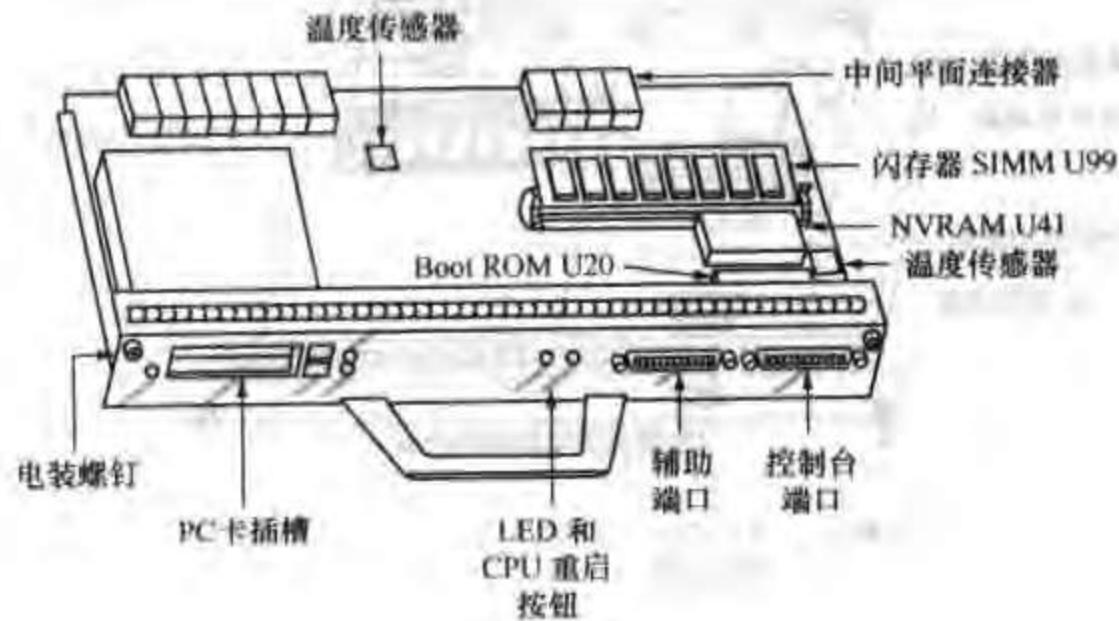


图 2-50 C7200-I/O

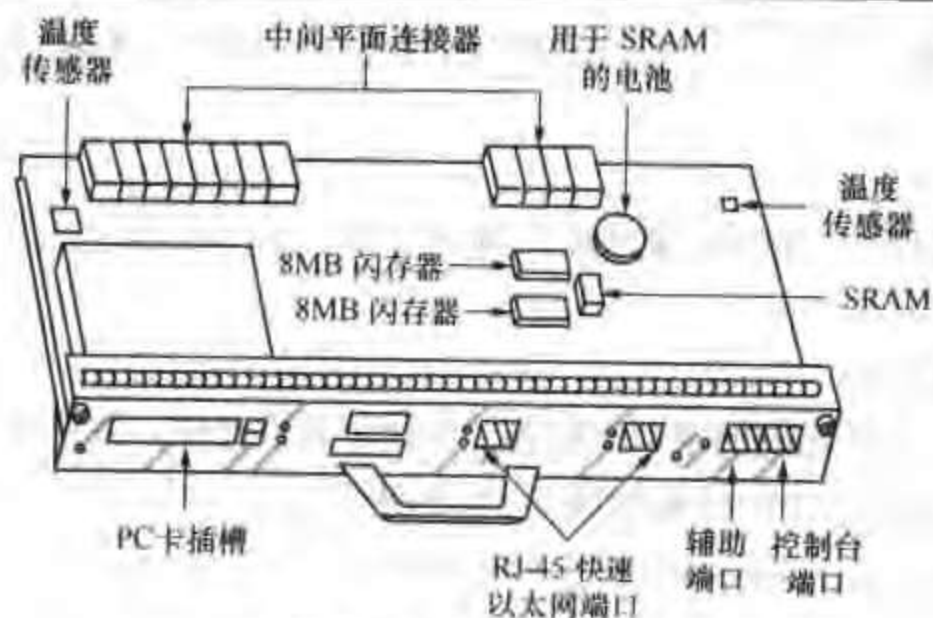


图 2-51 C7200-I/O-2FE/E

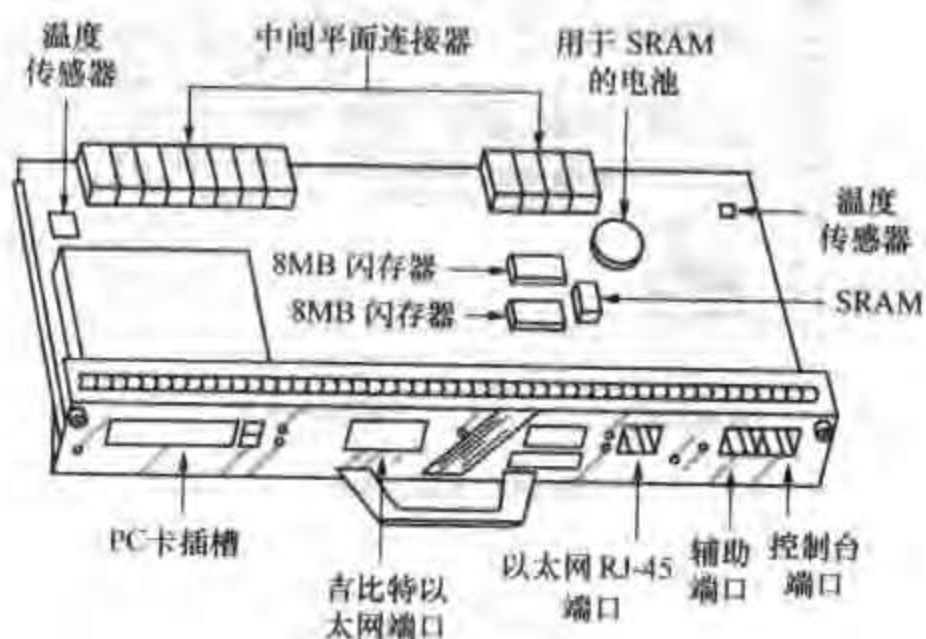


图 2-52 C7200-I/O-GE+E

如果想进一步了解 Cisco 7200 系列路由器，请访问下面网址：
<http://www.cisco.com/global/CN/products/rt/7200/index.shtml>

2.5.6 Cisco 7500 系列路由器

Cisco 7500 系列路由器（如图 2-53 所示）是 Cisco 主要的高端多协议路由器平台。这些系统结合了 Cisco 行之有效的软件技术以及卓越的可靠性、可用性、服务能力和性能特性，可以满足当今最关键的互联网的需求。Cisco 7500 系列给信息系统专业人员提供所需的灵活性，使他们能够满足互联网核心和分布点不断变化的要求。

Cisco 7500 系列路由器的关键特性如下：

（1）高性能交换

通过支持高速介质和高密度配置，为关键任务应用提供高度的性能；通过利用通用接口处理器（VIP）和 Cisco Express Forwarding 的处理功能，Cisco 7500 系列的系统容量每秒可以超过 100 万个信息包。

（2）全面的 Cisco IOS 软件支持和高性能网络服务的增强



图 2-53 Cisco 7500 系列路由器

高速执行服务质量、安全、压缩和加密等网络服务；VIP 技术通过分布式 IP 服务扩展了这些服务的性能。

(3) 高密度端口

提供高密度端口以及广泛的局域网和广域网介质，大大降低了每端口成本，并允许灵活地进行配置。

(4) 公用端口适配器

VIP 利用和 Cisco 7200 相同的端口适配器，简化了备件存储，并保护了客户的接口投资。Cisco 7500 系列各路由器的结构如图 2-54~2-59 所示。

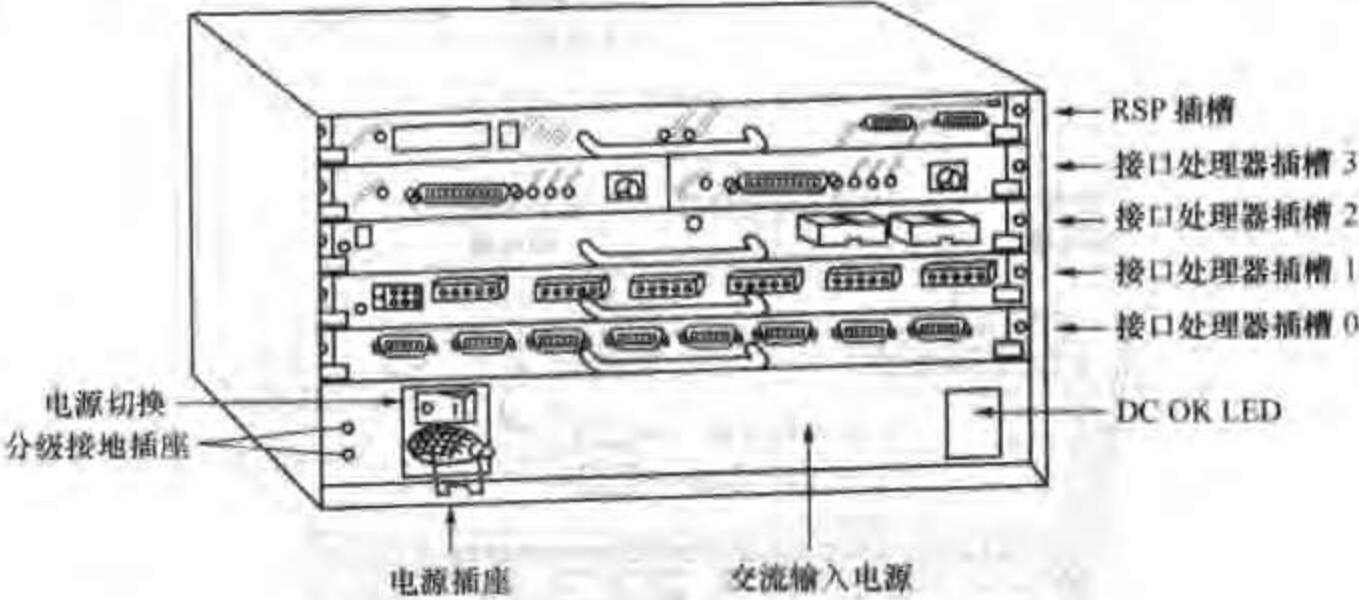


图 2-54 Cisco7505

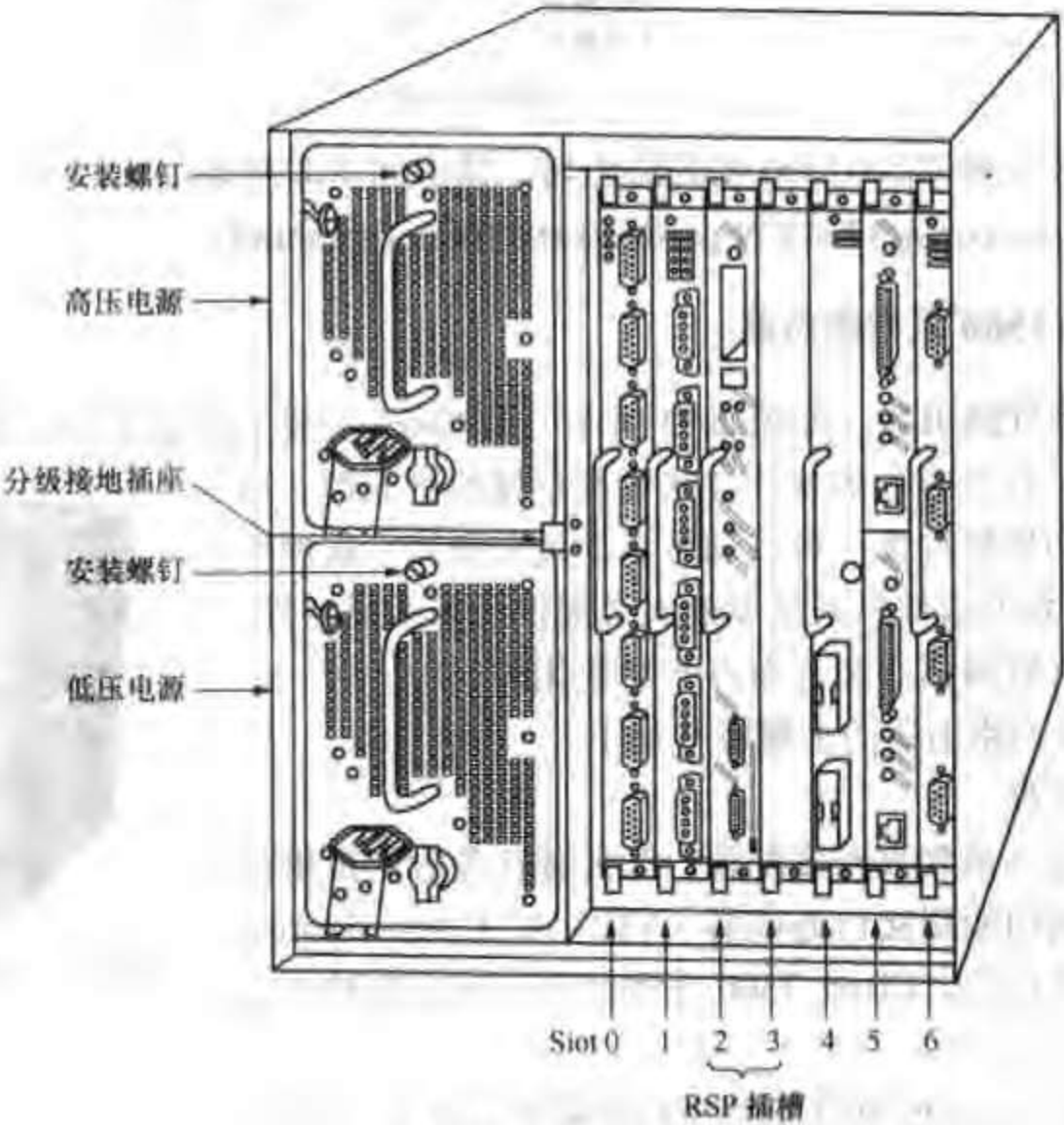


图 2-55 Cisco7507

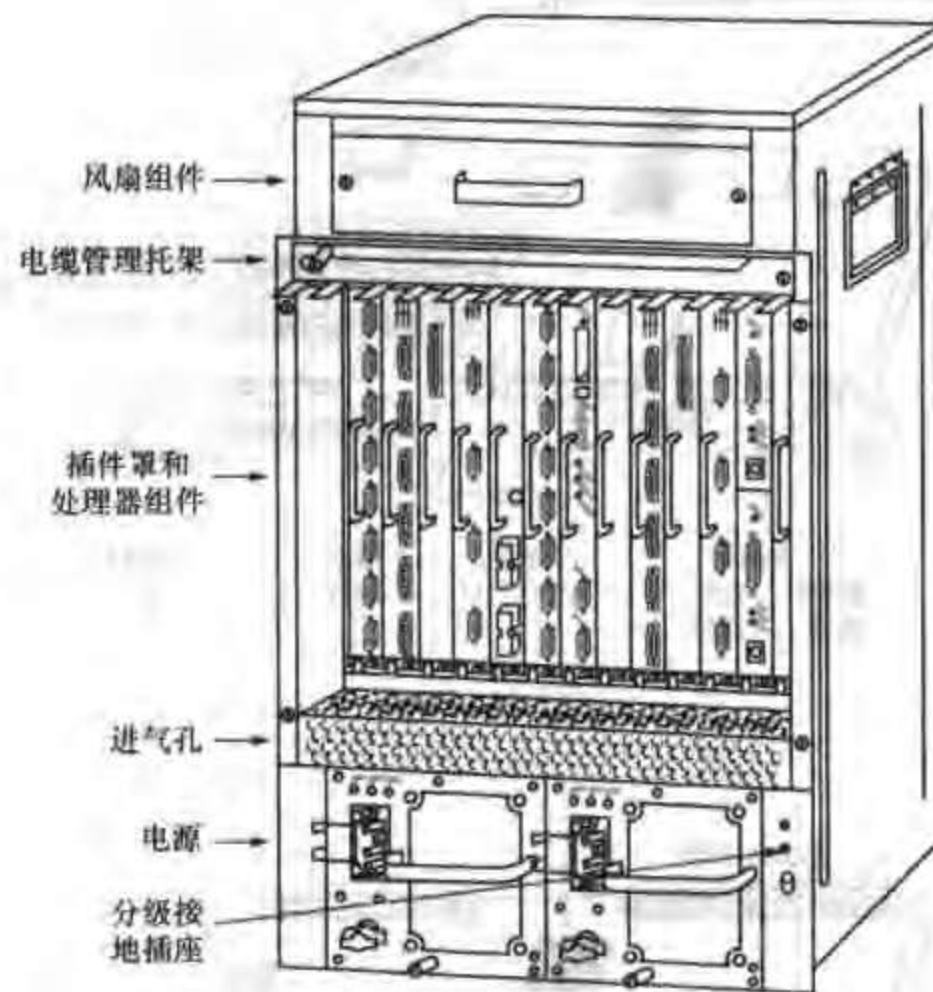


图 2-56 Cisco7513

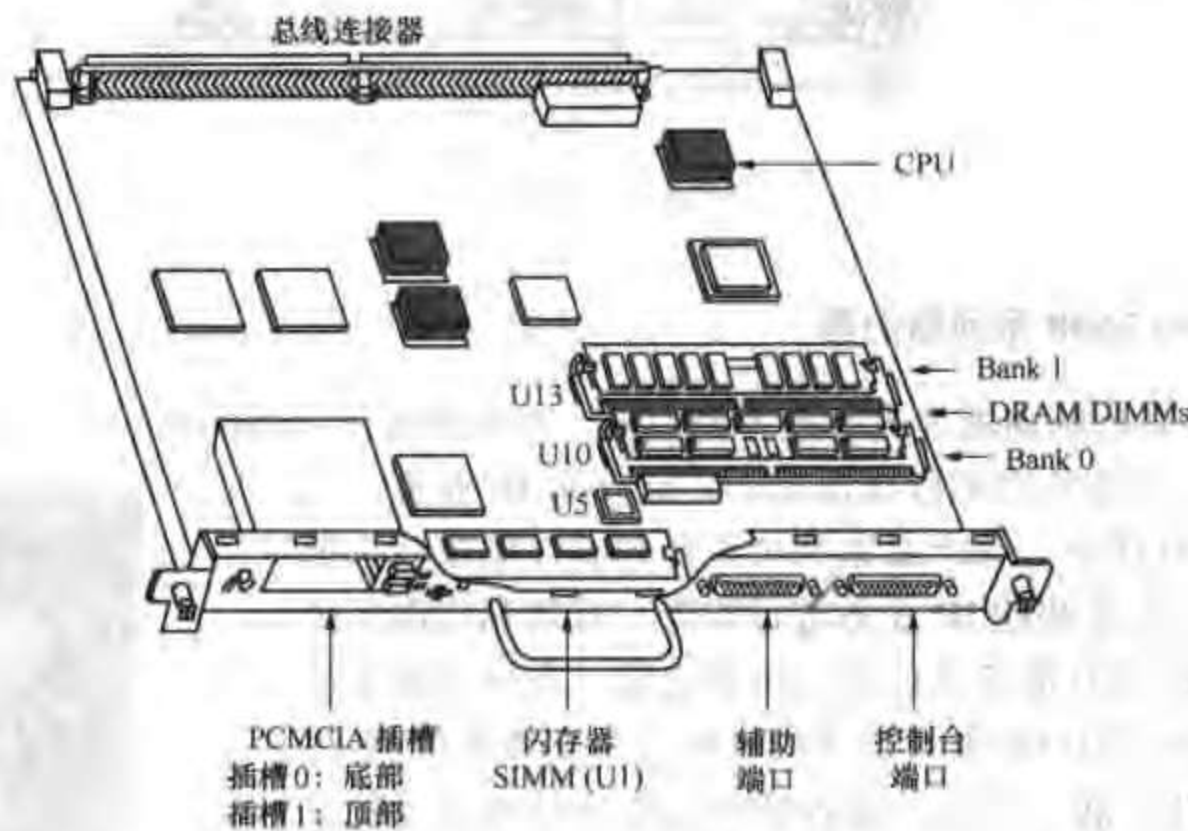


图 2-57 RSP4/RSP4+

如果想进一步了解 Cisco7500 系列路由器，请访问下面网址：

<http://www.cisco.com/global/CN/products/rt/7500/index.shtml>

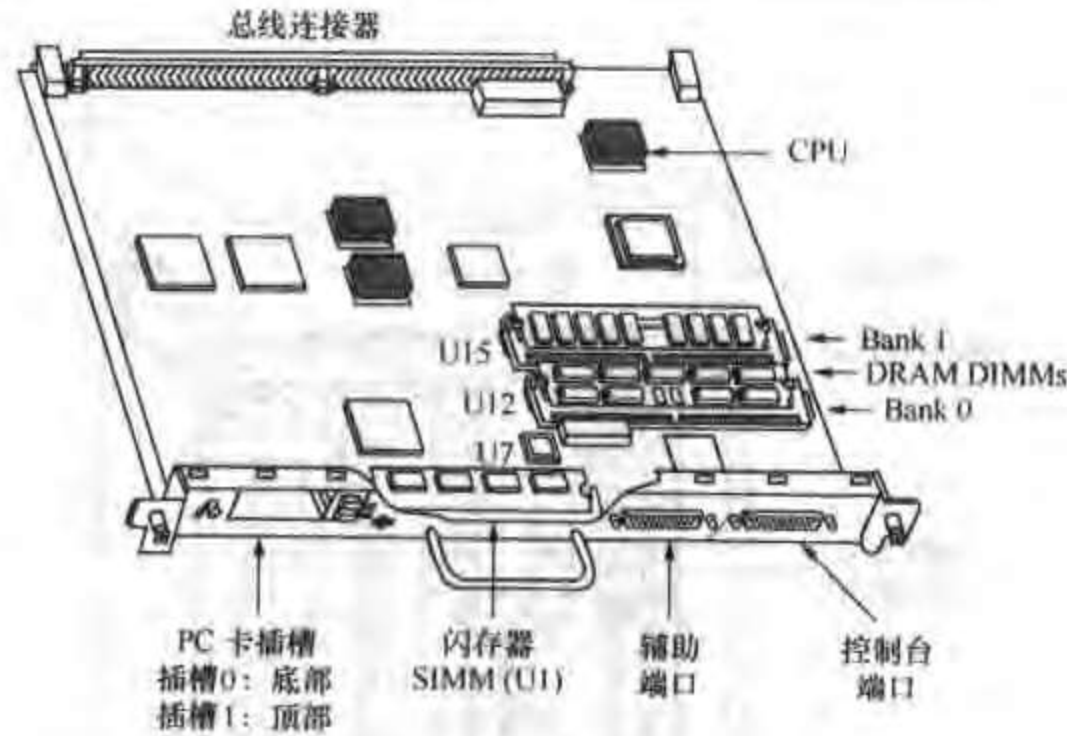


图 2-58 RSP8

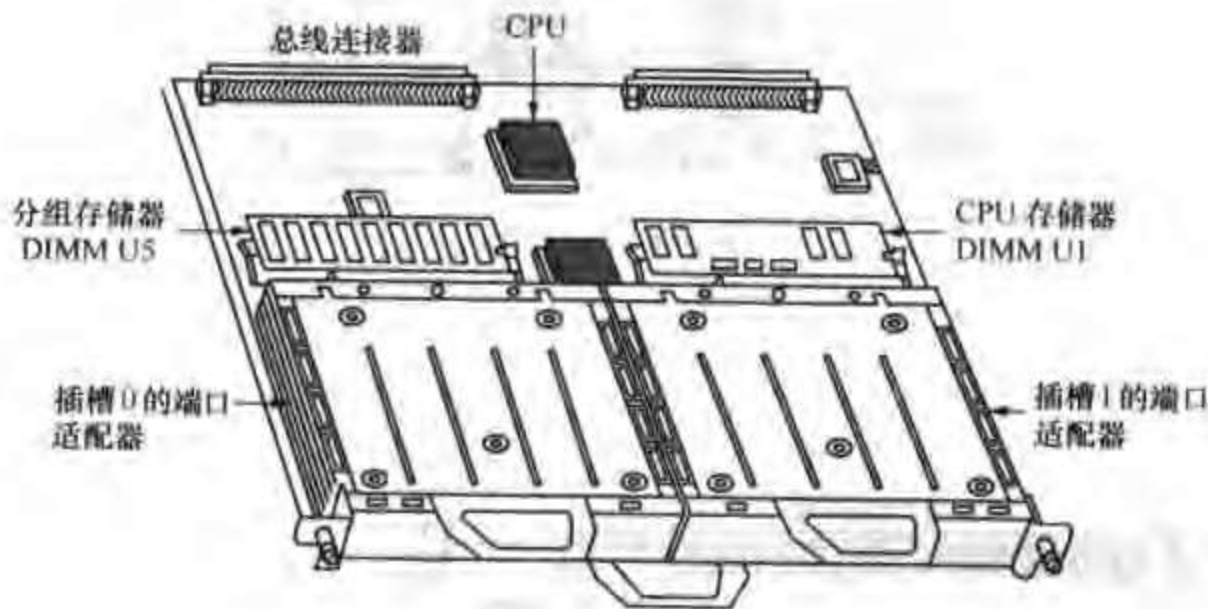


图 2-59 VIP4-80

2.5.7 Cisco 7600 系列路由器

Cisco 7600 系列路由器为光纤业务路由器，可在服务供应商的网络边缘提供光纤 WAN 和 MAN 网络，主要致力于以线速提供高起点的 IP 业务，其实物图如图 2-60 所示。该产品系列可在多种高性能接口上把直接光纤连接与大量智能 IP 业务进行组合，有效利用服务供应商网络。OSR 能在服务供应商网络的边缘（在这里业务的生成及提供对整个用户群具有巨大的影响力）实现性能和 IP 业务应用的线性扩展。目前，服务供应商能使其网络以光速支持业务，从而使其业务能够脱颖而出，赢得竞争优势。Cisco 7600 光纤业务路由器是 Cisco 端到端 IP+光纤解决方案的重要组件，能够帮助服务供应商突破业务和带宽壁垒，增加收入和利润。



图 2-60 Cisco 7600 系列路由器

说明：目前的 Cisco7600 路由器和 Catalyst6500 交换机采用相同的硬件，软件方面有所不同，未来会有所变化。

如果想进一步了解 Cisco7600 系列路由器，请访问下面网址：

<http://www.cisco.com/global/CN/products/rt/7600/index.shtml>

2.5.8 Cisco 12000 系列路由器

Cisco 12000 系列吉比特比特交换路由器（GSR）是 Cisco 为支持服务供应商和企业 IP 骨干网核心而设计和开发的重要的路由选择产品。如图 2-61 所示，Cisco 12000 系列有 3 种型号：Cisco 12008、12012 和 12016（5Tbit/s GSR 太比特系统）。

Cisco 12008 配有 8 个插槽，最多可以支持 84 个 DS3、28 个 OC-3c/STM-1c 和 28 个 OC-12c/STM-4c 或 7 个 OC-48c/STM-16c 接口。

Cisco 12012 配有 12 个插槽，最多可以支持 132 个 DS3、44 个 OC-3c/STM-1c 和 44 个 OC-12c/STM-4c 或 11 个 OC-48c/STM-16c 接口。

Cisco 12016（最新推出的 5-Tbit/s GSR 太比特系统）有 16 个插槽，最多可以支持 180 个 DS3、60 个 OC-3c/STM-1c 和 60 个 OC-12c/STM-4c 或 15 个 OC-48c/STM-16c 接口，将来还能支持 15 个 OC-192c/STM-64c 接口。

Cisco 12000 系列 GSR 产品的结构设计旨在满足当今 IP 核心骨干网的高带宽、高性能、多业务和多可靠性要求。

Cisco 12000 系列 GSR 产品的所有主要系统组件都采用了运营商级设计，提供冗余功能：处理器、交换机结构、LC、电源和冷却设备，最大限度地减少故障导致的网络中断；热切换功能可以在不中断业务的情况下增加或更换组件；交换结构冗余使业务可以在发生故障时切换到备份结构，而不会丢失数据或中断用户会话；自动保护切换（APS）/复用段保护（MPS）可实现 SONET/SDH 恢复功能，从而提供接口冗余度。

Cisco 12000 系列 GSR 产品符合网络设备构建系统（NEBS）和欧洲电信标准协会（ETSI）的标准，因此可安装在服务供应商的中心交换局。

如果想进一步了解 Cisco 12000 系列路由器，请访问下面网址：

<http://www.cisco.com/global/CN/products/rt/12000/index.shtml>



图 2-61 Cisco 12000 系列路由器

2.6 Cisco 防火墙产品

世界领先的 Cisco Secure PIX 防火墙系列，能够为当今的网络客户提供无与伦比的安全性、可靠性和性能。它所提供的完全防火墙保护以及 IP 安全（IPSec）虚拟专用网（VPN）

能够将内部网络与外部严格分开。Cisco 的防火墙产品以“PIX”为商标,包含 501、506、515、525、535 等多款产品。目前,网络集成项目中常用的 Cisco 防火墙有以下几个产品: 501、506E、515E、525E 和 535E,如图 2-62 所示。下面分别介绍一下这几个产品。

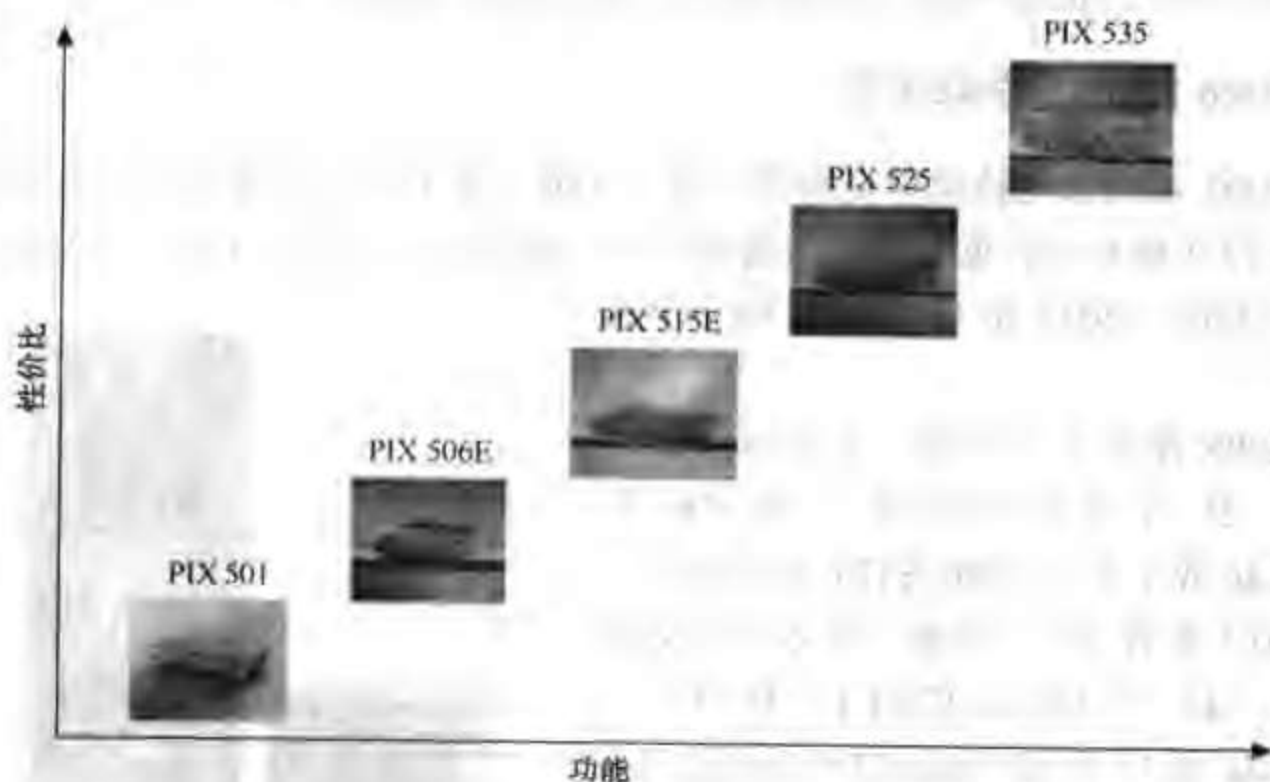


图 2-62 Cisco 防火墙产品线

2.6.1 Cisco PIX501 系列防火墙

Cisco PIX 501 防火墙（如图 2-63 所示）可以通过一个可靠的、即插即用的安全设备为小型办公室和远程办公人员提供企业级的安全性。Cisco PIX 501 防火墙是市场领先的 Cisco PIX 防火墙系列的一部分，可以通过一个紧凑的、整合的解决方案提供强大的安全功能、小型办公室联网功能和强大的远程管理功能，尤其适用于保障高速的、“永续运行的”宽带环境的安全。



图 2-63 Cisco PIX501 系列防火墙

1. 针对小型办公室环境的企业级安全性

Cisco PIX 501 防火墙是一种针对特定需求而设计的安全设备，可以在单独的一个设备中提供丰富的安全服务，包括状态监测防火墙、虚拟专用网（VPN）和入侵防范等。利用 Cisco 最新的自适应安全算法（ASA）和 PIX 操作系统，PIX 501 可以确保其后的所有用户的安全，并可以帮助他们防范互联网的潜在威胁。它的功能强大的状态监测技术可以跟踪所有经过授权的用户网络请求，防止未经授权的用户对网络访问。利用 PIX 501 灵活的访问控制功能，管理员还可以对经过防火墙的网络流量实施定制的策略。

Cisco PIX 501 防火墙还可以利用其基于标准的互联网密钥交换（IKE）/IP 安全（IPSec）VPN 功能，确保远程办公机构通过互联网与企业网络之间进行的所有网络通信的安全。通过利用 56bit 数据加密标准（DES）或者可选的高级 168bit 三重 DES（3DES）对数据进行加密，当您的敏感企业数据安全地在互联网中传输时，别人将无法窥探到它们。

PIX 501 的集成化入侵防范功能可以防止您的网络受到各种常见的攻击。通过查找超过

55 种不同的攻击“签名”，PIX 可以严格检测各种攻击，并可以实时地阻截它们或者向您发出通知。

通过提供各种与 Cisco 高端吉比特 PIX 防火墙相同的安全功能，PIX 501 可以通过便于使用和部署的解决方案提供所有宽带用户非常需要的丰富的保护功能。

2. 简便的、高速的小型办公室联网

Cisco PIX 501 防火墙可以通过其集成化的、高性能四端口 10/100Mbit/s 交换机为多个计算机共享一个宽带连接提供一种方便的方法。而且，Cisco PIX 防火墙可以提供网络地址解析 (NAT) 和端口地址解析 (PAT) 等功能，因而可以隐藏您的网络设备的实际网络地址。用户还可以利用 PIX 中内置的动态主机配置协议 (DHCP) 服务器获得即插即用的联网功能，DHCP 服务器在启动以后可以自动为其管辖的计算机分配网络地址。Cisco PIX 501 防火墙可以提供与大多数宽带联网环境无缝集成所必需的各种功能。

3. 强大的远程管理功能

PIX 501 是一个可靠的、便于维护的平台，可以提供多种配置、监控和诊断方式。PIX 管理解决方案的范围非常广泛：从一个集成化的、基于 Web 的管理工具到集中的、基于策略的工具，以及对各种远程监控协议的支持，例如简单网络管理协议 (SNMP) 和系统日志。

PIX 设备管理器 (PDM) 可以为管理员提供一个直观的、基于 Web 的界面，从而使他们可以方便地配置和监控一台 PIX 501，而不需要在管理员的计算机上安装任何软件（除了一个标准的 Web 浏览器以外）。管理员可以利用 PIX 501 所提供的命令行界面 (CLI)，通过多种方式（包括远程登陆、安全解释程序 (SSH)，以及通过控制端口实现的带外接入）对 PIX 501 进行远程配置、监控和诊断。

管理员还可以通过 Cisco VPN/安全管理解决方案 (VMS) 中提供的 Cisco 安全策略管理器 (CSPM) 3.0 方便地对很多 PIX 501 防火墙进行远程管理。CSPM 3.0 是一种可扩展的、下一代的 PIX 防火墙集中管理解决方案，具有多种功能，包括基于任务的接口、交互式网络拓扑图、策略向导和策略输出功能等。

4. 软件使用许可证

(1) 10 名用户使用许可证

Cisco PIX 501 防火墙的 10 名用户使用许可证可以支持 10 个并发的源 IP 地址从内部网络经过 PIX 501。集成的 DHCP 服务器最多可以支持 32 个 DHCP 出租。

(2) 50 名用户使用许可证

Cisco PIX 501 防火墙的 50 名用户使用许可证，最多可以支持 50 个并发的源 IP 地址从内部网络经过 PIX 501。集成的 DHCP 服务器最多可以支持 128 个 DHCP 出租。随着企业需求的增长，还可以购买一个将用户数量从 10 名增加到 50 名用户的升级使用许可证，从而增加企业对 PIX 501 设备的投资价值。

(3) 3DES 和 DES 使用许可证

在订购 PIX 501 时，可以选择两种加密使用许可证（168bit 3DES 和 56bit DES）中的一种，或者可以在购买以后再进行升级。请注意，这些使用许可证受到美国对于加密技术出口限制的制约。

如果想进一步了解 PIX501 防火墙，请访问下面网址：

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2031/index.html>

2.6.2 Cisco PIX506E 系列防火墙

Cisco PIX 506E 系列防火墙（如图 2-64 所示）是应用极为广泛的 Cisco PIX 506 防火墙的增强版本，可以通过一个可靠的、强大的安全设备为远程办公室和分支机构提供企业级的安全性。Cisco PIX 506E 防火墙是市场领先的 Cisco PIX 防火墙系列的一部分，可以通过一个经济有效的、高性能的解决方案提供丰富的安全功能和强大的远程管理功能，尤其适用于为远程/分支机构保障互联网连接。PIX 506E 还提供了更高的 3DES VPN 性能，在使用某些应用时，性能比 PIX 506 高出 70%。



图 2-64 Cisco PIX506E 系列防火墙

1. 针对远程办公室/分支机构环境的企业级安全性

Cisco PIX 506E 防火墙是一种针对特定需求而设计的安全设备，可以在单独的一个设备中提供丰富的安全服务，包括状态监测防火墙、虚拟专用网（VPN）和入侵防范等。利用思科最新的自适应安全算法（ASA）和 PIX 操作系统，PIX 506E 可以确保其后的所有用户的安全，并可以帮助他们防范互联网的潜在威胁。它的功能强大的状态监测技术可以跟踪所有经过授权的用户网络请求，防止未经授权的用户对网络访问。利用 PIX 506E 灵活的访问控制功能，管理员还可以对经过防火墙的网络流量实施定制的策略。PIX 506E 与您的后端企业数据库无缝集成，因此可以通过直接使用 TACACS/RADIUS 或间接使用 Cisco 安全访问控制服务器（ACS）严格验证外部对网络资源的访问。

Cisco PIX 506E 防火墙还可以利用其基于标准的互联网密钥交换（IKE）/IP 安全（IPSec）VPN 功能，确保远程办公机构通过互联网与企业网络之间进行的所有网络通信的安全。通过利用 56bit 数据加密标准（DES）或者可选的高级 168bit 三重 DES（3DES）对数据进行加密，当您的敏感企业数据安全地在互联网中传输时，别人将无法窥探到它们。

PIX 506E 的集成化入侵防范功能可以防止您的网络受到各种常见的攻击。通过查找超过 55 种不同的攻击“签名”，PIX 可以严格检测各种攻击，并可以实时地阻截它们或者向您发出通知。

2. 强大的远程管理功能

Cisco PIX 506E 是一个可靠的、便于维护的平台，可以提供多种配置、监控和诊断方式。PIX 管理解决方案的范围非常广泛：从一个集成化的、基于 Web 的管理工具到集中的、基于策略的工具，以及对各种远程监控协议的支持，例如简单网络管理协议（SNMP）和系统日志。

PIX 设备管理器（PDM）可以为管理员提供一个直观的、基于 Web 的界面，从而使他们可以方便地配置和监控一台 PIX 506E，而不需要在管理员的计算机上安装任何软件（除了一个标准的 Web 浏览器以外）。管理员可以利用 PIX 506E 所提供的命令行界面（CLI），通过多种方式（包括远程登陆、安全解释程序（SSH），以及通过控制端口实现的带外接入）对 PIX 506E 进行远程配置、监控和诊断。

管理员还可以通过 Cisco VPN/安全管理解决方案（VMS）中提供的 Cisco 安全策略管理

器 (CSPM) 方便地对很多 PIX 506E 防火墙进行远程管理。CSPM 3.0 是一种可扩展的、下一代的 PIX 防火墙集中管理解决方案, 具有多种功能, 包括基于任务的接口、交互式网络拓扑图、策略向导、策略输出功能等。

3. 软件使用许可证

这里只介绍 3DES 和 DES 使用许可证。在订购 PIX 506E 时, 可以选择两种加密使用许可证 (168bit 3DES 和 56bit DES) 中的一种, 或者可以在购买以后再进行升级。请注意, 这些使用许可证受到美国对于加密技术出口限制的制约。

如果想进一步了解 PIX506E 防火墙, 请访问下面网址:

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps4336/index.html>

2.6.3 Cisco PIX515E 系列防火墙

Cisco PIX 515E 系列防火墙 (如图 2-65 所示) 是被广泛采用的 Cisco PIX 515 平台的增强版本, 它可以提供业界领先的状态防火墙和 IP 安全 (IPSec) 虚拟专用网服务。Cisco PIX 515E 针对中小型企业和企业远程办公机构而设计, 具有更强的处理能力和集成化的、基于硬件的 IPSec 加速功能。



图 2-65 Cisco PIX515E 系列防火墙

Cisco PIX 515E 多功能的单机架单元 (1RU) 机箱可以支持 6 个接口, 使之成为那些需要一个具

有 DMZ 支持的、成本低廉的安全解决方案的企业理想选择。作为全球领先的 Cisco PIX 防火墙系列的一部分, 它可以为今天的网络用户提供无以伦比的安全性、可靠性和性能。

Cisco PIX 515E 是一个针对特定需求而设计的防火墙设备, 可以提供前所未有的安全性。它可以与 Cisco PIX 操作系统 (OS) 紧密集成, 该操作系统是一个专用的、强化的系统, 可以消除在通用的操作环境中经常出现的安全漏洞和性能损耗。

该系统的核心是一种基于自适应安全算法 (ASA) 的保护机制, 可以提供针对状态的、面向连接的防火墙功能, 同时阻截常见的拒绝服务 (DoS) 攻击。

Cisco PIX 515E 还是一个全功能的 VPN 网关, 可以在公共网络上安全地传输数据。它可以通过 56bit 数据加密标准 (DES) 或者 168bit 三重 DES (3DES) 支持站点间和远程接入 VPN 应用。根据所选择的 Cisco PIX 515E 型号的不同, VPN 功能可以作为 Cisco PIX OS 的一项服务提供, 也可以通过一个集成的、基于硬件的 VPN 加速卡 (VAC) 提供, 这种加速卡最多可以提供 63Mbit/s 的吞吐量和 2000 个 IPSec 隧道。

通过部署一个冗余的热备份单元可以实现对高可用性的支持。这种故障恢复方式可以通过自动的状态同步保持并发的连接。这确保了即使在系统发生故障的情况下, 进程也会得以保持, 而整个切换过程对于网络用户来说是完全透明的。

该防火墙目前有 3 种型号, 分别可以提供不同等级的接口密度、故障恢复功能和 VPN 吞吐量。

1. 有限制的软件使用许可证

Cisco PIX 515E “有限制” (PIX 515E-R) 型号可以为那些寻求具有最低限度接口密度和 VPN 吞吐量的、强大的 Cisco PIX 防火墙的企业提供出色的价值。它具有 32MB 的 RAM, 最

多可以支持 3 个 10/100Mbit/s 快速以太网接口。

2. 无限制的软件使用许可证

Cisco PIX 515E 的“无限制”(PIX 515E-UR)型号可以通过集成化的、基于硬件的 VPN 加速支持状态故障恢复、添加 LAN 接口和增加 VPN 吞吐量,从而拓展了这个系列的功能。它具有一个集成化的 VAC, 64MB 的 RAM, 最多可以支持 6 个 10/100Mbit/s 快速以太网接口。Cisco PIX 515E-UR 还可以与一个热备份的 Cisco PIX 防火墙共享状态信息,从而能够实现完全的防火墙冗余。

3. 故障恢复软件使用许可证

Cisco PIX 515E 的“故障恢复”(PIX 515E-FO)型号采用了独特的设计,可以与一个 PIX 515E-UR 协作,提供一个成本非常低廉的、高可用性的解决方案。它工作在热备份模式下,所扮演的角色是一个用于保存当前进程的完整的冗余系统。它的硬件配置与 PIX 515E-UR 相同,并能够以低廉的价格提供最高等级的可用性。

如果想进一步了解 PIX515E 防火墙,请访问下面网址:

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps4094/index.html>

2.6.4 Cisco PIX525 系列防火墙

Cisco Secure PIX 525 系列防火墙(如图 5-66 所示)是世界领先的 Cisco Secure PIX 防火墙系列的组成部分,能够为当今的网络客户提供无与伦比的安全性、可靠性和性能。它所提供的完全防火墙保护以及 IP 安全(IPSec)虚拟专用网(VPN)能力是特别适合于保护企业总部的边界。

1. 强壮的安全特性

Internet 的发展为企业、政府和专用网络带来了更大的安全风险。现有的解决方案如运行在应用层的基于代理的防火墙具有很多限制条件,包括性能低、需要昂贵的通用平台、使用开放系统如 UNIX 时本身具有安全风险等。

而 Cisco Secure PIX 防火墙能够提供强大的安全保护能力,它的保护机制的核心是能够提供面向静态连接防火墙功能的自适应安全算法(ASA)。静态安全性虽然比较简单,但与包过滤相比,功能却更加强劲;另外,与应用层代理防火墙相比,其性能更高,扩展性更强。ASA 可以跟踪源和目的地址、传输控制协议(TCP)序列号、端口号和每个数据包的附加 TCP 标志。只有存在已确定连接关系的正确的连接时,访问才被允许通过 Cisco Secure PIX 防火墙。这样,内部和外部的授权用户就可以透明地访问企业资源,而同时保护了内部网络不会受到非授权访问的侵袭。

另外,实时嵌入式系统还能进一步提高 Cisco Secure PIX 防火墙系列的安全性。虽然 UNIX 服务器是广泛采用开源代码的理想开放开发平台,但通用的操作系统并不能提供最佳的性能和安全性。而专用的 Cisco Secure PIX 防火墙是为了实现安全、高性能的保护而专门设计。

2. 与 IPSec 互操作的安全 VPN

从传统上来说,防火墙通过维护所连接网段之间所有连接的静态控制实现了边界安全



图 2-66 Cisco PIX525 系列防火墙

性。目前,越来越多的客户正在寻求除了提供访问控制以外,还能提供 VPN 服务的防火墙。利用 VPN,远程用户或分布在各地的分支机构能够以更低的成本安全地访问企业网,同时,使用 Internet 访问可以大大降低与以前的专线或其他专用网络相关的电信费用。公司就不需要维护大型的 Modem 池和访问服务器来处理远程的拨号用户,而这些都是需要花费大量资金并且让管理员头痛的事情。现在,只需要向 ISP 进行本地呼叫,用户就可以通过 Internet 安全地访问专用的企业内部网 (Intranet)。

PIX 525 实现了在 Internet 或所有 IP 网络上的安全保密通信。它集成了 VPN 的主要功能——隧道、数据加密、安全性和防火墙,能够提供一种安全、可扩展的平台来更好、更经济高效地使用公共数据服务来实现远程访问、远程办公和外部网连接。PIX 525 可以同时连接高达 4 个 VPN 层,为用户提供完整的 IPSec 标准实施方法,其中 IPSec 保证了保密性、完整性和认证能力。对于安全数据加密, Cisco 的 IPSec 实现方法全部支持 56 位数据加密标准 (DES) 和 168 位三重 DES 算法。

3. 极端的可靠性

PIX 防火墙提供了空前的可靠性,其平均无故障时间 (MTBF) 超过 60000 小时。即使是达到了这样高的水平,那些把 Internet、Intranet 或 Extranet 连接当作企业生命线的企业还是认识到了防火墙冗余是一项关键因素。防火墙的每一分钟停止运行都意味着收入、机会或关键信息的接失。Cisco 已经创建了配合 PIX 525-UR 使用的故障切换捆绑程序,能够简单、便宜地满足上述要求。该程序包为企业接供了特别设计在故障切换模式下运行的第 2 个防火墙,而其价格仅是标准 PIX 525 UR 捆绑件的一小部分。

4. 令人惊奇的灵活性

Cisco Secure PIX 525 防火墙支持各种网络接口卡 (NIC)。标准 NIC 包括单端口或 4 端口 10/100Mbit/s 快速以太网、吉比特以太网、4/16 令牌环和双连接多模 FDDI 卡。

另外,PIX 525 还提供多种电源选件,用户可以选择交流或 48V 直流电源。每一种选件都配有为第 2 个“故障切换”PIX 系统准备的成对儿产品,从而实现最高的冗余和高可用性。

5. 限制软件

包含有限软件许可证的 PIX 525 提供了入门级的企业安全和性能。525-R 包括 128MB 的 RAM,能够使用多达 6 个 10/100Mbit/s 快速以太网接口。

6. 无限制软件

包含有无限制许可证的 PIX 525 是为大型企业而设计,能够提供所有 PIX 525-R 的功能。另外,PIX525-UR 还增加了静态切换到备用 PIX 防火墙的能力,支持并又增加了 2 个 (总共 8 个) 10/100Mbit/s 快速以太网端口。它具备足够的能力来处理 28 万同时连接,纯文本吞吐量高达 370 Mbit/s。

7. 出口考虑

PIX 525 加密软件可以在有控制的条件下出口。请参考有关出口控制网站:

<http://www.cisco.com/wwl/export/crypto/> 有关具体的出口问题,请与 export@cisco.com 联系。

如果想进一步了解 PIX525 防火墙,请访问下面网址:

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2118/index.html>

2.6.5 Cisco PIX535 系列防火墙

Cisco Secure PIX535 防火墙（如图 2-67 所示）提供的承载级的性能可以满足大型企业网络和服务提供商的需要。作为世界领先的 Cisco Secure PIX 防火墙系列的组成部分，PIX 535 能够为当今的网络客户提供无与伦比的安全性、可靠性和性能。该防火墙将静态防火墙和 IP 安全（IPSec）虚拟专网（VPN）功能与吉比特以太网吞吐量灵活地结合在一起。

PIX 535 是一种能够提供强大保护能力的通用防火墙设备。它与 PIX 操作系统（OS）紧密集成在一起，该操作系统是一种消除了安全漏洞和性能退化开销的专用固化系统。PIX535 防火墙的核心是基于自适应安全算法（ASA）的一种保护机制，它可以提供面向静态连接的防火墙功能，能够进行 50 万个同时连接，并同时防止常见的拒绝服务（DoS）攻击。



图 2-67 Cisco PIX535 系列防火墙

另外，PIX 535 还是一种能够通过公网安全传输数据的全功能 VPN 网关，它支持使用 56bit 数据加密标准（DES）或 168bit 3DES 对 VPN 应用进行站点到站点和远程访问。PIX 535 的集成 VPN 功能可以得到 VPN 加速卡（VAC）选件的支持，能够提供 100 Mbit/s 的吞吐量和 2000 个 IPSec 隧道。

高可用性是通过部署一个冗余的热备用单元来实现的，该故障切换选件通过自动静态同步维护了同时连接。这保证了即使是在系统故障情况下，也能够维护对话，并且保证切换过程对网络用户而言是透明地完成。另外，PIX 535 还允许您向交流或直流型号添加可选的冗余、热插拔电源，使其成为一种真正的容错安全设备。

1. 有限软件许可

包含有限软件许可的 PIX 535 配有 512MB 的 RAM，支持多达 6 个吉比特以太网或 10/100Mbit/s 快速以太网接口以及一个 VAC。

2. 无限软件许可

包含无限软件许可的 PIX 535 配有 1GB 的 RAM，支持多达 8 个吉比特以太网或 10/100Mbit/s 快速以太网接口以及一个 VAC。另外，PIX 535-UR 还添加了与热备用 PIX 共享状态信息以实现完全防火墙冗余的能力。

3. 故障切换软件许可

包含故障切换软件许可的 PIX 535 工作在热备用模式。作为维护当前对话的完整的冗余系统，它能够以很低的价格提供非常高的可用性。

如果想进一步了解 PIX535 防火墙，请访问下面网址：

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2119/index.html>

2.7 小 结

本章我们首先简要地介绍了有关网络设备选购方面的知识，然后分别对 Cisco 公司的交换机、路由器和防火墙产品进行了较为详细的介绍，尤其是对模块化的产品如何选择做了介

绍，例如，Cisco6500 系列交换机的选择包括机箱、电源、风扇、引擎、各种模块的选择等，Cisco 的模块化的产品的选择是非常复杂的，它涉及的内容非常多，这里我们希望通过简要的介绍和相应的案例来使读者能够快速地了解其中的方法，使用户知道如何去选配一台 Cisco 的模块化的产品。

本章我们提供了大量的 Cisco 网络产品的图片，目的是希望大家能对 Cisco 网络产品有一个直观的印象，而不仅局限于想象。

第3章 企业网组建

本章将涵盖下列有关企业网方面的关键主题：

- 典型企业网构成
- 企业内部局域网模块
- 企业广域互联模块
- 企业 Internet 出口模块

通过对本章的学习，希望大家能对以下一些方面有所了解：

- (1) 什么是企业网；
- (2) 常见的企业网由哪几部分组成；
- (3) 如何根据用户的需求，合理地进行产品选型，构建企业的局域网部分；
- (4) 如何根据用户的需求，合理地进行产品选型，构建企业的广域网部分；
- (5) 如何根据用户的需求，合理地进行产品选型，构建企业的 Internet 接入部分。

3.1 简介

顾名思义，企业网就是为某个企业服务的计算机网络，通常企业网包括企业内部局域网部分、总部与分支机构互连的广域网部分以及用于企业上网的 Internet 接入部分。对于不同的企业可能在设备的选择上有所不同，但总体结构上没有太大的区别，当然，对于一个小型企业，由于在外地没有分支机构，组建一个局域网也就可以满足需要了，如果有上网的需要可以再加上 Internet 接入部分。总之，我们可以根据企业的具体规模和需求来规划相应的企业网。下面我们就来详细地介绍企业网的构成，以及如何选择 Cisco 的相关设备来构建一个典型的企业网。

3.2 典型企业网构成

典型的企业网，一般会在企业总部建有一个大规模的局域网，用来连接公司总部的一座或几座大楼，以支持研发、生产、市场、销售和服务等应用。在各分支机构一般会有一个相对小一些的局域网。各分支机构和移动用户通过申请电信提供的 DDN、帧中继、数字电路、ATM 或 ISDN 等数据通信业务相互连接而构成企业的总体网路。

企业建网的根本目的在于实现信息的安全共享和加快数据交换和处理的速度，从而提高工作效率，最终实现增强企业竞争力的目的。紧紧围绕这个目的，我们就会从根本上理解企

业网络的构成。为了要实现数据的共享及快速的交换,首先,数据必须电子化,其次将各节点连接起来,这样就可以共享信息了,而通过交换机互连起来的各节点就构成了企业的局域网:如果企业需要与外界进行沟通,或对外提供服务,那么企业网就必须增加建立一个 Internet 接入网,很难想像企业会构建一个完全封闭起来局域网:如果我们的企业逐步壮大,在外地有了分支机构,而企业的许多业务也需要在网上进行,这时,就需要将分支机构和总部连接起来,构建一个企业的广域网络。我们当然可以直接铺设线路,从而构成一个更大的局域网(类比局域网的构建),如果分支机构和总部的距离较近还可以考虑,如果分支机构和总部分布在不同的城市,这样做的费用将是非常惊人的,所以即使在同一城市我们往往也不采用这种方式。那么,此时我们该如何来做呢?通常我们会采用以下几种不同的连接方式:(1)通过电信公司的已有线路进行互连,即通过申请电信公司的数据链路(DDN、Frame-Relay、数字电路、ISDN 等)完成互连;(2)通过 VPN 技术来互连,即在公用的 Internet 上建立一条私有的通道。

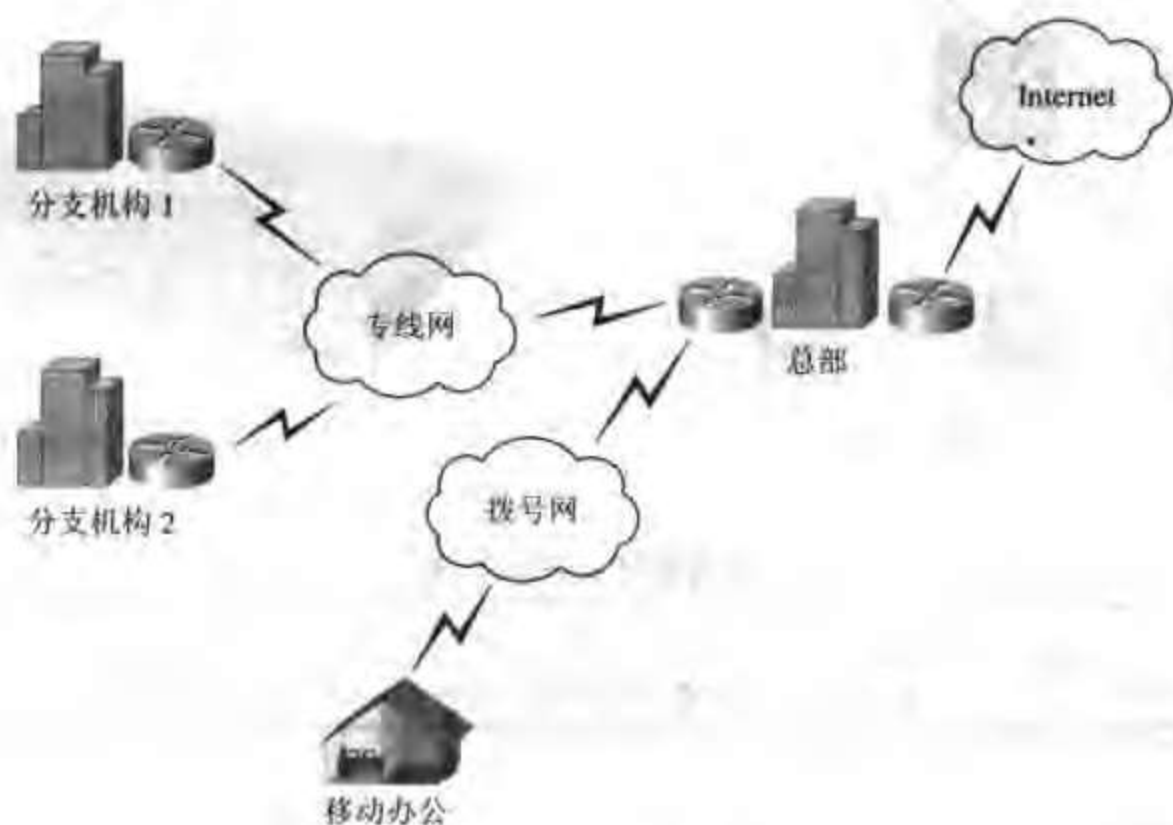


图 3-1 典型企业网

通过上述的互连,就构成了一个标准的企业网。下面我们就分不同的模块分别进行介绍。

3.3 企业内部局域网模块

3.3.1 超小型局域网

超小型局域网指公司总通信节点数在 45 点以下,数据的交换在一台交换机上即可完成的简单的网络。典型的超小型局域网如图 3-2 所示。

1. 案例 1

(1) 需求描述

企业内部需要联网的节点数为 30 点，需要百兆交换到桌面，部门之间可以任意访问。

(2) 选型分析

企业总节点数 30 点，选用一台 48 端口的低端交换机即可，可选 Catalyst2950G-48 或 Catalyst3550-48，区别是 2950 不支持三层交换而 3550 支持（三层交换可以等同为路由，区别是路由器通过软件实现路由而三层交换机通过硬件实现路由），由于本例中不需要划分 VLAN，也就不需要三层交换功能，因此我们可以选择 2950。

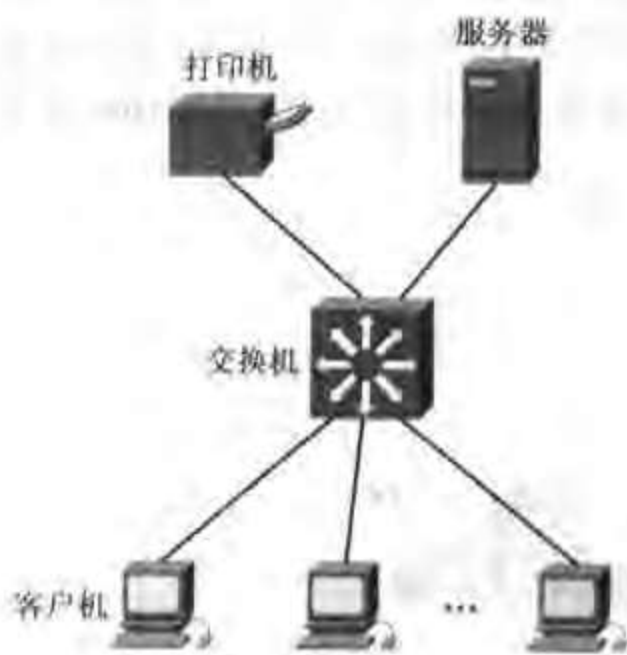


图 3-2 超小型局域网



图 3-3 Catalyst2950G-48

表 3-1 本方案选择产品列表

产 品	描 述	数 量
WS-C2950G-48-EI	带有 2 GBIC 插槽，图像增强功能的 Catalyst 2950, 48 10/100	1

2. 案例 2

(1) 需求描述

企业内部需要联网的节点数为 40 点，需要百兆交换到桌面，要求只有经理可以访问财务部的主机，财务部的主机可以对外任意访问。

(2) 选型分析

企业总节点数 45 点以下，选用一台 48 端口的低端交换机即可，可选 Catalyst2950G-48 或 Catalyst3550-48，区别是 2950 不支持三层交换而 3550 支持，在本例中需要将财务部和其他部门分割开来，即划分为不同的 VLAN（虚拟局域网），但又允许经理访问财务部的机器，这时我们需要具有三层交换功能的交换机，因此我们就选择 3550。



图 3-4 Catalyst3550-48

表 3-2

本方案所选产品列表

产 品	描 述	数 量
WS-C3550-48-SMI	48-10/100 + 2 GBIC 端口; SMI	1

说明：这里我们也可以使用 EMI 版本，但价格会更高。SMI 和 EMI 的主要区别如下：SMI 也支持路由功能但只支持静态路由和动态的 RIP 协议；EMI 支持静态路由和所有的动态路由协议（RIP、EIGRP、ISIS、OSPF、BGP 等）。

3.3.2 小型局域网

在小型局域网络中，总通信节点数一般在 45 点以上（通常在 200 点以内），网络结构一般分为两层，在核心层会有一台具有三层交换功能的交换机用于通信数据快速交换，在接入层一般为纯二层的交换机。小型局域网一般的应用集中于文件共享、办公自动化系统、邮件和网站等，它的数据多为非时间敏感型数据。典型的小型局域网如图 3-5 所示。

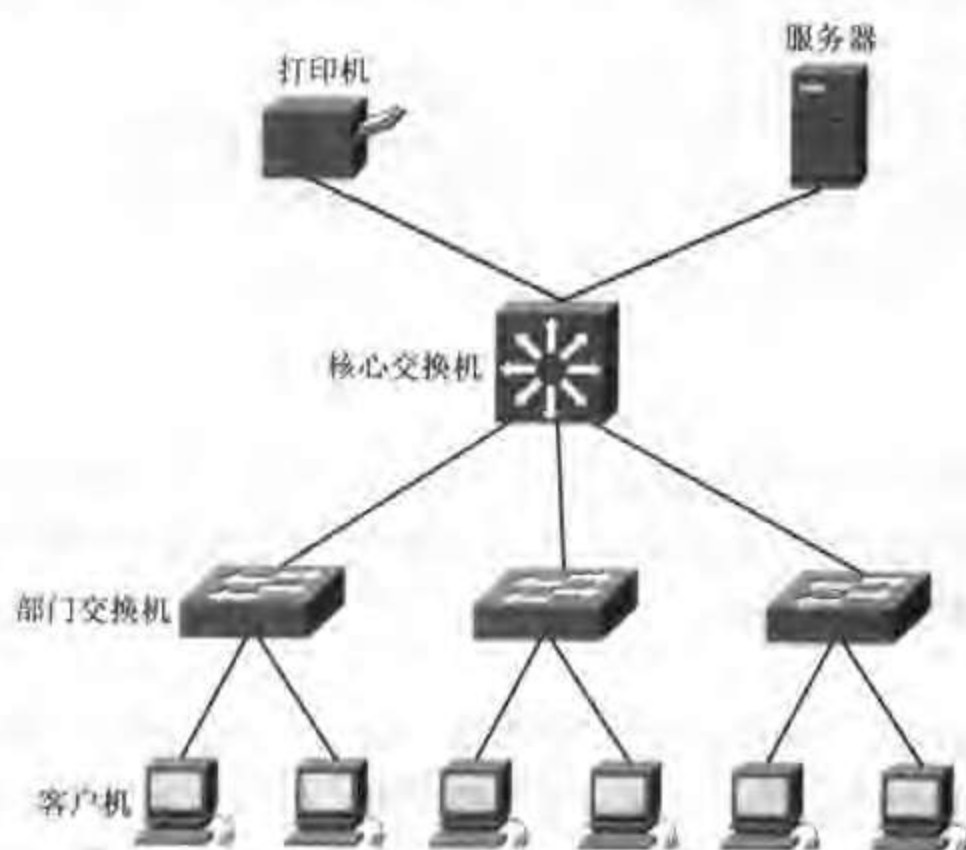


图 3-5 小型局域网

1. 案例 1

(1) 需求描述

企业内部需要联网的节点数为 100 点，信息点的分布为：1 楼 40 点，2~4 楼各 20 点，大楼主干采用光纤布线，楼层需要百兆交换到桌面。企业主要应用为内部文件共享、邮件和办公自动化（OA）系统。

(2) 选型分析

企业总节点数 100 点，应用为内部文件共享、邮件和办公自动化（OA）系统，这些都是非时间敏感型应用，并非一刻不能停机，因此我们可以在核心放置一台 Catalyst3550-12G（如图 3-6 所示），支持各楼层数据的快速交换，它有 10 个 GBIC 插槽和 2 个 10/100/1000BaseT 端口，可用于和各楼层的交换机实现吉比特互连，由于大楼的主干采用光纤布线，所以我们可选用 WS-G5484 GBIC 模块用于和各楼层光纤互连。各楼层交换机我们可根据楼层的节点

数分别进行选择，一楼我们选择 Catalyst2950G-48，2~4 楼我们选择 Catalyst2950G-24，这两款交换机都有两个 GBIC 插槽，可选用 WS-G5484 GBIC 模块（如图 3-7 所示）用于光纤上联核心交换机。



图 3-6 Catalyst3550-12G



图 3-7 WS-G5484

表 3-3 本方案所选产品列表

产 品	描 述	数 量
WS-C3550-12G	10 GBIC 端口 + 2-10/100/1000 端口; EMI	1
WS-C2950G-48-EI	带有 2 GBIC 插槽，图像增强功能的 Catalyst 2950, 48 10/100	1
WS-C2950G-24-EI	带有 2 GBIC 插槽，图像增强功能的 Catalyst 2950, 24 10/100	1
WS-G5484	1000BASE-SX 短波长 GBIC (仅用于多模)	8

2. 案例 2

(1) 需求描述

企业内部需要联网的节点数为 200 点，信息点的分布为：1~5 楼各 40 点，大楼主干采用光纤布线，楼层需要百兆比特交换到桌面。企业主要应用为内部文件共享、办公自动化（OA）系统，对外提供邮件和网站服务等。

(2) 选型分析

企业总节点数 200 点，应用为内部文件共享、办公自动化（OA）系统、邮件和网站服务等，这些都是非时间敏感型应用，并非一刻不能停机，但相比案例 1 它的节点数更多，同时它有对外提供的服务，因此我们可以在核心放置一台 Catalyst4507R（如图 3-8 所示），它的背板带宽达到 64Gbit/s，可支持各楼层数据的高速交换。它支持引擎的冗余，在一定程度上提高了系统的可靠性。我们选择 4 代引擎 WS-X4515（如图 3-9 所示），它有 48MPacket/s 的分组转发率，可实现快速的数据转发，选择 WS-X4306-GB 模块（如图 3-10 所示），它有 6 个 GBIC 插槽，可用于和各楼层的交换机实现吉比特互连，由于大楼的主干采用光纤布线，所以我们可选用 WS-G5484 GBIC 模块用于和各楼层光纤互联。各楼层交换机我们可根据楼层的节点数分别进行选择，1~5 楼我们各选择一台 Catalyst2950G-48，这款交换机有两个 GBIC 插槽，可选用 WS-G5484 GBIC 模块用于光纤上连核心交换机。

表 3-4 本方案所选产品列表

产 品	描 述	数 量
WS-C4507R	Catalyst 4500 Chassis (7-插槽), 风扇, 无 p/s, Red Sup Capable	1
PWR-C45-1000AC	Catalyst 4500 1000W AC 电源 (仅用于数据)	1
PWR-C45-1000AC/2	Catalyst 4500 1000W AC 电源 备用	1

续表

产 品	描 述	数 量
CAB-7KACA	AC 电源线	2
WS-X4515	Catalyst 4500 监视器 IV (2 GE),控制台(RJ-45)	1
WS-X4515/2	Catalyst 4507R 备用监视器 IV,(2 GE),控制台(RJ-45)	1
S4KL3-12113EW	Cisco IOS BASIC L3 Cat4500 SUP 3/4(RIP,St,路由器,IPX,AT)	1
WS-X4306-GB	Catalyst 4500 吉比特以太网模块,6 端口 (GBIC)	1
WS-C2950G-48-EI	带有 2 GBIC 插槽,图像增强功能的 Catalyst 2950,48 10/100	5
WS-G5484	1000Base-SX 短波长 GBIC (仅用于多模)	10



图 3-8 Catalyst4507R



图 3-9 WS-X4515



图 3-10 WS-X4306-GB

3.3.3 中大型局域网

在中大型局域网络中,总通信节点数一般在 200 点以上,网络结构根据具体应用的不同可分为两层结构和三层结构两种。

两层结构是将网络分为两层:核心层和接入层。在核心层会放置具有三层交换功能的交换机用于通信数据快速交换;在接入层一般为纯二层的交换机。两层结构典型的局域网如图 3-11 所示。

三层结构是将网络分为三层:核心层、汇聚层和接入层。在核心层会放置具有三层交换功能的交换机用于通信数据快速交换;在汇聚层一般放置具有三层交换功能的交换机用于跨 VLAN 的访问,以及设置相应的安全策略;在接入层一般为纯二层的交换机。其中在核心层和汇聚层之间往往启用动态路由协议替代传统的交换网中的生成树协议来避免网络冗余所产

生的环路。三层结构典型的局域网如图 3-12 所示。

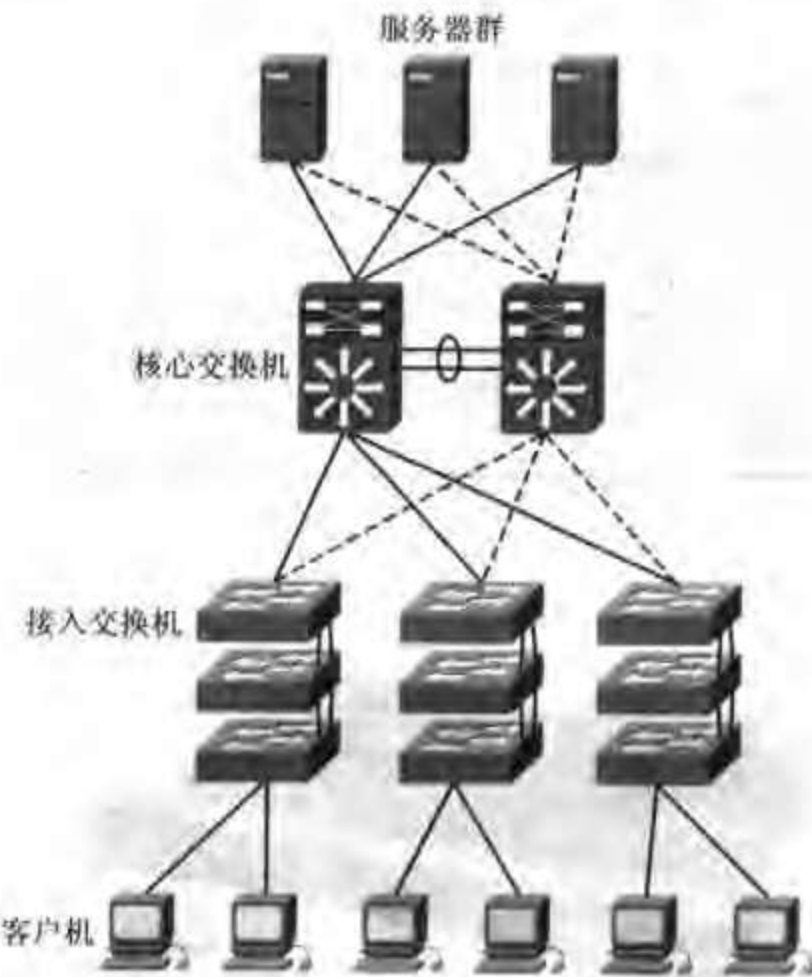


图 3-11 两层结构中大型局域网

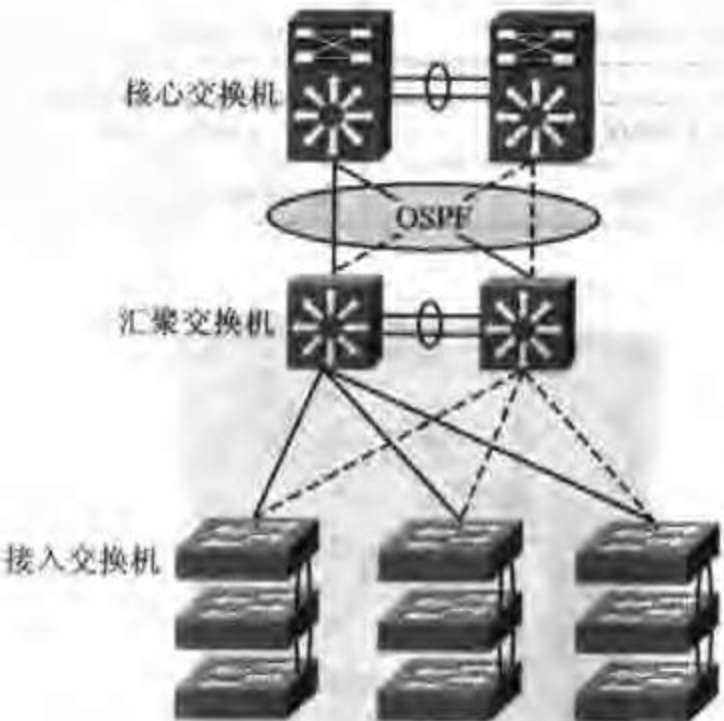


图 3-12 三层结构中大型局域网

说明：具体一个网络采用两层还是三层结构要视这个网络的数据流量而定，如果有大量的本地跨 VLAN 的访问，比如不同部门间的访问，这时可采用三层结构，这样大量的跨 VLAN 的访问就可在汇聚层的交换机上实现，而不用都集中在核心交换机上；而如果本地跨 VLAN 的访问数据量并不大，大量的数据是客户机对服务器和对外的访问，这些数据必然要穿越核心交换机，这时就可采用两层结构。目前，80% 以上的企业网络采用的都是两层结构的网络架构，三层结构的网络更多地应用在电信运营商的网络中。

1. 案例 1

(1) 需求描述

企业内部需要联网的节点数为 400 点，信息点的分布为：1~10 层各 40 点，网络中心位于 1 层，整个大楼主干采用光纤布线，楼层需要百兆交换到桌面。企业网络的主要应用分为两部分，一部分是基础的网络应用它包括内部文件共享、办公自动化（OA）系统、邮件和网站服务等；另一部分是企业的业务应用系统。企业网中大部分的用户数据来自对业务应用系统的访问，同时业务应用系统的可靠性也要求最高。

(2) 选型分析

企业总节点数 400 点，应用分为基础网络应用和企业的业务系统。由于业务系统对可靠性有很高的要求，因此，整体网络结构我们采用冗余配置，避免单点故障（当然，我们这里只讨论网络方面的可靠性，对于整个业务系统，为了保证其整体的稳定可靠，除了网络系统，我们还应该考虑其他方面的因素，比如服务器采用冗余系统，供电方面采用 UPS 等）。由于企业网中大部分的用户数据来自对业务应用系统的访问，因此整个网络我们采用二层结构。

整体网络结构定下来之后，我们来进行核心和接入层设备的选型。根据网络中数据量的

大小, 我们可确定核心层的设备, 如果没有具体的数据, 我们可以参考经验值进行选择, 就拿这个案例来说, 整个网络有 400 个信息点, 如果按 1:3 的并发率来计算, 整个网络就有约 140 个点同时进行数据传输, 每个信息点 100Mbit/s, 那么整个网络就需要 14Gbit/s, 也就是说如果要让这 140 个点进行数据的无阻塞的线速转发, 那么整个网络的带宽就必须大于 14Gbit/s, 如果考虑到尖峰时刻 (400 点同时进行网络访问) 的流量 40Gbit/s, 那意味着我们的核心设备最好应具有 40Gbit/s 以上的处理能力。在这里我们可以选用 Cisco 的 Catalyst4507R, 它的背板带宽达到 64Gbit/s, 同时它支持引擎的冗余, 这在一定程度上提高了系统的可靠性。我们选择 4 代引擎 WS-X4515, 它有 48MPacket/s 的分组转发率, 可实现三层数据的快速转发。在模块方面, 我们选择两块 WS-X4306-GB 模块, 共 12 个 GBIC 插槽, 可用于和各楼层的交换机实现吉比特互连, 由于大楼的主干采用光纤布线, 所以我们可选用 WS-G5484 GBIC 模块用于和各楼层光纤互连。由于用于业务系统的服务器直接连接在核心交换机上, 线路采用的是吉比特铜缆, 所以我们还需选择一块 WS-X4424-GB-RJ45 用于服务器的连接。至此核心交换机我们就选完了, 至于是否采用冗余电源和引擎, 我的建议是如果采用了双核心结构, 即整机是冗余的, 那么模块就没必要非要冗余, 当然如果资金允许, 所有部分都采用冗余最好。

各楼层交换机我们可根据楼层的节点数分别进行选择, 1~10 层我们各选择一台 Catalyst2950G-48, 这款交换机有两个 GBIC 插槽, 可选用 WS-G5484 GBIC 模块用于光纤上连核心交换机。

说明: 核心设备的背板最好 40Gbit/s 以上, 并不代表低于 40Gbit/s 不能运行, 它只表示如果低于 40Gbit/s, 那么在高峰时刻, 网络可能会产生拥堵。

表 3-5 本方案所选设备列表

产 品	描 述	数 量
核心交换机		
WS-C4507R	Catalyst 4500 Chassis (7 插槽), 风扇, 无 p/s, Red Sup Capable	2
PWR-C45-1000AC	Catalyst 4500 1000W AC 电源 (仅用于数据)	2
CAB-7KACA	AC 电源线	2
WS-X4515	Catalyst 4500 监视器 IV (2 GE), 控制台 (RJ-45)	2
S4KL3-12113EW	Cisco IOS BASIC L3 Cat4500 SUP 3/4(RIP, St. 路由器, IPX, AT)	2
WS-X4306-GB	Catalyst 4500 吉比特以太网模块, 6 端口 (GBIC)	4
WS-X4424-GB-RJ45	Catalyst 4500 24-port 10/100/1000 模块 (RJ45)	2
接入交换机		
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	10
WS-G5484	1000Base-SX 短波长 GBIC (仅用于多模)	40

本方案所选设备见图 3-8~3-10, 其中新添的 WS-X4424-GB-RJ45 模块如图 3-13 所示。

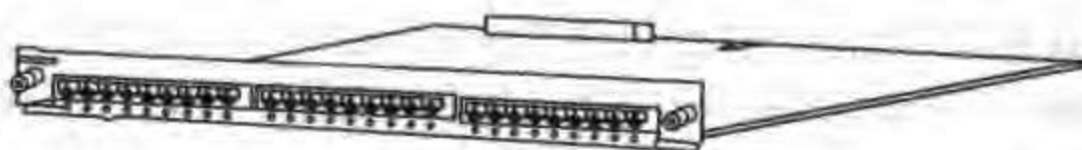


图 3-13 WS-X4424-GB-RJ45

2. 案例 2

(1) 需求描述

整个企业包括 5 栋楼，分属于 5 个不同的子公司。需要联网的节点数为 1500 点，信息点的分布为：1~5 号楼各 300 点，每栋楼内信息点的分布为 1 层 20 点，2~7 层各 40 点。5 栋楼之间采用光纤互连，各栋楼内主干采用光纤布线，楼层需要百兆比特交换到桌面，网络中心机房位于 1 号楼。企业网络的主要应用分为三部分，一部分是基础的网络应用，它包括内部文件共享、办公自动化（OA）系统、邮件和网站服务等；另一部分是拓展的网络应用，它包括 IP 语音系统、视频会议等；最后是企业的业务应用系统。其中，基础和拓展网络应用楼盖整个企业，而业务应用系统分属不同的子公司。企业网中很大一部分的用户数据来自对业务应用系统的访问，同时对业务应用系统的可靠性也要求最高，另外，IP 语音和视频会议系统对网络的质量要求也很高。

(2) 选型分析

企业总节点数 1500 点，楼据需求的描述我们知道业务系统对可靠性有很高的要求，因此，整体网络结构我们需要采用冗余配置，避免单点故障（当然，我们这里只讨论网络方面的可靠性，对于整个业务系统，为了保证其整体的稳定可靠，除了网络系统，我们还应该考虑其他方面的因素，比如服务楼采用冗余系统，供电方面采用 UPS 等）。由于企业网中大部分的用户数据来自对业务应用系统的访问，而业务系统分布于各个楼内，因此整个网络我们建议采用三层结构。

整体网络结构定下来之后，我们来进行核心层、汇聚层和楼入层设备的选型。楼据网络中数据量的大小，我们可确定核心层的设备，如果没有具体的数据，可以参考经验值进行选择。就拿这个案例来说，整个网络有 1500 个信息点，如果楼 1:3 的并发率来算，整个网络就有约 500 个点同时进行数据传楼，每个信息点 100Mbit/s，那么整个网络就需要 50Gbit/s，如果考虑到尖峰时刻（1500 点同时进行网络访问）的流量 150Gbit/s，那意味着楼心设备最好应具有 150Gbit/s 以上的处理能力，也就是说如果要让这 1500 个点进行数据的无阻塞的线速转发，那么整个网络的带宽就必须大于 150Gbit/s，在这里我们可以选用 Cisco 的 Catalyst6506，配置二代引擎 WS-X6K-S2-MSFC2 和矩阵楼块 WS-C6500-SFM，它的背楼带宽可达到 256Gbit/s，包转发率达到 170MPacket/s。同时它支持引擎的冗余，这在一定程度上提高了系统的可靠性。在模块方面，我们选择一块 WS-X6516-GBIC 模块，共 16 个 GBIC 楼槽，可用于和各栋楼的汇聚层交楼机实现吉比特互连，由于整个网络的主干采用光纤布线，且各栋楼至 1 号楼网络中心机房之间的距离小于 500m，所以我们可选用 WS-G5484 GBIC 模块用于和各楼进行光纤互联（如果大于 500m 而小于 10km，我们需要选择 WS-G5486 楼块；如果大于 10km 而小于 70km，我们需要选择 WS-G5487 模块）。由于用于基础网络服务（OA、WWW、Email、DNS）的服务器直楼连楼在核心交换机上，线路采用的是吉比特铜缆，所以我们还需选择一块 WS-X6548-GE-TX 用于服务楼的连接。至此楼心交楼机我们就选完了，至于是否采用冗余电源和引擎，我的建议是如果采用了双核心结构，即整机是冗余的，那么楼块就没必要非要冗余，当然这要取决于我们网络的重要性的我们对网络可靠性的评估，即如果网络由于单点故障导致瘫痪，那么我们的损失有多大，如果这个楼失非常巨大，那么还是建议进行引擎和电源的冗余配置。

选择完核心交换机，下面我们来进行汇聚层交换机的选型。楼据需求楼述我们知道各栋

楼的信息点都为 300 点,如果按 1:3 的并发率来算,各栋楼都约有 100 个点同时进行数据传输,每个信息点 100Mbit/s,那么网络就需要 10Gbit/s,也就是说如果要是让这 100 个点进行数据的无阻塞的线速转发,那么网络的带宽就必须大于 10Gbit/s,如果考虑到尖峰时刻(300 点同时进行网络访问)的流量 30Gbit/s,那意味着我们的汇聚层设备最好应具有 30Gbit/s 以上的处理能力。在这里我们可以选用 Cisco 的 Catalyst4507R,它的背板带宽达到 64Gbit/s,同时它支持引擎的冗余,这在一定程度上提高了系统的可靠性。我们选择 4 代引擎 WS-X4515,它有 48MPacket/s 的分组转发率,可实现三层数据的快速转发。在模块方面,我们选择两块 WS-X4306-GB 模块,共 12 个 GBIC 插槽,可用于和各楼层的交换机实现吉比特互连。由于大楼的主干采用光纤布线,所以我们可选用 WS-G5484 GBIC 模块用于和各楼层光纤互联。由于用于业务系统的服务器直接连接在汇聚层交换机上,线路采用的是千兆铜缆,所以我们还需选择一块 WS-X4424-GB-RJ45 用于服务器的连接。这样汇聚层交换机我们就选完了,由于汇聚层交换机相当于各楼内的核心交换机,且业务系统直接挂在汇聚层交换机上,所以我们建议汇聚层交换机采用冗余设计,单机采用电源冗余。

接入层交换机我们可根据楼层的节点数分别进行选择,在 1 层选择 Catalyst2950G-24,在 2~7 层各选择一台 Catalyst2950G-48。这款交换机有两个 GBIC 插槽,可选用 WS-G5484 GBIC 模块用于光纤上连核心交换机。

本方案中介绍的各种设备图片如图 3-14~3-18 所示。

表 3-6 本方案所选设备列表

产 品	描 述	数 量
核心交换机		
WS-C6506	Cat 6506 Chassis, 6 插槽, 12RU, 无电源, 无风扇架	2
WS-C6K-6SLOT-FAN	Catalyst 6000, 风扇架, 6-插槽系统	2
WS-CAC-1000W	Catalyst 6000 1000W AC 电源	2
WS-CAC-1000W/2	Catalyst 6000 第 2 个 1000W AC 电源	2
CAB-7KACA	AC 电源线	4
S6S22ALV-12119E	Catalyst 6000 SUP2/MSFC2 IOS 仅用于企业 LAN	2
WS-X6K-S2-MSFC2	Catalyst 6500 监视器引擎-2, 2GE, plus MSFC-2 / PFC-2	2
WS-C6500-SFM	Catalyst 6500 光交换模块	2
WS-X6548-GE-TX	Catalyst 6500 48-端口可用光纤 10/100/1000 模块	2
WS-X6516-GBIC	Catalyst 6500 16-端口吉比特以太网模块 可用光纤 (Req. GBICs)	2
汇聚交换机		
WS-C4507R	Catalyst 4500 Chassis (7-插槽), 风扇, 无 p/s, Red Sup Capable	10
PWR-C45-1000AC	Catalyst 4500 1000W AC 电源 (仅用于数据)	10
CAB-7KACA	AC 电源线	10
WS-X4515	Catalyst 4500 监视器 IV (2 GE), 控制台 (RJ-45)	10
S4KL3-12113EW	Cisco IOS BASIC L3 Cat4500 SUP 3/4(RIP, St 路由器, IPX, AT)	10
WS-X4306-GB	Catalyst 4500 吉比特以太网模块, 6 插槽 (GBIC)	20
WS-X4424-GB-RJ45	Catalyst 4500 24-端口 10/100/1000 模块 (RJ45)	10
接入交换机		
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	30
WS-C2950G-24-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 24 10/100	5
WS-G5484	1000Base-SX 短波长 GBIC (仅用于多模)	184

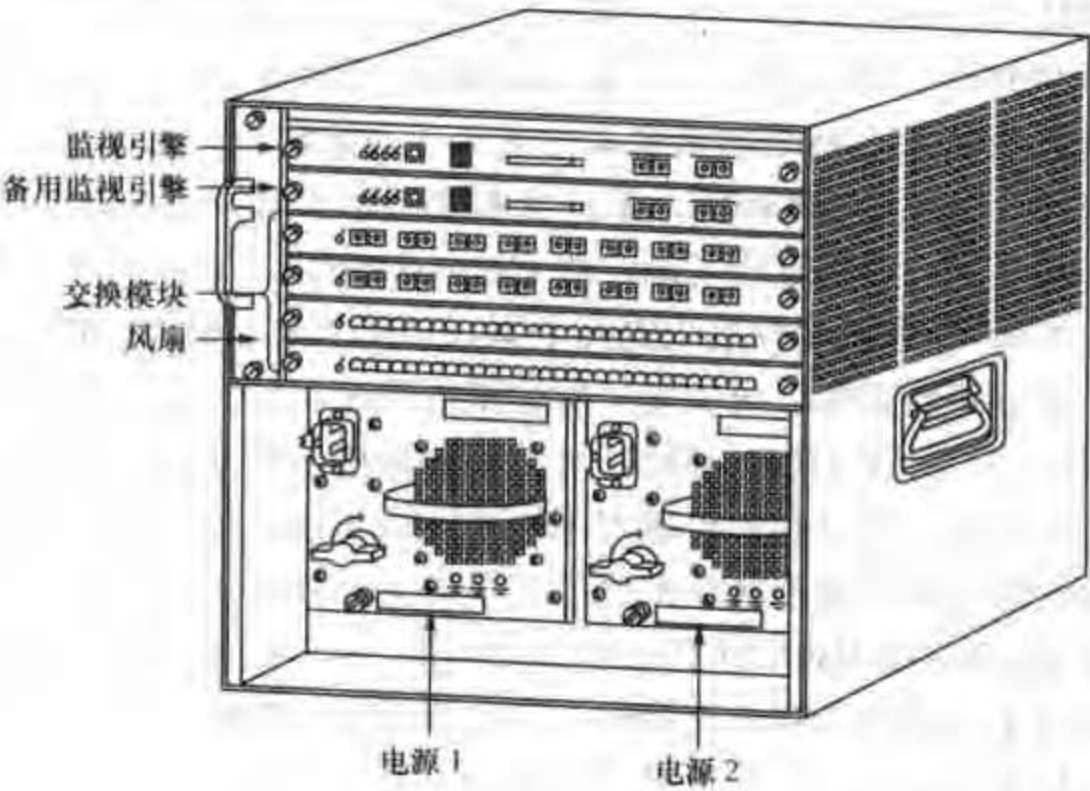


图 3-14 Catalyst6506



图 3-15 WS-X6K-S2-MSFC2 引擎



图 3-16 WS-C6500-SFM



图 3-17 WS-X6516-GBIC



图 3-18 WS-X6548-GE-TX

3.4 企业广域网互联模块

企业分支机构的设立或连锁经营体系的建立，甚至合作伙伴之间运营体系的完善都迫使企业建立广域互联网络，系统实现跨地域经营。互联网技术的发展，给广域连接提供了更多的选择，在充分考虑带宽、安全性、费用等因素的情况下，建立合适的广域互联方式将有助

于提高企业运营效率。

企业建立广域网互联,将分布在不同地域间的机构实现广域互联一般有两种途径:一是通过线路构建企业自身的真实的专用广域网;二是使用加密认证技术在 Internet 上构建虚拟的通道,从而实现虚拟专用网络(VPN)。两种技术比较如下所述。

1. 专用广域网

企业建立专用广域网主要是通过租用电信运营商的专用线路来实现。该网络系统为封闭式,安全性很高,但联网费用较高。专线主要有:分组数据交换(X.25)、数字数据网(DDN)帧中继(Frame-Relay)及数字电路业务等。

DDN: 利用各种数字传输通道(光纤、数字微波、卫星),提供各种速率的数字专用电路,实现数据及多媒体信息的通信,适合实现中高速的局域网互联。

帧中继: 使用数据包交换技术,终端工作站可动态共享网络介质和带宽,提高使用网络带宽的灵活性和有效性,提高网络使用效率。

注意: DDN 更适合点到点的网络连接,当网络结构是一个中心和多个分支节点时,采用 DDN 线路,网络设备需要有和分支节点数相等的串口数,而采用帧中继线路只需要一个串口就可以了,因此采用帧中继更节省费用。

X.25: 常用于公共载波分组交换网,可以满足不同设备及系统间的网络通信。其主要特点是在一条电路上可以同时开放多条虚电路,网络具有动态路由及先进的差错检验功能,网络性能稳定。但速度较慢。和帧中继相比,X.25 多了许多差错校验的功能,在数据的传输效率上很低,目前企业网络已很少采用 X.25 进行广域互联。

PSTN: 即公用交换电话网(Public Switch Telephone Network)。利用公用交换电话网络,移动用户或小分支机构可方便的接入中心网络。

ISDN: ISDN 是综合业务数字网(Integrated Service Digital Network)的简称,它是基于公共电话网的全数字网络,利用普通的电话线,可开展各种业务,例如打电话、发传真、上网、局域网互联、开会议电视、专线备份等。

数字电路: 数字电路业务是一种直接在电信传输网上进行数字信号传送的业务,是基于准同步数字序列(PDH)、同步数字序列(SDH)等先进光纤数字传输技术组建的宽带核心传送网络,利用各种新的传输技术进行高速数字信号传送的业务。该业务可向用户提供 2Mbit/s~2.5Gbit/s 各种传输速率的全透明电路,为客户提供高效的信息传送通路。目前多数大型企业的广域互联采用的都是数字电路线路。

注意: 数字电路接入是指不依赖 CHINADDN、CHINAFRN 等电信业务网,而是直接通过电信传输网络进行数据的传输。

企业专用网的组网如图 3-19 所示。

2. 虚拟专用网

利用覆盖全球的因特网(Internet),可实现廉价的网络互联。但由于业务是运行在因特网上,其安全性一直是使用者担心的焦点。随着加密技术的发展,安全问题已逐步得到解决。通过在网络的两端对数据加密,VPN 可实现数据安全的传输。随着 ADSL 接入方式的普及,在我国越来越多的中小企业选择采用 VPN 的方式来构建自己虚拟专用网从而实现广域互联,如图 3-20 所示。

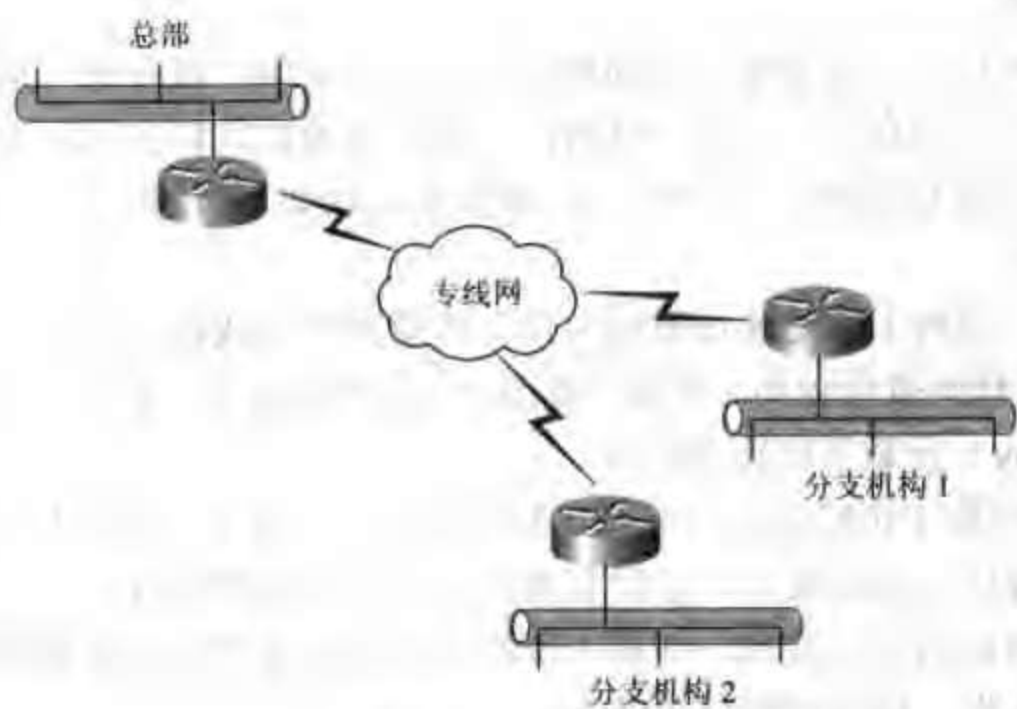


图 3-19 企业专用网



图 3-20 企业虚拟专网 (VPN)

了解了常见的广域网互联方式之后，我们来分析几个具体的案例。

1. 案例 1

(1) 需求描述

企业总部设在北京，在上海、广州和西安分别设有分支机构，总部有 60 人左右，每个分支机构有 10 人左右。企业网络平台主要用于企业内部文件共享、电子邮件和办公自动化 (OA) 系统以及企业的财务系统，整个网络的数据量不是很大。总部和分支机构需要分别通过本地的 ISP 接入 Internet。

(2) 选型分析

根据需求描述，我们知道企业网络主要用于内部文件共享、电子邮件和办公自动化 (OA) 系统以及企业的财务系统，这些都是企业内部的应用系统，因此需要构建一个企业的私有网络。根据前面的讲述我们知道，有两种构建企业广域私有网络的方式，一种是采用专线的方

式,另一种是采用 VPN 的方式。根据需求我们知道该企业的网络应用数据量并不大,如果采用专线方式构建企业私有网,必然需要在总部和分支之间向电信公司申请专有线路,这将是一笔非常可观的费用。同时由于总部和分支需要分别接入 Internet,根据企业的具体应用,我们建议总部采用 512kbit/s DDN,分支采用 ADSL 的方式接入,然后在分支和总部之间建立 VPN 来构建企业的私有网络,这样既能保证企业内网的一些应用,又不影响公司正常的上网。

在设备的选择上,根据具体的业务量,我们建议在总部采用 Cisco2621XM,配置 WIC-1T 串口模块用于 DDN 的接入,同时配置一台 PIX515UR 防火墙,用于公司内网的防护以及和分支机构建立 VPN 通道;每个分支机构采用一台 Cisco1721 路由器,配置 WIC-1ADSL ADSL 模块用于 ADSL 的接入,同时加配 VPN 模块 MOD1700-VPN,用于 VPN 的加速。本案例的拓扑图如图 3-21 所示。

说明:(1)在总部选择 PIX515UR,是因为它既可以实现企业内网的防护,又具有 VPN 的功能,同时它具有 VPN 的硬件加速模块,能够大幅度提高 VPN 加解密的速率,从而提高网络的整体性能;如果利用接入路由器 Cisco2621xm 和 Cisco1721 来通过软件加密的方式建立 VPN 通道,性能会下降很多。(2)MOD1700-VPN 模块用于在 Cisco1721 路由器上实现 VPN 的硬件加解密。

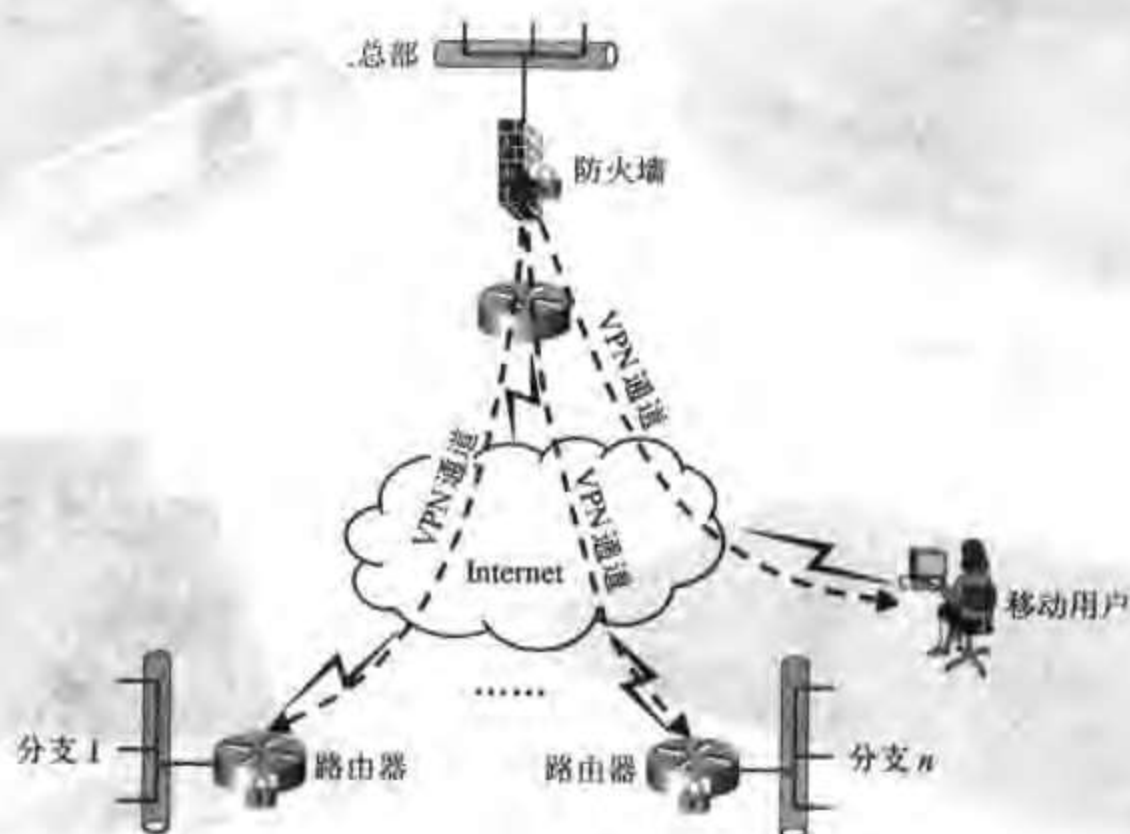


图 3-21 本案例拓扑图

本案例所选设备列于表 3-7 中。

表 3-7

本案例所选设备列表

产 品	描 述	数 量
中心端设备		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP	1
CAB-ACA	插头,电源线,10A	1
S26C-12215T	Cisco 2600 Ser IOS IP	1

		续表
产 品	描 述	数 量
WIC-IT	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1
PIX-515E-UR-BUN	PIX 515E-UR 束 (Chassis, Unrestricted SW, 2 FE, VAC+)	1
分支设备		
CISCO1721	10/100BaseT 模块路由器 w/2 WAN 插槽, 32M 闪存/64M DRAM	3
WIC-1ADSL	1 端口 ADSL WAN 接口板	3
MOD1700-VPN	Cisco 1700 系列 VPN 模块	3
SI7C7K9-12213T	Cisco 1700 IOS IP/ADSL PLUS IPSEC 3DES	3
CAB-ACA	插头, 电源线, 10A	3
CAB-ADSL-RJ11	用于 xDSL 的 Lavender 电缆, 直通, RJ-11, 2m	3

上述设备的图片如 3-22~3-27 所示。



图 3-22 Cisco1721



图 3-23 WIC-1ADSL



图 3-24 Cisco2621XM



图 3-25 WIC-IT



图 3-26 CAB-V35MT



图 3-27 PIX515UR

2. 案例 2

(1) 需求描述

企业总部设在北京,在全国 15 个地市有分支机构,总部有员工 200 人左右,分支机构的员工数在 50 人左右。企业网主要承载两部分应用:一部分是基础的网络应用,包括内部文件共享、邮件和办公自动化(OA)系统等;另一部分是企业的业务应用系统,此应用系统为 B/S 结构,对带宽的需求比较小。

(2) 选型分析

由于企业应用包括基础应用和业务系统应用两部分,内部文件共享、邮件和办公自动化(OA)系统,这些基础的网络应用对网络的可靠性、安全性要求都不是很高,但企业的业务应用系统是企业正常运行的根本,它的可靠和安全直接影响企业的生存,因此我们需要采用专线方式构建一个企业私有网络,同时,我们还需要在各分支和总部间构建一条备份线路,一旦主线路断掉,备份线路立即启用。在专线的选择上,低速专线(又称窄带专线,指 2Mbit 以下的专线)主要包括 DDN 和帧中继,在本案例中,企业有 15 个分支机构,如果采用 DDN 专线,那么在总部,我们需要配置 15 个串口用来和分支机构点到点互联,那无疑将增大开销,同时也增大了出故障的可能性。而采用帧中继线路,我们在中心只需 1 个串口和 15 个分支互联,这将非常方便。在备份线路的选择上,通常可选 PSTN 或 ISDN 在本方案中,应用系统的数据量不是很大,同时考虑到, PSTN 比 ISDN 使用广泛,而且费用相对较低,因此,我们选择 PSTN 作为本方案的备份链路。在带宽的选择上,我们需要综合考虑应用系统的业务量和整体的并发连接数,这往往需要向应用系统的开发人员进行咨询,有的时候还需要我们进行相应的测试,在本案例中我们设定每个分支 128kbit/s,总部 2Mbit/s。

在设备的选择上,根据具体的业务量,我们建议在总部采用 Cisco3725,配置 WIC-1T 串口模块用于和分支机构 DDN 的互连,配置 NM-1CE1U 和 NM-30DM 模块用于分支机构的 PSTN 接入;分支采用 Cisco2621XM,配置 WIC-1T 串口模块用于和总部 DDN 的互连,配置 WIC-1AM 模块用于 PSTN 接入总部。所选设备列于表 3-8 中。

表 3-8 本案例所选设备列表

产 品	描 述	数 量
总部路由器		
CISCO3725	3700 系列, 2 插槽, Dual FE, 多业务接入路由器	1
S372IPB-12302T	Cisco 3725 Ser IOS IP BASE	1
NM-1CE1U	1 端口信道化的 E1/ISDN-PRI 不平衡网络模块	1
CAB-E1-BNC	E1 电缆 BNC 75ohm/Unbal 5m	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1
NM-30DM	30 端口数字 Modem 网络模块	1
CAB-AC	电源线, 110V	1
分支路由器		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP	15
S26C-12215T	Cisco 2600 Ser IOS IP	15
WIC-1AM	1 端口模拟 Modem WAN 接口线	15

续表

产 品	描 述	数 量
WIC-1T	1 端口串行 WAN 接口板	15
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	15
CAB-ACA	插头, 电源线, 10A	15

上述设备的图片如图 3-28~3-37 所示。



图 3-28 Cisco3725



图 3-29 WIC-1T



图 3-30 CAB-V35MT



图 3-31 NM-1CE1U



图 3-32 NM-30DM

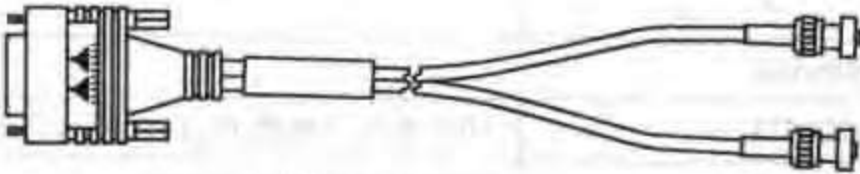


图 3-33 CAB-E1-BNC



图 3-34 Cisco2621XM 正面



图 3-35 WIC-1T



图 3-36 CAB-V35MT



图 3-37 WIC-1AM

3. 案例 3

(1) 需求描述

同案例 2

(2) 选型分析

在专线的选择上，案例 2 中我们选择帧中继线路，在本案例中我们选择另一种广泛使用的线路，即 E1 线路。备份线路我们选择 PSTN。在带宽的选择上，每个分支 128kbit/s，总部 2Mbit/s。

在设备的选择上，根据具体的业务量，我们建议在总部采用 Cisco3725，配置 NM-1CE1U 模块用于和分支机构 E1 的互连，配置另一个 NM-1CE1U 模块和一个 NM-30DM 模块用于分支机构的 PSTN 接入；分支采用 Cisco2621XM，配置 WIC-1T 串口模块用于和总部 E1 的互连，配置 WIC-1AM 模块用于 PSTN 接入总部。所选设备列于表 3-9 中。

表 3-9 本案例所选设备列表

产 品	描 述	数 量
总部路由器		
CISCO3725	3700 系列 2 插槽，双 FE，多业务接入路由器	1
S372IPB-12302T	Cisco 3725 Ser IOS IP BASE	1
NM-1CE1U	1 端口信道化 E1/ISDN-PRI 不平衡网络模块	2
CAB-E1-BNC	E1 电缆 BNC 75Ω/Unbal 5m	2
NM-30DM	30 端口数字 Modem 网络模块	1
CAB-AC	电源线，110V	1
分支路由器		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP	15
S26C-12215T	Cisco 2600 Ser IOS IP	15
WIC-1AM	1 端口模拟 Modem WAN 接口板	15
WIC-1T	11 端口串行 WAN 接口板	15
CAB-V35MT	V.35 电缆，DTE，插头，3m	15
CAB-ACA	插头，电源线 10A	15

本案例所选设备图片同案例 2 中描述的一致。

4. 案例 4

(1) 需求描述

企业总部设在北京，在全国 20 个省设有一级分支机构，每个省的 5 个地市设有二级分支机构；总部有员工 200 人左右，每个一级分支机构的员工数在 50 人左右，每个二级分支机

构的员工数在 20 人左右。企业网络的主要应用分为三部分：一部分是基础的网络应用，它包括内部文件共享、办公自动化（OA）系统、邮件和网站服务等；另一部分是拓展的网络应用，它包括 IP 语音系统、视频会议等；最后是企业的业务应用系统。其中，基础和拓展网络应用覆盖整个企业，而业务应用系统采用分布式设计，各地市的业务数据首先汇总到省中心数据库，经过处理后再发送到企业总部的中心数据库。企业网中很大一部分的用户数据来自对业务应用系统的访问，同时对业务应用系统的可靠性也要求最高。另外，IP 语音的应用会大大地节省企业的日常开销，不过 IP 语音和视频会议系统对网络的质量要求也很高。

（2）选型分析

由于企业应用包括基础网络应用、拓展网络应用和业务系统的应用三部分：内部文件共享、邮件和办公自动化（OA）系统，这些基础的网络应用对网络的可靠性、安全性要求都不是很高，但企业的业务应用系统是企业的根本，它的可靠和安全直接影响企业的生存，因此我们需要采用专线方式构建一个专有的企业的私有网络。同时，我们还需要在二级分支机构和一级分支机构之间以及一级分支机构和总部之间构建一条备份线路，一旦主线路断掉，备份线路立即启用。在专线的选择上，由于本企业属于大型企业，其主要的业务应用要运行在本网上，同时企业的 IP 电话和视频会议系统也运行在本网上，因此我们选择的专线需要具有较高的带宽，在 2Mbit/s 以上的专线类型中，ATM 和 SDH 数字线路方式是常见的接入类型，在本方案中我们选择 SDH，总部选用 155Mbit/s SDH 线路，20 个省级一级分支机构各申请 2 条 E1 线路，一条用于和总部互连，另一条用于连接 5 个市级二级分支机构，5 个市级二级分支机构各申请一条 256kbit/s 的 DDN 线路用于和省级分支机构连接。在备份线路方面，总部和省各申请一条 ISDN PRI 线路（30B+D）用于和下级互连，下级分支机构各申请一条 ISDN 线路和上级机构连接。

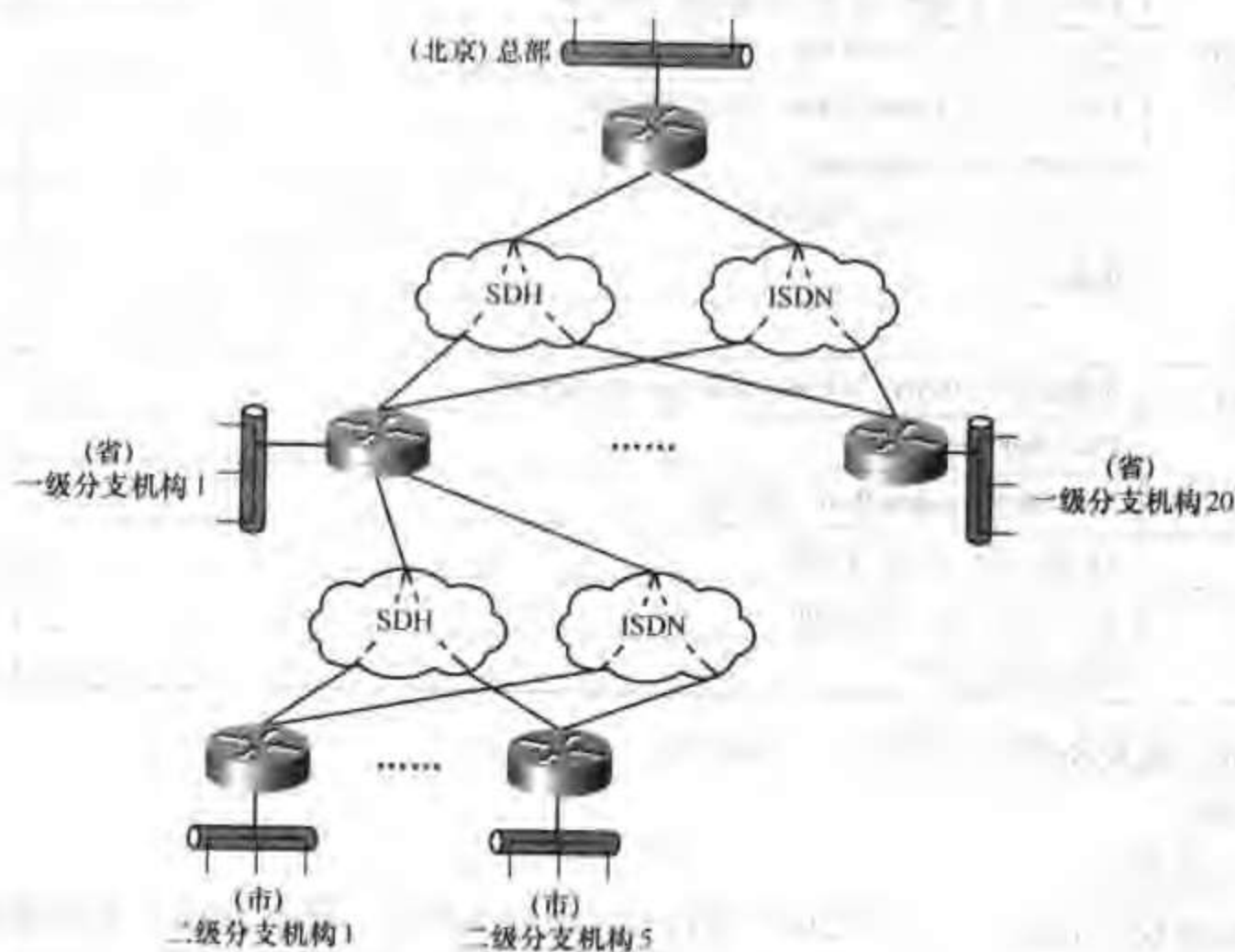


图 3-38 本案例拓扑图

说明：在总部也可以采用申请多条 E1 线路的方法和省级分支机构互连，那样会占用核心路由器很多槽位，同时由于线路很多，增加了许多故障点，因此我们建议申请 155M 的 SDH 线路，直接采用 Cisco 的 PA-MC-STM-1 模块。

在设备的选择上，根据具体的业务量，我们建议在总部采用 Cisco7507，配置 PA-MC-STM-1 模块用于和省级（一级）分支机构 SDH 的互连，配置 NM-1CE1U 模块用于省级（一级）分支机构的 ISDN 接入；省级（一级）分支机构采用 Cisco3745，配置 2 个 NM-1CE1U 模块分别用于和总部 2M 的互连以及和市级（二级）分支机构的互连，另配 1 个 NM-1CE1U 模块用于市级（二级）分支机构的 ISDN 接入；市级（二级）分支机构采用 Cisco2621XM，配置 1 块 WIC-1T 串口模块用于和省级（一级）分支机构的连接，另配 WIC-1B-S/T 模块用于和省级（一级）分支机构的 ISDN 连接。本案例拓扑图如图 3-38 所示。

本案例所选设备列于表 3-10 中。

表 3-10 本案例所选设备列表

产 品	描 述	数 量
总部路由器		
CISCO7507/8X2-MX	Cisco 7507, 7 插槽, MIX-Enabled, 双总线, 2 RSP8, 2 PS	1
PWR-7507/4X2	Cisco 7507/4x2 双 AC 电源、任选 (默认)	1
CAB-7KACA	AC 电源线	2
S75A-12114E	Cisco RSPx 系列 IOS 企业网	1
RSP8	Cisco 7505/7507/7513/7576 路由交换处理器 (默认)	1
RSP8	Cisco 7505/7507/7513/7576 路由交换处理器 (默认)	1
VIP4-80	通用接口处理器 4, Model 80	1
PA-2FE-TX	2 端口快速以太网 100Base TX 端口适配器	1
PA-MC-STM-1SM1	1 端口多通路 STM-1 单模式端口适配器	1
NM-1CE1U	1 端口信道化 E1/ISDN-PRI 不平衡网络模块	1
CAB-E1-BNC	E1 电缆 BNC 75Ω (不平衡) 5m	1
MEM-RSP8-64M	RSP8 64MB DRAM 可选 (默认)	1
MEM-RSP8-FLC20M	RSP Flash Card, 20 MB 可选 (默认)	1
MEM-RSP8-64M	RSP8 64MB DRAM 可选 (默认)	1
MBM-RSP8-FLC20M	RSP Flash Card 20 MB 可选 (默认)	1
MEM-VIP4-64M-SD	64 MB SDRAM 可选 for VIP4 (默认)	1
省（一级）分支机构路由器		
CISCO3745	3700 系列, 4 插槽, 双 FE, 多业务接入路由器	20
S374C-12215T	Cisco 3745 Ser IOS IP	20
PWR-3745-AC	AC 电源 (用于 Cisco 3745)	20
CAB-ACA	插头, 电源线 10A	20
NM-1CE1U	1 端口信道化 E1/ISDN-PRI 不平衡网络模块	40
CAB-E1-BNC	E1 电缆 BNC 75Ω (不平衡) 5m	40
市（二级）分支机构路由器		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP	100
CAB-ACA	插头, 电源线, 10A	100
S26C-12215T	Cisco 2600 Ser IOS IP	100

		续表
产 品	描 述	数 量
WIC-1T	1 端口串行 WAN 接口板	100
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	100
WIC-1B-S/T	1 端口 ISDN WAN 接口板(拨号或专用线路)	100

上述所选设备的图片如图 3-39~3-41 所示。



图 3-39 Cisco7500



图 3-40 PA-MC-STM-1 模块



图 3-41 WIC-1B-S/T 模块

3.5 企业 Internet 出口模块

前面的两节我们分别对企业的局域网部分和广域网互联部分进行了介绍，到目前为止我们所有的讲述都集中在企业的内部网络，即到目前为止我们的数据只能在本企业内部互通。而现在的企业越来越希望和本企业外进行信息的交互，这时我们就需要将企业接入 Internet。其实我们可以将企业的 Internet 接入看作是广域网互联的一个子集，即如果企业的总部有 Internet 的出口，而如果分支机构通过总部来接入 Internet，那么我们就可以将总部看成是分支的 Internet 接入提供商（ISP）。由此我们可以看出 ISP 也就是专门提供 Internet 接入服务的企业。目前我国常见的 Internet 接入方式和企业广域网互联采用的线路基本相同，如 DDN、帧中继、PSTN、ISDN、数字电路等接入方式。除此之外，刚刚兴起的宽带接入方式，如 ADSL、CABLE MODEM 和光纤接入方式也越来越多地成为现在许多企业的首选。下面我们就对我国常用的 Internet 接入方式作一简单的介绍。

PSTN: 这是最容易实施的方法, 费用低廉。只要一条可以连接 ISP 的电话线和一个账号就可以。但缺点是传输速度低, 线路可靠性差。适合对可靠性要求不高的办公室以及小型企业。如果用户多, 可以多条电话线共同工作, 提高访问速度。我们常用的 163、169 拨号上网, 采用的就是这种方式。

ISDN: ISDN 目前在国内迅速普及, 价格大幅度下降, 有的地方甚至是免初装费用。两个信道共具有 128kbit/s 的速率, 快速的连接以及比较可靠的线路, 可以满足中小型企业浏览以及收发电子邮件的需求。而且还可以通过 ISDN 和 Internet 组建企业 VPN。这种方法的性能价格比很高, 在国内大多数的城市都有 ISDN 接入服务。但是目前 ISDN 正受到 ADSL 的强有力的冲击。

ADSL: 非对称数字用户环路, 可以在普通的电话铜缆上提供最高 8Mbit/s 的下行和最高 640kbit/s 的上行传输, 目前我们普遍采用的是 ADSL, 上下行都是 512kbit/s, 可进行视频会议和影视节目传输, 非常适合中、小企业。可是它也有弱点: 用户距离电信的交换机的线路距离一般不能超过 4~6km, 这限制了它的应用范围。目前在我国采用 ADSL 方式上网的用户越来越多。

DDN 专线: 这种方式适合对带宽要求比较高的应用, 如企业网站。它的特点也是速率比较高, 范围从 64kbit/s~2Mbit/s。但是, 由于整个链路被企业独占, 所以费用很高, 因此中小企业较少选择。这种线路优点很多: 有固定的 IP 地址、可靠的线路运行、永久的连接等等。但是性能价格比太低, 除非用户资金充足, 否则不推荐使用这种方法。

光纤接入: 在一些城市开始兴建高速城域网, 主干网速率可达几十 Gbit/s, 并且推广宽带接入。光纤可以铺设到用户的路边或者大楼, 可以以 100Mbit/s 以上的速率接入。这种方式适合大型企业。

无线接入: 由于铺设光纤的费用很高, 对于需要宽带接入的用户, 一些城市提供无线接入。用户通过高频天线和 ISP 连接, 距离在 10km 左右, 带宽为 2~11Mbit/s, 费用低廉, 但是受地形和距离的限制, 适合城市里距离 ISP 不远的用户。性能价格比很高。

Cable Modem 接入: 目前, 我国有线电视网遍布全国, 很多的城市提供 Cable Modem 接入 Internet 方式, 速率可以达到 10Mbit/s 以上, 但是 Cable Modem 的工作方式是共享带宽的, 所以有可能在某个时间段出现速率下降的情况。

企业 Internet 接入的拓扑图如图 3-42 所示。

1. 案例 1

(1) 需求描述

公司大约有 20 人左右, 接入 Internet 主要目的是查询信息, 电子邮件等。

(2) 选型分析

根据需求描述我们知道企业上网的主要目的是浏览信息和日常的电子邮件的收发, 同时公司只有 20 个员工, 如果按并发率为 1:2 来计算, 公司同时会有 10 人访问 Internet, 按目前 ADSL 接入的带宽 (512kbit/s) 计算, 每人会有 50kbit/s 左右的带宽, 这对一般的信息浏

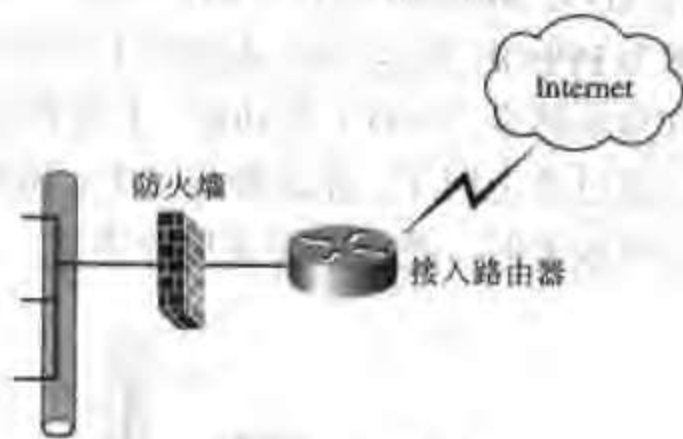


图 3-42 Internet 接入

览和邮件交互来讲,已经足够了,另外 ADSL 的接入费用相当便宜。因此我们选用 ADSL 的接入方式。

在设备的选择上,根据具体的 ADSL 配置方式的不同而有所不同,下面我们就目前最为常见的几种 ADSL 配置方式(如图 3-43~3-46 所示)进行分别的介绍。

(3) 方式一

在方式一中,电信提供的 ADSL Modem 配置为桥接模式,我们需要一台计算机作为 PPPOE 的客户端,配置电信分配的用户名和密码用来拨号;同时这台机器还要承担代理服务器的角色,这样其他的客户机,只要将网关指向它,就可以通过其上网了。在这种方式中,需要一台配置双网卡的计算机作为代理服务器,它负责数据包的转发和缓存,因此它的性能的高低直接影响了网络的性能。



图 3-43 方式一

(4) 方式二

在方式二中,我们将电信提供的 ADSL Modem 配置为路由模式(注意,并非所有电信提供的 ADSL Modem 都具有路由功能,详情请查看产品的说明书),这时我们将 ADSL Modem 配置为 PPPOE 的客户端,配置电信分配的用户名和密码用来拨号;这种模式的 ADSL Modem 具有地址转换(NAT)的功能,其他的客户机只要将网关指向 ADSL Modem 的内口地址,就可以通过其上网了。在这种方式中,所用设备最少,但 ADSL Modem 承担的压力也最大,当客户机较多时,建议不要采用此方式。

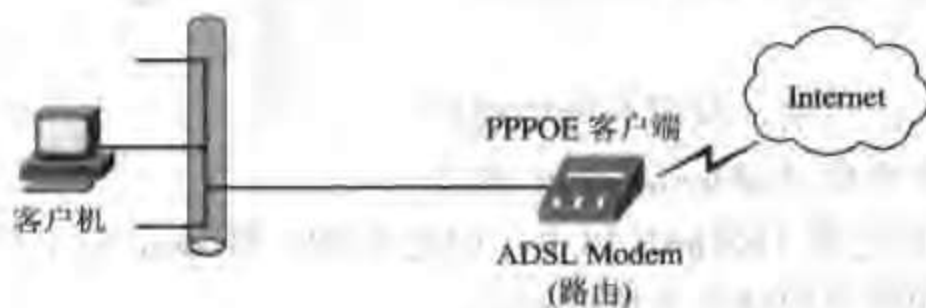


图 3-44 方式二

(5) 方式三

方式三可以看成是方式一的变种,方式三是将方式一中的代理服务器换成了专用路由器,由路由器来承担 PPPOE 拨号和地址转换(NAT)的功能。这种方式是企业用户经常采用的一种方式,因为它采用专用的路由器设备来负责数据包的转发,因此它的性能和稳定性较方式一有很大的提高。



图 3-45 方式三

(6) 方式四

方式四可以看成是方式二的变种，方式四是将方式二中的 ADSL 猫换成了专用路由器，由路由器来承担 PPPOE 拨号和地址转换（NAT）的功能。这种方式是采用 ADSL 模块，来直接接电话线，舍去了电信提供的 ADSL Modem，这种方式和方式三有相近的地方，即都是专用路由设备来实现数据包转发和地址转换（NAT），不同点是方式三采用的模块更加便宜，因此使用范围更广。

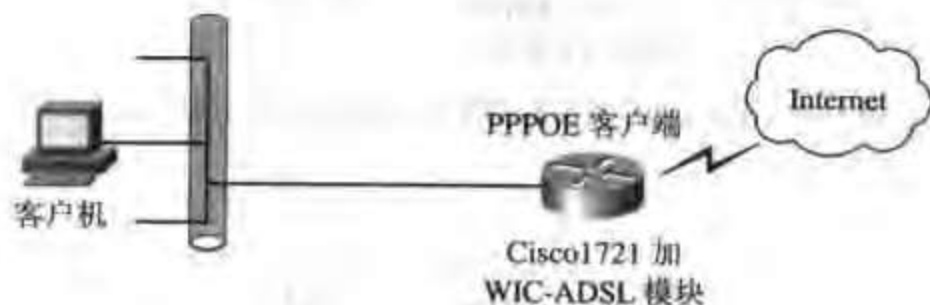


图 3-46 方式四

上述几种方式中用到的 WIC-1ENET 模块和 WIC-1ADSL 模块实物图如图 3-47 和 3-48 所示。



图 3-47 WIC-1ENET 模块



图 3-48 WIC-1ADSL 模块

2. 案例 2

(1) 需求描述

企业有员工 100 人左右，企业 Internet 接入主要承担两部分应用：一部分是常规的信息浏览查询及电子邮件等应用；另一部分是企业的对外信息发布系统，即企业的网站。

(2) 选型分析

由于企业上网不仅限于常规的信息查询和浏览，还包括对外界提供的信息应用，这就对

网络的可靠性、安全性提出了更高的要求,同时由于要将公司的网站系统放置在本地,所以需要固定的公网 IP 地址,因此我们需要采用专线方式接入 Internet。在专线的选择上,低速专线(又称窄带专线,指 2Mbit/s 以下的专线)的 Internet 接入方式主要就是 DDN; 2Mbit/s 以上的 Internet 接入主要包括城域以太网接入。在带宽的选择上,我们需要综合考虑信息发布系统的访问量和企业对外的访问量,本案例中,企业的网站主要起宣传的作用,因此在线访问量不会很大,我们主要还是考虑对外的访问,按 1:2 的并发计算,同时会有 50 人上网,选用 2Mbit/s 的 DDN 线路,每人会有 40kbit/s 的带宽,这对一般的访问已经足够。

在设备的选择上,根据具体的业务量,我们建议选用 Cisco2621XM,配置 WIC-1T 串口模块用于 Internet 的接入,如图 3-49 所示。

说明:对于详细的 DDN 线路的介绍及具体的接入方式,请参考第 5 章的广域网设置部分。



图 3-49 采用 DDN 接入方式的企业 Internet 接入组网拓扑图

3.6 小 结

通过对本章的学习,我们知道企业网就是为某个企业服务的计算机网络,通常是由局域网、广域网和 Internet 接入三部分组成。

局域网方面我们按照规模和复杂程度将它分为了超小型局域网、小型局域网和中大型局域网 3 个级别,用相应的案例分别进行了介绍;广域网方面我们按其实现方式的不同分为 VPN 方式广域网和专线方式广域网,分别用案例进行了设计和产品选型的讲解;Internet 接入方面我们根据其采用的电信链路的不同,分别对目前使用最为广泛的接入形式(ADSL 和 DDN)的接入用案例进行了介绍。

对每一个内容的讲解我们都遵循“用户需求—选型分析—设备列表—产品图片”这样一条主线来进行,我们希望通过这样的讲解,使大家对企业的网络不单有结构上的概念,同时也对最为常用的局域网、广域网和 Internet 接入能有较为清晰的理解。

第4章 Cisco 交换机配置

本章将涵盖下列有关 Cisco 交换机配置方面的关键主题：

- Cisco 交换机基础
- Cisco 交换机配置基础
- Cisco 交换机经典配置案例

通过本章的学习，希望大家对以下一些方面有所了解：

- (1) 什么是交换机；
- (2) 交换机的工作原理是什么；
- (3) 交换机的硬件结构；
- (4) 交换机的常用配置命令；
- (5) 如何快速在企业网中配置交换机。

4.1 概 述

交换机是企业网中用于构建局域网部分的主要设备。在超小型的企业网中，交换机甚至不用任何的配置，几台 PC 机和服务器直接接到交换机上就可以互相通信，所有计算机共享一个广播域（一个网段）。更多的企业网需要我们对交换机进行各种针对其应用需求的不同的配置，本章我们就来详细地介绍有关 Cisco 交换机的一些知识，以及如何利用 Cisco 交换机来接建一个典型的企业园区网。

4.2 Cisco 交换机基础

1. 什么是交换，什么是交换机？

交换和交换机最早起源于电话通信系统（PSTN），我们现在还能在老电影中看到这样的场面：首长（主叫用户）拿起话筒来一阵猛接，局端是一排播满线头的机器，戴着送受话器的话务小姐接到连接要求后，把线头接在相应的出口，为两个用户端建立起连接，直到通话结束。这个过程就是通过人工方式建立起来的交换。当然现在我们早已普及了程控交换机，交换的过程都是自动完成的。

在计算机网络系统中，交换概念的提出是对于共享工作模式的改进。我们知道 Hub（集线器）就是一种共享设备，Hub 本身不能识别目的地址，当同一局域网内的 A 主机给 B 主机传输数据时，数据分组在以 Hub 为架构的网络上是以广播方式传输的，由每一台终端通过验

证数据分组头的地址信息来确定是否接收。也就是说,在这种工作模式下,同一时刻网络上只能传输一组数据帧,如果发生碰撞还得重传。这种方式就是共享网络带宽。

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有的端口都挂接在这条背部总线上,控制电路收到数据分组以后,处理端口会查找内存中的地址对照表以确定目的 MAC 地址(网卡的硬件地址)的 NIC(网卡)挂接在哪个端口上,通过内部交换矩阵迅速将数据分组传送到目的端口,目的 MAC 地址若不存在才广播到所有的端口,接收端口回应后交换机会“学习”新的地址,并把它添加入内部地址表中。

使用交换机也可以把网络“分段”,通过对照地址表,交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发,可以有效地隔离广播风暴,减少误分组和错分组的出现,避免共享冲突。交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段,连接在其上的网络设备独自享有全部的带宽,无须同其他设备竞争使用。当节点 A 向节点 D 发送数据时,节点 B 可同时向节点 C 发送数据,而且这两个传输都享有网络的全部带宽,都有着自己的虚拟连接。假使这里使用的是 100Mbit/s 的以太网交换机,那么该交换机这时的总流量就等于 $2 \times 100\text{Mbit/s} = 200\text{Mbit/s}$;而使用 100Mbit/s 的共享式 Hub 时,一个 Hub 的总流量也不会超出 100Mbit/s。

总之,交换机是一种基于 MAC 地址识别,能完成封装转发数据分组功能的网络设备,它位于 OSI 参考模型的数据链路层(第二层),因此又称为二层设备。交换机可以“学习”MAC 地址,并将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,使数据帧直接由源地址到达目的地址。

2. 交换机的类型

按照使用的网络类型,网络交换机可分为以太网交换机、令牌环交换机、FDDI 交换机、ATM 交换机等。以太网交换机目前占局域网交换机的绝大多数,现在几乎成为局域网的标准交换设备。因此,除特别说明之外,本书中提到的局域网交换机一般均指以太网交换机。严格地说,一般意义的“以太网”(IEEE 802.3)指的是 10Mbit/s (10Base)以太网,而并不包括 100Mbit/s (100Base)的快速以太网(IEEE 802.3u)、吉比特以太网(IEEE 802.3z 和 IEEE 802.3ab)和 10Gbit/s 以太网。但是为了表述方便,本书将各种传输速率的交换机统称为“以太网交换机”。

3. 交换机的工作原理

以太网交换机的原理很简单,它检测从以太网端口来的数据分组的源和目的地的 MAC 地址,然后与系统内部的动态查找表进行比较,若数据分组的 MAC 地址不在查找表中,则将该地址加入查找表中,并将数据分组发送给相应的目的端口。简单来说,交换机包括两方面的主要功能:地址学习以及转发和过滤。

下面我们分别来对这两个功能进行介绍。

(1) 地址学习

交换机是第二层设备,它根据目标的 MAC 地址进行数据转发的。因此它必须能够学习到网络设备的 MAC 地址。下面我们通过一个模拟的案例来说明交换机的这一功能,具体过程如图 4-1~4-4 所示。

四台主机 PC1、PC2、PC3、PC4 分别连接到交换机的 Fa0/1 (Fastethernet 0/1,即快速以太网接口)、Fa0/2、Fa0/3 和 Fa0/4。

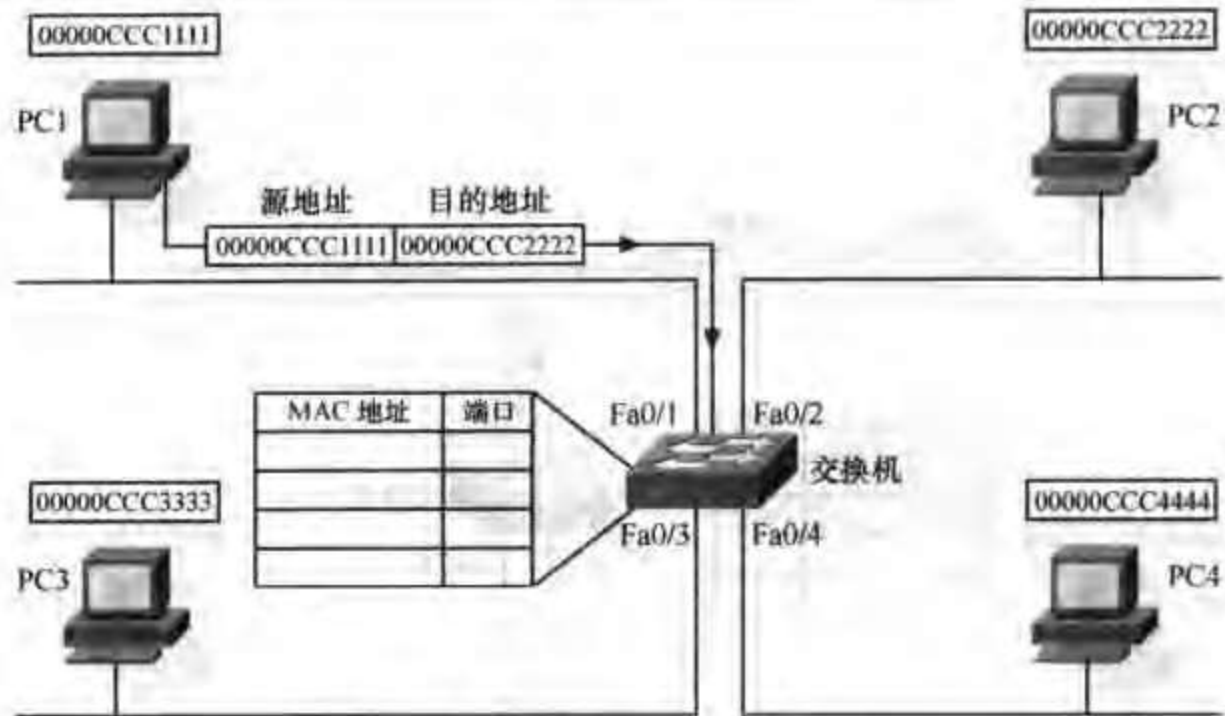


图 4-1 PC1 传递信息给 PC2

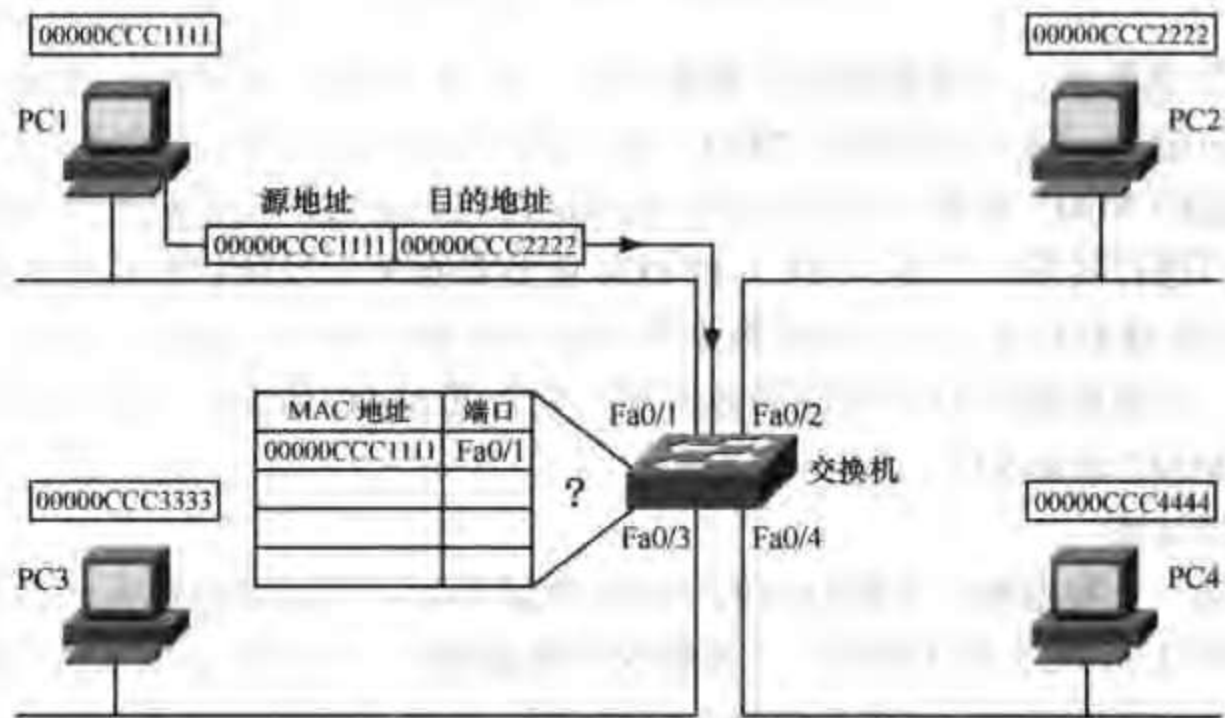


图 4-2 交换机学习到了 PC1 的地址

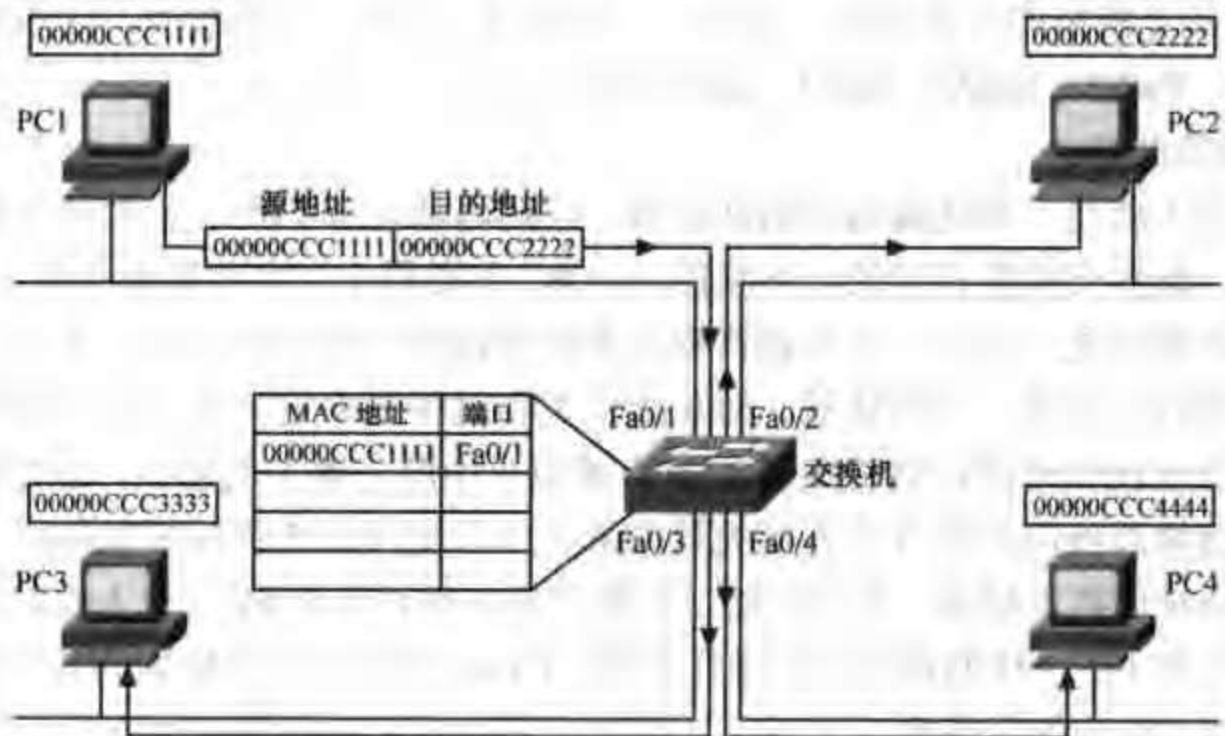


图 4-3 交换机负责将此数据向所有端口转发 (广播)

