中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3com.com

Cisco Systems

CISCO NETWORKING ACADEMY PROGRAM

ciscopress.com



思科网络技术学院教程（第三、四学期）（第三版）

Cisco Networking Academy Program
CCNA 3 and 4
Companion Guide
Third Edition

The only authorized textbook for the Cisco Networking Academy Program

内附光盘



[美] Cisco Systems 公司
Cisco Networking Academy Program 著
天津大学| 电子科技大学| 中山大学
—— 思科网络技术学院 —— 译

人民邮电出版社
POSTS & TELECOM PRESS

CH3C 思科华为3COM 让技术不再孤单，让学习不再流浪

中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3com.com

CISCO SYSTEMS

思科网络技术学院教程（第三、四学期）（第三版）

本书是思科公司认可的思科网络技术学院项目的教材，是对基于Web教程的补充。编写本教程的目的是为了帮助学生准备CCNA认证考试，并为进入网络管理领域提供必需的知识。本教程深入讨论了交换机的设计、配置和维护，局域网（LAN）和虚拟局域网(VLAN)，还覆盖了广域网(WAN)和网间分组交换（IPX）路由选择，增强型外部网关协议（EIGRP）和网络故障排除等内容。此外，本教程还扩展了学生在综合业务数字网（ISDN）、点到点协议（PPP）和帧中继技术设计、配置和维护方面的知识。

新版本的更新和扩充与基于Web教程的内容相对应，并且提供了很多额外的学习辅导，包括：

- 新增了无类路由选择、单域OSPF、交换机配置、生成树协议、VLAN中继连接协议、规划可控的IP地址等内容，对EIGRP、交换概念与设计和VLAN等内容进行了较大的改动和增补。
- 与CCNA在线教程高度一致，帮助学生加深课堂上的学习体验。
- 每章开始的“目标”列出了各章重要内容，术语表列出了关键术语及其定义。
- 明确标识了与实验手册对应的工作表和实验。
- 每章末尾有用于跟踪进度和指导学习的复习题。

内附光盘



附带光盘中包含了网络学院开发的众多资料，这是在任何其他书中无法获得的，包括：e-Lab实验、带有可自定义考试引擎的500道模拟试题、关于Cisco设备的动画片断、覆盖概念的教学视频以及覆盖网络安全、网络管理和住宅网络的附加内容。

ciscopress.com

ISBN 7-115-12212-1

9 787115 122124 >

人民邮电出版社网址 www.ptpress.com.cn

ISBN7-115-12212-1/TP·3931
定价：60.00元（附光盘）

思科华为3COM 让技术不再孤单，让梦想不再流浪 CH3C

中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3com.com



思科网络技术学院教程（第三、四学期）（第三版）

[美] Cisco Systems公司
Cisco Networking Academy Program 著
天津大学 | 电子科技大学 | 中山大学
思科网络技术学院 —— 译

CH3C 思科学院3COM 让技术不再孤单，让学习不再流浪

人民邮电出版社

中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3com.com

图书在版编目（CIP）数据

思科网络技术学院教程. 第3、4学期：第3版 / 美国思科公司，美国思科网络技术学院著；黄海译. —北京：人民邮电出版社，2004.7

ISBN 7-115-12212-1

I. 思… II. ①美…②美…③黄… III.计算机网络—教材 IV. TP393

中国版本图书馆 CIP 数据核字（2004）第 059470 号

版 权 声 明

Cisco Systems, Inc Cisco Networking Academy Program: Cisco Networking Academy Program CCNA 3 and 4 Companion Guide Third Edition （ISBN 1-58713-113-7）

Copyright ©2003 by Cisco Systems, Inc.

All rights reserved.

本书中文简体字版由美国 Cisco Press 出版公司授权人民邮电出版社出版。未经出版者书面许可，对本书的任何部分不得以任何方式复制或抄袭

版权所有，侵权必究

思科网络技术学院教程

（第三、四学期）（第三版）

◆ 著 [美] Cisco Systems 公司
Cisco Networking Academy Program

译 天津大学 电子科技大学 中山大学
—— 思科网络技术学院 ——

责任编辑 陈 昇

◆ 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 ciscobooks@ptpress.com.cn
网址 http://www.ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：35.75
字数：995 千字 2004 年 7 月第 1 版
印数：10 001-21 000 册 2004 年 9 月北京第 2 次印刷

著作权合同登记 图字：01-2003-1478 号

ISBN 7-115-12212-1/TP・3931

定价：60.00 元（附光盘）

本书如有印装质量问题，请与本社联系 电话：(010)67129223

中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3com.com

内容提要

思科网络技术学院项目（*Cisco Networking Academy Program*）是Cisco Systems公司在全球范围推出的一个主要面向初级网络工程技术人员的培训项目，其培训内容与CCNA类似。

本书为思科网络技术学院第三、四学期的配套书面教程，主要内容包括：OSI参考模型和路由选择、无级路由选择、单区域OSPF、增强内部网关路由选择协议、交换概念与局域网设计、交换机、交换机配置、生成树协议、虚拟局域网、VLAN中继协议、扩展的IP地址、广域网技术、点到点协议、ISDN和DDR、帧中继、网络管理介绍、光网络基础、网络管理、网络认证考试复习、Network+认证考试概览、CCNA认证考试复习、关于融合网络技术的介绍、制定网络安全和网络管理策略、虚拟专用网。每章的最后还提供了复习题。附录A包含了本书中使用的所有关键词的术语表；附录B是每章结尾复习题的答案。

本书为新的思科网络技术学院教学计划的第三、四学期的书面教材，编写本书的目的是为了帮助学生准备CCNA认证考试，并帮助他们掌握必要的网络知识。

中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3com.com

为实施人才强国战略贡献力量

（代序言）

在《思科网络技术学院教程》（第三版）中文版出版之际，我谨代表思科系统网络技术有限公司，感谢各位学员朋友对思科网络技术学院的厚爱，感谢人民邮电出版社长期以来的合作与支持，感谢译者、编辑及所有相关人员为此付出的努力。

思科公司总裁兼首席执行官钱伯斯认为，互联网和教育，作为推动社会经济发展的两个核心动力，将深刻改变国家、企业和个人在未来时代的核心竞争力。现在，这一理念已经得到越来越多的认同和支持。

回首 1997 年，作为互联网和教育相结合的产物，思科系统公司启动了思科网络技术学院这一非赢利性的全球网络技术教育项目。到目前为止，思科公司为该项目的投入已达 2 亿美元，在全球 150 多个国家建立了 1 万余所思科网络技术学院。来自全球大学、职业技术学校、中学、团体机构和其他教育组织的 45 万学员正在参加学习。在中国，第一所思科网络技术学院 1998 年成立于复旦大学。短短 6 年时间，已经在全国建立了 200 所思科网络技术学院，培养超过 2 万名毕业生。最近，思科公司又与教育部签署协议，面向全国 35 所示范性软件学院提供全面的基于思科网络技术学院的网络技术课程体系，以帮助中国培养一大批兼通网络技术的复合型软件人才。

在思科网络技术学院，参加学习的学员不仅来自经济发达省份，也来自西部欠发达地区；既有在校的大学生甚至中学生，也有已经处于重要岗位的在职人员。2000 年 6 月，钱伯斯第三次访华之际，思科向 30 所西部高校捐建了思科网络技术学院，希望网络能为东西部地区协调发展做出贡献，得到了西部地区的热烈响应。2001 年 10 月，江泽民主席在第九届亚太经合组织会议（APEC）

中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3com.com

上宣布发起“人力资源能力建设促进项目”。作为该计划的积极参与者，思科系统公司在此后的三年中，为 APEC 各成员国选派的 400 名学员提供思科 CCNA、CCNP 培训及认证。此外，联合国开发计划署（UNDP）、国际电信联盟（ITU）也分别与思科合作，在贫困和欠发达地区成立思科网络技术学院，用以缩小地区间的数字鸿沟。

展望未来，网络还有更大的潜能等待着我们一起去发掘。在国家高瞻远瞩地提出人才强国战略之今天，思科将一如继往地发挥自己特有的网络技术优势，尤其是通过思科网络技术学院这一非盈利性的全球教育项目，帮助中国的人才资源能力建设，最终发动更多的人投身到网络经济大潮中，为消除数字鸿沟、发展国民经济贡献力量！

杜家滨

思科系统公司全球副总裁

思科系统（中国）网络技术有限公司 总裁

2004 年 6 月

CH3C 思科华为3COM 让技术不再孤单，让天堂不再遥远

中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3com.com

序

Internet已给全球许许多多的人和他们的雇主带来了新的巨大商机。许多公司和组织在网络上的投资已经带来了生产力的大幅度提高。一些研究表明在整个经济体系中，生产力都有了大幅度的提高。提高效率、增加利润和改善生活水平的愿望已经成为现实，而且还在不断发展之中。

这种生产力的提高不是简单地通过购买网络设备就可以达到的，它需要有专门的人才去规划、设计、安装、配置、操作和维护网络，并为网络排除故障。网络管理人员必须要确保他们规划的网络是安全的并能持续稳定地工作。他们需要根据组织的需求，组织对网络的依赖程度，以及组织的发展来布署新的网络功能。

为满足互连网络社区的众多教育需求，思科系统公司创立了思科网络技术学院项目。思科网络技术学院是一个综合性的学习项目，它向学生提供在全球经济环境中所必需的关于Internet的技能。思科网络技术学院将面对面的教学、基于Web的课程内容、在线测试、学生成绩跟踪、动手实验、教师培训与支持，以及备考行业标准认证融为一体。

思科网络技术学院不断地增强教学之间的融合。基于Internet的评估和教师支持系统就是其中最大、最有效的部分，它包括每周7天、每天24小时的面向思科网络技术学院的教师的服务系统。通过在线评估和反馈系统向学生提示尚需继续学习的内容，思科网络技术学院帮助学生以螺旋式的方式对课程进行学习。

为网络技术学院设计的思科全球学习网络（Cisco Global Learning Network）基础设施向世界范围内的学生提供丰富的、交互式的、个性化的课程。Internet强大的力量能改变人们工作、生活、娱乐和学习的方式，思科网络技术学院项目则是这场变革的先锋。

由Cisco Press出版的这套教程是思科网络技术学院项目最畅销的配套教程之一。这些书籍由思科全球教育事业部（Cisco Worldwide Education）和Cisco Press共同规划，它们为思科网络技术学院的在线学习内容提供了综合的支撑。Cisco Press出版的这些书籍是思科系统公司惟一授权的针对思科网络技术学院的书，包含纸稿和光盘，从而确保思科网络技术学院的学生能获得最大的学习

收益。

我希望你们能成功，思科系统公司和Internet将伴随着你们的学习历程。我也希望你们在完成思科网络技术学院的课程后不断地学习。除了出版“思科网络技术学院教程”书籍以外，Cisco Press还出版了大量的网络技术和认证书籍，它们提供了丰富的资源。思科系统公司也建立了一个由多家专业培训公司构成的网络——思科培训合作伙伴（Cisco Learning Partners）——他们提供全套的思科培训课程。他们提供的培训方式有多种，包括电子学习、自主学习及教师指导学习。他们的教师是思科认证的，教材是思科提供的。当你准备学习时，请访问思科网站（Cisco.com）的“Learning&Events”部分，以了解思科公司及其培训合作伙伴的全部教育支持。

感谢你选择本书，也感谢你选择思科网络技术学院项目！

Kevin Warner
思科系统公司
全球教育事业部高级总监

CH3C 思科华为3COM 让技术不再孤单，让梦想不再流浪

前 言

本书是对思科网络技术学院项目课堂教学和实验课程的补充。思科网络技术学院项目的课程能帮助你在计算机网络技术领域获得职业机会或参加进一步的学习和培训。

本书的目的是使你获得比已经使用的在线教程更多的训练。本书也覆盖了适用于思科认证网络工程师（CCNA）认证考试的所有主题。本书严格遵守了思科在网络技术学院课程中所使用的风格和格式。最后，本书附有光盘，其中包含教学视频资料、电子实验（e-Lab）活动、图片集（PhotoZooms）和备考练习问题，所有这些内容都是以交互式的多媒体形式出现，可以用作学习参考资料。

本书介绍和扩展了你在设计、配置和维护交互机、局域网（LAN）和虚拟局域网（VLAN）方面的知识和实践经验。本书所覆盖的内容使你能获得与配置局域网、广域网、内部网关路由选择协议（IGRP）、增强型内部网关路由选择协议（EIGRP）和网络故障排除技能相关的实践经验。另外，本书还扩展了你在广域网、综合业务数字网（ISDN）、点到点协议（PPP）和帧中继的设计、配置和维护方面的知识和实践经验。

本书不仅能帮助你准备CCNA认证考试，也能帮助你准备CompTIA的Network+认证考试。

本书的目标

本书的目标是向你教授Cisco所支持的网络技术，帮助你理解如何设计和构建网络，如何配置Cisco路由器。本书设计与思科网络技术学院项目课程共同使用或者作为单独的参考书。

本书的读者

本书的主要读者是对网络技术感兴趣的学生，尤其是参加思科网络技术学院项目的学生。在课堂教学时，本书可作为在线教程的补充。

本书同样适合于培训教师、从业人员以及一般用户。本书所采用的友好的、非技术性的表述方式对于那些愿意远离专业技术手册

而获得大量技术知识的读者而言是理想的选择。

本书的特点

本书包含了很多有用的特性，能帮助你理解计算机系统并对系统中的问题进行故障排除：

• **目标**——每章的开头都会列出学完本章后要掌握的目标。另外，这些目标提供了关于本章所包含概念的参考。

• **图、例和表**——本书包含了许多插图、配置实例和表格，它们可以帮助你加深对理论、概念、强化概念的命令以及安装顺序等内容的理解，并且使你能更形象地体会章节的内容。此外，特定的实例还提供了现实生活中会遇到的情形，并详述了问题和解决方案。

• **各章总结**——在每章的结尾都有本章中概念的总结，它提供了本章的纲要，是复习的好帮手。使用它可以评估对本章主题的掌握情况。

• **关键术语**——总结了本章中所包含的最重要的术语。可以作为学习的助手。此外，这些关键术语能够加深你对本章所介绍概念的理解。阅读每章时，任何蓝色显示的术语都将在“关键术语”部分进行定义。

• **复习题**——第1到17章的结尾都有练习题，可作为进一步的评估使用。这些问题强化了各章节中介绍的概念，可以使你在学习新的一章之前检测一下自己对本章内容的理解。

• **技能培养**——本书中所引用的工作表单和实验活动都可以在《思科网络技术学院教程实验手册（第三、四学期）》（第二版）中找到。这些实验活动使你能够把理论与实践结合起来。

本书的组织方式

本书分为23个章节和两个附录。第1章是复习、第2~10章适用于CCNA 3在线教程、第11~16章适用于CCNA4在线教程。17~22章是额外的材料，能帮助你准备像CCNA和CompTIA Network+这样的考试，还能帮助你获得关于最新技术的知识。下面是对各章内容的总结：

• **第1章“复习：OSI参考模型与路由选择”**——本章对开放系统互连（OSI）参考模型进行了复习，并对与路由选择相关的网络规划设计问题进行了概述。

• **第2章“无类路由选择介绍”**——本章介绍了关于可变长度子网掩码（VLSM）的基础知识以及如何使用和为什么要使用VLSM。本章描述了VLSM的配置。也研究了路由选择信息协议（RIP）的历史和RIPv2的基本组件。最后，本章还论述了如何对RIPv2进行配置、验证和故障排除。

• **第3章“单区域OSPF”**——本章讨论了链路状态路由选择协议的基础知识、单区域OSPF的概念以及单区域OSPF的配置。

• **第4章“增强内部网关路由选择协议”**——本章介绍了EIGRP的基本概念，并与IGRP进行了比较。还描述了对EIGRP进行配置、验证和故障排除的步骤。

• **第5章“交换的概念与局域网设计”**——本章讨论了局域网中的各种问题以及提高局域网性能的可能解决方案。此外，本章还介绍了使用网桥、交换机和路由器进行网络分段的优点和缺点，并介绍了交换、桥接和路由选择对网络吞吐量的影响。最后，本章介绍了以太网、快速以太网和VLAN技术及其各自的益处。

• **第6章“交换机”**——本章介绍了802.3局域网，以及在局域网设计中使用局域网分段的优点和不足。此外，本章还描述了基本的2层桥接和交换功能。

• **第7章“交换机配置”**——本章描述了局域网交换的过程。介绍了配置交换机并对配置进行验证的步骤，描述了密码恢复和固件升级过程。

• **第8章“生成树协议”**——本章提供了关于生成树协议和冗余拓扑结构的概述。

• **第9章“虚拟局域网”**——本章讨论了虚拟局域网（VLAN）的基本概念和益处。还介绍了如何对VLAN进行配置、验证、保存、删除和故障排除。

• **第10章“VLAN中继协议”**——本章提供了关于中继（trunking）的概述。此外，还介绍了VTP的概念、工作原理和配置。最后，本章还讨论了关于VLAN间路由选择的基础知识。

• **第11章“扩展的IP地址”**——本章描述了用NAT和PAT的网络进行扩展时所涉及的各个组件。还讨论了DHCP的工作原理、配置和故障排除步骤。

• **第12章“广域网技术”**——本章介绍了广域网环境中使用的各种协议和技术。描述了广域网的基本知识，包括常用的广域网技术、广域服务的类型、封装格式和链路选择。最后，本章讨论了点到点链路、电路交换、分组交换、虚拟电路、拨号服务和广域网设备。

• **第13章“点到点协议”** 本章讨论了定义PPP通信的基本组件、过程和工作原理。此外，本章还描述了如何配置和验证PPP和PPP身份验证。

• **第14章“ISDN和DDR”**——本章介绍了ISDN通信的服务、标准、组件、工作原理和配置。

• **第15章“帧中继”**——本章讨论了帧中继服务、标准、组件和工作原理。另外，本章还讨论了帧中继服务的配置任务以及监控和维护帧中继连接的命令。

• **第16章“网络管理介绍”**——本章概要介绍了广域网（WAN）设计中使用的方法论。包括对WAN通信的描述以及设计WAN的过程和需要考虑的问题。本章还包含了关于收集用户对WAN设计需求的过程和使用分层设计模型的益处。本章讨论了各种类型的工作站和服务器的基本组件，包括Microsoft、UNIX和Apple等各种系统。此外，本章还介绍了各种网络管理工具、OSI和网络管理模型以及管理软件如何收集信息并记录问题。

• **第17章“光网络基础”**——本章描述了光网络的速度、数据传送、容量和扩展性是如何提供的。本章还讨论了光网络的功能、由密集波分复用（DWDM）所提供的更强的扩展性和光网络所提供的解决方案。

• **第18章“网络管理”**——本章讨论了网络管理基本内容。介绍了网络文档、网络安全性、网络维护、数据恢复、服务器管理、服务器维护和网络故障排除。

• **第19章“Network+认证考试复习”**——本章对你成功通过Network+认证考试所需要知道的主题进行了复习。

• **第20章“CCNA认证考试复习”**——通过复习CCNA考试所覆盖的主题，本章能帮助你准备CCNA认证考试。

• **第21章“关于融合网络技术的介绍”**——本章描述了传统的语音、视频和数据网络的实施方式，并解释了各种类型的数据语音技术。本章还介绍了对融合的语音、视频和数据网络的需求。此外，本章还介绍了Cisco集成化语音、视频和数据体系结构（AVVID）和针对融合型网络的新应用。

• **第22章“制定网络安全和网络管理策略”**——本章帮助你与你的网络设计客户一同制定有效的安全策略。本章还将帮助你选择正确的工具和产品来实施这些策略。

• **第23章“虚拟专用网”**——本章用虚拟专用网作为安全性的一个明确的实例。本章覆盖了利用公共网络进行私有通信所用的基本机制。

• **附录A“术语表”**——术语表包含了本书中使用的所有关键术语的定义。

• **附录B“复习题答案”**——本附录提供了各章末尾“复习题”的问题答案。

关于光盘

本书所附的光盘能帮助你进一步提高学习效果。光盘中包括了配有CCNA考试练习问题的测试引擎、交互式e-Lab实验、关于网络设备和硬件的插图、强化难点概念的教学视频和动画。这些材料使你在教室以外也能参加学习和培养技能，从而实现了对自主学习的支持。光盘还提供了下列

内容：

- 易用的图形化用户界面。
- 分章节的各种练习和资源。
- 在线教程中没有的信息和练习。
- 关于考试练习问题的准确简明的答案。
- 学习者主导的练习和学习。
- 适合各个层次的学习者。
- 本书的术语表以及第19章的内容。

最后，这些学习工具不仅强调概念，也突出了学以致用的重要性。本光盘能帮助你理解网络技术，达到理论联系实践的效果。

思科系统公司网络图标图例

思科系统公司使用一套标准化的图标来表示在网络拓扑图中的各种设备。下列的图标图例显示你在本书中可能遇到的最常用的一些图标。



命令语法约定

本书命令语法的约定与Cisco IOS命令参考手册（Command Reference）中的约定是一样的。在命令参考手册中对约定的描述如下：

- 竖线（|）用于分开可选的、互斥的选项。
- 方括号（[ ]）表示任选项。
- 花括号（{ }）表示必选项。
- 方括号中的花括号加（比如[{ }]）表示需要在任选项中选择一个。
- **黑体**字表示照原样输入的命令和关键字。
- *斜体*字表示用户应该输入具体值的参数。

目　录

第一部分　复习

第1章　复习：OSI参考模型与路由选择 ……3

1.1　层次网络模型：OSI参考模型 ……4
1.1.1　对等层通信 ……5
1.1.2　数据封装 ……5
1.2　物理层 ……6
1.2.1　以太网/802.3物理连接 ……7
1.3　数据链路层 ……7
1.3.1　以太网/802.3接口 ……8
1.4　网络层 ……8
1.4.1　IP寻址与子网 ……8
1.4.2　路径选择 ……9
1.4.3　路径通信 ……10
1.4.4　ICMP ……11
1.4.5　ARP ……11
1.4.6　路由选择 ……12
1.4.7　被动路由协议与路由选择协议的对比 ……14
1.4.8　关于IP路由选择的配置任务 ……16
1.5　传输层 ……17
1.5.1　对上层应用进行分段 ……17
1.5.2　建立连接 ……17
1.5.3　数据传输 ……18
1.5.4　用窗口操作实现可靠性 ……18
1.5.5　确认技术 ……18
1.6　总结 ……19
1.7　关键术语 ……20
1.8　复习题 ……23

第二部分 CCNA 3：交换基础与中级路由选择

第2章 无类别路由选择介绍 ……27

2.1 CIDR概述 ……27
2.1.1 为什么需要CIDR ……27
2.2 路由聚合与超网 ……28
2.2.1 超网与地址分配 ……29
2.3 可变长子网掩码 ……30
2.3.1 VLSM的特征 ……30
2.3.2 计算VLSM ……32
2.3.3 配置VLSM ……33
2.3.4 使用RIP和IGRP时的VLSM ……33
2.4 路由汇总（Route Summarization）……34
2.4.1 在一个字节内汇总 ……35
2.4.2 汇总非连续网络 ……36
2.5 路由翻动（Route flapping） ……36
2.6 RIPv2 ……37
2.6.1 RIP的简史 ……37
2.6.2 RIPv2功能 ……38
2.6.3 比较RIPv1和RIPv2 ……38
2.6.4 配置RIPv2 ……39
2.6.5 验证RIPv2 ……40
2.6.6 对RIP进行故障排除 ……42
2.7 缺省路由 ……43
2.8 总结 ……44
2.9 关键术语 ……45
2.10 复习题 ……46

第3章 单区域OSPF ……47

3.1 单区域OSPF的概念 ……47
3.1.1 OSPF概述 ……48
3.1.2 OSPF术语 ……48
3.1.3 OSPF状态 ……49
3.1.4 比较OSPF和距离矢量路由选择协议 ……52
3.1.5 最短路径优先算法 ……52
3.1.6 OSPF网络类型 ……53
3.1.7 OSPF的Hello协议 ……53
3.1.8 OSPF的运行步骤 ……54
3.1.9 建立路由器毗邻关系 ……54
3.1.10 选举DR和BDR ……55
3.1.11 发现路由 ……56

3.1.12 选择最佳路由 ……56
3.1.13 维护路由信息 ……57
3.2 单区域OSPF配置 ……58
3.2.1 配置环回地址 ……58
3.2.2 修改OSPF路由器优先级 ……59
3.2.3 修改OSPF成本的量值 ……60
3.2.4 配置OSPF身份验证 ……61
3.2.5 配置OSPF定时器 ……61
3.3 在NBMA中配置OSPF ……62
3.3.1 全网状帧中继 ……63
3.3.2 部分网状帧中继 ……64
3.3.3 点对多点型OSPF ……65
3.4 传播缺省路由 ……65
3.5 常见OSPF配置问题 ……66
3.6 验证OSPF配置 ……66
3.7 总结 ……67
3.8 关键术语 ……68
3.9 复习题 ……69

第4章 增强内部网关路由选择协议 ……71

4.1 EIGRP概述 ……71
4.1.1 EIGRP规程与技术 ……72
4.1.2 EIGRP的益处 ……73
4.1.3 独立于被动路由协议 ……74
4.2 EIGRP术语 ……74
4.2.1 邻居表（Neighbor Table） ……74
4.2.2 拓扑表（Topology Table） ……74
4.2.3 后继（Successor） ……75
4.2.4 可行后继（Feasible Successor） ……75
4.2.5 后继和可行后继的选择 ……76
4.2.6 活动粘滞路由（Stuck in Active Routes） ……77
4.2.7 路由选择表（Routing Table） ……77
4.2.8 路由标记（Route Tagging） ……77
4.3 EIGRP特性与技术 ……78
4.3.1 邻居发现和恢复 ……78
4.3.2 可靠传输协议 ……79
4.3.3 DUAL有限状态机 ……79
4.3.4 PDM ……80
4.4 EIGRP分组类型 ……80
4.4.1 Hello分组 ……80
4.4.2 确认分组 ……81
4.4.3 更新分组 ……81

4.4.4 查询和回复分组 ……81
4.5 EIGRP收敛 ……82
4.6 配置EIGRP ……83
4.6.1 为IP配置EIGRP ……83
4.6.2 在NBMA中配置带宽 ……84
4.6.3 在多点网络中配置带宽 ……84
4.6.4 在混合多点网络中配置带宽 ……84
4.6.5 使用ip bandwidth-percent命令 ……85
4.6.6 配置EIGRP汇总 ……85
4.7 验证基本的EIGRP ……86
4.8 总结 ……87
4.9 关键术语 ……88
4.10 复习题 ……89

第5章 交换的概念与局域网技术 ……91

5.1 以太网/802.3局域网 ……91
5.1.1 以太网/802.3局域网的发展 ……91
5.1.2 影响网络性能的因素 ……95
5.1.3 以太网/802.3网络的要素 ……95
5.1.4 半双工以太网 ……95
5.1.5 全双工以太网 ……96
5.2 局域网交换技术简介 ……97
5.2.1 局域网分段 ……97
5.2.2 使用网桥的局域网分段 ……98
5.2.3 使用路由器的局域网分段 ……99
5.2.4 使用交换机的局域网分段 ……100
5.3 交换机的基本操作 ……101
5.3.1 以太网交换机延迟 ……104
5.3.2 第2层与第3层交换技术 ……104
5.3.3 第2层交换与第3层交换的含义 ……105
5.3.4 对称交换和非对称交换 ……105
5.3.5 内存缓冲 ……106
5.4 局域网设计 ……106
5.4.1 网络设计的目标 ……106
5.4.2 局域网设计的考虑因素 ……107
5.4.3 服务器的位置和功能 ……107
5.4.4 网络分段问题 ……107
5.4.5 广播域问题 ……108
5.4.6 局域网设计方法论 ……109
5.4.7 影响局域网可用性因素 ……109
5.4.8 物理网络拓扑的设计 ……110
5.4.9 第1层设计 ……110

5.4.10 第2层设计 ……112
5.4.11 第3层设计 ……117
5.4.12 基本的第2层桥接和交换 ……120
5.4.13 交换机和网桥如何过滤帧 ……123
5.4.14 过滤类型 ……123
5.5 总结 ……124
5.6 关键术语 ……125
5.7 复习题 ……128

第6章 交换机 ……131

6.1 交换机概述 ……131
6.2 交换机启动 ……132
6.2.1 Catalyst交换机的物理启动 ……132
6.2.2 交换机的LED指示灯 ……133
6.2.3 在交换机POST阶段检查端口LED ……135
6.2.4 观察交换机的初始启动输出 ……135
6.2.5 查看交换机命令行界面的帮助信息 ……137
6.3 局域网交换机与分级网络设计 ……140
6.3.1 核心层 ……140
6.3.2 汇聚层 ……141
6.3.3 接入层 ……141
6.3.4 交换式局域网、接入层概述 ……141
6.3.5 接入层交换机 ……141
6.3.6 汇聚层概述 ……142
6.3.7 汇聚层交换机 ……143
6.3.8 核心层概述 ……144
6.3.9 核心层交换机 ……144
6.4 总结 ……145
6.5 关键术语 ……146
6.6 复习题 ……147

第7章 交换机配置 ……149

7.1 微分段 ……149
7.2 交换机如何学习地址 ……152
7.3 交换机的各种转发方式 ……154
7.3.1 存储转发交换 ……154
7.3.2 贯穿式交换 ……154
7.3.3 对称交换 ……155
7.3.4 非对称交换 ……155
7.3.5 内存缓冲技术 ……156
7.4 交换机和冲突域 ……157
7.5 交换机和广播域 ……158

7.6 交换机与PC之间的通信 ……159
7.6.1 PC到交换机的传输 ……160
7.6.2 交换机之间的通信 ……160
7.7 检验Catalyst交换机的初始配置 ……160
7.7.1 检验Catalyst交换机的缺省配置 ……161
7.7.2 交换机端口属性 ……162
7.7.3 VLAN属性 ……162
7.7.4 闪存目录 ……163
7.7.5 显示IOS版本信息 ……163
7.7.6 使用缺省配置的好处 ……164
7.8 Catalyst交换机的网络设置 ……164
7.8.1 恢复交换机的缺省配置 ……165
7.8.2 指定交换机的主机名和密码 ……165
7.8.3 指定交换机的IP地址和缺省网关 ……165
7.8.4 设置端口属性 ……166
7.8.5 基于Web的界面 ……167
7.9 管理MAC地址表 ……167
7.9.1 配置静态MAC地址 ……169
7.9.2 配置端口安全性 ……169
7.10 实施添加、迁移和改变 ……170
7.11 管理交换机操作系统映像和设备配置文件 ……170
7.12 恢复1900/2950的密码 ……171
7.13 升级1900/2900固件的IOS ……171
7.14 总结 ……171
7.15 关键术语 ……172
7.16 复习题 ……173

第8章 生成树协议 ……175

8.1 冗余拓扑概述 ……175
8.1.1 什么是冗余 ……175
8.1.2 冗余拓扑 ……176
8.1.3 冗余交换拓扑 ……176
8.1.4 广播风暴 ……177
8.1.5 帧的重复传送 ……177
8.1.6 MAC数据库的不稳定性 ……178
8.2 生成树概述 ……178
8.2.1 生成树的运行 ……179
8.2.2 利用生成树构造无环路拓扑 ……180
8.3 STP的高级功能 ……180
8.3.1 选择根网桥 ……181
8.3.2 STP端口状态的转换过程 ……182
8.3.3 选举指定端口 ……184

8.3.4 路径成本 ……186
8.3.5 STP计时器 ……186
8.3.6 重新计算生成树 ……188
8.3.7 收敛 ……188
8.4 RSTP ……188
8.4.1 RSTP端口状态 ……189
8.4.2 转换到转发状态 ……189
8.5 总结 ……190
8.6 关键术语 ……191
8.7 复习题 ……192

第9章 虚拟局域网 ……195

9.1 VLAN介绍 ……195
9.2 用VLAN和路由器构成的广播域 ……197
9.3 VLAN的运行方式 ……198
9.4 端到端的VLAN ……200
9.5 地理性VLAN ……201
9.6 VLAN的优点 ……201
9.6.1 变动的管理 ……201
9.6.2 VLAN与安全 ……201
9.7 在VLAN中使用集线器 ……203
9.8 VLAN的类型 ……203
9.9 VLAN帧标识 ……203
9.9.1 IEEE 802.1Q：帧标记 ……203
9.9.2 交换机间链路协议 ……204
9.9.3 FDDI 802.10 ……204
9.9.4 局域网仿真（LANE） ……205
9.10 VLAN的配置 ……205
9.10.1 配置静态VLAN ……206
9.11 验证VLAN的配置 ……207
9.12 保存VLAN的配置 ……208
9.13 删除VLAN的配置 ……208
9.14 VLAN故障排除 ……209
9.15 总结 ……210
9.16 关键术语 ……212
9.17 复习题 ……213

第10章 VLAN中继协议 ……215

10.1 中继（Trunking） ……215
10.1.1 中继的概念 ……216
10.1.2 中继的运行方式 ……216
10.1.3 VLAN和中继 ……217

10.1.4 交换机命令行界面 ……218
10.1.5 中继的实现 ……218
10.2 VLAN中继协议 ……220
10.2.1 VTP的历史 ……220
10.2.2 VTP的概念 ……220
10.2.3 VTP的好处 ……221
10.2.4 VTP域 ……221
10.2.5 VTP模式 ……221
10.2.6 VTP的实施 ……223
10.2.7 VTP的配置 ……224
10.2.8 VTP剪裁 ……226
10.3 VLAN间路由选择 ……227
10.3.1 VLAN间的问题和解决方案 ……228
10.3.2 被隔离的广播域 ……229
10.3.3 寻找VLAN间的路由 ……229
10.3.4 物理和逻辑接口 ……230
10.3.5 将物理接口划分为多个子接口 ……230
10.3.6 配置VLAN间路由选择 ……230
10.4 总结 ……231
10.5 关键术语 ……232
10.6 复习题 ……233

第三部分 CCNA 4：广域网技术

第11章 扩展IP地址 ……237

11.1 Internet协议（IP）概述 ……237
11.2 NAT和PAT ……239
11.2.1 NAT和PAT的特性 ……241
11.2.2 配置NAT和PAT ……242
11.2.3 验证NAT和PAT的配置 ……246
11.2.4 NAT和PAT配置的故障排除 ……246
11.2.5 NAT的优点和缺点 ……247
11.3 DHCP概述 ……248
11.3.1 DHCP介绍 ……249
11.3.2 BOOTP和DHCP的区别 ……250
11.3.3 DHCP的特性 ……250
11.3.4 DHCP的运行方式 ……251
11.3.5 配置DHCP的操作 ……252
11.3.6 验证DHCP的操作 ……252
11.3.7 DHCP配置的故障排除 ……253
11.3.8 DHCP中继 ……253

11.4 总结 ……255
11.5 关键术语 ……256
11.6 复习题 ……257

第12章 广域网技术 ……259

12.1 广域网技术概述 ……259
12.2 广域网设备 ……261
12.3 广域网标准 ……262
12.4 广域网封装 ……264
12.5 广域网链路的选择 ……264
12.5.1 电路交换连接 ……264
12.5.2 分组交换连接 ……264
12.5.3 分组和电路交换 ……265
12.6 广域网技术 ……266
12.6.1 模拟拨号 ……266
12.6.2 ISDN ……267
12.6.3 租用线 ……268
12.6.4 X.25 ……269
12.6.5 帧中继（Frame Relay） ……269
12.6.6 ATM ……270
12.6.7 数字用户线（DSL）……271
12.6.8 电缆调制解调器（Cable Modem）……271
12.7 广域网通信 ……272
12.7.1 局域网/广域网集成 ……274
12.7.2 识别和选择网络能力 ……275
12.7.3 识别和选择连网模型 ……276
12.7.4 分级网络设计模型 ……276
12.7.5 3层设计模型 ……276
12.7.6 3层模型组件 ……278
12.7.7 分级广域网设计的优点 ……279
12.7.8 服务器的放置 ……281
12.8 广域网设计 ……282
12.8.1 设计广域网的步骤 ……283
12.8.2 收集需求 ……284
12.8.3 分析需求 ……285
12.8.4 敏感性测试 ……286
12.8.5 广域网拓扑 ……286
12.8.6 如何识别和选择连网能力 ……287
12.8.7 广域网设计的其他考虑事项 ……287
12.9 总结 ……288
12.10 关键术语 ……289
12.11 复习题 ……290

第13章 点到点协议 ……293

13.1 PPP分层体系结构 ……294
13.2 建立PPP会话 ……296
13.3 PPP身份验证协议 ……297
13.3.1 PAP ……297
13.3.2 CHAP ……297
13.4 PPP封装与验证过程 ……298
13.5 串行点到点连接 ……301
13.6 时分多路复用 ……301
13.7 分界点 ……302
13.8 数据终端设备（DTE）与数据通信设备（DCE）……302
13.9 HDLC封装 ……304
13.10 配置HDLC封装 ……304
13.11 串行接口的故障排除 ……305
13.12 配置PPP ……309
13.13 配置PPP封装 ……309
13.14 配置PPP身份验证 ……310
13.15 检验串行PPP封装配置 ……311
13.16 对串行PPP封装配置进行故障排除 ……312
13.17 总结 ……313
13.18 关键术语 ……315
13.19 复习题 ……316

第14章 ISDN和DDR ……319

14.1 ISDN标准 ……319
14.2 ISDN概述 ……320
14.3 ISDN标准及接入方式 ……322
14.4 ISDN3层模型及协议 ……323
14.5 ISDN呼叫建立 ……325
14.6 ISDN功能和参考点 ……326
14.7 确定路由器的ISDN接口 ……327
14.8 ISDN交换机类型 ……328
14.9 ISDN配置 ……328
14.9.1 配置ISDN BRI ……329
14.9.2 配置ISDN PRI ……331
14.9.3 验证ISDN配置 ……332
14.9.4 ISDN配置的故障排除 ……334
14.10 DDR路由 ……334
14.11 DDR运行方式 ……335
14.12 传统DDR ……336
14.13 为DDR定义静态路由 ……336

14.14 为DDR指定期望流量 ……337
14.15 配置DDR拨号器信息 ……337
14.16 拨号器原型（Dialer Profiles） ……339
14.17 配置拨号器原型 ……340
14.18 验证DDR配置 ……340
14.19 总结 ……342
14.20 关键术语 ……343
14.21 复习题 ……344

第15章 帧中继 ……347

15.1 帧中继概述 ……347
15.1.1 帧中继术语 ……348
15.1.2 帧中继运行方式 ……350
15.1.3 帧中继本地管理接口（LMI） ……352
15.1.4 LMI的运行方式 ……352
15.1.5 LMI的扩展 ……353
15.2 全局寻址 ……353
15.2.1 组播 ……354
15.2.2 反向ARP ……354
15.2.3 反向ARP和LMI运行的各个阶段 ……354
15.2.4 帧中继映射 ……355
15.2.5 帧中继交换表 ……355
15.3 帧中继运行总结 ……355
15.4 帧中继子接口 ……357
15.4.1 水平分割路由选择环境 ……357
15.4.2 使用子接口解决可达性问题 ……358
15.5 基本帧中继配置 ……358
15.5.1 配置串行接口 ……359
15.5.2 检验串行接口的配置 ……359
15.5.3 检验帧中继运行并确认连通性 ……360
15.5.4 确认线路的连通 ……360
15.5.5 确认帧中继映射 ……361
15.5.6 确认到中心站点路由器的连通性 ……362
15.5.7 配置子接口 ……362
15.5.8 配置可选命令 ……364
15.6 总结 ……365
15.7 关键术语 ……366
15.8 复习题 ……367

第16章 网络管理介绍 ……371

16.1 桌面和服务器操作系统简介 ……371
16.1.1 工作站 ……371

16.1.2 服务器 ……373
16.1.3 客户机/服务器关系 ……375
16.1.4 NOSs ……376
16.1.5 Window NT、Window 2000和Windows .NET ……378
16.1.6 UNIX和Linux ……379
16.1.7 Macintosh OS X ……383
16.2 服务器上的服务 ……383
16.2.1 文件共享 ……383
16.2.2 FTP和文件传输 ……384
16.2.3 Web服务 ……384
16.2.4 DNS ……384
16.2.5 DHCP ……384
16.3 网络管理 ……385
16.3.1 OSI和网络管理模型 ……385
16.3.2 标准：SNMP和CMIP ……386
16.3.3 SNMP操作 ……387
16.3.4 管理信息和MIB结构 ……390
16.3.5 SNMP协议 ……390
16.3.6 配置SNMP ……393
16.3.7 RMON ……393
16.3.8 系统日志（Syslog） ……394
16.4 总结 ……395
16.5 关键术语 ……396
16.6 复习题 ……397

第四部分 CCNA：额外资料

第17章 光网络基本原理 ……401

17.1 光网络基础 ……401
17.1.1 光技术的商业推动力 ……402
17.1.2 光纤系统 ……402
17.1.3 光纤传输系统 ……402
17.1.4 光 ……403
17.2 光纤 ……405
17.2.1 光纤类型 ……405
17.2.2 光纤的几何问题 ……406
17.2.3 衰减 ……408
17.2.4 光过滤器 ……408
17.2.5 光放大器 ……409
17.3 光传输和复用 ……410
17.3.1 SONET技术 ……410

17.3.2 SONET复用分级结构 ……411
17.3.3 DWDM系统 ……412
17.4 总结 ……415
17.5 关键术语 ……416
17.6 复习题 ……417

第18章 网络管理 ……419

18.1 网络文档 ……419
18.1.1 主配线架（MDF）和中间配线架（IDF）规划 ……420
18.1.2 服务器和工作站配置详细资料 ……420
18.1.3 软件列表 ……421
18.1.4 维护记录 ……421
18.1.5 安全性评估 ……421
18.1.6 用户策略 ……422
18.2 网络安全 ……424
18.2.1 数据恢复 ……424
18.2.2 备份操作 ……425
18.2.3 冗余技术 ……426
18.3 环境因素 ……427
18.3.1 电源条件 ……427
18.3.2 EMI和RFI ……427
18.3.3 软件病毒 ……427
18.4 网络性能 ……428
18.4.1 服务器管理 ……429
18.4.2 客户机/服务器网络 ……430
18.4.3 网络控制 ……432
18.5 网络管理中行政管理的一面 ……432
18.5.1 理解和建立网络的管理界限 ……433
18.5.2 网络成本 ……434
18.5.3 错误报告文档 ……434
18.6 网络监控 ……434
18.6.1 连接监控 ……435
18.6.2 通信监控 ……435
18.6.3 SNMP ……435
18.6.4 远程监控 ……436
18.7 网络故障排除 ……438
18.7.1 故障排除过程 ……438
18.7.2 故障排除的各种技术 ……438
18.7.3 各种软件工具 ……443
18.8 总结 ……447
18.9 关键术语 ……449

第19章 Network+认证考试复习 ……451

第20章 CCNA认证考试复习 ……453

20.1 OSI模型 ……453
20.1.1 应用层 ……453
20.1.2 表示层 ……454
20.1.3 会话层 ……454
20.1.4 传输层 ……454
20.1.5 网络层 ……454
20.1.6 数据链路层 ……455
20.1.7 物理层 ……455
20.2 桥接/交换 ……455
20.2.1 全双工和半双工以太网的运行方式 ……455
20.2.2 贯穿式交换和存储转发交换的区别 ……456
20.2.3 虚拟局域网（VLAN）的运行方式和好处 ……457
20.3 被路由协议 ……457
20.3.1 IP地址的不同类型，包括子网划分和私有地址 ……458
20.3.2 子网划分 ……459
20.3.3 十进制、十六进制和二进制之间的转换 ……461
20.4 路由选择协议 ……462
20.4.1 外部和内部路由选择协议 ……465
20.4.2 在路由器上启用RIP和IGRP ……465
20.4.3 IGRP和RIP使用的路由选择度量标准 ……466
20.4.4 比较和对比区分距离矢量、链路状态和混合协议的关键操作 …466
20.5 广域网协议 ……468
20.5.1 帧中继的关键术语和特征 ……469
20.5.2 区分LAPB、帧中继、ISDN/LAPD、HDLC、PPP和DDR ……469
20.5.3 配置ISDN BRI和传流的按需拨号路由选择（DDR） ……470
20.5.4 通过TFTP进行配置文件管理 ……471
20.5.5 如何加载一个软件映像备份 ……471
20.5.6 配置文件管理 ……472
20.5.7 通过TFTP管理IOS映像 ……473
20.6 因特网控制消息协议 ……474
20.6.1 ICMP消息传送 ……475
20.6.2 错误报告和错误纠正 ……475
20.6.3 不可达网络 ……475
20.6.4 用ping测试目的地的可达性 ……477
20.7 访问列表 ……478
20.7.1 ACL概述 ……478
20.7.2 创建ACL的原因 ……479
20.8 Cisco设备、IOS与网络基础 ……479
20.8.1 路由器初始启动输出 ……479

20.8.2 建立一个超级终端会话 ……480
20.8.3 登录进入路由器 ……481
20.8.4 键盘帮助 ……481
20.8.5 IOS编辑命令 ……484
20.8.6 路由器命令历史 ……484
20.8.7 对命令错误进行故障排除 ……485
20.8.8 Cisco IOS的目的 ……485
20.8.9 Cisco IOS的运行 ……485
20.8.10 Cisco IOS的特征 ……486
20.8.11 show version命令 ……486
20.8.12 路由器用户界面 ……487
20.8.13 Cisco IOS故障排除 ……487
20.9 总结 ……488
20.10 关键术语 ……489

第21章 关于融合型网络技术的介绍 ……491

21.1 传统网络 ……491
21.2 关于语音和数据网络的介绍 ……492
21.2.1 帧中继语音 ……492
21.2.2 ATM语音 ……492
21.2.3 IP语音 ……493
21.2.4 比较各种数据语音技术 ……493
21.3 语音、视频和数据网络 ……494
21.3.1 Cisco AVVID ……494
21.3.2 融合网络的各种应用 ……495
21.3.3 IP PBX ……495
21.3.4 统一消息传送 ……495
21.3.5 Cisco IP联络中心 ……496
21.4 QoS的常见问题 ……497
21.4.1 延迟（Delay） ……497
21.4.2 抖动（Jitter） ……497
21.4.3 丢包（Lost Packets） ……498
21.4.4 回声（Echo） ……498
21.4.5 Cisco IOS 软件的QoS技术 ……498
21.5 总结 ……499
21.6 关键术语 ……500

第22章 制定网络安全和网络管理策略 ……501

22.1 网络安全性设计 ……501
22.1.1 确定网络资产并分析风险 ……502
22.1.2 分析安全需求和折衷方案 ……502
22.1.3 制定安全方案 ……502

22.1.4 定义安全策略 ……503
22.1.5 安全策略的组成部分 ……503
22.1.6 制定安全过程 ……503
22.2 安全机制 ……503
22.2.1 身份验证（Authentication） ……504
22.2.2 授权（Authorization） ……504
22.2.3 记帐（审核）（Accounting（Auditing）） ……504
22.2.4 数据加密（Data Encryption） ……505
22.2.5 分组过滤器（Packet Filter） ……506
22.2.6 防火墙（Firewalls） ……507
22.2.7 入侵检测（Intrusion Detection） ……507
22.2.8 物理安全性（Physical security） ……507
22.3 选择安全解决方案 ……507
22.3.1 保护因特网连接 ……508
22.3.2 保护因特网域名系统服务 ……508
22.3.3 逻辑网络设计和因特网连接 ……508
22.3.4 IP安全协议 ……509
22.3.5 保护拨号访问 ……509
22.3.6 保护网络服务 ……510
22.3.7 保护用户服务 ……510
22.4 总结 ……511
22.5 关键术语 ……512

第23章 虚拟专用网 ……515

23.1 VPN的运行方式 ……515
23.1.1 VPN的优点 ……515
23.1.2 VPN的类型 ……516
23.1.3 服务水平协议 ……516
23.1.4 VPN示例 ……517
23.1.5 网络A各站点间的VPN ……517
23.2 VPN的实施 ……518
23.2.1 安全审核 ……518
23.2.2 范围和应用的需求 ……518
23.2.3 文档编制 ……518
23.2.4 安全策略 ……518
23.3 Cisco的VPN设计 ……518
23.3.1 隧道概述 ……519
23.3.2 Cisco的虚拟拨号服务 ……520
23.3.3 Cisco L2TP的实施 ……520
23.3.4 端到端虚拟拨号过程 ……521
23.4 虚拟拨号服务要点 ……522
23.4.1 身份验证与安全机制 ……522

23.4.2 授权 ……522
23.4.3 地址分配 ……522
23.4.4 记帐 ……523
23.5 总结 ……523
23.6 关键术语 ……524

第五部分 附录

附录A 术语表 ……526

附录B 复习题答案 ……527

第一部分 复习

第1章 复习：OSI参考模型与路由选择



第1章　复习：OSI参考模型与路由选择

目标

学习完本章之后，你将能够：

- 描述OSI参考模型全部功能及它能解决的问题。
- 描述OSI参考模型物理层的特性。
- 描述OSI参考模型数据链路层的特性。
- 描述OSI参考模型网络层的特性。
- 描述OSI参考模型传输层的特性。
- 描述网络中路由选择的功能。
- 理解路由选择协议的不同类别。

网络是包含多种介质、多种协议，并且与一个组织的中心办公室以外的网络互连的复杂环境。良好设计和仔细安装能减少伴随网络环境变化而产生的问题。

不论设备性能和介质能力如何先进，设计、建设和维护一个***网络***（network）都是一项具有挑战性的任务。即使是一个仅由50个路由节点组成的小型网络也能产生导致后果无法预测的复杂问题。有数千个节点的大型网络则会产生更多复杂的问题。

本章将对开放系统互连（Open System Interconnection，OSI）参考模型进行回顾，并对与路由相关的网络规划和设计进行概要介绍。使用OSI参考模型作为网络设计的参考便于适应网络的变化。使用OSI参考模型作为网络设计的层次结构可让你按层次来设计网络。OSI 参考模型是建设和设计网络的核心，其每一层都完成推动数据通信的特定任务。本章着眼于第1层到第4层。这 4 层定义了：

- 局域网和广域网介质的类型和速度。
- 数据是如何在介质中传送的。
- 寻址方案的类型。
- 如何进行流量控制。
- 路由选择协议的类型。

请注意配合本书配套光盘上的e-Lab实验、视频和插图一起阅读本章内容，光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

1.1　层次网络模型：OSI参考模型

网络模型使用分层来能简化网络的功能。将网络功能进行划分称为*分层*（layering）。为了理解分层的重要性，让我们来考虑一下OSI参考模型，它是用来理解和实现计算机通信的分层模型。通过分层，OSI参考模型简化了两台计算机互相通信所要完成的任务。每层集中完成特定的功能，因此允许网络的设计者为每层选择适当的网络设备和功能。在OSI参考模型中，它的7层分别表示不同的功能。

划分网络功能的原因包括：

- 分层把网络操作分成不太复杂的单元。
- 分层为即插即用的兼容性定义了标准接口。
- 分层使设计者能够专心设计和开发功能模块。
- 分层提高了不同网络模块功能的对称性，让它们能很好地一起工作。
- 分层使得一个区域的变化不会影响其他区域，这样每个区域都能更快地发展。
- 分层把复杂的网络通信过程分解成了独立的、易于学习的操作。

如图1-1显示，OSI参考模型的每层完成特定的功能：

- **应用层（第7层）**——这一层给用户应用程序提供网络服务。例如，字处理应用程序使用这一层的文件传输服务。
- **表示层（第6层）**——这一层提供数据表示和编码格式，以及数据传输语法的协商。它确保应用程序能使用从网络送达的数据，并且应用程序发送的信息能在网络上传送。
- **会话层（第5层）**——这一层负责建立、维护和管理应用程序之间的会话。
- **传输层（第4层）**——这一层提供流量控制、窗口操作和纠错功能。它还负责数据流的分段和重组。传输层具有保证连接和提供可靠传输的能力。传输层还负责分配一个端口号，用来把信息传递给上层。
- **网络层（第3层）**——这一层通过标识终端点的逻辑地址定义端到端的分组传送，从而决定把数据从一个地方移到另一个地方的最佳路径。路由器在这一层上工作。第3层使用管理员能够进行管理的逻辑寻址方案。该层可以使用IP协议的寻址方案或AppleTalk、DECnet、VINES和IPX寻址方案。
- **数据链路层（第2层）**——这一层提供了跨越介质的物理传输过程。它提供错误检测，在某些情况提供错误纠正、网络拓扑和流量控制。这一层使用*介质访问控制（MAC）*地址，也称为物理地址或硬件地址。
- **物理层（第1层）**——这一层提供电气的、机械的、规程的及功能的手段来激活和保持系统间的物理链路。这一层使用的物理介质有双绞线、同轴电缆和光纤等。



图1-1　7层OSI参考模型



实验活动　OSI模型和TCP/IP模型

在这个实验中，描述和对比OSI模型和TCP/IP模型层次。列举每一层的TCP/IP协议和功能。



实验活动　OSI模型封装和设备

在这个实验中，描述OSI模型各层及其特点，并指出各层数据封装的单元和设备。

1.1.1 对等层通信

OSI参考模型定义了每一层的功能，任何网络设备生产厂家都可将其用于指导设计和开发网络设备。OSI参考模型描述了在不同计算机上，应用程序的信息是如何通过网络介质传送的。当要发送的信息逐层向下传送时，信息越到下层就越不像人类的语言，而更像计算机能够理解的“1”和“0”。

每一层使用自己层的协议与其他系统的对等层相互通信。每一层协议与对等层交换的信息称为协议数据单元（PDU，Protocal Data Units）。

图1-2是OSI中通信的一个例子。在主机与主机间对等层协议的通信中，对等层依靠相邻层提供的服务来进行通信，每一层由其下一层对其提供服务。举个例子，主机A发送信息给主机B。主机A的应用程序与主机A的应用层通信，主机A的应用层再与主机A的表示层通信，主机A的表示层再与主机A的会话层通信等等，直到到达主机A的物理层。物理层在网络物理介质上发送（和接收）信息。当信息在网络物理介质上传送并被主机B接收后，会以相反的方向向上通过主机B的各层（先是物理层，然后是数据链路层等等），直到最终到达主机B的应用层。

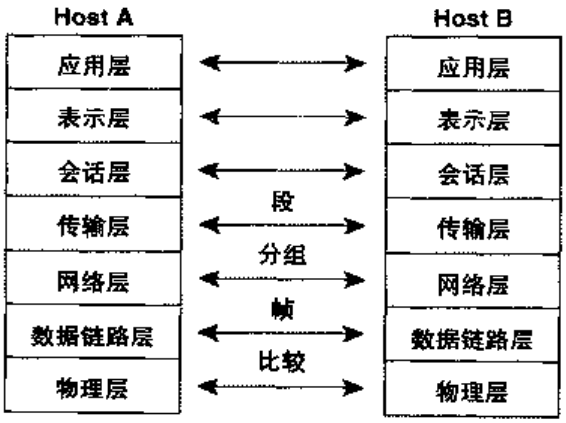


图1-2 OSI参考模型通信

尽管主机A的每一层只与它自己的相邻层通信，但主机的每一层总有一个主要任务必须要执行。每一层的主要任务是与主机B的对等层进行通信。也就是说A主机第1层的任务是与B主机的第1层通信；A主机第2层的任务是与B主机的第2层通信；等等。

OSI参考模型的分层禁止了不同主机间的对等层之间的直接通信。因此主机A的每一层必须依靠主机A相邻层提供的服务来与主机B的对等层通信。假设主机A的第4层必须与主机B的第4层通信。那么，主机A的第4层就必须使用主机A第3层提供的服务。第4层叫做服务用户（service user），第3层叫做服务提供者（service provider）。第3层通过一个服务接入点（SAP，Service Access Point）给第4层提供服务。这些服务接入点使得第4层能要求第3层提供服务。

如图1-2所示，TCP的段成为在IP协议节点间交换的网络层***分组***（Packts）（或者叫***数据报***（datagramy））的一部分。接着，IP协议的分组必须成为在直接相连设备间交换的数据链路帧的一部分。最终，这些帧必须转换为比特，因为这些数据是使用硬件通过物理层协议来传输的。

1.1.2 数据封装

主机B的第4层如何知道主机A的第4层想要什么呢？把第4层的特定要求存储为控制信息，这些控制信息附加在实际应用信息的分组***报头***（header）中并在对等层之间进行传输。每一层都依靠于OSI参考模型中其下一层提供的服务功能。为了提供这些服务，下层通过封装把上层的PDU放入它的数据字段；然后该层将会把它要使用的所有报头和报尾进行添加以执行本层的功能。

数据报头和数据的概念是相对的，这取决于对当前信息单元进行分析的层。例如，到了第3层，一个信息单元便包含第3层的报头的后续的数据。但第3层数据潜在地包含了从第4、5、6、7层来的报头。此外，第3层的报头却只是第2层的数据。这些概念如图1-3所示。最后，并不是所有层都需要加报头。一些层只是简单地对它们

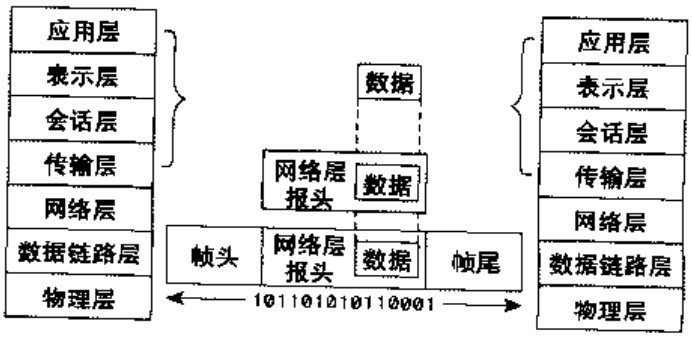


图1-3 网络层

接收的实际数据进行一些转换，使得数据对于相邻层是可读的。

网络层通过把数据封装在一报头内来实现数据在网络中的传送。例如，网络层向传输层提供服务，传输层把数据提交给网络层。网络层将数据封装在报头内。报头包含完成传输所要求的信息，例如源和目的逻辑地址。接着，数据链路层也向网络层提供服务，把网络层信息封装在一个帧内。帧头含有完成数据链路功能所需信息。例如，帧头包含物理地址。物理层也向数据链路层提供服务，把数据链路帧编码成能在介质（通常是铜线或光纤）中传输的，由“1”和“0”构成模式。

例如，假设主机A想发送下列E-mail给主机B：

The small gray cat ran up the wall to try to catch the red bird.

将该E-mail发送到合适目的地数据封装过程包括5个转换步骤：

步骤1　当用户发送E-mail消息时，其中的字母和数字字符被转化成数据，从第7层向下传到第5层，然后在网络上传输。

步骤2　在第4层通过使用段，传输功能把数据进行打包使它能用于网络传输，并确保E-mail系统两端的消息主机能可靠通信。

步骤3　数据在第3层被放入分组（或数据报），其中包含源和目的逻辑地址的网络报头。然后，网络设备沿着一条选定的路径在网络上发送这些分组。

步骤4　每个网络设备在第2层必须把分组放入帧内，以连接到链路上下一台直连的网络设备。选定的网络路径上的每台设备都需要通过成帧（framing）来连接下一台设备。请记住，路由器是第3层设备，它使用IP地址来选择分组到达目的地必须经过的路径。路由器选择了一条路径以后，它通常是把分组从它的一个有MAC地址的第2层接口发往另一台路由器的MAC地址。

步骤5　在第1层，帧必须转换成可以在介质（通常是铜线或是光纤）中传输的“1”和“0”模式。时钟（Clocking）功能使得设备能区分在介质中传送的比特。所选路径中的物理网络介质可能不同。例如，E-mail消息可能来自一个LAN，然后通过校园网的骨干，再经过WAN链路，直到到达另一个远端LAN中的目的地。

1.2　物理层

目前以太网和IEEE 802.3占据着局域网协议的最大份额。如今，以太网（Ethernet）这个名词常用来指所有使用带冲突检测载波侦听多路访问（CSMA/CD）的局域网，这些局域网通常符合IEEE 802.3在内的各种以太网规范。

以太网设计用于填补长距离、低速网络和在非常有限距离内高速传送数据的计算机机房专用网络之间的空白。对于需要在本地通信介质上传送偶发的，峰值数据速率很多大量通信的应用场合，以太网非常适合。

以太网指的是一个局域网实现家族，主要包含3类：

- **以太网和 IEEE 802.3**

—— 运行于同轴电缆和双绞线上的10Mbit/s局域网规范。

- **100Mbit/s以太网**

—— 也称作快速以太网（Fant Ethernet），它规定了运行在双绞线电缆上的100Mbit/s规范。

- **1000Mbit/s 以太网**

—— 也称作吉比特以太网（Gigubit Ethernet），它规定了运行在光纤和双绞线电缆上的1Gbit/s规范。

由于非常灵活、易于实施和容易理解，以太网作为一种基本的介质技术生存了下来。尽管其他技术已经得到了发展，并有取代以太网的可能，但是网络管理员已经使用以太网以及以太网的派生技术有效地满足了一系列校园网应用要求。为了解决以太网的局限性，有创造性的用户（和标准化

组织）已经创造了越来越高的以太网传输容量。批评家也许认为以太网是一种不能发展的技术，但其的下层传输方案仍然是目前园区网应用中传输数据的主要手段之一。

1.2.1 以太网/802.3物理连接

以太网和IEEE 802.3线路标准定义了以10 Mbit/s运行的总线型局域网。

图1-4描述了3个定义的布线标准：

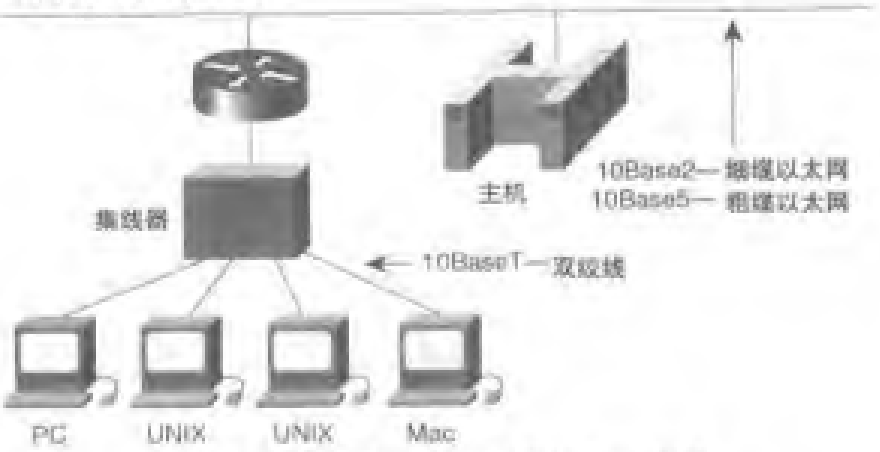


图1-4 10Base2、10Base5和10BaseT标准

- 10Base2——也称*细缆以太网*（thin Ethernet或ThinNet），10Base2允许网段在同轴电缆上的最大传输范围是185m。
- 10Base5——也称*粗缆以太网*（thick Ethernet），10Base5允许网络段在同轴电缆上的最大传输范围是500m。
- 10BaseT——10BaseT在便宜的双绞线上传送以太网帧，最大传输范围是100m。

10Base2、10Base5和10BaseT标准提供了在同一个局域网段中访问多台工作站的能力。以太网和IEEE 802.3布线标准规定了一种总线拓扑的网络，这种总线拓扑的网络在终端工作站和实际网络介质间用电缆连接。在以太网中，这根电缆叫做收发器电缆（tranceiver cable）。收发器电缆与附在物理介质上的收发设备相连接。IEEE 802.3的配置大致相同，只是连接电缆称为***附接单元接口（Attachment unit interface，AUI）***，收发器称为介质连接单元（Media attachment unit，MAU）。在这两种情况下，连接电缆都是与终端工作站内的接口板（或接口电路）连接的。

通过一条从工作站的附属单元接口到与以太网同轴电缆直接相连的中间集中设的电缆，各个工作站实现了到网段的连接。10BaseT以太网也使用总线拓扑结构，但只是一种逻辑总线，因为它是通过集线器或交换机的电路来实现的。在物理上，10BaseT以太网使用星形或扩展星形拓扑结构，所有的网络节点都连接到中央集线器或局域网交换机。

1.3 数据链路层

访问网络介质发生在OSI参考模型的数据链路层。数据链路层，也就是第2层，它与物理层相邻，MAC地址就位于这一层。没有两个MAC地址是相同的。***网络接口卡（Network Interface Card，NIC）***是你插进计算机里的扩展板，它使得计算机能够连到网络上。大部分网卡根据特定的网络类型、协议和介质而设计，尽管这样，一些网卡可以用于多种类型网络。在网络上，网卡是设备接到介质的地方，并且每个网卡都有惟一的MAC地址。

在每个网卡出厂前，硬件制造商给它分配一个MAC地址，这个地址被编程写入网卡上一个芯片中。由于MAC地址在网卡中，如果更换一台计算机的网卡，这个工作站的物理地址就改变为新网卡的MAC地址。

MAC地址用16进制表示。有两种MAC地址格式：0000.0c12.3456和00-00-0c-12-34-56。

设想你管理一个汽车旅馆。207房间有一个锁A，钥匙A能开207房间的门；410房间有一个锁F，钥匙F能开410房间的门。

你决定将房间207和410的锁互换。换完锁后，钥匙A能开房间410的门，钥匙F能开房间207的门。

类似地，锁就像网卡。当网卡交换时，与之匹配的钥匙也必须交换。计算机的MAC地址在网卡中，如果更换了网卡，MAC地址也随之改变。

在一个以太网上，当一台设备想向另一台设备发送数据时，它可以使用MAC地址建立一条通向其他设备的通信路径。当数据从源设备发送到网络时，它携带想去的目的MAC地址。当数据沿着网络介质传送时，网络上每台设备的网卡检查自己的MAC地址是否与这个帧携带的物理目的地址匹配。如果不匹配，则网卡忽略这个帧。该帧继续沿着网络向下一站传送。

如果匹配，网卡把该帧进行一次拷贝，把帧放在计算机的数据链路层中。即使由网卡产生了这份拷贝并放在计算机中，原始的帧仍然会沿着网络传输。这样其他网卡就可以看到它，并决定是否匹配。

1.3.1　以太网/802.3接口

以太网和802.3数据链路提供了在连接两台设备的物理链路上的数据传输，如图1-5所示，3台设备在以太网LAN上能直接相连。MAC机在左边，基于Intel的PC在中间，它们的数据链路层使用的MAC地址显示在下方。右边路由器上每个局域网的接口也使用MAC地址。为了标识路由器上的802.3接口，可以使用*Cisco互连网络操作系统（IOS Cisco Internetwork Operate System）*的端口类型缩写E，后面再跟一个接口编号（例如FA0）。

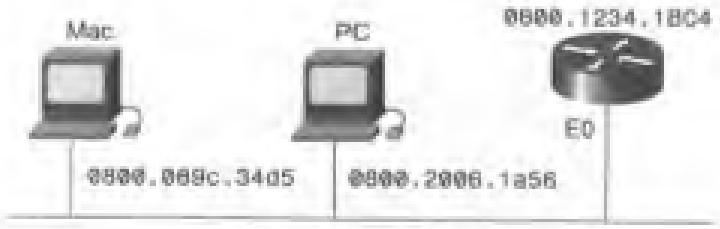


图1-5　以太网/802.3接口

注：在模块化路由器上的快速以太网接口指定为Fa0/0（2600和其他型号）。缩写Fa表示快速以太，0/0表示0插槽上的0端口或接口。

1.4　网络层

运行在OSI参考模型网络层的几种协议为：

- IP协议，提供对被选路的数据报（或者分组）无连接的、*尽力的（best-effort）传输*。它不关心数据报的内容，而是要寻找一条把数据报移到目的地的路径。
- **因特网控制消息协议（ICMP）**，提供控制和发送消息的能力。
- **地址解析协议（ARP）**，根据已知IP地址决定数据链路层地址。
- **反向地址解析协议（RARP）**，在数据链路层地址已知时，决定网络层地址。

1.4.1　IP寻址与子网

在TCP/IP环境中，终端工作站与服务器、主机或其他终端工作站通信。这是因为使用TCP/IP协议组的每个节点都有一个惟一的32比特逻辑地址，即IP地址。另外，在TCP/IP协议环境里，每个网络被看作一个单独的、惟一的地址。在访问到这个网络内的单个主机之前，必须首先能访问到这个网络。

网络能被分割成一系列更小的被称为**子网**（Subnetworks）的网络。如图1-6所示。IP地址分成



图1-6 子网

网络号、子网号和主机号。子网使用惟一的32位子网地址，它是通过从地址主机字段借位产生的。子网地址对于同一网络上的其他设备是不可见的，因为详细的子网规划信息不会与邻居路由器共享。

子网使得网络地址空间得到更有效的利用。从外部看这个网络没有什么变化，但是从组织内部看会有一个附加的结构。路由器用子网地址决定目标网络，这限制了到其他网段的通信量。在图1-7中，网络172.16.0.0被分成4个子网：172.16.1.0、172.16.2.0、172.16.3.0和172.16.4.0。

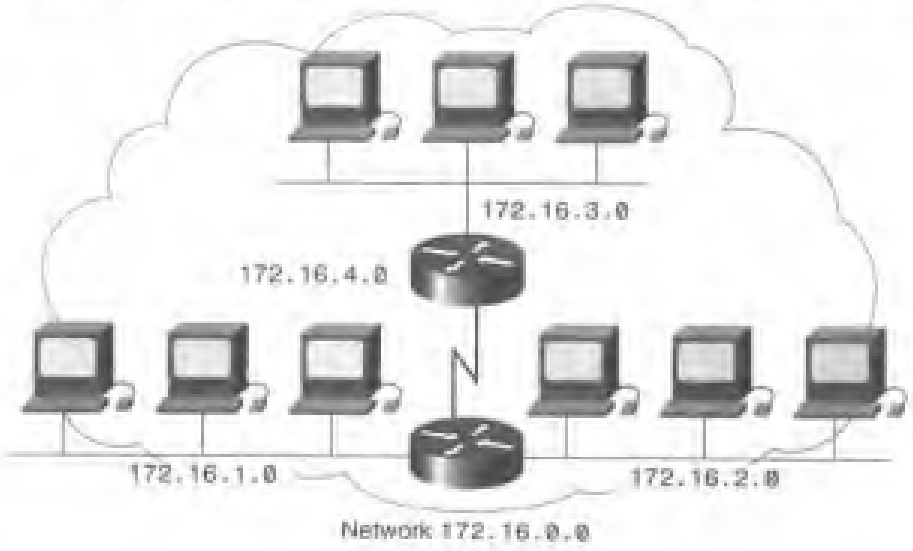


图1-7 划分子网

1.4.2 路径选择

路径选择（path determination）是指通信穿过网云所应该采取的传输路径。路径选择功能使路由器能评估到目的地的可用路径，并建立对分组的优先处理方式。如图1-8所示，路由器评估通信传输的最佳路径。路径选择发生在第3层，即网络层。当评估网络路径时，路由选择服务使用网络拓扑信息。这些信息可以由网络管理员进行配置或通过运行于网络中的动态过程收集。

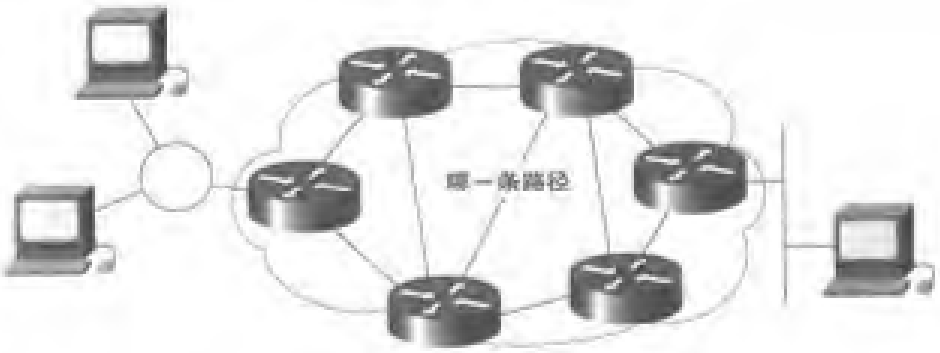


图1-8　路径选择

在网络中，网络层提供尽力的端到端分组传输服务给它的用户（即传输层）。网络层根据IP路由选择表从源网络发送分组到目的网络。当路由器决定了所使用的路径后，它使用交换功能来处理这个分组。交换功能是指路由器从一个接口接收一个分组，并把它转发到另一个体现了到达目的地的最佳路径的接口或端口。

1.4.3　路径通信

要使路径通信有真正的实用性，网络必须始终能代表路由器之间的所有可用路径。地址必须包含关于介质连接的路径信息，以便路由选择进程能将分组从源传送到目的地。如图1-9所示，路由器之间的每一条线都有一个数字，它代表路由选择进程可以使用的子网地址。这些地址必须转换成能被路由选择进程处理的信息。

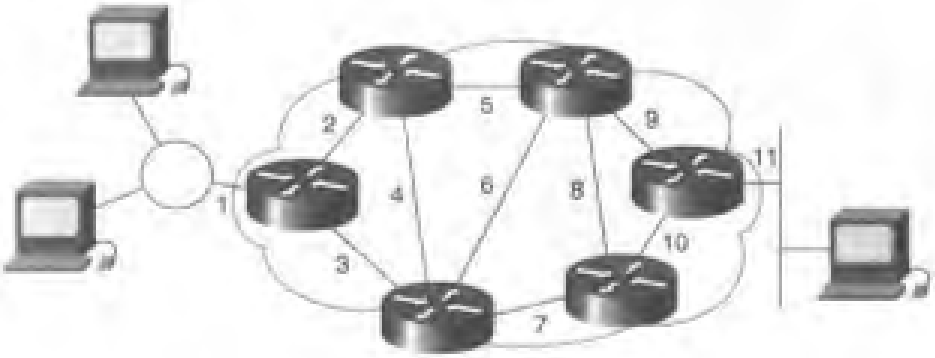


图1-9　路径通信

网络地址包含路径部分和主机部分。路径部分指明在网络云内被路由器使用的路径；主机部分指明网络上的特定端口或设备。路由器使用网络地址来确定一个网络内分组的源或目的网络。

大多数网络协议的寻址方案使用了某种形式的主机或节点地址。图1-10显示了连接到路由器的3个网络号以及共享一个网络号1的3台主机。对于某些网络层协议，网络管理员根据网络寻址方案提前分配网络地址来建立这种联系。对于其他的网络层协议，地址分配是部分或完全动态的。

在整个网络上使用第3层地址，避免了不必要的广播，从而提高了带宽的利用率。广播造成了不必要的通信，并且浪费了那些本来不需要接收广播的设备和线路的容量。通过使用端到端的一致性编址方案来表示介质的连接路径，使得网络层不需要使用一些不必要的设备或链路就能找到一条到达目的地的路径。

网络	主机
1	1 2 3
2	1
3	1

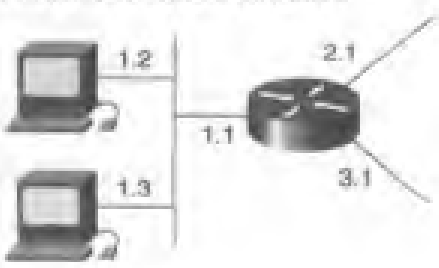


图1-10　寻址方案

1.4.4 ICMP

ICMP消息是通过IP数据报传送的，它用来发送错误和控制消息。ICMP使用下列定义的消息类型（还有其他一些消息未包括在下面的列表中）：

- 目的不可达（*Destination unreachable*）。
- 超时（*Time exceeded*）。
- 参数问题（*Parameter problem*）。
- 源抑制（*Source quench*）。
- 重定向（*Redirect*）。
- 回应请求（*Echo request*）。
- 回应回复（*Echo reply*）。
- 时间标记请求（*Timestamp request*）。
- 时间标记回复（*Timestamp reply*）。
- 消息请求（*Information request*）。
- 消息回复（*Information reply*）。
- 地址请求（*Address request*）。
- 地址回复（*Address reply*）。

路由器发送一条目的不可达消息，指明主机、端口或网络不可达。图1-11显示了一台路由器收到一个不能被送到最终目的地的分组；因此，这台路由器向源设备发送一条ICMP主机不可达消息。这个消息可能无法传送，因为不知道到达目的地的路由。ping命令的结果也可能包括其他的ICMP消息，例如不可达消息和超时消息。

另一方面，图1-12显示了对ping命令成功回复的回应回复（echo reply）消息。

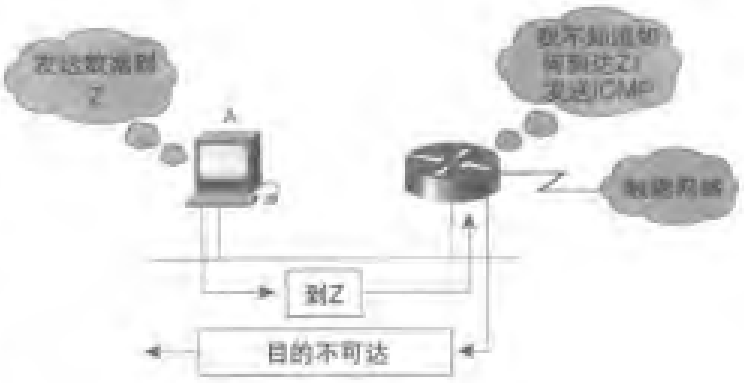


图1-11 无法送达的分组

1.4.5 ARP

为了在以太网上进行通信，源站点必须知道目的站点的IP地址和MAC地址。当源站点确定了目的站点的IP地址后，源站点的IP协议将查看自己的ARP表来定位目的站点的MAC地址。如果源站点在它的ARP表中定位到目的IP地址所对应的目的MAC地址，它将会把这个MAC地址与IP地址进行绑定，并用它们来进行数据封装。于是数据分组通过网络介质被发送，并被目的站点接收。

当网络设备需要发送数据时，它会在它的ARP表中查找目的地址。如果在表中未能找到这个地址，就会广播一个ARP请求来查找目的站点的MAC地址。网络上的每一台设备都将收到这个广播。

本地ARP通过查看子网掩码来解析地址。术语*本地ARP*（local ARP）是指发送请求的主机和目的主机共享同一介质或线缆的时候。（见图1-13）。

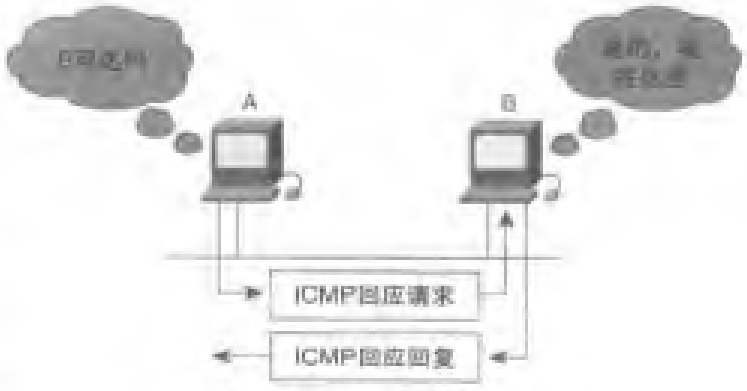


图1-12 ping命令的结果

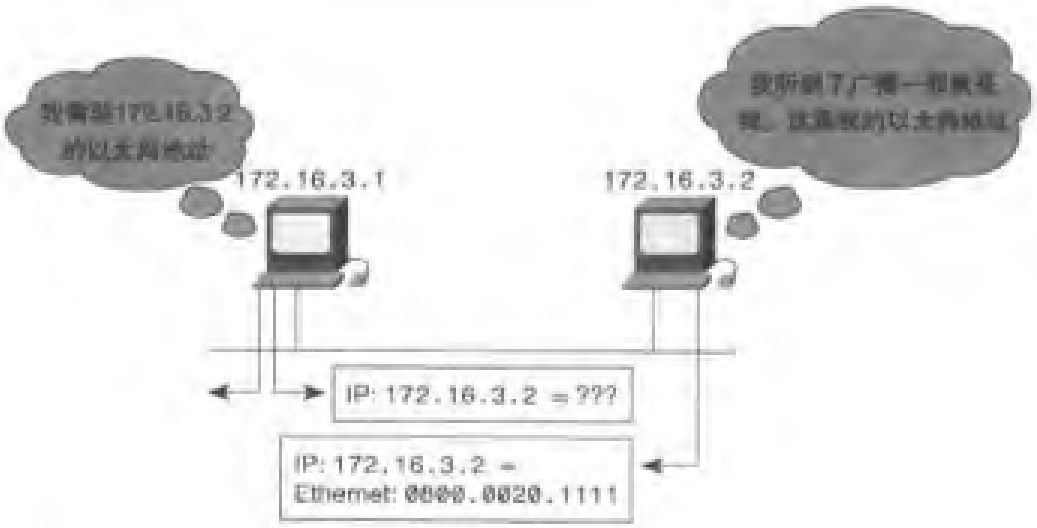


图1-13　本地ARP

1.4.6　路由选择

网络层必须与各种类型的下层联系和接口。路由器必须能够无缝地处理被封装进不同下层帧的分组，而不改变分组的第3层地址。图1-14显示了LAN到LAN进行路由选择的一个例子。在这个例子中，来自以太网1的主机4的分组需要一条到网络2上主机5的路径。

在检查它的路由选择表条目时，路由器发现到网络2的最佳路径使用输出端口To0，To0是到令牌环局域网的接口。尽管当路由器把分组通信从以太网1交换到令牌网2时，下层的数据帧必须改变，但第3层的源和目的地址仍然不变。局域网主机依靠路由器及其相符合的网络地址来找到最佳路径。在图1-14中，目的地址仍然是网络2的主机5，而不论下层的封装有什么不同。

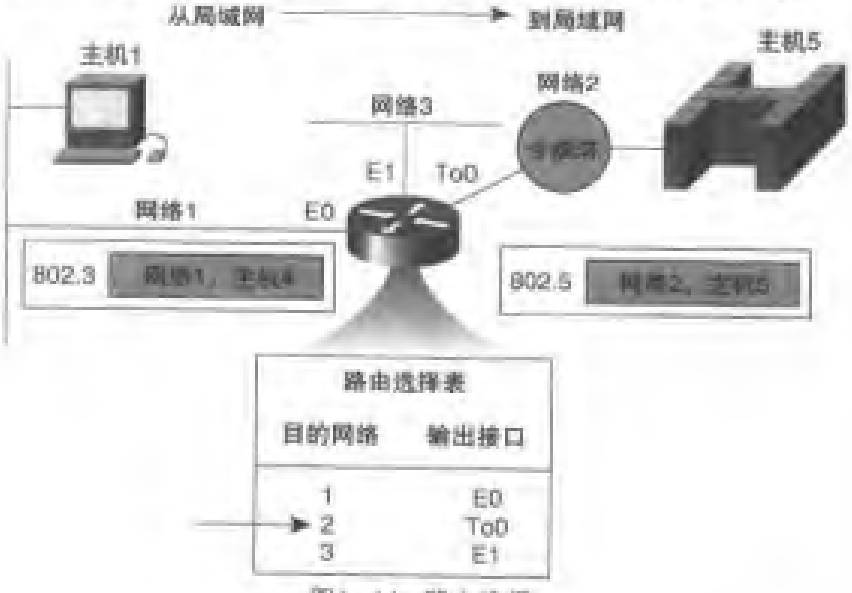


图1-14　路由选择

1　路由器的各种操作

路由器通常把分组从一条数据链路传送到另一条数据链路。为了传送分组，路由器使用了两个基本的功能：路径选择（Path determination）功能和交换（switching）功能。路由器沿着路径把分组传给下一个网络，并使用地址的网络部分进行路径选择。图1-15显示了路由器如何用寻址完成路由选择功能和交换功能。

交换功能让路由器能从一个接口接收分组并转发到第二个接口。路径选择功能使路由器能选择最合适的接口来转发分组。地址的节点部分是指路由器的某一特定端口，该端口通向那个方向的毗邻路由器。

目的网络	方向和路由器的端口
1.0 2.0 3.0	1.1 2.1 3.1



图1-15 路由器操作

当一台主机的应用程序需要向位于另外一个网络的目的地发送分组时，路由器便会从某个接口收到一个数据链路层帧。网络层软件检查分组报头以决定目的网络，然后再查看路由选择表。路由选择表把网络与输出端口联系起来。原始的帧被剥去并丢弃。分组被再次封装进所选端口的数据链路帧，并放进发送到该路径的下一跳（hop）的队列（queue）中。

每当分组被交换到另一台路由器时都会发生上述过程。当分组到达包含目的主机的网络的路由器时，分组被再次封装为目的局域网的数据链，并发送到目的主机。

2 静态路由与动态路由对比

静态路由选择（static routing）是手工管理的。网络管理员把它输入路由器的配置中。只要网络的拓扑发生变化并需要更改路由选择表时，网络管理员就必须手动更新静态路由选择。由于不发送路由选择更新（对于RIP，每30秒一次），静态路由选择减少了额外开支。

动态路由选择（Dynamic routing）与静态路由选择不一样。网络管理员输入配置命令，启动动态选择路由后，会以一定的时间隔自动更新路由信息或者只要从网络上收到新信息就会发生这种更新。作为更新过程的一部分，关于路由选择知识的动态变化在路由器之间相互交换。

静态路由选择有一些有用的应用。它允许网络管理员指定关于网络中受限制部分的广播内容。出于安全原因，管理员可以隐藏网络的一部分。而动态路由选择趋向于揭露一切。

另外，当某个网络只能通过一条路径访问时，有一条到这个网络的静态路由就足够了。这种类型的区域叫**存根网络**（stub network）。配置到存根网络的静态路由选择能避免动态路由选择额外开销，因为关于它的路由选择更新不用发送了。

3 缺省路由实例

缺省路由可以是网络管理员的静态配置的结果。图1-16显示了***缺省路由***（default route）的一种用法——缺省路由是一个路由选择表的条目，它用于对下一跳没有直接列在路由选择表中的分组进行定向。在这个例子中，X公司路由器拥有对公司X网络的知识，但是并不拥有对其他网络的知识。

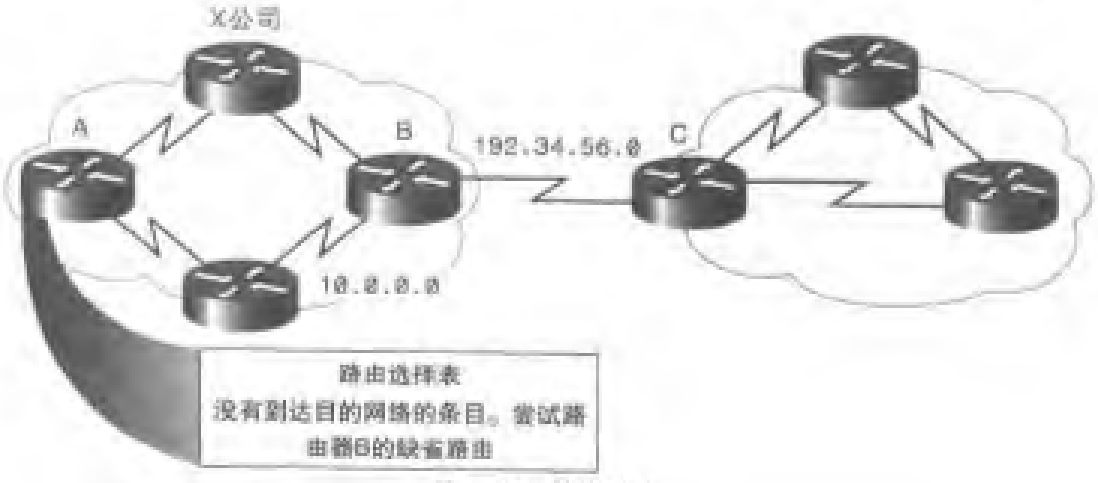


图1-16 缺省路由

即便是可能的，通过Internet网云来维护关于所有可访问网络的知识也是不必要和不合理的。

X公司并不维护关于制定网络的知识，而是通过缺省路由来获知它能通过将分组传送到Internet来到达任何未知的目的地。

1.4.7　被动路由协议与路由选择协议的对比

被动路由协议（routed protocol）与**路由选择协议**（routing protocol）这两个相似的术语在理解上经常出现混乱：

被动路由协议（Routed protocol）——任何在其网络层地址中提供信息，使得分组能基于寻址方案从一台主机转发到另一台主机。被动路由协议定义了分组内各个字段的格式和用途。分组通常从一个端系统传送到另一个端系统。IP是被动路由协议的一个例子。

路由选择协议（Routing protocol）——通过提供共享路由选择信息的机制来支持被动路由协议的协议。路由选择协议的消息在路由器之间传递。路由选择协议允许通过路由器间的通信来更新和维护路由选择表。TCP/IP中路由选择协议的例子有：**路由选择信息协议**（RIP）、**内部网关路由选择协议**（IGRP）、**增强内部网关路由选择协议**（Enhanced IGRP）以及**开放最短路径优先**（OSPF）协议。

1　路由选择协议

动态路由选择的成功基于两个基本的路由器功能：

- 维护路由选择表。
- 以路由选择更新的形式及时发布知识给其他路由器。

动态路由选择依靠路由选择协议来共享知识。路由选择协议定义了一套规则，路由器用它来与相邻路由器通信。例如，一种路由选择协议描述了：

- 更新如何被发送。
- 更新中包含了哪些内容。
- 何时发送更新。
- 如何定位更新的接收者。

外部路由选择协议用于自治系统（autonomous system）间的通信。自治系统是在共同管理下并共享一个公共路由选择策略的网络的集合。内部路由选择协议在单个自治系统内部使用。

2　IP路由选择协议

在OSI参考模型的网络层（第3层），路由器能使用IP路由选择协议把数据传送到正确的地点，通过执行下列的某种特定的协议来实现。IP路由选择协议的例子包括：

- RIP——一种距离矢量路由选择协议。
- IGRP——Cisco的距离矢量路由选择协议。
- OSPF——一种链路状态路由选择协议。
- EIGRP——一种平衡混合型路由选择协议。

3　路由选择协议分类

大多数内部路由选择协议归为3个基本类型之一：距离矢量（distance vector）、链路状态（Link state）或平衡混合型（balanced-vector）。**距离矢量路由选择协议**（distance-vector routing protocol）决定了到网络上任一链路的距离和方向（矢量）。**链路状态路由选择协议**（link-state routing

protocol），也叫**最短路径优先**（shortest path first [SPF] protocol）协议）会重建整个网络的实际拓扑结构（或至少是路由器所在部分的网络）。**平衡混合型协议**（balanced-hybird protocol）综合了链路状态协议和距离矢量协议的特点。

4 收敛

路由选择协议用于决定流量从特定源到特定目的地的最佳路由，是动态路由选择的基础。由于网络扩展、重新配置或网络故障造成网络拓扑变化时，关于网络的知识也必须随之改变。关于网络的知识必须是关于新拓扑的精确的、一致的视图。这种精确的、一致的视图被称为收敛（convergence）。

当网络中的所有路由器都使用相同网络知识来运行时，那么这个网络可以说是收敛的。快速收敛是所希望的网络特征，因为它节省那些因为路由器使用过时的网络知识来做出那些可能是不正确的、无用的或两者兼有的路由选择决定的时间。

5 距离矢量路由选择协议

路由器之间定期的更新用于交流拓扑的变化。路由选择协议通过定期地从一台路由器到另一台路由器传送路由选择表的拷贝来实现。例如，在图1-17中，每台路由器都从它的直接邻居那里收到一个路由选择表。路由器B从路由器A那里收到消息，然后路由器B增加一个距离矢量数（比如跳数）来加大这个距离矢量，并把这个路由选择表传给它的其他邻居，路由器C。这种逐步过程发生在所有方向上、所有直接相邻的路由器之间。

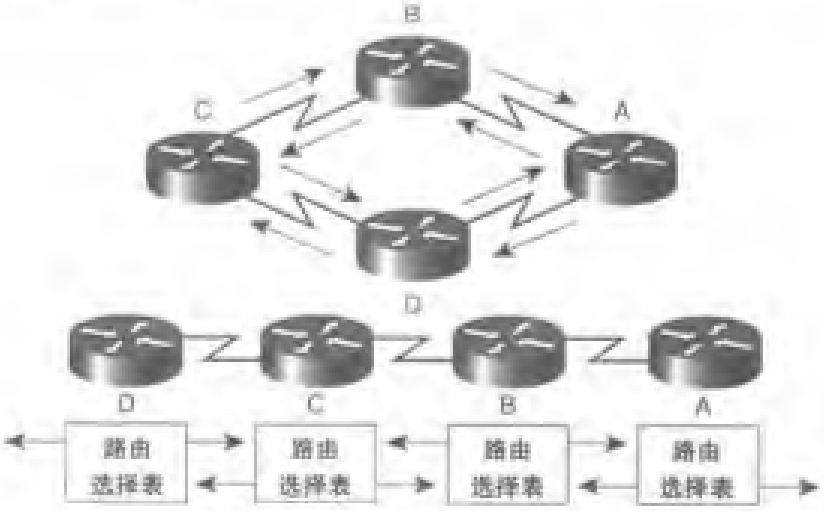


图1-17 距离矢量路由选择协议

通过这种方式，协议收集了到各个网络的距离，使它能维护一个关于网络拓扑信息的数据库。但距离矢量协议无法让路由器了解网络的精确拓扑结构。

6 链路状态路由选择协议

路由选择使用的第2种基本协议是链路状态协议。链路状态路由选择协议维护一个复杂的拓扑信息数据库。距离矢量协议没有关于远端网络的特定信息并且不了解远端路由器，但是链路状态路由选择协议保存了远端路由器的全部知识，以及自己与远端路由器之间是如何相互连接的。

链路状态路由选择协议使用了**链路状态通告**（link-state advertisements，LSA）、拓扑数据库、SPF协议，所产生的SPF树以及关于路径和到每个网络的端口的路由选择表。工程师们已经在OSPF路由选择协议中实现了链路状态的概念。

7　距离矢量路由选择协议和链路状态路由选择协议对比

可以从几个关键方面对距离矢量路由选择协议与链路状态路由选择协议进行比较：

• 距离矢量路由选择协议从邻居的路由选择表信息获得所有拓扑数据。链路状态路由选择协议通过积累所有相邻和远程路由器的LSA来获得网络拓扑的完整视图。

• 距离矢量路由选择协议是根据当路由选择表从一台路由器移到另一台路由器时增加它收到的度量值来决定最佳路径的。对于链路状态路由选择协议，每台路由器单独计算自己到目的地的最短路径。

• 对于大多数距离矢量路由选择协议，拓扑改变的更新来自路由选择表的定期更新。这些表通过一台路由器传给另一台路由器，这样经常会导致较慢的收敛。对于链路状态路由选择协议，更新通常是由拓扑改变而引发的。如果传给所有其他路由器的LSA相对较少，通常会导致任意网络拓扑改变时，收敛速度较快。

1.4.8　关于IP路由选择的配置任务

选择IP作为路由选择协议牵涉到对全局参数的设置。全局参数包括选择一种路由选择协议（例如RIP或IGRP），分配IP网络号但不指定子网值。

1　IP地址配置

使用 ip address 命令来建立接口的逻辑网络地址。使用 term ip netmask-format 命令指定当前会话的网络掩码格式。格式选项有位数、点分十进制（缺省）和十六进制数。

2　动态路由选择配置

动态路由选择发生在路由器互相发送定期路由选择更新消息时。这些包含新信息的消息一旦被接收，路由器就重新计算新的最佳路径并向其他路由器发送更新消息。

表1-1是启动路由选择进程的命令。

表1-1　Router和Network命令

命令	描述
router *protocol*	定义一种IP路由选择协议，可以是RIP、IGRP、OSPF或EIGRP
network	network子命令是为每个路由选择进程的强制配置命令

表1-2中的network命令是需要的，因为它使路由选择进程决定哪个接口将参与发送和接收路由选择更新：

表1-2　Network 命令

Network命令	描述
network *network number*	指定一个直接相连的网络

3　RIP

RIP的主要特性包括：

• 它是一种距离矢量路由选择协议。

• 使用跳数作为路径选择的度量值。

• 允许最大跳数是15。

• 路由选择更新缺省是每30秒广播一次。

路由器通过路由选择更新学习网络拓扑。命令router rip选择RIP作为路由选择协议。命令

network分配一个直接与路由器相连的基于IP的网络地址范围。路由选择进程把接口与合适的地址联系起来，并在特定的网络上开始处理分组，如图1-18所示：

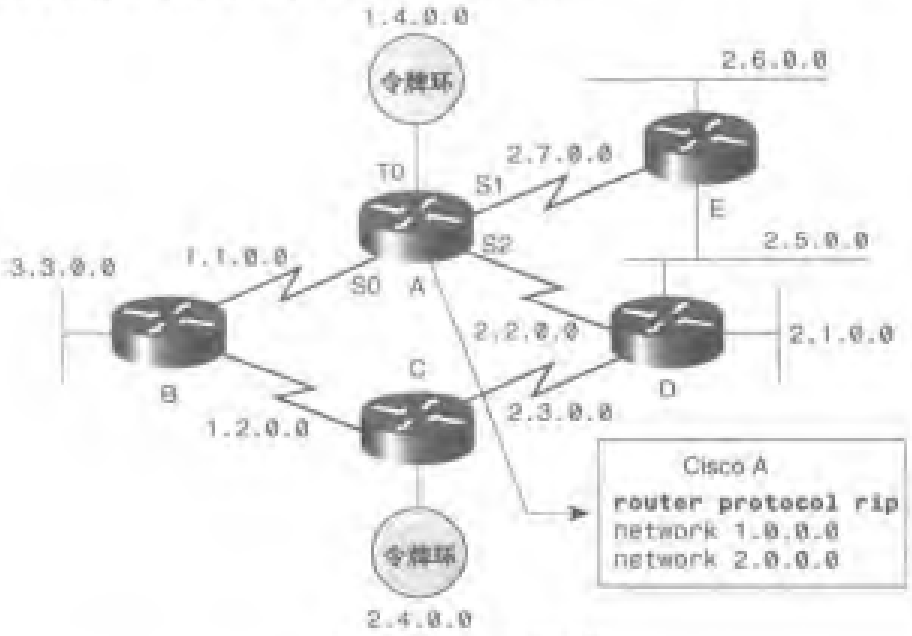


图1-18 路由选择更新

- router rip——选择RIP作为路由选择协议。
- network 1.0.0.0——指定一个直连的网络。
- network 2.0.0.0——指定一个直连的网络。

Cisco路由器A连接到网络1.0.0.0和2.0.0.0的接口将发送和接收RIP更新。

1.5 传输层

传输层在发送数据时，它能确保数据的完整性。实现它的一种方法是**流量控制**（flow control）。流量控制避免了源主机使目的主机缓冲区溢出。溢出会带来严重的问题，因为它们会导致数据丢失。

传输层服务也允许根据用户的要求在主机和目的地之间进行可靠数据传输。为了获得数据的可靠传输，在两端之间的通信系统建立面向连接的关系。可靠传输能完成：

- 对上层应用进行分段。
- 建立连接。
- 传输数据。
- 用窗口操作提供可靠性。
- 使用确认技术。

1.5.1 对上层应用进行分段

使用分层网络模型的一个原因是若干个应用能共享同一传输连接。传输功能一段接一段地完成。这意味着不同的应用能以先来先服务的原则发送数据段。这些分段可能发送到同一目的地或许多不同的目的地。

1.5.2 建立连接

为了建立连接，一台机器发起的呼叫必须被另一台机器接收。两台机器操作系统中的协议软

件模块通过在网络上发消息来验证传输是否被授权和双方是否准备就绪。在所有同步结束后，连接就建立了，数据传输开始。在传输过程中，两机器继续用它们的协议软件通信来验证数据是否正确接收。

数据传送开始，发送和接收应用程序必须通知各自的操作系统：连接将要被初始化。图1-19描述了在发送和接收系统之间的一个典型连接。当你碰到某人时，往往握住他的手表示欢迎。握手这个动作都被双方理解为友好欢迎的信号。我们也可以用同样的方式说明网络上的连接。第1步握手，或欢迎要求同步。第2和第3步握手确认初始的同步请求并确定对方的同步连接参数。最后一个握手用来通知目的地，确认双方都同意连接已经建立。在连接建立后便开始数据传输。

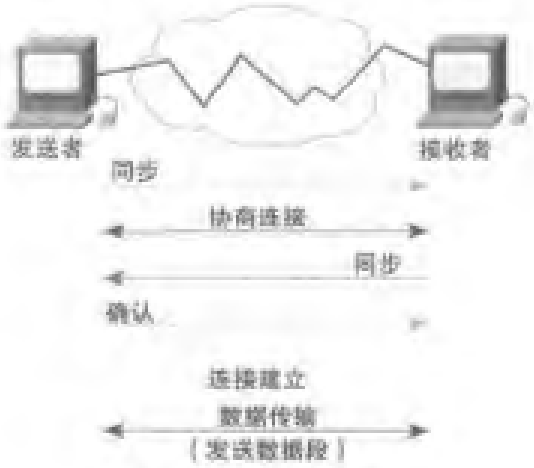


图1-19　网络连接

1.5.3　数据传输

当进行数据传输时，有两种原因都会造成拥塞。首先，高速的计算机可能产生远远超过网络传输能力的流量。其次，如果许多计算机同时需要向一个目的地发送数据报，目的地会发生拥塞，尽管不是因为任一个源导致了这一问题。

当数据报来得太快以致主机或网关不能处理时，它们会暂时存放在存储器里。传输功能会产生一个"未准备好"的信息给发送者，而不让数据丢失。如果流量继续发生，主机或网关会最终耗尽存储器，并且必须丢弃继续到来的数据报。如图1-20所示，一个指示器像一个交通信号灯，通知发送者停止发送数据。当接收器能处理其他的数据时，接收器发送一个"准备好"的传输指示，这有点像"走"信号。当发送器收到这个指示时，发送者会恢复段的传输。



图1-20　数据传输

1.5.4　用窗口操作实现可靠性

在多数面向连接的可靠数据传输基本形式中，数据分组必须按发送的顺序传递到接收方。如果数据分组丢失、破坏、重复或接收顺序出错，则协议失败。基本的解决方法是每收到一个数据段就发送一个收到的确认。

如果发送者发送每个段后必须等待确认，那么传输会变得很慢。由于发送者在完成传输数据分组后到完成处理接收到的确认数据分组之前还有一段时间，可以在这段时间内传输更多的数据。发送者允许传送的未确认的（还没有收到确认的）数据分组个数叫窗口（window）。

窗口操作是控制端到端传输的信息量的一种方法。某些协议是根据分组数来测量；TCP/IP根据字节数来测量。

1.5.5　确认技术

可靠传输保证从一台机器发出的数据流会通过数据链路发送到另一台机器，而不发生重复或数据

丢失。带重传的肯定确认（Positive acknowleigement with retransmission）是一种保证数据流可靠传输的技术。肯定确认要求发送一个收条给发送端，即收到数据后发回一个确认消息。发送方保留了它关于发送的每个数据分组的记录，并在发送下一个数据分组之前等待确认。发送端在发送一个数据段后会启动一个定时器，而且在确认到达之前如果定时器超时，它会重发这个数据段。

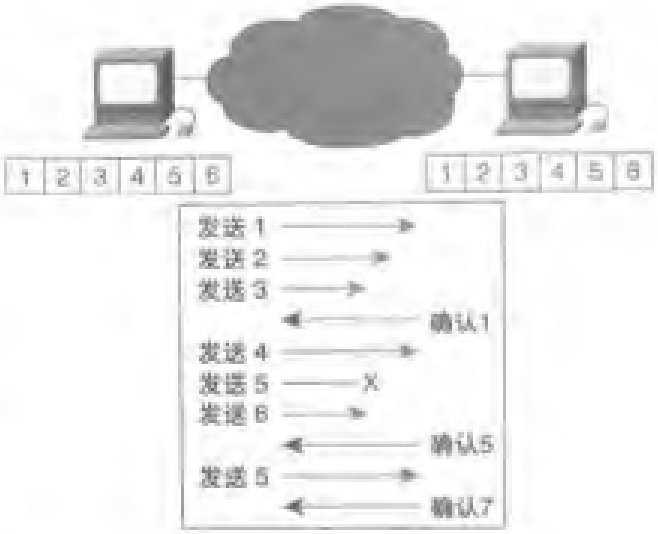


图1-21 确认技术

肯定确认要求接收端与源发送端方进行接收确认，当接收到数据时向源发送端发回确认消息。

图1-21显示了发送端发送数据分组1、2和3。接收端通过要求发送分组4来确认这些分组。一旦收到这确认分组后，发送端发送分组4、5和6。如果分组5没到达目的地，接收端用重新发送分组5的请求来进行确认。发送端重新发送分组5，并且必须收到一个确认再继续发送分组7。

1.6 总结

- 通过分层，OSI参考模型简化了两台计算机进行通信所需的任务。
- 每层协议都与对等层交换信息，交换的信息叫PDU。
- OSI参考模型的每一层依靠它的下一层提供服务功能。下层通过封装把从高层来的PDU放入它的数据域，然后，这一层可以增加任意的头和尾来实现它的功能。
- 术语“以太网”经常用来指遵循以太网标准（包括IEEE 802.3）的所有CSMA/CD局域网。
- 以太网和802.3数据链路提供跨越连接两台设备物理链路的数据传输。
- IP协议为数据报提供无连接的、尽力的传输路由选择。它不关心数据报的内容，而是寻找一条把数据报移动到目的地的路径。
- ICMP消息通过IP数据报传送，用来发送错误和控制消息。
- ARP用来把IP地址映射到MAC地址，例如以太网，这使得信息可以在多种介质中传输。
- 交换功能让路由器能从一个接口上接收分组，然后从另一个接口上转发出去。
- 被动路由协议是网络层协议，它依据网络层地址提供的足够信息让分组能基于寻址方案从一台主机能发到另一台主机。
- 路由选择协议通过共享路由选择信息的机制来支持被动路由协议。路由选择协议消息在路由器之间传递。
- 大多数路由选择协议都属于两种基本协议的一种：距离向量路由选择协议和链路状态路由选择协议。
- 路由器必须能够原封不动地把分组封装进不同的下层，而不改变分组的第3层地址。
- IP路由选择协议例子包括RIP、IGRP、OSPF和EIGRP。
- 传输层服务可以根据用户的要求在主机和目的地之间进行可靠数据传输。

请参考本书光盘上与本章相关的视频、插图和e-Lab实验活动，这些内容主要用作本章学习内容的补充。

1.7 关键术语

应用层（*applicationg layer*） OSI参考模型的第7层。这一层向用户应用程序提供网络服务。例如，这一层的文件传输服务向某个文字处理应用程序提供服务。

地址解析协议（*Address Resolution Protocol，ARP*） 它是把IP地址映射到MAC地址的IP协议。定义在RFC 826中。

附接单元接口（*attachment unit interface，AUI*） 它是介质连接单元与网络接口卡之间的IEEE 802.3接口。AUI这一名词也可以指AUI电缆所连接的背后的后背板端口，例如在Cisco LightStream 以太网访问卡上就有这种情况，AUI也叫做收发器电缆。

平衡混合型协议（*balanced-hybrid protocol*） 它综合了链路状态和距离矢量协议的特点。

尽力传送（*best-effort delivery*） 描述的是网络系统没有复杂的确认系统以保证信息可靠传送时的传送方式。

Cisco互连网络操作系统软件（Internetwork Operating System Software，Cisco IOS软件） Cisco系统软件为在CiscoFusion结构下的所有产品提供了常用的功能、可扩展性和安全性。Cisco IOS软件在确保支持种类繁多的协议、介质、业务和平台的同时，允许集中化、整体化和自动化地安装以及对互连网的管理。