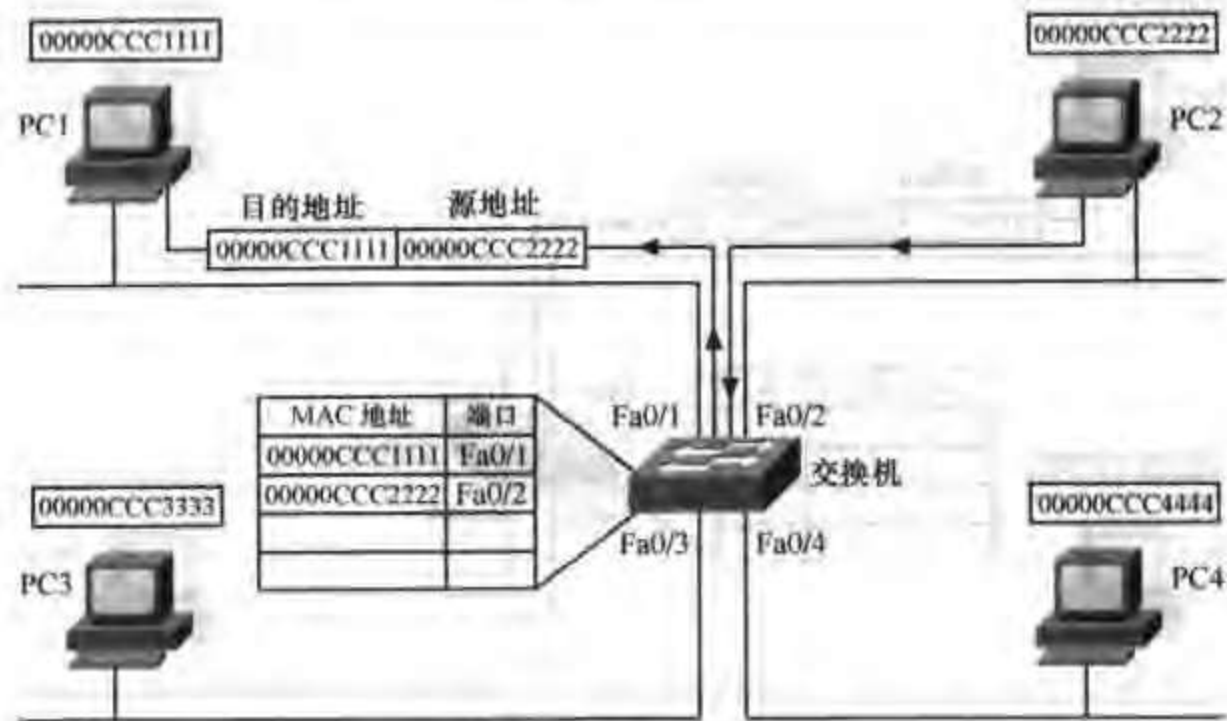


图 4-4 交换机学习到了 PC2 的地址

PC1 向 PC2 发数据，交换机收到此数据帧后，将 PC1（源）的 MAC 地址，和收到此数据帧的端口对应起来，放入交换机的 MAC 地址表中，这个过程就是地址学习的过程。此时交换机查询自己的 MAC 地址表发现没有目标地址对应的条目，交换机则负责将此数据帧向自己的所有端口进行转发（广播），PC3 和 PC4 收到数据帧后发现目标地址不是自己，将数据帧丢弃，PC2 发现目标是自己，将此数据帧拆封并向上层传送。相反，当 PC2 对 PC1 的信息做出反应后，交换机收到 PC2 返回的数据帧，并将其 MAC 地址和对应的端口号作为条目放入交换机的 MAC 地址表中。

(2) 转发和过滤

交换机收到一个数据帧，查询自己的 MAC 地址表后，可以做出转发或过滤（不转发）的决定，例如 PC1 向 PC3 发送数据，交换机收到数据帧后，查询自己的 MAC 地址表，发现一条和目标地址匹配的条目，它对应的端口为 Fa0/3，因此交换机将此数据帧从 Fa0/3 端口送出，具体过程如图 4-5 所示。与此对应的是交换机将不会把此数据帧发往端口 Fa0/1、Fa0/2、Fa0/4，这也就是交换机的过滤功能。同样，如果 PC1 向 PC2 发送数据，则交换机将不会来此数据发往端口 Fa0/1、Fa0/2、Fa0/4，如图 4-6 所示。

4. 交换机的结构

交换机实际上就是一台特殊用途的计算机，它的内部也有 CPU、内存和主板，只不过这些部件是专门为数据交换而设计的（不像我们的 PC 主要用于文字和图像处理）。我们通常所说的交换机的背板带宽（注意：有人将背板带宽和背板吞吐量混在一起，实际上背板带宽是一个设计量，而吞吐量是一个测试量，即总线位宽和时钟频率定下来后，带宽也就定了，但实际测试的吞吐量往往不能达到带宽值），有点类似于电脑主板上的总线，是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。一台交换机的背板带宽越高，处理数据的能力就越强，同时价格也越高。交换机除了和我们熟知的传统的 PC（个人电脑）有类似的体系结构外，它还和 PC 一样拥有相应的操作系统，Cisco 交换机的结构如图 4-7 所示。下面我们就来认识一下 Cisco 的交换机。

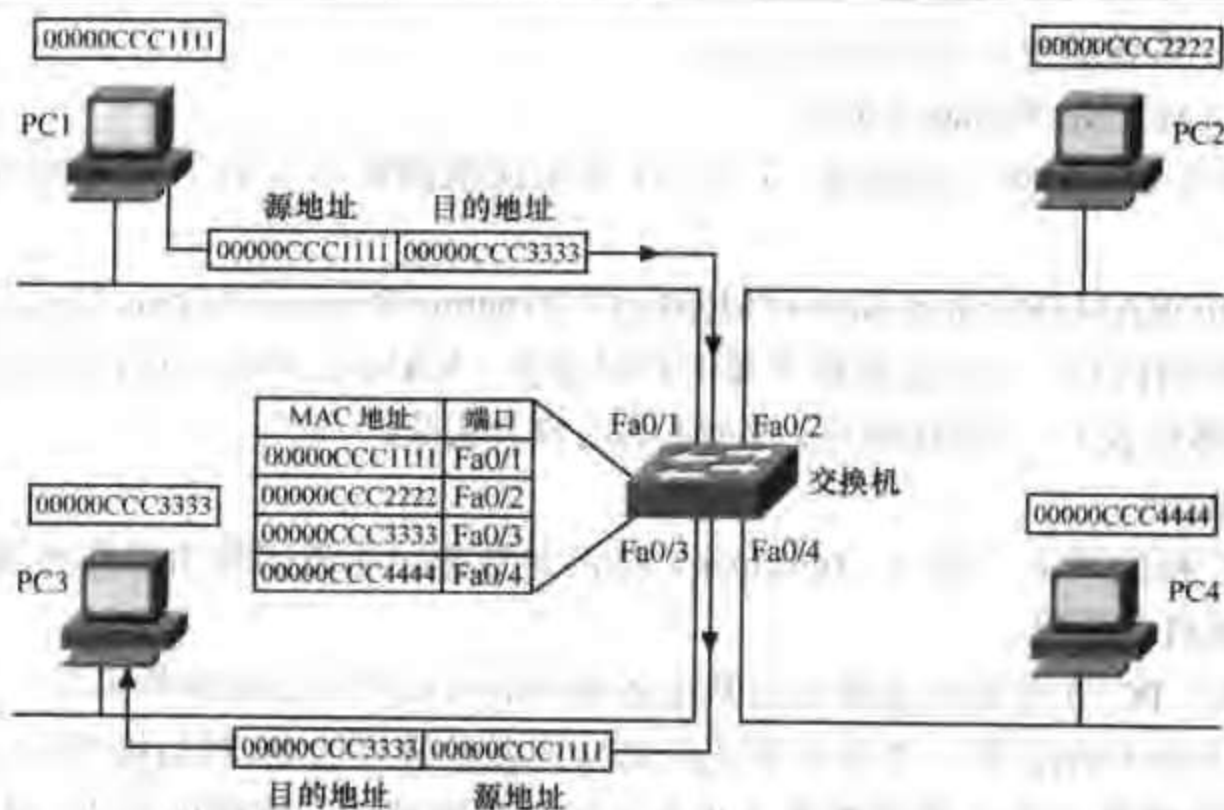


图 4-5 数据转发

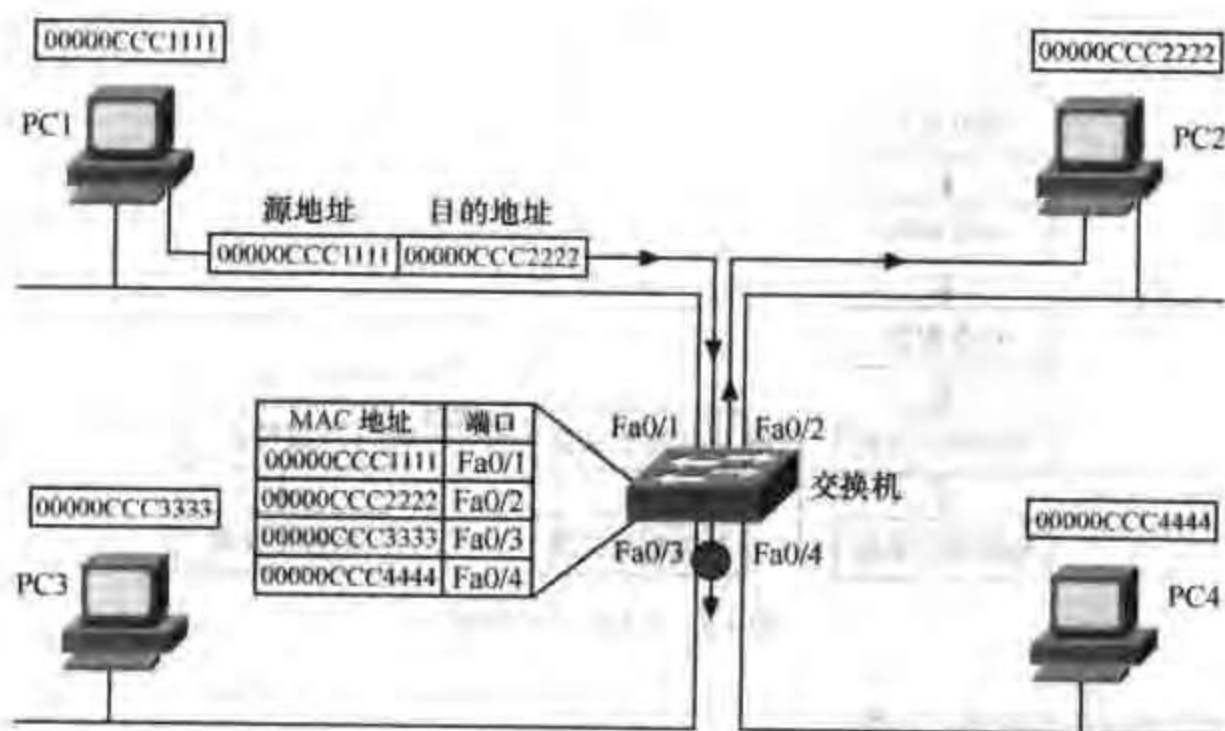


图 4-6 数据过滤

总体来说 Cisco 的交换机是由 CPU、RAM、NVRAM、FLASH、ROM 和一些相应的接口通过内部总线相连而构成。下面我们分别来介绍：

(1) CPU

相当于 PC 的 CPU (中央处理器)。是交换机的大脑，负责整个系统的计算和控制。

(2) ROM

相当于 PC 的 BIOS (基本输入输出系统)。存放引导程序和 IOS 的一个最小子集。它是只读存储器，系统掉电，程序不会丢失。

(3) Flash

相当于 PC 的硬盘。包含交换机的操作系统 (IOS) 和其他代码。它是一种可擦写、可

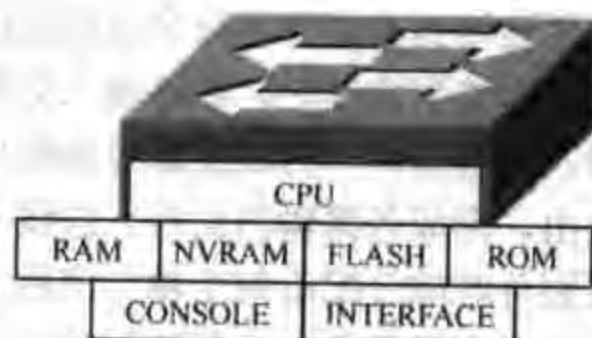


图 4-7 Cisco 交换机结构

编程的存储器，系统掉电，程序不会丢失。

(4) NVRAM (No-Volatile RAM)

相当于我们 PC 的第二块硬盘。专门存放交换机的配置文件。系统掉电，程序不会丢失。

(5) RAM/DRAM (Random Access Memory / Dynamic Random Access Memory)

相当于 PC 的内存，它是交换机主要的存储部件。RAM 也叫做工作存储器，包含动态的配置信息（如路由表）。为系统掉电，RAM 的内容会丢失。

(6) Interfaces

相当于 PC 机的网卡，接口（Interface）指的是数据分组进出路由器的网络连接。

5. 交换机启动过程

就和我们的 PC 在开机时需要进行系统各部分的自检然后加载操作系统一样，交换机也要经历一个类似的启动过程：首先对系统各部分的硬件进行检测，然后检查启动配置文件（配置了操作系统从哪里引导），根据配置文件指定的引导路径去寻找操作系统，最后从 NVRAM 中将配置文件加载到 RAM，如果没有配置就进入系统的初始配置状态。交换机启动流程如图 4-8 所示。



图 4-8 交换机启动流程

6. 以太网交换体系架构分类

以太网交换体系结构基本可以分为 3 类：总线结构、共享存储器结构以及交换矩阵结构。

总线结构交换机的特点是：各个模块共享同一背板总线结构，每个入端通过输入处理部件连接到总线上，每个出端通过输出处理部件连接到总线上。各路输入交换数据经过输入处理部件，再经过总线由输出处理部件取出，形成各路输出信号。总线采用时分方式划分时段分配给每个输入部件。总线上传送速率有极限值，而且输入处理部件向总线发送数据的速率和输出处理部件接收数据的速率也有极限值，因此总线结构交换单元的数据吞吐率会受到较大限制。一般情况下，

基于总线结构的交换机背板最高容量平均为 2Gbit/s。总线结构交换机的体系结构如图 4-9 所示。

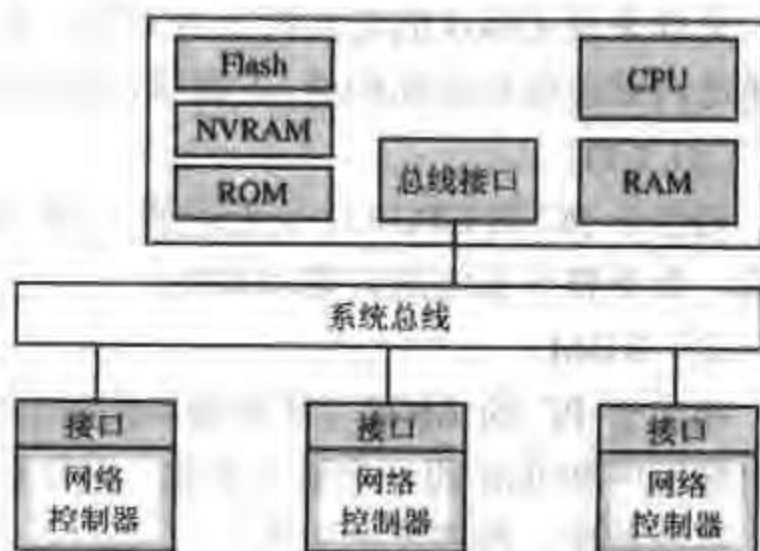


图 4-9 总线结构交换机

共享存储器结构交换机是总线结构的变形。各路输入数据经过输入处理部件进入存储器，输出处理部件从存储器中取出数据，形成各路输出信号。存储器相当于数据缓冲池。由于数据直接从存储器传输到输出端口，这种设计不需要背板。这类交换机易于实现，但端口数与存储器容量扩展到一定程度时存储器操作会有延迟；另这种设计中增加冗余交换引擎困难且成本高，故这种交换机无法避免单故障隐患。共享内存型交换机适合于小系统、堆叠式系统或较大系统中的分布式交换模块。

交换矩阵结构交换机又称为纵横制交换机。由于高速集成电路的发展，这种结构易于构建高速的交换模块。在交换矩阵结构交换机的全矩阵实施方案中，每个模块连接至其他模块，构成全网状背板。每个模块都有自己的一组连接线，因而不必设置中央交换阵列。背板总容量 $=N \times (N-1) \times$ （一条点对点链路的传输速度），其中 N 等于连接点数量，一条点对点链路的传输速度可达到 1Gbit/s 或更高。由于是网状连接，这种结构在扩大端口数时会导致模板成本迅速增加。同时每个模块都提供网状连接，扩容时还要重复提供系统时钟和控制功能。成本和复杂性高是这种交换机容量增加的主要限制因素。某些矩阵交换机的实施方案为了降低成本而减少了模块上的缓冲器容量，但减少缓冲器容量会引起阻塞现象的发生。

4.3 Cisco 交换机配置

4.3.1 基本设置方式

一般来说，可以用 4 种方式来设置交换机，如图 4-10 所示。

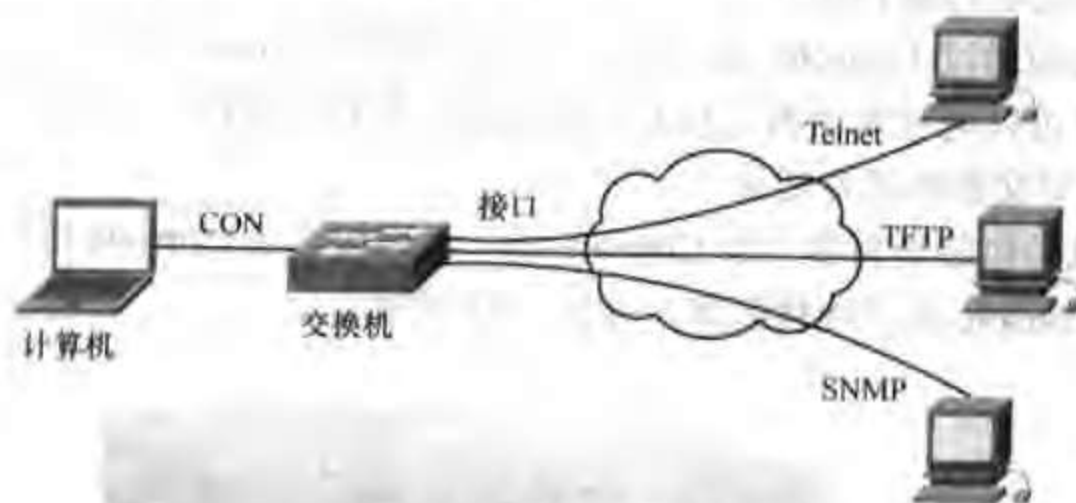


图 4-10 交换机配置方式

- CON: Console 口接终端或运行终端仿真软件（如超级终端）的微机；
- Telnet: 可以通过 Telnet 配置交换机；
- TFTP: 可以通过 TFTP 服务器下载配置信息，TFTP Server 可以运行在 UNIX 工作站或者 PC 工作站上，可以让它作为一个集中的仓库；
- SNMP: 可以通过一个运行网管软件（如 CiscoWorks）的工作站来管理交换机的配置。

除了以上介绍的几种方法外，有些交换机还支持通过 Web 方式进行配置，例如 Catalyst2950 和 Catalyst3550 支持 CMS 进行配置，如图 4-11 所示。

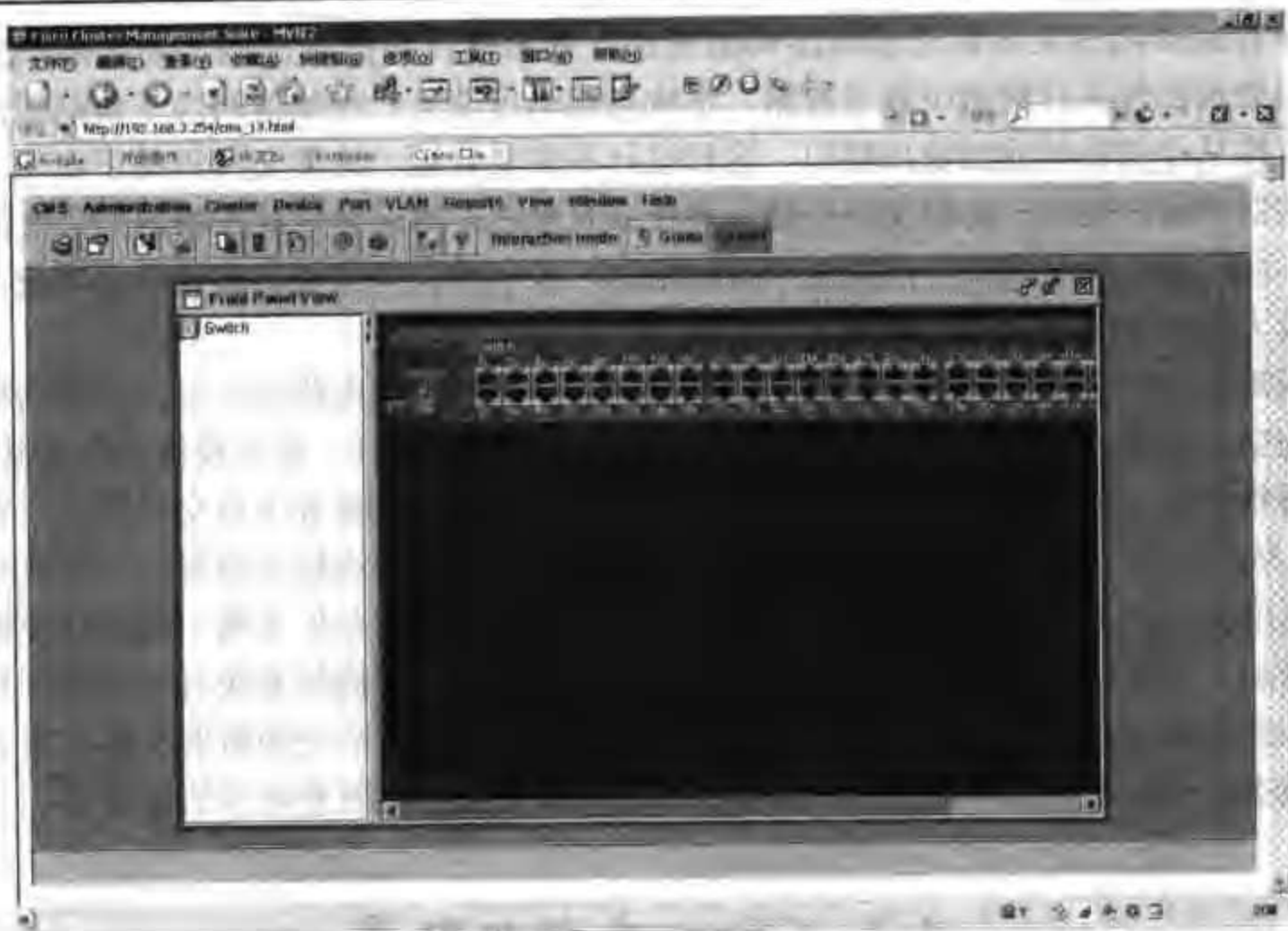


图 4-11 交换机通过 Web 方式进行配置

当我们拿到一台新的交换机后，如果只是简单地用来替代 Hub，那么完全可以不进行任何的配置，但通常情况我们都需要对交换机进行一些基本的设置，比如为了便于管理，我们往往需要给交换机设置一个管理 IP 地址，除此之外，还需要给交换机设置相应的密码，这样就可以远程对交换机进行配置了。

第一次配置必须通过 Console 端口进行，只有当通过 Console 端口对交换机进行了相应的配置后，我们才可以通过其他的几种方式对它进行配置和管理。下面我们首先介绍一下如何通过 Console 口对交换机进行配置。

(1) 新交换机的包装里自带一条 Console 线，我们用这条 Console 线将我们 PC 的 COM 端口和交换机的 Console 端口连接起来，如图 4-12 所示。



图 4-12 通过 Console 口配置交换机

(2) 单击“开始”——“程序”——“附件”——“通讯”——“超级终端”，如图 4-13 所示。

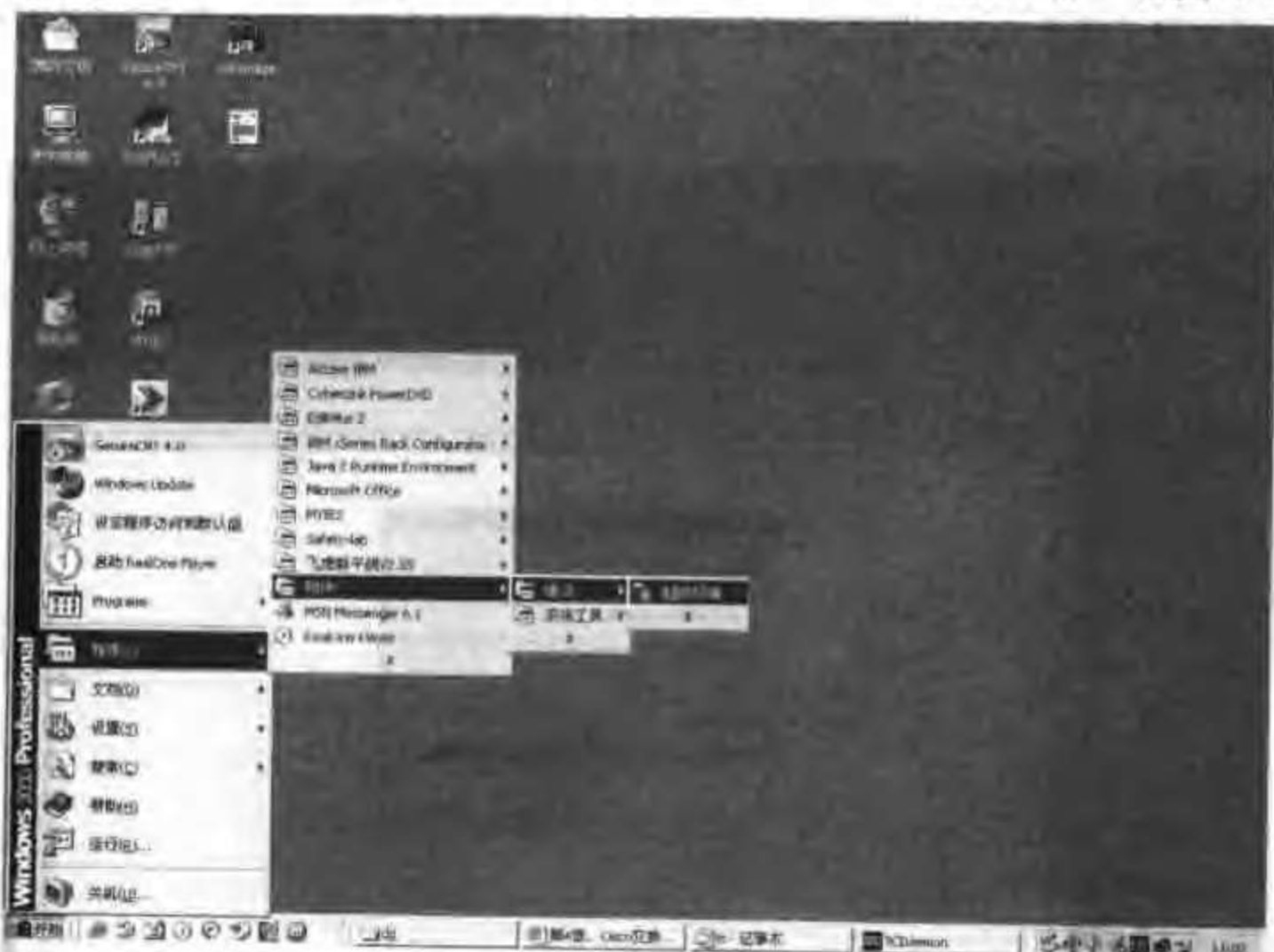


图 4-13 打开“超级终端”对话框

(3) 在弹出的对话框中输入此次连接的名称（可以随便命名），这里我们取名“myswitch”，然后，单击“确定”，如图 4-14 所示。



图 4-14 命名

(4) 在弹出的对话框中的“连接时使用”一栏，我们选择 Console 线连接的 COM 端口，如果不知道使用了哪个 COM 端口，可依次尝试。这里我们选择“COM1”，然后单击“确定”，如图 4-15 所示。



图 4-15 选择 COM 端口

(5) 在弹出的对话框中，需要我们对 COM 端口进行设置，我们进行如下的设置：

每秒位数（波特率）：9600

数据位：8

奇偶校验：无

停止位：1

数据流控制：无

我们可以简单地单击“还原为默认值”按钮，来对以上这些参数进行设置。设置完这些参数后单击“确定”，如图 4-16 所示。

(6) 经过以上的设置，我们就可以和交换机正常通信了，如果交换机正常启动，直接回车我们就可以看到如图 4-17 所示的画面。

4.3.2 IOS 和 SET 命令集介绍

Cisco 交换机的操作系统分两种，即 CataOS 和 IOS，相应的命令也分为 SET 和 IOS 两种命令集。Cisco 目前的园区网交换产品有 Catalyst2950、3550、3750、4500、6500，其中 2950、3550 和 3750 为 IOS 的操作系统，4500 和 6500 有 CataOS 操作系统也有 IOS 操作系统，但最新的引擎都只支持 IOS 操作系统，可见 Cisco 正在逐步将其路由和交换的全线产品整合到 IOS 的操作系统之上。下面的内容我们将主要针对 IOS 命令集进行讲解，如

果想了解 SET 命令集, 请参阅 Cisco 公司的相关资料, 例如 CatOS7.6 手册的链接网址为:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_7_6/index.htm

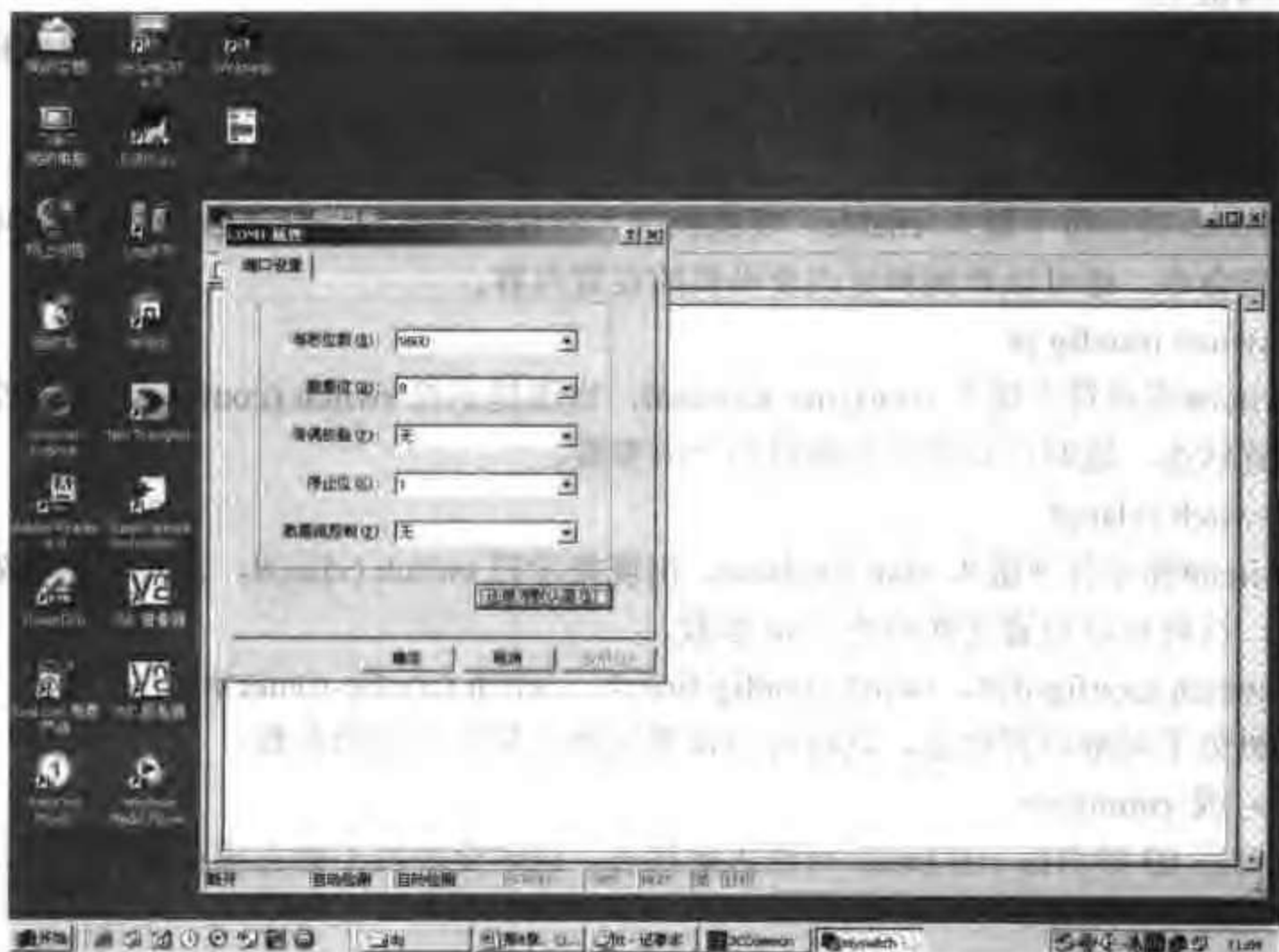


图 4-16 设置 COM 端口



图 4-17 启动交换机

4.3.3 IOS 命令状态

(1) switch >

交换机处于用户命令状态，这时用户可以看交换机的连接状态，访问其他网络和主状，但不能看到和更改交换机的设置内容。

(2) switch #

在 switch>提示符下键入 enable，交换机进入特权命令状态 switch#，这时不但可以执行所有的用户命令，还可以看到和更改交换机的设置内容。

(3) switch (config) #

在 switch#提示符下键入 configure terminal，出现提示符 switch (config)#，此时交换状处于全局设置状态，这时可以设置交换机的全局参数。

(4) switch (vlan) #

在 switch#提示符下键入 vlan database，出现提示符 switch (vlan)#，此时交换机处于 vlan 设置状态，这时可以设置交换机的 vlan 参数。

(5) switch (config-if) #, switch (config-line) #, switch (config-router) #, ...

交换机处于局部设置状态，这时可以设置交换机某个局部的参他。

(6) > 或 rommon>

在开机后 60 秒内按 ctrl-break 可进入此状态，这时交换机不能完成正常的功能，只能进行软件升级和手工引导。

(7) 设置对话状态

此状态是一台新交换机开机时自动进入的状态，在特权命令状态使用 SETUP 命令也可进入此状态，这时可通过对话方式对交换机进行设置。

所有命令的进入和退出如图 4-18 所示。

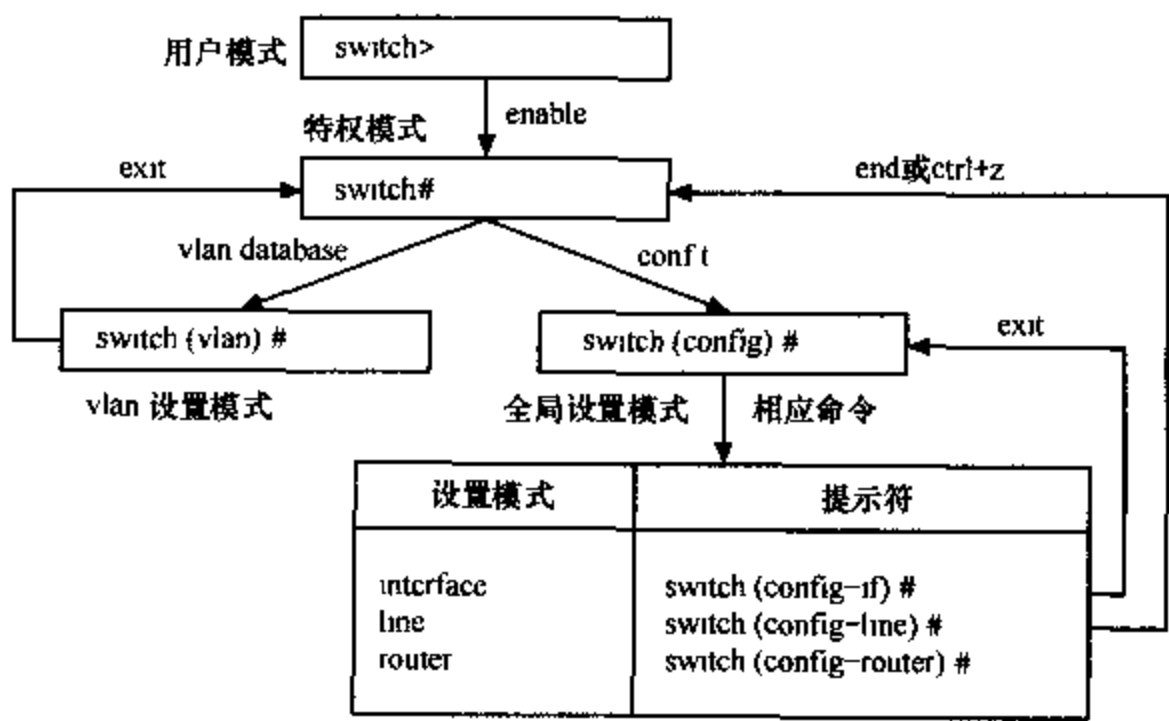


图 4-18 IOS 命令状态

说明：

(1) 在特权模式主要运行如下一些内容：

- ① 设置和系统相关的一些内容，如系统时间的设置（switch# clock set）；
 - ② 进行配置的检查 and 测试，如各种 show 命令、ping 命令等；
 - ③ 进行文件管理，如保存、清除配置等（copy run start、erase start）。
- (2) 其他的配置基本上都要先进入配置模式后再进行配置。
- (3) 我们可以在 VLAN 的设置模式进行 VLAN 配置，也可以进入配置模式进行配置。
- (4) 在最新的 IOS 上我们可在全局配置和其它各种配置模式下运行 do 命令来模仿特权模式下的命令，如“switch(config)# do show run”就等于“switch# show run”。

4.3.4 IOS 文件管理

像任何一种操作系统一样，IOS 也有自己的用于文件管理的命令，通过这些命令 IOS 可以方便地对操作系统和配置文件进行管理。

Config term: 进入配置模式

Copy run start (Write memory): 保存配置文件到 NVRAM

Copy start run (Config memory): 将配置文件从 NVRAM 调入内存

Copy run tftp (Write net): 保存配置文件到 tftp 服务器

Copy tftp run (Config net): 将配置文件从 tftp 服务器调入内存

Copy start tftp: 保存 NVRAM 的配置文件到 tftp 服务器

Copy tftp start: 将配置文件从 tftp 服务器拷贝到 NVRAM

Copy tftp flash: 将配置文件或操作系统软件 (IOS) 从 tftp 服务器拷贝到 flash 中

Copy flash tftp: 将配置文件或操作系统软件 (IOS) 从 flash 拷贝到 tftp 服务器中

Erase start (Write erase): 删除配置文件

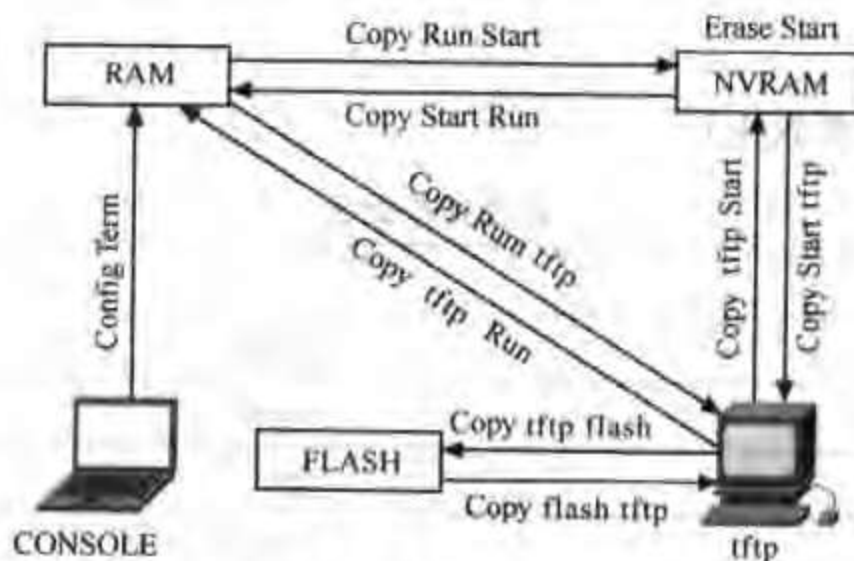


图 4-19 IOS 文件管理

4.3.5 IOS 常用命令

1. 帮助

在 IOS 操作中，无论任何状态和位置，都可以键入“？”得到系统的帮助，如下所示：

Switch#?

Exec commands:

<1-99>

Session number to resume

access-enable

Create a temporary Access-List entry

access-template

Create a temporary Access-List entry

archive

manage archive files

cd

Change current directory

clear

Reset functions

clock

Manage the system clock

cns

CNS snbsystem

configure

Enter configuration mode

connect

Open a terminal connection

copy

Copy from one file to another

debug

Debugging functions (see also 'undebug')

delete

Delete a file

dir

List files on a filesystem

disable

Turn off privileged commands

... ..

Switch#

Switch#configure ?

memory

Configure from NV memory

network

Configure from a TFTP network host

overwrite-network

Overwrite NV memory from TFTP network host

terminal

Configure from the terminal

<cr>

Switch#

2. 改变状态命令，见表 4-1

表 4-1 改变状态命令

任 务	命 令
进入特权命令状态	enable
退出特权命令状态	disable
进入设置对话状态	setup
进入全局设置状态	config terminal
退出全局设置状态	end
进入端口设置状态	interface type slot/number
进入线路设置状态	line type slot/number
进入路由设置状态 (对于三层交换机)	router protocol
退出局部设置状态	exit

3. 显示命令，见表 4-2

表 4-2

显示命令

任 务	命 令
查看版本及引导信息	<code>show version</code>
查看运行设置	<code>show running-config</code>
查看开机设置	<code>show startup-config</code>
显示端口信息	<code>show interface type slot/number</code>
显示路由信息	<code>show ip router</code>

4. 拷贝命令

用于 IOS 及 CONFIG 的备份和升级，详见上节“IOS 文件管理”。

5. 网络命令，见表 4-3

表 4-3

网络命令

任 务	命 令
登录远程主机	<code>telnet hostname IP address</code>
网络侦测	<code>ping hostname IP address</code>
路由跟踪	<code>trace hostname IP address</code>

6. 基本设置命令，见表 4-4

表 4-4

基本设置命令

任 务	命 令
全局设置	<code>config terminal</code>
设置访问用户及密码	<code>username username password password</code>
设置特权密码	<code>enable secret password</code>
设置路由器名	<code>hostname name</code>
设置静态路由	<code>ip route destination subnet-mask next-hop</code>
启动 IP 路由	<code>ip routing</code>
端口设置	<code>interface type slot/number</code>
设置 IP 地址	<code>ip address address subnet-mask</code>
激活端口	<code>no shutdown</code>
物理线路设置	<code>line type number</code>
启动登录进程	<code>login [local tacacs server]</code>
设置登录密码	<code>password password</code>

`show version`: 显示系统的硬件配置、软件版本、配置文件的源和名字以及启动镜像

`show processes`: 显示当前活动进程

`show protocols`: 显示已经配置的协议

`show memory`: 显示路由器的内存信息

`show ip route`: 显示路由表

`show flash`: 显示闪存设备的信息

`show running-config`: 显示当前活动配置

show startup-config: 显示备份配置文件

show interfaces: 显示已经配置的接口属性

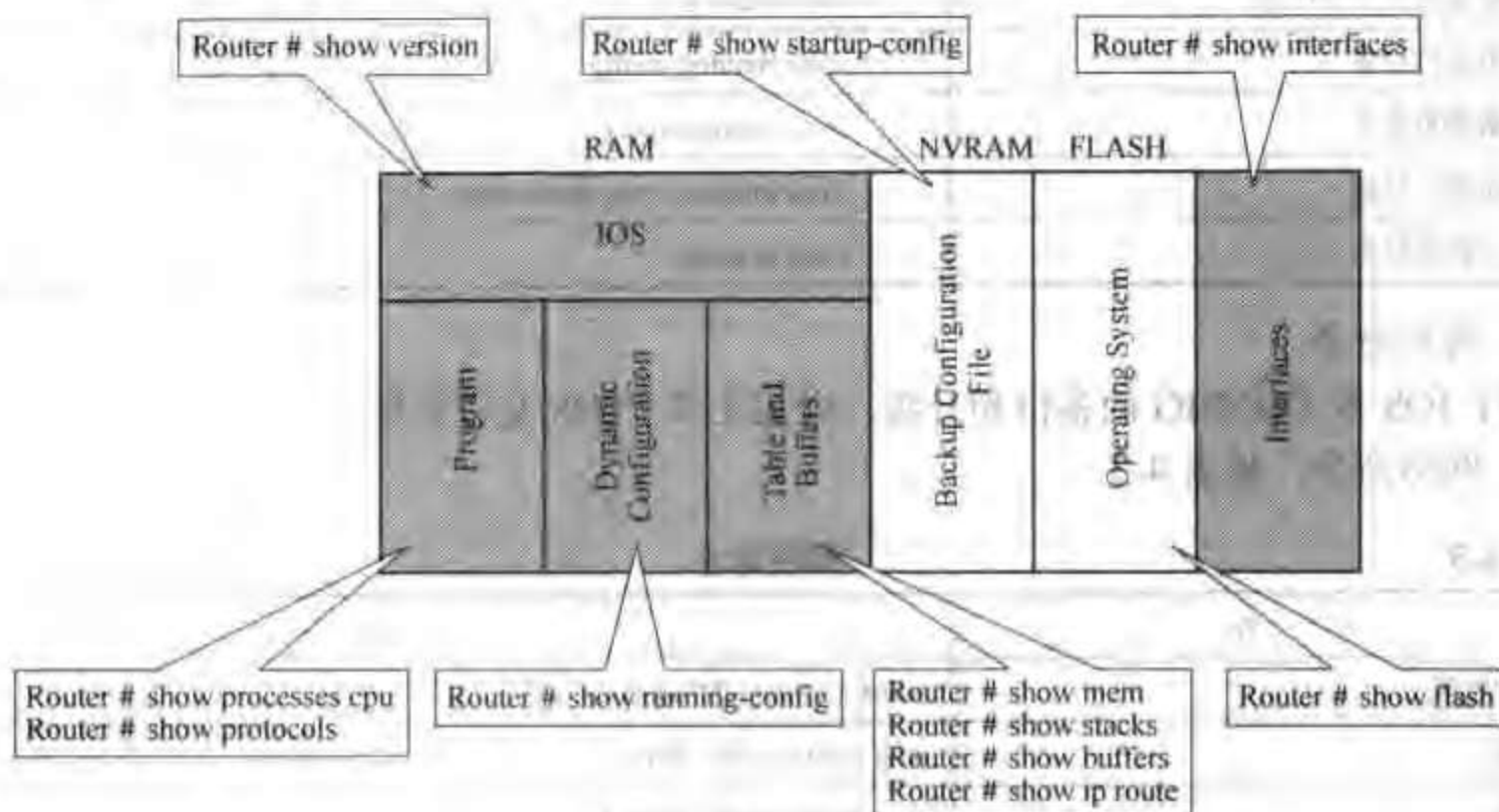


图 4-20 配置显示示意图

4.3.6 交换机基本配置模板

交换机的具体配置根据不同的需求会有很大的不同，但所有的交换机都有一些共同的部分，这些部分我们可以作为基本的模板用于交换机的最初始配置。

(1) 设主机名和密码

```
hostname cisco
```

```
enable password cisco
```

(2) 禁止 DNS 查询

```
no ip domain-lookup
```

(3) 为 log 和 debug 设置时间戳

```
service timestamps debug uptime
```

```
service timestamps debug datetime
```

```
service timestamps log uptime
```

```
service timestamps log datetime
```

(4) 设置 Telnet 登录参数

```
line vty 0 4
```

```
password cisco
```

```
login
```

(5) 基本安全的设置

```
hostname cisco
```

```
enable password cisco
```

```
line con 0
```



```
login
line vty 0 4
password cisco
login
no ip http server
no snmp-server
no service finger
no ntp
no cdp run
no service udp-small-servers
no service tcp-small-servers
```

完整的配置步骤如下:

```
hostname cisco
enable password cisco
no ip domain-lookup
service timestamps debug uptime
service timestamps debug datetime
service timestamps log uptime
service timestamps log datetime
line con 0
login
line vty 0 4
password cisco
login
no ip http server
no snmp-server
no service finger
no ntp
no cdp run
no service udp-small-servers
no service tcp-small-servers
```

说明:

上面这段配置我们可以保存起来作为一个基础配置, 在配置任何交换机的时候, 都可以将这段配置首先粘贴进交换机, 然后再进行后面章节介绍的功能配置, 当然以上的密码一定要改成自己的密码。

4.3.7 端口配置

1. 配置一组端口, 见表 4-5

在配置端口参数的时候, 我们往往需要一次对一组端口进行配置, Cisco 交换机的 IOS

在版本 12.1 后支持 “interface range” 这一命令，极大地方便了配置。

表 4-5 配置一组端口

命 令	目 的
configure terminal	进入配置状态
interface range {port-range}	进入组配置状态
	可以使用平时的端口配置命令进行配置
end	退回
show interfaces [interface-id]	验证配置
copy running-config startup-config	保存（等同命令 “write memory” ）

注：

- （1）端口号之间需要加入空格，如：int range fa 0/1 - 5 是有效的，而 int range fa 0/1-5 是无效的。
- （2）所有在同一组的端口必须是相同类别的。

配置举例：

Switch# configure terminal

Switch(config)# interface range fastethernet0/1 - 5

Switch(config-if-range)# no shutdown

Switch(config-if-range)#

*Oct 6 08:24:35: %LINK-3-UPDOWN: interface fastethernet0/1, changed state to up

*Oct 6 08:24:35: %LINK-3-UPDOWN: interface fastethernet0/2, changed state to up

*Oct 6 08:24:35: %LINK-3-UPDOWN: interface fastethernet0/3, changed state to up

*Oct 6 08:24:35: %LINK-3-UPDOWN: interface fastethernet0/4, changed state to up

*Oct 6 08:24:35: %LINK-3-UPDOWN: interface fastethernet0/5, changed state to up

*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: line protocol on interface fastethernet0/05, changed state to up

*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: line protocol on interface fastethernet0/3, changed state to up

*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: line protocol on interface fastethernet0/4, changed state to up

Switch(config-if-range)#end

Switch#copy run start

Switch#

2. 配置二层端口

交换机端口默认都是二层端口，在支持三层交换的交换机上（Catalyst 3550、3750、4500、6500），我们可以将每一个端口都配置成路由端口（在接口状态下，输入 “no switchport” 命令），如果一个端口已经配置为路由端口，我们可以在其接口状态下，输入 “switchport” 命令使其恢复为交换端口。

- （1）配置端口速率及双工模式，见表 4-6

可以配置接速以太口的速率为 10/100Mbit/s 及吉比特以太口的速率为 10/100/1000Mbit/s，

但对于 GBIC 端口则不能配置速率及双工模式。

表 4-6 配置二层端口速率及双工模式

命 令	目 的
<code>configure terminal</code>	进入配置状态
<code>interface interface-id</code>	进入端口配置状态
<code>speed {10 100 1000 auto nonegotiate}</code>	设置端口速率
<code>duplex {auto/full/half}</code>	设置全双工或半双工
<code>end</code>	退出
<code>show interfaces interface-id</code>	显示有关配置情况
<code>copy running-config startup-config</code>	保存（等同命令“write memory”）

配置举例：

```
Switch# configure terminal
Switch(config)# interface fastethernet0/5
Switch(config-if)# speed 100
Switch(config-if)# duplex full
Switch(config-if)# end
Switch# copy run start
Switch#
```

（2）配置端口描述，见表 4-7

表 4-7 配置二层端口描述

命 令	目 的
<code>configure terminal</code>	进入配置模式
<code>interface interface-id</code>	进入要加入描述的端口
<code>description string</code>	加入描述（最多 240 个字符）
<code>end</code>	退回
<code>show interfaces interface-id description</code> or <code>show running-config</code>	验证
<code>copy running-config startup-config</code>	保存（等同命令“write memory”）

配置举例：

```
Switch# config terminal
Switch(coufig)# interface fastethernet0/5
Switch(config-if)# description link to tech
Switch(config-if)# end
Switch# show interfaces fastethernet0/5 description
```

Interface	Status	Protocol	Description
-----------	--------	----------	-------------

表 4-9 监控端口和控制器的状态

命 令	目 的
show interfaces [interface-id]	显示所有端口或某一端口的状态和配置
show interfaces interface-id status [err-disabled]	显示一系列端口的状态或错误—关闭的状态
show interfaces [interface-id] switchport	显示二层端口的状态，可以用来决定此端口是否为二层或三层端口
show interfaces [interface-id] description	显示端口描述
show ip interface [interface-id]	显示所有或某一端口的 IP 可用性状态
show running-config interface [interface-id]	显示当前配置中的端口配置情况
show version	显示软硬件等情况

配置举例：

Switch#show interfaces status

port	Name	Status	VLAN	Duplex	Speed	Type
fa0/1		connected	trunk	a-full	a-100	10/100Base-TX
fa0/2		notconnect	1	auto	auto	10/100Base-TX
fa0/3		notconnect	1	auto	auto	10/100Base-TX
fa0/4		notconnect	1	auto	auto	10/100Base-TX
fa0/5		notconnect	1	auto	auto	10/100Base-TX
fa0/6		notconnect	1	auto	auto	10/100Base-TX
fa0/7		notconnect	1	auto	auto	10/100Base-TX
fa0/8		notconnect	1	auto	auto	10/100Base-TX
fa0/9		connected	4	a-full	a-100	10/100Base-TX
fa0/10		notconnect	1	auto	auto	10/100Base-TX
fa0/11		notconnect	1	auto	auto	10/100Base-TX
fa0/12		connected	1	a-half	a-10	10/100Base-TX

.....

Switch#show interfaces fa0/9 switchport

Name: Fa0/9

Switchport: Enabled

Administrative Mode: dynamic desirable

Operational Mode: static access

Administrative Trunking Encapsulation: negotiate

Operational Trunking Encapsulation: native

Negotiation of Trunking: on

Access Mode VLAN: 4 (VLAN0004)

Trunking Native Mode VLAN: 1 (default)

Administrative Private-VLAN Host-association: none

Administrative private-vlan mapping: none

Operational Private-VLAN: none

Trunking VLANs Enabled: all

Pruning VLANs Enabled: 2-1001

Protected: false

Unknown Unicast Blocked: disabled

Unknown Multicast Blocked: disabled

Voice VLAN: none (Inactive)

Appliance Trust: none

Switch#

```
Switch#show running-config interface fastethernet 0/1
```

Building configuration...

Current configuration : 131 bytes

!

```
interface fastethernet0/1
```

```
switchport trunk encapsulation isl
```

```
switchport mode trunk
```

no ip address

spanning-tree portfast

end

Switch1#

(2) 刷新端口计数器, 见表 4-10

表 4-10

刷新端口计数器命令

命 令	目 的
clear counters [<i>interface-id</i>]	清除端口计数器
clear interface <i>interface-id</i>	重置某一端口的硬件逻辑
clear line [<i>number/console 0/vty number</i>]	重置异步串口的硬件逻辑

注: `clear counters` 命令只清除用 `show interface` 所显示的计数, 不影响用 `snmp` 得到的计数。

配置举例：

Switch1#clear counters fastetheru0/9

```
Clear "show interface" counters on this interface [confirm]y
```

Switch1#

```
7w1d: %CLEAR-5-COUNTERS: clear counter on interface fastethernet0/9 by vty0
(192.168.3.128)
```

Switch#

(3) 关闭和打开端口, 见表 4-11

表 4-11

关闭和打开端口命令

命 令	目 的
configure terminal	进入配置状态
interface [vlan <i>vlan-id</i>] [{fastethernet gigabitethernet} <i>interface-id</i>] {port-channel <i>port-channel-number</i> }	进入要操作的端口
shutdown	关闭端口
no shutdown	打开端口
end	退出
show running-config	验证

配置举例:

```
Switch# configure terminal
```

```
Switch(config)# interface fastethernet0/5
```

```
Switch(config-if)# shutdown
```

```
Switch(config-if)#
```

```
*Sep 30 08:33:47: %LINK-5-CHANGED: interface fastethernet0/5, changed state to a
administratively down
```

```
Switch# configure terminal
```

```
Switch(config)# interface fastethernet0/5
```

```
Switch(config-if)# no shutdown
```

```
Switch(config-if)#
```

```
*Sep 30 08:36:00: %LINK-3-UPDOWN: interface fastethernet0/5, changed state to up
```

4.3.8 VLAN 配置

VLAN 的出现打破了传统网络的许多固有观念,使网络结构变得灵活、方便、随心所欲。VLAN 就是不考虑用户的物理位置而根据功能、应用等因素将用户逻辑上划分为一个个功能相对独立的工作组,每个用户主机都连接在一个支持 VLAN 的交换机端口上并属于一个 VLAN。同一个 VLAN 中的成员都共享广播,而不同 VLAN 之间广播信息是相互隔离的。这样,就将整个网络分割成多个不同的广播域。每一个 VLAN 均可看成是一个逻辑网络,发往另一 VLAN 的数据包必须由路由器或网桥转发(如图 4-21 所示)。由于 VLAN 被看成是一个逻辑网络,它具有自己的网桥管理信息库(MIB)并可支持自己的生成树。

VLAN 常常与 IP 子网相联系,同一 IP 子网属于同一 VLAN。在三层交换机上 VLAN 之间的数据包可以由 VLAN 虚拟端口(SVI)进行转发。

以下的介绍都是基于 Cisco 交换机的 VLAN。Cisco 的 VLAN 实现通常是以端口为中心的,与节点相连的端口将确定它所驻留的 VLAN。将端口分配给 VLAN 的方式有两种:静态的和动态的。

形成静态 VLAN 的过程是将端口强制性地分配给 VLAN 的过程,即先在 VTP Server (VLAN Trunking Protocol Server)上建立 VLAN,然后将每个端口分配给相应的 VLAN 的过程。这是我们创建 VLAN 最常用的方法。

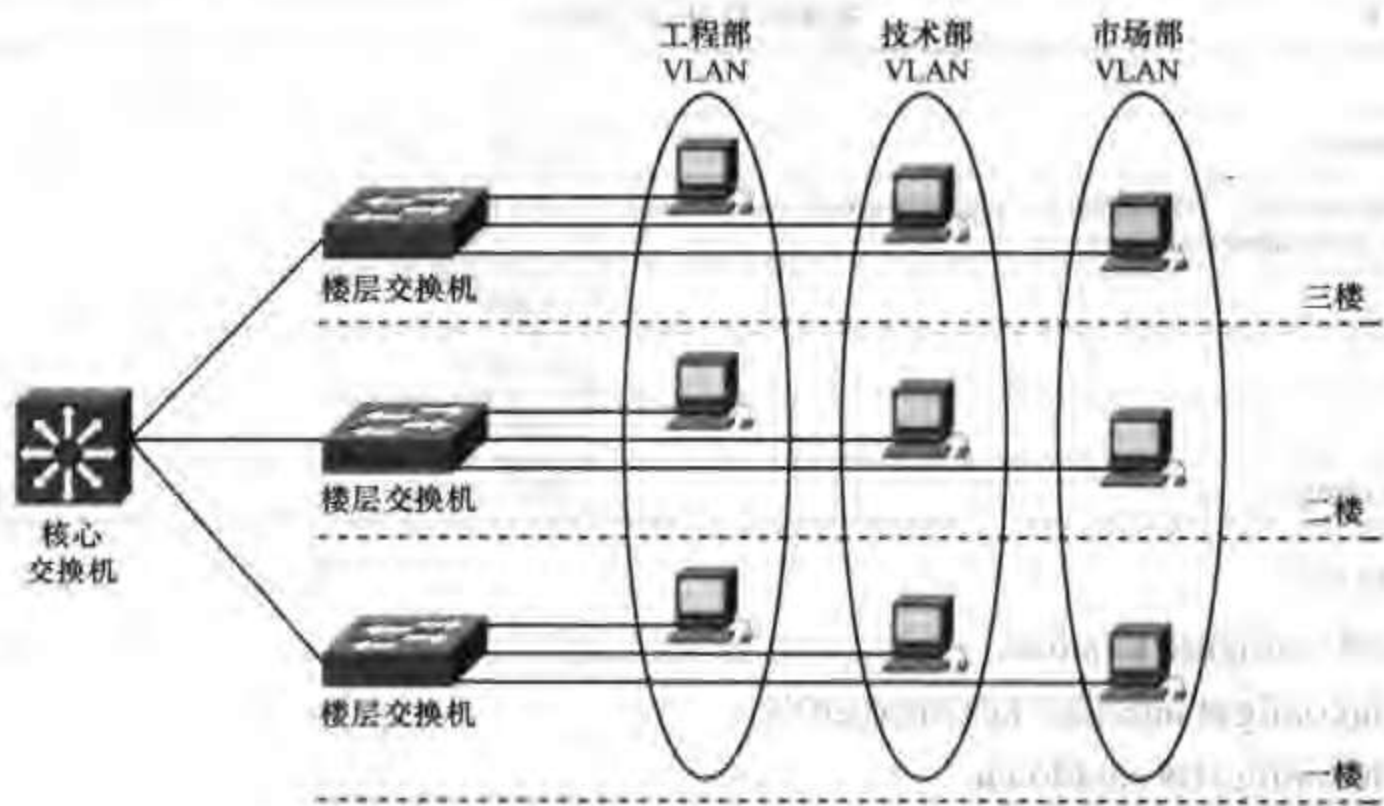


图 4-21 VLAN 示意图

动态 VLAN 形成很简单，由具体的机器决定自己属于哪个 VLAN，即先建立一个 VMPS (VLAN Membership Policy Server) VLAN 管理策略服务器，里面包含一个文本文件，该文件中存有与 VLAN 映射的 MAC 地址表。交换机根据这个映射表决定将端口分配给何种 VLAN。这种方法有很大的优势，但创建数据库是一项非常艰苦而且非常繁琐的工作。

下面以实例说明如何在一个典型的快速以太网局域网中实现 VLAN，如图 4-22 所示。所谓典型局域网就是指由一台具备三层交换功能的核心交换机接几台楼层交换机（不一定具备三层交换能力）。我们假设核心交换机名称为 core；楼层交换机分别为 fl1、fl2、fl3，分别通过吉比特光纤端口 g0/1 与核心交换机相连；并且假设 VLAN 名称分别为 engineering、techniqy、marketing。

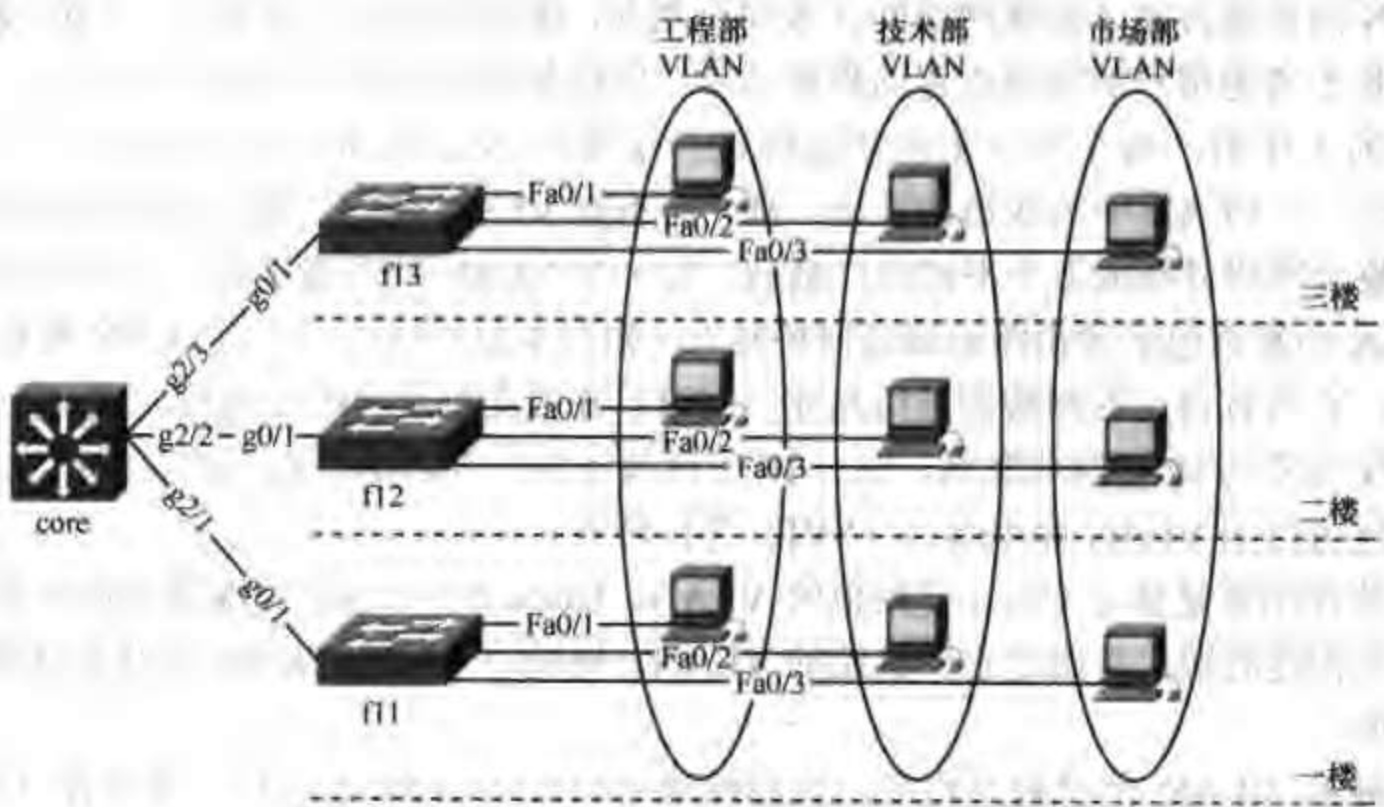


图 4-22 典型 VLAN 配置案例

说明:

在实际工程中, 往往不会在每个楼层都设配线架, 通常情况是 2~3 层楼共用一个配线架。当然, 我们可以将这里的 1、2 和 3 层 (fl1、fl2 和 fl3) 想像成实际工程中的 1、4、7 层。

需要做的工作:

- (1) 设置 VTP DOMAIN (核心、分支交换机上都设置);
- (2) 配置中继 (核心、分支交换机上都设置);
- (3) 创建 VLAN (在 server 上设置);
- (4) 将交换机端口划入 VLAN;
- (5) 配置三层交换;
- (6) 设置 VTP DOMAIN, VTP DOMAIN 称为管理域。

交换 VTP 更新信息的所有交换机必须配置为相同的管理域。如果所有的交换机都以中继线相连, 那么只要核心交换机上设置一个管理域, 网络上所有的交换机都加入该域, 这样管理域里所有的交换机就能够了解彼此的 VLAN 列表。

在核心交换机上的配置过程如下:

```
! ---进入 VLAN 配置模式
core#vlan database
! ---设置 VTP 管理域名称 test
core(vlan)#vtp domain test
! ---设置交换机为服务器 (server) 模式
core (vlan)#vtp server
```

在楼层交换机上的配置过程如下:

```
! ---进入 VLAN 配置模式
fl1#vlan database
! ---设置 VTP 管理域名称 test
fl1(vlan)#vtp domain test
! ---设置交换机为客户机 (client) 模式
fl1(vlan)#vtp client

! ---进入 VLAN 配置模式
fl2#vlan database
! ---设置 VTP 管理域名称 test
fl2(vlan)#vtp domain test
! ---设置交换机为客户机 (client) 模式
fl2(vlan)#vtp client

! ---进入 VLAN 配置模式
fl3#vlan database
! ---设置 VTP 管理域名称 test
fl3(vlan)#vtp domain test
! ---设置交换机为客户机 (client) 模式
```



```
fl3(vlan)#vtp client
```

另外，还有一种简单的配置 VTP 的方式，如下：

```
core#conf t
```

```
core(config)#vtp domain test
```

```
core(config)#vtp mode server
```

```
fl1#conf t
```

```
fl1(config)#vtp domain test
```

```
fl1(config)#vtp mode client
```

```
fl2#conf t
```

```
fl2(config)#vtp domain test
```

```
fl2(config)#vtp mode client
```

```
fl3#conf t
```

```
fl3(config)#vtp domain test
```

```
fl3(config)#vtp mode client
```

注意：这里设置核心交换机为 Server 模式是指允许在该交换机上创建、修改、删除 VLAN 及其他一些对整个 VTP 域的配置参数，同步本 VTP 域中其他交换机传递来的最新的 VLAN 信息；Client 模式是指本交换机不能创建、删除、修改 VLAN 配置，也不能在 NVRAM 中存储 VLAN 配置，但可同步由本 VTP 域中其他交换机传递来的 VLAN 信息。

（1）配置中继为了保证管理域能够覆盖所有的分支交换机，因此必须配置中继

Cisco 交换机能够支持任何介质作为中继线，为了实现中继可使用 Cisco 特有的 ISL 标签，也可使用国际标准协议 dot1q。中继协议是一个在交换机之间、交换机与路由器之间及交换机与服务器之间传递多个 VLAN 信息及 VLAN 数据流的协议，通过将交换机之间相连的端口配置为中继端口，即可跨越交换机进行整个网络的 VLAN 分配和进行配置。

在核心交换机上配置如下：

```
! ---进入下联端口（g2/1）
```

```
core(config)#interface gigabitethernet 2/1
```

```
! --配置端口的描述（连接 fl1 的 g0/1）
```

```
core(config-if)#description link to fl1 g0/1
```

```
! --指定本端口为二层（交换）端口
```

```
core(config-if)#switchport
```

```
! ---配置中继协议为 dot1q
```

```
core(config-if)#switchport trunk encapsulation dot1q
```

```
! ---指定端口的模式为中继（trunk）端口
```

```
core(config-if)#switchport mode trunk
```

```
! ---进入下联端口（g2/2）：
```

```
core(config)#interface gigabitethernet 2/2
```

```
! --配置端口的描述（连接 fl2 的 g0/1）
```



```
core(config-if)#description link to fl2 g0/1
! --指定本端口为二层（交换）端口：
core(config-if)#switchport
! ---配置中继协议为 dot1q:
core(config-if)#switchport trunk encapsulation dot1q
! ---指定端口的模式为中继（trunk）端口
core(config-if)#switchport mode trunk
```

```
! ---进入下联端口（g2/2）
core(config)#interface gigabitethernet 2/3
! --配置端口的描述（连接 fl3 的 g0/1）
core(config-if)#description link to fl3 g0/1
! --指定本端口为二层（交换）端口
core(config-if)#switchport
! ---配置中继协议为 dot1q
core(config-if)#switchport trunk encapsulation dot1q
! ---指定端口的模式为中继（trunk）端口
core(config-if)#switchport mode trunk
```

在楼层交换机上配置如下：

```
! ---进入上联端口（g0/1）
fl1(config)#interface gigabitethernet 0/1
! ---配置中继协议为 dot1q
fl1(config-if)# switchport trunk encapsulation dot1q
! ---指定端口的模式为中继（trunk）端口
fl1(config-if)#switchport mode trunk
```

```
! ---进入上联端口（g0/1）：
fl2(config)#interface gigabitEthernet 0/1
! ---配置中继协议为 dot1q
fl2(config-if)# switchport trunk encapsulation dot1q
! ---指定端口的模式为中继（trunk）端口
fl2(config-if)#switchport mode trunk
```

```
! ---进入上联端口（g0/1）
fl3(config)#interface gigahitEthernet 0/1
! ---配置中继协议为 dot1q
fl3(coufig-if)# switchport trunk encapsulation dot1q
! ---指定端口的模式为中继（trunk）端口
fl3(config-if)#switchport mode trunk
```


此时，管理域就设置完毕了。

(2) 创建 VLAN，一旦建立了管理域，就可以创建 VLAN 了

! ---进入 VLAN 配置模式

```
core#vlan database
```

! ---创建一个编号为 10 名字为 engineering 的 VLAN

```
core(vlan)#Vlan 10 name engineering
```

! ---创建一个编号为 20 名字为 techniqy 的 VLAN

```
core(vlan)#Vlan 20 name techniqy
```

! ---创建一个编号为 30 名字为 marketing 的 VLAN

```
core(vlan)#Vlan 30 name marketing
```

另外，还有一种简单的创建 VLAN 的方式，如下所示：

```
core#conf t
```

```
core(config)#vlan 10,20,30
```

注意，这里的 VLAN 是在核心交换机上建立的。其实，只要是在管理域中的任何一台 VTP 属性为 Server 的交换机上建立 VLAN，它就会通过 VTP 通告整个管理域中的所有的交换机。但如果要将具体的交换机端口划入某个 VLAN，就必须在该端口所属的交换机上进行设置。

(3) 将交换机端口划入 VLAN

例如，要将 f11、f12、f13 接入交换机的端口 fa0/1 划入 engineering VLAN，端口 fa0/2 划入 techniqy VLAN，端口 fa0/3 划入 marketing VLAN。

! ---进入端口 fa0/1

```
f11(config)#interface fastethernet 0/1
```

! ---设置端口模式 (access)

```
f11(config-if)#switchport mode access
```

! ---配置本端口属于 VLAN 10

```
f11(config-if)#switchport access vlan 10
```

! ---进入端口 fa0/2

```
f11(config)#interface fastethernet 0/2
```

! ---设置端口模式 (access)

```
f11(config-if)#switchport mode access
```

! ---配置本端口属于 VLAN 20

```
f11(config-if)#switchport access vlan 20
```

! ---进入端口 fa0/3

```
f11(config)#interface fastethernet 0/3
```

! ---设置端口模式 (access)

```
f11(config-if)#switchport mode access
```

! ---配置本端口属于 VLAN 30


```
fl1(config-if)#switchport access vlan 30
```

```
! ---进入端口 fa0/1
```

```
fl2(config)#interface fastethernet 0/1
```

```
! ---设置端口模式 (access)
```

```
fl2(config-if)#switchport mode access
```

```
! ---配置本端口属于 VLAN 10
```

```
fl2(config-if)#switchport access vlan 10
```

```
! ---进入端口 fa0/2
```

```
fl2(config)#interface fastethernet 0/2
```

```
! ---设置端口模式 (access)
```

```
fl2(config-if)#switchport mode access
```

```
! ---配置本端口属于 VLAN 20
```

```
fl2(config-if)#switchport access vlan 20
```

```
! ---进入端口 fa0/3
```

```
fl2(config)#interface fastethernet 0/3
```

```
! ---设置端口模式 (access)
```

```
fl1(config-if)#switchport mode access
```

```
! ---配置本端口属于 VLAN 30
```

```
fl2(config-if)#switchport access vlan 30
```

```
! ---进入端口 fa0/1
```

```
fl3(config)#interface fastethernet 0/1
```

```
! ---设置端口模式 (access)
```

```
fl3(config-if)#switchport mode access
```

```
! ---配置本端口属于 VLAN 10
```

```
fl3(config-if)#switchport access vlan 10
```

```
! ---进入端口 fa0/2
```

```
fl3(config)#interface fastethernet 0/2
```

```
! ---设置端口模式 (access)
```

```
fl3(config-if)#switchport mode access
```

```
! ---配置本端口属于 VLAN 20
```

```
fl3(config-if)#switchport access vlan 20
```

```
! ---进入端口 fa0/3
```

```
fl3(config)#interface fastethernet 0/3
```

```
! ---设置端口模式 (access)
```



```
fl3(config-if)#switchport mode access
! ---配置本端口属于 VLAN 30
fl3(config-if)#switchport access vlan 30
(4) 配置三层交换
```

到这里, VLAN 已经基本划分完毕。但是, VLAN 间如何实现三层(网络层)交换呢? 这时就要给各 VLAN 分配网络(IP)地址了。给 VLAN 分配 IP 地址分两种情况: 其一, 给 VLAN 所有的节点分配静态 IP 地址; 其二, 给 VLAN 所有的节点分配动态 IP 地址。下面就这两种情况分别介绍。

假设给 VLAN engineering 分配的接口 IP 地址为 172.16.1.254/24, 网络地址为 172.16.1.0; VLAN techniqy 分配的接口 IP 地址为 172.16.2.254/24, 网络地址为 172.16.2.0; VLAN marketing 分配接口 IP 地址为 172.16.3.254/24, 网络地址为 172.16.3.0。如果动态分配 IP 地址, 则设网络上的 DHCP 服务器 IP 地址为 172.16.100.1。

① 给 VLAN 所有的节点分配静态 IP 地址

首先在核心交换机上分别设置各 VLAN 的接口 IP 地址。核心交换机将 VLAN 作为一种接口对待, 就像路由器上的一样, 如下所示:

```
! ---进入 VLAN 10 接口
core(config)#interface vlan 10
! ---为 VLAN10 接口配置 IP
core(config-if)#ip address 172.16.1.254 255.255.255.0
```

```
! ---进入 VLAN 20 接口
core(config)#interface vlan 20
! ---为 VLAN20 接口配置 IP
core(config-if)#ip address 172.16.2.254 255.255.255.0
```

```
! ---进入 VLAN 30 接口
core(config)#interface vlan 30
! ---为 VLAN30 接口配置 IP
core(config-if)#ip address 172.16.3.254 255.255.255.0
```

再在各个接入 VLAN 的计算机上设置与所属 VLAN 的网络地址一致的 IP 地址, 并且把默认网关设置为该 VLAN 的接口地址。这样, 所有的 VLAN 也可以互访了。

② 给 VLAN 所有的节点分配动态 IP 地址

首先在核心交换机上分别设置各 VLAN 的接口 IP 地址和同样的 DHCP 服务器的 IP 地址, 如下所示:

```
! ---进入 VLAN 10 接口
core(config)#interface vlan 10
! ---为 VLAN10 接口配置 IP
core(config-if)#ip address 172.16.1.254 255.255.255.0
! ---为 VLAN10 接口配置 DHCP Server
```



```
core(config-if)#ip helper-address 172.16.100.1
```

! ---进入 VLAN 20 接口

```
core(config)#interface vlan 20
```

! ---为 VLAN20 接口配置 IP

```
core(config-if)#ip address 172.16.2.254 255.255.255.0
```

! ---为 VLAN10 接口配置 DHCP Server

```
core(config-if)#ip helper-address 172.16.100.1
```

! ---进入 VLAN 30 接口

```
core(config)#interface vlan 30
```

! ---为 VLAN30 接口配置 IP

```
core(config-if)#ip address 172.16.3.254 255.255.255.0
```

! ---为 VLAN10 接口配置 DHCP Server

```
core(config-if)#ip helper-address 172.16.100.1
```

再在 DHCP 服务器上设置网络地址分别为 172.16.1.0、172.16.2.0、172.16.3.0 的作用域,并将这些作用域的“路由器”选项设置为对应 VLAN 的接口 IP 地址。这样,可以保证所有的 VLAN 也可以互访了。

最后在各个接入 VLAN 的计算机进行网络设置,将 IP 地址选项设置为自动获得 IP 地址即可。

4.4 Cisco 交换机经典配置案例

4.4.1 案例 1

此案例是配置如图 4-23 所示的小型局域网。

1. 需求接述

企业内部需要联网的节点数为 200 点,信息点分布在 1~5 层,网络中心设在一楼,大楼主干采用光纤布线,在 1 层和 3 层设楼层配线架,楼层需要百兆交换到桌面。企业主要应用为内部文件共享、办公自动化(OA)系统,对外提供邮件和网站服务等。网络核心是一台 Catalyst4507R,配置双引擎,另外配置 WS-X4306-GB 模块,用于和各楼层的交换机实现吉比特互连。网络需要划分 VLAN 用于隔离广播,同时从安全方面考虑,财务部的主机不能被其他部门的主机访问。本方案所选产品见表 4-12。

表 4-12

本方案所选产品列表

产 品	描 述	数 量
WS-C4507R	Catalyst 4500 Chassis (7 插槽),风扇,无 p/s, Red Sup Capable	1
PWR-C45-1000AC	Catalyst 4500 1000W AC 电源 (仅用于数据)	1
PWR-C45-1000AC/2	Catalyst 4500 1000W AC 备用电源	1

续表

产 品	描 述	数 量
CAB-7KACA	AC 电源线	2
WS-X4515	Catalyst 4500 监视器 IV (2 GE),控制台(RJ-45)	1
WS-X4515/2	Catalyst 4507R 备用监视器 IV,(2 GE),控制台(RJ-45)	1
S4KL3-12113EW	Cisco IOS BASIC L3 Cat4500 SUP 3/4(RIP,St.Routes,IPX,AT)	1
WS-X4306-GB	Catalyst 4500 吉比特以太网模块,6 端口 (GBIC)	1
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	5
WS-G5484	1000BASE-SX 短波长 GBIC (仅用于多模)	4

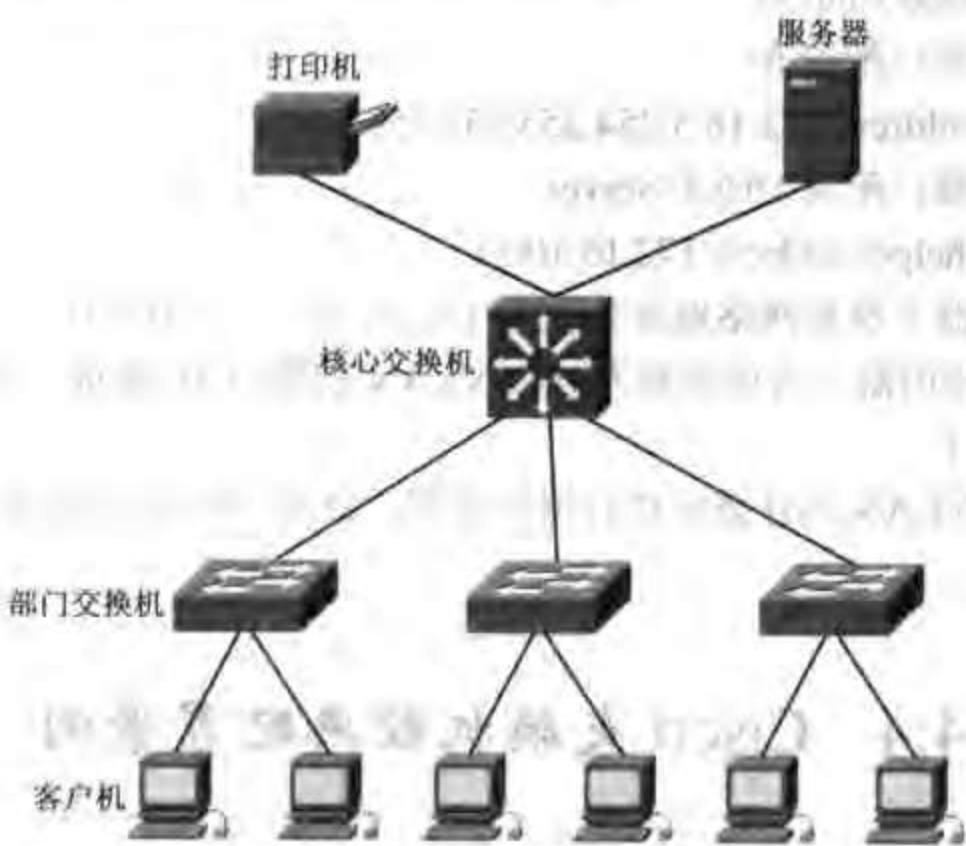


图 4-23 小型局域网

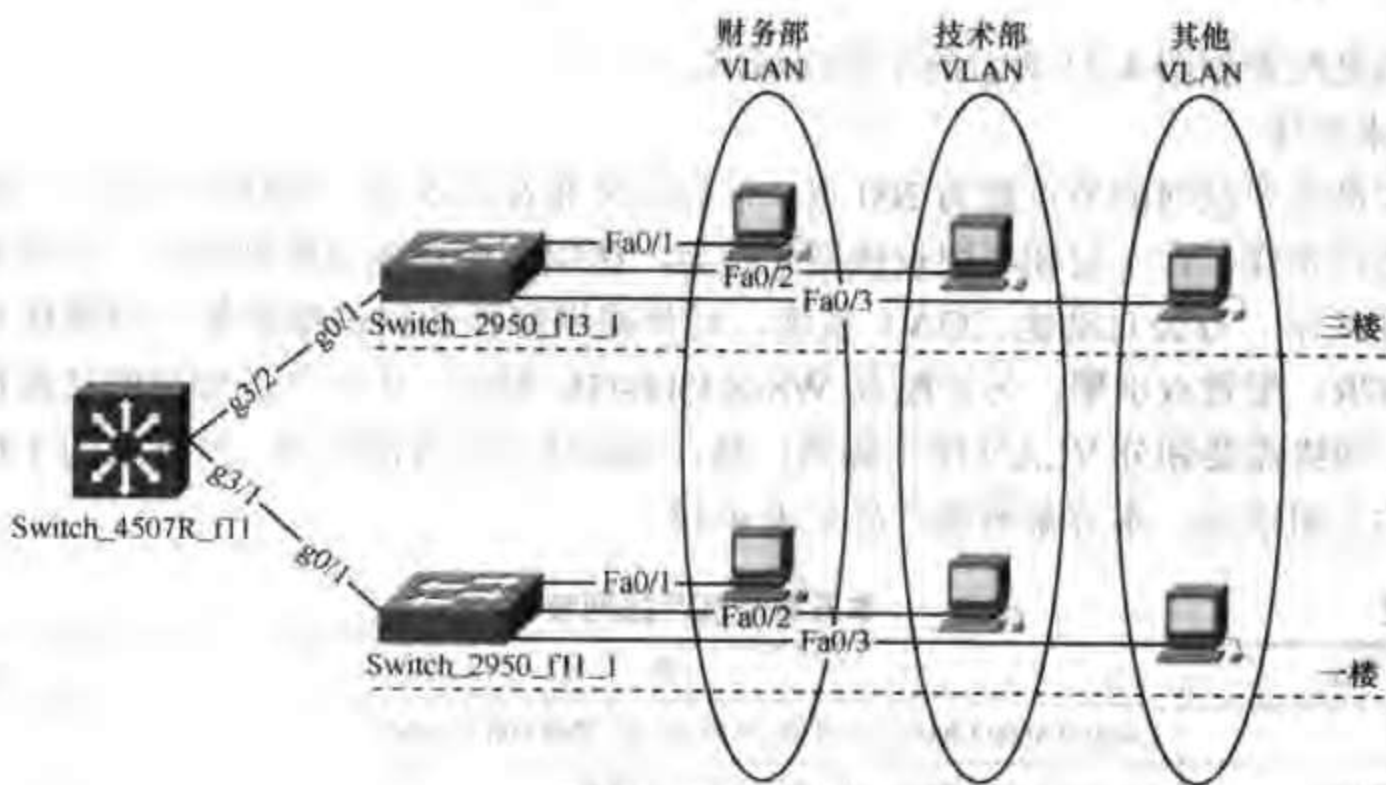


图 4-24 交换机配置

需要做的工作如下:

- (1) 交换机基础性配置;
- (2) 设置 VTP DOMAIN (核心、分支交换机上都设置);
- (3) 配置中继 (核心、分支交换机上都设置);
- (4) 创建 VLAN (在 VTP Server 上设置);
- (5) 将交换机端口划入 VLAN;
- (6) 配置三层交换;
- (7) 配置 VLAN 访问控制 (VACL)。

2. 配置文档

(1) 交换机基础性配置

在核心交换机和楼层交换机上的基础性配置除主机名和密码外, 其他基本相同。在做网络配置时, 我们通常会对所有的网络设备进行规范的命名, 命名的规则往往遵从简单和易于识别的原则, 这里我们设置命名规则, “类别_型号_楼层_序号”, 比如, “switch_2950_fl1_1” 表示“一层的的第一台 2950 交换机”, 当只有一台时, 序号可省略。

交换机的基础性配置如下:

```
hostname switch_4507R_fl1
```

```
enable password cisco
```

```
no ip domain-lookup
```

```
service timestamps debug uptime
```

```
service timestamps debug datetime
```

```
service timestamps log uptime
```

```
service timestamps log datetime
```

```
line con 0
```

```
login
```

```
line vty 0 4
```

```
password cisco
```

```
login
```

```
no ip http server
```

```
no snmp-server
```

```
no service finger
```

```
no ntp
```

```
no cdp run
```

```
no service udp-small-servers
```

```
no service tcp-small-servers
```

注意: 带阴影的部分根据具体的交换机进行相应的设置。

(2) 设置 VTP DOMAIN

在核心交换机上配置如下:

```
Switch_4507R_fl1 #vlan database
```

```
Switch_4507R_fl1 (vlan)#vtp domain test
```



```
Switch_4507R_fl1 (vlan)#vtp server
```

在楼层交换机上配置如下:

```
Switch_2950_fl1_1#vlan database
```

```
Switch_2950_fl1_1 (vlan)#vtp domain test
```

```
Switch_2950_fl1_1 (vlan)#vtp client
```

```
Switch_2950_fl3_1#vlan database
```

```
Switch_2950_fl3_1 (vlan)#vtp domain test
```

```
Switch_2950_fl3_1 (vlan)#vtp client
```

另外, 还有一种简单的配置 VTP 的方式, 如下所述:

```
Switch_4507R_fl1 #conf t
```

```
Switch_4507R_fl1 (config)#vtp domain test
```

```
Switch_4507R_fl1 (config)#vtp mode server
```

```
Switch_2950_fl1_1#conf t
```

```
Switch_2950_fl1_1 (config)#vtp domain test
```

```
Switch_2950_fl1_1 (config)#vtp mode client
```

```
Switch_2950_fl3_1#conf t
```

```
Switch_2950_fl3_1 (config)#vtp domain test
```

```
Switch_2950_fl3_1 (config)#vtp mode client
```

(3) 配置中继

在核心交换机上配置如下:

```
Switch_4507R_fl1 (config)#interface gigabitethernet 3/1
```

```
Switch_4507R_fl1 (config-if)#description link to Switch_2950_fl1_1 g0/1
```

```
Switch_4507R_fl1 (config-if)#switchport
```

```
Switch_4507R_fl1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_4507R_fl1 (config-if)#switchport mode trunk
```

```
Switch_4507R_fl1 (config)#interface gigabitethernet 3/2
```

```
Switch_4507R_fl1 (config-if)#description link to Switch_2950_fl3_1 g0/1
```

```
Switch_4507R_fl1 (config-if)#switchport
```

```
Switch_4507R_fl1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_4507R_fl1 (config-if)#switchport mode trunk
```

在楼层交换机上配置如下:

```
Switch_2950_fl1_1 (config)#interface gigabitethernet 0/1
```

```
Switch_2950_fl1_1 (config-if)#description link to Switch_4507R_fl1 g3/1
```

```
Switch_2950_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_2950_fl1_1 (config-if)#switchport mode trunk
```

```
Switch_2950_fl3_1 (config)#interface gigabitethernet 0/1
```

```
Switch_2950_fl3_1 (config-if)#description link to Switch_4507R_fl1 g3/2
```



```
Switch_2950_fl3_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_2950_fl3_1 (config-if)#switchport mode trunk
```

(4) 创建 VLAN

(5) 在核心交换机 4507R 上配置 VLAN

其实，只要是在管理域中的任何一台 VTP 属性为 Server 的交换机上建立 VLAN，它就会通过 VTP 通告整个管理域中的所有的交换机。

```
Switch_4507R_fl1 #vlan database
```

```
Switch_4507R_fl1 (vlan)#Vlan 10 name finance
```

```
Switch_4507R_fl1 (vlan)#Vlan 20 name techniqy
```

```
Switch_4507R_fl1 (vlan)#Vlan 30 name other
```

另外，还有一种简单的创建 VLAN 的方式，如下：

```
Switch_4507R_fl1 #conf t
```

```
Switch_4507R_fl1 (config)#vlan 10,20,30
```

(6) 将交换机端口划入 VLAN

这里我们假设要将 Switch_2950_fl1_1、Switch_2950_fl3_1 接入交换机的端口 fa0/1 划入 finance VLAN（财务部 VLAN），端口 fa0/2 划入 techniqy VLAN（技术部 VLAN），端口 fa0/3 划入 other VLAN（其他部门 VLAN）。

```
Switch_2950_fl1_1 (config)#interface fastethernet 0/1
```

```
Switch_2950_fl1_1 (config-if)#switchport mode access
```

```
Switch_2950_fl1_1 (config-if)#switchport access vlan 10
```

```
Switch_2950_fl1_1 (config)#interface fastethernet 0/2
```

```
Switch_2950_fl1_1 (config-if)#switchport mode access
```

```
Switch_2950_fl1_1 (config-if)#switchport access vlan 20
```

```
Switch_2950_fl1_1 (config)#interface fastethernet 0/3
```

```
Switch_2950_fl1_1 (config-if)#switchport mode access
```

```
Switch_2950_fl1_1 (config-if)#switchport access vlan 30
```

```
Switch_2950_fl3_1 (config)#interface fastethernet 0/1
```

```
Switch_2950_fl3_1 (config-if)#switchport mode access
```

```
Switch_2950_fl3_1 (config-if)#switchport access vlan 10
```

```
Switch_2950_fl3_1 (config)#interface fastethernet 0/2
```

```
Switch_2950_fl3_1 (config-if)#switchport mode access
```

```
Switch_2950_fl3_1 (config-if)#switchport access vlan 20
```

```
Switch_2950_fl3_1 (config)#interface fastethernet 0/3
```

```
Switch_2950_fl3_1 (config-if)#switchport mode access
```

```
Switch_2950_fl3_1 (config-if)#switchport access vlan 30
```

(7) 配置三层交换

到目前为止，各部门已经划入不同的 VLAN。但是，此时只有本 VLAN 的主机之间可以

互相访问，不同 VLAN 的主机之间是不能互访的。为了让不同 VLAN 之间可以互访，我们需要为不同的 VLAN 之间架起一座桥梁，这时就要给各 VLAN 接口分配网络（IP）地址了，这个地址也就是各 VLAN 主机的网关地址。

表 4-13 给出了 VLAN 和 IP 地址的分配表。

表 4-13 此方案中各 VLAN 和 IP 地址的分配表

部 门	VLAN 名	VLAN ID	网关地址	网段地址
财务部	finance	10	192.168.1.254	192.168.1.0/24
技术部	technmqy	20	192.168.2.254	192.168.2.0/24
其他部门	other	30	192.168.3.254	192.168.3.0/24

```
Switch_4507R_fl1 (config)#interface vlan 10
Switch_4507R_fl1 (config-if)#ip address 192.168.1.254 255.255.255.0

Switch_4507R_fl1 (config)#interface vlan 20
Switch_4507R_fl1 (config-if)#ip address 192.168.2.254 255.255.255.0

Switch_4507R_fl1 (config)#interface vlan 30
Switch_4507R_fl1 (config-if)#ip address 192.168.3.254 255.255.255.0
```

然后在各个接入 VLAN 的计算机上设置与所属 VLAN 的网络地址一致的 IP 地址，并且把默认网关设置为该 VLAN 的接口地址。这样，所有的 VLAN 也可以互访了。

(8) 配置 VLAN 访问控制（VACL）

根据用户的需求知道，财务部的主机不能被其他部门的用户访问到，而财务部的主机又需要访问外部。

通常考虑，我们可以定义一条访问控制列表（ACL），禁止其他部门网段对财务部网段的访问，然后将其应用到各部门的 VLAN 接口上，配置如下：

```
Switch_4507R_fl1 (config)#access-list 101 deny ip any 192.168.1.0 0.0.0.255
Switch_4507R_fl1 (config)#access-list 101 permit ip any any
Switch_4507R_fl1 (config)#interface vlan 20
Switch_4507R_fl1 (config-if)#ip access-group 101 in
Switch_4507R_fl1 (config)#interface vlan 30
Switch_4507R_fl1 (config-if)# ip access-group 101 in
```

虽然从表面上看，这样配置是禁止了 VLAN20、VLAN30 对 VLAN10 的访问，但实际的结果是 VLAN10 对 VLAN20、VLAN30 的访问也被禁止掉了，这是为什么呢？

让我们回忆一下，在两台主机 A 与 B 之间要实现通信，需要些什么条件呢？答案是既需要 A 能向 B 发包，也需要 B 能向 A 发包，任何一个方向的包被阻断，通信都不能成功，在上面的配置中就存在这样的问题。例如，VLAN10 中的主机 A 访问 VLAN20 中的主机 B 时，数据包可以被发送到主机 B，但由主机 B 返回的数据包在到达交换机的 VLAN20 接口时，被接口上配置的 ACL 阻断了。由于普通的 ACL 不具备检测会话状态的能力，所以普通的 ACL 也就无法实现单向访问控制。

要想实现真正意义上的单向访问控制应该怎么办呢？我们希望在财务部访问其他部门

时,能在其他部门的 ACL 中临时生成一个反向的条目,这样就能实现单向访问了。这里就需要使用到反身访问控制列表技术。

在本案例中我们给出如下配置:

```
Switch_4507R_fl1 (config)#ip access-list extend outfilter
```

```
Switch_4507R_fl1 (config-ext-nacl)#permit tcp any 192.168.0.0 0.0.255.255 reflect mytest  
timeout 200
```

```
Switch_4507R_fl1 (config-ext-nacl)#permit udp any 192.168.0.0 0.0.255.255 reflect mytest  
timeout 200
```

```
Switch_4507R_fl1 (config-ext-nacl)#permit icmp any 192.168.0.0 0.0.255.255 reflect mytest  
timeout 200
```

```
Switch_4507R_fl1 (config-ext-nacl)#permit ip any any
```

```
Switch_4507R_fl1 (config)#ip access-list extend infilter
```

```
Switch_4507R_fl1 (config-ext-nacl)# evaluate mytest
```

```
Switch_4507R_fl1 (config-ext-nacl)# deny ip any 192.168.1.0 0.0.0.255
```

```
Switch_4507R_fl1 (config-ext-nacl)# permit ip any any
```

```
Switch_4507R_fl1 (config)#interface vlan 10
```

```
Switch_4507R_fl1 (config-if)#ip access-group outfilter in
```

```
Switch_4507R_fl1 (config)#interface vlan 20
```

```
Switch_4507R_fl1 (config-if)#ip access-group infilter in
```

```
Switch_4507R_fl1 (config)#interface vlan 30
```

```
Switch_4507R_fl1 (config-if)# ip access-group infilter in
```

下面我们对上述配置进行解释:

① 新增了一个命名的访问控制列表 (Outfilter) 并应用在需要对外访问的接口下 (财务部所在的 VLAN10) 的 in 方向, 该控制列表中具备 reflect 关键字的条目将被用来建立反向 ACL 条目。

② reflect mytest timeout xxx: 其中的 reflect 关键字表明该条目可用于建立反向的 ACL 条目。mytest 是 reflect 组的名字, 具备相同 reflect 组名字的所有的 ACL 条目为一个 reflect 组。timeout xxx 表明由这条 ACL 条目所建立起来的反向 ACL 条目在没有流量的情况下, 多长时间后会消失, 时间单位为秒。

③ evaluate mytest: 这一句的意思是有符合 mytest 这个 reflect 组中所定义的 ACL 条目的流量发生时, 在 evaluate 语句所在的当前位置动态生成一条反向的 permit 语句。

如需对反身访问控制列表进行深入的了解, 参见 Cisco 相关的文档:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c3.html

4.4.2 案例 2

此案例是配置如图 4-25 所示的中型局域网络。

1. 需求描述

企业内部需要联网的节点数为 400 点，信息点的分布在 1-10 层，网络中心位于 1 层，整个大楼主干采用光纤布线，楼层需要百兆交换到桌面，楼层配线架分别设在 1、4、7 层的配线间。企业网络的主要应用分为两部分：一部分是基础的网络应用它包括内部文件共享、办公自动化（OA）系统、邮件和网站服务等；另一部分是企业的业务应用系统。企业网中大部分的用户数据来自对业务应用系统的访问，同时业务应用系统的可靠性也要求最高。对于整个业务系统，为了保证其整体的稳定可靠，网络结构采用了冗余配置，在这里选用了两台 Catalyst4506，在模块方面，选择两块 WS-X4306-GB 模块用于和各楼层的交换机实现吉比特互连，由于用于业务系统的服务器直接连接在核心交换机上，线路采用的是吉比特铜缆，所以还需选择一块 WS-X4424-GB-RJ45 用于服务器的连接。

表 4-14 列出了本方案所选设备。

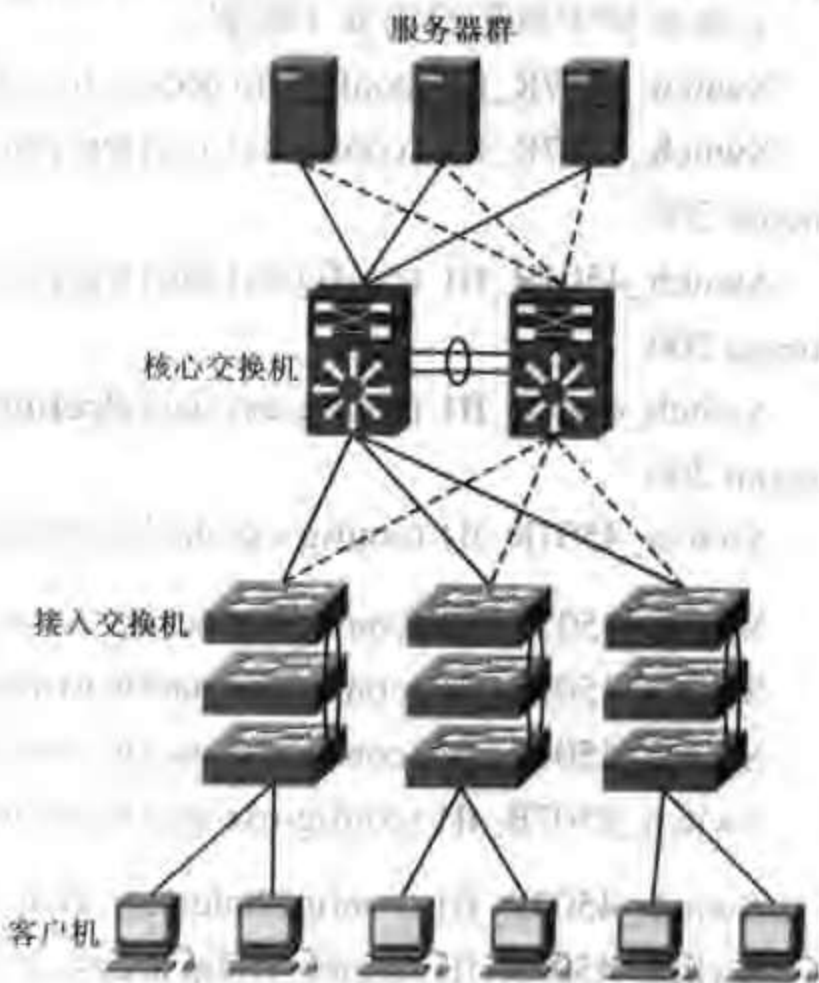


图 4-25 中大型局域网

表 4-14 本方案所选设备列表

产 品	描 述	数 量
核心交换机		
WS-C4507R	Catalyst 4500 Chassis (7 插槽), 风扇, 无 p/s, Red Sup Capable	2
PWR-C45-1000AC	Catalyst 4500 1000W AC 电源 (仅用于数据)	2
CAB-7KACA	AC 电源线	2
WS-X4515	Catalyst 4500 监视器 IV (2 GE), 控制台 (RJ-45)	2
S4KL3-12113EW	Cisco IOS BASIC L3 Cat4500 SUP 3/4 (RIP, St. 路由器, IPX, AT)	2
WS-X4306-GB	Catalyst 4500 吉比特以太网模块, 6 端口 (GBIC)	4
WS-X4424-GB-RJ45	Catalyst 4500 24 端口 10/100/1000 模块 (RJ45)	2
接入交换机		
WS-C2950G-48-EI	带有 2 GBIC 插槽、图像增强功能的 Catalyst 2950, 48 10/100	10
WS-G5484	1000BASE-SX 短波长 GBIC (仅用于多模)	40

需要做的工作:

- (1) 交换机基础性配置;
- (2) 设置 VTP DOMAIN (核心、分支交换机上都设置);
- (3) 配置中继 (核心、分支交换机上都设置);
- (4) 配置链路捆绑 (Ethernet-Channel);
- (5) 创建 VLAN (在 VTP server 上设置);

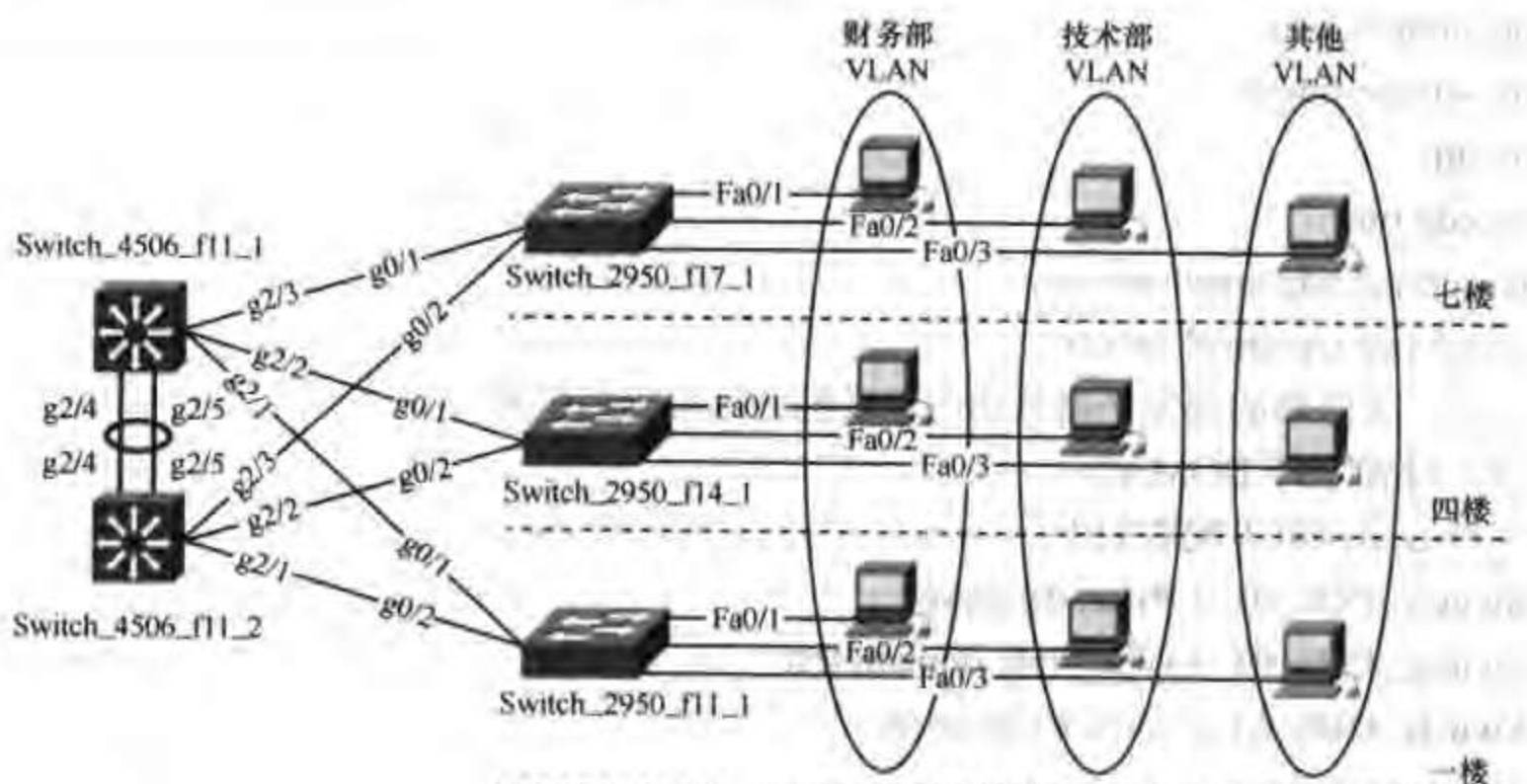


图 4-26 大中型局域网交换机配置

- (6) 设置生成树的根;
- (7) 将交换机端口划入 VLAN;
- (8) 配置三层交换;
- (9) 配置 HSRP;
- (10) 配置 VLAN 访问控制 (VACL)。

2. 配置文档

(1) 交换机基础性配置

在核心交换机和楼层交换机上的基础性配置除主机名和密码外，其他基本相同。本案例中设备的命名规则，沿用案例 1 的方式，即采用“类别_型号_楼层_序号”的原则，比如，“switch_2950_f11_1”表示“一楼的第一台 2950 交换机”，当只有一台时，序号可省略。

交换机的基础性配置如下：

```
hostname Switch_4506_f11_1
enable password cisco
no ip domain-lookup
service timestamps debug uptime
service timestamps debug datetime
service timestamps log uptime
service timestamps log datetime
line con 0
login
line vty 0 4
password cisco
login
no ip http server
```



```
no snmp-server
no service finger
no ntp
no cdp run
no service ndp-small-servers
no service tcp-small-servers
```

注意：带阴影的部分根据具体的交换机进行相应的设置。

(2) 设置 VTP DOMAIN

在核心交换机上配置如下：

```
Switch_4506_fl1_1 #vlan database
Switch_4506_fl1_1 (vlan)#vtp domain test
Switch_4506_fl1_1 (vlan)#vtp server
```

```
Switch_4506_fl1_2 #vlan database
Switch_4506_fl1_2 (vlan)#vtp domain test
Switch_4506_fl1_2 (vlan)#vtp client
```

在楼层交换机上配置如下：

```
Switch_2950_fl1_1#vlan database
Switch_2950_fl1_1 (vlan)#vtp domain test
Switch_2950_fl1_1 (vlan)#vtp client
```

```
Switch_2950_fl4_1#vlan database
Switch_2950_fl4_1 (vlan)#vtp domain test
Switch_2950_fl4_1 (vlan)#vtp client
```

```
Switch_2950_fl7_1#vlan database
Switch_2950_fl7_1 (vlan)#vtp domain test
Switch_2950_fl7_1 (vlan)#vtp client
```

另外，还有一种简单的配置 VTP 的方式，如下：

```
Switch_4506_fl1_1 #conf t
Switch_4506_fl1_1 (config)#vtp domain test
Switch_4506_fl1_1 (config)#vtp mode server
```

```
Switch_4506_fl1_2 #conf t
Switch_4506_fl1_2 (conflg)#vtp domain test
Switch_4506_fl1_2 (config)#vtp mode client
```

```
Switch_2950_fl1_1#conf t
Switch_2950_fl1_1 (config)#vtp domain test
Switch_2950_fl1_1 (config)#vtp mode client
```

```
Switch_2950_fl4_1#conf t
```



```
Switch_2950_fl4_1 (config)#vtp domain test
```

```
Switch_2950_fl4_1 (config)#vtp mode client
```

```
Switch_2950_fl7_1#conf t
```

```
Switch_2950_fl7_1 (config)#vtp domain test
```

```
Switch_2950_fl7_1 (config)#vtp mode client
```

(3) 配置中继

在核心交换机上配置如下：

```
Switch_4506_fl1_1 (config)#interface gigabitEthernet 2/1
```

```
Switch_4506_fl1_1 (config-if)#description link to Switch_2950_fl1_1 g0/1
```

```
Switch_4506_fl1_1 (config-if)#switchport
```

```
Switch_4506_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_4506_fl1_1 (config-if)#switchport mode trunk
```

```
Switch_4506_fl1_1 (config)#interface gigabitEthernet 2/2
```

```
Switch_4506_fl1_1 (config-if)#description link to Switch_2950_fl4_1 g0/1
```

```
Switch_4506_fl1_1 (config-if)#switchport
```

```
Switch_4506_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_4506_fl1_1 (config-if)#switchport mode trunk
```

```
Switch_4506_fl1_1 (config)#interface gigabitEthernet 2/3
```

```
Switch_4506_fl1_1 (config-if)#description link to Switch_2950_fl7_1 g0/1
```

```
Switch_4506_fl1_1 (config-if)#switchport
```

```
Switch_4506_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_4506_fl1_1 (config-if)#switchport mode trunk
```

```
Switchb_4506_fl1_2 (config)#interface gigabitEthernet 2/1
```

```
Switch_4506_fl1_2 (config-if)#description link to Switch_2950_fl1_1 g0/2
```

```
Switch_4506_fl1_2 (config-if)#switchport
```

```
Switch_4506_fl1_2 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_4506_fl1_2 (config-if)#switchport mode trunk
```

```
Switch_4506_fl1_2 (config)#interface gigabitEthernet 2/2
```

```
Switch_4506_fl1_2 (config-if)#description link to Switch_2950_fl4_1 g0/2
```

```
Switchb_4506_fl1_2 (config-if)#switchport
```

```
Switch_4506_fl1_2 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_4506_fl1_2 (config-if)#switchport mode trunk
```

```
Switchb_4506_fl1_2 (config)#interface gigabitEthernet 2/3
```

```
Switch_4506_fl1_2 (config-if)#description link to Switch_2950_fl7_1 g0/2
```

```
Switch_4506_fl1_2 (config-if)#switchport
```

```
Switch_4506_fl1_2 (config-if)#switchport trunk encapsulation dot1q
```



```
Switch_4506_fl1_2 (config-if)#switchport mode trunk
```

在楼层交换机上配置如下:

```
Switch_2950_fl1_1 (config)#interface gigabitEthernet 0/1
```

```
Switch_2950_fl1_1 (config-if)#description link to Switch_4506_fl1_1 g2/1
```

```
Switch_2950_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_2950_fl1_1 (config-if)#switchport mode trunk
```

```
Switch_2950_fl1_1 (config)#interface gigabitEthernet 0/2
```

```
Switch_2950_fl1_1 (config-if)#description link to Switch_4506_fl1_2 g2/1
```

```
Switch_2950_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_2950_fl1_1 (config-if)#switchport mode trunk
```

```
Switch_2950_fl4_1 (config)#interface gigabitEthernet 0/1
```

```
Switch_2950_fl4_1 (config-if)#description link to Switch_4506_fl1_1 g2/1
```

```
Switch_2950_fl4_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_2950_fl4_1 (config-if)#switchport mode trunk
```

```
Switch_2950_fl4_1 (config)#interface gigabitEthernet 0/2
```

```
Switch_2950_fl4_1 (config-if)#description link to Switch_4506_fl1_2 g2/1
```

```
Switch_2950_fl4_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_2950_fl4_1 (config-if)#switchport mode trunk
```

```
Switch_2950_fl7_1 (config)#interface gigabitEthernet 0/1
```

```
Switch_2950_fl7_1 (config-if)#description link to Switch_4506_fl1_1 g2/1
```

```
Switch_2950_fl7_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_2950_fl7_1 (config-if)#switchport mode trunk
```

```
Switch_2950_fl7_1 (config)#interface gigabitEthernet 0/2
```

```
Switch_2950_fl7_1 (config-if)#description link to Switch_4506_fl1_2 g2/1
```

```
Switch_2950_fl7_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_2950_fl7_1 (config-if)#switchport mode trunk
```

(4) 配置链路捆绑 (以太网通道)

在两台核心设备之间配置多链路捆绑, 能形成更大的数据传输的通道, 有利于数据的快速转发, 同时也能实现链路的冗余。在本案例中我们将两台核心交换机的两个千兆端口捆绑成一条 4Gbps (全双工) 的逻辑通道。

```
Switch_4506_fl1_1 (config)#interface gigabitEthernet 2/4
```

```
Switch_4506_fl1_1 (config-if)#description link to Switch_4506_fl1_2 g2/4
```

```
Switch_4506_fl1_1 (config-if)#switchport
```

```
Switch_4506_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Switch_4506_fl1_1 (config-if)#switchport mode trunk
```

```
Switch_4506_fl1_1 (config-if)#channel-group 1 mode desirable
```

```
Switch_4506_fl1_1 (config)#interface gigabitEthernet 2/5
```

```
Switch_4506_fl1_1 (config-if)#description link to Switch_4506_fl1_2 g2/5
```



```

Switch_4506_fl1_1 (config-if)#switchport
Switch_4506_fl1_1 (config-if)#switchport trunk encapsulation dot1q
Switch_4506_fl1_1 (config-if)#switchport mode trunk
Switch_4506_fl1_1 (config-if)#channel-group 1 mode desirable
Switch_4506_fl1_1 (config)#interface port-channel 1
Switch_4506_fl1_1 (config-if)#switchport
Switch_4506_fl1_1 (config-if)#switchport trunk encapsulation dot1q
Switch_4506_fl1_1 (config-if)#switchport mode trunk
Switch_4506_fl1_2 (config)#interface gigabitEthernet 2/4
Switch_4506_fl1_2 (config-if)#description link to Switch_4506_fl1_1 g2/4
Switch_4506_fl1_2 (config-if)#switchport
Switch_4506_fl1_2 (config-if)#switchport trunk encapsulation dot1q
Switch_4506_fl1_2 (config-if)#switchport mode trunk
Switch_4506_fl1_2 (config-if)#channel-group 1 mode desirable
Switch_4506_fl1_2 (config)#interface gigabitEthernet 2/5
Switch_4506_fl1_2 (config-if)#description link to Switch_4506_fl1_1 g2/5
Switch_4506_fl1_2 (config-if)#switchport
Switch_4506_fl1_2 (config-if)#switchport trunk encapsulation dot1q
Switch_4506_fl1_2 (config-if)#switchport mode trunk
Switch_4506_fl1_2 (config-if)#channel-group 1 mode desirable
Switch_4506_fl1_2 (config)#interface port-channel 1
Switch_4506_fl1_2 (config-if)#switchport
Switch_4506_fl1_2 (config-if)#switchport trunk encapsulation dot1q
Switch_4506_fl1_2 (config-if)#switchport mode trunk

```

(5) 创建 VLAN

其实，我们只需要在管理域中的任何一台 VTP 属性为 Server 的交换机上建立 VLAN，它就会通过 VTP 通告整个管理域中的所有交换机。本案例中，“test”域中的 VTP Server 是 Switch_4506_fl1_1，因此我们只需在它上进行 VLAN 的配置即可。

```

Switch_4506_fl1_1 #vlan database
Switch_4506_fl1_1 (vlan)#Vlan 10 name finance
Switch_4506_fl1_1 (vlan)#Vlan 20 name techniqy
Switch_4506_fl1_1 (vlan)#Vlan 30 name other

```

另外，还有一种简单的创建 VLAN 的方式，如下：

```

Switch_4507R_fl1 #conf t
Switch_4507R_fl1 (config)#vlan 10,20,30

```

(6) 设置生成树的根

我们这里将 VLAN10、20、30 的生成树的首根 (primary root) 都设到 Switch_4506_fl1_1 上，将次根 (secondary root) 设到 Switch_4506_fl1_2 上，这样保证在主交换机

(Switch_4506_fl1_1) 宕机的情况下, 辅交换机 (Switch_4506_fl1_2) 可以快速正常的接管工作。

说明: 其实我们可以不用手工设置生成树的根, 所有交换机会通过生成树算法来计算各 VLAN 的根, 但这样的结果可能会导致某个接入层交换机被选为了生成树的根, 这样大量的负载就可能会由此接入交换机来承担, 而性能更高的核心交换机就不能充分体现其价值。因此, 我们通常的做法是, 手工将各 VLAN 生成树的根指定为性能更高的核心设备, 如下:

```
Switch_4506_fl1_1 (config)# spanning-tree vlan 10 root primary
Switch_4506_fl1_1 (config)# spanning-tree vlan 20 root primary
Switch_4506_fl1_1 (config)# spanning-tree vlan 30 root primary

Switch_4506_fl1_2 (config)# spanning-tree vlan 10 root secondary
Switch_4506_fl1_2 (config)# spanning-tree vlan 20 root secondary
Switch_4506_fl1_2 (config)# spanning-tree vlan 30 root secondary
```

经过以上的配置后, VLAN10、20、30 的生成树的首根就被设为了 Switch_4506_fl1_1, 次根被设为了 Switch_4506_fl1_2, 如果 Switch_4506_fl1_1 宕机, Switch_4506_fl1_2 将接替它, 成为 VLAN10、20、30 的生成树的首根。

(7) 将交换机端口划入 VLAN

这里我们假设要将 Switch_2950_fl1_1、Switch_2950_fl4_1、Switch_2950_fl7_1 接入交换机的端口 fa0/1 划入 finance VLAN (财务部 VLAN), 端口 fa0/2 划入 techniqy VLAN (技术部 VLAN), 端口 fa0/3 划入 other VLAN (其他部门 VLAN)。配置如下:

```
Switch_2950_fl1_1 (config)#interface fastethernet 0/1
Switch_2950_fl1_1 (config-if)#switchport mode access
Switch_2950_fl1_1 (config-if)#switchport access vlan 10
Switch_2950_fl1_1 (config)#interface fastethernet 0/2
Switch_2950_fl1_1 (config-if)#switchport mode access
Switch_2950_fl1_1 (config-if)#switchport access vlan 20
Switch_2950_fl1_1 (config)#interface fastethernet 0/3
Switch_2950_fl1_1 (config-if)#switchport mode access
Switch_2950_fl1_1 (config-if)#switchport access vlan 30

Switch_2950_fl4_1 (config)#interface fastethernet 0/1
Switch_2950_fl4_1 (config-if)#switchport mode access
Switch_2950_fl4_1 (config-if)#switchport access vlan 10
Switch_2950_fl4_1 (config)#interface fastethernet 0/2
Switch_2950_fl4_1 (config-if)#switchport mode access
Switch_2950_fl4_1 (config-if)#switchport access vlan 20
Switch_2950_fl4_1 (config)#interface fastethernet 0/3
Switch_2950_fl4_1 (config-if)#switchport mode access
Switch_2950_fl4_1 (config-if)#switchport access vlan 30

Switch_2950_fl7_1 (config)#interface fastethernet 0/1
```



```

Switch_2950_f17_1 (config-if)#switchport mode access
Switch_2950_f17_1 (config-if)#switchport access vlan 10
Switch_2950_f17_1 (config)#interface fastethernet 0/2
Switch_2950_f17_1 (config-if)#switchport mode access
Switch_2950_f17_1 (config-if)#switchport access vlan 20
Switch_2950_f17_1 (config)#interface fastethernet 0/3
Switch_2950_f17_1 (config-if)#switchport mode access
Switch_2950_f17_1 (config-if)#switchport access vlan 30

```

(8) 配置三层交换

到目前为止，各部门已经划入不同的 VLAN。但是，此时只有本 VLAN 的主机之间可以互相访问，不同 VLAN 的主机之间是不能互访的。为了让不同 VLAN 之间可以互访，我们需要为不同的 VLAN 之间架起一座桥梁，这时就要在三层核心设备上给各 VLAN 接口分配网络（IP）地址了。由于两台核心设备互为备份，也就是都可能会成为各 VLAN 之间互访的桥梁，因此我们需要在两台核心交换机上分别为所有的 VLAN 各配置一个接口地址，这个地址也就是各 VLAN 主机的网关地址。

下面的表 4-15 和 4-16 给出 VLAN 和 IP 地址的分配表。

表 4-15 基于核心交换机 1 (Switch_4506_f11_1) 的 VLAN 和 IP 地址的分配表

部 门	VLAN 名	VLAN ID	网关地址	网段地址
财务部	finance	10	192.168.1.254	192.168.1.0/24
技术部	techniqy	20	192.168.2.254	192.168.2.0/24
其他部门	other	30	192.168.3.254	192.168.3.0/24

表 4-16 基于核心交换机 2 (Switch_4506_f11_2) 的 VLAN 和 IP 地址的分配表

部 门	VLAN 名	VLAN ID	网关地址	网段地址
财务部	finance	10	192.168.1.253	192.168.1.0/24
技术部	techniqy	20	192.168.2.253	192.168.2.0/24
其他部门	other	30	192.168.3.253	192.168.3.0/24

```

Switch_4506_f11_1 (config)#interface vlan 10
Switch_4506_f11_1 (config-if)#ip address 192.168.1.254 255.255.255.0

Switch_4506_f11_1 (config)#interface vlan 20
Switch_4506_f11_1 (config-if)#ip address 192.168.2.254 255.255.255.0

Switch_4506_f11_1 (config)#interface vlan 30
Switch_4506_f11_1 (config-if)#ip address 192.168.3.254 255.255.255.0

Switch_4506_f11_2 (config)#interface vlan 10
Switch_4506_f11_2 (config-if)#ip address 192.168.1.253 255.255.255.0

Switch_4506_f11_2 (config)#interface vlan 20
Switch_4506_f11_2 (config-if)#ip address 192.168.2.253 255.255.255.0

```



```
Switch_4506_fl1_2 (config)#interface vlan 30
```

```
Switch_4506_fl1_2 (config-if)#ip address 192.168.3.253 255.255.255.0
```

然后在各接入 VLAN 的计算机上设置与所属 VLAN 的网络地址一致的 IP 地址，并且把默认网关设置为该 VLAN 的接口地址。这样，所有的 VLAN 也可以互访了。

问题：现在两台核心交换机上都配有 VLAN 的接口 IP 地址，那么 VLAN 中的主机到底应该将网关设为哪个 IP 地址呢？

答：根据前面我们的配置可知 Switch_4506_fl1_1 是各 vlan 生成树的首根，因此我们应选 Switch_4506_fl1_1 上配的地址为自己的网关，如果 Switch_4506_fl1_1 发生了故障，这时 Switch_4506_fl1_2 接替了 Switch_4506_fl1_1 的位置，这时为了正常通信，用户须将网关改为 Switch_4506_fl1_2 上配的 IP 地址。因为这样的改动影响面太大，所以这里就引出了下面我们要讲的一个内容——HSRP，通过 HSRP 的配置后，客户机就不用来回改动自己的网关了。

(9) 配置 HSRP

通俗地讲，HSRP 就是将两台配置为热备份的三层设备（路由器、带三层功能的交换机、防火墙等）虚拟成一台设备，这样使得在设备进行切换的时候网络的整体结构和配置保持稳定。

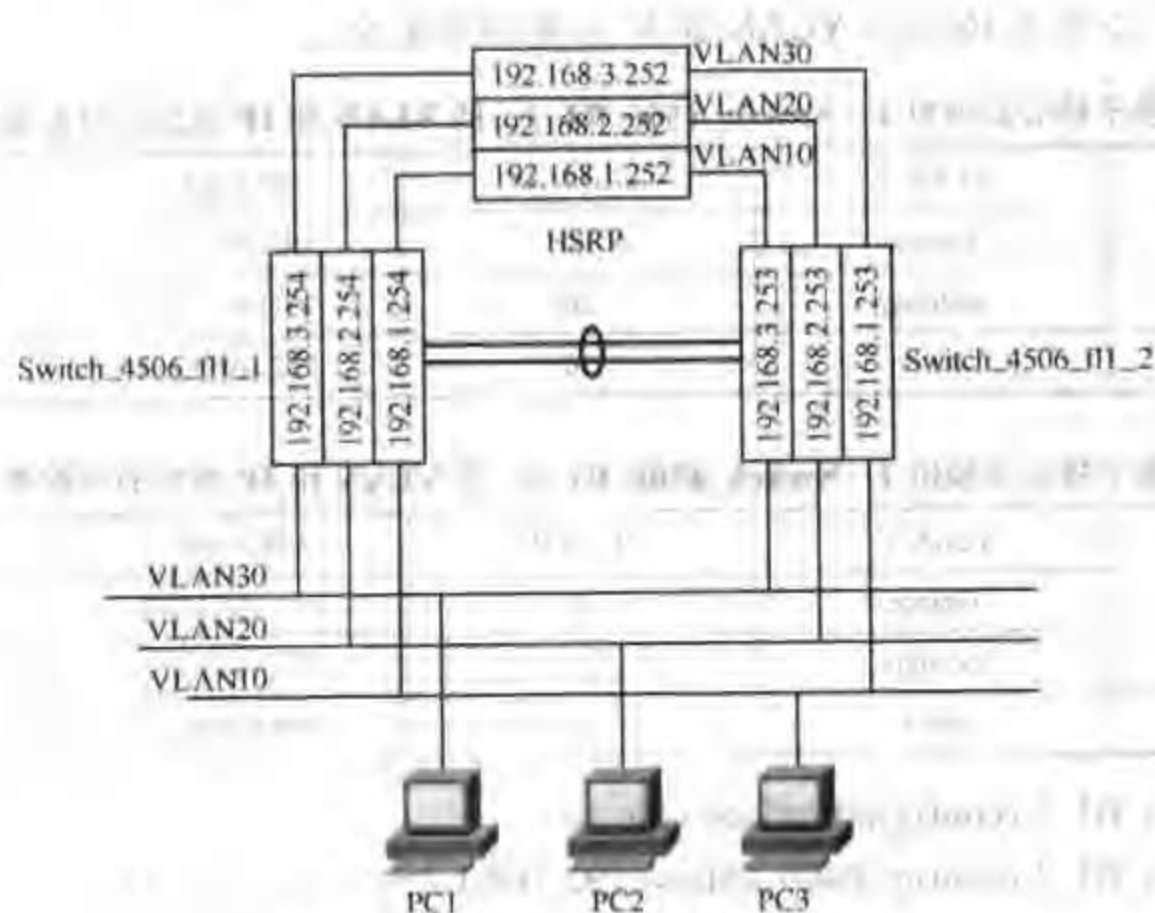


图 4-27 本案例中为各 VLAN 分配的虚拟地址

在本案例中，我们为各 VLAN 分配的虚拟地址如图 4-27 所示，VLAN10 为 192.168.1.252，VLAN20 为 192.168.2.252，VLAN30 为 192.168.3.252。具体配置如下：

```
Switch_4506_fl1_1 (config)#interface vlan 10
```

```
Switch_4506_fl1_1 (config-if)#ip address 192.168.1.254 255.255.255.0
```

```
Switch_4506_fl1_1 (config-if)#standby 1 ip 192.168.1.252
```

```
Switch_4506_fl1_1 (config-if)#standby 1 priority 150
```

```
Switch_4506_fl1_1 (config)#interface vlan 20
```



```
Switch_4506_fl1_1 (config-if)#ip address 192.168.2.254 255.255.255.0
```

```
Switch_4506_fl1_1 (config-if)#standby 2 ip 192.168.2.252
```

```
Switch_4506_fl1_1 (config-if)#standby 2 priority 150
```

```
Switch_4506_fl1_1 (config)#interface vlan 30
```

```
Switch_4506_fl1_1 (config-if)#ip address 192.168.3.254 255.255.255.0
```

```
Switch_4506_fl1_1 (config-if)#standby 3 ip 192.168.3.252
```

```
Switch_4506_fl1_1 (config-if)#standby 3 priority 150
```

```
Switch_4506_fl1_2 (config)#interface vlan 10
```

```
Switch_4506_fl1_2 (config-if)#ip address 192.168.1.253 255.255.255.0
```

```
Switch_4506_fl1_2 (config-if)#standby 1 ip 192.168.1.252
```

```
Switch_4506_fl1_2 (config-if)#standby 1 priority 110
```

```
Switch_4506_fl1_2 (config)#interface vlan 20
```

```
Switch_4506_fl1_2 (config-if)#ip address 192.168.2.253 255.255.255.0
```

```
Switch_4506_fl1_2 (config-if)#standby 2 ip 192.168.2.252
```

```
Switch_4506_fl1_2 (config-if)#standby 2 priority 110
```

```
Switch_4506_fl1_2 (config)#interface vlan 30
```

```
Switch_4506_fl1_2 (config-if)#ip address 192.168.3.253 255.255.255.0
```

```
Switch_4506_fl1_2 (config-if)#standby 3 ip 192.168.3.252
```

```
Switch_4506_fl1_2 (config-if)#standby 3 priority 110
```

(10) 配置 VLAN 访问控制 (VACL)

根据用户的需求知道, 财务部的主机不能被其它部门的用户访问到, 而财务部的主机又需要访问外部。根据案例 1 我们知道, 最好采用反身访问控制列表, 由于本案例采用双核心交换机设计, 因此需要在两台核心设备上均采用相应的设置。具体配置如下:

```
Switch_4506_fl1_1 (config)#ip access-list extend outfilter
```

```
Switch_4506_fl1_1 (config-ext-nacl)#permit tcp any 192.168.0.0 0.0.255.255 reflect mytest  
timeout 200
```

```
Switch_4506_fl1_1 (config-ext-nacl)#permit udp any 192.168.0.0 0.0.255.255 reflect mytest  
timeout 200
```

```
Switch_4506_fl1_1 (config-ext-nacl)#permit icmp any 192.168.0.0 0.0.255.255 reflect mytest  
timeout 200
```

```
Switch_4506_fl1_1 (config-ext-nacl)#permit ip any any
```

```
Switch_4506_fl1_1 (config)#ip access-list extend infilter
```

```
Switch_4506_fl1_1 (config-ext-nacl)# evaluate mytest
```

```
Switch_4506_fl1_1 (config-ext-nacl)# deny ip any 192.168.1.0 0.0.0.255
```

```
Switch_4506_fl1_1 (config-ext-nacl)# permit ip any any
```

```
Switch_4506_fl1_1 (config)#interface vlan 10
```



```
Switch_4506_fl1_1 (config-if)#ip access-group outfilter in
Switch_4506_fl1_1 (config)#interface vlan 20
Switch_4506_fl1_1 (config-if)#ip access-group infilter in
Switch_4506_fl1_1 (config)#interface vlan 30
Switch_4506_fl1_1 (config-if)# ip access-group infilter in

Switch_4506_fl1_2 (config)#ip access-list exteud outfilter
Switch_4506_fl1_2 (config-ext-nacl)#permit tcp any 192.168.0.0 0.0.255.255 reflect mytest
timeout 200
Switch_4506_fl1_2 (config-ext-nacl)#permit udp any 192.168.0.0 0.0.255.255 reflect mytest
timeout 200
Switch_4506_fl1_2 (config-ext-nacl)#permit icmp any 192.168.0.0 0.0.255.255 reflect mytest
timeout 200
Switch_4506_fl1_2 (config-ext-nacl)#permit ip any any

Switch_4506_fl1_2 (config)#ip access-list extend infilter
Switch_4506_fl1_2 (config-ext-nacl)# evaluate mytest
Switch_4506_fl1_2 (config-ext-nacl)# deny ip any 192.168.1.0 0.0.0.255
Switch_4506_fl1_2 (config-ext-nacl)# permit ip any any

Switch_4506_fl1_2 (config)#interface vlan 10
Switch_4506_fl1_2 (config-if)#ip access-group outfilter in
Switch_4506_fl1_2 (config)#interface vlan 20
Switch_4506_fl1_2 (config-if)#ip access-group infilter in
Switch_4506_fl1_2 (config)#interface vlan 30
Switch_4506_fl1_2 (config-if)# ip access-gronp infilter in
```

4.5 小 结

在本章的开始我们对交换机的概念、原理及交换机的硬件结构作了简要的介绍，接下来我们对交换机的配置方式以及一些常用的配置命令进行了介绍，最后我们通过几个具体的案例，详细讲解了如何快速地配置一个企业的局域网络。

第5章 Cisco 路由器配置

本章将涵盖下列有关 Cisco 路由器配置方面的关键主题

- Cisco 路由器基础
- 广域网互联设置
- 路由协议设置
- 访问控制及地址转换
- Cisco 路由器经典配置案例

目标:

通过本章的学习, 希望读者对以下一些方面的内容有所了解:

- (1) 什么是路由器;
- (2) 路由器的工作原理是什么;
- (3) 路由器的硬件结构;
- (4) 路由器的基本配置命令;
- (5) 我国常用广域链路及配置方法;
- (6) 常用路由协议及其配置方法;
- (7) 如何快速构建企业的广域网络。

5.1 简介

路由器是企业网中用于广域互连以及 Internet 接入的主要设备。当今, 可能再小的企业都会有一台路由器用于 Internet 的接入 (俗称上网), 路由器也是小型企业网络里调试难度最大的设备。因为小企业里信息点较少, 交换机通常不用调试或只需简单地划分一下 VLAN 即可工作, 而路由器往往需要更多配置。由于路由器的调试通常会和各种电信线路打交道, 这就需要调试人员除了对网络知识要有更多的了解之外, 还需要对电信部门提供的各种线路有所了解。本章将对我国电信部门常用的一些线路进行介绍, 同时结合 Cisco 的路由器进行配置的讲解。

5.2 Cisco 路由器基础

1. 什么是路由器?