收敛（*convergence*） 一组网络互连设备运行特定路由选择协议的速度和能力，在网络拓扑改变以后能与网络互连拓扑保持一致。

数据链路层（*data link layer*） 它指的是OSI参考模型的第2层。该层提供了通过物理链路提供可靠的数据传输。数据链路层考虑物理寻址、网络拓扑、线路要求、错误通知、帧的顺序传输和流量控制。IEEE已经把数据链路层分成了两个子层：MAC子层和LLC子层。数据链路层有时只简称作链路层。本层大致对应SNA模型的数据链路控制层。

数据报（*datagram*） 它指在没有事先建立一条虚电路的情况下，在传输介质上作为网络层单元发送的信息的逻辑分组。IP数据报是互连网上的主要信息单元。术语帧、数据报、分组和数据段用于描述在OSI参考模型的各层及各种技术环境中的逻辑信息分组。

缺省路由（*default route*） 指的是路由选择表中未直接列出的路由选择项，它用于指示数据帧下一跳的方向。

距离矢量路由选择协议（*distance-vector routing protocol*） 是一种路由选择协议，它遍历一条路由的所有跳数来寻找一棵最短路径生成树。距离矢量路由选择算法需要每台路由器在更新路由选择表后只向它的邻接路由器发送出整个更新路由选择表。距离矢量路由选择算法虽然易于形成环路路由，但是它比链路状态路由选择协议计算起来简单。它也被叫做Bellman-Ford路由选择算法。

动态路由选择（*dynamic routing*） 它指的是能够自动适应网络拓扑或者通信变化的路由选择。它也称作自适应路由选择（adaptive routing）。

增强型内部网关路由选择协议（*Enhanced Interior Gateway Routing Protocol，EIGRP*） Cisco开发的一个更先进版本的IGRP。能提供更好的收敛特性和操作效率，结合了链路状态协议和距离矢量协议的优点。

流量控制（*flow control*） 它是一种保证发送设备不会用数据淹没接收设备的技术。当接收设备中的

缓冲区充满时，就发送一个消息给发送设备暂停传送，直到缓冲区内的数据被处理掉。在IBM网络中，这项技术被称为步调控制（pacing）。

报头（*header*） 网络上传输的数据在封装时放在数据前的控制信息。

跳（*hop*） 指分组在两个网络节点（例如两台路由器）之间通过。

因特网控制信息协议（*Internet Control Message Protocol，ICMP*） 网络层的因特网协议，它报告错误并且提供IP分组处理过程中的其他相关信息。在RFC 792中定义。

内部网关路由选择协议（*Interior Gateway Routing Protocol，IGRP*） 是由Cisco公司开发的一种协议，在大型、异构网络中用于解决有关路由选择的问题。

IP地址（*IP address*） 分配给使用TCP/IP协议的主机的32位地址。IP地址分为5类（A、B、C、D或E），写成圆点分隔的4个8进制数。（即点分隔的十进制数）。每个地址包括网络地址、可选的子网地址和主机地址。网络地址和子网地址一起用于路由选择，主机地址用于标识网络或子网中独立的主机。子网掩码用于从IP地址中提取网络和子网信息。也称为Internet地址。

分层（*Layering*） OSI参考模型所使用的网络功能的划分方法。它简化了两台互相通信的计算机所需要完成的任务。

链路状态路由选择协议（*link-state routing protocol*） 在这种路由选择协议中，每台路由器通过广播或者组播的方式通告它的邻居路由器到达互连网络中所有节点的代价。链路状态路由选择协议创建了整个网络的一致视图，不易产生路由选择环路，但这些都是通过更大的计算难度和更广泛的通信来实现的（相对于距离矢量路由选择协议）。

链路状态通告（*link-state advertisement，LSA*） 链路状态路由选择协议使用的一种广播分组，它包含关于邻居路由器和路径开销的信息。接收方路由器通过LSA来维护路由选择表。有时LSA也被称为链路状态分组（LSP，Link-state packets）。

介质访问控制（*Media Access Control，MAC*） 数据链路层的一部分，包含6字节（48位）的源地址和目的地址，以及获得传输许可的方法。

介质连接单元（*media attachment unit*） 一种用于以太网和IEEE 802.3网络的设备。提供工作站的AUI端口和以太网的常用介质之间的接口。介质连接单元既可以集成在工作站里面，也可以作为一个独立的设备，它所实现物理层的功能包括，转换以太网接口的数据、冲突检测和发送数据到网络中。有时也被称为介质访问单元（Media access unit）或收发器（tranceiver）。

网络（*network*） 计算机、打印机、路由器、交换机以及其他能通过某种传输介质相互通信的设备集合。

网络层（*network layer*） OSI模型的第3层。这一层提供两个终端系统之间的连接和路径选择，网络层是发生路由选择的层。大致相当于SNA模型的路径控制层。

网络接口卡（*network interface card，NIC*） 为计算机系统提供网络通信能力的电路板。NIC包含有一个制作商分配的MAC地址，这个地址用作计算机在局域网中的物理地址。

开放最短路径优先协议（*Open Shortest Path First protocol，OSPF协议*） 一种链路状态、分层路由选择协议，在因特网团体中被推荐作为RIP协议的替代者。OSPF特性包括最低开销路由选择、多路径路由选择和负载均衡。

分组（*packet*） 一系列由控制信息头部和用户数据（通常）组成的信息组合，常用于表示网络层的数据单元。面本语数据报、帧、消息、段等用于描述OSI模型的各层及各个技术中的逻辑信息分组。

路径选择（*path determination*）　数据通信通过网络云时选择走哪一条路径。路径选择在OSI模型中的网络层完成。

协议数据单元（*protocol data unit*，*PDU*）　关于“分组”的OSI术语。

物理层（*physical layer*）　OSI参考模型的第1层。物理层定义了端系统之间物理链路的使用、维护和关闭的电气、机械、规程及功能的规范。与SNA模型的物理控制层相当。

表示层（*presentation layer*）　OSI参考模型的第6层。这一层提供数据的表示方法、编码的格式化以及数据传输语法的协商。它确保应用程序能够使用从网络中接收到的数据并且使应用程序发送的信息能在网络中传输。

队列（*queue*）　1. 通常指等待处理的一组有序的元素列表。2. 在路由器端口等待路由器接口转发的一队分组。

反向地址解析协议（*Reverse Address Resolution Protocol*，*RARP*）　TCP/IP协议栈中的协议，提供一种通过MAC地址来查找IP地址的方法。

路由选择信息协议（*Routing Information Protocol*，*RIP*）　UNIX BSD系统提供的协议。这是因特网上最为普遍的内部网关协议（IGP）。RIP使用跳数作为路由选择度量值。

被动路由协议（*routed protocol*）　路由器用来实现路由的协议。路由器必须能够解释该被路由协议说明的逻辑网络互连。被路由协议的一些例子包括AppleTalk、DECnet和IP。

路由选择协议（*routing protocol*）　通过执行某种指定的路径选择方法来完成路由选择的协议。路由选择协议的一些实例包括IGRP、OSPF和RIP。

会话层（*session layer*）　OSI参考模型的第5层。这一层负责建立、维护和管理应用程序之间的会话。

最短路径优先协议SPF（*shortest path first*，SPF）protocol　迭代路径的长度，以确定最短路径生成树的路由选择算法。通常在链路状态路由选择协议中使用。亦称作Dijkstra算法。

静态路由选择（*static routing*）　静态路由选择通过手工配置并输入到路由选择表中，通常比动态路由选择协议选择的路径有更高的优先级。

存根网络（*stub network*）　与路由器只有单一连接的网络。

子网掩码（*subnet mask*）　用于从IP地址中抽取网络和子网信息的掩码。

子网（*subnetwork*）　将一个网络分割成一系列更小的网络。

传输层（*transport layer*）　OSI参考模型的第4层。这一层将数据分割并重组成数据流。传输层具有保证连接和提供可靠传输的特性。

窗口（*window*）　接收方能接收的字节数目。

1.8 复习题

1. OSI模型的哪一层最恰当地描述了10BaseT标准？
   A. 数据链路层
   B. 网络层
   C. 物理层
   D. 传输层
2. 下列哪一项最恰当地描述了OSI模型中传输层的功能？
   A. 它通过流量控制来发送数据
   B. 它提供传输的最佳路径
   C. 它决定网络寻址
   D. 它允许网络分段
3. 下列哪一个功能是路由器用来在网络中转发数据分组的？
   A. 应用程序和介质
   B. 路径选择和交换
   C. 广播和冲突检测
   D. 上述答案都不对
4. 下列哪两项是动态路由选择的基本类型？
   A. 静态及缺省
   B. TCP和UDP交换
   C. 距离矢量和链路状态
   D. 上述答案都不对
5. 当网络中的所有路由器都使用着相同的知识时，下列哪一项可以用来描述这个网络？
   A. 收敛
   B. 形式化
   C. 重新配置
   D. 上述答案都不对
6. 描述数据封装的用途。
7. 描述OSI模型中传输层的主要功能。
8. 描述ICMP的用途。
9. 描述TCP/IP实现中的窗口操作。
10. 描述OSI模型中网络层的主要功能。
11. 哪一条命令用来为一个网络配置RIP路由选择进程？
    A. router rip **area** *area-id*
    B. router rip **network** *network-number*
    C. router rip **neighbour** *ip-address*
    D. router rip **neighbour** *summary*
12. 下列哪一项最恰当地描述了TCP/IP协议栈？
    A. 在上层中与OSI参考模型紧密映射
    B. 支持所有的物理标准和数据链路协议
    C. 有序传输数据报信息
    D. 在接收位置将数据报汇集成完整的消息
13. 哪一项最恰当地描述了经过封装的数据分组的结构？

A. 段头部，网络头部，数据，帧尾部
B. 段头部，网络头部，数据，段尾部
C. 帧头部，网络头部，数据，帧尾部
D. 帧头部，段头部，数据，段尾部

14. 哪一项技术使用了窗口操作来保证一台电脑发送的数据流通过数据链路发送到另外一台电脑时不出现数据重复和丢失？
A. 确认和重传
B. 封装和广播
C. 校验和流控
D. 同步和确认

15. 动态路由选择的一个优点是什么？
A. 网络开销小，可以减少网络流量
B. 由于安全级别高，可以减少未经授权的网络信息中断
C. 当拓扑结构和流量发生改变时可以自动调整
D. 网络带宽需求小，运算更有效

16. 下列哪些项最恰当地描述了传输层的主要功能？
A. 使用TCP协议对数据流进行分段或重组
B. 建立、维持、管理应用程序间的会话
C. 为用户程序提供网络服务
D. 利用MAC地址提供通过传输介质的物理传输，处理错误通告、网络拓扑结构和流量控制

17. 在RIP路由选择协议中，发送路由选择更新的频率是多少？
A. 每30秒
B. 每60秒
C. 每90秒
D. 只当管理员向路由器发出请求时

18. 下列哪一项是正确的？
A. MAC寻址是一种层次化寻址系统，它分配惟一的MAC地址
B. 网桥使用IP地址使数据能够通过网络传播
C. MAC地址应用在数据链路层，并在硬件上编码写进网络接口卡
D. 当设备从一个网络移到另外一个网络中时，它的MAC地址将发生改变

19. 网络分层模型的好处是什么？
A. 简化网络
B. 为了标准化
C. 把互连网络的复杂性划分为独立的、更易理解的操作子集
D. 以上答案均正确

20. 路由器为分组进行路径选择执行了下列哪一种功能？
A. 简单的将另外一个头部加入到分组帧中，最后解析目标机器的IP地址
B. 参照路由选择表，决定使用哪一个端口来发送数据到目的网络
C. 向除了数据到达以外的所有端口广播数据帧
D. 执行以上所有功能

第二部分　CCNA 3：交换基础与中级路由选择

第2章　无类别路由选择介绍
第3章　单区域OSPF
第4章　增强内部网关路由选择协议
第5章　交换的概念与局域网技术
第6章　交换机
第7章　交换机配置
第8章　生成树协议
第9章　虚拟局域网
第10章　VLAN中继协议

第二部分　CCNA 3：交换基础与中级路由选择

第2章　无类别路由选择介绍
第3章　单区域OSPF
第4章　增强内部网关路由选择协议
第5章　交换的概念与局域网技术
第6章　交换机
第7章　交换机配置
第8章　生成树协议
第9章　虚拟局域网
第10章　VLAN中继协议



第2章　无类别路由选择介绍

目标

学习完本章之后，你将能够：

- 描述无类别域间路由选择（CIDR）的特性。
- 利用可变长度子网掩码（VLSM）计算子网。
- 描述利用VLSM进行路由汇总。
- 描述路由选择信息协议第二版（RIPv2）的特性。
- 配置RIPv2。
- 验证RIPv2和对其进行故障排除。

本章将介绍无类别路由选择、无类别域间路由选择、可变长度子网掩码，RIP第1版和第2版。

请注意应配合本书附带光盘上的e-Lab实验、视频和插图一起阅读本章内容，光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

2.1　CIDR概述

随着IP网络爆炸性地发展，更重要的是全球Internet的飞速发展，可用的IP地址空间正在缩小，核心的Internet路由器处理能力也逐渐耗尽。CIDR（发音“cider”）就是为了解决这些问题而设计的。

CIDR使用普遍的网络前缀来取代旧的基于A、B、C类地址的IP地址分配过程。与之前的8位、16位或24位网络标识符（或前缀）限制相反，CIDR可以使用长度从13位到27位的前缀。这样，地址块可以分配给小如32台主机或大如500,000台主机的网络使用。这种地址分配方法更加贴近一个机构的特定使用需求。

在CIDR中，IP地址表示方法有些改变。一个CIDR地址包括标准的32位长的IP地址和表示网络前缀长度的信息。例如，在CIDR地址206.13.01.48/25中，“/25”表示前25位用来标识一个惟一的网络，而剩下的位则用来标识特定的主机。206.13.01.48/25也可以写成206.13.01.48 255.255.255.128。

2.1.1　为什么需要CIDR

路由器使用一种忽略类别的IPv4寻址方式，称为无类别域间路由选择（Classless interdomain

routing, CIDR）。在一个有类别的系统中，路由器决定一个地址的类别，并根据该类别识别网络和主机。而在CIDR中，路由器使用前缀来描述有多少位是网络位（地址的开始几个位，或称前缀），剩下的位则是主机位。表示前缀的数字跟在地址的结尾，用斜杠（/）来表示，例如，10.10.10.10/30，这里“/30”是前缀。一个地址的网络和主机部分不再受完整8位组的限制。

CIDR最初在1993年的RFC1 517、1518、1519和1520中提出，并在不久后的1994年开始使用。通过提供以下的特性，CIDR显著提高了IPv4的可扩展性和效率：

- 将有类别的寻址方式替换成了更灵活、浪费更少的无类别方案。
- 加强了路由聚合，亦即超网（Supernetting）。

下面的章节将更详尽地描述路由聚合、超网和地址分配。

2.2　路由聚合与超网

通过使用比特掩码而不是使用地址类来决定一个地址的网络部分，CIDR允许路由聚合（aggregation）或汇总（summarize）路由选择信息。这样可以缩小路由器路由选择表的大小。换句话说，就是只用一个地址和掩码的组合来表示多个网络的路由。

如果没有CIDR和路由聚合（route aggregation），路由器必须每表2-1所示的每个B类网络维护一个表项。

表2-1中阴影覆盖的列标识了16个比特，表示基于有类别规则的网络号。有类别路由器必须使用这16个比特来处理B类网络。因为这8个网络号的前16比特是**惟一的**，所以有类别路由器可以识别8个不同的网络并为每个网络创建一条路由选择表项。

表2-1　16比特长的路由聚合和超网

网络号	第1个8位组	第2个8位组	第3个8位组	第4个8位组
172.24.0.0/16	10101100	00011000	00000000	00000000
172.25.0.0/16	10101100	00011001	00000000	00000000
172.26.0.0/16	10101100	00011010	00000000	00000000
172.27.0.0/16	10101100	00011011	00000000	00000000
172.28.0.0/16	10101100	00011100	00000000	00000000
172.29.0.0/16	10101100	00011101	00000000	00000000
172.30.0.0/16	10101100	00011110	00000000	00000000
172.31.0.0/16	10101100	00011111	00000000	00000000

然而，表2-2中阴影覆盖部分所示的8个具有公共的比特。如果表2-1中**粗体**所示的最后的公共比特是由前缀定义的，那么路由器将定位到一个可以表示多个网络的公共网络号。这就是路由汇总（route summarization），可以节省路由选择表的空间。

表2-2所示为8个示例的网络地址前13个比特相同。

表2-2　13比特长的路由聚合和超网

网络号	第1个8位组	第2个8位组	第3个8位组	第4个8位组
172.24.0.0/16	10101100	00011000	00000000	00000000
172.25.0.0/16	10101100	00011001	00000000	00000000
172.26.0.0/16	10101100	00011010	00000000	00000000
172.27.0.0/16	10101100	00011011	00000000	00000000
172.28.0.0/16	10101100	00011100	00000000	00000000
172.29.0.0/16	10101100	00011101	00000000	00000000
172.30.0.0/16	10101100	00011110	00000000	00000000
172.31.0.0/16	10101100	00011111	00000000	00000000

支持CIDR的路由器可以使用一个长为13比特的前缀来汇总这些路由信息，供这8个网络（也仅

仅是这8个网络）共享：

10101100 00011

将该前缀用十进制表示，而地址的剩余部分用0来填补，并与13比特的子网掩码配对，得到：

10101100 00011000 00000000 00000000=172.24.0.0

11111111 11111000 00000000 00000000=255.248.0.0

这样，可以用一个地址和掩码定义一个无类别的前缀，从而将这8个网络汇总为：172.24.0.0/13。

通过使用前缀地址来汇总路由，可以保持路由选择表条目可管理，这是由于以下原因：

- 更高效的路由选择。
- 重新计算路由选择表或者在路由选择表中排序查找匹配所消耗的CPU时间大幅减少。
- 对路由器内存的需求降低。

超网（Supernetting）是指用一个比特掩码将多个有类别的网络聚合成单个网络地址的过程。超网和路由聚合是同一方法的不同名称，尽管在聚合的网络处于共同的管理控制下时最常用的是超网这个术语。

A类地址和B类地址空间实际上已经耗尽，这使得大型组织别无选择，只能从其服务提供商那里申请多个C类网络地址。如果一个公司可以获得一块连续的C类网络地址，超网可以使得这些地址看起来像是一个大网络或者超网。

2.2.1 超网与地址分配

假设XYZ公司需要供400台主机使用的地址。在有类别的寻址系统中，XYZ可能向因特网地址授权中心申请一个B类地址。如果该公司获得一个B类地址并将该地址用来作为由400台主机构成的逻辑组的地址，那么数以万计的地址都将浪费。XYZ公司的另外一个选择是申请2个C类地址，即508（2×254）个主机地址。这种方法的缺点是XYZ公司将不得不在自己内部的逻辑网络之间进行路由选择，并且缺省的因特网路由器将需要为XYZ公司的网络维护2条路由选择表项，而不是一条。

在一个无类别的寻址系统中，超网允许XYZ公司使用自身需要的地址空间而不造成地址浪费或增加不必要的路由选择表开销。通过使用CIDR，XYZ公司只需要向它的网络服务提供商（ISP）申请一个地址块，而不是向授权中心，例如InterNIC去申请。ISP评估XYZ公司的需求并从它的大CIDR地址块中分配一个地址空间给XYZ公司。提供商假设管理地址空间的任务是在一个无类别系统中进行。在这个系统中，因特网上的其他路由器只需要为该提供商的网络保留一个汇总路由或超网路由，而提供商自身为该网络保留的路由则要细致得多。这种办法彻底减少了因特网上路由选择表的大小。

在下面的例子里，XYZ公司获得2个相邻的C类地址，207.21.54.0和207.21.55.0。如果你仔细查看表2-3中的阴影部分，你会发现这些网络地址具有相同的23位前缀：

11001111 00010101 0011011

表2-3 超网和地址分配

网络号	第1个8位组	第2个8位组	第3个8位组	第4个8位组
207.21.54.0	11001111	00010101	00110110	00000000
207.21.55.0	11001111	00010101	00110111	00000000

当使用23位的掩码（207.21.54.0/23）形成超网后，该地址空间可以提供超过400个主机地址（2^9或512台主机）而不会产生采用一个B类地址所带来的巨大浪费。通过ISP扮演CIDR地址块寻址授权方的角色，该ISP客户的网络（包括XYZ公司）可以在各个Internet路由器上作为一个超网来传播。在图2-1中，ISP管理一个256个C类地址组成的地址块，并用16位的前缀207.21.0.0/16将它们传播到整个互连网上。

CIDR使ISP可以分级地分配和管理连续地址构成块，通过这种特性，IPv4地址空间将获得以下的好处：

- 有效的地址分配。
- 路由选择表条目的减少。

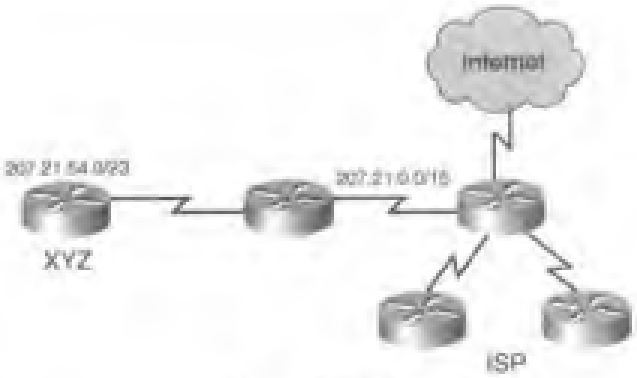


图2-1　CIDR寻址

2.3　可变长子网掩码

可变长子网掩码（VLSM，Variable-length subnet masks）是为了解决在一个网络中使用多种层次的子网化IP地址的问题而发展起来的。这种策略只能在所用的路由选择协议都支持的情况才能使用，例如开放式最短路径优先路由选择协议（OSPF）和增强内部网关路由选择协议（EIGRP）。RIP版本1由于出现早于VLSM而无法支持。而RIP版本2则可以支持VLSM。

VLSM允许一个组织在同一个网络地址空间中使用多个子网掩码。利用VLSM可以使管理员"把子网继续划分为子网"，使寻址效率达到最高。

2.3.1　VLSM的特征

当为一个IP网络分配不止一个子网掩码时，可以认为网络使用了可变长子网掩码，能克服单一子网掩码所造成的固定数目、固定大小子网的局限。本节内容描述了可变长子网掩码的特性。

在图2-2中，网络172.16.14.0/24被分成了几个更小的子网：

- 使用同一个掩码/27划分子网。
- 未使用的一个/27子网被更进一步划分成3个/30子网。

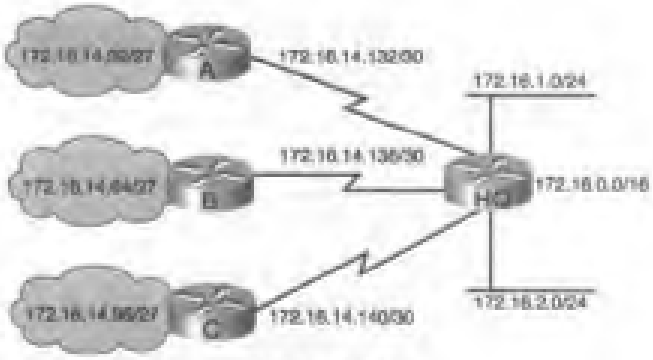


图2-2　VLSM

VLSM提供了在一个网络中包括多用子网掩码的能力，并且能对一个已存在的子网地址进一步划分。VLSM具备以下优点：

- **更有效地使用IP地址**——如果不使用VLSM，各公司就必须在整个A、B、C类网络中使用一个单一的子网掩码。

例如，在图2-2中，考虑将网络地址172.16.0.0/16用/24掩码分成子网，在这个范围里的一个网络172.16.14.0/24用掩码/27进一步分成更小的子网。这些更小的子网范围是从172.16.14.0/27到172.16.14.224/27。在图2-2中，将其中的子网172.16.14.128/27用掩码/30再分成只有2个主机地址的小子网，用于广域网链路。这些掩码为/30的小子网范围从172.16.14.128/30直到172.16.14.156/30。在图2-2中，广域网链路使用了该范围内的172.16.14.132/30，172.16.14.136/30和172.16.14.140/30这3个小子网。

- **使用路由汇总的能力更强**——VLSM允许地址规划中有更多的等级水平，也可以在路由选择表中使用汇总更有效地进行路由选择。例如，在图2-2中，子网172.16.14.0/24汇总了所有从172.16.14.0中进一步划分出来的地址，包括172.16.14.0/27到172.16.14.128/30。

考虑从C类地址207.21.24.0的主机部分借用3比特所创建的子网，如表2-4所示。

如果使用ip subnet-zero命令，该掩码将创建7个可用的子网，每个子网30台主机。可以将这些子网中的4个提供给机构的远程办公室使用。如图2-3，在地点A、B、C和D。

表2-4　同一个掩码划分出的子网

子网号	子网地址
子网1	207.21.24.0/27
子网2	207.21.24.32/27
子网3	207.21.24.64/27
子网4	207.21.24.96/27
子网5	207.21.24.128/27
子网5	207.21.24.160/27
子网6	207.21.24.192/27
子网7	207.21.24.224/27

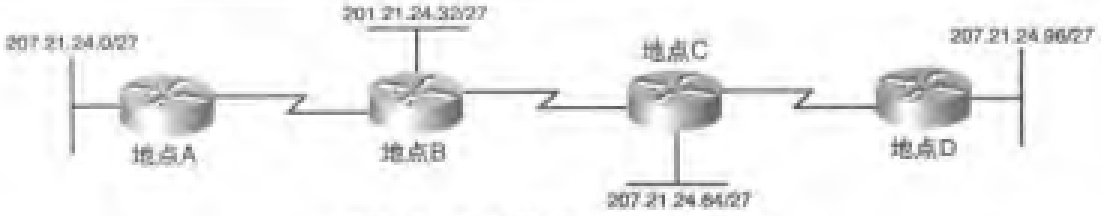


图2-3　使用子网向WAN提供地址

不幸的是，现在只剩下3个子网用于将来的扩展，并且还要给4个地点间的3条点到点广域网链路提供地址。如果分配剩下的3个子网给广域网链路，就完全耗尽了所有地址。此外，浪费能容纳30台主机的子网来为这些只有两个节点的网络提供地址，将浪费掉超过三分之一的可用地址。

你可能已经猜到，有办法可以避免这种浪费。在过去的20年中，网络工程师已经开发了3种策略来为点到点WAN链路高效地提供地址。

- 使用VLSM。
- 使用私有地址（RFC 1918）。
- 使用无编号IP（IP unnumbered）。

私有地址和无编号IP将在本章的“路由汇总”部分进一步讨论。这里先关注VLSM。如果用VLSM解决地址问题，那么C类地址可以分成大小不同的组（或子网）。大的子网用于局域网，很小的子网用于广域网链路和其他特殊情况。

用30比特的掩码来生成只有两个有效主机地址的子网，恰好是点到点连接所需要的地址数量。图2-4显示了如何通过将前缀扩展到30，从而把1个子网分成8个子网。你可以看到，如果使用3个剩余子网中的一个（子网6，或207.21.24.192/27），并且用30比特掩码再对其划分子网，将会发生什么情况。

Subnet 0	207.21.24.0/27
Subnet 1	207.21.24.32/27
Subnet 2	207.21.24.64/27
Subnet 3	207.21.24.96/27
Subnet 4	207.21.24.128/27
Subnet 5	207.21.24.160/27
Subnet 6	207.21.24.192/27
Subnet 7	207.21.24.224/27

Subnet 0	207.21.24.192/30
Subnet 1	207.21.24.196/30
Subnet 2	207.21.24.200/30
Subnet 3	207.21.24.204/30
Subnet 4	207.21.24.208/30
Subnet 5	207.21.24.212/30
Subnet 6	207.21.24.216/30
Subnet 7	207.21.24.220/30

图2-4　用VLSM继续划分子网

用这种方法进一步划分子网207.21.24.192/27，则可以提供8个用于点到点网络的地址范围。例如，网络207.21.24.192/30可以为地点A和地点B的路由器之间的点到点串行链路提供地址，如图2-5所示。207.21.24.193分配给地点A的WAN接口，而207.21.24.194分配给地点B的WAN接口。



图2-5　用VLSM为点到点连接提供地址

2.3.2　计算VLSM

正如前面所讨论的，利用VLSM，可以将一个已经划分了子网的地址再细分。设想一下，假如你有一个子网地址172.16.32.0/20，需要给一个有10台主机的网络分配地址。现在分配了20比特给网络地址，保留12比特给主机，可是你现在有超过4,000（2^{12}-2=4,094）个主机地址，大部分都将被浪费。利用VLSM可以对172.16.32.0/20进一步划分，得到更多的网络地址，并且每个网络的主机数减少。例如，划分172.16.32.0/20为172.16.32.0/26，得到64（2^6）个子网，每个子网可以支持62（2^6-2=62）台主机。参见图2-6。

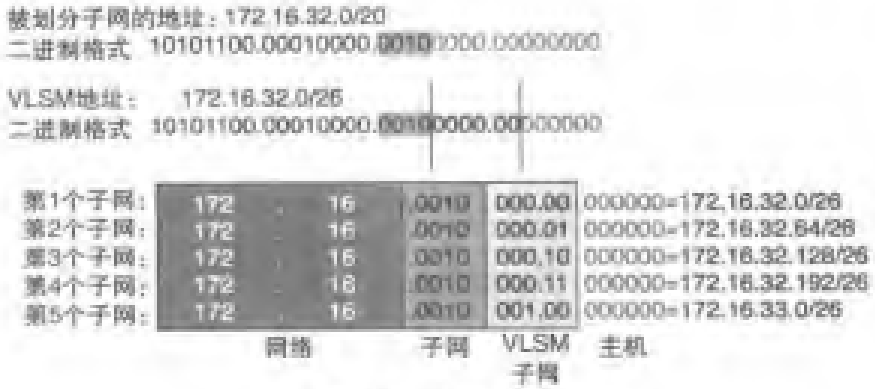


图2-6　计算VLSM

使用下面的步骤进一步划分172.16.32.0/20为172.16.32.0/26：

步骤1　把172.16.32.0写成二进制格式。

步骤2　在第20和第21个比特之间划一条垂直线，如图2-6所示（/20是最初的子网分界线）。

步骤3　在第26和第27个比特之间划一条垂直线，如图2-6所示（最初的/20子网分界线向右扩展了6比特，成为/26）。

步骤4　用两条分界线之间的比特，从低到高计算64个子网地址，图2-6显示了可用的前5个子网。

VLSM通常用于最大化一个网络的可用地址。例如，因为点到点的串行链路只要求两个主机地址，用a/30的子网不会浪费宝贵的IP地址。

在图2-7中，以太网段所使用地址是那些从172.16.32.0/20再细分为/26的子网。图2-7举例说明了子网地址应用在哪里取决于所要求的主机数量。例如，WAN的连接使用/30的掩码，这样的掩码只允许有两台主机，对于一对路由器之间的点到点连接刚好够用。

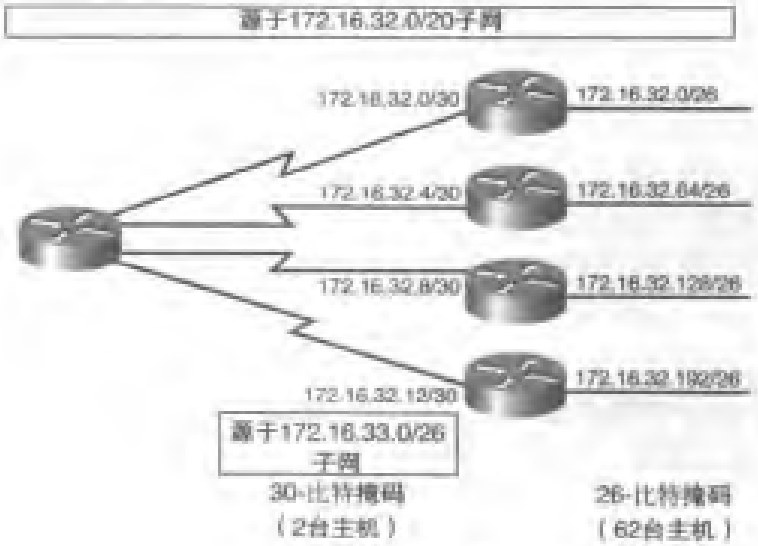


图2-7　VLSM例子

为了计算用于广域网的子网地址，进一步划分未使用的/26子网。在该例中，172.16.32.0/26被前缀/30再划分为多个子网。这就多了4个子网比特。因此，生成16（2^4）个用于广域网连接的子网。

切记只有未使用的子网才能进一步划分。换句话说，如果你已经使用了某个子网中的地址，那么这个子网不能再细划分。



实验活动 计算VLSM子网

在这个实验中，用VLSM更有效地利用给定IP地址和尽可能地减小顶层路由选择信息的数量。

2.3.3 配置VLSM

本节内容介绍如何在Cisco路由器上配置VLSM。例2-1显示了位于地点A的路由器（RTA）在以太网（e0）端口配置27比特掩码，而在串行（s0）端口配置30比特掩码所需的命令。

例2-1 配置VLSM

```
RTA(config)#interface e0
RTA(config-if)#ip add 207.21.24.33 255.255.255.224
RTA(config-if)#interface s0
RTA(config-if)#ip add 207.21.24.193 255.255.255.252

RTA#show 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
       E1-OSPF external type1, E2-OSPF external type 2, E-EGP
       i-IS-IS, L1-IS-IS level-1, L2-IS-IS level-2,
    *-candidate default

Gateway of last resort is not set
  207.21.24.0 is variably subnetted, 2 subnets, 2 masks
C 207.21.24.32 255.255.255.224 is directly connected, Ethernet0
C 207.21.24.192 255.255.255.252 is directly connected, Serial0
```

为了使在不同大小子网中的路由器能相互正确地更新路由选择信息，它们必须在路由选择更新信息中发送掩码。如果在路由选择更新中不含有子网信息，路由器将只依据传统的地址类别和它们自己的子网掩码来发送，只有忽略地址类别和使用无类别前缀的路由选择协议才能够配合VLSM正确地工作（参见表2-5）。

表2-5 有类别和无类别路由选择协议

有类别路由选择协议	无类别路由选择协议
RIP版本1	RIP版本2
IGRP	EIGRP
EGP	OSPF
BGP3	IS-IS
	BGP4

2.3.4 使用RIP和IGRP时的VLSM

有两种常见的内部网关协议，RIP版本1和IGRP，不在它们的路由更新中发送子网信息，因此它

们不支持VLSM。一旦收到一个路由更新分组，这两种有类别路由选择协议便用下面的方法之一来判断地址的网络前缀：

• 如果路由器收到有关一个网络的信息，并且如果接收接口属于同一个网络（但在不同的子网），则路由器应用配置在接收接口上的子网掩码。

• 如果路由器收到有关一个网络的信息，但该信息与接收接口上所配置的网络地址的信息不同，则路由器应用缺省的（根据类别）子网掩码。

尽管有它的局限性，RIP仍然是流行的路由选择协议，并且实际上被所有的IP路由器支持。RIP的普遍性来源于它的简单性和普遍兼容性。但是RIP的第1个版本（RIPv1）有几个关键的不足：

• RIPv1不在它的路由选择更新中发送子网掩码信息。没有子网信息，就不能支持VLSM和CIDR。

• 路由选择更新采用广播方式，这会增加网络通信。

• 不支持验证。

1988年，RFC 1058描述了新的（且被改进了的）RIP版本2来解决这些不足。

• RIPv2发送子网信息，并且支持VLSM和CIDR。

• 使用D类地址224.0.0.9，通过组播传送路由选择更新，提高了效率。

• 在路由选择更新中提供验证功能。

由于这些关键特性，应尽可能用RIPv2代替RIPv1，除非网络上的传统设备不能支持它。

当RIP在Cisco路由器上第一次启用时，路由器会侦听版本1和版本2的更新，但只发送版本1的更新。要想利用版本2的功能，可以使用例2-2中的命令关闭对版本1的支持并启用版本2的更新。

例2-2　配置RIP版本2

```
Router(config)#router rip
Router(router-config)#version 2
```

RIP的简洁设计确保它会继续生存下去。已经有一个新版本的设计能够支持将来的IPv6网络。



实验活动　复习关于RIP的基本路由器配置

在本次实验中，要连接和配置工作站和路由器。使用表中已定义的B类网络建立一个IP寻址方案，并在路由器上配置RIP。

2.4　路由汇总（Route Summarization）

使用CIDR和VLSM不仅防止地址浪费，也提供了路由聚合（route aggregation）或汇总（route summarization）。没有路由汇总，Internet骨干路由可能在1997年之前就已经崩溃了。

图2-8示例了路由汇总如何减轻上游路由器的负担。网络和子网大小不同的复杂分层体系通过前缀地址在各点进行汇总，直到整个网络作为一条聚合路由被发布：200.199.48.0/20。

回忆一下，这种路由汇总或超网，只有当网络的路由器运行无类别路由选择协议，如OSPF或EIGRP时才是可能的。无类别路由选择协议在路由选择更新中带有与32比特地址相对应的前缀长度（子网掩码）。在图2-8中，最终到达网络提供商的汇总路由包含一个机构中所有地址公共的20比特前缀：200.199.48.0/20或11001000 11000111 0001。为了让汇总正常工作，必须认真地以分级方式来分配地址，以便汇总的地址能够共享高位比特。

如图2-9中的例子，路由器A既可以发送3条路由选择更新条目，也可以把地址汇总为一个单独的网络号。图2-9显示了路由172.16.25.0/24、172.16.26.0/24和172.16.27.0/24如何汇总为172.16.0.0/16。

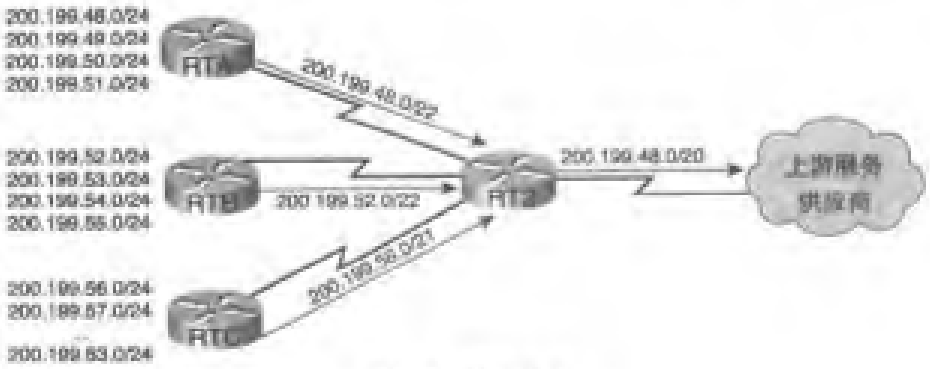


图2-8 路由汇总

图2-9中的路由器可以转发路由到网络172.16.0.0/16，包含该网络中所有的子网。但是，如果172.16.0.0的其他子网存在于网络的其他地方（例如，如果172.16.0.0是不连续的），用这种方法汇总可能就不正确了。不连续的网络和汇总将在后面讨论。

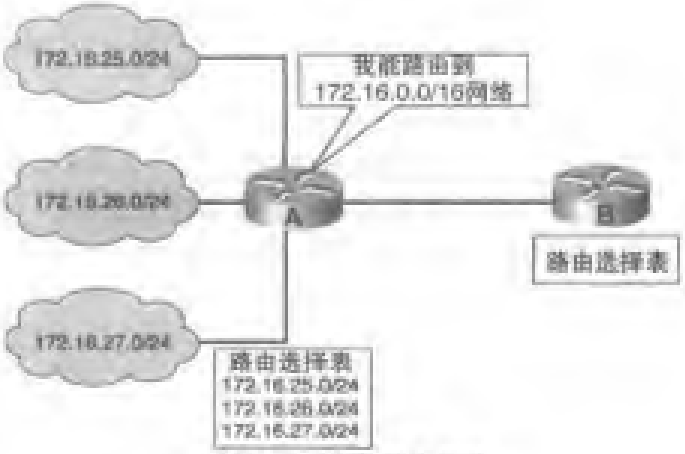


图2-9 更多的路由汇总

在一个大型、复杂的网络中使用路由汇总的另一个好处是能将其他路由器的拓扑变动隔离开。也就是说，如果在172.16.27.0/24域中有某一条链路出现翻动（flapping）（在up和down状态之间快速变换），汇总路由不会变化。因此，域外的路由器不需要由于这种翻动行为而不断修改自己的路由选择表。

当网络地址是一大块连续网络地址，数目是2的幂次数时，在这样的子网环境下路由汇总效率最高。例如4、16或512个地址可以用单独的一条路由选择条目表示，因为汇总掩码是二进制掩码，就像子网掩码，所以必须发生在二进制边界线上（是2的幂次数）。

路由选择协议由基于网络中共享的网络号对路由进行汇总或聚合。无类别路由选择协议，如RIPv2、OSPF、IS-IS和EIGRP，基于子网地址支持路由汇总，包括VLSM地址。有类别路由选择协议，如RIPv1和IGRP，在有类别的网络边缘自动汇总路由，不支持在其他边界上进行路由汇总。

路由汇总在RFC1518中描述，“使用CIDR的IP地址分配结构（An Architecture for IP Address Allocation with CIDR）”。

2.4.1 在一个字节内汇总

假设路由器收到下列路由的更新信息，如图2-10所示。

172.16.168.0/24
172.16.169.0/24
172.16.170.0/24
172.16.171.0/24
172.16.172.0/24
172.16.173.0/24
172.16.174.0/24
172.16.175.0/24

为了确定汇总路由，路由器要确定在所有地址中都能匹配的高位比特。通过将这些IP地址转换



图2-10　在一个字节内汇总

成二进制格式，就可以确定在这些IP地址中共享的公共比特。在图2-10中，前21比特是这些地址公共的。因此，最好的路由汇总就是172.16.168.0/21。当地址的数量是2的幂次数时，可以汇总这些地址。如果不是2的幂次数，就要把这些地址分组，分别对各个组进行汇总。

为使路由器将最大数量的IP地址聚合为单独的一条路由，IP地址规划应该是分级的。当使用VLSM时，这个过程尤其重要。

2.4.2　汇总非连续网络

有类别路由选择协议在网络边缘自动汇总。至RIPv1和IGRP不能改变这种行为，该行为会导致重要的结果是：

- 子网不能发布到不同的主网络中。
- 不连续的子网相互不可见。

在图2-11中，RIPv1不能发布172.16.5.0 255.255.255.0和172.16.6.0 255.255.255.0子网，因为RIPv1不能发布子网；路由器A和路由器B都发布172.16.0.0。当路由选择跨过网络192.168.14.0时会造成混乱。在这个例子中，路由器从两个不同的方向收到关于172.16.0.0的路由，因此它无法做出正确的路由选择决定。

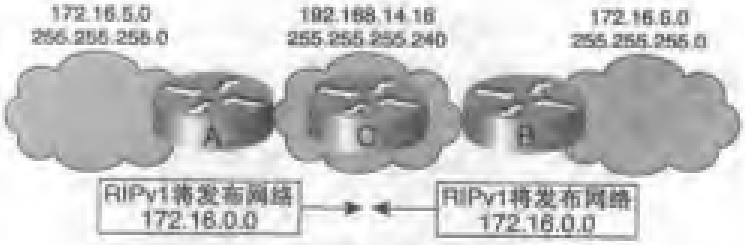


图2-11　汇总非连续网络

通过用RIPv2、OSPF、IS-IS或IGRP来解决这个问题，不使用汇总是因为子网信息将带着它们真正的子网掩码发布出去。

Cisco IOS 软件也提供无编号IP（IP unnumbered）功能，允许不连续的子网被一条无编号的链路分开。无编号的链路是一条没有指定IP地址的链路，但仍被其他子网见到，以避免非连续链路。一个没有使用无编号IP功能的无编号连接会导致非连续链路。

2.5　路由翻动（Route Flapping）

当路由器接口在“up”和“down”状态之间快速变换时就会产生路由翻动（Route Flapping）。这可能是由很多原因引起的，包括接口故障或端接不良的介质。

路由汇总有效地将上游路由器从路由翻动问题中隔离出来。如果连接着200.199.56.0网络的

RTC的接口“down”了，RTC将把这条路由从它的路由选择表中删除。如果路由器没有配置路由汇总，RTC将向RTZ发送一个有关取消到网络200.199.56.0的路由的触发更新（triggered update）。依次，RTZ将向其上游方向的下一台路由器发送有关该路由的更新信息，依此类推。每次当这些路由器接收新的路由更新信息时，它们的处理器必须投入工作。处理器的工作可能会很繁重以致明显地影响到分组转发性能。如果到网络200.199.56.0的RTC接口只在几秒种后就恢复“up”，考虑一下它对性能的影响。路由器又将发送路由更新并且重新进行路由计算。当RTC的链路几秒种后又回到“down”状态时又会发生什么？然后又恢复“up”？这就是路由翻动，它可能会因为过度的路由更新和重新计算削弱路由器的性能。

然而，路由汇总配置可以防止因RTC路由翻动对其他路由器的影响。RTC向RTZ发送包含8个网络（200.199.56.0到200.199.63.0）的一个超网（200.199.56.0/21）有关的路由更新信息。到其中一个网络的路由丢失并不影响到超网的路由。尽管RTC可能忙于处理它自己的路由翻动问题，RTZ（和所有上游方向的路由器）不会注意到。路由归纳可以有效地将其他路由器从路由翻动问题中隔离开。

2.6 RIPv2

网络需要可扩展。换句话说，网络必须能够成长。所选的路由选择协议对网络的可扩展性会造成很大的区别。所以明智地选择路由选择协议是非常重要的。一般来说，RIP被认为适合小型网络但不适用于大型网络。RIPv1是有类别路由选择协议，但是RIPv2是无类别路由选择协议。有类别的方法局限在于，它需要在主要网络的边缘自动汇总为有类别网络。这意味着RIPv1不支持VLSM而RIPv2支持。

2.6.1 RIP的简史

在像Internet这样的国际性网络中，只使用单一的路由选择协议是不可能的。更合适的作法是将网络组织为多个自治系统（AS, Autonomous Systems）。每一个AS都由单独的机构管理。每个AS都有自己的路由选择技术，可能与其他AS不同。在一个AS内使用的路由选择协议叫做内部网关协议（IGP, Interior Gateway Protocol）。另一种协议叫做外部网关协议（EGP Exterior Gateway Protocol），在AS之间传送路由选择信息。RIP设计用于工作在中等大小的AS中，并不打算用于更复杂的环境。

RIPv1被认为是有类别的IGP。它是距离矢量路由选择协议，以定义好的时间间隔（如30秒）向邻居路由器广播完整的路由选择表。RIP用跳数作为度量值，15是最大跳数。正如前面所提到的，如果RIPv1收到一个路由更新分组，它会通过下面的其中一种方式来判定地址的网络前缀：

- 如果路由器收到有关一个网络的信息，并且如果接收接口属于这同一个网络（但在不同的子网），则路由器应用配置在接收接口上的子网掩码。
- 如果路由器收到有关一个网络的信息，但该网络地址信息与接收接口上所配置的网络地址信息不同，则路由器应用缺省的（根据类别）子网掩码。

对于A类地址，缺省掩码是255.0.0.0。

对于B类地址，缺省掩码是255.255.0.0。

对于C类地址，缺省掩码是255.255.255.0。

RIPv1是一种普遍并且流行的路由选择协议，因为实际上所有的IP路由器都支持它。RIP的普遍性来源于它的简单性和普遍兼容性。RIPv1能够在多达6条等值路径上负载均衡（缺省是4条路径）。

回忆RIPv1的一些局限性：

- 它不在路由更新中发送子网掩码信息。
- 它基于广播255.255.255.255发送路由更新信息。

- 它不支持验证。
- 它不支持VLSM或CIDR。

例2-3显示如何配置RIPv1。

例2-3　配置RIPv1

```
Sydney(config)# router rip
Sydney(config-router)# network 172.16.0.0
Sydney(config-router)# network 192.168.100.0
```

2.6.2　RIPv2功能

RIPv2是RIPv1的改进版本。它具有以下特性：

- 用跳数作为度量值，最大值为15。
- 是距离矢量路由选择协议。
- 用抑制定时器（hold-down timer）防止路由选择环路，缺省值为180秒。
- 用水平分隔（split horizon）防止路由选择环路。
- 用16跳作为无限距离的能量值。
- 发送有子网掩码的路由选择信息。
- 通过沿每条路由传送掩码来支持VLSM，以便子网能被确切地定义。
- 提供身份验证功能。
- 同时使用明文和MD5。
- 在路由选择更新信息中包含下一跳路由器的IP地址。
- 使用外部路由标记（enternal route tags）。
- 提供组播传送路由选择更新。

RIPv2提供前缀路由选择，可以在路由更新信息中发送子网掩码信息。RIPv2支持无类别路由选择，在同一网络中不同的子网使用不同的子网掩码（VLSM）。

RIPv2在它的路由更新中提供身份验证功能。在一个接口上可以用一套密钥作为身份验证的检查。RIPv2支持在RIPv2分组中的包含验证类型。这个选择可以是明文的也可以是MD5加密的。明文是缺省的方式（MD5可以用于鉴别路由更新的源）。MD5通常用于加密和enable secret密码，并且是不可逆的。

RIPv2使用D类地址224.0.0.9组播传送路由选择更新信息，可提高效率。

2.6.3　比较RIPv1和RIPv2

RIP使用距离矢量算法判定到互连网络任意链路的方向和距离。如果到目的地有多条链路，RIP选择跳数最少的路径。然而，因为跳数是RIP使用的惟一度量值，所以它不一定选择最快的路径，它只计算跳数。

RIPv1允许路由器在可设定的时间间隔更新路由选择表。缺省的更新时间间隔是每30秒一次。RIPv1持续地发送路由选择更新，很快生成网络流量。为防止分组陷入无限环路，RIP有一个最大跳数值15。如果目的网络超过15跳，就会被认为目的不可到达并丢弃分组。当在一个大型、不同种类的网络中路由时，这种情况就会导致可扩展性方面的问题。RIPv1用水平分割防止环路。这意味着RIPv1只有当不是从这个接口学习到相应路由时，才会从该接口发布路由出去。抑制（hold-down）措施在抑制定时器规定的时间内忽略任何关于一个网络的新信息。

下面归纳了当路由器使用RIPv1时的行为：

- 直连的子网对于路由器是已知的，这些路由会发布给邻居路由器。

- 广播路由选择更新信息，所有的邻居路由器通过单个广播学到更新信息。
- 路由器通过侦听更新信息来学习新的路由信息。
- 在更新信息中每条路由都有一个度量值描述该路由有多“好”。
- 如果存在很多条路由至同一目的，使用度量值最小的那条。
- 拓扑信息包含在路由选择更新中，至少包括子网和度量值信息。
- 邻居路由器期待周期性地更新路由。
- 没有及时收到路由更新会导致删除以前从邻居路由器学到的路由。
- 从其他邻居路由器学到的路由被假定是来自于那台邻居路由器。

表2-6对RIPv1和RIPv2作比较。

表2-6 比较RIPv1和RIPv2

RIPv2	RIPv1
支持身份验证	无身份验证
无类别子网掩码，VLSM	有类别掩码
下一跳主机	下一网关
组播——224.0.0.9	广播——255.255.255.255
使用路由标记	不使用路由标记
加上RIPv1所有的功能	

2.6.4 配置RIPv2

RIPv2是动态路由选择协议，通过指定路由选择协议的名称（RIP版本2），并分配IP网络编号而不指定子网值来配置。本节内容描述在Cisco路由器上配置RIPv2所使用的基本命令。

为了启动一种动态路由选择协议，必须完成下面的任务：

- 选择一种路由选择协议，如RIPv2。
- 指定IP网络号，无须指定子网值。
- 为接口分配适当的网络或子网地址及适当的子网掩码。

RIPv2用组播与其他路由器通信。路由选择度量值帮助路由器发现到每个网络或子网的最佳路径。

router命令用于启动一个路由选择进程。network命令能实现以下3项功能：

- 路由选择更新信息都从某个接口组传送出去。
- 如果它们从相同接口进入，路由选择更新将被处理。
- 直接连到接口的子网被发布。

network命令是需要的，因为它允许路由选择进程决定哪些接口将要参与发送和接收路由选择更新信息。network命令能在路由器上所有位于特定网络内的接口上启动路由选择协议。network命令也使得路由器将该网络发布出去。

命令router rip和version 2指定RIPv2作为路由选择协议，命令network标识参与的直连网络。

参看图2-12，路由器A的配置包括以下内容：

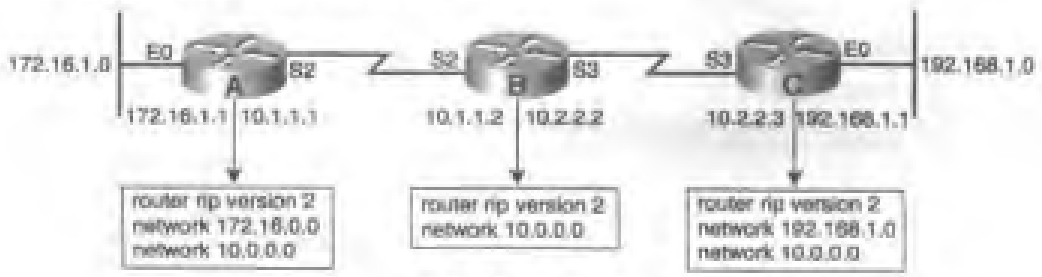


图2-12 配置RIP

- router rip——启动RIP作为路由选择协议。
- version 2——指定版本2作为所使用的RIP版本。
- network 172.16.0.0——指定一个直连的网络。
- network 10.0.0.0——指定一个直连的网络。