路由器是一种连接多个网络或网段的网络设备, 它能对不同网络或网段之间的数据信息

进行“翻译”，以使它们能够相互“读”懂对方的数据，从而构成一个更大的网络。

路由器主要完成两项工作，即“寻径”和“转发”。“寻径”是指建立和维护路由表的过程，主要由软件实现；“转发”是指把数据分组从一个接口转到另一接口的过程，主要由硬件完成。

2. 路由器的工作原理

路由器工作在 OSI 模型中的下三层，其最高层为网络层，路由器利用网络层定义的“逻辑”上的网络地址（即 IP 地址）来区别不同的网络，实现网络的互连和隔离，保持各个网络的独立性。路由器不转发广播消息，而把广播消息限制在各自的网络内部。发送到其他网络的数据先被送到路由器，再由路由器转发出去。路由器通过统一的第三层来屏蔽底两层的不同，从而实现多个独立的异种网互联，并通过路由表实现寻径；由于路由器是一个存储/转发设备，因此它可以实现分组的过滤、优先、排队等流量管理。路由器的工作原理如图 5-1 所示。

寻径的依据是经过每个路由器中的路由表。路由表指明了从源站点到目的站点的一条路径。路由协议是生成路由表的方法，分为静态路由协议和动态路由协议。

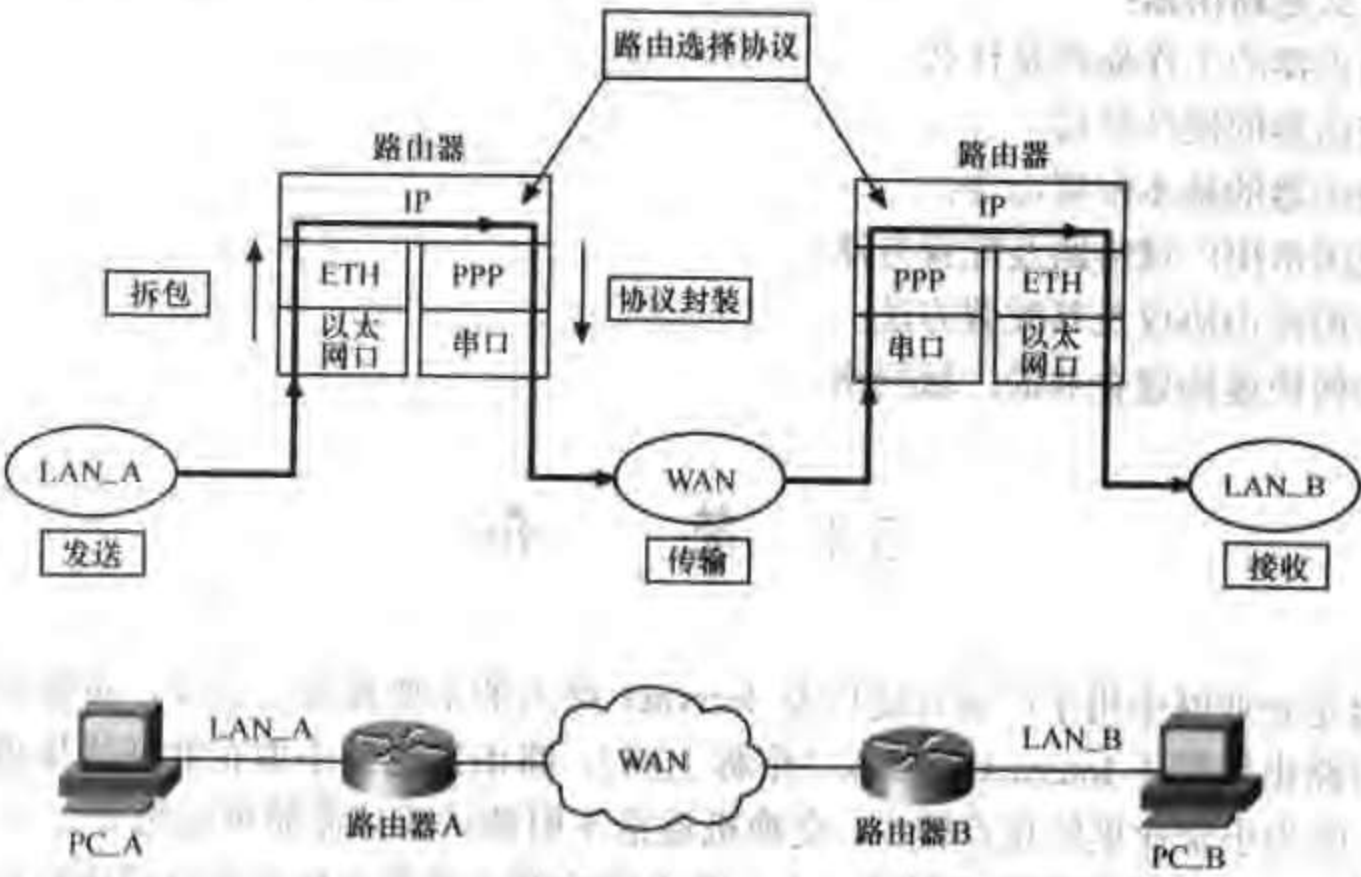


图 5-1 路由工作原理

5.2.1 Cisco 路由器基本构成

我们可以认为路由器就是一台特殊功能的计算机，它的主要功能就是用来进行路由计算和数据包的转发，而不是传统的文字和图像处理。既然是计算机，它就应该和我们熟知的传统的 PC（个人电脑）有类似的体系结构，同时，它也应该有相应的操作系统（IOS）。下面我们就来认识一下 Cisco 的路由器。

总体来说 Cisco 的路由器是由 CPU、RAM、NVRAM、FLASH、ROM 和一些相应的接口通过内部总线相连而构成，如图 5-2 所示。下面分别对它们进行介绍。

CPU:

相当于 PC 的 CPU（中央处理器）。是路由器的大脑，负责整个系统的计算和控制。

ROM:

相当于 PC 的 BIOS（基本输入输出系统）。存放引导程序和 IOS 的一个最小子集。它是只读存储器，系统掉电，程序不会丢失。

Flash:

相当于 PC 的硬盘。包含路由器的操作系统（IOS）和其它微代码。它是一种可擦写、可编程的存储器，系统掉电，程序不会丢失。

NVRAM（No-Volatile RAM）:

相当于 PC 的第二块硬盘。专门存放路由器的配置文件。系统掉电，程序不会丢失。

RAM/DRAM（Random Access Memory / Dynamic Random Access Memory）:

相当于 PC 的内存。它是路由器主要的存储部件。RAM 也叫做工作存储器，包含动态的配置信息（如路由表）。系统掉电，其内容会丢失。

Interfaces:

相当于 PC 的网卡。接口指的是数据包进出路由器的网络连接。路由器支持的接口类型包括 Ethernet、Token Ring、Serial、BRI、ATM、FDDI 等。

Auxiliary Ports:

相当于 PC 的串口（异步），通过在此接口接一个 MODEM（调制解调器），我们可以进行拨号连接。Cisco IOS 软件允许将 Auxiliary Port 作为异步连接的网络接口使用。

就和 PC 开机需要进行系统各部分的自检然后加载操作系统一样，路由器也要经历一个类似的启动过程：首先对系统各部分的硬件进行检测，然后检查启动配置文件（配置了操作系统从哪里引导），根据配置文件指定的引导路径去寻找操作系统，最后从 NVRAM 中将配置文件加载到 RAM。如果没有进行配置，就进入系统的初始配置状态（Setup 状态）路由器的启动过程如图 5-3 所示。

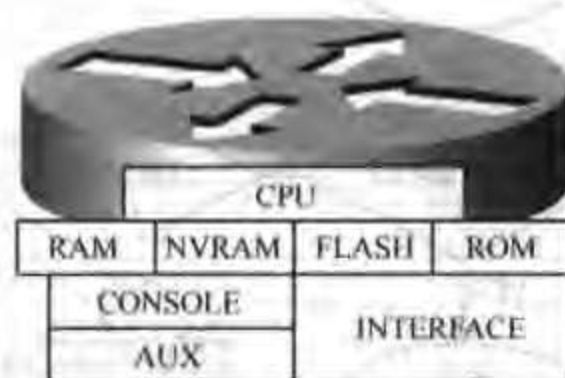


图 5-2 Cisco 路由器结构



图 5-3 路由器启动流程

以上是大多数路由器启动的一个大致流程，Cisco 路由器的启动也大致相仿：首先运行 ROM 的程序，进行系统自检和引导，然后读 Flash 内的 IOS，装入 DRAM 中，并从 NVRAM 中读入路由器的配置，计算并生成路由表，如图 5-4 所示。

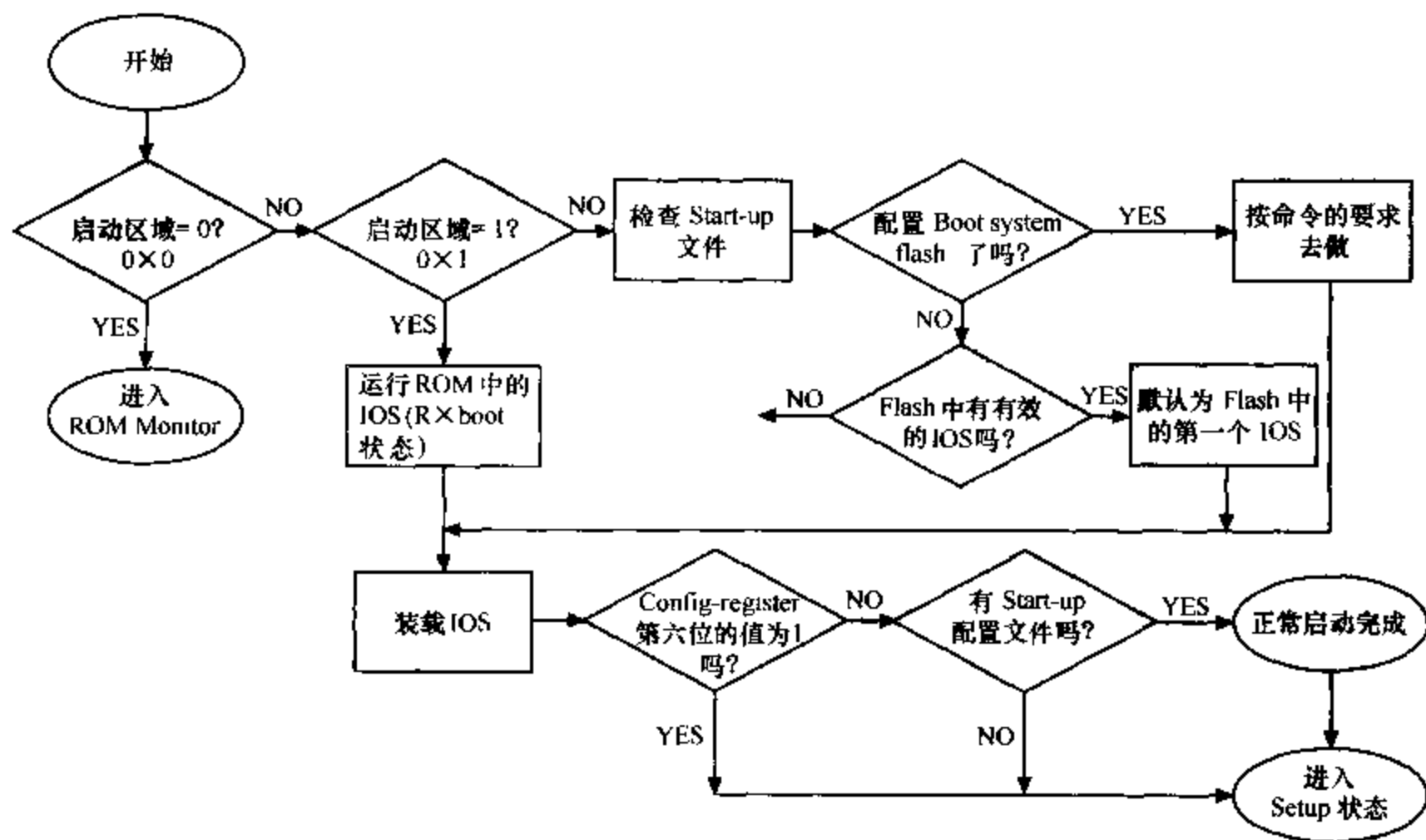


图 5-4 Cisco 路由器详细启动流程

5.2.2 基本设置方式

一般来说，可以用下面 5 种方式来设置路由器。

- CON: Console 口接终端或运行终端仿真软件（如超级终端）的微机；
- AUX: Auxiliary 口接 MODEM，通过电话线与远方的终端或运行终端仿真软件的微机相连，注意 AUX 口可作为 Console 端口的备份，配置方法是在全局配置模式下输入“line aux 0”进入 AUX 端口模式，然后输入“no modem inout”；
- Telnet: 经过配置可以通过 telnet 配置路由器；
- TFTP: 可以通过 TFTP 服务器下载配置信息。要想实现此方式，需要在一台计算机上安装 TFTP Server 程序，此计算机需要和路由器能通过 tftp 协议通信。注意，这种方式还可用于软件的备份和升级；
- SNMP: 可以通过一个运行网管软件（如 CiscoWorks）的工作站来管理路由器的配置；路由器的配置方式如图 5-5 所示。

注意：在以上的 5 种方式中，通过 Console 口和使用 Telnet 这两种方式是最常用的。

当我们拿到一台新的路由器后，第一次必须通过 Console 端口进行设置，当通过 Console 端口对路由器进行了相应的配置后，我们才可以通过其他的几种方式对路由器进行配置和管理。下面我们首先介绍一下如何通过 Console 口对路由器进行配置。

(1) 新路路由器的包装里自带一条 Console 线，用这条 Console 线将 PC 的 COM 端口和路由器的 Console 口连接起来，如图 5-6 所示。

(2) 在 PC 的桌面上单击“开始”-“程序”-“附件”-“通讯”-“超级终端”，如图 5-7 所示。

(3) 在弹出的对话框中输入此次连接的名称（可以随便命名），这里我们取名为“myrouter”，然后，单击“确定”，如图 5-8 所示。



图 5-8 输入连接名称并单击“确定”

(4) 在弹出的对话框中的“连接时使用”一栏，我们选择 Console 线连接的 COM 端口，如果不知，可依次尝试。这里我们选择“COM1”，然后单击“确定”，如图 5-9 所示。



图 5-9 选择 Console 线连接的 COM 端口

(5) 在弹出的对话框中，需要我们对 COM 端口进行设置，现在进行如下的设置：

每秒位数 (波特率): 9600

数据位: 8

奇偶校验: 无

停止位: 1

数据流控制: 无

我们可以简单地单击“还原为默认值”按钮, 来对以上这些参数进行设置。设置完这些参数后, 单击“确定”, 如图 5-10 所示。

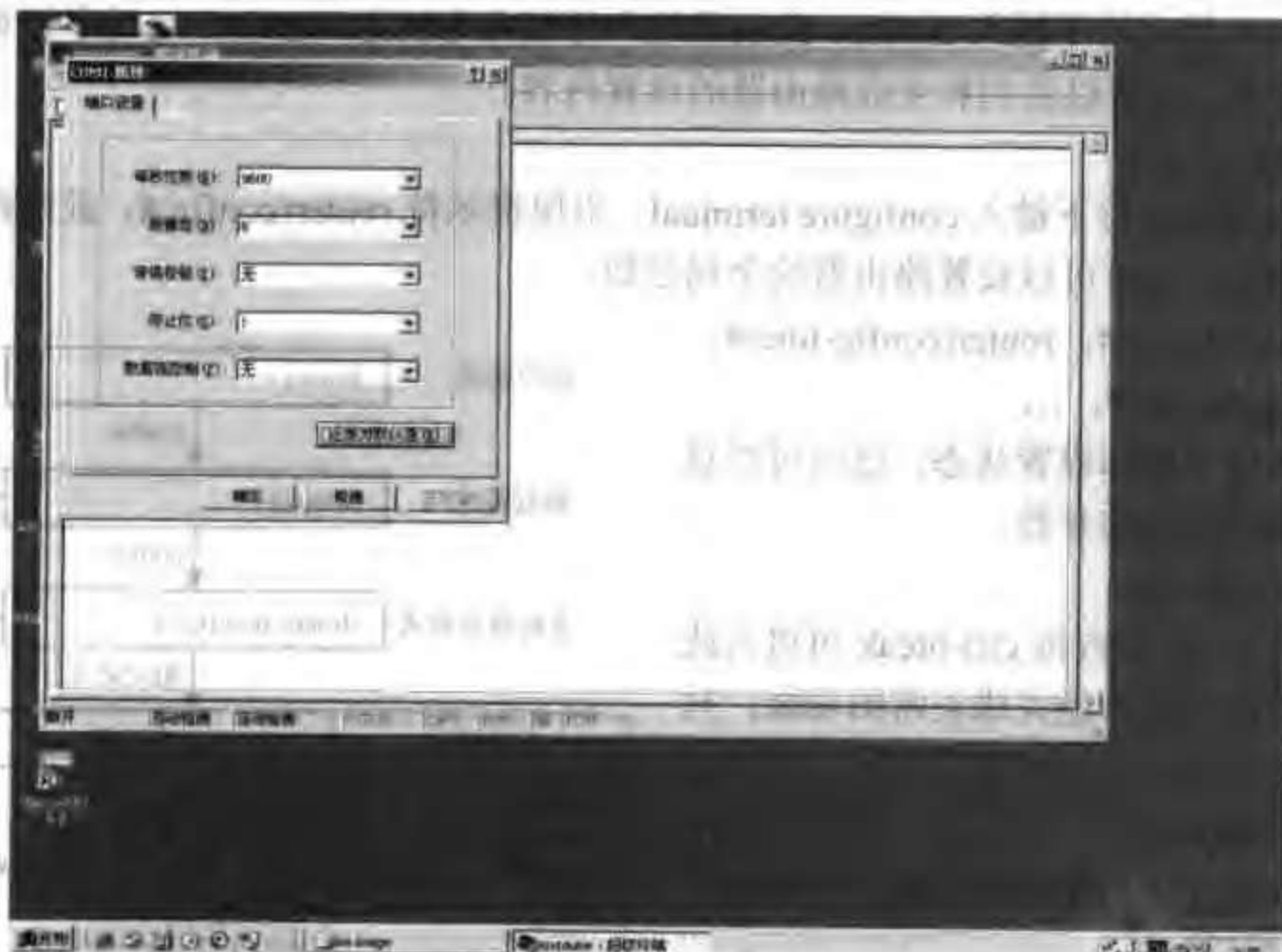


图 5-10 对 COM 端口进行设置

(6) 经过以上的设置, 就可以和路由器正常通信了。如果路由器正常启动, 直接回车, 我们就可以看到如图 5-11 所示的画面。

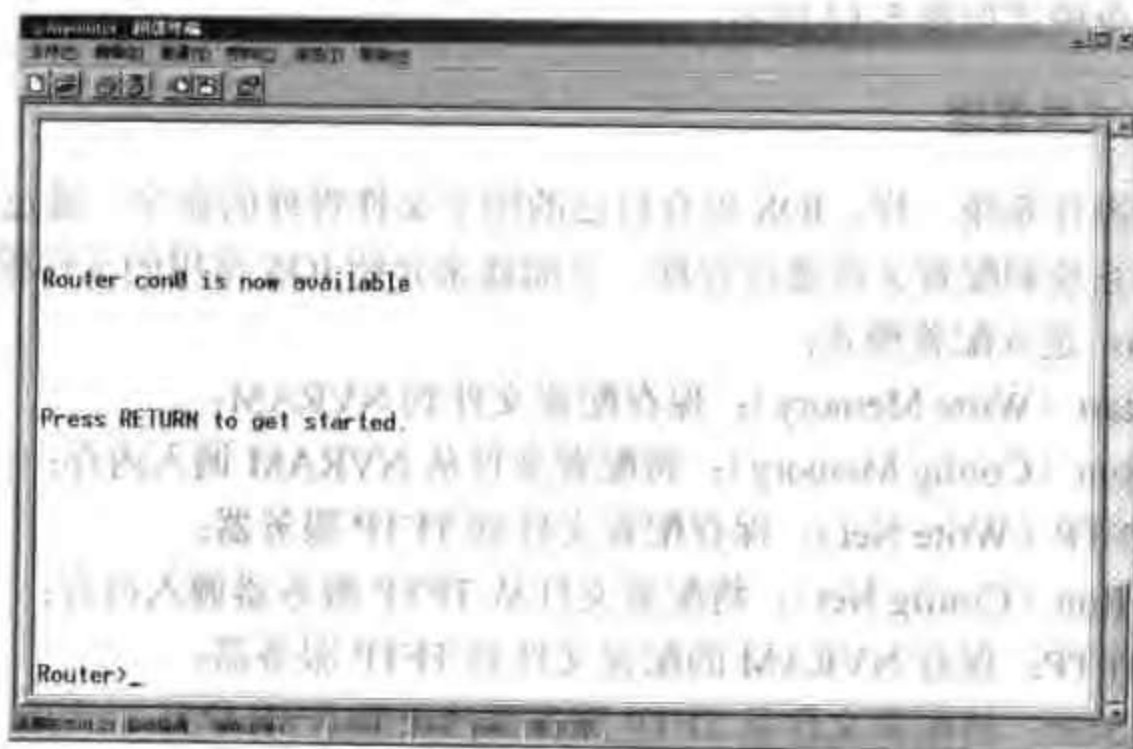


图 5-11 路由器启动的显示画面

5.2.3 IOS 命令状态

IOS 命令状态如下：

router >

路由器处于用户命令状态，这时用户可以看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。

router #

在 router>提示符下键入 enable，路由器进入特权命令状态 router#，这时不但可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

router (config) #

在 router#提示符下键入 configure terminal，出现提示符 router(config)#，此时路由器处于全局设置状态，这时可以设置路由器的全局参数。

router(config-if)#, router(config-line)#,

router(config-router)#, ...

路由器处于局部设置状态，这时可以设置路由器某个局部的参数。

> 或 rommon>

在开机后 60 秒内按 ctrl-break 可进入此状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。

router (boot)>

路由器处于 RXBOOT 状态。

设置对话状态

这是一台新路由器开机时自动进入的状态，在特权命令状态使用 setup 命令也可进入此状态，这时可通过对话方式对路由器进行设置。

路由器的命令模式如图 5-12 所示。

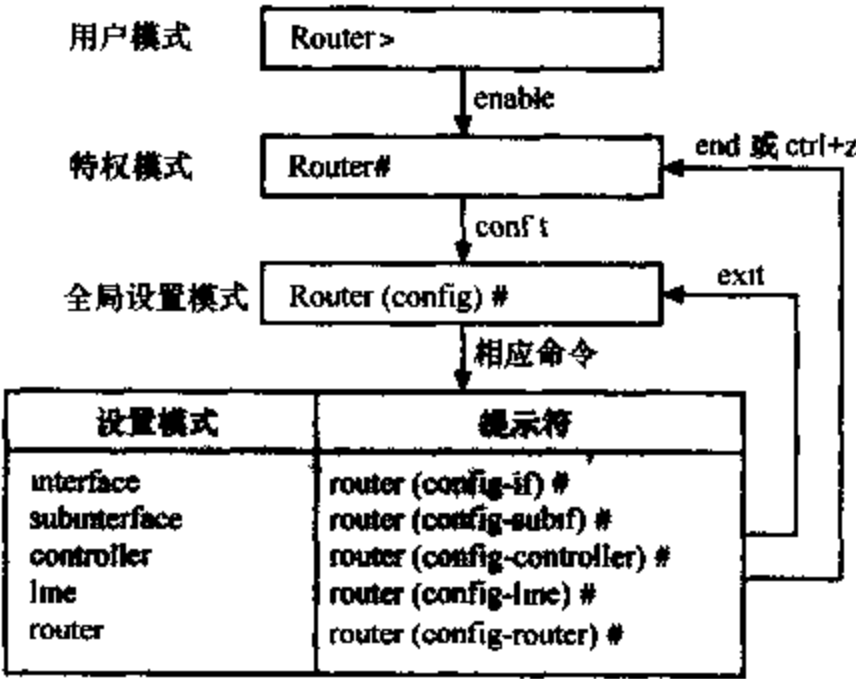


图 5-12 路由器命令模式

5.2.4 IOS 文件管理

像任何一种操作系统一样，IOS 也有自己的用于文件管理的命令。通过这些命令 IOS 可以方便地对操作系统和配置文件进行管理。下面就来介绍 IOS 常用的文件管理命令。

Config Term: 进入配置模式;

Copy Run Start (Write Memory): 保存配置文件到 NVRAM;

Copy Start Ruu (Config Memory): 将配置文件从 NVRAM 调入内存;

Copy Run TFTP (Write Net): 保存配置文件到 TFTP 服务器;

Copy TFTP Run (Config Net): 将配置文件从 TFTP 服务器调入内存;

Copy Start TFTP: 保存 NVRAM 的配置文件到 TFTP 服务器;

Copy TFTP Start: 将配置文件从 TFTP 服务器拷贝到 NVRAM;

Copy TFTP Flash: 将配置文件或操作系统软件 (IOS) 从 TFTP 服务器拷贝到 Flash 中;

Copy Flash TFTP: 将配置文件或操作系统软件（IOS）从 Flash 拷贝到 TFTP 服务器中；
Erase Start (Write Erase): 删除配置

文件。

IOS 的文件管理如图 5-13 所示。

5.2.5 IOS 常用命令

IOS 常用的命令如下：

(1) 帮助

在 IOS 操作中，无论任何状态和位置，都可以键入“？”得到系统的帮助。

(2) 改变命令状态

要改变命令状态，可用表 5-1 中所列的各条命令。

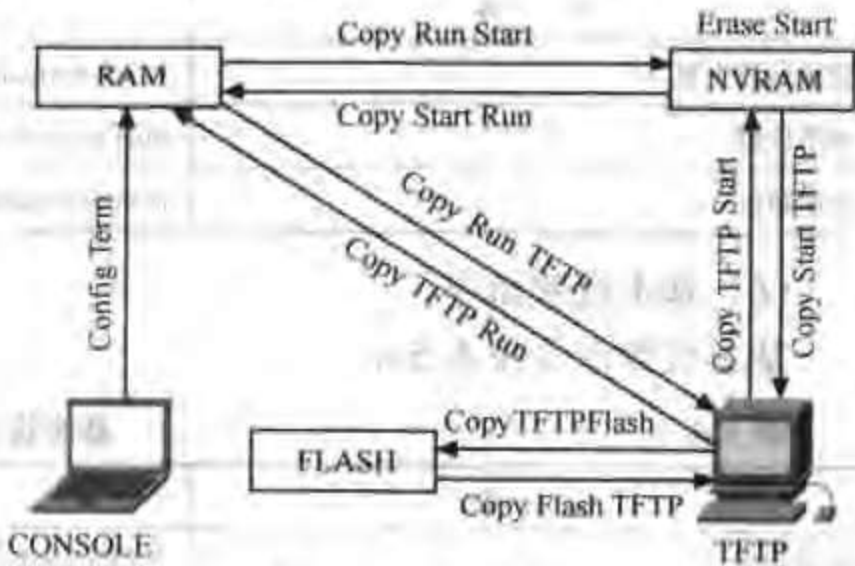


图 5-13 IOS 文件管理

表 5-1 改变命令状态的命令

任 务	命 令
进入特权命令状态	enable
退出特权命令状态	disable
进入设置对话状态	setup
进入全局设置状态	config terminal
退出全局设置状态	end
进入端口设置状态	interface type slot/number
进入子端口设置状态	interface type number.subinterface [point-to-point multipoint]
进入线路设置状态	line type slot/number
进入路由设置状态	router protocol
退出局部设置状态	exit

(3) 显示命令

显示命令见表 5-2。

表 5-2 显示命令

任 务	命 令
查看版本及引导信息	show version
查看运行设置	show running-config
查看开机设置	show startup-config
显示端口信息	show interface type slot/number
显示路由信息	show ip route

(4) 拷贝命令

用于 IOS 及 CONFIG 的备份和升级，相见上节“IOS 文件管理”。

(5) 网络命令

网络命令见表 5-3。

表 5-3 网络命令

任 务	命 令
登录远程主机	<code>telnet hostname IP address</code>
网络侦测	<code>ping hostname IP address</code>
路由跟踪	<code>trace hostname IP address</code>

(6) 基本设置命令
基本设置命令见表 5-4。

表 5-4 基本设置命令

任 务	命 令
全局设置	<code>config terminal</code>
设置访问用户及密码	<code>username username password password</code>
设置特权密码	<code>enable secret password</code>
设置路由器名	<code>hostname name</code>
设置静态路由	<code>ip route destination subnet-mask next-hop</code>
启动 IP 路由	<code>ip routing</code>
启动 IPX 路由	<code>ipx routing</code>
端口设置	<code>interface type slot/number</code>
设置 IP 地址	<code>ip address address subnet-mask</code>
设置 IPX 网络	<code>ipx network network</code>
激活端口	<code>no shutdown</code>
物理线路设置	<code>line type number</code>
启动登录进程	<code>login [localtacacs server]</code>
设置登录密码	<code>password password</code>

IOS 常用的查询命令如图 5-14 所示。其中，

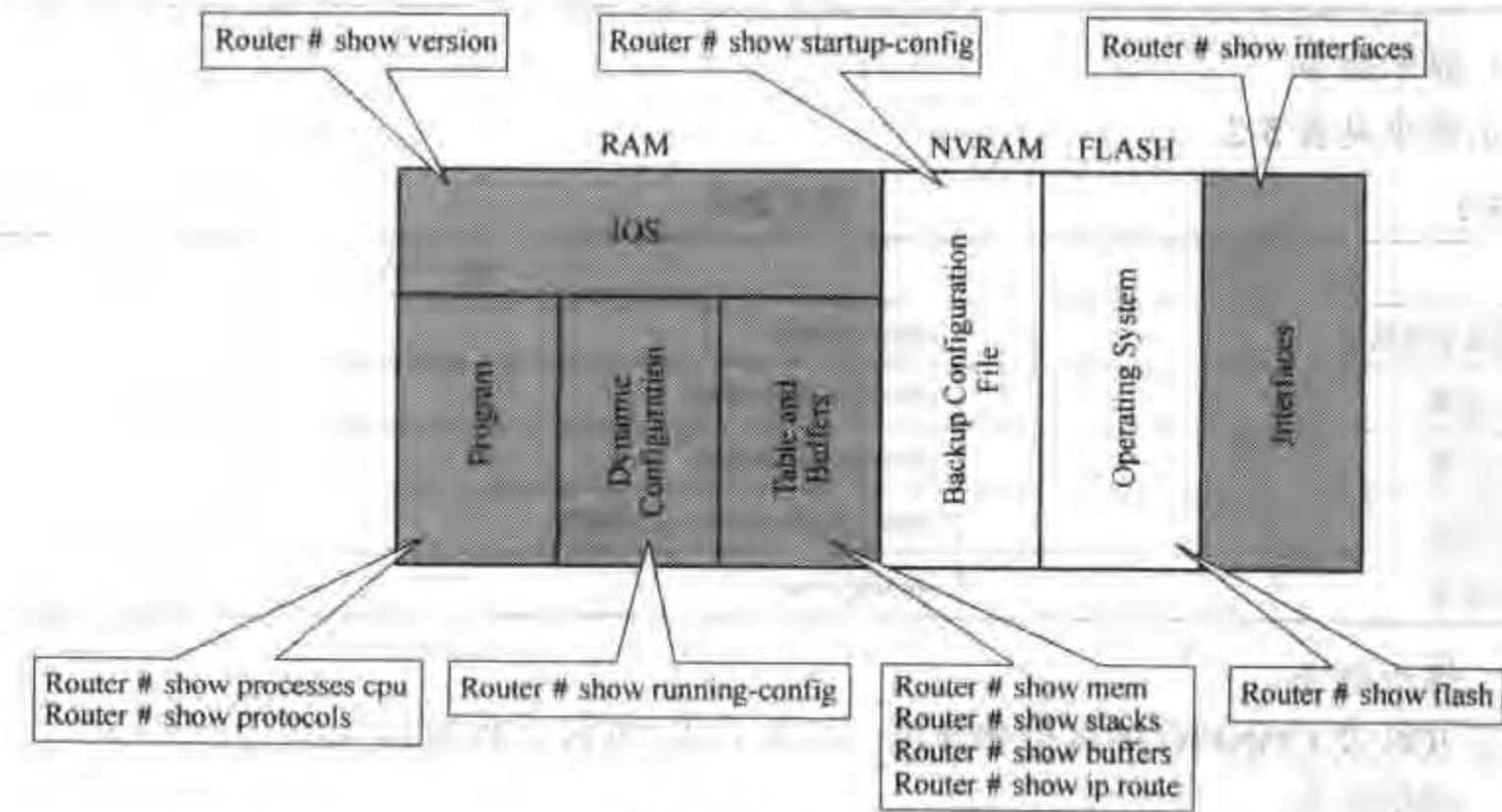


图 5-14 IOS 常用查询命令

show version: 显示系统的硬件配置, 软件版本, 配置文件的源和名字, 以及启动镜像;
show processes: 显示当前活动进程;
show protocols: 显示已经配置的协议;
show memory: 显示路由器的内存信息;
show ip route: 显示路由表;
show flash: 显示闪存设备的信息;
show running-config: 显示当前活动配置;
show startup-config: 显示备份配置文件;
show interfaces: 显示已经配置的接口属性。

5.2.6 路由器基本配置镜像

路由器的配置根据不同的链路、不同的需求会有很大的不同, 但所有的路由器都有一些共同的部分, 我们可以将这些共同的部分作为基本的镜像用于路由器的最初始配置。

(1) 设主机名和密码

```
hostname cisco
```

```
enable password cisco
```

(2) 禁止 DNS 查询

```
no ip domain-lookup
```

(3) 为 log 和 debug 设置时间戳

```
service timestamps debug uptime
```

```
service timestamps debug datetime
```

```
service timestamps log uptime
```

```
service timestamps log datetime
```

(4) 设置 Telnet 登录参数

```
line vty 0 4
```

```
password cisco
```

```
login
```

(5) 基本安全的设置

```
hostname cisco
```

```
enable password cisco
```

```
line con 0
```

```
login
```

```
line vty 0 4
```

```
password cisco
```

```
login
```

```
no ip http server
```

```
no snmp-server
```

```
no service finger
```

```
no ntp
```



```
no cdp run
no service udp-small-servers
no service tcp-small-servers
综合以上各方面的配置命令，其完整的配置如下：
hostname cisco
enable password cisco
no ip domain-lookup
service timestamps debug nptime
service timestamps debug datetime
service timestamps log uptime
service timestamps log datetime
line con 0
login
line vty 0 4
password cisco
login
no ip http server
no snmp-server
no service finger
no ntp
no cdp run
no service udp-small-servers
no service tcp-small-servers
```

说明：上面这段配置我们可以保存作为一个基础配置，在配置任何路由器的时候，都可以将这段配置首先粘贴进路由器，然后再进行以下的功能配置。当然，其中的密码“Cisco”一定要改成自己的密码。

5.3 广域网互联设置

路由器是网络层的设备，它的主要作用是用来实现企业的广域互连。要想正确地搭建广域网，必须对电信提供的各种线路有所了解，下面就对我国的电信网以及电信部门所提供的各种线路作一简单介绍。

5.3.1 电信网搭介

通过对第1章的学习我们了解到，按地理位置可以将计算机网络分为局域网、广域网和城域网。局域网一般在几十米~几公里范围内，往往采用自己布线的方式构建。广域网的范围非常大，可以跨越国界、洲界，甚至全球范围，它是网络的公共部分。在我国，广域网一般需要租用电信部门的线路搭建而成。由于搭建广域网需要用到电信部门提供的各种线路，

下面就电信网做一个简单的介绍，在其后的几节将分别对各种链路进行介绍。

电信网是为公众提供电信服务的一类网络，是整个社会信息化的基础。电信网按功能可以分为传输网、业务网和支撑网，如图 5-15 所示。

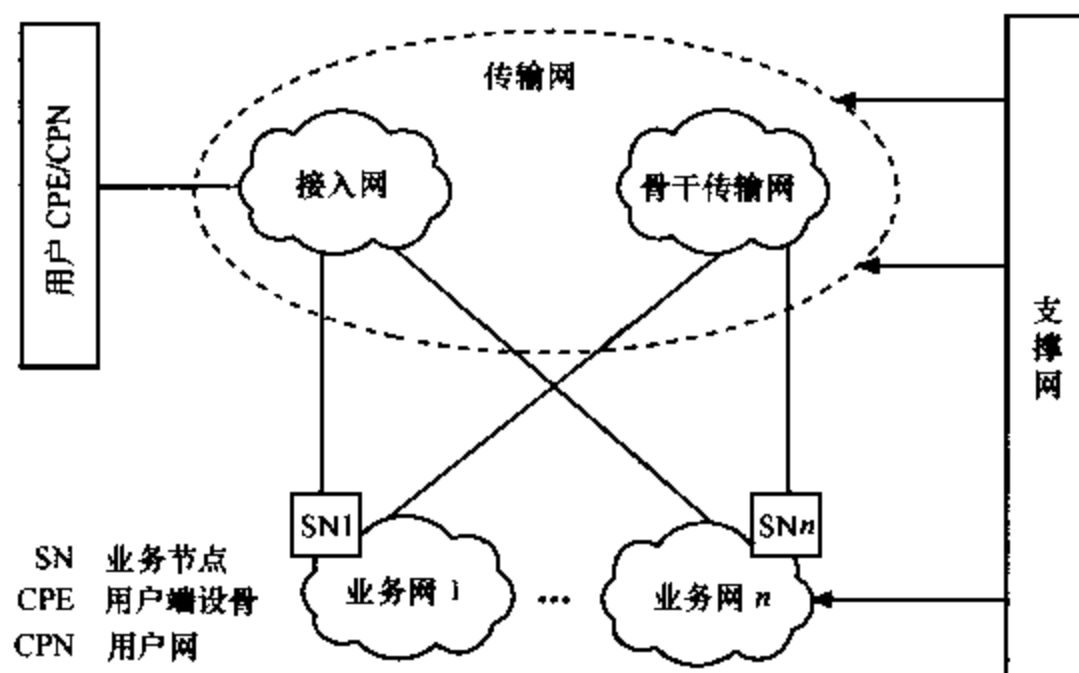


图 5-15 电信网结构

1. 业务网

业务网是指向公众提供电信业务的网络，包括固定电话网、移动电话网、IP 电话网、数据通信网、窄带综合业务数字网（N-ISDN）、宽带综合业务数字网（B-ISDN）等。

电信公司的业务主要包括语音和数据两大类。语音业务包括我们日常使用最多的固定电话、移动电话以及现在已经非常普遍的 IP 电话和 ISDN 业务；数据业务包括使用最多的 DDN 和帧中继等。

注意：

1. ISDN 业务既可以认为是语音业务，也可以认为是数据业务。
2. 现在使用越来越多的数字电路（PCM）业务实际是直接接入传输网的一种业务。

在组建广域网络时，主要会接触到电信公司所提供的各种数据业务。在以后的几节将分别介绍在我国使用最为广泛的几种电信公司的线路。

2. 传输网

传输网指数字信号的传输网络，包括骨干传输网和接入网。在上面所提到的各种业务网络中的各种不同的业务信号，都将以数字信号的形式通过传输网进行传输。因此传输线路、传输设备是电信网的重要的基础设施。由传输线路、传输设备组成的传输网是整个电信网的基础。

在电信网中，为了提高信道的利用率，在线路上传输的信号一般都是经过时分复用以后形成的数字信号的群路信号。在数字传输系统中，有网种数字传输系列，一种叫“准同步数字系列”（Plesiochronous Digital Hierarchy），简称为 PDH；另一种叫“同步数字系列”（Synchronous Digital Hierarchy），简称为 SDH。

PDH 的时分复用速率等级见表 5-5。

表 5-5	PDH 时分复用速率等级	
	欧洲 (E)	美国 (T)
一次群	2 048Mbit/s	1.544Mbit/s
二次群	8 448Mbit/s	6 312Mbit/s
三次群	34 368Mbit/s	44 736Mbit/s
四次群	139 264Mbit/s	274.176Mbit/s
五次群	564 992Mbit/s	

SDH 的速率等级见表 5-6。

表 5-6	SDH 速率等级	
SDH 等级	SONET 等级	标准速率
STM-1	OC-3	155 520Mbit/s
STM-4	OC-12	622 080Mbit/s
STM-16	OC-48	2488 320Mbit/s
STM-64	OC-192	9953 280Mbit/s

在数字通信系统中，传送的信号都是数字化的脉冲序列。这些数字信号流在数字交换设备之间传输时，其速率必须完全保持一致，才能保证信息传送的准确无误，这就叫做“同步”。采用准同步数字系列（PDH）的系统，是在数字通信网的每个节点上都分别设置高精度的时钟，这些时钟的信号都具有统一的标准速率。尽管每个时钟的精度都很高，但总还是有一些微小的差别。为了保证通信的质量，要求这些时钟的差别不能超过规定的范围。因此，这种同步方式严格来说不是真正的同步，所以叫做“准同步”。在以往的电信网中，大部分都是使用 PDH 设备。这种系列对传统的点到点通信有较好的适应性。而随着数字通信的迅速发展，点到点的直接传输越来越少，而大部分数字传输都要经过转接，因而 PDH 系列便不能适合现代电信业务开发的需要，也不能适合现代化电信网管理的需要。SDH 就是适应这种新的需要而出现的传输体系。最早提出 SDH 概念的是美国贝尔通信研究所，它被称为光同步网络（SONET），是高速、大容量光纤传输技术和高度灵活、又便于管理控制的智能网技术的有机结合。最初的目的是在光路上实现标准化，便于不同厂家的产品能在光路上互通，从而提高网络的灵活性。1988 年，ITU-T（原 CCITT）接受了 SONET 的概念，重新将其命名为“同步数字系列（SDH）”，使它不仅适用于光纤，也适用于微波和卫星传输的技术体制，并且使其网络管理功能大大增强。

- SDH 技术与 PDH 技术相比，有如下明显优点：
- （1）具有统一的传输速率（从表 5-5 中可以看出，PDH 有欧洲的 E 和北美的 T 两种速率标准），统一的接口标准，为不同厂家设备间的互联提供了可能。
 - （2）网络管理能力大大加强。
 - （3）提出了自愈网的新概念。用 SDH 设备组成的带有自愈保护能力的环网形式，可以在传输媒体主信号被切断时，自动通过自愈网恢复正常通信。
 - （4）采用字节复接技术，使网络中上下支路信号变得十分简单。

由于 SDH 具有上述显著优点，它将成为实现信息高速公路的基础技术之一。我国的数字传输网在 PDH 规模很小时就开始了 SDH 的建设，到目前为止，SDH 传输网已是我国数字

传输网的主体。但是在与信息高速公路相连接的支路和叉路上, PDH 设备仍将有用武之地。

3. 支撑网

支撑网是对电信网的正常运营起到支持作用的一类网络, 包括信令网、同步网和管理网。信令网通过公共的网络传送信令; 同步网提供全网同步的时钟; 管理网则通过计算机系统对全网进行统一的管理。

通过以上的介绍, 读者可以对我国的电信网有一个大致的结构上的了解, 下面就对我国提供的一些常见的数据通信业务分别进行介绍, 其中包括 DDN、帧中继、数字电路、ISDN、PSTN 和 ADSL 等。

5.3.2 数字数据网 (DDN)

1. 简介

数字数据网 (DDN, Digital Data Network) 是利用光纤、数字微波或卫星等数字传输通道和各种数字交叉复用设备组成的, 它可以为客户提供 $N \times 64\text{ kbit/s}$ 速率的高质量透明传输专线电路, 以满足客户组建专网或连接 Internet 的需要。

DDN 利用数字信道传输数据信号, 与传统的模拟信道相比, 具有传输质量高、速度快、带宽利用率高等一系列优点:

(1) 传帧质量高: 接成 DDN 的基本单位是节点, 节点间主要通过光纤连接, 构成网状的拓朴结构, 因此它的传帧质量是很高的;

(2) 透明传输: DDN 传输信道本身不提供任何协议和接程约束, 由智能化的用户终端接定通信协议, 所以它是全透明网, 面向各类数据客户开放;

(3) 专线方式的同步数据网: DDN 采用数字方式来传帧数据, 要求全网时钟同步。DDN 以专线方式传输, 完全占用所分配的數字信道, 服务质量有保证;

(4) 具有固定的传输速率, 其网络时延低: DDN 向用户接供的是半永久性的数字连接, 沿途不进行复杂的软件处理, 因此延时较短, 避免了分组网中传输时延大且不固定的较点。用户根据约定的协议, 在固定带宽和约定速率下进行可靠传帧, 时延小, 性能稳定, 可靠性高;

(5) 具有灵活的连接方式: DDN 支持数据、语音、图像传输等多种业务, 支持多种接入速率, 范围从 2.4 kbit/s 到 2 Mbit/s 不等, 可满足客户对不同通信速本的要求;

(6) DDN 提供端到端的连接, 对于用户而言, 相当提供了一条专用的电路;

(7) 覆盖范围广: 我国可与世界上主要国家开通此类专线, 在全国范围内可与县市我城市直接开通此类专线, 这也是 DDN 在我国被广泛使用的原因之一。

我国目前开放的 DDN 专线种类包括: 本地、国内长途、国际 (含港、接、台地区) 长途。具体办理手续可到各地电信的数据业务营业处查询, 或拨打电信服务热线 1000 进行咨询。

国内 DDN 接路的月租费率见表 5-7, 国际线路的月机费率见我 5-8。

表 5-7

国内 DDN 线路月租费 (单位: 元/月)

速 率	本地营业区内	本地营业区间	国内长途
9.6kbit/s	1000	1300	2500
19.2kbit/s	1200	1500	2700

续表

速 率	本地营业区内	本地营业区间	国内长途
64kbit/s	1500	2000	3500
128kbit/s	2000	2500	5000
256kbit/s	2500	3200	5500
384kbit/s	3200	4000	6200
512kbit/s	3800	5200	7000
768kbit/s	4300	6200	8000
1Mbit/s	5000	7500	9000
2Mbit/s	6000	8000	12000

表 5-8 国际 DDN 线路月租费（单位：元/月）

速 率	中国港澳台地区	亚洲各国	欧美澳非各国
9 6kbit/s	3000	15000	16000
19 2kbit/s	3400	17000	18000
64kbit/s	5200	26000	27000
128kbit/s	6800	34000	34000
256kbit/s	7800	39000	40000
384kbit/s	9800	49000	50000
512kbit/s	11400	57000	59000
768kbit/s	13200	66000	68000
1Mbit/s	14800	74000	77000
1 5Mbit/s	17400	87000	95000
2Mbit/s	20000	100000	100000

注：具体费用请咨询当地电信部门。

2. 典型应用

DDN 业务提供点到点的专线连接，它的优点是不涉及协议，且勿需在每个网络节点对所传数据进行缓存和处理，从而使专线电路的网络具有高速和低延时的特点。但对数据应用来说，它最大的缺点是要求每对需要通信的端点之间，都需建立一条独立的物理线路。所以，当一点对多点或多点对多点通信时，用户就需申请许多端口；其次专线电路和带宽是固定的，因此在处理突发性业务时就显得很困难，这样用户就需购买足够的带宽去应付“突发性”业务；再其次，由于专线电路是点对点方式，在空闲时间内，虽然未使用带宽，却仍需付费。综上所述，如果用户需要高流量，低延时的业务可申请点对点的专线电路，但需付出高成本的代价。DDN 的典型应用拓扑如图 5-16 所示。

在一般情况下，用户的总部或地市分部如果汇集的电路数比较多，带宽需求较大，建议采用将节点机放置在用户机房，用户设备直接用电缆连接到节点的方式。根集用户的网络规模，用户设备建议使用 Cisco 的 7500、7200 或 3700 系列的路由器，DDN 线路为点到点线路，因此有多少个分支就需要申请多少条 DDN 线路，同时设备上也就需要多少个串口。

为方便维护,减少端口数量,建议在中心端采用 CE1 (信道化的 E1) 端口 (我们将在数字电路部分进行讲解)。对于分支点,建议采用外线或光纤直接连入就近的节点,需要与端口速率相适应的基带猫或 DTU 或光猫等接入设备 (具体接入方式见下面的用户入网方式部分)。用户设备建议使用 Cisco 的 1700 或 2600 系列的路由器,或者其他品牌同等容量的路由器。如用户速率低于 64kbit/s,则配置 V.24 端口;如用户速率为 64~1920kbit/s,建议配置 V.35 端口;如用户速率为 1984kbit/s,或带宽总需求为 2Mbit/s,则建议采用 CE1 (信道化的 E1) 端口。

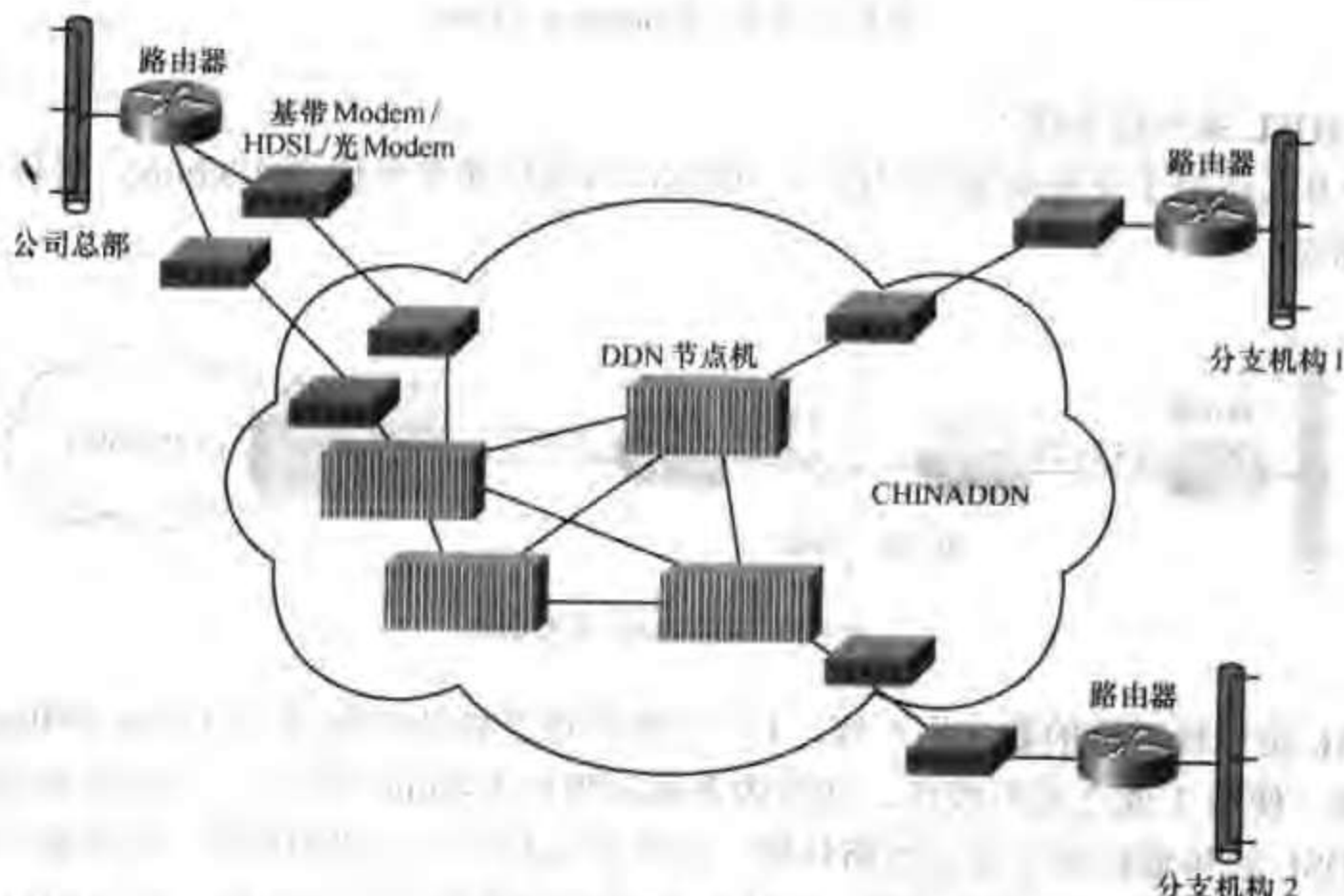


图 5-16 DDN 典型应用

3. 用户入网方式

根据我国 DDN 技术体制的要求,用户入网包括以下几种常见的方式:

(1) 通过 DDN 的数据终端设备 (DTU) 接入 DDN

用户直接利用 DDN 提供的远程数据终端设备 (DTU) 接入 DDN,而无需增加单独的调制解调器,如图 5-17 所示。

特点:DDN 网管中心可对用户端放置的数据终端设备进行远程系统配置、参数修改和日常维护管理。通常情况下,其支持的距离在 5km 之内,通信速率不超过 128kbit/s。



图 5-17 采用 DTU 接入 DDN

(2) 通过调制解调器 (基带猫) 接入 DDN

用户在距 DDN 的接入点比较远的情况下采用这种接入方式, 它支持的距离较 DTU 稍远一些 (10km 以内), 通信速率不超过 128kbit/s。这种接入方式如图 5-18 所示。



图 5-18 采用基带 Modem 接入 DDN

(3) xDSL 系列设备接入

这种方式适用于支持高速用户接入, HDSL 的通信速率可达 2048kbit/s, 其接入方式如图 5-19 所示。



图 5-19 采用 HDSL 接入 DDN

HDSL 是一种对称的数字用户线, 上下行通道通过传统的铜线可以实现 2Mbit/s 的数字信号传输。使用 1 或 2 对双绞线, 在国内普遍应用的 0.4mm 线径上, 其传送距离可达 3~5km。HDSL 的传输距离会受到线路环阻、线路质量和环境干扰的限制。这些都是由 HDSL 传输系统的不同的编码方法决定的。HDSL 系统线路编码方法有多种, 如 2B1Q、2B2T、4B3T、QAM 和 CAPD 等。目前常用的有两种, 即 2B1Q 编码和 CAP 编码。两者都符合欧洲电信标准协会 (ETST) 的 ETR152 建议 (即 E1 HDSL 的技术规范)。目前市场上的主流产品应用以 2B1Q 为主, 主要设备供应商如 Alcatel、百令达、RAD、台联等都选用了 2B1Q 作为编码方式。

SHDSL 由于采用了 TC-PAM 的编码方式, 传输距离比 HDSL 产品要提高 10% 左右。可以采用 1 对或 2 对双绞线传输, 有很强的频谱兼容性和抗干扰性能, 并具有速率自适应等传输特性。目前主要的设备厂家的 HDSL 设备和 SHDSL 设备都可以实现 1 对线或 2 对线应用。2 对线应用相比 1 对线应用可以提供更远的传输距离和更稳定的信号质量。

(4) 节点机接入

这种方式适用于 DDN 用户专线较集中的位置, 特别适用于集团用户中心节点。DDN 节点机可通过若干条数字中继从几方向接入 CHINADDN 网, 确保集团用户中心节点的稳定性、可靠性、可用性及可扩展性。采用节点机接入具有维护方便、易于管理的优点, 是集团用户理想的接入解决方案, 如图 5-20 所示。

(5) 通过光纤线路接入

适用于光纤到户的用户, 其通信速率可灵活选择。通常采用多模光纤, 传输距离可达 2km。如采用单模光纤, 传输距离可达 50km。

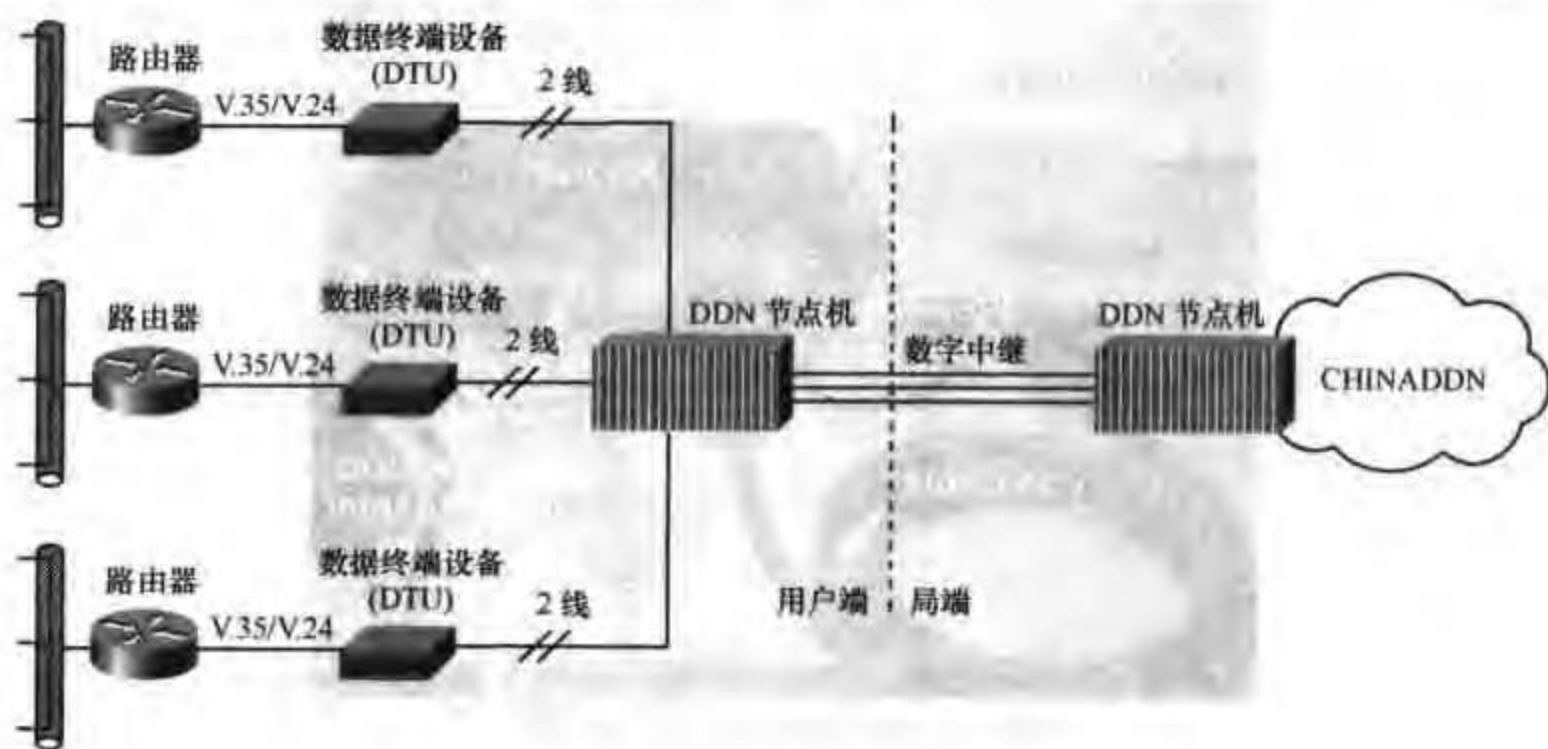


图 5-20 采用节点机接入 DDN

通过光 Modem 接入的方式如图 5-21 所示。

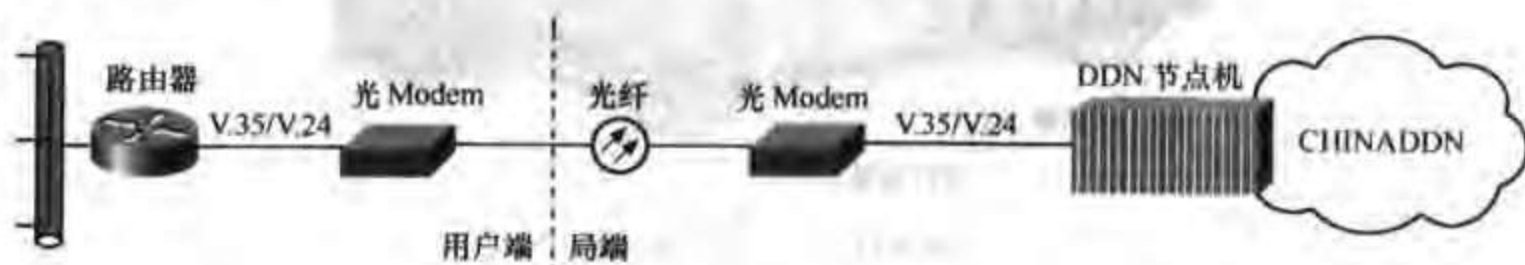


图 5-21 采用光 Modem 接入 DDN

4. 案例分析

案例 1

两个路由器通过 DDN 专线互连，实现两个局域网间的通信。拓扑结构如图 5-22 所示：

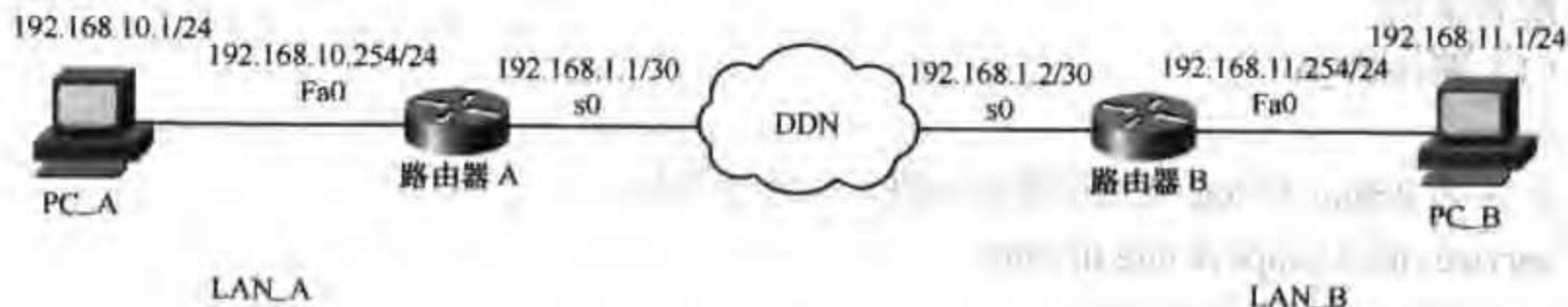


图 5-22 DDN 案例 1 的拓扑结构

说明：

所选用的路由器为 Cisco1721，各配置一块 WIC-1T 同步串口卡，用于 DDN 的互连。路由器和基带 Modem 的连接如图 5-23 所示。

本案例所采用的设备和相应的模块如图 5-24~图 5-26 所示。



图 5-23 路由器和基带 Modem 的连接



图 5-24 Cisco1721 路由器



图 5-25 WIC-1T 接口卡



图 5-26 CAB-V35MT 线缆

配置文档:

(1) 路由器_A

!

!--为 debug 和 log 分别设置时间戳, 以便于排错:

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

!--将设置的口令加密:

```
service password-encryption
```

!--关闭不必要的服务:

```
no service tcp-small-servers
```

```
no service udp-small-servers
```

!

! ---设置主机名为“Router_A”:

hostname Router_A

!

! ---设置特权密码为“cisco”:

enable password cisco

!

! ---不设置 DNS Server 值:

no ip name-server

!

! ---允许是 0 子网:

ip subnet-zero

! ---禁止 DNS 查询:

no ip domain-lookup

! ---启用 IP 路由进程:

ip routing

!

! ---进入接口配置模式:

interface FastEthernet 0

! ---启用接口:

no shutdown

! ---设置接口的描述, 方便排错:

description connected to LAN_A

! ---为接口设置 IP 地址:

ip address 192.168.10.254 255.255.255.0

! ---设置发送 keepalive 数据包的时间间隔, 以太网默认认为 10 秒:

keepalive 10

!

! ---进入接口配置模式:

interface Serial 0

! ---启用接口:

no shutdown

! ---设置接口的描述, 方便排错:

description connected to Router_B

! ---为接口设置 IP 地址:

ip address 192.168.1.1 255.255.255.252

! ---设置此接口的链路封装协议为 PPP:

encapsulation ppp

!

! ---启用动态路由协议 rip, 进入路由配置模式:


```
router rip
! ---指定 rip 采用版本 2:
version 2
! ---为路由协议指定应用的网段:
network 192.168.10.0
network 192.168.1.0
! ---取消路由协议的自动汇总:
no auto-summary
!
!
! ---启用无类别属性, 用于告诉路由器当目的网络没有出现在路由表中时通过默认路由
转发数据包:
ip classless
! ---禁用 HTTP 服务:
no ip http server
! ---启用 snmp 网管服务, 设“RO”(readonly 只读)权限的“community”(社区)字符
串为“public”:
snmp-server community public RO
! ---未设 snmp 网管的位置信息:
no snmp-server location
! ---未设 snmp 网管的联系人信息:
no snmp-server contact
!
! ---进入 console 接口配置模式:
line console 0
! ---为控制台连接设置超时的时限, “0 0”代表“0 分 0 秒”, 即永不超时:
exec-timeout 0 0
! ---为控制台连接设置登录密码为“cisco”:
password cisco
! ---配置控制台接口为允许登录:
login
!
! ---进入 VTY (Telnet) 接口配置模式:
line vty 0 4
! ---为 Telnet 连接设置登录密码为“cisco”:
password cisco
! ---配置 VTY 接口为允许登录:
login
!
```

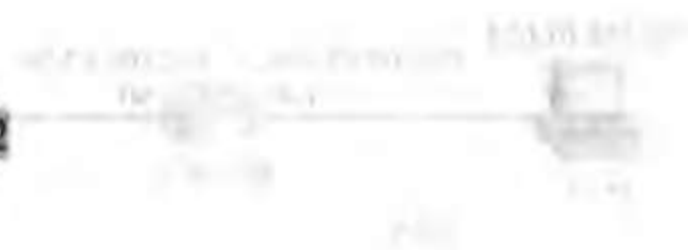

注意：以上我们对 Router_A 的每条配置命令都作了注释，在以后的案例配置中，我们只对新出现的配置命令进行注释，相同的部分我们就不再重新注释。

(2) 路由器_B

```

!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_B
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0
no shutdown
description connected to LAN_B
ip address 192.168.11.254 255.255.255.0
keepalive 10
!
interface Serial 0
no shutdown
description connected to Router_A
ip address 192.168.1.2 255.255.255.252
encapsulation ppp
!
router rip
version 2
network 192.168.11.0
network 192.168.1.0
no auto-summary
!
!

```




```
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
```

说明：

(1) 以上配置中带阴影的部分是为完成本案例所必需配置的部分，其余的配置都是方便管理或有关安全方面的配置。

(2) 本案例中路由部分是采用的动态路由协议 **RIP**，其实对于本案例这样相对简单的网络来说，采用静态路由应该是更好的选择，我们可以采用如下的命令来替代上述配置文档中的 **RIP** 路由协议配置部分：

路由器_A：

```
ip route 192.168.11.0 255.255.255.0 192.168.1.2
```

路由器_B：

```
ip route 192.168.10.0 255.255.255.0 192.168.1.1
```

案例 2

DDN 专线连接 Internet，其拓扑结构如图 5-27 所示。

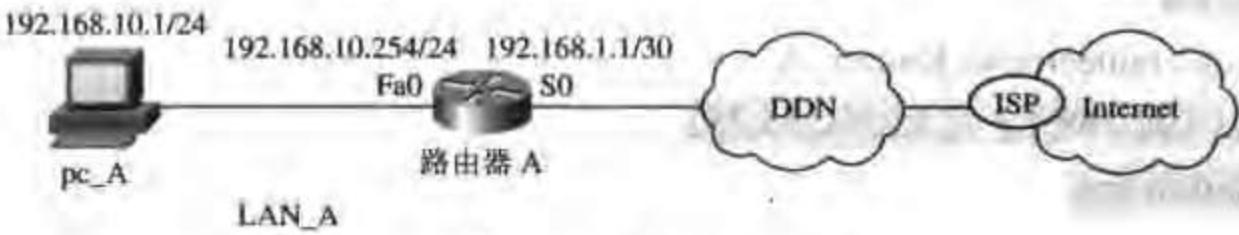


图 5-27 DDN 案例 2 的拓扑结构

说明：

所选用的路由器为 Cisco1721，配置一块 WIC-IT 同步串口卡，用于 DDN 的接入。本案例所采用的设备和模块同案例 1。

配置文档：

路由器_A

！


```

service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_A
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0
no shutdown
description connected to LAN
ip address 192.168.10.254 255.255.255.0
! ---配置此接口为地址转换（NAT）的内接口：
ip nat inside
keepalive 10
!
interface Serial 0
no shutdown
description connected to Internet
ip address 192.168.1.1 255.255.255.252
! ---配置此接口为接口转换的外接口：
ip nat outside
encapsulation ppp
!
! Access Control List 1
!
! ---取消访问控制列表“1”：
no access-list 1
! ---重新定义访问控制列表“1”为“允许 192.168.10.0/24 网段”：
access-list 1 permit 192.168.10.0 0.0.0.255
!

```


! Dynamic NAT

!

! ---配置动态地址转换的失效时间，默认为值为 86400 秒：

ip nat translation timeout 86400

! ---定义从 ISP 那里申请到的公网 IP 在企业内部的分配策略，这里定义了一个地址池“Router-natpool-1”，它所涵盖的地址将被内网用户用来上网：

ip nat pool Router-natpool-1 202.96.38.4 202.96.38.6 netmask 255.255.255.248

! ---将访问控制列表“1”与地址池“Router-natpool-1”对应，即如果“PC_A”将网关地址指向“192.168.10.254”，当它上网时，它的内网地址“192.168.10.1”将被转换为“202.96.38.4”至“202.96.38.6”中的一个；“overload”表示，如果有多于地址池中定义的地址数量（这里是 3）的用户访问外部，那么多个内网地址可能会被转换为同一公网地址，不同内网地址之间可以通过不同的端口来识别，这样利用地址池定义的 3 个公网地址就可以带领所有的内网用户上网：

ip nat inside source list 1 pool Router-natpool-1 overload

!

ip classless

!

! IP Static Routes

! ---配置默认路由：

ip route 0.0.0.0 0.0.0.0 Serial 0

no ip http server

snmp-server community public RO

no snmp-server location

no snmp-server contact

!

line console 0

exec-timeout 0 0

password cisco

login

!

line vty 0 4

password cisco

login

!

说明：以上配置中带阴影的部分是为完成本案例所必需配置的部分。

5.3.3 帧中继（Frame Relay）

1. 简介

帧中继（Frame Relay）是由 X.25 分组交换技术发展而来，在当前数据通信中得到广泛

应用的一种广域网技术。通信的数字化提高了网路的可靠性和终端设备的智能化程度，使数据传输的差错率降低到可以忽略不计的地步。帧中继正是利用现代通信网的这一优点，以帧为单位在网络上传输，并将流量控制、纠错等功能全部交由智能终端设备处理的一种新型高速网络接口技术。

帧中继和分组交换类似，但却以比分组容量大的帧为单位而不是以分组为单位进行数据传输，而且，它在网络上的中间节点对数据不进行误码纠错。帧中继技术在保持了分组交换技术的灵活及较低的费用同时，缩短了传输时延，提高了传输速率。同时，帧中继采用虚电路技术，能充分利用网路资源，支持多种数据型业务。因此，它成为了当今实现局域网（LAN）互连、局域网与 Internet 连接等应用的理想解决方案。其主要特点有：

（1）高效性：帧中继使用统计时分复用技术，共享传输线路和网路端口，提高了网路资源的利用率；用户还可在有空余带宽时，超过预定值“偷占”更多的带宽（EIR），而只付预定带宽（CIR）的费用，非常适合于出现突发性大数据量业务的用户。

（2）可靠性和灵活性：帧中继虽然利用端到端机制实现错误恢复，但网路本身也是可靠的，有 PVC 管理和拥塞管理机制，以保证网路充分运行。帧中继网在组建和用户接入上方便灵活，对高层协议保持透明，无兼容性问题。

（3）支持质量服务等级（QOS）：可以实现质量服务等级，可以实现用户高可靠性传输、保证的性能、低时延和安全性（在信息传送的质量保证上稍逊于 DDN 等时分复用技术）。

（4）网络覆盖性好：我国可与世界上主要国家开通此类专线，在全国范围内可与地市级城市直接开通此类专线。在中国电信投资建设的，并已投入运营的中国公用分组交换数据网（CHINAPAC）和中国公用数字数据网（CHINADDN）上均可开设帧中继业务。同时中国电信于 1997 年建成了采用 ATM 平台的可提供信元中继的帧中继业务的中国公用帧中继宽带业务网（CHINAFRN）。基于 CHINAFRN 的帧中继业务由于是建立在中国电信的 ATM 网络平台之上的，因此，在网络上实际是 ATM 信元在高速传送，这样，不仅保证用户网络的先进性，可扩展性，而且，可以方便地、无输地由帧中继过渡到 ATM，从而实现高带宽通信。它可接供高速数连接（如局域网互联），主要是为商业、金融、企业等集团用户组建较高速的专网，接供 OA、视频、网络应用等高质量的网络服务。

申请接中继专线的具体办理手续，可到各地电信的数据业务营业处查询，或接打电信服务热线 1000 进行咨询。客户在申请帧中继电路时，是以 PVC 为单位的，每一条 PVC 都要注明 CIR、Bc、Be、DLCI 等参数。请务必记住这些参数，因为在调试路由器时会用到它们。

办理帧中继业务的费用一般包括一次性费用和月租费两部分。一次性费用包括：工料费和调试费；月租费包括：端口月租费和虚电路（PVC）月租费。这些费用的费率见表 5-9 和 5-10。

表 5-9 帧中继端口月租费一览表（单位：元/月）

端口速率	64kbit/s	128kbit/s	256kbit/s	384kbit/s	512kbit/s	768kbit/s	1Mbit/s	2Mbit/s
月租费	260	300	400	450	500	650	750	1000

注：1. 端口速率低于 64kbit/s 的按 64kbit/s 端口月租费收取。

2. 表中未列明的端口速率，其资费按相邻两端口速率资费的平均值收取。

表 5-10 帧中继虚电路 (PVC) 月租费一览表 (单位: 元/月)

标准速率 (CIR)	本地网 营业区内	本地网 营业区间	国内长途	国 际		
				中国港澳台地区	亚洲各国	欧、美、澳、非各国
8kbit/s	290	440	990	1550	8800	9400
16kbit/s	390	540	1190	1800	10000	10500
32kbit/s	450	650	1300	2000	11500	11500
48kbit/s	500	750	1500	2300	13000	13500
64kbit/s	550	800	1700	2600	14500	14600
128kbit/s	700	1000	2100	3400	18000	18400
256kbit/s	800	1150	2200	3500	19000	19600
384kbit/s	850	1350	2300	3800	20000	20500
512kbit/s	1000	1450	2500	4100	22300	23100
768kbit/s	1150	1600	2700	4600	25800	26550
1Mbit/s	1250	2000	3000	5200	28900	30050
2Mbit/s	1500	2200	4000	7000	39000	39000

注: 1. 表中未列明速率的帧中继虚电路 (PVC) 的资费为单向电路 (即该条电路只能完成一个方向的数据传输功能) 资费。

2. 表中未列明速率的帧中继虚电路 (PVC), 其资费按相邻两速率电路资费的平均值计收。

说明: 以上费用为参考费用, 具体费用请咨询当地电信部门。

2. 典型应用

帧中继技术适用于以下三种情况:

(1) 当用户需要数据通信, 其带宽要求为 64kbit/s~2Mbit/s, 而参与通信的各方多于两个的时候使用帧中继是一种较好的解决方案;

(2) 通信距离较长时, 建议选帧中继。因为帧中继的高效性使用户可以享有帧好的经济性;

(3) 当数据业务量为突发性时, 由于帧中继具有动态分配带宽的功能, 选用帧中继可以有效地处理突发性数据。

典型的帧中继组网的网络拓扑结构如图 5-28 所示。

一般用户的总部或地市分部如果汇集的电路数比帧多, 带宽需求帧大, 则建议首选采用以 ATM 方式就近接入节点的方式, 配置端口为 STM-1 端口。也可采用节点机到户的接入方式, 建议采用 CE1 (信道化的 E1) 端口。根据用户的网络规模, 用户设备建议使用 Cisco 的 7500、7200 或 3700 系列的路由器。对于 FR 网络没有覆盖到的分支点, 建议采用通过 DDN 帧入的方式, 用户通过与端口速率相适应的基带猫或 DTU 接入的方式。用户设备建议使用 Cisco 的 1700 或 2600 系列的路由器。如用户速率低于 64kbit/s, 则配置 V.24 端口, 如用户速率为 64kbit/s~1920kbit/s, 建议配置 V.35 端口。如用户速率为 1984kbit/s, 或带宽总需求为 2Mbit/s, 则可采用 CE1 (信道化的 E1) 端口, 采用光纤直连到 FR 节点机的方式。

3. 用户入网方式

目前可提供帧中继业务的数据网络有全国骨干帧中继网, 也可使用新桥 DDN 网内的帧中继引擎板开通帧中继业务。对于低速帧中继业务可通过新桥 DDN 网内以帧中继 OVER DDN 的方式或经由 DDN 网接入宽带 ATM 网开通; 对于高速客户可使用光纤或 HDSL 直

接接入 ATM 网;对于某些已放置 DDN 节点机的集团客户可经由 E1 模块或 V.35 模块接入。相对于 DDN 电路,帧中继更适用于点到多点的业务。DDN 的点到多点业务只能提供轮询方式,在一段时间内,主点只能与一个从点进行通信,并且轮询的实现要靠终端软件辅助实现。帧中继业务采用与分组网类似的 PVC 方式,可提供与所有从站并发地进行双工通信的能力。另外,由于帧中继支持突发数据,也比较适合于局域网互连或业务突发量较大的应用。

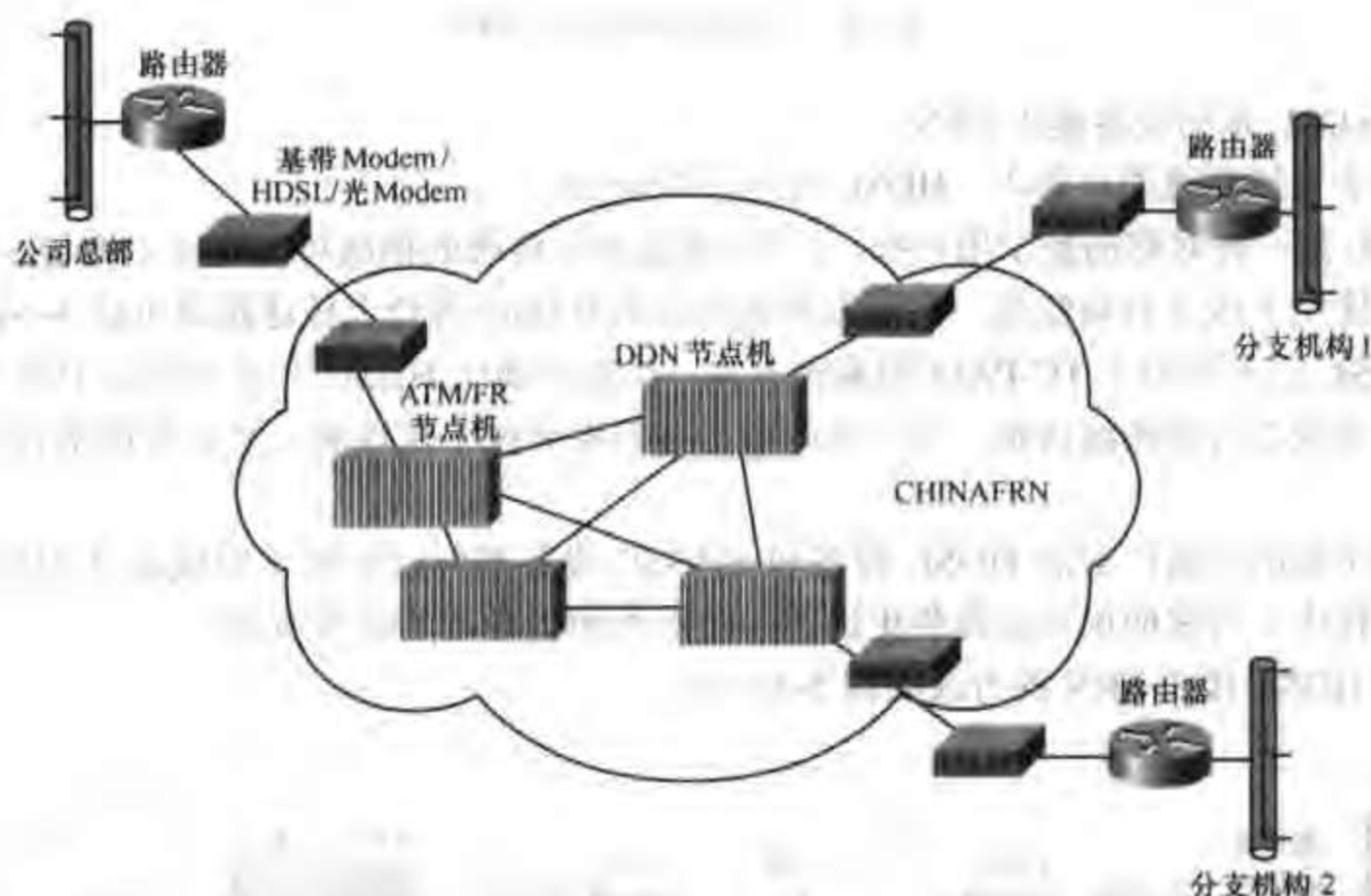


图 5-28 帧中继典型应用

在我国,帧中继用户入网方式和 DDN 用户入网完全一样,包括以下几种常见方式:

(1) 通过 DDN 的数据终端设备 (DTU) 接入 FRN

用户直接利用 DDN 提供的远程数据终端设备 (DTU) 接入 FRN,而无需增加单独的调制解调器,如图 5-29 所示。

特点:网管中心可对用户端放置的数据终端设备进行远程系统配置,参数修改和日常维护管理。通常情况支持距离在 5km 之内,通信速率不超过 128kbit/s。

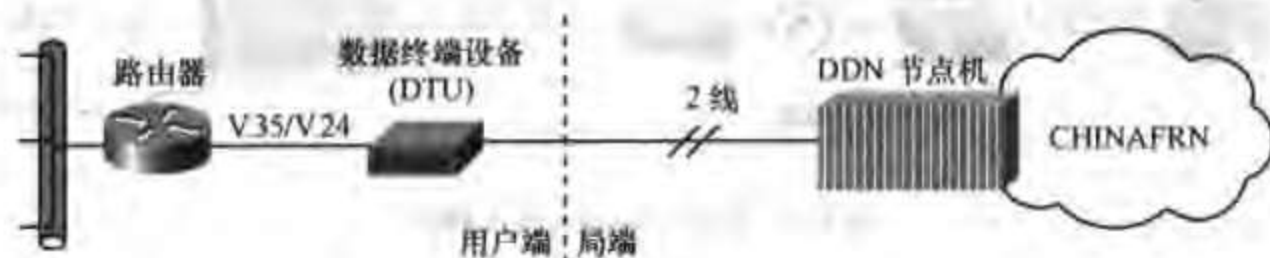


图 5-29 采用 DTU 接入 FRN

(2) 通过调制解调器 (基带 Modem) 接入 FRN

用户在距 FRN 的接入点比较远的情况下采用,支持距离较 DTU 稍远一些 (10km 以内),

通信速率不超过 128kbit/s，其接入方式如图 5-30 所示。



图 5-30 采用基带 Modem 接入 FRN

(3) xDSL 系列设备接入 FRN

适用于支持高速用户接入，HDSL 可达 2048kbit/s。

HDSL 是一种对称的数字用户线，上下行通道通过传统的铜线可以实现 2Mbit/s 的数字信号传输。使用 1 或 2 对双绞线，在国内普遍应用的 0.4mm 线径上传送距离可达 3~5km。

SHDSL 由于采用了 TC-PAM 的编码方式，传输距离比 HDSL 产品要提高 10%左右。可以采用 1 对或 2 对双绞线传输，有很强的频谱兼容性和抗干扰性能，并具有速率自适应等传输特性。

目前主要的设备厂家的 HDSL 设备和 SHDSL 设备都可以实现 1 对线或 2 对线应用，2 对线应用相比 1 对线应用可以提供更远的传输距离和更稳定的信号质量。

采用 HDSL 接入 FRN 的方式如图 5-31 所示。

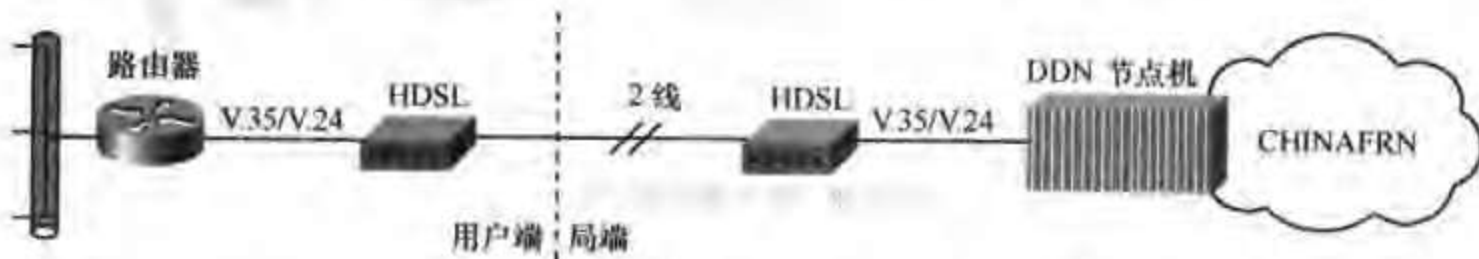


图 5-31 采用 HDSL 接入 FRN

(4) 通过光纤线路接入

这种方式适用于光纤到户的用户，通信速率可灵活选择。其接入方式如图 5-32 所示。

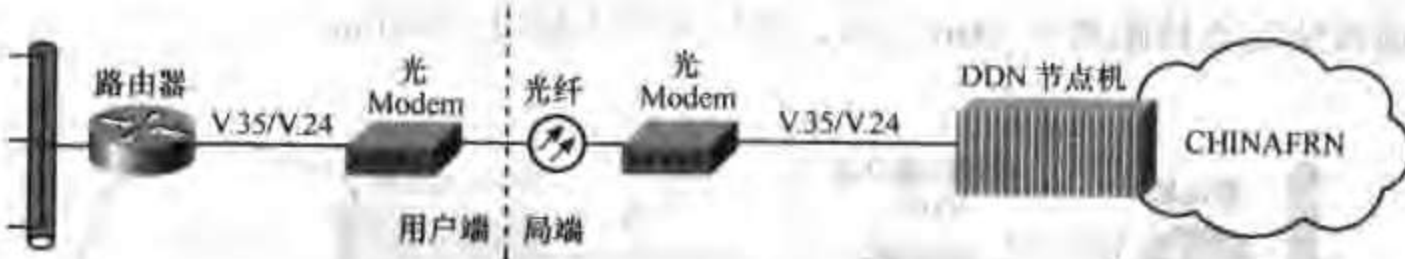


图 5-32 采用光 Modem 接入 FRN

4. 案例分析

案例 1

三台路由器通过帧中继线路互联，实现三个局域网之间的通信。其拓扑图如图 5-33 所示。

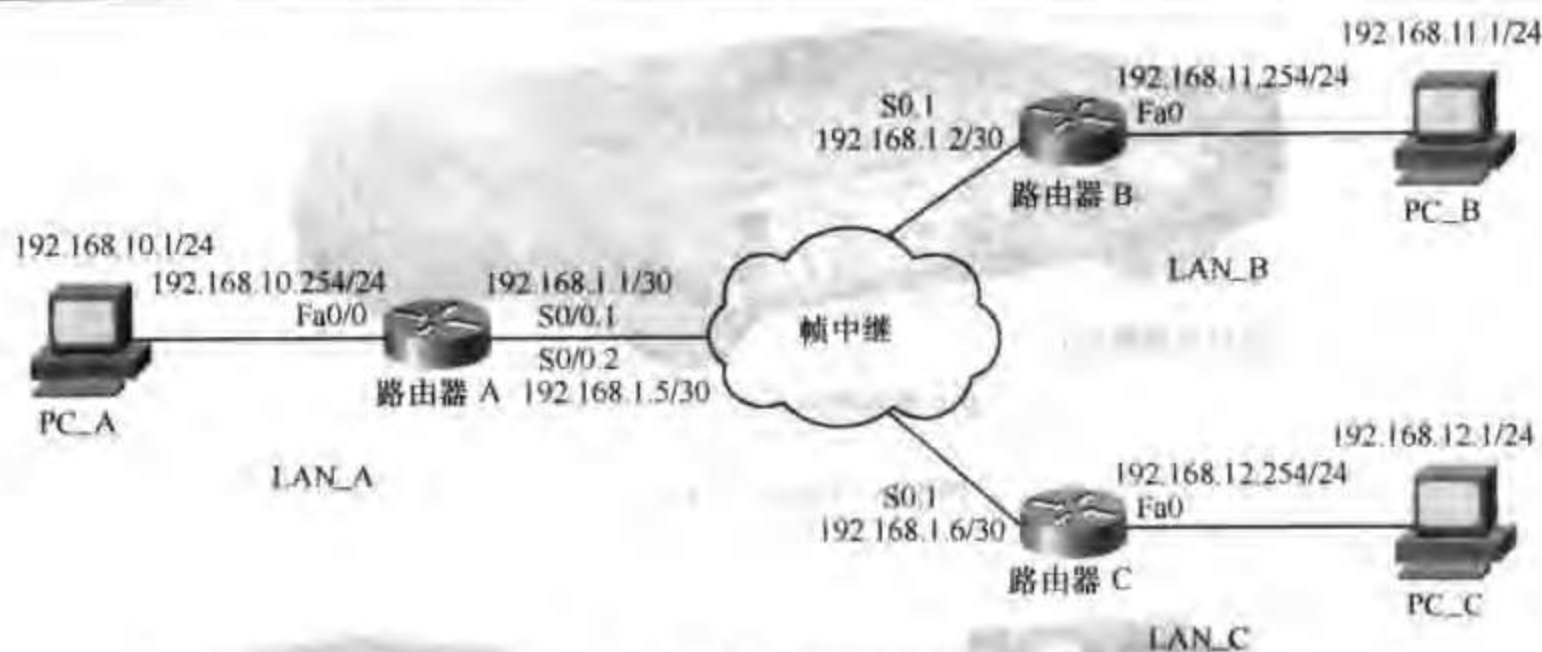


图 5-33 FrameRelay 案例 1 的拓扑结构

说明:

LAN_A (总部) 采用 Cisco2621XM 路由器, 配置 WIC-1T 串口卡, 用于接入帧中继网, 从而与各分支机构互连; LAN_B、LAN_C (分支 B、C) 采用 Cisco1721, 同样配置 WIC-1T 串口卡接入帧中继网。

路由器和基带 Modem 的连接如图 5-34 所示。

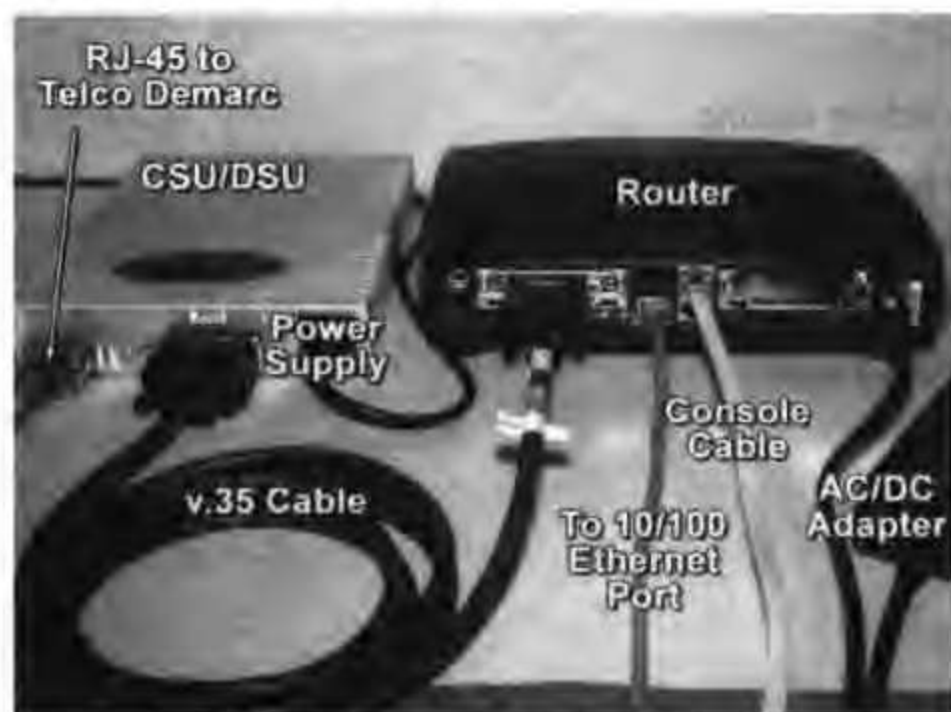


图 5-34 路由器和基带 Modem 的连接图

本案例所采用的设备和相应的模块如图 5-35~图 5-38 所示。

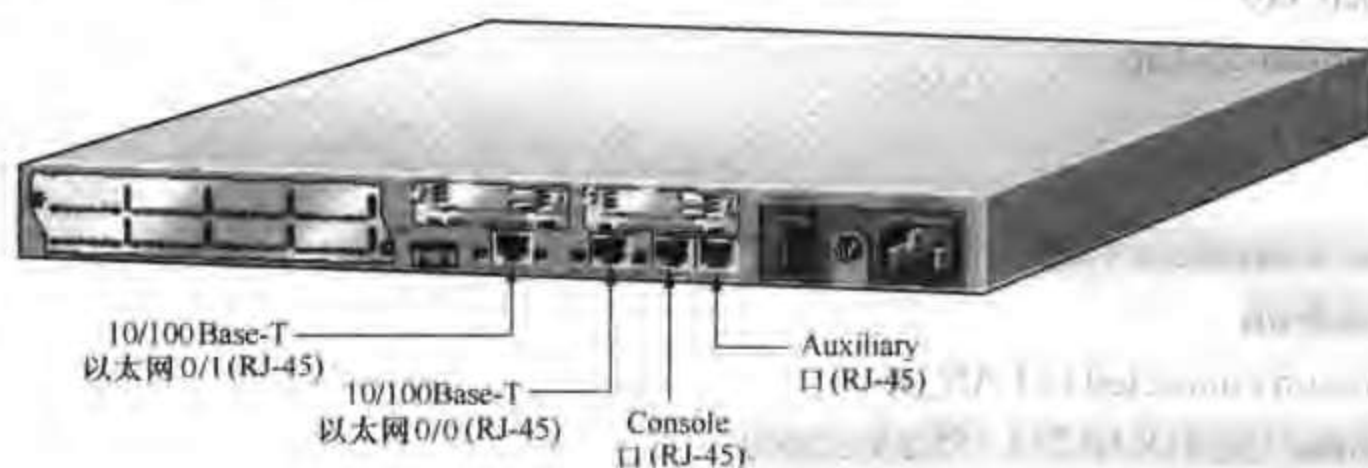


图 5-35 Cisco2621XM 路由器



图 5-36 Cisco1721 路由器



图 5-37 WIC-1T 接口卡



图 5-38 CAB-V35MT 线缆

配置文档:

(1) 路由器 A

!

service timestamps debug uptime

service timestamps log uptime

service password-encryption

no service tcp-small-servers

no service udp-small-servers

!

hostname Router_A

!

enable password cisco

!

no ip name-server

!

ip subnet-zero

no ip domain-lookup

ip routing

!

interface FastEthernet 0/0

no shutdown

description connected to LAN_A

ip address 192.168.10.254 255.255.255.0

keepalive 10


```
!
interface FastEthernet 0/1
  no description
  no ip address
  shutdown
!
```

```
interface Serial 0/0
```

```
  no shutdown
```

```
  no description
```

```
  no ip address
```

! ---配置链路层封装协议为“frame-relay”:

```
  encapsulation frame-relay
```

! ---配置帧中继的信令为“ansi”，主要信令包括“cisco”“ansi”和“q933a”，具体采用哪种信令，要咨询线路提供商:

```
  frame-relay lmi-type ansi
```

```
!
```

! ---进入子接口配置模式，并指定子接口为点到点链路“point-to-point”:

```
interface Serial 0/0.1 point-to-point
```

```
  no shutdown
```

```
  description connected to Router_B
```

```
  ip address 192.168.1.1 255.255.255.252
```

! ---设置子接口的 dlcI 号，并指定封装格式为“ietf”，默认封装格式为“cisco”，如果对接设备都是 Cisco 公司的产品，我们通常设为“cisco”，如果是不同厂家的产品，我们建议采用“ietf”的封装格式:

```
  frame-relay interface-dlci 101 ietf
```

```
!
```

```
interface Serial 0/0.2 point-to-point
```

```
  no shutdown
```

```
  description connected to Router_C
```

```
  ip address 192.168.1.5 255.255.255.252
```

```
  frame-relay interface-dlci 102 ietf
```

```
!
```

```
ip classless
```

```
!
```

```
! IP Static Routes
```

```
ip route 192.168.11.0 255.255.255.0 Serial 0/0.1 1
```

```
ip route 192.168.12.0 255.255.255.0 Serial 0/0.2 1
```

```
no ip http server
```

```
snmp-server community public RO
```



```
no snmp-server location
```

```
no snmp-server contact
```

```
!
```

```
line console 0
```

```
exec-timeout 0 0
```

```
password cisco
```

```
login
```

```
!
```

```
line vty 0 4
```

```
password cisco
```

```
login
```

```
!
```

```
(2) 路由器 B
```

```
!
```

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
service password-encryption
```

```
no service tcp-small-servers
```

```
no service udp-small-servers
```

```
!
```

```
hostname Router_B
```

```
!
```

```
enable password cisco
```

```
!
```

```
no ip name-server
```

```
!
```

```
ip subnet-zero
```

```
no ip domain-lookup
```

```
ip routing
```

```
!
```

```
interface FastEthernet 0
```

```
no shutdown
```

```
description connected to LAN_B
```

```
ip address 192.168.11.254 255.255.255.0
```

```
keepalive 10
```

```
!
```

```
interface Serial 0
```

```
no shutdown
```

```
no description
```



```

no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
!
interface Serial 0.1 point-to-point
no shutdown
description connected to Router_A S0/0.1
ip address 192.168.1.2 255.255.255.252
frame-relay interface-dlci 100 ietf
!
ip classless
!
! IP Static Routes
ip route 192.168.10.0 255.255.255.0 Serial 0.1 1
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
(3) 路由器 C
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_C
!
enable password cisco

```



```

!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0
  no shutdown
  description connected to LAN_C
  ip address 192.168.12.254 255.255.255.0
  keepalive 10
!
interface Serial 0
  no shutdown
  no description
  no ip address
  encapsulation frame-relay
  frame-relay lmi-type ansi
!
interface Serial 0.1 point-to-point
  no shutdown
  description connected to Router_A S0/0.2
  ip address 192.168.1.6 255.255.255.252
  frame-relay interface-dlci 100 ietf
!
ip classless
!
! IP Static Routes
ip route 192.168.10.0 255.255.255.0 Serial 0.1 1
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login

```



```

!
line vty 0 4
  password cisco
  login
!
end

```

5.3.4 数字电路

1. 简介

数字电路业务是一种直接在电信传输网上进行数字信号传送的业务，是基于准同步数字传输网络（PDH）、同步数字传输网络（SDH）等先进光纤数字传输技术组建的宽带核心传送网络，利用各种新的传输技术进行高速数字信号传送的业务。该业务可向用户提供 2 Mbit/s~2.5Gbit/s 各种传输速率的全透明电路，为客户提供高效的信息传送通路。

注意：数字电路接入是指不依赖 CHINADDN、CHINAFRN 等电信业务网，而是直接通过电信传输网络进行数据的传输。

数字电路为用户提供端到端的全透明高速数字信号传送服务。它具有如下的特点：

- （1）它使用国际通用的 G.703、STM-1 等标准接口；
- （2）通信速率可根据需要进行选择，有 2Mbit/s、8Mbit/s、34Mbit/s、155Mbit/s、622Mbit/s、2.5Gbit/s 等速率；
- （3）数字电路是一种全透明的物理通道，支持数提、语音、图像等多种业务，对客户通信协议没有任何要求，客户可自由选择网络设备及通信协议；
- （4）数字电路传输质量高，网络时延小，实时性强；
- （5）数字电提技术成熟，拥有完善的网络管理监信性能和各种网络保护机制，具有很高的安全可靠性能；
- （6）数字电路传输网络（PDH、SDH）覆盖面广，可通达国内外主要城市；
- （7）数字电路价格低，性能价格比优。

申请数字电路的具体手续，可到各地电信的数据业务营业处查询，或拨打电信服务热线 1000 进行咨询。数字电路的收费情况见表 5-11 和表 5-12。

表 5-11 国内数字电路月租费（单位：元/月）

速率	本地营业区内	本地营业区间	国内长途
2Mbit/s	2000	4000	6000
8Mbit/s	6000	11000	17000
34Mbit/s	16000	31000	47000
155Mbit/s	44000	88000	132000
622Mbit/s	123000	247000	370000
2.5Gbit/s	344000	688000	1033000

表 5-12 国际数字电路月租费（单位：元/月）

速率	中国港、澳、台地区	亚洲各国	欧、美、澳、非各国
2Mbit/s	20000	100000	100000
8Mbit/s	56000	280000	280000
34Mbit/s	180000	780000	780000
45Mbit/s	210000	900000	900000
155Mbit/s	440000	2200000	2200000
622Mbit/s	1230000	6150000	6150000
2.5Gbit/s	3440000	17210000	17210000

说明：表 5-11 和表 5-12 中的费用为参考费用，具体费用请咨询当地电信部门。

2. E1 介绍

E1 线路是数字电路的一种，接入速率为 2Mbit/s，CE1 是通道化的 E1，就是把 2Mbit/s 的传输分成了 32 个 64kbit/s 的时隙，其中最多可有 31 个信道承载数据。通常 E1 线路有三种使用方法，一是将整个 2Mbit/s 用作一条链路，如 DDN 2Mbit/s；二是将 2Mbit/s 用作若干个 64kbit/s 及其组合，如 128Kbit/s，256kbit/s 等，这就是 CE1；三是用作语音交换机的数字中继，这也是 E1 最本来的用法，是把一条 E1 作为 32 个 64kbit/s 来用，但是时隙 0 和时隙 15 是用作传输信令的，所以一条 E1 可以传 30 路语音。PRI 就是其中的最常用的一种接入方式，标准叫 PRA 信令。

电信部门可提供 E1 和 CE1 两种线路，但一接用户用到的 E1 线路都是 CE1，除非你特别说明要使用 E1，CE1 可以当 E1 用，但 E1 却不可以作 CE1。

E1 的接口分为平衡和非平衡两种，平衡是指两条输出端信号全部输出，是 120Ω；而非平衡的两条输出端信号只有一条输出，而另一条则接地，是 75Ω。从外观上看，平衡电接在路由器端为 DB-15（公）连接器，在网络端是 RJ-45 连输器（如图 5-40 所示的 CAB-E1-PRI）；非平衡电缆在路由器端为 DB-15（公）连接器，在网络端是 BNC 头（如图 5-39 所示的 CAB-E1-ENC）。

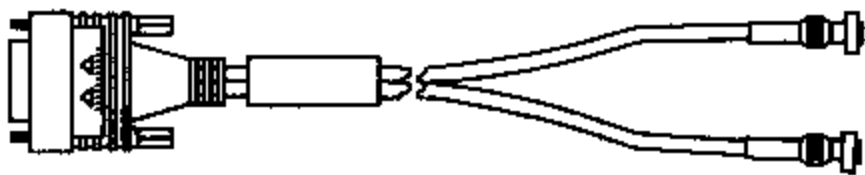


图 5-39 CAB-E1-BNC 线缆



图 5-40 CAB-E1-PRI 线缆

3. 典型应用

数字电路适用于任何高速率、信息量大、实时性强的信息传送，可广泛用于银行、证券、教育、ISP 等大信息量传送的行业，也适用于任何局域网之间的高速互连，以及会议电接、远程输育、远程医疗等实时性强的话音多媒体的传送。目前在国内数字电路主要应用在如下几方面：

- （1）网络互连：用户利用数字电路将多个地点的计算机网络互连，组成跨区域的广域网络。用户既可直接采用接字电路 G.703 接口进行网络互连，也可以通过加装 V.35 或 10M 以太网接口转换器进行网络间的连输。
- （2）连接互联网络：用户可通过把接字电路连接到互联网服务供应商的接入服务器中，

实现用户高速互联网专线接入。

(3) 视频信号传送：数字电路高速稳定的传输特性、优异性能价格比是组建视频电视会议、实时图像监控系统的最佳选择。

典型的数字电路组网的网络拓扑结构如图 5-41 所示。

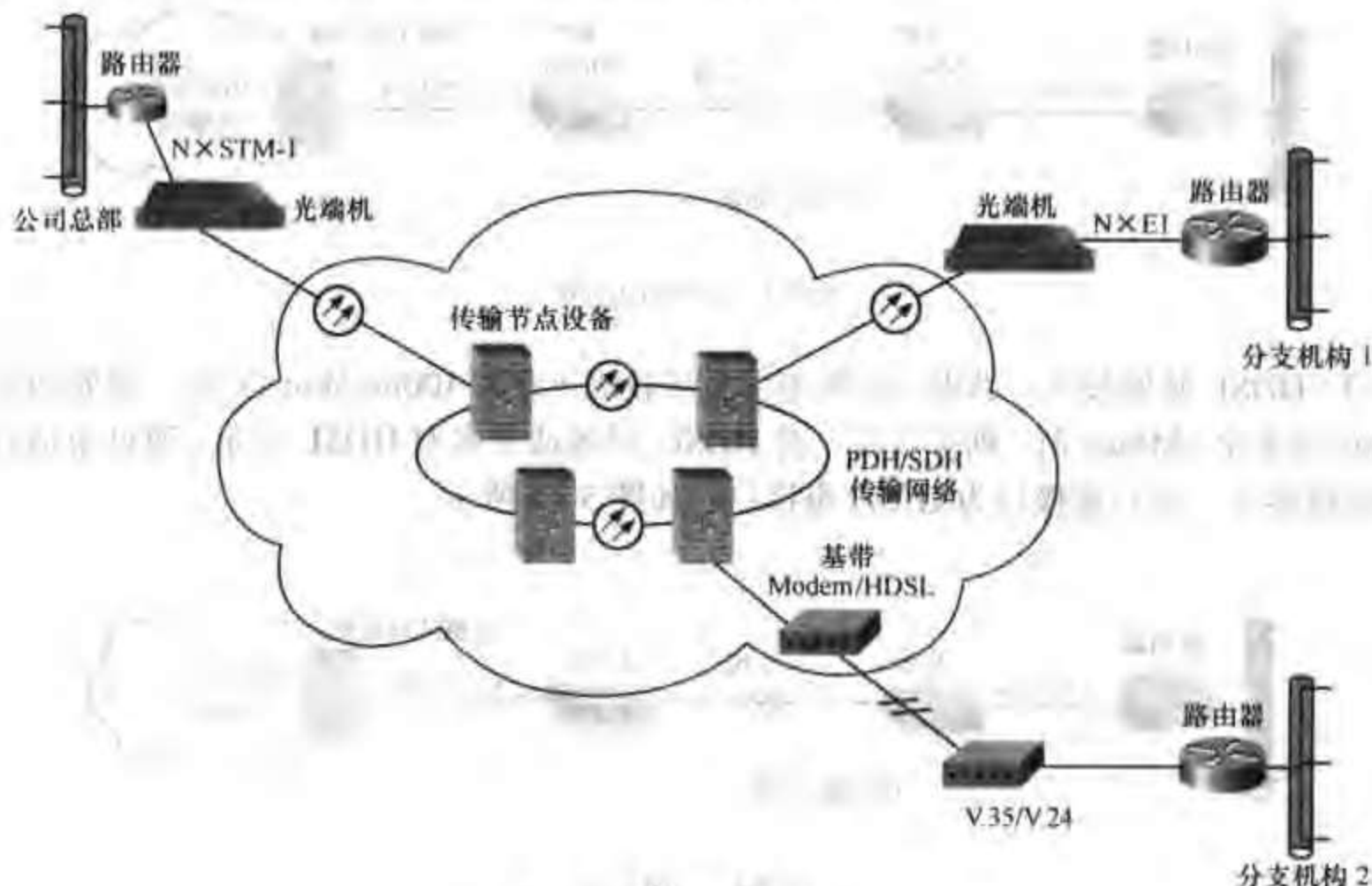


图 5-41 数字电路典型应用

一般用户的总部或地市分部如果汇集的电路数比较多，带宽需求较大，则建议首选采用以数字电路方式就近接入节点的方式，如果每个分支的带宽为 2Mbit/s 或 2Mbit/s 以上，这样我们在总部就必须要有更高的带宽，否则就会形成瓶颈。根据具体的情况，在总部我们可以选择多端口的 E1 模块，或采用 155Mbit/s 的 Multichannel STM-1 模块；如果每个分支的带宽为 64kbit/s、128kbit/s 等，这样我们在总部就可以采用通道化的 E1（CE1）模块。根据用户的网络规模，总部设备建议使用 Cisco 的 7500、7200 或 3700 系列的路由器。分支设备建议使用 Cisco 的 1700 或 2600 系列的路由器。

4. 用户入网方式

(1) 直接电缆线接入：当用户与电信公司的机房在同一建筑物内时（距离在 100m 以内），可以直接用同轴电缆接入。用户端接口为 G.703 电接口，接入的速率范围可以从 2~45Mbit/s。如图 5-42 所示。



图 5-42 直接电缆接入

(2) 基带 Modem 接入：当用户距离电信机房较远（通常 100m~3km 范围），需要的带宽为小于 2Mbit/s 时，则可以用一对基带 Modem 设备通过市话音频双绞线实现接入，用户端接口为 V.35 或 V.24 电接口。如图 5-43 所示。



图 5-43 基带 Modem 接入

(3) HDSL 延伸接入：当用户距离电信机房较远（通常 100m~3km 范围），需要的带宽为 2Mbit/s 或多个 2Mbit/s 时，则可以用一对 HDSL 设备或者多对 HDSL 设备，通过市话音频双绞线实现接入，用户端接口为 G.703 电接口。如图 5-44 所示。



图 5-44 HDSL 接入

(4) 光纤接入：对于带宽要求比较高、距离远（通常 3km 以外）的用户，可以将小容量的光端机直接放置在用户机房内，用光纤连接电信公司传输骨干网络，接入的总带宽取决于传输节点设备的容量。如图 5-45 所示。



图 5-45 光纤接入

5. 案例分析

案例 1

三台路由器通过 PCM 线路互联，实现三个局域网之间的通信。其拓扑图如图 5-46 所示。

说明：LAN_A（总部）采用 Cisco3725 路由器，配置 NM-1CE1U 模块，通过 2Mbit/s 线路接入传输网，从而和各分支机构互联；LAN_B、LAN_C（分支 B、C）采用 Cisco2621XM，配置 WIC-1T 串口卡，各申请 128kbit/s 线路接入传输网。

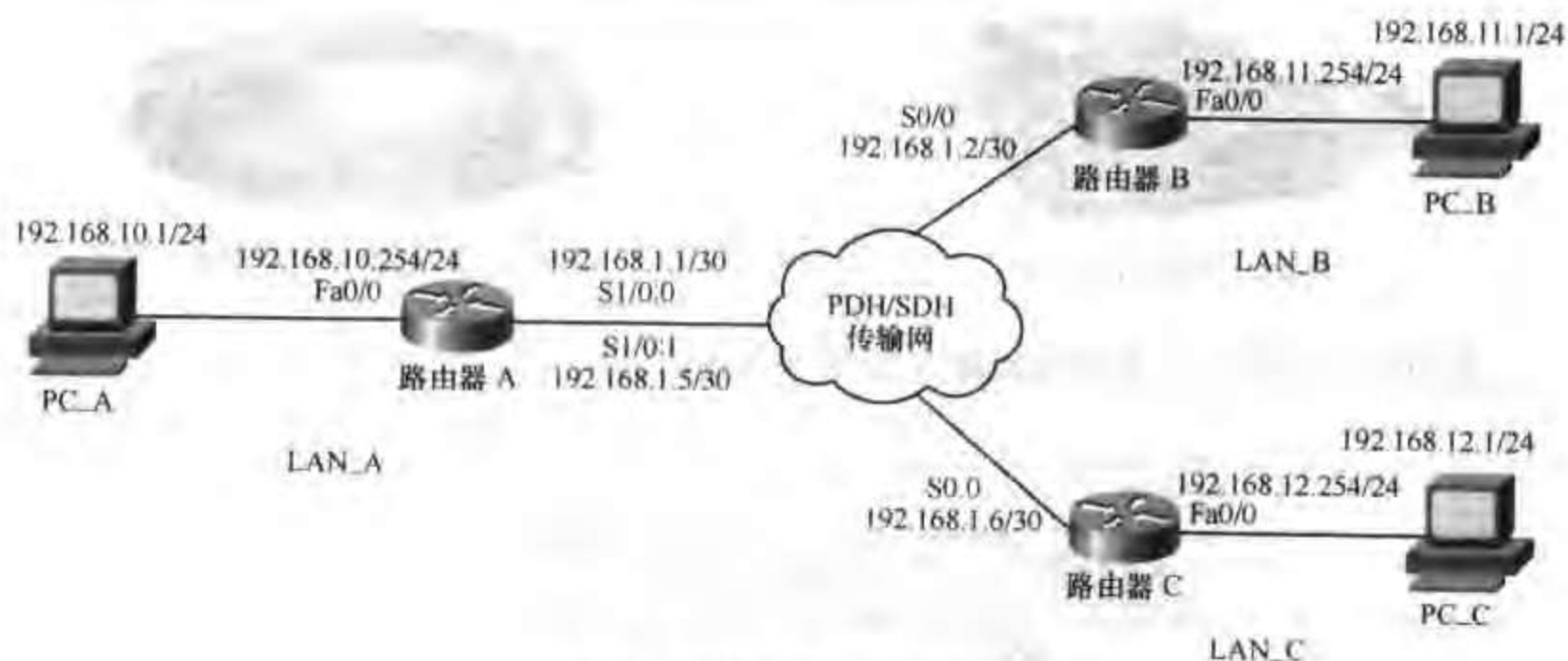
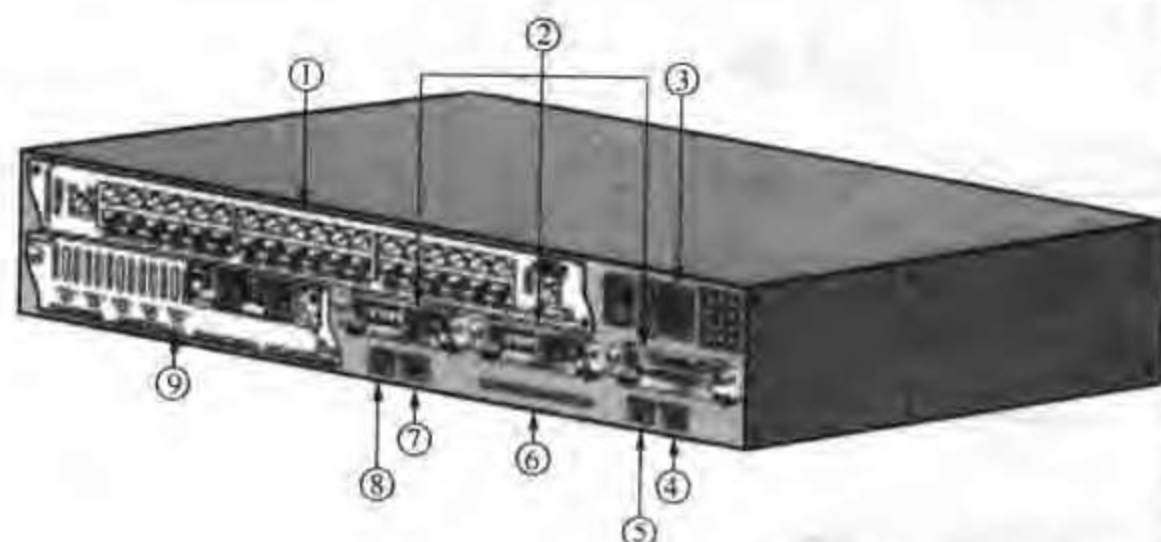


图 5-46 数字电路案例 1 的拓扑结构

本案例所采用的设备和相应的模块如图 5-47~图 5-52 所示。



1	Double-width network module slot
2	WAN Interface card slots (3 WIC slots)
3	Power supply
4	Auxiliary port
5	Console port
6	Compact Flash slot
7	Fast Ethernet 0/0
8	Fast Ethernet 0/1
9	Single-width network module slot

图 5-47 Cisco3725 路由器

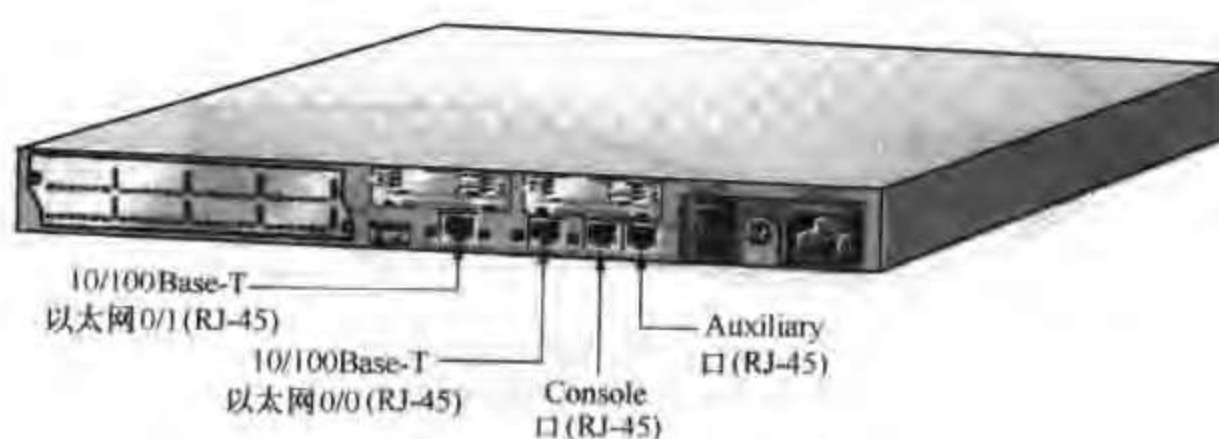


图 5-48 Cisco2621XM 路由器



图 5-49 NM-1CE1U 模块



图 5-50 CAB-E1-BNC 线缆



图 5-51 WIC-IT 接口卡



图 5-52 CAB-V35MT 线缆

本案例所采用模块的连接图如图 5-53 和图 5-54 所示。

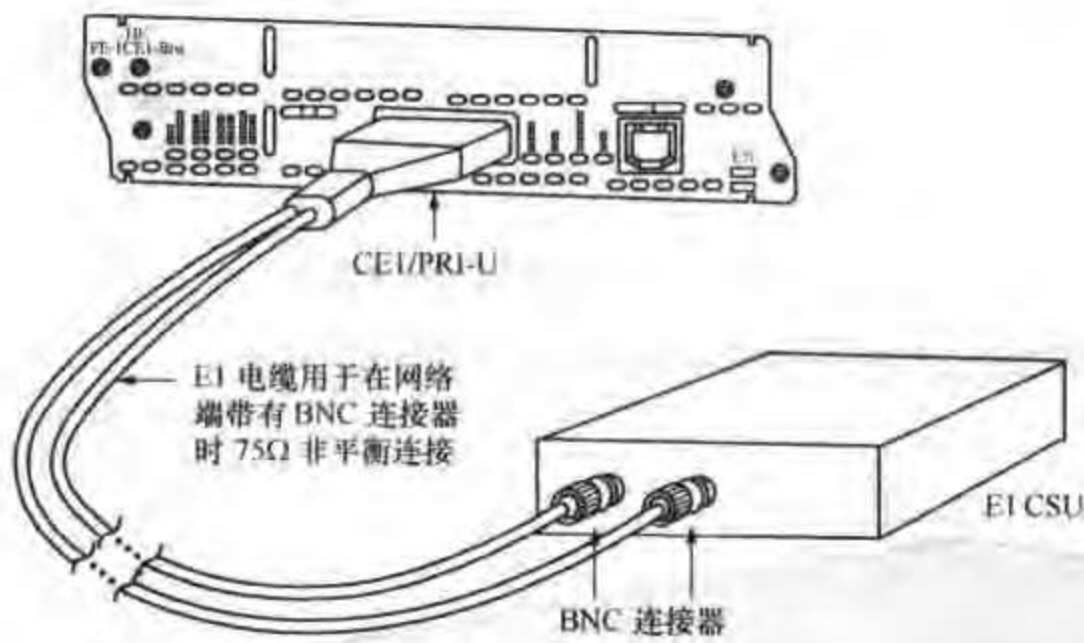


图 5-53 NM-ICEIU 模块连接图

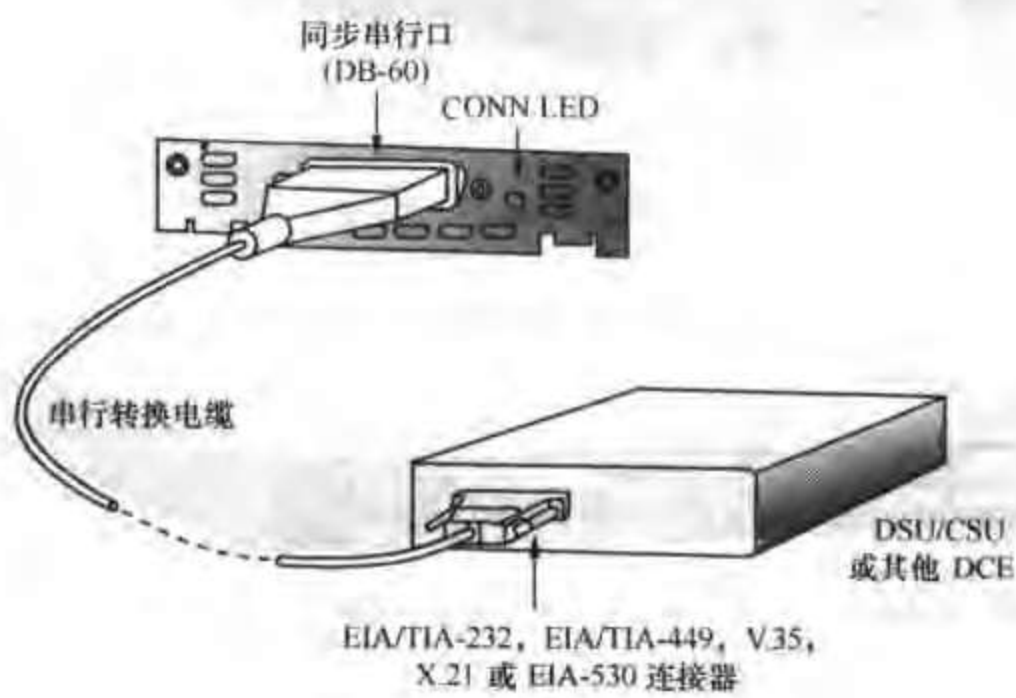


图 5-54 WIC-IT 模块连接图

配置文档

(1) 路由器 A

!

```
service timestamps debug uptime
service timestamps log uptime
service password-encryption
```



```

no service tcp-small-servers
no service udp-small-servers
!
hostname Router_A
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0/0
  no shutdown
  description connected to LAN_A
  ip address 192.168.10.254 255.255.255.0
  keepalive 10
!
interface FastEthernet 0/1
  no description
  no ip address
  shutdown
!
!
! ---进入 E1 卡配置模式:
controller e1 1/0

```

! ---配置 CE1/PRI 接口的帧校验格式, 不进行帧校验为 “no-crc4”, 采用 4 字节 CRC 校验为 “crc4” 具体采用哪一种格式请咨询线路提供商:

```
framing no-crc4
```

! ---进行时隙的划分, 这里将 1、2 时隙捆绑为 “0” 组, 3、4 时隙捆绑为 “1” 组, “0” 和 “1” 组分别对应下面的虚拟串口 “Serial 1/0:0” 和 “Serial 1/0:1”:

```
channel-group 0 timeslot 1-2
```

```
channel-group 1 timeslot 3-4
```

```
!
```

```
!
```

```
interface Serial 1/0:0
```

```
no shutdown
```

```
description connected to Router_B
```



```

encapsulation ppp
ip address 192.168.1.1 255.255.255.252
!
interface Serial 1/0:1
no shutdown
description connected to Router_C
encapsulation ppp
ip address 192.168.1.5 255.255.255.252
!
ip classless
!
! IP Static Routes
ip route 192.168.11.0 255.255.255.0 Serial 1/0:0 1
ip route 192.168.12.0 255.255.255.0 Serial 1/0:1 1
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
(2) 路由器 B
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_B
!
enable password cisco

```



```

!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0/0
no shutdown
description connected to LAN_B
ip address 192.168.11.254 255.255.255.0
keepalive 10
!
interface Serial 0/0
no shutdown
description connected to Router_A S1/0:0
encapsulation ppp
ip address 192.168.1.2 255.255.255.252
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 0/0 1
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
(3) 路由器 C
!

```



```

service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_C
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0/0
  no shutdown
  description connected to LAN_C
  ip address 192.168.12.254 255.255.255.0
  keepalive 10
!
interface Serial 0/0
  no shutdown
  description connected to Router_A S1/0:1
  encapsulation ppp
  ip address 192.168.1.6 255.255.255.252
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 0/0 1
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0

```



```

password cisco
login
!
line vty 0 4
password cisco
login
!

```

案例 2

ISDN、模拟 Modem 均可拨号连接 LAN。其拓扑图如图 5-55 所示。

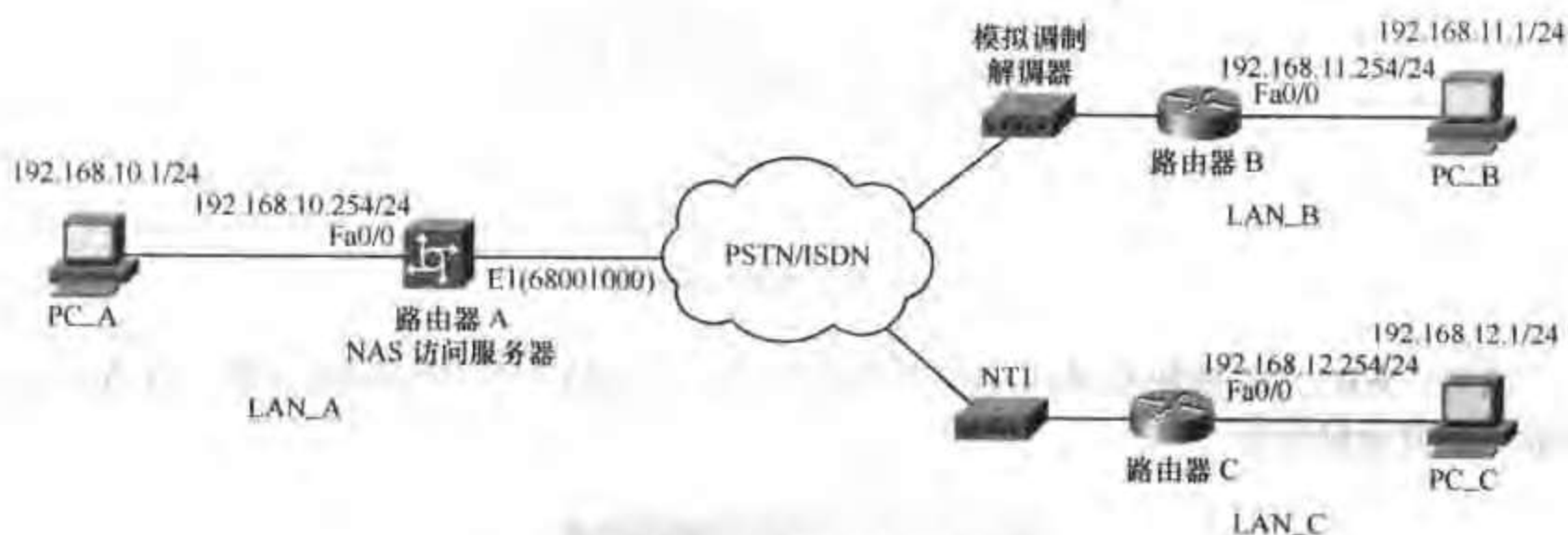


图 5-55 数字电路案例 2 的拓扑结构

说明：LAN_A（总部）采用 Cisco3725 路由器，配置 NM-1CE1U 模块，通过 2M PRI 线路接入 PSTN 网，用于各分支机构的拨入，可支持模拟信号和数字信号的拨入；LAN_B（分支 B）采用 Cisco2621XM，配置 WIC-1AM 接口卡，LAN_C（分支 C）采用 Cisco2621XM，配置 WIC-1B-S/T 接口卡。

本案例所用设备同案例 1，所用不同的模块如图 5-56~图 5-59 所示。



图 5-56 NM-30DM 模块



图 5-57 NM-1CE1U 模块



图 5-58 WIC-1AM 接口卡



图 5-59 WIC-1B-S/T 接口卡

新采用模块的连接方式如图 5-60 和图 5-61 所示。

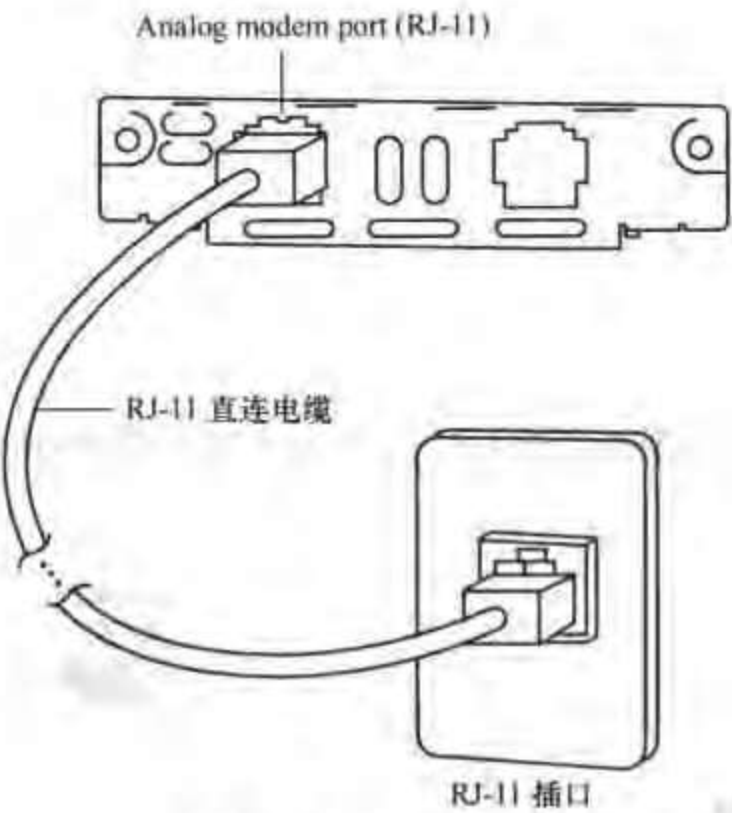


图 5-60 WIC-1AM 连接示意图

说明：WIC-AM 模块和 WIC-A/S 模块的区别在于 AM 已内置调制解调器，而 A/S 需要外接一个调制解调器。

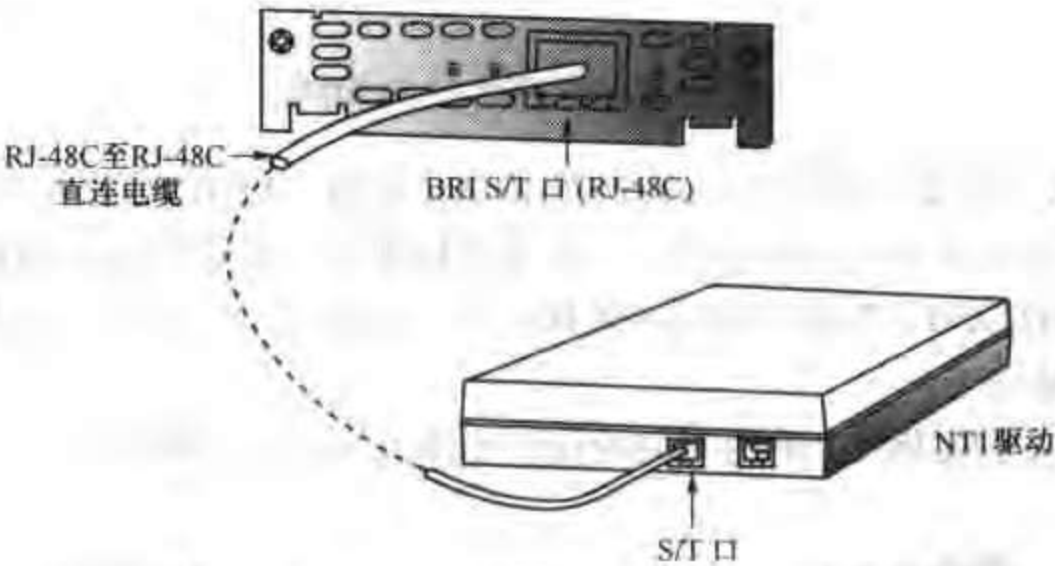


图 5-61 WIC-1B-S/T 连接示意图

配置文档：

(1) 路由器 A

！

```
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
```

！

```
hostname Router_A
```



```
!  
enable password cisco  
!---定义本地认证数据库:  
username Router_C password cisco  
username Router_B password cisco  
!  
no ip name-server  
!  
!---指定 ISDN PRI 的线路类型为“primary-net5”，具体类型请咨询线路提供商:  
isdn switch-type primary-net5  
!  
ip subnet-zero  
no ip domain-lookup  
ip routing  
!  
controller EI 1/0  
no shutdown  
framing no-crc4  
!---指定 ISDN PRI 的线路编码格式为“hdb3”，具体格式请咨询线路提供商:  
linecode hdb3  
!---把 PRI 接口划分为 31 个信道，其中第 16 个信道（对应逻辑接口 Serial0/0:15）是管理信道:  
pri-group timeslots 1-31  
!  
!---进入逻辑接口 Serial0/0:15（管理信道）:  
interface Serial1/0:15  
no shutdown  
description connected to Router_C  
ip unnumbered FastEthernet0/0  
encapsulation ppp  
!---指定本接口属于拨号组 1，注意组号和下面定义的“dialer-list 1”对应:  
dialer-group 1  
isdn switch-type primary-net5  
!---将模拟 Modem 呼叫转接到内部数字 Modem 来处理:  
isdn incoming-voice modem  
!---为拨入的 ISDN 呼叫从地址池“isdnpool”中分配 IP 地址:  
peer default ip address pool isdnpool  
!---指定 PPP 的认证方式，这里采用“pap”方式:  
ppp authentication pap
```


!

!--建立一个异步拨号组，用于接收模拟 Modem 呼叫:

```
interface Group-Async1
```

```
ip unnumbered FastEthernet0/0
```

```
encapsulation ppp
```

!--为异步串口指定建立链路的方式，默认值是“dedicate”。可以有两种建立链路的方式：①直接方式（Dedicate）：拨号成功之后，直接采用链路层协议配置参数建立链路；②交互方式（Interactive）：拨号成功之后，主叫方向对端发送配置命令（与用户从远端手工键入配置命令效果相同），设置对端的链路层协议工作参数，然后建立链路。比较常用的是直接方式，但在与同样支持交互方式的路由器（如 Cisco 路由器等）互连时，采用交互方式显得更为灵活。

```
async mode interactive
```

!--为拨入的模拟呼叫从地址池“pstnpool”中分配 IP 地址:

```
peer default ip address pool pstnpool
```

!--指定 PPP 的认证方式，这里采用“pap”方式:

```
ppp authentication pap if-needed
```

!--指定此模拟拨号组对应的端口:

```
group-range 33 62
```

!

```
interface FastEthernet 0/0
```

```
no shutdown
```

```
description connected to LAN_A
```

```
ip address 192.168.10.254 255.255.255.0
```

!

```
interface FastEthernet 0/1
```

```
no description
```

```
no ip address
```

```
shutdown
```

!

!

```
! Dialer Control List 1
```

!

!--为拨号组 1 指定激活拨号的条件，这里所有的 IP 接入都可以激活拨号:

```
no dialer-list 1
```

```
dialer-list 1 protocol ip permit
```

!

!--为数字和模拟拨入用户定义地址池:

```
ip local pool isdnpool 192.168.10.201 192.168.10.220
```

```
ip local pool pstnpool 192.168.10.221 192.168.10.240
```



```

!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
! ---进入 Modem 口线模式:
line 33 62
! ---配置为自动登录:
  autoselect during-login
! ---配置为自动选择 PPP 协议:
  autoselect ppp
! ---配置为使用本地数据库进行认证:
  login local
! ---配置端口为允许拨入和拨出:
  modem InOut
! ---自动识别 modem:
  modem autoconfigure discovery
! ---连通后自动执行 ppp 命令:
  autocommand ppp default
!
(2) 路由器 B
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!

```



```
hostname Router_B
!
enable password cisco
username Router_A password cisco
!
! ---定义拨号脚本“dialout”:
chat-script dialout "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30 CONNECT <
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0/0
no shutdown
description connected to LAN_B
ip address 192.168.11.254 255.255.255.0
ip nat inside
!
interface FastEthernet 0/1
no description
no ip address
shutdown
!
! ---进入异步接口配置模式:
interface async 1
description connected to Router_A
! ---自动协商来从远端获得地址:
ip address negotiated
encapsulation ppp
async mode interactive
! ---设定接口为按需拨号 (DDR):
dialer in-band
! ---指定拨号串,“68001000”为拨入远端所需的电话号码:
dialer string 68001000
dialer-group 1
ppp authentication pap
! ---向远端发送认证需要的用户名和密码:
```



```

ppp pap sent-username Router_B password cisco
ip nat outside
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
ip nat inside source-list 1 interface async 1 overload
!
access-list 1 permit any
!
ip route 0.0.0.0 0.0.0.0 async 1
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
line 1
  autoselect during-login
  autoselect ppp
  modem InOut
  modem autoconfigure discovery
  autocommand ppp
! ---指定拨出所用的脚本“dialout”:
script dialer dialout
transport input all
flowcontrol hardware

```


!

(3) 路由器 C

!

service timestamps debug uptime

service timestamps log uptime

service password-encryption

no service tcp-small-servers

no service udp-small-servers

!

hostname Router_C

!

enable password cisco

username Router_A password cisco

!

no ip name-server

!

isdn switch-type basic-net3

!

ip subnet-zero

no ip domain-lookup

ip routing

!

!

interface FastEthernet 0/0

no shutdown

description connected to LAN_C

ip address 192.168.12.254 255.255.255.0

ip nat inside

!

interface FastEthernet 0/1

no description

no ip address

shutdown

!

interface BRI 0/0

no shutdown

description connected to Router_A

ip address negotiated

isdn switch-type basic-net3


```
encapsulation ppp
dialer in-band
dialer string 68001000
dialer-group 1
ppp authentication pap
ppp pap sent-username Router_C password cisco
no cdp enable
ip nat outside
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
ip nat inside source-list 1 interface bri 0/0 overload
!
access-list 1 permit any
!
ip route 0.0.0.0 0.0.0.0 bri 0/0
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
```

5.3.5 ISDN

1. 简介

ISDN (Integrated Service Digital Network) 是综合业务数字网的简称,它是基于公共电话

网的全数字网络,利用普通的电话线,可开展各种业务,例如打电话、发传真、上网、局域网互连、开会议电视、专线备份等。

ISDN 的业务覆盖了现有各种通信网的全部业务。它通过现有的电话线,不仅可以提供电话业务,还能提供传真、数据、图像等多种多样的新业务,因此,ISDN 也被形象地称为“一线通”。“一线通”可以在一条电话线上连接 8 部相同或不同的通信终端,并能使两部终端同时使用,如一部上网,另一部用来打电话;一部用来打电话,另一部用来发传真……。ISDN 还可以用于会议电视、DDN 专线备份、局域网互连等,而且“一线通”的速度更快,质量更高。综合业务数字网有窄带(N-ISDN)和宽带(B-ISDN)之分,目前我们所说的“一线通”指的是在 N-ISDN 上提供的业务。

ISDN 可以向用户提供两种接口,它们是基本速率接口(BRI)和一次群速率接口(PRI)。基本速率接口包括两个能独立工作的 B 信道(64kbit/s)和一个 D 信道(16kbit/s),可提供速率为 128kbit/s 的通信;一次群速率接口则可提供速率为 2.048Mbit/s 的通信。其中, B 信道用来传输话音、数据和图像, D 信道用来传输信令或分组信息。

ISDN 与现在使用的模拟电话相比,它的优点可以概括为简单、方便、快捷、灵活和高质量,这表现在下面几点:

(1) 综合的通信业务:一条电话线可当两条用:可以同时使用两部电话;在上网的同时拨打、接收电话、收发传真;还可以使用两台计算机同时上网。通过配置适当的终端设备,也可以实现可视电话或会议电视功能,即使用户双方远隔千里,其音容笑貌却就在眼前。

(2) 呼叫连接速度快:现在人们上 Internet 网浏览通常采用的是模拟电话线和 Modem,模拟电话线传送速率低,传输质量差,在数据传送时尤为如此。而 ISDN 则改变了这一情况,呼叫连接速度更快,用户线的传输速率是 64kbit/s 或 128kbit/s,一般如果我们使用的是模拟 Modem,从拨号至最后连接到网上可以进行浏览,约需要 20s 左右,同时伴有刺耳的拨号声,而 ISDN 进行拨号仅仅需要 1s。

(3) 传输质量高:ISDN 由于采用端到端数字传输,即从用户终端到对方用户终端之间全部是数字传输,传输质量明显提高。接收用户端声音失真很小,而数据传输的比特误码特性比电话线路至少改善了 10 倍。

(4) 使用灵活方便:我们只需使用一个入网接口,使用普通电话号码,就能从网络得到多种服务。用户在这个接口上可以连接各种不同种类的终端,而且统一的接口使终端设备像家用电器一样可以方便地在不同的地点之间搬动。

(5) 费用适宜:由于使用单一网络来提供多种业务,提高了网络资源的利用,可以以低廉的费用向用户提供服务;而用户不必购买和安装不同的设备和线路来接入不同的网络,只需要一个接口就能够实现各种业务,大大节省了投资。

2. ISDN 的用户—网络接口规范

在 ITU-T I.411 建议中,根据功能群(用户接入 ISDN 所需的一组功能)、参考点(用来区分功能群的概念上的点)的概念,提出了 ISDN 用户—网络接口的参考配置。

功能群分为:

NT1: 主要实现物理层的功能,包括提供传输功能、环路测试等等;

TE1: TE1 是符合 ISDN 网络接口标准的用户终端设备,可直接与 NT1 连接,如数字话

机、BRI 接口的路由器等；

TA：完成适配功能，将非 ISDN 标准的终端（TE2）接入 ISDN；

TE2：TE2 是不符合标准的终端设备，需经过一个终端适配器 TA 才能接入 NT1，如模拟电话、模拟 Modem、计算机等；

参考点分为：

U：靠近网络侧的接口，是网络的边界；

S/T：标准的 ISDN 接口；

R：非 ISDN 标准终端（TE2）与终端适配器（TA）之间的接口。

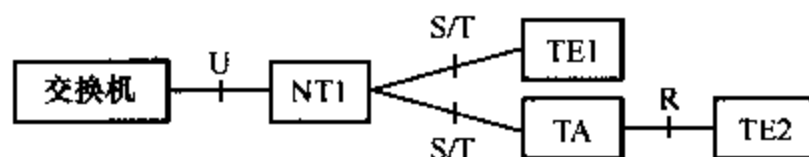


图 5-62 ISDN 用户—网络接口规范图

ISDN 的用户—网络接口规范如图 5-62 所示。

3. 典型应用

ISDN 可向用户提供各种各样的业务。目前 CCITT（现在的 ITU）将 ISDN 业务分为三类：承载业务、用户终端业务和补充业务。

（1）承载业务

承载业务是 ISDN 提供的信息传送业务。常用的承载业务有：话音业务、3.1kHz 音频业务和不受限 64kbit/s 数字业务。打电话时一般采用话音业务。3.1kHz 音频承载业务主要用于用调制解调器进行数据传输或用模拟传真机发传真的情况。若要使用 ISDN 拨号上网，则需要用不受限 64kbit/s 数字业务。

（2）用户终端业务

用户终端业务是指所有面向用户的应用业务，它既包含了网络的功能，又包含了终端设备的功能。用户可以使用电话、4 类传真、数据传输、会议电视等用户终端业务，但均需要终端设备的支持。

（3）补充业务

补充业务则是 ISDN 在承载业务和用户终端业务的基础上提供的其他附加业务，目的是为了给用户提供更方便的服务。

目前常见的补充业务有：多用户号码、主叫号码显示、呼叫等待、呼叫保持等。当然，用户首先需要到电信局去申请这些业务。这些业务确实可给用户带来很大的方便。例如，呼叫等待业务可以使在两个电话同时使用时，外面的电话还能打进来。呼叫保持则使用户在打电话时，将现有的电话暂时挂起，去打新的电话或接听其他电话，结束后再将原来的电话恢复。而多用户号码使用户的一根 ISDN 电话线可以有两个或几个不同的电话号码，用户可以把一个号码用于传真，另一个用于电话。

目前，ISDN 作为一种数据业务主要用于企业网广域骨干链路的备份，以及超小型企业或家庭用户的 Internet 接入。ISDN 的典型应用如图 5-63 所示。

4. 用户接入方式

ISDN 可以向用户提供两种接口，它们和基本速率接口（BRI）和一次群速率接口（PRI）。基本速率接口包括两个能独立工作的 B 信道（64kbit/s）和一个 D 信道（16kbit/s），可提供速率为 128kbit/s 的通信，如图 5-64 所示。一次群速率接口则可提供速率为 2.048Mbit/s 的通信。其中 B 信道用来传输语音、数据和图像，D 信道用来传输信令或分组信息，如图 5-65 所示。

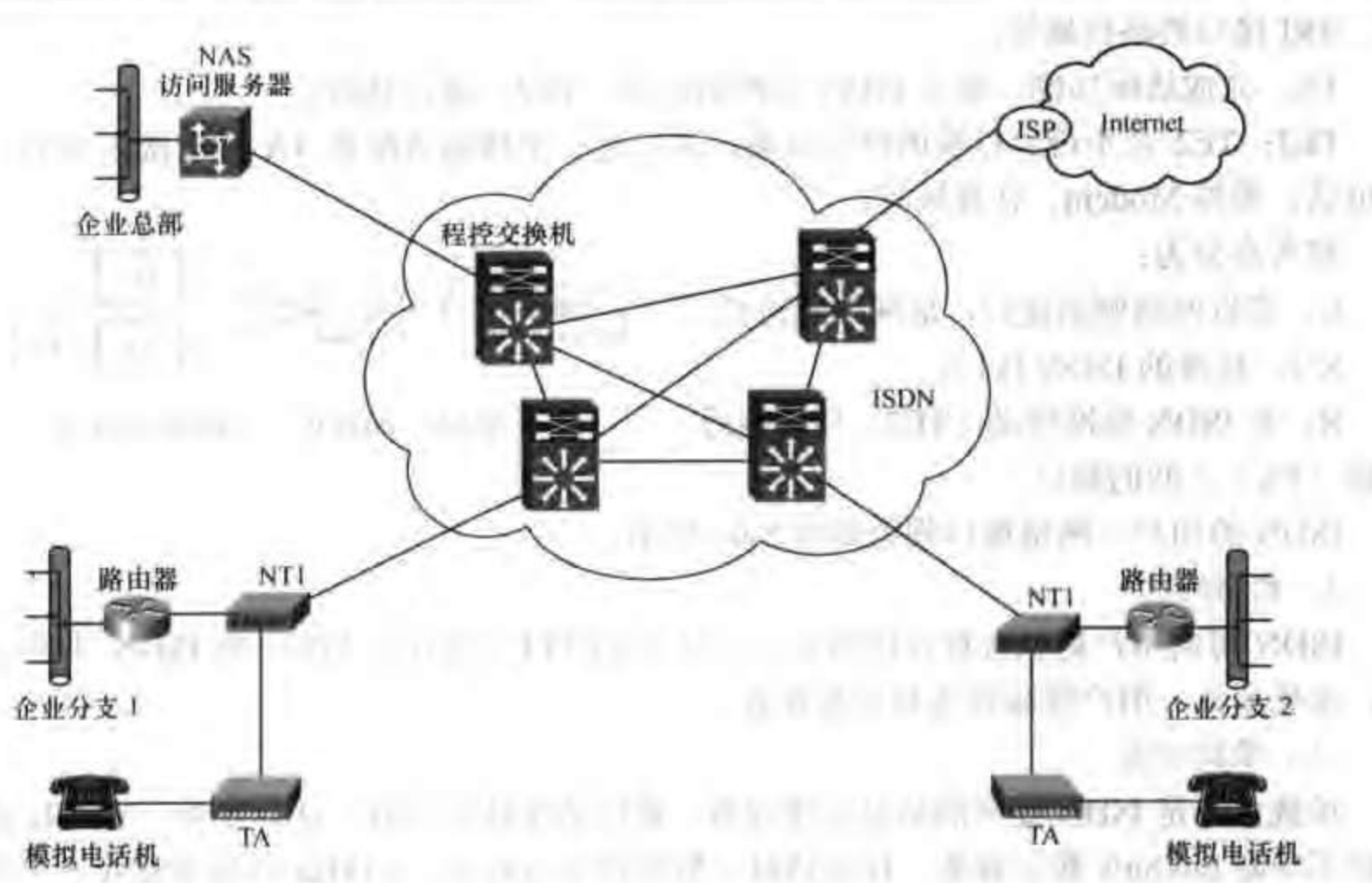


图 5-63 ISDN 典型应用

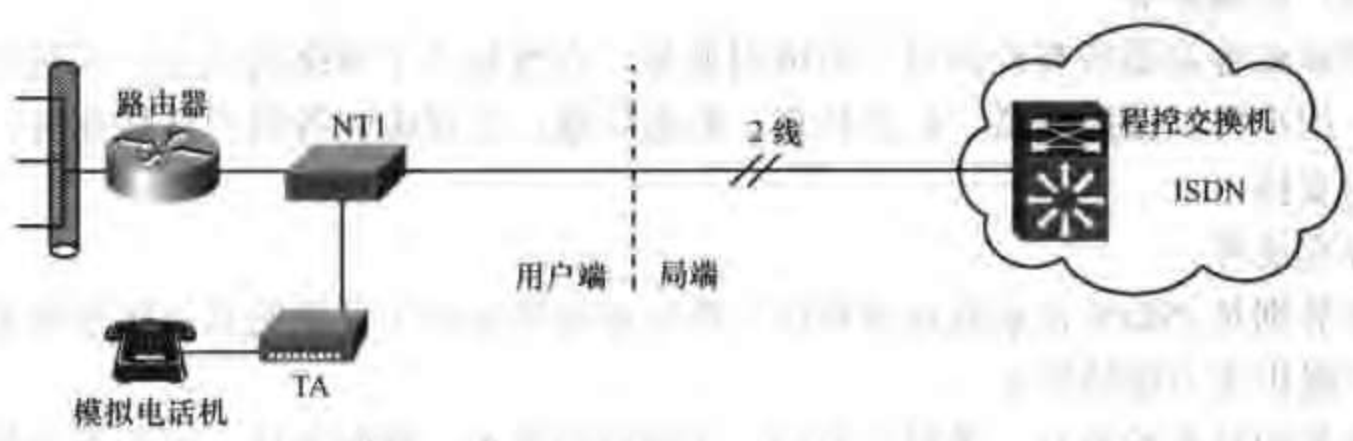


图 5-64 ISDN BRI 接入



图 5-65 ISDN PRI 接入

5. 案例分析

案例 1

两局域网通过 ISDN 互连，其拓扑结构如图 5-66 所示。

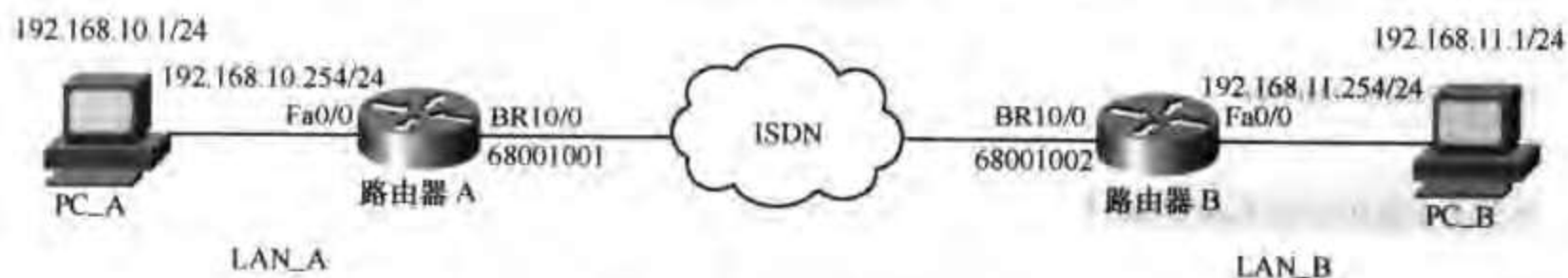


图 5-66 ISDN 案例 1 的拓扑结构

说明：Router_A 和 Router_B 都采用 Cisco2621XM 路由器，配置 WIC-1B-S/T 接口卡，LAN_A 和 LAN_B 通过 ISDN 互连。

WIC-1B-S/T 和 NT1 的连接方式如图 5-67 所示。

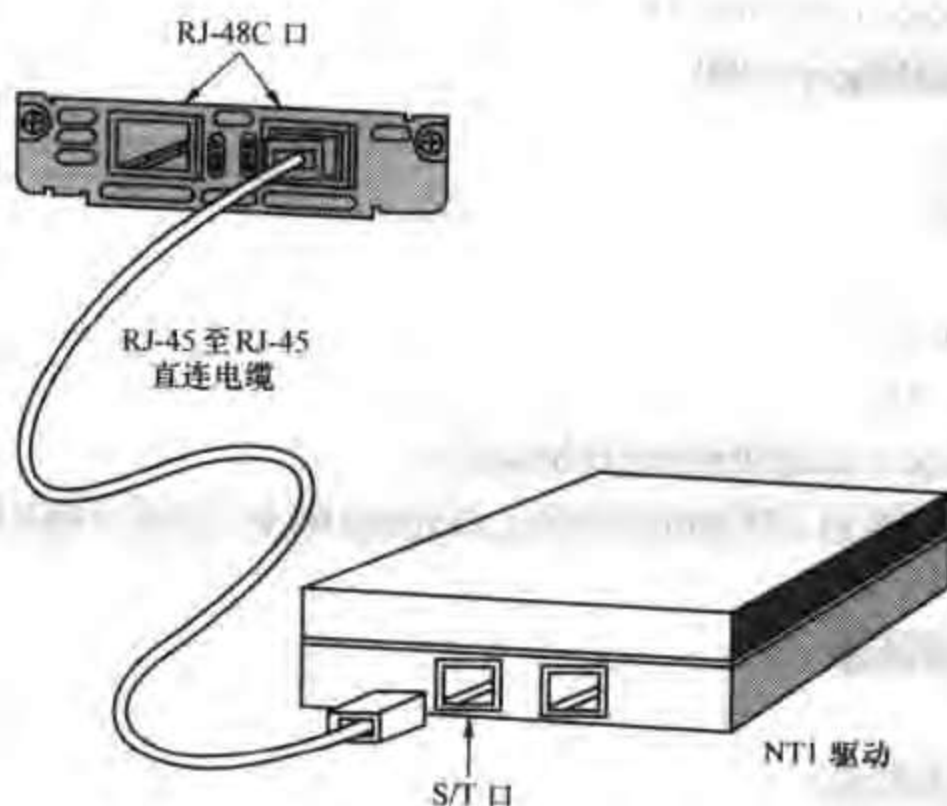


图 5-67 WIC-1B-S/T 和 NT1 的连接示意图

配置文档：

(1) 路由器 A

!

service timestamps debug uptime

service timestamps log uptime

service password-encryption

no service tcp-small-servers

no service udp-small-servers

!

hostname Router_A

!

enable password cisco

username Router_B password cisco


```

!
no ip name-server
!
isdn switch-type basic-net3
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Dialer 1
  description connected to Router_B
  ip unnumbered FastEthernet 0/0
  no ip split-horizon
  encapsulation ppp
  dialer in-band
  dialer idle-timeout 120
  dialer hold-queue 10
  dialer map snapshot 1 name Router_B broadcast
  dialer map ip 192.168.11.254 name Router_B speed 64 broadcast 68001002
  dialer-group 1
  ppp authentication chap
  no ppp multilink
  snapshot server 15 dialer
  no cdp enable
!
interface FastEthernet 0/0
  no shutdown
  description connected to LAN_A
  ip address 192.168.10.254 255.255.255.0
  no keepalive
!
interface FastEthernet 0/1
  no description
  no ip address
  shutdown
!
interface BRI 0/0
  no shutdown
  description connected to Router_B

```



```

no ip address
dialer rotary-group 1
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
router rip
version 2
network 192.168.10.0
no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
(2) 路由器 B
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_B
!

```

```

no ip address
dialer rotary-group 1
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
router rip
version 2
network 192.168.10.0
no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
(2) 路由器 B
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_B
!

```



```
enable password cisco
username Router_A password cisco
!
no ip name-server
!
isdn switch-type basic-net3
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Dialer 1
description connected to Router_A
ip unnumbered FastEthernet 0/0
no ip split-horizon
encapsulation ppp
dialer in-band
dialer idle-timeout 120
dialer hold-queue 10
dialer map snapshot 1 name Router_A broadcast 68001001
dialer map ip 192.168.10.254 name Router_A speed 64 broadcast 68001001
dialer-group 1
ppp authentication chap
no ppp multilink
snapshot client 15 360 suppress-statechange-update dialer
no cdp enable
!
interface FastEthernet 0/0
no shutdown
description connected to LAN_B
ip address 192.168.11.254 255.255.255.0
no keepalive
!
interface FastEthernet 0/1
no description
no ip address
shutdown
!
interface BRI 0/0
```



```

no shutdown
description connected to Router_A
no ip address
dialer rotary-group 1
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
router rip
version 2
network 192.168.11.0
no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!

```

案例 2

ISDN 拨号连接 Internet。其连接方式如图 5-68 所示。

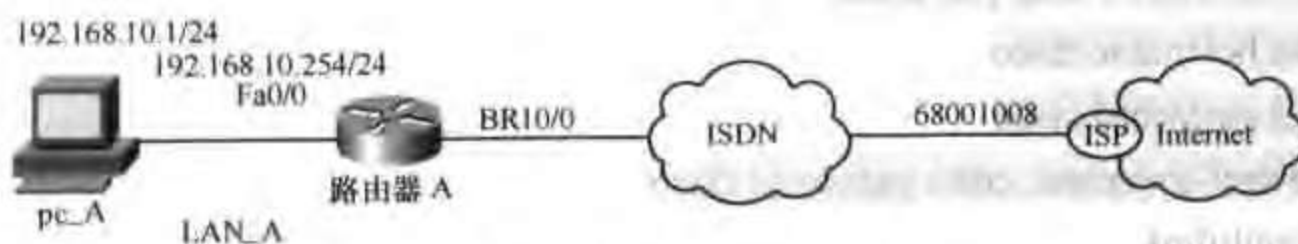


图 5-68 ISDN 案例 2 的拓扑结构

说明: Router_A 采用 Cisco2621XM 路由器, 配置 WIC-1B-S/T 接口卡。

配置文档:

路由器 A

!

service timestamps debug uptime

service timestamps log uptime

service password-encryption

no service tcp-small-servers

no service udp-small-servers

!

hostname Router_A

!

enable password cisco

!

no ip name-server

!

isdn switch-type basic-net3

!

ip subnet-zero

no ip domain-lookup

ip routing

!

interface Dialer 1

description connected to Internet

ip address negotiated

ip nat outside

no ip split-horizon

encapsulation ppp

dialer in-band

dialer idle-timeout 120

dialer string 68001008

dialer hold-queue 10

dialer-group 1

ppp authentication chap pap callin

ppp chap hostname cisco

ppp chap password cisco

ppp pap sent-username cisco password cisco

no ppp multilink

no cdp enable




```

!
interface FastEthernet 0/0
  no shutdown
  description connected to LAN_A
  ip address 192.168.10.254 255.255.255.0
  ip nat inside
  keepalive 10
!
interface FastEthernet 0/1
  no description
  no ip address
  shutdown
!
interface BRI 0/0
  no shutdown
  description connected to Internet
  no ip address
  dialer rotary-group 1
!
! Access Control List 1
!
no access-list 1
access-list 1 permit 192.168.10.0 0.0.0.255
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
! Dynamic NAT
!
ip nat translation timeout 86400
ip nat translation tcp-timeout 86400
ip nat translation udp-timeout 300
ip nat translation dns-timeout 60
ip nat translation finrst-timeout 60
ip nat inside source list 1 interface Dialer 1 overload
!
!

```



```
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Dialer 1
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
```

5.3.6 PSTN

1. 简介

公用交换电话网 (PSTN, Published Switched Telephone Network) 接入技术是利用 PSTN 通过调制解调器拨号实现用户接入的方式。这是大家非常熟悉的一种接入方式, 目前最高的速率为 56kbit/s, 已经达到信道容量的极限。这种速率远远不能够满足宽带多媒体信息的传输需求, 但由于电话网非常普及, 用户终端设备 Modem 很便宜, 而且不用申请就可开户。只要家里有电脑, 把电话线接入 Modem 就可以直接上网。因此, PSTN 拨号接入方式还是非常普及, 但随着 ADSL 等宽带接入方式的不断发展和普及, PSTN 接入方式将会逐渐被淘汰。

2. 典型应用

目前 PSTN 作为一种接入手段主要用于企业网广域骨干链路的备份, 以及超小型企业或家庭用户的 Internet 接入。PSTN 的典型应用如图 5-69 所示。

3. 用户入网方式

PSTN 作为电信公司一个覆盖面极广的业务网络, 其主要的业务是向用户提供语音方面的业务。作为数据传输的手段, 往往需要采用模拟调制解调器来实现其数据方式的接入。

4. 案例分析

案例 1

通过模拟 Modem 拨号连接, 实现两个 LAN 的互连。其连接方式如图 5-71 所示。

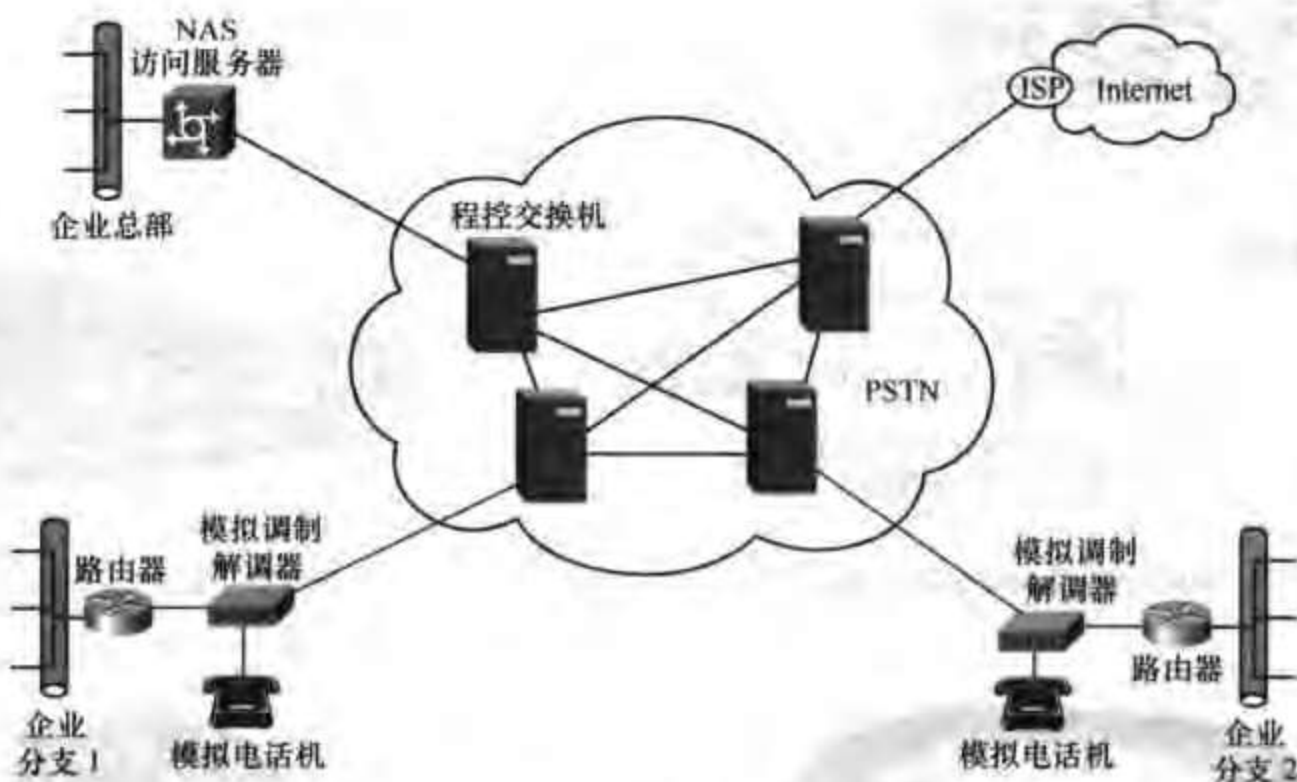


图 5-69 PSTN 接入典型应用

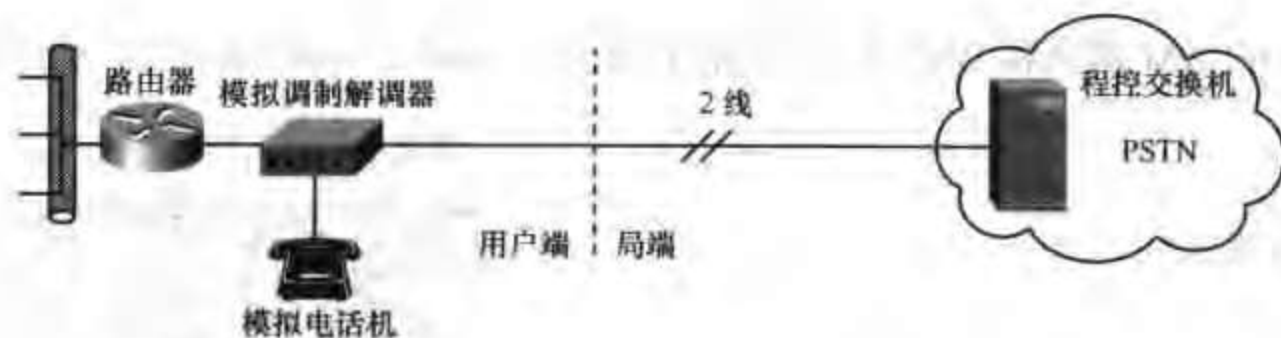


图 5-70 PSTN 接入

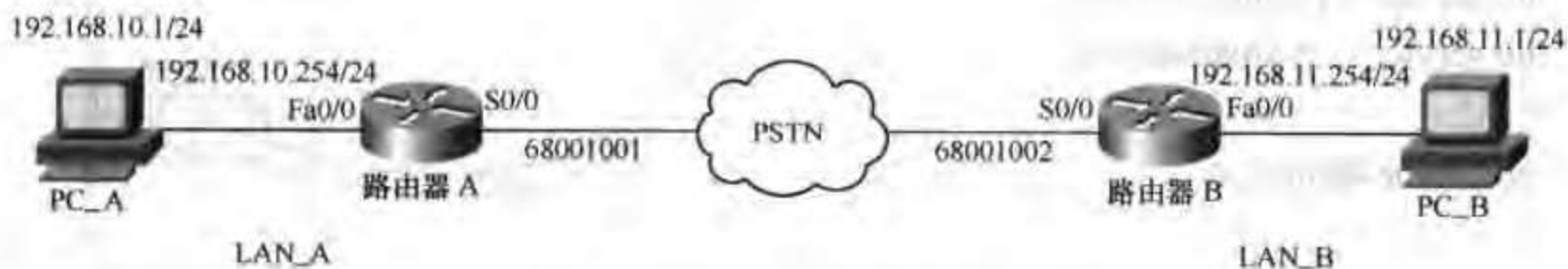


图 5-71 通过 PSTN 连接两个 LAN 的拓扑结构

说明: Router_A 和 Router_B 都采用 Cisco2621XM 路由器, 配置 WIC-2A/S 接口卡, LAN_A 和 LAN_B 通过 PSTN 互连。

WIC-2A/S 与 Modem 的连接方式如图 5-72 所示。

连接中所用的接口卡和线缆如图 5-73~图 5-75 所示。

新采用模块的连接图如图 5-76 所示。

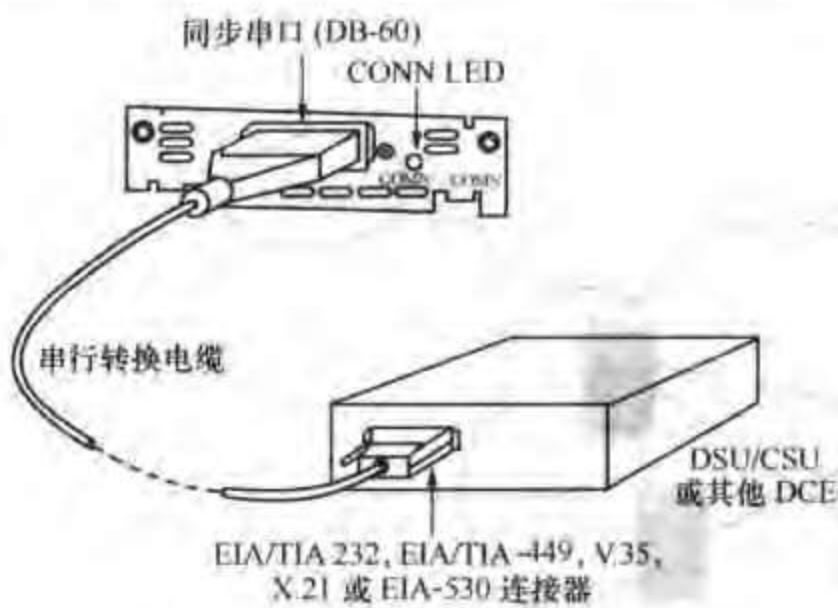


图 5-72 WIC-2A/S 和 Modem 的连接示意图



图 5-73 WIC-2A/S 接口卡



图 5-74 CAB-SS-232MT 线缆



图 5-75 WIC-1AM 接口卡

说明：WIC-AM 模块和 WIC-A/S 模块的区别在于 AM 已内置 Modem，而 A/S 需要外接一个 Modem。

配置文档：

(1) 路由器 A

```
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_A
!
enable password cisco
username Router_B password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
```

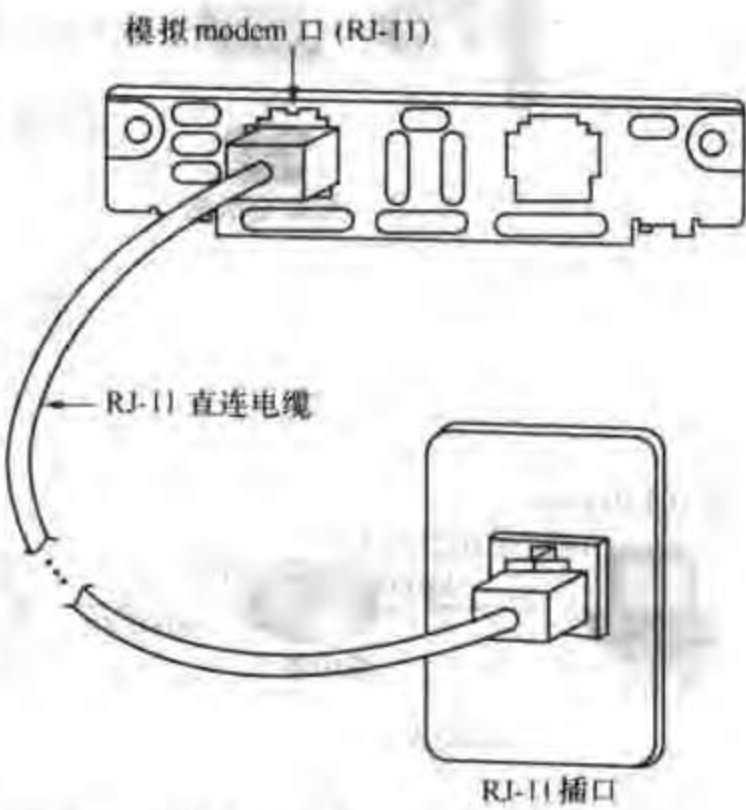


图 5-76 WIC-1AM 连接示意图


```
ip routing
chat-script default ABORT ERROR ABORT BUSY ABORT "NO ANSWER" "" "ATDT\T"
TIMEOUT 60 CONNECT \c
modemcap entry default:FD=&F:AA=S0=1:CD=&C1:DTR=&D3:NEC=E0:NRS=Q1
!
interface Dialer 1
  description connected to Router_B
  ip unnumbered FastEthernet 0/0
  encapsulation ppp
  dialer in-band
  dialer idle-timeout 120
  dialer hold-queue 10
  dialer map snapshot 1 name Router_B broadcast
  dialer map ip 192.168.11.254 name Router_B modem-script default broadcast 68001002
  dialer-group 1
  pulse-time 3
  ppp authentication chap
  snapshot server 15 dialer
  no cdp enable
!
interface FastEthernet 0/0
  no shutdown
  description connected to LAN_A
  ip address 192.168.10.254 255.255.255.0
  no keepalive
!
interface FastEthernet 0/1
  no description
  no ip address
  shutdown
!
interface Serial 0/0
  physical-layer asyuc
  no shutdown
  description connected to Router_B
  no ip address
  async mode dedicated
  dialer rotary-group 1
!
```



```
interface Serial 0/1
  no description
  no ip address
  shutdown
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
router rip
  version 2
  network 192.168.10.0
  no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
line 1
  modem InOut
  modem autoconfigure type default
  transport input all
  stopbits 1
  speed 38400
  flowcontrol hardware
!
```



```
end
(2) 路由器 B
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_B
!
enable password cisco
username Router_A password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
chat-script default ABORT ERROR ABORT BUSY ABORT "NO ANSWER" "" "ATDT\T"
TIMEOUT 60 CONNECT \c
modemcap entry default:FD=&F:AA=S0=1:CD=&C1:DTR=&D3:NEC=E0:NRS=Q1
!
interface Dialer 1
description connected to Router_A
ip unnumbered FastEthernet 0/0
encapsulation ppp
dialer in-band
dialer idle-timeout 120
dialer hold-queue 10
dialer map snapshot 1 name Router_A modem-script default broadcast 68001001
dialer map ip 192.168.10.254 name Router_A modem-script default broadcast 68001001
dialer-group 1
pulse-time 3
ppp authentication chap
snapshot client 15 360 suppress-statechange-update dialer
no cdp enable
!
interface FastEthernet 0/0
```



```
no shutdown
description connected to LAN_B
ip address 192.168.11.254 255.255.255.0
no keepalive
!
interface FastEthernet 0/1
no description
no ip address
shutdown
!
interface Serial 0/0
physical-layer async
no shutdown
description connected to Router_A
no ip address
asyuc mode dedicated
dialer rotary-group 1
!
interface Serial 0/1
no description
no ip address
shutdown
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
router rip
version 2
network 192.168.11.0
no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server locatiou
no snmp-server contact
```



```
!  
line console 0  
  exec-timeout 0 0  
  password cisco  
  login  
!  
line vty 0 4  
  password cisco  
  login  
!  
line 1  
  modem InOut  
  modem autoconfigure type default  
  transport input all  
  stopbits 1  
  speed 38400  
  flowcontrol hardware  
!  
end
```

案例 2

Internet 接入

Internet 接入的连接如图 5-77 所示。

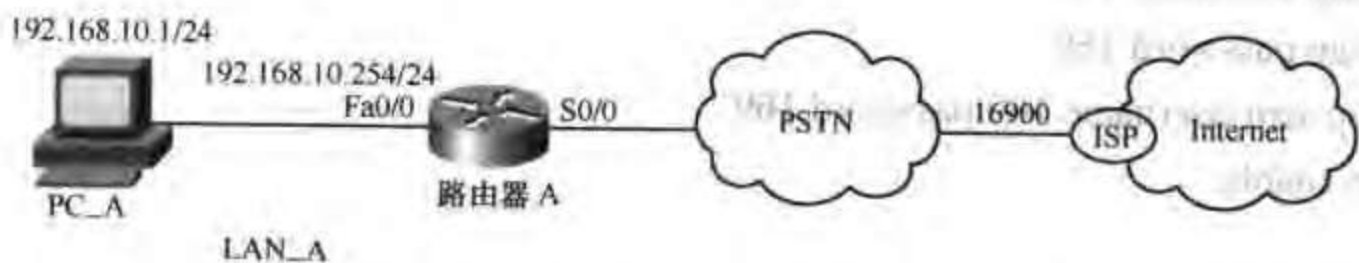


图 5-77 Internet 接入的拓扑结构

配置文档如下：

路由器 A

```
!  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption  
no service tcp-small-servers  
no service udp-small-servers  
!  
hostname Router_A
```



```
!  
enable password cisco  
!  
no ip name-server  
!  
ip subnet-zero  
no ip domain-lookup  
ip routing  
modemcap entry default:FD=&F:AA=S0=1:CD=&C1:DTR=&D3:NEC=E0:NRS=Q1  
!  
interface Dialer 1  
    description connected to Internet  
    ip address negotiated  
    ip nat outside  
    encapsulation ppp  
    dialer in-band  
    dialer idle-timeout 120  
    dialer string 16900  
    dialer hold-queue 10  
    dialer-group 1  
    pulse-time 3  
    ppp authentication chap pap callin  
    ppp chap bostname 169  
    ppp chap password 169  
    ppp pap sent-username 169 password 169  
    no cdp enable  
!  
interface FastEthernet 0/0  
    no shutdown  
    description connected to LAN_A  
    ip address 192.168.10.254 255.255.255.0  
    ip nat inside  
    keepalive 10  
!  
interface FastEthernet 0/1  
    no description  
    no ip address  
    shutdown  
!
```



```
interface Serial 0/0
  physical-layer async
  no shutdown
  description connected to Internet
  no ip address
  async mode dedicated
  dialer rotary-group 1
!
interface Serial 0/1
  no description
  no ip address
  shutdown
!
! Access Control List 1
!
no access-list 1
access-list 1 permit 192.168.10.0 0.0.0.255
!
! Dynamic NAT
!
ip nat translation timeout 86400
ip nat translation tcp-timeout 86400
ip nat translation udp-timeout 300
ip nat translation dns-timeout 60
ip nat translation finrst-timeout 60
ip nat inside source list 1 interface Dialer 1 overload
!
router rip
  version 2
  network 192.168.10.0
  passive-interface Dialer 1
  no auto-summary
!
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Dialer 1
no ip http server
```



```
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
line 1
  modem InOut
  modem autoconfigure type default
  transport input all
  stopbits 1
  speed 38400
  flowcontrol hardware
!
end
```

5.3.7 ADSL

1. ADSL 简介

近年来随着 Internet 的迅猛发展, 普通 Modem (模拟调制解调器) 拨号的速率, 已远远不能满足人们获取大容量信息的需要, 用户对接入速率的要求越来越高。如今一种名叫 ADSL 的技术已投入实际使用, 使用户享受到了高速冲浪的快乐。

ADSL 是英文 Asymmetrical Digital Subscriber Loop (非对称数字用户线) 的缩写, ADSL 技术是运行在原有普通电话线上的一种新的高速宽带技术, 它利用现有的一对电话铜线, 为用户提供上、下行非对称的传输速率 (带宽)。

ADSL 是利用分频技术把普通语音与数据信号分离, 普通语音信道占据原来 4kHz 以下的电话频段, 上行数字信道占据 10~50kHz 的中间频段, 下行数字信道占据 1MHz 以下的离端频段, 下行 (从网络到用户) 最高可达到 8Mbit/s, 上行 (从用户到网络) 最高可达到 640kbit/s, 为用户提供宽带接入服务。

ADSL 最初主要是针对视频点播业务开发的, 随着技术的发展, 逐步成为了一种较方便的宽带接入技术, 为电信部门所重视。通过网络电视的机顶盒, 用 ADSL 可以实现许多以前在低速率下无法实现的网络应用。

ADSL 技术的特点如下:

- (1) 可直接利用现有用户电话线, 节省投资。
- (2) 可享受超高速的网络服务, 为用户提供上、下行不对称的传输带宽。
- (3) 节省费用, 上网同时可以打电话, 互不影响, 而且上网时不需要另交电话费。
- (4) 安装简单, 不需要另外申请线路, 只需要在普通电话线上加装 ADSL 调制解调器, 在电脑上装上网卡即可。

下面将 ADSL 技术与其他常见的接入技术进行对比:

(1) ADSL 与普通拨号 Modem 的比较: 比起普通拨号 Modem 的最高速率 56K, ADSL 的速率优势是不言而喻的, 而且它在同一铜线上分别传送数据和语音信号, 数据信号并不通过电话交换机设备, 所以在线并不需要拨号, 这意味着上网无须缴纳额外的话费。

(2) ADSL 与 ISDN 的比较: 二者的相同点是都能够进行语音、数据、图像的综合通信, 但 ADSL 的速率是 ISDN 的 60 倍左右。ISDN 提供的是 2B+D 的数据通道, 其速率最高可达到 144kbit/s, 接入网络是窄带的 ISDN 交换网络, 而 ADSL 的下行速率可达 8Mbit/s, 它的语音部分走的是传统的 PSTN 网, 而数据部分则接入宽带 ATM 平台。

(3) ADSL 与 DDN 的比较: ADSL 非对称接入方式, 上行最高 640kbit/s, 下行最高 8Mbit/s, 相对于 DDN 对称性的数据传输更适合于现代网络的特点。同时 ADSL 费用较之 DDN 要低廉得多, 接入方式也较灵活。

(4) ADSL 和 Cable Modem 的比较: ADSL 在网络拓扑的选择上采用星型拓扑结构, 为每个用户提供固定、独占的保证带宽, 而且可以保证用户发送数据的安全性, 而 Cable Modem 的线路为总线型, 一般国外有线电视承诺的 10Mbit/s 甚至 30Mbit/s 的信道带宽是一群用户共享的, 一旦用户数增多, 每个用户所分配的带宽就会急剧下降, 而且共享型网络拓扑致命的缺陷就是它的安全性, 数据传送基于广播机制, 同一个信道的每个用户都可以接收到该信道中的数据分组。

2. 典型应用

目前 ADSL 主要用于 Internet 的接入。在 ADSL 使用中, 用户通过 ADSL 连接至 DSLAM, DSLAM 上联 ATM 交换机, 在作为宽带 IP 接入的方式中, 该 PVC 连接至电信公司的 B_RAS, 通过 B_RAS 的终结, 接入到 Internet 网络。ADSL 典型应用如图 5-78 所示。

3. 用户入网方式

ADSL 通常有两种接入方式: ADSL 虚拟拨号和 ADSL 专线接入。

(1) ADSL 虚拟拨号

ADSL 虚拟拨号是在 ADSL 的数字线上进行拨号, 不同于模拟电话线上用调制解调器的拨号, 而采用专门的协议 PPP over Ethernet。拨号后, 直接由验证服务器进行检验, 用户需输入用户名与密码, 检验通过后就建立起一条高速的用户数字, 并分配相应的动态 IP。虚拟拨号用户需要通过一个用户帐号和密码来验证身份, 这个用户帐号和密码是用户申请接入时由接入提供商提供的。

(2) ADSL 专线接入

ADSL 专线接入不同于虚拟拨号方式, 它是采用一种类似于专线的接入方式, 用户连接和配置好 ADSL 调制解调器后, 在自己的 PC 的网络设置里设置好相应的 TCP/IP 协议及网络参数 (IP 和掩码、网关等都由接入提供商事先分配好)。开机后, 用户端和局端会自动建立起一条链路。所以, ADSL 的专线接入方式是具有固定 IP 地址、自动连接等特点的类似于专线的方式。

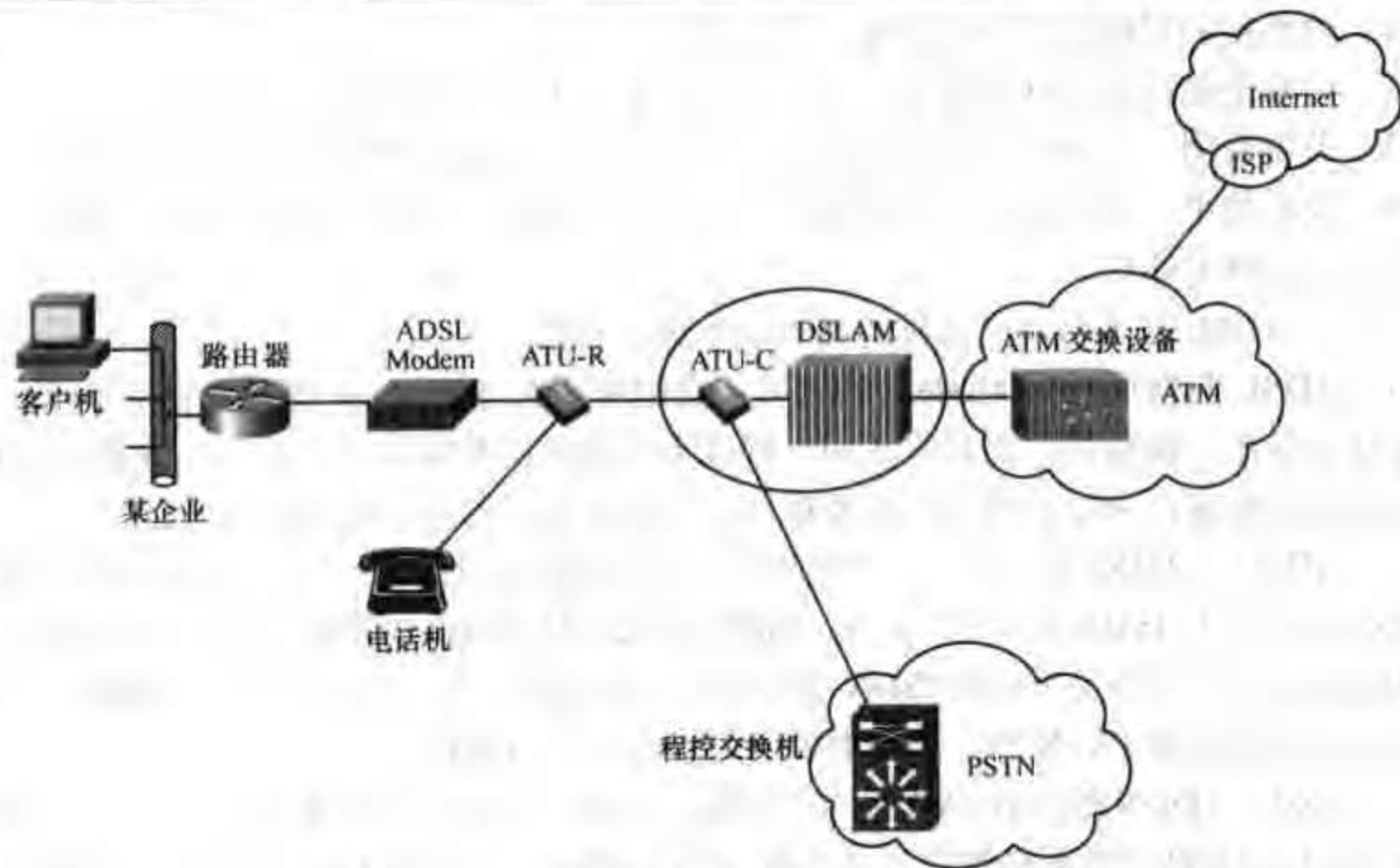


图 5-78 ADSL 典型应用

以上两种接入方式的入网拓扑如图 5-79 所示。



图 5-79 ADSL 入网方式

虽然 ADSL 存在以上两种入网方式，但虚拟拨号的使用范围远远大于专线方式，以至于人们一谈起 ADSL，就自然地认为是拨号的 ADSL，因此以下我们主要针对拨号 ADSL 进行介绍。通常我们申请 ADSL 之后，接入提供商（例如中国网通）会提供给我们一个用户名和一个密码，而我们也会有多种方式来接入 Internet，下面将分别对这些接入方式进行介绍。

(1) 方式一

这种接入方式如图 5-80 所示。

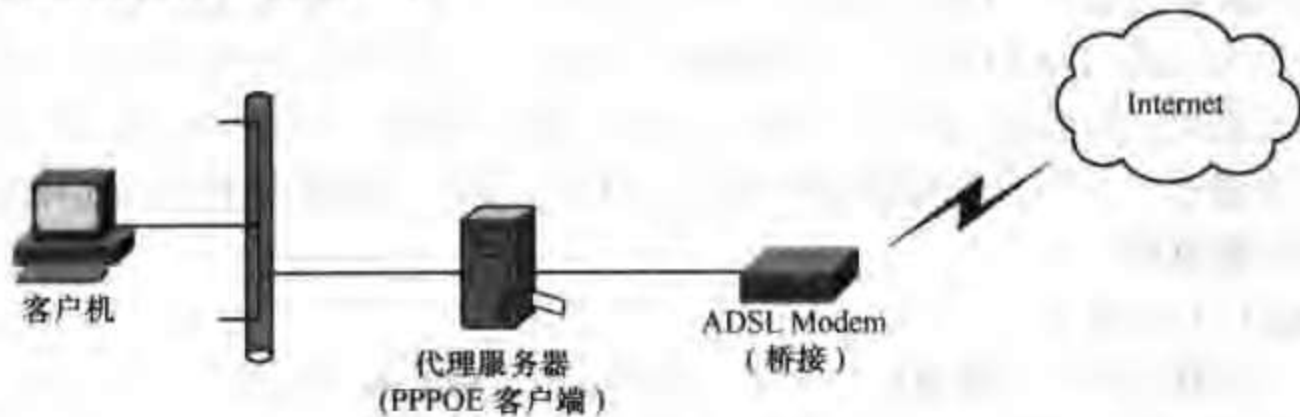


图 5-80 方式一

在方式一中，电信公司提供的 ADSL Modem 配置为桥接模式，并需要一台计算机作为

PPPOE 的客户端，配置电信公司分配的用户名和密码用来拨号。同时，这台机器还要承担代理服务器的角色，这样其他的客户机只要将网关指向它，就可以通过其上网了。在这种方式中，需要一台配置双网卡的计算机作为代理服务器，它负责数据分组的转发和缓存，因此它的性能的高低直接影响了网络的性能。

(2) 方式二

方式二的接入方式如图 5-81 所示。

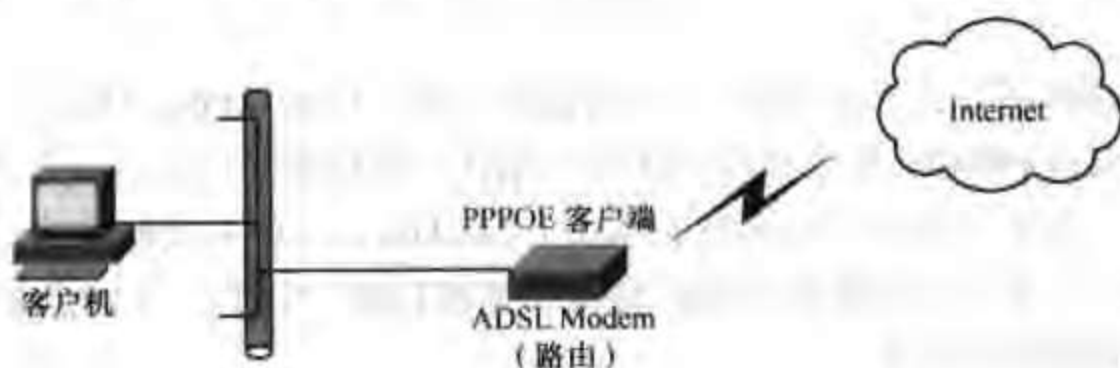


图 5-81 方式二

在方式二中，将电信公司提供的 ADSL Modem 配置为路由模式（注意，并非所有电信公司提供的 ADSL Modem 都具有路由功能，详情请查看产品的说明书）。这时我们将 ADSL Modem 配置为 PPPOE 的客户端，配置电信公司分配的用户名和密码用来拨号。这种方式的 ADSL Modem 具有地址转换（NAT）的功能，其他的客户机只要将网关指向 ADSL Modem 的内口地址，就可以通过其上网了。在这种方式中，所用设备最少，但 ADSL Modem 承担的压力也最大，当客户机较多时，建议不要采用此方式。

(3) 方式三

方式三的接入方式如图 5-82 所示。



图 5-82 方式三

方式三可以看成是方式一的变种。方式三是将方式一中的代理服务器换成了专用路由器，由路由器来承担 PPPOE 拨号和地址转换（NAT）的功能。这种方式是企业用户经常采用的一种方式，因为它采用专用的路由器设备来负责数据分组的转发，因此它的性能和稳定性较方式一有很大的提高。

(4) 方式四

方式四的接入方式如图 5-83 所示。



图 5-83 方式四

方式四可以看成是方式二的变种。方式四是将方式二中的 ADSL Modem 换成了专用路由器，由路由器来承担 PPPoE 拨号和地址转换（NAT）的功能。这种方式是采用 ADSL 模块，来直接接电话线，舍去了电信公司提供的 ADSL Modem。这种方式和方式三有相近的地方，即都是用专用路由设备来实现数据分组的转发和地址转换（NAT），不同点是方式三采用的模块更加便宜，因此使用范围更广。

4. 案例分析

案例 1

局域网通过 ADSL 拨号上网。其连接方式如图 5-84 所示。

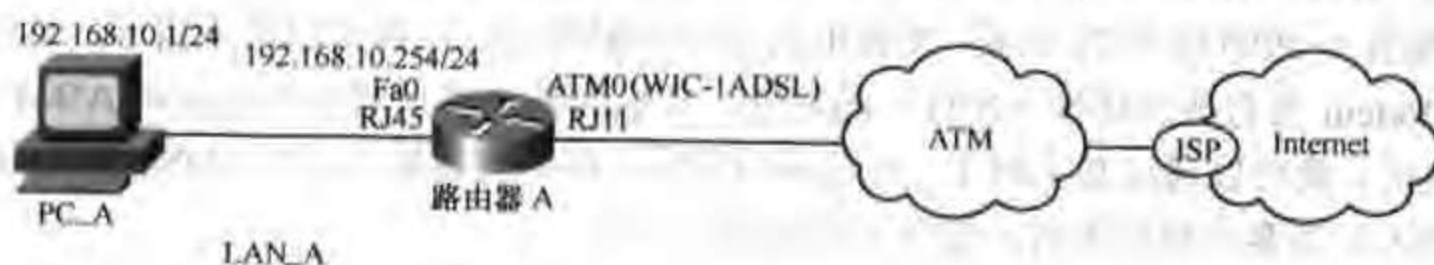


图 5-84 ADSL 案例 1 示意图

说明：Router_A 采用 Cisco1721 路由器，配置 WIC-1ADSL 接口卡，LAN_A 通过 ADSL 接入 Internet。

注意：WIC-1ADSL 接口卡可应用在以下两种环境中：

(1) 可用在 Cisco2600/3600/3700 路由器的 NM-1FE1R2W、NM-1FE2W、NM-2FE2W 和 NM-2W 模块中，软件版本需要 IP PLUS 版，最低版本为 12.1(5)YB。

(2) 可用在 Cisco1700 路由器上，软件 image 的平台需要为 c1700，而不能是 c1720 或 c1750。为了支持 PPPoE，版本必须具有 ADSL+PLUS 特性集，最低版本为 12.1(3)XP。

WIC-1ADSL 的连接，如图 5-85 所示。

本案例所采用的设备和相应的模块如图 5-86 和图 5-87 所示。

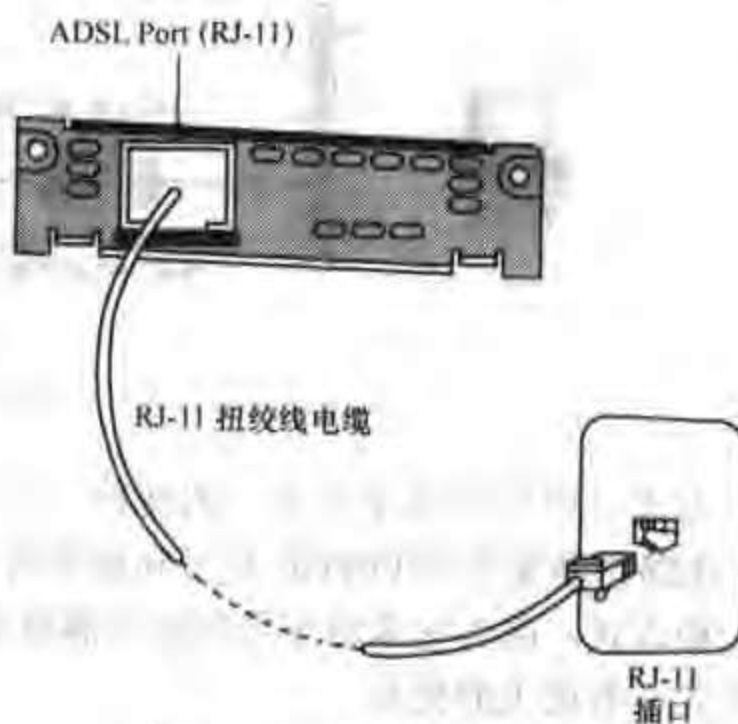


图 5-85 WIC-1ADSL 连接示意图



图 5-86 Cisco1721 路由器



图 5-87 WIC-1ADSL 模块

配置文档:

路由器 A

!

service timestamps debug uptime

service timestamps log uptime

service password-encryption

no service tcp-small-servers

no service udp-small-servers

!

hostname Router_A

!

enable password cisco

!

no ip name-server

!

ip subnet-zero

no ip domain-lookup

ip routing

!

!--由于 ADSL 的 PPPOE 应用是通过虚拟拨号来实现的所以在路由器中需要使用 VPDN 的功能:

vpdn enable


```
no vpdn logging
!
! ---为 PPPOE 启动 VPDN 的进程:
vpdn-group pppoe
! ---作为 PPPOE 客户端向 PPPOE 终结设备请求连接:
request-dialin
! ---设置拨号协议为 PPPOE:
protocol pppoe
!
interface FastEthernet 0
no shutdown
description connected to LAN_A
ip address 192.168.10.254 255.255.255.0
keepalive 10
!
! ---设置 ADSL 端口:
interface ATM0
no ip address
no atm ilmi-keepalive
bundle-enable
dsl operating-mode auto
hold-queue 224 in
!
! --- ADSL 的通信依靠 VC, 所以必须设定点到点 VC:
interface ATM0.1 point-to-point
! ---设置 PVC 的相关参数, 即 VCI 和 VPI 的值, 如果不清楚请向接入提供商查询:
pvc 8/35
! --- PPPOE 拨号进程使用了常规的拨号进程, 这里引用了 dialer-pool 1:
pppoe-client dial-pool-number 1
!
! ---建立一个虚拟拨号端口:
interface Dialer1
! ---由于局端提供动态地址, 所以必须设定地址为协商获得:
ip address negotiated
!---修改 mtu 值以适用于 ADSL 网络,以太网的默认 MTU 值是 1500 字节 (1492 + PPPOE
headers = 1500):
ip mtu 1492
! ---为启用 NAT 转换, 设置该端口为外部网络:
ip nat outside
```


! ---使用 PPP 的帧格式:

encapsulation ppp

dialer pool 1

dialer-group 1

! ---设置拨号的验证方式为 pap:

ppp authentication pap callin

! ---发送用户名和密码, 如果不清楚请向接入提供商查询:

ppp pap sent 100000100000 pass 12345678

!

! ---设置 NAT 的转换方式, 使用了 dialer 1 端口的动态地址:

ip nat inside source list 1 interface Dialer1 overload

!

ip classless

!

! IP Static Routes

! ---将所有不可路由的数据报转发给 ADSL 线路, 设定缺省路由:

ip route 0.0.0.0 0.0.0.0 dialer1

no ip http server

!

access-list 1 permit any

!

! Dialer Control List 1

!

no dialer-list 1

dialer-list 1 protocol ip permit

!

snmp-server community public RO

no snmp-server location

no snmp-server contact

!

line console 0

exec-timeout 0 0

password cisco

login

!

line vty 0 4

password cisco

login

!

案例 2

局域网通过 ADSL 拨号上网。其连接方式如图 5-88 所示。

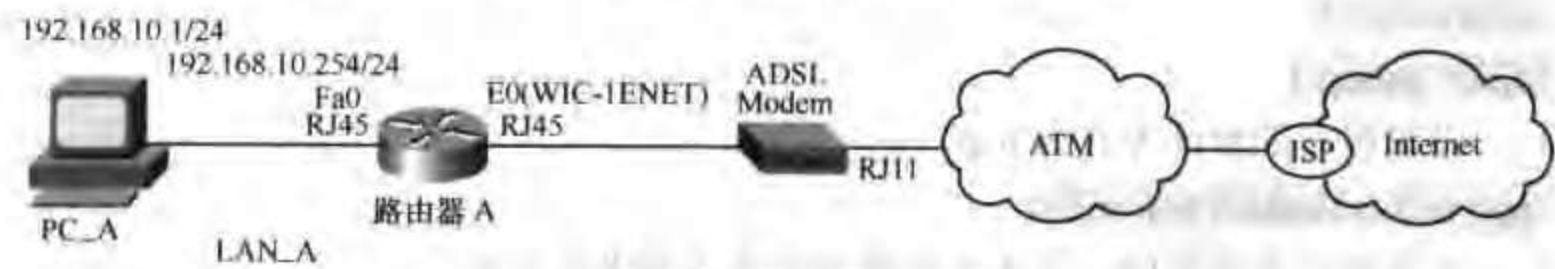


图 5-88 ADSL 案例 2 示意图

说明：

Router_A 采用 Cisco1721 路由器，配置 WIC-1ENET 接口卡，LAN_A 通过 ADSL 接入 Internet。

注意：

WIC-1ENET 只用在 Cisco1700 系列路由器上，为了支持 PPPOE，其版本必须具有 ADSL+PLUS 特性集，最低版本为 12.1(3)XT1。

本案例新采用的模块如图 5-89 所示。



图 5-89 WIC-1ENET 模块

配置文档

路由器 A

！

```
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
```

！

```
hostname Router_A
```

！

```
enable password cisco
```

！

```
no ip name-server
```

！

```
ip subnet-zero
```

```
no ip domain-lookup
```

```
ip routing
```

！

```
vpdn enable
```

```
no vpdn logging
```

！

```
vpdn-group pppoe
```



```

request-dialin
protocol pppoe
!
interface FastEthernet 0
no shutdown
description connected to LAN_A
ip address 192.168.10.254 255.255.255.0
keepalive 10
!
! ---设置 WIC-1ENET 端口:
interface Ethernet0
pppoe enable
pppoe-client dial-pool-number 1
!
interface Dialer1
ip address negotiated
ip mtu 1492
ip nat outside
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication pap callin
ppp pap sent 100000100000 pass 12345678
!
ip nat inside source list 1 interface Dialer1 overload
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 dialer1
no ip http server
!
access-list 1 permit any
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!

```




```
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
```

小结:

到目前为止, 我们已经将我国提供的主要的数据业务进行了介绍, 下面进行一下总结:

企业建构自己的广域网络通常可采用 DDN、FrameRelay、PDH/SDH 线路, PSTN、ISDN 主要用于作为上述线路的备份, 以上所有线路都可作为 Internet 的接入手段, 我们可以将 ISP 看成是具有 Internet 出口的企业总部, 而需要 Internet 接入的客户可看成是 ISP 的分支机构, 这样就将 Internet 接入看成是企业广域互连的一种特例。ADSL 是最新涌现出的一种接入线路, 和 PSTN、ISDN 相比, 它具有较高的性价比, 现在逐渐成为家庭主流的 Internet 接入手段。企业广域网络建构示意图如图 5-90 所示, Internet 接入如图 5-91 所示。

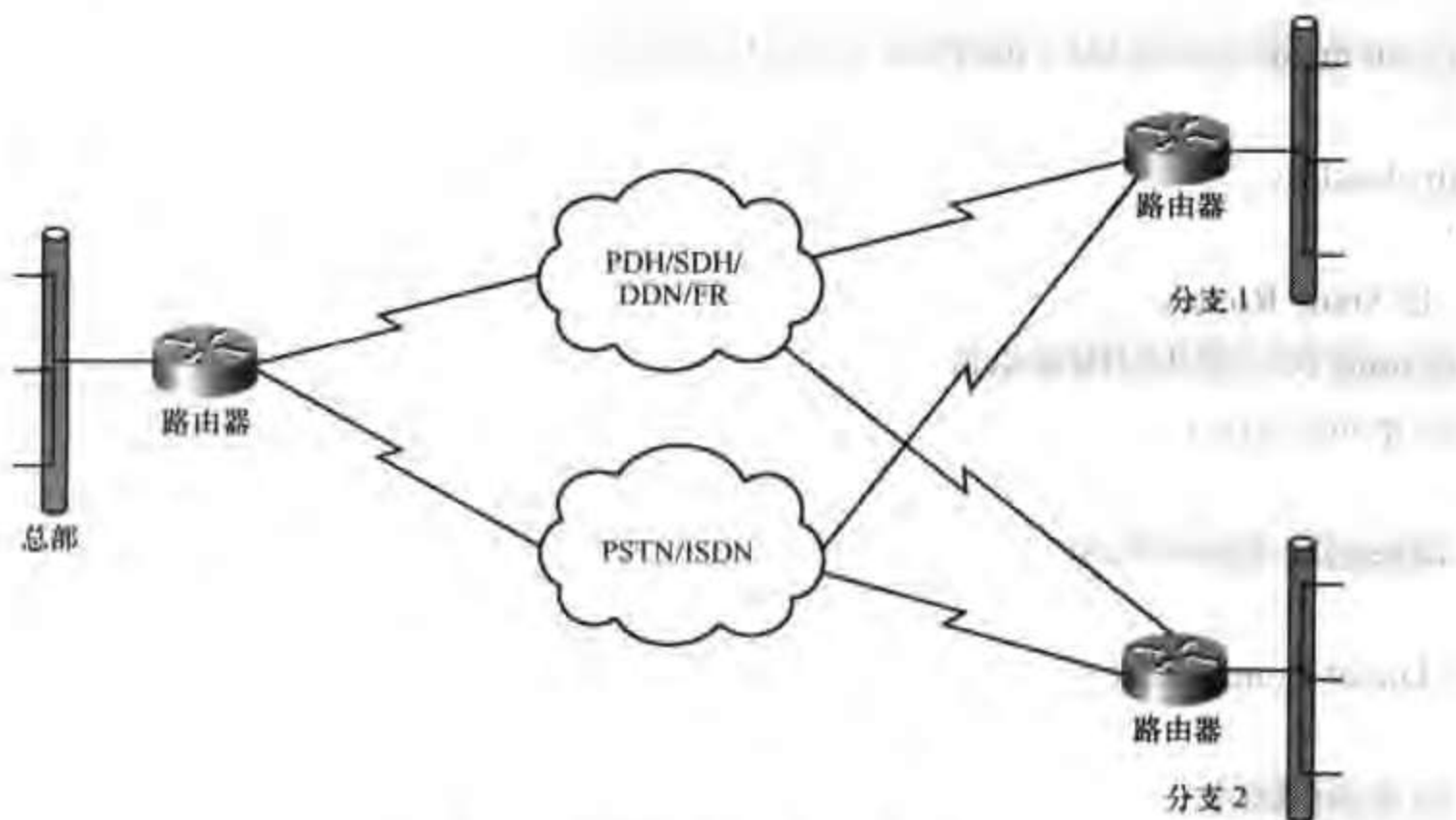


图 5-90 企业广域网络建构示意图

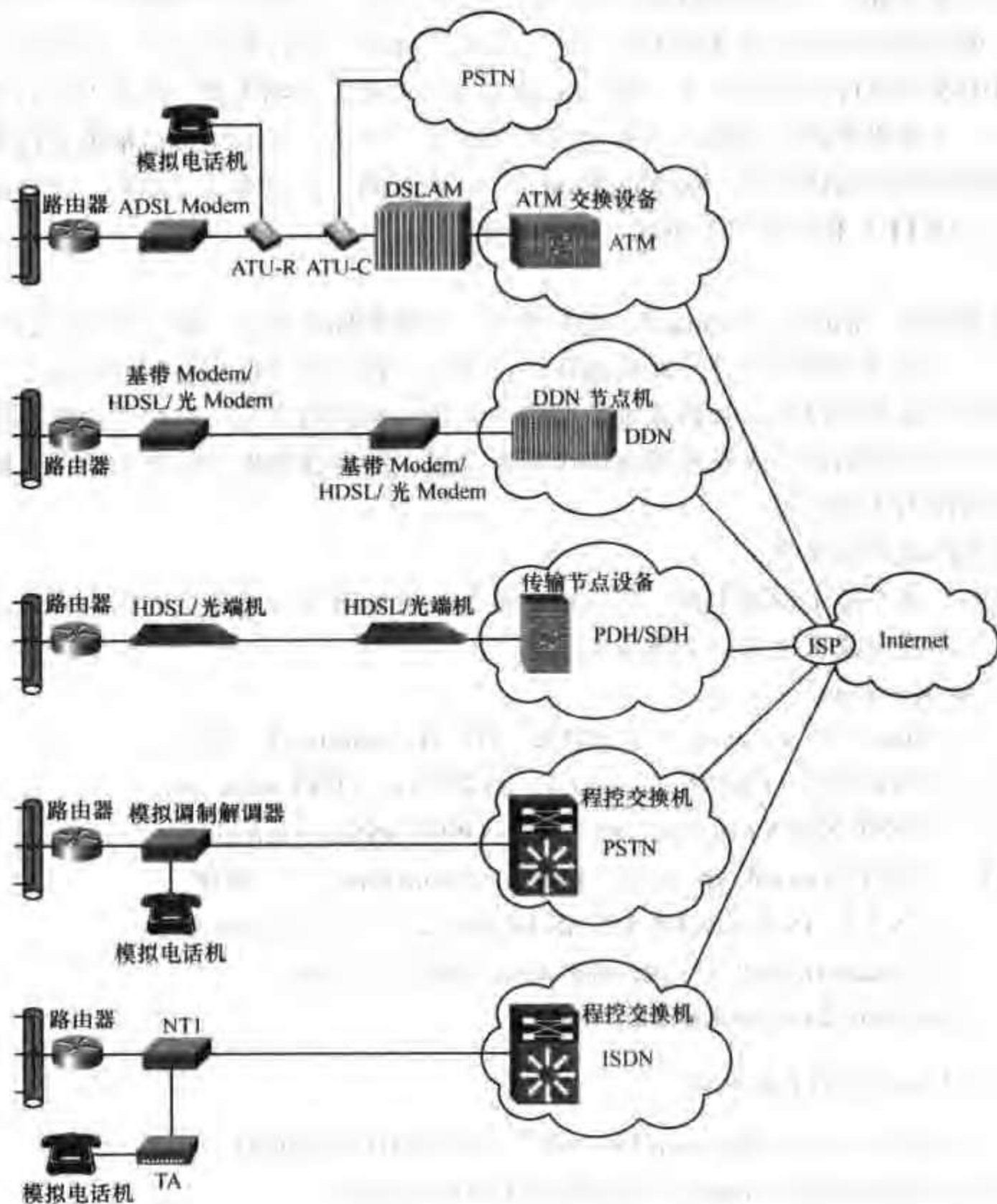


图 5-91 Internet 接入汇总

5.4 路由协议设置

在学习本节的内容前，先对下列有关术语及其内容作一些介绍：

(1) 路由选择协议和路由转发协议

在前面我们曾介绍过路由器主要完成两项工作，即“寻径”和“转发”。“寻径”是指建立和维护路由表的过程，主要由软件实现；“转发”是指把数据分组从一个接口转到另一接口的过程，是由硬件实现的。下面我们就来介绍路由器功能中的“寻径”部分，即路由器是如何判定到达目的地的最佳路径的。

为了判定最佳路径，路由选择算法必须启动并维护包含路由信息的路由表，其中的路由信息依赖于所用的路由选择算法而不尽相同。路由选择算法将收集到的不同信息填入路由表中，根据路由表可将目的网络与下一跳（Nexthop）的关系告诉路由器。路由器间互通信息进行路由更新，更新维护路由表使之正确反映网络的拓扑变化，并由路由器根据量度来决定最佳路径。这就是路由选择协议（Routing Protocol），例如路由信息协议（RIP）、开放式最短路径优先协议（OSPF）和边界网关协议（BGP）等。

注意：

路由选择协议（Routing Protocol）是负责建立和维护路由表的，路由转发协议（Routed Protocol）是负责发送数据分组的。路由选择协议和路由转发协议是相互配合又相互独立的概念，路由转发协议根据路由选择协议维护的路由表进行数据的转发，同时路由选择协议要利用路由转发协议提供的功能来发布路由协议数据分组。通常我们提到的路由协议，除非特别说明，都是指路由选择协议。

（2）静态路由和动态路由

说到路由，就不能不提路由表，因为路由器实际就是根据自己维护的路由表来进行路径的选择的。下面我们就来认识一下路由表：

```
Router_A#sh ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

```
R    192.168.11.0/24 [120/1] via 192.168.1.2, 00:00:03, Serial0/0
```

```
C    192.168.10.0/24 is directly connected, FastEthernet0/0
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C        192.168.1.1/32 is directly connected, Serial0/0
```

```
C        192.168.1.0/30 is directly connected, Serial0/0
```

```
S    192.168.15.0/24 [1/0] via 192.168.1.2
```

```
Router_A#
```

以上是一个标准的路由表，下面我们截取其具有代表性的一项来进行分析。

```
R    192.168.11.0/24 [120/1] via 192.168.1.2, 00:00:03, Serial0/0
```

① ② ③ ④ ⑤ ⑥ ⑦

根据上面这条路由我们了解到路由表的每一项包含 7 个内容：

① 路由信息源：该项表明此条路由是如何获得的，这里的“R”表示通过“RIP”路由协议获得，所有的信息源代码在路由表的最上方显示；

② 目的地址：该项表明此条路由的目的地是哪里；

- ③ 管理距离：该项表明获得此条路由的协议的管理距离；
- ④ 度量值：该项表明此条路由所采用的度量；
- ⑤ 下一跳地址：该项表明为了到达目的地要经历的下一跳；
- ⑥ 该表项的时效：该项表明此条路由距上次更新有多长时间（注意只有动态路由协议才有此项）；
- ⑦ 到达下一跳的本端接口：该项表明为了到达下一跳需要将数据分组从本端的该端口送出。

从上面实际的路由表中我们可以看出，通常有两种构建路由表的方式：一种是通过手工输入建立静态路由表；另一种则是通过某种路由算法动态形成路由表。

静态路由是手工输入的，它不能随网络的改变而自动改变。因此静态路由一般只用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。

动态路由是网络中运行相同路由协议的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由器表的过程。它能实时地适应网络结构的变化。如果路由更新信息表明网络发生了变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。这些信息通过各个网络，引起各路由器重新启动其路由算法，并更新各自的路由表以动态地反映网络拓扑变化。动态路由适用于网络规模大、网络拓扑复杂的网络。当然，各种动态路由协议会不同程度地占用网络带宽和 CPU 资源。

（3）路由表项的优先级

在一个路由器中，可同时配置静态路由和一种或多种动态路由。它们各自维护的路由表都提供给转发程序，但这些路由表的表项间可能会发生冲突（即可能会有多条路由到达相同的目的地），如图 5-92 所示。

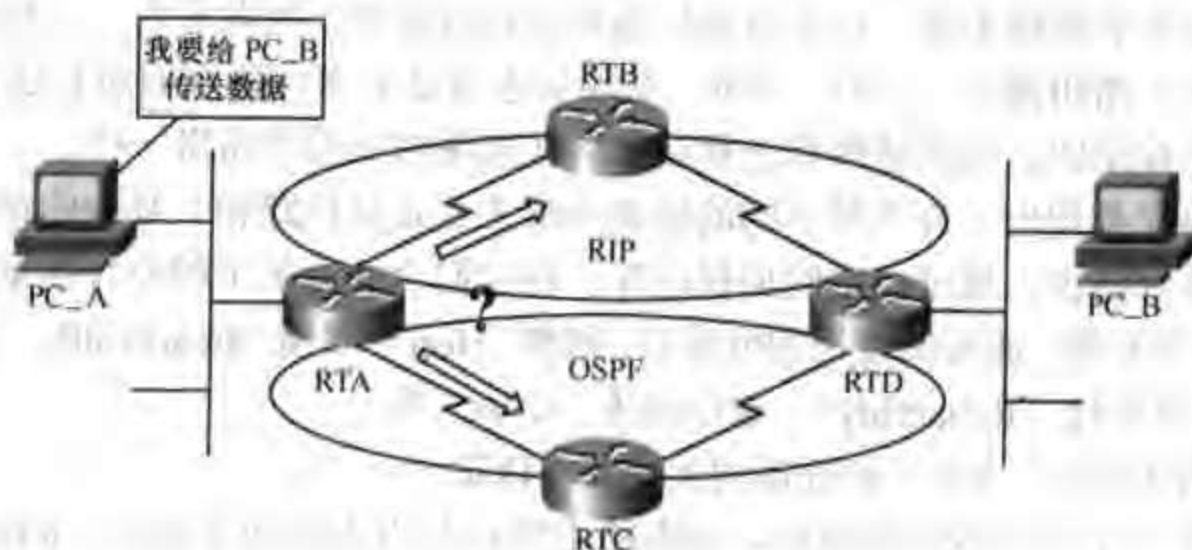


图 5-92 路由表项优先级

这种冲突可通过配置各路由表的优先级来解决。通常静态路由具有默认的最高优先级，当其他路由表表项与它矛盾时，均按静态路由转发。默认的各路由协议的优先级见表 5-13（管理距离越小表明优先级越高）。

表 5-13 路由协议的默认管理距离

路由协议或类型	默认管理距离
Direct connect (直连接口)	0
指向本路由器接口的静态路由	0
指向下一跳路由器接口的静态路由	1
EBGP (外部 BGP)	20
EIGRP	90
IGRP	100
OSPF	110
IS IS	115
RIP	120
IBGP (内部 BGP)	200

(4) 路由算法

路由算法在路由协议中起着至关重要的作用，采用何种算法往往决定了最终的寻径结果，因此选择路由算法一定要仔细。目前我们最常用的是距离矢量和链路状态两种路由算法，下面我们就来简单介绍一下这两种算法。

距离矢量 (D-V) 算法 (也称为 Bellman-Ford 算法)：这种算法要求每个路由器将其路由表的全部信息发送到其邻居节点上，每个节点都从其邻居处获得更新的路由表后进行相应的路径计算，得出自己的路由表，因此采用距离矢量算法的路由器并不知道整个网络的结构。

链路状态 (L-S) 算法 (也称最短路径算法)：这种算法要求每个路由器将自己已知的链路状态向该区域的其他路由器通告，这些通告称为链路状态通告 (LSA)。通过这种方式，区域内的每台路由器都建立了一个本区域的完整的链路状态数据库。然后路由器根据收集到的链路状态信息来建立自己的网络拓扑图，形成一个到各个目的网段的路由表项。

从本质上来说，链路状态算法只将少量更新信息发送至网络各处，而距离矢量算法要发送大量更新信息至邻接路由器。由于链路状态算法收敛更快，因此它在一定程度上比距离向量算法更不易产生路由循环。但另一方面，链路状态算法要求比距离向量算法有更强的 CPU 能力和更多的内存空间，因此链路状态算法将会在实现时显得更昂贵一些。

各种路由算法都使用了许多种不同的度量标准去决定最佳路径。复杂的路由算法可能采用多种度量来选择路由，通过一定的加权运算，将它们合并为单个的复合度量，再填入路由表中，作为寻径的标准。通常所使用的度量有：跳数 (Hop)、带宽 (Bandwidth)、延时 (Delay)、负载 (Load)、可靠性 (Reliability)、通信成本 (Cost) 等。

(5) 内部网关协议 (IGP) 和外部网关协议 (EGP)

根据是否在一个自治域内部使用，动态路由协议分为内部网关协议 (IGP) 和外部网关协议 (EGP)。这里的自治域指一个具有统一管理机构、统一路由策略的网络。自治域内部采用的路由选择协议称为内部网关协议，常用的有 RIP、OSPF、IGRP、EIGRP；外部网关协议主要用于多个自治域之间的路由选择，常用的是 BGP 和 BGP-4。

5.4.1 静态路由

当网络集模较小，网络拓扑结构相对固定时，可以采用静态路由来构建我们的网络。

静态路由的配置命令如下:

```
Router(config)# ip route <network> [mask] [address|interface] [distance] [permanent]
```

其中各参数的含义见表 5-14。

表 5-14

静态路由配置参数的含义

项 目	含 义
network	目标网络的网路号
mask	子网掩码
address	下一跳 IP 地址
interface	本端的接口号码
distance	管理距离, 缺省值为 1
permanent	表明这个路径是永远存在

下面我们通过一个具体的例子来说明如何用静态路由来构建网络, 如图 5-93 所示。

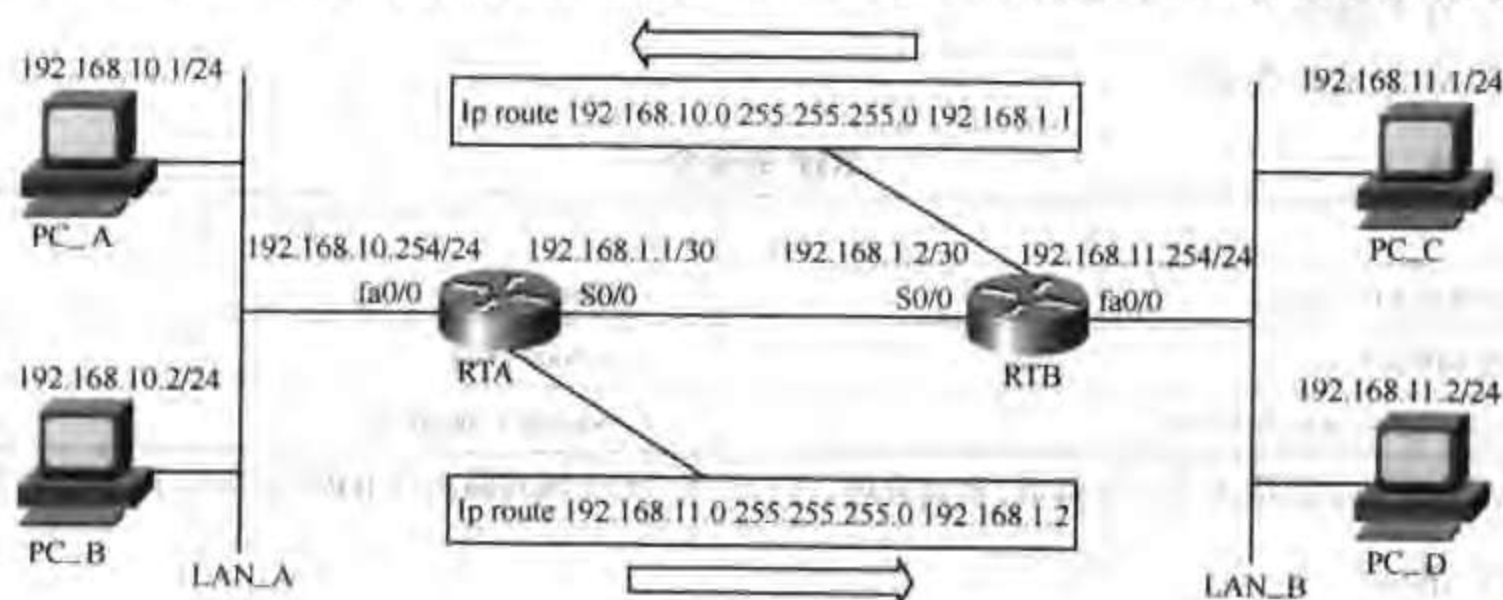


图 5-93 静态路由示例

注意: 在配置静态路由时千万要记住, 在远端的路由器上也要配置返回的路由, 始终要记住“通信是双向的”。

默认路由是静态路由的一个特例。它表明当路由表中不存在目的网络的路由信息时, 数据分组就被发送到默认路由所指的地址, 如图 5-94 所示。默认路由的配置命令如下:

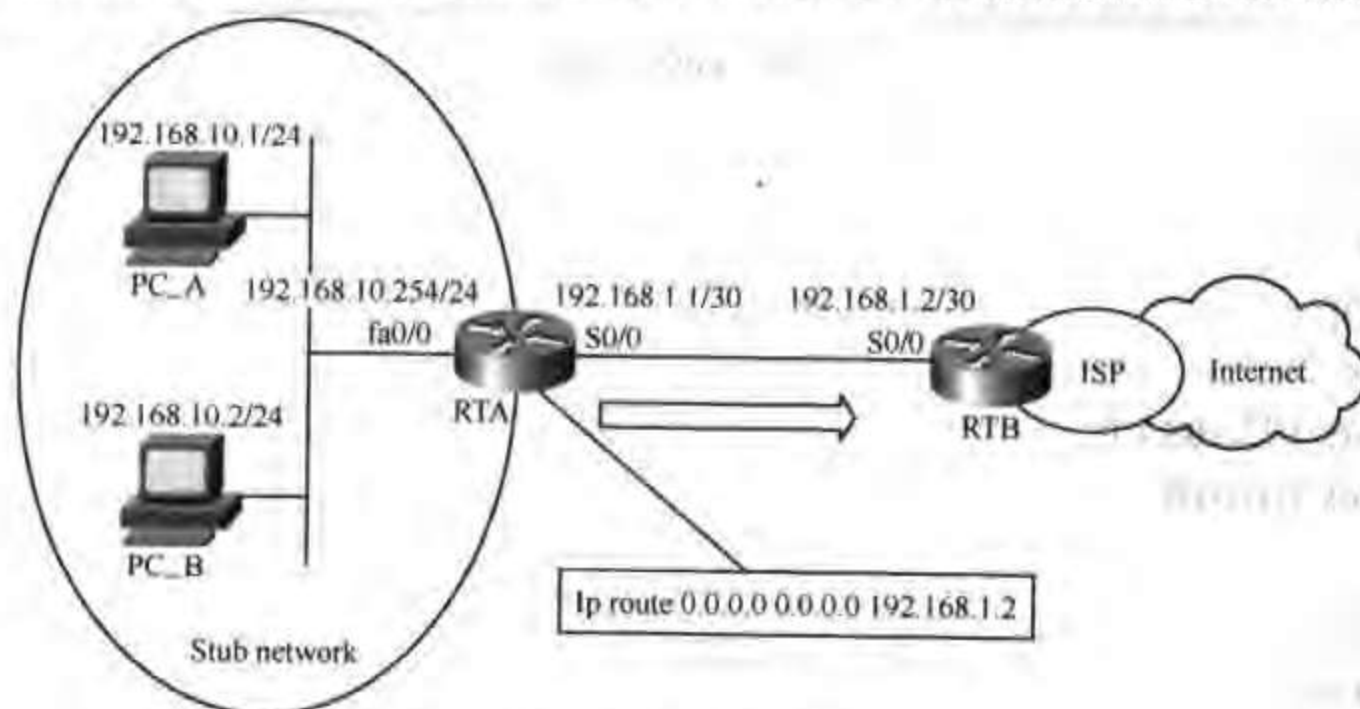


图 5-94 默认路由示例


```
Router(config)# ip route 0.0.0.0 0.0.0.0 <IP- address-of-next-hop-router>
```

5.4.2 RIP 协议

RIP (Routing information Protocol) 是应用较早、使用较普遍的一种内部网关协议 (IGP, Interior Gateway Protocol), 适用于小型同类网络, 是典型的距离矢量 (Distance-Vector) 路由协议。

RIP 包括两个版本, 版本 1 通过广播 UDP 报文来交换路由信息, 版本 2 通过使用组播 (224.0.0.9) 来交换路由信息。RIP 采用跳数 (Hop) 作为尺度来衡量路由距离, 跳数是一个数据分组到达目标所必须经过的路由器的数目。如果到相同目标有两个不等速或不同带宽的路由器, 但跳跃计数相同, 则 RIP 认为两个路由是等距离的。RIP 最多支持的跳数为 15, 即在源和目的网间所要经过的最多路由器的数目为 15 个, 跳数 16 表示不可达。

- (1) 有关命令
- 有关命令见表 5-15。

表 5-15 RIP 的命令

任 务	命 令
指定使用 RIP 协议	router rip
指定 RIP 版本	version {1 2}
指定与该路由器相连的网络	network network

注: Cisco 的 RIP 版本 2 支持验证、密钥管理、路由汇总、无类域间路由 (CIDR) 和变长子网掩码 (VLSM)

- (2) 举例
- 一种典型的 RIP 配置如图 5-95 所示。



图 5-95 RIP 配置示例

配置如下:

路由器 1:

```
router rip
version 2
network 192.168.1.0
network 10.0.0.0
!
```

路由器 2:

```
router rip
version 2
```



```
network 192.168.1.0
network 172.16.0.0
```

！
相关调试命令：

```
show ip protocol
show ip route
```

5.4.3 EIGRP 协议

EIGRP（加强型内部网关路由协议）是 Cisco 公司开发的距离矢量路由协议，它支持 IP、IPX 等多种网络层协议，是另一种内部网关协议（IGP）。EIGRP 是一个平衡混合型路由协议（Cisco 公司创造的术语），既有传统的距离矢量协议的特点（路由信息依靠邻居路由器通告，遵守路由水平分割和毒性逆转规则，路由自动归纳，配置简单），又有传统的链路状态路由协议的特点，即没有路由跳数的限制，当路由信息发生变化时，采用增量更新的方式，保留对所有可能路由（网络的拓扑结构）的了解、支持变长子网掩码、路由手动归纳。该协议同时又具有自己独特的特点：支持非等成本路由上的负载均衡，采用差分更新算法（DUAL）在确保无路由环路的前提下，收敛迅速。因而适用于中、大型网络。

（1）有关命令

EIGRP 的有关命令见表 5-16。

表 5-16 EIGRP 的有关命令

任 务	命 令
指定使用 eigrp 协议	<code>router eigrp autonomous-system</code>
指定与该路由器相连的网络	<code>network network</code>
指定与该路由器相邻的节点地址	<code>neighbor ip-address</code>

注：autonomous-system 可以随意建立，并非实际意义上的 autonomous-system，但运行 eigrp 的路由器要想交换路由更新信息其 autonomous-system 需相同。

（2）举例

EIGRP 的配置示例如图 5-96 所示。

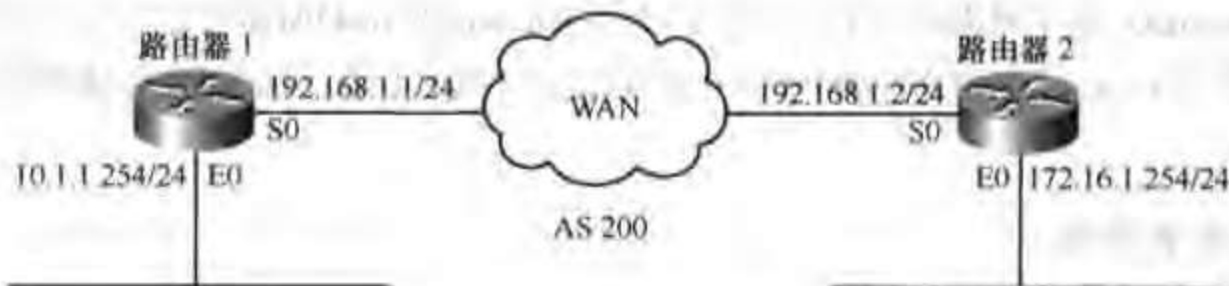


图 5-96 EIGRP 配置示例

配置如下：

路由器 1：

```
router eigrp 200
```



```
network 192.168.1.0
network 10.0.0.0
!
```

路由器 2:

```
router eigrp 200
network 192.168.1.0
network 172.16.0.0
!
```

相关调试命令:

```
show ip protocol
show ip route
```

5.4.4 OSPF 协议

OSPF (Open Shortest Path First) 是一个由网间工程任务组织 (IETF) 的内部网关协议工作组为 IP 网络开发的一种链路状态路由协议, 它也是一种内部网关路由协议 (IGP)。

链路是路由器接口的另一种说法, 因此 OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库, 生成最短路径树, 每个 OSPF 路由器使用这些最短路径构造路由表。其文档见 RFC2178。

(1) 有关命令

OSPF 协议的有关命令见表 5-17。

表 5-17 OSPF 的命令

任 务	命 令
指定使用 OSPF 协议	<code>router ospf process-id</code>
指定与该路由器相连的网络	<code>network address wildcard-mask area area-id</code>
指定与该路由器相邻的节点地址	<code>neighbor ip-address</code>

注: 1. OSPF 路由进程 process-id 必须指定范围在 1~65535 之内, 多个 OSPF 进程可以在同一个路由器上配置, 但最好不这样做。多个 OSPF 进程需要多个 OSPF 数据库的副本, 必须运行多个最短路径算法的副本。process-id 只在路由器内部起作用, 不同路由器的 process-id 可以不同。

2. wildcard-mask 是子网掩码的反码, 网络区域 ID area-id 为 0~4294967295 内的十进制数, 也可以是带有 IP 地址格式的 x.x.x.x。当网络区域 ID 为 0 或 0.0.0.0 时为主干域。不同网络区域的路由器通过主干域学习路由信息。

(2) 基本配置举例:

OSPF 的基本配置如图 5-97 所示。

配置如下:

路由器 1:

```
!
router ospf 100
```



```

network 192.168.1.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.255 area 1
!

```

!

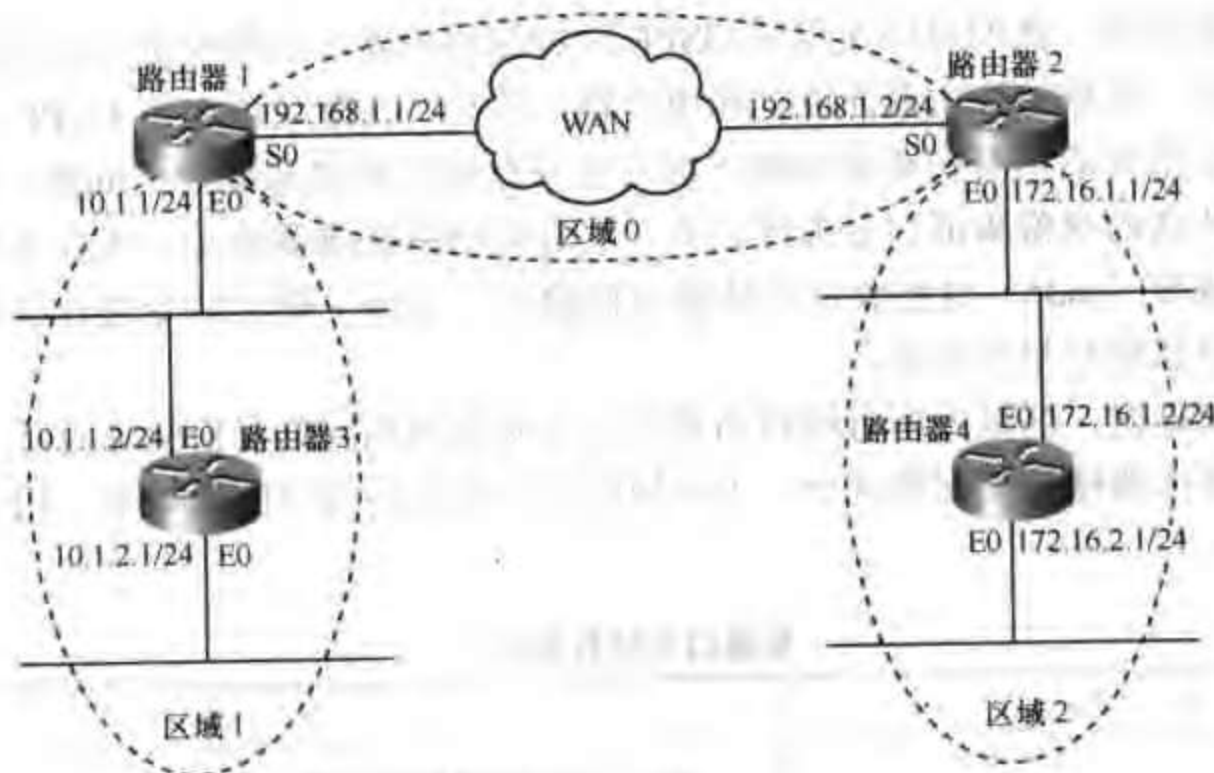


图 5-97 OSPF 配置示例

路由器 2:

!

```
router ospf 200
```

```
network 192.168.1.0 0.0.0.255 area 0
```

```
network 172.16.1.0 0.0.0.255 area 2
```

!

路由器 3:

!

```
router ospf 300
```

```
network 10.1.0.0 0.0.255.255 area 1
```

!

路由器 4:

!

```
router ospf 400
```

```
network 172.16.0.0 0.0.255.255 area 2
```

!

相关调试命令:

```
debug ip ospf events
```

```
debug ip ospf packet
```

```
show ip ospf
```

```
show ip ospf database
```



```
show ip ospf interface
show ip ospf neighbor
show ip route
```

(3) 使用身份验证

为了安全的原因，我们可以在相同 OSPF 区域的路由器上启用身份验证的功能，只有经过身份验证的同一区域的路由器才能互相通告路由信息。在默认情况下 OSPF 不使用区域验证。通过两种方法可启用身份验证功能：纯文本身身份验证和消息摘要（md5）身份验证。纯文本身身份验证传送的身份验证口令为纯文本，它会被网络探测器确定，所以不安全，不建议使用。而消息摘要（md5）身份验证在传输身份验证口令前，要对口令进行加密，所以一般建议使用此种方法进行身份验证。

使用身份验证时，区域内所有的路由器接口必须使用相同的身份验证方法。为启用身份验证，必须在路由器接口配置模式下，为区域的每个路由器接口配置口令。相关的命令见表 5-18。

表 5-18 配置口令的有关命令

任 务	命 令
指定身份验证	area area-id authentication [message-digest]
使用纯文本身身份验证	ip ospf authentication-key password
使用消息摘要(md5)身份验证	ip ospf message-digest-key keyid md5 key

以下列举两种验证设置的示例，示例的网络分布及地址分配环境与以上基本配置举例相同，只是在路由器 1 和路由器 2 的区域 0 上使用了身份验证的功能。

例 1. 使用纯文本身身份验证，配置如下：

路由器 1:

```
interface ethernet 0
ip address 10.1.1.1 255.255.255.0
!
interface serial 0
ip address 192.168.1.1 255.255.255.0
ip ospf authentication-key cisco
!
router ospf 100
network 192.168.1.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.255 area 1
area 0 authentication
```

路由器 2:

```
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
!
```



```
interface serial 0
ip address 192.168.1.2 255.255.255.0
ip ospf authentication-key cisco
```

```
!
router ospf 200
network 192.168.1.0 0.0.0.255 area 0
network 172.16.1.0 0.0.0.255 area 2
area 0 authentication
```

```
!
```

例 2. 消息摘要(md5)身份验证, 配置如下:

路由器 1:

```
interface ethernet 0
ip address 10.1.1.1 255.255.255.0
!
interface serial 0
ip address 192.168.1.1 255.255.255.0
ip ospf message-digest-key 1 md5 cisco
```

```
!
```

```
router ospf 100
network 192.168.1.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.255 area 1
area 0 authentication message-digest
```

```
!
```

路由器 2:

```
interface ethernet 0
ip address 172.16.1.1 255.255.255.192
!
```

```
interface serial 0
ip address 192.168.1.2 255.255.255.0
ip ospf message-digest-key 1 md5 cisco
```

```
!
```

```
router ospf 200
network 192.168.1.0 0.0.0.255 area 0
network 172.16.1.0 0.0.0.255 area 2
area 0 authentication message-digest
```

```
!
```

相关调试命令:

```
debug ip ospf adj
debug ip ospf events
```


5.4.5 BGP 协议

BGP 是为 TCP / IP 互联网设计的外部网关协议，用于多个自治域之间。它既不是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法。它的主要功能是与其他自治域的 BGP 交换网络可达信息。各个自治域可以运行不同的内部网关协议。BGP 更新信息包括网络号 / 自治域路径的成对信息。自治域路径包括到达某个特定网络须经过的自治域串，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。

5.4.6 重新分配路由

在实际工作中，我们会遇到使用多个 IP 路由协议的网络。为了使整个网络正常地工作，必须在多个路由协议之间进行成功的路由再分配。

以下列举了 OSPF 与 RIP 之间重新分配路由的设置范例，如图 5-98 所示。

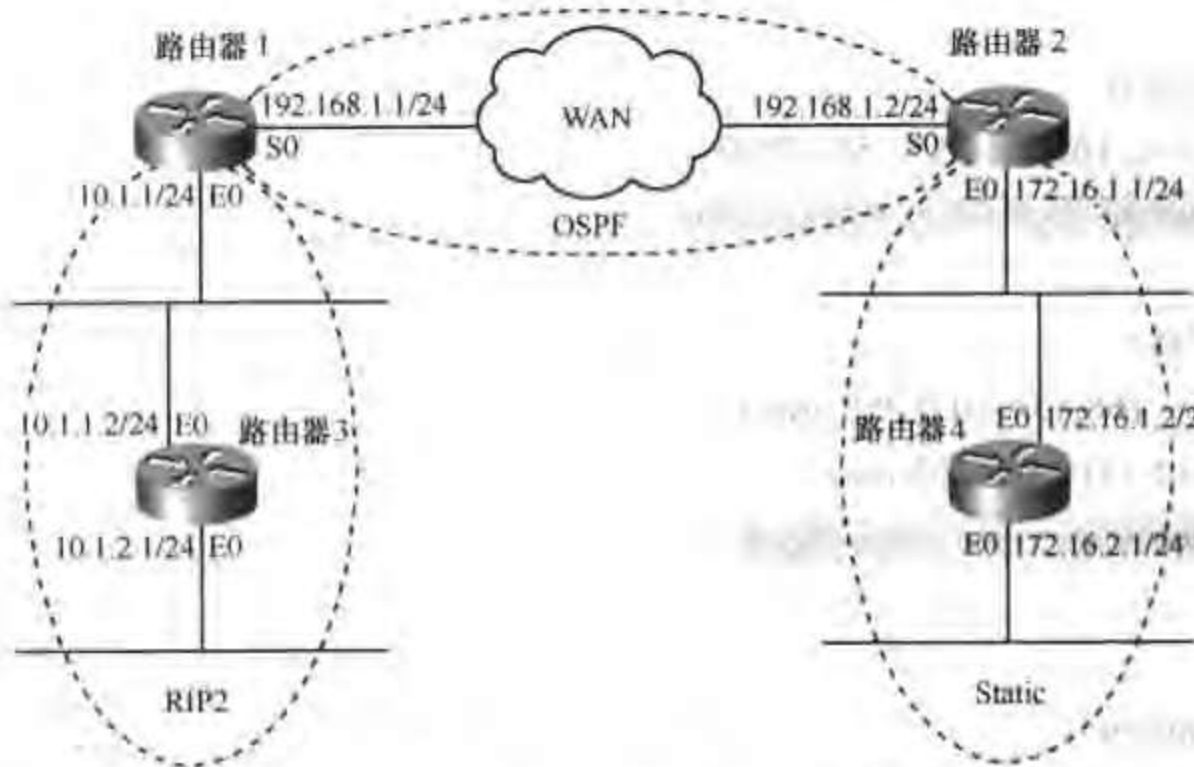


图 5-98 路由重分布配置示例

路由器 1 的 Serial 0 端口和路由器 2 的 Serial 0 端口运行 OSPF，在路由器 1 的 Ethernet 0 端口运行 RIP 2，路由器 3 运行 RIP2，路由器 2 有指向路由器 4 的 192.168.2.0/24 网的静态路由，路由器 4 使用默认静态路由。需要在路由器 1 和路由器 3 之间重新分配 OSPF 和 RIP 路由，在路由器 2 上重新分配静态路由和直连的路由。

本案例所涉及的命令见表 5-19。

表 5-19 路由重分配的部分命令

任 务	命 令
重新分配直连的路由	redistribute connected
重新分配静态路由	redistribute static
重新分配 OSPF 路由	redistribute ospf process-id metric metric-value
重新分配 RIP 路由	redistribute rip metric metric-value

配置如下:

路由器 1:

```
interface ethernet 0
  ip address 10.1.1.1 255.255.255.0
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
!
router ospf 100
  redistribute rip metric 10
  network 192.168.1.0 0.0.0.255 area 0
!
router rip
  version 2
  redistribute ospf 100 metric 1
  network 10.1.1.0
```

!

路由器 2:

```
interface ethernet 0
  ip address 172.16.1.1 255.255.255.0
!
interface serial 0
  ip address 192.168.1.2 255.255.255.0
!
router ospf 200
  redistribute connected subnet
  redistribute static subnet
  network 192.168.1.0 0.0.0.255 area 0
!
ip route 172.16.2.0 255.255.255.0 172.16.1.2
!
```

路由器 3:

```
interface ethernet 0
  ip address 10.1.1.2 255.255.255.0
!
router rip
  version 2
  network 10.1.1.0
!
```



```
路由器 4:
interface ethernet 0
 ip address 172.16.1.2 255.255.255.0
!
interface ethernet 1
 ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

5.5 访问控制和地址转换

5.5.1 访问控制

访问控制列表（Access Control List, ACL）作为一种数据分组过滤的手段，有着非常广泛的应用。应用在路由器接口上的访问控制列表用来控制端口进出的数据分组。访问列表（access-list）就是一系列允许和拒绝条件的集合，通过访问列表可以过滤进入和送出的数据分组的请求，实现对路由器和网络的安全控制。路由器一个一个地检测分组与访问列表的条件，在满足第一个匹配条件后，就可以决定路由器接收或拒收该分组。如果一个数据分组的报头跟表中某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。数据分组只有在跟第一个判断条件不匹配时，它才被交给 ACL 中的下一个条件判断语句进行比较。如果匹配（假设为允许发送），则不管是第一条还是最后一条语句，数据都会立即发送到目的接口。如果所有的 ACL 判断语句都检测完毕，仍没有匹配的语句出口，则该数据分组将视为被拒绝而被丢弃。

访问控制列表具有区分数据分组的功能，因此，它可以控制“什么样的数据分组”，可以做“什么样的事情”，例如：

- ACL 可以限制特定用户（网段或主机）或特定类型的网络流量，从而提高网络性能；
- ACL 可以在路由器接口处决定哪种类型（如 HTTP、DNS）的通信流量被转发或被阻塞，从而提高网络的安全；
- ACL 可用于 QoS 保证中，提供对通信流量的控制手段，使得不同的数据流具有不同的优先级，比如语音数据比邮件传输的数据具有更高的优先级；
- ACL 可用于 DDR 中，来定义哪些数据分组可以触发拨号；
- ACL 可用于地址转换（NAT）中，来定义哪些数据分组需要进行地址转换；
- ACL 还广泛的应用在路由策略中，用于路由信息的过滤。

当访问控制列表用于数据流的过滤时，定义的列表必须应用到相应的接口上（ip access-group access-list-number {in | out}），由于对一个接口而言数据的流动是双向的，因此在应用此列表时，需要说明它是应用于流入的数据还是流出的数据。流入和流出路由器的访问控制如图 5-99 和图 5-100 所示。



图 5-99 入口访问控制



图 5-100 出口访问控制

访问控制列表主要包括两种类型：标准访问列表和扩展访问列表。标准 ACL 只检查分组的源地址；扩展 ACL 既检查分组的源地址，也检查分组的目的地地址，也可以检查特殊的协议类型、端口以及其他参数，因此具有更大的自由度。在路由器配置中，标准 ACL 和扩展 ACL 的区别是由 ACL 的序号来体现的，标准 ACL 的序列号范围是 1~99，扩展 ACL 的序列号范围是 100~199。

下面我们来讲解如何配置访问控制列表。ACL 的配置分为两个步骤：

第一步：在全局配置模式下，使用下列命令创建 ACL：

```
Router (config)# access-list access-list-number {permit | deny } {test-conditions}
```

其中，access-list-number 为 ACL 的序列号。人们使用较频繁的序列号是标准的 IP ACL (1~99) 和扩展的 IP ACL (100~199)。

注意：在路由器中，如果使用 ACL 的序列号进行配置，则列表不能插入或删除行（动态编辑）。如果列表要插入或删除一行，必须先去掉该 ACL，然后重新配置。当然可以将原 ACL 粘贴到一个文本文件中，然后进行相应的修改，完成后再粘贴回路由器中，采用这种“拷贝—粘贴”方法也是配置路由器的一个技巧。

第二步：在接口配置模式下，使用 access-group 命令将第一步中创建的 ACL 应用到某一接口上：

```
Router (config-if)# ip access-group access-list-number {in | out }
```


其中，in 和 out 参数可以控制接口中不同方向的数据分组，ACL 在一个接口可以进行双向控制（即配置两条命令，一条为 in，一条为 out），但是在一个接口的一个方向上，只能有一个 ACL 控制。

注意：把定义好的 ACL 应用在网络的什么地方，是能否实现原有的目的和有效地减少不必要的通信流量的关键。通常情况下，标准 ACL 要尽量靠近目的端，扩展 ACL 要尽量靠近源端。当然这不是绝对的，具体放在那个位置，要根据具体的情况分析。下面我们通过一个例子来说明。

在下面的案例中，LAN_A 只允许 LAN_B 访问，拒绝其他网段的数据。根据此要求，定义了一个标准访问列表（`access-list 1 permit 192.168.11.0 0.0.0.255`），下面我们来分析将此访问列表放置在网络的哪个位置能最好地实现此功能。

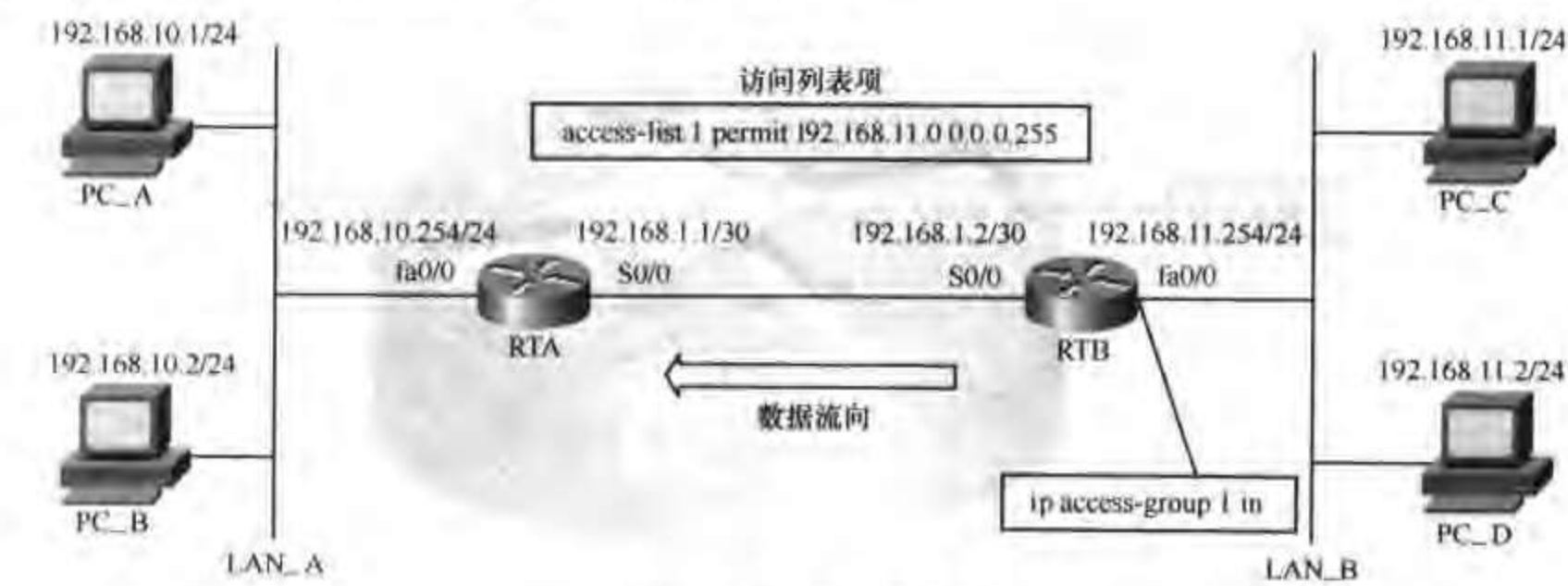


图 5-101 标准 ACL 放置位置之一

当将定义的 ACL 放置在 RTB 的 fa0/0 接口时（如图 5-101 所示），根据列表的定义，只有源自 192.168.11.0 网段的数据可以从此接口进入，如果此接口下还有其他的网段将被过滤掉。就本案例而言，如此放置将不能满足用户的要求，因为用户的目的是只允许源自 192.168.11.0 网段的数据进入 192.168.10.0 网段，而图 5-101 中的放置方式将不能过滤 192.168.1.0/30 网段的数据进入 LAN_A。同时，如果 RTA 如果还有其他的接口，那么图 5-101 中的放置方式也不能过滤其他网段的数据通过该接口进入 LAN_A。



图 5-102 标准 ACL 放置位置之二

当将定义的 ACL 放置在 RTB 的 S0/0 接口时 (如图 5-102 所示), 根据列表的定义, 只有源自 192.168.11.0 网段的数据可以从此接口送出, 其他的网段将被过滤掉。和如图 5-101 所示的位置的分析一样, 如此放置将不能满足用户的要求, 因为图 5-102 所示的放置方式同样将不能过滤 192.168.1.0/30 网段的数据进入 LAN_A。同时, 如果 RTA 如果还有其他的接口, 那么该放置方式也不能过滤其他网段的数据通过该接口进入 LAN_A。

当将定义的 ACL 放置在 RTA 的 S0/0 接口时 (如图 5-103 所示), 根据列表的定义, 只有源自 192.168.11.0 网段的数据可以从此接口进入路由器, 其他的网段将被过滤掉。就本案例而言, 如此放置将能够满足用户的要求, 因为用户的目的实际是只允许源自 192.168.11.0 网段的数据进入 192.168.10.0 网段, 图 5-103 所示的放置方式将保证只有 192.168.11.0 网段的数据可以进入路由器 RTA, 因为 RTA 除 fa0/0 之外只有这一个接口, 因此对进入的数据分组做的过滤就相当于对送出的数据分组作过滤。同时, 如此放置方式还可以节省路由器的资源 (区别于下面介绍的放置方式)。

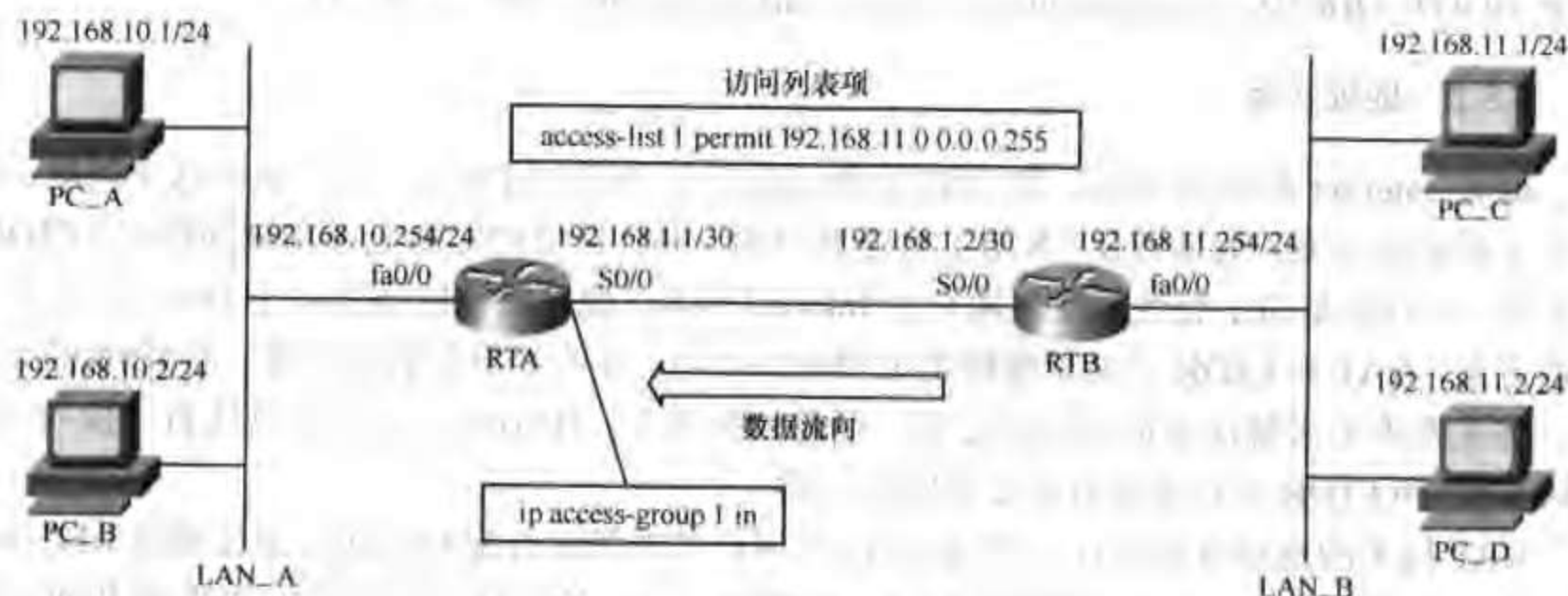


图 5-103 标准 ACL 放置位置之三

当然如果 RTA 还有其他的接口, 那么图 5-103 中的放置方式将不能过滤其他网段的数据通过该接口进入 LAN_A, 从而不能满足用户需求。

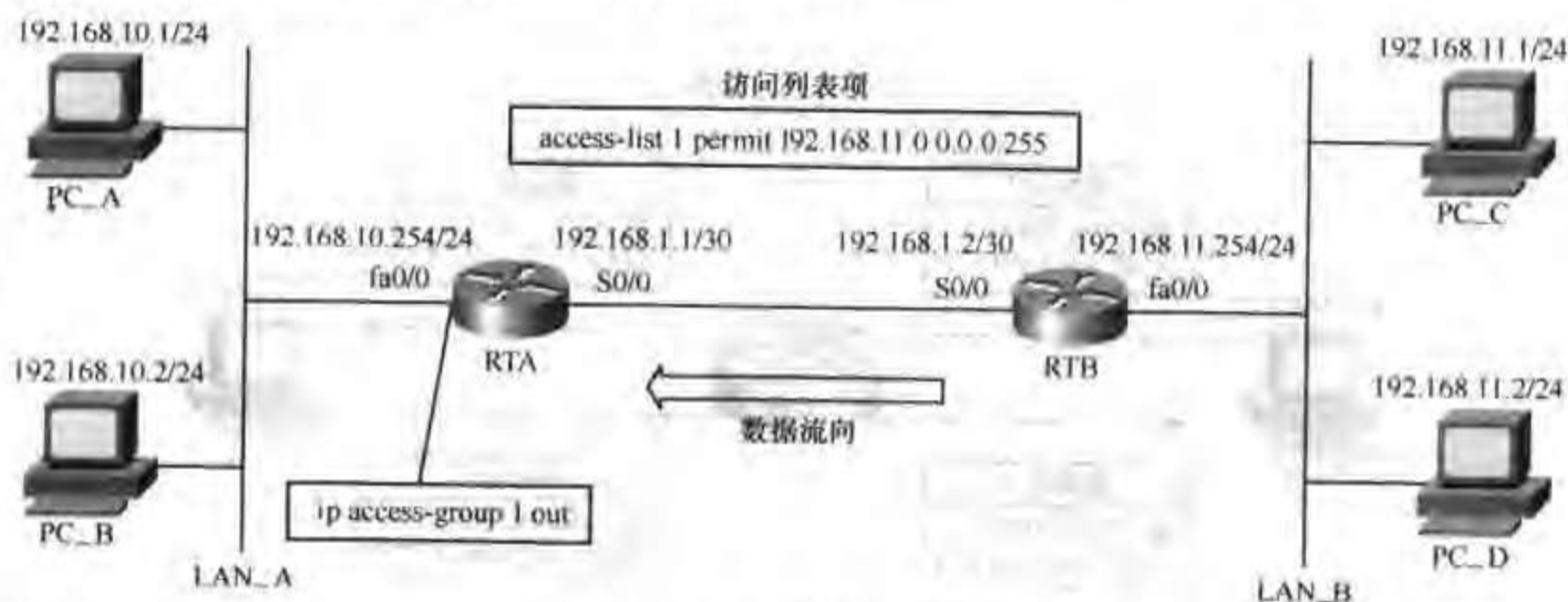


图 5-104 标准 ACL 放置位置之四

当将定义的 ACL 放置在 RTA 的 fa0/0 接口时 (如图 5-104 所示), 根据列表的定义, 只

有源自 192.168.11.0 网段的数据可以从此接口送出,从而进入 LAN_A,其他的网段将被过滤掉。就本案例而言,如此放置是最能够满足用户的要求的,因为用户的目的是只允许源自 192.168.11.0 网段的数据进入 192.168.10.0 网段,图 5-104 中的放置方式将保证只有 192.168.11.0 网段的数据可以进入 LAN_A,不管 RTA 是否还有其他的接口。当然,如果 RTA 没有其他的接口,我们建议采用如图 5-103 所示的放置方式,因为那样会节省路由器的资源。

与标准访问列表相比,扩展访问列表更能精确地定义一个数据流。因为标准 ACL 只根据源地址来标识数据流,而扩展 ACL 可根据源地址、目的地址、协议号、源端口、目的端口这 5 个元素来标识一个数据流。

访问控制列表涉及的内容非常多,除了标准和扩展 ACL 之外还有命名 ACL、动态 ACL (Lock-and-key)、反身 ACL (reflect)、基于内容的 ACL (CBAC)、基于时间的 ACL 等等。如果读者感兴趣,请参考 Cisco 的相关文档。

http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Technologies:ACCESS-LIST_ARP_BOOT_DHCP&s=Implementation_and_Configuration#Samples_and_Tips

5.5.2 地址转换

随着 Internet 的迅速发展,IP 地址短缺已成为十分突出的问题。为了解决这个问题,出现了多种解决方案,地址转换 (NAT) 就是其中的一种。其他的比如无类别域间路由 (CIDR) 的开发,其目的是为了有效地使用现有的 Internet 地址。地址短缺的根源在于 IPv4 中 32 位的编址方案,NAT 和 CIDR 只能是缓解地址短缺的趋势,并不能真正解决问题。而 IPv6 的开发是一种从根本上来解决地址短缺的方案,但是目前来看,IPv6 投入商业运营还有一段时间,所以 NAT 和 CIDR 在目前来看还是非常有用的。

NAT 技术的原理就是指在一个网络内部,用户可以随意分配 IP 地址(建议采用 RFC1918 指定的私有 IP 地址),而不需要经过申请。在网络内部,各计算机间通过内部的 IP 地址进行通信。当内部的计算机需要访问外部 Internet 网络时,具有 NAT 功能的设备(比如:路由器)负责将其内部的 IP 地址转换为合法的 IP 地址(即经过申请的 IP 地址)。从而使得一个私有网络可以通过少量的 Internet 注册的 IP 地址连接到外部世界。NAT 的原理如图 5-105 所示。

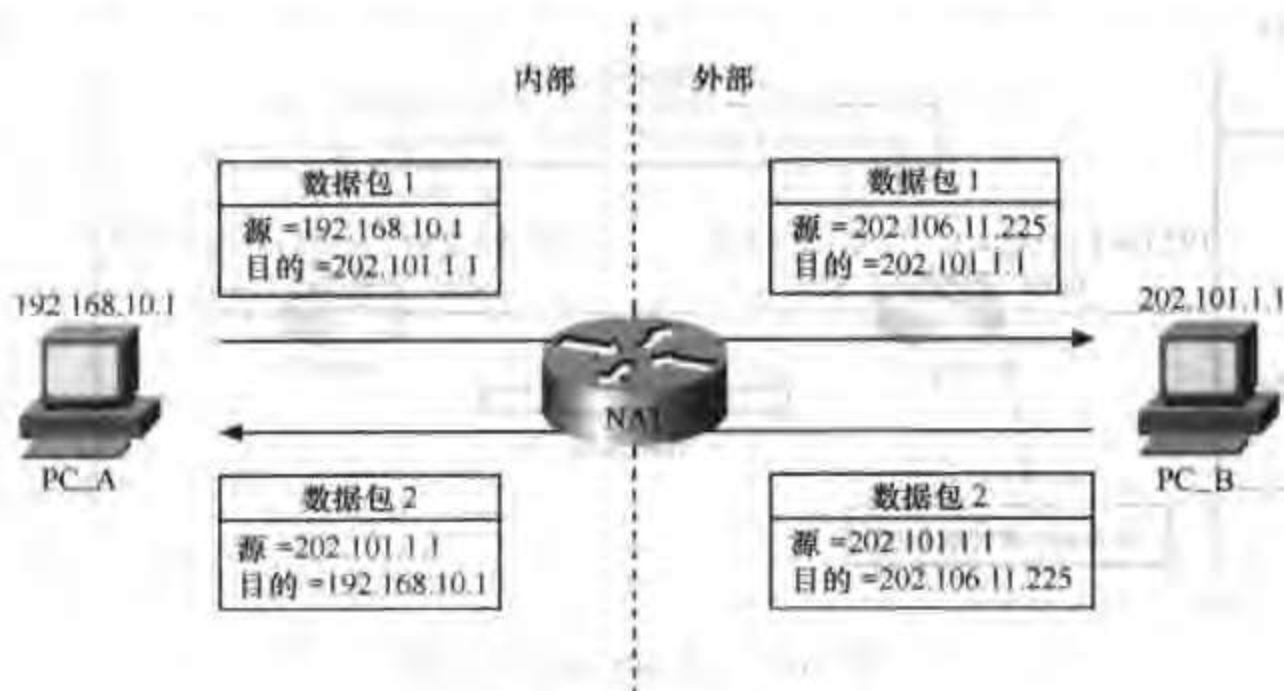


图 5-105 NAT 原理

在图 5-105 中, PC_A 具有一个私有 IP 地址 (RFC1918 指定), PC_B 具有一个公网的 IP 地址, 当 PC_A 向 PC_B 发送一个数据分组时, 数据分组要通过一个运行 NAT 的设备 (这里是一台路由器, 也可以是防火墙)。NAT 将数据分组中的源地址 (192.168.10.1) 转换成一个公网地址 (可以在 Internet 上路由的公开地址, 这里是 202.106.11.225。注意, 此地址需要在路由器上设置, 具体配置方法见以下部分), 并将此转换后的数据分组转发出去; PC_B 给 PC_A 发送回应数据分组的时候, 数据分组的地址是 202.106.11.225, 数据分组再次通过 NAT 路由器时, 目的地址又换成了 PC_A 的私有地址 (192.168.10.1)。这样, PC_A 和 PC_B 间就完成了通信。

需要配置 NAT 功能的路由器至少要有两个内部接口 (Inside), 一个外部接口 (Outside)。内部接口连接的网络用户使用的是私有 IP 地址; 外部接口连接的是外部的网络, 使用电信部门分配的 IP 地址 (可以是公有 IP 也可以使用私有 IP)。另外, 想要使用 NAT 功能, 路由器的 IOS 必须支持 NAT 功能。

关于 NAT 的几个概念:

(1) 内部本地地址 (Inside Local Address): 分配给内部设备的地址 (通常为 RFC1918 定义的私有 IP 地址)。

(2) 内部全局地址 (Inside Global Address): 通过这个地址, 外部可以知道内部设备。需要申请才可取得的 IP 地址。

(3) 外部本地地址 (Outside Local Address): 通过这个地址, 内部设备可以知道外部设备。

(4) 外部全局地址 (Outside Global Address): 分配给外部设备的地址。这些地址不会向内部公布。

通过上面的介绍, 读者对 NAT 的工作原理有了一定的了解, 下面就来看看如何在 Cisco IOS 的路由器上配置 NAT。

NAT 设置可以分为静态地址转换、动态地址转换和复用动态地址转换三种方式。

(1) 静态地址转换

静态地址转换将内部本地地址与内部合法地址进行一对一地转换, 且需要指定与哪个合法地址进行转换。如果内部网络有 WWW 服务器或 FTP 服务器等可以为外部用户提供服务, 则这些服务器的 IP 地址必须采用静态地址转换, 以便外部用户可以使用这些服务。

静态地址转换基本配置步骤如下:

步骤 1、在内部本地地址与内部合法地址之间建立静态地址转换。在全局设置状态下输入:
ip nat inside source static 内部本地地址 内部合法地址

例如: ip nat inside source static 192.168.11.201 202.106.11.231

步骤 2、指定连接内部网络的内部端口, 在连接内网的端口设置状态下输入:
ip nat inside

步骤 3、指定连接外部网络的外部端口, 在连接外网的端口设置状态下输入:
ip nat outside

注: 可以根据实际需要定义多个内部端口及多个外部端口。

(2) 动态地址转换

动态地址转换也是将内部本地地址与内部合法地址一对一地转换, 但是动态地址转换是从内部合法地址池中动态地选择一个未使用的地址来对内部本地地址进行转换的。其转换步

骤如下:

步骤 1. 建立一个全局地址池

`ip nat pool wyx 起始地址 结束地址 掩码`

例如: `ip nat pool wyx 202.106.11.225 202.106.11.230 netmask 255.255.255.240`

步骤 2. 定义一个标准访问列表

`access-list 10 permit 地址 通配符 any`

例如: `access-list 10 permit 192.168.11.0 0.0.0.255 any`

步骤 3. 定义内部地址与内部全局地址池之间的转换

`ip nat inside source list 10 pool wyx`

步骤 4. 定义内部端口和外部端口 (同上)

`ip nat inside /ip nat outside`

(3) 复用动态地址转换 (PAT)

复用动态地址转换首先是一种动态地址转换,但是它可以允许多个内部本地地址共用一个内部合法地址。对只申请到少量 IP 地址但却经常同时有多个用户接入外部网络的情况,这种转换极为有用。其转换步骤如下:

步骤 1. 建立一个全局地址池

`ip nat pool wyx 起始地址 结束地址 掩码`

例如: `ip nat pool wyx 202.106.11.225 202.106.11.225 netmask 255.255.255.240`

步骤 2. 定义一个标准访问列表

`access-list 10 permit 地址 通配符 any`

例如: `access-list 10 permit 192.168.11.0 0.0.0.255 any`

步骤 3. 定义内部地址和内部全局地址池之间的转换

`ip nat inside source list 10 pool wyx overload`

步骤 4. 定义内部端口和外部端口 (同上)

`ip nat inside /ip nat outside`

下面通过一个具体的案例来了解一下 NAT 在企业网中的具体应用,如图 5-106 所示。

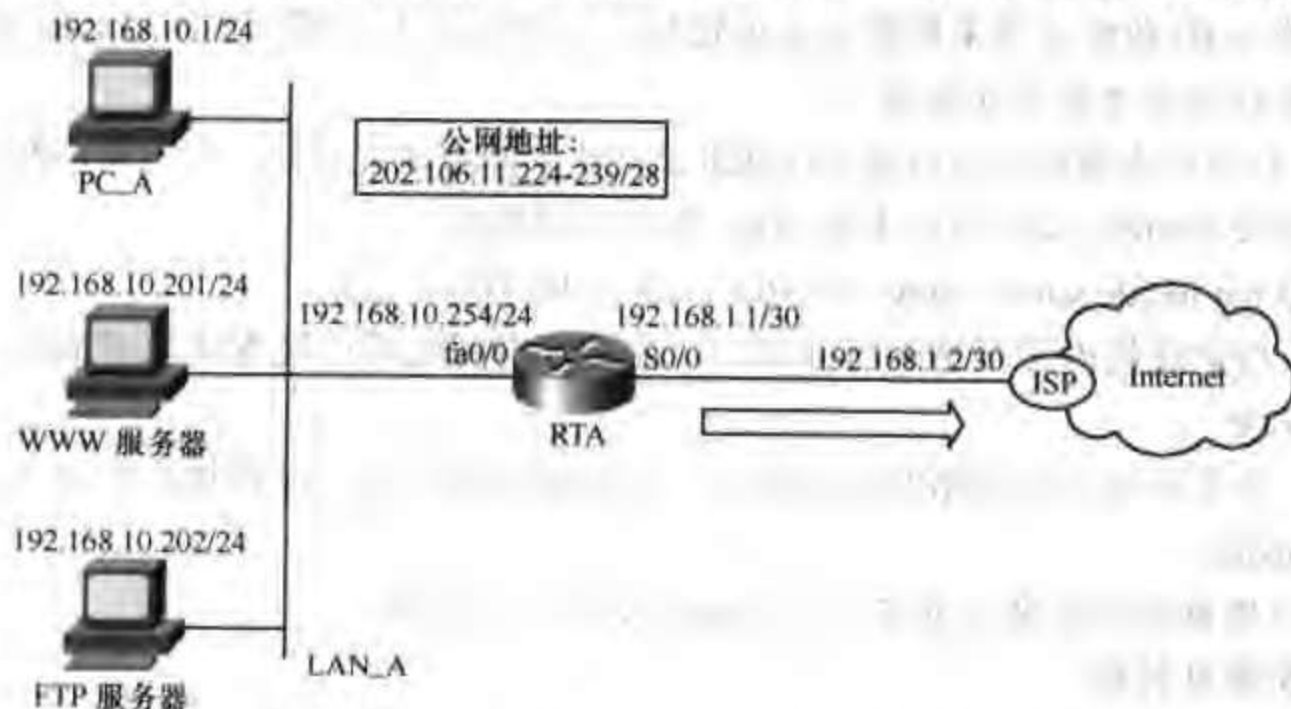


图 5-106 NAT 配置案例

在本案例中，LAN_A 是一个企业的内网，该企业申请了一根专线，获得 ISP 分配的 16 个公网的 IP 地址，地址为 202.106.11.224~239/28（注意：其中 202.106.11.224/28 是网络地址，202.106.11.239/28 是广播地址，这两个地址不可用，其他 14 个地址可用）。企业自己搭建了 WWW 和 FTP 服务器，用于企业的宣传和向用户提供下载服务。下面我们看如何配置企业的接入路由器 RTA 来实现以上的功能。

配置文档：

RTA

!

service timestamps debug uptime

service timestamps log uptime

service password-encryption

no service tcp-small-servers

no service udp-small-servers

!

hostname RTA

!

enable password cisco

!

no ip name-server

!

ip subnet-zero

no ip domain-lookup

ip routing

!

interface FastEthernet 0/0

no shutdown

description connected to LAN_A

ip address 192.168.10.254 255.255.255.0

! ---配置此接口为地址转换（NAT）的内接口：

ip nat inside

keepalive 10

!

interface FastEthernet 0/1

no description

no ip address

shutdown

!

interface Serial 0/0

no shutdown


```
description connected to Internet
```

```
ip address 192.168.1.1 255.255.255.252
```

! ---配置此接口为接口转换的外接口:

```
ip nat outside
```

```
encapsulation ppp
```

```
!
```

```
!
```

! ---取消访问控制列表“1”:

```
no access-list 1
```

! ---重新定义访问控制列表“1”为“允许 192.168.10.0/24 网段”:

```
access-list 1 permit 192.168.10.0 0.0.0.255
```

```
!
```

```
!
```

! ---配置静态 NAT 映射, 使内部地址 192.168.10.201 对应公网地址 202.106.11.231, 该配置主要用于向外提供服务的服务器:

```
ip nat inside source static 192.168.10.201 202.106.11.231
```

```
ip nat inside source static 192.168.10.202 202.106.11.232
```

```
!
```

! ---定义从 ISP 那里申请到的公网 IP 在企业内部的分配策略, 这里定义了一个地址池“RTA-natpool-1”, 它所涵盖的地址将被内网用户用来上网:

```
ip nat pool RTA-natpool-1 202.106.11.225 202.106.11.230 netmask 255.255.255.240
```

! ---将访问控制列表“1”与地址池“RTA-natpool-1”对应, 即如果“PC_A”将网关地址指向“192.168.10.254”, 当它上网时, 它的内网地址“192.168.10.1”将被转换为“202.106.11.225”~“202.106.11.230”中的一个; “overload”表示, 如果有多于地址池中定义的数量(比如有 20 用户)的用户访问外部, 那么多个内网地址可能会被转换为同一公网地址, 不同内网地址之间可以通过不同的端口来识别, 这样利用地址池定义的 6 个公网地址就可以带领所有的内网用户上网:

```
ip nat inside source list 1 pool RTA-natpool-1 overload
```

```
!
```

```
!
```

```
ip classless
```

```
!
```

```
ip route 0.0.0.0 0.0.0.0 Serial 0/0
```

```
no ip http server
```

```
snmp-server community public RO
```

```
no snmp-server location
```

```
no snmp-server contact
```

```
!
```

```
line console 0
```



```

exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
end

```

以上只是大致介绍了 NAT 的原理和一些基本的应用, 如果大家对 NAT 的其他应用感兴趣, 请参考 Cisco 的相关文档。该文档可登录下列网址查询:

http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Internetworking:NAT&s=Implementation_and_Configuration#Samples_and_Tips

5.6 Cisco 路由器经典配置案例

案例 1

企业总部和分支机构通过帧中继线路互连, 各分支采用异步拨号方式作为主链路的备份。

1. 网络拓扑

网络拓扑如图 5-107 所示。

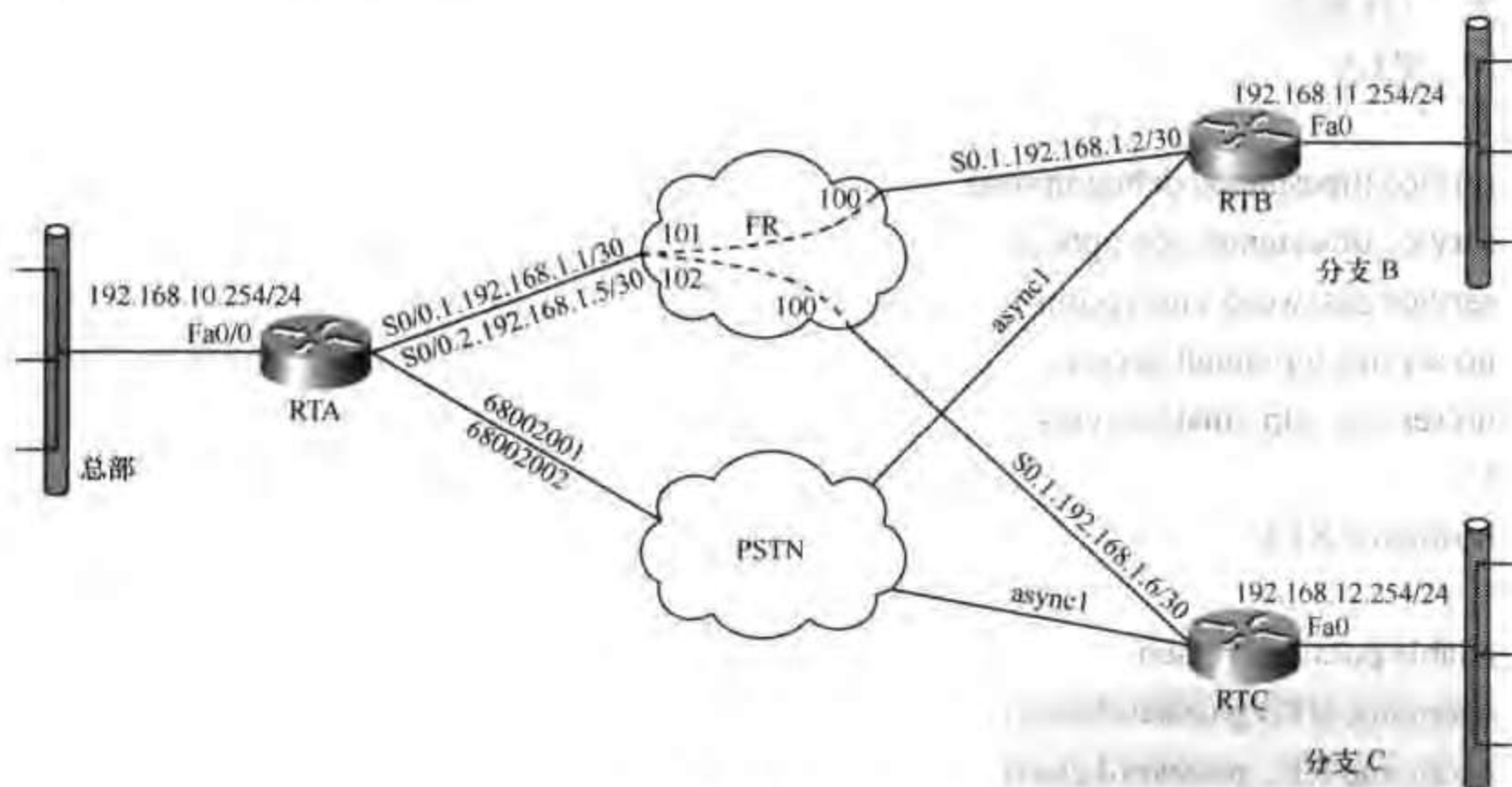


图 5-107 经典配置案例 1 拓扑图

说明: 企业总部和各分支所用的设备及其规格见表 5-20。

表 5-20 所用设备及其规格

产 品	描 述	数 量
总部设备		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP,32F/128D	1
CAB-ACA	插头,电源线,10A	1
S26C-12306	Cisco 2600 Ser IOS IP	1
NM-8AM	8 端口模拟 Modem 网络模块	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1
分支 B 设备		
CISCO1721	10/100BaseT 模块路由器 w/2 WAN 插槽, 32M 闪存/64M DRAM	1
CAB-ACA	插头,电源线,10A	1
S17C-12308T	Cisco 1700 IOS IP	1
WIC-1AM	1 端口模拟 Modem WAN 接口板	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1
分支 C 设备		
CISCO1721	10/100BaseT 模块路由器 w/2 WAN 插槽, 32M 闪存/64M DRAM	1
CAB-ACA	插头,电源线,10A	1
S17C-12308T	Cisco 1700 IOS IP	1
WIC-1AM	1 端口模拟 Modem WAN 接口板	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1

2. 具体配置

(1) RTA

```
!  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption  
no service tcp-small-servers  
no service udp-small-servers  
!  
hostname RTA  
!  
enable password cisco  
username RTB password cisco  
username RTC password cisco  
!  
no ip name-server  
!
```



```

ip subnet-zero
no ip domain-lookup
ip routing
!
interface Group-Async1
ip unnumbered FastEthernet0/0
encapsulation ppp
dialer-group 1

```

! ---为异步串口指定建立链路的方式，默认值是“dedicate”。可以有两种建立链路的方式：①直接方式（Dedicate）：拨号成功之后，直接采用链路层协议配置参数建立链路；②交互方式（Interactive）：拨号成功之后，主叫方向对端发送配置命令（与用户从远端手工键入配置命令效果相同），设置对端的链路层协议工作参数，然后建立链路。比较常用的是直接方式，但在与同样支持交互方式的路由器（如 Cisco 路由器等）互连时，采用交互方式显得更为灵活。

```

async mode interactive
! ---为拨入的模拟呼叫从地址池“pstnpool”中分配 IP 地址：
peer default ip address pool pstnpool
! ---指定 PPP 的认证方式，这里采用“pap”方式：
ppp authentication pap if-needed
! ---指定此模拟拨号组对应的端口：
group-range 33 40
!
!
interface FastEthernet 0/0
no shutdown
description connected to zb
ip address 192.168.10.254 255.255.255.0
no keepalive
!
interface FastEthernet 0/1
no description
no ip address
shutdown
!
interface Serial 0/0
no shutdown
no description
no ip address
encapsulation frame-relay

```



```

frame-relay lmi-type ansi
!
interface Serial 0/0.1 point-to-point
no shutdown
description connected to RTB
ip address 192.168.1.1 255.255.255.252
frame-relay interface-dlci 101 ietf
!
interface Serial 0/0.2 point-to-point
no shutdown
description connected to RTC
ip address 192.168.1.5 255.255.255.252
frame-relay interface-dlci 102 ietf
!
ip local pool pstnpool 192.168.10.221 192.168.10.240
!
! ---为拨号组 1 指定激活拨号的条件，这里所有的 IP 访问都可以激活拨号：
no dialer-list 1
dialer-list 1 protocol ip permit
!
ip route 192.168.11.0 255.255.255.0 Serial 0/0.1 1
ip route 192.168.12.0 255.255.255.0 Serial 0/0.2 1
ip route 192.168.11.0 255.255.255.0 Group-Async1 200
ip route 192.168.12.0 255.255.255.0 Group-Async1 200
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login

```



```

!
! ---进入 Modem 口线模式:
line 33 40
! ---配置为自动登录:
autoselect during-login
! ---配置为自动选择 PPP 协议:
autoselect ppp
! ---配置为使用本地数据库进行认证:
login local
! ---配置端口为允许拨入和拨出:
modem InOut
! ---自动识别 modem:
modem autoconfigure discovery
! ---连通后自动执行 ppp 命令:
autocommand ppp default
! ---允许所有协议进入:
transport input all
! ---配置为硬件流控:
flowcontrol hardware
!
end
(2) RTB
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname RTB
!
enable password cisco
username RTA password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing

```


! ---定义拨号脚本“dialout”:

```
chat-script dialout "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30 CONNECT \c
```

!

```
interface FastEthernet 0
```

```
no shutdown
```

```
description connected to 分支 B
```

```
ip address 192.168.11.254 255.255.255.0
```

```
no keepalive
```

!

```
interface Serial 0
```

```
no shutdown
```

```
no description
```

```
no ip address
```

```
encapsulation frame-relay
```

```
frame-relay lmi-type ansi
```

!