路由器A的接口连接网络172.16.0.0和10.0.0.0，或它们的子网，将发送和接收RIPv2的路由选择更新。这些更新信息使路由器学习网络的拓扑结构。路由器B和C有相似的RIP配置，只是所指定的网络号不同。



实验活动　将RIPv1转换成RIPv2

在本次实验中，启动路由选择协议RIPv1，然后再转换成RIPv2路由选择协议。

2.6.5　验证RIPv2

命令show ip protocols和show ip route显示了关于路由选择协议和路由选择表的信息。本节内容描述如何用show命令验证RIP配置。

命令show ip protocols显示关于路由选择协议的值和与路由器相关的路由选择协议时钟信息。例2-4显示了图2-12中路由器A上show ip protocols命令的输出。

例2-4　show ip protocols命令输出

```
RouterA#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 12 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
Redistributing rip
Default Version Control: send version 1 receive any version
    Interface    Send    Receive    Triggard RIP    Key-Chain
    Ethernet0    1       1 2
    Serial2      1       1 2
  EIGRP maximum metric variance 1
    Routing for Networks:
    10.0.0.0
    172.16.0.0
Routing Information Sources:
    Gateway Distance Last Update
    (this router) 120 02:12:15
    10.1.1.2 120 01:09:01
Distance: (default is 120)
```

在例2-4中，路由器被配置使用了RIP协议，并且每30秒会发送一次路由选择表的更新信息（这个间隔时间是可配置的）。如果一台运行了RIP协议的路由器在180秒或更长的时间里没有收到来自其他路由器的更新信息，那么路由器将标记相应未更新的路由为无效路由。在例2-4中，抑制定时

器设置为180秒时，路由信息将一直被标记为“possibly down”的状态，直到180秒过去才会由down的状态更新为up状态。

如果在240秒“消除定时器设定（flash timer setting）”后仍然没有更新信息，路由器将删除该路由选择表条目。在例2-4中，从路由器A收到了路由器B的更新信息起已经过去了18秒。

路由器从网络得到的路由信息列在“Routing for Networks”列。路由器从相邻运行RIP协议的路由器得到的路由信息列在“Routing Information Sources”列。

缺省距离120是指RIP路由协议的管理距离（administrative distance）。

可以使用show ip interface brief命令列出接口IP信息和状态的摘要。

show ip route命令显示IP路由选择表的内容，见例2-5。

例2-5 show ip route命令输出

```
RouterA#show 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
    172.16.0.0/16 is subnetted, 1 subnets
C       172.16.1.0/24 is directly connected, Ethernet0
    10.0.0.0/24 is subnetted, 3 subnets
R       10.2.2.0/24 [120/1] via 10.1.1.2, 00:00:07, Serial2
C       10.1.1.0/24 is directly connected, Serial2
R       192.168.1.0/24 [120/1] via 10.1.1.2, 00:00:07, Serial2
```

路由选择表包含了所有的已知的网络和子网条目，并且包含了表明路由信息是如何被学到的代码。表2-7中列出该命令输出的关键字段和他们的功能说明。

表2-7 路由表输出解释

输出	描述
R or C	标识路由信息的来源。例如，C代表该路由的原始来源是直连的子网。R表示该路由是从其他运行RIP的路由器学到的
192.168.1.0 10.2.2.0	指明远端网络的地址
120/1	括号中的第一个数字是路由信息来源的管理距离；第二个数字是路由的度量值。（例如，1跳）
Via 10.1.1.2	指定了到远端网络的下一跳的路由器地址
00:00:07	指定了自路由上次更新后所经过的时间为时：分：秒
Serial 2	指定了到达指定网络所要通过的接口

检验输出，查看路由选择表中的路由选择信息是否正确，如果路由选择信息没有交换，（也就是说.如果使用show ip route命令的输出中没有通过路由选择协议学到的路由条目），使用路由器上的show running-config或 show ip protocols 特权EXEC命令检查可能的路由选择协议配置错误。



实验活动　验证RIPv2配置

在这个实验中，你将启动RIP版本1和版本2路由选择协议，并且通过使用各种各样的show命令验证RIPv2路由选择协议。

2.6.6　对RIP进行故障排除

本节解释debug ip rip 命令的用法。

使用debug ip rip命令显示RIP路由选择协议发送和接收路由选择信息时的路由更新情况。使用no debug all 或 undebug all命令关掉所有的调试。

例2-6显示了一台正在被调试的路由器从另一台源地址为10.1.1.2路由器收到的更新信息。该路由器在路由选择表更新信息中发送了关于两个目的网络的信息。被调试的路由器也发送了路由选择表的更新信息，在两种情况下都是以广播地址255.255.255.255作为目的地址。括号中的地址是封装在IP报头中的源地址。由于这是RIPv1，更新是通过广播地址发送的。RIPv2将通过D类多播地址224.0.0.9发送路由选择更新，这将会更有效率。

例2-6　debug ip rip命令

```
RouterA#debug ip rip
RIP protocol debugging is on
RouterA#
00:06:20: RIP: received v1 update from 10.1.1.2 on Serial2
00:06:24:      10.2.2.0 in 1 hops
00:06:24:      192.168.3.0 in 2 hops
00:06:33: RIP: sending v1 update to 255.255.255.255 via Ethernet0 (172.16.1.1)
00:06:34:      network 10.0.0.0, metric 1
00:06:36:      network 192.168.1.0, metric 3
00:06:34: RIP: sending v1 update to 255.255.255.255 via Serial2 (10.1.2.1)
00:06:34:      network 176.168.0.0, metric 1
```

debug ip rip命令的输出有时可以看到下列信息，这种情况出现在启动或某个事件发生时，比如接口转换或用户手动地清除了路由选择表：

```
RIP: broadcasting general request on Ethernet0
RIP: broadcasting general request on Ethernet1
```

下列的信息很可能由于从发送端送过来的损坏分组导致：

```
RIP: bad version 128 from 160.89.80.43
```

debug ip rip输出和说明见表2-8。

表2-8　debug ip rip输出解释

输出	描述
RIP:broadcasting general request on Ethernet0 as startup	接口转换，或用户手动清除接口
RIP:bad version 128 from 160.89.80.43	来自160.89.80.43的坏包
RIP:received v2 update from 150.100.2.3 on Serial0	从150.100.2.3发送的RIP及版本
RIP:sending v1 update to 255.255.255.255 via Serial0 (150.100.2.2)	在Serial0上配置了RIPv1，
RIP:ignored v1 packet from 150.100.2.2 (illegal version)	该路由器未配置RIPv1
RIP:sending v2 update to 224.0.0.9 via FastEthernet0 (150.100.3.1)	配置了RIPv2并且正在发送更新
RIP:build update entries 150.100.2.0/24 via 0.0.0.0, metric 1, tag0	使用缺省路由和标签

实验活动 使用debug对RIPv2进行故障排除

在这个实验中，在两台路由器上配置RIPv2。然后使用debug命令验证正确的rip操作并且分析在路由器之间传送的数据。

2.7 缺省路由

在缺省的情况下,路由器学习到目的地的路径有3不同的方法：

- **静态路由**是由系统管理员手工定义到达目的地的下一跳地址，由于不知道其他的路由，因此有助于安全和减小流量。
- **缺省路由**也是由系统管理员手工定义的，是在没有到达目的地的已知路由的情况下所走的路径。缺省路由有助于保持路由选择表的简短。当到达目的地网络的路由不在路由选择表中时，分组将被送到缺省网络。
- **动态路由选择协议**是路由器通过接收周期性更新来学习到达目的地的路由的，这些更新信息是从其他使用路由选择协议（如RIP协议）的路由器发送的。

一个简单的例子，静态路由能使用在例2-7中的命令定义。

例2-7 静态路由

```
Router(config)# ip route 172.16.1.0  255.255.255.0  172.16.2.1
```

ip default-network 命令用于在使用了动态路由选择协议的网络中建立缺省路由，见例2-8。

例2-8 动态缺省路由

```
Router(config)#ip default-network 192.168.20.0
```

在将路由选择表设置为能够处理所有的必须配置的网络后，确保所有的剩余分组都会发到指定的位置，通常是很有用的，例如一台路由器与因特网连接时。这被称为路由器的缺省路由。所有的在路由选择表中没定义的分组都会发送到路由器指定的缺省接口。图2-13显示出分组将被发往在例2-8中定义的缺省网络。

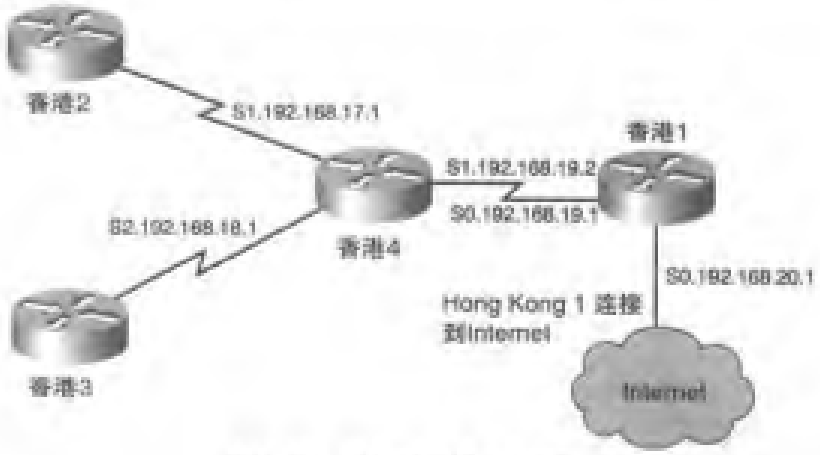


图2-13 缺省路选择由w/RIP

ip-default network命令通常配置在那些与一台有静态缺省路由的路由器相连的路由器上。

例2-9中显示了一条定义静态缺省路由的命令，它既能用于静态路由选择协议也能用于动态路由选择协议。

在图2-13中，香港2和香港3使用香港4作为缺省网关。香港4使用接口192.168.19.2作为它的缺省网关。香港1为所有的内部的主机发送分组到Internet。为了能让香港1路由这些分组，有必要配置

一条缺省路由，见例2-9。

例2-9　缺省路由

```
HongKong1(config)#ip route 0.0.0.0  0.0.0.0  192.168.20.1
```

多个0表示具有任何掩码的任何目的网络。缺省路由指的是4个一组的零路由。在图中，香港1只有一条路通往因特网，通过接口192.168.20.1。

2.8　总结

在本章中，你学习了以下内容：

- 无类别域间路由选择（CIDR）取代基于类别边界分配IP地址的旧方法。
- CIDR的概念于1993首先在 RFC 1517、1518、1519和1520中提出，在1994开始使用。
- CIDR中介绍了超网和路由聚合。
- VLSM允许网络管理员更有效地分配IP地址。无类别路由的使用让VLSM更有效率，因为有类别网络边界不再必要。
- 路由汇总在子网中是最有效的。
- RIPv1和v2是使用跳数作为路由选择度量值的距离矢量路由选择协议，每30秒一次广播路由选择更新。
- RIPv1在更新路由信息时，不发送子网掩码信息，因此不支持VLSM和CIDR。它使用广播的方式进行路由更新，增加了网络流量，并且不支持认证。
- RIPv2发送子网信息，支持VLSM和CIDR。它使用组播的方式，用D类地址224.0.0.9进行路由更新，更加有效率，并且在路由更新时还提供对身份验证的支持。
- router RIP命令指定RIP作为路由选择协议。
- network命令标识参与路由协议的网络。RIPv2支持验证、子网掩码、下一台主机信息、多播和路由标记。

为了补充本章你所学内容，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验活动。

2.9 关键术语

无类别域间路由选择（*classless interdomain routing, CIDR*） 无类别路由选择协议基于路由聚合。CIDR允许路由器把路由聚合在一起以减少核心路由器携带的路由选择信息数量。利用CIDR，几个IP网络在组外看起来像是单个的、大型的实体。在CIDR中，IP地址和它们的子网掩码写成圆点分隔的4段8位组，后跟一个反斜杠和表示子网掩码的前缀。

缺省路由（*default route*） 不指定一个替代路径时，设备自动选择的路由。

路由汇总（*route summarization*） OSPF和IS-IS中发布的地址合集。在OSPF中，路由汇总将产生一个单独的汇总路由，并由区域边界路由器通告到其他区域。

静态路由（*static route*） 固定的且不能改变的路由。

超网（*supernetting*） IP网络地址的聚合，作为一个单一的无类别网络地址通告。

可变长子网掩码（*variable-length subnet mask, VLSM*） 在不同的子网上为相同的网络号指定不同子网掩码的能力。VLSM有助于优化可用地址空间。

2.10　复习题

1. 当172.17.15.0/24用额外的4位进行子网划分时，以下哪两个地址是合法的子网地址？（选择2个答案）

A. 172.17.15.0
B. 172.17.15.8
C. 172.17.15.40
D. 172.17.15.96
E. 172.17.15.248

2. 点到点的广域网链接中最有效的子网掩码是什么？

A. 255.255.255.0
B. 255.255.255.224
C. 255.255.255.252
D. 255.255.255.248

3. 下列哪项是CIDR的特性？（选择所有正确的答案）

A. 有类别寻址
B. 超网
C. 路由选择表中更多的项
D. 路由聚合

4. 网络172.21.136.0/24和172.21.143.0/24的汇总地址是什么？

A. 172.21.136.0/21
B. 172.21.136.0/20
C. 172.21.136.0/22
D. 172.21.128.0/2

5. 哪种路由选择协议在它的路由选择更新中不包含子网掩码信息？

A. EIGRP
B. OSPF
C. RIPv1
D. RIPv2

6. 下列哪种方法在一个单一的IP地址内表示一个IP地址集合？

A. 有类别路由选择
B. 超网
C. 地址转换
D. 路由汇总



第3章　单区域OSPF

目标

学习完本章之后，你将能够：

- 描述OSPF。
- 描述指定路由器的选举过程。
- 列出OSPF的网络类型。
- 在单区域中配置OSPF。
- 对OSPF进行验证和故障排除。

链路状态路由选择协议是复杂的、可扩展的路由选择协议。本章就介绍这种行业标准的开放最短路径优先路由选择协议（OSPF，Open Shortest Path First）。本章描述了OSPF的路由器选举过程（router-election process）和OSPF如何运行在各种不同的网络中。介绍了如何配置基本的单区域OSPF网络，同时也包括对OSPF配置进行验证和故障排除的过程。

请注意应配合本书附带光盘上的e-Lab实验、视频和插图一起阅读内容，光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

3.1　单区域OSPF的概念

链路状态路由选择协议与距离矢量路由选择协议不同。链路状态协议泛洪（flooding）链路状态信息，使每台路由器有一个完整的网络拓扑视图。对于距离矢量协议，路由器不会了解完整的网络拓扑。OSPF是一种链路状态协议。

在OSPF中，最短路径优先算法（该算法是计算机科学家Dijkstra发明的）用于确定最佳路径——到链路成本最低的路径。

最短路径优先（SPF Shortest Path First）算法用于点到点的网络连接。为了在目前多样的网络中实现OSPF协议，OSPF必须知道它所运行的网络类型。

在交换OSPF链路状态信息前，OSPF协议会在路由器之间建立邻居关系（neighbor relationship）。OSPF的Hello协议就用于此目的。

OSPF是一种复杂的协议，可以用一套操作步骤描述。

3.1.1　OSPF概述

OSPF是一种基于开放标准的链路状态路由选择协议。多个IETF标准中都对OSPF有描述，最新的是RFC 2328。

其名字中的“开放（open）”是指OSPF是对公众开放的，非专有的。由于更具扩展性，OSPF正在成为比RIP协议更受青睐的内部网关协议（IGP）。

RIP不能扩展到超过15跳，收敛慢，并且在做路由决定时，因为忽略了像带宽这样关键因素而容易选择较慢的路由。

OSPF解决了所有的这些限制，已被证明是一种健壮的，可扩展的路由选择协议，适用于目前的网络。对于小型网络，可以在单个区域中应用OSPF，对于大型网络，可以在多个区域中应用它。

OSPF可以在大型网络中使用。如果使用了分级的网络设计原则，OSPF路由选择便能扩展到大型网络。大型的OSPF网络使用分级设计原则。多个区域联接到一个分配区（distribution area），区域0（Area 0），也称为骨干（backbone）。这种设计方法可以对大量的路由选择更新信息进行控制。通过定义区域，可以减少路由选择开销，加快收敛，限制某个区域，提高网络的性能。

OSPF网络分为多个部分，称为“*区域（areas）*”，可以高效地控制网络运行。区域0是主区域。所有OSPF网络都有一个区域0，而且它也作为主分配区（main distribution area）。

3.1.2　OSPF术语

作为一种链路状态路由选择协议，OSPF的运行方式与距离矢量路由选择协议不同。链路状态路由器识别邻居路由器并与这些邻居建立通信关系。OSPF有一套新的术语。如图3-1。

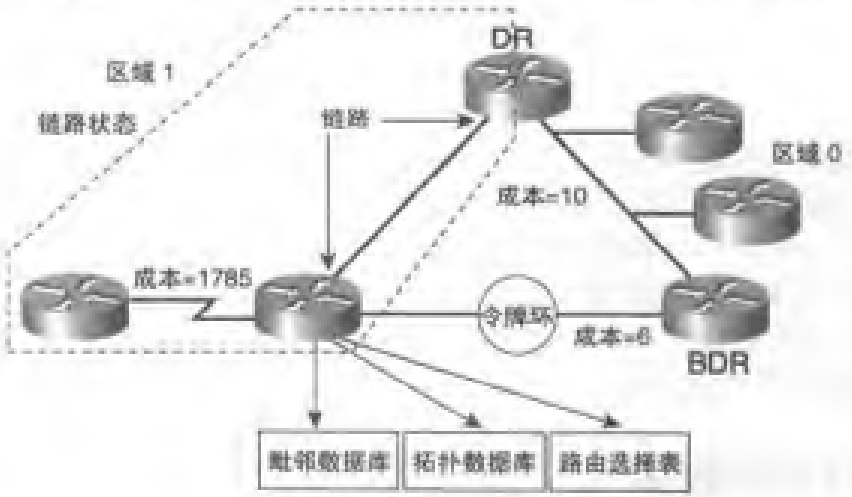


图3-1　OSPF术语

从OSPF邻居那里收集到的并不是一张完整的路由选择表。OSPF路由器互相告知它们自己的连接（或链路）状态，如图3-2显示。信息会泛洪到其他的邻居。*泛洪（Flooding）*是信息从除接收

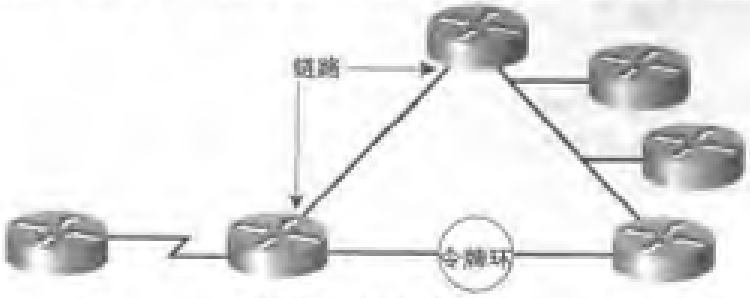


图3-2　OSPF链路

信息的端口以外的所有端口发送出去的过程。OSPF路由器通告自己的链路状态并传递接收到的链路状态信息。

区域1内的路由器处理这些，建立一个链路状态或者拓扑数据库，如图3-3所示。在OSPF区域内的每台路由器，如图3-4所示，都具有相同的链路状态数据库。每台路由器与邻居路由器具有关于链路状态的相同信息。一个自治系统可以分为多个区域，这些区域都是带有主机的毗邻网络。带有多个接口的路由器可以加入多个区域。这种路由器称为区域边界路由器（ABR, Area Border Routers），它会为每个区域维护一个单独的拓扑数据库。

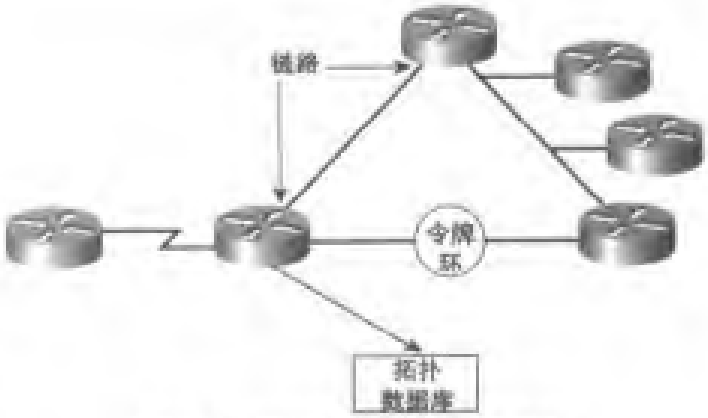


图3-3 OSPF链路状态拓扑数据库

每台路由器在路由器上的数据库运行*最短路径优先（SPF）算法*，也称为Dijkstra算法。该计算决定到目的地的最佳路由。SPF算法将成本加和（它是一个基于带宽的值）如图3-5所示，它把成本最低的链路添加到路由选择表中，路由表也称为转发数据库。

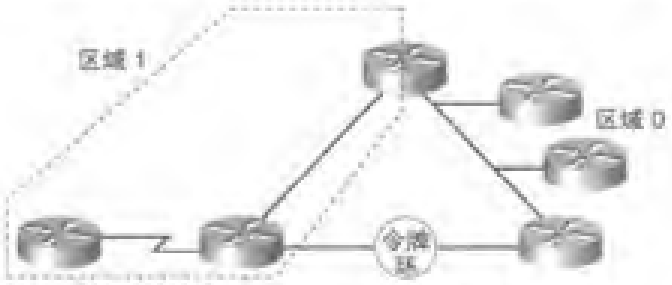


图3-4 OSPF链路状态区域

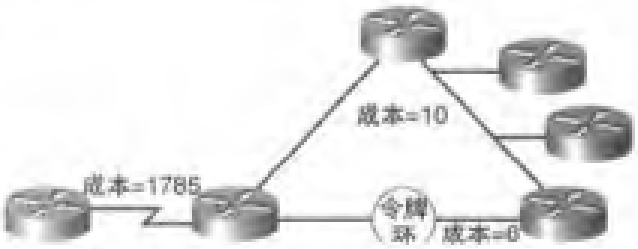


图3-5 OSPF成本

OSPF在毗邻数据库（adjacency database）中记录关于邻居路由器的信息。为了减少在同一个网络中几个邻居互相交换信息的数量，OSPF路由器会选举*指定路由器（DR, designated router）*和*备份指定路由器（BDR, backup designated router）*，作为路由信息交换的集中点。

3.1.3 OSPF状态

OSPF路由器为了与它的邻居有效地共享链路状态信息而建立各种关系或状态。与之相对，距离矢量路由选择协议，如RIP，只是盲目地将它们完整路由选择表从其每个接口上广播或者多播出去，希望外面有路由器能够接收它们。缺省时，每30秒，RIP路由器就发送其惟一的一种消息——它们完整的路由选择表。相反，OSPF路由器依靠5种不同种类的分组来识别它们的邻居并更新链路状态信息。表3-1显示了OSPF的分组类型。

这5种分组类型使OSPF能完成精密复杂的通信。这些分组类型在以后的章节会详细讨论，在这里，你应该开始熟悉OSPF路由器之间可能出现的各种关系，各种OSPF网络类型和OSPF Hello协议。

表3-1 OSPF分组类型

OSPF分组类型	描述
Type 1：Hello	与邻居建立和维护毗邻关系
Type 2：数据库描述分组（DBD, Database Description Packet）	描述一个OSPF路由器链路状态数据库的内容
Type 3：链路状态请求（LSR, Link State Request）	请求相邻路由器发送其链路状态数据库中的特定项
Type 4：链路状态更新（LSU, Link State Update）	向邻居路由器发送链路状态通告
Type 5：链路状态确认（LSACK, Link-state Acknowledgment）	确认收到了邻居路由器的LSA

有效设计和排除OSPF网络故障的关键是理解OSPF路由器之间的关系和状态。OSPF的接口可以处于下面7种状态之一。OSPF毗邻关系按照列表中的状态，从上至下逐步发展。

- Down（停止）。
- Init（初始）。
- Two-way（双向）。
- ExStart（准启动）。
- Exchange（交换）。
- Loading（加载）。
- Full adjacency（全毗邻）。

1　Down状态

在“Down”状态下，OSPF进程还没有与任何邻居交换信息，OSPF在等待进入“Init”状态。

2　Init状态

OSPF路由器以固定的时间间隔（通常10秒）发送类型1（Hello）分组，以便与邻居路由器建立关系。当一个接口收到第一个Hello分组后，路由器就进入到Init状态，这意味着路由器知道有个邻居在等待将相互之间的关系发展到下一步。

一般来说，存在着两种关系：Two-Way状态和Adjacency状态，但在它们之间还有很多阶段。路由器在建立任何关系之前必须从邻居路由器那里收到一个Hello分组。

3　Two-Way状态

每台OSPF路由器都使用hello分组试图与同一IP网络（或子网）中的所有邻居路由器建立two-way状态或者双向通信。Hello分组中含有发送者已知的OSPF邻居列表。当路由器看到它自己出现在一台邻居路由器的hello分组中，它就进入two-way状态。如图3-6，当RTB了解到路由器RTA知道它时，它就宣布与路由器RTA之间进入two-way状态。

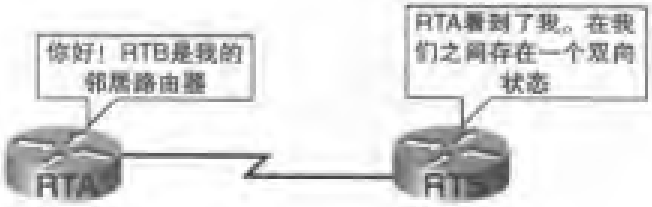


图3-6　OSPF Two-way状态

two-way状态是OSPF邻居之间可以具有的最基本关系，但在处于这种关系中的路由器之间是不能共享路由信息的。要想了解其他路由器的链路状态并最终建立一张路由选择表，每台OSPF路由器必须至少建立一个毗邻关系。它是OSPF路由器之间的一种高级关系，涉及一系列逐步前进的状态。它们不仅依赖于hello分组，还依赖于其他4种OSPF分组。。迈向full adjacency状态的第一步是“Exstart”状态。

4　ExStart状态

从技术角度看，当路由器与它的邻居进入到Exstart状态后，它们之间的会话就表征为一种毗邻关系，但这时路由器还没有变成full adjacency状态。Exstart状态是用类型2数据库描述（DataBase Description，DBD）分组，也称为DDP（Database Description Packet）建立的。两台邻居的路由器用Hello分组来协商它们之间的关系中谁是“主”谁是“从”并用DBD分组交换数据库信名。如图3-7所示。

有最高OSPF路由器ID的路由器将胜出并变成“主”（OSPF路由器ID将在本章后面的章节讨论）。当邻居路由器建立了它们之间的主从角色后，它们就进入“exchange”状态并开始发送路由选择信息。

5 Exchange 状态

如图3-7所示，在Exchange状态下，邻居路由器使用类型2的DBD分组来相互发送它们的链路状态信息。换句话说，路由器相互描述自己的链路状态数据库。路由器将它们所学习到的信息与其现存的链路状态数据库进行比较，如果任何一台路由器接收到不在其数据库中的有关链路的信息，该路由器就向其邻居请求有关该链路的完整更新信息。完整的路由选择信息在“Loading”状态下交换。



图3-7 OSPF 路由发现

6 Loading状态

在相互描述过各自的链路状态数据库后，路由器用类型3的分组（LSR）请求更完整的信息。当路由器接收到一个LSR时，它会用一个类型4的分组（LSU）进行回应。这些类型4的LSU分组含有确切的LSA，LSA是链路状态类型路由选择协议的核心。如图3-7所示，类型4的LSU分组（需要用类型5的数据包，称为LSAcks，进行确认。

7 Full Adjacency状态

Loading状态结束后，路由器就变成full adjacency状态。每台路由器都保存着一张毗邻路由器列表，称为毗邻数据库（adjacency database）。不要把毗邻数据库、链路状态数据库或转发数据库混淆，表3-2列出了OSPF的重要数据库。

表3-2 OSPF数据库

数据库	描述
毗邻数据库（Adjacencies database）	列出所有已经与路由器建立起双向通信关系的邻居路由器。每个路由器的该表都是不同的
链路状态数据库（拓扑结构数据库）（Link-state database topological database）	列出关于网络中所有其他路由器的信息。该数据库显示出了网络的拓扑结构。一个区域中的所有路由器都有相同的链路状态数据库
转发数据库（路由选择表）Forward database（route table）	列出了在链路状态数据库上运行一种算记所产生的路由。每个路由器的路由表都是不同的，其中包含了关于如何及向哪里发送分组到其他路由器的信息。

3.1.4　比较OSPF和距离矢量路由选择协议

OSPF使用链路状态技术而RIP使用距离矢量技术。链路状态路由器维护一张公共的网络拓扑结构图，并且一旦有新的网络发现或网络改变时就交换信息。

链路状态路由器不会像距离矢量路由选择协议那样定期广播它们的路由选择表。因此在维护路由选择表时相比距离矢量路由选择协议使用较少的带宽。

RIP适用于小型的网络。OSPF设计用于满足大型的、可升级的网络的需要。RIP基于跳数进行最佳路径选择，这样选出来的路径有可能会是速度最低的路径。RIP与其他距离矢量路由选择协议一样，都使用简单的算法来计算最佳路径的。由于SPF算法是一种复杂的算法，故使用距离矢量路由选择算法的路由器比运行OSPF协议的路由器使用更少的内存和处理器资源。

OSPF基于和带宽相关的成本进行路由选择，带宽越大，OSPF链路的成本越低。OSPF选择最快的无环路径，即最短路径优先树，作为网络中的最佳路径。

OSPF能保证无环路由选择，而距离矢量路由选择协议则会导致路由选择环路。

如果链路出现不稳定，泛洪链路状态信息会导致不同步的LSA，和路由器之间不一致的路由选择。

OSPF解决了以下的问题：

- 收敛速度。
- 支持可变长度子网掩码（VLSM）。
- 网络规模。
- 路径选择。
- 成员分组。

在大型的网络中，由于路由选择表在与其直接相连的路由器之间拷贝和共享，故RIP的收敛可能会需要几分钟的时间。使用OSPF时收敛速度比较快，由于只有网络中的变化才会泛洪到区域里其他的路由器。当只有网络中的变化信息被发送的时候，更新信息被称为，增量更新（incremental update）。

OSPF是一种无类别的协议，支持VLSM。RIPv1不支持VLSM而RIPv2支持。RIP的最大跳数是15跳，它认为15跳以外的路由器是不可达的，这使RIP只能在小型的网络中使用。OSPF不受网络规模限制，能适用于中型到大型的网络。

RIP根据邻居路由器对某一网络的报告进行跳数加1来选择到达该网络的路径。RIP把到达目的网络的跳数进行比较以确定最短的距离或跳数。这种简单的算法并不要求路由器拥有强大的处理器和大量的内存。RIP在决定最佳路径时并不考虑可用带宽的大小。

OSPF用成本（cost）——基于带宽的度量值来选择路径。所有的OSPF路由器都必须获得整个网络的完整信息，用于每台路由器计算最短路径。这种复杂的算法要求OSPF路由器拥有比RIP路由器更强的处理能力和更大的内存。

RIP使用平面拓扑，位于同一RIP区域的路由器和其他所有的RIP路由器交换所有的信息。OSPF使用区域，一个网络可以被分为多个路由器群集。通过这种方式，OSPF控制了到这些区域的通信量，并使得一个区域内的变化不影响其他区域。这种分级化的方法使得网络能有效地扩展。

3.1.5　最短路径优先算法

OSPF使用最短路径优先算法来确定到达目的地的最佳路径。在这种算法中，最佳的路径是成本最低的路径。这种算法由一位名叫Dijkstra的荷兰计算机科学家发明，于1959年提出。这种算法认为网络是一个节点的集合，节点间通过点到点链路连接。

每条链路都有自己的成本。每个节点都有自己的名字。每个节点都有关于全部链路状况的完整数据库，因此关于网络物理拓扑的完整信息是已知的。最短路径算法接着就以节点作为起始点计算出一个无环拓扑，并依次检查它所拥有的关于毗邻节点的信息。

3.1.6 OSPF网络类型

因为OSPF路由器之间需要有毗邻关系才能共享路由选择信息，所以路由器将试图在它所连接的每个IP网络上与至少一台路由器建立毗邻关系。有些路由器可能会试图与所有的邻居路由器建立毗邻关系，另外一些路由器则可能会试图与一或两台路由器建立毗邻关系。OSPF路由器根据连接它们的网络类型来决定与谁建立毗邻关系的。在建立了毗邻关系后，将会交换链路状态信息。如图3-8及下列所示，OSPF接口可识别3种类型的网络：

- 广播型多路访问。
- 非广播型多路访问（NBMA）。
- 点到点网络。

网络管理员还可以在接口配置第4种网络类型：点到多点型（point-to-multipoint）网络。表3-3列出了OSPF的网络类型。

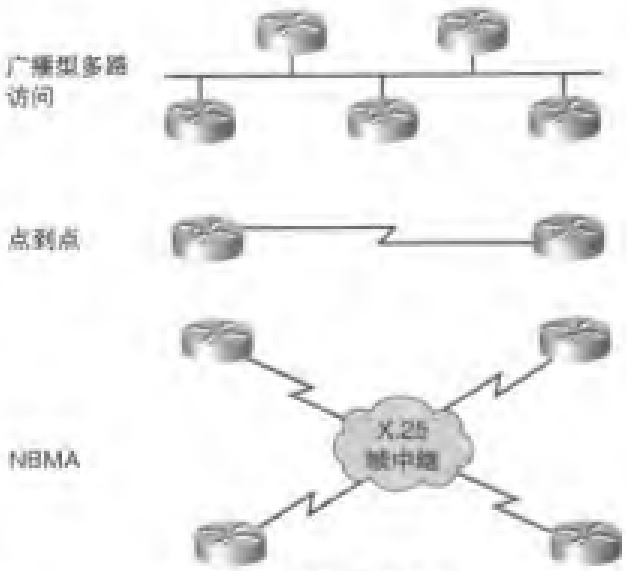


图3-8 OSPF网络类型

在多路访问型网络中，我们并不能预测出有多少台路由器连接到网络中。在*点到点型网络*中，仅仅有两台连接的路由器。如果每台路由器都与所有其他路由器建立full adjacency关系，开销将会很大。例如，5台路由器将会建立10个毗邻关系并发送10条链路状态信息。10台路由器将会建立45个毗邻关系。概括的说，n台路由器将建立n*（n-1）/2个毗邻关系。

表3-3 OSPF网络类型

网络类型	确定性特征	是否选举DR?
广播型多路访问	以太网、令牌环或FDDI	是
非广播型多路访问	帧中继、X.25、SMDS	是
点到点	PPP，HDLC	否
点到多点	由管理员配置	否

避免产生这种开销的方法是选举一台指定路由器（DR designated route）。这台路由器与广播网段中所有的其他路由器建立毗邻关系。DR担当网段的发言人，网段上的所有其他路由器均向DR发送它们的链路状态信息。如前一个例子所列的情况，分别只有5个和10个链路状态需要发送。DR路由器使用组播地址224.0.0.5来向所有其他路由器发送链路状态信息。

尽管通过选举DR能提高效率，但这样依然存在缺点，DR有可能导致单点故障。因此我们再选择另一备份指定路由器（BDR，backup designated route），以便在DR失效时接替其职责。如图3-9所示，DR和BDR接收LSA。为确保DR和BDR均能查看所有路由器发送的链路状态，组播地址224.0.0.6用来表示所有的指定路由器。

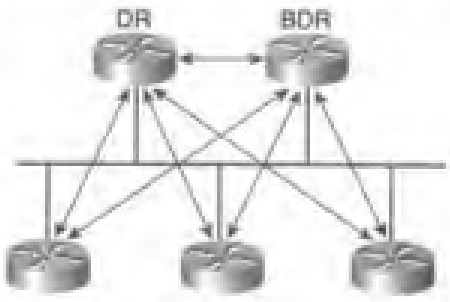


图3-9 DR和BDR接收LSA

因为在点到点型网络中只存在两个节点，所以不需要选举DR和BDR。两台路由器相互间建立全毗邻关系。

3.1.7 OSPF的Hello协议

当路由器在某个接口上启动一个OSPF路由选择进程时，它将发送一个Hello分组，并继续以固定的时间间隔发送Hello分组。管理OSPF的Hello分组交换的规则称为Hello协议（Hello protocol）。

在OSI模型的第3层，Hello分组的寻址地址为组播地址224.0.0.5，该地址代表“所有OSPF路由器”。OSPF路由器使用hello分组来发起新的毗邻关系，并确认邻居路由器仍在运行。缺省情况下，Hello分组在广播型多路访问和点到点型网络上每10秒钟发送一次。在连接NBMA网络的接口上，例如帧中继，Hello分组每30秒钟发送一次。在多路访问型网络中，Hello协议选举一台指定路由器（DR）和一台备份指定路由器（BDR）。

尽管Hello分组比较小，但它含有OSPF分组报头。如图3-10所示，Hello分组的“类型”字所取值为1。

如图3-11所示，Hello分组承载的信息是所有邻居为了形成毗邻关系并交换链路状态信息所必须都认同的。

版本	类型	分组长度
路由器ID		
区域ID		
校验和		身份验证类型
身份验证数据		

图3-10　OSPF分组头

网络掩码		
Hello间隔	可选项	路由器优先级
失效间隔		
指定路由器		
备用指定路由器		
邻居路由器ID		
邻居路由器ID		
如果需要，可以添加额外的邻居路由器ID原码，直到报头的末尾		

图3-11　OSPF的Hello报头

3.1.8　OSPF的运行步骤

OSPF路由器的运行分为下列5个不同的步骤：

1　建立路由器毗邻关系。
2　选举一个DR和BDR（如果需要的话）。
3　发现路由。
4　选择适当的路由。
5　维护路由选择信息。

下面各节将分别对这些步骤作详细的描述。

3.1.9　建立路由器毗邻关系

路由器OSPF运行的第一步是建立路由器毗邻关系（router adjacencies）。图3-12所示的每台路由器都将试图与其处于相同IP网络上的另一台路由器建立毗邻关系。

要与另一台路由器建立毗邻关系，RTB将发送Hello分组，通告它自己的路由器ID。

假定RTB的配置是正确的，它将从接口S0和E0以组播方式向外发送Hello分组。路由器RTA和RTC都应该能收到这些Hello分组，随后它们将把路由器RTB加到自己Hello分组的邻居ID字段中，并

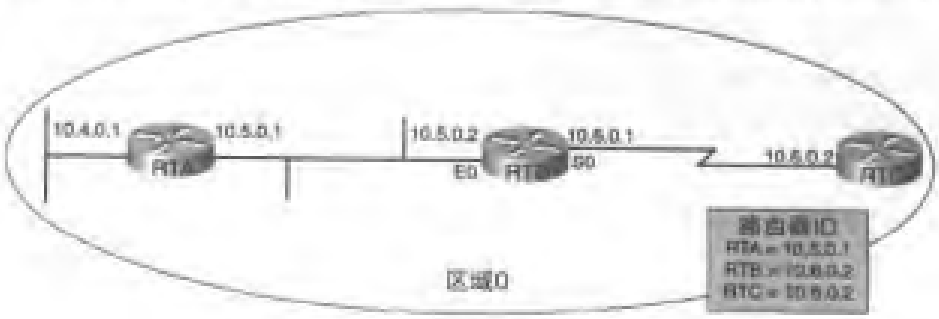


图3-12　OSPF拓扑结构示例

与RTB进入Init状态。

路由器RTB从它的两个邻居那里收到了Hello分组，并在Hello分组的邻居ID字段中看到了它自己的ID号码（10.6.0.1）。RTB宣布它与路由器RTA进入了two-way状态，同时也与路由器RTC进入了two-way状态。

到了这一步，RTB将决定和谁建立毗邻关系，这要根据各接口所连接网络的类型而定。如果是点到点型网络，路由器就与它惟一的链路伙伴建立毗邻关系。如果是多路访问型网络，RTB将进入选举DR和BDR的过程，除非这两个角色都已经建立了（就像在Hello分组头中所通告的）。

如果需要进行选举，OSPF路由器将进入下一节所描述的过程。如果不需要进行选举，路由器就直接进入ExStart状态，如“发现路由”一节所述。

3.1.10 选举DR和BDR

因为多路访问网络可以支持两台以上的路由器，所以OSPF选举一个DR作为所有链路状态更新和LSA的集中点。因为DR的角色非常重要，所以还要选举一个BDR作为DR的备份，一旦DR失效后，BDR可以平滑地接替。图3-13说明了DR和BDR的选举过程。

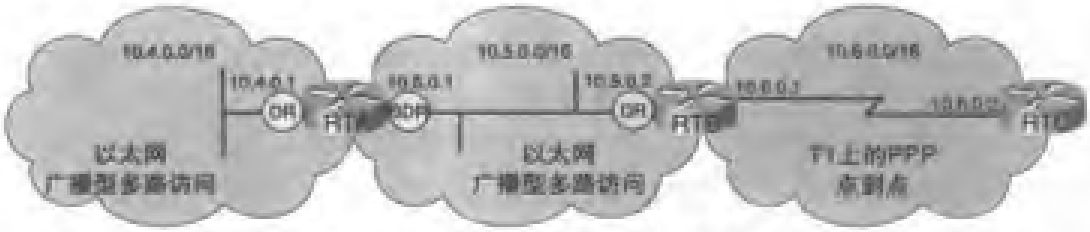


图3-13 OSPF的DR和BDR选举过程

与任何选举一样，DR/BDR的选择过程也是可以操纵的。“选票”是Hello分组，它含有路由器的ID和优先级。在各毗邻路由器之间有最高优先级的路由器将赢得选举并成为DR，有次高优先级的路由器被选举为BDR。在选择了DR和BDR之后，它们会保持它们的角色，直到有一台失效，即使有新的具有更高优先级的路由器在网络上出现也不会改变。Hello分组会将现有DR和BDR的身份通知给新加入的路由器。

OSPF路由器都有相同的缺省优先级值：1。网络管理员可以在任何给定的OSPF接口上设置一个在0到255之间的优先级值。为0的优先级值将阻止路由器在该接口上被选举为DR/BDR。优先级值255将确保路由器至少会与其他路由器并列。当出现并列（优先级值相等）的情况时，将用路由器ID做进一步评判：如果两台路由器有相同的优先级，具有最高路由器ID的路由器将赢得选举。应该用优先级值来操纵，因为每个接口都可以有它惟一的优先级值。你可以简单地配置路由器在一个接口上赢得选举而在另一接口上选举失败。

让我们来看一下DR选举过程是如何影响我们的示例网络的。如图3-16所示，路由器RTB和RTC是在一条点到点链路上通过PPP协议连接起来的，所以不需要在网络10.6.0.0/16上选举DR，因为在该链路上只存在着两台路由器。

因为网络10.4.0.0/16和网络10.5.0.0/16是多路访问型以太网，它们可能会连接着两台以上的路由器。即使只有一台路由器连接到一个多路访问型网段上，也会选举DR，因为可能会陆续有新的路由器连接到该网络。因此，在网络10.4.0.0/16和网络10.5.0.0/16上必须要进行DR选举。

> 注：DR和BDR的选举是以各个网络为基础的。一个OSPF区域可以含有多个IP网络，所以每个区域通常会含有多个DR和BDR。

在我们的实例中，路由器RTA担当双重角色，既是DR又是BDR。因为它是网络10.4.0.0/16中惟

一的路由器，所以RTA选举它自己作为DR。网络10.4.0.0/16是一个多路访问型网络，存在着更多路由器加入进来的可能性，所以要选举一个DR。RTA还是网络10.5.0.0/16选举的亚军，所以它是该网络的BDR。尽管RTB与RTA有相同的优先级值，但它还是被选举为网络10.5.0.0/16的DR，因为它的路由器ID（10.5.0.2）比RTA的ID（10.5.0.1）高。

选举结束并建立起双向通信之后，路由器就准备好与毗邻路由器共享路由选择信息并建立它们的链路状态数据库了。该过程将在下一节中讨论。

3.1.11 发现路由

在一个多路访问型网络上，路由选择信息的交换发生在DR或BDR与网络上的所有其他路由器之间。作为网络10.5.0.0/16上的DR和BDR，RTA和RTB将交换链路状态信息。

在一个点到点或点到多点型网络中的链路伙伴也要参与到交换过程中。这意味着路由器RTB和RTC将共享链路状态数据。

但是谁先开始呢？这个问题在Exstart过程的第一阶段中回答。ExStart状态的目的是要在两台路由器之间建立主/从关系。

在ExStart状态下的DBD分组中宣布路由器ID最高的路由器成为主路由器，如图3-7所示。由主路由器发起链路状态信息的交换，从路由器对主路由器进行响应。RTB将与RTA和RTC进行该过程。

在定义了各自的主、从角色之后，路由器就进入到Exchange状态。如图3-7所示，主路由器带领从路由器进行一系列DBD分组交换，这些DBD分组简单地描述了每台路由器的链路状态数据库。

这些描述包括链路状态类型、通告路由器的地址、链路的成本以及序列号。

路由器通过发送一个LSAck（类型5）分组来确认收到了DBD分组，其中包含所收到DBD分组的序列号。每台路由器将它所收到的DBD中所含有的信息与它已有的信息进行比较。如果DBD通告了一个新的或更新过的链路状态，路由器便通过发送一个针对该项的LSR（类型3）分组进入Loading状态，如图3-2所示。

作为对LSR的回应，路由器用LSU（类型4）分组发送完整的链路状态信息。LSU中包含有LSA。

在Loading状态结束后，路由器就到达full adjacency状态（进入Full状态），如图3-7，RTB已经与路由器RTA和RTC建立了full adjacency关系。

毗邻路由器在建立自己的路由选择表并对通信进行路由选择前必须进入Full状态。到这时，相邻的路由器都应该具有相同的链路状态数据库。

3.1.12 选择最佳路由

当路由器具有了完整的链路状态数据库后，它就准备好要创建自己路由选择表以便能够转发通信了。本章前面已经提到过，OSPF采用成本（cost）度量值来决定到目的地的最佳路径。缺省成本度量值是基于传输介质的带宽。一般来说，成本随着链路速率的增大而降低。例如，RTB的10Mbit/s以太网接口比它的T1串行线路接口的成本低，因为10Mbit/s比1.544Mbit/s快。

为了计算到目的地的最低成本，RTB采用最短路径优先（SPF）算法。简单地讲，SPF算法将本地路由器（称为根（root））到目的地网络之间的所有链路成本相加求和。如果存在多条到目的路径，则优先选用成本最低的路径。图3-14显示了这个过程。缺省情况下，OSPF在路由选择表中最多保存4个等值路由项以进行均衡负载。

有时一条链路（例如串行线路），可能会快速地up和down（称为翻动（flapping））。如果一条翻动的链路导致产生了一系列的LSU，那么接收到这些更新的路由器将不得不重新运行SPF算法来计算新的路由选择表。长时间的翻动可能会严重影响路由器的性能，不断重复进行的SPF计算会导致路由器CPU负担过重。而且，连续不断的更新还可能会使链路状态数据库永远不会收敛。

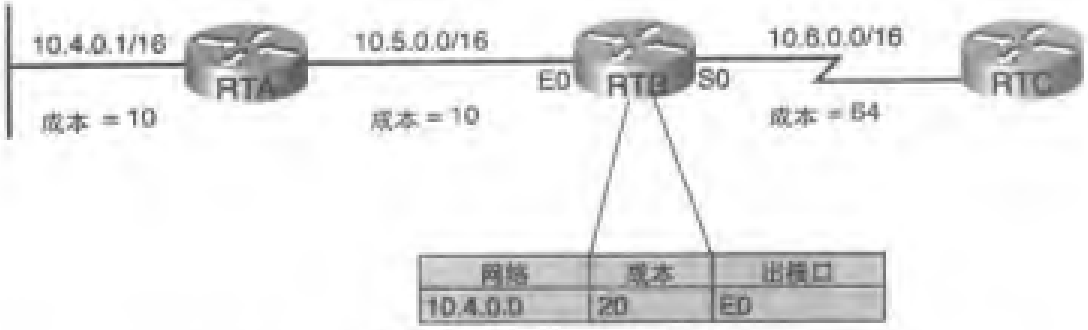


图3-14 OSPF选择最佳路由

要将这个问题的影响减至最小，Cisco IOS使用SPF保持定时器（SPF Wold timer）。每次接收到一个LSU时，路由器在运行SPF算法之前先等待由保持定时器所规定的一段时间。timers-spf命令让我们可以调整该值，缺省为10秒。

在RTB用SPF算法选择最佳路由后，它就会进入OSPF运行的最后阶段。

3.1.13 维护路由信息

当路由器RTB将路由添加到路由选择表中之后，它还必须不断地维护路由选择信息。当链路状态发生变化时，OSPF路由器通过泛洪过程将这一变化通知给网络中的其他路由器。Hello协议的失效时间间隔（dead interval）提供了一种判断链路伙伴发生故障的简单机制。如果RTB未从RTA收到消息的持续时间超过了失效时间间隔，RTB就宣布自己到RTA链路失效。

RTB随后将发送一个含有该新链路状态信息的LSU：

- 在点到点型网络上，不存在DR或BDR。新链路状态信息被发送到组播地址224.0.0.5。所有的OSPF路由器都会侦听发往该地址的分组。
- 在多路访问型网络中，存在着DR和BDR，它们与网络上的所有其他OSPF路由器维持着毗邻关系。当DR或BDR需要发送一个链路状态更新时，它会将该更新发送到组播地址224.0.0.5（所有OSPF路由器）。而在该多路访问型网络中的所有其他路由器都只与DR和BDR建立毗邻关系，因此它们只将LSU发送给DR和BDR。出于这个原因，DR和BDR有它们自己的组播地址：224.0.0.6。非DR/BDR路由器将它们的LSU发送到地址224.0.0.6，即所有的OSPF DR（和BDR）。

在图3-15中，路由器注意到链路状态的变化，并组播传送含有已更新LSA条目的LSU分组到224.0.0.6，该地址是所有的OSPF的DR（和BDR）的地址。

当DR接收并确认了发送到组播地址224.0.0.6的LSU后，它用组播地址224.0.0.5将该LSU泛洪给网络上的所有OSPF路由器。每台路由器用一个LSAck分组确认收到了LSU。

如果一台OSPF路由器还连接着另外的网络，它会通过将该LSU转发给那个多路访问网络上的DR将LSU泛洪到该网络。或者如果是一个点到点型网络，它就转发给毗邻路由器。DR随后会将该LSU以组播方式泛洪给其网络中的其他OSPF路由器。

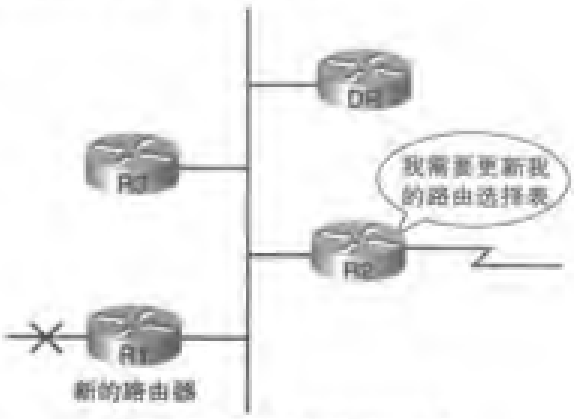


图3-15 OSPF链路状态信息

在收到一个含有新信息的LSU之后，OSPF路由器将更新它的链路状态数据库，它对新的信息运行SPF算法来重新计算路由选择表。在SPF保持定时器超时后，路由器就切换到新的路由选择表。

如果一条路由已经存在于路由器中，当路由器对新信息运行SPF算法时该旧路由仍会继续使用。但如果SPF算法是在计算一条新的路由，那么路由器在SPF计算完毕之前是不会使用它的。

需要注意的是，即使链路状态没有发生变化，OSPF路由选择信息也周期性更新。每个LSA条目有自己的年龄定时器（agetimer）。缺省的定时器值是30分钟。当一条LSA条目过期后，该条目的发源路由器向网络发送LSU以确认这条链路仍然是活动的。

3.2　单区域OSPF配置

为了配置OSPF，你必须在路由器上启动OSPF协议，配置路由器的网络地址和区域信息，如图3-16的步骤：

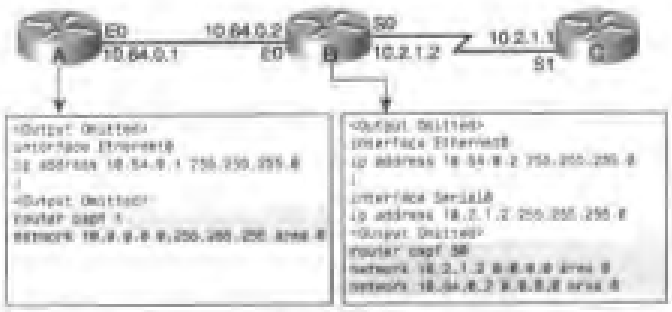


图3-16　基本OSPF配置

步骤1　用以下语法在路由器启动OSPF协议：

```
router(config)#router ospf process-id
```

进程ID是指本地路由器的一个进程号码。这个进程ID用于区分同一台路由器上多个OSPF进程。进程ID的取值范围是1~65,535之间。不必从1开始。很多网络管理员在整个自治系统（AS）保持相同的进程ID。你可以在一台路由器上运行多个OSPF进程。但是并不推荐这种做法，因为它会产生多个数据库，这会额外增加路由器的开销。

步骤2　用以下语法在路由器上标识IP网络：

```
router(config-router)#network address wildcard-mask area area-id
```