```
interface Serial 0.1 point-to-point
```

```
no shutdown
```

```
description connected to RTA
```

```
ip address 192.168.1.2 255.255.255.252
```

```
frame-relay interface-dlci 100 ietf
```

```
backup interface async 1
```

!

!

! ---进入异步接口配置模式:

```
interface async 1
```

```
description connected to RTA
```

! ---自动协商来从远端获得地址:

```
ip address negotiated
```

```
encapsulation ppp
```

```
async mode interactive
```

! ---设定接口为按需拨号 (DDR):

```
dialer in-band
```

! ---指定拨号串, “68002001” 为拨入远端所需的电话号码:

```
dialer string 68002001
```

```
dialer-group 1
```

```
ppp authentication pap
```

! ---向远端发送认证需要的用户名和密码:

```
ppp pap sent-username RTB password cisco
```



```

!
no dialer-list 1
dialer-list 1 protocol ip permit
!
ip route 0.0.0.0 0.0.0.0 Serial 0.1
ip route 0.0.0.0 0.0.0.0 async1 200
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
line 1
  autoselect during-login
  autoselect ppp
  modem InOut
  modem autoconfigure discovery
  autocommand ppp
! ---指定拨出所用的脚本“dialout”:
script dialer dialout
transport input all
flowcontrol hardware
!
end
(3) RTC
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption

```



```

no service tcp-small-servers
no service udp-small-servers
!
hostname RTC
!
enable password cisco
username RTA password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
! ---定义拨号脚本 "dialout":
chat-script dialout "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30 CONNECT &
!
interface FastEthernet 0
no shutdown
description connected to 分支 C
ip address 192.168.12.254 255.255.255.0
no keepalive
!
interface Serial 0
no shutdown
no description
no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
!
interface Serial 0.1 point-to-point
no shutdown
description connected to RTA
ip address 192.168.1.6 255.255.255.252
frame-relay interface-dlci 100 ietf
backup interface async 1
!
!
! ---进入异步接口配置模式:
interface async 1

```



```

description connected to RTA
! ---自动协商来从远端获得地址:
ip address negotiated
encapsulation ppp
async mode interactive
! ---设定接口为按需拨号 (DDR):
dialer in-band
! ---指定拨号串, "68002002" 为拨入远端所需的电话号码:
dialer string 68002002
dialer-group 1
ppp authentication pap
! ---向远端发送认证需要的用户名和密码:
ppp pap sent-username RTC password cisco
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
ip route 0.0.0.0 0.0.0.0 Serial 0.1
ip route 0.0.0.0 0.0.0.0 async 1 200
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
line 1
autoselect during-login
autoselect ppp
modem InOut

```

```

RTA#configure terminal
RTA#ppp interface serial 0
RTA#ppp authentication pap
RTA#ppp pap sent-username RTC password cisco
RTA#dialer in-band
RTA#dialer string 68002002
RTA#dialer-group 1
RTA#ip route 0.0.0.0 0.0.0.0 serial 0.1
RTA#ip route 0.0.0.0 0.0.0.0 async 1 200
RTA#no ip http server
RTA#snmp-server community public RO
RTA#no snmp-server location
RTA#no snmp-server contact
RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```

```

RTA#

```



```
modem autoconfigure discovery
autocommand ppp
! ---指定拨出所用的脚本“dialout”:
script dialer dialout
transport input all
flowcontrol hardware
!
end
```

案例 2

企业总部和分支机构通过 E1 线路互连,各分支采用异步拨号或 ISDN 方式作为主链路的备份。

1. 网络拓扑

网络拓扑如图 5-108 所示。

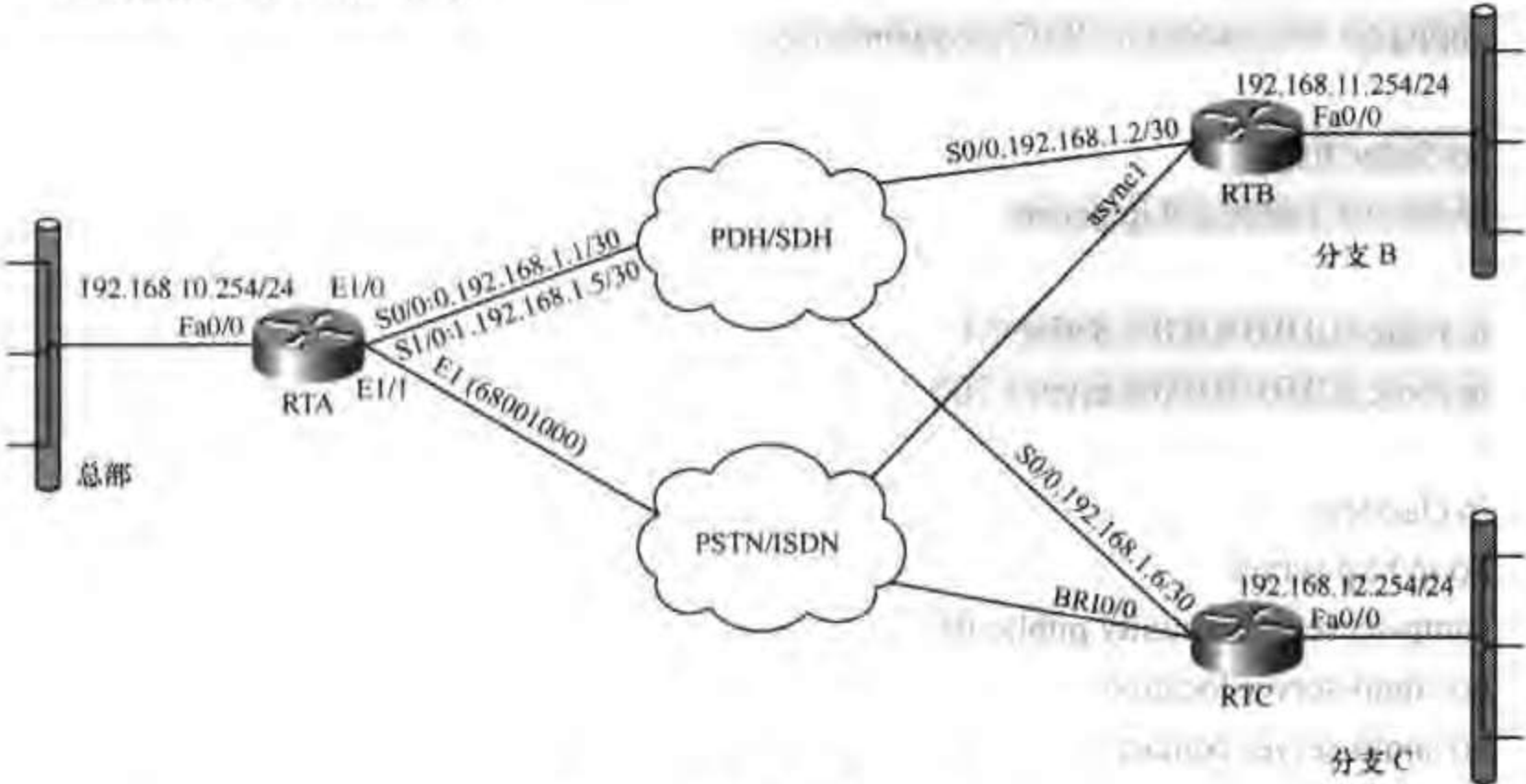


图 5-108 经典配置案例 2 拓扑图

说明：本案例中企业总部和各分支机构所用的设备及其规格见表 5-21。

表 5-21 案例 2 中所用设备及其规格

产 品	描 述	数 量
总部设备		
CISCO3725	3700 系列, 2 插槽, 2 FE, 多业务路由器 32 闪存/256DRAM	1
CAB-ACA	插头, 电源线, 10A	1
S372C-12309	Cisco 3725 Ser IOS IP	1
NM-2CE1U	2 端口信道化 E1/ISDN-PRI 不平衡网络模块	1
NM-30DM	30 端口数 Modem 网络模块	1
CAB-E1-BNC	E1 电缆 BNC 75Ω (不平衡) 5m	1
CAB-E1-PRI	E1- ISDN PRI 电缆, 3m	1
分支 B 设备		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP, 32 闪存/128DRAM	1

续表

产 品	描 述	数 量
CAB-ACA	插头,电源线,10A	1
S26C-12306	Cisco 2600 Ser IOS IP	1
WIC-1AM	1 端口模拟 Modem WAN 接口板	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1
分支 C 设备		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP,32F/128D	1
CAB-ACA	插头, 电源线,10A	1
S26C-12306	Cisco 2600 Ser IOS IP	1
WIC-1B-S/T	1 端口 ISDN WAN 接口板(拨号和专用线)	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1

2. 具体配置

(1) RTA

```
!  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption  
no service tcp-small-servers  
no service udp-small-servers  
!  
hostname RTA  
!  
enable password cisco  
username RTB password cisco  
username RTC password cisco  
!  
no ip name-server  
!  
ip subnet-zero  
no ip domain-lookup  
ip routing  
!  
interface FastEthernet 0/0  
no shutdown  
description connected to zb  
ip address 192.168.10.254 255.255.255.0
```



```

keepalive 10
!
interface FastEthernet 0/1
  no description
  no ip address
  shutdown
!
!

```

! ---进入 E1 卡配置模式:

```

controller E1 1/0
  no shutdown

```

! ---配置 CE1/PRI 接口的帧校验格式, 不进行帧校验为 “no-crc4”, 采用 4 字节 CRC 校验为 “crc4” 具体采用什么格式请咨询线路提供商:

```

framing no-crc4

```

! ---进行时隙的划分, 这里将 1、2 时隙捆绑为 “0” 组, 3、4 时隙捆绑为 “1” 组, “0” 和 “1” 组分别对应下面的虚拟串口 “Serial 1/0:0” 和 “Serial 1/0:1”:

```

channel-group 0 timeslot 1-2
channel-group 1 timeslot 3-4

```

```

!
controller E1 1/1
  no shutdown
  framing no-crc4

```

! ---指定 ISDN PRI 的线路编码格式为 “hdb3”, 具体格式请咨询线路提供商:

```

linecode hdb3

```

! ---把 PRI 接口划分为 31 个信道, 其中第 16 个信道 (对应逻辑接口 Serial0/0:15) 是管理信道:

```

pri-group timeslots 1-31

```

```

!
!
interface Serial 1/0:0
  no shutdown
  description connected to RTB
  encapsulation ppp
  ip address 192.168.1.1 255.255.255.252
!
interface Serial 1/0:1
  no shutdown
  description connected to RTC
  encapsulation ppp

```



```
ip address 192.168.1.5 255.255.255.252
```

! ---进入逻辑接口 Serial1/1:15 (管理信道):

```
interface Serial1/1:15
```

```
no shutdown
```

```
description dialin interface
```

```
ip unnumbered FastEthernet0/0
```

```
encapsulation ppp
```

! ---指定本接口属于拨号组 1, 注意组号和下面定义的“dialer-list 1”对应:

```
dialer-group 1
```

```
isdn switch-type primary-net5
```

! ---将模拟 Modem 呼叫转接到内部数字 Modem 来处理:

```
isdn incoming-voice modem
```

! ---为拨入的 ISDN 呼叫从地址池“isdnpool”中分配 IP 地址:

```
peer default ip address pool isdnpool
```

! ---指定 PPP 的认证方式, 这里采用“pap”方式:

```
ppp authentication pap
```

```
!
```

! ---建立一个异步拨号组, 用于接收模拟 Modem 呼叫:

```
interface Group-Async1
```

```
ip unnumbered FastEthernet0/0
```

```
encapsulation ppp
```

! ---为异步串口指定建立链路的方式, 默认值是“dedicate”。可以有两种建立链路的方式: ①直接方式 (Dedicate): 拨号成功之后, 直接采用链路层协议配置参数建立链路; ②交互方式 (Interactive): 拨号成功之后, 主叫方向对端发送配置命令 (与用户从远端手工键入配置命令效果相同), 设置对端的链路层协议工作参数, 然后建立链路。比较常用的是直接方式, 但在与同样支持交互方式的路由器 (如 Cisco 路由器等) 互连时, 采用交互方式显得更为灵活。

```
async mode interactive
```

! ---为拨入的模拟呼叫从地址池“pstnpool”中分配 IP 地址:

```
peer default ip address pool pstnpool
```

! ---指定 PPP 的认证方式, 这里采用“pap”方式:

```
ppp authentication pap if-needed
```

! ---指定此模拟拨号组对应的端口:

```
group-range 33 62
```

```
!
```

```
ip classless
```

```
!
```

! ---为拨号组 1 指定激活拨号的条件, 这里所有的 IP 访问都可以激活拨号:


```
no dialer-list 1
dialer-list 1 protocol ip permit
!
! ---为数字和模拟拨入用户定义地址池:
ip local pool isdnpool 192.168.10.201 192.168.10.220
ip local pool pstnpool 192.168.10.221 192.168.10.240
!
ip route 192.168.11.0 255.255.255.0 Serial 1/0:0 1
ip route 192.168.12.0 255.255.255.0 Serial 1/0:1 1
ip route 192.168.11.0 255.255.255.0 Group-Async 1 200
ip route 192.168.12.0 255.255.255.0 Group-Async 1 200
!
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
! ---进入 Modem 口线模式:
line 33 62
! ---配置为自动登录:
autoselect during-login
! ---配置为自动选择 PPP 协议:
autoselect ppp
! ---配置为使用本地数据库进行认证:
login local
! ---配置端口为允许拨入和拨出:
modem InOut
! ---自动识别 modem:
modem autoconfigure discovery
! ---连通后自动执行 ppp 命令:
```



```
autocommand ppp default
```

```
!
```

```
end
```

(2) RTB

```
!
```

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
service password-encryption
```

```
no service tcp-small-servers
```

```
no service udp-small-servers
```

```
!
```

```
hostname RTB
```

```
!
```

```
enable password cisco
```

```
username RTA password cisco
```

```
!
```

```
! ---定义拨号脚本“dialout”:
```

```
chat-script dialout "" "AT" TIMEOUT 30 OK "ATDT \t" TIMEOUT 30 CONNECT \c
```

```
!
```

```
no ip name-server
```

```
!
```

```
ip subnet-zero
```

```
no ip domain-lookup
```

```
ip routing
```

```
!
```

```
interface FastEthernet 0/0
```

```
no shutdown
```

```
description connected to fzB
```

```
ip address 192.168.11.254 255.255.255.0
```

```
keepalive 10
```

```
!
```

```
interface Serial 0/0
```

```
no shutdown
```

```
description connected to RTA S1/0/0
```

```
encapsulation ppp
```

```
ip address 192.168.1.2 255.255.255.252
```

```
!
```

```
! ---进入异步接口配置模式:
```

```
interface async 1
```



```

description connected to RTA
! ---自动协商来从远端获得地址:
ip address negotiated
encapsulation ppp
async mode interactive
! ---设定接口为按需拨号 (DDR):
dialer in-band
! ---指定拨号串, "68001000" 为拨入远端所需的电话号码:
dialer string 68001000
dialer-group 1
ppp authentication pap
! ---向远端发送认证需要的用户名和密码:
ppp pap sent-username Router_B password cisco
!
! Dialer Control List 1
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
!
ip classless
!
ip route 0.0.0.0 0.0.0.0 Serial 0/0 1
ip route 0.0.0.0 0.0.0.0 async 1 200
!
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!

```



```

line 1
 autoselect during-login
 autoselect ppp
 modem InOut
 modem autoconfigure discovery
 autocommand ppp
 ! --指定拨出所用的脚本“dialout”:
 script dialer dialout
 transport input all
 flowcontrol hardware
 !
end

```

(3) RTC

```

!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname RTC
!
enable password cisco
username RTA password cisco
!
no ip name-server
!
isdn switch-type basic-net3
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0/0
 no shutdown
 description connected to fzC
 ip address 192.168.12.254 255.255.255.0
 keepalive 10
!

```



```
interface Serial 0/0
no shutdown
description connected to RTA S1/0:1
encapsulation ppp
ip address 192.168.1.6 255.255.255.252
!
interface BRI 0/0
no shutdown
description connected to RTA
ip address negotiated
isdn switch-type basic-net3
encapsulation ppp
dialer in-band
dialer string 68001000
dialer-group 1
ppp authentication pap
ppp pap sent-username RTC password cisco
no cdp enable
!
no dialer-list 1
dialer-list 1 protocol ip permit
ip classless
!
ip route 0.0.0.0 0.0.0.0 Serial 0/0 1
ip route 0.0.0.0 0.0.0.0 BRI0/0 200
!
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
```



```
!  
end
```

5.7 小 结

本章开始对路由器的原理、结构进行了简要的介绍，然后用较大的篇幅重点介绍了我国常用的广域链路，尤其对各种链路的典型应用、入网方式以及典型的配置作了详细的介绍。之后又对常用的路由协议和广泛应用的访问控制列表及地址转换作了相应的讲解，最后通过两个具体的案例对企业网中路由器的配置方法作了链示。

下面我们给出常用配置路由器的指导。

Cisco 路由器配置指导：

- 步骤 1. 进行物理线路的连接；
- 步骤 2. 配置接口链路层协议（HDLC、PPP、Frame-Relay）；
- 步骤 3. 配置网络层协议（IP 地址、路由协议）；
- 步骤 4. 配置其他功能和访问控制（Qos、NAT、ACL）。

第6章 Cisco 防火墙配置

本章将涵盖下列有关 Cisco 防火墙配置方面的关键主题

- Cisco 防火墙基础
- Cisco 防火墙经典配置案例

目标:

通过本章的学习, 希望大家对以下一些方面有所了解:

- (1) 什么是防火墙;
- (2) 防火墙的主要功能是什么;
- (3) 为什么要在企业网中布置防火墙;
- (4) 防火墙有哪些种类;
- (5) 防火墙的硬件结构;
- (6) 防火墙的配置命令 (nameif、interface、ip address、global、nat、route、static、conduit);
- (7) 如何快速在企业网中搭建防火墙。

6.1 简 介

随着信息技术突飞猛进的发展, 特别是 Internet 的快速发展和全球信息高速公路的建设, 使各国的信息化进程急剧加快。信息技术和网络空间, 给社会的经济、科技、文化、教育和管理的各个方面注入了新的活力, 企业利用 Internet 来提高办事效率和市场反应速度, 以便更具竞争力。网络信息化的应用, 也使得数据资料的传输和存取都变得方便、快捷, 客户、销售商、移动用户、异地员工和内部人员之间的即时沟通成为可能。

人们在享受信息化带来的众多好处的同时, 也面临着日益突出的信息安全问题。企业信息化程度越高, 企业的商业秘密就越容易被窃取, 尤其是各种高度网络化的对大众提供服务的网络银行、电子商务等系统的安全, 直接影响到企业的形象和利益。

网络安全的考虑涉及许多方面, 比如, 从物理层的机房安全 (防火防盗), 到链路层的加密, 到网络层的隔离、访问控制, 再到操作系统的漏洞扫描、应用层的访问控制和加密等。另外还有防病毒系统的建立, 以及非常重要的企业内部网络安全防范与安全管理制度建立等等。但就目前来看, 专用的安全产品主要包括: 防火墙、入侵检测系统和防病毒系统。这里我们主要讲解应用最为广泛的防火墙。

6.2 Cisco 防火墙基础

1. 什么是防火墙

传统上认为, 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共网)之间的用于信息过滤的设备。它往往是不同网络之间信息的惟一出入口, 能根据企业的安全策略控制(允许、拒绝、监测)出入网络的信息流, 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。

作为内部网络与外部公共网络之间的第一道屏障, 防火墙是最先受到人们重视的网络安全产品之一。虽然从理论上讲, 防火墙处于网络安全的最底层, 负责网络间的安全认证与传输, 但随着网络安全技术的整体发展和网络应用的不断变化, 现代防火墙技术已经逐步应用于网络层之外的其他安全层次, 目前的防火墙不仅要完成传统防火墙的过滤任务, 同时还能为各种网络应用提供相应的安全服务。另外还有多种防火墙产品正朝着分布式安全、数据安全与设备认证、防止病毒与黑客侵入等方向发展。

2. 防火墙的功能

通常将防火墙作为一个边界设备放置在彼此“不友好”的两个网络之间, 在两个环境之间提供了一个安全网关。这个网关作为一个检查点对所有进出的数据流进行检查和过滤, 在被保护网络和外部网络之间架起一道屏障, 以防止发生不可预测的、潜在的破坏性侵入。

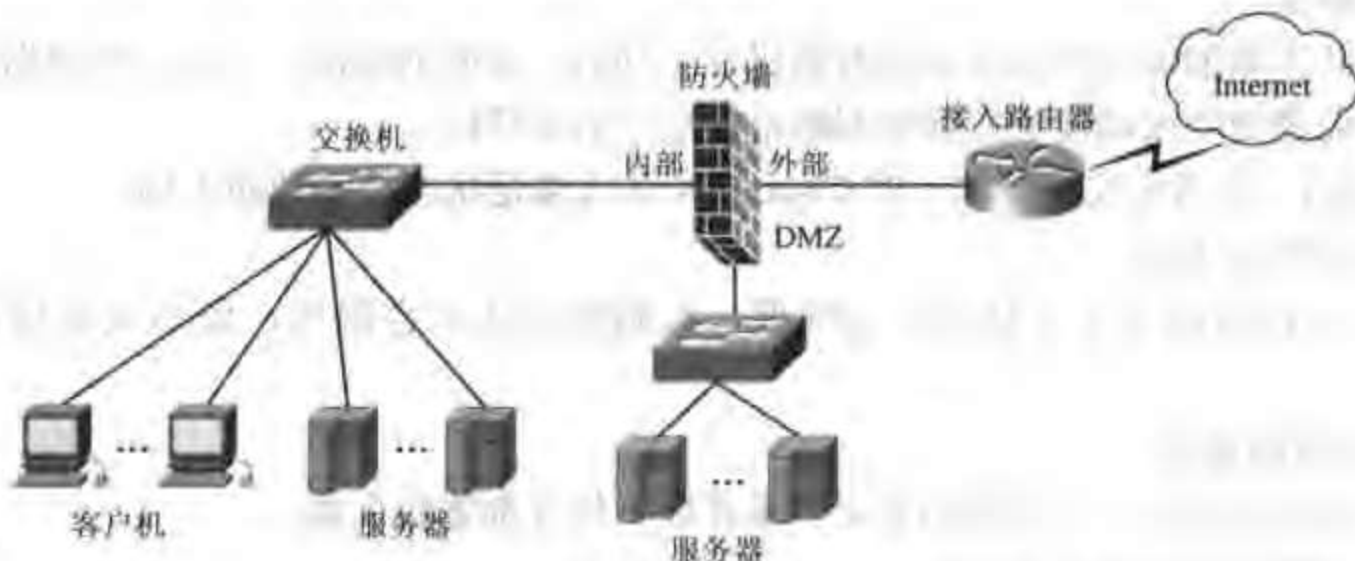


图 6-1 采用防火墙的常用网络

3. 为什么使用防火墙

(1) 防火墙可以控制不安全的服务。因为只有授权的协议和服务才能通过防火墙, 这就大大降低了子网的暴露度, 从而提高了网络的安全度。

(2) 防火墙可以控制对主机的访问。由于防火墙不允许访问不需要访问的主机或服务, 它在网络的边界形成了一道关卡。如果一个用户很少提供网络服务, 或几乎不跟外部站点打交道, 那么设置防火墙就是他保护自己主机的最好选择。

(3) 防火墙可以对信息进行记录。当防火墙系统被配置为所有内部 Intranet 网络与外部 Internet 连接均需经过的安全系统时, 防火墙系统就能够对所有的访问作出日志记录。日志是对一些可能的攻击进行分析和防范的十分重要的情报。另外, 防火墙系统也能够对正常的网

络使用情况作出统计。通过对统计结果的分析，可以使得网络资源获得更好的使用。

4. 防火墙的分类

根据防火墙所采用的技术不同，可以分为 4 种基本类型：包过滤型、代理型、监测型和复合型。

(1) 包过滤型

包过滤型防火墙依据网络的分包传输技术而设计。网络上的数据都是以“包”为单位进行传输的，数据被分割成为一定大小的数据包，每一个数据包中都会包含发送方的 IP 地址和接收方的 IP 地址、TCP/UDP 源端口和目标端口、TCP 链路状态等。

防火墙通过读取数据包中的地址信息来判断这些“包”是否来自可信任的安全站点，一旦发现来自危险站点的数据包，防火墙便会将这些数据拒之门外。同时，系统还会按照预先设定过滤原则过滤信息包，那些不符合规定的 IP 地址的信息包会被防火墙过滤掉，以保证网络系统的安全。系统管理员也可以根据实际情况灵活制定判断规则。

Cisco 的 IOS 可配置为包过滤的防火墙。

(2) 代理型

代理型防火墙也可以被称为代理服务器，它的安全性要高于包过滤型产品，并已经开始向应用层发展。它作用在应用层，其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。实际中的应用网关通常由专用工作站实现。

微软公司的 ISA Server 可认为是一个代理型防火墙。

(3) 监测型

监测型防火墙能够对网络各层的数据进行主动的、实时的监测，在对这些数据加以分析的基础上，监测型防火墙能够有效地判断出各层中的非法侵入。

采用 ASA（自适应安全算法）的 Cisco PIX 防火墙是状态检测型防火墙。

(4) 复合型防火墙

把基于包过滤的方法与基于应用代理、监测的方法结合起来，便形成了复合型防火墙产品。

5. 防火墙的部署

一个企业可以依照一个完整的安全体系在以下位置部署防火墙：

(1) 在大型网络的服务器群前；

(2) 在 Internet 的出口处；

(3) 在广域网系统中，由于安全的需要，总部的局域网可以将各分支机构的局域网看成不安全的系统，（通过公网 PSTN、DDN、Frame Relay 等连接）在总部的局域网和各分支机构连接时采用防火墙隔离；

(4) 总部的局域网和分支机构的局域网通过 Internet 连接时，需要各自来装防火墙。

6. 防火墙的策略

防火墙可以采取如下两种理念之一来定义防火墙的策略。

(1) 未经说明许可的就是拒绝，即“封闭型”策略。防火墙默认阻来所有流经的信息，每个需要通过的信息流必需明确配置为准许。这是一个值得推荐的方法，它将创建一个非常安全的环境。当然，该理念的不足在于过于强调安全而减弱了可用性，限制了用户可以申请

的服务的数量。

(2) 未说明拒绝的均为许可,即“开放型”策略。防火墙默认准许所有流经的信息通过,每个需要阻塞的信息流必需明确配置为拒绝。当然,该理念的不足在于它将可用性置于比安全更为重要的地位,增加了保证私有网安全性的难度。

在一个企业网中,防火墙应该是全局安全策略的一部分,构建防火墙时首先要考虑其保护的范围。企业网的安全策略应该在细致的安全分析、全面的风险假设以及商务需求分析基础上来制定。

6.2.1 Cisco 防火墙基本构成

我们可以认为防火墙就是一台特殊功能的计算机,它的主要功能就是用来进行数据包的过滤和检测,而不是像传统计算机那样进行文字和图像处理。既然是计算机,它就应该和我们熟知的传统的 PC (个人电脑) 有类似的体系结构,同时,它也应该有相应的操作系统 (PIX OS)。下面我们就来认识一下 Cisco 的 PIX 防火墙。

总体来说 PIX 是由 CPU、RAM、NVRAM、FLASH、ROM 和一些相应的接口通过内部总线相连而构成。下面我们对它们分别进行介绍。

(1) CPU

相当于 PC 机的 CPU (中央处理器),是 PIX 的大脑,负责整个系统的计算和控制。

(2) ROM

相当于 PC 机的 BIOS (基本输入输出系统),存放引导程序和 PIX OS 的一个最小子集。它是只读存储器,系统掉电,程序不会丢失。

(3) Flash

相当于 PC 机的硬盘,包含 PIX 的操作系统 (PIX OS) 和其他微代码。它是一种可擦写、可编程的存储器,系统掉电,程序不会丢失。

(4) RAM/DRAM (Random Access Memory / Dynamic Random Access Memory)

相当于 PC 机的内存,它是 PIX 主要的存储部件。RAM 也叫做工作存储器,包含动态的配置信息。系统掉电,RAM 的内容会丢失。

(5) Interface (接口)

相当于 PC 机的网卡,接口指的是数据包进出 PIX 的网络连接处。

下面介绍一下 PIX 的启动过程。

就和我们的 PC 机开机需要进行系统各部分的自检然后加载操作系统一样,PIX 也要经历一个类似的启动过程:首先对系统各部分的硬件进行检测,然后检查启动配置文件(配置了操作系统从哪里引导),根据配置文件指定的引导路径去寻找操作系统,最后将配置文件加载到 RAM,如果没有配置则进入系统的初始配置状态。

防火墙通常至少会有 3 个接口,主要用来隔离不同的安全区域,因此防火墙通常会创建 3 个区域:内部区域、外部区域和 DMZ 区(非军事化区)。

(1) 内部区域:内部区域是被信任的区域。它通常指企业的内部网,涉及企业的主要服务器(不对外提供服务)和各部门的客户机。

(2) 外部区域:外部区域是不被信任的区域。防火墙主要保护内部和 DMZ 区的设备,使它们免受外部的威胁。

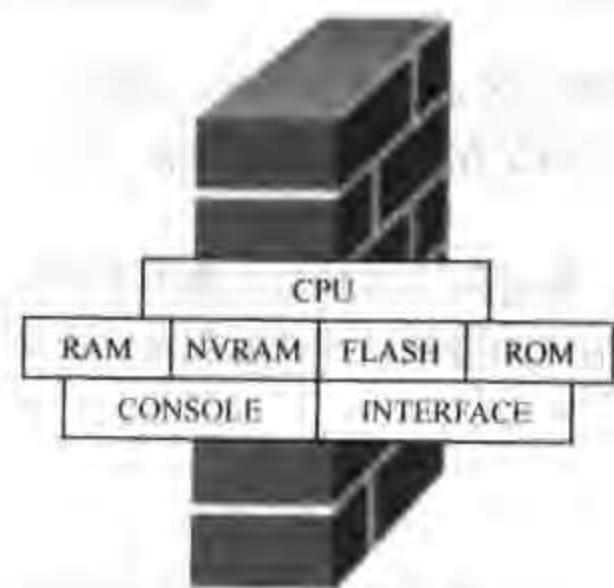


图 6-2 PIX 防火墙结构



图 6-3 PIX 启动流程

(3) DMZ 区（非军事化区）：DMZ 区是一个介于内部区域和外部区域之间的区域，它对于外部用户通常是可以访问的。企业对外提供服务的服务器（如 WWW、E-mail、DNS 等服务器）通常设置在这一区域，它使得外部用户可以访问企业的公开信息，但却不允许他们访问企业的内部网络。由于 DMZ 区允许外部的访问，所以容易受到外部的攻击，这就需要对此区域的服务器进行精心的配置（及时更新操作系统的补丁，关闭不必要的服务等）。

DMZ 区可根据具体的需求来增减，但内部接口和外部接口是必不可少的。

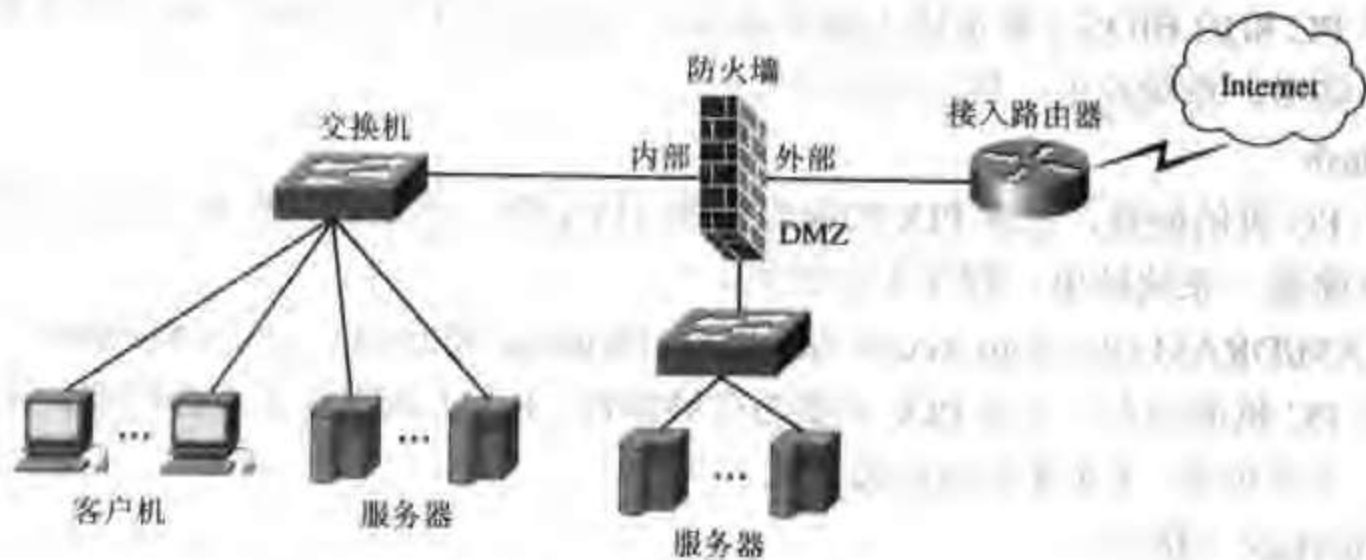


图 6-4 防火墙典型应用

防火墙的基本职责是完成以下功能：

- 不允许外部设备访问内部网络；
- 允许外部设备有限地访问 DMZ 区；
- 允许内部设备访问外部网络；
- 允许内部设备有限地访问 DMZ 区。

6.2.2 基本设置方式

一般来说，可以用 5 种方式来设置 PIX 防火墙。

(1) CON：适合通过 Console 接口终端或运行终端仿真软件（如超级终端）的微机来配置 PIX；

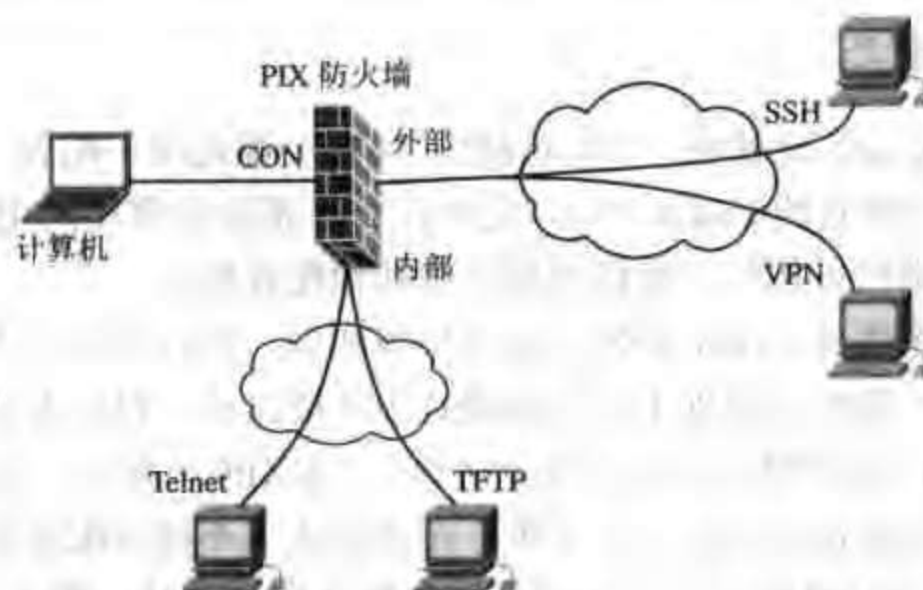


图 6-5 PIX 配置方式

(2) Telnet: 经过配置可以通过 PIX 的内网口 (inside), 利用 telnet 配置 PIX;

(3) TFTP: 经过配置可以通过 PIX 的内网口 (inside), 利用 TFTP 服务器下载配置信息。TFTP Server 可以运行在 Unix 工作站或者 PC 工作站上, 可以让它作为一个集中的仓库;

(4) VPN: 可以通过在一个运行 VPN 客户端软件 (如 Cisco Secure VPN Client) 的 PC 机和配置了 VPN 的 PIX 之间建立虚拟通道来实现对 PIX 的配置;

(5) SSH: SSH 是和 Telnet 类似的一种应用程序, Telnet 以明文方式发送数据, 而 SSH 采用密文的方式传输数据, 因此具有更高的安全性。

注意:

- 远程用户 (outside) 只能通过 SSH 或 VPN 来进行对 PIX 的配置;
- PIX 支持 SNMP 协议, 但我们只能通过 SNMP 监视 PIX, 但不能通过它进行配置。

一般通过 Console 口对 PIX 进行初次设置, 此时终端的硬件设置如下:

波特率 : 9600

数据位 : 8

停止位 : 1

奇偶校验: 无

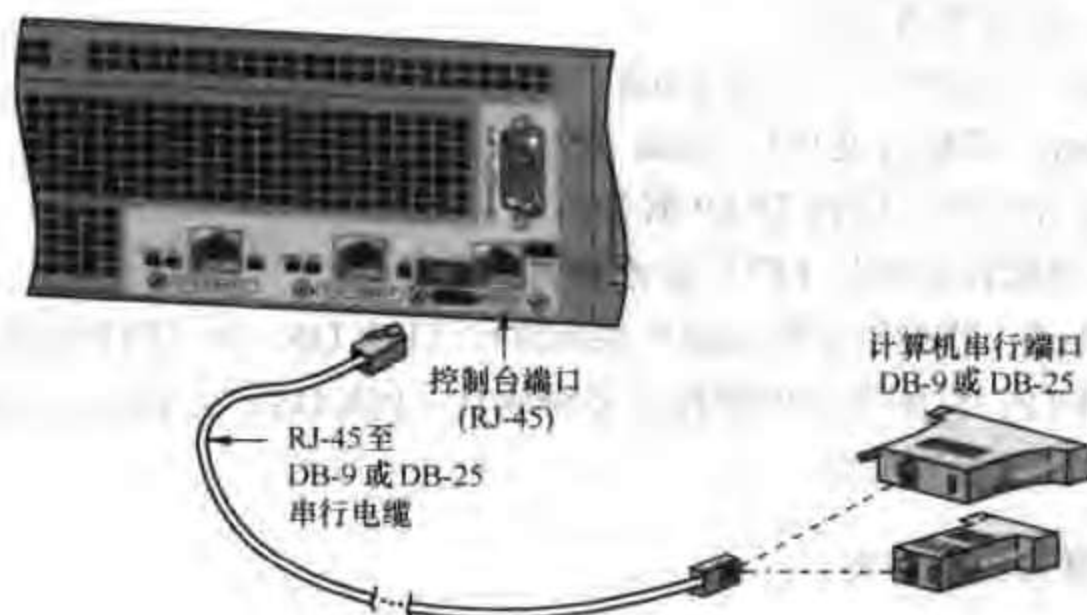


图 6-6 PIX 控制台连接

6.2.3 PIX 命令状态

在使用任何一种 Cisco 设备时，命令行接口（CLI）都是用于配置、监视并维护那台设备的主要用户接口。对于所有的 Cisco 产品，交互式 CLI 都是最常用的用户接口。Cisco 设备采用的基本管理模式有用户可执行、特权可执行和其他配置模式。

PIX 防火墙的命令集与 Cisco IOS 的命令集很相似，但在语法上不完全相同。当想要使用一个特定的命令时，我们必须处于适当的模式下才能执行。PIX 提供了下列 4 种模式：

（1）非特权模式：这种模式又称为用户可执行（EXEC）模式，提示符为 >。在这种模式下，我们可以使用全部命令中的一个子集。在此模式下不能对配置进行改动。

（2）特权模式：在这种模式下，我们可以对配置进行改动，提示符为 #。一旦进入此模式，我们就可以访问配置模式。

（3）配置模式：在这种模式下，所有的特权、非特权和配置命令都可以使用，提示符为（config）#。

（4）监控模式：当用户要进行 PIX OS 的升级或进行密码恢复时我们会用到此模式，提示符为 monitor>。

PIX OS 的各种命令模式和提示符见表 6-1。

表 6-1 PIX OS 的各种命令模式和提示符

模 式	提 示 符
非特权模式	pixfirewall>
特权模式	pixfirewall#
配置模式	pixfirewall(config)#
监控模式	monitor>

6.2.4 PIX 文件管理

像任何一种操作系统一样，PIX OS 也有自己的用于文件管理的命令。通过这些命令 PIX 可以方便地对操作系统和配置文件进行管理。

Config Term：进入配置模式

Write Memory：保存配置文件到 Flash

Config Memory：将配置文件从 Flash 调入内存

Write Net：保存配置文件到 TFTP 服务器

Config Net：将配置文件从 TFTP 服务器调入内存

Copy TFTP Flash：将配置文件或操作系统软件（PIX OS）从 TFTP 服务器拷贝到 Flash 中

Copy Flash TFTP：将配置文件或操作系统软件（PIX OS）从 Flash 拷贝到 Tftp 服务器中

Write Erase：删除配置文件

6.2.5 PIX 常用配置命令

有 6 个配置命令被认为是配置 PIX 防火墙的基础。它们分别是 nameif、interface、ip address、nat、global 和 route。nat、global 和 route 命令虽然不是必需的，但是为了让数据流

通过 PIX 防火墙，必须对它进行配置。nat 和 global 命令通常用于提供从一个相对可信的网络到一个不太可信的网络的访问。

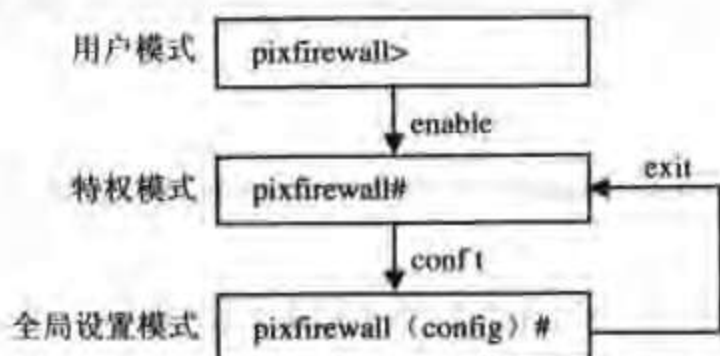


图 6-7 PIX OS 命令模式

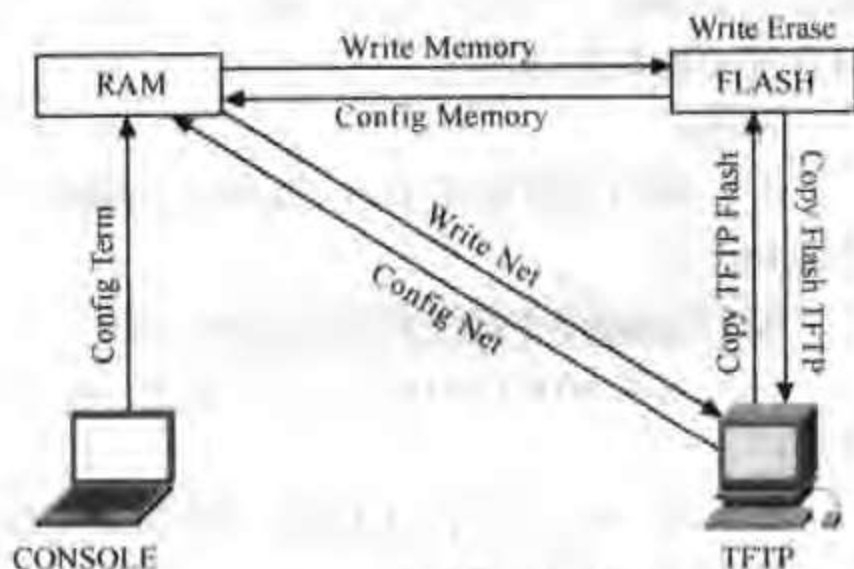


图 6-8 PIX OS 的文件管理命令

(1) nameif 命令

命令 nameif 为 PIX 防火墙的每一个接口分配一个名字，并指定它的安全级别（PIX 防火墙的内部接口和外部接口除外，它们的名字是缺省的，其中 ethernet0 被命名为 outside，安全级别为 0；ethernet1 被命名为 inside，安全级别为 100）。

举例：

！---将接口 ethernet2 命名为 dmz，并为其分配安全级别 50

```
nameif ethernet2 dmz security50
```

(2) interface 命令

命令 interface 用于确定硬件类型，设置硬件速度，并启用接口。当在 PIX 防火墙上安装一块附加的以太网接口卡时，PIX 防火墙可以自动识别。对于任何以太网接口，应尽量避免使用 auto 关键字；否则，可能发生双工不匹配，从而导致性能降低。最好在 PIX 和与其连接的设备接口上硬性设置速度和双工模式。

默认情况下，接口是处于 shutdown 状态的。

举例：

！---将接口 ethernet2 设为 100Mbit/s，全双工，并启用它

```
interface ethernet2 100full
```

！---关闭接口 ethernet2

```
interface ethernet2 100full shutdown
```

(3) ip address 命令

PIX 防火墙上的每个接口都必须配置一个 IP 地址。配置完成后，可用 show ip address 命令查看为接口分配的 IP 地址。

举例：

！---为接口 dmz 分配 ip 地址

```
ip address dmz 192.168.1.1 255.255.255.0
```

(4) nat 命令，global 命令

nat（网络地址翻译）使内部用户的私有 IP 地址转换为外部的全球惟一的公有 IP 地址，

这样,一方面可以节约日益紧张的 IP 资源,另一方面可以有效地保护内网,使其对外不可见。
nat 命令用来指定将被翻译的网段或主机地址, global 命令用来定义翻译完成后的网络地址。
除了和 global 命令联合使用, nat 命令还可以单独使用,这时它不可用来进行地址的翻译,而只作简单的数据转发。

举例:

! ---将内部地址段 10.1.1.0/24 进行翻译(其中 1 代表全局地址池,必须和相应的 global 命令相匹配)

```
nat (inside) 1 10.1.1.0 255.255.255.0
```

(注:可用 0.0.0.0 0.0.0.0 代表所有地址,简写为 0.0,如 nat (inside) 1 0.0 表示将所有内部地址进行翻译)

! ---将 nat 标号为 1 的地址段中的地址翻译为地址池 202.1.1.1 至 202.1.1.10 中的一个地址,掩码为 255.255.255.0

```
global (outside) 1 202.1.1.1-202.1.1.10 netmask 255.255.255.0
```

! ---将 nat 标号为 1 的地址段中的地址翻译为地址 202.1.1.11,不同的地址翻译到同一地址的不同端口号

```
global (outside) 1 202.1.1.11 netmask 255.255.255.0
```

! ---将 dmz 的网段 172.16.1.0/24 进行透明转发,不作地址翻译(0 代表透明转发)

```
nat (dmz) 0 172.16.1.0 255.255.255.0
```

(5) route 命令

route 命令用于配置静态路由。

举例:

! ---为外部接口,配置缺省路由,将所有从 outside 接口离开的数据包发往地址 192.168.1.2

```
route outside 0.0.0.0 0.0.0.0 192.168.1.2
```

注意:nameif 和 interface 配置的对象为硬件的接口,如 ethernet0、ethernet1...;而 ip address、nat、global 和 route 命令配置的对象是逻辑的接口,即由 nameif 定义的接口,如 outside、inside、dmz 等。

到目前为止,我们已经了解了配置 PIX 防火墙所需要的最根本的 6 个命令,掌握这些命令已足以应付大多数的网络情况,但很多时候我们需要实现对数据包更加精确的控制,这时我们就需要用到另一个命令 outbound。它是一个 PIX 专用的访问列表命令,用于过滤由内至外的数据包(注:由外至内的过滤使用下面讲解的 conduit 命令)。

(6) outbound 命令、apply 命令

outbound 命令可根据源和目的 IP 地址以及目的端口号和协议进行过滤,它需要和 apply 命令一起使用。

举例:对于 Internet 上的一些敏感资源,如一些不健康站点,我们可以查到其 IP 地址(使用 nslookup),并对出境的访问加以控制。在 PIX 防火墙上的配置如下:

! ---定义访问列表,禁止对地址 202.11.1.1(假设的地址)的 www 访问

```
outbound 10 deny 202.11.1.1 255.255.255.255 www tcp
```

! ---将访问列表应用到内接口上, outgoing_dest 是指根据目的过滤,如果根据源地址过滤,使用 outgoing_src 命令


```
apply (inside) 10 outgoing_dest
```

以上所有的命令主要针对的是由内到外的访问，如果我们需要对外提供服务，即需要由外至内的访问，那该怎么办呢？下面我们就来介绍另外的两个重要的命令，通过对它们的配置，我们可以实现由外至内的访问。

(7) static 命令, conduit 命令

static 命令用于将一个本地（内部或 DMZ 区）的 IP 地址静态映射到一个外部全局的 IP 地址，有了这样的映射，我们就有了从外到内的入口，但要真正进入内部，还必须使用 conduit 命令为相应的数据流配置通道。

举例：

！---将内部地址 10.1.1.199 静态映射成外部地址 192.168.1.199（注意 192.168.1.199 在这里代表全局地址）

```
static (inside,outside) 192.168.1.199 10.1.1.199 netmask 255.255.255.255
```

！---允许外部任何地址对 192.168.1.199 进行 www 的访问（结合上一条命令，可知实际访问的是内部提供 www 服务的主机 10.1.1.199）

```
conduit permit tcp host 192.168.1.199 eq www any
```

注意：outbound 和 conduit 命令已经被标准的访问列表（类似 IOS）所取代，Cisco 也建议大家使用最新的访问控制命令，因为在未来的软件版本里，将不再支持 outbound 和 conduit 命令。下面我们将上面的两个例子用最新的命令重新配置一下：

```
access-list inside_acl deny tcp any host 202.11.1.1 eq 80
```

```
access-list inside_acl permit ip any any
```

```
access-group inside_acl in interface inside
```

```
access-list outside_acl permit tcp any host 192.168.1.199 eq 80
```

```
access-group outside_acl in interface outside
```

通过对上面这些命令的学习，我们已经掌握了配置 PIX 防火墙的精髓，如果需要深入了解 PIX 防火墙的配置，请参阅 Cisco 公司的网站上的内容：<http://www.cisco.com/go/pix>

6.2.6 防火墙基本配置模板

大多数网络中防火墙作为一个边界设备，放置在 Internet 的出口处，这时通常只需要对防火墙进行网络地址转换（nat）的配置，如果有临时要对外提供的服务（如外地出差人员，想临时通过 ftp 访问公司内部的文件服务器），这时可通过 static 和 conduit 命令的组合来实现。我们之所以在这里特别强调“临时”的概念，因为这样做是极不安全的。如果有长期对外提供的服务，一定要将防火墙放置在 DMZ 区，从而使它和内网进行安全隔离。下面我们分这两种情况分别进行介绍。

(1) 只有内部和外部接口的 PIX 防火墙配置模板如下：

```
nameif ethernet0 outside security0
```

```
nameif ethernet1 inside security100
```

```
enable password cisco
```

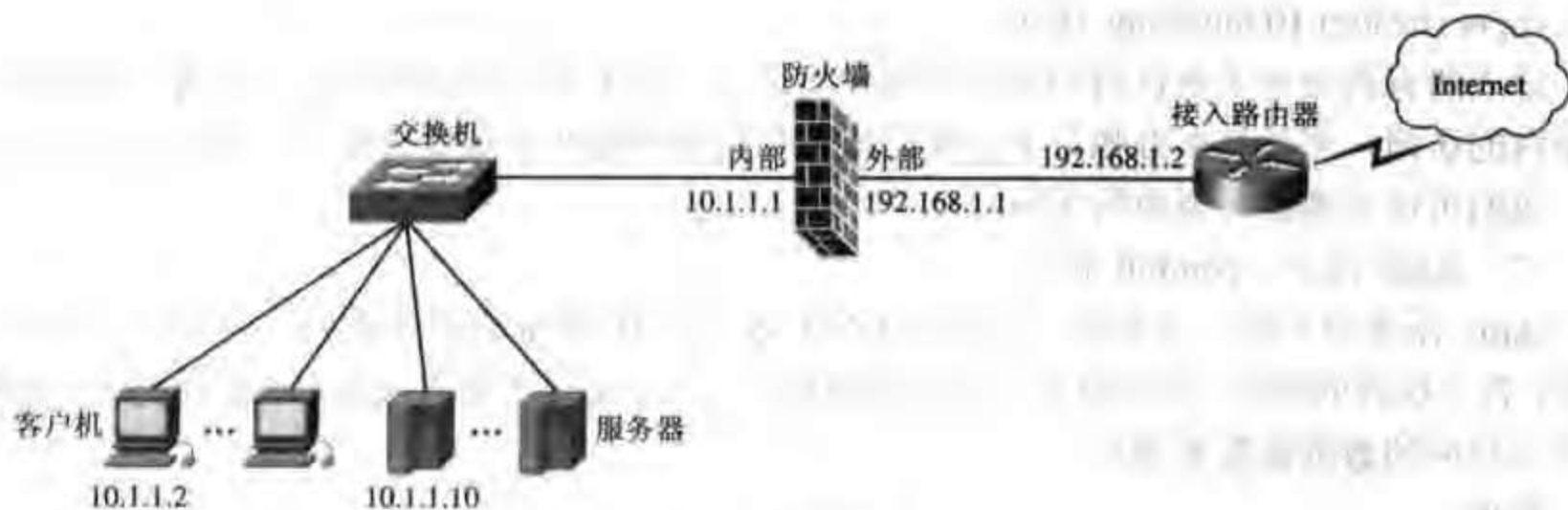



图 6-9 两接口配置图

```
passwd cisco
```

```
hostname pixfirewall
```

```
! --启用内外接口
```

```
interface ethernet0 auto
```

```
interface ethernet1 auto
```

```
! --设置内外接口的地址
```

```
ip address outside 192.168.1.1 255.255.255.0
```

```
ip address inside 10.1.1.1 255.255.255.0
```

```
! --设置全局复用地址池
```

```
global (outside) 1 192.168.1.200-192.168.1.253
```

```
! --单个 PAT 地址
```

```
global (outside) 1 192.168.1.254
```

```
! --转换所有内部地址
```

```
nat (inside) 1 0 0
```

```
! --将服务器 10.1.1.10 的地址映射为 192.168.1.10
```

```
static (inside,outside) 192.168.1.10 10.1.1.10 netmask 255.255.255.255
```

```
! --允许外部任何地址对 192.168.1.10 进行 ftp 的访问
```

```
conduit permit tcp host 192.168.1.10 eq ftp any
```

```
! --设置缺省路由
```

```
route outside 0.0.0.0 0.0.0.0 192.168.1.2
```

注意：在路由器上要配置到内网网段（10.1.1.0/24）的路由。

(2) 包括内部、外部和 DMZ 接口的 PIX 防火墙

配置模板如下：

```
nameif ethernet0 outside security0
```

```
nameif ethernet1 inside security100
```

```
! --定义 dmz 接口
```

```
nameif ethernet2 dmz security50
```

```
enable password cisco
```

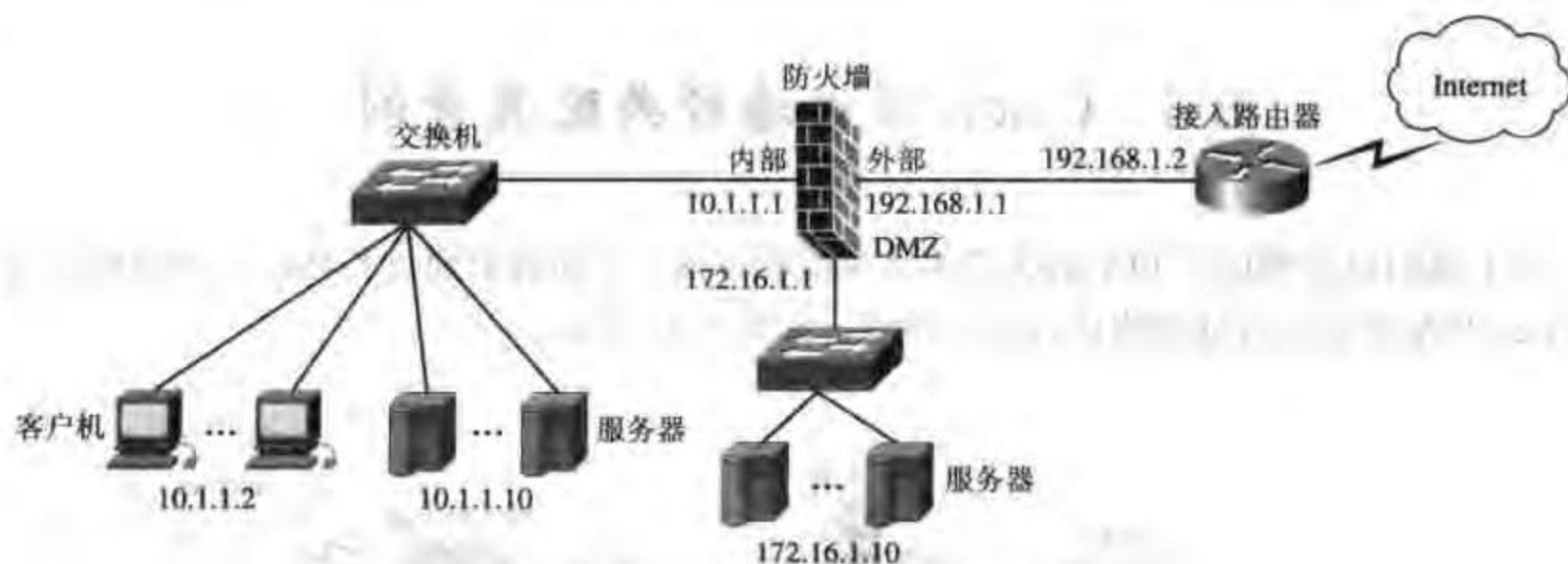



图 6-10 三接口配置图

```

passwd cisco
hostname pixfirewall
! ---启用内外和 dmz 接口
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
! ---设置内外接口的地址
ip address outside 192.168.1.1 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip address dmz 172.16.1.1 255.255.255.0
! ---设置全局复用地址池
global (outside) 1 192.168.1.200-192.168.1.253
! ---单个 PAT 地址
global (outside) 1 192.168.1.254
! ---设置 dmz 区复用地址池
global (dmz) 1 172.16.1.200-172.16.1.253
! ---转换所有内部地址
nat (inside) 1 0 0
! ---转换 dmz 区的地址
nat (dmz) 1 0 0
! ---将服务器 172.16.1.10 的地址映射为 192.168.1.10
static (dmz,outside) 192.168.1.10 172.16.1.10 netmask 255.255.255.255
! ---允许外部任何地址对 192.168.1.10 进行 www（端口 80）的访问
conduit permit tcp host 192.168.1.10 eq 80 any
! ---设置缺省路由
route outside 0.0.0.0 0.0.0.0 192.168.1.2

```

注意：在路由器上要配置到内网网段（10.1.1.0/24）的路由。

6.3 Cisco 防火墙经典配置案例

以上我们已经掌握了 PIX 防火墙的常见配置方法, 下面我们通过具体的示例说明如何使用 Cisco PIX 对企业内部网络进行安全管理, 如图 6-11 所示。

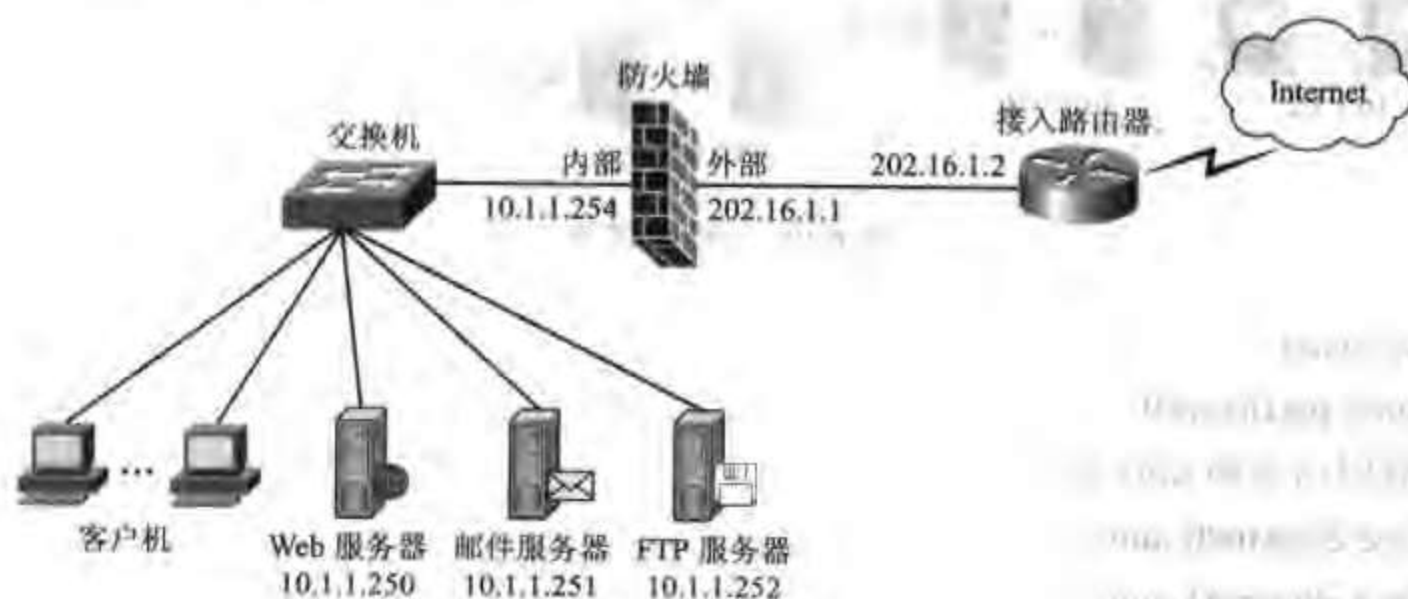


图 6-11 企业网络安全管理

1. 需求描述

Cisco PIX 安装 2 个网络接口, 一个连接外部网段, 另一个连接内部网段, 在内部网段上运行的有 WWW 服务器、电子邮件服务器和 FTP 服务器, 通过 Cisco PIX, 我们希望达到的效果是: 对内部网络的所有机器进行保护, Internet 上的主机只能访问内网的 WWW 服务器、电子邮件服务器和 FTP 服务器。内部主机通过 PIX 进行地址转换以实现上网。

ISP 分配给该企业的公网 IP 地址为 202.16.1.0~202.16.1.15 (注: 这是我们为本案例虚构的地址, 如果与某单位的地址重合, 纯属偶然), 子网掩码为 255.255.255.240, 在分配的地址段中, 202.16.1.0 为网络地址, 202.16.1.15 为广播地址, 因此可用的公网地址只有 202.16.1.1~202.16.1.14。

需要做的工作:

- (1) IP 地址规划;
- (2) 配置网络接口;
- (3) 配置由内至外的访问;
- (4) 配置由外至内的访问;
- (5) 常规配置。

2. 配置文档

(1) IP 地址规划

在配置 PIX 之前, 应该对网络进行详细的规划和设计, 要分配的 IP 地址如下:

- ① 每个 PIX 网络接口的 IP 地址 (Inside、Outside 等);
- ② 如果要进行网络地址转换, 则要提供一个 IP 地址池供 NAT 使用 (NAT 是网络地址转换技术, 它可以将使用保留地址的内部网段上的机器映射到一个合法的 IP 地址上以便进行

Internet 访问);

③ 外部网段的路由器地址。

表 6-2 本案例 IP 地址分配表

项 目		IP 地址
Pix	Outside	202.16.1.1/28
	Inside	10.1.1.254/24
	Web	202.16.1.14/28
	Email	202.16.1.13/28
	Ftp	202.16.1.12/28
	Nat Pool	202.16.1.3~7/28
	Pat	202.16.1.8/28
Router	Outside	unnumbered inside
	Inside	202.16.1.2/28

(2) 配置网络接口

PIX 使用 `nameif` 和 `ip address` 命令进行网络接口配置。首先使用下面的语句定义内部网段和外部网段的网络接口:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

PIX 防火墙使用 Intel 的 10/100Mbit/s 网卡, 使用下面的命令定义接口配置为自适应:

```
interface ethernet0 auto;
interface ethernet1 auto;
```

最后, 我们定义接口的 IP 地址和掩码:

```
ip address inside 10.1.1.254 255.255.255.0
ip address outside 202.16.1.1 255.255.255.240
```

(3) 配置由内至外的访问

在前面, 我们定义了内部网段安全值为 100, 外部网段安全值为 0。用户在安全值高的区域访问安全值低的区域, 需要使用 `nat` 和 `global` 命令; 相反, 如果允许安全值低的区域的用户访问安全值高的区域的用户, 则需要使用 `static` 和 `conduit` 命令:

```
nat (inside) 1 0 0
global (outside) 1 202.16.1.3-202.16.1.7
global (outside) 1 202.16.1.8
```

其中 1 为 NAT ID, 3 条语句中的 NAT ID 应一样。第一句表示允许所有机器对外访问, 第二句定义 NAT 使用的地址池, 第三句定义 NAT 转换地址。

定义外部路由: 对于外部网段, 还需要定义外部路由。该路由是防火墙外部网段的缺省路由, 命令语句如下:

```
route outside 0 0 202.16.1.2 1
```

其中 0 0 表示外部网段的缺省路由, 1 表示从防火墙到路由器只有一跳。

(4) 配置由外至内的访问

根据需求我们知道, 由外至内的访问主要包括外部对 Web、E-mail、FTP 服务器的访问。

缺省情况下, PIX 拒绝所有来自外部网段的访问请求。当 Web 服务器等设备放在防火墙的内部网段上时, 为了使外部网络上的用户可以访问到, 必须使用 `static` 和 `conduit` 命令来进行配置。下面, 我们给出允许外部网络访问内部网络上的 Web 服务器的命令:

```
static (inside,outside) 202.16.1.14 10.1.1.250 netmask 255.255.255.255
```

```
conduit permit tcp host 202.16.1.14 eq www any
```

其中, 第一条命令语句将在内部网段的 Web 服务器 10.1.1.250 映射一个外部合法地址 202.16.1.14; 第二条命令语句允许所有外部主机通过 TCP 端口 80 访问 202.16.1.14 这台服务器。

同理, 我们给出允许外部网络访问内部网络上的邮件服务器和 FTP 服务器的命令:

```
static (inside,outside) 202.16.1.13 10.1.1.251 netmask 255.255.255.255
```

```
conduit permit tcp host 202.16.1.13 eq smtp any
```

```
static (inside,outside) 202.16.1.12 10.1.1.252 netmask 255.255.255.255
```

```
conduit permit tcp host 202.16.1.12 eq ftp any
```

做完配置后, 不要忘记保存设置, 使用 `write memory` 命令将配置信息写入 flash。

至此, 我们对防火墙的功能性配置就完成了, 即现在的防火墙已经可以完成需求中描述的那些功能了, 但我们还需要对它进行一些常规的配置, 也可以称为管理性配置, 如主机名、密码等, 这些配置主要是为了方便我们管理而用的。

(5) 常规配置

① 设置主机名为 PIX515

```
Pixfirewall (config) # hostname PIX515
```

```
PIX515 (config) #
```

② 设置密码

```
PIX515 (config) # passwd cisco
```

```
PIX515 (config) # enable password cisco
```

③ 设置 telnet 访问控制

在 PIX 中, 我们可以定义只允许某些机器通过 telnet 访问防火墙。需要注意的是, 这里进行 telnet 访问的机器必须在内部网段上, 以增强安全性。

```
telnet 10.1.1.0 255.255.255.0
```

即允许 10.1.1.0 网段的主机使用 telnet 访问防火墙。

```
telnet timeout 15
```

即将空闲时间设置为 15 分钟, 当访问防火墙的机器 15 分钟内没有任何操作时, 将自动断开连接。

telnet 访问的缺省口令是 cisco, 可以通过 `passwd` 命令来修改口令。

④ 设置 SSH 访问控制

SSH 是和 telnet 类似的一种应用程序, telnet 以明文方式发送数据, 而 SSH 采用密文的方式传输数据, 因此具有更高的安全性。从外网对 PIX 防火墙进行配置只能通过 SSH 或 VPN 的方式。通常我们需要以下两个步骤来配置 SSH:

步骤 1, 生成并保存 RSA 密钥。


```
pix(config)#hostname test
test(config)#domain-name work.com
test(config)#ca generate rsa key 1024
test(config)#ca save all
```

步骤 2, 指定允许连接到 PIX 防火墙的主机。

```
test(config)#ssh 192.168.1.1 255.255.255.255 inside
test(config)#enable password cisco
test(config)#passwd cisco
```

⑤ 允许使用 ping 命令

```
conduit permit icmp any any
```

此命令的作用是: 允许在内部网段和外部网段使用 ping 命令进行网络测试。因为 ping 命令使用的是 ICMP 协议, 在设置和调试期间, 一般开放此功能, 当防火墙工作正常后, 也可以关闭此项功能。

到此为止, 我们已经比较详细地介绍了 PIX 防火墙通常会使用到的一些设置命令, 以及一些常见的配置模型, 当然, 如果大家需要更深层次地了解 PIX 防火墙, 建议大家可以查阅 Cisco 网站上的有关 PIX 的文档。这里我们给出一个比较有用的链接: <http://www.cisco.com/go/pix>

6.4 小 结

在本章的开始, 我们对防火墙的概念、原理及防火墙的硬件结构作了简要的介绍, 接下来对防火墙的配置方式以及一些常用的配置命令进行了介绍, 最后通过几个具体的案例, 详细讲解了目前使用最为广泛的几种防火墙的配置。下面我们给出常用配置防火墙的指导。

Cisco PIX 防火墙配置指导:

- 步骤 1, 命名接口并指定安全值 (nameif);
- 步骤 2, 启用接口 (interface);
- 步骤 3, 配置内外网卡和 DMZ 区的 IP 地址 (ip address);
- 步骤 4, 指定外部地址范围 (global);
- 步骤 5, 指定要进行转换的内部地址 (nat);
- 步骤 6, 设置指向内部网和外部网的缺省路由 (route);
- 步骤 7, 配置静态 IP 地址对映 (static);
- 步骤 8, 设置某些控制选项。

第 7 章 典型企业网构建案例

本章将涵盖下列有关企业网构建方面的关键主题：

- 小企业构建案例
- 中型企业网构建案例
- 大型企业网构建案例

7.1 简 介

通过前面几章的介绍，读者已经对企业网的组成结构，如何选择相应的设备来构建企业网（局域网、广域网和 Internet 接入部分）等知识有了一定的了解，同时也学习了组建企业网所需的主要设备（路由器、交换机和防火墙）的相关知识及配置方法。在学习和了解了上述的一些内容后，接下来将这些相对分散的部分结合起来，组装成适合用户要求的各式各样的企业网络。下面就通过几个具体的案例来进行说明。

7.2 小企业网络构建案例

7.2.1 案例 1

1. 需求描述

企业内部需要联网的节点数为 30 点，需要百兆比特交换到桌面，部门之间可以任意访问，内部网络主要用途是部门间信息的共享，接入 Internet 的主要目的是上网查询资料和收发电子邮件。

此案例的拓扑结构如图 7-1 所示。

2. 选型分析

交换机：

企业总节点数 30 点，选用一台 48 端口的低端交换机即可，可选 Catalyst2950G-48 或 Catalyst3550-48，区别是 2950 不支持三层交换而 3550 支持（三层交换可以等同为路由，区别是路由器通过软件实现路由而三层交换机通过硬件实现路由）。本案例中，部门之间可以任意访问，因此不需要划分 VLAN，也就不需要三层交换功能，因此我们可以选择 2950。

路由器：

根据需求描述我们知道企业上网的主要目的是浏览信息和日常的电子邮件的收发，同

时公司只有 30 个员工, 如果按并发 1:2 来计算, 公司同时会有 15 人接入 Internet。按目前 ADSL 接入的带宽 (512kbit/s) 计算, 每人会有 30k 左右的带宽, 这对一般的信息浏览和邮件交互来讲, 已经足够了。另外 ADSL 的接入费用相当便宜。因此我们选用 ADSL 的接入方式。

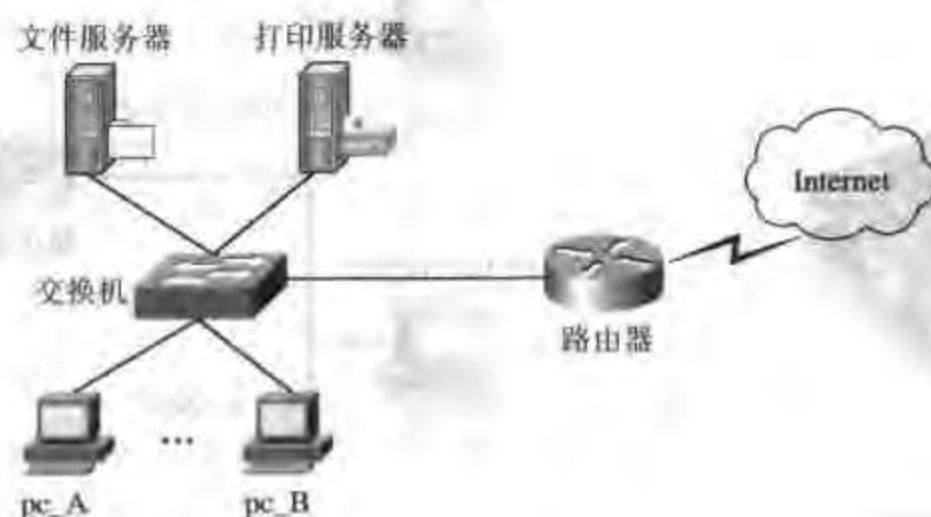


图 7-1 案例 1 拓扑图

在设备的选择上, 由于数据量不大, 所以可以选择 Cisco1721 加 WIC-1ADSL 模块的方式。

3. 产品列表

本案例所用产品见表 7-1, 有关产品如图 7-2~图 7-4 所示。

表 7-1

本案例产品列表

产 品	描 述	数 量
交换机		
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	1
路由器		
CISCO1721	10/100BaseT 模块路由器 w/2 WAN 插槽, 32M 闪存/64M DRAM	1
WIC-1ADSL	1 端口 ADSL WAN 接口板	1
SI7C7K9-12213T	Cisco 1700 IOS IP/ADSL PLUS IPSEC 3DES	1
CAB-ACA	插头, 电源线, 10A	1
CAB-ADSL-RJ11	Lavender 电缆用于 xDSL, 直通, RJ-11, 2m	1



图 7-2 Catalyst2950G-48



图 7-3 Cisco1721

4. 配置文档

本案例的配置方式如图 7-5 所示。其各部分具体配置如下：



图 7-4 WIC-1ADSL



图 7-5 案例 1 配置图

(1) 局域网部分

在本案例中，局域网交换机没有任何功能上的设置要求，只要加上电就可以工作了，但是一些常规的管理性和安全性的配置还是需要的。常见配置如下：

```
hostname cisco
enable password cisco
no ip domain-lookup
service timestamps debug uptime
service timestamps debug datetime
service timestamps log uptime
service timestamps log datetime
line con 0
login
line vty 0 4
password cisco
login
no ip http server
no snmp-server
no service finger
no ntp
no cdp run
no service udp-small-servers
no service tcp-small-servers
```

注意：以上 hostname（主机名）和 password（密码）部分，用户要根据自己的实际情况进行修改。

(2) 广域网部分

本案例中企业没有分支机构，因此没有构建自己的广域网络。

(3) Internet 接入部分

```
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Router_A
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
```

!--由于 ADSL 的 PPPoE 应用是通过虚拟拨号来实现的所以在路由器中需要使用 VPDN 的功能:

```
vpdn enable
no vpdn logging
!
!--为 PPPoE 启动 VPDN 的进程:
vpdn-group pppoe
!--作为 PPPoE 客户端向 PPPOE 终结设备请求连接:
request-dialin
!--设置拨号协议为 PPPoE:
protocol pppoe
!
interface FastEthernet 0
no shutdown
description connected to LAN_A
ip address 192.168.10.254 255.255.255.0
keepalive 10
!
!--设置 ADSL 端口:
interface ATM0
```



```

no ip address
no atm ilmi-keepalive
bundle-enable
dsl operating-mode auto
hold-queue 224 in
!
! --- ADSL 的通信依靠 VC, 所以必须设定点到点 VC:
interface ATM0.1 point-to-point
! --- 设置 PVC 的相关参数, 即 VCI 和 VPI 的值, 如果不清楚请向接入提供商查询:
pvc 8/35
! --- PPPoE 拨号进程使用了常规的拨号进程, 这里引用了 dialer-pool 1:
pppoe-client dial-pool-number 1
!
! --- 建立一个虚拟拨号端口:
interface Dialer1
! --- 由于局端提供动态地址, 所以必须设定地址为协商获得:
ip address negotiated
! --- 修改 mtu 值以适用于 ADSL 网络, 以太网的默认 MTU 值是 1500 字节 (1492 + PPPoE
headers = 1500):
ip mtu 1492
! --- 为启用 NAT 转换, 设置该端口为外部网络:
ip nat outside
! --- 使用 PPP 的帧格式:
encapsulation ppp
dialer pool 1
dialer-group 1
! --- 设置拨号的验证方式为 pap:
ppp authentication pap callin
! --- 发送用户名和密码, 如果不清楚请向接入提供商查询:
ppp pap sent 100000100000 pass 12345678
!
! --- 设置 NAT 的转换方式, 使用了 dialer 1 端口的动态地址:
ip nat inside source list 1 interface Dialer1 overload
!
ip classless
!
! --- 将所有不可路由的数据报转发给 ADSL 线路, 设定缺省路由:
ip route 0.0.0.0 0.0.0.0 dialer1
no ip http server

```



```

!
access-list 1 permit any
!
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!

```

7.2.2 案例 2

1. 需求描述

企业内部需要联网的节点数为 200 点, 信息点分布在 1~5 楼, 网络中心设在一楼, 大楼主干采用光纤布线, 在 1 楼和 3 楼设楼层配线架, 楼层需要百兆比特交换到桌面。企业主要包括技术部、财务部、销售部等, 部门间需划分 VLAN 进行隔离, 企业主要应用为内部文件共享、办公自动化系统 (OA), 对外提供邮件和网站服务等。企业总部申请了一根 DDN 专线, 接入当地 ISP, 用于 Internet 的接入, 同时用于和外地分支机构的 VPN 连接; 外地分支机构申请一条 ADSL 线路, 拨号接入 Internet, 同时该线路也用于和总部的 VPN 连接, 如图 7-6 所示。

2. 选型分析

(1) 交换机

企业总节点数 200 点, 应用为内部文件共享、办公自动化系统 (OA)、收发邮件和网站服务等, 这些都是非时间敏感型应用, 并非一刻不能停机, 因此没有必要设置核心设备的冗余, 我们可以在核心放置一台 Catalyst4507R, 它的背板带宽达到 64Gbit/s, 可支持各楼层数据的高速交换。它支持引擎的冗余, 在一定程度上提高了系统的可靠性。我们选择 4 代引擎 WS-X4515, 它有 48Mbit/s 的分组转发率, 可实现快速的数据转发; 选择 WS-X4306-GB 模块, 它有 6 个 GBIC 插槽, 可用于和各楼层的交换机实现吉比特互连。由于大楼的主干采用光纤布线, 所以我们可选用 WS-G5484 GBIC 模块用于和各楼层光纤互连。各楼层交换机我们可根据楼层的信息点数分别进行选择, 1 楼配线间汇聚 1~2 楼的信息点, 共 80 点, 选用两台

Catalyst2950G-48 交换机。3 楼配线间汇聚 3~5 楼的信息点，共 120 点，选用三台 Catalyst2950G-48 交换机，这款交换机有两个 GBIC 插槽，可选用 WS-G5484 GBIC 模块用于光纤上连核心交换机。

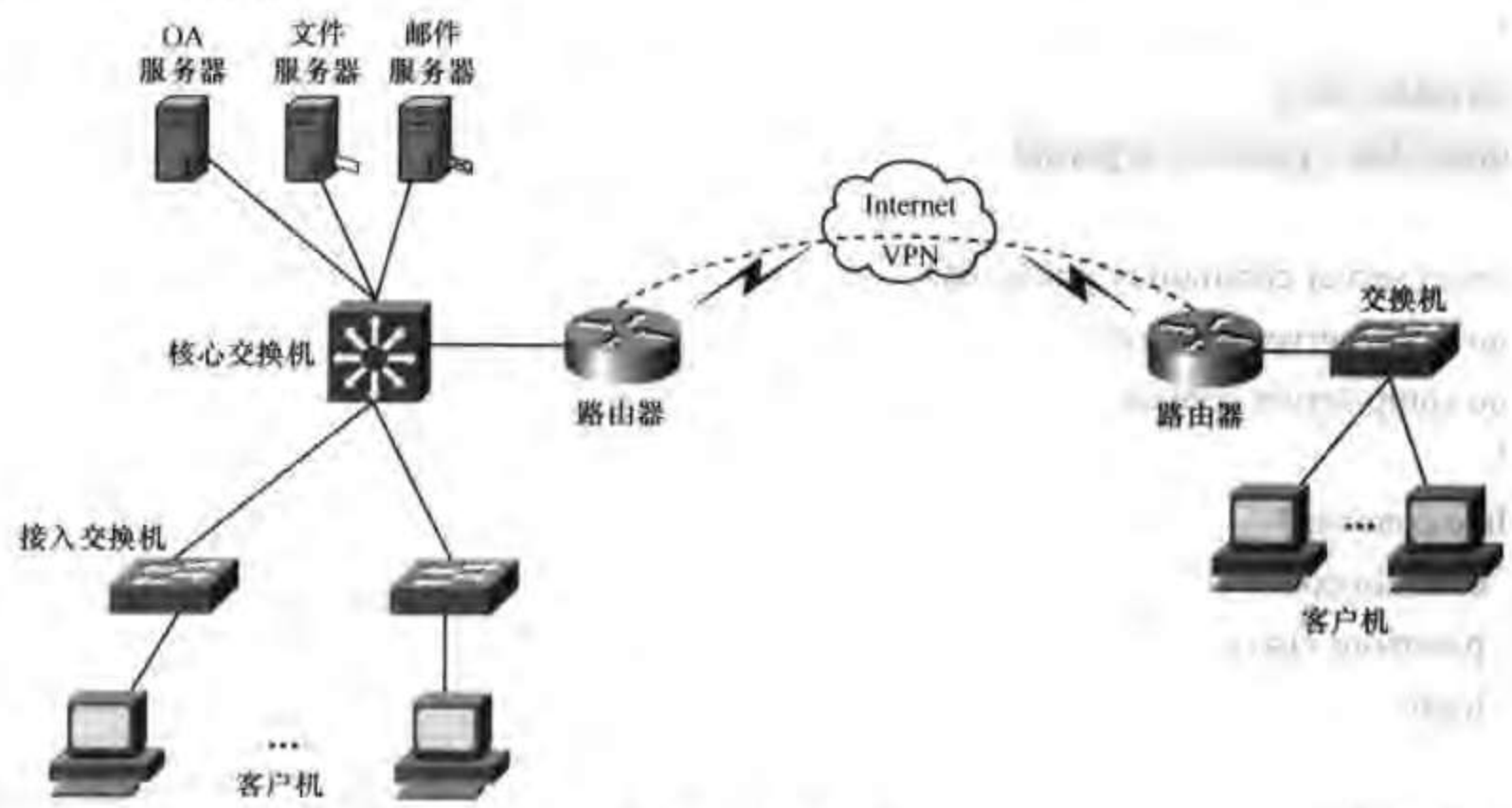


图 7-6 案例 2 拓扑图

(2) 路由器

根据需求描述，我们知道企业的主要应用为内部文件共享、办公自动化系统（OA），对外提供邮件和网站服务等，外地分支机构需要和总部通过 VPN 方式互连；企业有员工 200 人，如果按并发率 1：2 来计算，同时会有 100 人上网（通常达不到如此高的并发率），如果按申请 2Mbit/s 的 DDN 来计算，每人会有大约 20kbit/s 的带宽，对于正常的数据库访问来说是够用的；对于分支机构来说，信息点较少，采用经济实用的 ADSL 接入方式接入 Internet，分支机构对总部的访问可通过 VPN 的方式来实现。

设备的选择上，总部选用 Cisco2621xm 路由器加 WIC-1T 接口卡用于 DDN 的接入；分支选择 Cisco1721 加 WIC-1ADSL 接口卡用于 ADSL 的接入。

3. 产品列表

本案例所选用的产品见表 7-2。

表 7-2 本案例产品列表

产 品	描 述	数 量
总部		
交换机		
WS-C4507R	Catalyst 4500 Chassis (7-插槽), 风扇, 无 p/s, Red Sup Capable	1
PWR-C45-1000AC	Catalyst 4500 1000W AC 电源 (仅用于数据)	1
PWR-C45-1000AC/2	Catalyst 4500 1000W AC 备用电源	1
CAB-7KACA	AC 电源线	2
WS-X4515	Catalyst 4500 监视器 IV (2 GE), 控制台(RJ-45)	1
WS-X4515/2	Catalyst 4507R 备用监视器 IV, (2 GE), 控制台(RJ-45)	1
S4KL3-12113EW	Cisco IOS BASIC L3 Cat4500 SUP 3/4(RIP, St 路由器, IPX, AT)	1

		续表
产 品	描 述	数 量
WS-X4306-GB	Catalyst 4500 吉比特以太网模块, 6 端口 (GBIC)	1
WS-X4448-GB-RJ45	Catalyst 4500 48 端口 10/100/1000 模块 (RJ45)	1
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	5
WS-G5484	1000BASE-SX 短波长 GBIC (仅用于多模)	10
路由器		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP, 32 闪存/128 DRAM	1
CAB-ACA	插头, 电源线, 10A	1
S26C-12306	Cisco 2600 Ser IOS IP	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1
分支		
交换机		
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	1
路由器		
CISCO1721	10/100BaseT 模块路由器 w/2 WAN 插槽, 32M 闪存/64M DRAM	1
WIC-1ADSL	1 端口 ADSL WAN 接口板	1
MOD1700-VPN	Cisco 1700 系列 VPN 模块	1
S17C7K9-12213T	Cisco 1700 IOS IP/ADSL PLUS IPSEC 3DES	1
CAB-ACA	插头, 电源线, 10A	1
CAB-ADSL-RJ11	Lavender 电缆用于 xDSL, 直通, RJ-11, 2m	1

所选用产品的外观如图 7-7~图 7-16 所示。



图 7-7 Catalyst4507R



图 7-8 WS-X4515



图 7-9 WS-X4306-GB



图 7-10 WS-G5484



图 7-11 Catalyst2950G-48



图 7-12 Cisco2621XM



图 7-13 WIC-1T



图 7-14 CAB-V35MT



图 7-15 Cisco1721



图 7-16 WIC-1ADSL

4. 配置文档

本案例的设备配置如图 7-17 所示。

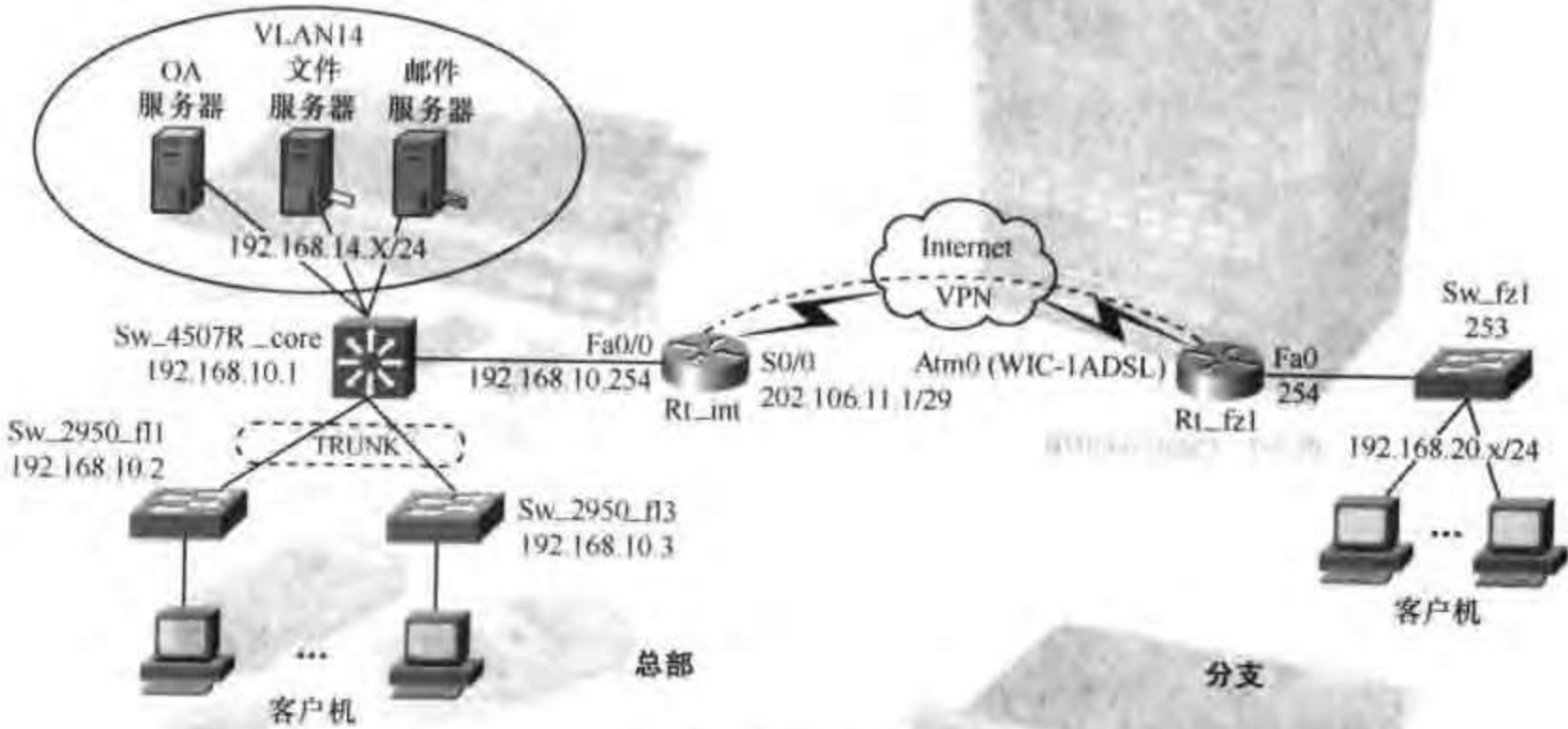


图 7-17 案例 2 配置图

(1) 局域网部分

局域网部分的配置如图 7-18 所示。

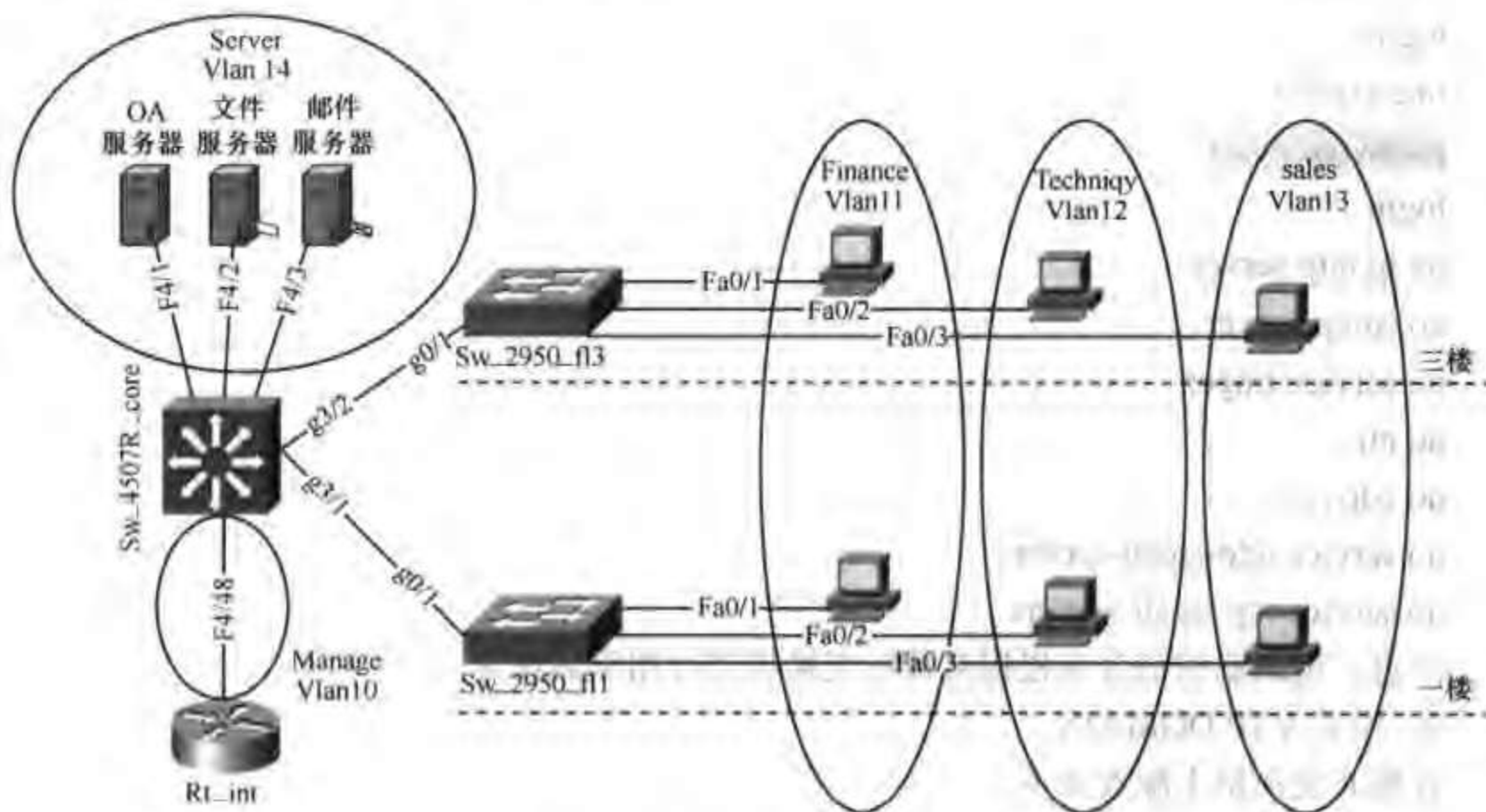


图 7-18 本案例局域网部分配置图

在局域网部分，需要做的工作包括：

- ① 交换机基础性配置；
- ② 设置 VTP DOMAIN（核心、接入交换机上都设置）；
- ③ 配置中继（核心、接入交换机上都设置）；
- ④ 创建 VLAN（在 VTP Server 上设置）；
- ⑤ 将交换机端口划入 VLAN；
- ⑥ 配置三层交换；
- ⑦ 配置路由。

下面我们分步来进行说明：

① 交换机基础性配置

对于核心交换机和楼层交换机的基础性配置，除主机名和密码外，其他基本相同。在做网络配置时，我们通常会对所有的网络设备进行规范的命名，命名的规则往往遵从简单和易于识别的原则，这里我们设置命名规则为，“类别_型号_作用_序号”。比如，“Sw_2950_f11”表示“一楼的 2950 交换机”，当只有一台时，序号可省略。

交换机的基础性配置如下：

```
hostname Sw_4507R_core
enable password cisco
no ip domain-lookup
service timestamps debug uptime
service timestamps debug datetime
service timestamps log uptime
```



```
service timestamps log datetime
line con 0
login
line vty 0 4
password cisco
login
no ip http server
no snmp-server
no service finger
no ntp
no cdp run
no service udp-small-servers
no service tcp-small-servers
```

注意：带阴影的部分应根据具体的交换机进行相应的设置。

② 设置 VTP DOMAIN

在核心交换机上配置如下：

```
Sw_4507R_core #vlan database
Sw_4507R_core (vlan)#vtp domain test
Sw_4507R_core (vlan)#vtp server
```

在楼层交换机上配置如下：

```
Sw_2950_fl1#vlan database
Sw_2950_fl1 (vlan)#vtp domain test
Sw_2950_fl1 (vlan)#vtp client
```

```
Sw_2950_fl3#vlan database
Sw_2950_fl3 (vlan)#vtp domain test
Sw_2950_fl3 (vlan)#vtp client
```

另外，还有一种简单的配置 VTP 的方式，如下所示：

```
Sw_4507R_core#conf t
Sw_4507R_core (config)#vtp domain test
Sw_4507R_core (config)#vtp mode server

Sw_2950_fl1#conf t
Sw_2950_fl1 (config)#vtp domain test
Sw_2950_fl1 (config)#vtp mode client
```

```
Sw_2950_fl3#conf t
Sw_2950_fl3 (config)#vtp domain test
Sw_2950_fl3 (config)#vtp mode client
```

③ 配置中继

在核心交换机上配置如下：


```
Sw_4507R_core (config)#interface gigabitEthernet 3/1
Sw_4507R_core (config-if)#description link to Sw_2950_fl1 g0/1
Sw_4507R_core (config-if)#switchport
Sw_4507R_core (config-if)#switchport trunk encapsulation dot1q
Sw_4507R_core (config-if)#switchport mode trunk
```

```
Switch_4507R_fl1 (config)#interface gigabitEthernet 3/2
Switch_4507R_fl1 (config-if)#description link to Sw_2950_fl3 g0/1
Switch_4507R_fl1 (config-if)#switchport
Switch_4507R_fl1 (config-if)#switchport trunk encapsulation dot1q
Switch_4507R_fl1 (config-if)#switchport mode trunk
```

在楼层交换机上配置如下:

```
Sw_2950_fl1 (config)#interface gigabitEthernet 0/1
Sw_2950_fl1 (config-if)#description link to Sw_4507R_core g3/1
Sw_2950_fl1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl1 (config-if)#switchport mode trunk
```

```
Sw_2950_fl3 (config)#interface gigabitEthernet 0/1
Sw_2950_fl3 (config-if)#description link to Sw_4507R_core g3/2
Sw_2950_fl3 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl3 (config-if)#switchport mode trunk
```

④ 创建 VLAN

在核心交换机 4507R 上配置 VLAN。(其实,只要是在管理域中的任何一台 VTP 属性为 Server 的交换机上建立 VLAN,它就会通过 VTP 通告整个管理域中的所有的交换机。)

```
Sw_4507R_core #vlan database
Sw_4507R_core (vlan)#Vlan 10 name manage
Sw_4507R_core (vlan)#Vlan 11 name finance
Sw_4507R_core (vlan)#Vlan 12 name techniqa
Sw_4507R_core (vlan)#Vlan 13 name sales
Sw_4507R_core (vlan)#Vlan 14 name server
```

另外,还有一种简单的创建 VLAN 的方式,如下所示:

```
Sw_4507R_core #conf t
Sw_4507R_core (config)#vlan 10,11,12,13,14
```

⑤ 将交换机端口划入 VLAN

在核心交换机上,需要将它的 fa4/1、4/2、4/3 端口划入 server VLAN(服务器),端口 fa4/48 划入 manage VLAN(管理)。

```
Sw_4507R_core (config)#interface range fastEthernet 4/1 - 3
Sw_4507R_core (config-if-range)#switchport mode access
Sw_4507R_core (config-if-range)#switchport access vlan 14
Sw_4507R_core (config)#interface fastEthernet 4/48
```



```
Sw_4507R_core (config-if)#switchport mode access
Sw_4507R_core (config-if)#switchport access vlan 10
```

说明: interface range 命令可以实现一次对多个端口进行配置,而不必分别配置每个端口。
在楼层交换机方面,我们假设要将 Sw_2950_f11、Sw_2950_f13 接入交换机的端口 fa0/1 划入 finance VLAN (财务部),端口 fa0/2 划入 techniqy VLAN (技术部),端口 fa0/3 划入 sales VLAN (销售部)。

```
Sw_2950_f11 (config)#interface fastEthernet 0/1
Sw_2950_f11 (config-if)#switchport mode access
Sw_2950_f11 (config-if)#switchport access vlan 11

Sw_2950_f11 (config)#interface fastEthernet 0/2
Sw_2950_f11 (config-if)#switchport mode access
Sw_2950_f11 (config-if)#switchport access vlan 12

Sw_2950_f11 (config)#interface fastEthernet 0/3
Sw_2950_f11 (config-if)#switchport mode access
Sw_2950_f11 (config-if)#switchport access vlan 13

Sw_2950_f13 (config)#interface fastEthernet 0/1
Sw_2950_f13 (config-if)#switchport mode access
Sw_2950_f13 (config-if)#switchport access vlan 11

Sw_2950_f13 (config)#interface fastEthernet 0/2
Sw_2950_f13 (config-if)#switchport mode access
Sw_2950_f13 (config-if)#switchport access vlan 12

Sw_2950_f13 (config)#interface fastEthernet 0/3
Sw_2950_f13 (config-if)#switchport mode access
Sw_2950_f13 (config-if)#switchport access vlan 13
```

⑥ 配置三层交换

到目前为止,VLAN 的划分已经结束。但是,此时只有本 VLAN 的主机之间可以互相访问,不同 VLAN 的主机之间是不能互访的。为了让不同 VLAN 之间可以互访,需要为不同的 VLAN 之间架起一座桥梁,这时就要给各 VLAN 接口分配网络 (IP) 地址了,这个地址也就是各 VLAN 主机的网关地址。

相应的 VLAN 和 IP 的分配表见表 7-3。

表 7-3 VLAN 及其 IP 地址

部 门	VLAN 名	VLAN ID	网关地址	网段地址
管理	manage	10	192.168.10.253	192.168.10.0/24
财务部	finance	11	192.168.11.253	192.168.11.0/24
技术部	techniqy	12	192.168.12.253	192.168.12.0/24
销售部	sales	13	192.168.13.253	192.168.13.0/24
服务器	server	14	192.168.14.253	192.168.14.0/24


```
Sw_4507R_core (config)#interface vlan 10
Sw_4507R_core (config-if)#ip address 192.168.10.253 255.255.255.0

Sw_4507R_core (config)#interface vlan 11
Sw_4507R_core (config-if)#ip address 192.168.11.253 255.255.255.0

Sw_4507R_core (config)#interface vlan 12
Sw_4507R_core (config-if)#ip address 192.168.12.253 255.255.255.0

Sw_4507R_core (config)#interface vlan 13
Sw_4507R_core (config-if)#ip address 192.168.13.253 255.255.255.0

Sw_4507R_core (config)#interface vlan 14
Sw_4507R_core (config-if)#ip address 192.168.14.253 255.255.255.0
```

完成上述配置后，在各接入 VLAN 的计算机上设置与所属 VLAN 的网络地址一致的 IP 地址，并且把默认网关设置为该 VLAN 的接口地址。这样，所有的 VLAN 也可以互访了。

⑦ 配置路由

在本案例中，由于结构相对简单，所以可以采用静态路由。在这里只需在核心交换机上配置默认路由，使其指向边界路由 Rt_int 即可。当然，为了使分支机构能够访问到总部里的各个 VLAN，还需要在边界路由器上为各个 VLAN 设置相应的路由。

```
Sw_4507R_core (config)# ip route 0.0.0.0 0.0.0.0 192.168.10.254
```

(2) 广域网和 Internet 接入部分

在本案例中和分支机构的广域网互连实际采用的是 VPN 技术，而 VPN 又是架构在 Internet 之上的，所以在这里将 Internet 接入和 VPN 的配置一起进行介绍，但在实际配置时，建议先配置 Internet 接入，等 Internet 接入正常后再配 VPN，这样思路会比较清晰，架果出现问题也比较容易排错。

① Rt_int

```
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Rt_int
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
```



```

no ip domain-lookup
ip routing
!
!
crypto isakmp enable
crypto isakmp identity address
!
!—— IKE 策略
crypto isakmp policy 1
  encryption des
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
group 1
!
!—— IPsec 策略
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto dynamic-map mymap 10
  match address 110
  set transform-set myset
!
crypto map mytrans 10 ipsec-isakmp dynamic mymap
!
!
interface FastEthernet 0/0
  no shutdown
  description connected to zb_LAN
  ip address 192.168.10.254 255.255.255.0
! ---配置此接口为地址转换（NAT）的内接口：
  ip nat inside
  keepalive 10
!
interface FastEthernet 0/1
  no description
  no ip address
  shutdown
!
interface Serial 0/0

```



```

no shutdown
description connected to Internet
ip address 202.106.11.1 255.255.255.248
! ---配置此接口为接口转换的外接口:
ip nat outside
encapsulation ppp
crypto map mytrans

```

!—— 定义引发 IPsec VPN 的数据

```

access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 110 deny ip 192.168.10.0 0.0.0.255 any

```

!—— 定义进行 NAT 的数据

```

access-list 120 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 120 permit ip 192.168.10.0 0.0.0.255 any

```

!

```

route-map nonat permit 10
match ip address 120

```

! ---配置静态 NAT 影射, 使内部地址 192.168.14.201 (File_server) 对应公网地址 202.106.11.2, 内部地址 192.168.14.202 (Mail_server) 对应公网地址 202.106.11.3, 该配置主要用于向外提供服务的服务器:

```

ip nat inside source static 192.168.14.201 202.106.11.2
ip nat inside source static 192.168.14.202 202.106.11.3

```

!

! ---定义从 ISP 那里申请到的公网 IP 在企业内部的分配策略, 这里定义了一个地址池 “natpool”, 它所涵盖的地址将被内网用户用来上网:

```

ip nat pool natpool 202.106.11.4 202.106.11.6 netmask 255.255.255.248

```

! ---将路由影射 “nonat” 定义的数据与地址池 “natpool” 对应, 即内网用户如果上网时其内部地址将被转换为 “202.106.11.4” ~ “202.106.11.6” 中的一个, 如果访问远程分支机构时, 不做地址转换, 而是引发 IPsec VPN 隧道的建立; “overload” 表示, 如果有多于地址池中定义的地址数量 (比如有 40 用户) 的用户访问外部, 那么多个内网地址可能会被转换为同一公网地址, 不同内网地址之间可以通过不同的端口来识别, 这样利用地址池定义的 3 个公网地址就可以带领所有的内网用户上网:

```

ip nat inside source route-map nonat pool natpool overload

```

!

```

ip classless

```

!

```

ip route 0.0.0.0 0.0.0.0 Serial 0/0

```

```

no ip http server

```

```

snmp-server community public RO

```



```

no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
end
② Rt_fz1
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Rt_fz1
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
crypto isakmp enable
crypto isakmp identity address
!
!—— IKE 策略
crypto isakmp policy 1
  encryption des
  hash md5
  authentication pre-share

```



```
crypto isakmp key cisco123 address 202.106.11.1
```

```
group 1
```

```
!
```

!——IPSec 策略

```
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

```
!
```

```
crypto map mymap 1 ipsec-isakmp
```

```
set peer 202.106.11.1
```

```
set transform-set myset
```

```
match address 110
```

```
!
```

!——由于 ADSL 的 PPPoE 应用是通过虚拟拨号来实现的所以在路由器中需要使用 VPDN 的功能:

```
vpdn enable
```

```
no vpdn logging
```

```
!
```

!——为 PPPoE 启动 VPDN 的进程:

```
vpdn-group pppoe
```

!——作为 PPPoE 客户端向 PPPOE 终结设备请求连接:

```
request-dialin
```

!——设置拨号协议为 PPPoE:

```
protocol pppoe
```

```
!
```

```
interface FastEthernet 0
```

```
no shutdown
```

```
description connected to fz1_LAN
```

```
ip address 192.168.20.254 255.255.255.0
```

```
keepalive 10
```

```
!
```

!——设置 ADSL 端口:

```
interface ATM0
```

```
no ip address
```

```
no atm ilmi-keepalive
```

```
bundle-enable
```

```
dsl operating-mode auto
```

```
hold-queue 224 in
```

```
!
```

!——ADSL 的通信依靠 VC, 所以必须设定点到点 VC:

```
interface ATM0.1 point-to-point
```


! ---设置 PVC 的相关参数, 即 VCI 和 VPI 的值, 如果不清楚, 请向接入提供商查询:

pvc 8/35

! --- PPPoE 拨号进程使用了常规的拨号进程, 这里引用了 dialer-pool 1:

pppoe-client dial-pool-number 1

!

! ---建立一个虚拟拨号端口:

interface Dialer1

! ---由于局端提供动态地址, 所以必须设定地址为协商获得:

ip address negotiated

!---修改 mtu 值以适用于 ADSL 网络, 以太网的默认 MTU 值是 1500 字节 (1492 + PPPoE headers = 1500):

ip mtu 1492

! ---为启用 NAT 转换, 设置该端口为外部网络:

ip nat outside

! ---使用 PPP 的帧格式:

encapsulation ppp

dialer pool 1

dialer-group 1

! ---设置拨号的验证方式为 pap:

ppp authentication pap callin

! ---发送用户名和密码, 如果不清楚, 请向接入提供商查询:

ppp pap sent 100000100000 pass 12345678

crypto map mymap

!

!—— 定义引发 IPsec VPN 的数据:

access-list 110 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

access-list 110 deny ip 192.168.20.0 0.0.0.255 any

!—— 定义进行 NAT 的数据:

access-list 120 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

access-list 120 permit ip 192.168.20.0 0.0.0.255 any

!

route-map nonat permit 10

match ip address 120

!

! ---设置 NAT 的转换方式, 使用了 dialer 1 端口的动态地址:

ip nat inside source route-map nonat interface Dialer1 overload

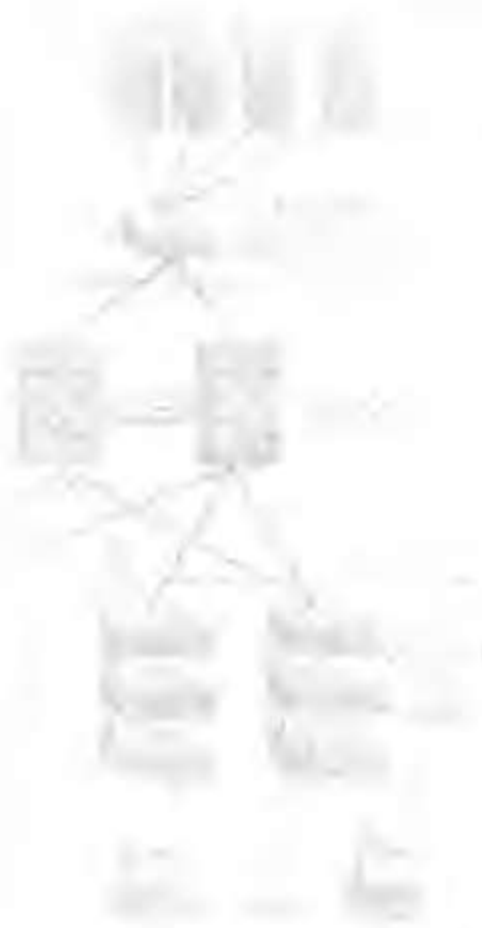
!

ip classless

!

! ---将所有不可路由的数据报转发给 ADSL 线路, 设定缺省路由:

```
ip route 0.0.0.0 0.0.0.0 dialer1
no ip http server
!
!
dialer-list 1 protocol ip permit
!
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
```



7.3 中型企业网络构建案例

1. 需求描述

企业内部需要联网的节点数为 2000 点, 信息点的分布为: 1~10 楼各 200 点, 网络中心位于 1 楼, 整个大楼主干采用光纤布线, 楼层需要百兆交换到桌面。楼层配线架分别设在 1、3、5、7、9 层的配线间。企业主要包括技术部、财务部、销售部等, 部门间需划分 VLAN 进行隔离。企业网络的主要应用分为两部分: 一部分是基础的网络应用, 它包括内部文件共享、办公自动化系统 (OA), 邮件和网站服务等; 另一部分是企业的业务应用系统。企业网中大部分的用户数据来自对业务应用系统的访问, 同时业务应用系统的可靠性的要求也最高。企业总部申请了一根 E1 数字线路, 用于和外地分支机构之间的互连, 同时申请一条 DDN 专线接入当地 ISP, 用于 Internet 的接入。分支机构 1 和 2 各申请一条 256k 线路用于和总部互连, 分支机构 1 采用模拟电话线路 (PSTN) 作为主干线路的备份, 分支机构 2 采用 ISDN 作为主干线路的备份。本案例的拓扑结构如图 7-19 所示。

2. 选型分析

(1) 交换机

企业总节点数 2000 点, 应用分为基础网络应用和企业的业务系统。由于业务系统对可靠性有很高的要求, 因此, 整体网络结构应采用冗余配置, 避免单点故障 (当然, 这里只讨

论网络方面的可靠性,对于整个业务系统,为了保证其整体的稳定可靠,除了网络系统,还应该考虑其他方面的因素,比如服务器采用冗余系统,供电方面采用 UPS 等)。由于企业网中大部分的用户数据来自对业务应用系统的访问,因此整个网络采用二层结构。

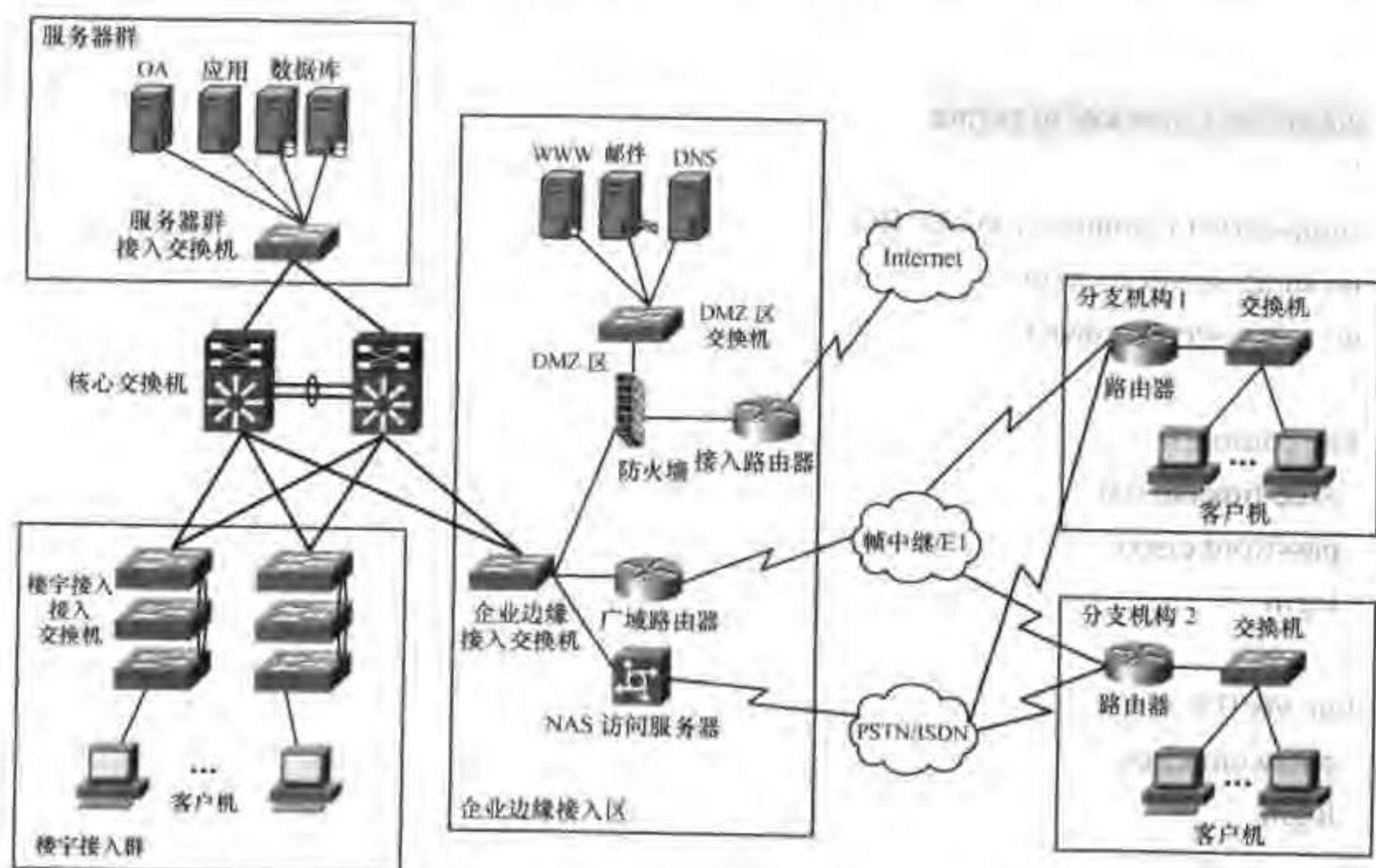


图 7-19 本案例的拓扑图

整体网络结构定下来之后,即可进行核心和接入层设备的选型。根据网络中数据量的大小,可确定核心层的设备,如果没有具体的数据,则可以参考经验值进行选择。就拿这个案例来说,整个网络有 2000 个信息点,如果按 1:2 的并发率来算,整个网络就有约 1000 个点同时进行数据传输,每个信息点 100Mbit/s,那么整个网络就需要 100Gbit/s。也就是说,如果要让这 1000 个点进行数据的无阻塞的线速转发,那么整个网络的带宽就必须大于 100Gbit/s。如果考虑到尖峰时刻(2000 点同时进行网络访问)的流量 200G,那意味着我们的核心设备最好应具有 200G 以上的处理能力。目前 Cisco 只有 Catalyst6500 系列交换机满足这一要求,其中 Catalyst6500 的二代引擎具有 256G 的背板带宽,新一代的 720 引擎具有 720G 的背板带宽。二代引擎要满足 256G 的处理能力,必须另外配矩阵模块,这样无形中多占了一个插槽,同时也就多了一个可能的故障点。更重要的是,加上这些之后,二代引擎的价格和 720 引擎的价格相差无几,因此,从性价比、可靠性和扩展性上考虑,我们建议选择配置 720 引擎的 Catalyst6509。在模块方面,选择一块 WS-X6516-GBIC 模块,共 16 个 GBIC 插槽,可用于和各楼层的交换机实现吉比特互联。由于大楼的主干采用光纤布线,所以可选用 WS-G5484 GBIC 模块用于和各楼层光纤互联。至此核心交换机就选完了。至于是否采用冗余电源和引擎,提出如下建议:如果采用了双核心结构,即整机是冗余的,那么模块就没必要非要冗余,当然这要取决于网络的重要性的我们对网络可靠性的评估。即如果网络由于单点故障导致瘫痪,那么企业的损失可能有多大。如果这个损失非常巨大,还是建议进行引擎和

电源的冗余配置。

各楼层交换机可根据楼层的信息点数分别进行选择，每两层楼设一个配线间汇聚两层楼的信息点共 400 点。比如 1 楼配线间汇聚 1~2 楼的信息点（共 400 点），可选用 9 台 Catalyst2950G-48 交换机进行堆叠设置，整个堆叠体通过 WS-G5484 GBIC 模块双上联至网络核心。其他配线间和 1 层配线间完全相同。

除了楼层的交换机外，还需要为服务器区和边缘接入区以及防火墙的 DMZ 区分别选择一台交换机。这里，根据具体的信息点数，为服务器区和边缘接入区选择 Catalyst2950G-24 交换机，它通过 WS-G5484 GBIC 模块双上联至网络核心。DMZ 区可以选择 WS-C2950-24 百兆交换机。

说明：

① 上述的选型分析是基于网络的瓶颈集中在核心交换机上而做出的，如果网络的瓶颈在其他部分，可根据具体情况进行分析；

② 核心设备的背板最好 200G 以上，并不代表低于 200G 不能运行，它只表示如果低于 200G，那么在尖峰时刻，网络可能会产生拥堵。

（2）路由器

由于企业应用包括基础应用和业务系统的应用两部分，内部文件共享、邮件和办公自动化系统（GA）这些基础的网络应用对网络的可靠性、安全性要求都不是很高，但企业的业务应用系统是企业正常运行的根本，它的可靠和安全直接影响企业的生存。因此需要采用专线方式构建一个专有的企业的私有网络。同时，还需要在各分支和总部间构建一条备份线路，一旦主线路断掉，备份线路立即启用。在专线的选择上，低速专线（又称窄带专线，指 2M 以下的专线）主要包括 DDN 和帧中继。在本案例中，企业总部申请了一根 E1 数字线路，用于和外地分支机构之间的互连，同时申请一条 DDN 专线接入当地 ISP，用于 Internet 的接入。分支机构 1 和 2 各申请一条 256K 线路用于和总部互连，分支机构 1 采用模拟电话线路（PSTN）作为主干线路的备份，分支机构 2 采用 ISDN 作为主干线路的备份。

在设备的选择上，根据具体的业务采，建议在总部采用 Cisco3725，配置 NM-1CE1U 模块用于和分支机构 E1 的互连，另外选用 Cisco2621xm 路由器配 NM-1CE1U 模块和 NM-30DM 模块用于分支机构的 PSTN 或 ISDN 接入，作为主干线路的备份；分支机构 1 采用 Cisco2621XM，配置 WIC-1T 串口模块用于和总部 E1 的互连，配置 WIC-1AM 模块用于 PSTN 备份接入总部；分支机构 2 采用 Cisco2621XM，配置 WIC-1T 串口模块用于和总部 E1 的互连，配置 WIC-1B-S/T 模块用于 ISDN 备份接入总部。

本案例所用的产品见表 7-4，其外观如图 7-20~图 7-33 所示。

表 7-4

本案例产品列表

产 品	描 述	数 量
总部		
交换机		
WS-C6509	Cat 6509 Chassis, 9 槽槽, 15RU, 无电源, 无风扇架	2
S733Z-12217SXB	Cisco CAT6000-SUP720 IOS IP	2
WS-SUP720	Catalyst 6500/Cisco 7600 监视器 720 光纤 MSFC3 PFC3A	2
WS-X6516-GBIC	Catalyst 6500 16 端口吉比特以太网模块 光纤可用 (Req GBICs)	2

		续表
产 品	描 述	数 量
WS-C6K-9SLOT-FAN2	Catalyst 6509 高速风扇架	2
WS-CAC-2500W	Catalyst 6000 2500W AC 电源	4
CAB-AC-2500W-INT	电源线, 250Vac 16A, INTL	4
WS-G5484	1000BASE-SX 短波长 GBIC (仅用于多模)	32
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	45
WS-C2950G-24-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 24 10/100	2
WS-C2950-24	24 端口, 10/100 Catalyst 交换, 仅用于标准图像功能	1
WS-G5484	1000BASE SX 短波长 GBIC (仅用于多模)	14
路由器		
CISCO3725	3700 系列, 2 插槽, 双 FE, 多业务接入路由器	1
S372IPB-12302T	Cisco 3725 Ser IOS IP BASE	1
NM-ICE1U	1 端口信道化 E1/ISDN-PRI 不平衡网络模块	1
CAB-E1-BNC	E1 电缆 BNC 75Ω (不平衡) 5m	1
CAB-ACA	插头, 电源线, 10A	1
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP, 32 闪存/128DRAM	1
S26C-12306	Cisco 2600 Ser IOS IP	1
NM-ICE1U	1 端口信道化 E1/ISDN-PRI 不平衡网络模块	1
CAB-E1-BNC	E1 电缆 BNC 75Ω (不平衡) 5m	1
NM-30DM	30 端口数字 Modem 网络模块	1
CAB-ACA	插头, 电源线, 10A	1
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP, 32 闪存/128DRAM	1
S26C-12306	Cisco 2600 Ser IOS IP	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V 35 电缆, DTE, 插头, 3m	1
CAB-ACA	插头, 电源线, 10A	1
防火墙		
PIX-515E-UR-BUN	PIX 515E-UR Bundle (Chassis, Unrestricted SW, 2 FE, VAC+)	1
PIX-1FE	PIX 10/100 快速以太网接口板, RJ45	1
分支 1		
交换机		
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	1
路由器		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP, 32 闪存/128DRAM	1
S26C-12306	Cisco 2600 Ser IOS IP	1
WIC-1AM	1 端口模拟 Modem WAN 接口板	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V 35 电缆, DTE, 插头, 3m	1
CAB-ACA	插头, 电源线, 10A	15
分支 2		
交换机		

续表

产 品	描 述	数 量
WS-C2950G-48-EI	带有 2 GBIC 插槽, 图像增强功能的 Catalyst 2950, 48 10/100	1
路由器		
CISCO2621XM	中等性能双 10/100 以太网路由器 w/Cisco IOS IP,32 闪存/128DRAM	1
S26C-12306	Cisco 2600 Ser IOS IP	1
WIC-1B-S/T	1 端口 ISDN WAN 接口板(拨号和专线)	1
WIC-1T	1 端口串行 WAN 接口板	1
CAB-V35MT	V.35 电缆, DTE, 插头, 3m	1
CAB-ACA	插头,电源线,10A	1



图 7-20 Catalyst6509



图 7-21 WS-SUP720



图 7-22 WS-X6516-GBIC



图 7-23 WS-X6548-GE-TX



图 7-24 Cisco3725



图 7-25 NM-1CE1U



图 7-26 NM-30DM



图 7-27 CAB-EI-BNC



图 7-28 Cisco2621XM 正面



图 7-29 WIC-1T



图 7-30 CAB-V35MT



图 7-31 WIC-1AM



图 7-32 WIC-1B-S/T



图 7-33 PIX515E

3. 配置文档

本案例中各设备的配置如图 7-34 所示。

(1) 局域网部分

局域网部分的配置如图 7-35 所示。

在局域网部分需要进行如下配置工作：

- ① 交换机基础性配置；
- ② 设置 VTP DOMAIN（核心、接入交换机上都设置）；
- ③ 配置中继（核心、接入交换机上都设置）；
- ④ 配置链路捆绑（Ethernet-Channel）；

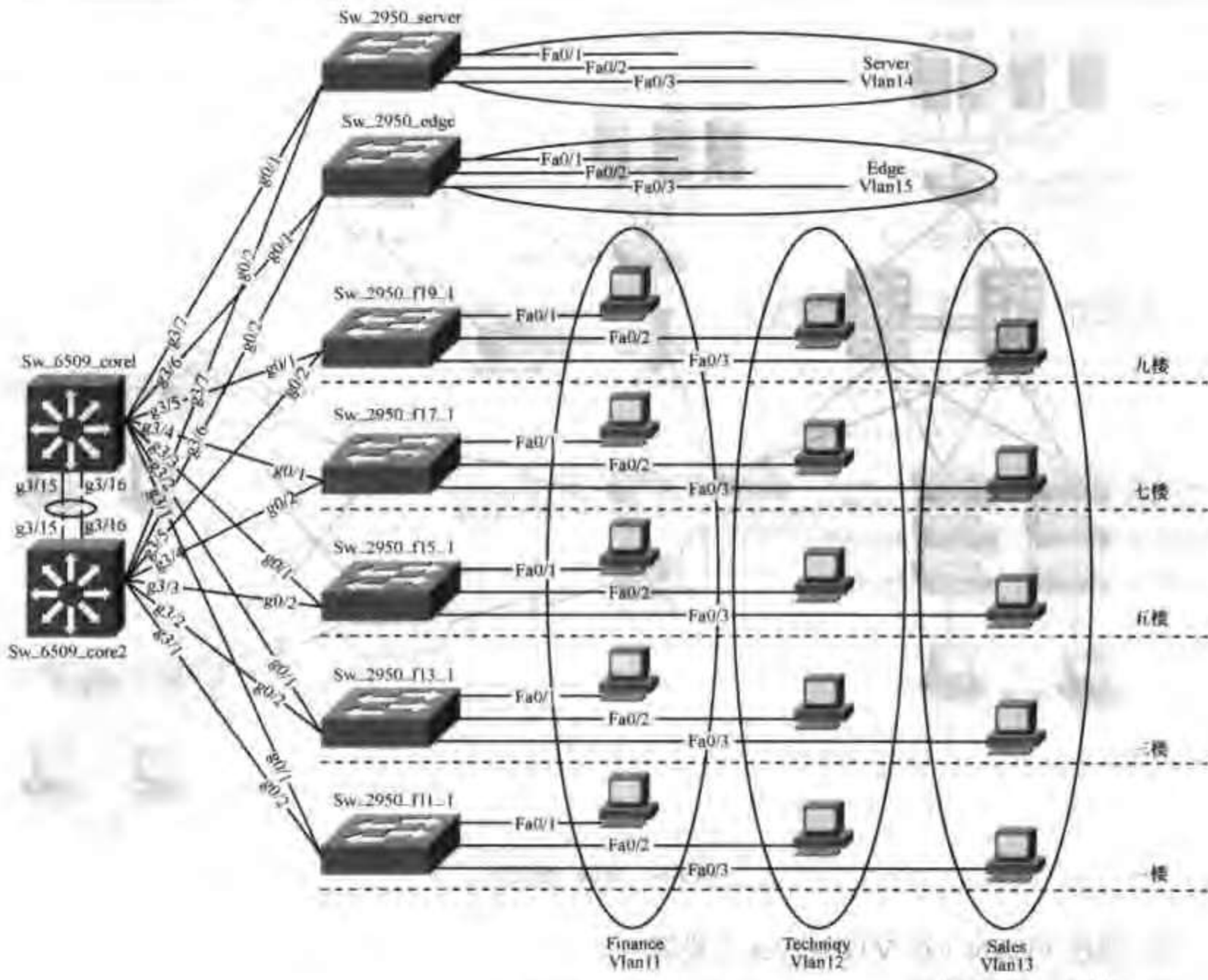


图 7-35 本案例局域网部分配置图

```
service timestamps log datetime
line con 0
login
line vty 0 4
password cisco
login
no ip http server
no snmp-server
no service finger
no ntp
no cdp run
no service udp-small-servers
no service tcp-small-servers
```

注意：带阴影的部分根据具体的交换机进行相应的设置。

② 设置 VTP DOMAIN

在核心交换机上配置如下：


```
Sw_6509_core1 #vlan database
Sw_6509_core1 (vlan)#vtp domain test
Sw_6509_core1 (vlan)#vtp server

Sw_6509_core2 #vlan database
Sw_6509_core2 (vlan)#vtp domain test
Sw_6509_core2 (vlan)#vtp client
```

在楼层交换机上配置如下：

```
Sw_2950_fl1_1#vlan database
Sw_2950_fl1_1 (vlan)#vtp domain test
Sw_2950_fl1_1 (vlan)#vtp client

Sw_2950_fl3_1#vlan database
Sw_2950_fl3_1 (vlan)#vtp domain test
Sw_2950_fl3_1 (vlan)#vtp client

Sw_2950_fl5_1#vlan database
Sw_2950_fl5_1 (vlan)#vtp domain test
Sw_2950_fl5_1 (vlan)#vtp client

Sw_2950_fl7_1#vlan database
Sw_2950_fl7_1 (vlan)#vtp domain test
Sw_2950_fl7_1 (vlan)#vtp client

Sw_2950_fl9_1#vlan database
Sw_2950_fl9_1 (vlan)#vtp domain test
Sw_2950_fl9_1 (vlan)#vtp client
```

另外，还有一种简单的配置 VTP 的方式，如下所示：

```
Sw_6509_core1 #conf t
Sw_6509_core1 (config)#vtp domain test
Sw_6509_core1 (config)#vtp mode server

Sw_6509_core2 #conf t
Sw_6509_core2 (config)#vtp domain test
Sw_6509_core2 (config)#vtp mode client

Sw_2950_fl1_1#conf t
Sw_2950_fl1_1 (config)#vtp domain test
Sw_2950_fl1_1 (config)#vtp mode client

Sw_2950_fl3_1#conf t
Sw_2950_fl3_1 (config)#vtp domain test
Sw_2950_fl3_1 (config)#vtp mode client
```



```
Sw_2950_fl5_1#conf t
Sw_2950_fl5_1 (config)#vtp domain test
Sw_2950_fl5_1 (config)#vtp mode client
```

```
Sw_2950_fl7_1#conf t
Sw_2950_fl7_1 (config)#vtp domain test
Sw_2950_fl7_1 (config)#vtp mode client
```

```
Sw_2950_fl9_1#conf t
Sw_2950_fl9_1 (config)#vtp domain test
Sw_2950_fl9_1 (config)#vtp mode client
```

③ 配置中继

在核心交换机上配置如下：

```
Sw_6509_core1 (config)#interface gigabitEthernet 3/1
Sw_6509_core1 (config-if)#description link to Sw_2950_fl1_1 g0/1
Sw_6509_core1 (config-if)#switchport
Sw_6509_core1 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core1 (config-if)#switchport mode trunk
```

```
Sw_6509_core1 (config)#interface gigabitEthernet 3/2
Sw_6509_core1 (config-if)#description link to Sw_2950_fl3_1 g0/1
Sw_6509_core1 (config-if)#switchport
Sw_6509_core1 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core1 (config-if)#switchport mode trunk
```

```
Sw_6509_core1 (config)#interface gigabitEthernet 3/3
Sw_6509_core1 (config-if)#description link to Sw_2950_fl5_1 g0/1
Sw_6509_core1 (config-if)#switchport
Sw_6509_core1 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core1 (config-if)#switchport mode trunk
```

```
Sw_6509_core1 (config)#interface gigabitEthernet 3/4
Sw_6509_core1 (config-if)#description link to Sw_2950_fl7_1 g0/1
Sw_6509_core1 (config-if)#switchport
Sw_6509_core1 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core1 (config-if)#switchport mode trunk
```

```
Sw_6509_core1 (config)#interface gigabitEthernet 3/5
Sw_6509_core1 (config-if)#description link to Sw_2950_fl9_1 g0/1
Sw_6509_core1 (config-if)#switchport
Sw_6509_core1 (config-if)#switchport trunk encapsulation dot1q
```



```
Sw_6509_core1 (config-if)#switchport mode trunk
```

```
Sw_6509_core2 (config)#interface gigabitEthernet 3/1
```

```
Sw_6509_core2 (config-if)#description link to Sw_2950_fl1_1 g0/2
```

```
Sw_6509_core2 (config-if)#switchport
```

```
Sw_6509_core2 (config-if)#switchport trunk encapsulation dot1q
```

```
Sw_6509_core2 (config-if)#switchport mode trunk
```

```
Sw_6509_core2 (config)#interface gigabitEthernet 3/2
```

```
Sw_6509_core2 (config-if)#description link to Sw_2950_fl3_1 g0/2
```

```
Sw_6509_core2 (config-if)#switchport
```

```
Sw_6509_core2 (config-if)#switchport trunk encapsulation dot1q
```

```
Sw_6509_core2 (config-if)#switchport mode trunk
```

```
Sw_6509_core2 (config)#interface gigabitEthernet 3/3
```

```
Sw_6509_core2 (config-if)#description link to Sw_2950_fl5_1 g0/2
```

```
Sw_6509_core2 (config-if)#switchport
```

```
Sw_6509_core2 (config-if)#switchport trunk encapsulation dot1q
```

```
Sw_6509_core2 (config-if)#switchport mode trunk
```

```
Sw_6509_core2 (config)#interface gigabitEthernet 3/4
```

```
Sw_6509_core2 (config-if)#description link to Sw_2950_fl7_1 g0/2
```

```
Sw_6509_core2 (config-if)#switchport
```

```
Sw_6509_core2 (config-if)#switchport trunk encapsulation dot1q
```

```
Sw_6509_core2 (config-if)#switchport mode trunk
```

```
Sw_6509_core2 (config)#interface gigabitEthernet 3/5
```

```
Sw_6509_core2 (config-if)#description link to Sw_2950_fl9_1 g0/2
```

```
Sw_6509_core2 (config-if)#switchport
```

```
Sw_6509_core2 (config-if)#switchport trunk encapsulation dot1q
```

```
Sw_6509_core2 (config-if)#switchport mode trunk
```

在楼层交换机上配置如下：

```
Sw_2950_fl1_1 (config)#interface gigabitEthernet 0/1
```

```
Sw_2950_fl1_1 (config-if)#description link to Sw_6509_core1 g3/1
```

```
Sw_2950_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Sw_2950_fl1_1 (config-if)#switchport mode trunk
```

```
Sw_2950_fl1_1 (config)#interface gigabitEthernet 0/2
```

```
Sw_2950_fl1_1 (config-if)#description link to Sw_6509_core2 g3/1
```

```
Sw_2950_fl1_1 (config-if)#switchport trunk encapsulation dot1q
```

```
Sw_2950_fl1_1 (config-if)#switchport mode trunk
```



```
Sw_2950_fl3_1 (config)#interface gigabitEthernet 0/1
Sw_2950_fl3_1 (config-if)#description link to Sw_6509_core1 g3/1
Sw_2950_fl3_1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl3_1 (config-if)#switchport mode trunk
Sw_2950_fl3_1 (config)#interface gigabitEthernet 0/2
Sw_2950_fl3_1 (config-if)#description link to Sw_6509_core2 g3/1
Sw_2950_fl3_1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl3_1 (config-if)#switchport mode trunk

Sw_2950_fl5_1 (config)#interface gigabitEthernet 0/1
Sw_2950_fl5_1 (config-if)#description link to Sw_6509_core1 g3/1
Sw_2950_fl5_1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl5_1 (config-if)#switchport mode trunk
Sw_2950_fl5_1 (config)#interface gigabitEthernet 0/2
Sw_2950_fl5_1 (config-if)#description link to Sw_6509_core2 g3/1
Sw_2950_fl5_1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl5_1 (config-if)#switchport mode trunk

Sw_2950_fl7_1 (config)#interface gigabitEthernet 0/1
Sw_2950_fl7_1 (config-if)#description link to Sw_6509_core1 g3/1
Sw_2950_fl7_1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl7_1 (config-if)#switchport mode trunk
Sw_2950_fl7_1 (config)#interface gigabitEthernet 0/2
Sw_2950_fl7_1 (config-if)#description link to Sw_6509_core2 g3/1
Sw_2950_fl7_1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl7_1 (config-if)#switchport mode trunk

Sw_2950_fl9_1 (config)#interface gigabitEthernet 0/1
Sw_2950_fl9_1 (config-if)#description link to Sw_6509_core1 g3/1
Sw_2950_fl9_1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl9_1 (config-if)#switchport mode trunk
Sw_2950_fl9_1 (config)#interface gigabitEthernet 0/2
Sw_2950_fl9_1 (config-if)#description link to Sw_6509_core2 g3/1
Sw_2950_fl9_1 (config-if)#switchport trunk encapsulation dot1q
Sw_2950_fl9_1 (config-if)#switchport mode trunk
```

④ 配置链路捆绑（以太网通道）

在两台核心设备之间配置多链路捆绑，能形成更大的数据传输的通道，有利于数据的快速转发，同时也能实现链路的冗余。在本案例中，将两台核心交换机的两个吉比特端口捆绑成一条 4Gbit/s（全双工）的逻辑通道。

```
Sw_6509_core1 (config)#interface gigabitEthernet 3/15
```



```

Sw_6509_core1 (config-if)#description link to Sw_6509_core2 g3/15
Sw_6509_core1 (config-if)#switchport
Sw_6509_core1 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core1 (config-if)#switchport mode trunk
Sw_6509_core1 (config-if)#channel-group 1 mode desirable
Sw_6509_core1 (config)#interface gigabitEthernet 3/16
Sw_6509_core1 (config-if)#description link to Sw_6509_core2 g3/16
Sw_6509_core1 (config-if)#switchport
Sw_6509_core1 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core1 (config-if)#switchport mode trunk
Sw_6509_core1 (config-if)#channel-group 1 mode desirable
Sw_6509_core1 (config)#interface port-channel 1
Sw_6509_core1 (config-if)#switchport
Sw_6509_core1 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core1 (config-if)#switchport mode trunk
Sw_6509_core2 (config)#interface gigabitEthernet 3/15
Sw_6509_core2 (config-if)#description link to Sw_6509_core1 g3/15
Sw_6509_core2 (config-if)#switchport
Sw_6509_core2 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core2 (config-if)#switchport mode trunk
Sw_6509_core2 (config-if)#channel-group 1 mode desirable
Sw_6509_core2 (config)#interface gigabitEthernet 3/16
Sw_6509_core2 (config-if)#description link to Sw_6509_core1 g3/16
Sw_6509_core2 (config-if)#switchport
Sw_6509_core2 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core2 (config-if)#switchport mode trunk
Sw_6509_core2 (config-if)#channel-group 1 mode desirable
Sw_6509_core2 (config)#interface port-channel 1
Sw_6509_core2 (config-if)#switchport
Sw_6509_core2 (config-if)#switchport trunk encapsulation dot1q
Sw_6509_core2 (config-if)#switchport mode trunk

```

⑤ 创建 VLAN

其实，我们只需要在管理域中的任何一台 VTP 属性为 Server 的交换机上建立 VLAN，它就会通过 VTP 通告整个管理域中的所有的交换机。本案例中，“test”域中的 VTP Server 是 Sw_6509_core1，因此我们只需对它进行 VLAN 的配置即可。

```

Sw_6509_core1 #vlan database
Sw_6509_core1 (vlan)#Vlan 2 name manage
Sw_6509_core1 (vlan)#Vlan 11 name finance

```



```
Sw_6509_core1 (vlan)#Vlan 12 name techniqy
Sw_6509_core1 (vlan)#Vlan 13 name sales
Sw_6509_core1 (vlan)#Vlan 14 name server
Sw_6509_core1 (vlan)#Vlan 15 name edge
```

另外，还有一种简单的创建 VLAN 的方式，如下所示：

```
Sw_6509_core1 #conf t
Sw_6509_core1 (config)#vlan 2,11,12,13,14,15
```

⑥ 设置生成树的根

这里将 Vlan2、11、12 的生成树的首根 (Primary Root) 设到 Sw_6509_core1 上，次根 (Secondary Root) 设到 Sw_6509_core2 上，将 Vlan13、14、15 的生成树的首根 (Primary Root) 设到 Sw_6509_core2 上，次根 (Secondary Root) 设到 Sw_6509_core1 上，这样使网络的负载可以均衡地分布在两台核心上，同时保证在主交根机宕机的情况下，辅交根机可以快速正常地接管工作。

说明：其实我们可以不用手工设置生成树的根，所有交换机会通过生成树算法来计算各 vlan 的根，但这样的结果可能会导致某个接入层交换机被选为了生成树的根，这样大量的负载就可能会由此接入交换机来承担，而性能更高的核心交换机就不能充分体现其价值。因此，通常的做法是，手工将各 vlan 生成树的根指定为性能更高的核心设备。

```
Sw_6509_core1 (config)# spanning-tree vlan 2 root primary
Sw_6509_core1 (config)# spanning-tree vlan 11 root primary
Sw_6509_core1 (config)# spanning-tree vlan 12 root primary
Sw_6509_core1 (config)# spanning-tree vlan 13 root secondary
Sw_6509_core1 (config)# spanning-tree vlan 14 root secondary
Sw_6509_core1 (config)# spanning-tree vlan 15 root secondary

Sw_6509_core2 (config)# spanning-tree vlan 13 root primary
Sw_6509_core2 (config)# spanning-tree vlan 14 root primary
Sw_6509_core2 (config)# spanning-tree vlan 15 root primary
Sw_6509_core2 (config)# spanning-tree vlan 2 root secondary
Sw_6509_core2 (config)# spanning-tree vlan 11 root secondary
Sw_6509_core2 (config)# spanning-tree vlan 12 root secondary
```