对于每个网络，你必须标识其所属的区域。关键字*address*可以是网络地址、子网地址或者接口地址。路由器会通过比较通配符来对地址进行解释。因为OSPF支持CIDR和VLSM（RIPv1和IGRP则不支持），所以通配符是必须有的。参数*area-id*是必须的，即使在同一个区域内配置OSPF。同样注意，多个IP网络可以属于同一区域。

设计和实现大型OSPF网络需要从单一区域开始配置OSPF路由选择协议。OSPF配置的方法与其他路由协议选择相似。不同的地方是需要在network语句中输入被发布的网络。这是因为OSPF是链路状态协议。

OSPF的成功运行需要一个进程ID和路由器ID。路由器ID来自于一个活动的接口。如果这个接口失效了，OSPF进程就无法继续。为了保证OSPF的稳定性，我们配置环回地址（loop back address）作为路由器的ID。另外，在广播型多路访问网络中，需要选举指定路由器（DR）。这台路由器代表网络中其他路由器向网段中传播链路状态信息。你可能希望确保特定的路由器被选为DR。给这样路由器配置高的优先级就可以确保它选举成为DR。

3.2.1　配置环回地址

当OSPF进程启动时，Cisco IOS使用最高的本地IP地址作为其OSPF路由器的ID，但如果为环路接口配置了IP地址，路由器将会使用该环路接口地址，而不管它的值大小。配置环回接口地址的句法如下：

```
router(config)#interface loopback number
router(config-if)#ip address ip-address subnet-mask
```

使用环回地址作为路由器的ID可以确保稳定性，因为该接口不会出现链路失效的情况。要取代最高的接口IP地址，该环回接口必须在OSPF进程开始之前配置。

在基于OSPF的网络中，我们建议所有的关键路由器都使用环回地址。为了避免路由选择问题，在配置环回地址的时候最好配置一个32bit的子网掩码。如例3-1所示。

例3-1 用主机掩码配置环回地址

```
router(config)#interface loopback0
router(config-if)#ip address 192.168.1.1 255.255.255.255
```

32比特的掩码通常称为主机掩码（host mask），因为它是指定一个主机，而不是一个网络或者子网。

注： 为了防止伪路由的传播，OSPF通常把环回地址用一个32位的掩码的主机路由（host route）进行通告。

3.2.2 修改OSPF路由器优先级

网络管理员可以通过修改缺省值为1的OSPF路由器优先级来操纵DR/BDR的选举。优先级为0的路由器将不会被选为DR/BDR。每个OSPF的接口都可以宣告一个不同的优先级值。我们可以使用ip ospf priority命令来配置优先级（数字范围从0~255），其语法如下：

```
router(config-if)#ip ospf priority number
```

要将路由器E0接口的优先级值设置为0（以使它不能赢得网络上的DR/BDR选举），可以使用例3-2显示的命令。

例3-2 设置e0接口的优先级

```
RTB(config)#interface e0
RTB(config-if)#ip ospf priority 0
```

为了让优先级值在选举中能起作用，必须在选举开始前就把它配置好，可以用另一条命令show ip ospf来显示接口的优先级和其他关键信息，如例3-3所示。例子中的输出内容说明了哪些路由器被选为DR和BDR、网络类型（在这个例子中是广播型多路访问网络）、链路成本（10）和指定接口的定时器时间间隔。所配置的定时器时间间隔包括Hello时间（10秒）、失效（Dead）时间（40秒）、等待（Wait）时间（40秒）和重传（retransmit）时间（5秒）。OSPF定时器会在下面一节介绍。

优先级越高，路由器就越有可能被选举成为DR。输入ip ospf priority命令来修改参与OSPF的接口的优先级值。例3-3中，show ip ospf interface命令显示接口的优先级值和其他关键信息。

例3-3 使用命令show ip ospf interface

```
Routers#show ip ospf interface e0

Ethernet0 is up, line protocol is up
    Internet Address 10.5.0.2, Area 0
    Process ID 1, Router ID 10.6.0.1, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State Dr, Priority 1
    Designated Router (ID) 10.6.0.2, Interface address 10.6.0.1
    Backup Designated router (ID) 10.5.0.1, Interface address 10.5.0.1
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
        Hello due in 00:00:03
    Index 1/1, flood queue length 0
    Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.5.0.1 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```



实验活动　配置OSPF的路由进程

在本实验中，你可以为一个包含两台路由器的OSPF区域制定IP寻址方案。然后配置和验证OSPF路由选择。



实验活动　配置路由器的环回地址。

在本实验中，你将观察多路访问型网络中DR和BDR的选举过程。配置环回地址，以增加OSPF的稳定性。指定每个OSPF接口的优先级，迫使特定的路由器被选为DR。

3.2.3　修改OSPF成本的量值

OSPF使用成本（cost）作为决定最佳路由的度量值（Metric）。Cisco的IOS基于接口带宽（bandwidth）来自动确定链路成本。成本用以下的公式计算：

10^8/带宽

要让OSPF能够正确地计算路由，连接到同一条链路上的所有接口必须对链路使用相同的成本。可以对成本进行变更以影响OSPF成本计算的结果。最常见的要求成本改变的情况发生在一个存在多厂商设备的路由选择环境中，这是因为要与其他厂家的成本值相等。

基于所使用的技术，链路都有缺省的成本值。管理员可以修改一条链路的OSPF成本值。表3-4列出了缺省链路成本。

表3-4　OSPF缺省成本

介质	成本
56-kbit/s串行链路	1,785
T1（1.544Mbit/s串行链路）	64
E1（2.048Mbit/s串行链路）	48
10Mbit/s以太网	10
16Mbit/s令牌环	6
100Mbit/s快速以太网，FDDI	1

链路成本的设置可以使用下列接口配置命令：

```
Router(config-if)#ip ospf cost number
```

number的取值可以在1~65，535之间变化。另一个影响OSPF链路成本的方法是在接口上设置带宽值，如例3-4。成本值越小，链路就越好。

例3-4　设置OSPF带宽

```
Router(config)# interface serial 0/0
Router(config-if)# bandwidth 64
```

串行接口的缺省带宽取值是1544。



实验活动 修改OSPF的成本度量值

在本实验中，需要配置和验证OSPF的路由选择。然后在接口上修改OSPF的成本度量值。

3.2.4 配置OSPF身份验证

如果确保路由选择信息来自特定的源，网络的安全性就得到加强。OSPF允许路由器之间互相进行身份验证。

在缺省的情况下，路由器相信从一台路由器发送过来的路由选择信息。路由器也相信这些信息没有被修改过。为了保证这种信任，在一定区域内的路由器可以配置成互相验证。

身份验证也是针对接口的配置。在路由器中各个OSPF的接口上可以指定不同的身份验证密钥，作为同一区域OSPF路由器之间的密码。下面就是配置OSPF身份的语法：

```
router(config-if)#ip ospf authentication-key password
```

配置了密码后，可以用下面的语法在整个区域范围内启动身份验证，该命令需要在所有参与的路由器点键入：

```
router(config-router)#area number authentication [message-digest]
```

尽管关键字message-digest是一个可选项，但是我们推荐使用这条命令时，总是使用该关键字。因为在缺省的情况下，认证密码是明文方式传送的，用数据包嗅探器（packet sniffer）就可以轻易地捕获OSPF的分组，并解码出没有加密的密码。如果使用关键字message-digest，路由器则只是在链路上传送密码的消息摘要或哈希值，而不传送密码本身。除非接收的路由器配置了正确的验证密钥，否则任何人都无法明白消息摘要的含意。

如果选择使用message-digest身份验证，验证密钥就不会被使用。作为替代，你必须在路由器OSPF的接口上配置一个消息摘要密钥。命令语法如下：

```
router(config-if)#ip ospf message-digest-key key-id md5[encryption-type]password
```

MD5验证会产生一个消息摘要。这是一种基于密钥和分组内容杂乱数据。接收信息的路由器使用共享parsword值重新计算分组的摘要。如果摘要相匹配，路由器就会相信分组源，并认为分组的内容没有被修改过。encryption-type用于标识所使用的身份验证类型。对于消息摘要验证，包含keyID和消息摘要的验证数据库字段会添加到分组中。消息摘要就像一个水印那样不能伪造。



实验活动 配置OSPF认证

在本实验中，通过在OSPF区域中配置OSPF验证来提高OSPF网络的安全性。

3.2.5 配置OSPF定时器

在一些情况下，必须加快链路状态失效的报告速度。在OSPF中，这可以通过配置OSPF实时器实现。

由于OSPF的路由器需要交换信息，所以它们的必须有相同Hello时间间隔和失效时间间隔。在缺省情况下，失效时间间隔是Hello时间间隔的4倍。

这意味着在路由器宣布失效前有4次机会发送Hello分组。

广播型的OSPF网络中，缺省的Hello时间间隔是10秒，缺省的失效时间间隔是40秒。在非广播型的网络中，缺省的Hello时间间隔是30秒，缺省的失效时间间隔是120秒。这些缺省值可以使OSPF有效的运作，所以一般不用更改。

网络管理员不能任意地选择定时器的值。改变定时器的时间可以提高OSPF网络性能，在改动这些定时器时间之前需要提供可以改善OSPF网络性能的理由，这些定时器的时间值必须与其他路由器的定时器值相匹配。

要在接口类型配置Hello时间间隔和失效时间间隔，使用如下的语法：

```
Router(config-if)#ip ospf hello-interval seconds
Router(config-if)#ip ospf dead-interval seconds
```

实验活动　配置OSPF定时器

在本实验中，通过配置OSPF定时器加快链路状态失效的报告速度。

3.3　在NBMA中配置OSPF

另一种OSPF网络，非广播型多路访问（NBMA，nonbroadcost multiaccess）包括可能两个以上的节点，并且尝试选举DR和BDR。常用的NBMA实现包括帧中继、X.25和交换式多兆比数据业务（SMDS）。NBMA网路遵循OSI模型第2层中过滤广播和组播的规则。图3-17汇总了OSPF网络的类型。

NBMA的网络使用OSPF会产生一些问题，例如组播的Hello分组交换。在图3-18的例子中RTA、RTB和RTC都属于同一IP子网，它们尝试选出DR和BDR。然而，如果这些路由器在网络中互相不能收到组播Hello分组，它们就无法做出有效的选举。在没有管理员介入的情况下，就会产生一个奇怪的选举。在RTA看来，RTC是没有参与选举的。同样的，RTC在选举的过程中也会忽略了RTA。这种糟糕的选举方法会导致作为中心的路由器RTB无法成为DR。

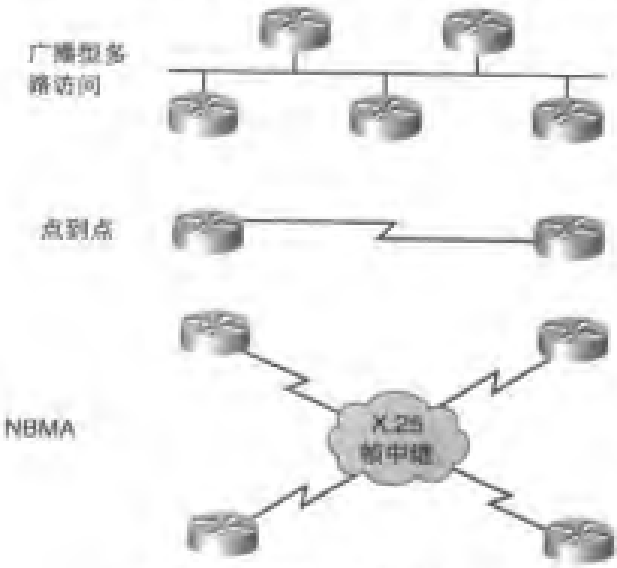


图3-17　OSPF网络类型

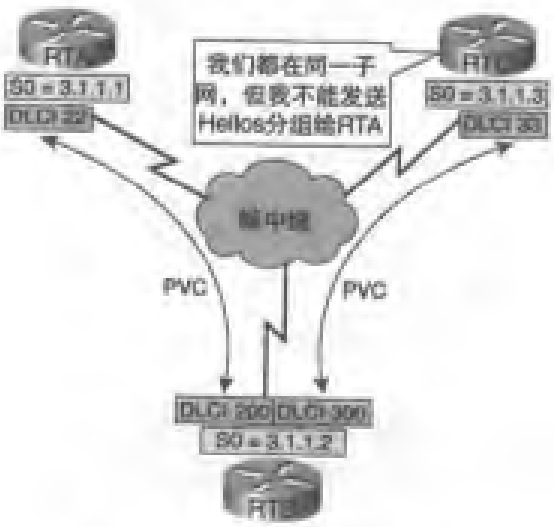


图3-18　NBMA网络中OSPF邻居状态

Cisco的IOS提供到了一些配置OSPF的选项以克服NBMA的局限性，包括neighbor命令、点到点子接口（point-to-point subinterfaces）和点到多点的配置。具体使用哪种解决方案依赖于你的NMBA网络拓扑结构。

在为帧中继网络（或者X.25网络）选择一种OSPF配置策略前，必须理解各种NBMA拓扑。基本来说，对于帧中继网络，有两种可能的物理拓扑结构：

- 全网状结构。
- 部分网状结构包含轴辐型拓扑（hub-and-spoke topology）。

图3-19显示了帧中继的拓扑。

下列各节将描述在全网状和部分网状帧中继网络中如何配置OSPF协议。

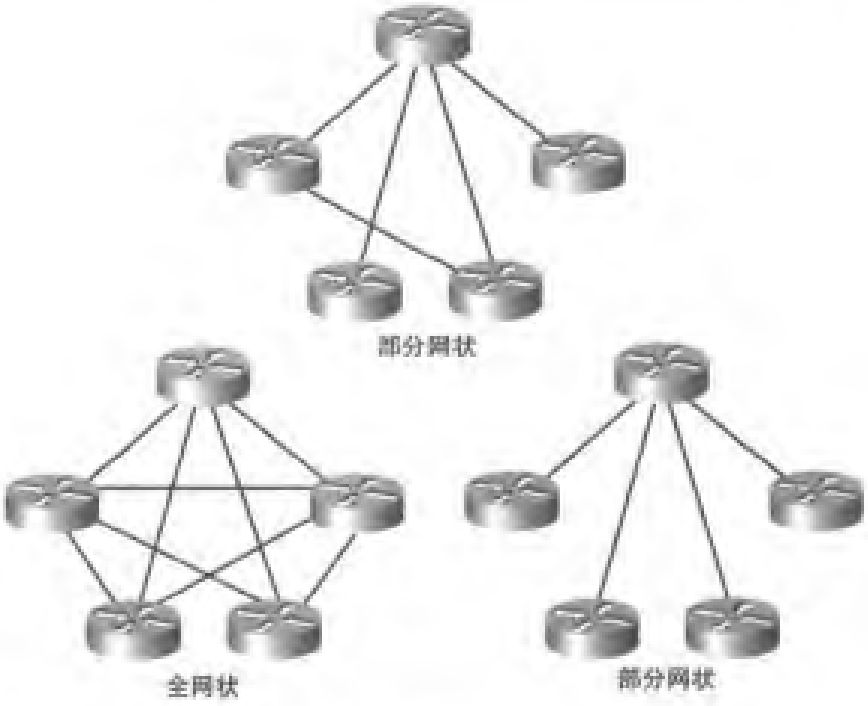


图3-19 OSPF帧中继拓扑结构

3.3.1 全网状帧中继

由于帧中继技术可以在单一接口上支持多个逻辑连接，使其为一种廉价和灵活的广域网链路选择，所以很多组织都布署了帧中继技术。全网状结构利用了帧中继可以在一个串行接口中支持多条永久的虚电路（PVC）的能力。在全网状拓扑结构中，每台路由器都有一条PVC线路连接到其他的路由器。如图3-20所示。

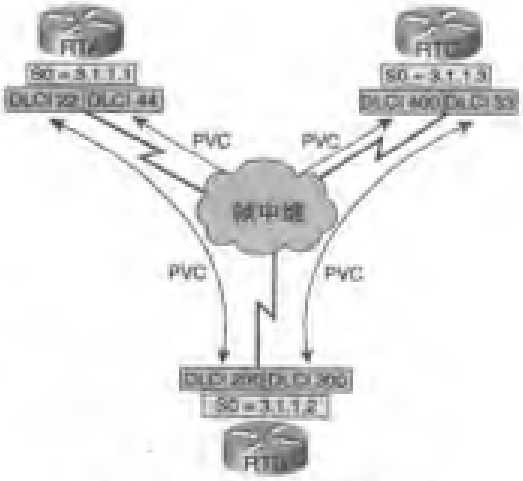


图3-20 OSPF全网状帧中继

要使得OSPF能在一个不支持广播的多路访问全网状拓扑结构中正常工作，必须在每台路由器上手工输入OSPF的邻居路由器地址，每次一个。OSPF的命令neighbor用于告诉路由器其邻居的IP地址。因此，它可以在不使用组播的情况下与邻居交换路由选择信息。例3-5说明了命令neighbor如何使用。

例3-5 使用OSPF neighbor命令

```
RTA(config)#router ospf 1
RTA(config-router)#network 3.1.1.0 0.0.0.255 area 0
RTA(config-router)#neighbor 3.1.1.2
RTA(config-router)#neighbor 3.1.1.3
```

指定每台路由器的邻居并不是在这种类型的环境下使OSPF正常工作的惟一选择。下面一节将解释如何配置子接口，以消除对neighbor命令的依赖。

配置子接口以建立点到点网络

IOS子接口功能性可用于将多路访问型网络分隔成多个点到点型网络构成的集合。

图3-21，每条PVC线路分配了不同的IP子网。

OSPF自动将这种配置看作是点到点型网络，而不是NMBA，即使是在这些接口上配置了帧中继。回忆一下，OSPF点到点型网络不需要选举DR。帧中继路由器使用反向ARP（Inverse ARP）或帧中继映射（Frame Relay map）来获得链路伙伴的IP地址，以交换路由选择信息。

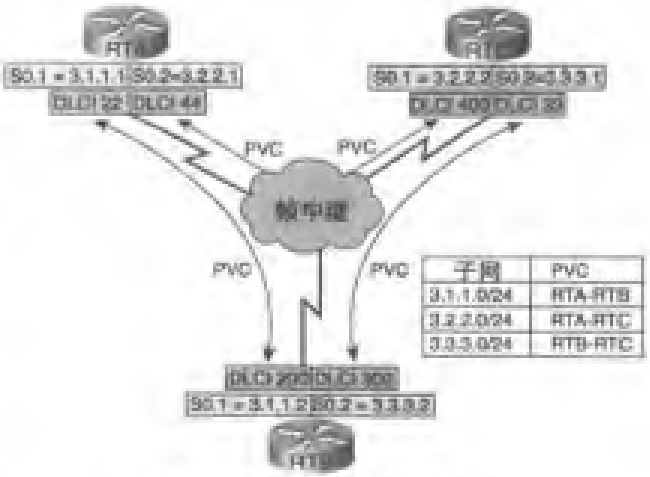


图3-21　OSPF 全网状子接口

全网状拓扑有很多好处，包括最大限度的容错性能。不幸的是，全网状拓扑结构价格昂贵，因为每条PVC线路都需要向运营商租用。一个组织需要租用45条PVC线路用于支持10台路由器的全网状结构。如果用子接口创建点到点型网络，那么还需要分配和管理45个IP子网，这样也会增加费用。

3.3.2　部分网状帧中继

由于全网状互连拓扑结构的成本太高，许多机构都使用部分网状结构代替。部分网状结构是由至少一台路由器维持对其他路由器的多个连接，但不是每台路由器都有到所有其他路由器的直接连接。最经济的部分网状拓扑结构是轴辐型（hub-and-spoke）拓扑结构。在这种结构中，一台中心路由器连接着其他的多台分支路由器。

这种星型拓扑结构虽然是一种经济的广域网解决方法，但它同时会引起单点故障的风险（中心路由器）。组织之所以使用帧中继技术是因为它成本低廉，而并不是它的容错能力强。因为租借的专线（非帧中继链路）通常用来承载任务关键型数据。所以一个经济的帧中继技术对于普通应用来说还是很有意义的。

不幸的是，在全网状拓扑结构中工作得很好的命令neighbor在轴辐型拓扑结构中不能正确工作。在图3-22中的中心路由器可以看到所有的分支路由器，并用neighbor命令将路由选择信息发送给它们。但分支路由器只能向中心路由器发送Hello分组。

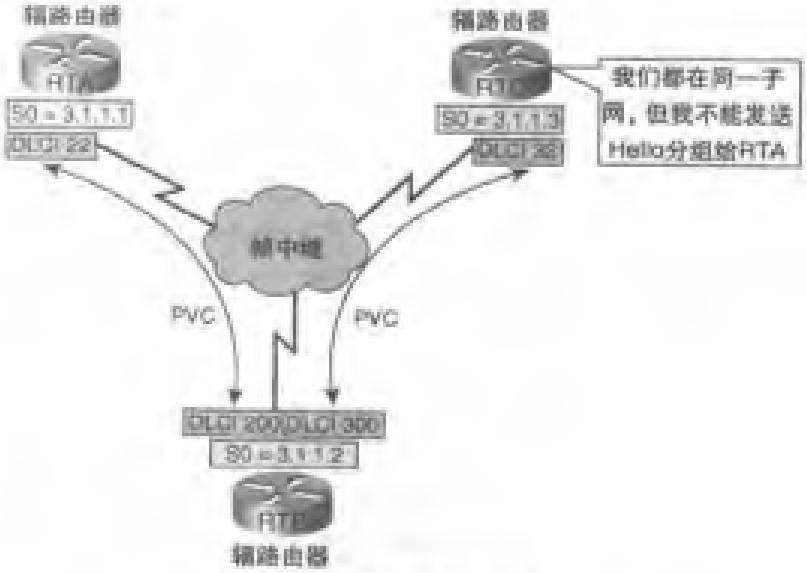


图3-22　OSPF轴辐型拓扑

DR/BDR的选举会进行，但只有中心路由器能看到所有的候选路由器。要让这种OSPF网络能够正常工作，必须由中心路由器担当DR。因此，应该在所有分支路由器上将OSPF接口的优先级设置为0。回忆一下，在一个网络中，优先级为0的路由器是不可能被选为DR或者BDR的。

第二种处理这种拓扑结构的方法是把该网络分成多个点到点连接，以彻底避免DR/BDR问题。如图3-23所示，点到点网络不会选举DR/BDR。

尽管它们使OSPF的配置变得比较直接，但是这种点到点网络用于轴辐型结构中时还是有很大的缺点，必须为每条链路分配一个子网，这样就会导致广域网地址复杂和难以管理。虽然广域网寻址

问题可以通过使用无编号IP地址（IP unnumbered）功能来予以避免，但很多组织的广域网管理策略不允许使用该特性。有没有对点到点型配置的可行代替选择呢？幸运的是，Cisco IOS提供了一种相对较新的方法：一个轴辐型物理拓扑可以被手工配置为一个点到多点网络类型，如下面一节所述。

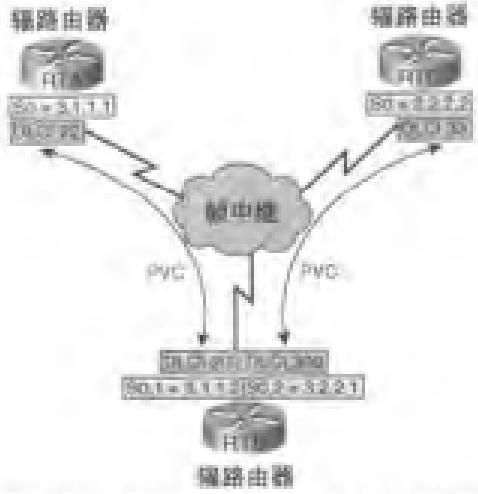


图3-23 OSPF轴辐型拓扑的点到点配置

3.3.3 点对多点型OSPF

在一个点到多点型网络中，一台辐路由器被直接连接到多台辐路由器，但所有广域网接口的地址都在同一个IP子网中，如图3-24所示。

我们在前面已经看过如图3-24所示的逻辑拓扑结构，OSPF在该NBMA网络类型中不能正常运行。通过手工将OSPF网络改变成为点到多点的网络类型，就可以让该逻辑拓扑结构正常工作。路由器RTA和RTC之间的路由选择将通过RTB完成，它有到RTA和ETC的虚电路。注意：当使用该特性时，不需要手工配置邻居，反向ARP（Inverse ARP）将会发现它们。

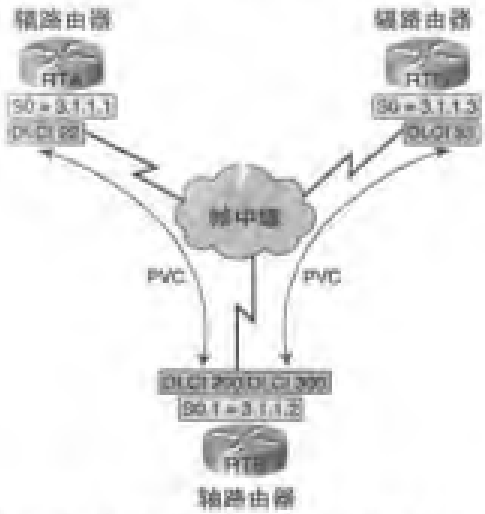


图3-24 OSPF轴辐型拓扑的点到多点配置

点到多点网络有以下特性：

- 毗邻关系在所有相邻路由器之间被建立。在一个点到多点型网络中没有DR/BDR。不会为点到多点网络产生网络LSA。不需要为点到多点型接口或点到多点型网络邻居配置路由器优先级。
- 当发出一个路由器LSA时，点到多点型接口被作为点到点的链路的集合报告给该接口的所有邻居，还通过单个的存根链路（stub link）通告接口的IP地址（成本为0）。

当从一个非广播型接口向外泛洪时，LSU或LSAck分组必须被复制送到该接口的每个邻居。

要配置点到多点网络类型，必须用下面的命令语法来取代所检测到的OSPF网络类型：

```
router(config-if)#ip ospf network point-to-multipoint
```

还应该使用“frame-relay map ip”命令来配置该接口，其命令语法如下：

```
router(config-if)#frame-relay map ip address dlci broadcast
```

关键字“broadcast”允许路由器通过指定的DLCI号将广播分组发送给所映射的邻居。

在一个点到多点型网络配置中，OSPF将非广播型网络上所有的路由器到路由器连接都作为点到点链接处理。不需要为该网络选举DR。可以使用“neighbor”命令来手动指定邻居，也可以通过用反向ARP来动态发现。

简而言之，点到多点型OSPF配置可以在没有管理复杂度的情况下提供高效的运行方式。

3.4 传播缺省路由

为了访问一些不在路由选择表的网络，必须在边界路由器上配置缺省网点。这些缺省路由信息也会被传播到OSPF区域中的所有其他路由器。

在OSPF路由选择中，域路由选择表使得在该域中的所有网络都可以到达。OSPF域的用户可能

需要访问域外的网络（如Internet）。

缺省路由使得路由器能将包含未知地址的分组发送给路由选择表中可能有该地址的路由器。

配置缺省路由的方法是建立一个“最后的网关（Gateway of Last Resort）”。静态路由的配置语法是使用网络0.0.0.0和子网掩码0.0.0.0：

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [interface | next-hop address]
```

根据“通过将分组的目的地址与子网掩码进行与运算以确定网点”的规则，上述路由能匹配任何的网络地址。要在OSPF区域向所有的路由器传播缺省路由，应该使用以下的配置语句：

```
Router(config-router)#default-information originate
```

在OSPF区域的所有路由器都会学习到边界路由器提供的缺省路由，而且这条缺省路由的接口是活动的。



实验活动　在OSPF域中传播缺省路由

在这个实验中，要求在OSPF网络中传播缺省路由，这样，在OSPF区域的所有网络都可以连接到外部网络。

3.5　常见OSPF配置问题

为了更有效、快速和成功地使用OSPF，网络管理员需要了解常见的配置问题。OSPF路由选择协议在单一区域中不能成功使用有许多原因。一台OSPF路由器必须和其他OSPF路由器建立一邻居（neighbor）或者毗邻（adjacency）关系，以便交换路由选择信息。不能建立邻居关系的情况，可能由下面的原因引起：

- Hello分组没有在邻居路由器之间发送。
- Hello时间间隔和失效时间间隔不相同。
- 接口的网络类型不同。
- 身份验证口令或密钥不同。

在OSPF中，路由选择是十分重要的，要确保以下几点：

- 所有接口要有正确地址和子网掩码。
- network area语句有正确的通配符掩码（wildcast masks）。
- network area语句将接口放入正确的区域。

3.6　验证OSPF配置

为了验证OSPF的配置，可以用下面的show命令查看。表3-5列出了这些命令。

表3-5　OSPF操作和统计命令

命令	描述
show ip protocol	显示路由器的定时器、过滤器、度量值，网络和其他信息等参数
show ip route	显示路由器通过学习获得的路由和这些路由是如何学习回来的。这是确定本地路由器和其他网络之间连接的最好方法之一
show ip ospf interface	检验已经配置在目标的区域中的接口。如果没有指定环回地址，接口地址就会被认为是路由器ID。它也显示定时器的时间间隔，包括Hello分组的时间间隔，还能显示所有毗邻关系
show ip ospf	显示最短路径优先算法（SPF）执行的次数。它也显示拓扑结构没有发生改变时，链路状态的更新时间间隔
show ip ospf neighbor detail	显示邻居路由器的详细信息，包括它们的优先级和状态（例如init、exstart或者full）

续表

命令	描述
show ip ospf database	显示路由器维护的拓扑数据库的内容。这条命令可以显示路由器ID和OSPF的进程ID。用这条命令的一些关键字可以显示数据库的类型。可以访问www.cisco.com查看关于这些关键字的详细内容
clear ip route*	清除整个IP路由选择表
clear ip route *a.b.c.d*	清除路由选择表中关于a.b.c.d网络的路由
debug ip ospf	调试OSPF

3.7 总结

本章讨论了以下的内容：

• 在单区域中使用OSPF路由选择协议适合于小型网络。

• OSPF协议的配置与其他路由选择协议相似。不同的是它是一种链路状态协议。

• OSPF需要一个进程ID和一个路由器ID。

• 通过配置一个环回地址可以确保OSPF的稳定。

• 在广播型多路访问网络中，要选举指定路由器（DR）。DR代表其他路由器传播链路状态给网段。在接口上配置OSPF优先级可以确保选定的路由器被选为DR。

• 网络管理员可以通过控制链路成本和定时器来影响链路状态的通告，也可以通过配置路由器身份验证来增加安全性。

• 常见的一些OSPF配置问题和能验证OSPF的配置的一些命令。

• OSPF链路状态路由选择协议不同于距离矢量路由协议，例如RIP。OSPF的路由器基于网络拓扑结构的完整信息来决定最佳路径。OSPF决定最佳路径的度量值是成本（cost），它是基于链路的速度。配合分级设计，OSPF适用于大型网络。

• 最短路径算法用于决定最佳的无环路径，即到达链路或网络成本最低的路径。因为OSPF路由器需要一个完整网络拓扑，并且SPF算法很复杂，所以需要内存更多的更强大的路由器。

• 最短路径优先算法（SPF）用于点到点网络的连接。为了在目前各种网络中实现OSPF，OSPF必须知道到它运行的网络的类型。为了能在多路访问型网络中高效地运行，选举DR作为链路状态信息交换的中心是十分必要的，选举BDR是为了可靠。

• OSPF使路由器之间在交换路由选择信息前建立邻居关系。OSPF的Hello协议用于在毗邻路由器（adjacent routers）间建立邻居关系。

为了补充本章学习过的内容，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

3.8　关键术语

骨干（*backbone*）　网络中起主要传输数据作用的路径，通常是其他网络的源头或者目的。

备份指定路由器（*backup designated router，BDR*）　用作指定路由器的备份。

指定路由器（*designated router，DR*）　为多路访问型网络产生LSA的一台OSPF路由器，它在OSPF的运行中负有特殊的责任。每个至少连接两台路由器的多路访问型OSPF网络中有一台被OSPF的Hello协议选举为指定路由器。指定路由器可以减少在一个多路访问型网络上所需的毗邻关系数量，这继而又能减少路由选择协议的通信量并且减少拓扑结构数据库的大小。

泛洪（*flooding*）　除已经接收信息的端口外，向其他所有端口发送信息的过程。

Hello协议（*Hello protocol*）　OSPF系统用于建立和维护邻居关系所用的协议。

环回（*loopback*）　127.0.0.1地址被指定为机器软件的环回接口地址。环回接口与硬件无关，它不需要物理的连接。

链路状态通告（*link-state advertisement，LSA*）　链路状态型路由选择协议所用的一种广播分组。它含有与邻居和路径成本有关的信息。LSA被接收方路由器用于维护它们的路由选择表。有时也称为链路状态分组（LSP, link-state packet）。

多路访问网络（*multi-access network*）　允许多台设备同时连接和通信的一种网络。

点到点（*point-to-point*）　一个接收者和一个发送者之间发生的通信。

进程ID（*process identifier，process ID*）　在OSPF配置过程中指定的一个数字，用于标识路由器上每个OSPF进程。

路由器ID（*router identifier，router ID*）　用于标识参与OSPF路由器的IP地址。可以用具有最高IP地址的活动接口地址或者环回地址作为路由器ID。

sniffer　一种用于监控网络上传送数据的程序和设备。

最短路径优先算法（*shortest path first，algorithm SPF algorithm*）　迭代路径的长度，以确定最短路径生成树的路由选择算法。通常在链路状态路由选择协议中使用。亦称作Dijkstra算法。

3.9 复习题

1. 在DR和BDR选举出来后，OSPF网络处于哪种状态？
   A. ExStart
   B. Full
   C. Loading
   D. Exchange
2. 哪种类型的OSPF分组可以建立和维持邻居路由器的比邻关系？
   A. 链路状态请求
   B. 链路状态确认
   C. Hello分组
   D. 数据库描述
3. OSPF缺省的成本度量值是基于下列哪一项？
   A. 延时
   B. 带宽
   C. 效率
   D. 网络流量
4. 下面哪个组播地址代表所有的OSPF路由器？
   A. 224.0.0.6
   B. 224.0.0.1
   C. 224.0.0.4
   D. 224.0.0.5
5. 下面哪条命令可以改变接口的OSPF优先级？
   A. ip priority number ospf
   B. ip ospf priority number
   C. ospf priority number
   D. set priority ospf number
6. 下面哪个组播地址用于将LSU发送给所有DR/BDR路由器？
   A. 224.0.0.6
   B. 224.0.0.1
   C. 224.0.0.4
   D. 224.0.0.5
7. 下列哪种特性是NBMA网络共有的？
   A. 只支持两台路由器
   B. 支持两台以上的路由器
   C. 不选举DR
   D. 完全支持广播和组播分组
8. 下面哪条命令允许路由器交换路由选择更新而且不使用组播？
   A. ip ospf neighbor
   B. ospf neighbor
   C. neighbor
   D. ip neighbor
9. 下面哪条命令能显示路由器所知道的路由，以及它们各自是如何学到的？

A. show ip protocol
B. show ip route
C. show ip ospf
D. show ip ospf neighbor detail



第4章　增强内部网关路由选择协议

目标

学习完本章后，你将能够：

- 描述EIGRP特征和基本原理。
- 描述DUAL。
- 列出EIGRP的数据结构。
- 配置EIGRP。
- 对EIGRP进行验证和故障排除。

在本章中，你将学习Cisco的专有协议——增强内部网关路由选择协议（EIGRP）。你将学习如何配置、验证EIGRP以及进行故障排除，并对EIGRP与内部网关路由选择协议（IGRP）进行比较。另外，你将了解EIGRP的关键概念、技术及数据结构。在这些概念性的介绍之后，你将学习EIGRP收敛、以及EIGRP中称为扩散更新算法（DUAL，Diffusing Update Algorithm）的先进路由选择算法的基本工作方式。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图，光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

4.1　EIGRP概述

EIGRP是基于IGRP的Cisco专有路由选择协议。

IGRP是一种有类别路由选择协议，而与之不同，EIGRP支持无类别域间路由选择（CIDR），它允许网络设计者利用CIDR和可变长子网掩码（VLSM）将地址空间最大化利用。与IGRP相比，EIGRP有更快的收敛时间、更强的可扩展性以及更高级的路由环路处理方法。

此外，EIGRP能够取代Novell的路由选择信息协议（RIP）和AppleTalk的路由选择表维护协议（RTMP Routing Table Maintenance Protocol），可以使IPX和AppleTalk网络更高效地运行。

EIGRP经常被描述为一种提供最好的距离矢量和链路状态算法的混合路由选择协议。从技术上讲，EIGRP是依赖于那些通常与链路状态协议相关连特性的一种高级的距离矢量路由选择协议。OSPF的一些最好的特性，例如部分更新和邻居发现，被类似地使用在EIGRP。然而，EIGRP比OSPF更容易配置。

对于主要是基于Cisco路由器所建设的大型的、多协议网络来说，EIGRP是一个理想的选择。

4.1.1　EIGRP规程与技术

Cisco于1994年发布了EIGRP，作为其专有的距离矢量路由选择协议—IGRP的一种可扩展的、改进的版本。EIGRP与IGRP使用相同的距离矢量技术，并且下层的距离信息保持一致。

在EIGRP中，收敛特性和运行效率都有了明显的改善。这就在保持现有IGRP投资的同时提供了一种改进的体系结构。

1　兼容模式

IGRP和EIGRP相互兼容。这种兼容性提供了与IGRP路由器之间的无缝的互操作性。这种互操作性很重要，它使用户可以利用两种协议的优势。EIGRP提供多协议支持，而IGRP则不能。

2　度量值计算

EIGRP和IGRP使用不同的度量值计算方法。EIGRP用一个取值为256的因子扩展了IGRP的度量值，因为EIGRP使用了32位长度的度量值，而IGRP使用24位的度量值。通过乘以或除以256，EIGRP可以很容易地与IGRP交换信息。IGRP和EIGRP都使用下面的度量值计算：

度量值=[K1*带宽+（K2*带宽）/（256–负载）+（K3*延迟）]*[K5/（可靠性+K4）]

下面是缺省的常数值：

K1=1

K2=0

K3=1

K4=0

K5=0

当K4和K5都等于0时，方程中[K5/（可靠性+K4）]部分对度量值没有影响。因此，在缺省常数值情况下，度量值方程是：

度量值=带宽+延迟

IGRP和EIGRP使用下面的方程来决定度量值计算所用到的值（注意EIGRP有256的比例）：

IGRP的带宽=（10,000,000/带宽）

EIGRP的带宽=（10,000,000/带宽）*256

IGRP的延迟=延迟/10

EIGRP的延迟=（延迟/10）*256

3　跳数

EIGRP也使用最大跳数，其值为224。这已经足以支持现今最大的互连网络。IGRP的最大跳数是255，而RIP的最大值是15。

4　自动的协议重新分配

为了使不同的路由选择协议（如OSPF和RIP）共享信息，需要进行高级的配置。然而，在IGRP和EIGRP间，共享或重新分配（redistribute）信息是自动的，只要二者使用相同的自治系统号。

在图4–1中，RTB自动地把EIGRP学到的路

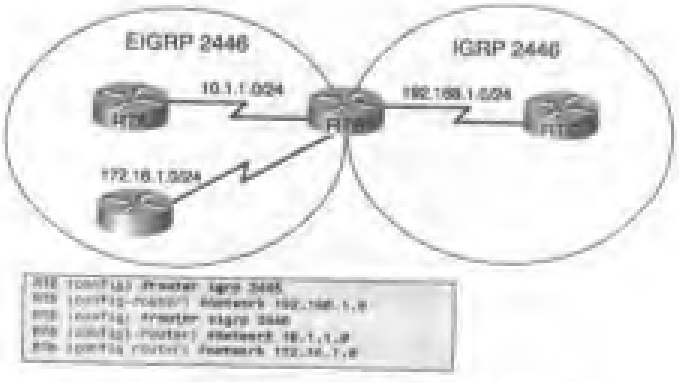


图4–1　EIGRP和IGRP共享路由信息

由重新分配到IGRP自治系统，反之亦然。

5 路由标记

EIGRP将它从IGRP（或任何外部源）学到的路由标记为外部的，因为这些路由不是起源于EIGRP路由器。IGRP不能区分内部路由（Internal routes）和外部路由（External routes）。

对于例4-1中的路由器，在show ip route命令的输出中，EIGRP路由用“D”来标记，并且外部路由用“EX”标记。RTA识别出了从EIGRP学到的网络（172.16.0.0）和从IGRP重新分配的网络（192.168.1.0）之间的不同。在RTC的表中，IGRP协议不做这样的区分。

例4-1 show ip route

```
RTA#show ip route
<output omitted>
C       10.1.1.0 is directly connected, Serial0
D       172.16.1.0 [90/2681856] via 10.1.1.1, Serial0
D  EX 192.168.1.1 [170/2681856] via 10.1.1.1, 00:00:04, Serial0

RTC#show ip route
<output omitted>
C       192.168.1.0 is directly connected, Serial0
I       10.0.0.0 [100/10476] via 192.168.1.1, 00:00:04 Serial0
I       172.16.0.0 [100/10476] via 192.168.1.1, 00:00:04, Serial0
```

只运行IGRP的RTC只能看到IGRP路由（用“I”来标识），尽管事实上10.1.1.0和172.16.0.0是由EIGRP重新分配而来。

4.1.2 EIGRP的益处

EIGRP的运行与IGRP有很大不同。做为一种先进的距离矢量路由选择协议，EIGRP在更新邻居信息和维护路由选择信息时更像一种链路状态协议。EIGRP优于简单距离矢量协议的方面包括如下：

- **快速收敛**——EIGRP路由器能够快速地收敛是因为它们依赖于一种叫做***DUAL***的先进路由选择算法。DUAL保证在路由计算过程中的每一个瞬间无环路的运行，并且允许参与拓扑变化的路由器在同一时间同步。
- **带宽的高效利用**——通过发送部分的，有界的更新，以及在网络稳定时最少地消耗带宽，EIGRP实现了对带宽的高效利用。
  - **部分的，有界的更新**——EIGRP路由器生成部分的、增量的更新，而不是发送它的整个表。这与OSPF的运行有些类似，但与OSPF不同的是，EIGRP路由器仅向那些需要这些信息的路由器发送这些增加的更新，而不是这一区域内所有的路由器。由于这个原因，这些增量的更新被叫做有界的更新（bounded updates）。
  - **网络稳定时带宽的最小消耗**——EIGRP不使用定时的路由选择更新，而使用小的hello分组相互间保持联系。尽管hello分组经常地被交换，但它们并没消耗大量的带宽。与之相对，RIP和IGRP每30秒和90秒重复性地向邻居发送整个路由选择表。
- **支持VLSM和CIDR**——与IGRP不同，EIGRP通过在路由选择更新中交换子网掩码来对无类别IP提供全面支持。
- **多种网络层支持** ——EIGRP通过协议无关模块（PDM）支持IP、IPX和AppleTalk。

4.1.3　独立于被动路由协议

PDM使EIGRP免于不断地修订。一种被动路由协议（如IP）的演化可能需要新的协议模块，但对EIGRP来说不需要重写。

4.2　EIGRP术语

EIGRP路由器在内存中保持方便可用的路由及拓扑信息，以便对变化做出快速反应。与OSPF一样，EIGRP将这些信息保存在多个表或数据库中。

EIGRP用特殊的方法处理路由。路由被赋于一定的状态，并可以通过加标记来提供额外的有用信息。

4.2.1　邻居表（Neighbor Table）

邻居表（neighbor Table）是EIGRP中最重要的表。每台EIGRP路由器维护一个列出毗邻路由器的邻居表。这个表可以和OSPF使用的毗邻数据库（adjacency database）相类比。对于所支持的每种协议，EIGRP都有一个邻居表。

当最新发现的邻居被学到时，邻居的地址和接口被记录下来。这个信息被保存在邻居数据结构中。当一个邻居发送一个hello分组时，它通告一个保持时间（hold time），这个保持时间是一台路由器认为一个邻居是可到达的和可操作的一个时间量。换句话说，如果在保持时间内没有收到hello分组，保持时间就超时了。当保持时间超时时，DUAL——EIGRP的距离矢量算法——即被告知拓扑变化并且必须重新计算新的拓扑。

在邻居表里可以找到如下字段：

- **邻居地址Neighbor address**（*Address*）——邻居路由器的网络层地址。
- **保持时间Hold time**（*Hold Uptime*）——在认为连接失效以前从一个邻居处没有获得任何信息的等待间隔。起初，等待的分组是一个hello分组，但在当前的Cisco IOS 软件版本中，可以是在第一个hello分组重置定时器后的任何EIGRP分组。
- **平稳的往返定时器Smooth Round-Trip Timer**（*SRTT*）——发送并从邻居处接收分组所用的平均时间。这个时间决定了重传的时间间隔（RTI，retransmit interval）。
- **队列计数Queue count**（*Q Cnt*）——队列中等待传送的分组数。如果这个值持续高于0，路由器中可能存在拥塞问题。0值意味着队列中没有EIGRP分组。
- **序列号Sequence Number**（*Seq No*）——从邻居收到的最后一个分组的编号。EIGRP使用这个字段来确认邻居的传输及标识乱序的分组。邻居表支持可靠的、按顺序的分组传送，并且可以看作类似于在IP分组的可靠传送中使用的TCP协议。

4.2.2　拓扑表（Topology Table）

拓扑表由自治系统中所有的EIGRP路由选择表构成。EIGRP距离矢量算法——DUAL——根据邻居和拓扑表提供的信息计算到每个目的地的最低成本路由。通过跟踪这些信息，EIGRP路由器可以很快地确定并切换到替代路由。主路由（或继承路由）信息被放置在路由选择表中，同时复制到拓扑表中。

EIGRP路由器为每一种配置的网络协议维护一个拓扑表。这个表包括路由器学到的所有目的地的路由条目。所学到的到某个目的地的所有路由都维护在拓扑表中。

拓扑表包括下列字段：

- **可行距离Feasible distance**（*FD is xxxx*）——可行距离（FD）是到每一个目的地的最低计算度量值。例如，在例4-2中，到达32.0.0.0的可行距离是2195456，FD的取值为2 195 456。

例4-2 EIGRP拓扑表

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
    R - Reply Status

P  32.0.0.0/8, 1 successors, FD is 2195456
        via 200.10.10.10 (2195456/281600), Serial1
P  170.32.0.0/16/8, 1 successors, FD is 2195456
        via 199.55.32.10 (2195456/2169856) Ethernet0
        via 200.10.10.5 (2195456/281600), Serial0
P  200.10.10.8/30, 1 successors, FD is 2169856
        via connected, Serial1
P  200.10.10.12/30, 1 successors, FD is 2681856
        via 200.10.10.10 (2681856/2169856), Serial1
P  200.10.10.0/24, 1 successors, FD is 2169856
        via summary (2169856/0), Null0
P  3200.10.10.4/30, 1 successors, FD is 2169856
        via connected, Serial0
P  205.205.205.0/24, 1 successors, FD is 2221056
        via 199.55.32.10 (2221056/2195456), /Ethernet0
        via 200.10.10.5 (2707456/2195456), Serial0
```

• **路由来源Route source**（*via xxx.xxx.xxx.xxx*）——路由来源是指最初发布这条路由的路由器的标识号。这一字段仅当该路由是从外部的EIGRP网络学到时才填入。路由标记在基于策略的路由选择时特别有用。例如，在例4-2中，到32.0.0.0的路由来源是200.10.10.10 标为Via 200.10.10.10。

• **报告距离Reported distance**——路径的报告距离（RD）是毗邻的邻居报告的到一个指定目的地的距离。在例4-2中，到达32.0.0.0的报告距离是281,600，标为12 195 456/281 600。

• **接口信息Interface information**——通过其可以到达目的地的接口。

• **路由状态Route status**——路由可以标识为被动的（P，passive）——表示路由是稳定的和可用的，或活动的（A，active）——表示路由正在使用DUAL（EIGRP的矢量算法）重新计算的过程中。

EIGRP对拓扑表进行了排序，继承路由在顶部，下面是可行继承路由。在底部，EIGRP列出了DUAL认为在拓扑表中是环路的路由。

4.2.3 后继（Successor）

后继（Successor）是指被选中作为到达一个目的地所使用的主要路由的路由。DUAL从包含在邻居表和拓扑表中的信息里标识出这条路由，并将其放在路由选择表中。对于任何特定的路由可以有多达4条后继路由。它们可以有相等的或不相等的成本，并被标识为到达给定目的地的最好的无环路径。后继拓扑表中也有后继路由的副本。

4.2.4 可行后继（Feasible Successor）

可行后继（FS，feasible Successor）是一条备份路由。这些路由与后继路由同时也被标识出来，

但它们仅保存在拓扑表中。拓扑表中可以保留一个目的地的多条可行后继路由。对一个目的地路由不必强制指定可行后继路由。

一台路由器把它的可行后继看作是比它离目的地更近的下游邻居。这是邻居路由器所发布的到目的地的成本。如果后继路由失效，路由器寻找一条标识为可行后继的路由。这个路由被提升为后继路由。可行后继路由必须具有比现有的到达目的地的后继路由更低的成本。如果从现有信息中没有标识出可行后继路由，路由器就将路由置为“活动（active）”状态，并向所有邻居发送查询分组以重新计算当前拓扑。路由器从回答查询请求的应答分组中接收新的数据，并可以从中标识出新的后继路由或可行后继路由。然后路由器将该路由置为“被动（passive）”状态。

4.2.5　后继和可行后继的选择

一台EIGRP路由器如何决定哪些路由器做为后继而哪些路由器做为可行后继？假设RTA的路由选择表中包含一条经由RTB到达网络Z的路由（见图4-2）。从RTA的观点看，RTB是网络Z的当前的后继；RTA将目的地为网络Z的分组转发给RTB。RTA必须至少有一个到达网络Z的后继使DUAL可以将其放在路由选择表中。

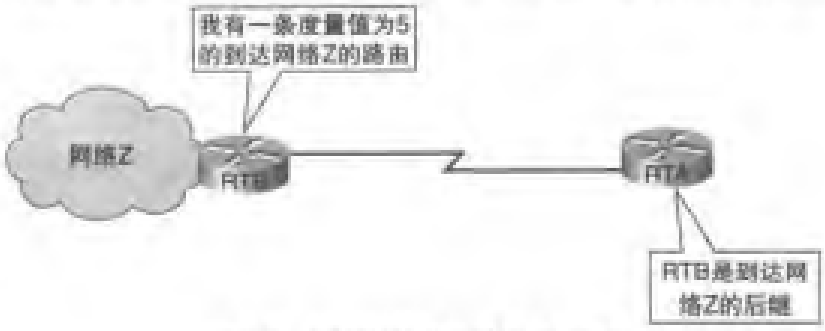


图4-2　EIGRP中的后继与可行后继

RTA可以有多于一个到达网络Z的后继吗？如果RTC宣称有一条到达网络Z的路由并且和RTB有相同的度量值，RTA也把RTC看作是后继，并且DUAL安装经由RTC到达网络C的第2条路由。

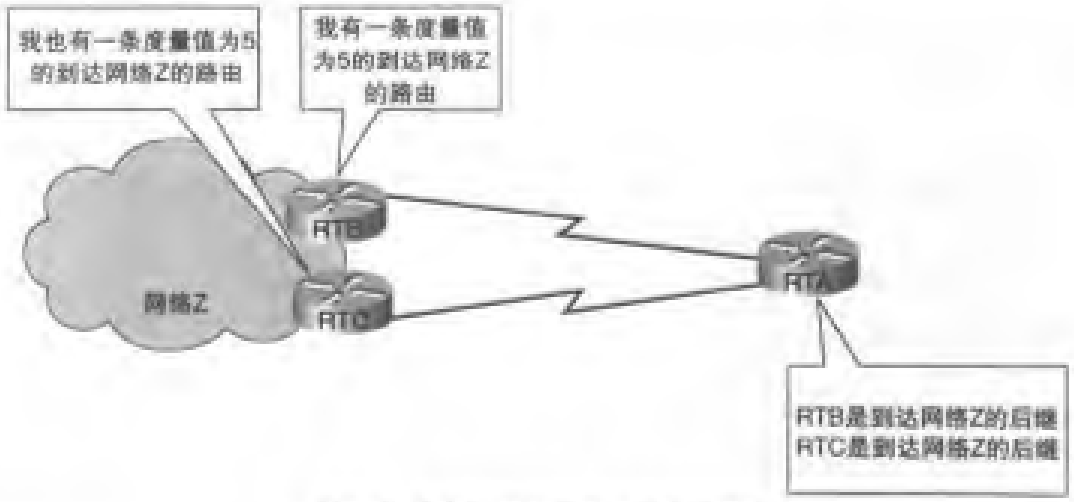


图4-3　EIGRP中的后继与可行后继2

RTA的其他邻居中，任何通告有到网络Z的无环路由（所报告的距离大于最佳路由的度量，但小于可行距离）的路由器都在拓扑表中被称为可行后继，如图4-4所示。

一台路由器把它的可行后继看作是比它离目的地更近的下游邻居。如果后继出了问题，DUAL可以很快地从拓扑表中识别出一条可行后继，并且形成到达目的地的新路由。如果不存在到达目的地的可行后继，DUAL把路由置为“活动”状态。拓扑表中的条目可以有两种状态之一：主动的或被动的。这些状态指明了由条目所指示的路由的状态，而不是条目的状态。

被动状态的路由是稳定的和可用的。主动状态的路由是DUAL在重新计算的路由。重新计算发

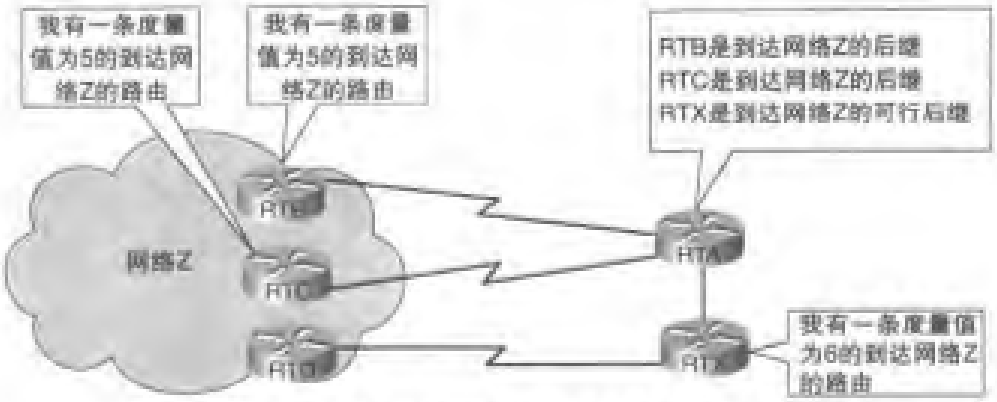


图4-4 EIGRP中的后继与可行后继

生在路由变得不可用，并且DUAL没有找到可行后继时。当这种情况发生时，路由器必须请求邻居的帮助，以发现一条到达目的地的新的、无环的路径。邻居路由器必须回复这一请求。如果一个邻居有一条路由，它就回复有关后继的信息。如果没有，邻居将告知发送者它也没有到达目的地的路由。

过多的重新计算是网络不稳定性的征兆，并将导致性能下降。为了防止收敛问题，DUAL总是在进行重新计算之前试图找到可行后继。如果有可行后继，DUAL可以很快地生成新的路由而避免重新计算。

4.2.6 活动粘滞路由（Stuck in Active Routes）

如果查询所发往的一台或多台路由器在180秒（3分钟）的活动时间（active time）内没有用回复做出响应，有问题的路由则被置成“活动粘滞（stuck in active）状态”。当这种情况发生时，EIGRP会清除没有发出回复的邻居，并在日志中记录为已经变为“活动”的路由写入“活动粘滞”错误消息。

4.2.7 路由选择表（Routing Table）

通过使用DUAL，EIGRP从拓扑表中选择到达目的地的最佳路由并将其放在路由选择表中。每台EIGRP路由器都为每种网络协议维护一个路由选择表。

4.2.8 路由标记（Route Tagging）

拓扑表可以记录有关每条路由的附加信息。EIGRP把路由分为内部的和外部的。EIGRP为每条路由添加一个路由标记（route tag）以标识这种分类。内部路由起源于EIGRP自治系统内部。

外部路由起源于EIGRP自治系统外部。从其他路由选择协议，如RIP、OSPF和IGRP，所学到的或重新分配的路由是外部路由。起源于EIGRP自治系统外部的静态路由是外部路由。标记可以被配置为0~255之间的数字，作为定制标记。

所有的外部路由都包含在拓扑表中并且标以下列信息：

- 向EIGRP网络重新分配路由的EIGRP路由器的标识号（路由器ID）。
- 目的地的自治系统号。
- 外部网络所用的协议。
- 从外部协议接收的成本或度量值。
- 可配置的管理标记。

例4-3显示了某条外部路由的拓扑表项。

例4-3　查看路由标记信息

```
Router#show ip eigrp topology 204.100.50.0
IP-EIGRP topology entry for 204.100.50.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2297856
  Routing Descriptor Blocks:
  10.1.0.1 (Serial0), from 10.1.0.1, Send flag is 0x0
    Composite metric is (2297856/128256), Route is External
    Vector metric:
      Minimum bandwidth is 1544 Kbit
      Total delay is 25000 microseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
    External data:
      Originating router is 192.168.1.1
      AS number of route is 0
      External protocol is Connected, external metric is 0
      Administrator tag is 0 (0x00000000)
```

为了开发一个精确的路由选择策略，需要利用路由标记，特别是管理员标记（administrator tag）（示例中的阴影部分）。可以把管理员标记配置成0到255间的任何数；从效果上讲，这是一个可以用来实现特定路由选择策略的定制标记。可以根据任何路由标记，包括管理员标记，来接受、拒绝或传播外部路由。由于可以按照需要配置管理员标记，路由标记的功能提供了高度的控制性。这一级别的精确性和灵活性被证实在EIGRP网络与基于策略的边界网关协议（BGP）相互作用时特别有用。

4.3　EIGRP特性与技术

EIGRP包括许多新的技术，其中每一项相对于IGRP和其他路由选择协议都表现出在运行效率、收敛速度或功能上的改善。这些技术归属于下列4种类型之一：

- 邻居发现和恢复。
- 可靠传输协议。
- DUAL有限状态机算法。
- 协议相关模块。

4.3.1　邻居发现和恢复

简单的距离矢量路由器不与邻居建立关系。RIP和IGRP路由器仅在配置的接口上广播或组播更新。相反，EIGRP路由器与其邻居主动地建立联系，很像OSPF路由器使用的方法。图4-5显示了EIGRP的毗邻关系（adjacencies）是如何建立的。EIGRP路由器使用小的hello分组与邻居路由器（neighbor routers）建立毗邻关系。在高带宽链路上，缺省为每5秒发送一次hello分组，而在低带宽多点链路上，为每60秒一次。一台EIGRP路由器假设，只要它从已知的邻居收到hello分组，这些邻

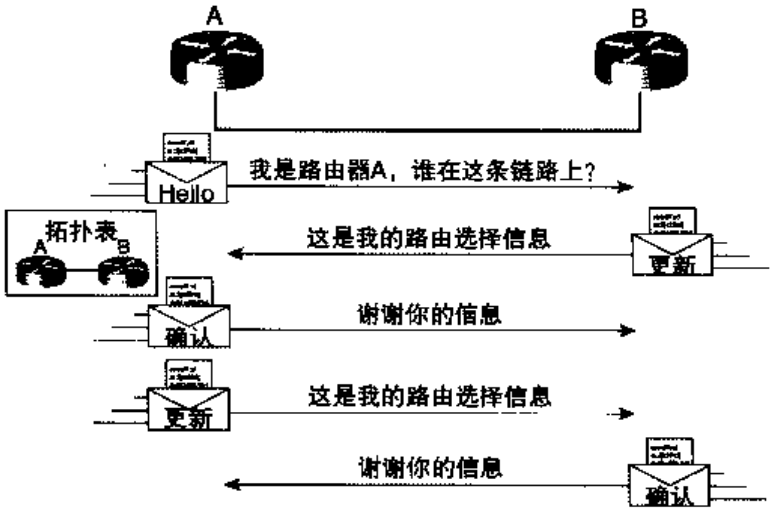


图4-5 EIGRP邻居相互交换路由信息

居（以及它们的路由）就是可用的，即被动的。

通过建立毗邻关系，EIGRP路由器可以：

- 动态地学习加入其网络的新路由。
- 确定那些不可到达或不可操作的路由器。
- 重新发现先前不可到达的路由器。

4.3.2 可靠传输协议

可靠传输协议（Reliable Transport Protocol）是一种传输层协议，它可以保证EIGRP分组有序地发送到所有的邻居。在IP网络中，主机使用TCP来顺序化分组并保证它们的及时传送。然而，EIGRP是协议无关的。（也就是说，它不像RIP、IGRP和OSPF那样依赖于TCP/IP来交换路由选择信息。）为保持与IP无关，EIGRP使用可靠传输协议（Reliable Transport Protocol）作为专有的传输层协议来保证路由选择信息的发送。

EIGRP可以根据情况请求可靠传输协议来提供可靠的或不可靠的服务。例如，hello分组不需要可靠传输的开销，因为它们很频繁并且应该保持很小。然而，其他路由选择信息的可靠传输可以在事实上加速收敛，因为EIGRP路由器不用在重传输之前等待定时器失效。

使用可靠传输协议，EIGRP可以同时组播和单播到不同的对等体，使效率最大化。

4.3.3 DUAL有限状态机

EIGRP的核心是DUAL，它是EIGRP的路由计算引擎。这一技术的全称是DUAL有限状态机器（FSM，finite-state machine）。FSM是一台抽象的机器，而不是一台带有运动部件的机械设备。FSM定义了一个某些事情的可能状态的集合，什么事件可以引起这些状态，以及这些状态可以导致什么事件。设计者使用FSM来描述一台设备、计算机程序或路由选择算法是如何与一系列输入事件相互作用的。DUAL FSM包括所有在EIGRP网络中计算和比较路由所用到的逻辑。

DUAL跟踪邻居通告的所有路由，并使用每条路由的复合度量值来比较它们。DUAL还保证每条路由都是无环路的。然后DUAL算法将最低成本路径插入到路由选择表中。这些主路由就是已知的后继路由。后继路由的副本也被放置在拓扑表中。

EIGRP在邻居表和拓扑表中保持重要的路由信息和拓扑信息方便可用。在网络中断的情况下，这些表向DUAL提供全面的路由信息。DUAL使用这些表中的信息很快地选择替代路由。如果链路

中断，DUAL在拓扑表中寻找一条替代路径，即可行后继。送往目的网络的分组立即转发到可行后继，从此，它被提升为后继，如图4-6所示。

注意在图4-6的例子中，路由器D没有标识可行后继。路由器D到路由器A的FD（或计算成本）是2，而经由路由器C的发布距离AD（或报告距离）是3。因为AD小于最佳路由度量值但大于FD，所以没有可行后继放在拓扑表中。路由器C和路由器E都有一条标识的可行后继，因为路由是无环路的并且因为下一跳路由器的AD小于后继的FD。

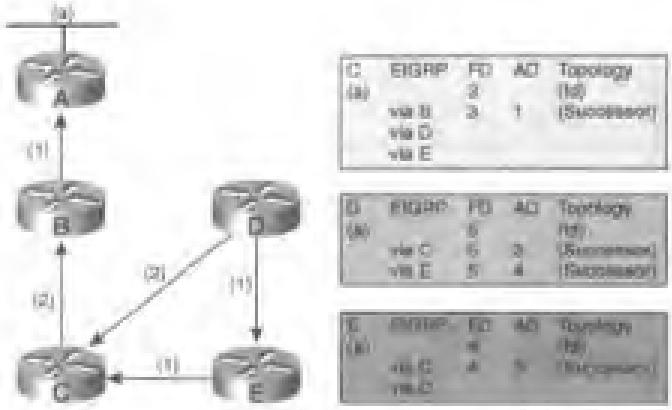


图4-6　EIGRP DUAL计算收敛

4.3.4　PDM

EIGRP最具吸引力的特性之一是它的模块化设计。模块化或分层的设计被证实是最具扩展性和适用性的。通过PDM，EIGRP支持多种被动路由协议，如IP、IPX和AppleTalk。理论上讲，EIGRP可以通过增加PDM来很容易地适应新的或修订的被动路由协议（如Ipv6）。图4-7从概念上展示了PDM是如何工作的。

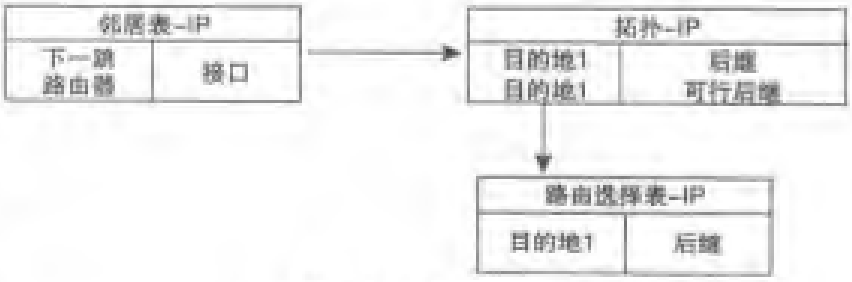


图4-7　EIGRP PDM

每个PDM负责与其所针对的被动路由协议相关的所有功能。IP-EIGRP模块的责任包括：

- 发送并接收承载IP数据的EIGRP分组。
- 向DUAL通报所接收的新的IP路由选择信息。
- 在IP路由选择表中维护DUAL路由选择决定的结果。
- 重新分配从其他的支持IP的路由选择协议所学到的路由选择信息。

4.4　EIGRP分组类型

类似于OSPF，EIGRP依赖于几种不同种类的分组来维护它的各种表和与邻居路由器建立复杂的关系。下面是EIGRP的5种分组类型：

- **问候**（*hello*）。
- **确认**（*Acknowledgment*）。
- **更新**（*Update*）。
- **查询**（*Query*）。
- **回复**（*Reply*）。

4.4.1　Hello分组

EIGRP依赖于hello分组来发现、验证和重发现邻居路由器。如果EIGRP路由器在保持时间间隔（hold time interval）内没有收到其他路由器的hello分组，之后又重新建立了通信，就称为导致重发现（rediscovery）。

EIGRP路由器以固定的（和可配置的）时间间隔发送hello分组，被称之为hello间隔（hello interval）。缺省的hello间隔依赖于接口的带宽，如表4-1所示。

表4-1 Hello间隔

带宽	链路示例	缺省hello间隔	缺省保持时间
小于或等于1.544Mbit/s	多点帧中继	60秒	180秒
大于1.544Mbit/s	T1、点到点	5秒	15秒

EIGRP的hello分组通过组播发送。在IP网络中，EIGRP路由器发送hello分组到组播地址224.0.0.10。

EIGRP路由器将关于邻居的信息保存在邻居表中。邻居表中包括序列号（Seq No）字段以记录每个邻居发送的最后一个EIGRP分组的编号。邻居表也包含一个“保持时间”字段，记录了最后收到分组的时间。分组应该在保持时间间隔内收到以保持被动状态（即可到达的和可操作的）。

如果在保持时间段内没有收到来自邻居的hello分组，EIGRP就认为这个邻居出现了故障，并且DUAL必须开始重新评价路由选择表。缺省情况下，保持时间3倍于hello间隔，但是管理员可以根据需要配置两个定时器。

OSPF需要邻居路由器具有相同的hello时间间隔和失效时间间隔以保证通信。EIGRP没有这个约束。邻居路由器通过交换hello分组相互学习各自的定时器，同时它们使用这些信息来构造稳定的关系，而不管定时器值是否一致。

Hello分组总是不可靠地传送并且不需要确认。

4.4.2 确认分组

EIGRP路由器在“可靠的”交互期间使用确认分组来表示收到了任何的EIGRP分组。“可靠传输协议”可以在EIGRP主机间提供可靠的通信。为了可靠，接收者必须确认发送者的消息。作为“无数据”的hello分组，确认分组用于这一目的。与多播的hello分组不同，确认分组是单播的，并发往指定的主机。确认也可以搭载在其他类型的EIGRP分组上，如回复分组（reply packets）。

4.4.3 更新分组

当路由器发现新的邻居时，便使用更新分组（update packets）。一台EIGRP路由器向新的邻居发送单播的更新分组使之可以被加入到拓扑表中。为了向新发现的邻居传达所有的拓扑信息，可能需要多个更新分组。

当路由器检测到拓扑变化时也使用更新分组。在这种情况下，EIGRP路由器向所有邻居发送组播的更新分组，提醒它们这一变化。

所有的更新分组都是可靠传送的。

4.4.4 查询和回复分组

当EIGRP路由器需要从一个或所有的邻居那里得到指定的信息时，使用查询分组（query packets）。回复分组用于响应一个查询。

如果一台EIGRP路由器丢失了某条路由的后继，并且找不到其可行后继，DUAL则将这条路由置为活动状态。然后，路由器向所有邻居组播一个查询，寻找到达目的网络的后继。邻居必须发送回复，无论是提供有关后继的信息，还是指示没有关于后继信息。

查询可以是组播或单播，而回复总是单播。两种类型的分组都是可靠传送的。

4.5　EIGRP收敛

DUAL的精密算法导致了EIGRP异常快速的收敛。为了更好地理解使用DUAL的收敛，来看图4-8中的情形。RTA可以经由3台不同的路由器RTX、RTY或RTZ到达网络24。

在图4-8中，为了简化计算，EIGRP的综合度量值由链路成本来代替。RTA的拓扑表包含邻居通告的所有路由的列表。对每个网络，RTA保留到达该网络的真实（计算的）成本，也保留一个来自邻居的通告成本（报告距离），如表4-2所示。

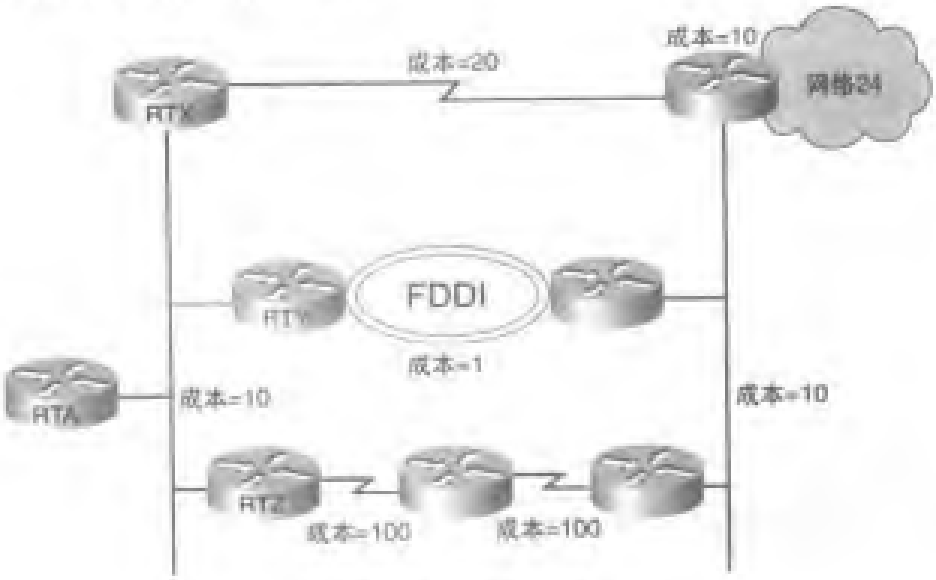


图4-8　EIGRP收敛

表4-2　复合度量值

邻居	到网络24的计算成本	到网络24的报告距离
RTY	21	21
RTZ	230	220
RTX	40	30

最初，RTY以其最低计算成本成为通向网络24的后继。RTA通向网络24的最低计算成本是31，这个值是到达网络24的FD。

RTA按照下面3步过程选择到达网络24的可行后继。

步骤1　确定哪个邻居到网络24的RD值小于RTA到网络24的FD值。FD是31，RTX的RD是30，而RTZ的RD是220（见表4-2）。因此，RTX的RD低于当前的FD，而RTZ的RD大于当前FD。

步骤2　从剩余的可用路由中确定到达网络24的最小计算成本。经由RTX的计算成本是40，而经由RTZ的计算成本是230。因此，RTX提供了最低的计算成本。

步骤3　确定是否有路由器既满足步骤1的标准也满足步骤2的标准。RTX满足二者，所以它是可行后继。

当RTY失效时，RTA立即使用RTX（可行后继）向网络24转发分组。向备份路由快速转换的能力是EIGRP异常快速的收敛的关键。

RTZ能够成为可行后继吗？使用与上面相同的3个步骤，RTA发现RTZ的通告成本是220，并不小于RTA的FD值31。因此，RTZ（还）不能成为可行继承路由。FD只在活动到被动（active-to-passive）的转换的过程中变化，而这种情况没有发生，因此它保持为31。从这点看，因为网络24没有到活动状态的转换，DUAL完成了一次本地计算（local computation）。

当RTA不能找到可行后继时，会将网络24从被动转换为活动，并向邻居查询有关网络24的信息。这一过程即是已知的扩散计算（diffusing camputation）。当网络24处于活动状态时，FD被重置。这

使得RTA最终接受RTZ为到达网络24的后继。

4.6 配置EIGRP

本节包括了常用的EIGRP配置过程。应特别注意EIGRP用于建立与毗邻路由器的关系、计算主要和备份路由以及在必要时响应到特定目的地已知路由的失效。

4.6.1 为IP配置EIGRP

尽管DUAL很复杂，但配置EIGRP IP相对简单。EIGRP的配置命令随被动路由的协议而变化。本节包括了对IP协议的EIGRP配置方法。参考图4-9。

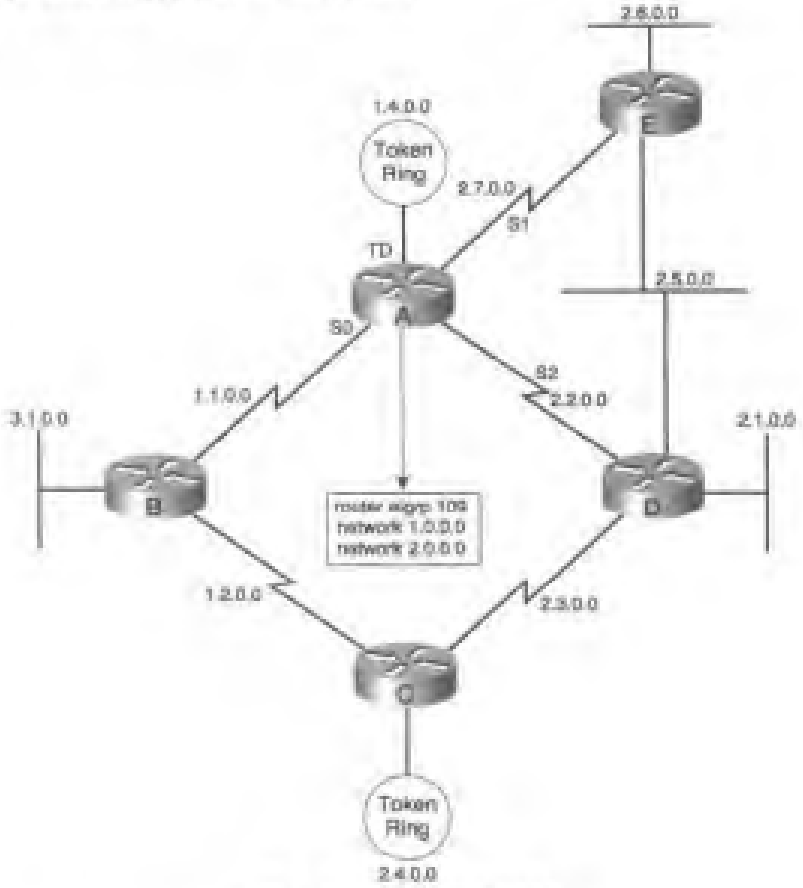


图4-9 为IP配置EIGRP

按照下列步骤为IP配置EIGRP：

步骤1 使用下面的命令启动EIGRP并定义自治系统：

```
router(config)# router eigrp autonomous-system-number
```

其中*autonomous-system-number*是标识惟一自治系统的编号。它标识了属于一个互连网络中的所有路由器。在互连网络内的所有路由器上，该值必须一致。

步骤2 用下面的命令指的在该路由器上哪些网络属于EIGRP自治系统：

```
router(config-router)# network network-number
```

其中*network-number*是网络编号，决定了路由器的哪个接口参与EIGRP以及路由器向哪个网络通告。网络号用IP地址的分类输入。例如，网络2.2.0.0和2.7.0.0可以用下面的network命令输入：

```
router(config-router)# network 2.0.0.0
```

network命令仅配置连接的网络。例如，网络3.1.0.0（在图4-9的左侧）没有直连到路由器A。

因此，这个网络不在路由器A的配置中。

步骤3　当使用EIGRP配置串行链路时，在接口上配置带宽是很重要的。如果这些端口的带宽没有改变，EIGRP会使用缺省带宽，这可能与实际带宽不一致。如果链路较慢、路由器可能无法收敛、路由选择更新可能丢失或者可能导致次优的路径选择。使用下面的命令来配置带宽：

```
router(config-if)# bandwidth kilobits
```

bandwidth命令仅用于路由选择进程，并且要与接口的线路速度相匹配。

步骤4　Cisco也建议在所有EIGRP配置中增加如下命令：

```
router(config-if)# eigrp log-neighbor-change
```

这条命令启动了邻居邻带变化的日志以监视路由选择系统的稳定性，有助于发现问题。



实验活动　配置EIGRP

在本实验室中，你将在两台路由器上配置EIGRP并用ping验证其连接。

4.6.2　在NBMA中配置带宽

当在非广播型多路访问（NBMA）网云中，如帧中继，配置EIGRP时应遵循下列3条规则：

- EIGRP的通信量不能超过虚电路（VC）的承诺信息速率（CIR）容量。
- EIGRP在所有VC上的合计通信量不能超过接口的访问线路速度。
- 每条VC上分配给EIGRP的带宽在两个方向上必须一致。

如果理解并遵从了这些规则，EIGRP可以在WAN上很好地工作。如果在WAN的配置上不加注意，EIGRP会使网络崩溃。

4.6.3　在多点网络中配置带宽

在NBMA网云中，bandwidth命令的配置依赖于VC的设计。如果在多点配置中，串行线路有多个VC，并且这些VC均匀地共享带宽，则将带宽设置为所有CIR的总和。例如，在图4-10中，每一条VC的CIR为56Kbit/s。因为有4条VC，所以带宽设置为224（4×56）。

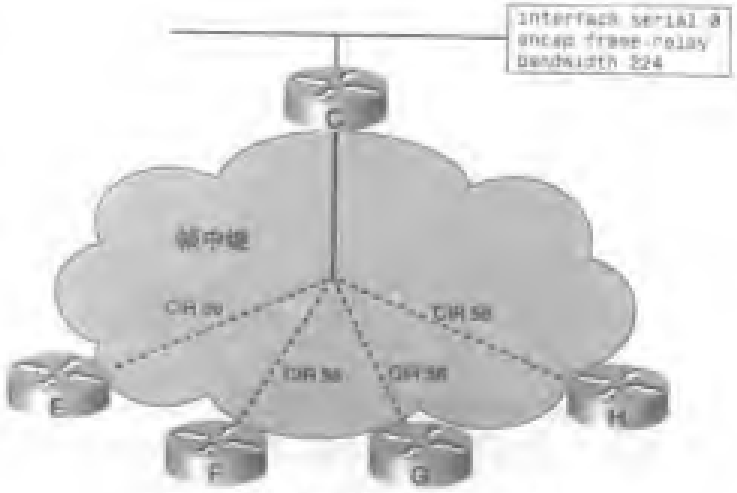


图4-10　EIGRP WAN配置纯多点

4.6.4　在混合多点网络中配置带宽

如果多点网络中为VC分配不同的带宽，则需要一种更复杂的解决方法。可以使用下面两种主要方法之一：

- 取最低的CIR并乘以VC数——如图4-11所示，作用于物理接口。这样配置的问题是会使较高带宽的链路利用不足。
- 使用子接口——bandwidth命令能够在每个子接口上进行配置，可以允许每条VC上有不同的速度。在这种情况下，要为不同CIR的链路配置子接口。具有相同CIR配置的链路表现为具有一个带宽的单一接口，反映为所有电路的聚合。在图4-12中，有3条VC具有相同的CIR，为256Kbit/s。所有这3条VC被组合在一起作为一个多点子接口（multipoint subinterface），Serial 0.1。余下的一条具有较低的56Kbit/s CIR的VC，被分配为一个点到点子接口（point-to-point subinterface），Serial 0.2。

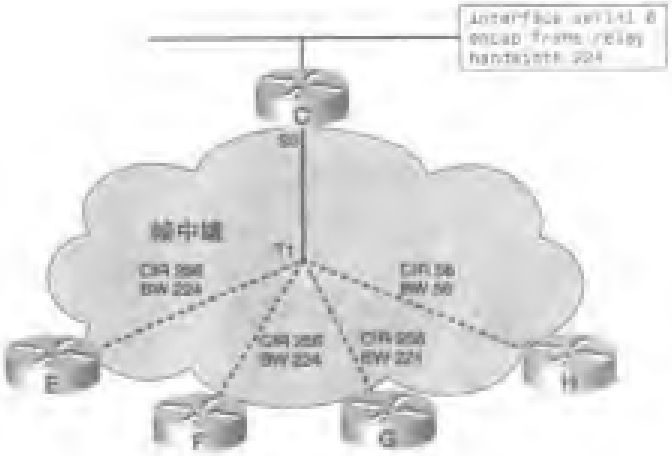


图4-11 EIGRP WAN 配置——混合多点

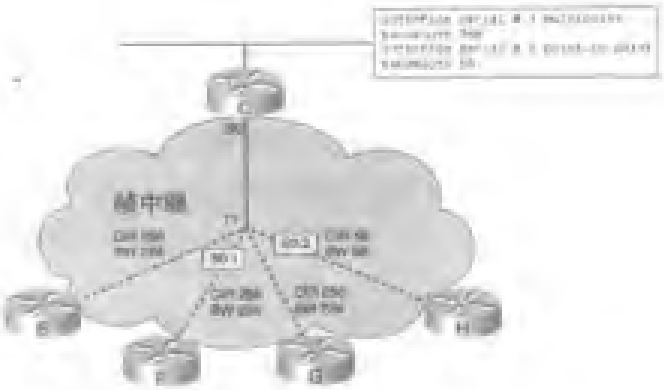


图4-12 EIGRP WAN 配置——更优的混合多点

4.6.5 使用ip bandwidth-percent命令

ip bandwidth-percent命令用于配置在一个接口上EIGRP可以使用带宽的百分比。缺省情况下，EIGRP被设置为最多可以使用一个接口的百分之五十的带宽来交换路由选择信息。为了计算百分比的和值，ip bandwidth-percent命令依赖于bandwidth命令所设的值。

当一个链路的带宽设置不能反映其实际速度时，就要使用ip bandwidth-percent命令。带宽值可能由于各种原因被人工设置得很低，比如调整路由选择的度量值，或是提供较多配额给多点帧中继配置。无论什么原因，可以通过设置ip bandwidth-percent为高的值来配置EIGRP，以克服人工配置的较低的带宽。在某些情况下，百分比甚至可能被设成大于100。

例如，假设一条路由器串行链路的实际带宽为64Kbit/s，但带宽值被人为地设置为一个低值，为32Kbit/s。图4-13显示了如何调整EIGRP使得它根据串行接口的实际带宽限制路由选择协议的流量。这个例子中设置了Serial 0在自治系统24中EIGRP进程所用带宽的百分比。因为32Kbit/s的百分之百是32，因此EIGRP可以使用实际带宽64Kbit/s的一半。图4-13给出了其细节。

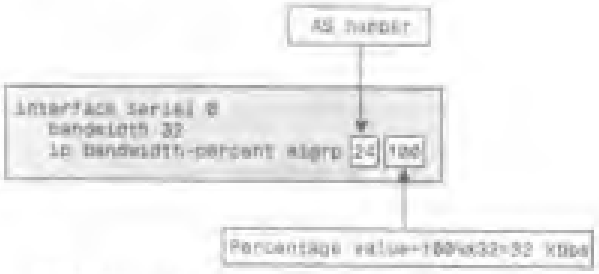


图4-13 EIGRP ip bandwidth-percent命令

4.6.6 配置EIGRP汇总

EIGRP在有类别边界（有类别寻址中定义的，某个网络地址结束的边界）自动地汇总路由。这意味着即使RTC只连接子网2.1.1.0，它仍然会发布其连接整个A类网络—2.0.0.0。在许多情况下，自动汇总是一件好事，它保持路由选择表尽可能地压缩。



图4-14 EIGRP自动汇总

然而，在某些情况下自动汇总可能不是一个好的选择。如果有不连续的子网，如图4-15，必须关闭路由选择的自动汇总以使工作正常。

要关闭自动汇总，使用下列命令：

```
router(config-router)# no auto-summary
```

在EIGRP中，可以手动配置一个前缀用作汇总地址。手工汇总路由配置在各个接口上，因此应

首先选择那些传播路由汇总的接口。然后，汇总地址可以用ip summary-address eigrp命令来定义。命令的语法如下：

```
router(config-if)# ip summary-address eigrp autonomous-system-number ip-address mask
administrative-distance
```

EIGRP汇总路由的缺省管理距离5。可选地，它能被配置为1~255之间的值。

图4-15中的RTC可以用例4-4中的命令来配置：

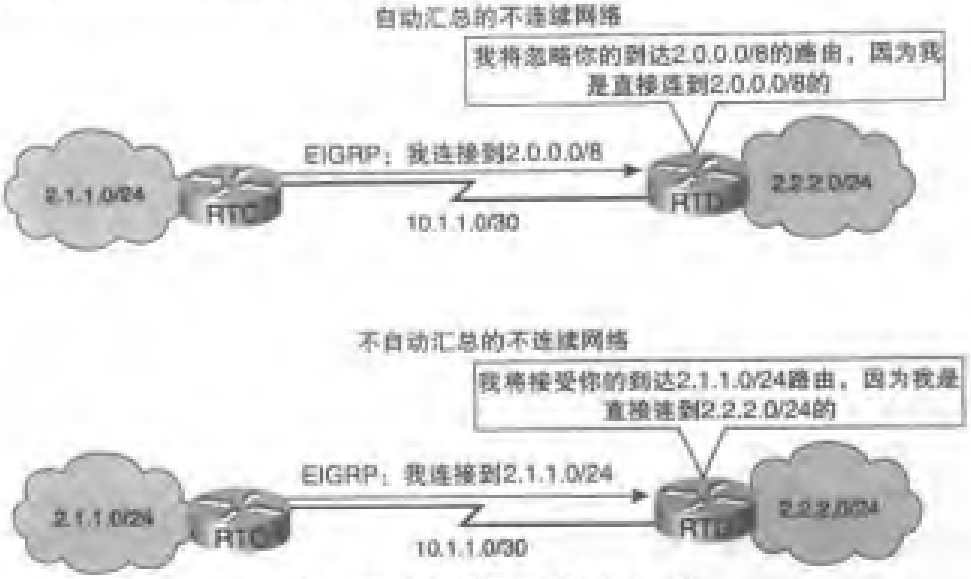


图4-15　EIGRP基于类的自动汇总

例4-4　手工汇总