经过以上的配置后，Vlan2、11、12 的生成树的首根就被设为了 Sw_6509_core1，次根被设为了 Sw_6509_core2，而 Vlan13、14、15 的生成树的首根则设为了 Sw_6509_core2，次根被设为了 Sw_6509_core1。

⑦ 将交根机端口划入 VLAN

这里，假设要将 Sw_2950_fl1_1、Sw_2950_fl3_1、Sw_2950_fl5_1、Sw_2950_fl7_1、Sw_2950_fl9_1 接入交根机的端口 fa0/1 划入 finance VLAN (财务部)，端口 fa0/2 划入 techniqy VLAN (技术部)，端口 fa0/3 划入 sales VLAN (销售部)；将 Sw_2950_server 服务器区接入交根机的 fa0/1~fa0/3 划入 server VLAN (服务器)；将 Sw_2950_edge 边界区接入交根机的

fa0/1~fa0/3 划入 edge VLAN（边界）。

配置如下：

```
Sw_2950_fl1_1 (config)#interface fastEthernet 0/1
Sw_2950_fl1_1 (config-if)#switchport mode access
Sw_2950_fl1_1 (config-if)#switchport access vlan 11
Sw_2950_fl1_1 (config)#interface fastEthernet 0/2
Sw_2950_fl1_1 (config-if)#switchport mode access
Sw_2950_fl1_1 (config-if)#switchport access vlan 12
Sw_2950_fl1_1 (config)#interface fastEthernet 0/3
Sw_2950_fl1_1 (config-if)#switchport mode access
Sw_2950_fl1_1 (config-if)#switchport access vlan 13

Sw_2950_fl3_1 (config)#interface fastEthernet 0/1
Sw_2950_fl3_1 (config-if)#switchport mode access
Sw_2950_fl3_1 (config-if)#switchport access vlan 11
Sw_2950_fl3_1 (config)#interface fastEthernet 0/2
Sw_2950_fl3_1 (config-if)#switchport mode access
Sw_2950_fl3_1 (config-if)#switchport access vlan 12
Sw_2950_fl3_1 (config)#interface fastEthernet 0/3
Sw_2950_fl3_1 (config-if)#switchport mode access
Sw_2950_fl3_1 (config-if)#switchport access vlan 13

Sw_2950_fl5_1 (config)#interface fastEthernet 0/1
Sw_2950_fl5_1 (config-if)#switchport mode access
Sw_2950_fl5_1 (config-if)#switchport access vlan 11
Sw_2950_fl5_1 (config)#interface fastEthernet 0/2
Sw_2950_fl5_1 (config-if)#switchport mode access
Sw_2950_fl5_1 (config-if)#switchport access vlan 12
Sw_2950_fl5_1 (config)#interface fastEthernet 0/3
Sw_2950_fl5_1 (config-if)#switchport mode access
Sw_2950_fl5_1 (config-if)#switchport access vlan 13

Sw_2950_fl7_1 (config)#interface fastEthernet 0/1
Sw_2950_fl7_1 (config-if)#switchport mode access
Sw_2950_fl7_1 (config-if)#switchport access vlan 11
Sw_2950_fl7_1 (config)#interface fastEthernet 0/2
Sw_2950_fl7_1 (config-if)#switchport mode access
Sw_2950_fl7_1 (config-if)#switchport access vlan 12
Sw_2950_fl7_1 (config)#interface fastEthernet 0/3
Sw_2950_fl7_1 (config-if)#switchport mode access
Sw_2950_fl7_1 (config-if)#switchport access vlan 13
```



```

Sw_2950_fl9_1 (config)#interface fastEthernet 0/1
Sw_2950_fl9_1 (config-if)#switchport mode access
Sw_2950_fl9_1 (config-if)#switchport access vlan 11
Sw_2950_fl9_1 (config)#interface fastEthernet 0/2
Sw_2950_fl9_1 (config-if)#switchport mode access
Sw_2950_fl9_1 (config-if)#switchport access vlan 12
Sw_2950_fl9_1 (config)#interface fastEthernet 0/3
Sw_2950_fl9_1 (config-if)#switchport mode access
Sw_2950_fl9_1 (config-if)#switchport access vlan 13

Sw_2950_server (config)#interface range fastEthernet 0/1 - 3
Sw_2950_server (config-if-range)#switchport mode access
Sw_2950_server (config-if-range)#switchport access vlan 14

Sw_2950_edge (config)#interface range fastEthernet 0/1 - 3
Sw_2950_edge (config-if-range)#switchport mode access
Sw_2950_edge (config-if-range)#switchport access vlan 15

```

⑧ 配置三层交换

到目前为止，VLAN 的划分已经结束。但是，此时只有本 VLAN 的主机之间可以互相访问，不同 VLAN 的主机之间还不能互访。为了让不同 VLAN 之间可以互访，需要为不同的 VLAN 之间架起一座桥梁，这时就要在三层核心设备上给各 VLAN 接口分配网络（IP）地址了。由于两台核心设备互为备份，也就是都可能会成为各 VLAN 之间互访的桥梁，因此需要在两台核心交换机上分别为所有的 VLAN 各配置一个接口地址，这个地址也就是各 VLAN 主机的网关地址。这里给出 VLAN 和 IP 的分配表，见表 7-5 和表 7-6。

表 7-5 核心交换机 1 (Sw_6509_core1)

部 门	VLAN 名	VLAN ID	网关地址	网段地址
管理	manage	2	192.168.2.252	192.168.10.0/24
财务部	finance	11	192.168.11.252	192.168.11.0/24
技术部	techniqy	12	192.168.12.252	192.168.12.0/24
销售部	sales	13	192.168.13.252	192.168.13.0/24
服务器	server	14	192.168.14.252	192.168.14.0/24
边界	edge	15	192.168.15.252	192.168.15.0/24

表 7-6 核心交换机 2 (Sw_6509_core2)

部 门	VLAN 名	VLAN ID	网关地址	网段地址
管理	manage	2	192.168.2.253	192.168.10.0/24
财务部	finance	11	192.168.11.253	192.168.11.0/24
技术部	techniqy	12	192.168.12.253	192.168.12.0/24
销售部	sales	13	192.168.13.253	192.168.13.0/24
服务器	server	14	192.168.14.253	192.168.14.0/24
边界	edge	15	192.168.15.253	192.168.15.0/24


```
Sw_6509_core1 (config)#interface vlan 2
Sw_6509_core1 (config-if)#ip address 192.168.2.252 255.255.255.0
Sw_6509_core1 (config)#interface vlan 11
Sw_6509_core1 (config-if)#ip address 192.168.11.252 255.255.255.0
Sw_6509_core1 (config)#interface vlan 12
Sw_6509_core1 (config-if)#ip address 192.168.12.252 255.255.255.0
Sw_6509_core1 (config)#interface vlan 13
Sw_6509_core1 (config-if)#ip address 192.168.13.252 255.255.255.0
Sw_6509_core1 (config)#interface vlan 14
Sw_6509_core1 (config-if)#ip address 192.168.14.252 255.255.255.0
Sw_6509_core1 (config)#interface vlan 15
Sw_6509_core1 (config-if)#ip address 192.168.15.252 255.255.255.0

Sw_6509_core2 (config)#interface vlan 2
Sw_6509_core2 (config-if)#ip address 192.168.2.253 255.255.255.0
Sw_6509_core2 (config)#interface vlan 11
Sw_6509_core2 (config-if)#ip address 192.168.11.253 255.255.255.0
Sw_6509_core2 (config)#interface vlan 12
Sw_6509_core2 (config-if)#ip address 192.168.12.253 255.255.255.0
Sw_6509_core2 (config)#interface vlan 13
Sw_6509_core2 (config-if)#ip address 192.168.13.253 255.255.255.0
Sw_6509_core2 (config)#interface vlan 14
Sw_6509_core2 (config-if)#ip address 192.168.14.253 255.255.255.0
Sw_6509_core2 (config)#interface vlan 15
Sw_6509_core2 (config-if)#ip address 192.168.15.253 255.255.255.0
```

再在各接入 VLAN 的计算机上设置与所属 VLAN 的网络地址一致的 IP 地址，并且把默认网关设置为该 VLAN 的接口地址。这样，所有的 VLAN 也可以互访了。

现在还有一个问题：两台核心交换机上都配有 VLAN 的接口 IP 地址，那么 VLAN 中的主机到底应该将网关设为哪个 IP 地址呢？

根据前面的配置可知，Sw_6509_core1 是 VLAN2、11、12 生成树的首根，因此属于这三个 VLAN 的主机，应选 Sw_6509_core1 上配的地址为自己的网关；相反，属于 VLAN13、14、15 的主机应选 Sw_6509_core2 上配的地址为自己的网关。这样配置存在一定的问题，虽然正常情况下可以工作，但 VLAN 中的主机在核心发生故障时无法实现切换。比如，如果 Sw_6509_core1 发生了故障，这时 Sw_6509_core2 接替了 Sw_6509_core1 的位置，但 VLAN2、11、12 中的主机网关仍然指向 Sw_6509_core1，因此无法和其他 VLAN 正常通信。这时为了正常通信，用户须将网关改为 Sw_6509_core2 上配的 IP 地址。因为这样的改动影响面太大，所以这里就引出了下面所要介绍的一个内容——HSRP，通过 HSRP 的配置后，客户机就不用来回改动自己的网关了。

⑨ 配置 HSRP

通俗地讲，HSRP 就是将两台配置为热备份的三层设备（路由器、带三层功能的交换机、防火墙等）虚拟成一台设备，这样使得在设备进行切换的时候网络的整体结构和配置保持稳定。

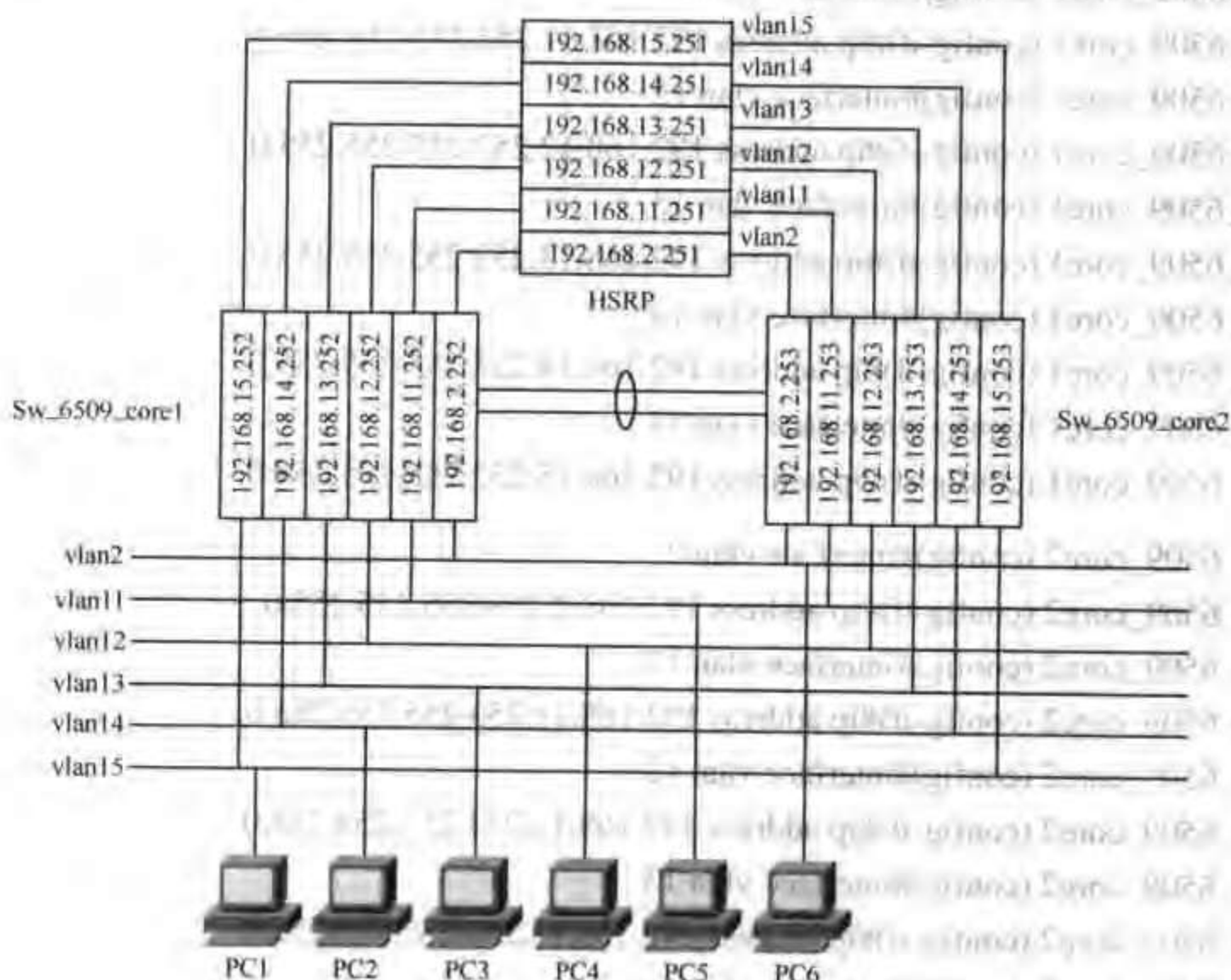


图 7-36 各 VLAN 的虚拟地址

在本案例中，我们为各 VLAN 分配的虚拟地址如图 7-36 所示。其中，vlan2 为 192.168.2.251，vlan11 为 192.168.11.251，vlan12 为 192.168.12.251，vlan13 为 192.168.13.251，vlan14 为 192.168.14.251，vlan15 为 192.168.15.251。具体配置如下：

```
Sw_6509_core1 (config)#interface vlan 2
```

```
Sw_6509_core1 (config-if)#ip address 192.168.2.252 255.255.255.0
```

```
Sw_6509_core1 (config-if)#standby 1 ip 192.168.2.251
```

```
Sw_6509_core1 (config-if)#standby 1 priority 150
```

```
Sw_6509_core1 (config)#interface vlan 11
```

```
Sw_6509_core1 (config-if)#ip address 192.168.11.252 255.255.255.0
```

```
Sw_6509_core1 (config-if)#standby 2 ip 192.168.11.251
```

```
Sw_6509_core1 (config-if)#standby 2 priority 150
```

```
Sw_6509_core1 (config)#interface vlan 12
```

```
Sw_6509_core1 (config-if)#ip address 192.168.12.252 255.255.255.0
```

```
Sw_6509_core1 (config-if)#standby 3 ip 192.168.12.251
```

```
Sw_6509_core1 (config-if)#standby 3 priority 150
```



```
Sw_6509_core1 (config)#interface vlan 13
Sw_6509_core1 (config-if)#ip address 192.168.13.252 255.255.255.0
Sw_6509_core1 (config-if)#standby 4 ip 192.168.13.251

Sw_6509_core1 (config)#interface vlan 14
Sw_6509_core1 (config-if)#ip address 192.168.14.252 255.255.255.0
Sw_6509_core1 (config-if)#standby 5 ip 192.168.14.251

Sw_6509_core1 (config)#interface vlan 15
Sw_6509_core1 (config-if)#ip address 192.168.15.252 255.255.255.0
Sw_6509_core1 (config-if)#standby 6 ip 192.168.15.251

Sw_6509_core2 (config)#interface vlan 2
Sw_6509_core2 (config-if)#ip address 192.168.2.253 255.255.255.0
Sw_6509_core2 (config-if)#standby 1 ip 192.168.2.251

Sw_6509_core2 (config)#interface vlan 11
Sw_6509_core2 (config-if)#ip address 192.168.11.253 255.255.255.0
Sw_6509_core2 (config-if)#standby 2 ip 192.168.11.251

Sw_6509_core2 (config)#interface vlan 12
Sw_6509_core2 (config-if)#ip address 192.168.12.253 255.255.255.0
Sw_6509_core2 (config-if)#standby 3 ip 192.168.12.251

Sw_6509_core2 (config)#interface vlan 13
Sw_6509_core2 (config-if)#ip address 192.168.13.253 255.255.255.0
Sw_6509_core2 (config-if)#standby 4 ip 192.168.13.251
Sw_6509_core2 (config-if)#standby 4 priority 150

Sw_6509_core2 (config)#interface vlan 14
Sw_6509_core2 (config-if)#ip address 192.168.14.253 255.255.255.0
Sw_6509_core2 (config-if)#standby 5 ip 192.168.14.251
Sw_6509_core2 (config-if)#standby 5 priority 150

Sw_6509_core2 (config)#interface vlan 15
Sw_6509_core2 (config-if)#ip address 192.168.15.253 255.255.255.0
Sw_6509_core2 (config-if)#standby 6 ip 192.168.15.251
Sw_6509_core2 (config-if)#standby 6 priority 150
```

⑩ 配置路由

为满足用户的需求，分支机构的用户需要访问总部的业务应用系统和 OA 办公自动化系统，总部用户需要接入 Internet。具体配置如下：

```
Sw_6509_core1 (config)#ip route 192.168.20.0 255.255.255.0 192.168.15.4
Sw_6509_core1 (config)#ip route 192.168.30.0 255.255.255.0 192.168.15.4
```



```
Sw_6509_core1 (config)#ip route 0.0.0.0 0.0.0.0 192.168.15.1
```

```
Sw_6509_core2 (config)#ip route 192.168.20.0 255.255.255.0 192.168.15.4
```

```
Sw_6509_core2 (config)#ip route 192.168.30.0 255.255.255.0 192.168.15.4
```

```
Sw_6509_core2 (config)#ip route 0.0.0.0 0.0.0.0 192.168.15.1
```

(2) 广域网部分

① Rt_wan

```
!
```

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
service password-encryption
```

```
no service tcp-small-servers
```

```
no service udp-small-servers
```

```
!
```

```
hostname Rt_wan
```

```
!
```

```
enable password cisco
```

```
!
```

```
no ip name-server
```

```
!
```

```
ip subnet-zero
```

```
no ip domain-lookup
```

```
ip routing
```

```
!
```

```
interface FastEthernet 0/0
```

```
no shutdown
```

```
description connected to zb
```

```
ip address 192.168.15.2 255.255.255.0
```

```
standby 1 ip 192.168.15.4
```

```
standby 1 priority 150
```

```
keepalive 10
```

```
!
```

```
interface FastEthernet 0/1
```

```
no description
```

```
no ip address
```

```
shutdown
```

```
!
```

```
!
```

```
! ---进入 E1 卡配置模式:
```



```
controller E1 1/0
```

```
no shutdown
```

! ---配置 CE1/PRI 接口的帧校验格式, 不进行帧校验为 “no-crc4”, 采用 4 字节 CRC 校验为 “crc4” 具体采用什么格式请咨询线路提供商:

```
framing no-crc4
```

! ---进行时隙的划分, 这里将 1~4 时隙 (256k) 捆绑为 “0” 组, 5~8 时隙 (256k) 捆绑为 “1” 组, “0” 和 “1” 组分别对应下面的虚拟串口 “Serial 1/0:0” 和 “Serial 1/0:1”:

```
channel-group 0 timeslot 1-4
```

```
channel-group 1 timeslot 5-8
```

```
!
```

```
!
```

```
interface Serial 1/0:0
```

```
no shutdown
```

```
description connected to Rt_fz1
```

```
encapsulation ppp
```

```
ip address 192.168.1.1 255.255.255.252
```

```
!
```

```
interface Serial 1/0:1
```

```
no shutdown
```

```
description connected to Rt_fz2
```

```
encapsulation ppp
```

```
ip address 192.168.1.5 255.255.255.252
```

```
!
```

```
ip classless
```

```
!
```

```
!
```

```
ip route 192.168.20.0 255.255.255.0 Serial 1/0:0
```

```
ip route 192.168.30.0 255.255.255.0 Serial 1/0:1
```

```
ip route 192.168.2.0 255.255.255.0 192.168.15.251
```

```
ip route 192.168.11.0 255.255.255.0 192.168.15.251
```

```
ip route 192.168.12.0 255.255.255.0 192.168.15.251
```

```
ip route 192.168.13.0 255.255.255.0 192.168.15.251
```

```
ip route 192.168.14.0 255.255.255.0 192.168.15.251
```

```
!
```

```
no ip http server
```

```
snmp-server community public RO
```

```
no snmp-server location
```

```
no snmp-server contact
```

```
!
```



```

line console 0
  exec-timeout 0 0
  password cisco
  login
  !
line vty 0 4
  password cisco
  login
  !
end
② Rt_remote
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Rt_remote
!
enable password cisco
username Rt_fz1 password cisco
username Rt_fz2 password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0/0
  no shutdown
  description connected to zb
  ip address 192.168.15.3 255.255.255.0
  standby 1 ip 192.168.15.4
  keepalive 10
!
interface FastEthernet 0/1
  no description

```



```
no ip address
```

```
shutdown
```

```
!
```

```
controller E1 1/0
```

```
no shutdown
```

```
framing no-crc4
```

! ---指定 ISDN PRI 的线路编码格式为“hdb3”，具体格式请咨询线路提供商：

```
linecode hdb3
```

! ---把 PRI 接口划分为 31 个信道，其中第 16 个信道（对应逻辑接口 Serial0/0:15）是管理信道：

```
pri-group timeslots 1-31
```

```
!
```

! ---进入逻辑接口 Serial0/0:15（管理信道）：

```
interface Serial1/0:15
```

```
no shutdown
```

```
description dialin interface
```

```
ip unnumbered FastEthernet0/0
```

```
encapsulation ppp
```

! ---指定本接口属于拨号组 1，注意组号和下面定义的“dialer-list 1”对应：

```
dialer-group 1
```

```
isdn switch-type primary-net5
```

! ---将模拟 Modem 呼叫转接到内部数字 Modem 来处理：

```
isdn incoming-voice modem
```

! ---为拨入的 ISDN 呼叫从地址池“isdnpool”中分配 IP 地址：

```
peer default ip address pool isdnpool
```

! ---指定 PPP 的认证方式，这里采用“pap”方式：

```
ppp authentication pap
```

```
!
```

! ---建立一个异步拨号组，用于接收模拟 Modem 呼叫：

```
interface Group-Async1
```

```
ip unnumbered FastEthernet0/0
```

```
encapsulation ppp
```

! ---为异步串口指定建立链路的方式，默认值是“dedicate”。可以有两种建立链路的方式：①直接方式（Dedicate）：拨号成功之后，直接采用链路层协议配置参数建立链路；②交互方式（Interactive）：拨号成功之后，主叫方向对端发送配置命令（与用户从远端手工键入配置命令效果相同），设置对端的链路层协议工作参数，然后建立链路。比较常用的是直接方式，但在与同样支持交互方式的路由器（如 Cisco 路由器等）互连时，采用交互方式显得更为灵活。

```
async mode interactive
```


! ---为拨入的模拟呼叫从地址池“pstnpool”中分配 IP 地址:

```
peer default ip address pool pstnpool
```

! ---指定 PPP 的认证方式, 这里采用“pap”方式:

```
ppp authentication pap if-needed
```

! ---指定此模拟拨号组对应的端口:

```
group-range 33 62
```

```
!  
ip classless
```

```
!  
!  
!
```

! ---为拨号组 1 指定激活拨号的条件, 这里所有的 IP 访问都可以激活拨号:

```
no dialer-list 1
```

```
dialer-list 1 protocol ip permit
```

```
!  
!  
! ---为数字和模拟拨入用户定义地址池:
```

```
ip local pool isdnpool 192.168.15.201 192.168.15.220
```

```
ip local pool pstnpool 192.168.15.221 192.168.15.240
```

```
!  
ip route 192.168.2.0 255.255.255.0 192.168.15.251
```

```
ip route 192.168.11.0 255.255.255.0 192.168.15.251
```

```
ip route 192.168.12.0 255.255.255.0 192.168.15.251
```

```
ip route 192.168.13.0 255.255.255.0 192.168.15.251
```

```
ip route 192.168.14.0 255.255.255.0 192.168.15.251
```

```
!  
no ip http server
```

```
snmp-server community public RO
```

```
no snmp-server location
```

```
no snmp-server contact
```

```
!  
line console 0
```

```
exec-timeout 0 0
```

```
password cisco
```

```
login
```

```
!  
!
```

```
line vty 0 4
```

```
password cisco
```

```
login
```

```
!  
!
```

! ---进入 Modem 口线模式:

line 33 62

! ---配置为自动登录:

autoselect during-login

! ---配置为自动选择 PPP 协议:

autoselect ppp

! ---配置为使用本地数据库进行认证:

login local

! ---配置端口为允许拨入和拨出:

modem InOut

! ---自动识别 modem:

modem autoconfigure discovery

! ---连通后自动执行 ppp 命令:

autocommand ppp default

!

end

③ Rt_fz1

!

service timestamps debug uptime

service timestamps log uptime

service password-encryption

no service tcp-small-servers

no service udp-small-servers

!

hostname Rt_fz1

!

enable password cisco

username Rt_remote password cisco

!

! ---定义拨号脚本 "dialout":

chat-script dialout "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30 CONNECT \c

!

no ip name-server

!

ip subnet-zero

no ip domain-lookup

ip routing

!

interface FastEthernet 0/0


```

no shutdown
description connected to fz1_LAN
ip address 192.168.20.254 255.255.255.0
keepalive 10
!
interface Serial 0/0
no shutdown
description connected to Rt_wan S1/0:0
encapsulation ppp
ip address 192.168.1.2 255.255.255.252
!
! ---进入异步接口配置模式:
interface async 1
description connected to Rt_remote
! ---自动协商来从远端获得地址:
ip address negotiated
encapsulation ppp
async mode interactive
! ---设定接口为按需拨号 (DDR):
dialer in-band
! ---指定拨号串, "68001000" 为拨入远端所需的电话号码:
dialer string 68001000
dialer-group 1
ppp authentication pap
! ---向远端发送认证需要的用户名和密码:
ppp pap sent-username Rt_fz1 password cisco
!
!
no dialer-list 1
dialer-list 1 protocol ip permit
!
!
ip classless
!
ip route 0.0.0.0 0.0.0.0 Serial 0/0 1
ip route 0.0.0.0 0.0.0.0 async 1 200
!
no ip http server
snmp-server community public RO

```



```

no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
line 1
  autoselect during-login
  autoselect ppp
  modem InOut
  modem autoconfigure discovery
  autocommand ppp
! --指定拨出所用的脚本“dialout”:
  script dialer dialout
  transport input all
  flowcontrol hardware
!
end

```

④ Rt_fz2

```

!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Rt_fz2
!
enable password cisco
username Rt_remote password cisco
!
! --定义拨号脚本“dialout”:

```



```

chat-script dialout "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30 CONNECT &
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface FastEthernet 0/0
no shutdown
description connected to fz2_LAN
ip address 192.168.30.254 255.255.255.0
keepalive 10
!
interface Serial 0/0
no shutdown
description connected to Rt_wan S1/0:1
encapsulation ppp
ip address 192.168.1.6 255.255.255.252
!
! ---进入异步接口配置模式:
interface async 1
description connected to Rt_remote
! ---自动协商来从远端获得地址:
ip address negotiated
encapsulation ppp
async mode interactive
! ---设定接口为按需拨号 (DDR):
dialer in-band
! ---指定拨号串, "68001000" 为拨入远端所需的电话号码:
dialer string 68001000
dialer-group 1
ppp authentication pap
! ---向远端发送认证需要的用户名和密码:
ppp pap sent-username Rt_fz2 password cisco
!
!
no dialer-list 1
dialer-list 1 protocol ip permit

```



```

!
!
ip classless
!
ip route 0.0.0.0 0.0.0.0 Serial 0/0 1
ip route 0.0.0.0 0.0.0.0 async1 200
!
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
line 1
  autoselect during-login
  autoselect ppp
  modem InOut
  modem autoconfigure discovery
  autocommand ppp
! ---指定拨出所用的脚本“dialout”:
  script dialer dialout
  transport input all
  flowcontrol hardware
!
end

```

(3) Internet 接入部分

① PIX_515

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
! ---定义 dmz 接口:

```



```
nameif ethernet2 dmz security50
enable password cisco
passwd cisco
hostname PIX_515
! ---启用内外和 dmz 接口:
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
! ---设置内外接口的地址:
ip address outside 202.106.11.225 255.255.255.240
ip address inside 192.168.15.1 255.255.255.0
ip address dmz 192.168.16.5 255.255.255.0
! ---设置全局复用地址池:
global (outside) 1 202.106.11.229-202.106.11.233
! ---单个 PAT 地址:
global (outside) 1 202.106.11.234
! ---将 dmz 区的服务器影射到外网, 使外网用户可通过公网地址对其进行访问:
static (dmz,outside) 202.106.11.235 192.168.16.1 netmask 255.255.255.255
static (dmz,outside) 202.106.11.236 192.168.16.2 netmask 255.255.255.255
static (dmz,outside) 202.106.11.237 192.168.16.3 netmask 255.255.255.255
! ---内网用户访问 dmz 区不做地址转换:
static (inside,dmz) 192.168.2.0 192.168.2.0 netmask 255.255.255.0
static (inside,dmz) 192.168.11.0 192.168.11.0 netmask 255.255.255.0
static (inside,dmz) 192.168.12.0 192.168.12.0 netmask 255.255.255.0
static (inside,dmz) 192.168.13.0 192.168.13.0 netmask 255.255.255.0
static (inside,dmz) 192.168.14.0 192.168.14.0 netmask 255.255.255.0
static (inside,dmz) 192.168.15.0 192.168.15.0 netmask 255.255.255.0
! ---所有内部地址访问外网进行地址转换:
nat (inside) 1 0 0
! ---允许外部任何地址对 dmz 区的服务器进行相应的访问:
access-list allowin permit tcp any host 202.106.11.235 eq http
access-list allowin permit tcp any host 202.106.11.236 eq smtp
access-list allowin permit tcp any host 202.106.11.237 eq domain
access-list allowin permit udp any host 202.106.11.237 eq domain
! ---将访问列表应用到防火墙的外口上:
access-group allowin in interface outside
! ---设置缺省路由:
route outside 0.0.0.0 0.0.0.0 202.106.11.226
route inside 192.168.0.0 255.255.0.0 192.168.15.251
```


② Rt_internet

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
service password-encryption
```

```
no service tcp-small-servers
```

```
no service udp-small-servers
```

```
!
```

```
hostname Rt_internet
```

```
!
```

```
enable password cisco
```

```
!
```

```
no ip name-server
```

```
!
```

```
ip subnet-zero
```

```
no ip domain-lookup
```

```
ip routing
```

```
!
```

```
interface FastEthernet 0/0
```

```
no shutdown
```

```
description connected to PIX_515
```

```
ip address 202.16.11.226 255.255.255.240
```

```
keepalive 10
```

```
!
```

```
interface FastEthernet 0/1
```

```
no description
```

```
no ip address
```

```
shutdown
```

```
!
```

```
interface Serial 0/0
```

```
no shutdown
```

```
description connected to Internet
```

```
ip address 192.168.1.1 255.255.255.252
```

```
encapsulation ppp
```

```
!
```

```
ip classless
```

```
!
```

```
ip route 0.0.0.0 0.0.0.0 Serial 0/0
```

```
no ip http server
```



```
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
  exec-timeout 0 0
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
end
```

至此，整个企业网络就构建完成了，当然还可以根据用户的具体需求，在此基础上进行安全方面的完善。比如，在 VLAN 接口处设置相应的访问列表以控制相关部门之间的访问，在边界路由器上进行 RFC1918 地址的过滤等。另外，还要对所有的网络设备进行基础安全性的设置使其更健壮，如设置合理的加密口令、关闭不需要的服务、设置日志等。

7.4 大型企业网络构建案例

大型的企业网络主要指那些运营商的网络或是规模极大的国家超大企业和机构的网络，如银行、电力、铁路等的网络。这些网络的典型结构如图 7-37 所示。

在局域网部分，通常会采用双核心星型结构，层次多为三层结构。核心多采用 Cisco 的高端交换机 Catalyst6500 系列交换机，汇聚层多采用 Catalyst4500 系列交换机（或 Catalyst3750 系列交换机），接入层多采用 Catalyst2950 系列交换机。

在广域网部分，通常为多级架构（图 7-37 中只画了一级），如国家级中心至省中心的一级骨干网络，省中心至地市中心的二级骨干网络，地市中心至各县的三级网络。主干线路通常采用 SDH，备份线路可采用 ISDN 和 PSTN。各级骨干路由器根据业务量的不同可采用 Cisco7500、7200、3700、2600、1700 等系列的路由器。

在 Internet 接入部分，对于运营商（ISP、ICP、IDC）来说通常会采用接入两个上级 ISP 的冗余方案，对于自身拥有独立 AS 号的大型运营商，会在边界运行 BGP 协议以对路由进行细致的控制；如果没有独立的 AS 号，可采用策略路由的方式对路由进行控制。

对于大型的企业网络的构建，可以采用和前两案例相同的方式，将整个网络分割为局域网、广域网和 Internet 接入三部分来分别进行配置。由于这样的大型网络相对较少，在这里就不再花费大量的篇幅讲解它的具体配置了，如果读者对这方面感兴趣，可以参考 Cisco 的相关文档。

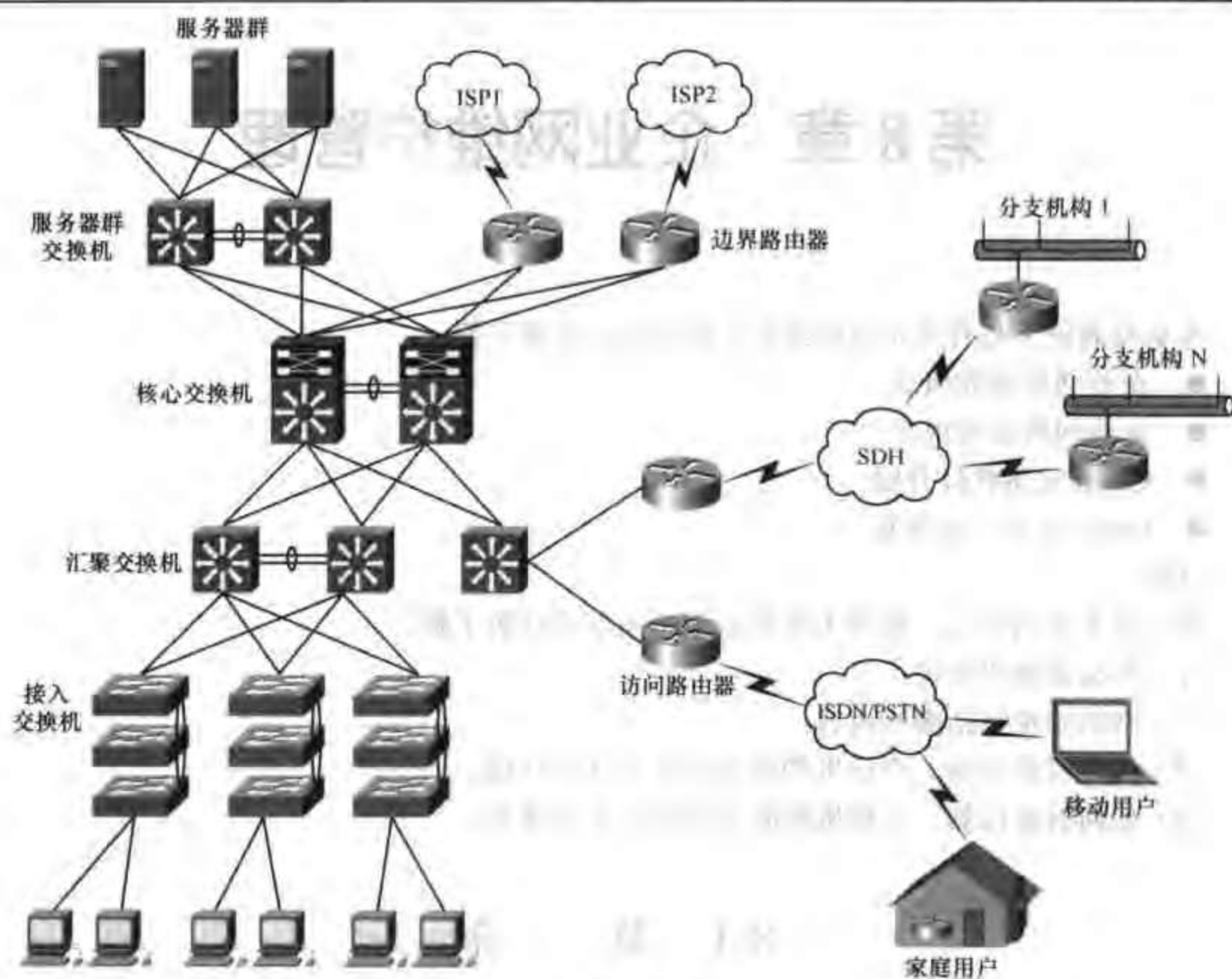


图 7-37 案例 4 拓扑图

7.5 小 结

本章通过几个具体的案例对如何构建一个完整的企业网络作了较为详细的说明。虽然各个企业的网络由于具体需求的不同会有很大的区别，但从总体架构上看是类似的，因此本章通过几个具有代表性的案例对不同规模的网络进行了仿真，相信它会为大家构建自己的网络起到一定的指导作用。

第8章 企业网维护管理

本章将涵盖下列有关企业网维护管理方面的关键主题

- 企业网管理的概念
- 企业网管理的内容
- Cisco 设备软件升级
- Cisco 设备口令恢复

目标:

通过对本章的学习,希望大家对以下一些方面有所了解:

- (1) 什么是网络管理;
- (2) 网络管理包括哪些内容;
- (3) 如何对路由器、交换机和防火墙进行软件升级;
- (4) 如何对路由器、交换机和防火墙进行密码恢复。

8.1 简介

企业网络建成后是不是就可以高枕无忧了呢?答案是否定的。作为企业信息化的基础设施,网络越来越成为企业不可缺少的重要组成部分,因为它不仅承担着资源共享、邮件传递、网络信息发布等基本的网络信息服务,而且现在越来越多的企业将自己的业务系统搬上了网络,比如银行的交易系统、证券的行情交易系统、铁概的售票系统等,这时网络的质量就直接决定了社会生活和经济生活的质量。因此,作为保障网络正常运行的网络管理就成为企业必不可少的一个关键环节。

网络的维护和管理涉及到方方面面,有制度规范上的,也有技术手段上的。但总的来说,网络管理是一种机制,而不是简单的排错过程。下面我们就来介绍有关网络管理的知识。

8.1.1 网络管理的概念

实际上,网络管理并不是一个什么新概念。从广义上讲,任何一个系统都需要管理,只是根据系统的大小、复杂程度的高低,管理在整个系统中的重要性也就有重有轻。网络系统规模的日益扩大和网络应用水平的不断提高,一方面使得网络的维护成为网络管理的重要问题之一,例如排除网络故障更加困难,维护成本上升等;另一方面,如何提高网络性能也成为网络系统应用的主要问题。既然网络管理越来越重要,那么到底什么是网络管理呢?

按照国际标准化组织（ISO）的定义，网络管理是指规划、监督、控制网络资源的使用和在网络上进行的各种活动，以使网络的性能达到最优。网络管理的目的在于提供对计算机网络进行规划、设计、操作运行、管理、监视、分析、控制、评估和扩展的手段，从而合理地组织和利用系统资源，提供安全、可靠、有效和友好的服务。

通俗一点来讲：网络管理就是通过某种方式对网络状态进行调整，使网络能正常、高效地运行。其目的很明确，就是使网络中的各种资源得到更加高效的利用，当网络出现故障能及时作出报告和处理，并协调、保持网络的高效运行等。

8.1.2 网络管理的内容

网络维护管理是一项复杂的工作，做好这项工作的第一步就是要了解网络管理所包含的内容。网络管理工作一般是由以下7个部分组成。

（1）网络文档管理

网络文档管理是指作为企业网络的管理部门必须有一套完整的网络规划方案、网络配置的详细文档、综合布线的详细文档、各种设备的使用说明以及有关这些文档的管理制度。

（2）网络设备管理

网络设备管理是指对各种网络设备进行系统升级和日常的维护。

（3）网络配置管理

网络配置管理是指掌握和控制网络的状态，包括网络内各个设备的状态及其连接关系，端口及路由的配置；收集当前系统状态的有关信息，更改系统的配置等。配置管理的典型方法是用逻辑图来描绘所有的网络设备及其逻辑关系，并将网络的确切物理布局以适当的比例映射到这个逻辑图上。用精心设计的各种图标来表示各种网络对象，而这些图标又往往涂上不同颜色表示相应设备的不同状态。

（4）网络安全管理

网络安全管理包括各种级别、层次的安全防护措施的管理，是对网络资源及其重要信息访问的约束和控制，包括验证网络用户的访问权限和优先级，检测和记录未授权用户企图进行的不应有的操作等。

（5）网络性能管理

网络性能管理是指收集网络运行的各种统计信息，例如设备和链路的负载、可用性及其可靠性、网络的可用率等，优化网络性能，消除网络中的瓶颈，实现网络流量分布的均匀性，实现各种策略管理。性能管理主要考察网络运行的好坏。

（6）网络故障管理

网络故障管理是指维护并检查错误日志，接受错误检测报告并做出反应，跟踪错误检测报告并做出反应，跟踪及辨认错误，执行诊断测试，纠正错误等。故障管理便于检测、定位和排除网络硬件和软件中的故障。

（7）网络账务管理

网络账务管理是指对网络节点的告警事件（告警的产生、告警的内容和告警的清除）的统计，以及各个用户和应用程序对网络资源的使用情况的记录和统计。账务管理提供了一种计算一个特定网络或网段的运行成本的手段。

以上这几部分内容，有的可以通过管理员亲自管理，有的则需要借助软件（网管软件）来实现，同时并不是任何网络都需要所有内容的管理，由哪些管理要根据用户的具体需求和网络的类型来定。

对于一个地点相对集中的小型网络，网络管理的所有内容一般可由网络管理员来承担，但对于有许多分支节点的大型网络来说，采用一套合适的网络管理软件，将会大大地降低网络管理员的劳动强度，同时提高管理的效率，因为目前市场上流行的网络管理软件，大多可以实现网络的集中、可视化管理。本章我们会对 Cisco 公司的网管软件 Ciscoworks2000 进行简要的介绍。

下面几节我们将对网络的文档管理、设备管理进行详细的介绍，安全管理和故障管理由于涉及内容较多，我们将在下两章对它们进行单独讲解，至于配置管理、性能管理和账务管理往往是由通过各种网络管理的软件来实现的，我们在本书中不作讲解，大家如有兴趣可参考相关的书籍。

8.2 文 档 管 理

从制度规范上来说，对于管理企业网络的信息管理部门必须有一套完整的有关企业网络的文档（这包括网络规划方案、网络配置的详细文档、综合布线的详细文档、各种设备的使用说明等）以及有关这些文档的管理制度。

文档整理是网络维护和管理规范化基础，是信息系统风险控制的关键。良好的文档对于设备管理、系统维护、人员培训学习都有很大的帮助，同时编写文档也是对整个系统的进一步认识和理解。文档分为文本文档和电子文档，维护小组应该同时拥有这两种资料。

一般来说，在企业网络建成后，集成商会提供以下一些文档（见表 8-1）：

- 综合布线的详细文档（包括完整布线图、关键设备的网线编号、端口对应表等）；
- 网络规划方案（包括网络拓扑图、使用的网络协议和路由协议、网络地址的分配将）；
- 网络设备参数（包括设备网络地址、MAC 地址、系统版本号、硬件指标等）；
- 网络配置的详细文档（包括网络实际连接图、IP 地址的分配表、所有设备的详细配置等）。

表 8-1 某企业的网络管理文档

序 号	机器名	IP 地址	MAC 地址	备 注
1	Tech1	192.168.1.11	00-10-a4-89-53-58	技术部 1 号机
2	Tech2	192.168.1.12	00-90-f5-e1-10-11	技术部 2 号机
3	Tech3	192.168.1.13	00-0c-11-10-13-60	技术部 3 号机
4	Tech4	192.168.1.14	00-0a-23-58-20-38	技术部 4 号机
5	Tech5	192.168.1.15	00-39-22-45-24-90	技术部 5 号机
.....				

除了以上提到的一些集成商提供的文档外，作为网络管理员还应编写如下一些文档：

- 网络安全控制表（控制列表的制定、系统服务资源的分布、用户网络名和口令、用户拥有的权限等）；
- 机房维护记录（包括设备配置更改记录、用户维护记录、机房工程维护记录、设备测试记录、设备保养记录等）；
- 机房保密制度；
- 网络常规检测和排错方法；
- 网络监控报表和网络应急计划。

上面的介绍已经包括了大多数网络管理所需的文档，但网络管理者可根据自己的经验制定更符合本企业网络状况的相关文档。总之，我们所有的努力都应始终围绕网络管理的目的进行：使网络能正常、高效地运行，当网络出现故障时能及时进行排查和处理。

8.3 设备管理

一般来说网络设备的质量还是很有保证的，但不能排除故障的可能性，故障可能发生在整套设备的背板，或设备的某个模块上，也可能是设备的电源或风扇。特别要说明的是，机房的环境对网络设备的影响很大，如温度、湿度、噪声、接地和灰尘。例如，如果灰尘积累造成设备通风不畅，很容易使设备的电源或风扇损坏，从而造成设备停止运转或设备组件温度升高，设备运转不稳定，加速老化。所以必须定期进行网络设备的除尘工作。再看电源问题，某些 CSU/DSU 设备对电源有一定的要求，如果电压达不到设备的技术参数，可能会对通信的质量造成影响，甚至造成通信中断。当然我们还能通过系统命令和管理软件直接监控设备的运转状态（如在 Cisco 的设备上可通过 `show controller`、`show environment all`、`show log` 等命令组合或使用 CiscoWorks 软件实时观察设备）。

设备的配置是导致软故障的最主要原因。配置涉及到人的因素，对系统功能和网络各种协议的理解会直接影响到设备配置的方法。但对于企业网络来说，一般在集成商调试完成后，用户很少自己进行大规模的改动（往往只是对用户密码进行修改），即便需要改动，用户往往会请集成商来做。因此，维护人员没有必要对网络设备的设置进行改动，日常只需查看一下这些设备的日志即可（如 `syslog` 信息）。

除了上述介绍的一些对网络设备日常的维护项目外，对网络设备进行软件升级和口令恢复也是非常重要的内容。因为假如由于软件损坏影响到网络的运行，而你除了向集成商求助外没有其他的任何办法，这样显然对自己很不利。所以作为网络维护人员有必要掌握一些基本的设备维护的知识。

8.4 Cisco 设备软件升级

在企业网络的日常维护中，对操作系统的维护是非常重要的部分，和其他常见的操作系统（如 Windows、Linux 等）一样，Cisco 网络设备的操作系统也可以进行升级，下面我们分别对路由器、交换机和防火端的软件升级进行相应的介绍。

8.4.1 Cisco 路由器软件升级或恢复

在对 Cisco 路由器安装或升级一个新的操作系统时,可能需要升级路由器的 RAM 或 Flash,或者将两者都升级。每个版本的 IOS 软件对系统都有不同的需求,具体的需求要到 Cisco 的网站查询(详见下面介绍的步骤)。

如果不小心使用了命令 `erase flash`,那么将会发生什么就可想而知了。因此,建议在拿到路由器等网络设备时,最好先将它的 IOS 等操作系统备份出来,以防万一!当然如果确实出于无意或好奇而将 IOS 删掉,或者打算给路由器添加新的功能(如 ADSL、IPSEC VPN 等)而需将现有的 IOS 进行升级,这时就需要下载新的 IOS 软件(需要有 CCO 的帐号),下载的详细过程介绍参见附录。软件下载完成后,我们就可以开始进行软件的升级了。

通常我们会在两种模式下对路由器进行软件的安装或升级,一种是在路由器正常运行模式下主动地进行软件的升级,另外一种是在路由器不能正常启动时被迫进行的软件升级或恢复,下面我们分别进行介绍。

1. 正常模式

路由器在正常使用之中,我们由于某种需要(比如需要支持 VPDN)而必须对路由器进行软件升级,这时我们可在路由器的正常运行模式实施软件的升级。



图 8-1 路由器软件升级连接图

整个升级的流程大致包括 4 个步骤:

- (1) 下载要升级的软件;
- (2) 建立 PC 机和路由器之间的连接(连接方式如图 8-1 所示);
- (3) 通过 tftp 备份 IOS 和配置文件;
- (4) 进行设备升级。

详细步骤如下所述。

步骤 1, 首先下载相应的 IOS 软件。

- (1) 登陆到 Cisco 公司软件下载的网址 www.cisco.com/go/software。

说明:要想下载软件需要有 Cisco 的 CCO 帐号(一般 Cisco 公司的代理商有这样的帐号),如图 8-2 所示。

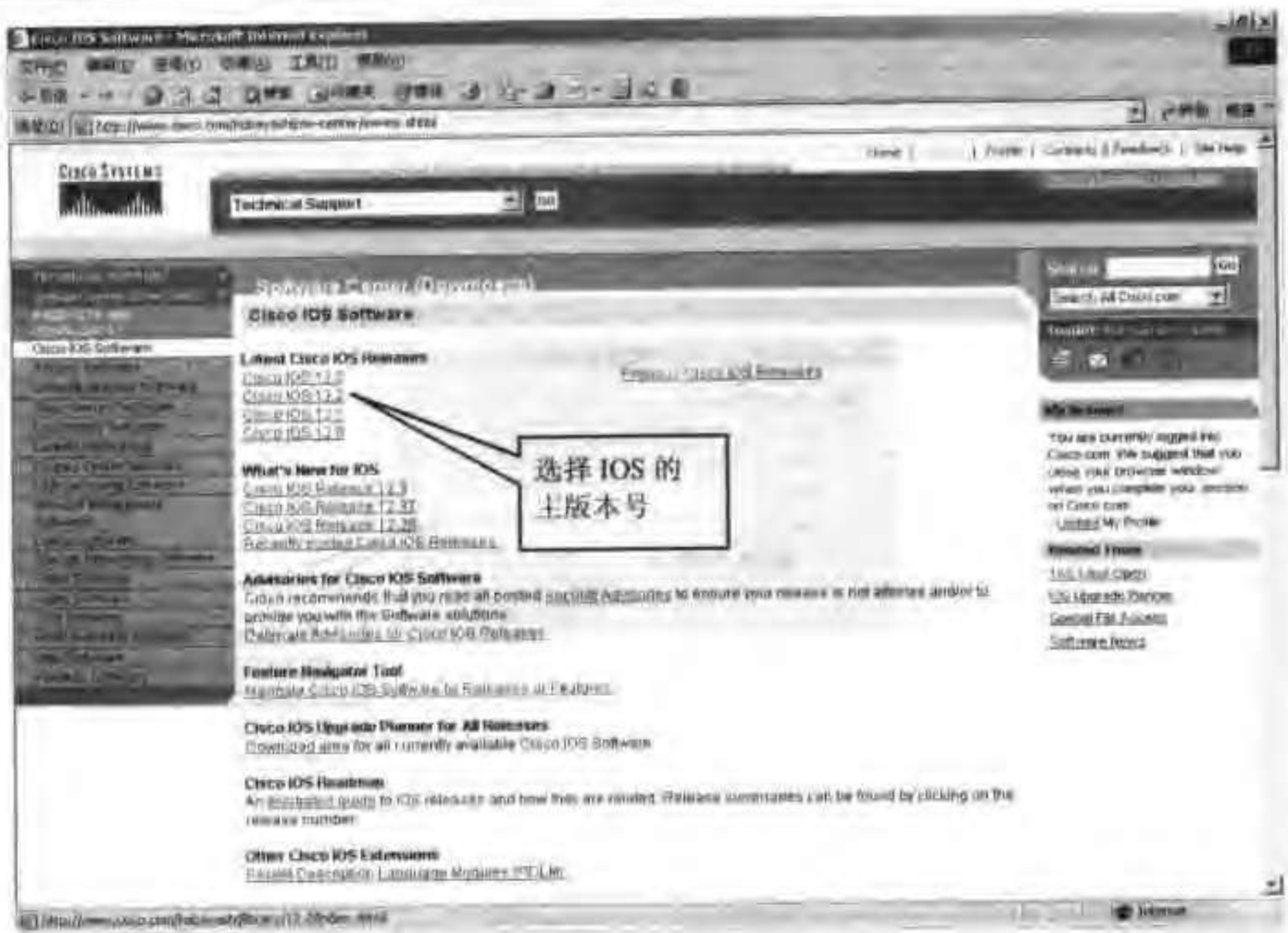


图 8-4 选择 IOS 主版本号

(4) 选择对软件进行下载，如图 8-5 所示。

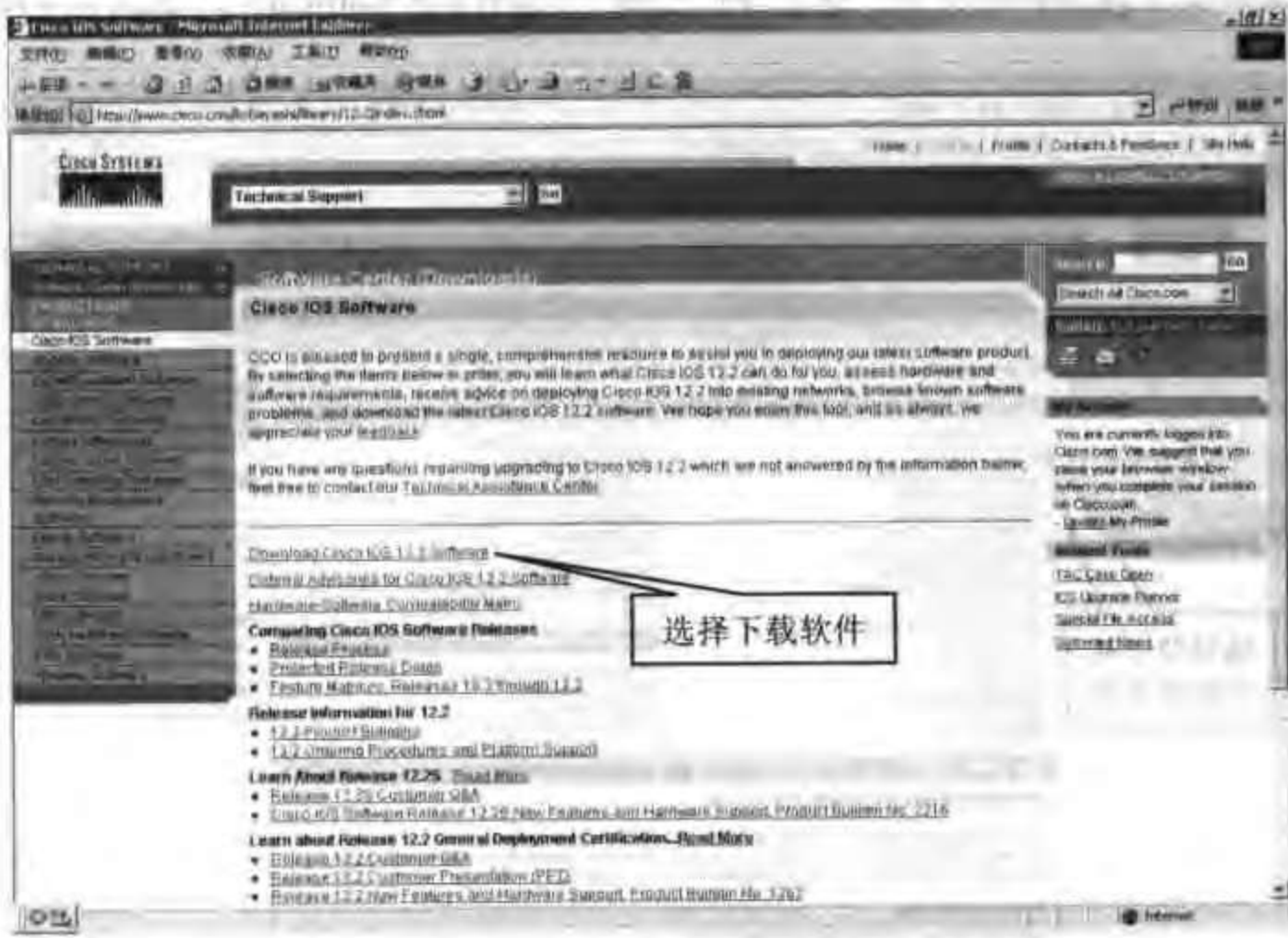


图 8-5 选择下载软件

(5) 选择硬件平台，这里我们选择“2620-2621”，如图 8-6 所示。



图 8-8 选择具体发行版本

(8) 弹出的对话框给出该软件“c2600-is-mz.122-23.bin”所要求的硬件环境，从图 8-9 中我们看出该软件要求路由器最少具有 48M 的内存和 16M 的闪存。



图 8-9 查看要求的硬件环境

(9) 右键点击我们要下载的文件，选择“目标另存为”，在弹出的对话框中选择文件保

存的目录,然后单击保存,如图8-10所示。



图 8-10 保存下载文件

步骤2,软件下载完成后,我们需要用 Console 线将 PC 机的串口(COM)和路由器的 Console 端口连接起来(如图8-1所示),并通过 PC 机上 Windows 操作系统自带的超级终端程序登陆到路由器上进行相应的配置(也可以采用其他的终端仿真程序)。以下是具体的操作步骤。

(1) 单击“开始”——“程序”——“附件”——“通讯”——“超级终端”,如图8-11所示。

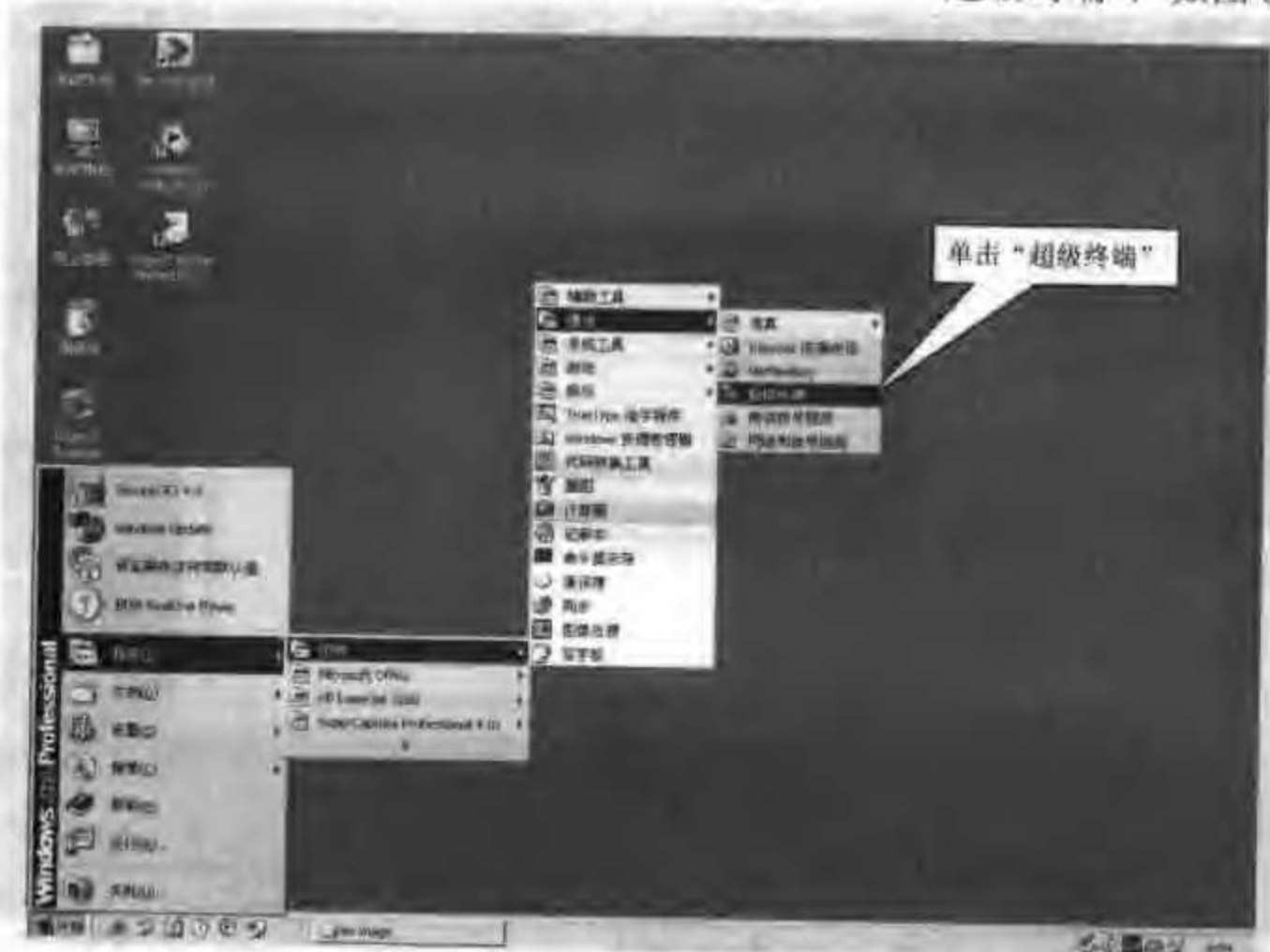


图 8-11 进入“超级终端”

(2) 在弹出的对话框中，为本次连接指定一个名字，这里我们将本次连接命名为“myrouter”，然后单击“确定”按钮，如图 8-12 所示。



图 8-12 指定命名

(3) 在弹出的对话框中的“连接时使用”一栏，选择 Console 线连接使用的 COM 端口，这里我们使用的是 COM1 端口，如图 8-13 所示。



图 8-13 选择 COM 端口

(4) 在接下来的对话框中, 我们进行如下的选择 (如图 8-14 所示):

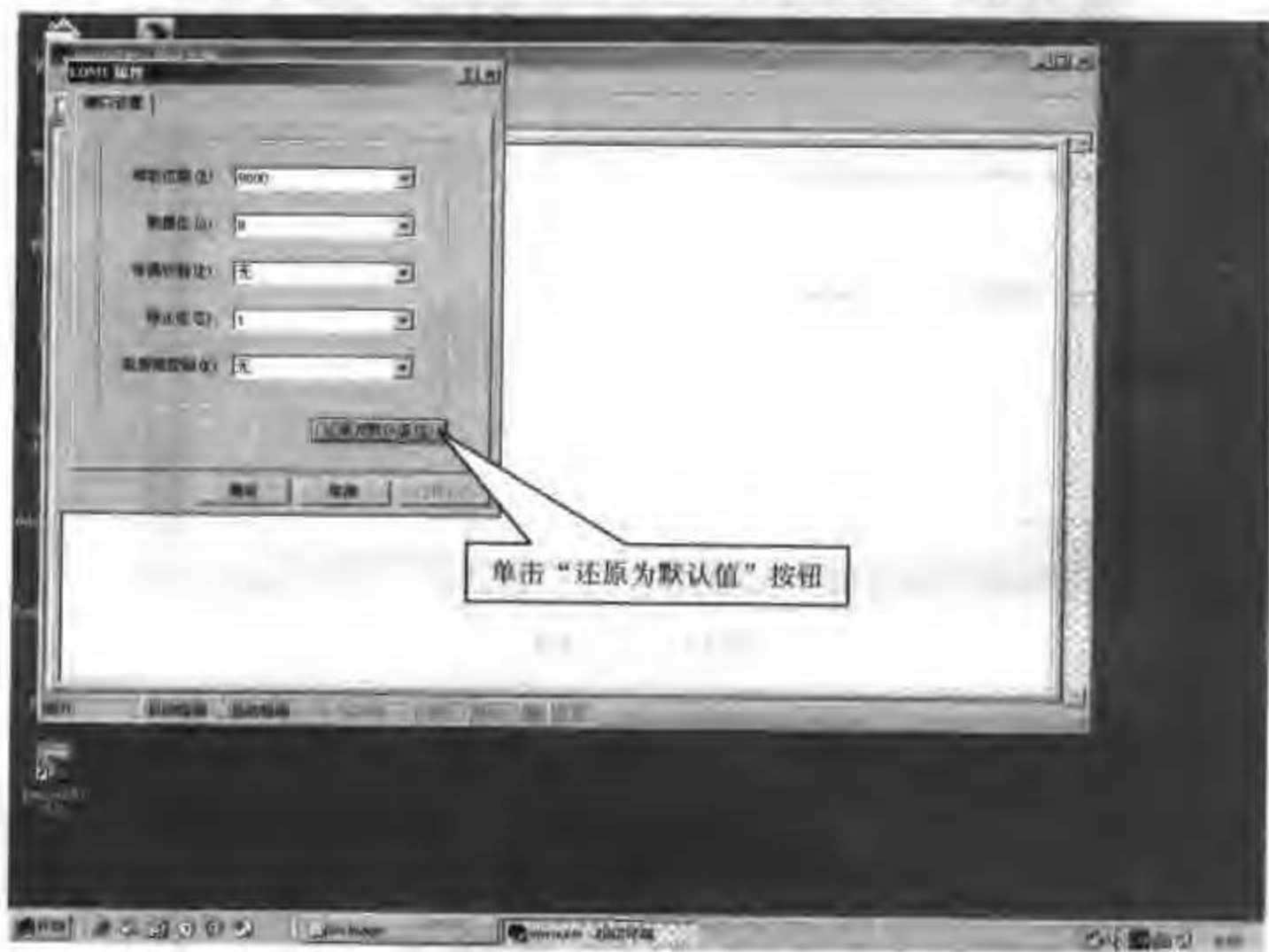


图 8-14 选择参数

每秒位数 (B): 9600

数据位 (D): 8

奇偶校验 (P): 无

停止位 (S): 1

数据流控制 (F): 无

也可以直接点击“还原为默认值”按钮来获取以上的参数值, 然后点击“确定”按钮。

(5) 在接下来弹出的对话框中 (如图 8-15), 直接回车可以看到“Router>”提示符, 这表示我们已经和路由器已经正确地建立了连接。

注意: “Router>”提示符中的“Router”是路由器的用户名, 如果路由器存在配置, 用户名可能会有所不同。另外, 如果路由器是初次配置, 那么会出现“Would you like to enter the initial configuration dialog? [yes/no]:”提示符, 如果选择“yes”我们会进入“setup 对话框”配置模式, 如果选择“no”则会进入“CLI 命令行”配置模式。一般情况下, 我们会进入“CLI 命令行”配置模式对路由器进行配置。

步骤 3, 在我们成功的用超级终端和路由器建立连接后, 下面我们要做的就是通过 tftp 来对原来的 IOS 和配置文件进行备份。首先需要做的就是用交叉线将路由器的以太口 and PC 机的以太口相连, 然后我们需要为路由器的接口和 PC 机分配 IP 地址 (注意: 要分在一个网段), 如图 8-17~8-19 所示。

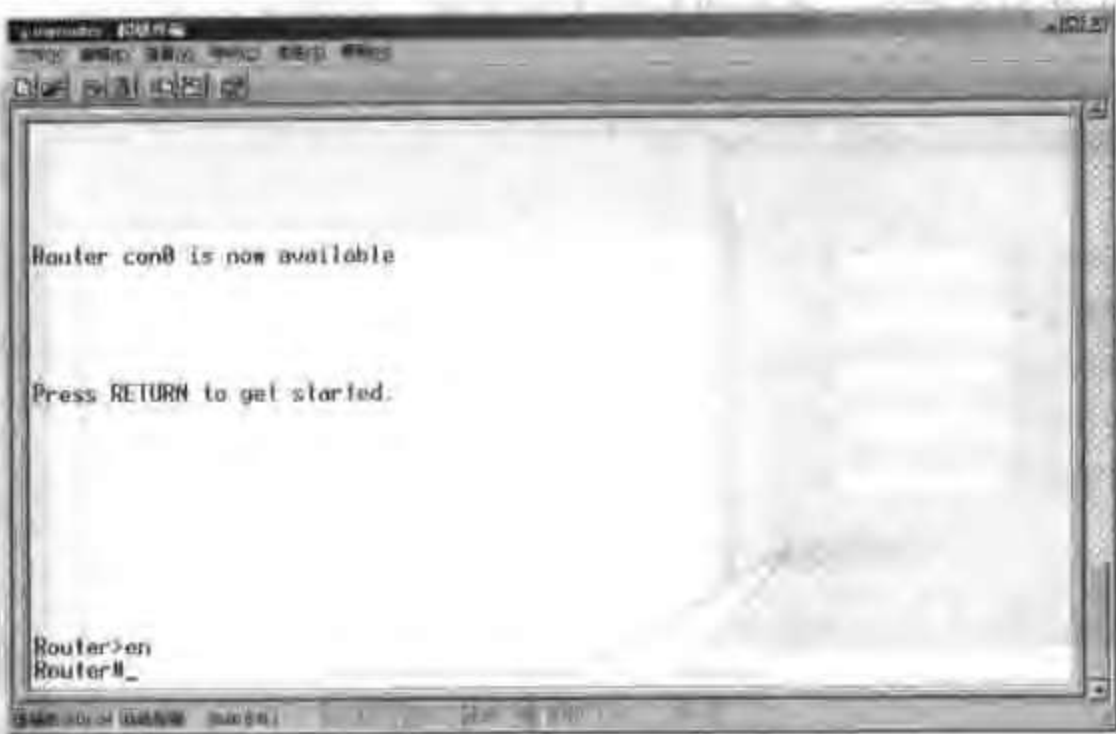


图 8-15 建立连接

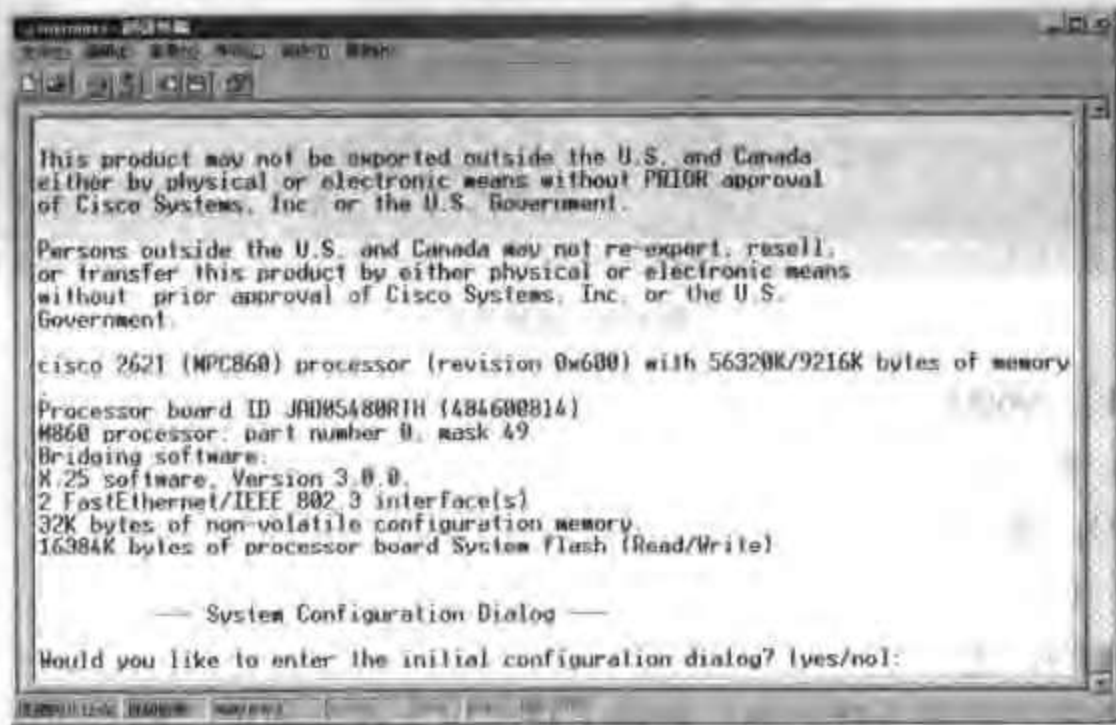


图 8-16 进行路由器配置



图 8-17 分配路由器 IP 地址



图 8-18 分配快速以太网口 IP 地址

步骤 4, 在做完以上工作后, 下面我们需要做的就是开始进行设备的软件升级。

首先, 我们需要在 PC 上打开 TFTP Server 软件, 这里我们所用的软件是 3COM 公司的 3Cdaemon, 具体过程如图 8-20~8-22 所示。



图 8-19 分在同一网段的路由器接口 IP 地址及快速以太网口 IP 地址

做完上述工作后, 下面我们开始软件的升级, 具体步骤如下所述。

(1) 在 Router# 模式下, 输入 “copy tftp flash:” 命令:

Router# copy tftp flash:

(2) 在接下来的 “Address or name of remote host []?” 提示符, 输入安装 tftp server 的 PC 的 IP 地址, 这里是 “192.168.3.121”;

Address or name of remote host []? 192.168.3.121



图 8-20 选择软件路径

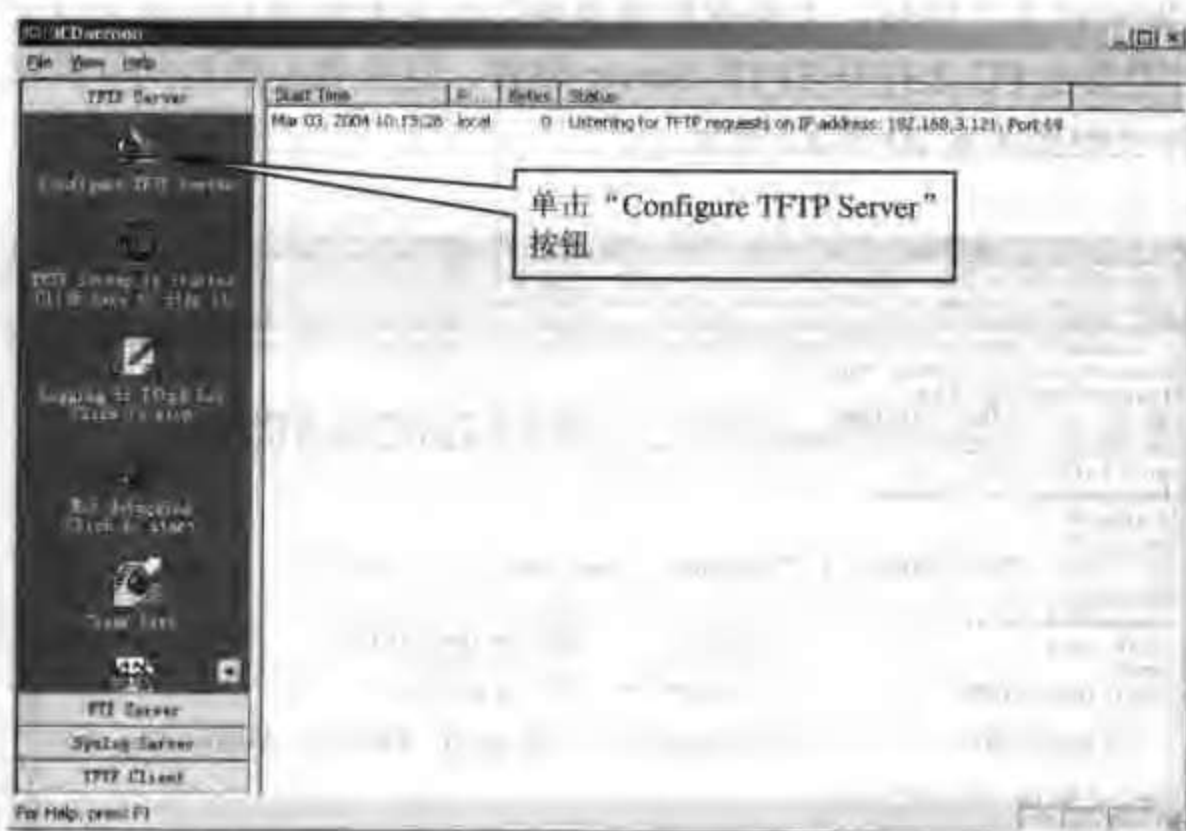


图 8-21 打开 TFTP Server 软件

(3) 在接下来的“Source filename []?”提示符，输入要升级的软件名，这里是“c2600-is-mz.122-23.bin”：

Source filename []? c2600-is-mz.122-23.bin

(4) 在接下来的“Destination filename [c2600-is-mz.122-23.bin]?”提示符，输入要升级的软件名，这里是“c2600-is-mz.122-23.bin”。

(5) 在接下来的“Erase flash: before copying? [confirm]”提示符，如果 flash 的空间足够，我们可以输入“n”即不用删除原来的软件，如果 flash 空间不够，那么我们可以直接回车，从而删除原来的软件，这里选择删除原来的软件，直接回车后，升级过程开始，“eeeeee”表示系统正在删除原来的软件，“!!!!!!”表示系统正在将软件从 tftp server 复制到 flash 中。



图 8-24 信息显示(二)



图 8-25 信息显示 (三)



图 8-26 信息显示(四)

步骤 2, 启动 TFTP 服务器, 并将要下载的版本文件放于指定的目录下。

步骤 3, 开启路由器电源, 由于没有有效的版本, 路由器会直接进入监控模式 (如果路由器内还有损坏的 IOS, 我们需要敲 “ctrl+break” 键进入监控模式)。超级终端的提示为 “rommon1>” 而不是我们平常见到的主机名, 如图 8-27 所示。



图 8-27 进入监控模式

步骤 4, 按如下命令设置参数。

假定计算机 IP 地址为 192.168.1.1, 而路由器的以太网口 IP 地址为 192.168.1.2, 子网掩码均为 255.255.255.0, 在监控模式下将 IP 地址 192.168.1.2 配置到路由器的第一个以太网口, 从而建立起路由器与 TFTP 服务器之间的连接。

```
Rommon1>IP_ADDRESS=192.168.1.2
Rommon2>IP_SUBNET_MASK=255.255.255.0
Rommon3>TFTP_SERVER=192.168.1.1
Rommon4>DEFAULT_GATEWAY=192.168.1.1
Rommon5>TFTP_FILE=c2600-i-mz.122-15.T
Rommon6>tftpdnld
```

通过上述命令, 在路由器监控模式下将 IP 地址 192.168.1.2 配置到路由器的第一个以太网口, 从而建立起路由器与 TFTP 服务器之间的连接, 并将版本文件下载到路由器的闪存 (Flash) 中。

步骤 5, 配置寄存器值, 将操作系统重新写入寄存器。

```
Rommon6>confreg
```

当出现提示: do you wish to change the configuration? y/n 选择 y
其他选 n。

当出现提示: change the boot characterist? y/n 选择 y
选择参数 2。

此时路由器的寄存器中会恢复原来的版本。

步骤 6, 重启路由器。

Rommon7>reset

机器重启后，会恢复正常的状态。

(2) 方法 2，使用 xmodem 命令，通过 Console 口将 IOS 软件灌进路由器。

这种方式的特点是不需要使用网线，只要计算机的串口与路由器的 CONSOLE 口相连就可以。Xmodem 是计算机通信中广泛使用的异步文件传输协议，以 128 字节块的形势传输数据，并且每个块都进行校验，如果接收方校验正确，则发送认可信息，发送方发送下一字块。

步骤 1，将计算机与路由器用 CONSOLE 线连接好后，打开超级终端，启动路由器，进入监控模式状态。

Rommon1>

步骤 2，输入 xmodem 命令。

Rommon1>xmodem -cx ?

会提示如下警告：

WARNING: All existing data in bootflash will be lost!

Invoke this application only for disaster recovery.

Do you wish to continue? y/n [n]: y

此时选择 y

Ready to receive file ? ...

此时路由器的 flash 进入接收数据状态。

步骤 3，打开超级终端程序，点击“传送”菜单的“发送文件”项，选择要传送的版本文件：c2600-i-mz.122-15.T，并选择 xmodem 的传送协议并确认后，经过几秒的校验，文件会以 xmodem 的方式从计算机拷贝到路由器中，根据软件大小传输时间会不同，一般需用时半小时以上（甚至几小时）才能将文件传完。

步骤 4，配置寄存器值，将操作系统重新写入寄存器。

Rommon6>confreg

当出现提示：do you wish to change the configuration ? y/n 选择 y

其他选 n。

当出现提示：change the boot characterist ? y/n 选择 y

选择参数 2。

此时路由器的寄存器中会恢复原来的版本。

步骤 5，重启路由器。

Rommon7>reset

机器重启后，会恢复正常的状态。

小结：

用 TFTP 的方法的优点是下载速度较快，缺点是容易出现校验错误，另外在许多路由器里没有 tftpdnld 命令。而用 xmodem 的方法的缺点是传输速度慢，花费时间较多，但它具有边传送边校验的优点，而且较为稳定，又无须另外使用辅助软件。同时，所有的路由器都支持 xmodem 命令。所以，我们建议在有 tftpdnld 命令的路由器上尽量使用第 1 种方法，在没有 tftpdnld 命令的路由器上只能使用第 2 种方法。

注意:

默认 xmodem 的传输速率是 9600bit/s, 我们可以设置 console 的速率为 115200bit/s, 从而提高 xmodem 的传输速率, 方法如下:

Rommon8>confreg

当出现 “do you wish to change the configuration? y/n [n]:” 时输入 “y” (选择 yes)

当出现 “change console baud rate? y/n [n]:” 时输入 “y” (选择 yes)

当出现 “enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400, 4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]:” 时输入 “7” (选择 7, 选用最大的 115200bit/s 速率的 xmodem 传输)

Rommon9>reset

注意: 在键入 reset 键之前, 开始定义串口速度, 将其速度调为 115200bit/s, 然后再修改超级终端里设置速率为 115200bit/s, 记住, 一定这么做! 否则出现乱码! 然后关闭这个超级终端, 重新建立一个超级终端连接, (期间系统重新启动) 启动后, 可按上述 xmodem 方法进行传输, 此时的速度会快很多。另外, 如果在路由器的配置里, line con 0 下面存在 speed xxx 命令, 需要我们将它去掉, 否则终端速率改不过来。

8.4.2 Cisco 交换机软件升级

在对 Cisco 交换机安装或升级一个新的操作系统时, 可能需要升级交换机的 RAM 或 Flash, 或者将两者都升级。每个版本的 IOS 软件对系统都有不同的需求, 具体的需求需要到 Cisco 的网站查询 (参见上节路由器 IOS 软件下载部分的相关内容)。

如果你不小心使用了命令 erase flash, 那么将会发生什么就可想而知了。因此, 我们建议在你拿到交换机时, 最好先将它的 IOS 操作系统备份出来, 等到网络配置完成后, 将配置文件也备份出来, 以防万一! 如果 IOS 被删除或由于其他原因而损坏, 或者你打算给交换机添加新的功能而需将现有的 IOS 进行升级, 如将 catalyst3550smi 升级到 catalyst3550emi 来支持动态路由 ospf 等, 这时你就需要下载新的 IOS 软件 (你需要有 CCO 的账号), 下载的过程和路由器的 IOS 软件下载过程很相似, 只是在选择下载的软件的类型时选择 “LAN Switching Software”。软件下载完成后, 我们就可以开始进行软件的升级了。

通常我们会在两种模式下对交换机进行软件的安装或升级, 一种是在交换机正常运行模式下主动地进行软件的升级, 另外一种是在交换机不能正常启动时被迫进行软件升级或恢复。下面我们对这两种模式分别进行介绍。

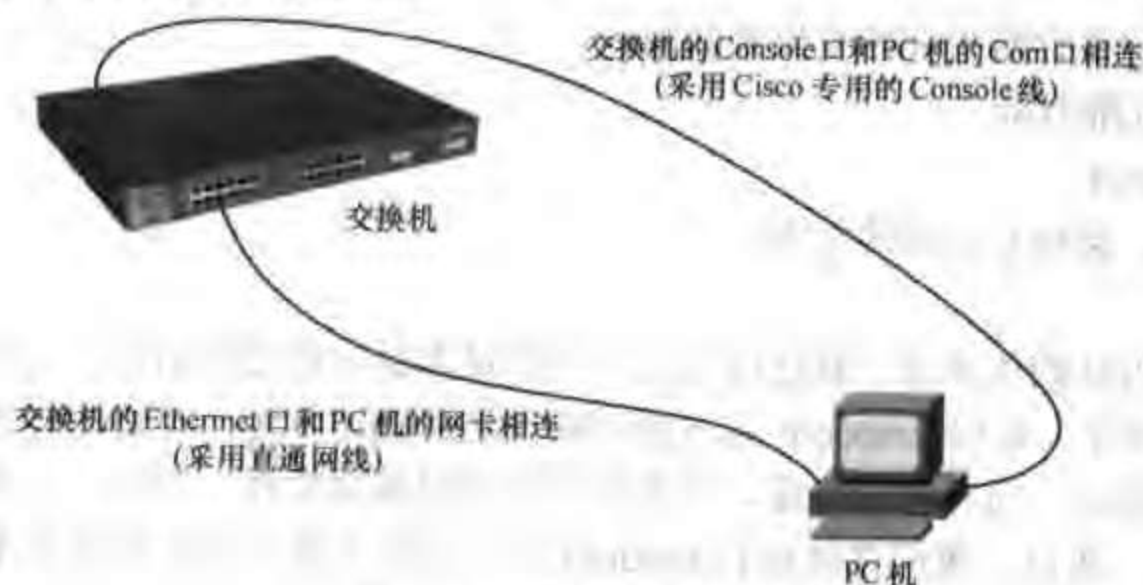


图 8-31 交换机软件升级连接图

1. 正常模式

在交换机正常运行模式下，我们有两种方式来升级交换机，一种是通过下载交换机的“.bin”文件来完成升级，另一种是通过下载“.tar”文件来完成。我们这里分别称这两种方式为“.bin”方式和“.tar”方式。

(1) “.bin”方式

整个升级的流程大致包括4个步骤：

- ① 下载要升级的软件；
- ② 建立PC机和交换机之间的连接（连接方式如图8-31所示）；
- ③ 通过tftp备份软件和配置文件；
- ④ 进行设备升级。

详细步骤如下所述。

步骤1，我们需要下载要升级的交换机的软件，具体方法可参考路由器的IOS软件下载部分，不同之处是在选择下载的软件的类型时选择“LAN Switching Software”。本案例中我们将为Catalyst2950交换机升级软件，下载的软件是“c2950-i6q4l2-mz.121-13.EA1.bin”。

步骤2，软件下载完成后，我们需要用Console线将PC机和交换机的Console端口连接起来（如图8-31所示），并通过PC机上Windows操作系统自带的超级终端程序登陆到交换机上进行相应的配置（也可以采用其他的终端仿真程序）。具体的操作步骤和路由器的类似。

步骤3，在我们成功的用超级终端和交换机建立连接后，下面我们要做的就是通过TFTP来对原来的IOS和配置文件进行备份：首先需要做的就是用直通线将PC的以太网口和交换机上一个属于VLAN1的接口相连，然后我们需要为交换机的管理接口（VLAN1接口）和PC机分配IP地址（注意，要分在一个网段）。

在交换机上进行如下操作：

```
Switch#conf t
Switch(config)#int vlan 1
Switch(config-if)#ip add 192.168.0.121 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#int f0/1
Switchb(config-if)#switch mode access
Switch(config-if)#switch access vlan 1
Switch(config-if)#no shut
```

做完上述配置后，将PC机连到交换机的f0/1端口（或其他任意的属于VLAN1的端口），将PC机的IP地址配置为和交换机为同一地址段，这里我们配置为“192.168.0.120”。我们可以用ping命令来验证交换机和PC机的连通性。

```
C:\>ping 192.168.0.121
```

```
Pinging 192.168.0.121 with 32 bytes of data:
```

```
Reply from 192.168.0.121: bytes=32 time<10ms TTL=128
```

```
Reply from 192.168.0.121: bytes=32 time<10ms TTL=128
```


Reply from 192.168.0.121: bytes=32 time<10ms TTL=128

Reply from 192.168.0.121: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.0.121:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

备份交换机软件我们采用“copy flash tftp”命令，备份配置文件我们采用“copy run tftp”命令。

步骤4，在做完以上工作后，下面我们需要做的就是开始进行设备的软件升级。

首先，我们需要在 PC 上打开 TFTP server 软件，然后我们开始软件的升级，具体步骤如下：

a. 在 Switch# 模式下（注意本案例中我们将交换机的主机名改为了“Cisco2950”，因此相应地也就变为“Cisco2950#”模式），输入“dir flash:”命令（如图 8-32 所示），验证目前是否有足够的空间来存放新的软件，如果空间不足，就需要将原来的软件删除（如图 8-33 所示）。



图 8-32 输入“dir flash:”命令

b. 在 Cisco2950# 模式下，输入“copy tftp flash:”命令：

Cisco2950# copy tftp flash:

c. 在接下来的“Address or name of remote host [?]:”提示符，输入安装 tftp server 的 PC 的 IP 地址，这里是“192.168.0.120”：

Address or name of remote host [?]: 192.168.0.120

d. 在接下来的“Source filename [?]:”提示符，输入要升级的软件名，这里是“c2950-i6q4l2-mz.121-13.EA1.bin”：

Source filename [?]: c2950-i6q4l2-mz.121-13.EA1.bin



图 8-37 保存与重启



图 8-38 验证是否运行新软件

- ② 建立 PC 机和交换机之间的连接;
- ③ 通过 TFTP 备份软件和配置文件;
- ④ 进行设备升级。

详细步骤如下:

步骤 1, 下载升级需要的交换机的软件, 具体方法参考“.bin”方式的步骤 1, 本案例中我们将下载的软件是“c2950-i6q4l2-mz.121-13.EA1.tar”。

步骤 2, 软件下载完成后, 我们需要建立 PC 机和交换机之间的连接, 方法同“.bin”方式。

步骤 3, 在我们成功的建立 PC 机和交换机之间的连接后, 下面我们要做的就是通过 tftp 来对原来的 IOS 和配置文件进行备份, 方法同“.bin”方式。

步骤 4, 在做完以上工作后, 下面我们需要做的就是开始进行设备的软件升级。

首先, 我们需要在 PC 上打开 tftp server 软件, 然后我们开始软件的升级, 具体步骤如下

所述。

a. 在 Switch# 模式下（注意本案例中我们将交换机的主机名改为了“Cisco2950”，因此相应地也就变为“Cisco2950#”模式），输入“dir flash:”命令（如图 8-39 所示），验证目前是否有足够的空间来存放新的软件，如果空间不足，就需要将原来的软件删除（如图 3-40 所示）。



图 8-39 输入“dir flash”命令

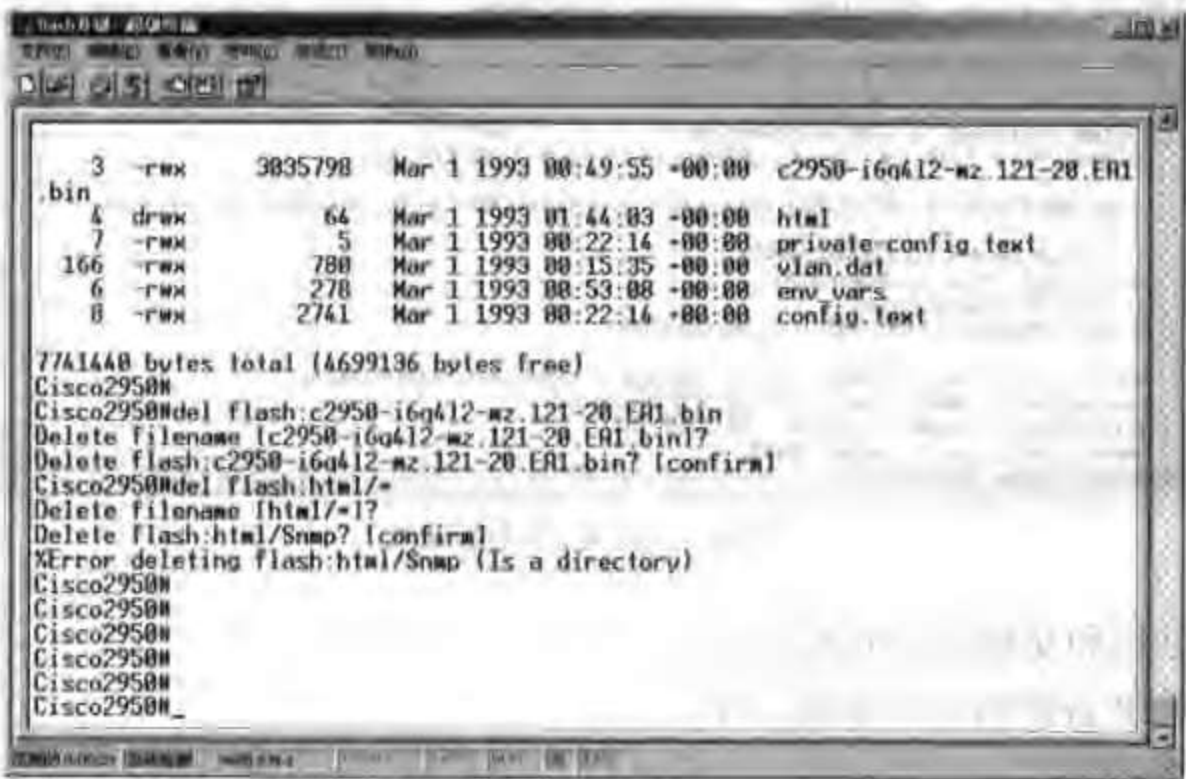


图 8-40 删除原软件

b. 在 Cisco2950# 模式下，输入“archive tar /xtract tftp://<tftp server ip>/<filename> flash:”命令（如图 8-41 所示）：

Cisco2950# archive tar /xtract tftp://192.168.0.120/ c2950-i6q4l2-mz.121-13.EA1.tar flash:

注意：如果你要升级的交换机的软件版本早于“12.1(6)EA2”，请直接用“tar”来代替“archive tar”命令。

输入上述命令后回车，系统便开始升级。

system software:

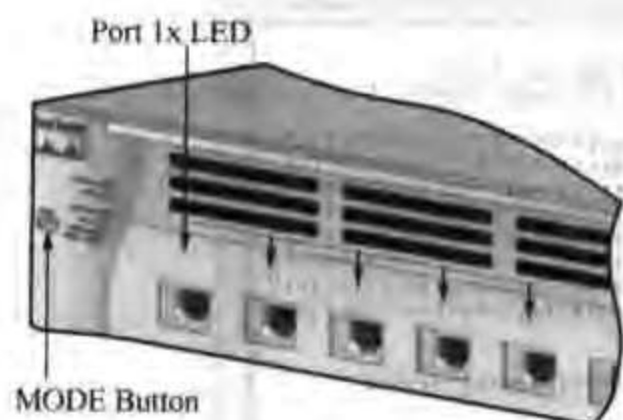


图 8-42 Catalyst3550 LED



图 8-43 Catalyst2950 LED

flash_init

load_helper

boot

步骤 5, 输入 flash_init;

步骤 6, 输入 load_helper;

步骤 7, 输入 dir flash:

这时显示:

switch: dir flash:

Directory of flash:/

2	-rwx	1751538	<date>	c3500XL-c3h2s-mz.120-5.4.WC.1.bin
3	-rwx	94375	<date>	c3500XL-diag-mz-120-5.3.WC.1
4	drwx	10176	<date>	html
5	-rwx	272	<date>	env_vars
6	-rwx	111	<date>	info
167	-rwx	1952	<date>	config.text
166	-rwx	111	<date>	info.ver
168	-rwx	5040	<date>	vlan.dat

472576 bytes available (3140096 bytes used)

通过上面的输出我们看出交换机的 Flash 里还存在软件 c3500XL-c3h2s-mz.120-5.4.WC.1.bin, 交换机不能正常启动有可能是此文件损害或者系统配置的引导参数不对, 我们在这里可以手工输入 “boot flash: c3500XL-c3h2s-mz.120-5.4.WC.1.bin” 命令来尝试从该软件引导, 如果系统能正常启动, 则说明软件是好的, 那么应该是系统配置的引导参数不对, 我们可以修改引导参数从而恢复整个系统; 如果系统不能正常启动, 则说明此软件已损坏, 那么我们就需要重新给此交换机灌入软件。

步骤 8, 如果在 “switch:” 模式下输入 “dir flash:” 命令显示系统中没有软件, 或存在软件但输入 “boot” 命令后系统不能正常启动, 那么我们只能通过 xmodem 的方式来恢复交换机的软件, 操作命令如下:


```
switch: copy xmodem: flash: c3500XL-c3h2s-mz.120-5.4.WC.1.bin
```

在计算机上打开超级终端程序，点击“传送”菜单的“发送文件”项，选择要传送的版本文件：c3500XL-c3h2s-mz.120-5.4.WC.1.bin，并选择 xmodem 的传送协议并确认后，经过几秒的校验，文件会以 xmodem 的方式从计算机拷贝到交换机的 flash 中，根据软件大小传输时间会不同，一般需用时半小时以上（甚至几小时）才能将文件传完。

至此交换机的软件升级和恢复就完成了。

8.4.3 Cisco 防火墙软件升级

PIX OS 5.1 之前的软件版本不能提供将一个软件映像直接通过 TFTP 下载到 Flash 中的方式。因此，如果要升级必须建立一张启动帮助磁盘。而在 PIX OS 5.1 版之后，引入了 copy tftp flash 命令，可用作将一个映像直接拷贝到 PIX 的 Flash 中（这和路由器的方式一样）。由于目前的防火墙多数为运行 5.1 以后的版本，所以我们主要针对 5.1 以后的版本进行介绍，至于以前的版本，请参考 Cisco 的相关文档。

通常我们会在两种模式下对 PIX 进行软件的安装或升级，一种是在 PIX 正常运行模式下主动的进行软件的升级，另外一种是在 PIX 不能正常启动时被迫进行的软件升级或恢复，下面我们分别进行介绍。

1. 正常模式

PIX 在正常使用之中，我们由于某种需要（比如修补某个 bug），而必须对路由器进行软件升级，这时我们可在 PIX 的正常运行模式实施软件的升级。

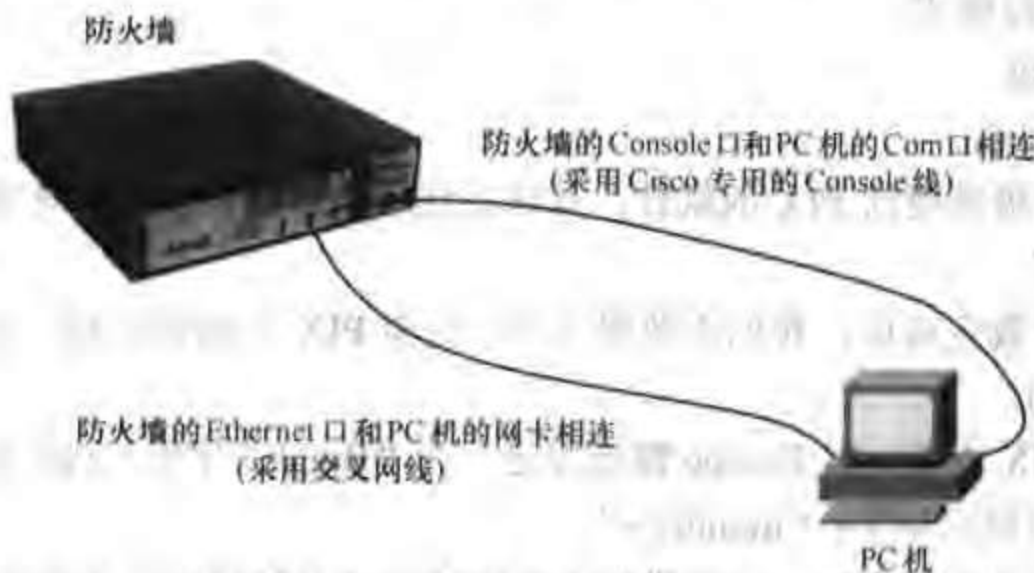


图 8-44 PIX 软件升级连接图

整个升级的流程大致包括 4 个步骤：

- ① 下载要升级的软件；
- ② 建立 PC 机和 PIX 防火墙之间的连接（连接方式见上图）；
- ③ 通过 TFTP 备份原软件和配置文件；
- ④ 进行设备升级。

详细步骤如下：

步骤 1，下载升级需要的 PIX 的软件，具体方法参考路由器 IOS 软件下载部分，不同之处是在下载软件的选择时选择“Cisco Secure Software”选项，然后在“Cisco Secure Software”的下载页面选择“Cisco Secure PIX Firewall Software”，本案例中我们下载的软件是

“pix633.bin”。

步骤 2，软件下载完成后，我们需要建立 PC 机和 PIX 之间的连接，具体方法和路由器及交换机的操作相同。

步骤 3，在我们成功的建立 PC 机和交换机之间的连接后，下面我们要做的就是通过 tftp 来对原来的 PIX OS 和配置文件进行备份，备份软件用“copy flash tftp”命令，备份配置用“write net”命令。

步骤 4，在做完以上工作后，下面我们需要做的就是开始进行设备的软件升级。首先，我们需要在保存“pix633.bin”的 PC 上打开 tftp server 软件，然后在正常运行的 PIX 命令行输入“copy tftp flash”，接下来系统会提示“address or name of remote host[]?”此时输入 PC 的 IP 地址；接着在出现“source file name[]?”提示时输入我们下载的软件“pix633.bin”，回车后出现“!!!!!!”表示复制过程正式开始，等软件安装完后我们可以重新启动 PIX 来验证升级是否成功。

2. 监控模式

如果 PIX 的软件因为意外丢失或损坏了，那么我们就不能正常地启动 PIX，此时我们只能在监控模式（Monitor）下来对 PIX 进行软件的恢复或升级，这和路由器在监控模式恢复其软件有许多相似的地方。

和在正常模式一样，整个恢复的过程大致包括 4 个步骤：

- ① 下载要恢复或升级的软件；
- ② 建立 PC 机和 PIX 防火墙之间的连接；
- ③ 进入 PIX 监控模式；
- ④ 进行设备升级。

详细步骤如下所述。

步骤 1，下载升级需要的 PIX 的软件，具体方法和正常模式相同，本案例中我们下载的软件是“pix633.bin”。

步骤 2，软件下载完成后，我们需要建立 PC 机和 PIX 之间的连接，具体方法和路由器及交换机的操作相同。

步骤 3，开启 PIX 电源，按 Escape 键或发送一个“Break”字符，PIX 会直接进入监控模式，此时超级终端的提示如下：“monitor>”。

步骤 4，在做完以上工作后，下面我们需要做的就是开始进行设备的软件升级。

首先，我们需要在 PC 上启动 TFTP 服务器，并将下载的软件“pix633.bin”放于指定的目录下。然后我们开始软件的升级，假定 PC 机的 IP 地址为 192.168.1.1，而 PIX 的以太网口 IP 地址为 192.168.1.2，子网掩码均为 255.255.255.0，在监控模式下将 IP 地址 192.168.1.1 配置到 PIX 的内网口（默认为 eth1），从而建立起 PIX 与 TFTP 服务器之间的连控。

具体步骤如下：

```
monitor> interface 1
```

```
monitor> address 192.168.1.2
```

```
monitor> server 192.168.1.1
```

```
monitor> ping 192.168.1.1
```

```
Sending 5, 100-byte 0x5b8d ICMP Echoes to 192.168.1.2, timeout is 4 seconds:!!!!
```


Success rate is 100 percent (5/5)

通过上述命令，在 PIX 监控模式下将 IP 地址 192.168.1.2 配置到 PIX 的内网口，从而建立起 PIX 与 TFTP 服务器之间的连接，下面我们将软件安装到 PIX 的闪存（flash）中。

```
monitor> file pix633.bin
```

```
monitor> tftp
```

```
tftp pix633.bin@192.168.1.1
```

至此我们就完成了对 PIX 的软件恢复。

8.5 Cisco 设备口令恢复

在日常的管理工作中，密码的管理是非常重要的一点，企业中的网管人员也许会离开公司，这时文档交接中很重要的一点是设备密码的交接。但在实际的工作中我们经常会发现很多企业在这方面很不重视，导致经常是新来的网管面对一堆没有密码的设备，一筹莫展。即便我们做好了文档工作，也难免会百密一疏，如果我们忘记了设备的密码，这时就需要对密码进行恢复。Cisco 的所有设备都有相应的密码恢复手段。下面我们就常用的路由器、交换机和防火墙进行讲解，其他所有网络设备的具体恢复方法可参考 Cisco 公司网站的资料：

<http://www.cisco.com/warp/public/474/>

8.5.1 Cisco 路由接口令恢复

为了真正理解路由器口令恢复的过程，我们就需要对路由器的引导过程有所了解，这就需要我们对控制路由器引导过程的引导寄存器进行简要的介绍。我们在正常运行的路由器中运行“show version”命令，就可以看到该路由器的引导寄存器的值，路由器默认的值是“0x2102”（如图 8-45 所示），下面我们就来分析一下引导寄存器。

寄存器位	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
寄存器值(2 进制)	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0
寄存器值(16 进制)	2				1					0			2			

图 8-45 16bit 引导寄存器的默认值

引导寄存器包接 16bit，各位代表的含义见表 8-2。

表 8-2 引导寄存器各位的含义

位	含 义	默认值
0-3	这 4bit 被称为寄存器的引导字段，它控制路由器从哪里引导。 如果该字段值为 0x0，路由器会被引导到 ROM 监控模式（rommon>）。 如果该字段值为 0x1，路由器会从主板的 ROM 引导，ROM 中如果存在简化版的 IOS，就进入 boot 模式（Router(boot)>）。 如果该字段值为 0x2-0xF，路由器会根据配置文件里的系统引导命令（boot system）进行引导，如果没有系统引导命令，路由器将默认引导 Flash 中的第一个 IOS。	0010

		续表
位	含 义	默认值
4	该比特被称为强制引导位。该位设为 1 意味着路由器将强制按照配置文件中的系统引导命令进行引导，如果配置文件中没有系统引导命令，路由器将会进入 boot 模式，默认该位为 0，意味着如果没有系统引导命令，路由器还将尝试引导 FLASH 中的第一个 IOS。	0
5, 11, 12	这 3bit 被称为控制台速率设置位。第 5、11 和 12 一起工作用来设置控制台的波特率 (bit/s)，路由器控制台的默认波特率是 9600bit/s (5、11、12 都置 0)，我们建议不要更改此项设置。	0
6	该比特被称为忽略 NVRAM 位。该位设为 1 意味着路由器启动时将忽略 NVRAM 里的配置文件。当我们进行密码恢复时会将此位设为 1。	0
7	该位被称为 OEM 位。它被用于 OEM 版本的路由器。该位设为 1 时，系统引导的 banner (Cisco System 的标志) 将失效。	0
8	该比特被称为屏蔽暂停键位。如果该位设为 0 意味着路由器在正常运行时，可通过按下单键使操作系统暂停运行，通常我们并不希望这样，因此默认该位为 1。注意屏蔽暂停键时，我们依然可以在路由器引导的起始 60 秒内，通过按暂停键将路由器暂停下来。	1
9	保留位。	0
10, 14	这 2bit 被称为广播格式位。我们知道默认网络广播地址是网络地址全 1 (第 10 和 14bit 都为 0) 的地址，但通过设置第 10 和 14bit，我们可以改变网络广播地址的格式，比如我们通过将第 10bit 设为 1 而第 14bit 设为 0，就可以把网络全 0 和主机全 1 的地址认为是网络广播地址，这主要是为了向后兼容许多老的 UNIX 主机，通常情况下我们不用改变此默认设置。	0
13	该比特被称为网络引导失败响应位。该位设为 1 意味着路由器在 5 次网路引导失败后将自动从缺省位置载入 IOS。如果该位设为 0 意味着路由器会不停的重复网络引导，即使失败，它也不会从 ROM 中去引导 IOS。	1
15	该比特称为显示出厂诊断位。该位设为 1 意味着路由器将显示出厂诊断信息，此时路由器将强制忽略 NVRAM。	0

了解了引导寄存器各比特的含义之后，我们再来熟悉一下路由器的引导过程，如图 8-46 所示。

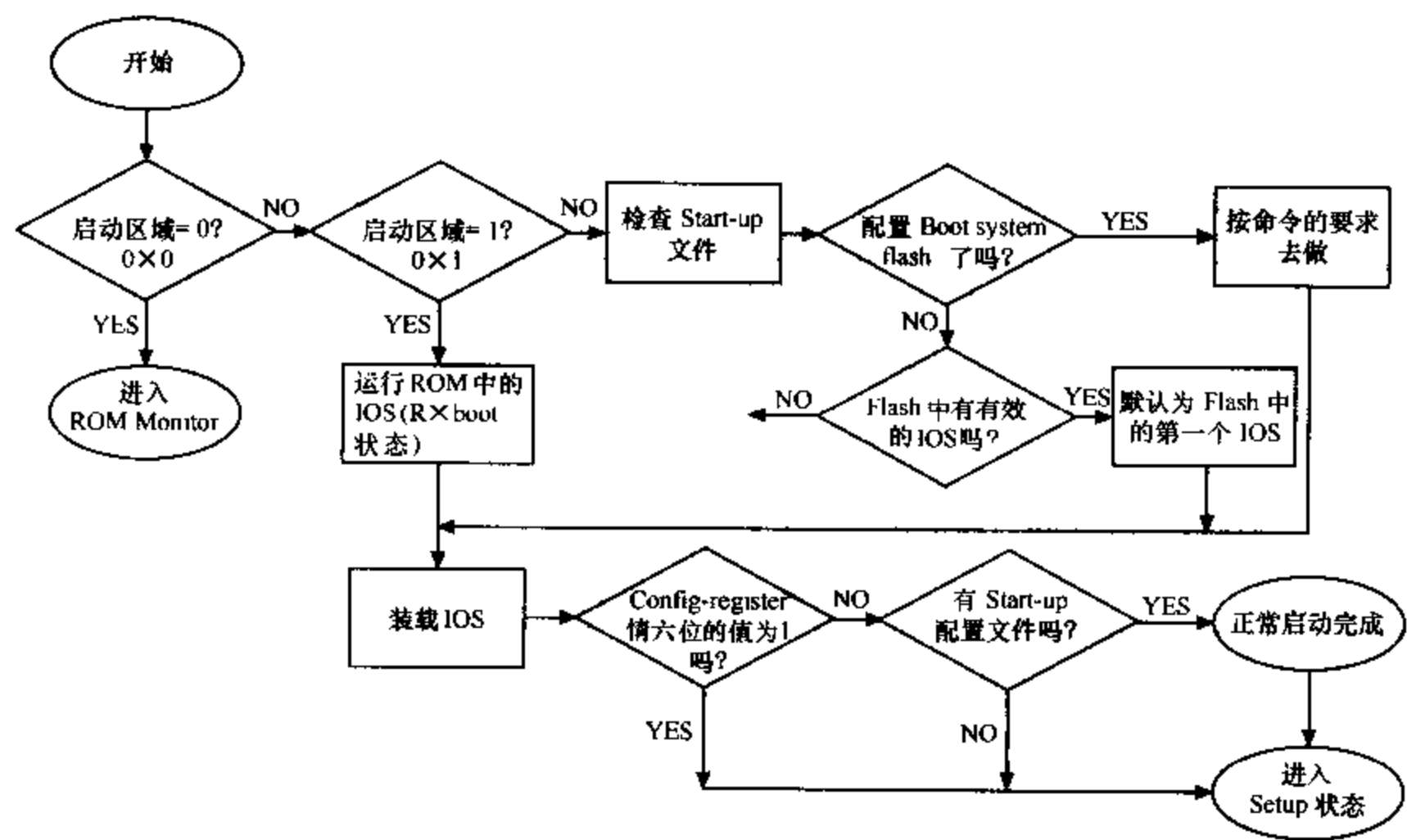


图 8-46 路由器引导过程

当我们对引导寄存器的工作原理和路由器的引导过程熟悉之后, 密码恢复的过程也就变得非常清晰和易于理解了。由于我们配置的密码都保存在配置文件 (Startup-Config) 里, 而路由器的配置文件是保存在 NVRAM 里的, 因此我们可以通过将引导寄存器的第 6bit 的值改为 1 来使得路由器在引导时忽略 NVRAM 里的配置信息 (如图 8-47 所示), 从而无需密码就可以直接进入路由器的配置模式。当然此时路由器的配置信息还是存在于 NVRAM 里, 我们可以通过 “show startup-config” 命令来查看, 为了重新使用原来的配置文件, 我们可以通过 “copy startup-config running-config” 命令将配置文件调入内存中, 同时不要忘记将原来的密码改掉和将关闭的端口打开 (No Shutdown), 以及将引导寄存器值改回默认的 0x2102。最后我们再运行 “copy running-config startup-config” 或 “write memory” 命令, 将配置文件重新保存, 此时的配置文件除了重新修改的密码部分外, 和原来的配置文件完全相同, 从而实现了恢复密码的目的。

寄存器位	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
寄存器值(2 进制)	0	0	1	0	0	0	0	1	0	1	0	0	0	0	1	0
寄存器值(16 进制)	2				1				4				2			

图 8-47 密码恢复所采用的引导寄存器值

明白了上面介绍的密码恢复的原理后, 下面我们来看一下密码恢复的详细步骤。

步骤 1, 将计算机串口 (COM) 和路由器 Console 口相连, 启动计算机的超级终端, 设置其参数为: 波特率为 9600, 数据位为 8, 奇偶校验为无, 停止位为 1, 流控选择无。具体步骤参见路由器软件升级的相关内容。

步骤 2, 启动路由器并在前 60 秒内按 “Ctrl+Break” 键使路由器进入 ROM 监控模式。

路由器有两种不同的监控模式 “>” 和 “rommon>”。如果是 2000、2500、3000 等以早期的 2000 系列主板为代表的路由器, 监控模式为 “>”; 如果是 1003、1600、1700、2600、3600、4500、4700、7200、7500 等基于 RISC 平台的路由器, 其监控模式是 “rommon>”。

如果是 “>” 使式, 按如下方式修改引导寄存器值:

>O/R 0x2142 将引导寄存器值的第 6 位设为 1, 从而忽略 NVRAM。

>Initialize 重新引导路由器。

如果是 “rommon>” 模式, 按如下方式修改引导寄存器值:

rommon 1 >confreg

当出现提示 “Do you wish to change configuration[y/n]? ” 时, 回答 y。

之后的问题回答 n 直到你到达 “ignore system config info[y/n]? ” 提示时, 回答 y。

(以上步骤也可采用 “rommon 1 >confreg 0x2142” 来代替)

rommon 2 >reset 重新引导路由器。

步骤 3, 路由器重新引导后, 当提示是否进入对话配置时 “Would you like to enter the initial configuration dialog? [yes]:”, 回答 “no” (如误输入 “yes”, 立刻按 Ctrl+C 退出); 当出现 “Press RETURN to get started!” 时, 按回车就进入了路由器的普通用户模式 “Router>”; 此时我们可以输入 “Router>enable” 进入特权模式; 进入特权模式后我们切记一定将引导配置文件拷贝到内存中 “Router#copy start run”, 至此我们的工作已经完成了一大半了,

下面我们要做的事情就是重新为路由器设置密码；恢复原有的引导寄存器值并启用所有的接口。

(1) 进入配置模式

```
Router#configure terminal
```

(2) 重新配置口令

```
Router(config)#enable secret newpass
```

```
Router(config)#line console 0
```

```
Router (config-line)#login
```

```
Router (config-line)#password newpass
```

```
Router (config-line)#exit
```

(3) 恢复原始配置寄存器值并激活所有端口

```
Router(config)#config-register 0x2102
```

```
Router(config)#interface xx
```

```
Router(config)#no shutdown
```

(4) 保存配置

```
Router (config)#end
```

```
Router#write memory
```

至此我们就完成了对路由器密码的恢复工作，如果你还想了解具体型号的具体步骤，请参阅 Cisco 的相关文档，相关链接如下：

<http://www.cisco.com/warp/public/474/>

8.5.2 Cisco 交换机口令恢复

交换机的口令恢复原理和路由器略有不同，交换机不用修改引导寄存器的值，而是在一个类似于路由器的监控模式的“switch:”中断控制台模式中，将 Flash 中的引导配置文件“config.txt”改一个文件名，比如“config.old”，这样当交换机重新启动时找不到引导配置文件“config.txt”，它就会认为此交换机没有配置文件，从而我们可以不用密码而进行任何操作，当然接下来我们要做的就是将“config.old”再改名为“config.txt”，同时不要忘记修改密码。具体操作的步骤如下所述。

步骤 1，拔掉交换机的电源线。

步骤 2，将计算机串口和交换机 Console 口相连，启动计算机超级终端，设置其参数为：

每秒位数 (B)：9600

数据位 (D)：8

奇偶校验 (P)：无

停止位 (S)：1

数据流控制 (F)：无

步骤 3，按住交换机前面板的“mode”按钮，插上电源线，当端口 1 上面的灯不亮后，放松“mode”按钮。

注意：我们这里是按 Catalyst3550 来作示范，如果是 2950 或 2955 交换机在这一步的操作会有所不同。如果是 2950 我们将看前面板上的“STAT”状态灯不亮后，放松“mode”按

钮；如果是 2955 交换机，我们将用“Ctrl+Break”键来中断交换机进入“switch:”模式。

步骤 4，这时超级终端上应该显示：

The system has been interrupted prior to initializing the flash file system.

The following commands will initialize the flash file system, and finish loading the operating system software:

flash_init

load_helper

boot

步骤 5，输入 flash_init

步骤 6，输入 load_helper

步骤 7，输入 dir flash:

这时显示：

switch: dir flash:

Directory of flash:/

2	-rwx	1751538	<date>	c3500XL-c3h2s-mz.120-5.4.WC.1.bin
3	-rwx	94375	<date>	c3500XL-diag-mz-120-5.3.WC.1
4	drwx	10176	<date>	html
5	-rwx	272	<date>	env_vars
6	-rwx	111	<date>	info
167	-rwx	1952	<date>	config.text
166	-rwx	111	<date>	info.ver
168	-rwx	5040	<date>	vlan.dat

472576 bytes available (3140096 bytes used)

步骤 8，输入 rename flash:/config.text flash:/config.old

switch: rename flash:/config.text flash:/conflg.old

步骤 9，输入 boot，重新启动系统，如下：

switch: boot

步骤 10，系统启动完后显示：Continue with the configuration dialog? [yes/no]：

输入“no”。

步骤 11，输入 enable，进入 enable 模式后，输入 rename flash:conflg.old flash:config.text

Switch#rename flash:conflg.old flash:config.text

步骤 12，接着按以下步骤操作：

Switch# copy flash:config.text system:running-config

Source filename [config.text]? (press Return)

Destination filename [running-config]? (press Return)

步骤 13，接着按以下步骤操作：

switch#configure terminal

switch(config)#no enable secret


```
switch(config)#no enable password
```

```
switch(config)#exit
```

```
switch#write memory
```

这时，系统就恢复没有密码的状态了，当然我们可以重新设置密码。

至此我们就完成了对交换机密码的恢复工作，如果你还想了解具体型号的具体步骤，请参阅 Cisco 的相关文档，相关链接如下：

<http://www.cisco.com/warp/public/474/>

8.5.3 Cisco 防火墙口令恢复

Cisco PIX 防火墙的口令恢复原理和路由器及交换机都不同，它不用像路由器那样在监控模式里修改引导寄存器的值，也不用像交换机那样进入“switch:”中断控制台去修改引导配置文件的名称，PIX 需要做的是将一个特殊的恢复口令的文件传送到 PIX 中，通过这个文件在不改动配置的情况下，可以使已配置的口令无效。根据 PIX 防火墙的不同的型号，存在两种不同的口令恢复的方法。对于老的防火墙使用软盘恢复的方法；对于新的防火墙（如 PIX501、PIX506、PIX515、PIX525 和 PIX535）都使用在监控模式下通过 TFTP 的方式来传送恢复口令文件从而恢复口令的方法。由于我们可能接触的绝大多数都是新的防火墙，所以这里我们只介绍后一种口令恢复的方式，至于软件恢复的方法，感兴趣的用户可参考 Cisco 相关的文档。

整个口令恢复的过程大致包括 4 个步骤：

- ① 下载恢复口令所需的软件；
- ② 建立 PC 机和 PIX 防火墙之间的连接；
- ③ 进入 PIX 监控模式；
- ④ 进行设备口令的清除。

详细步骤如下所述。

步骤 1，下载恢复口令所需要的软件，根据 PIX 运行的软件版本，下载与其相应的口令恢复软件，其名称为 npxx.bin（xx 是 PIX 防火墙上运行的软件的版本号），下载软件的具体方法和前面我们接触的其他软件的下载过程相同，我们这里下载的软件是“np63.bin”。

步骤 2，软件下载完成后，我们需要建立 PC 机和 PIX 之间的连接，具体方法和路由器及交换机的操作相同。

步骤 3，开启 PIX 电源，按 Escape 键或发送一个“Break”字符，PIX 会直接进入监控模式，此时超级终端的提示如下：“monitor>”。

步骤 4，在做完以上工作后，下面我们需要做的就是开始进行设备口令的恢复工作。

首先，我们需要在 PC 上启动 TFTP 服务器，并将下载的软件“np63.bin”放于指定的目录下。然后我们开始口令的恢复，假定 PC 机的 IP 地址为 192.168.1.1，而 PIX 的以太网口 IP 地址为 192.168.1.2，子网掩码均为 255.255.255.0，在监控模式下将 IP 地址 192.168.1.1 配置到 PIX 的内网口（默认为 eth1），从而建立起 PIX 与 TFTP 服务器之间的连接。

具体步骤如下：

```
monitor> interface 1
```

```
monitor> address 192.168.1.2
```



```
monitor> server 192.168.1.1
```

```
monitor> ping 192.168.1.1
```

```
Sending 5, 100-byte 0x5b8d ICMP Echoes to 192.168.1.2, timeout is 4 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5)
```

通过上述命令，在 PIX 监控模式下将 IP 地址 192.168.1.2 配置到 PIX 的内网口，从而建立起 PIX 与 TFTP 服务器之间的连接，下面我们将软件拷贝到 PIX 的闪存（Flash）中。

```
monitor> file np63.bin
```

```
monitor> tftp
```

```
tftp np63.bin@192.168.1.1
```

软件拷贝成功后，当出现 “Do you wish to erase the passwords? [yn]” 提示时，输入 “y”，这时口令就成功地被清除了。

```
Do you wish to erase the passwords? [yn] y
```

```
Passwords have been erased.
```

```
Rebooting....
```

至此我们就完成了对 PIX 密码的恢复工作，如果你还想了解具体型号的具体步骤，请参阅 Cisco 的相关文档，相关链接如下：

<http://www.cisco.com/warp/public/474/>

8.6 SNMP 网管协议

SNMP（Simple Network Management Protocol，简单网络管理协议）是由 IETF 的研究小组为了解决 Internet 上的路由器管理问题而提出的，和 WWW、SMTP 和 FTP 一样，它工作于 TCP/IP 模型的应用层。随着 Internet 的迅速发展，SNMP 目前已成为事实上的网络管理协议，在 Internet 骨干设备和绝大多数厂商的网络产品中得到广泛采用。这既取决于 TCP/IP 协议的主导地位，也取决于 SNMP 协议自身的简单易行。

SNMP 使用嵌入到网络设施中的代理软件来收集网络通信信息和有关网络设备的统计数据。代理不断地收集统计数据，如所收到的字节数等，并把这些数据记录到一个管理信息库（MIB，Management Information Base）中，网管员通过向代理的 MIB 发出查询信号就可以得到这些信息，这个过程就叫做轮询（Polling），是 SNMP 最基本的特点。SNMP 的体系架构如图 8-48 所示。

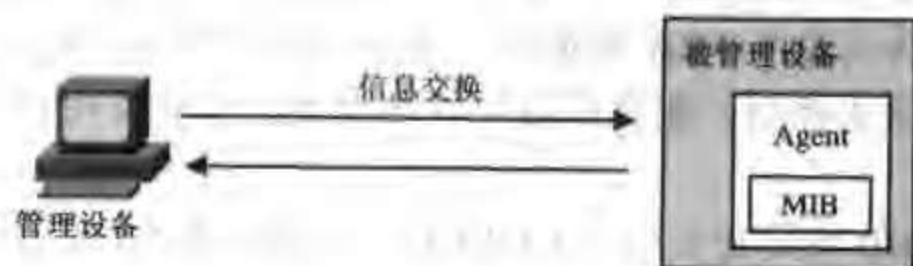


图 8-48 SNMP 的体系结构

由图 8-48 我们看出一个典型的网络管理系统包括 4 个要素：管理设备、被管理设备、网管代理（Agent）和管理信息数据库（MIB）。下面我们就来对它们进行一下简单的介绍。

（1）管理设备

在 SNMP 中，网络管理设备是网络管理的实体，其上运行网络管理软件，它对网络设备发送各种查询报文，并接收来自被管理设备的响应及陷阱（Trap）报文，将结果显示出来。管理设备通常是一台工作站、PC Server 或者就是一台 PC 机，通过数据网络本身与被管设备相连（如局域网口），它在网络中就是一个主机，因此在通常的网络里面都是带内网管，即管理数据和普通传输的数据是混杂在一起传输的。

（2）被管理设备

在 SNMP 中，被管理设备是启用了 SNMP 的设备，例如配置了 SNMP 的路由器、交换机等。例如：