```
RTC(config)#router eigrp 2446
RTC(config-router)#no auto-summary
RTC(config-router)#exit
RTC(config)#Interface serial0
RTC(config-if)#Ip summary-address eigrp 2446 2.1.0.0 255.255.0.0
Thus, RTC will add a route to its table, as follows:
D 2.1.0.0/16 is a summary, 00:00:22, Null0
```

汇总路由来源于Null0而不是一个实际的接口。这是因为这条路由是用于通告的，而不是表示一条RTC可用于到达那个网络的路径。在RTC上，这条路由的管理距离为5。

在图中，RTD忽略了汇总并接收了这条路由，再给这条路由分配一个“正常”EIGRP路由管理距离（缺省值为90）。在RTC的配置中，自动汇总通过no auto-summary命令关闭。如果自动汇总没有关闭，RTD就会收到两条路由：手工汇总路由（2.1.0.0/16）和自动的、有类别汇总地址（2.0.0.0/8）。

在多数情况下，选择手工汇总时，应该使用no auto-summary命令。

4.7　验证基本的EIGRP

可以使用各种show命令来验证EIGRP的运行情况。表4-3列出了主要的EIGRP show命令并简要讨论了它们的功能。

表4-3 基本的EIGRP show命令

命令	描述
Show ip eigrp neighbors *[type number] [details]*	显示EIGRP邻居表。使用type和number选项来指定接口。detail关键字用于扩展输出
Show ip eigrp interfaces *[type number] [as-number] [details]*	显示每个接口的EIGRP信息。可选的关键字限定了关于特定接口或自治系统的输出。detail关键字用于扩展输出
Show ip eigrp topology *[as-number] | [[ip-address] mask]*	显示EIGRP拓扑表中所有可行后继。可选的关键字可以基于自治系统号或指定网络地址过滤输出
Show ip eigrp topology *[active | pending | zero-successors]*	根据所使用的关键字，显示拓扑表中活动的（active）、未决的（pending）或无后继的所有路由
Show ip eigrp topology all-links	显示EIGRP拓扑中所有路由，而不仅是可行后继
Show ip eigrp traffic *[as-number]*	显示发送和接收的EIGRP分组号。通过可选的自治系统号能过滤命令的输出

Cisco IOS的debug特性也提供了有用的EIGRP监控命令，如表4-4中所列。

表4-4 基本的EIGRP debug命令

命令	描述
debug eigrp fsm	这一命令帮助你观察EIGRP可行后继的活动，并决定路由选择进程是否在安装或删除路由更新
debug eigrp packet	这条命令的输出显示了EIGRP分组的发送和接收。这些分组的类型可以是hello、更新、请求、查询或回复分组。EIGRP可靠传输算法使用的序列号和确认号也在输出中显示



实验活动 验证基本IGRP配置

在本实验中，你在2台路由器上配置EIGP，并使用Ping和其他IGRP命令验证各种配置。

4.8 总结

本章讨论了以下的内容：

- EIGRP是基于IGRP的Cisco所有路由选择协议。
- EIGRP具有快速收敛、增强的可扩展性以及更高级的路由环路处理能力。
- EIGRP可以取代Novell的RIP和AppleTalk的RTMP，能提高IPX和AppleTalk网络的效率。
- EIGRP是一种先进的距离矢量路由选择协议，依赖于那些通常链路状态协议才具有的特性。OSPF的一些最好的特性，如部分更新和邻居发现，都被类似地用于EIGRP。
- 对于主要基于Cisco路由器构建的大型的、多协议的网络，EIGRP是一个理想的选择。
- 本章也包含了用于配置、验证EIGRP及故障排除的步骤和命令。

作为本章内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

4.9 关键术语

延迟（*delay*） 从发送方发起一个事务的开始到发送方收到的第一个响应之间的时间。也是延特定路经将分组从源移动到目的地所需的时间。

扩散更新算法（DUAL，Diffusing Update Algorithm） 增强IGRP所使用的收敛算法，能够在路由计算过程中每一瞬间提供无环路的运算。允许拓扑变化涉及的路由器在相同时间同步，而不涉及的路由器不受变化影响。

可行距离（*feasible distance，FD*） 到每一目的地的最小计算度量值。

可行后继（*feasible succersor，FS*） 备份路由。这些路由在后继被标识的同时被标识出来，但它们只保留在拓扑表中。

邻居表（*neighbor table*） 运行EIGRP的路由器用于维护毗邻路由器列表的表。EIGRP对支持的每种协议都有一个邻居表。

报告距离（*reported distance，RD*） 毗邻路由器报告的到达某个指定目的地的距离。

可靠传输协议（*Reliable Transport Protocol*） 传输层协议，能保证到所有邻居的EIGRP分组有序的传送。

活动粘滞（*Stuck in active*） 路由的一种状态。如果查询所发往的一台或多台路由器在180秒（3分钟）的活动时间内没有用回复作出响应，路由则处于活动粘滞状态。

后继（*Successor*） 被选择作为用来到达一个目的地的主要路由的路由。

拓扑表（*topdogy table*） 由自治系统内所有EIGRP路由选择表构成的表，用于向路由器提供自治系统内部所有目的地路由的知识。

4.10 复习题

1. 如何配置IGRP和EIGRP之间的自动重新分配?
   A. 用不同的自治系统号配置两种协议。
   B. 用不同的DS号配置两种协议。
   C. 用同样的自治系统号配置两种协议。
   D. 用同样的DS号配置两种协议。
2. 哪种协议结合了链路状态和距离矢量路由选择协议二者的优点?
   A. IP
   B. OSPF
   C. IGRP
   D. EIGRP
3. 哪个算法用来获得快速的收敛?
   A. Dijkstra算法
   B. 扩散更新算法
   C. 收敛算法
   D. 双收敛算法
4. EIGRP可以通过使用PDM支持哪种协议?
   A. IS-IS
   B. SNMP
   C. IPX
   D. DHCP
5. 哪个表包含了路由器所学到的到达各个目的地的路由项，并且为所配置的每种被动路由协议维护一个单独的表?
   A. 拓扑表
   B. 路由选择表
   C. 邻居表
   D. 后继表
6. 下列哪一项用于建立比邻关系?
   A. DUAL有限状态机
   B. Hello分组
   C. 拓扑表
   D. 可靠传输协议
7. 下列哪一项保证了到达所有邻居的EIGRP分组的有序传送?
   A. DUAL 有限状态机
   B. Hello分组
   C. 拓扑表
   D. 可靠传输协议
8. DUAL在跟踪所有路由、比较它们、保证它们无环路后做什么?
   A. 向路由选择表中插入多达4条最低成本路径
   B. 决定最佳路径并用hello分组向邻居路由器通告
   C. 通过PDM支持其他被路由协议
   D. 向邻居路由器发送一个单播查询

9. EIGRP如何防止外部路由发生路由选择环路？
   A. 拒绝所带路由器ID标志与自身ID相等的外邻路由
   B. 通过存储作为可行后继的路由器标识
   C. 拒绝所通告的综合能量小于路由器当前最佳能量的所有邻居路由器
   D. 存储所有在路由表中称为“有环路”的邻接路由
10. 在高带宽的连接中，如点到点的串行连接和多点电路，EIGRP使用多长的Hello间隔？
   A. 5秒
   B. 10秒
   C. 60秒
   D. 120秒



第5章　交换的概念与局域网技术

目标

学习完本章后，你将能够：

- 描述以太网/802.3局域网。
- 了解局域网交换的概念。
- 了解并利用局域网设计概念。
- 描述基本的第2层桥接和交换过程。

目前，网络设计者正从使用网桥和集线器转移到主要使用*交换机*（switches）和*路由器*（routers）来构建网络。

本章将讨论局域网（*LAN*）中的问题和提高LAN性能的可能解决方案。你将学到LAN*拥塞*（congestion）及其对网络性能的影响，以及在一个网络内进行LAN分段的好处。此外，你还将学到使用网桥、交换机和路由器进行LAN分段的优缺点，以及在网络吞吐量方面使用*交换*（switching）、桥接（bridging）、路由选择（routing）各自的效果。同时将学到有效的LAN设计的基本要求、目标和考虑因素。最后，你将学到如*以太网*（Ethernet）、*快速以太网*（Fast Ethernet）和*吉比特以太网*（Gigabit Ethernet）等各种交换技术的优点，虚拟以太网（VLAN）及其在LAN设计中的应用。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图，光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

5.1　以太网/802.3局域网

最通用的LAN体系结构是以太网。以太网用来在网络设备之间传输数据，例如计算机、打印机和文件服务器。

5.1.1　以太网/802.3局域网的发展

最早被广泛应用的LAN技术是基于线型总线的，使用粗缆或细缆布线。理解这些基本架构的一些局限性是很重要的，这将使你能看到今天的LAN交换技术所处的位置。

下面是粗缆以太网局限性的汇总列表：

- 限制在500m以内以保证信号不衰减。

- 每500m需要一个中继器（repeater）。
- 限制站点数量和放置的位置。
- 昂贵，体积大，穿越建筑物困难。
- 增加新用户相对简单。
- 提供10Mbit/s的共享带宽。
- 线型总线的不良连接或断开都会中断LAN通信。

下面是细缆以太网局限性的汇总列表：

- 比粗缆便宜，且所需空间小。
- 穿越建筑物仍旧困难。
- 增加用户时需要中断网络。
- 提供10Mbit/s的共享带宽。
- 线型总线的不良连接或断开都会中断LAN通信。

在网络中加入集线器或集中器可以改善粗、细缆以太网技术。集线器是第1层设备，有时可以认为它是一个以太网集中器（Ethernet concentrator）或者是多端口中继器（multiport repeater）。集线器的引入允许更多的用户对网络有更大的访问量。可以再生信号的主动集线器（active hubs）也允许网络延伸到更远的距离，如图5-1所示。集线器在接收数据信号时不做决定，它只是简单地对收到的数据信号进行再生和放大并传至所有连接的设备。在线型总线网络中，总线电缆中任何位置的一个断点或者是到一台用户工作站的不良连接都将导致LAN失效，使其不可用。当使用较新的以太网技术时，如集线器或者交换机，连接一个用户的电缆上的断点不会影响网络上的其他用户。另一方面，集线器或者交换机会成为单一的故障点。

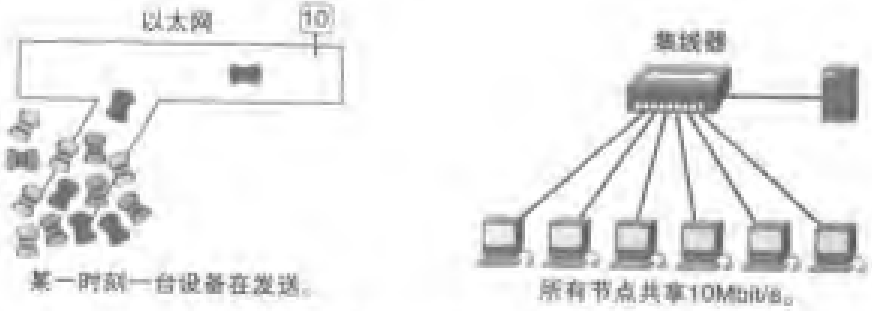


图5-1　集线器

以太网从根本上讲是一种共享技术，所有用户在给定的LAN分段中竞争同一个可用带宽，如图5-2所示。这种状况和几辆汽车在同一时间内试图通过一条单车道道路类似。因为道路只有一条车道，在某一时刻只能允许一辆汽车通过。在网络中引入集线器就会导致更多的用户争抢同一带宽。

冲突（collision）是以太网的副产品。如果2台或者多台设备试图同时发送数据，那么就会发生冲突。这种状况就类似于2辆汽车并到一条车道而导致碰撞。直到碰撞被清除后交通才得以恢复。当一个网络中冲突太多的时候，会导致缓慢的网络响应时间，表示网络变得过于拥塞，或者是太多的用户试图在同一时间访问网络。

像中继器和集线器这类的第1层设备，只是简单地放大信号以获得更远的传送距离。第2层设备较之第1层设备更智能。第2层设备根据包含在传输数据帧头内的*介质访问控制地址*（MAC address）作出转发决定。

网桥（bridge）是第2层设备，用于划分（分段）网络，并能在两个网段之间收集和选择性地传送数据帧。网桥是通过学习每一个相连网段中所有设备的MAC地址来完成这些功能的。利用收集的信息，网桥构建一个桥接表，并且根据这个表转发或阻塞通信。这样形成了较小的*冲突域*

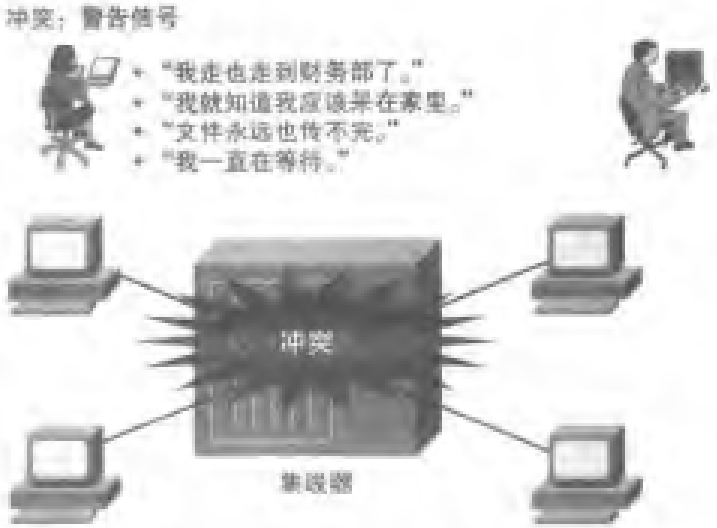


图5-2 冲突

（collision domains）和较高的网络效率。网桥不能限制广播通信，但是，网桥的确在网络中提供了更强的通信控制，并减少了冲突。

交换机也是第2层设备，可以被看作多端口网桥（multiport bridge）。交换机通过更好的通信控制来减少冲突，如图5-3所示。交换机能根据数据帧内的MAC地址作出转发决定。像其他第2层设备所做的那样，交换机也会学习连接在每个端口的各个设备的MAC地址，这些信息均被记录在内容可寻址存储器（CAM, content-addressable memory）里的交换表中。

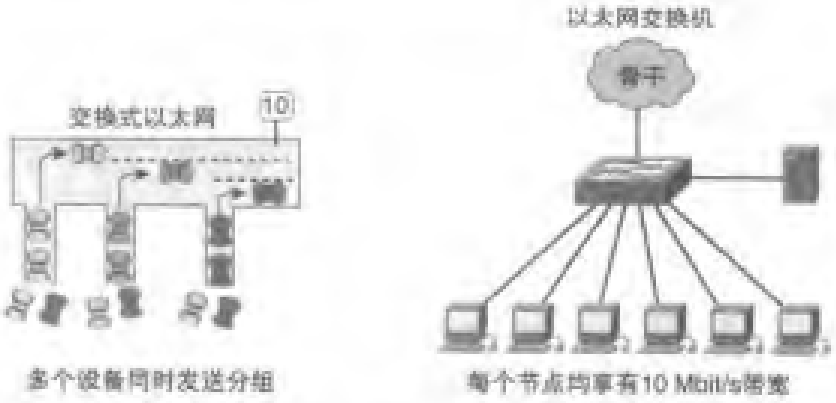


图5-3 第2层交换机

交换机在想要通信的两台连接的设备之间建立一条虚电路。当虚电路被建立之后，在两台设备之间就建立了专用的通路。网络中交换机的使用提供了*微分段*（microsegmentation）功能。理论上，这样可以在源和目的之间建立无冲突环境，允许可用带宽的最大利用率。交换机也使多路并发虚电路的连接很容易实现。这类似于高速公路被分成多条车道，每一辆车都有专用的车道。图5-4说明了第1层的集线器和第2层的交换机的不同点。

第2层设备的缺点是它们被迫转发那些广播到网络上所有连接设备的帧。当网络中的广播通信过多时，网络响应时间将变得缓慢。

路由器是第3层设备。路由器的转发决定是基于一组网络地址而不是单个的第2层MAC地址。路由器使用*路由选择表*（routing table）来记录可访问的网络的第3层地址。作为网络的管理者，你可以手工输入这些网络，或者你可以让路由器通过路由选择协议学习这些网络，或通过邻居路由器发现这些网络。

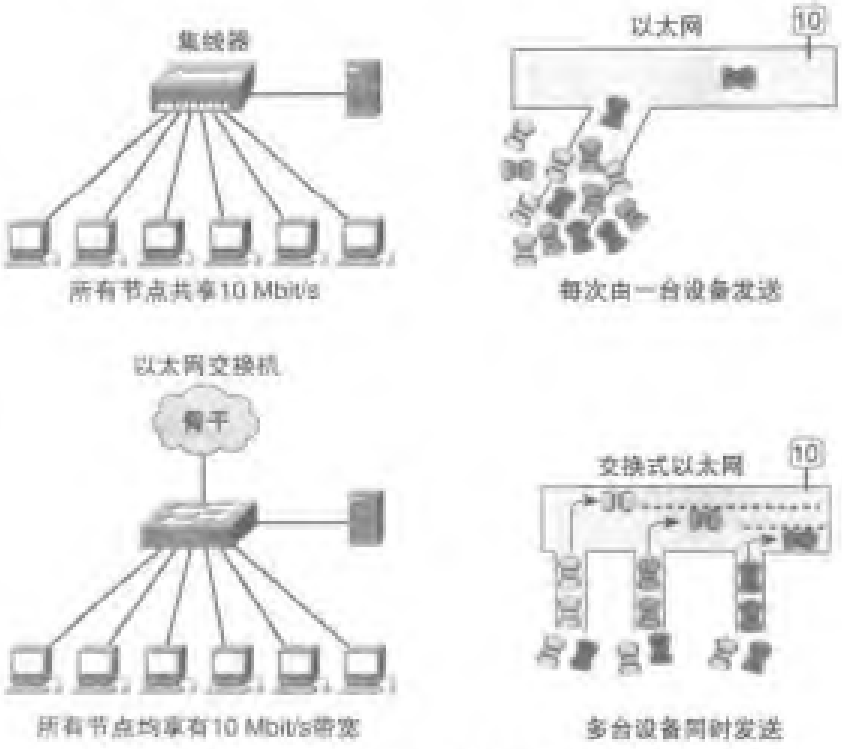


图5-4　交换机、路由器与集线器的对比

路由器的目的是检查进入的分组（第3层数据），为它们选择通过网络的最佳路径，然后将它们交换至合适的输出端口。路由器不会被强迫转发广播。因此，路由器减少了网络中的冲突域和**广播域**（broadcast domain）。路由器是大型网络上最重要的通信管理设备。事实上它们使得任何类型的计算机都可以与世界上任何地方的其他计算机通信。

LAN中通常会组合布署使用了第1、2层和第3层设备，如图5-5所示，该图显示了一台集线器（第1层）、两台交换机（第2层）和一台路由器（第3层）。设备布署依赖于组织特定需求中的要素。

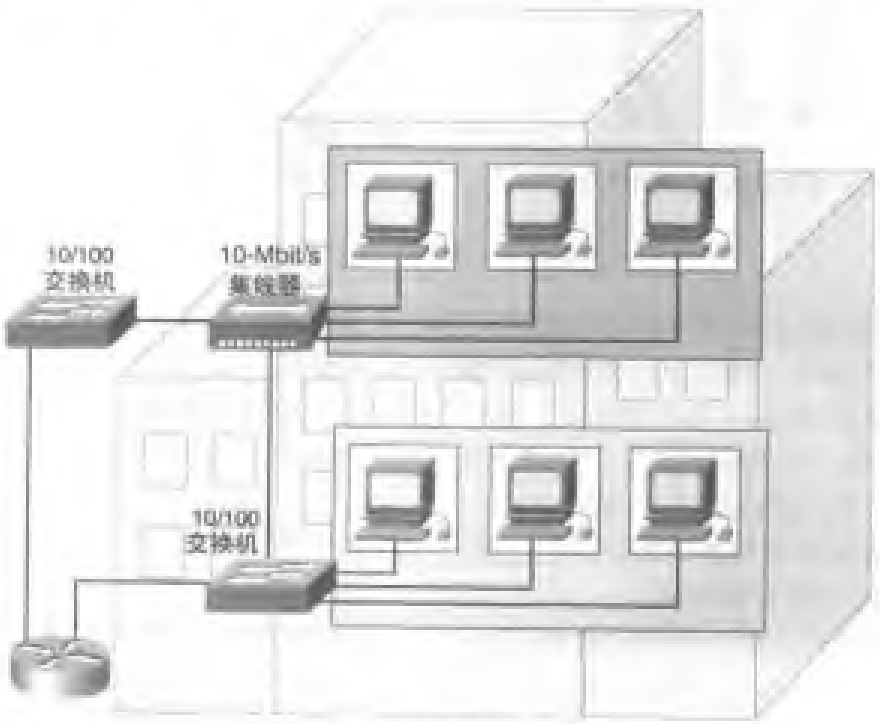


图5-5　目前的LAN

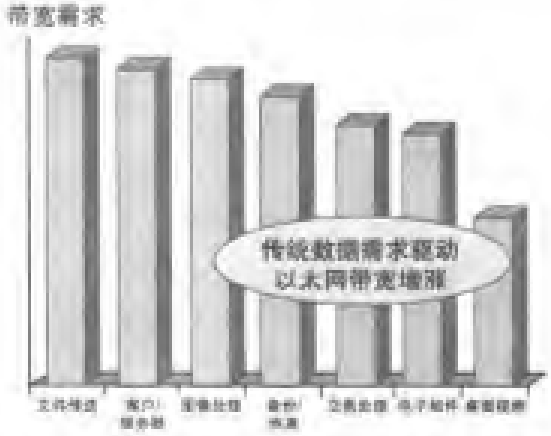
5.1.2 影响网络性能的因素

如今局域网正变得越来越拥塞和不堪重负。除了不断增长的网络用户，图5-6中显示的几个其他因素也一起增加了传统LAN的负担：

• 存在于当前桌面操作系统（如Windows、UNIX和Mac）中的多任务环境允许并发的网络事务。这种增加的能力导致了对网络资源需求的增加。

• 3种最普遍的桌面操作系统（Windows、UNIX和Mac）都支持多任务，用户可以同时开始多个网络事务。Windows95的发布体现了包含多任务功能的重新设计的DOS/Windows。从此PC用户便增加了对网络资源的需求。

• 虽然像万维网（WWW）那样网络密集型应用在不断增加，客户/服务器应用使得管理员能对信息进行集中，使维护和保护这些信息变的更容易。客户/服务器应用使本地工作站从维护信息的繁重劳动和提供足够硬盘空间存储信息的成本中解脱出来。考虑到客户/服务器应用在成本上的益处，这样的应用将来可能更广泛地使用。



• 10 Mbit/s网段上的用户过多
• 太用户访问1台或者2台服务器
• 网络密集型应用（如彩色出版、CAD/CAM、成像技术和关系数据库）

图5-6 网络拥塞的典型原因

5.1.3 以太网/802.3网络的要素

最普通的LAN体系结构是以太网。以太网用来在网络上的设备之间传输数据，例如连接到相同传输介质的计算机、打印机和服务器。以太网介质使用数据帧广播的方式从共享介质上的所有节点发送和接收数据，如图5-7所示。

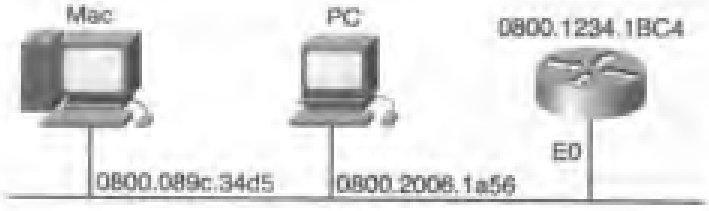
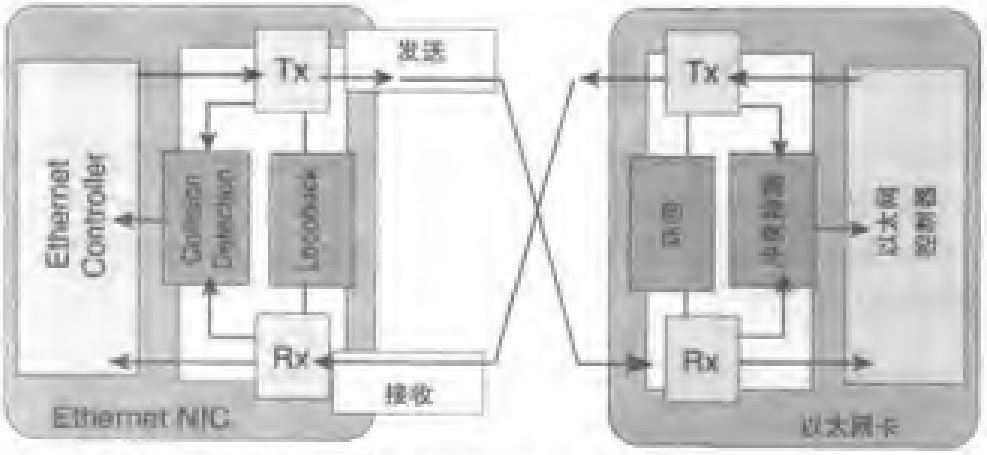


图5-7 以太网/802.3接口

5.1.4 半双工以太网

基础的以太网是一种半双工（half-duplex）技术。如图5-8所示，每个以太网主机在它发送附加

数据之前先查看网络中是否有数据在传送。如果网络已经被使用，发送就被推迟。尽管推迟了传送，两台或多台以太网主机还是可能同时发送数据，这将导致冲突。当冲突发生时，首先检测到这个冲突的主机会发送一个拥塞信号（jam signal）。一旦收到拥塞信号，每台主机将在企图发送前等待一个随机时间段。网络接口卡运行一种“回退算法”（back-off algorithm）来确定其再次试图发送消息前需要等待的随机时间长短。加入网络并开始发送的主机越多，冲突发生的可能性越大。



- 最重要的是发送（Rx）、接收（Tx）和冲突检测
- 以太网物理控制器提供多条电路

图5-8　半双工以太网设计

由于用户运行各种网络密集型的软件，如客户/服务器应用，这些使主机更频繁地和更长时间地发送数据，以太网LAN变得饱和。设备上用于以太网LAN的物理连接器（网络接口卡）提供了多条电路，使得设备间的通信得以发生。

5.1.5　全双工以太网

全双工以太网（Full-duplex Ethernet）可以同时发送和接收不同的分组。同时发送和接收需要使用线缆中的两对导线和每个节点之间的一个交换连接。这种连接被认为是点到点的（point-to-point），并且是无冲突的（collision free）。由于两个节点都能同时发送和接收，因此不需要进行带宽协商。只要现有的共享介质符合以太网的最低标准，就能供全双工以太网使用。

为了同时发送和接收数据，每个节点需要一个专用端口。全双工连接能使用10BASE-T、100BASE-TX（快速以太网）和1000BASE-TX（吉比特以太网）技术利用非屏蔽双绞线（UTP）铜介质来建立点到点的连接。连接也可由使用针对光纤介质的100BASE-FX（快速以太网）或1000BASE-X（吉比特以太网）技术建立。所有连接设备上的网络接口（网络接口卡、端口等等）必须具有全双工能力，并且能够支持同等的速率。以太网的10吉比特版本已经被标准化，但只在光纤介质上运行。

使用铜介质时，全双工以太网或快速以太网利用线缆中的两对电线，在一端的发送（TX）和另一端的接收（RX）之间创建一个直接连接。通过用这种方式连接两台工作站，就建立起一个无冲突的环境，因为数据的发送和接收发生在两条无竞争的电路上。UTP铜缆上的吉比特以太网使用线缆中所有的4对导线，利用精密的电路在两个方向同时传送。支持光纤的所有以太网版本都使用两条线，一条为TX，另一条为RX。

单独使用LAN交换可以减少冲突，因为每两个端口间的连接建立了一条专用虚拟电路。全双工传输翻倍了节点之间的带宽，显著地增加了带宽。工作站间的全双工传输可以通过点到点以太网连接获得。在两个占用高带宽的消费者之间，如一台交换机与一台服务器或两台交换机之间的连接，这一特性可能很重要。全双工传输提供了一个无冲突的传输环境，因为两个节点能同时发送和接收，

不进行带宽协商。

例如，在10Mbit/s的连接上，全双工传送可以提供10Mbit/s的发送容量和10Mbit/s的接收容量，等效于在单一连接中20Mbit/s的容量。同样，一个100Mbit/s连接能提供200Mbit/s的吞吐量，如图5-9所示。全双工通信支持多路径数据传送，速率最高可达2Gbit/s。



图5-9 全双工技术

5.2 局域网交换技术简介

交换是一种通过减少通信、增加带宽从而降低局域网拥塞的技术。*局域网交换机*（LAN swiiches）通常取代了共享集线器，并被设计工作在现有的线缆基础设施上，从而实现在不中断现有网络流量的情况下安装。

网络交换机采用微分段技术，降低局域网内部冲突的数量，从而增加了带宽。局域网交换机还支持像全双工通信和多路同时会话这样的功能。全双工通信可使两台设备在同时相互交流。全双工通信有效的将局域网交换机的传输吞吐量增加到2倍。在一个使用交换机的全双工局域网内，不会出现冲突。

有三种交换模式可以用于交换机内帧的传发：*贯穿式*（cut-through）、*存储转发式*（store-and-forword）、无碎片式（fragment-free）。每种交换模式的等待时间或者说*延迟*取决于交换机如何转发帧。速度越快的交换模式，发生的延迟时间越短。

在交换机内工作在OSI参考模型的第2层中的局域网交换机和网桥基于MAC地址转发帧，从而实现交换功能。如果第2层MAC地址未知，设备会试图将帧通过泛洪传输至想至的目的地址。交换机和网桥会转发所有广播帧，结果将形成贯穿整个网络的、不停息的广播风暴环路。*生成树*（spaning tree protocol）协议是阻止形成环路的协议，可以使交换机通过相互的交流发现网络的物理环路。*生成树*协议允许将多余的路径作为备份，在不需要时其中的一条路径会禁用。

5.2.1 局域网分段

对局域网进行分段有两个重要原因。第一是隔离分段间的通信，第二是通过产生小的冲突域获取更多带宽。

如果不进行局域网分段，比小工作组大的局域网将会被通信和冲突阻塞，几乎无法提供带宽。局域网的分段可以通过对网桥、交换机、路由器的实现。每种设备都有优点和缺点。网络可以被分为更小的单位，也就是网段（segment）。每一个网段都采用*CSMA/CD*的访问方式，维持网段内用户之间的通信。

图5-10显示的就是一个示例的分段以太网。整个网络有15台计算机，（6台文件服务器和9台（PC）。在网络中通过使用网段，通信时共享10Mbit/s的带宽的网段用户/设备更少。每个网段都是各自冲突域，如图5-11所示。

通过将网络划分为3个网段，网络管理员可以减少每个网段内部的网络拥塞。在网段内部传输数据时，每个网段内的5台设备可以共享10Mbit/s的带宽。在一个分段的以太局域网中，网段间传输的数据通过网桥、路由器、交换机在网络骨干上传输。骨干网段（网段4）传送来自其他三个网段的帧。

局域网交换的基本原理为：提供微分段，以利于专用网段的形成，为网络上的每个用户提供专用带宽。每个用户都可以使用全部的带宽，不需要跟其他用户争夺有效带宽。这就意味着连接到同一交换机上的成对设备可以在最小的冲突数量下并行通信。微分段技术通过降低冲突域的大小减少了冲突的数量。这就增强了每台连接到网络上的站点的网络容量。

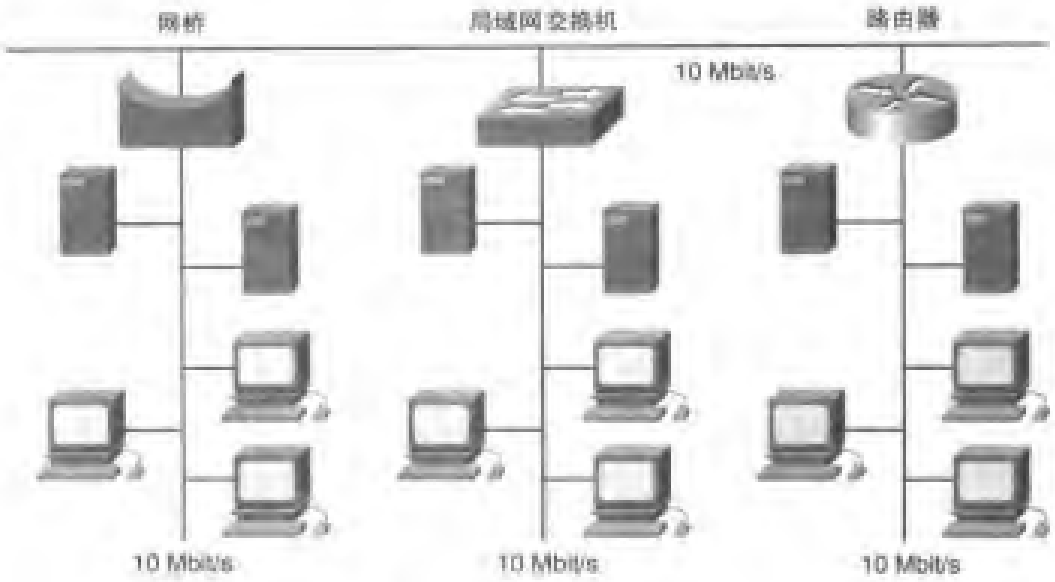


图5-10　分段的网络

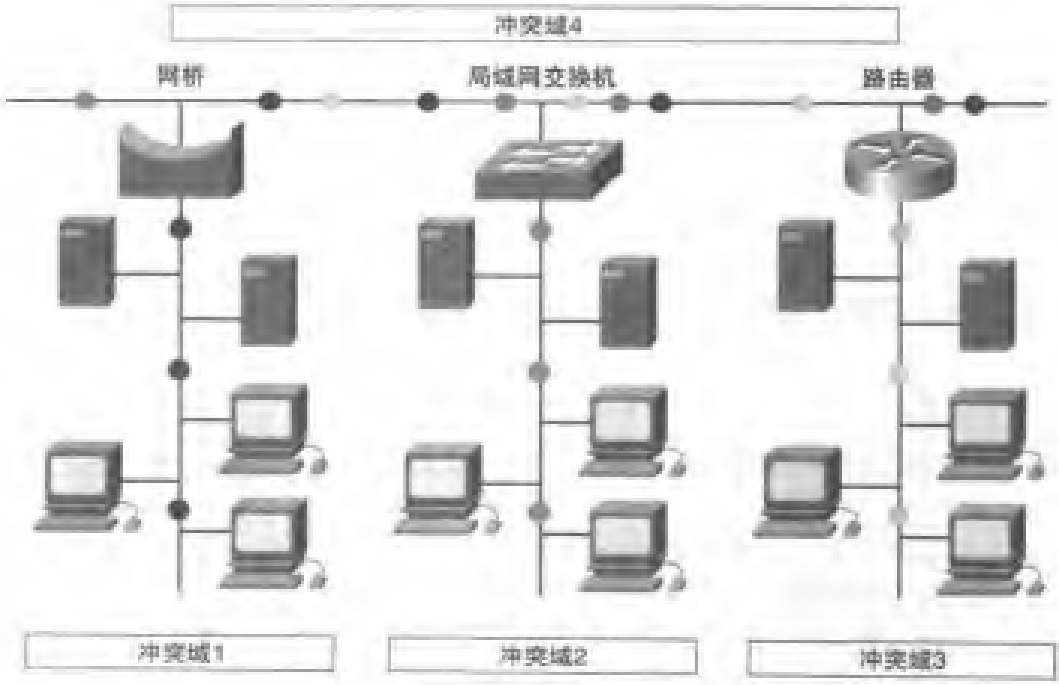


图5-11　冲突域

5.2.2　使用网桥的局域网分段

用网桥对局域网进行分段，每个网段上的用户数减少了，这就为每个用户提供了更多的带宽。相反，不用网桥对局域网进行分段时，每个用户的带宽较少，因为很多用户位于同一个未分段的LAN上。图5-12显示了使用网桥分段的局域网。

网桥通过构建包含各个网络设备地址的地址表并告知通过哪个网段到达该设备来“学习”网络的分段。图5-13显示了网桥如何使用桥接表来标识整个网络中的各个不同节点。网桥为第2层设备，能够根据帧的MAC地址转发数据帧。另外，网桥对网络上的其他设备是透明的。

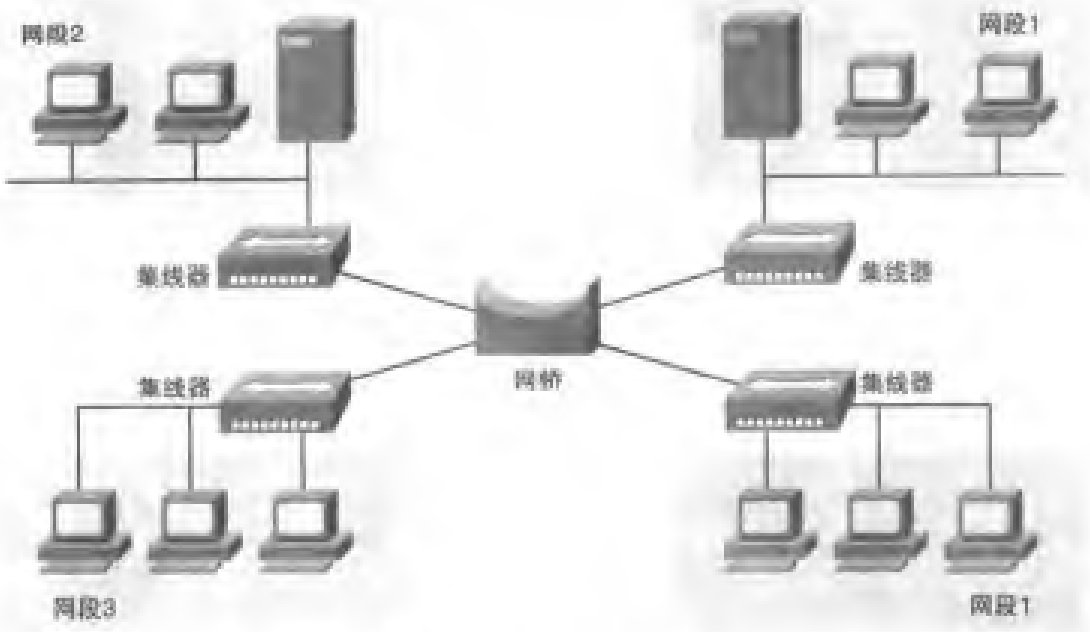


图5-12 使用网桥进行分段



图5-13 桥接表

如图5-14所示，网桥通过检查源MAC地址获知站A、B、C、D的位置。如果网桥获取了一个无法识别其源地址或目的地址的帧，网桥会将其源地址添加到桥接表中，并将帧转发到除了接收帧的接口之外的所有接口。当收到回复时，网桥检查源地址，并将该站加入到桥接表中。然后，网桥便能转发设备间的后续通信了。

网桥将网络的延迟增大了10%-30%。网络的延迟主要是因为网桥的决定时间或者网桥的数据传输时间。网桥被认为是一台存储转发设备，在将帧传输到所有的端口之前，网桥必须检查目的地址字段，并计算检查帧校验序列字段中的循环冗余校验（CRC）。如果目的端口忙，网桥可以临时存储帧直到目的端口空闲。

执行这些任务将减慢网络的传输，引起延迟的增加。

5.2.3 使用路由器的局域网分段

路由器是比普通的网桥更高级的设备。网桥在网络中是被动的，在数据链路层上运行。路由器在*网络层*上运行，路由器基于网络层协议地址作出在网段间的转发决定。通过将数据转发到跟工作站相连的集线器，路由器创建了最高级的分段。通过检查数据分组的目的地址和自己的路由选择表，路由器决定如何将帧转发到网段。如图5-15所示。

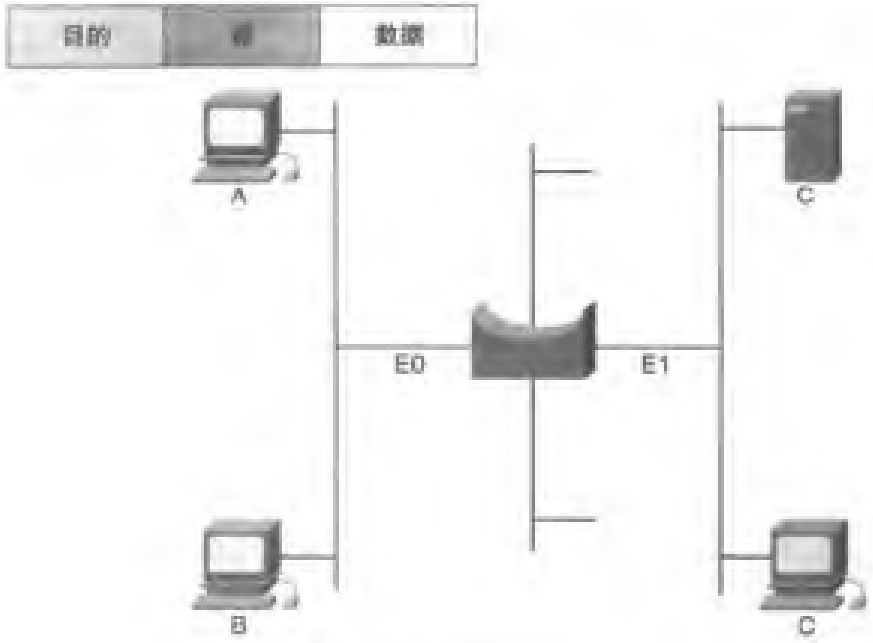


图5-14　使用网桥的分段



图5-15　使用路由器的分段

路由器必须通过检查分组来决定将分组转发至目的地的最佳路径。这个过程需要一定的时间。协议要求接收方对发送方发送的每一个分组进行确认（被称为是面向确认的协议（acknowledgement-oriented protocols））。这个过程大概会产生30%-40%的吞吐量损耗。所需确认最少的协议（滑动窗口协议（sliding-window protocols））。吞吐量有20%-30%的损耗。这是因为在发送方和接收方之间的数据通信比较少（也就是确认比较少）。

5.2.4　使用交换机的局域网分段

局域网交换减轻了类似于几台个人电脑（PC）和远程文件服务器之间传输时带宽的缺乏和网络瓶

颈。一台交换机可以将局域网分成多个微分段（microsegments），微分段由两台主机构成，如图5-16所示。这就可以在大的冲突域中产生很多小的无冲突域。虽然局域网交换机消除了冲突域，但所有与交换机相连的主机依然在同一个广播域内。因此，所有通过局域网交换机连接的节点能够看到一个节点发出的广播。其他优势包括低延迟，各端口帧转发速率高，与已有的802.3（CSMA/CD）兼容的接口卡、集线器、线缆的兼容性。

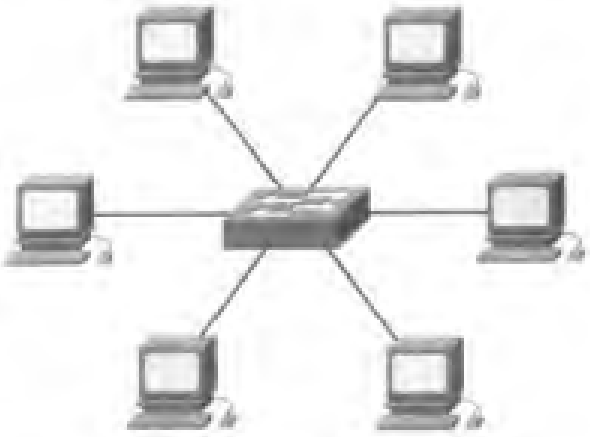


图5-16 使用交换机的分段

交换式以太网（Switched Ethernet）基于以太网（Ethernet），每个节点都直接与交换机的一个端口相连，或者跟与交换机端口相连的网段直接连接。这就在交换机的每个节点和每个分段之间产生了10 Mbit/s、100 Mbit/s或1 000 Mbit/s带宽的网络连接（由使用的以太网版本决定）。一台直接与10Mbit/s以太网交换机相连的电脑，有自己的冲突域，并且能够达到10 Mbit/s的带宽。例如，如果一台12口的交换机，各个端口都与一个设备相连，就会产生12个冲突域。

使用交换式以太网拓扑的局域网会创建一个仿佛只有两个节点——发送节点和接收节点的网络。这两个节点共享10Mbit/s带宽，这就意味着几乎所有的带宽都可以传输数据。因为交换式以太局域网对于带宽的利用率高，它可以提供比通过网桥或集线器连接的以太网更大的吞吐量。在交换式以太局域网中，可用的带宽可以接近100%。

通过创建专用的网络分段（点到点连接）并将这些分段连接到交换机内的虚拟网络上，以太网交换技术增加了网络上可用的带宽。这个虚拟网络电路只有在两个节点间需要通信时才会存在。这就是为什么它被称为虚电路（virtual circuit），它只有在需要的时候才会产生，并只存在于交换机内部。

交换机的一个缺点就是成本比集线器要高。然而，某些企业选择慢慢布署交换技术，即将集线器连接到交换机，直到有一天集线器能被全部取代。交换机的速度和处理能力将会不断提高，成本也会逐步降低。几乎所有新的以太局域网在设计时都应用了交换技术。

5.3 交换机的基本操作

交换技术通过减少通信、增加带宽，降低了以太局域网、令牌环局域网、光纤分布式数据接口局域网（FDDI）中的拥塞现象。局域网交换机通常用来取代共享集线器。局域网交换机设计用于使用现存的线缆基础设施，以便能在不中断现有网络通信的情况下进行安装。

在现今的数据传输中，所有的交换设备都执行两个基本的操作：

- **交换数据帧**：当帧从一条入介质到达，被发送到一条出介质时执行该功能。
- **维护交换操作**：交换机建立和维护交换表。

术语“桥接（bridging）”是指通过使用被称为“网桥（bridge）”的设备，连接两个或多个LAN网段的技术。交换机是应用桥接技术发展起来的，并通常被称为多端口网桥。网桥将数据报从一个网段传输到位于其他网段的各个目的地。当网桥开机并开始运行时，网桥会检查输入数据报的MAC地址，并建立已知目的地址的列表。如果网桥知道数据报的目的地址与源地址在一个网段内，会将报表丢弃，因为无需传送。如果网桥知道数据报的目的地在另一个网段，网桥会只将数据报传递到目的网段。如果网桥不知道目的网段，就会将数据报传输到除源网段以外的所有网段（称为泛洪）。网桥的主要优点就是限制了某些网段之间的通信。

网桥和交换机都连接到局域网网段，都通过MAC地址列表决定数据报需要传输到的目的网段，都能减少流量。在现今的网络中，交换机比网桥具有更多的功能，因为交换机提供了更强的连接，

比网桥更快的运行速度，能够支持新的功能，比如虚拟局域网（VLAN）。网桥一般通过软件实现交换，而交换机通过硬件实现交换。

本节主要讨论局域网交换机的基本操作。图5-17所示为一个局域网，有3台工作站，1台局域网交换机，和局域网交换机的地址列表。局域网交换机有4个接口（或叫做网络连接）。A工作站和C工作站都连接交换机的接口3，B工作站连接交换机的接口4。A、C工作站很可能连接到一个与交换机接口3相连的集线器。如图5-17所示，A工作站需要发送数据到B工作站。

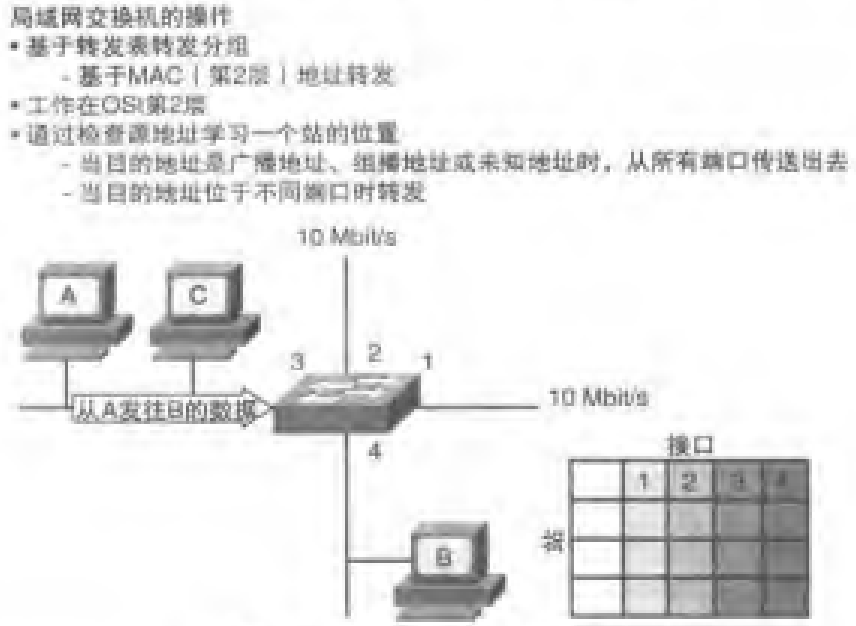


图5-17　LAN交换机基本操作

请注意，在通信穿越网络的过程中，交换机工作在第2层，这意味着交换机能查看MAC层地址。当A工作站发送，交换机接收帧时，交换机在通信通过时对其进行检查，以发现源MAC地址，并将其保存在地址表中，如图5-18所示。

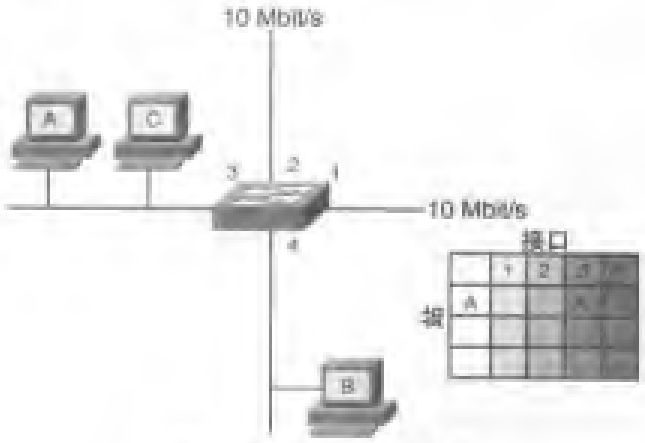


图5-18　构建一个地址表

当通信经过交换机时，地址列表将生成一条标识源工作站和它所连接的交换机接口的条目。交换机现在已经知道A工作站连接到哪里。当数据帧在交换机内时，由于目的工作站未知，数据帧会泛洪到所有的端口，如图5-19所示。

在地址表中加入地址条目后，B工作站向A工作站发回了一个响应。这样，交换机得知B工作站与接口4相连，如图5-20所示。

需要注意的是，该响应数据进入交换机时，这时交换机并不对其进行泛洪，交换机只会把数据

传递给接口3，因为他知道A工作站的位置，如图5-21。

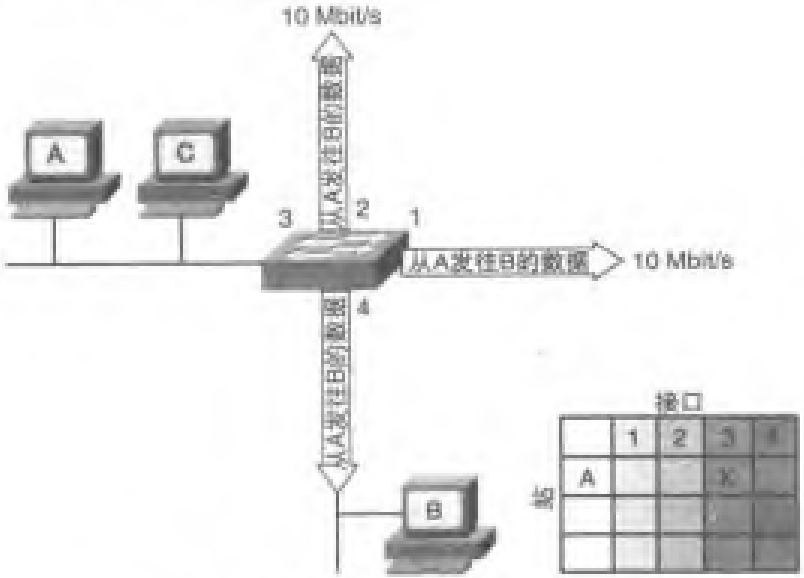


图5-19 泛洪数据到交换机的所有端口

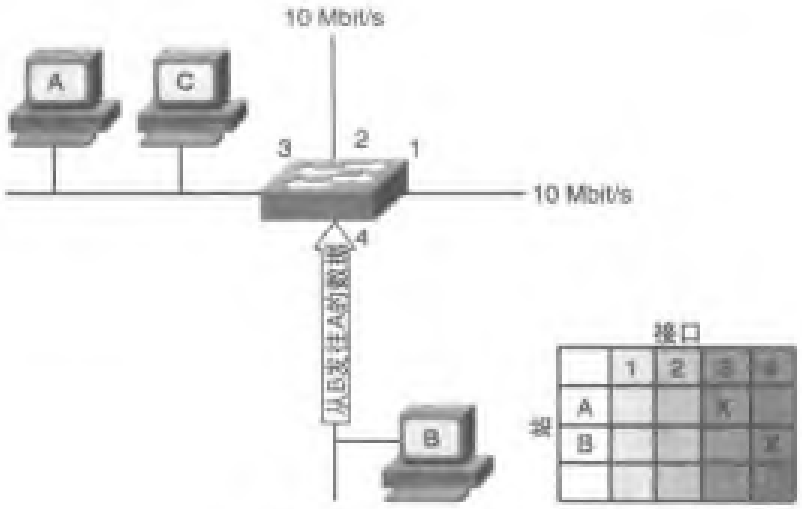


图5-20 响应泛洪消息

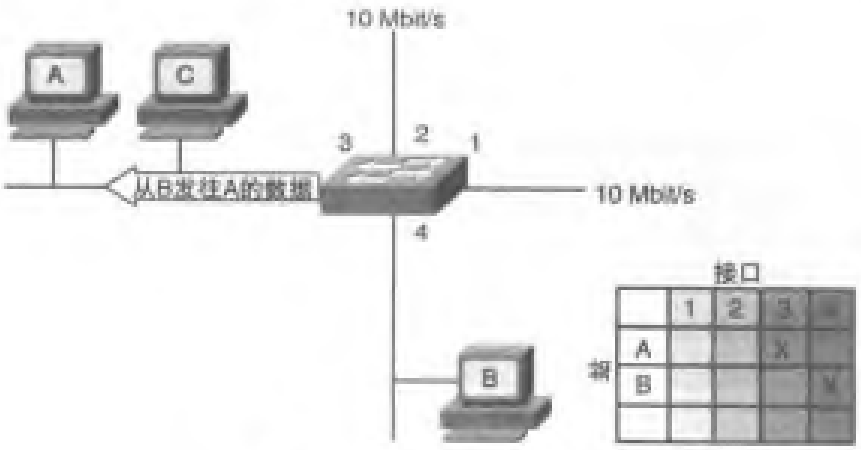


图5-21 传输数据到一个已知站

最初的传输能够指出MAC地址的来源，从而使交换机能更高效地传递网络中的通信。