```
Switch(config)#snmp-server community public ro
Switch(config)#snmp-server community private rw
```

（3）网管代理（Agent）

Agent 是驻留在被管理设备（如路由器、交换机等）上的软件模块，它可以获得本地设备的运转状态、设备特性、系统配置等相关信息，同时负责接受、处理来自管理设备的请求（Request）报文，然后将管理设备请求的参数的数值形成响应（Response）报文，发送回去，并在一些紧急情况下，如接口状态发生改变、呼叫成功等时候，主动通知管理设备（发送陷阱 Trap 报文）。网络管理设备上的网管软件则根据这些响应的数据包，通过构建直观的拓扑图等方式，便于网管人员进行设备的监控及管理。SNMP 协议就是用来规定网管软件和网管代理（Agent）之间是如何传递管理信息的应用层协议。网管代理在 UDP 的 161 端口接收网管软件的读写请求消息，网管设备在 UDP 的 162 端口接收代理的事件通告消息。路由器、交换器等许多网络设备的管理代理软件一般是由原网络设备制造商提供的，它可以作为底层系统的一部分，也可以作为可选的升级模块。设备厂商决定他们的管理代理软件可以控制哪些 MIB 对象，哪些对象可以反映管理代理软件开发者感兴趣的问题。

（4）管理信息数据库（MIB）

MIB 定义了一种数据对象，它可以被网络管理系统控制。MIB 是一个信息存储库，它包含了网络管理代理中的有关配置和性能的数据，有一个组织体系和公共结构，其中包含分属不同组的许多个数据对象，如图 8-49 所示。

MIB 数据对象以一种树状分层结构进行组织，这个树状结构中的每个分支都有一个专用的名字和一个数字形式的标识符。使用这个树状分层结构，MIB 浏览器能够以一种方便而且简洁的方式访问整个 MIB 数据库。这里包括了数千个数据对象，网管软件可以通过控制这些数据对象去控制、配置或监控网络设备。目前使用最广泛、最通用的 MIB 是 MIB-II。

说明：Cisco 的 MIB 变量是 1.3.6.1.4.1.9.x.y.z，在表 8-3~8-7 中我们列出了它的参数。

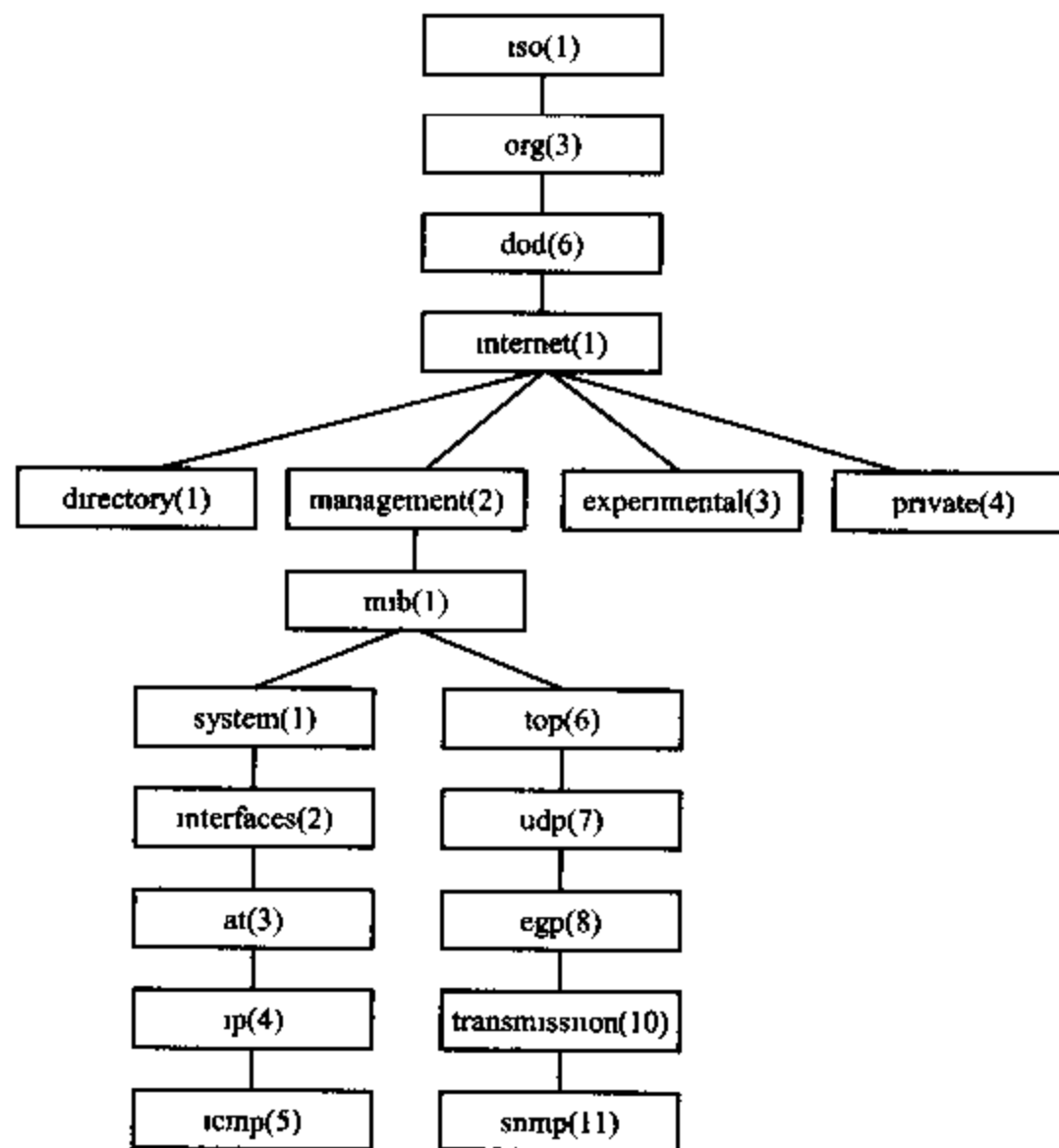


图 8-49 MIB 结构

表 8-3 故障管理

Chapter (x)	Section (y)	Variables (z)
local (2)	IP Group	locIPhow
		locIPwho
local (2)	Host Conf file (1)	file names (48-51)
	Net Conf file (1)	server providing file
local (2)	System Basic (1)	bootHost (6)
		name of boot image

表 8-4 配置管理

Chapter (x)	Section (y)	Variables (z)
local (2)	System Basic (1)	freeMem (8)
		whyReload (2)
CiscoMgmt (9)	Cisco Environmental Monitor Group (13)	physical status
local (2)	Interface (2)	packets dropped

表 8-5 安全管理

Chapter (x)	Section (y)	Variables (z)
local (2)	System (1)	authAddr (5)
		locIPSecurity

表 8-6 计费管理

Chapter (x)	Section (y)	Variables (z)
local (2)	IP Checkpt Acct(4.7.1)	packets sent
		packets dropped

表 8-7 性能管理

Chapter (x)	Section (y)	Variables (z)
local (2)	System (1)	CPU Utilization (56,57,58,61)
local (2)	Interface Group (2)	time between pkts
		num pkts transmit

比如我们想了解路由器重启的原因，我们就可以通过网管软件来向网管代理请求被管理设备（路由器）MIB 库中有关重启的参数，根据上表，我们知道该变量是“whyReload”其 MIB 标识符是“1.3.6.1.4.1.9.2.1.2”。下面是我们在网管时常会监控的 MIB 的参数。

被管理设备	需要监控的 MIB 参数
路由器	Free buffers,congestions,errors,drop packets,non-routed requests
交换机	Dropped packets, error rate,unauthorized users.
服务器	Number of processes, CPU and Disk utilization.

通过上面的介绍我们对 SNMP 的体系架构及其构成的要素有了一定的了解，下面我们来了了解一下 SNMP 的操作方式。

SNMP 以 GET-SET 方式替代了复杂的命令集，可以利用基本操作完成全部操作，同时，用户可以采用管理信息库标准或按标准的方式来定义自己的 MIB。这样就可以通过降低网管系统中众多代理部件的成本来降低整个网管系统的成本。

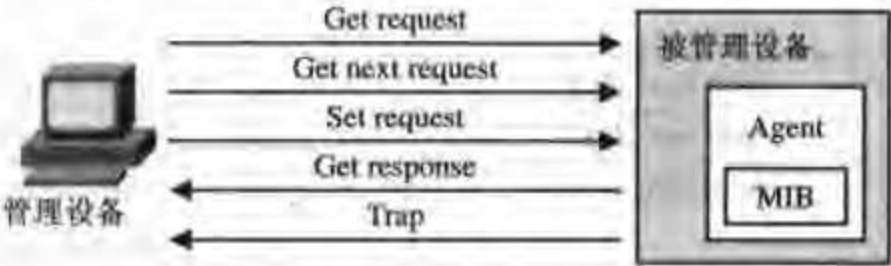


图 8-50 SNMP 提供的基本操作

从图 8-50 我们看出，SNMP 只提供了 3 种基本操作：获取网络设备信息（Get：读操作）、设置网络设备参数值（Set：写操作）和事件报告（Trap：陷阱操作）。SNMP 有 5 种协议数据单元（即消息）类型：Get-request、Get-Next-Request、Get-Response、Set-Request 和 Trap。其中，Get-request 和 Get-Next-Request 由网管软件发给网管代理，请求检索信息，网络代理以 Get-Response 响应它；网管软件使用 Set-Request 可以远程设置网络代理所在的网络设备的参数。这些都通过读或写 MIB 实现。在 5 种类型中，只有 Trap 是网络代理发起的（非请求信息），用于向管理工作站报告特定的事件，如设备的启动、关闭和其他变化等。

尽管目前 SNMP 使用非常广泛，但它建立在轮询（polling）上的管理机制依然存在着两个明显的弱点如下：

(1) 在大型的网络中, 轮询会产生巨大的网络管理通信流量, 因而会导致通信拥挤情况的发生。

(2) 它将收集数据的负担加在网络管理设备上, 当管理小范围的数据时, 管理设备也许能轻松应对, 但当处理非常大的网络时, 大量的管理数据也许会使管理设备停止工作。

目前来看, 对于第1个问题通常的解决方法是采用 QoS 将管理数据和其他业务数据分离开来, 优先保证业务数据的正常传输, 虽然此方法可以在一定程度上缓解业务通信拥挤的发生, 但不能从根本上解决问题。对于第2个问题目前采用的主要方法只能是提高管理设备的处理性能。

8.7 小 结

本章开始我们介绍了网络管理的概念以及网络管理包含的内容, 接着对企业网络管理中的文档管理和设备管理部分进行了相应的介绍, 其中对 Cisco 设备的软件维护作了较为详细的讲解, 最后简要介绍了简单网络管理协议 SNMP。

第9章 企业网安全配置

本章将涵盖下列有关企业网安全方面的关键主题

- 网络安全的风险分析
- 网络安全的部署

目标：通过对本章的学习，希望读者对以下一些方面的内容有所了解：

- (1) 企业网络面临的网络攻击有哪些；
- (2) 我们如何在企业网中部署各种安全策略。

9.1 简介

今天的 Internet 正以巨大的力度和广度冲击和改造着社会、经济、生活的传统模式，随着金融、政府等越来越多的机构将其业务系统放到网络上运行（比如银行的结算、证券的行情交易、铁路的售票等等），Internet 正在成为社会公众强烈依赖的社会重要基础设施，Internet 安全已成为普遍关注的焦点。一旦网络被攻击造成瘫痪，就可能意味着损失大量的资金，甚至可能导致许多公司的破产。

随着 Internet 的急剧扩大和上网用户数迅速增加，网络风险变得更加严重和复杂。原来由单个计算机安全事故引起的损害可能传播到其他系统，引起大范围的瘫痪和损失；另外加上缺乏安全控制机制和对因特网安全政策的认识不足，这些风险正日益严重。

针对企业网中存在的种种安全隐患，在进行企业网络的建设时，我们必须对各种安全风险认真分析，并且采取相应的安全措施，防患于未然。

9.2 企业网络安全的风险分析

在前面的章节中我们曾介绍过，一个典型的企业网，通常是由局域网、广域网和 Internet 接入三部分组成的一个综合体，这种模块化的方式便于我们对企业的网络进行安全方面的分析，也有利于整个安全系统的实施。

一个典型的企业网如图 9-1 所示。企业网络与大多数与 Internet 相连的网络一样，内部用户数据需要流出，外部用户数据需要流入。在企业网络中有以下一些威胁是我们需要考虑的：

① 首先是来自内部用户的威胁。尽管统计结果的百分比数有所不同，但大多数攻击来自于内部网络已是不争的事实。心怀不满的员工、公司间谍、访问的客人以及无意间中的病毒用户都是这类攻击的潜在来源。在我们设计网络的安全性时，非常重要的一点是要了解潜

在的内部威胁;

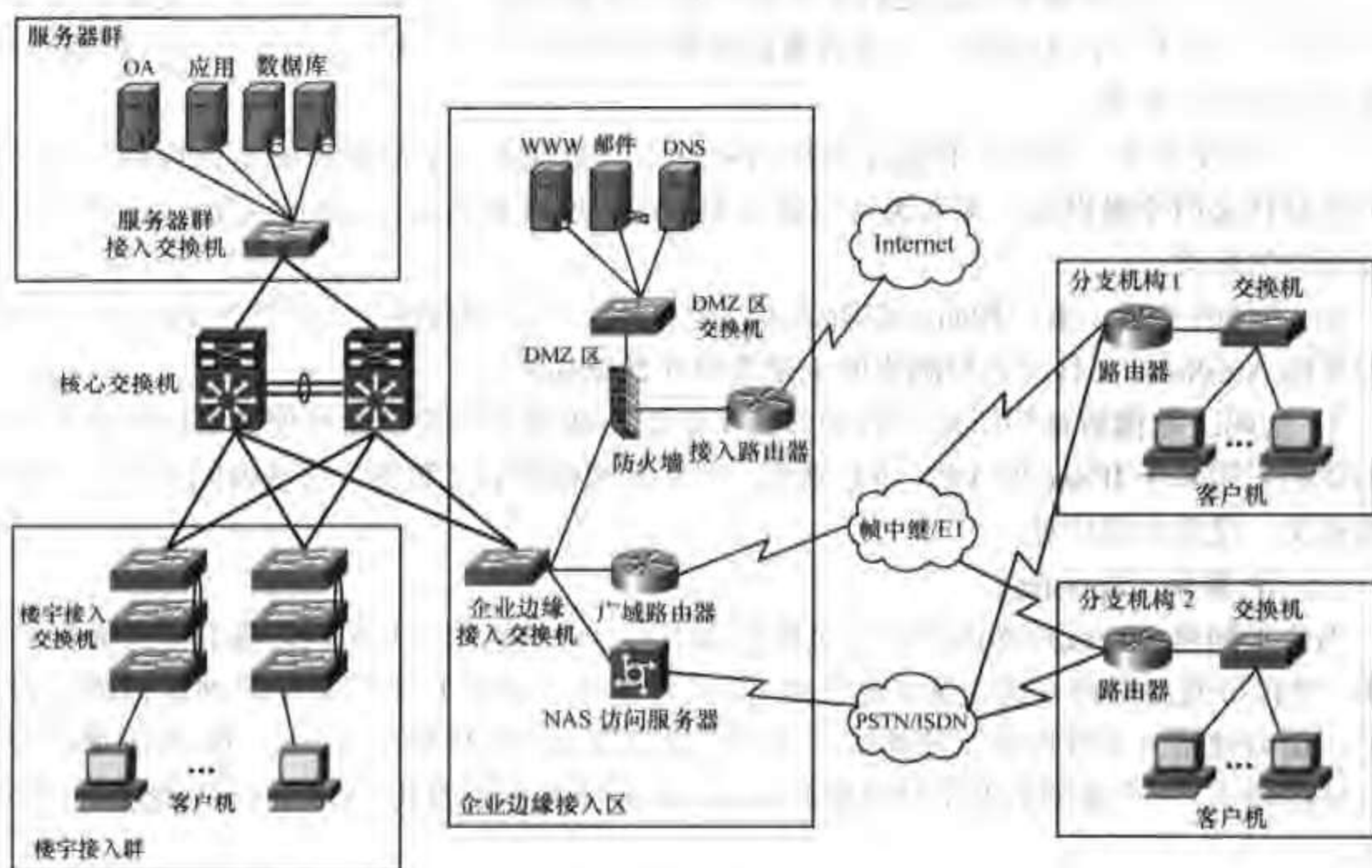


图 9-1 典型企业网

② 其次是对与 Internet 相连，可对外公开地址的主机的威胁。由于这些对外公开地址的主机通常是对外提供服务的服务器，如果这些系统存在漏洞，就很可能遭受应用层漏洞攻击和 DoS 攻击；

③ 最后，企业网络的远程接入系统也容易成为黑客的攻击对象。因为这些设备通常置于防火墙后面，一旦黑客通过它们拨号进入接入网络，他们就可假冒授权的网络用户，访问其他内网的资源。

下面再来具体介绍一下网络攻击的类型。网络攻击与作为其目标对象的系统具有同样的多样性。某些攻击极为复杂，而另外一些攻击则是毫无恶意的设备操作人员无意中造成的。

在分析攻击类型时，我们首先需要了解 TCP/IP 的一些内在局限性。最初的 Internet 是将各个政府部门与大学连接在一起，目的是促进学术交流与研究，因此它的特点是开放。Internet 的开创者从未想到 Internet 会在将来被广泛采纳。因此，在 Internet 协议（IP）的使用初期，安全性并未得到重视，所以多数 IP 设施具有内在的不安全因素。由于 IP 协议本身缺乏安全性的考虑，因此我们只有通过网络安全措施、服务来完善 IP 基础设施，从而减弱 Internet 协议固有的安全隐患。下面来介绍 IP 网络中常见的攻击类型及其相应的防范措施。

（1）数据窃听（Sniff）

数据窃听是一种软件应用，它通过处于混杂模式的网卡捕获通过某个冲突域的所有网络数据。通常我们利用数据窃听功能进行网络故障的排除或进行流量分析。但黑客可以利用它获取一些非常有用且敏感的信息，比如用户名和密码等。

通常我们可以采用如下几种方式减轻数据窃听带来的威胁:

① 验证: 进行严密的验证是防范数据窃听的首要措施。比如我们建议对关键设备采用一次性密码(OTP)。因为即使一个黑客通过数据窃听获得了这一密码, 这对他没有丝毫用处, 因为该密码已经作废;

② 采用交换机: 另外一种防止数据窃听的方法是部署一个交换式的基础设施。因为如果网络整体采用交换设备, 那么黑客只能获取他们所连接到的端口上的信息流, 这样可以大大减轻它的危害;

③ 防窃听工具: 第三种防止窃听的方法是使用专门检测网络上窃听情况的软件与硬件。比如采用 AntiSniff 工具可以检测出网上是否存在数据窃听;

④ 密码: 抵御数据窃听最有效的方法不是防止或查出窃听, 而是使其不能发挥作用。比如我们采用基于 IPSec 的 VPN 进行通信, 即使黑客窃听到了数据, 它获取的也是一些加密后的密文, 没有实质用处。

(2) IP 欺骗 (Spoofing)

当位于网络内部或外部的黑客主机模仿成为一台可信赖的计算机时, 我们称其进行了 IP 欺骗。黑客可通过两种方式达到上述目的。他可以使用一个位于可靠网络 IP 地址范围内的 IP 地址, 也可使用一个既可靠又能够访问网络上特定资源的授权外部 IP 址。IP 欺骗通常会引发其他的攻击。一个典型的例子是用骗取的源地址隐藏黑客的身份, 从而引发拒绝服务(DoS)攻击。

通过以下措施我们可以减轻 IP 欺骗的威胁, 但不能完全消除这种威胁:

① 访问控制: 防止 IP 欺骗最常用的方法是正确配置访问控制功能。我们可以配置访问列表拒绝任何来自外部网络而其源地址在内部网络的流量;

② RFC 2827 过滤: 我们应该在自己的边界路由器上过滤那些不属于自己网络的源地址的对外访问, 通过这种方法, 可以防止自己网络的用户欺骗其他网络;

③ RFC 1918 过滤: 我们应该在自己的边界路由器上过滤那些来自 Internet 上的私有地址(10.0.0.0~10.255.255.255、172.16.0.0~172.31.255.255、192.168.0.0~192.168.255.255)对自己内部网的访问。

(3) 拒绝服务 (DoS)

拒绝服务攻击(DoS)是最广为人知的攻击形式, 同时也是最难以被完全防止的。即使在黑客看来, DoS 攻击也是微不足道的, 因此这种攻击非常容易实施。但由于这种攻击容易实施而且潜在的危害性很大, 因此安全管理人员对 DoS 攻击也应予以特别的重视。这些攻击包括:

TCP SYN Flood;

Ping of Death;

Tribe Flood Network (TFN) 与 Tribe Flood Network 2000 (TFN2K);

Trinoo;

Stackeldraht;

Trinity。

DoS 攻击与其它多数攻击有所不同, 因为这种攻击的目的通常并不是进入某个网络或获取其中的信息。这种攻击的主要目的是使某种服务不能被正常使用, 而且这种攻击通常是通

过破坏网络、操作系统或应用内部的某些资源限制实现的。

对于特定的网络服务器应用，如一个 Web 服务器或 FTP 服务器，这些攻击希望达到的主要目的是获取这一服务器支持的所有可用连接并使其处于开放状态，同时将服务器或服务的合法用户排除在外。DoS 攻击也可以通过使用普通的因特网协议实现，如 TCP 与因特网控制信息协议（ICMP）。多数 DoS 攻击是利用了被攻击的系统的总体体系结构中存在的弱点，而不是软件错误或安全漏洞。但是，有些攻击会将大量不受欢迎而且无用的网络分组发到网上，或提供一些关于网络资源状态的错误信息，从而使网络性能受损。这种攻击通常是最难防范的，因此需要与上游网络供应商进行协调合作。如果那些势必会消耗网络的可用带宽的流量不被立即阻止，那么在它进入网络的地方对其进行阻止已为时太晚，因为可用的带宽这时已被消耗了。当这种攻击在同一时间从许多不同的系统发起时，通常将其称作分布式拒绝服务攻击（DDoS）。

通过以下三种方法我们可以减弱 DoS 攻击的威胁：

① 防 IP 欺骗特性：在路由器上正确配置防 IP 欺骗特性可以降低这种风险。因为黑客往往是隐藏其身份后进行攻击，如果他不能隐藏身份，可能也就不会冒然进行攻击；

② 防 DoS 特性：在路由器和防火墙上正确配置防 DoS 特性有助于限制攻击的危害。该特性通常是指对系统在某一特定时间允许开放的半开放连接的数量加以限制；

③ 流量限制：可以将网络上相对次要，但同时又被黑客用来进行 DoS 攻击的流量限制在一定的范围内。比如可以限制进入网络的 ICMP 流量，因为 ICMP 分组通常只是用于进行诊断，这样我们就可以减弱基于 ICMP 的 DDoS 的威力。

（4）密码攻击

黑客可以采用几种不同的方法实施密码攻击，包括暴力破解，特洛伊木马方式，IP 欺骗与数据窃听方式等。一旦他们拥有了用户的账号和密码，他们就拥有了和该用户完全相同的权利。更为严重的是，人们习惯于对他们所连接的每个系统均使用同一个密码。比如个人主机登陆密码、公司办公系统密码以及网上交易系统密码等，均采用同一个密码。这样，只要黑客攻破了安全性最低的一台主机，获取了其中的账号和密码，即使其他主机和系统拥有更高的安全级别，也是徒劳。

消除密码攻击最简单的方法是不要依赖于纯文本密码。使用一次性密码 OTP 或密码验证方法几乎可以完全消除密码攻击的威胁。

（5）中间人攻击

进行中间人攻击要求黑客能够访问在网上传输的网络数据。例如，某个 ISP 的工作人员获取了其雇主的网络和其他任何网络之间传输的网络数据，这就是一种典型的中间人攻击的例子。黑客通常是通过使用网络数据窃听以及路由和传输协议进行这种攻击的。这种攻击的主要目的是窃取信息、截获正在传输中的会话以便访问专用网络资源、进行流量分析以获取关于一个网络及其用途的信息、拒绝服务、破坏传输数据以及在网络会话中插入新的信息。

使用加密的传输能有效的防止中间人攻击。如果有人截获了一个加密会话中的数据，那么黑客看到的只是密码文字，而不是原来的信息。

（6）应用层攻击

黑客可以通过几种不同的方法实施应用层攻击。最常用的一种方法是利用服务器上普通

软件的常见弱点，包括邮件发送、超文本传输协议（HTTP）以及 FTP。利用这些弱点，黑客能够获得运行应用的账号的准许，从而得以访问计算机，上述帐号通常是一个特别的系统级帐号。关于这些应用层攻击的信息与说明有很多，目的是为了管理员能够用补丁程序排除问题。

与应用层攻击相关的一个主要问题是这些攻击经常使用被允许穿越防火墙的端口。例如，一个利用已知弱点对 Web 服务器进行攻击的黑客经常使用 TCP 端口 80。由于 Web 服务器为用户提供页面，因此防火墙需要允许对这一端口进行访问。在防火墙看来，黑客的入侵信息只是一种标准的端口 80 信息流。

应用层攻击永远不可能被完全消除，因为新的易受攻击点总会不断出现并被报告给因特网使用者。降低风险的最佳方法是实施良好的系统管理。以下是有助于降低应用层攻击风险的几种措施：

- ① 读取操作系统与网络日志文件并用日志分析应用对其进行分析；
- ② 用最新的补丁程序更新自己的操作系统和应用；
- ③ 使用入侵检测系统（IDS），目前我们常见的有两种入侵检测系统：基于网络的 IDS（NIDS）和基于主机的 IDS（HIDS）；

（7）网络侦察

网络侦察是指运用公用的信息和应用获得关于某个目标网络的信息。当黑客试图入侵某个网络时，他们通常需要在进行攻击前尽可能多地了解这一网络。这种侦察可以是域名系统（DNS）查询，ping 扫描或端口扫描。通过 DNS 查询可以获得以下信息，如谁拥有某个特定的域以及这个域被分配了什么地址。作为 DNS 查询结果的地址迅速探测能够显示某个特定环境中运行主机的状态。在这样一个列表被生成后，端口扫描工具可以循环处理所有已知的端口，以便完整地列出在迅速探测发现的主机上运行的所有服务。最后，黑客可以查看在主机上运行的应用的特点。这样可以获取具体的信息，这些信息有助于黑客破坏服务。

我们无法完全防止网络侦察攻击。例如，如果边缘路由器上的 ICMP 回声与回声应答功能被关闭，那么迅速探测可以被阻止，但却会影响网络诊断数据。但是，可以在迅速探测不完全的情况下轻松进行端口扫描，只不过所用的时间会比较长，因为这样还需要对可能不处于使用状态的 IP 地址进行扫描。在发生侦察攻击时，网络与主机级的入侵检测系统（IDS）通常会通知管理员。这样管理员就能更好地采取攻击预防措施或通知托管这一系统（启动了侦察探测程序）的 ISP。

（8）信任关系利用

严格来讲信任关系利用本身并不是一种攻击，真正的攻击是指非授权用户利用网络内部的某种信任关系进行攻击的行为。典型的例子是公司的周边网络连接。这些网络区域通常拥有 DNS，简单信息传输协议（SMTP）与 HTTP 服务器。由于它们均位于同一区域，因此对一个系统的破坏就会造成其他系统的受损，因为它们对其他与其网络相连的系统会比较信任。另外一个例子是位于防火墙外侧的系统与位于防火墙内侧的系统之间有信任关系。当外部系统被破坏时，它可以利用这种信任关系攻击内部的系统。

我们可以通过严格限制网络内部的信任水平来防止信任关系利用攻击。防火墙内侧的系统永远不能完全信任防火墙外部的系统。这种信任应限定到某些具体的协议，而且应该通过除 IP 地址之外的某种机制进行验证。

(9) 端口重定向

端口重定向攻击是一种信任关系利用类型的攻击，这种攻击利用一个被破坏的主机使信息流通过防火墙。假设一个防火墙有三个接口，每个接口有一个主机。外部的主机可与公共服务区（通常被称作 DMZ）的主机通信，但不能与防火墙内部的主机通信。而公共服务区的主机可与外部和内部的主机通信。如果黑客能够破坏公共服务区的主机，他们可以安装软件将信息流从外部主机直接重定向到内部主机。尽管这些通信并非违反防火墙规则，但现在外部主机通过公共服务主机上的端口重定向流程实现了与内部主机的连接。能够提供这种接入的应用的典型例子是 Netcat。

我们可以通过使用正确的信任模式（如前所述）防止端口重定向。假设系统受到攻击，基于主机的 IDS 可以帮助发现并防止黑客在主机上安装这样的应用程序。

(10) 未授权访问

未授权访问不是指某种具体的攻击，而是指当今网络中发生的多数攻击。如果有人想对一个 Telnet 登录系统进行攻击，他首先必须获得系统上的 Telnet 提示。在与 Telnet 端口建立连接后，一条信息会提示他：“使用这一资源需要经过授权。”如果这一黑客试图继续访问，他的行为就成为“未授权”的。这种攻击可以从网络内部和外部发起。

对未授权访问攻击的防范方法很简单。我们只需使黑客不易或不能利用未授权协议访问系统即可。例如，我们可以防止黑客访问某个需要为外部提供 Web 服务的服务器上的 Telnet 端口。如果黑客不能访问这一端口，那他就很难对其进行攻击。在网络中，防火墙的主要功能就是防止简单的未授权访问攻击。

(11) 病毒与特洛伊木马

最终用户工作站最易遭受病毒与特洛伊木马攻击。病毒是指与另一个程序相连的不良软件，专门在用户的工作站上执行某种破坏性功能。例如，这些病毒中有一种附属于 command.com（Windows 系统的主要解释机构），它能够删除某些文件并影响 command.com 的其他版本。特洛伊木马实际上是一种攻击工具，但整个应用却被编写得不像一个攻击工具。有一种特洛伊木马是一种在用户工作站上运行一个简单游戏的软件应用。在用户玩这个游戏时，特洛伊木马就会将自己的副本发送给用户地址簿中的每个用户。其他用户收到游戏后也会开始玩，特洛伊木马也就借此扩散开来。

通过在用户级和网络级有效使用防毒软件可以抵御这种攻击。防毒软件可以检测出多数病毒和许多特洛伊木马应用并防止它们在网络中扩散。随时了解这些攻击的最新发展情况也有助于更有效地防范这些攻击。随着新病毒或特洛伊木马应用的出现，企业需要随时了解最新的防毒软件和应用版本。

9.3 企业网络安全的部署

通过前面的介绍我们知道，企业网络的安全威胁可能来自企业网的外部，也可能来自企业网的内部，因此在进行企业网络的安全部署时，可以分别针对这两种威胁进行设计。在具体的实践当中，我们习惯上会按照企业网络构建时的模块划分而进行安全的部署。下面就针对构成企业网络的局域网、广域网和 Internet 接入三个模块进行安全方面的分析。

9.3.1 局域网模块

一个局域网的模块如图 9-2 所示。

在局域网模块中，心怀不满的员工、公司间谍、访问的客人以及无意间感染了病毒的用户都是会危及企业网安全的潜在威胁。局域网模块可以细分为网络核心区、楼宇接入区和服务器区。下面分别对这三个区域的防护进行介绍：

1. 网络核心区

网络核心区的主要目的是将信息流尽可能快速地进行传送和交换。在网络核心区通常发生的攻击有：数据窃听（Sniff）、信任关系利用和 IP 欺骗（Spoofing）等。

在网络核心区通常采用的防护手段有：采用交换架构的设备、采用访问控制和采用 RFC2827 地址过滤。

在网络的核心区通常应采用高性能的交换机，它可以有效地避免数据窃听的发生，因为每个交换的端口都处于一个独立的冲突域中。黑客如果将窃听设备（如安装了 Sniffer 程序的主机）接入核心交换机的一个端口，他只能窃听该端口正常通信的数据和广播数据，而不能获得其他用户的有用的数据。

网络核心区提供了对内部发起的攻击的有效防御。通过使用访问控制，它可减少一个 VLAN 中被攻陷的主机访问另一 VLAN 服务器上保密信息的机会。需要说明的是，我们这里是以两层结构的网络为例进行说明，如果是三层结构的网络，访问控制应设在汇聚层。

通过使用 RFC2827 过滤，在核心交换机上可以过滤那些不属于自己 VLAN 的源地址的对外访问，通过这种方法可以防止一源地址欺骗的发生。

另外，我们不需要在核心区构建入侵检测系统，因为它应该被放在最有可能遭受攻击的模块中，比如后面将要介绍的服务器区，以及 Internet 接入模块。

2. 楼宇接入区

楼宇接入区的主要目的是将大量的用户接入到网络中。在楼宇接入区通常发生的攻击有：数据窃听（Sniff）、病毒与特洛伊木马等。

在楼宇接入区通常采用的防护手段有：采用交换架构的设备和主机安装防病毒系统。

通常我们会在楼宇接入区采用低端的交换机，它可以有效地避免数据窃听的发生。楼宇接入区涉及到大量用户的接入，它是网络接入的最边缘地区，也是网络接入的发起地区，同时也往往是攻击发起的地区，网络内部的攻击往往是从楼宇接入区开始的，目前在该区域常采用防毒系统以防止接入主机感染各种病毒，进而攻击整个网络。

需要说明的是，原来我们并没有太多关注用户接入区的安全，认为只要 Internet 边界区域有足够高的安全性，就可以高枕无忧了。但随着各种病毒破坏性的增强，尤其是各种蠕虫

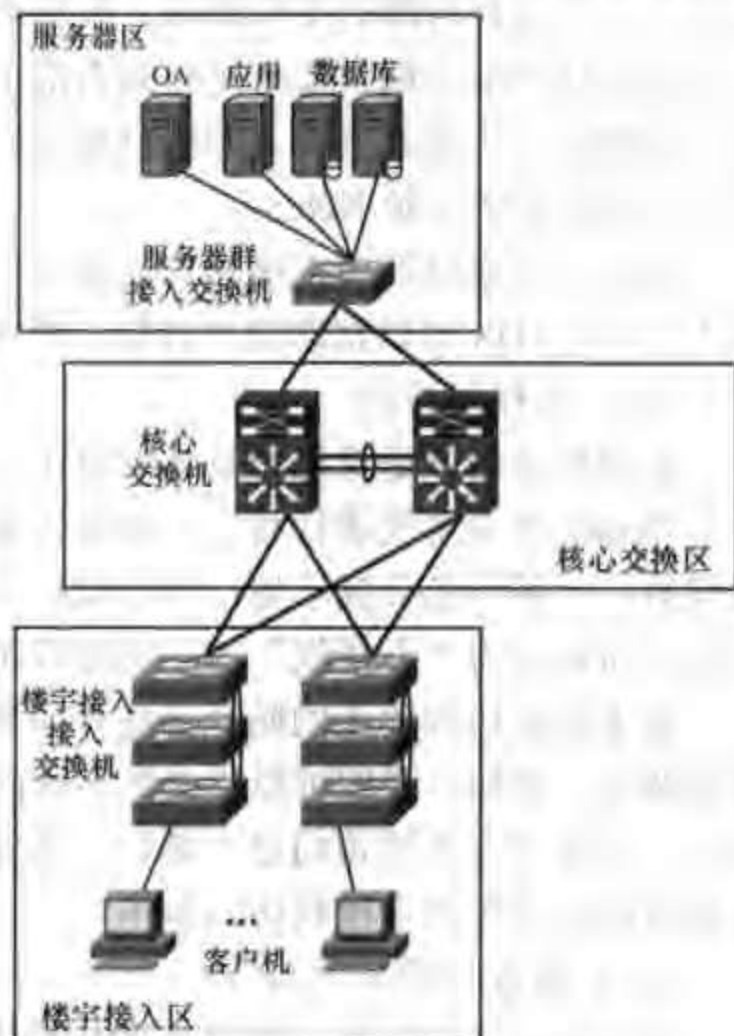


图 9-2 企业网局域网模块

病毒的大量涌现,使我们逐渐认识到用户接入区安全的重要性,比如 Cisco 最近推出的网络准入控制(NAC)就是针对用户接入区的一种安全防护措施。

3. 服务器区

服务器区的主要目的是向最终的用户提供应用服务。在服务器区通常发生的攻击有:数据窃听(Sniff)、IP 欺骗(Spoofing)、密码攻击、应用层攻击、信任关系利用、端口重定向、未授权访问和病毒与特洛伊木马等。

在服务器区通常采用的防护手段有:采用交换架构的设备、采用 RFC2827 地址过滤、采用基于主机的入侵检测系统(HIDS)、采用 PVLAN 保护各服务器、操作系统和应用程序的防护和采用防病毒系统。

从安全角度讲,服务器区是最容易被作为攻击目标的区域。因此在该区域需要设置较多的安全防护手段以缓解各种可能的攻击威胁。在服务器区我们通常采用一台交换机用于各服务器的接入,它可有效地防止数据窃听。同时,我们可以设置 RFC2827 地址过滤用于防止地址欺骗。通过设置基于主机和网络的入侵检测系统我们可以有效地防止密码攻击、应用层攻击、端口重定向以及未授权访问等攻击。另外,PVLAN 的使用使得位于同一 VLAN 的不同服务器之间相互隔离,有效地防止了信任关系利用的攻击。当然,合理设置操作系统和应用程序,定期升级各种安全补丁,以及采用先进的防病毒系统(更重要的是,定期升级病毒库)都可以有效地防止病毒和各种木马程序的侵袭。

9.3.2 广域网模块

企业网的广域网模块如图 9-3 所示。

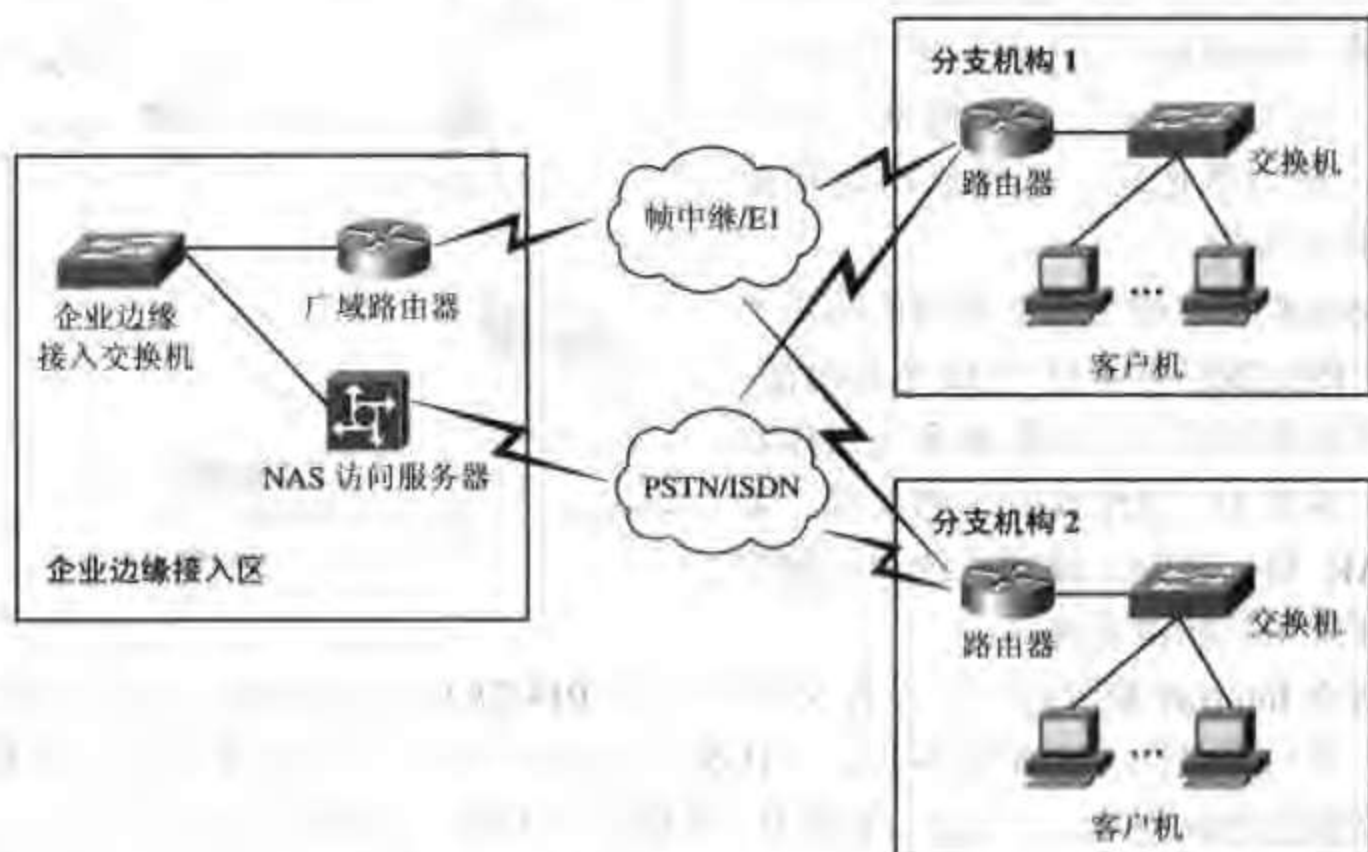


图 9-3 企业网广域网模块

企业网络的广域网模块是通过电信公司的线路构建的一个专属该企业的相对封闭的网络,但由于广域网模块通常会采用 PSTN 或 ISDN 作为其主链路的备份,同时也作为远程接入系统使用,而远程接入系统通常会成为黑客的攻击对象(因为这些设备通常置于防火墙的

后面,一旦黑客通过它们拨号进入接入网络,他们就可假冒授权的网络用户,访问其他内网的资源),由此在该模块我们也需要设置一些安全的防护手段。

在广域网模块通常发生的攻击有:IP 欺骗 (Spoofing)、密码攻击和中间人攻击等。

在广域网模块通常采用的防护手段有:采用 RFC2827 地址过滤、采用一次性密码 (OTP) 和采用数据加密。

为了防止 IP 欺骗的发生,通常在总部和分支的广域网接入路由器上设置 RFC2827 地址过滤。由于广域网是由电信公司提供的链路构成的,身在电信部门的员工是有可能对企业的网络构成中间人攻击的,我们最好对重要的数据进行加密传输,以防止中间人攻击。另外,远程接入部分通常是企业网络安全的软肋,它需要我们特别的防护,通常需要为远程接入的用户单独划分一个 VLAN,同时尽可能采用加密传输(如 IPSec 等)。另外,最好对拨入的电话号码作识别,即采用回拨技术 (Callback),这样使只有经过允许的电话号码才可以拨入。

9.3.3 Internet 接入模块

企业网的 Internet 接入模块如图 9-4 所示。

企业网的 Internet 接入模块为内部用户提供了访问因特网服务的可能,同时使得因特网上的用户能够访问企业对外提供服务的内容。因特网接入区是我们传统意义上认为的最为危险的区域,同时,现有的大多数防护手段也都是针对该区域设置的,比如防火墙和入侵检测系统通常就放置在该区域。

在 Internet 接入模块通常发生的攻击有:IP 欺骗 (Spoofing)、拒绝服务 (DoS)、密码攻击、应用层攻击、网络侦察、信任关系利用、端口重定向、未授权访问和病毒与特洛伊木马等。

在 Internet 接入模块通常采用的防护手段有:采用 RFC2827 和 RFC1918 地址过滤、采用基于主机和网络的入侵检测系统 (HIDS 和 NIDS)、采用 PVLAN 保护各服务器、采用限速 CAR 访问控制、操作系统和应用程序的防护和采用防病毒系统。

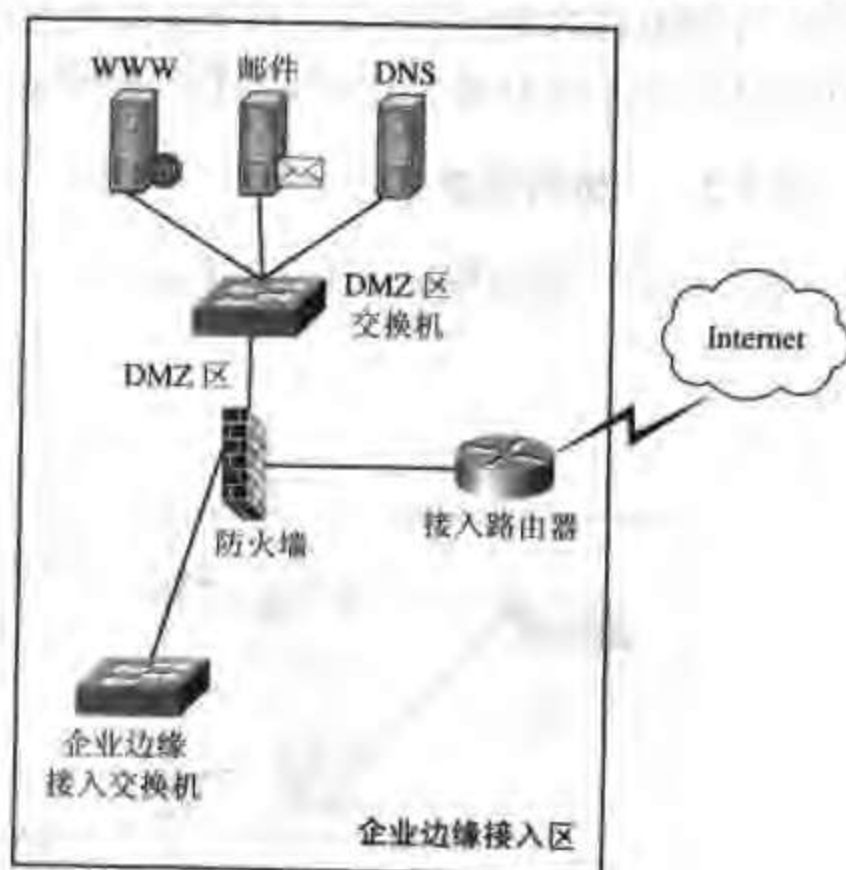


图 9-4 企业网 Internet 接入模块

企业网络 Internet 接入区可以设置 RFC1918 和 RFC2827 地址过滤,这样可以防止地址欺骗的发生,也可有效防止拒绝服务攻击 (DoS) 的发生。同时,对非重要信息流进行速率限制,也可缓解拒绝服务攻击 (DoS) 的威力。在防火墙 DMZ 区域的公共服务器,往往是黑客重点照顾的对象,可以在服务器上安装主机入侵检测系统 (HIDS),能有效地防止密码攻击、应用层攻击、端口重定向以及未授权访问等攻击。另外, PVLAN 的使用使得位于同一 VLAN 的不同服务器之间相互隔离,可有效地防止了信任关系利用的攻击。当然合理设置操作系统和应用程序,定期升级各种安全的补丁,以及采用先进的防病毒系统(更重要的是,定期升级病毒库)都可以有效地防止病毒和各种木马程序的侵袭。

9.4 企业网安全部署案例

通过上面的介绍,读者对在企业网络中进行安全的部署会有一个大致的了解,下面将通过一个具体的例子,介绍一下各种防范措施在企业网络中实现的方法。

本案例中企业网安全部署的情况如图 9-5 所示。

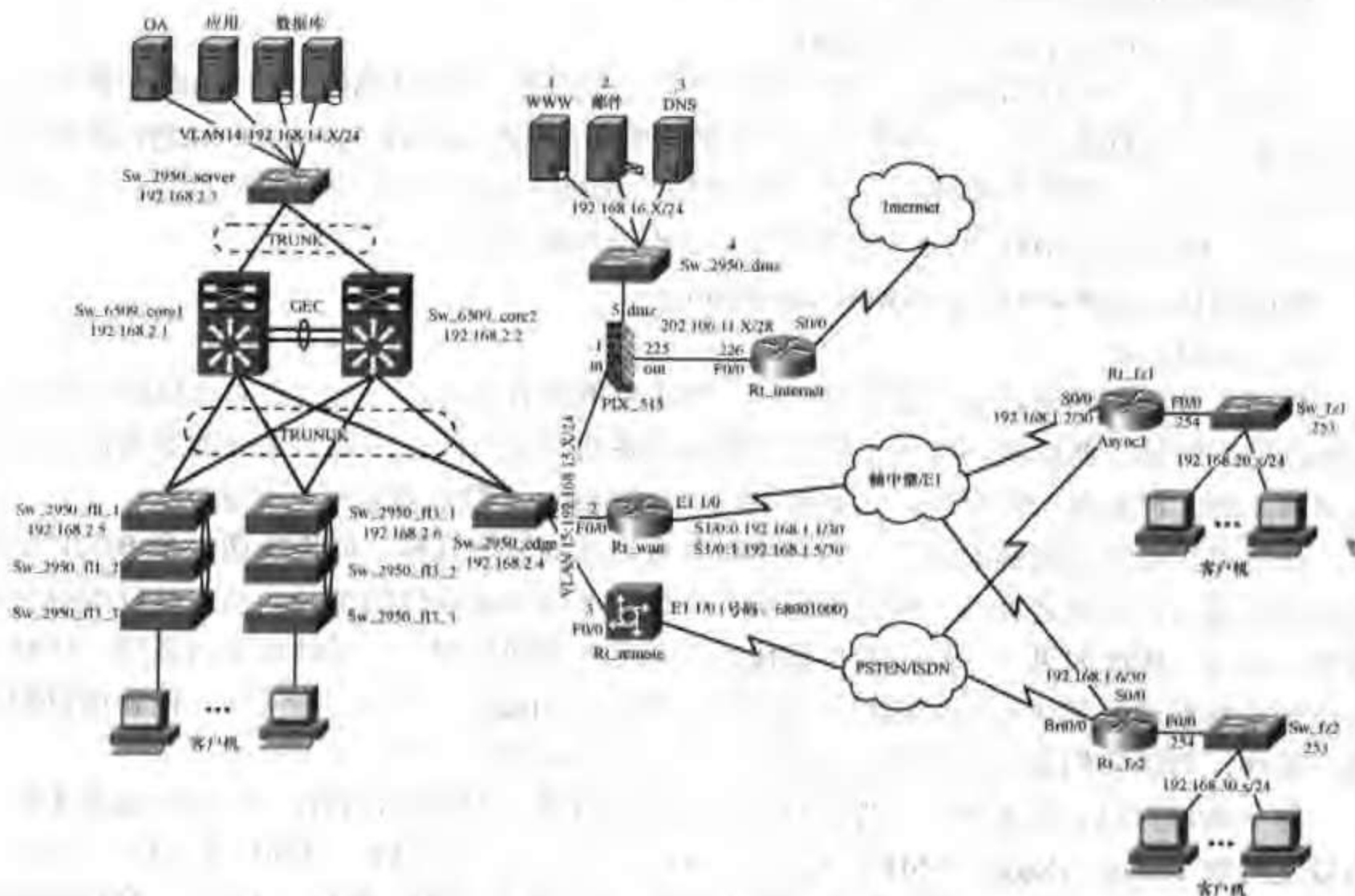


图 9-5 企业网络安全部署案例

9.4.1 网络设备通用安全设置

企业网中常用的网络设备包括交换机、路由器和防火墙。由于防火墙是专用的安全设备,所以它在自身的安全方面的考虑是比较全面的。比如,在默认情况下,它关闭了不必要的网络服务端口,从防火墙外端口是无法 Telnet 到防火墙上的,同时它也不响应 Ping 包,这样避免了许多潜在的攻击。对于交换机和路由器而言,它们的主要作用是进行数据的转发,因此在设备自身的安全性方面考虑的就不是很周全。比如,在默认情况下,交换机和路由器的许多网络服务端口都是打开的,这就等于为黑客预留了进入的通路。下面就来介绍一下如何将交换机和路由器设置得更为安全。

说明:为了方便下面我们以网络设备来特别指代交换机和路由器。

1. 口令管理

口令是用来防止对于网络设备的非授权访问的主要手段,是网络设备本身安全的一部

分。最好的口令处理方法是将这些口令保存在 TACACS+或 RADIUS 认证服务器上。但是通常网络设备会有一个本地口令进行权限访问。这时最好采用如下的方式进行设置:

(1) 使用 enable secret

enable secret 命令用于设定进入系统特权模式的口令。我们最好为其设置一个强壮的密码, 该密码应该不会被字典式攻击轻易破解。还有一点, 就是老的系统采用的是 enable password, 虽然它们的功能相似, 但是 enable password 采用的加密算法比较弱, 最好不要采用。

```
Router(Config)# enable secret iLou_qa09
```

(2) 使用 service password-encryption

这条命令用于对存储在配置文件中的口令和类似数据 (如 CHAP) 进行加密。避免当配置文件被不怀好意者看见, 从而获得这些数据的明文。但是 service password-encryption 的加密算法比较简单, 很容易被破译。这主要是针对 enable password 命令设置的口令。而 enable secret 命令采用的是 MD5 算法, 这种算法是很难进行破译的。

```
Router(Config)# service password-encryption
```

2. 访问控制

任何人登录到网络设备上都能够显示一些重要的配置信息。一个攻击者可以将该设备作为攻击的中转站。所以我们必须正确控制网络设备的登录访问。尽管大部分的登录访问缺省都是禁止的。但是有一些例外, 比如控制端口 (Console) 默认就是允许登录的。

控制端口是非常特殊的端口, 当网络设备重启动的开始几秒, 如果发送一个 Break 信号到控制台端口, 它就会进入一种监控模式, 在这里可以恢复系统的密码, 从而可以很容易控制整个系统。因此如果一个攻击者尽管他没有正常的访问权限, 但是能够重启系统 (切断电源或使系统崩溃) 和访问控制端口 (通过直连终端、Modem、终端服务器), 他就可以控制整个系统, 所以我们必须保证所有连接控制端口的访问的安全性。

除了通过控制台登录外, 另外还有许多登录的方法。根据配置和操作系统版本的不同, 可以支持如 Telnet、rlogin、SSH 以及非基于 IP 的网络协议如 LAT、MOP、X.29 和 V.120 等或者 Modem 拨号。所有这些都涉及到 TTY, 通常本地的异步终端和拨号 Modem 使用标准的“TTY”, 远程的网络连接不管采用什么协议都使用虚拟的 TTY, 即“VTY”。当然, 要控制对网络设备的访问, 最好就是控制这些 TTY 或 VTY, 比如加上一些认证或利用 login、no password 命令禁止访问。

(1) 控制 TTY

在缺省的情况下, 一个远端用户可以连接到一个 TTY, 称为“反向 Telnet”, 它允许远端用户和连接到这个 TTY 上的终端或 Modem 进行交互。但是这些特征允许一个远端用户连接到一个本地的异步终端或一个拨入的 Modem 端口, 从而构造一个假的登录过程来偷盗口令或其他非法活动, 所以最好禁止这项功能。可以采用 transport input none 设置任何异步或 Modem 不接收来自网络用户的连接。如果可能, 不要用相同的 Modem 拨入和拨出, 且禁止反向 Telnet 拨入。路由器有一个 AUX 端口, 该端口可以配置成控制端口, 因此如果不使用该端口, 最好将其设置为禁用。

```
Router(Config)# line aux 0
```

```
Router(Config-line)# transport input none
```



```
Router(Config-line)# no exec
```

(2) 控制 VTY

为了保证安全,任何 VTY 应该仅允许指定的协议建立连接。如一个 VTY 只支持 Telnet 服务,可以如下设置 `transport input telnet`。如果操作系统支持 SSH,最好配置只支持这个协议,避免使用明文传送的 Telnet 服务,采用如下设置: `transport input ssh`。也可以在 VTY 线路模式下,配置 `ip access-class` 来限制访问该 VTY 的 IP 地址范围。因为 VTY 的数目有一定的限制,当所有的 VTY 用完了,就不能再建立远程的网络连接了。这就有可能被利用进行拒绝服务攻击 (DoS)。这时攻击者不必登录进入,只要建立连接,到 login 提示符下就可以,消耗掉所有的 VTY,使得正常访问的用户无法登陆。对于这种攻击的一个好的防御方法就是,利用 `ip access-class` 命令限制最后一个 VTY 的访问地址,使其只向特定管理工作站打开,从而保证管理人员能够远程登录该设备。另一个方法是利用 `exec-timeout` 命令,配置 VTY 的超时。避免一个空闲的任务一直占用 VTY。类似地,也可以用 `service tcp-keepalives-in` 保证 Tcp 建立的进入连接是活动的,从而避免恶意的攻击或远端系统的意外崩溃导致的资源独占。更好的保护 VTY 的方法是关闭所有非基于 IP 的访问,且使用 IPSec 加密所有的远端与该设备的连结。

```
Router(Config)# line vty 0 4
```

```
Router(Config-line)# transport input telnet
```

```
Router(Config-line)# exec-timeout 5 0
```

3. 管理配置

目前,许多大企业的用户都利用基于 SNMP 的网管软件来进行网络的管理,另外,有些初级的用户习惯使用基于 HTTP 的 Web 方式管理网络设备。为此此网络设备必须对这些协议进行配置。

(1) SNMP

SNMP 是最常用的网络管理协议。目前常使用有两个版本 SNMPV1 和 SNMPV2。SNMPV1 存在着很多的安全问题,比如 `community` 字符串使用明文方式等,所以应尽量采用 SNMPV2,因为它采用基于 MD5 的数字认证方式,并且允许对于不同的管理数据进行限制。如果一定要使用 SNMPV1,则要仔细地配置,如避免使用缺省的 `community` 字符串“public”和“private”等,并避免对于每个设备都用相同的 `community`。

```
Router(Config)# snmp-server community Tx_Qbau86 ro
```

```
Router(Config)# snmp-server community Aud06X_qv rw
```

(2) HTTP

Cisco 的网络设备支持通过 Web 方式进行配置和管理,当然我们建议最好不要使用,因为这非常危险,如果选择使用 HTTP 进行管理,最好用 `ip http access-class` 命令限定可以访问的地址范围,且用 `ip http authentication` 命令进行配置认证。

建议禁用 HTTP 服务:

```
Router(Config)# no ip http server
```

4. 日志管理

日志对于网络设备来说是十分重要的,通过它可以了解网络设备运行的状况,如果设备出现故障,可以通过它查询原因。网络设备支持的日志如下所示:

(1) AAA 日志

主要收集关于用户拨入、登录等信息。这些日志信息发送到相应的 TACACS+或 RADIUS 认证服务器上。这些可以用 `aaa accounting` 实现。

```
Router(Config)# aaa new-model
```

```
Router(Config)# aaa authentication login default tacacs+
```

```
Router(Config)# aaa accounting network start-stop tacacs+
```

```
Router(Config)# aaa accounting exec start-stop tacacs+
```

```
Router(Config)# tacacs-server host 192.168.1.54 single
```

```
Router(Config)# tacacs-server key Axui_98pnB
```

(2) SNMP trap 日志

将系统状态的改变发送到 SNMP 管理工作站。

(3) 系统日志

根据配置记录大量的系统事件，并可以将这些日志发送到下列地方：控制台端口、Syslog 服务器、TTY 或 VTY、本地的日志缓存等。

我们这里最关心的就是系统日志，缺省的情况下，这些日志被送到控制台端口，通过控制台监视器来观察系统的运行情况，但是这种方式信息量小且无法记录下来供以后查看。最好是使用 syslog 服务器，将日志信息送到这个服务器保存下来。

5. 服务管理

网络设备通常都提供很多的服务如 Finger、Telnet 等，但是这些服务中有一些能够被攻击者利用，所以最好禁止所有不需要的服务。

(1) TCP 和 UDP 的小服务

Cisco 的网络设备提供一些基于 TCP 和 UDP 的小服务，如 echo、chargen 和 discard 等。这些服务很少被使用，而且容易被攻击者利用来越过分组过滤机制。如 echo 服务，就可以被攻击者利用进行数据分组的发送，看起来好像这些数据分组来自该设备本身，所以最好禁止这些服务。可以利用 `no service tcp-small-servers` 和 `no service udp-small-servers` 命令来实现。

```
Router(Config)# no service tcp-small-servers
```

```
Router(Config)# no service udp-small-servers
```

(2) Finger、NTP、CDP

Finger 服务可能被攻击者利用来查找用户和口令并进行攻击。NTP 不是十分危险的，但是如果没有一个很好的认证，则会影响设备的正确时间，导致日志和其他任务出错。CDP 可能被攻击者利用来获取网络设备的版本等信息，从而进行攻击。所以对于上面的几种服务如果没有十分的需求，最好禁用它们。可以用 `no service finger`、`no ntp enable`、`no cdp running`（或 `no cdp enable`）来实现。

```
Router(Config)#no cdp run
```

```
Router(Config-if)# no cdp enable
```

```
Router(Config-if)# no ntp
```

```
Router(Config)# no ip finger
```



```
Router(Config)# no service finger
```

6. 其他服务

除了上面介绍的一些安全设置之外，还有一些设置需要我们注意：

(1) 最好禁止 BOOTP 服务

```
Router(Config)# no ip bootp server
```

(2) 最好禁止从网络启动和自动从网络下载初始配置文件

```
Router(Config)# no boot network
```

```
Router(Config)# no servic config
```

(3) 最好禁止 IP Source Routing

```
Router(Config)# no ip source-route
```

(4) 建议如果不需要 ARP-Proxy 服务最好禁止它

```
Router(Config)# no ip proxy-arp
```

```
Router(Config-if)# no ip proxy-arp
```

(5) 最好禁止 IP Directed Broadcast

```
Router(Config)# no ip directed-broadcast
```

(6) 最好禁止 IP Classless

```
Router(Config)# no ip classless
```

(7) 最好禁止 ICMP 的 IP Unreachables, Redirects, Mask Replies

```
Router(Config-if)# no ip unreachable
```

```
Router(Config-if)# no ip redirects
```

```
Router(Config-if)# no ip mask-reply
```

(8) 如果没必要则禁止 WINS 和 DNS 服务

```
Router(Config)# no ip domain-lookup
```

(9) 最好明确禁止不使用的端口。

```
Router(Config)# interface fa0/5
```

```
Router(Config)# shutdown
```

通过上面的配置，我们就可以实现一个网络设备的基本的安全。下面我们给出对于使用 IOS 操作系统的 Cisco 路由器和交换机设备的通用的一个安全配置文档，当然它只针对设备本身的安全，并不包括针对具体应用所设的功能性配置。读者可以把这段配置稍加修改（如密码和 IP 地址等）用到自己的网络设备中，当然前提条件是要对它的作用有所了解。

！ 关闭不必要的服务

！

```
no ip domain-lookup
```

```
no cdp run
```

```
no ip http server
```

```
no ip source-route
```

```
no service finger
```

```
no ip bootp server
```



```
no ntp
no service udp-small-servers
no service tcp-small-servers
!
!启用日志和网管
!
service timestamp log datetime localtime
logging 192.168.2.250
snmp-server community bWxo_TaQ3M ro
!
!设置口令和访问控制
!
service password-encryption
enable secret z90kl_nzq
no enable password
no access-list 20
access-list 20 permit 192.168.2.0 0.0.0.255
access-list 20 deny any log
no access-list 21
access-list 21 permit host 192.168.2.250
access-list 21 deny any log
line vty 0 4
transport input telnet
access-class 20 in
login
password 0 XT98typ_76
exec-timeout 5 0
line con 0
login
password 0 XtyCGH_oiu
exec-timeout 5 0
line aux 0
transport input none
password 0 Wfty76_P0k
no exec
exit
banner motd #
This is a private system, unauthorized access is prohibited.
#
```


9.4.2 局域网模块

这里我们以第 7 章中介绍的一个案例为基础，介绍我们的安全设置。对局域网模块我们分成核心交换区、楼宇接入区和服务器区分别进行介绍。

1. 核心交换区

在核心交换机 Sw_6509_core1 和 Sw_6509_core2 上我们进行了相应的 VLAN 设置，见表 9-1 和表 9-2。

表 9-1 核心交换机 1 (Sw_6509_core1)

部 门	VLAN 名	VLAN ID	网关地址	网段地址
管理	manage	2	192.168.2.252	192.168.10.0/24
财务部	finance	11	192.168.11.252	192.168.11.0/24
技术部	techniqy	12	192.168.12.252	192.168.12.0/24
销售部	sales	13	192.168.13.252	192.168.13.0/24
服务器	server	14	192.168.14.252	192.168.14.0/24
边界	edge	15	192.168.15.252	192.168.15.0/24

表 9-2 核心交换机 2 (Sw_6509_core2)

部 门	VLAN 名	VLAN ID	网关地址	网段地址
管理	manage	2	192.168.2.253	192.168.10.0/24
财务部	finance	11	192.168.11.253	192.168.11.0/24
技术部	techniqy	12	192.168.12.253	192.168.12.0/24
销售部	sales	13	192.168.13.253	192.168.13.0/24
服务器	server	14	192.168.14.253	192.168.14.0/24
边界	edge	15	192.168.15.253	192.168.15.0/24

在核心交换机上，我们应该在这些 VLAN 的接口上配置 RFC2827 地址过滤，即一个 VLAN 接口应该只允许本 VLAN 的数据发出。例如，技术部的网段是 192.168.12.0/24，我们就应该在核心交换机上 VLAN12 的接口下配置访问控制列表，使得只有源地址属于 192.168.12.0/24 网段的数据才能通过核心交换机进行转发，这样可以有效地防止地址欺骗攻击的发生。下面我们给出具体的配置（两台核心交换机的配置相同）：

```
!  
interface Vlan2  
ip access-group 102 in  
!  
interface Vlan11  
ip access-group 111 in  
!  
interface Vlan12  
ip access-group 112 in  
!
```



```
interface Vlan13
ip access-group 113 in
!
interface Vlan14
ip access-group 114 in
!
interface Vlan15
ip access-group 115 in
!
access-list 102 permit ip 192.168.2.0 0.0.0.255 any
access-list 102 deny ip any any log
access-list 111 permit ip 192.168.2.0 0.0.0.255 any
access-list 111 deny ip any any log
access-list 112 permit ip 192.168.2.0 0.0.0.255 any
access-list 112 deny ip any any log
access-list 113 permit ip 192.168.2.0 0.0.0.255 any
access-list 113 deny ip any any log
access-list 114 permit ip 192.168.2.0 0.0.0.255 any
access-list 114 deny ip any any log
access-list 115 permit ip 192.168.2.0 0.0.0.255 any
access-list 115 deny ip any any log
```

2. 楼宇接入区

对于楼宇接入区，可以设置的安全方面的选项主要有端口绑定（MAC 地址和端口绑定）和 802.1x 认证。

（1）端口绑定

在需要作端口绑定的端口下（这里假设是 fa0/1），可以作如下配置：

```
int fa0/1
switchport mode access
switchport port--security
switchport port--security violation protect
```

（2）802.1x 认证

在需要作 802.1x 认证的交换机上，可以作如下配置：

```
aaa new-model
aaa authentication dot1x default group radius
radius-server host 192.168.2.111 auth-port 1812 key jkelhop
```

（192.168.2.111 指认证服务器的地址）

在需要配置认证的端口下配置 802.1x 选项，在这里，假设 fa0/1 端口需要认证

```
int fa0/1
dot1x port-control auto
```


3. 服务器区

在服务器区，为了防止黑客攻击了一台服务器后再攻击其他的服务器，最好将各个服务器进行隔离。由于它们同属一个 VLAN，为了实现隔离，需要用到 PVLAN。需要注意的是，在 Cisco 的低端交换机上并不支持 PVLAN（从 Catalyst3750 开始才支持），为了实现隔离，需要用到端口保护功能，它可以实现同一交换机上的被保护端口之间相互隔离。在本案例中，我们选用的是 Catalyst2950 交换机，因此可以设置端口保护来实现服务器之间的隔离，具体配置如下：

```
int fa0/1
  switchport protected
int fa0/2
  switchport protected
int fa0/3
  switchport protected
```

这里，假设交换机的 fa0/1、fa0/2 和 fa0/3 端口连接的服务器之间需要相互隔离。

9.4.3 广域网模块

在总部和分支机构的广域网路由器上，我们应该配置 RFC2827 地址过滤，即总部路由器（Rt_wan）的局域网接口（fa0/0）应该只允许企业拥有的网段数据（192.168.2.0/24、192.168.11.0/24、192.168.12.0/24、192.168.13.0/24、192.168.14.0/24、192.168.15.0/24）的进入，而广域网口应该只允许相应分支机构（分支 1：192.168.20.0/24，分支 2：192.168.30.0/24）的网段数据的进入。另外，分支机构的路由器（Rt_fz1、Rt_fz2）的广域网口应该只允许总部网段数据的进入，而局域网口应只允许本分支机构网段数据的进入。下面给出具体的配置（两台核心交换机的配置相同）：以下配置具体介绍了 WAN 模块中路由器上的接入控制：

```
Rt_wan:
!
interface fa0/0
ip access-group 150 in
!
interface Serial 1/0:0
ip access-group 120 in
!
interface Serial 1/0:1
ip access-group 130 in
!
access-list 150 permit ip 192.168.2.0 0.0.0.255 any
access-list 150 permit ip 192.168.11.0 0.0.0.255 any
access-list 150 permit ip 192.168.12.0 0.0.0.255 any
access-list 150 permit ip 192.168.13.0 0.0.0.255 any
access-list 150 permit ip 192.168.14.0 0.0.0.255 any
```



```
access-list 150 permit ip 192.168.15.0 0.0.0.255 any
access-list 150 deny ip any any log
!
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
access-list 120 deny ip any any log
!
access-list 130 permit ip 192.168.30.0 0.0.0.255 any
access-list 130 deny ip any any log
!
Rt_fz1:
!
interface fa0/0
ip access-group 120 in
!
interface Serial 0/0
ip access-group 150 in
!
access-list 150 permit ip 192.168.2.0 0.0.0.255 any
access-list 150 permit ip 192.168.11.0 0.0.0.255 any
access-list 150 permit ip 192.168.12.0 0.0.0.255 any
access-list 150 permit ip 192.168.13.0 0.0.0.255 any
access-list 150 permit ip 192.168.14.0 0.0.0.255 any
access-list 150 permit ip 192.168.15.0 0.0.0.255 any
access-list 150 deny ip any any log
!
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
access-list 120 deny ip any any log
!
Rt_fz2:
!
interface fa0/0
ip access-group 130 in
!
interface Serial 0/0
ip access-group 150 in
!
access-list 150 permit ip 192.168.2.0 0.0.0.255 any
access-list 150 permit ip 192.168.11.0 0.0.0.255 any
```



```

access-list 150 permit ip 192.168.12.0 0.0.0.255 any
access-list 150 permit ip 192.168.13.0 0.0.0.255 any
access-list 150 permit ip 192.168.14.0 0.0.0.255 any
access-list 150 permit ip 192.168.15.0 0.0.0.255 any
access-list 150 deny ip any any log
!
access-list 130 permit ip 192.168.30.0 0.0.0.255 any
access-list 130 deny ip any any log
!

```

9.4.4 Internet 接入模块

在 Internet 接入路由器 (Rt_internet) 上, 应该设置 RFC1918 和 RFC2827 地址过滤, 即它的广域网口 (S0/0) 应该只允许 ISP 分配给企业的网段地址 (202.16.11.224/28) 数据的送出, 同时应禁止源地址是私有地址的数据分组从广域网口进入。这样可以防止地址欺骗的发生, 也可有效防止拒绝服务攻击 (DoS) 的发生。同时, 对非重要信息流进行速率限制 (如 CAR), 也可缓解拒绝服务攻击 (DoS) 的威力。在防火墙 DMZ 区域的公共服务器, 往往是黑客重点照顾的对象, 我们需要在 DMZ 区的交换机上配置 PVLAN, 使用使得位于同一 VLAN 的不同服务器之间相互隔离, 这样可以有效地防止信任关系利用的攻击。下面将分别对这几个方面进行说明。

1. 采用 RFC2827 和 RFC1918 地址过滤

```

!
interface Serial 0/0
ip access-group 160 in
ip access-group 170 out
!
access-list 160 deny ip 192.168.0.0 0.0.0.255 any log
access-list 160 deny ip 172.16.0.0 0.15.255.255 any log
access-list 160 deny ip 10.0.0.0 0.255.255.255 any log
access-list 160 permit ip any any
!
access-list 170 permit ip 202.16.11.224 0.0.0.15 any log
access-list 170 deny ip any any

```

2. 采用限速 CAR 访问控制

我们应该在 Internet 接入路由器上使用 CAR (Control Access Rate) 来对 ICMP 数据分组的流量进行速率限制, 其配置如下:

```

!
interface Serial 0/0
rate-limit output access-group 180 128000 8000 8000 conform-action transmit exceed-action drop
!

```



```
access-list 180 permit icmp any any echo
access-list 180 permit icmp any any echo-reply
!
```

3. 采用 PVLAN 保护各服务器

在防火墙的 DMZ 区放置着企业对外提供服务的一些服务器，为了防止黑客攻击了一台服务器后再攻击其他的服务器，我们最好将各个服务器进行隔离。和局域网模块的服务器区一样，可以采用端口保护的方式来在 Catalyst2950 交换机上实现服务器之间的隔离，具体配置如下：

```
int fa0/1
  switchport protected
int fa0/2
  switchport protected
int fa0/3
  switchport protected
```

这里，假设交换机的 fa0/1、fa0/2 和 fa0/3 端口连接的服务器之间需要相互隔离。

4. 其他防护手段

除了上面介绍的一些防护手段外，如果我们的路由器的性能足够好（访问控制会消耗系统资源），还可以对来自 Internet 的数据进行进一步的过滤。比如，除了 RFC1918 和 RFC2827 地址过滤外，还可以将回环地址（127.0.0.0/8）、DHCP 自定义地址（169.254.0.0/16）、全网络地址（0.0.0.0/8）过滤掉。

```
!
interface Serial 0/0
  ip access-group 160 in
!
access-list 160 deny ip 127.0.0.0 0.255.255.255 any log
access-list 160 deny ip 169.254.0.0 0.0.255.255 any log
access-list 160 deny ip 0.0.0.0 0.255.255.255 any log
access-list 160 permit ip any any
```

另外，还可以对一些已知的攻击类型数据分组进行过滤：

```
!
interface Serial 0/0
ip access-group 160 in
!
```

过滤 TRINOO DDoS 攻击

```
access-list 160 deny tcp any any eq 27665 log
access-list 160 deny ndp any any eq 31335 log
access-list 160 deny udp any any eq 27444 log
```

过滤 Stacheldtraht DDoS 攻击


```
access-list 160 deny tcp any any eq 16660 log
access-list 160 deny tcp any any eq 65000 log
! 过滤 TrinityV3 攻击
access-list 160 deny tcp any any eq 33270 log
access-list 160 deny tcp any any eq 39168 log
! 过滤 SubSeven DDoS 攻击
access-list 160 deny tcp any any range 6711 6712 log
access-list 160 deny tcp any any eq 6776 log
access-list 160 deny tcp any any eq 6669 log
access-list 160 deny tcp any any eq 2222 log
access-list 160 deny tcp any any eq 7000 log
access-list 160 permit ip any any
```

9.5 小 结

本章我们对如何构建一个安全的企业网进行了介绍。首先，通过对各种攻击手段的分析，使读者了解了企业网络所面对的种种潜在的安全风险，然后有针对性地介绍了如何在企业网的各个区域进行安全的部署。最后，我们通过一个具体的实例，说明如何将各种防护手段落实到企业网的 Cisco 设备上。

第 10 章 企业网故障诊断与排除

本章将涵盖下列有关企业网故障诊断与排除方面的关键主题

- 系统化排错方法
- 分层排错思想
- 常用 IP 排错工具
- TCP/IP 连通故障排除
- 链路层故障排除
- 网络层故障排除
- Cisco 故障诊断和排除资源

目标：通过对本章的学习，希望读者对以下一些方面的内容有所了解：

- (1) 如何进行有效的排错；
- (2) 常见的链路层和网络层故障及其排除方法；
- (3) 我们有哪些常用的排错工具；
- (4) Cisco 提供给我们哪些可利用的排错的资源。

10.1 简介

今天的因特网是极其复杂的，无论其形式还是内容都在不断的变化，而且目前越来越多的机构将其业务系统放到网络上运行（比如银行的结算、证券的行情交易、铁路的售票等等）。这就使得许多工作都依赖于网络服务的有效性，一旦网络瘫痪，就可能意味着损失大量的变金，甚至可能导致公司的破产。

尽管我们非常了解目前网络所起的重要作用，尽管我们非常努力，同时也非常尽职尽责地进行了网络的设计和建设，但是网络实在是变化太快，因此许多问题还是会出乎于我们的想像而出现。这时，我们所希望的是在出现故障后能快速地定位故障点并让网络恢复正常工作。本章我们将学习这方面的知识。

10.2 系统化排错方法

面对复杂的网络状况，网络支持人员经常是在极大的压力下去发现和解决问题。当然，如果能很轻松地知道故障的原因并能很快解决它，那自然是好事。但是，很多时候事情并非是这样。因此，必须部署一种能够排除不同可能性并一步一步地朝问题的真实原因前进的技

术。这种技术可确保永远取得进展而不陷入循环或困惑之中。最终,有关人员或者可以确认什么被破坏、失效或被错误地配置,或者能够形成一个所做工作及发现情况的报告,并将此报告提交给那些能够运用这些信息进行进一步故障排除工作的人。最重要的是,不管是否解决了问题都不要浪费自己或他人的时间。不管是否解决了问题,所做的工作都是有意义的。

目前来看,一个普遍被接受的故障排除模型如图 10-1 所示,该模型反映了一个故障排除的基本流程。

根据图 10-1,我们了解到系统化的排错方法包括了以下几方面的内容:

- 定义问题;
- 收集事实;
- 考虑可能性;
- 建立行动计划;
- 执行行动计划;
- 观察结果;
- 重复过程;
- 记载事实。

下面对这些内容分别进行介绍。

(1) 定义问题

定义问题是根据相互关联的故障现象以及可能的故障原因对问题进行清楚地说明。如果网络原来有基准的信息,可在说明中参考。通常在定义问题时,需要给出故障现象的详细描述。

(2) 收集事实

收集事实是根据相关的故障现象采集尽可能多的有用的信息。这包括故障前、后网络设备以及其他相关设备的改动情况,在这一过程中往往需要用到一些检测的工具,如 ping, traceroute, show 等常用的命令,以及协议分析软件和网管软件等。

(3) 考虑可能性

考虑可能性是利用收集到的各种信息结合故障现象尽可能排除不可能的因素,从而缩小排错的范围。在该步骤中,我们还需要对剩下的一些可能导致故障的因素按其可能性进行排序。

(4) 建立行动计划

建立行动计划是指根据上一步当中对可能因素的排序,依次对各种可能因素设计相应的排错方案。在建立行动计划的时候切记一次不要修改太多的内容,尽可能做到一次只修改一项内容。这样,如果在排错过程中出现意外(如引入了新的故障),便于我们恢复至原来的状态。

(5) 执行行动计划

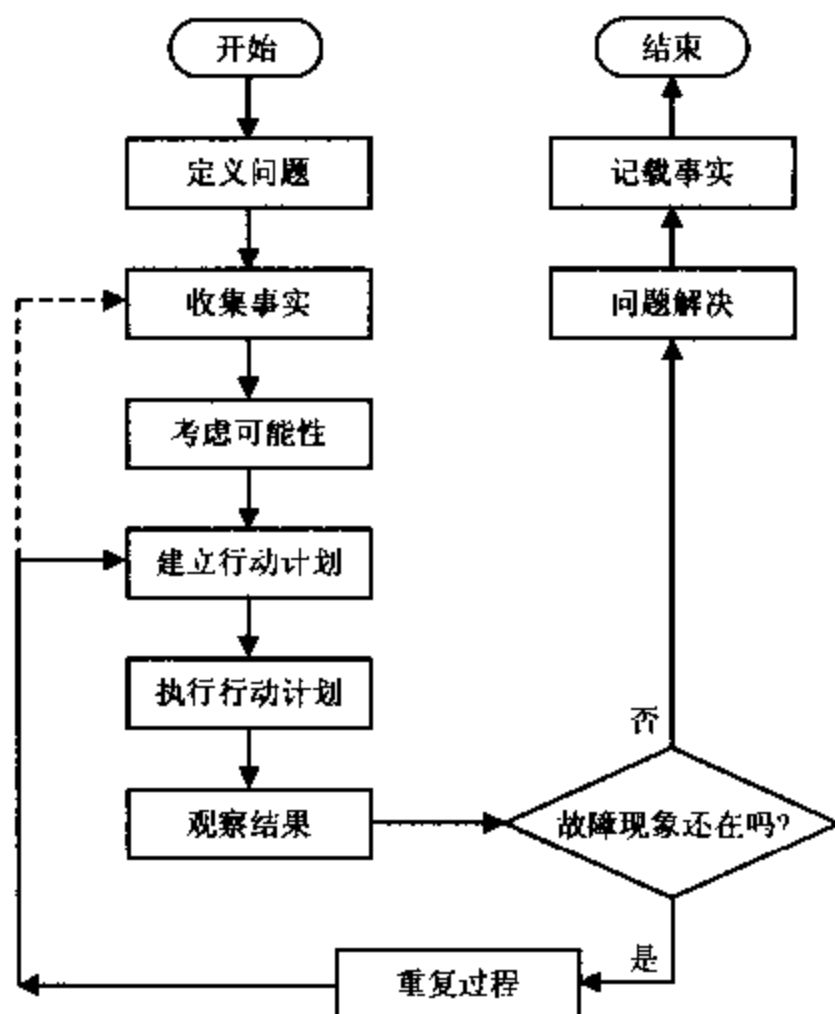


图 10-1 系统化排错方法模型

执行行动计划是指依据对可能导致故障的因素的排序，依次执行在上一步当中制定的针对该因素的行动计划。在该步骤中要牢记一次只修改一项内容的原则。

(6) 观察结果

在执行完上述的任何一个动作后，都要观察其产生的结果。如果故障消失且没有引入新的问题，就进入记载事实阶段；如果故障依然存在，就需要依据行动计划采取下一步行动。当然在采取新的行动之前，必须决定是否保留上一步采取的行动。

(7) 重复过程

重复过程是指依据对可能导致故障的因素的排序，不断地重复执行第(5)和(6)步直至问题解决。如果所有行动计划执行完后，问题依然存在，这时就需要重新回到第(3)步，考虑其他的可能因素，并由此制定新的行动计划、执行新的行动计划、观察结果如此反复直至问题解决。

(8) 记载事实

记载事实是指当故障排除之后，记载所做的工作。许多工程师对这一步的重要性都认识不够，往往是问题一解决，所有的事情都丢到脑后。其实，建立一个记录详细、完整的排错案例知识库，会节约自己和其他人大量的时间和精力，它的意义往往超过排错本身。

总之，系统化的排错方法就是指从故障现象出发，以各种手段收集尽可能多的信息，确定可能的故障点，制定各种排错的计划并依次执行，直至排除故障，恢复网络的正常运行。

10.3 分层排错思想

上面介绍了系统化的排错方法，应该说它是指导我们有效地进行排错的纲领。但仅仅有纲领还是不够的，还需要具体的方法。下面就来介绍在网络排错中非常重要的分层排错思想。

在前面的网络技术基础一章，我们介绍过网络通信协议的 ISO 参考模型，同时介绍了将通信协议分层有利于实现标准化、降低开发和学习的复杂性，也有利于通信的排错。这就好比制造业的生产线一样。比如汽车的生产非常复杂，如果我们不对其进行模块（工序）划分，那将非常困难，效率也会非常低。现在的一条汽车生产线往往划分为非常多的工序，每道工序只承担非常单一的任务（比如上螺丝），这样每道工序需要的技能比较单一，工作效率可以大幅度地提高，同时如果出错也很容易定位和解决。

OSI 参考模型可参见本书图 1-14。

(1) 物理层的故障主要表现在设备的物理连接方式是否恰当；连接电缆是否正确；Modem、CSU/DSU 等设备的配置及操作是否正确。确定路由器端口物理连接是否完好的最佳方法是使用 `show interface` 命令，检查每个端口的状态，解释屏幕输出信息，查看端口状态、协议建立状态等。

(2) 查找和排除数据链路层的故障，需要查看路由器的配置，检查连接端口的共享同一数据链路层的封装情况。每对接口要和与其通信的其他设备有相同的封装。通过查看路由器的配置检查其封装，或者使用 `show` 命令查看相应接口的封装情况。

(3) 排除网络层故障的基本方法是：沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址。如果路由没有在路由表中出现，应该通过检查来确定是否已经输

入适当的静态路由、默认路由或者动态路由。然后手工配置一些丢失的路由,或者排除一些动态路由选择过程的故障。

在排除比较复杂网络的故障时,我们常常需要从不同的角度来测试和分析故障的现象,以确定故障点,根据网络的七层结构的定义和功能逐一地进行分析和排查,这是传统的而且最基础的分析和测试方法。当然,在具体应用分层思想的时候会有不同的思路,我们可以采用自下而上也可以采用自上而下的方法。自下而上是指从物理层开始检测直到应用层;自上而下是指从应用协议中扑捉数据分组,分析数据分组统计和流量统计信息以获得有价值的资料。但根据我们的实践经验,最为有效的方法是,先检测网络层,然后根据网络层的状况向上或向下进行排查。这是因为网络层的 ping 和 traceroute 工具可以方便地测试网络的连通性。比如网络中的主机 PC_A 要访问主机 PC_B 的共享文件夹,如果不能正常访问,那么我们首先用 ping 命令来测试 PC_A 和 PC_B 之间的网络层连通性。如果网络层不通,那么我们就只需要针对下三层进行排查;而如果网络层是通的,那么我们才需要针对网络的上面几层进行排查。下面我们通过一个例子来说明:



图 10-2 PC_A 希望访问 PC_B

(1) PC_A 要访问 PC_B 的共享文件,在地址

栏输入“\\192.168.1.2”(192.168.1.2 是 PC_B 的 IP 地址),如图 10-2 所示。

(2) PC_A 收到如图 10-3 所示的错误信息,该信息表明 PC_A 不能正常访问 PC_B 的共享资源。下面我们第一步要做的就是测试两主机的网络层连通性。



图 10-3 错误提示

(3) PC_A 在 DOS 命令行运行“ping 192.168.1.2”命令,收到如图 10-4 所示的信息。根据该信息提示,我们可知 PC_A 和 PC_B 在网络层是不通的。由此,我们将排错的目标锁定在网络的下三层(物理层、链路层、网络层)。



图 10-4 运行 ping 命令及其返回的提示

10.4 IP 排错工具

用于 IP 排错的工具有许多,其中在主机上常用的命令包括用于测试连通性的 ping、tracert 命令,用于 arp 查询的 arp -a 命令,用于路由表查询 netstat -rn 命令和用于 DNS 查询的 nslookup 命令等;在 Cisco 设备上常用命令包括用于测试连通性的 ping、traceroute 命令,用于各种状态查询的 show 命令和用于监控的 debug 命令。除了上面这些操作系统内置的命令外,还有一些专用的工具可用于排错,比如用于数据分组分析的协议分析工具(如 NAI Snifferpro 和 WildPackets EtherPeek),另外还包括各种网络管理工具(如 CiscoWorks2000)。

在所有的排错工具中, ping 和 traceroute 是使用范围最广的两个命令,在几乎所有的操作系统里都内置了 ping 命令,同时,很多的操作系统也内置了 traceroute 命令(注意:在 Windows2000 操作系统里该命令是 tracert)。下面我们就对排错中常用的 ping、traceroute、show、debug 等命令进行详细介绍。

1. ping 命令

ping 是最常使用的故障诊断与排除命令。它由一组 ICMP 回应请求(Echo Request)报文组成,如果网络正常运行,将返回一组回应应答(Echo Reply)报文。ICMP 消息以 IP 数据分组的形式传输,因此接收到 ICMP 回应应答消息能够表明第三层(网络层)以下的连接都工作正常。

ping 命令实际上是向目标 IP 地址发送若干(缺省为 4 个)数据分组,如果本地 IP 地址与目标 IP 地址之间能够连通,目标地址将回复一条响应信息,如图 10-5 所示。响应信息包括响应时间和 TTL 值。



图 10-5 用 ping 命令检查网络层及以下层的连接

说明:

① 不同操作系统默认发送的数据分组的字节数和 TTL 值会有所不同,Windows2000 默认字节数是 32, TTL 值是 128;

② 响应时间低于 300ms 都被认为是正常的,而时间超过 400ms 时,则认为网络速度较慢;

③ 出于安全的原因,目前许多互联网上的设备都禁止 ping,因此不能完全根据 ping 的结果来作网络通断的定论。

在确认网络连通性的时候,我们通常会按照以下顺序进行 ping 的测试:

(1) ping 本地循环地址 127.0.0.1,确定本地 TCP/IP 配置是否正确。在命令提示行键入 ping 127.0.0.1,如果能够正常回应,如图 10-6 所示,这说明本地的 TCP/IP 协议运行是正常的。



图 10-6 运行 ping 127.0.0.1 及其响应

(2) ping 本机地址,检验本地 IP 地址设置是否正确。

(3) ping 缺省网关地址,检验能否与本地子网之外的主机进行通信。

(4) ping 远程子网上的目标地址,检验能否和目标地址远程通信。

如果以上 ping 命令均能够得到响应,说明 TCP/IP 配置能够支持网络通信。否则,针对相应的返回信息进行相应的设置检查。



图 10-7 运行 ping 命令及返回的超时信息

如果收到超时信息,即出现“请求暂停”(Request Time Out)信息,如图 10-7 所示,则

意味着目标地址没有在 1s 内响应。这说明本地 IP 地址与目标 IP 地址之间的 TCP/IP 连接不能建立，可能的原因包括目标 IP 地址不可用、网络故障、协议错误以及 TCP/IP 配置错误等。

如果收到目标不可达信息，即出现“Destination host unreachable”信息，如图 10-8 所示，则意味着本地没有目标的路由，可以用 netstat -rn 命令来查看本地路由表来验证。



图 10-8 运行 ping 命令及返回的目标不可达信息

具体在应用 ping 命令的时候，我们可以跟一些参数，通过这些参数来方便地进行各种测试。比如可以通过 ping -l 命令改变发送的数据分组的字节数来测试与 MTU 相关的网络故障，如图 10-9 所示是 ping 命令可用的一些参数和相应的说明。



图 10-9 ping 命令可用的参数及其说明

Cisco IOS 内置的 ping 命令不但支持 IP，而且支持大多数其他的桌面协议，如 IPX 和 AppleTalk 协议。IOS 的 ping 命令和主机系统的 ping 命令略有不同，IOS 的 ping 命令默认会发送回 5 个回应请求（Echo Request），5 个惊叹号（!）表明所有的请求都成功地接收到了响应（Echo Reply）。输出中还包括最大、最小和平均往返时间等信息。ping 的返回信息见表 10-1。

表 10-1

ping 命令返回的信息

状 态	说 明	原 因
!	收到 ICMP Echo Reply 信息	响应成功
.	请求超时	ping 测试包被防火墙或 ACL 阻断; ping 测试包到目标系统途经的路由器没有到目标的路由, 同时它没有发送 ICMP 目标不可达信息 (Destination Unreachable); ping 测试包到目标系统的路途中存在物理连接问题;
U	收到 ICMP Destination Unreachable 信息	ping 测试包到目标系统途经的路由器没有到目标的路由, 同时它没有发送 ICMP 目标不可达信息 (Destination Unreachable)
C	收到 ICMP Source Quench 信息	ping 测试包到目标系统途经的路由器或者目标系统本身收到过多的数据包, 需要检查相应设备的入口队列
&	收到 ICMP Time Exceeded 信息	ping 测试包到目标地址间可能存在路由循环

在 IOS 的特权模式下, 我们可以运行扩展的 ping 命令来实现更多的功能。扩展的 ping 命令的执行方式是在特权模式下直接键入 ping, 然后根据提示修改各种不同的属性。扩展 ping 的使用方法如下:

```
Router#ping
Protocol [ip]:
Target IP address: 192.168.1.2
Repeat count [5]: 10
Datagram size [100]: 1800
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 10, 1600-byte ICMP Echoes to 192.168.1.2, timeout is 2 seconds:
!!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 36/39/48 ms
```

首先我们介绍特权模式下的 ping 的各种可用属性。每种属性的缺省值在方括号中显示。

Protocol: 表示需要测试的协议, 默认是 IP 协议;

Target address: 表示该测试数据分组要到达的目标地址;

Repeat count: 表示 ping 重复的次数;

Datagram size: 表示该测试数据分组的长度, IOS 默认是 100 字节。如果怀疑数据分组由于延迟过长或者分段失败而丢失, 我们就可以提高数据分组的大小来进行相应的测试。例如, 这里我们使用 1800 字节的数据分组测试;

Timeout: 如果怀疑超时是由于响应过慢而不是报文丢失, 则可以提高该值;

Extended commands: 回答“y”以获得扩展属性;

Source address: 表示发出此测试数据分组的源地址;

Type of service: 根据 RFC 791 TOS 规定的属性, 通常缺省值为 0;

Set DF bit in IP header?: 通过设置 DF 位禁止分段, 即使是报文超过了定义的 MTU 也禁止分段;

Data pattern [0xABCD]: 通过改变数据模式可以测试线路的噪声;

Loose, Strict, Record, Timestamp, Verbose[none]: 这些都是 IP 报文头的属性。一般只使用 Record 属性和 Verbose, 其他属性很少被使用。Record 可以用来记录报文每一跳的地址, Verbose 属性给出每一个回应应答的响应时间;

Sweep range of sizes [n]: 该属性主要用于测试大报文被丢失、处理速度过慢或者分段失败等故障。

2. traceroute 命令

traceroute 命令通过发送探测数据分组到目标地址, 提供从本地 IP 地址到目标 IP 地址所经过的每一跳的信息。它通过控制 IP 报文的生存期 (TTL) 字段来实现。TTL 等于 1 的 ICMP 回应请求 (ICMP Echo Request) 报文将被首先发送, 路径上的第一个路由器将会丢弃该报文并且发送回标识错误消息的报文。错误消息通常是 ICMP 超时消息 (ICMP TTL Exceeded Message), 接收到该消息的设备能根据报文的源地址识别这一跳, 然后将报文的 TTL 字段加 1 继续发送。反复使用这一方法, 不断增加报文的 TTL 字段的值, 直到接收到目的地址的响应消息 (ICMP Echo Reply)。由此, 我们可以获得探测数据分组到达目标前所经历的所有中继站 (Hop) 的清单, 并显示到达每个中继站的时间。

需要说明的是, 不同操作系统 traceroute 的实现方式会略有不同, 通常在 Window 操作系统中采用的是 ICMP 协议, 而在 UNIX 操作系统中采用的是 UDP 协议。

traceroute 的功能尽管同 ping 命令有点类似, 但通过它所看到的信息要比 ping 命令详细得多, 它将本地送出的请求分组所到达的全部站点、所走的全部路由都显示出来, 并且显示出该路由的 IP、通过该 IP 的时延。在 Windows2000 中的命令是 tracert, 该命令后还可跟多个参数, 我们可以在 DOS 命令窗口键入 tracert 后回车, 得到这些参数的详细说明, 如图 10-10 所示。



图 10-10 tracert 命令及其参数的说明

下面我们在 DOS 命令行下用 `tracert` 命令来测试一下到 `www.sina.com.cn` 的路径情况, 如图 10-11 所示。

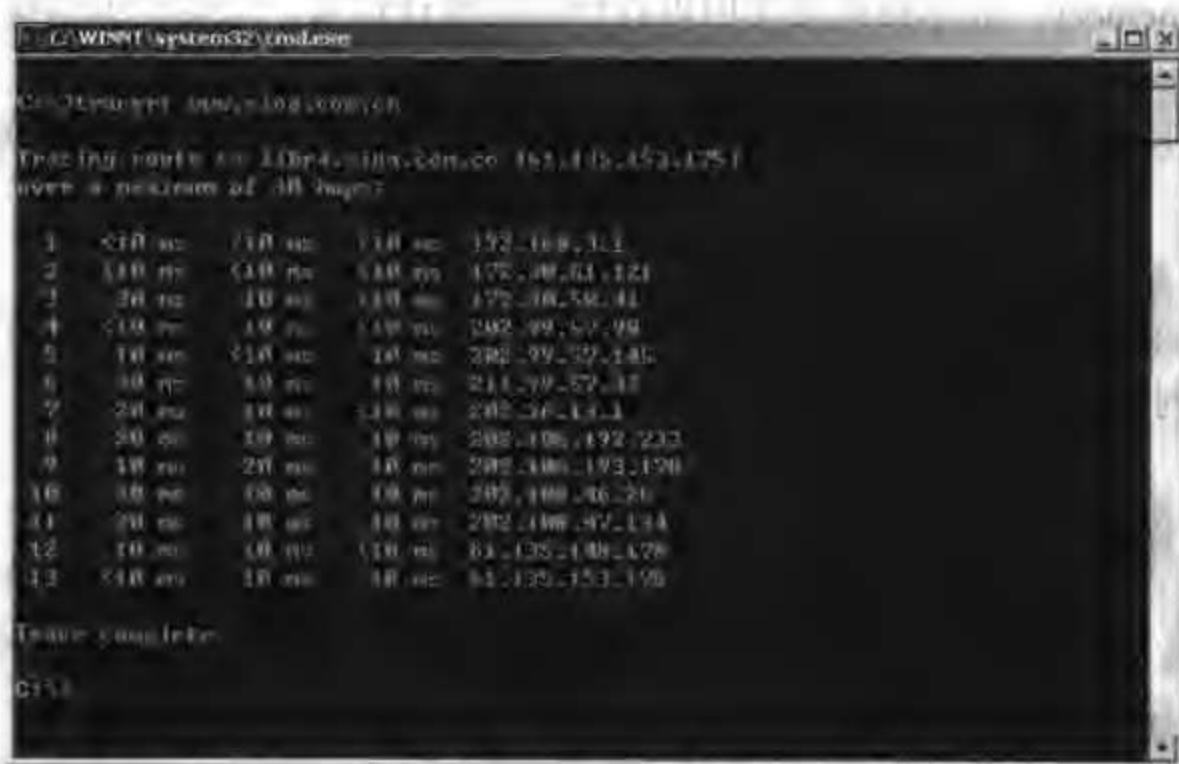


图 10-11 运行 `tracert` 命令及其响应

Cisco IOS 内置的 `traceroute` 命令的返回信息见表 10-2。

表 10-2 Cisco IOS 内置的 `traceroute` 命令的响应信息

状 态	说 明	原 因
nn msec	每一跳的响应时间	响应成功
*	响应超时	traceroute 测试包途经的路由器没有收到测试包; traceroute 测试包途经的路由器没有发送回 ICMP 超时信息 (ICMP "Packet Life Exceeded" Message) ;
A	管理性禁止	traceroute 测试包被防火墙或 ACL 阻断;
Q	收到 ICMP source quench 信息	traceroute 测试包途经的路由器收到过多的数据包, 需要检查相应设备的入口队列
H	收到 ICMP unreachable 信息	traceroute 测试包到目标系统之间可能存在路由循环

3. show 命令

`show` 是 Cisco 设备特有的一个用于显示设备状态和相关信息的工具。在对 Cisco 设备进行排错时会常常使用到各种 `show` 命令。下面是几个经常使用的 `show` 命令:

(1) `show interface`: 显示接口统计信息, 一些常用的 `show interface` 命令有:

`show interface fastethernet`

`show interface tokenring`

`show interface serial`

(2) `show controllers`: 显示接口卡控制器统计信息, 一些常用的 `show controllers` 命令有:

`show controllers e1`

`show controllers fastethernet`

(3) `show running-config`: 显示当前路由器正在运行的配置;

(4) `show startup-config`: 显示保存在 NVRAM 里的配置;

- (5) show flash: 显示 Flash 里的内容;
- (6) show buffers: 显示路由器中 buffer pools 统计信息;
- (7) show memory: 显示路由器使用内存情况的统计信息, 包括空闲池统计信息;
- (8) show processes: 显示路由器活动进程信息;
- (9) show version: 显示系统硬件、软件版本、配置文件和启动的系统映像及引导寄存器的值;
- (10) show ip route: 显示路由表信息。

应该说, Cisco 所提供的 show 命令是非常丰富的, 几乎针对所有配置都有相应的 show 命令。上面所列出的只是其中很小的一部分, 我们可以通过键入 “show ?” 查询相关的命令。

4. debug 命令

在超级用户模式下的 debug 命令能够提供数据传输的详细信息、节点产生的错误消息等非常有用的排错数据, 能够帮助我们对错误进行定位。虽然 debug 命令非常有用, 但是在使用 debug 命令的时候一定要非常注意, 因为它会占用大量的系统资源, 有可能会引起一些不可预测现象。通常我们不建议在生产网上运行 debug 命令, 除非你非常清楚这样运行的结果。debug 命令默认是显示在控制台端口上的, 我们可用 log buffer 命令把输出定向到 buffers 里面。如果我们是采用 telnet 连接的, 可用 “terminal monitor” 命令监控到控制台的 debug 信息。

Cisco 提供的 debug 命令非常丰富, 几乎针对各种配置都有相应的 debug 命令, 我们可以通过键入 “debug ?” 查询相关的命令。我们可以采用 “undebug all” 命令取消 debug 信息。

以上是几种常用的命令工具, 它们是所有网络从业人员都应该了解的常识。除此以外, 我们在 PC 机上还常使用 ipconfig 命令来查看 TCP/IP 的配置信息, 使用 arp 命令来查看及清除本机存储的 IP 与 MAC 的映射表。当上网出现问题时, 我们还常使用 nslookup 命令来验证 DNS 的工作是否正常。另外, 当广域网出现问题时, 我们往往需要和当地线路提供商配合进行相应的线路回路测试, 以排查线路的故障。有关的测试命令及手段如图 10-12 所示。

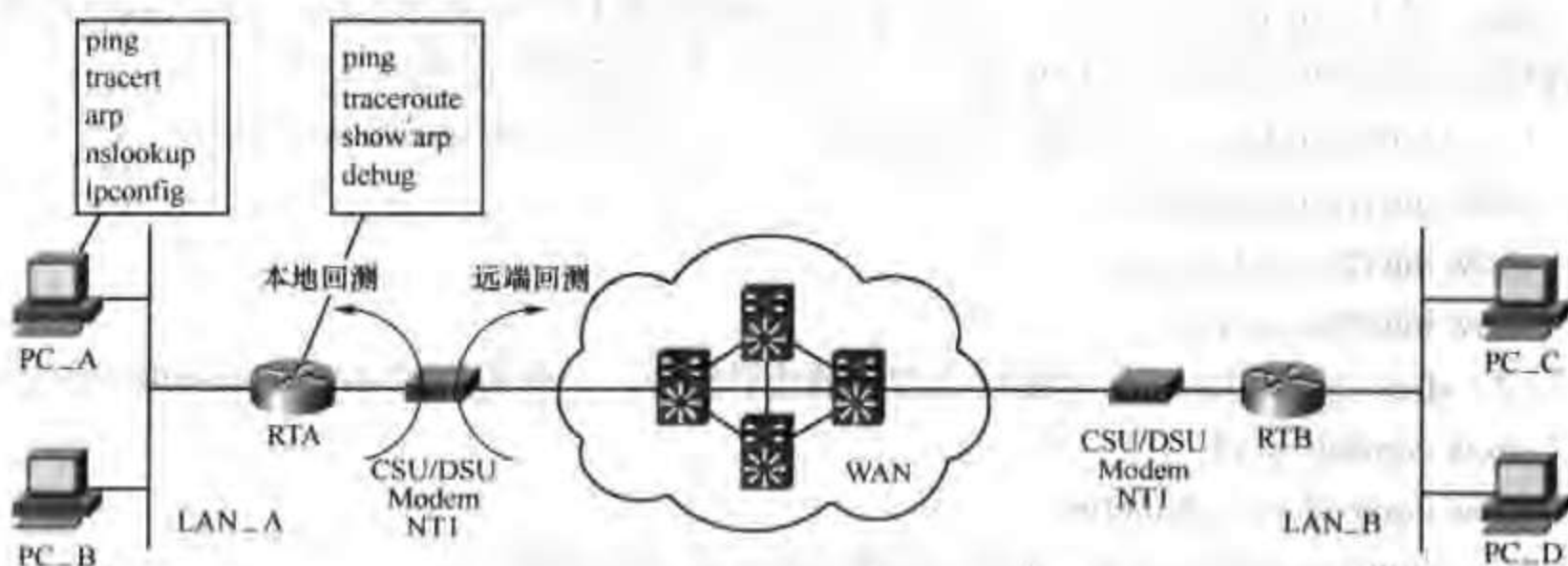


图 10-12 网络常用测试命令及手段

10.5 TCP/IP 连通性排错

在日常的网络通信中,我们最常遇到的就是网络的连通性问题,下面通过一个如图 10-13 所示的通用的网络连接的模型来讲解有关网络连通性的排错方法。

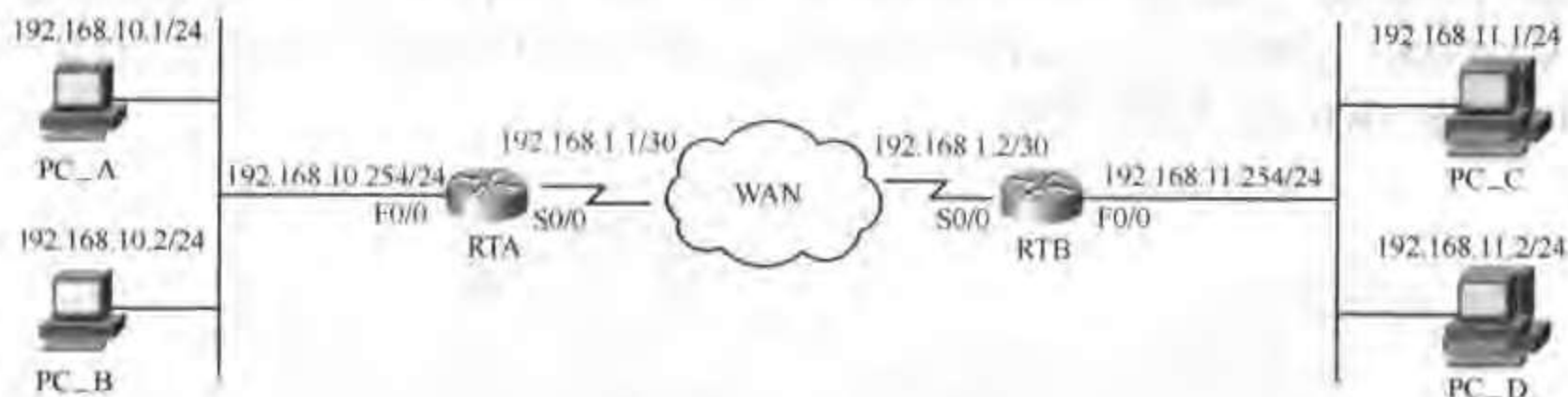


图 10-13 网络连通性模型

在该模型中, PC_A 和 PC_B 位于同一网段, PC_C 和 PC_D 位于同一网段, 下面我们分别来分析 PC_A 和 PC_B, 以及 PC_A 和 PC_C 通信的过程, 因为只有了解了通信的详细过程, 才能在排错的时候有的放矢。

(1) PC_A 和 PC_B 通信

当 PC_A ping PC_B 的时候(如图 10-14 所示), 由于 PC_A 和 PC_B 属于一个网段, PC_A 将首先查询自己的 ARP 缓存表。如果 ARP 表中有 PC_B 的 MAC 纪录 (00-90-f5-e1-10-11), ping 分组直接发往交换机 SWA。交换机 SWA 查询自身的 MAC 地址表, 找到 PC_B 的 MAC 地址所对应的交换机端口 (f0/2), 然后将此分组通过此端口发出, 从而到达 PC_B; 如果 PC_A 的 ARP 缓存表中没有 PC_B 的 MAC 纪录, 那么 PC_A 将首先发送 ARP 的查询分组, 来获取 PC_B 的 MAC 地址, 然后再将 ping 分组发往交换机进行后续的处理。

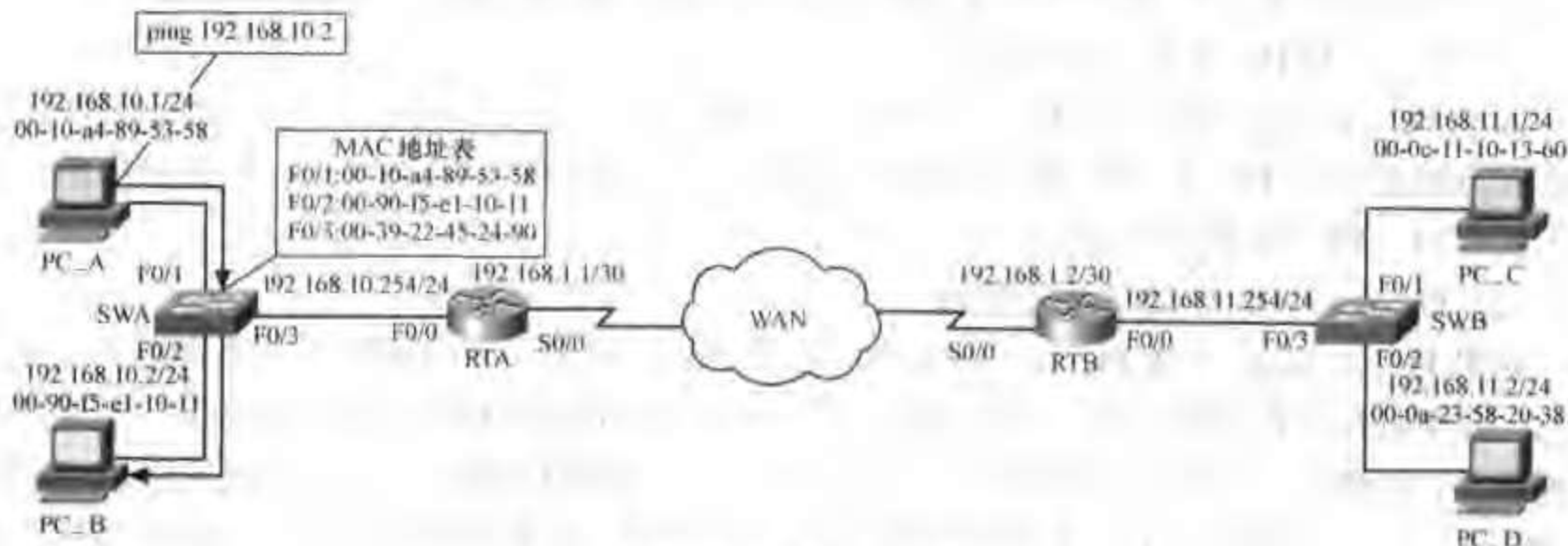


图 10-14 PC_A ping PC_B

(2) PC_A 和 PC_C 通信

当 PC_A ping PC_C 的时候(如图 10-15 所示), 由于 PC_A 和 PC_C 不属于同一个网段,

PC_A 将首先查询自己的路由表, 根据路由表的指示进行分组的转发。这里, PC_A 设置的网关(默认路由)为 192.168.10.254, 因此 ping 分组将被发送到路由器 RTA。RTA 查询自己的路由表, 找到与 PC_C 的 IP 地址最匹配(最长匹配原则)的条目, 将数据分组通过 S0/0 端口发送到路由器 RTB。RTB 查询自身的路由表, 发现 PC_C 和自己的 F0/0 端口在同一网段, 接着它又查询自身的 ARP 缓存表, 找到 PC_C 所对应的 MAC 地址(000c.1110.1360), 然后将该 ping 分组发到交换机 SWB 上。交换机 SWB 查询自己的 MAC 地址表, 找到该 MAC 地址所对应的端口, 然后将该数据分组从此端口送出, 最后到达 PC_C; 如果 RTB 上没有 PC_C 的 MAC 地址, 它将首先发送 ARP 查询分组以获取 PC_C 的 MAC 地址, 然后再将数据分组发往交换机 SWB 进行后续的处理。

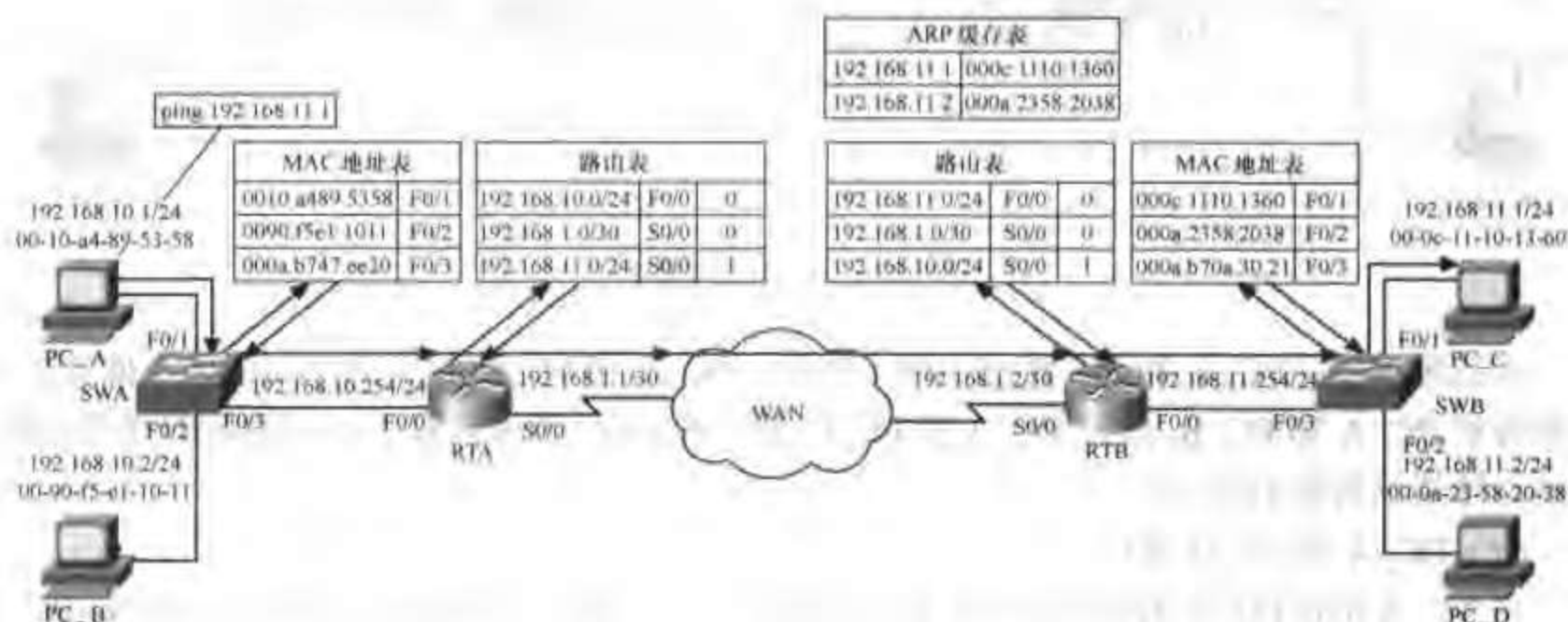


图 10-15 PC_A ping PC_C

这里需要特别说明的是, 通信是一个双向的过程, 一去一回才算一个完整的过程, 在网络排错的时候, 经常会发现单向通信的故障, 这是由于在配置网络时我们往往只注意去的路由, 而忽略了返回的路由。

有了对通信过程的了解, 下面来看一看如何排除此通信模型中常见的故障。

(1) PC_A 和 PC_B 通信故障排除

如果 PC_A ping 不通 PC_B, 由于 PC_A 和 PC_B 位于同一网段, 不涉及路由问题, 排查的重点将集中在 PC_A、PC_B 与交换机的连接上, 看看 PC_A、PC_B 与交换机的接口是否正常启用, 物理线路是否正常。

(2) PC_A 和 PC_C 通信故障排除

如果 PC_A ping 不通 PC_C, 由于 PC_A 和 PC_C 位于不同的网段, 需要查看 PC_A 至 PC_C 沿途所有设备的路由表, 看它们是否有 PC_C 所在网段的路由或默认路由。经常出现的问题是, 在 PC_A 至 PC_C 的路径上, 都有 PC_C 所在网段的路由, 但在返回的路径(PC_C 至 PC_A)上, 往往缺乏 PC_A 所在网段的路由, 所以出现单向通信的故障。如果路由都正常, 我们把主要精力放在在排查设备的接口以及物理线路上。在这里由于 PC_A 和 PC_C 的通信跨越了广域网, 因此在线路的排查时会涉及到与线路提供商的配合问题。广域链路的排错问题将在后面进行介绍。

10.6 链路层排错

根据 ISO 互联模型我们知道,除了物理层以外,所有网络层及网络层以上的应用都依赖于数据链路层的正常工作。数据链路层主要关注于相邻设备的互连参数,比如,封装协议、信令格式等等。在排除链路层的故障时,往往需要检查相连设备的相应的接口。

在进行链路层排错之前,一定要记住首先确信物理层是正常的。下面是检查物理层的一些基本的方法:

- (1) 查看 `show interface` 命令的第一行,确信接口连通 (up);
- (2) 查看接口的状态灯;
- (3) 查看接口线缆的连接情况。

10.6.1 局域网排错

在局域网的排错当中,主要涉及以太接口故障的排除。我们可以使用 `show interface` 命令查看接口的详细状况,包括链路状态、接口地址、帧封装格式、双工类型、速率、吞吐量、碰撞冲突、信息分组丢失等相关内容。下面通过一个 `show interface` 命令的实例进行具体的说明。

```
Router#show interface fastethernet 0/1
```

```
FastEthernet0/1 is up, line protocol is up
```

```
Hardware is AmdFE, address is 000a.b747.ee21 (bia 000a.b747.ee21)
```

```
Description: to LAN
```

```
Internet address is 192.168.1.20/24
```

```
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, reliability 255/255, txload 5/255, rxload 4/255
```

```
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
```

```
Full-duplex, 100Mb/s, 100BaseTX/FX
```

```
ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input 00:00:01, output 00:00:05, output hang never
```

```
Last clearing of "show interface" counters never
```

```
Input queue: 2/75/821/0 (size/max/drops/flushes); Total output drops: 0
```

```
Queueing strategy: fifo
```

```
Output queue :0/40 (size/max)
```

```
5 minute input rate 1613000 bits/sec, 332 packets/sec
```

```
5 minute output rate 2063000 bits/sec, 382 packets/sec
```

```
10665922 packets input, 2939567175 bytes
```

```
Received 13224 broadcasts, 0 runs, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```

```
0 watchdog
```

```
0 input packets with dribble condition detected
```



```
11665882 packets output, 3339305708 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
8177 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Router#

以上是一个标准的 show interface 命令的输出，下面进行详细的说明：

FastEthernet0/1 is up: 表示接口的物理层成功启动。

Line Protocol is Up: 表示接口的链路层成功启动。

Hardware is AmdFE, address is 000a.b747.ee21: 接口的硬件类型和 MAC 地址。

Description: 是用户自定义的对该接口的描述。使用这一功能给出接口准确的描述是十分重要的，尤其在大型网络中它对准确定位故障有很大的帮助。

Internet Address: 是用户为该接口设置的 IP 地址。

MTU: 表示该接口的最大传输单元，用户可以配置。

BW、DLY、Rely、Load(带宽、延迟、可靠性和负载): 这些参数主要用来计算 IGRP/EIGRP 路由的度量 (Metric)，从而影响路由的选择。注意，这些参数并不代表该物理接口真实的数值。

Encapsulation: 是指该接口的链路层封装类型 (在以太网中，对于 IP，Cisco 的缺省设置为 ARPA，而 IPX 的缺省设置为 Novell-Ether)。

Loopback: 表示该接口是否设置了回送。

Keepalive: 表示该接口是否设置了保持激活，默认的保持激活时间是 10s。

Full-duplex, 100Mbit/s: 表示该接口的双工模式是全双工，速率是 100Mbit/s。

ARP type: 表示 ARP 封装的类型。

ARP Timeout: 表示 ARP 的失效时间，默认是 4 个小时。

Last Input, Output: 表示最后一个数据分组被成功接收 (Input) 和发送 (Output) 后的时间，它对判断一个接口何时失效有帮助。

Output Hang: 表示接口由于传送问题导致复位后的时间。

Last Clearing of "Show Interface" Counters: 表示上次清除接口计数器后的时间。

Input Queue、Output Queue: 表示输入、输出队列的数据分组个数。

Queueing Strategy: 表示队列的排队策略 (FIFO 代表“先进先出”)。

5 Minute Input Rate: 表示最近 5min 接口的输入速率。

5 Minute Output Rate: 表示最近 5min 接口的输出速率。

Packets Input: 表示该接口接收的无差错数据分组总数。

Runts: 是指长度小于最小值而被丢弃的报文。在以太网中，任何长度小于 64 字节的数据分组被认为是超短数据分组 (Runt)。

Giants: 是指长度大于最大值而被丢弃的报文。在以太网中，任何长度大于 1518 字节的数据分组被认为是超长数据分组 (Giant)。

Input Errors: 指到达报文中检测到的错误，也可能表明网段本身发生了错误。

CRC: 指报文发送设备生成的循环冗余校验和与从接收的数据计算出的校验和不匹配的

数量。它可能由于网段的噪声引起,或者由于网卡故障、报文冲突引发。

Frame: 指接收到的帧的类型与路由器以太网帧类型(IP协议帧类型为 ARPA)不匹配的数量。

Overrun: 指由于输入速率超过接收方处理数据的能力,接收方的硬件不能把接收到的数据交给硬件缓冲区的次数。

Ignored: 接由于接口内部缓冲不足而被接口忽略的接收到的接据分组数。广播风暴和噪声突发可能引起该计数的增加。

Dribble Condition: 指接收到的帧比 MTU 大,但不属于 Giants。

Packets Output: 表示该接口发送的数据分组总数。

Output Errors: 接输出报文中的错误,它可能表明路由器接口本身发生了故障。

Interface resets: 指该接口被复位的次数。在检测到过多的错误时,路由器将重置接口。这些错误可能存在于局域网段中,也可能是接口本身的错误,在此不能够判断具体是哪儿发生故障。但是,如果伴随着大量的输出错误,则表明路由器接口本身发生故障。

Collisions: 指由于冲突导致重传的接据分组数。在以太网中,由于它采用的是 CSMA/CD 技术,因此存在冲突是正常的,但是出现过多的冲突是不正常的。根据经验,如果冲突超过输出数据分组总数的 0.1%,则认为网段含有太多的冲突。

Babble: 指持续接收到可疑的帧。

Deferred: 如果线路繁忙,报文在传输时将被延缓发送。

在排查网络连通性故障时,通常只关注 `show interface` 命令输出的第一行,即“FastEthernet0/1 is up, line protocol is up”,下面对几种可能出现的情况进行说明。

(1) FastEthernet0/1 is up, line protocol is up

表明该接口物理层和链路层都已正常启动。需要注意的是,当在接口下输入“no keepalive”命令后,即使接口不接线缆,也会出现“FastEthernet0/1 is up, line protocol is up”信息。因此,为了断定接口是否正常启动,需要结合“keepalive”信息一起考虑。

(2) FastEthernet0/1 is administratively down, line protocol is down

表明该接口物理层“管理性”关闭,链路层关闭。该信息主要是由于在接口下输入了“shutdown”命令。取消该信息,我们需要在接口下输入“no shutdown”命令。

(3) FastEthernet0/1 is disabled, line protocol is down

表明该接口物理层处于“无效”状态,链路层关闭。该信息的出现主要是由于在一个“keepalive”间隔时间内(默认为 10s),接口内遇到了超过 5000 个错误。

(4) FastEthernet0/1 is down, line protocol is down

表明该接口物理层关闭,链路层关闭。该信息主要是由于接口物理层的故障导致。

(5) FastEthernet0/1 is up, line protocol is down

表明该接口物理层已正常启动,但链路层关闭。该信息主要是由于未接线缆,或是连接线缆的故障所致。

10.6.2 广域网接路排错

同局域网类似,在广域网的排接当中,主要涉及串口故障的排除。和以太接口的排查一样,我们可以使用“show interface”命令查看接口的详细状况,包括链路状态、接口地址、

帧封装格式、双工类型、速率、吞吐量、碰撞冲突、信息包丢失等相关内容。下面通过一个“show interface”命令的实例进行具体的说明。

```
Router# show interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 254/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    8 packets input, 2320 bytes, 0 no buffer
    Received 8 broadcasts, 0 runts, 0 giants, 0 throttles
    1 input errors, 0 CRC, 1 frame, 0 overrun, 0 ignored, 0 abort
    4 packets output, 852 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  DCD=up   DSR=up   DTR=up   RTS=up   CTS=up
```

Router#

以上串口的输出内容和 10.6.1 节以太口的输出大致相同，读者可以参考以太口的说明来了解串口的输出内容。

在排查网络连通性故障时，通常只关注“show interface”命令输出的第一行，即“Serial0/0 is up, line protocol is up”，下面对几种可能出现的情况进行说明。

(1) Serial0/0 is up, line protocol is up

表明该接口物理层和链路层都已正常启动。需要注意的是，当在接口下输入“no keepalive”命令后，即使接口不接线缆，也会出现“Serial0/0 is up, line protocol is up”信息。因此，为了断定接口是否正常启动，需要结合“keepalive”信息一起考虑。

(2) Serial0/0 is administratively down, line protocol is down

表明该接口物理层“管理性”关闭，链路层关闭。该信息主要是由于在接口下输入了“shutdown”命令。取消该信息，我们需要在接口下输入“no shutdown”命令。

(3) Serial0/0 is down, line protocol is down

表明该接口物理层关闭，链路层关闭。该信息表示路由器到本地的 Modem 之间无载波

信号 CD。

(4) Serial0/0 is up, line protocol is down

表明该接口物理层已正常启动，但链路层关闭。该信息主要由以下几方面原因所致：

- ① 本地路由器未作配置；
- ② 远端路由器未开或未配置；
- ③ 路由器两端封装的协议不匹配；
- ④ 专线没有开通；

当确认自己没有配置错误时，可以和电信局联合作环路测试，以确定具体是哪一段线路出现了问题。

(5) Serial0/0 is up, line protocol is up(looped)

表明该接口物理层已正常启动，链路层也已启动，但存在环路。该信息主要由接口下的“loopback”命令，或线路上的环路等原因所致。

1. DDN 常见故障排除

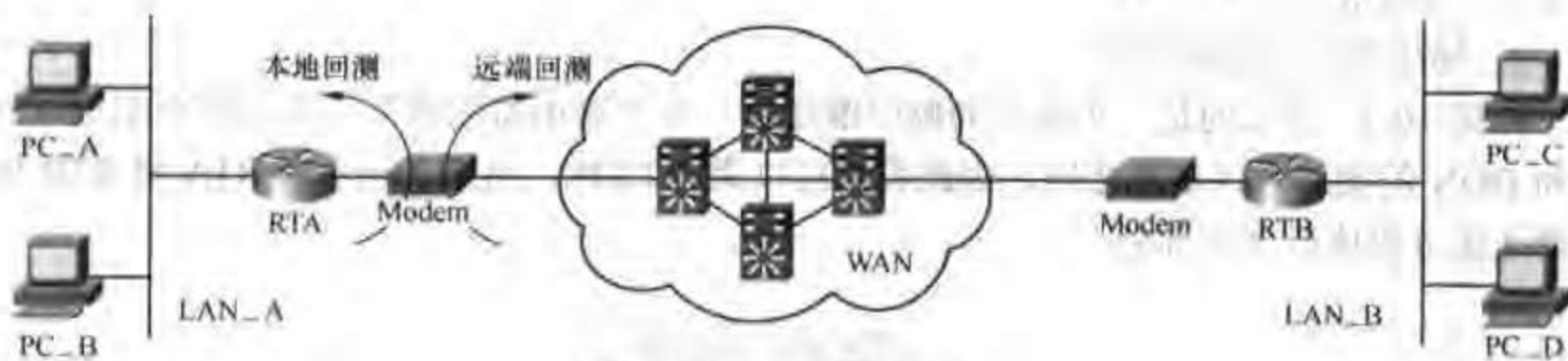


图 10-16 典型的 DDN 连接

如图 10-16 所示的是一个典型的 DDN 连接。由图中我们看出 RTA 至 RTB 的 DDN 连接实际是由以下几部分组成的：

- (1) RTA—本端 Modem；
- (2) 本端 Modem—本地电信局节点设备；
- (3) 本地电信局节点设备—远端电信局节点设备；
- (4) 远端电信局节点设备—远端 Modem；
- (5) 远端 Modem—RTB。

当 RTA 与 RTB 之间的连接出现问题时，我们的任务就是要检查出是哪一段不通并解决它。当然，首先要通过“show interface”命令查看接口的状态：

(1) Serial0/0 is administratively down, line protocol is down

表明该接口物理层“管理性”关闭，链路层关闭。该信息主要是由于在接口下输入了“shutdown”命令。取消该信息，我们需要在接口下输入“no shutdown”命令。

(2) Serial0/0 is down, line protocol is down

表明该接口物理层关闭，链路层关闭。该信息表示路由器到本地的 Modem 之间无载波信号 CD。连接串口和 Modem，开启 Modem，看 Modem 的发送灯 TD 是否亮。TD 灯亮表示路由器有信号发送给 Modem；TD 灯若不亮，请检查 Modem 线缆和端口，也可以用另外一个串口再试试看。

(3) Serial0/0 is up, line protocol is down

表明该接口物理层已正常启动，但链路层关闭。该信息主要由以下几方面原因所致：

① 本地路由器未作配置；

② 远端路由器未开或未配置；

③ 路由器两端封装的协议不匹配（路由器两端需要配置相同的封装协议，比如，如果 RTA 封装 PPP，RTB 封装 HDLC，那么就会出现该接口提示的信息）；

④ 专线没有开通；

当确认自己没有配置错误时，可以和电信局联合作环路测试，以确定具体是哪一段线路出现了问题。

(4) Serial0/0 is up, line protocol is up(looped)

表明该接口物理层已正常启动，链路层也已启动，但存在环路。该信息主要由接口下的“loopback”命令，或线路上的环路等原因所致。

需要说明的是，在调试 DDN 的时候，有一些非调试因素会导致网络的故障，比如线路的环阻、接地的电阻、零地电压等参数。通常线路的环阻应不大于 $1000\ \Omega$ 、接地的电阻不大于 $4\ \Omega$ 、零地电压不大于 $5V$ 。

2. 帧中继常见故障排除

如图 10-17 所示的是一个典型的帧中继连接。在“路由器配置”一章已经介绍过，帧中继和 DDN 的接入方式基本相同，因此我们可以类比 DDN，将图 10-17 中 RTA 至 RTB 的帧中继连接分割成以下几部分：

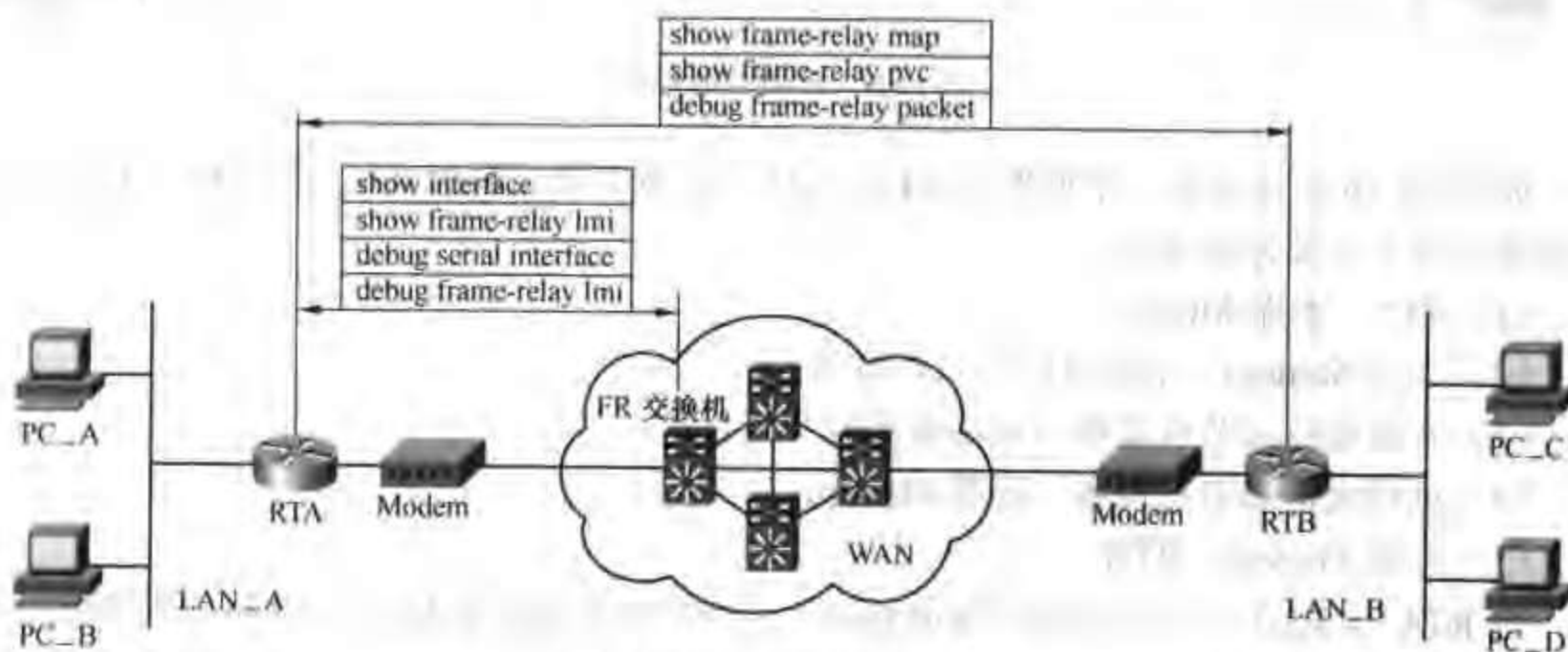


图 10-17 典型的帧中继连接

(1) RTA—本端 Modem；

(2) 本端 Modem—本地电信局节点设备；

(3) 本地电信局节点设备—远端电信局节点设备；

(4) 远端电信局节点设备—远端 Modem；

(5) 远端 Modem—RTB。

当 RTA 与 RTB 之间的连接出现问题时，我们的任务就是要检查出是哪一段不通并解决它。当然，首先要通过“show interface”命令查看接口的状态：

(1) Serial0/0 is administratively down, line protocol is down

表明该接口物理层“管理性”关闭，链路层关闭。该信息主要是由于在接口下输入了“shutdown”命令。取消该信息，我们需要在接口下输入“no shutdown”命令。

(2) Serial0/0 is down, line protocol is down

表明该接口物理层关闭，链路层关闭。该信息表示路由器到本地的 Modem 之间无载波信号 CD。连接串口和 Modem，开启 Modem，看 Modem 的发送灯 TD 是否亮。TD 灯亮表示路由器有信号发送给 Modem；TD 灯若不亮，请检查 Modem 线缆和端口，也可以用另外一个串口再试试看。

(3) Serial0/0 is up, line protocol is down

表明该接口物理层已正常启动，但链路层关闭。该信息主要由以下几方面原因所致：

- ① 本地路由器未作配置；
- ② 远端路由器未开或未配置；
- ③ 路由器两端封装的协议不匹配；
- ④ 路由器的 LMI 类型与帧中继接供商使用的类型不一致；
- ⑤ 专线没有开通；

当确认自己没有配置错误时，可以和电信局联合作环路测试，以确定具体是哪一段线路出现了问题。

(4) Serial0/0 is up, line protocol is up(looped)

表明该接口物理层已正常启动，链路层也已启动，但存在环路。该信息主要由接口下的“loopback”命令，或线路上的环路等原因所致。

和调试 DDN 一样，在调试帧中继时也要注意线路的环阻、接地的电阻、零地电压等参数。另外，Cisco 还提供了两条对于帧中继的排错非常重要的命令：“show frame-relay lmi”和“show frame-relay pvc”。使用“show frame-relay lmi”命令可方便地显示所有帧中继接口的 LMI 内容；使用“show frame-relay pvc”可验证 PVC 是否激活。PVC 有三种状态：Active、Inactive、Deleted：

Active 状态表示永久虚电路已经建立，两个节点之间的帧中继链路已经建立。

Inactive 状态表示帧中继提供商已提供对应于 DLCI 号的 PVC，但未被路由器使用。可以验证数据链路连接标识（DLCI，Data-Link Connection Identifier）编号，确认帧中继提供商提供的 DLCI 编号是否有误。设置 DLCI 时要注意：我方要设置对方的 DLCI 号，对方设置我方的 DLCI 号，通常出问题就是因为两个点之间的 DLCI 号用反了。另外，还要看双方是否将 DLCI 设置正确，如一方设置正确，而另一方有问题时，也会出现 Inactive 状态，所以双方应及时联系，共同排除故障。

Deleted 状态表示路由器配置的 DLCI 号未被帧中继接供商提供，因此 PVC 不能建立，所以被 deleted。在这种情况下，先确认 DLCI 号正确，然后再验证帧中继提供商是否已经激活 PVC。

说明：通常情况下，在出现 Deleted 状态时，我们应将注意力集中在本地的路由器上，而出现 Inactive 状态时，应将故障排除的注意力转向远端的路由器。

3. E1 常见故障排除

目前，在广域网的构建中，经常会使用到 E1 线路，当 E1 线路出现问题时，我们常常会在路由器上使用“show controller e1”命令进行排查，通过该命令可以了解 E1 接口的状态、

本地和远端告警的信息等。下面我们就对“show controller e1”命令进行详细的介绍。

说明：在“路由器配置”一章我们介绍了 E1 线路的配置方法，这里需要说明的是，通常情况下，如果电信部门不特别说明，一般的 E1 线路是指可划分时隙的 CE1，在配置 CE1 的两端路由器上，下面几个参数必须保持一致：时隙、framing、linecode、CRC 等。另外，时钟应该保持同步。

下面通过一个实例进行具体的说明。

```
Router#show controller e1
```

```
E1 1/0 is up
```

```
Applique type is Channelized E1 - balanced
```

```
No alarms detected.
```

```
Framing is CRC4, Line Code is HDB3, Clock Source is Line.
```

```
Data in current interval (457 seconds elapsed):
```

```
0 Line Code Violations, 0 Path Code Violations
```

```
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
```

```
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

```
Total Data (last 25 15 minute intervals):
```

```
1123 Line Code Violations, 53 Path Code Violations,
```

```
2 Slip Secs, 708 Fr Loss Secs, 25 Line Err Secs, 0 Degraded Mins,
```

```
1 Errored Secs, 0 Bursty Err Secs, 2 Severely Err Secs, 709 Unavail Secs
```

以上是一个标准的 show interface 命令的输出，下面进行详细的说明：

E1 1/0 is up: 表示 E1 控制器 1/0 正在运行，E1 controller 可能是这三种情况：up、down、administratively down。另外，如果打环，可以分为本地环和远端环。

Applique Type: 表示 E1 是平衡还是非平衡的，平衡的阻抗是 120Ω，非平衡的是 75Ω。

Framing: 当前帧类型，缺省的是 CRC4，还有 NO-CRC4。

Line Code: 当前的线路编码，缺省是：HDB3，其它还有 ami。

No alarms detected: 警告显示。可能的警告有：

传输者发送远端告警；

传输者正发送高警指示信息<alarm indication signal (AIS)>；

接收者有信号丢失；

接收者得到 AIS；

接收者有帧丢失；

接收者有远端告警；

接收者没有告警。

Data in current interval: 显示当前的累积时间，每隔 15 分钟刷新一次。

Line Code Violations: 表示发生 Bipolar Violation (BPV) 或者 Excessive Zeros (EXZ) 错误事件。

Path Code Violations: 表示有一个帧同步错误位在 D4 和 E1-no CRC 格式，或者一个 CRC 错误在扩展的超级帧 Extended Superframe (ESF)和 E1-CRC 格式。

Slip secs: 表示 DS1 帧有效负荷位的复制和删除，当相连收发两端的路由器不一致的情

况, 会出现 Slip secs。

Fr loss secs: 表示一个丢失帧发现的积累时间。

Line Err secs: 表示当一个或多个 Line Code Violation errors 发现积累的时间。

Degraded mins: 表示一个退化的时间(degraded minute)是被评估的错误率在 $1E-6$ 和 $1E-3$ 之间的时间。

Errored secs: 在 ESF 和 E1 CRC 链路, 它是指下面之一的错误被探测到的时间:

一个或多个 Path Code Violations;

一个或多个 Controlled Slip events;

对 SF 和 E1 no-CRC 链路, Bipolar Violations 存在的时间。

Bursty Err secs: 多于一个但是小于 320 个 Path Coding Violation 错误, 不是 Severely Errored Frame 发现以及没有发现进来的 AIS。Controlled slips 不包括在这个参数里面。

Severely Err secs:

对 ESF 信号, 它是指下面之一的错误被探测到的时间:

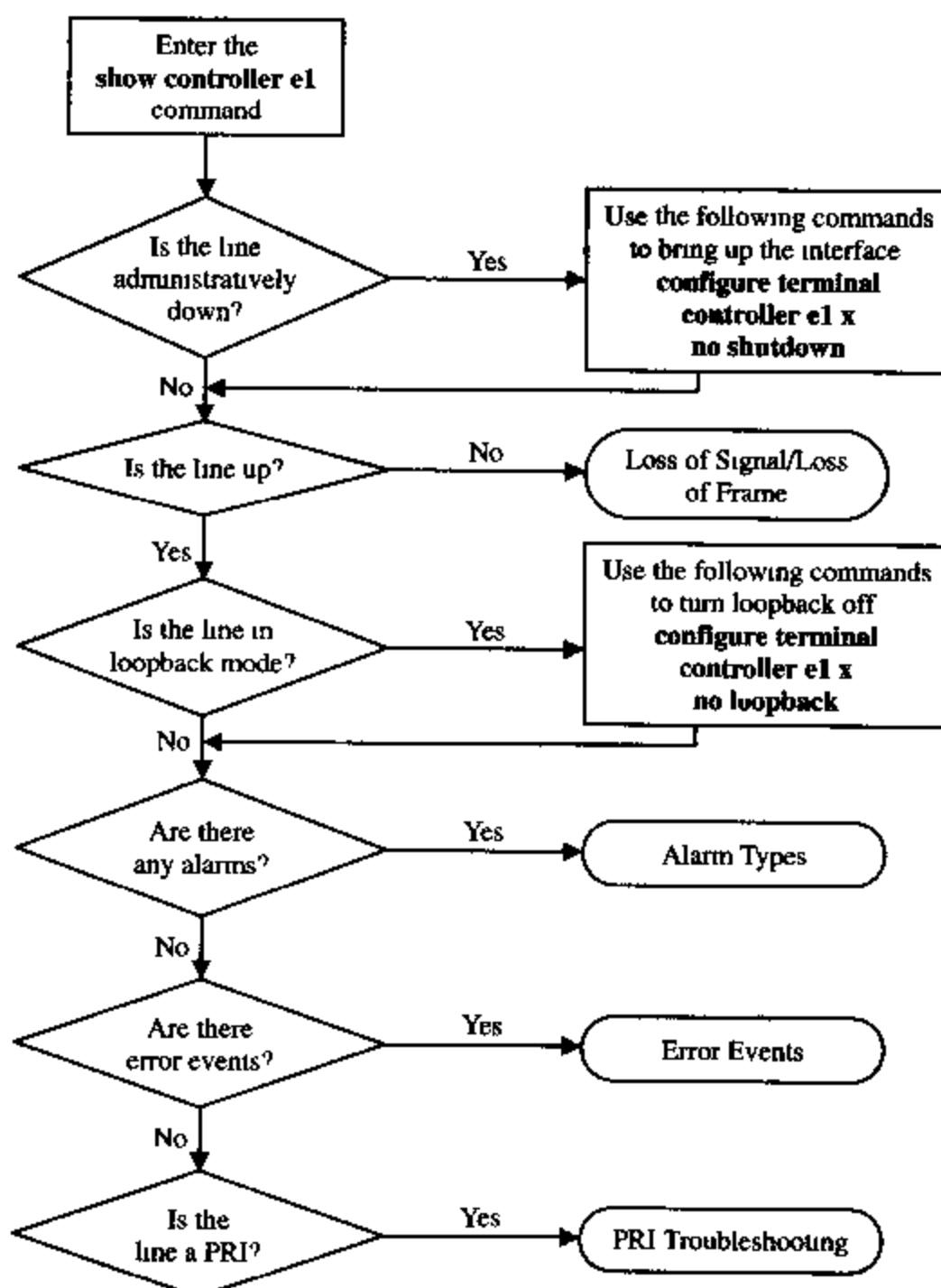


图 10-18 E1 线路排错流程之一

320 或者更多的 Path Code Violation 错误;

发现一个或者多个帧丢失;

一个 AIS 发现。

对 E1-CRC 信号, 它是指下面之一的错误被探测到的时间:

832 或者更多的 Path Code Violation 错误;

发现一个或者更多的帧丢失。

对 E1-nonCRC 信号, 这是 2048 个 Line Code Violations 或者更多存在的时间。

对 D4 信号, 是发现分帧错误 (Framing Errors), 或者帧丢失, 或者 1544 Line Code Violations 的时间。

Unavail Secs: 表示接口不用的总时间, 单位为秒。

上面我们给出了“show controller e1”命令的详细解释, 下面我们给出 E1 排错的流程图, 如图 10-18~图 10-23 所示, 希望对读者会有帮助。

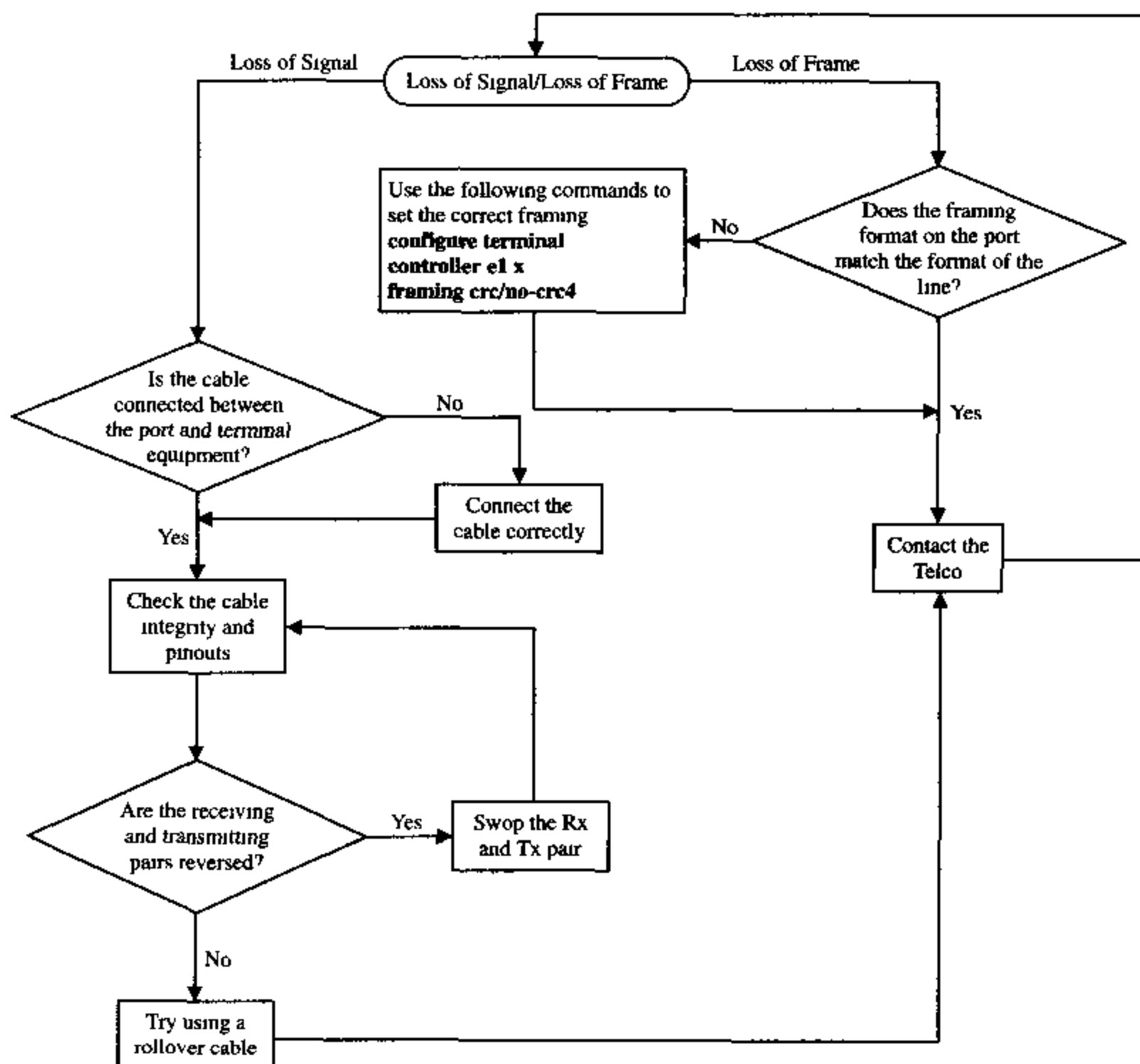


图 10-19 E1 线路排错流程之二

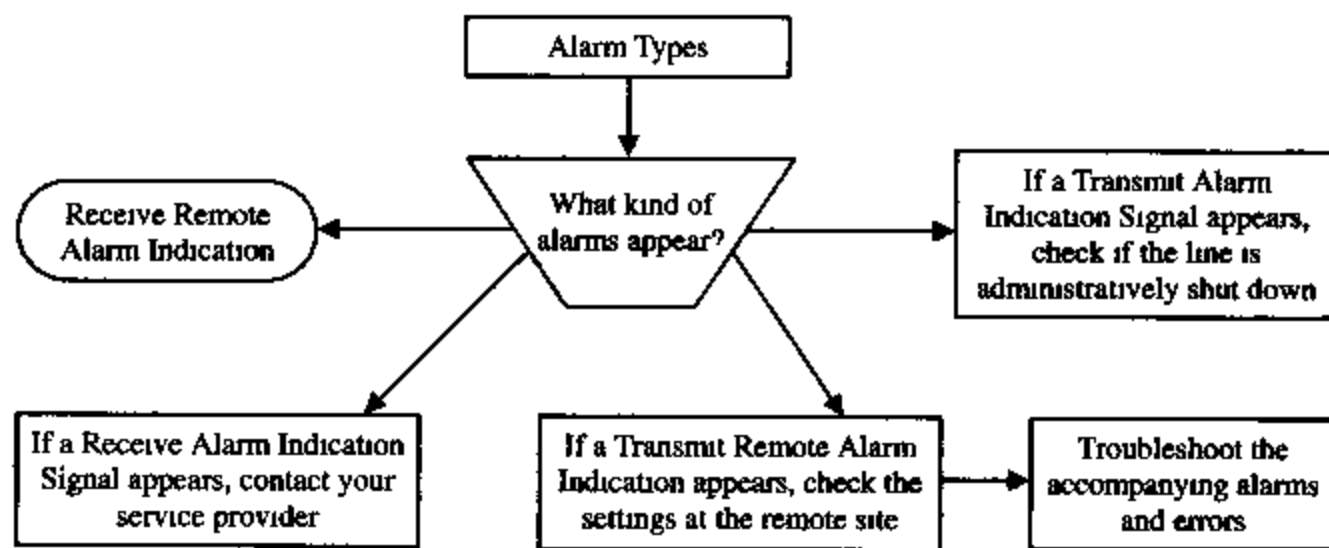


图 10-20 E1 线路排错流程之三

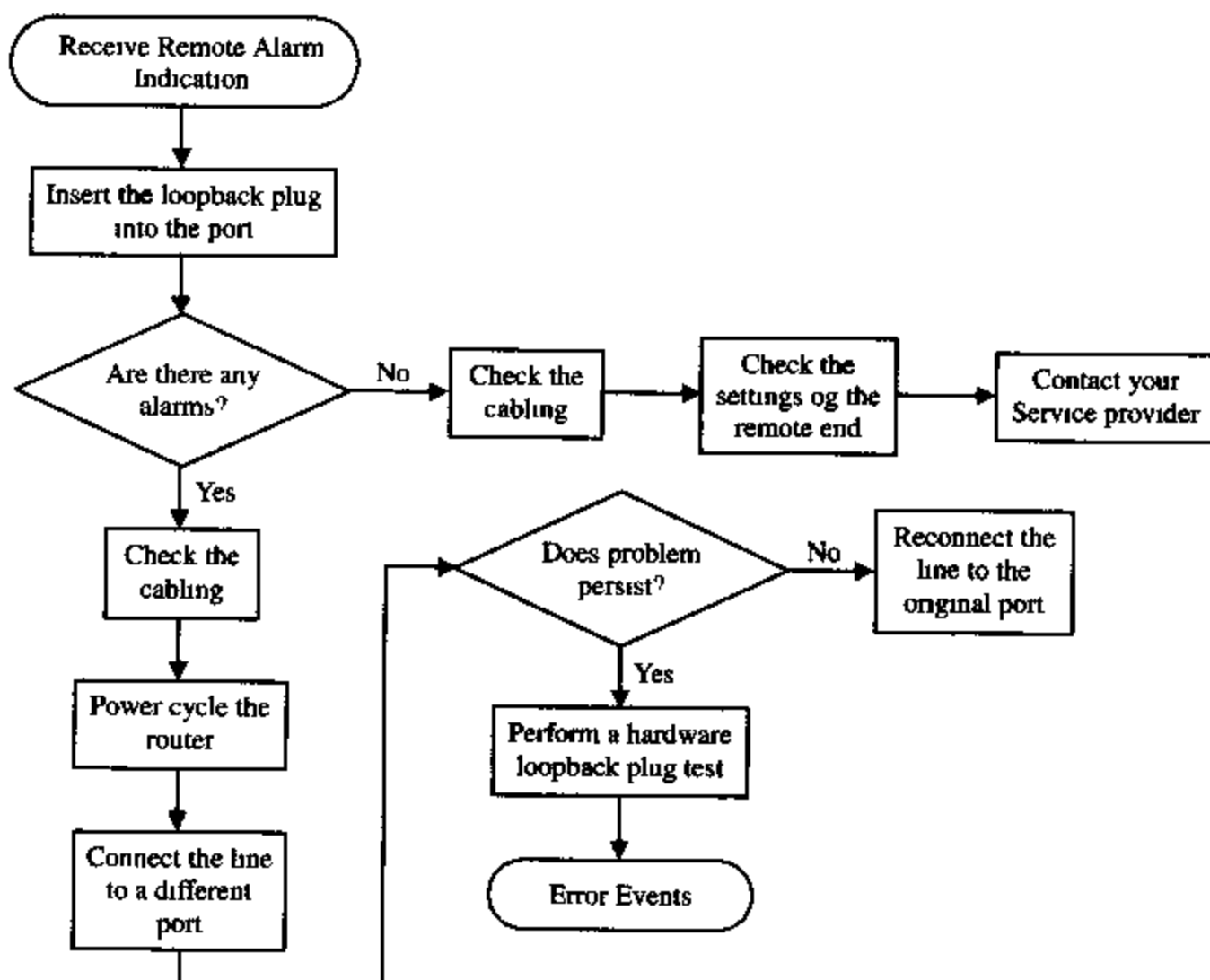


图 10-21 E1 线路排错流程之四

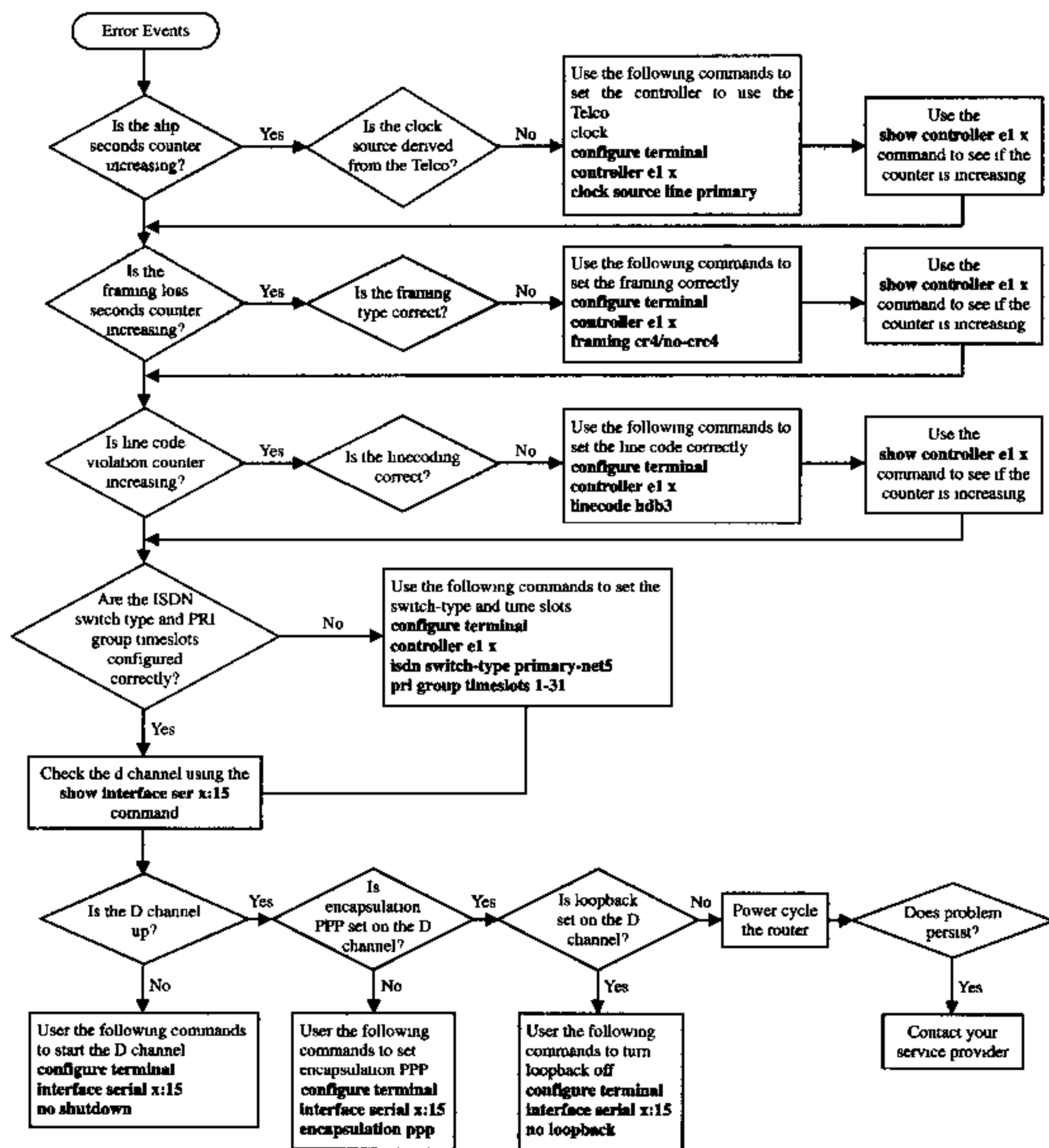


图 10-22 E1 线路排错流程之五

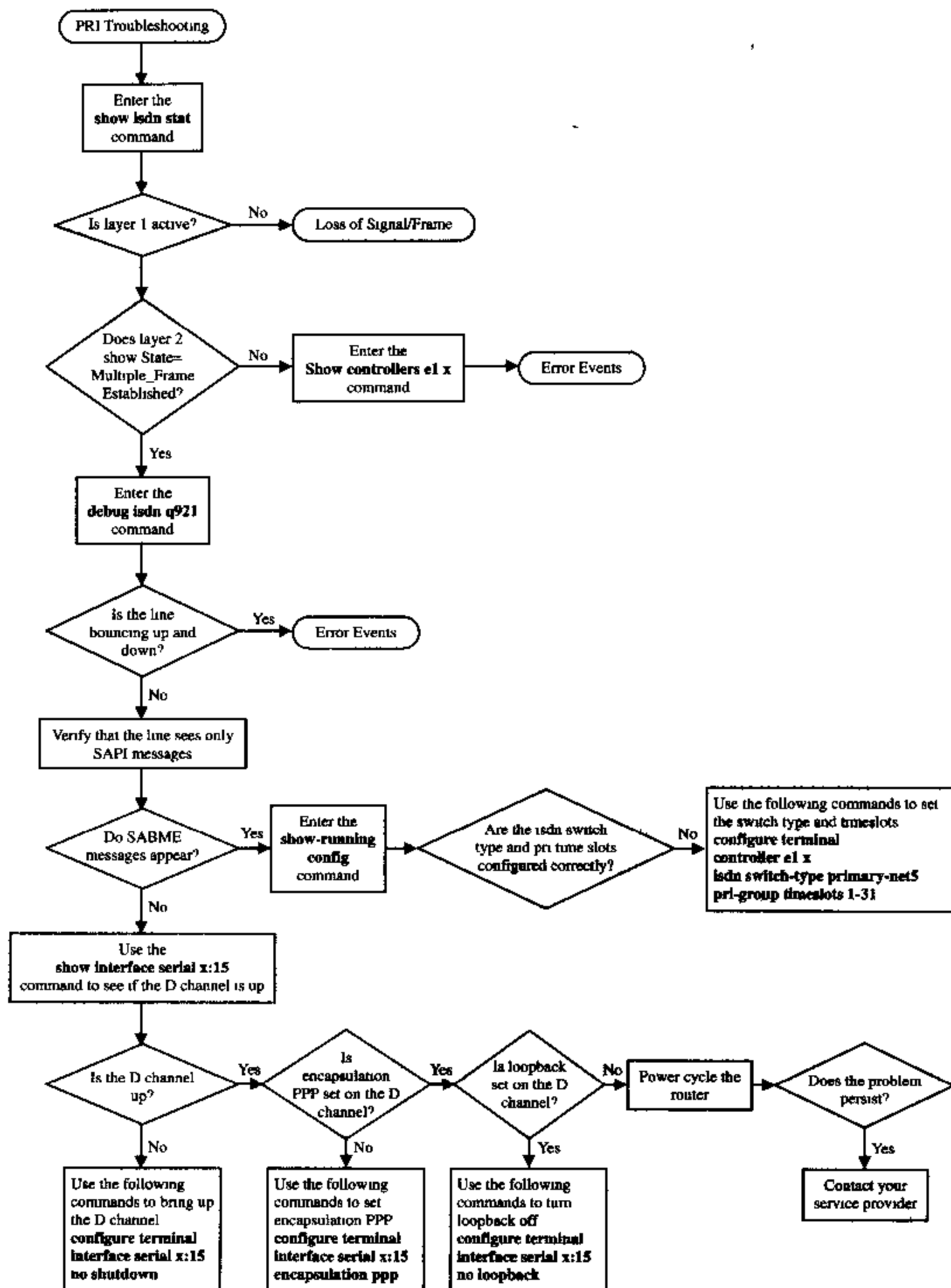


图 10-23 E1 线路排错流程之六

上面我们对最常使用的广域网链路类型（DDN、帧中继、E1）的排错进行了介绍，如果读者对其他的广域网链路如 ATM、POS 等感兴趣的话，请参考 Cisco 相关的文档，下面给出它

们的链接:

<http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Technologies&f=372>

10.7 网络层排错

网络层的故障主要表现在路由信息的错误上,这主要是由各种错误的路由协议的配置所导致。要想真正对路由进行排错,就需要对各种路由协议有较深的理解。这里我们不对各种路由协议进行分析,只给出最为基础也最为核心的路由表的解释,因为通过路由表,可以了解当前网络的状况,它可以告诉我们网络出现了故障。

Router#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

R 192.168.11.0/24 [120/1] via 192.168.1.2, 00:00:03, Serial0/0

C 192.168.10.0/24 is directly connected, FastEthernet0/0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.1/32 is directly connected, Serial0/0

C 192.168.1.0/30 is directly connected, Serial0/0

S 192.168.15.0/24 [1/0] via 192.168.1.2

Router#

以上是一个标准的路由表,下面我们截取其具有代表性的一项来进行分析。

R 192.168.11.0/24 [120/1] via 192.168.1.2, 00:00:03, Serial0/0

① ② ③ ④ ⑤ ⑥ ⑦

根据上面这条路由我们了解到路由表的每一项包含 7 个内容:

① 路由信息源:该项表明此条路由是如何获得的,这里的“R”表示通过“RIP”路由协议获得,所有的信息源代码在路由表的最上方显示;

② 目的地址:该项表明此条路由的目的地是哪里;

③ 管理距离:该项表明获得此条路由的协议的管理距离;

④ 度量值:该项表明此条路由所采用的度量;

⑤ 下一跳地址:该项表明为了到达目的地要经历的下一跳;

⑥ 该表项的时效:该项表明此条路由距上次更新有多长时间(注意只有动态路由协议才有此项);

⑦ 到达下一跳的本端接口：该项表明为了到达下一跳需要将数据分组从本端的该端口送出。

如果在网络的排错过程中，我们发现目的网络不在路由表中，就知道网络出现了故障。这时我们就可以针对各种路由协议进行相应的排查。如果读者对各种路由协议感兴趣，可参考 Cisco 的相关文档，以下是具体的链接。

<http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Technologies&f=770>

10.8 Cisco 故障诊断和排除资源

Cisco 的 CCO (Cisco Connection Online) 为我们提供了非常全面的有关 Cisco 产品的各种工具和信息，其中和排错有关的重要工具包括“Bug Toolkit”、“Error Message Decoder”和“Output Interpreter”。

在浏览器中输入“<http://www.cisco.com/go/tools>”，我们就可以到达 Cisco 的工具中心，这里涵盖了 Cisco 绝大多数的工具，如图 10-24 所示。

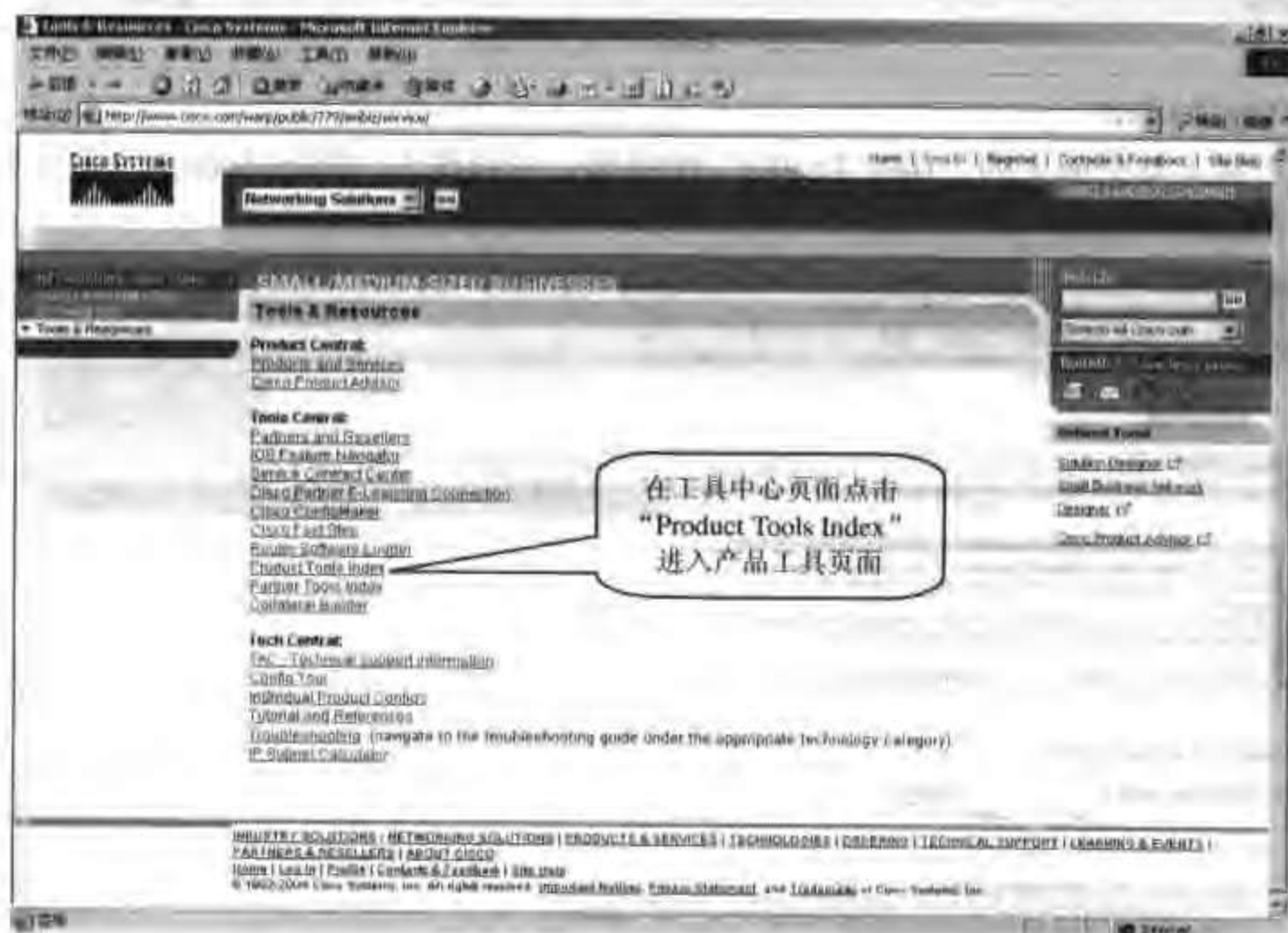


图 10-24 浏览 Cisco 的工具中心网页

在工具中心页面点击“Product Tools Index”，即可进入 Cisco 的产品工具页面，如图 10-25 所示。

在产品工具的页面我们可以看到“Bug Toolkit”、“Error Message Decoder”和“Output Interpreter”的链接，由此我们可以进入各个相应的工具。下面我们分别对这三个工具进行一下介绍。

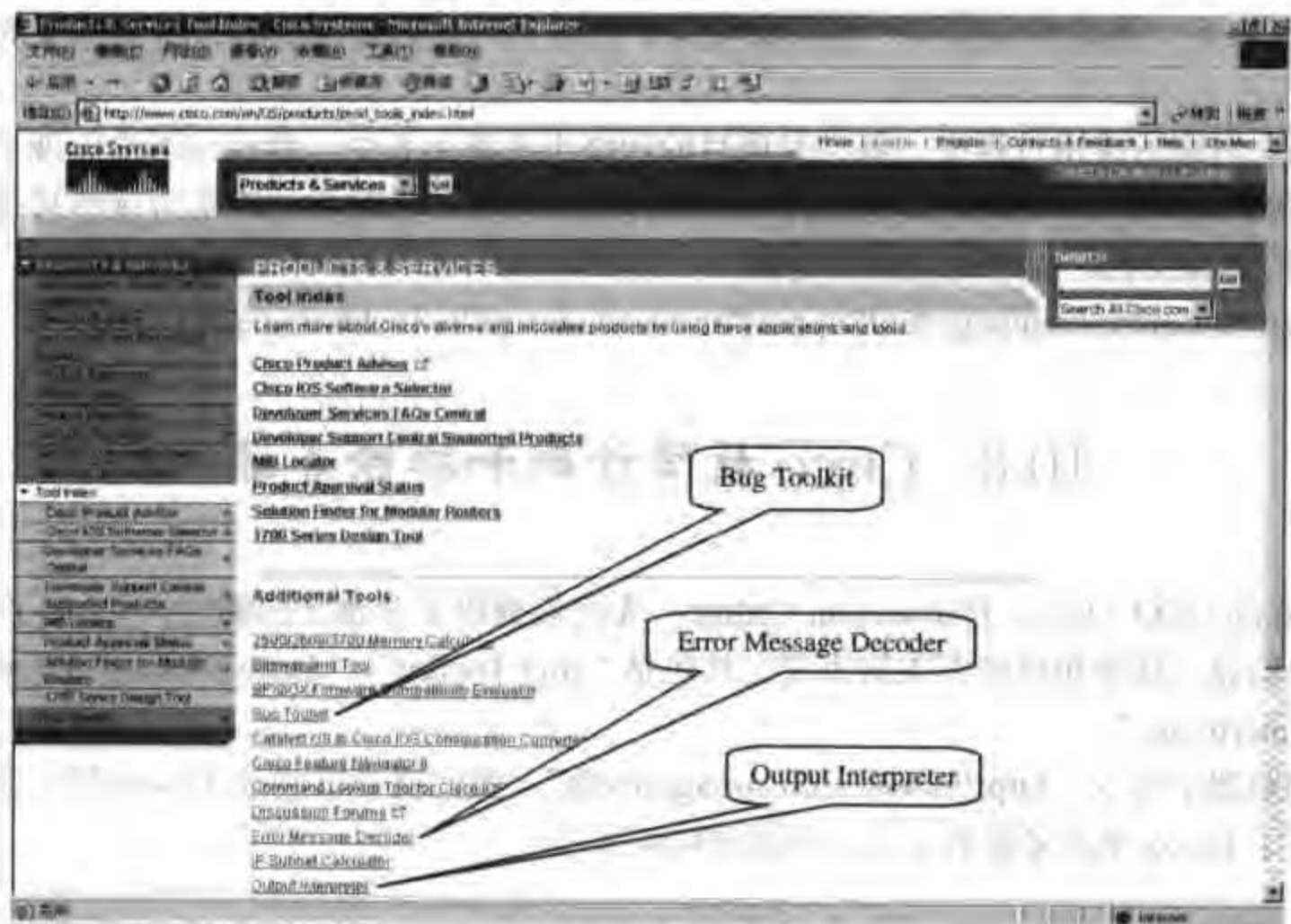


图 10-25 Cisco 的产品工具页面

(1) Bug Toolkit

单击产品工具页面上的“Bug Toolkit”的链接，可以进入“Bug Toolkit”工具页面，如图 10-26 所示。

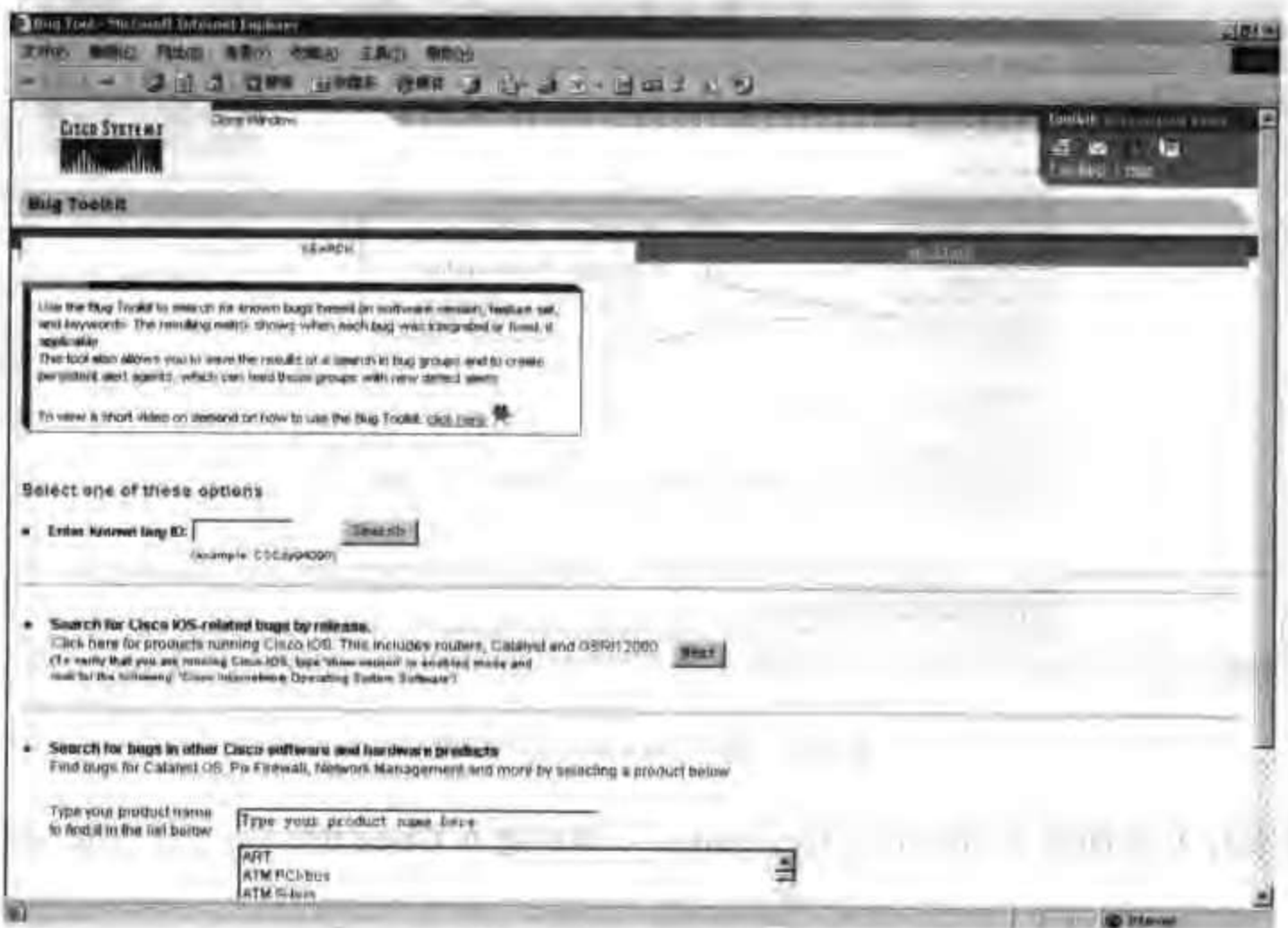


图 10-26 Cisco 的“Bug Toolkit”页面

通过此工具我们可以查询相关软件存在的 bug，根据 bug 给出的故障现象，我们可以判

断出自己网络的故障是否是由软件的 bug 引起的。

(2) Error Message Decoder

单击产品工具页面上的“Error Message Decoder”的链接,可进入“Error Message Decoder”工具页面,如图 10-27 所示。

我们可以将日志里记录的错误提示,通过此页面提交给 Cisco, Cisco 会给出可能导致错误的原因以及可以采取的排错手段的响应信息,如图 10-27~图 10-30 所示。



图 10-27 Error Message Decoder 页面之一

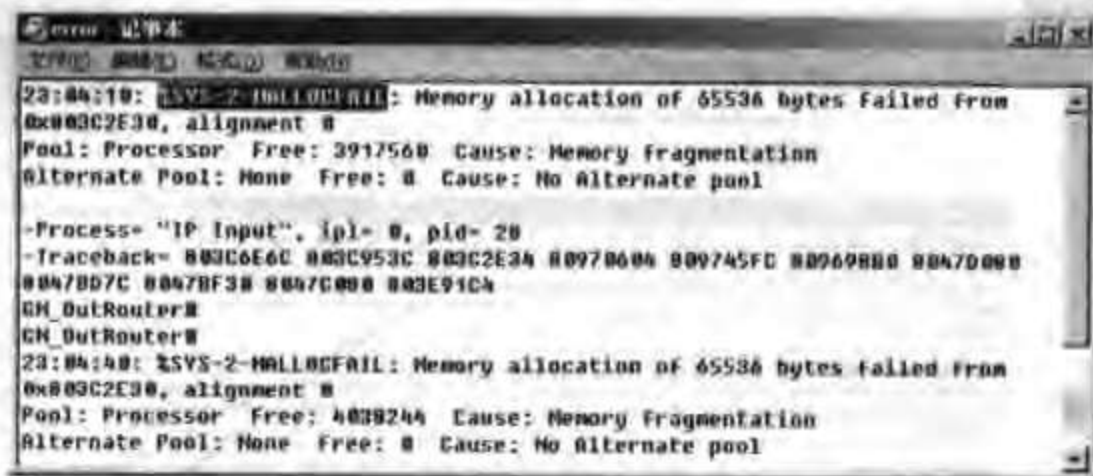


图 10-28 显示的 error 信息

Cisco 错误消息的格式如下:

%Facility - subfacility - Severity - Mnemonic : Message Text

Facility: 它指出错误消息涉及的设备名。该值可以是协议、硬件设备或者系统软件模块。

Subfacility: 它仅与通道接口处理器 (CIP) 卡有关。详细的信息可以参见 Cisco 文档的相关章节。

Severity: 它是一个范围在 0~7 之间的数字。数字的值越小,严重程度越高。

Mnemonic: 惟一标识错误消息的单值代码。该代码通常可以暗示错误的类型。

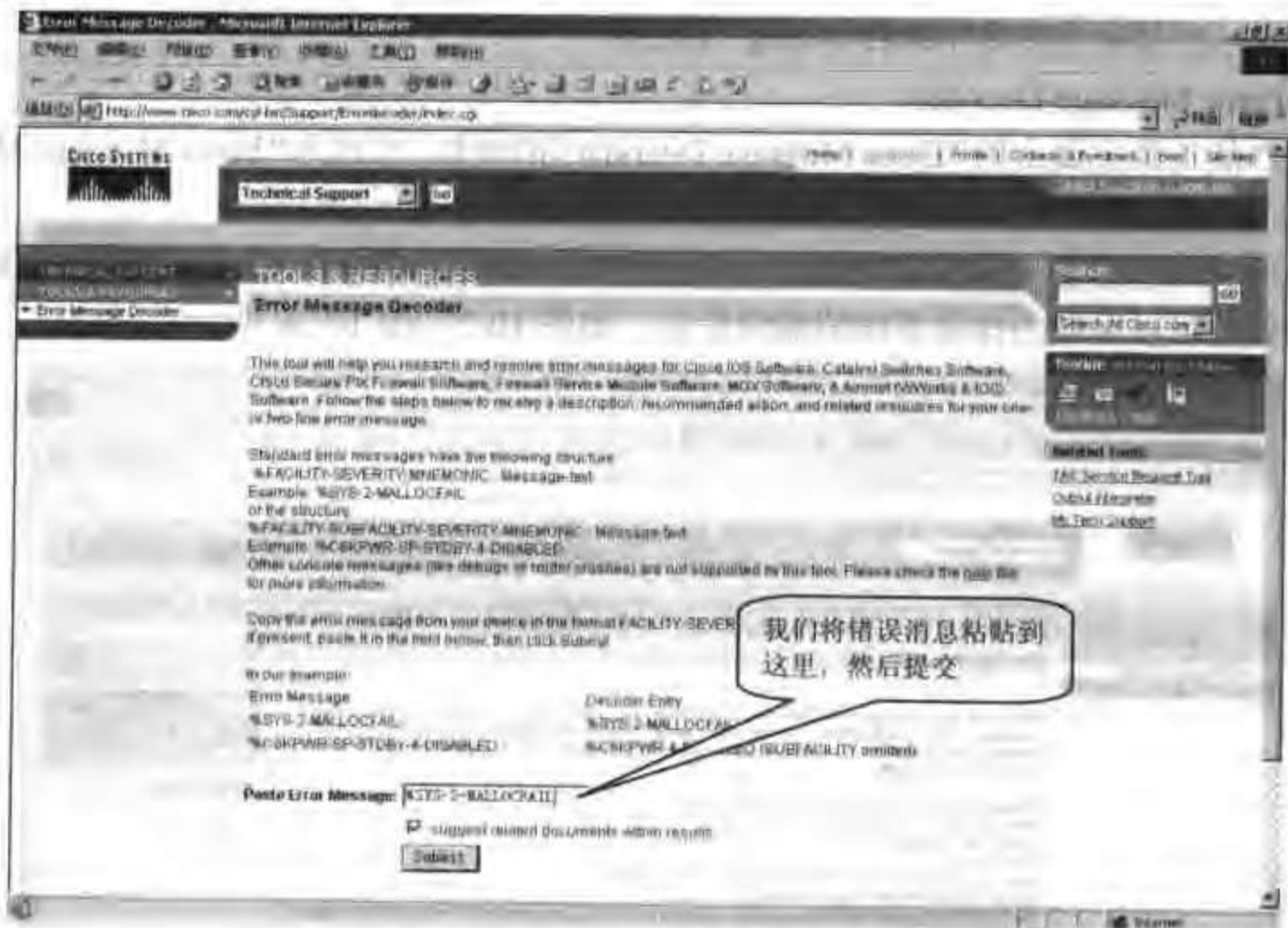


图 10-29 Error Message Decoder 页面之一

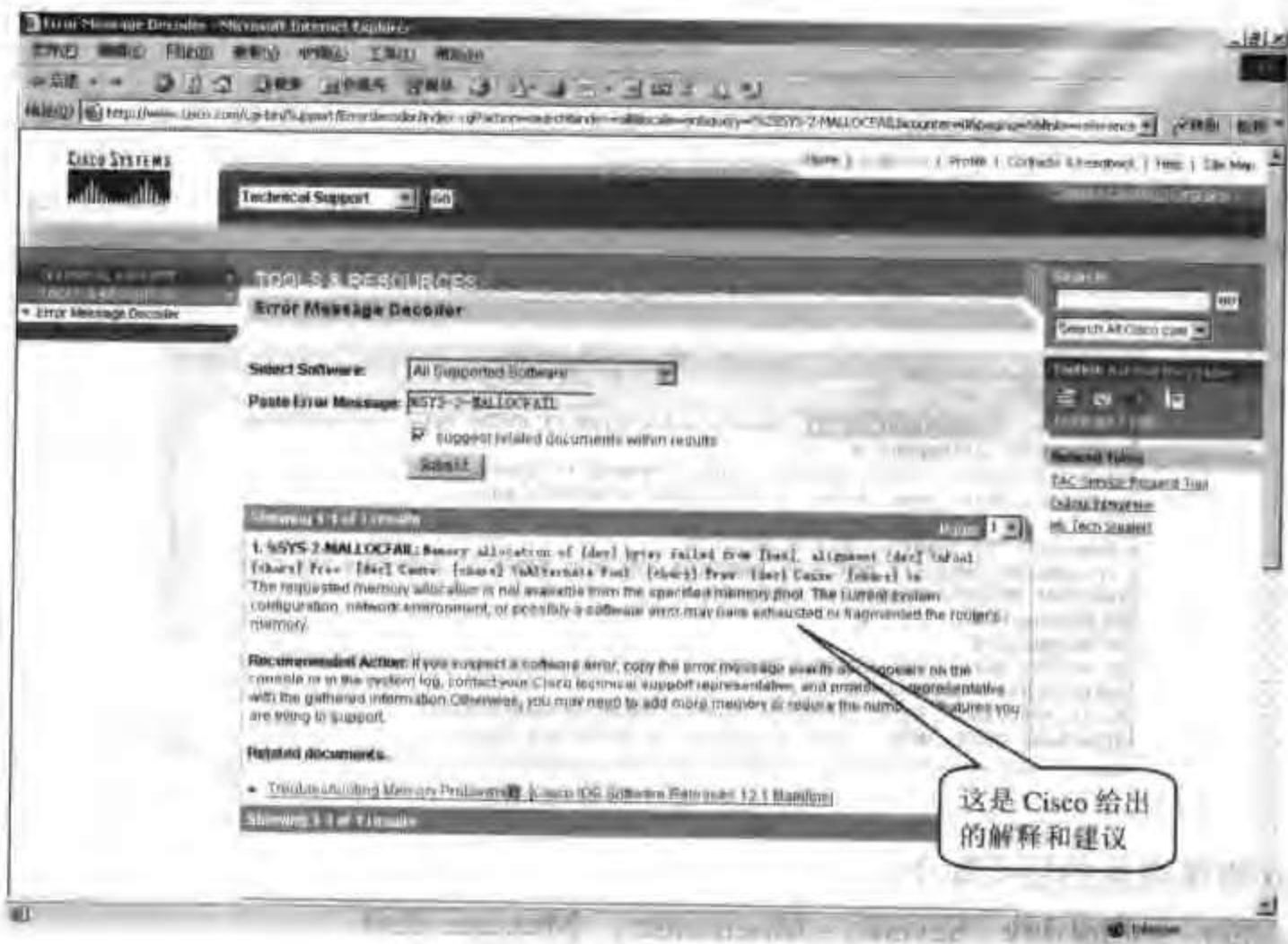


图 10-30 Error Message Decoder 页面之三

Message Text: 它是错误消息的简短描述，其中包括涉及的路由器硬件和软件信息。下面是一些错误消息的示例。

%DUAL-3-SIA: Route 171.155.148.192/26 stuck-in-active state in IP-EIGP 211. Cleaning up
%LANCE-3-OWNERR: Unit 0, buffer ownership error

(3) Output Interpreter

单击产品工具页面上的“Output Interpreter”的链接,可以进入“Output Interpreter”工具页面,如图 10-31 所示。

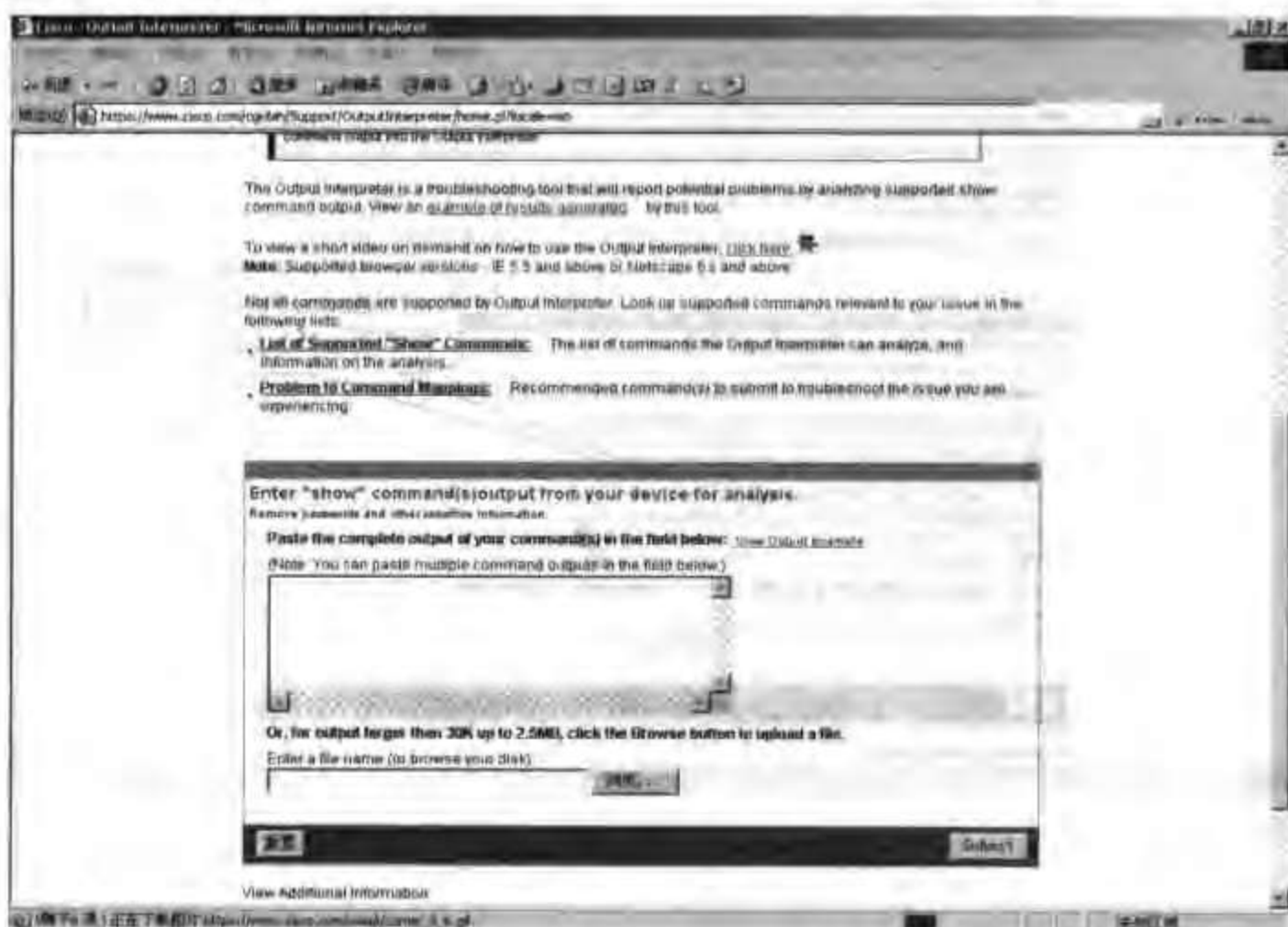


图 10-31 Cisco 的 Output Interpreter 页面之一

我们可以将 Cisco 设备的“show tech”信息通过此页面进行提交, Cisco 会给出可能存在的错误,以及可以采取的排错手段,如图 10-32~图 10-34 所示。



图 10-32 信息显示

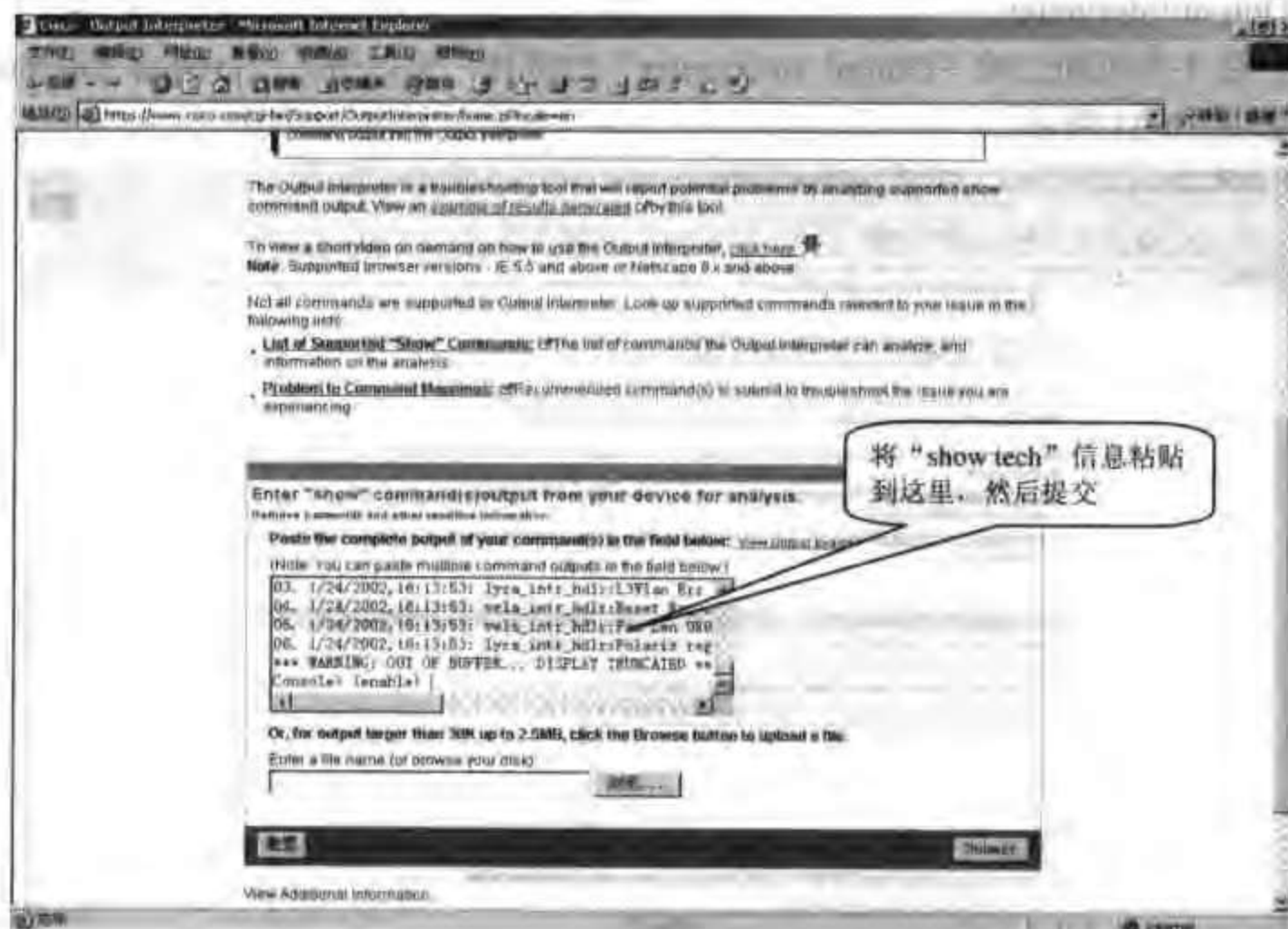


图 10-33 Output Interpreter 页面之二



图 10-34 Output Interpreter 页面之三

10.9 企业网排错案例

1. 案例 1

故障现象：公司远程分支机构一员工报告访问不了公司的服务器。公司的企业网如图 10-35 所示。



图 10-35 案例 1 中公司的企业网拓扑

分析：

在本章的开始，我们介绍了系统化的排错方法，其流程如图 10-1 所示。

针对本案例，我们可以按照图 10-1 中的流程进行排错：

(1) 定义问题：在本案例中，问题比较清楚，即远程分支的一个员工访问不了中心的服务器，需要注意的是，需要将问题定位到该员工的 PC 上（即 Pc_B）。

(2) 收集事实：通过询问和自己实际的测试，来收集与问题相关的一些事实，在本案例中我们可以收集以下一些事实：

- ① 分支其他员工的 PC 能否正常访问服务器；
- ② 总部员工的 PC 能否正常访问服务器；
- ③ 分支问题 PC (Pc_B) 能否 ping 通服务器 (Server_A)；
- ④ 分支问题 PC (Pc_B) 能否 ping 通总部路由器 (Router_A) 的广域网口地址 (192.168.1.1)；
- ⑤ 分支问题 PC (Pc_B) 能否 ping 通本地网关 (192.168.11.254)。

(3) 考虑可能性：根据上面收集到的事实，考虑各种可能导致故障的原因：

- ① 如果分支的其他员工的 PC 能够正常访问服务器，那么问题就存在于 Pc_B 上；
- ② 如果分支其他员工的 PC 也不能正常访问服务器，那么从分支的 PC 到服务器的所有设备都存在故障的可能。这时如果我们知道总部的 PC 可以正常访问服务器，即可以排除服务器故障的可能，那么故障就可能存在于 Router_A、Router_B 和广域链路上。但如果总部的 PC 也不能访问服务器，那么基本可以断定是服务器出了故障；

③ 如果分支问题 PC (Pc_B) 能 ping 通服务器 (Server_A)，说明 Pc_B 至服务器的网络层工作是正常的，因此问题可能出现在 Pc_B 或服务器的应用层上；

④ 如果分支问题 PC (Pc_B) 不能 ping 通服务器 (Server_A)，那说明 Pc_B 至服务器的网络层工作是不正常的，这时如果我们需要从 Pc_B 由远及近分别 ping Router_A 的广域网口地址 (192.168.1.1) 和 Router_B 的局域网口地址 (192.168.11.254)。如果能 ping 通 Router_A 的广域网口地址 (192.168.1.1)，说明问题存在于总部的局域网内，很有可能是服务器上缺乏网关地址或 Router_A 的局域网口 (Fa0/0) 存在问题；如果不能 ping 通 Router_A 的广域网口地址 (192.168.1.1)，但能 ping 通本地网关 (192.168.11.254)，说明问题可能出在广域链路上；

如果不能 ping 通本地网关 (192.168.11.254), 那么问题主要出在本地局域网内, 很可能是本地 PC (Pc_B) 的网关设置不正确或 Router_B 的局域网口 (Fa0/0) 存在问题。

(4) 根据可能的故障原因, 制定相应的排错计划:

① 如果问题存在于 Pc_B 本身, 这时极有可能是它的网关配置不正确, 或是其网卡驱动的问题, 重新配置网关或安装驱动程序, 排除故障;

② 如果分支的 PC 和总部的 PC 都不能正常访问服务器, 那么极有可能是服务器出了故障, 重新为其安装网卡驱动或替换新的网卡, 排除故障;

③ 如果问题出现在 Pc_B 或服务器的应用层上, 那么需要为服务器重新安装服务器软件或为 Pc_B 重新安装客户端软件, 排除故障;

④ 如果问题存在于总部的局域网内, 很有可能是服务器上缺乏网关地址或 Router_A 的局域网口 (Fa0/0) 存在问题, 这时需要重新配置服务器的网关, 或对 Router_A 的局域网口 (Fa0/0) 进行故障排除;

⑤ 如果问题出在广域链路上, 参照前面介绍的各种广域链路的排错方法进行故障排除;

⑥ 如果问题出在本地局域网内, 很可能是本地 PC (Pc_B) 的网关设置不正确或 Router_B 的局域网口 (Fa0/0) 存在问题, 这时需要重新配置 Pc_B 的网关, 或对 Router_B 的局域网口 (Fa0/0) 进行故障排除。

2. 案例 2

故障现象: 公司一员工反映访问不了 Internet。企业网接入 Internet 的拓扑如图 10-36 所示。

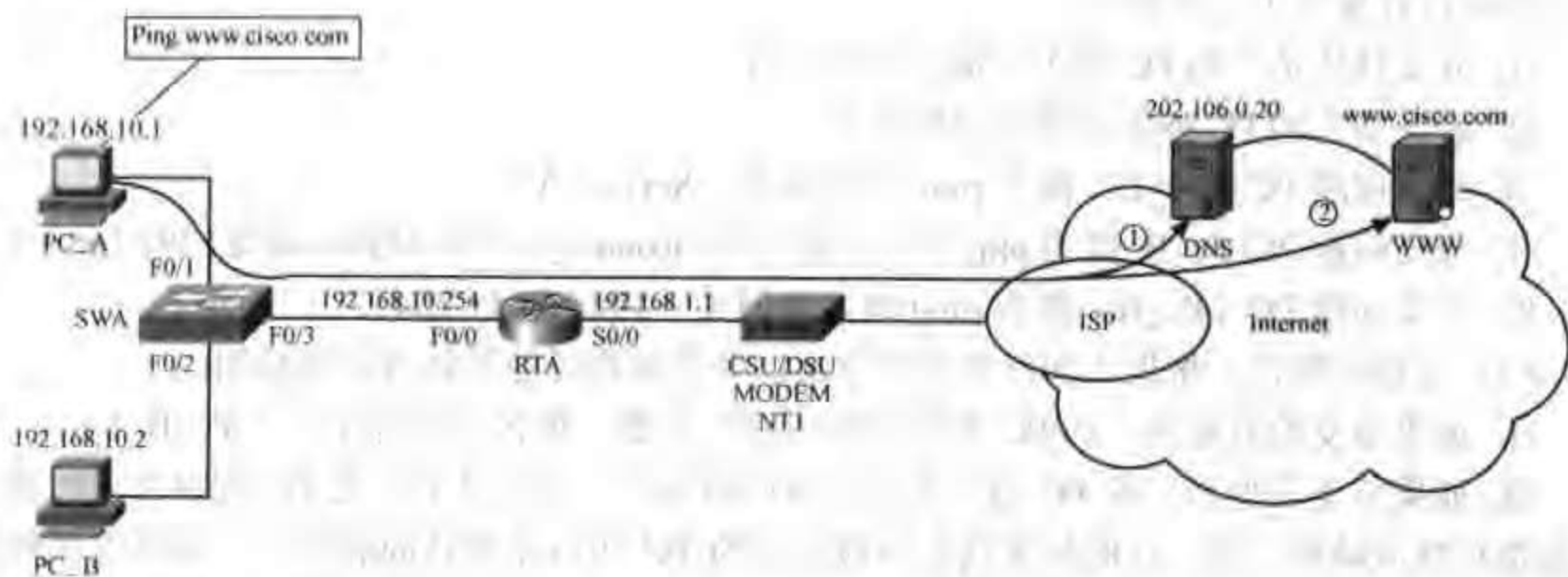


图 10-36 企业网接入 Internet 的拓扑

和案例 1 一样, 针对本案例同样采用系统化的方式进行排错:

(1) 定义问题: 在本案例中, 问题比较清楚, 即公司一个员工访问不了 Internet, 这里我们需要将问题定义为: Pc_A 无法访问 Cisco 的网站 (www.cisco.com);

(2) 收集事实: 通过询问和自己实际的测试, 来收集与问题相关的一些事实, 在本案例中, 可以收集以下一些事实:

① 问题 PC (Pc_A) 能否访问其他网站;

② 公司其他员工的 PC 能否正常访问 Internet;

③ 问题 PC (Pc_A) 能否 Ping 通公网 IP (比如 211.154.160.4), (需要说明的是我们所

举的公网上的 IP 一定是能够 Ping 的才可以, 因为现在许多公网的 IP 都是不允许 Ping 的);

④ 问题 PC (Pc_A) 能否正常接入 DNS 服务器 (nslookup)。如图 10-37 所示为 Pc_A 能正常接入 DNS。



注: 图中显示表明, 能正常访问 DNS 服务器, 从 DNS 服务器上也能正常解析到域名 www.cisco.com 的地址 (198.133.219.25)

图 10-37 问题 PC 能接入 DNS

⑤ 问题 PC (Pc_A) 能否 ping 通本地网关 (192.168.10.254)。

(3) 考虑可能性: 根据上面收集到的事实, 考虑各种可能导致故障的原因:

① 如果问题 PC (Pc_A) 能够访问其他网站, 那说明本地不存在问题, 问题可能是 DNS 不能解析那个域名 (www.cisco.com), 或是通往 Cisco 网站服务器的链路出了问题, 也有可能是 Cisco 网站服务器本身出了问题。

② 如果公司的其他员工的 PC 能够正常访问 Internet, 那么问题就存在于 Pc_A 上。

③ 如果公司的其他员工的 PC 也不能正常访问 Internet, 那么问题可能是本地局域网的故障、本地路由器 (RTA) 的故障、Internet 接入链路或是 DNS 解析的故障等。这时如果问题 PC (Pc_A) 能 Ping 通公网上的一个 IP (比如 211.154.160.4), 那么问题可能主要集中在 DNS 解析上; 如果不能 Ping 通公网上的一个 IP (比如 211.154.160.4), 但能 ping 通本地网关 (192.168.10.254), 那么问题可能存在于 Internet 接入链路上; 如果不能 ping 通本地网关 (192.168.10.254), 那么问题存在于本地局域网内。

(4) 根据可能的故障原因, 制定相应的排错计划

① 如果问题不存在于本地, 那没必要对本地进行调整。

② 如果问题存在于 Pc_A 上, 那么极有可能是该机的网关设置不正确或其网卡出了问题。如果网关不正确, 重新设置即可。另外, 可以通过 ping 同网段其他的 PC 来验证其网卡工作是否正常, 如果不正常重新为其安装网卡驱动或替换新的网卡, 排除故障。

③ 如果问题出现在 DNS 解析上, 那么我们可以重新配置另外一个 DNS, 排除故障。

④ 如果问题出在 Internet 接入链路上, 参照前面介绍的各种广域链路的排错方法进行故障排除。

⑤ 如果问题出在本地局域网内, 很可能是本地 PC (Pc_A) 的网关设置不正确或 RTA

的局域网口(Fa0/0)存在问题,这时需要重新配置 Pc_A 的网关,或对 RTA 的局域网口(Fa0/0)进行故障排除。

10.10 小 结

要顺利地诊断并排除网络故障,我们应该具备两方面的技能:一方面是对网络技术和各种协议要有一个清楚的理解,因为它是诊断与排除网络故障的基础;另一方面是需要将所掌握的知识以有条理的系统的方式应用于诊断和排除网络故障的过程中。

本章虽然讲述了一些排错的命令和 Cisco 提供给用户的排错的资源,但是我们更重视的是故障诊断与排除的系统化的方法,因为网络知识和各种工具固然重要,但只有采用系统化的方法才能真正使其发挥作用,达到事半功倍的效果。

附录 A Cisco IOS 命名规范

因特网操作系统软件（IOS，Internet Operation System Software）是 Cisco System 公司跨越主要路由和交换产品的软件平台，为不同需求的客户提供统一的操作控制界面，并提供对所有标准的网络互联协议和几十种 Cisco 私有网络协议的全面支持。IOS 软件不但可以完成 RIP、EIGRP、OSPF、ISIS、BGP 等路由计算功能，还集成了诸如 Firewall、NAT、DHCP、FTP、HTTP、TFTP、Voice、Multicast 等诸多服务功能，是业内最为复杂和完善的网络操作系统之一。

目前来看，Cisco 已将 IOS 软件应用到了其大部分产品当中，尤其是路由器和交换机产品基本上都合并到了 IOS 软件上。尽管 IOS 应用广泛，但是仍然有相当多的网络工程师对 IOS 的命名不甚了解，为了更好地管理这些设备，有必要对 Cisco IOS 软件的命名规范进行一下介绍。

Cisco 的 IOS 软件映像文件的文件名有一定的命名规则，下面我们来看一个实际的 Cisco 的 IOS 文件名：

c2600-is-mz.122-23

① ② ③ ④

从上例我们看出 Cisco IOS 文件名实际包括四个部分：

- ①：硬件平台；
- ②：特性集；
- ③：运行方式；
- ④：版本号。

下面我们分别对这四部分进行介绍。

（1）硬件平台：

c2600-is-mz.122-23 中的“c2600”代表了该软件适用的硬件平台，如“c2600”表示的是 Cisco2600 系列路由器，“RSP”代表的是 Cisco7500 路由器，而“GSR”则代表 Cisco 的高端产品吉比特交换路由器。常见的硬件平台代码见附表 A-1。

附表 A-1 硬件平台代码

代 码	硬件平台
c1700	Cisco 1700 系列路由器
c2600	Cisco 2600 系列路由器
c3620	Cisco 3620 路由器
c3640	Cisco 3640 路由器
c3660	Cisco 3660 路由器
c3725	Cisco 3725 路由器

续表

代 码	硬件平台
c3745	Cisco 3745 路由器
c7200	Cisco 7200 系列路由器
rsp	Cisco 75xx RSP
gsr	GSR 12000
ubr7200	通用宽带路由器 7200
c2950	Catalyst 2950 系列交换机
c3550	Catalyst 3550 系列交换机
cat4000	Catalyst 4000 系列交换机

注意：

Catalyst6000 系列交换机的软件有些特殊，它包括两种模式：一种是 Hybrid（杂交）模式，另一种是 Native（纯种）模式。

Hybrid 模式：是指交换机的引擎运行 CatOS 软件，处理二层的交换功能，而 MSFC 运行 IOS 软件，处理三层路由功能。在此模式下的软件代码见附表 A-2。

附表 A-2

Hybrid 模式的软件代码

代 码	硬件平台
cat6000-sup	监视器 1 和 1A (1 代引擎)
cat6000-sup2	监视器 2 (2 代引擎)
cat6000-sup720	监视器 720 (720 引擎)
c6msfc	MSFC 1 (1 代 MSFC)
c6msfc2	MSFC 2 (2 代 MSFC)
c6msfc3	MSFC 3 (3 代 MSFC)
c6msfc-boot	MSFC 1 boot image (1 代 MSFC 引导软件)
c6msfc2-boot	MSFC 2 boot image (2 代 MSFC 引导软件)

Native 模式：是指引擎和 MSFC 都统一运行一个 IOS 软件。在此模式下的软件代码见附表 A-3。

附表 A-3

Native 模式的软件代码

代 码	硬件平台
c6sup	监视器 1, MSFC 1 (1 代引擎, 1 代 MSFC)
c6sup11	监视器 1, MSFC 1 (1 代引擎, 1 代 MSFC)
c6sup12	监视器 1, MSFC 2 (1 代引擎, 2 代 MSFC)
c6sup22	监视器 2, MSFC 2 (2 代引擎, 2 代 MSFC)
s72033	MSFC 3, PFC 3 (720 引擎, 3 代 MSFC, 3 代 PFC)

(2) 特性集：

c2600-is-mz.122-23 中的“is”代表了该软件具有的特性集，如“is”表示的是 IP PLUS 特性集，其他常见的软件特性集代码见附表 A-4。

附表 A-4

软件特性集代码

代 码	特性集
a	APPN 特性集
b	AppleTalk
boot	Boot Image (引导软件)
c	远程访问服务子集
d	Desktop 特性集
f	FRAD 子集
g	ISDN 特性集
i	IP 特性集
j	企业特性集
j1	c2600/c3600 的基础企业版
k8	低于或等于 64 位加密(DES), 12.2 或更高版本
k9	高于 64 位的强加密(3DES、AES), 12.2 或更高版本
n	IPX 特性集
o	防火墙特性集
o3	有指令检测的 Firewall(Firewall 第二阶段)
q	异步
p	运营商特性集
r	IBM 特性集
s	11.2 或更高版本的 plus 特性集
s3	c2600/c3600 基本的 plus 特性集
v	VIP 和双 RSP 支持
x	X.25/FR/H.323
y	简化的 IP 特性集
y7	IP/ADSL (c1700)
z	可管理 MODEM
40	40 位加密
56	56 位加密
56t	56 位加密, 支持 IPSEC 12.1 或更高版本还包括 SSH

(3) 运行方式:

Cisco 早期的低端设备如 2500 系列的 IOS 并没有运行在内存中, 而是运行在 Flash 卡中。所以, IOS 文件名中指定了这一特性, 如 c2600-is-mz.122-23 中的“m”表示在内存(RAM)中运行, 如果是“f”表示在 Flash 卡中运行, 如果是“r”则表示在 ROM 中运行。文件名中的“z”表示的是映像文件经过了 ZIP 格式的压缩, 还可以是以“x”表示为 MZIP 压缩, 或者用“w”表示是 Stac 算法压缩。运行方式和压缩格式的代码见附表 A-5。

附表 A-5

运行方式和压缩格式代码

代 码	运行方式
f	Flash

续表

代 码	运行方式
m	RAM
r	ROM
l	重分配
代 码	压缩格式
z	zip 压缩(注意小写)
x	mzip 压缩
w	Stac 压缩

(4) 版本号:

c2600-is-mz.122-23 中的“122-23”代表了该软件的版本号。IOS 常见的版本号如下所示:
10.3、11.0、11.1、11.2、12.0、12.1、12.2、12.3

其中, 10.3~11.2 已基本停止使用;
12.0、12.1、12.2 为目前路由器中常见的版本;
12.3 为最新版本。

注意:

对于正在使用的生产网来说, 升级网络设备的软件是要冒一定风险的。新的软件版本尽管可以带来更多的新特性, 也往往会带来更多的软件 Bug 甚至是某些意想不到的错误。因此, 建议只有出现下列情况时, 才考虑升级并替换已经被证明能够稳定运行的新的软件版本:

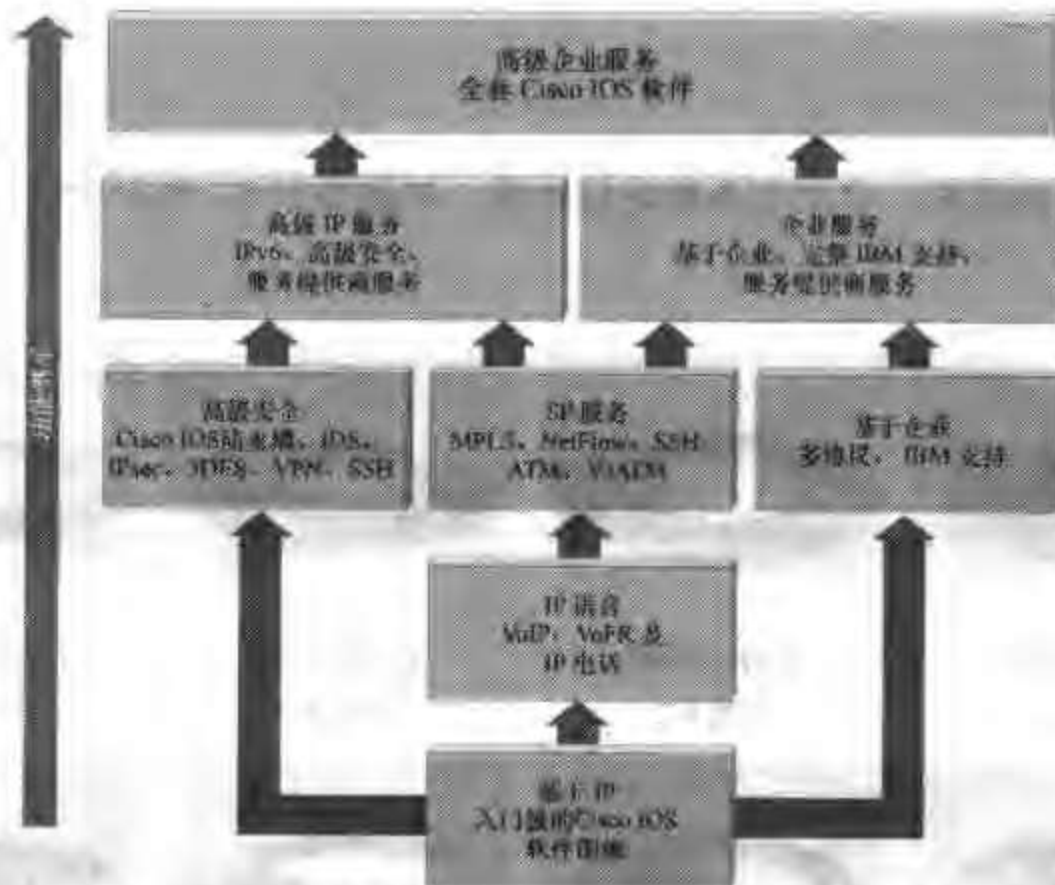
- 目前的软件版本不支持某些即将开展的新业务, 如 Voice/Video 或 QoS;
- 目前的软件版本不支持某些即将更新的硬件平台或板卡;
- 目前的软件版本即将进入停止服务期 (EOE);
- 目前的软件版本存在明显的安全漏洞或被证明有某些致命缺陷。

补充:

Cisco 从最新的 12.3 版 IOS 开始, 引入了“IOS 产品包”(IOS packaging)的概念, 目的是为了简化软件选择过程, 并减少功能集的混乱, 同时提供在不同平台与工具上采用一致的命名方式, 这将极大地方便用户对 IOS 的选择和使用。我们知道选择合适的 IOS 软件并非易事, 因为它有多达 44 个功能集。而有了 IOS 产品包后, 它将被整合为 8 个, 这 8 个产品包如下:

- ① IP 基础 (IP Base): 入门级预装包;
- ② IP 语音 (IP Voice): 在 IP 基础中加入了 IP 电话、VoIP、VoFR;
- ③ SP 服务 (SP Services): 在 IP 语音中加入了 NetFlow、SSH、ATM、VoATM、MPLS;
- ④ 高级安全 (Advanced Security): 在 IP 基础中加入了 Cisco IOS FW、IDS、SSH、IPsec VPN、3DES;
- ⑤ 企业基础 (Enterprise Base): 在 IP 基础中加入了多协议和 IBM 支持;
- ⑥ 企业服务 (Enterprise Services): 在企业基础中加入了完整的 IBM 支持、服务提供商服务;

- ⑦ 高级 IP 服务 (Advanced IP Services): 在 SP 服务中加入了 IPv6、高级安全特性;
- ⑧ 高级企业服务 (Advanced Enterprise Services): 完整的 Cisco IOS 软件。
- IOS 产品包如附图 A-1 所示。



附图 A-1 Cisco 的 IOS 产品包

说明: 图中每个产品包都继承了它下面的包中的所有功能和服务。

新软件包命名使用了以下类别:

基础 (Base): 入门级产品包 (包括 IP 基础和企业基础);

服务 (Services): 加入了 MPLS、NetFlow、IP 电话服务、VoIP、VoFR 以及 ATM (包括 SP 服务和企业服务);

高级 (Advanced): 加入了 VPN、Cisco IOS 防火墙、3DES 加密、Cisco IOS IPsec 以及入侵检测系统 (包括高级安全和高级 IP 服务);

企业 (Enterprise): 加入了多协议: IBM、IPX、Appletalk (包括企业基础和企业服务)。

附录 B 常用线缆介绍

在进行网络的构建时，会用到各种连接线缆，如附图 B-1~ B-16 所示为一些最为常用的线缆。



CAB-V35MT
附图 B-1



CAB-V35FC
附图 B-2



CAB-232MT
附图 B-3



CAB-232FC
附图 B-4



CAB-SS-V35MT
附图 B-5



CAB-SS-V35FC
附图 B-6



CAB-SS-232MT
附图 B-7



CAB-SS-232FC
附图 B-8



CAB-OCTAL-ASYNC
附图 B-9



CAB-OCT-V35-MT
附图 B-10



CAB-OCT-V35-FC
附图 B-11



CAB-E1PRI
附图 B-12



CAB-E1BNC
附图 B-13



SC-SC 光纤跳线
附图 B-14



ST-ST 光纤跳线
附图 B-15

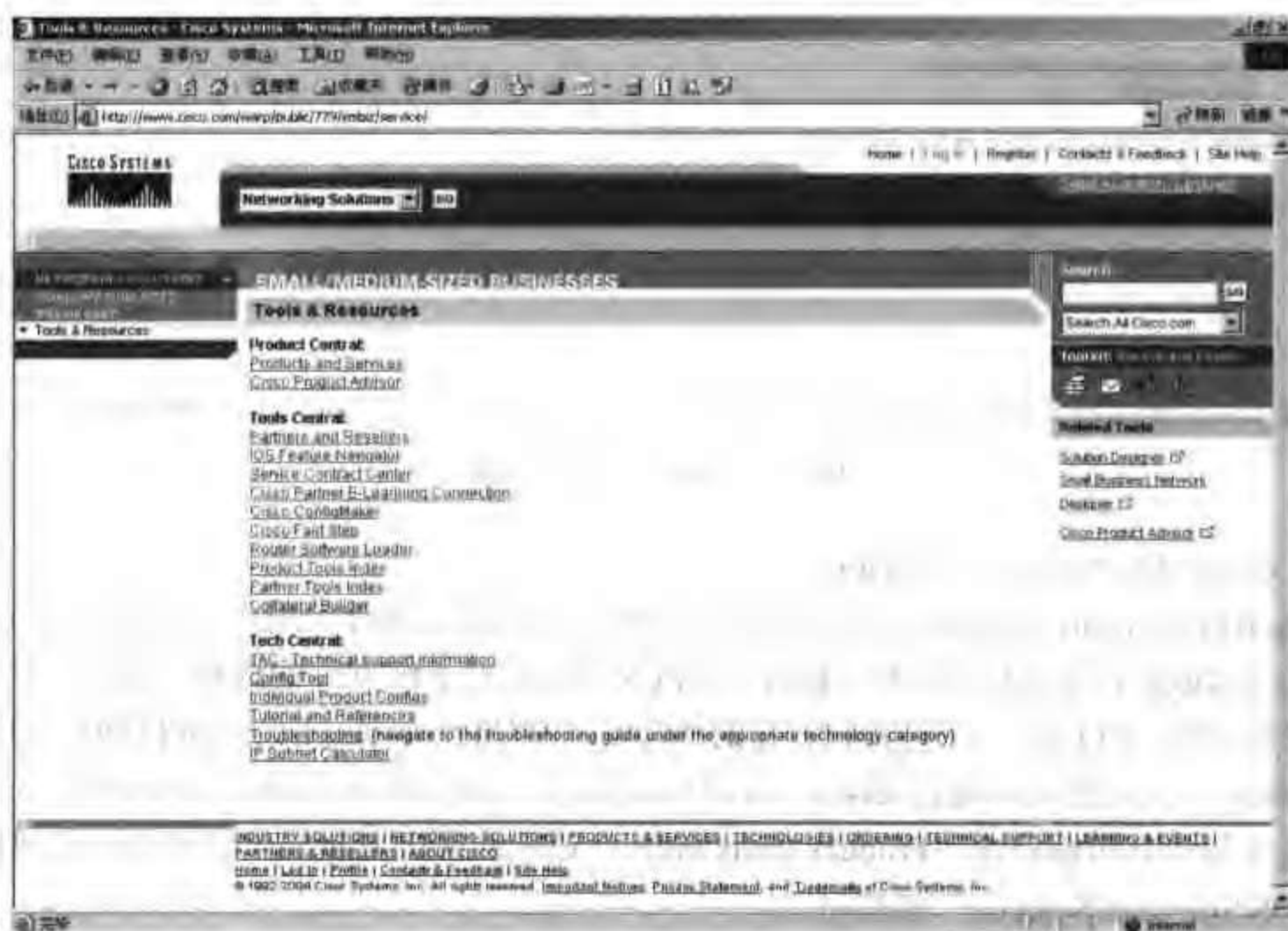


SC-ST 光纤跳线
附图 B-16

附录 C Cisco 常用工具和链接

Cisco 的网站 CCO (www.cisco.com 思科在线) 给我们提供了非常丰富的资源, 尤其是有关 Cisco 产品的各种工具和信息对我们学习和工作非常有帮助。下面就对常用的工具作一简要的介绍。

在浏览器中输入“<http://www.cisco.com/go/tools>”, 我们就可以到达 Cisco 的工具中心网页, 这里涵盖了 Cisco 绝大多数的工具, 如附图 C-1 所示。



附图 C-1 Cisco 的工具中心网页

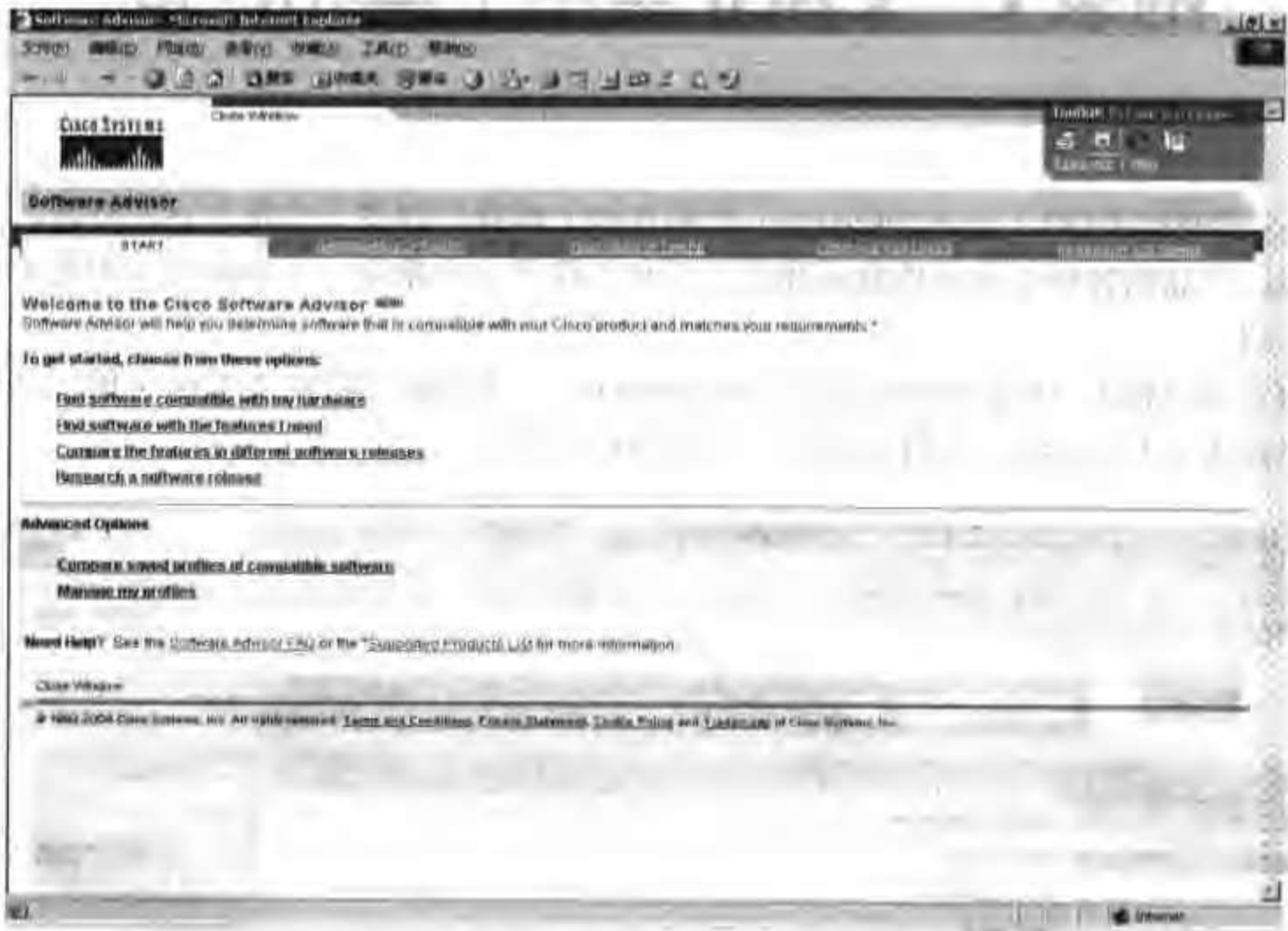
1. 售前工具

假如我们从事的是售前的工作, 那么就可能会使用到如下的几个工具:

(1) Cisco Software Advisor

Cisco 提供的工具 Software Advisor 是一套软件信息查询工具的集合, 它可以让访问者按照需要的硬件平台信息或是需要的软件特性信息进行 IOS 版本的查询, 同时还可以进行软件版本包含特性的比较, 如附图 C-2 所示。需要说明的是, 这个工具需要有一定权限的 CCO 账号才能访问到。它的链接地址是“<http://tools.cisco.com/Support/Fusion/FusionHome.do>”。我们也可以通过 Cisco 工具中心总页面 (<http://www.cisco.com/go/tools>) 进入, 方法是在工具中心

页面点击“Product Tools Index”进入产品工具页面，在产品工具页面点击“Software Advisor”链接进入。



附图 C-2 Software Advisor 页面

(2) Cisco IOS Software Selector

Cisco IOS Software Selector 可以帮助我们选择合适的 IOS 软件，用户可以根据硬件平台、所采用的技术或软件需支持的特性（BGP、MPLS 等）进行 IOS 软件的选择。这个工具同样需要有一定权限的 CCO 账号才能访问到。它的链接地址是“<http://tools.cisco.com/TTDIT/ISTMAIN/servlet/index>”，我们也可以通过 Cisco 工具中心总页面（<http://www.cisco.com/go/tools>）进入，方法是在工具中心页面点击“Product Tools Index”进入产品工具页面，在产品工具页面点击“Cisco IOS Software Selector”链接进入。

Cisco IOS Software Selecfor 的页面如附图 C-3 所示。

(3) IOS Feature Navigator

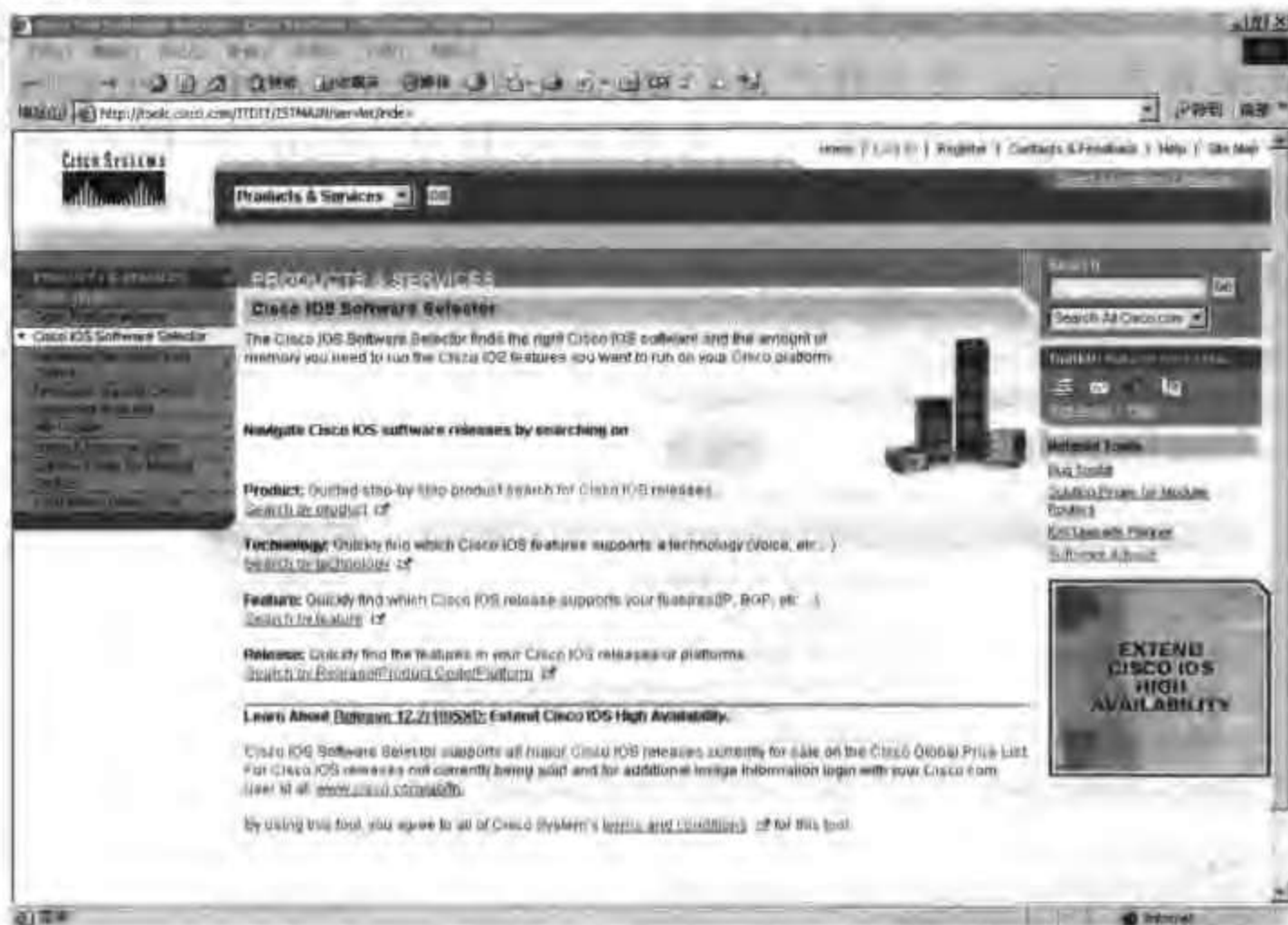
Cisco IOS Feature Navigator 可以帮助我们了解 IOS 软件对所需要的特性的支持。这个工具同样需要有一定权限的 CCO 账号才能访问到。它的链接地址是“<http://tools.cisco.com/TTDIT/CFN/jsp/index.jsp>”，我们也可以从 Cisco 工具中心总页面（<http://www.cisco.com/go/tools>）直接点击“IOS Feature Navigator”进入。

Cisco IOS Feature Navigator 的页面如附图 C-4 所示。

(4) Partner Business Central

Cisco Partner Business Central 是 Cisco 提供给合作伙伴的商务中心，从这里我们可以进行产品的查找、产品性能的比较、浏览及配置产品以及产品网上的采购等工作。这个工具同样需要有一定权限的 CCO 账号才能访问到。它的链接地址是“<http://www.cisco.com/dprg>”，如

附图 C-5 所示。



附图 C-3 Cisco IOS Software Selector 页面



附图 C-4 IOS Feature Navigator 的页面

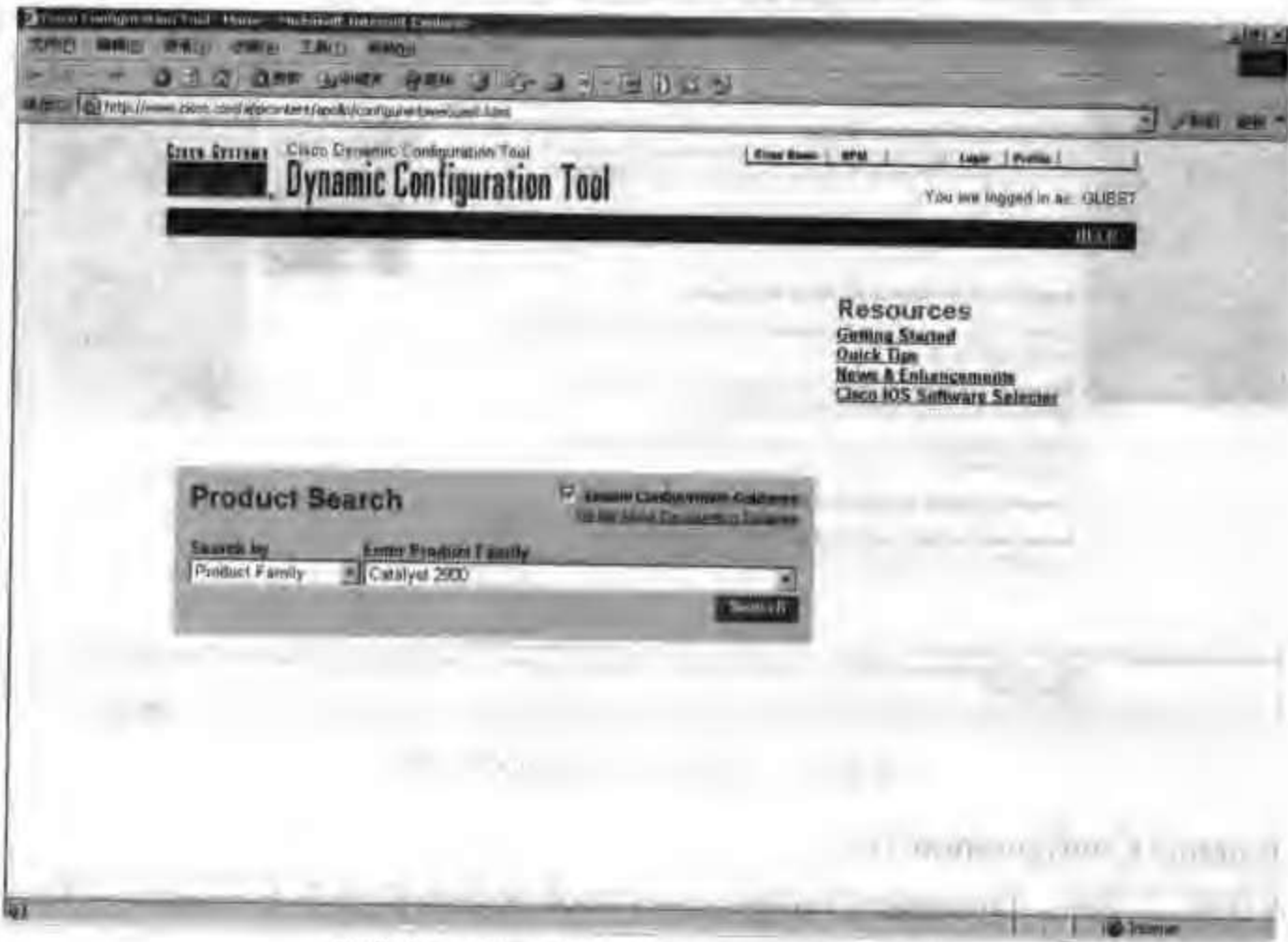
(5) Dynamic Configuration Tool

在所有售前工具中，Dynamic Configuration Tool 应该是使用率非常高的一个。因为 Cisco 的设备品目繁多，每种设备支持的模块也千差万别，因此想正确地为客户配置一款产品并非

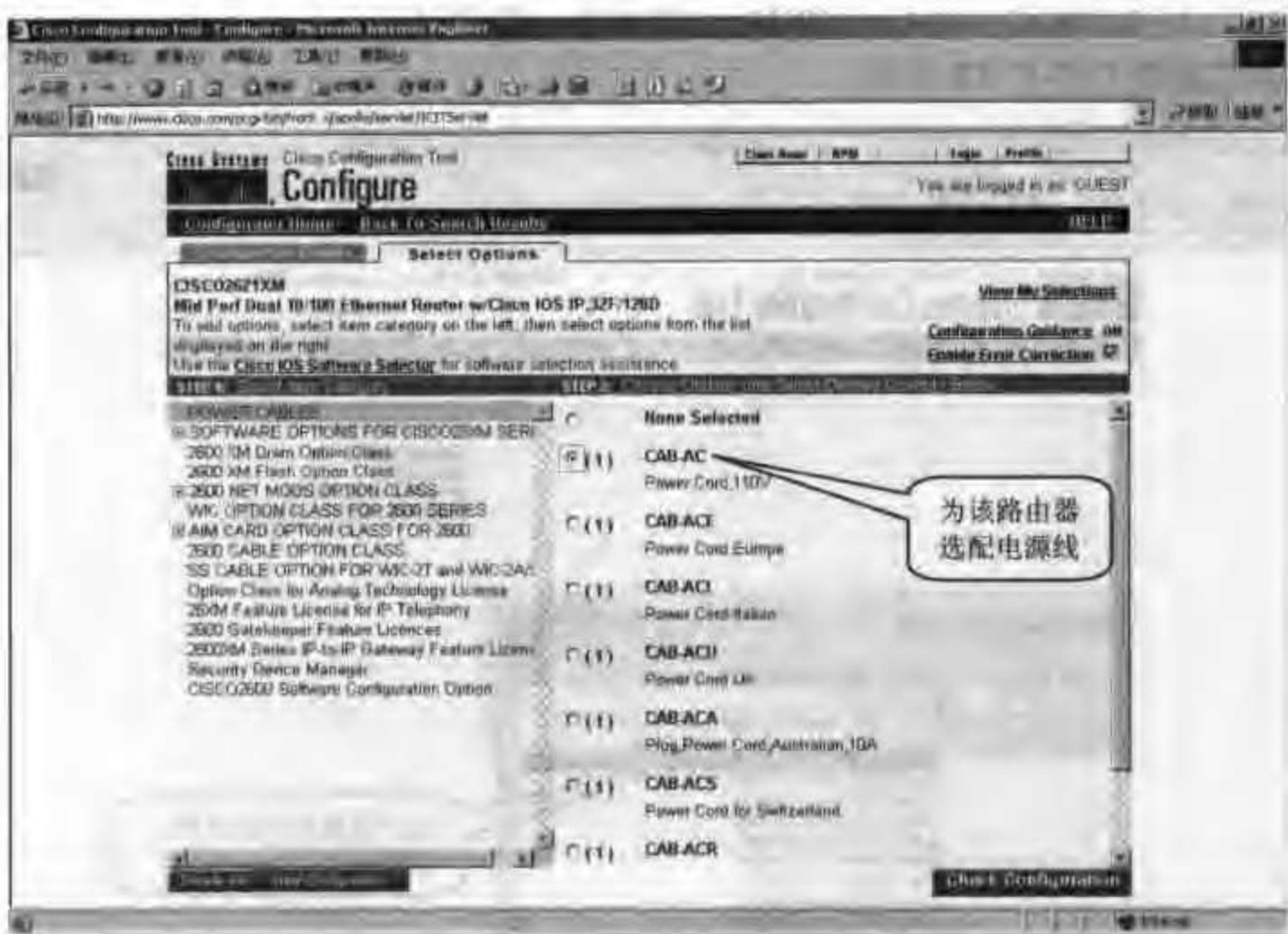
易事，即使多年从事售前工作的工程师也难免出错。幸好 Cisco 也意识到了这个问题，因此它给我们提供了一个非常有用的工具，那就是 Dynamic Configuration Tool。使用它我们就可以正确地配置出 Cisco 的各种产品。Dynamic Configuration Tool 的链接地址是“http://www.cisco.com/go/configtools”，我们也可以从 Cisco 工具中心总页面（http://www.cisco.com/go/tools）直接点击“Config Tool”进入，如附图 C-6 所示。



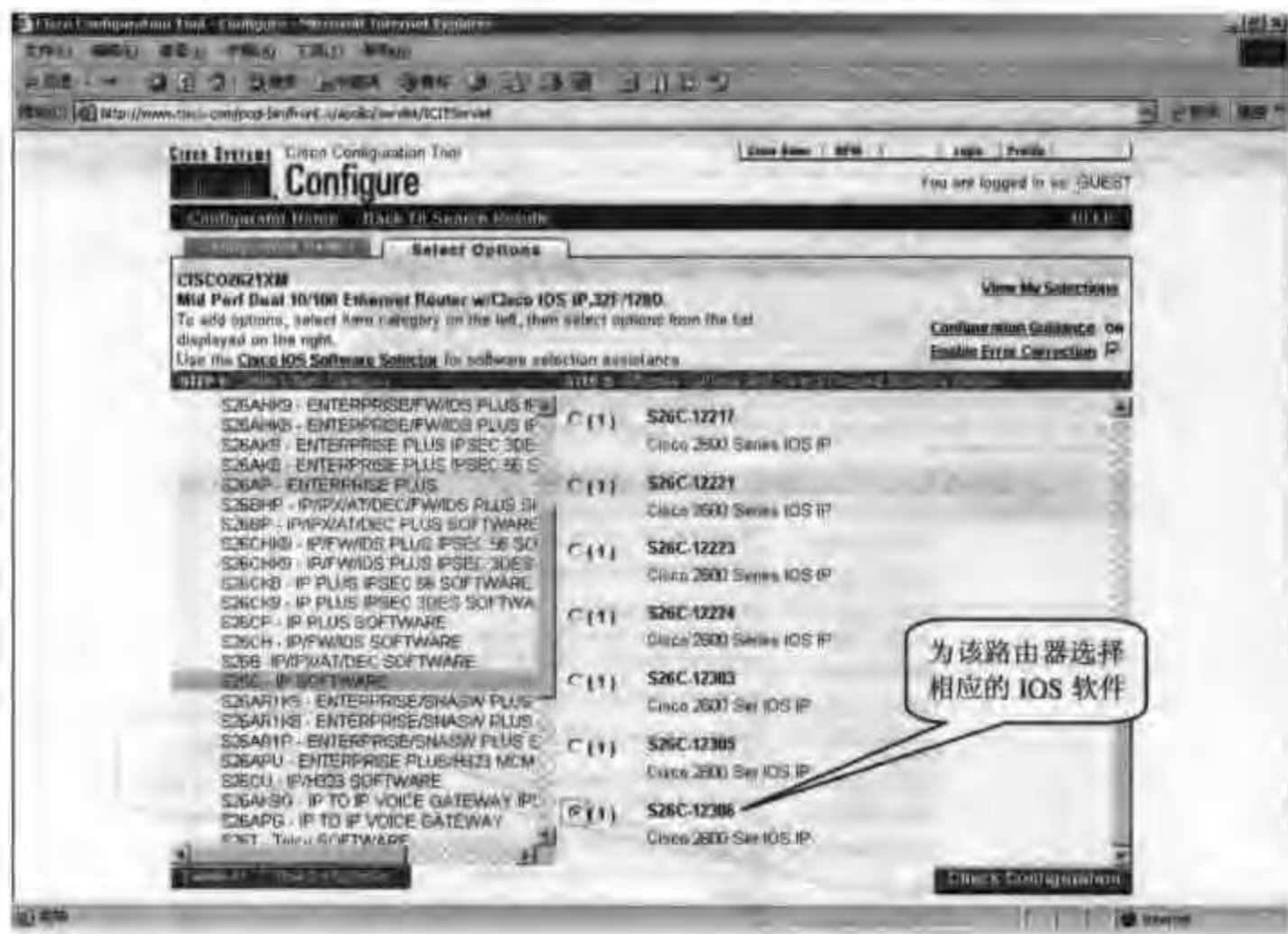
附图 C-5 Cisco Partner Business Central 页面



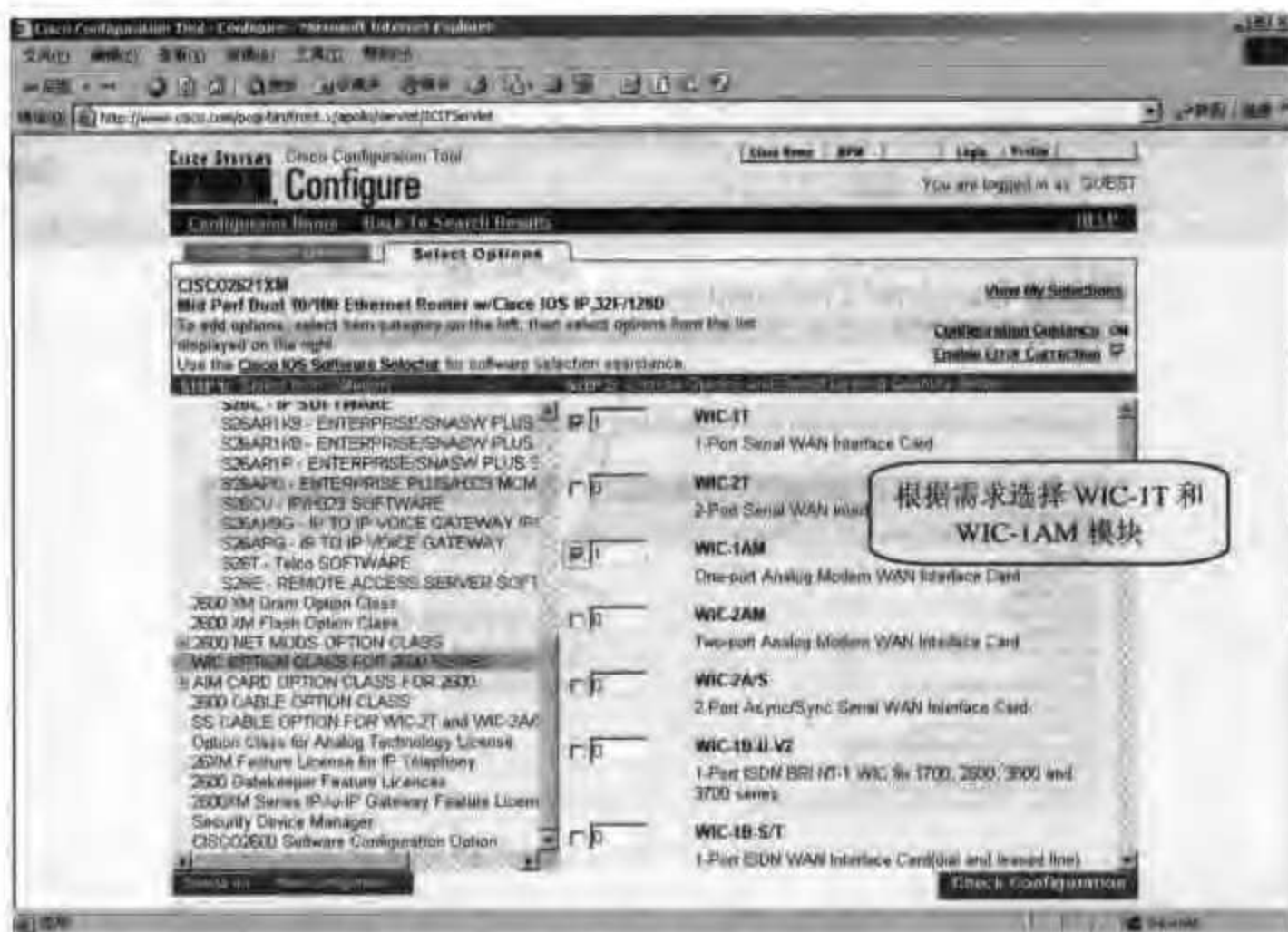
附图 C-6 Cisco Dynamic Configuration Tool 页面



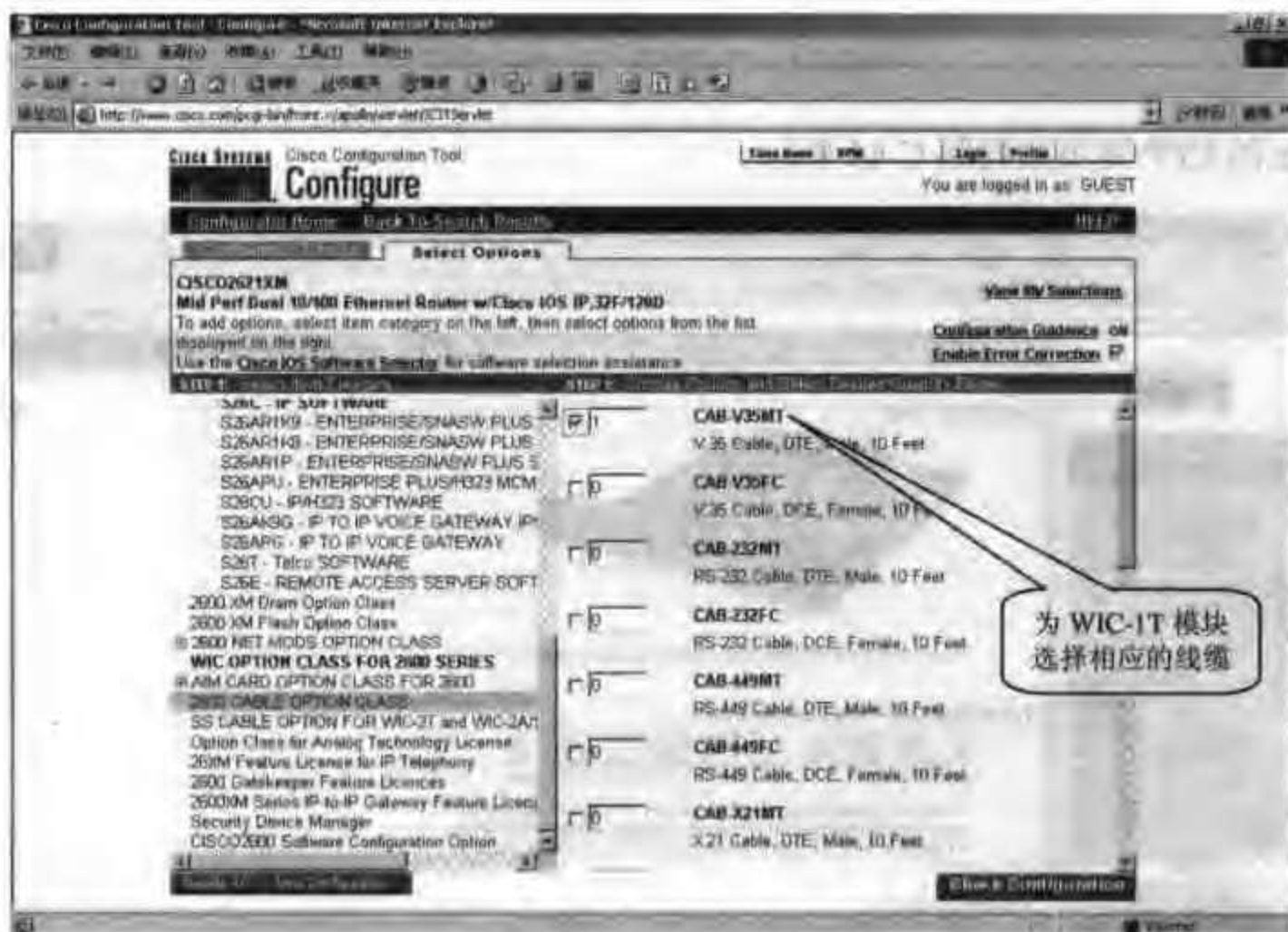
附图 C-9 产品配置之三（选配电源线）



附图 C-10 产品配置之四（选择 IOS）



附图 C-11 产品配置之五 (选择 WIC-1T 和 WIC-1AM)



附图 C-12 产品配置之六 (为 WIC-1T 选择线缆)

(6) Cisco CPP 网站

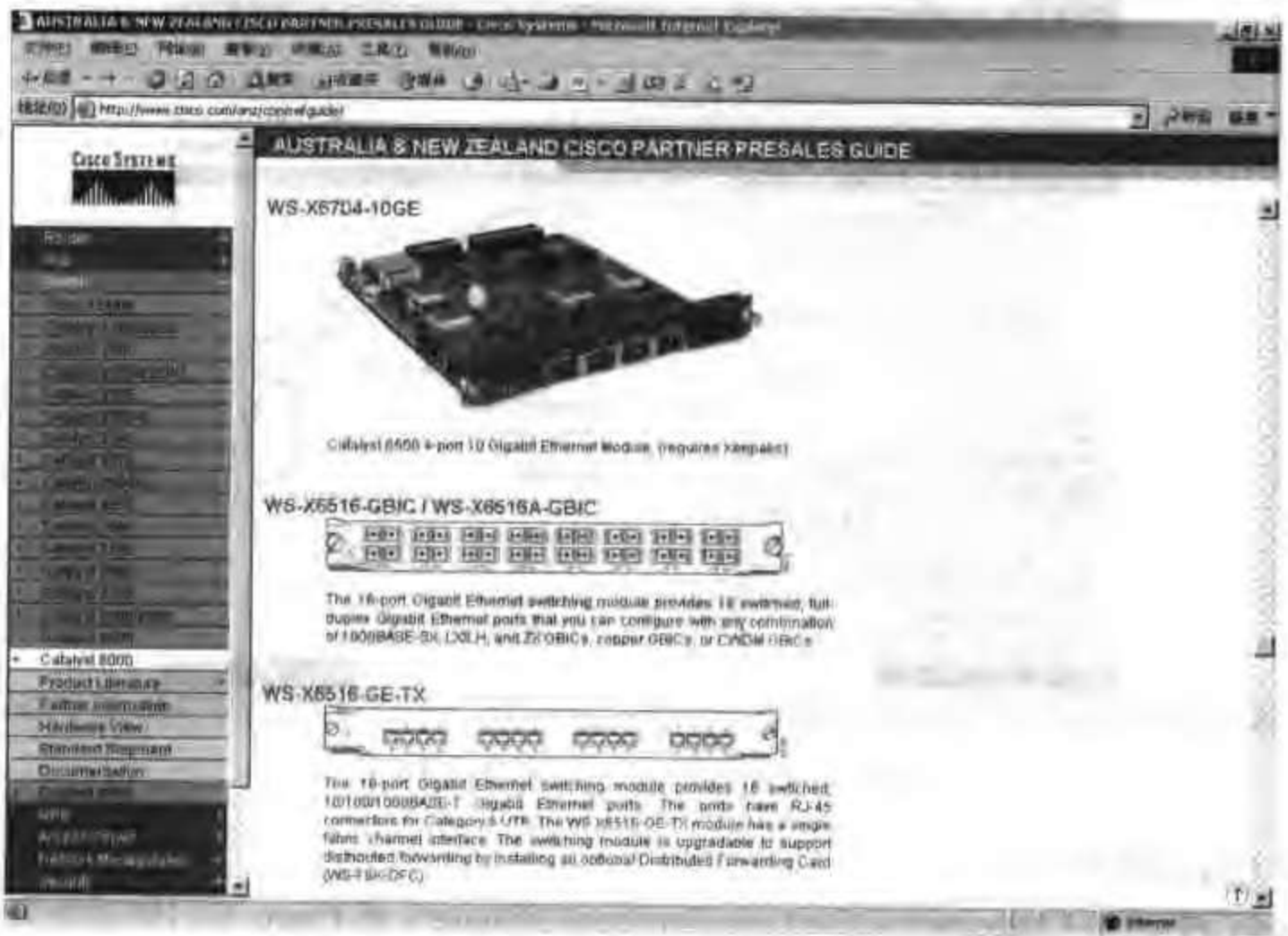
Cisco CPP 网站 (<http://www.cisco.com/anz/cpp/refguide/>) 是 Cisco 专门针对售前人员开设的网站, 里面涵盖的内容非常丰富, 但总体是按产品进行组织的。比如, 可以通过此网站提

供的所有产品的图片给客户建立起对产品直观的印象。



附图 C-13 产品配置之七（配置完成）

Cisco 的 CPP 网页如附图 C-14 所示。



附图 C-14 Cisco CPP 网页



附图 C-17 CPP 查看编码更改后显示的页面

2. 售后工具

假如我们从事的是售后的工作，那么可能会使用到如下的几个工具：

(1) Bug Toolkit

Cisco Bug Toolkits 是 Cisco 提供给我们的对 Cisco 的软硬件产品已知错误的查询工具，它有多种查询方式：

按 Bug 编号查询：Cisco 为每个已知的 Bug 指定了惟一的编号；

按 IOS 版本查询：每个版本的 IOS 的已知 Bug 的查询；

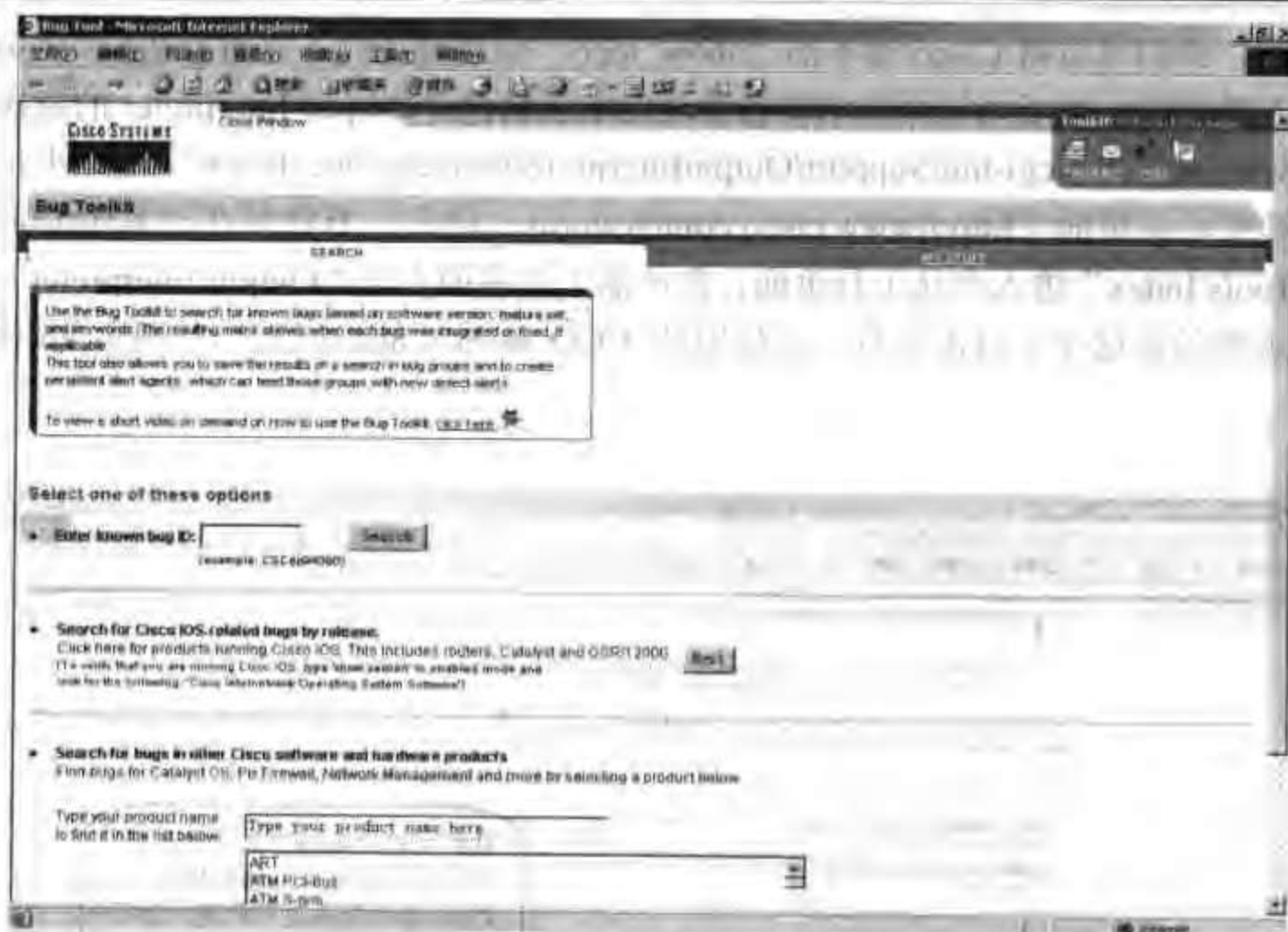
按硬件产品查询：除了路由产品之外的交换机系列，防火墙等其他产品的 Bug 查询。

Bug Toolkits 的链接地址是“http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl”，我们也可以通过 Cisco 工具中心总页面（<http://www.cisco.com/go/tools>）进入，方法是在工具中心页面点击“Product Tools Index”进入产品工具页面，在产品工具页面点击“Bug Toolkit”链接进入。其网页如附图 C-18 所示。

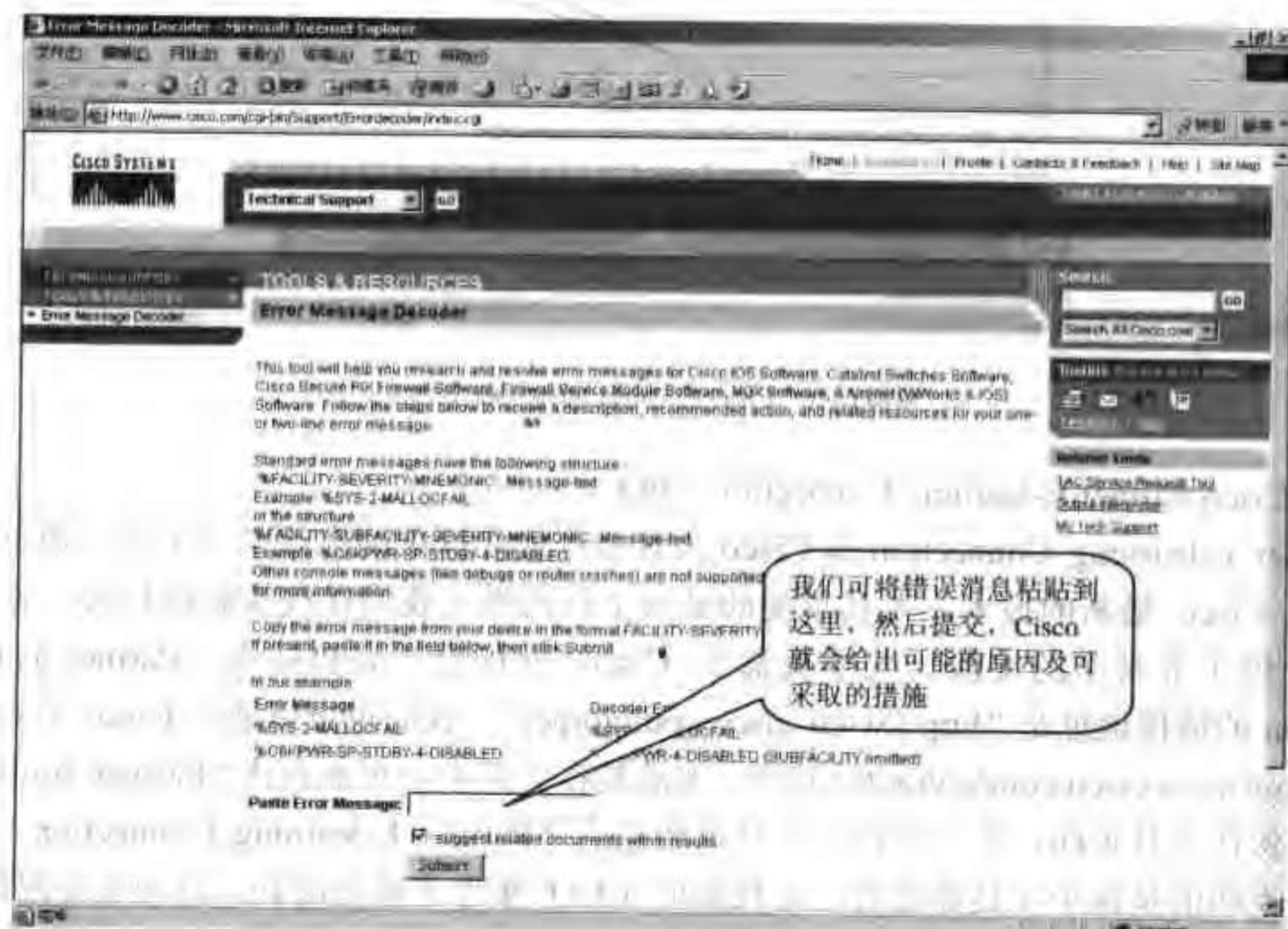
通过此工具我们可以查询相关软件存在的 bug，根据 bug 给出的故障现象，可以判断出自己网络的故障是否是由软件的 bug 引起的。

(2) Error Message Decoder

Cisco 提供的 Error Message Decoder 工具可帮助我们对错误信息进行查询，我们可以将日志里记录的错误提示，通过此工具进行提交，Cisco 会给出可能导致错误的原因以及可以采取的排错手段的响应信息。它的链接地址是“<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>”。我们也可以通过 Cisco 工具中心总页面（<http://www.cisco.com/go/tools>）进入，方法是在工具中心页面点击“Product Tools Index”进入产品工具页面，在产品工具页面点击“Error Message Decoder”链接进入。其网页如附图 C-19 所示。



附图 C-18 Cisco 的 Bug Toolkit 网页

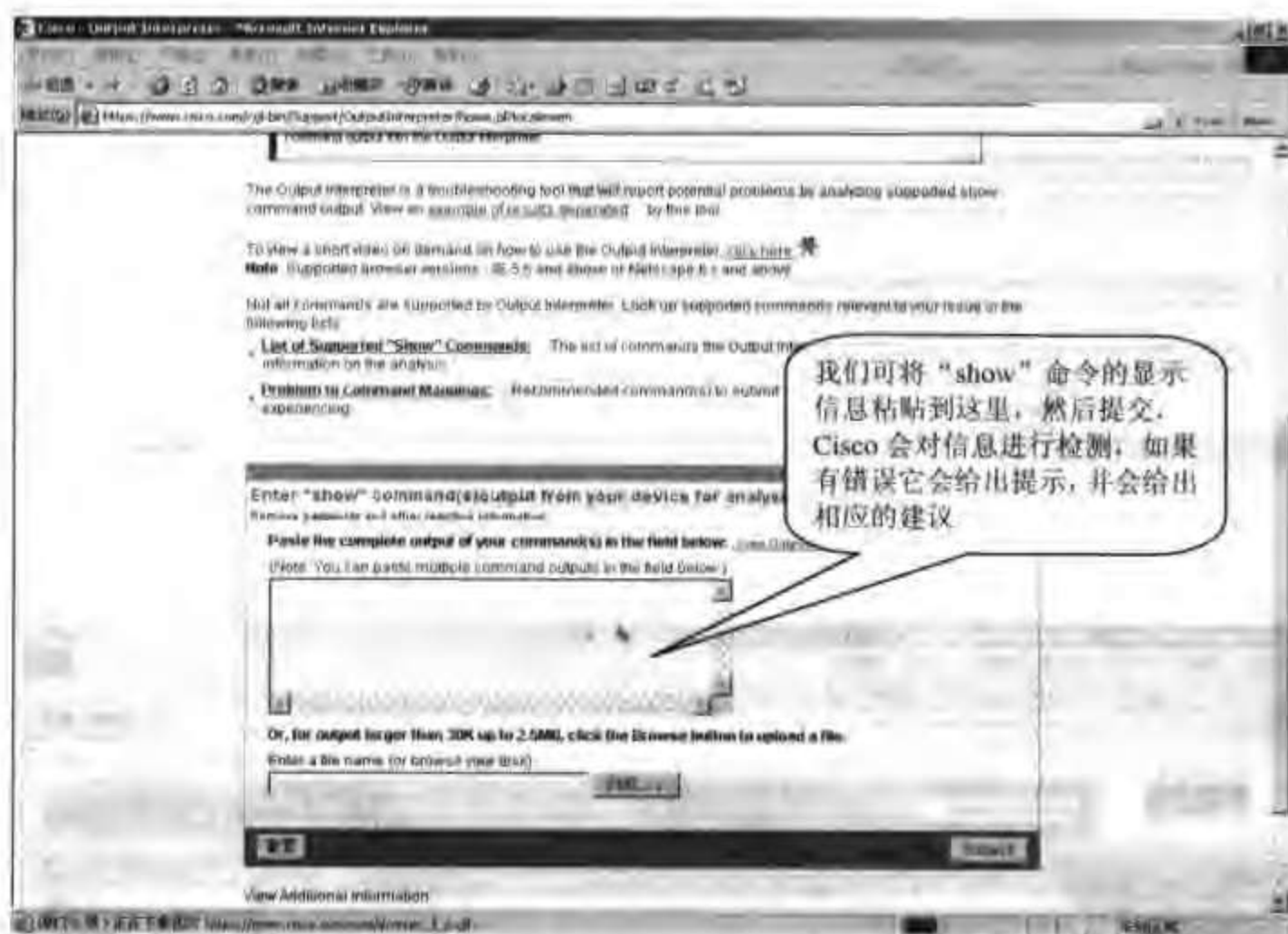


附图 C-19 Cisco 的 Error Message Decoder 页面

(3) Output Interpreter

Cisco 提供的 Output Interpreter 工具可帮助我们对 Cisco 的“show”命令提供的信息进

行错误检测, 我们可以将 Cisco 设备的“show tech”信息通过此工具进行提交, Cisco 会给出可能存在的错误, 以及可以采取的排错手段的响应信息。Output Interpreter 的链接地址是“<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl?locale=en>”。我们也可以通过 Cisco 工具中心总页面 (<http://www.cisco.com/go/tools>) 进入, 方法是在工具中心页面点击“Product Tools Index”进入产品工具页面, 在产品工具页面点击“Output Interpreter”链接进入。需要说明的是这个工具需要有一定权限的 CCO 账号才能访问到。其网页如附图 C-20 所示。



附图 C-20 Cisco 的 Output Interpreter 页面

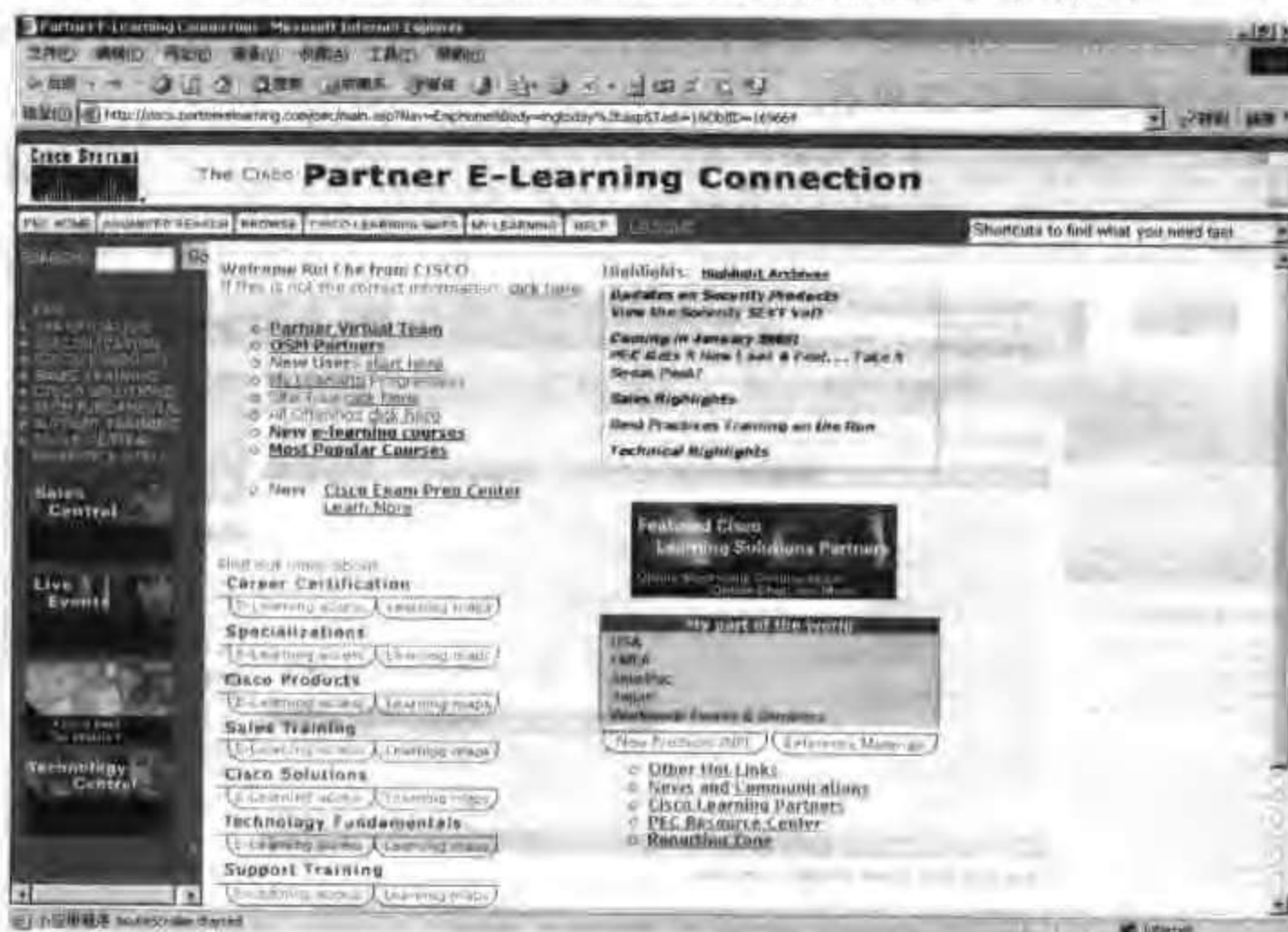
(4) Cisco Partner E-learning Connection (PEC)

Partner E-learning Connection 是 Cisco 为其合作伙伴提供的在线学习工具, 通过它, 用户可学习 Cisco 最新的技术, 尤其重要的是该工具提供了我们在线实验的机会, 它的 Lab Center 提供了非常多的实验, 几乎覆盖了 Cisco 所有的产品和技术。Partner E-learning Connection 的链接地址是“<http://www.cisco.com/go/pec>”, 我们也可以通过 Cisco 工具中心总页面 (<http://www.cisco.com/go/tools>) 进入, 方法是在工具中心页面点击“Partner Tools Index”进入合作伙伴工具页面, 在合作伙伴工具页面点击“Partner E-learning Connection”链接进入。需要说明的是这个工具需要有一定权限的 CCO 账号才能访问到。其网页如附图 C-21 所示。

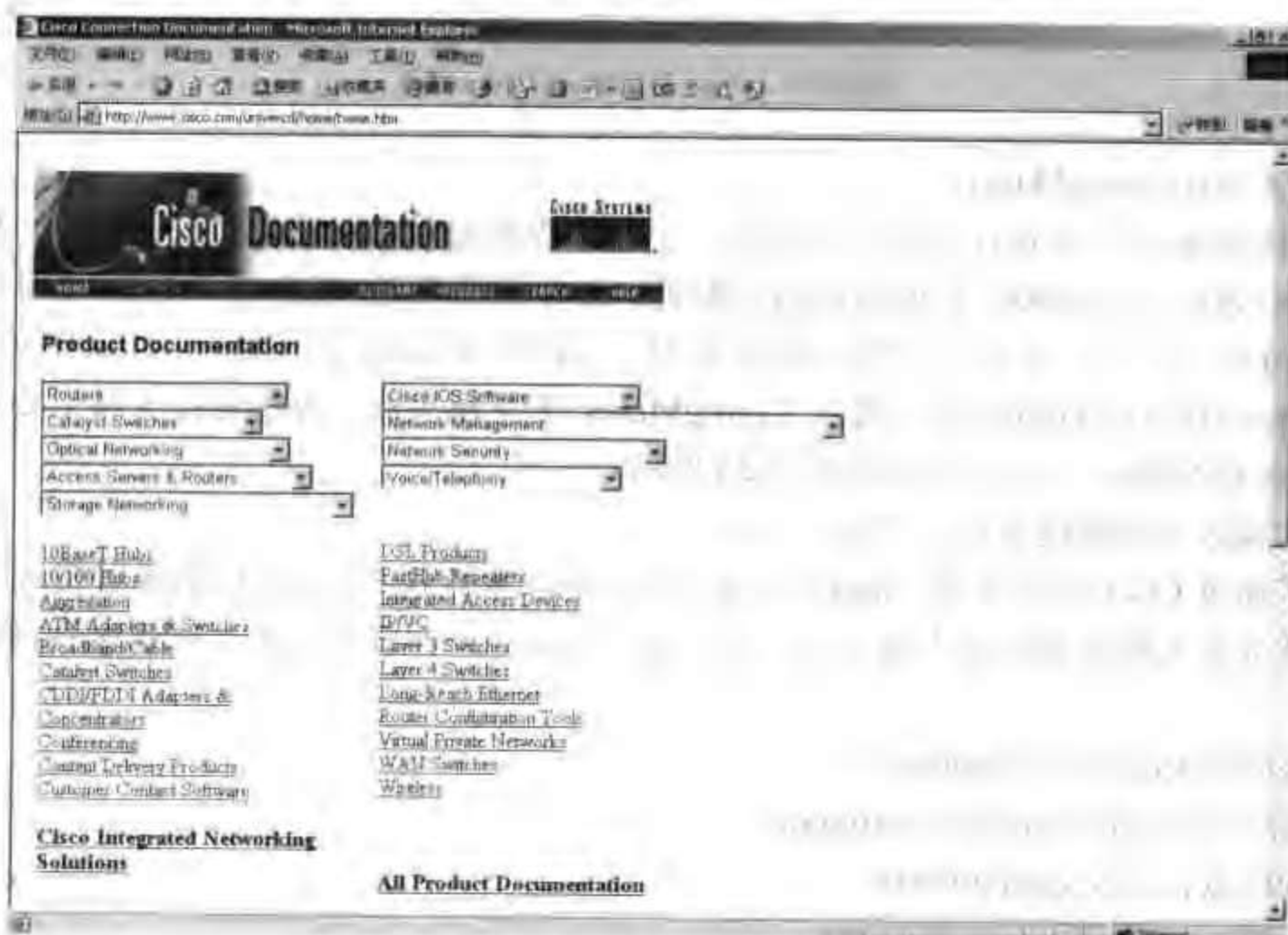
(5) Cisco Documentation

Cisco 提供的 Cisco Documentation 工具应该说是一个资料大全, 它涵盖了 Cisco 所有产品的相关资料, Cisco 会随产品附送 Cisco Documentation 的 CD-ROM, 用户可以通过该光盘全面学习有关 Cisco 的各种相关的技术内容。Cisco Documentation 的链接地址是

“http://www.cisco.com/univercd/home/home.htm”，其网页如附图 C-22 所示。



附图 C-21 Cisco 的 PEC 网页

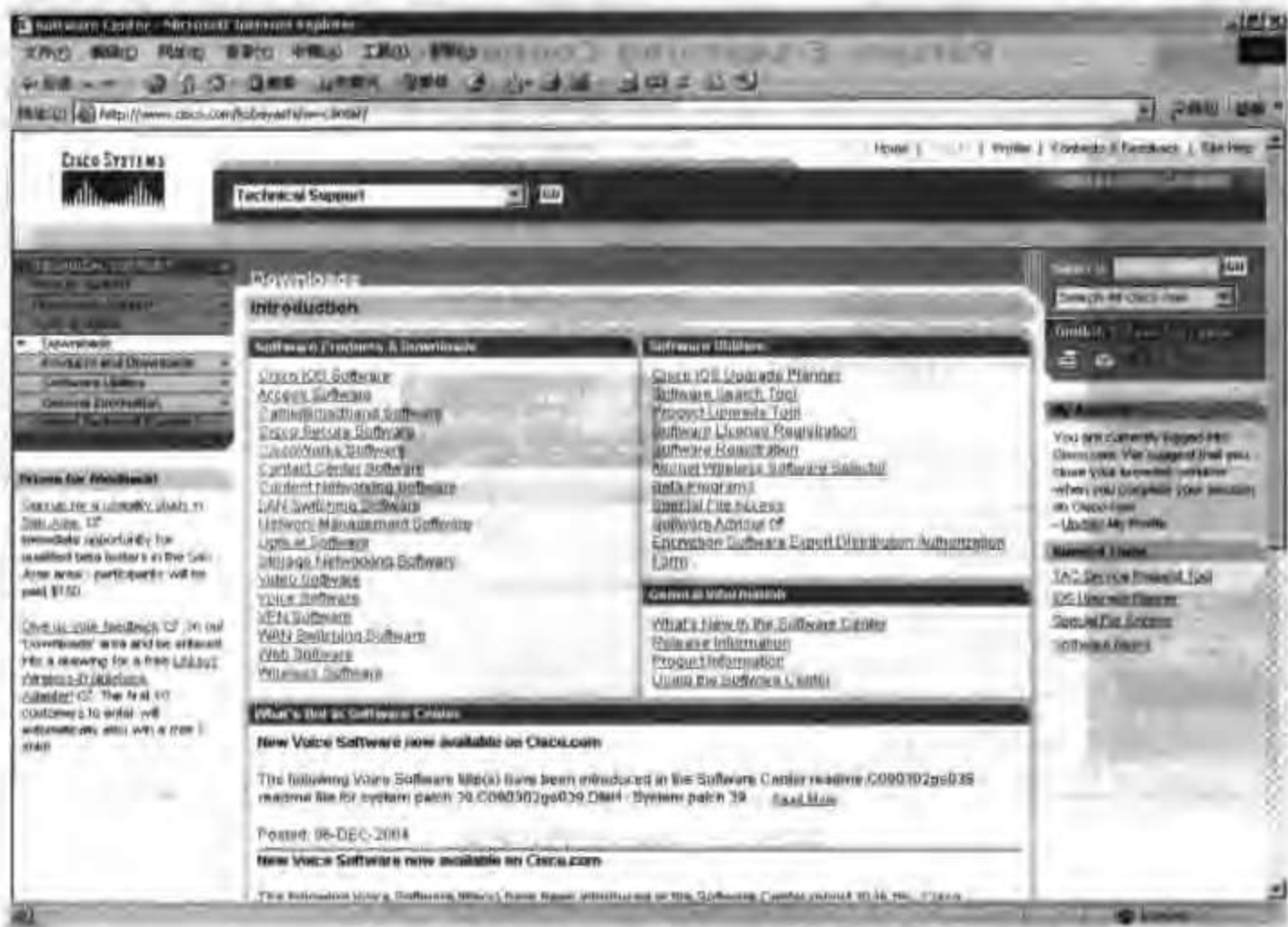


附图 C-22 Cisco Documentation 网页

(6) Cisco Software Center

Software Center 是 Cisco 提供给客户的软件下载中心，在这里可以下载到所有 Cisco 设备的操作系统软件（如 IOS 软件），另外还可以下载到有关 VPN、Video、Voice、Security、Wireless

以及网管方面的免费软件或试用版本。Software Center 的链接地址是“<http://www.cisco.com/go/software>”。需要说明的是这个工具需要有一定权限的 CCO 账号才能访问到。其网页如附图 C-23 所示。



附图 C-23 Cisco 的 Software Center 网页

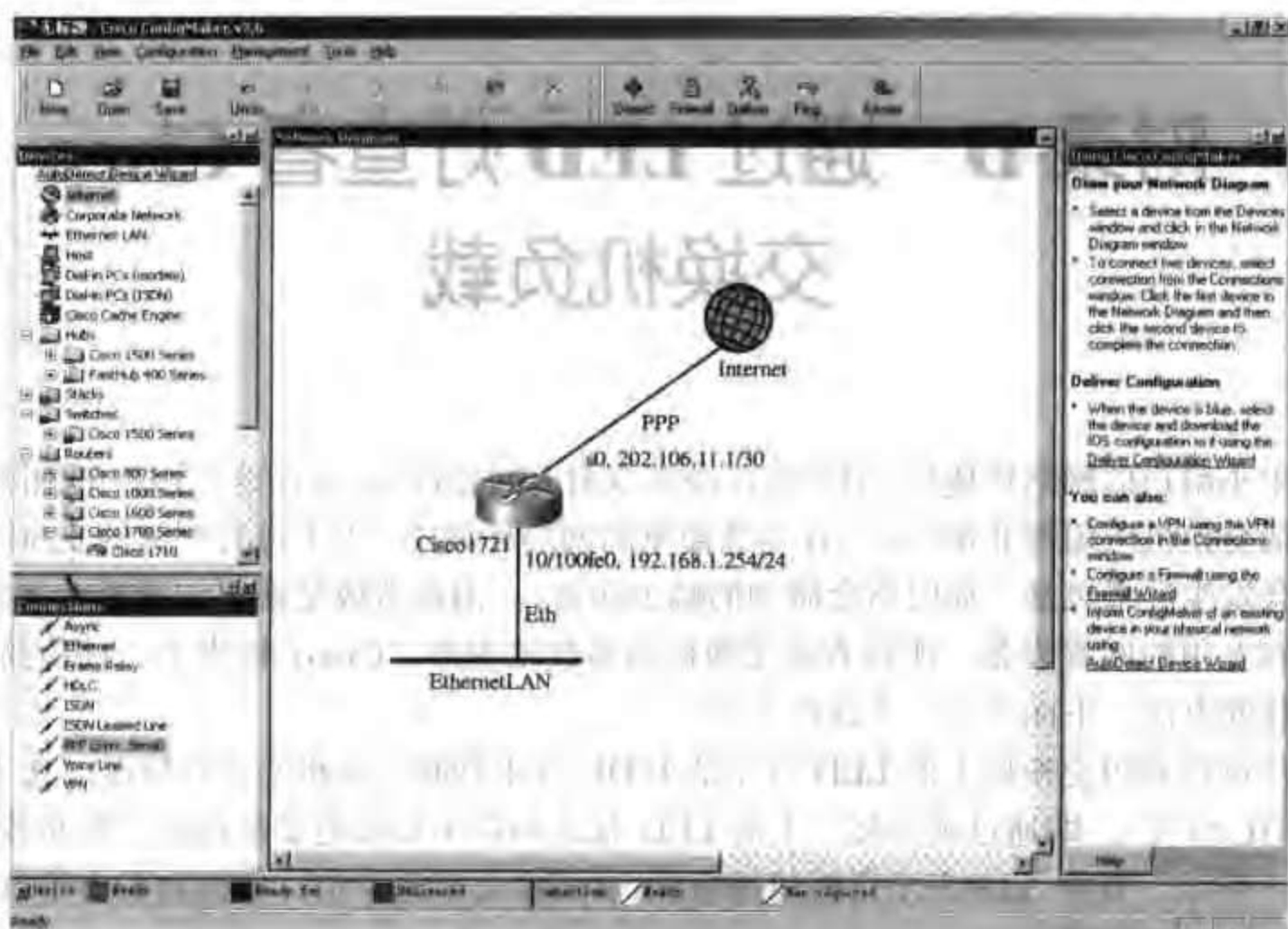
(7) Cisco ConfigMaker

ConfigMaker 是 Cisco 为用户提供的用于快速配置网络设备的工具软件，目前它支持从 Cisco800~Cisco4000 系列路由器的配置。对于不太熟悉 IOS 命令的初级用户来说，ConfigMaker 是一个非常实用的帮助工具。我们可以通过 Cisco 工具中心总页面（<http://www.cisco.com/go/tools>）进入 ConfigMaker 的下载页面，方法是在工具中心页面点击“Cisco ConfigMaker”。其网页如附图 C-24 所示。

3. Cisco 资源快速定位---“go”方式

除了通过 Cisco 的主页面（<http://www.cisco.com>）来查找 Cisco 提供的各种资源外，Cisco 还提供了非常人性化的快速查找方式，即“go”方式。下面将常用的一些快速查询链接介绍给读者：

- <http://www.cisco.com/go/tools>
- <http://www.cisco.com/go/configtools>
- <http://www.cisco.com/go/safe>
- <http://www.cisco.com/go/security>
- <http://www.cisco.com/go/vpn>
- <http://www.cisco.com/go/pec>
- <http://www.cisco.com/go/router>
- <http://www.cisco.com/go/netpro>



附图 C-24 Cisco ConfigMaker 页面

<http://www.cisco.com/go/fn>

<http://www.cisco.com/go/ccie>

<http://www.cisco.com/go/wireless>

<http://www.cisco.com/go/catalyst6500>

<http://www.cisco.com/go/catalyst4500>

<http://www.cisco.com/go/catalyst3550>

<http://www.cisco.com/go/catalyst2950>

<http://www.cisco.com/go/800>

<http://www.cisco.com/go/1600>

<http://www.cisco.com/go/1700>

<http://www.cisco.com/go/2500>

<http://www.cisco.com/go/2600>

<http://www.cisco.com/go/3600>

<http://www.cisco.com/go/3700>

<http://www.cisco.com/go/7200>

<http://www.cisco.com/go/7300>

<http://www.cisco.com/go/7400>

<http://www.cisco.com/go/7500>

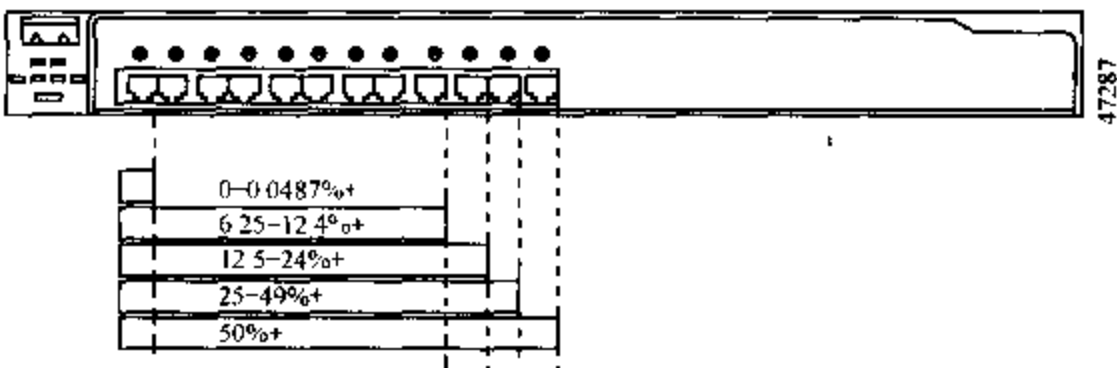
<http://www.cisco.com/go/7600>

<http://www.cisco.com/go/12000>

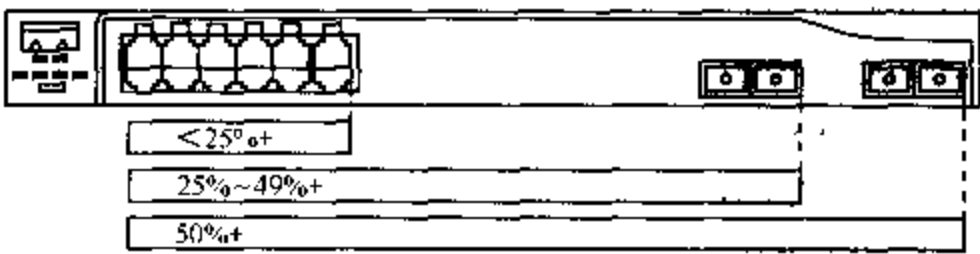
附录 D 通过 LED 灯查看 Cisco 交换机负载

在中小用户的网络环境中，用户往往没有专用的网管设备，而在这些用户的网络中，Cisco 的中低端交换机应用得非常广泛。在这些简单的网络环境中，由于没有严密的安全防范手段，所以常会发生广播风暴（如时常会碰到的蠕虫病毒），由此造成交换机的背板负载经常很高。由于没有专用的网管设备，所以查询交换机的负载很困难。Cisco 提供了一种简易的查看交换机负载的方法，下面介绍一下这种方法。

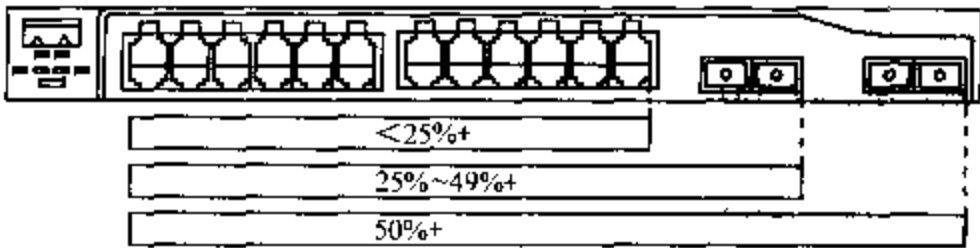
用户可以利用交换机上的 LED 灯中的 UTIL 灯来判断交换机的负载情况（按 MODE 键直到 UTIL 灯亮），即通过观察接口上的 LED 状态和总个数知道交换机的背板负载，如附图 D-1~D-9 所示。其中 xx%表示背板使用情况，+表示大于这个值，虚线和长方形框显示出你看到闪灯的接口范围。



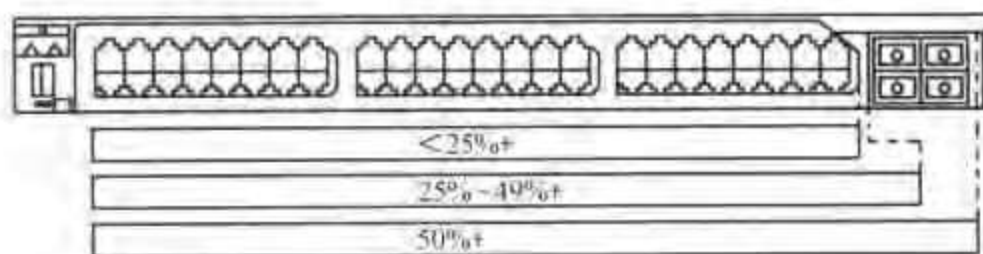
附图 D-1 Catalyst 2950-12、2950 24、2950C 24、2950SX-24 和 2950T-24 交换机



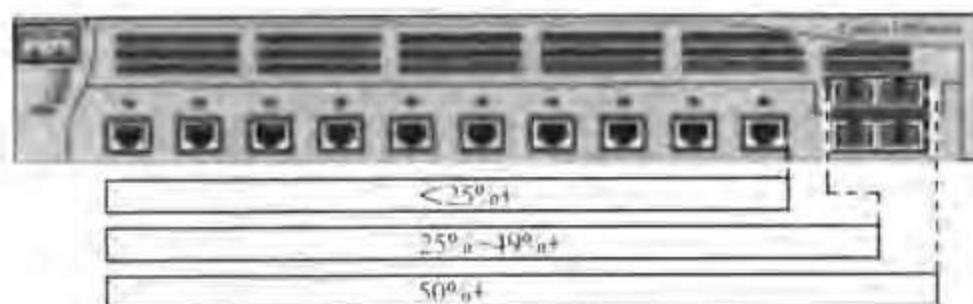
附图 D-2 Catalyst 2950G-12 EI 交换机



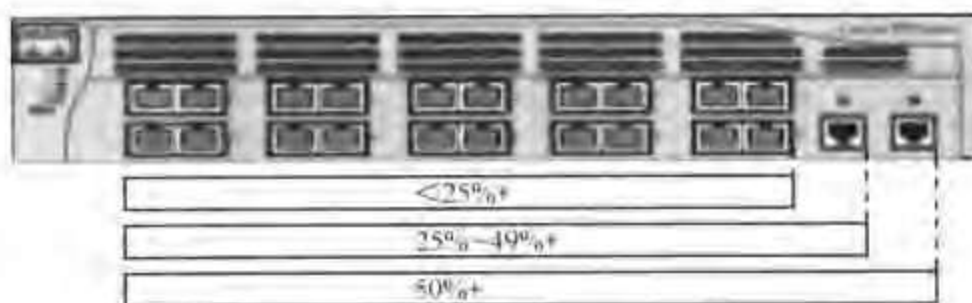
附图 D 3 Catalyst 2950G-24-EI 和 2950G-24-EI-DC 交换机



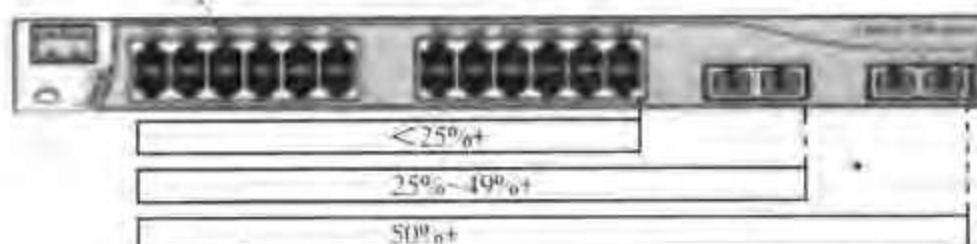
附图 D-4 Catalyst 2950G-48-EI 交换机



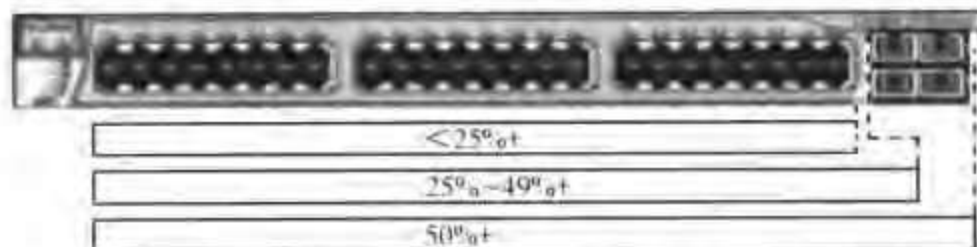
附图 D-5 Catalyst 3550-12T 交换机



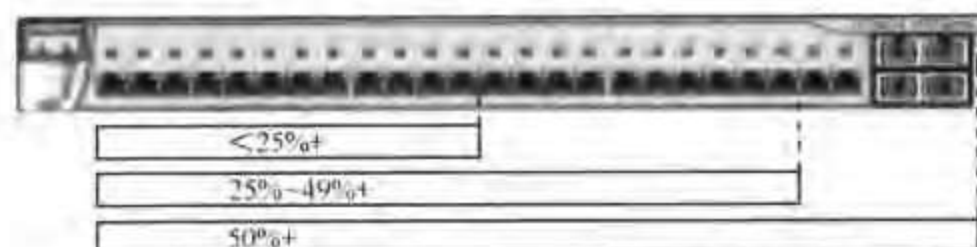
附图 D-6 Catalyst 3550-12G 交换机



附图 D-7 Catalyst 3550-24 and 3550-24-DC 交换机



附图 D-8 Catalyst 3550-48 交换机



附图 D-9 Catalyst 3550-24-FX 交换机

[G e n e r a l I n f o r m a t i o n]

书名= C I S C O企业网快速构建与排错手册

作者=

页数= 4 6 1

S S 号= 0

出版日期=

封面
书名
版权
前言
目录
正文