5.3.1　以太网交换机延迟

以太局域网中的每一台交换机都会增加网络的延迟。然而，延迟多少由交换机的品牌以及所采用的交换技术决定。正如随后要讲到的，各种交换模式（*存储转发交换*、*无碎片交换*、*快速转发*fast forward）的区别在于对进行的帧作出交换决定的时机不同。由于交换机“作出决定”而造成的延迟需要与帧进入和离开交换机端口的时间加和，以确定交换机总共的延迟。

集线器只是一种简单的转发帧的设备（没有过滤与决定过程），因此只有端口到端口的延迟。所有的这些只有一秒的数分之一的延迟看上去无关紧要，但不要忘记我们发送数据的速率为10Mbit/s（1bit/千万分之一秒）、100Mbit/s（1bit/亿万分之一秒）或1 000Mbit/s（1Gbit/s，1bit/十亿万分之一秒）。网络设备以令人难以置信的高速运行，所以每纳秒都很重要。

5.3.2　第2层与第3层交换技术

有两种交换数据帧的方式：一种是第2层交换技术，如图5-22所示；另一种是第3层交换技术，如图5-23所示。交换（switching）是从一个接口接收帧，并将其传送到另一个接口的过程。路由器采用第3层交换技术对分组进行路由，交换机（第2层交换机）采用第2层交换技术转发帧。



图5-22　第2层交换技术

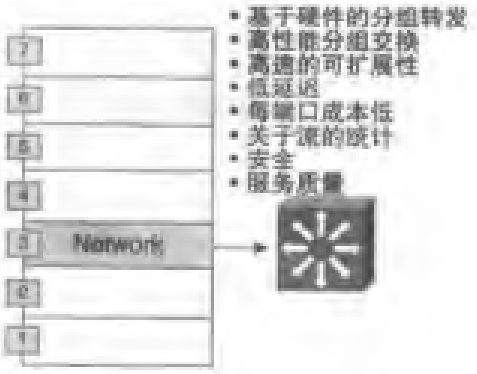


图5-23　第3层交换技术

第2层和第3层交换技术的区别在于确定输出接口时所使用的帧内的信息不同。采用第2层交换技术时，帧是基于MAC地址信息进行交换的。

采用第3层交换技术时，帧的交换基于网络层信息。不同于第3层交换技术，第2层交换技术不查看分组内网络层的信息，第2层交换查看帧内部的目的MAC地址。如果知道目的地址的位置下，第2层交换就将信息发送到适当的接口。第2层交换会建立和维护一个交换表以记录每个端口或接口的MAC地址信息。

如果第2层交换机不知道把帧传送到哪里，交换机将通过其所有端口把帧广播到整个网络，以便查找正确的目的地。在获得帧的回复后，交换机得知新地址的位置，并将地址添加到交换表中。

数据通信设备的制造商负责确定2层地址。这是由两部分构成的惟一地址：制造商（MFG）代码和惟一标识符。*电气与电子工程师协会*（IEEE）为每一个设备供应商分配MFG代码。设备供应商负责分配到惟一标识符。除了在SNA网络中，用户对于第2层地址几乎没有控制权，因为第2层地址是固定在设备中的。而第3层地址是可改变的。另外，第2层地址是全球惟一地址，采用了一个平面地址空间。

第3层交换在网络层上工作。它负责检查分组信息并根据分组的网络层目的地址转发分组。第3层交换技术也支持路由器的功能。

在绝大多数情况下，网络管理员可以决定第3层地址。因特网协议（IP）、网间分组交换（IPX）、Apple Talk等协议都使用第3层寻址。通过创建第3层地址，你可以创建作为单个寻址单元的本地区域（如街道、城市、州或国家），并为每个本实体分配一个编号。如果用户搬入另一座建筑，终端站将获得新的第3层地址，但第2层地址保持不变。

由于工作在OSI参考模型的第3层，路由器能使用现有的分级寻址结构或创建新的寻址结构。这样，被路由的网络可以将一个逻辑寻址结构与网络物理基础设施绑定。例如，为每个网段绑定TCP/IP子网或者IPX网络。交换（平面）网络中的通信流和被路由（分层）网络中的通信流有本质区别。由于分级网络能通过网络分级来确定最佳路径和包含广播域，因此能提供比平面网络灵活性更高的通信流。

5.3.3 第2层交换与第3层交换的含义

桌面式电脑处理能力的不断增强，对客户机/服务器以及多媒体应用技术的需求的增加，都对传统的共享-介质运行环境提出了更高的带宽需求。这些需求推动着网络设计者们在配线室用交换机取代集线器。

第2层交换机采用微分段技术满足对更大带宽和更高的性能的需求，但是网络设计者们会面对的是不断增长的子网络间通信的需求。例如，当用户每次访问服务器和位于其他子网络的资源时，流量必须通过第3层设备，如路由器。有可能这里是一个很大的瓶颈，会威胁到网络性能。为了避免这种瓶颈，网络设计者们在整个网络中都增加第3层功能，这样就减轻了中央路由器的负担。可以使用第3层交换机，它包含了路由选择技术。交换机通过分隔冲突域和有选择性的将通信传输到网络中恰当的网段，从而增加了网络带宽。

5.3.4 对称交换和非对称交换

对称交换是一种根据交换机上分配给每个端口的带宽描述局域网交换特征的方式。如图5-24所示。对称交换在相同带宽的端口方向建立交换连接，如全部为10Mbit/s端口，或全部为100Mbit/s端口。如图5-25所示。非对称局域网交换在带宽不同的端口之间建立交换连接，如10Mbit/s和100Mbit/s的组合或者100Mbit/s和1 000Mbit/s的组合。

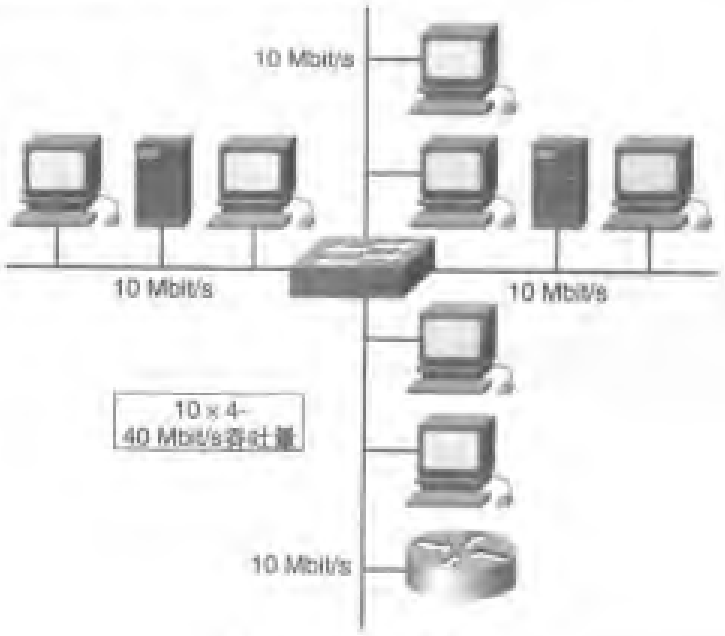


图5-24 对称交换

非对称交换技术多用于客户机/服务器环境中，该环境下多个客户机会同时与单个服务器进行通信，这要求服务器所连接的交换机端口能提供更多的专用带宽，以防止出现瓶颈。在下一节你将学到，在非对称交换中需要使用内存缓冲来使得100Mbit/s端口的通信能传送到10Mbit/s端口而不会在10Mbit/s端口上造成拥塞。在垂直布线或骨干网段的交换机之间也需要用非对称交换提供高带宽。

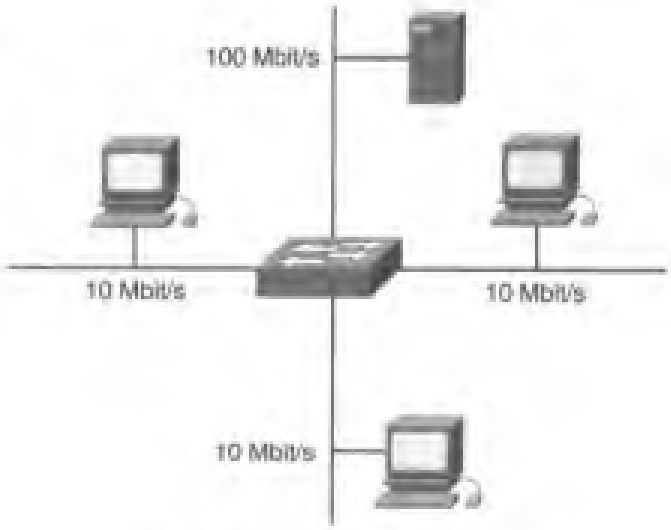


图5-25　非对称交换

5.3.5　内存缓冲

以太网交换机可能采用缓冲技术存储并将分组转发到正确的端口。当目的端口忙时也会用到缓冲技术。交换机中存储数据的内存区域被称为内存缓冲区（memory buffer）。内存缓冲区可以采用两种方法来转发分组：基于端口的内存缓冲（port-based memory buffering）和共享内存缓冲（shared memory buffering）。

采用基于端口的内存缓冲时，分组存储在与特定输入端口相连队列中。只有当队列中所有先于它的分组转发成功后，该分组才会被转发到输出端口。如果目的端口繁忙，单个分组可能延迟队列中所有的分组的传输。即使其他的分组能被传送到空闲的目的端口，也会受这单个分组的影响而产生延迟。

共享内存缓冲将所有的分组存储在交换机所有端口共享的一个公共的内存缓冲区中。分配给每个端口的内存大小由每个端口的需求量决定。这就叫做缓冲内存的动态分配（dynamic allocation of buffer memory）。然后，缓冲区内的分组被动态地连接到发送端口；即分组被链接到该发送端口的内存中。这便实现了从一个端口接收分组，然后从另一个端口发送，而不用将其移动到另一个队列中。

交换机维护需要转发的分组与目的端口的映射。在分组成功转发后，交换机清除该映射。因为内存缓冲区是共享的，分组大小是整个内存缓冲区尺寸的限制，而不是分组单个端口的内存大小。这就意味着传送大分组时的分组丢失更少。对于需要从100Mbit/s端口转发分组至10Mbit/s端口，或1 000Mbit/s端口转发分组至10Mbit/s的非对称交换而言，这是很重要的。

5.4　局域网设计

尽管设备的性能和介质的能力有了改进，但网络设计却正变得更加困难。发展趋势是涉及多种介质类型和与单个组织所控制的局域网以外的网络相互连接的复杂环境。记住这些关键因素很重要。仔细设计的网络能减少伴随网络环境发展而出现的困难。

确保建立一个高速、稳定的网络的几个关键步骤中的一个就是网络设计。如果网络的设计不正确，可能出现很多不可预见的错误，网络的增长也受到危害。设计过程是一个深入的过程。本章将对网络设计过程进行概述，也包括了局域网设计的目标、网络设计面临的问题、网络设计方法论和局域网拓扑的发展。

5.4.1　网络设计的目标

设计网络是一项富有挑战性的工作，并不仅仅是把计算机连接起来。要达到可靠、可管理和可扩展，网络需要具备很多特性。要设计一个可靠的、可管理、可扩展的网络，网络设计师应该意识到网络中每个主要组成部分都有其独特的设计需求。

设计局域网的第一步是建立和编写设计目标。这些设计目标对于每一个组织或者环境都是惟一的。下面是在绝大多数网络设计中的一些需求：

功能性（Functionality）——网络必须可工作。网络要满足用户的工作需求，为用户与用户之间、用户与应用之间的连接提供合理的速度和可靠性。

可扩展性（Scalability）——网络必须能够发展。最初的设计应该具有在不改变网络整体设计的前提下进行升级的能力。

适应性（Adaptability）——网络设计应该考虑到未来的技术，因此不应该包含可能限制新技术布署的因素。

可管理性（Manageability）——网络的设计应该便于网络监控和管理，以确保网络运行的稳定性。

这些需求在某些类型的网络中是具体的，在其他类型的网络中是笼统的。

5.4.2 局域网设计的考虑因素

随着类似占比特以太网等高速技术的出现，以及采用局域网交换技术和虚拟局域网技术（VLAN）的更加复杂的局域网体系结构的应用，很多组织正在升级现有的局域网络或者正在计划、设计和组建新的局域网。尽管异步传输模式（ATM）被广泛应用于广域网中，但它已经不再是今天的局域网设计所需要考虑的一个重要因素了。

为确保局域网带宽和性能的最大化，必须考虑局域网设计中的以下注意事项：

- 服务器的位置和功能。
- 网络分段问题。
- 广播域问题。

5.4.3 服务器的位置和功能

服务器提供文件共享、打印、通信以及各种应用服务。服务器的功能跟工作站不同。服务器运行专门的操作系统，像Netware、Windows NT/2000/XP、UNIX和Linix等。每一台服务器通常专门完成一项功能如电子邮件或文件共享。

服务器可以分为两大类：***企业服务器***（enterprise servers）和工作组服务器（workgroup servers）。企业服务器为网络上的所有用户提供如E-mail或者域名系统（DNS）这样的服务。E-mail或者DNS是组织内的所有人都需要的一种服务，是一种集中式功能。另一方面，工作组服务器支持一个特定的用户群体，提供如文字处理、文件共享这样的服务，这些服务都只有少部分用户群使用。

企业服务器一般放置在主配线间（main distribution facility, MDF）中。这样，到企业服务器的通信只需要传输到MDF，不需要通过其他网络传输。工作组服务器最好放置在靠近用户的中级配线间（intermediate distribution facilities, IDF）处，以便用户可以快速的访问这些服务器中的应用。通过将工作组服务器放在接近用户的位置，通信只需要经过到达某个IDF的网络基础设施，不会对网段内的其他用户造成影响。在MDF和IDF内部，第2层局域网交换机与这些服务器的连接速率应该有100Mbit/s或者更高。

5.4.4 网络分段问题

如图5-26所示，网络分段是将单一的冲突域分割为两个或更多的冲突域或者带宽域的过程。第2层（数据连接层）网桥或者交换机用来分割一个逻辑的***总线型拓扑***，形成多个分离冲突域，这样就可以为单个的工作站提供更多的带宽。在图5-27中，网桥和交换机虽然不转发冲突，但是他们转发广播分组，因此整个总线型拓扑仍然表现为一个单独的广播域。

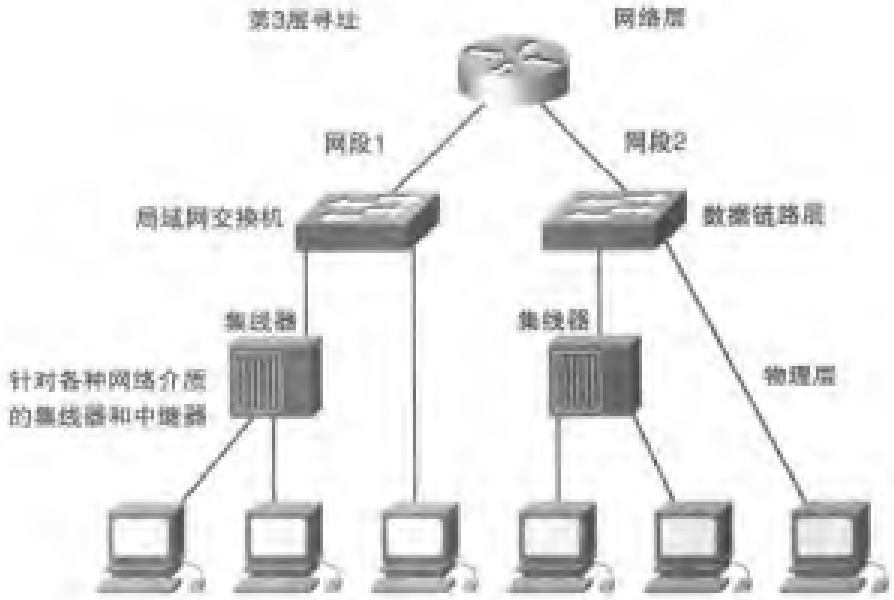


图5-26　局域网技术的发展

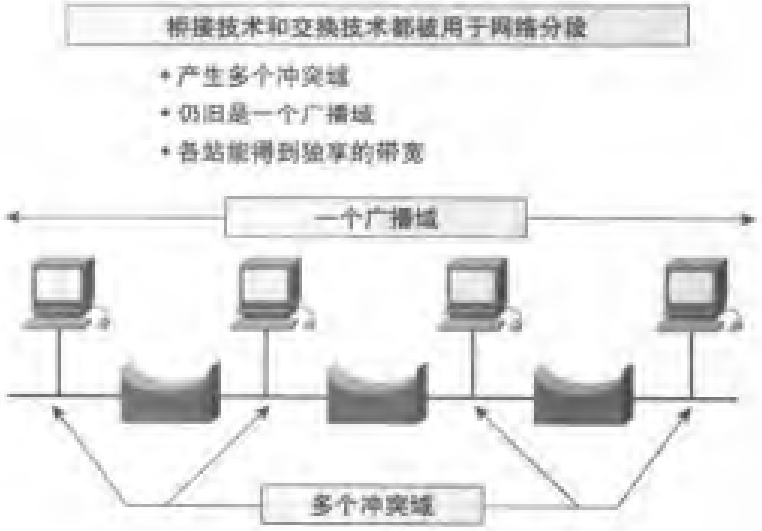


图5-27　分段

来自第2层广播域中的任何主机的所有广播，对于同一个广播域中的其他主机都是可见的。为建立连通性，广播对广播域内所有的主机必须是可见的。带宽域（bandwidth domain）的扩展性取决于总的通信量，广播域（broadcast domain）的扩展性取决于广播通信的总量。请记住网桥和交换机会转发广播（FF-FF-FF-FF-FF-FF）通信，而路由器通常不转发。

5.4.5　广播域问题

带宽域（bandwidth domain）是指跟网桥或者交换机上的一个端口连接的所有东西。如果采用以太网交换机，一个带宽域也就是一个冲突域。如图5-28所示。一台交换机可以在每个端口形成一个带宽域。一个带宽域中的所有工作站竞争使用相同的局域网带宽资源。在带宽域中来自任一主机的通信对于其他主机都是可见的。对于以太网冲突域而言，两台工作站同时传输就形成冲突。

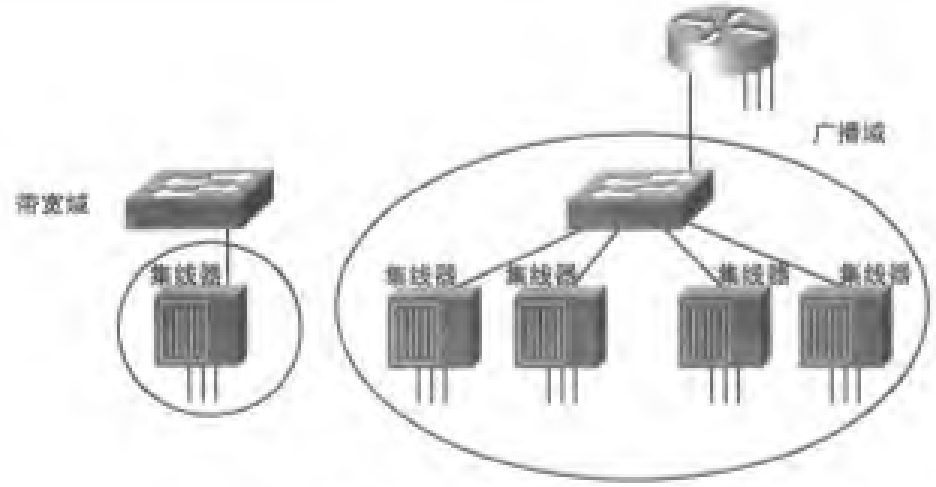


图5-28 带宽域和广播域

5.4.6 局域网设计方法论

为了有效地满足局域网用户的需求，局域网必须依据有计划的系统步骤来进行设计和实施。主要包括：

- 收集用户的需求和期望。
- 进行需求分析。
- 设计第1层、第2层、第3层局域网结构（拓扑）。
- 编写逻辑和物理网络的实施文档。

设计网络的第1步是搜集有关组织结构的数据。这些信息包括组织的历史和目前的状况、发展方向、运营政策和管理流程、办公系统和办公流程以及使用局域网的人员的观点。你需要回答下列问题：哪些人将使用网络？他们的技术水平、以及他们对于计算机和计算机应用的观点。回答类似这样的问题可以帮助你决定需要提供多少培训，以及需要多少人员来支持局域网。

理想情况下，信息收集的过程能够帮助你弄清并确定问题。你还需要确定是否有成文的政策。是否有数据被声明为任务关键数据？是否有某些操作被声明为任务关键操作？（任务关键（mission-critical）数据和操作是对企业至关重要的数据和操作，对它们的访问对于企业的日常运行是十分关键的）网络上允许哪些协议？是否只支持台式主机？

接下来，需要决定组织内谁有权利分配地址、命名、进行拓扑设计和配置。有些公司由一个中央管理信息系统（Mis）部门控制一切。其他公司的管理信息部门（MIS）比较小，需要委派人员对其进行管理。焦点在于资源的定位以及公司的约束条款。影响新的局域网系统建设的组织资源通常可以分为两类：计算机硬件/软件资源和人力资源。一个组织的现有计算机硬件和软件必须有文档记载，计划购置的软件和硬件必须得到确定。这些现有资源是如何连接和共享的？组织能够提供什么样的财物资源？记录这类事情有助于估计局域网的成本并做出预算。你必须确定自己理解了现有网络的性能。

设计网络的下一个步骤是分析在上一步获取的用户需求和网络需求。网络用户的需求会经常改变，例如，随着基于语音和视频的网络应用成为可能，关于增强网络带宽的压力会变得更大。

分析阶段的另一个组成部分是评估用户的需求。不能够及时、准确为用户提供信息的局域网几乎是无用的。因此，必须确保局域网的设计能够满足组织及其员工的信息需求。

5.4.7 影响局域网可用性因素

可用性（avaliability）用来衡量网络的有用程度（usefulness）。很多因素影响可用性，包括：

- 吞吐量。
- 响应时间。
- 对资源的访问。

每个客户对于可用性都有不同的定义。例如，他们可能需要在网络中传输语音和视频。这些服务需要网络或骨干提供更多的带宽。可以通过增加更多的资源来提高可用性，但资源的增加将导致成本的上升。网络设计就是要用最低的成本提供最高的可用性的方法。

5.4.8　物理网络拓扑的设计

在确定网络的整体需求后，下一步就是决定满足用户所有需求的网络整体拓扑。在这一节里，我们将集中讲述*星型拓扑*（star topology）和*扩展星型拓扑*（extended star topology）。如图5-29所示，星型拓扑、扩展星型拓扑应用以太网802.3技术。本教程中主要关注CSMA/CD星型拓扑是因为它是目前业界的主流配置。

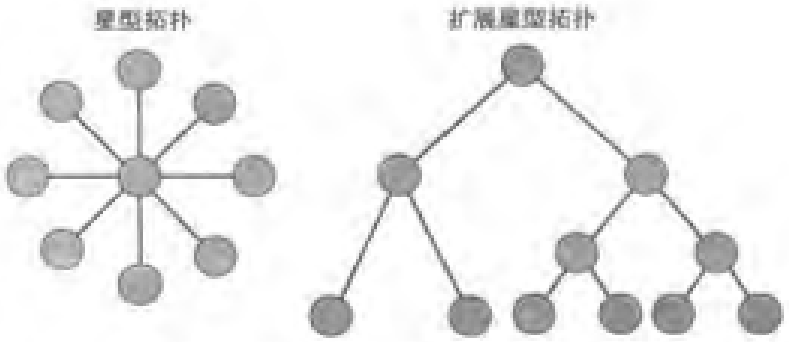


图5-29　广播域

如图5-27所示，局域网拓扑的设计可以分成符合OSI参考模型的3个独特的类别：网络层、数据链路层、物理层。这些方面将在下面的各节中进行讨论。

5.4.9　第1层设计

在这一节中，你将研究第1层星型拓扑和扩展星型拓扑，如图5-26所示。

在设计网络时，物理线缆是需要考虑的最重要部件之一。设计问题包括采用哪种线缆（通常铜线或者光纤）和整体的布线结构。第1层布线介质包括各种类型的介质，如5类UTP和光缆，以及关于布线方案的连接和布局，如图5-30所示。

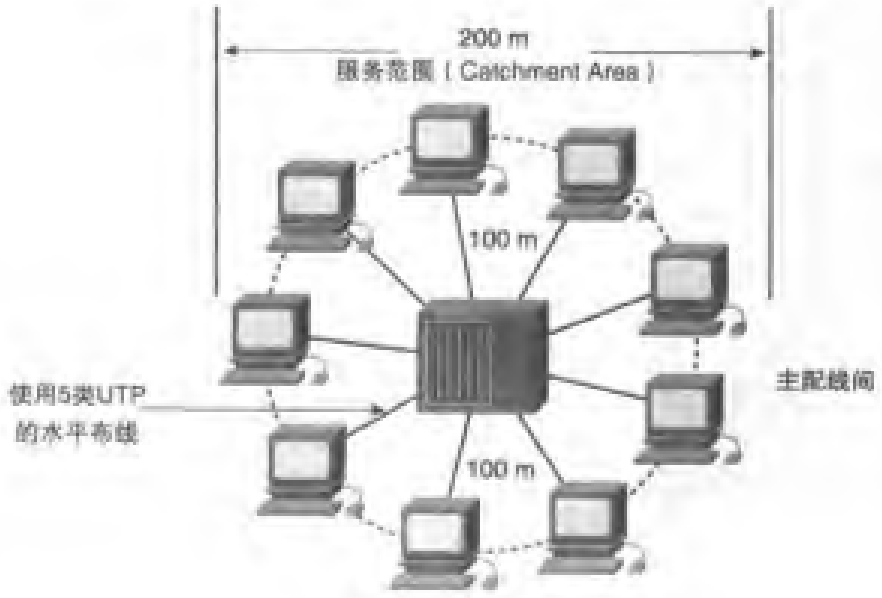


图5-30　星型拓扑

除了最大距离限制，你还必须仔细的评估各种类型的线缆，网络的有效性受下层线缆的影响。第1层的问题可以导致很多的网络问题。如果计划对一个网络进行重大的调整，必须进行完整的线缆检查，以确定哪些区域需要升级或重新布线。

无论是设计一个新的网络或是对已有网络进行重新布线，都应该在骨干和垂直布线中采用光纤，在水平布线中至少采用5类UTP，同时需要考虑新的超5类和6类UTP的标准。如果网络的设计寿命为7到10年，线缆的质量应该是优先考虑的，即使需要为每英尺花费更多的费用。线缆升级应该优于其他改变，企业应该确保——毫无例外的——这些系统满足工业标准，如TIA/EIA-568-B标准。

TIA/EIA-568-B标准规定，每一台连接到网络的设备都应该通过水平布线与中心位置相连。如果所有需要访问网络的主机都位于TIA/EIA-568-B标准规定的5类UTP的最大距离100米之内，就满足了该项要求。表5-1列出了各种线缆类型及其特性。

在只有一个配线间的简单星型拓扑中，MDF包括一个或多个水平交叉连接（HCC，horizontal cross connect）的配线板，如图5-31所示。HCC配线板用来连接第1层的水平布线和第2层的LAN交换机端口。与其他端口不同，交换机的级联（uplink）端口不进行水平交叉连接，而是通过跳线（patch cable）连接到3层路由器的以太网端口。这样，末端主机便有一个完整的到路由器的物理连接。

表5-1 IEE802.3线缆类型及其特性

特性	10 BASE-T	10 BASE-FL	100 BASE-TX	100 BASE-FX
数据速率	10Mbit/s	10Mbit/s	100Mbit/s	100Mbit/s
信号传输方式	基带	基带	基带	基带
介质类型	5类UTP	光纤	5类UTP	多模光纤（2线）
介质长度	100m	2 000m	100m	2 000m

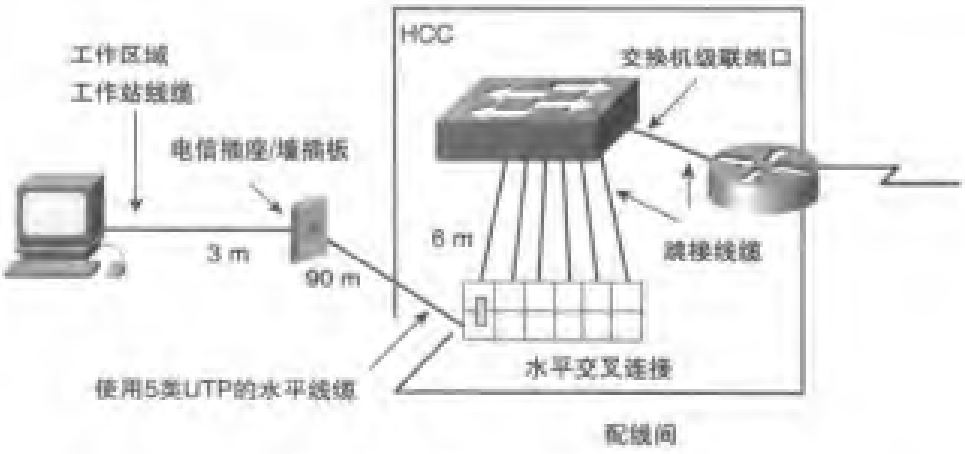


图5-31 在星型拓扑中的MDF

当更大型网络的主机之间的距离超过5类UTP标准规定的100m距离限制时，通常会有多个配线间。通过创建多个配线室，产生了多个服务区（catchment areas）。第二级配线室称为IDF。如图5-32所示。TIA/EIA 568-B标准规定IDF必须通过垂直布线（vertical cabling）跟MDF连接，也叫做骨干布线（backbone cabling）。

如图5-33所示，垂直交叉连接（VCC，vertical cross connect）用于各个IDF和中央的MDF的互连。因为垂直布线的长度通常会超过5类UTP规定的100m的距离限制，通常使用光纤布线，如图5-34所示。

快速以太网是一种带宽已经升级到100Mbit/s的以太网络。快速以太网采用标准的10BASE-T的面向广播的逻辑总线型拓扑，和针对MAC的CSMA/CD。快速以太网标准可分为几个不同类型：基于铜线的（100BASE-TX），基于光纤的（100BASE-FX），后者通常用于连接MDF和IDF，如图5-

33所示。使用10BASE-TX交换以太网到桌面，快速以太网作骨干对于多数的网络带宽需求而言已经足够了。比较新的网络使用基于光纤的吉比特以太网做垂直（骨干）线缆，和采用超5类线缆的快速以太网作为到桌面的水平连接。具体使用哪种需求取决于预算的限制。

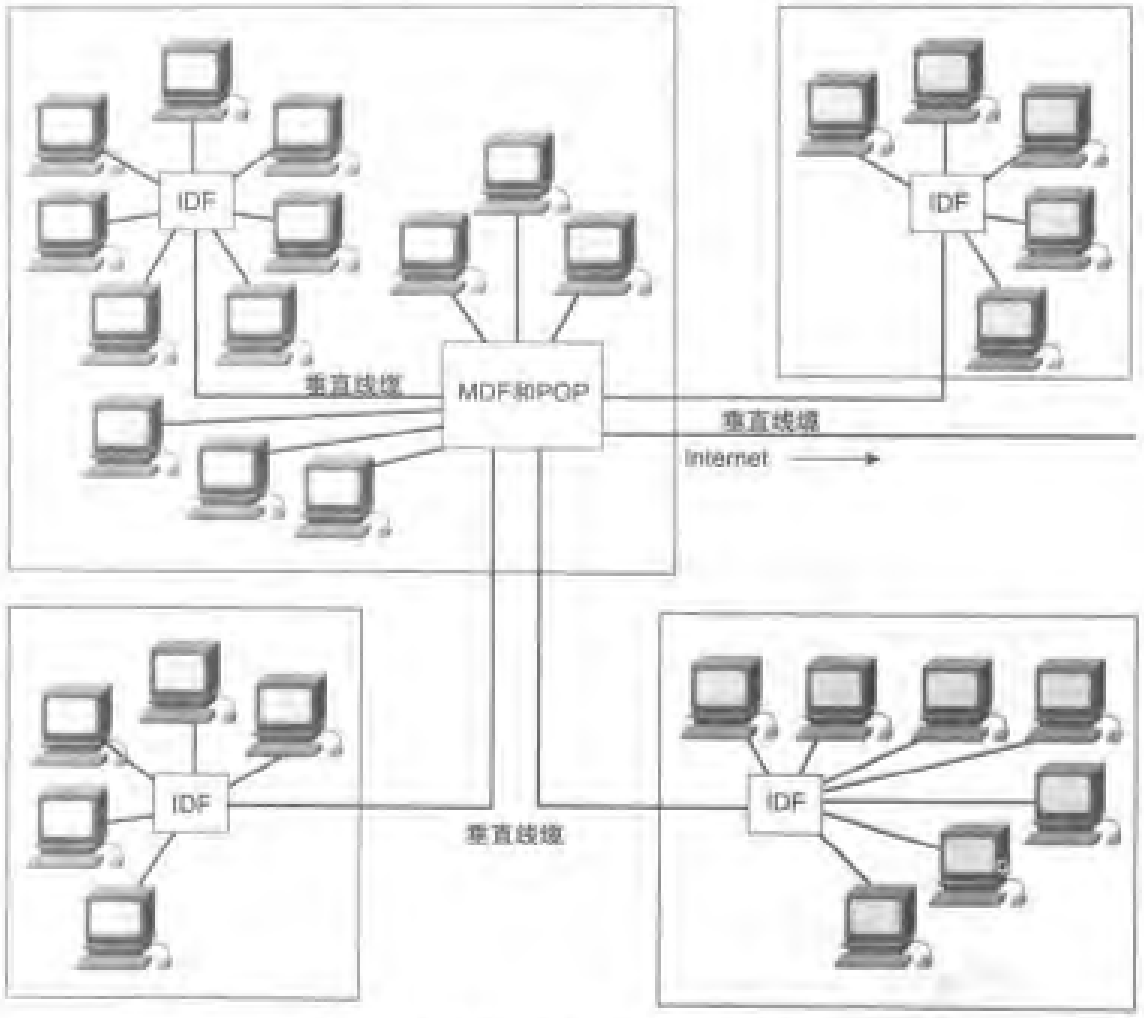


图5-32　扩展星型拓扑在多建筑物的校园内

如图5-36所示，逻辑图（logical diagram）是一种不包含实际布线安装调节的网络拓扑模型，这是局域网的基本路标。逻辑图的要素包括：

- MDF和IDF配线室的实际位置。
- 将IDF和MDF互连的线缆的种类和质量，以及有多少空余线缆可以用于增加配线室之间的带宽。例如：如果IDF1和MDF之间垂直布线的利用率为80%，则你可以用额外的两个线来使网络容量翻倍可以采用。
- 所有线缆段的详细文档记录。如图5-37所示，标识编号、该线缆段终位于HCC或VCC上的哪个端口。例如，假定203房间的网络不通。通过检查对照表（cut sheet），可以发现，203房间通过标记为203-1线缆与HCC1上端口13相连。这样，使用线缆测试仪可以判断问题是否出在第1层。如果是，可以使用另外2个可用连接中的一个重新取得连接，然后查找203-1的故障。

5.4.10　第2层设计

最常见的第2层设备（除了网卡，那时网络上的每台主机都必须配备的）是局域网交换机。第2层的设备决定冲突域和广播域的大小。本节集中介绍局域网第2层交换技术的实现。

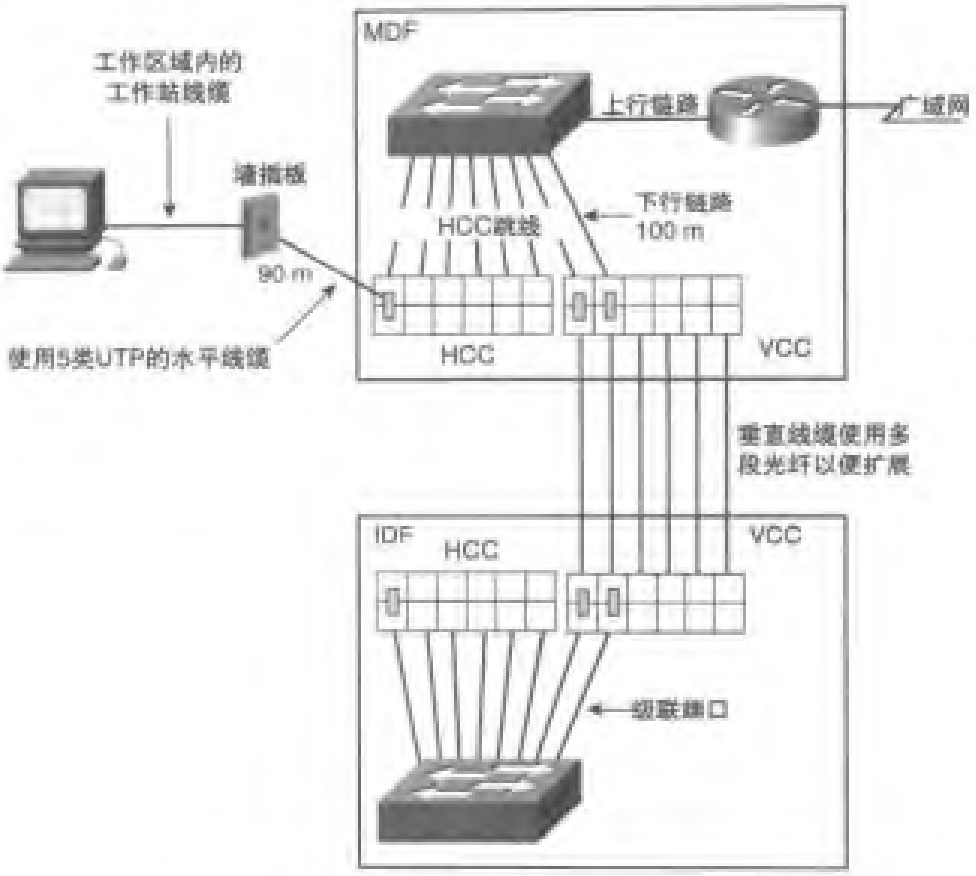


图5-33 扩展星型拓扑中的VCC

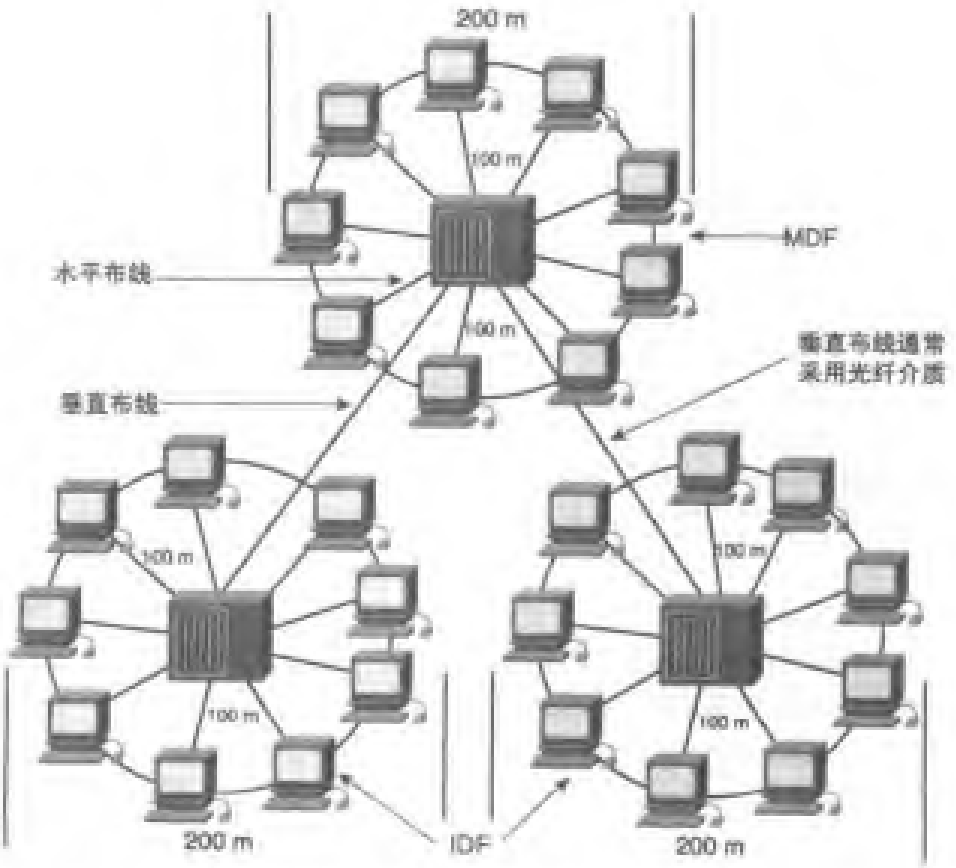


图5-34 扩展星型拓扑中的垂直布线

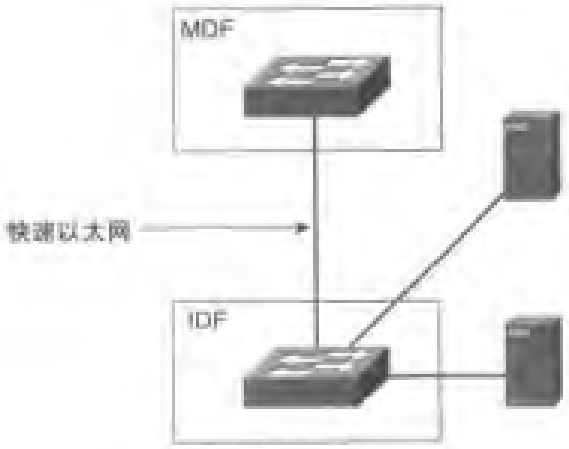


图5-35　MDF到IDF的垂直布线

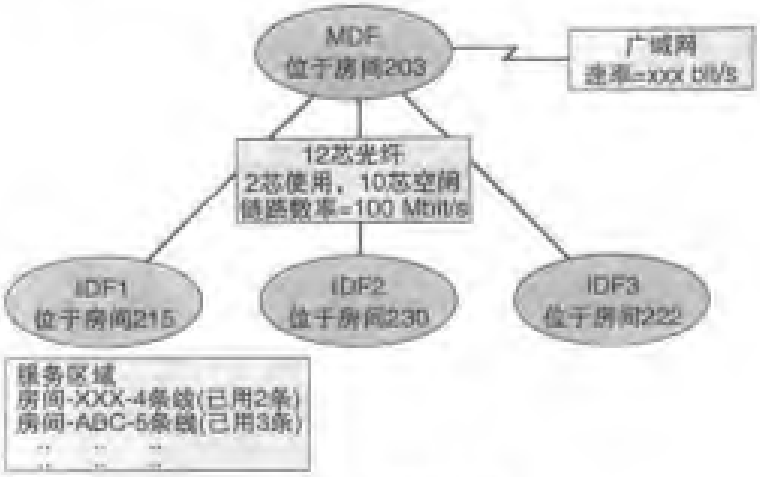


图5-36　逻辑网络图



连接	线缆标识	交叉连接单号/端口号	线缆类型	使用情况
IDF1到房间203	203-1	HCCI/Port 13	5类UTP	使用
IDF1到房间203	203-2	HCC1/Port 14	5类UTP	未使用
IDF1到房间203	203-3	HCC2/Port 3	5类UTP	未使用
IDF1到主配线间	IDF1-1	VCC1/Port 1	多模光纤	使用
IDF1到主配线间	IDF1-2	VCC1/Port 2	多模光纤	使用

图5-37　对照表

冲突和冲突域大小是对网络性能产生负面影响的两个因素。通过采用局域网交换技术，可以对网络进行微分段，从而消除冲突，减小冲突域的大小。如图5-38所示。局域网交换机的另一个重要特点是能够以端口为单位分配带宽，这样就能为垂直加线、级联线路和服务器分配更多的带宽。这种类型的交换通常称为非对称交换，它在不同带宽的端口之间提供交换连接。如在10Mbit/s和100Mbit/s端口之间，或者在100Mbit/s和1 000Mbit/s端口之间。

正如前面讲到的，微分段技术就是通过交换机增强工作组或者骨干的性能。通常，通过这种方式增强性能需要应用以太网交换技术。交换机可以跟集线器一起使用，为不同的用户和服务器提供适当的性能，如图5-39所示。随着每个端口的成本的降低，交换机的应用越来越广泛，特别是在设计新的局域网时。

如图5-40所示，通过在MDF中、IDF中以及MDF和IDF之间垂直布线中采用局域网交换技术，垂直布线可以传输MDF和IDF之间的所有数据通信；因此，垂直线缆的容量必须比IDF和工作站之间的线缆段的容量更大。水平线缆段通常使用5类或更好的UTP，并且线缆段长度不应超过100m，其上可支持10、100或1 000Mbit/s的链路。在普通的环境中，水平线缆段一般采用10Mbit/s的速率就足够了。虽然新型的局域网到桌面的速率一般都标配为10/100-Mbit/s。因为非对称局域网交换允许在一台交换机内部对10Mbit/s和100Mbit/s的端口、以及100Mbit/s和1 000Mbit/s的端口进行互连，所以下一个任务是决定MDF和每一个IDF所需要的10Mbit/s、100Mbit/s和1 000Mbit/s的端口的数量。可以通过查找用户每间房间内水平布线的数量、看服务区内布线总量、垂直布线数量的需求来决定各

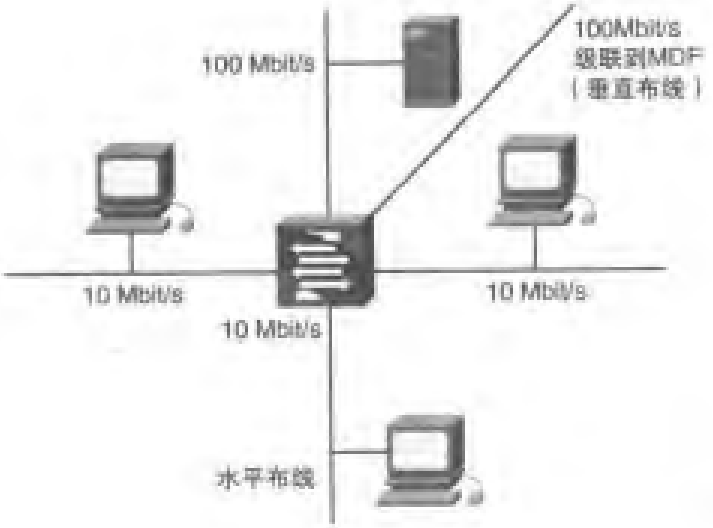


图5-38 非对称交换

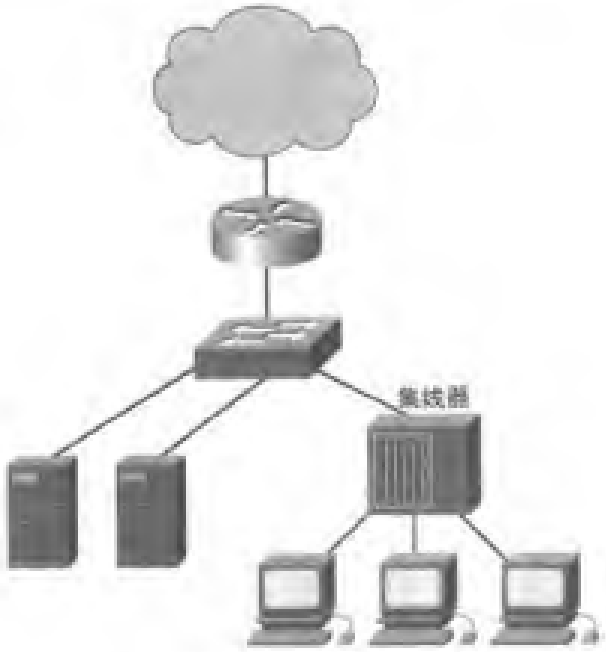


图5-39 减少网络拥塞

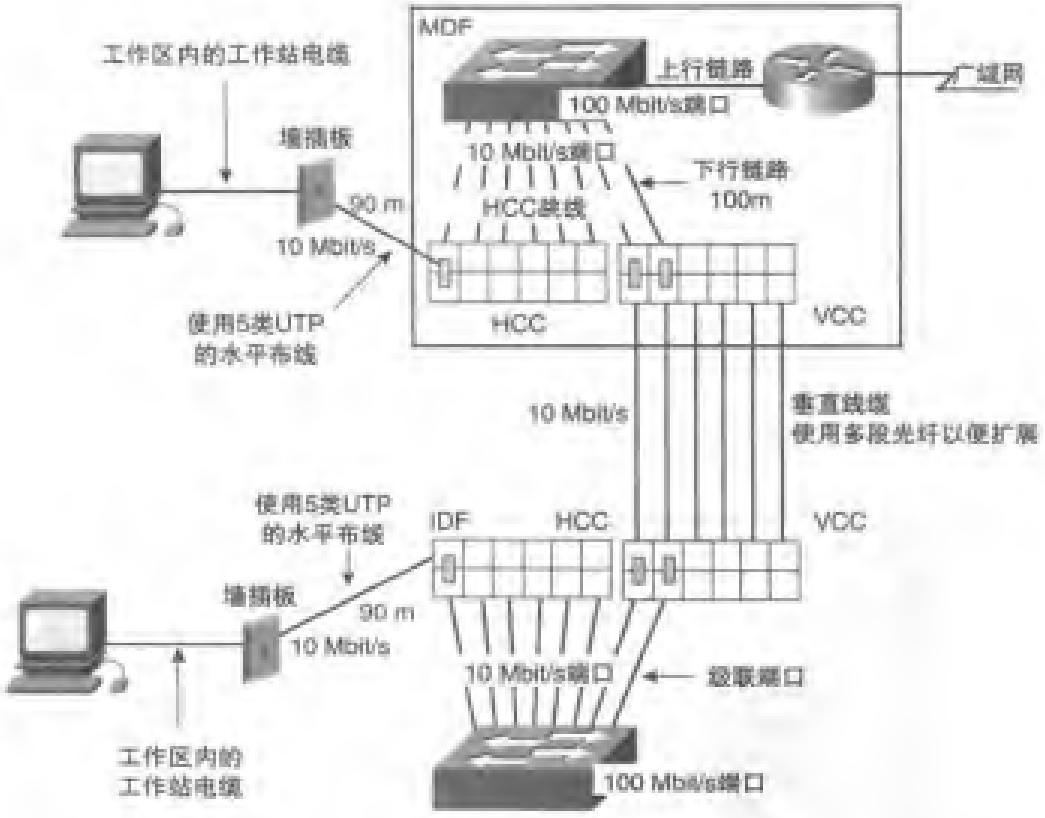


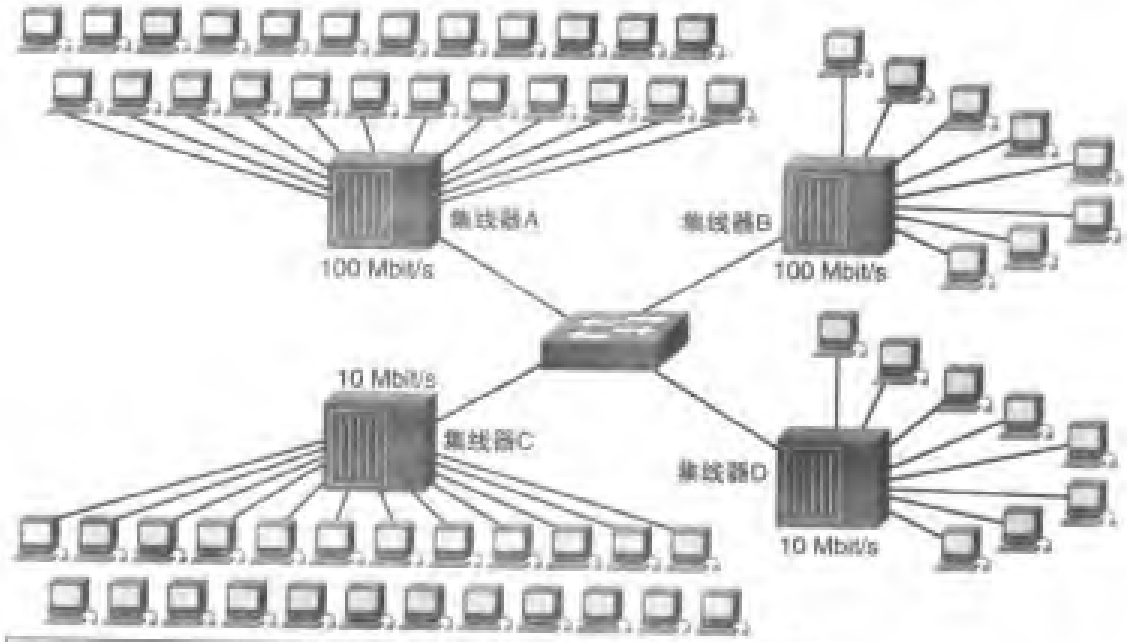
图5-40 第2层交换技术

类端口数量。例如，用户需求中说的每个房间需要配置4条水平线缆段。服务于这个服务区的IDF需要覆盖18个房间，那么，4线×18个房间=72个交换机端口。

要决定冲突域的大小，就必须决定在一台交换机上，有多少台物理主机与单个端口相连。这也影响每台主机的可用网络带宽。在理想状态下，局域网交换机的一个端口只与一台主机相连。这样冲突域的大小为2（源主机和目的主机）。正因为有这些小的冲突域，任意两台主机之间相互通信时，

一般不会有冲突产生。另一个使用局域网交换技术的方式就是在交换机端口上连接共享式LAN集成器，将多台主机连接到一个交换机端口，如图5-41所示。

如图5-42所示，所有与共享式LAN集线器相连的主机共享同一个冲突域和广播域。图5-43提供了一个演示，解释了在一个共享以太网环境中，单个用户带宽计算方法。在新型的局域网设计中，不会推荐将24个用户连接到集线器，然后再将集线器连接到交换机的一个端口上。



Hub A: 冲突域=24主机
带宽平均值=100 Mbit/s24主机=4.16 Mbit/s每台主机
Hub B: 冲突域=8主机
带宽平均值=100 Mbit/s8主机=12.5 Mbit/s每台主机
Hub C: 冲突域=24主机
带宽平均值=10 Mbit/s24主机=4167 Mbit/s每台主机
Hub D: 冲突域=8主机
带宽平均值=10 Mbit/s8主机=1.25 Mbit/s每台主机

图5-41　使用集线器时冲突域的大小

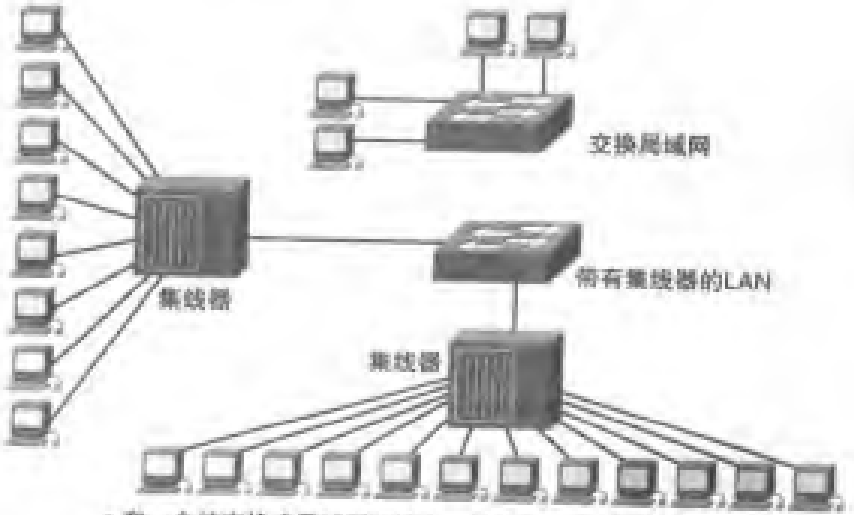


图5-42　2层交换机的冲突域

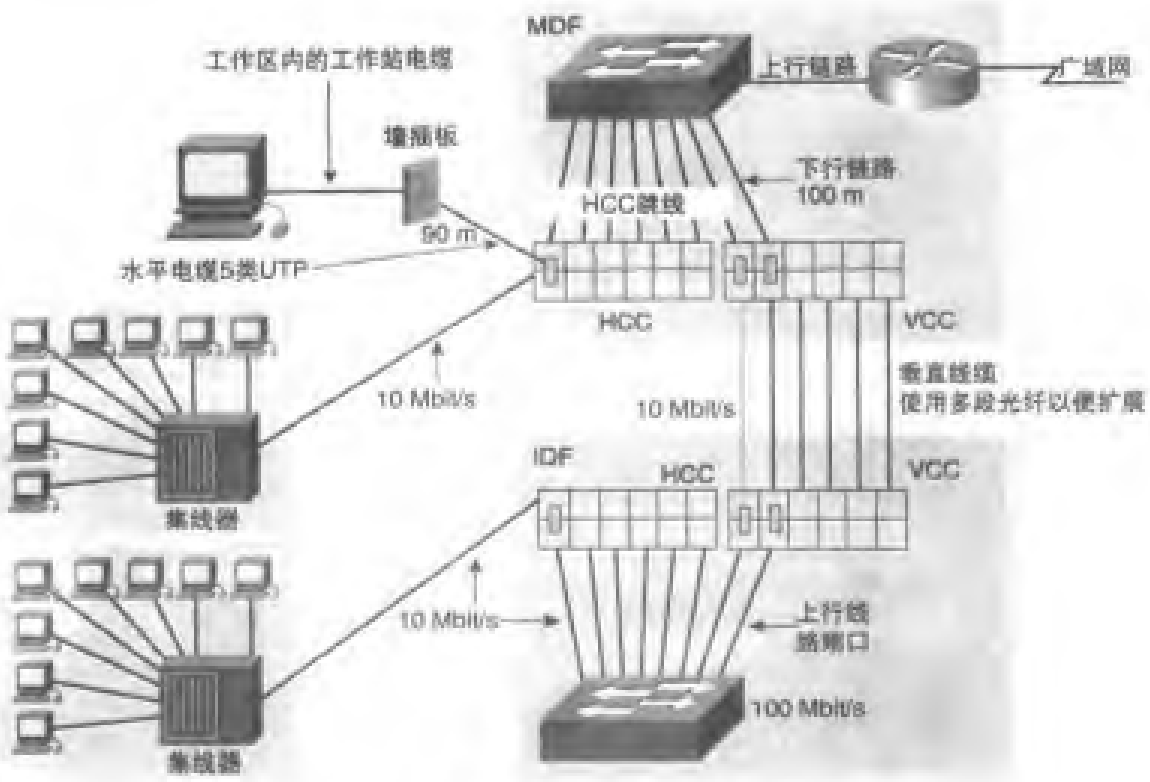


图5-43 带有集线器的第2层交换

注意有些老型号的交换机，比如Catalyst 1700，并不真正支持共享共一个冲突域和带宽，因为它们不维护多个MAC地址到一个端口的映射。在这种情况下，便存在很多广播和ARP请求。

共享介质的集线器通常用于在局域网交换环境中的水平电缆段创建多个连接点，如图5-43所示。这是一个可接受的方案，但是必须使冲突域尽可能小，并且要能按照网络设计的需求阶段整理出的规范保证主机需要的带宽。

随着网络的增长，带宽的需求也在增加。在MDF和IDF之间的垂直布线中，闲置光纤可以从VCC连接到交换机的100 Mbit/s端口上，如图5-44所示。通过启用另外一条链路，网络中的垂直布线的容量翻了一倍。

在水平布线中，通过将HCC重新插线到交换机的100 Mbit/s端口，并且把10 Mbit/s的集线器变成100 Mbit/s的集线器，网络带宽可以提高10倍。当选择第2层以太网（LAN）交换机的大小时，为了实现向更高带宽的迁移，需要保证有足够的100 Mbit/s的端口。而且要在每一条正在使用的电缆连接导线上标注运行速度。

5.4.11 第3层设计

如图5-45所示，第3层（网络层）设备，如路由器，可以建立独立的局域网（LAN）网段，网段之间基于第3层的寻址（如IP寻址）来实现通信。第3层设备的使用，如路由器，能将局域网分段为独立的物理和逻辑网络。路由器也可以实现到广域网（WAN）的连接，如连接Internet。

第3层路由选择基于第3层寻址（如IP网络和子网）决定独立物理网段间的通信流。路由器是网络拓扑中最强大的设备之一。

正如前面学习到的，路由器根据目的地址转发数据分组。路由器不转发基于LAN的广播，比如ARP请求。因而，路由器接口可以看作是一个广播域的起点和终点，广播不能到达其他LAN网段。

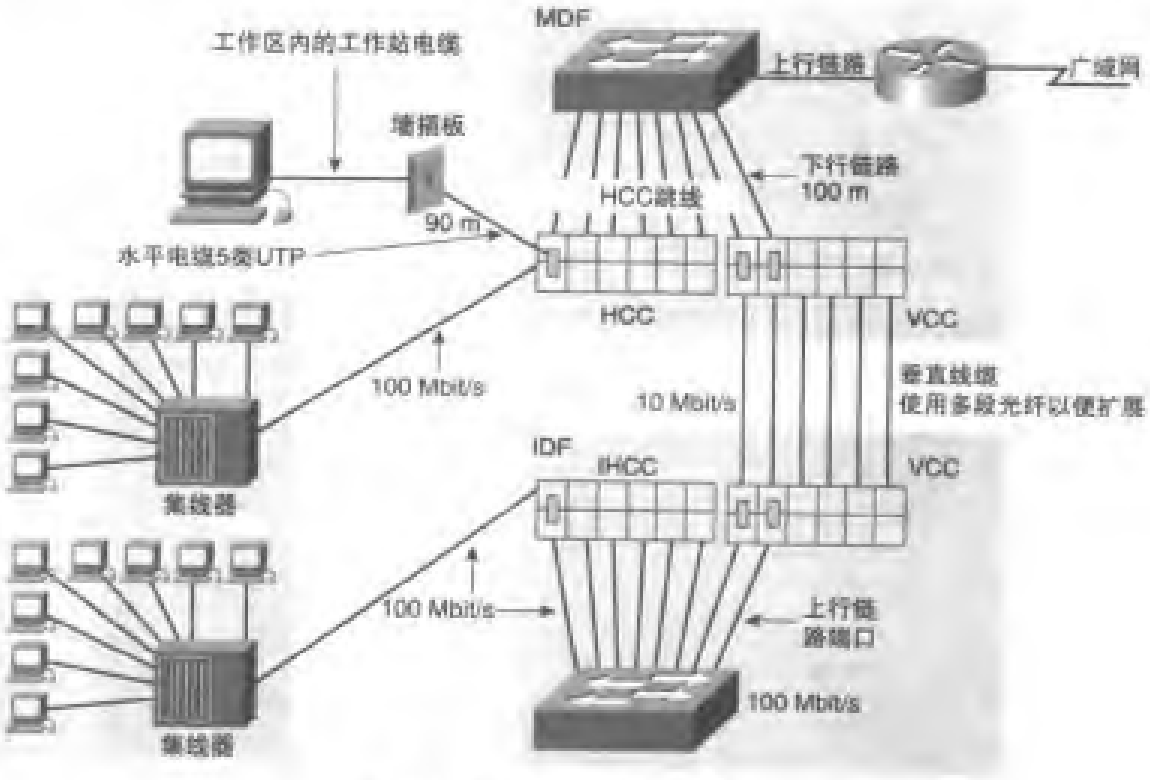


图5-44　第2层：向更高带宽迁移

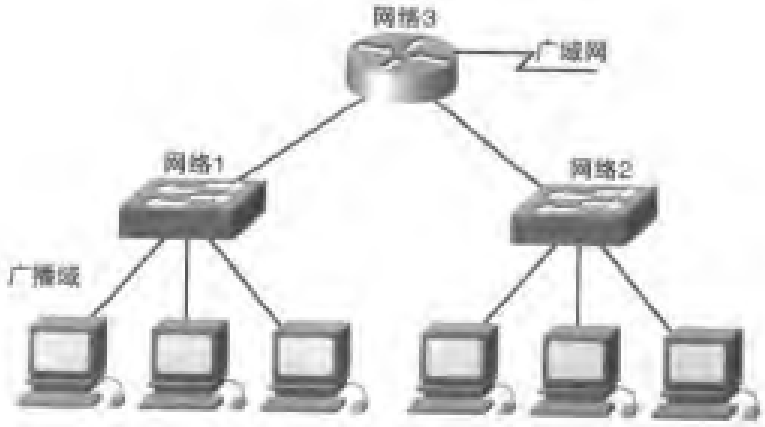


图5-45　第3层路由的实现方式

网络中的一个重要问题是广播（比如ARP请求）的总数。通过使用VLAN技术，可以将广播通信限制在一个VLAN中，从而建立更小的广播域，如图5-46所示。也可以根据分工建立VLAN组，利用VLAN来提高安全性，如图5-47所示。

如图5-46所示，物理端口关联用于实现VLAN分配。端口P0、P1和P4被分配到VLAN1中。VLAN2包含端口P2、P3和P5。VLAN1和VLAN2只有通过路由器才能够通信。这限制了广播域的大小，由路由器来决定VLAN1是否能够和VLAN2会话。这就意味着可以根据VLAN分配机制建立一个安全方案。

由于路由器可以作为广播的防火墙，所以它能提供扩展性。另外，因为第3层地址通常是有结构的，通过划分网络和子网，路由器能够提供更高的扩展性，所以要在第3层地址中增加结构信息，如图5-48所示。网络中实现更强的结构和更高扩展性的方法如图5-49所示。

网络被划分成子网后，最后一步是规划并记录网络中使用的IP寻址方案。路由选择技术会过滤

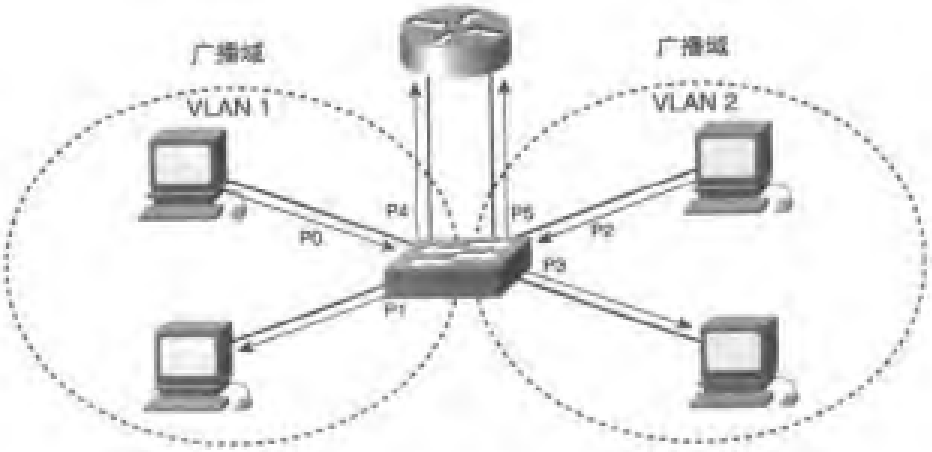


图5-46 VLAN通信

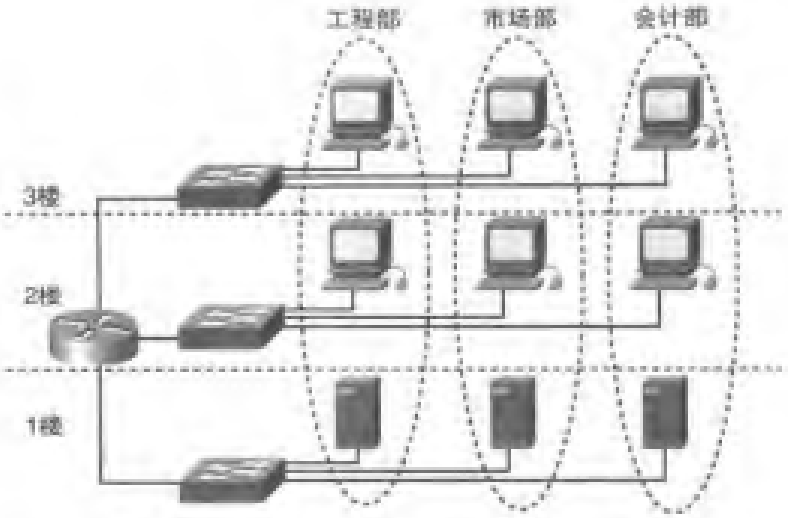


图5-47 VLAN实现

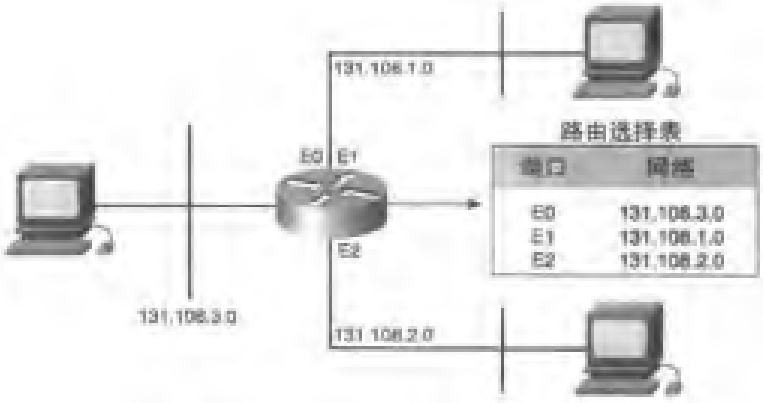


图5-48 路由器建立逻辑结构

数据链路层的广播和组播。通过给路由器端口增添子网或者是网络地址，可以按照需要分割互连网络。网络寻址和路由选择提供了内置的扩展性。在决定使用路由器还是交换机的时候，记住这样一个问题，“试图解决的是什么问题？”。如果问题是协议相关的而不是面向竞争的，路由器是合适的。路由器可以解决超量广播的问题、协议不能很好扩展的问题、安全问题以及网络层的寻址问题。然

逻辑地址	物理网络设备
x.x.x.1-x.x.x.10	路由器、局域网和广域网端口
x.x.x.11-x.x.x.20	局域网交换机
x.x.x.21-x.x.x.30	企业服务器
x.x.x.31-x.x.x.80	工作组服务器
x.x.x.81-x.x.x.254	主机

图5-49　逻辑寻址映射到物理网络

而路由器要比交换机更贵，配置也更难些。

路由器通过地址的结构化来建立IP子网，如图5-50所示。使用网桥和交换机时，对所有未知的地址都必须泛洪到端口上。使用路由器，则使用网络层寻址协议的主机可以解决寻找其他主机的问题而不需泛洪。如果目的地址是本地的，发送方主机将分组封装到数据链路帧头里，发送一个直接指向目的站点的单播帧。路由器不需要看这个帧，当然也就不用泛洪这个帧。发送方主机也许得使用ARP。这会引起一个广播，但这只是一个本地广播，不会被路由器转发。如果目的地址不是本地的，发送站点把分组传输给路由器（也就是它的缺省网关）。路由器根据自身的路由选择表，将帧发送到目的站点或者是下一跳。考虑到路由选择所提供的功能，很显然大型的、可扩展的局域网需要包含一些路由器。

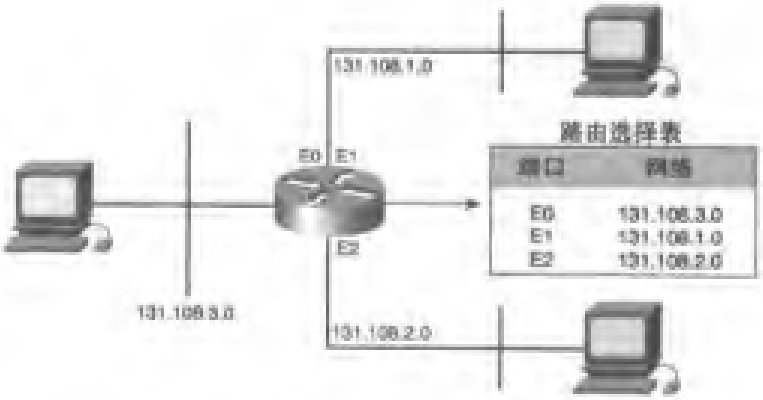


图5-50　使用路由器实施逻辑结构

图5-51显示包含多个物理网络的实施实例。从网络1发往网络2的所有数据通信必须经过路由器。网络1和网络2是两个分离的广播域。这两个网络有各自的第3层IP网络寻址/子网寻址方案。在一个第1层结构化布线方案中，通过跳线（patch cable）将水平线缆和垂直线缆跳接到适当的第2层交换机端口上，可以很容易地建立多个物理网络。这种实现方式具有很强的安全性。此外，路由器是局域网中通信的集中点。

在为客户规划完IP寻址方案之后，应该按照各个地点和该地点中的网络形成文档。如图5-52所示，为网络中重要主机的寻址设定标准惯例。要在整个网络中要保持该寻址方案的一致性。通过建立寻址图（addressing maps），可以得到一个网络的快照，如图5-53所示。建立网络的物理图（physical maps）有助于发现并解决网络的问题，如图5-54所示。

5.4.12　基本的第2层桥接和交换

本节将介绍交换机和网桥的主要功能，这些设备在OSI模型中被归类为第2层设备。另外还将讨

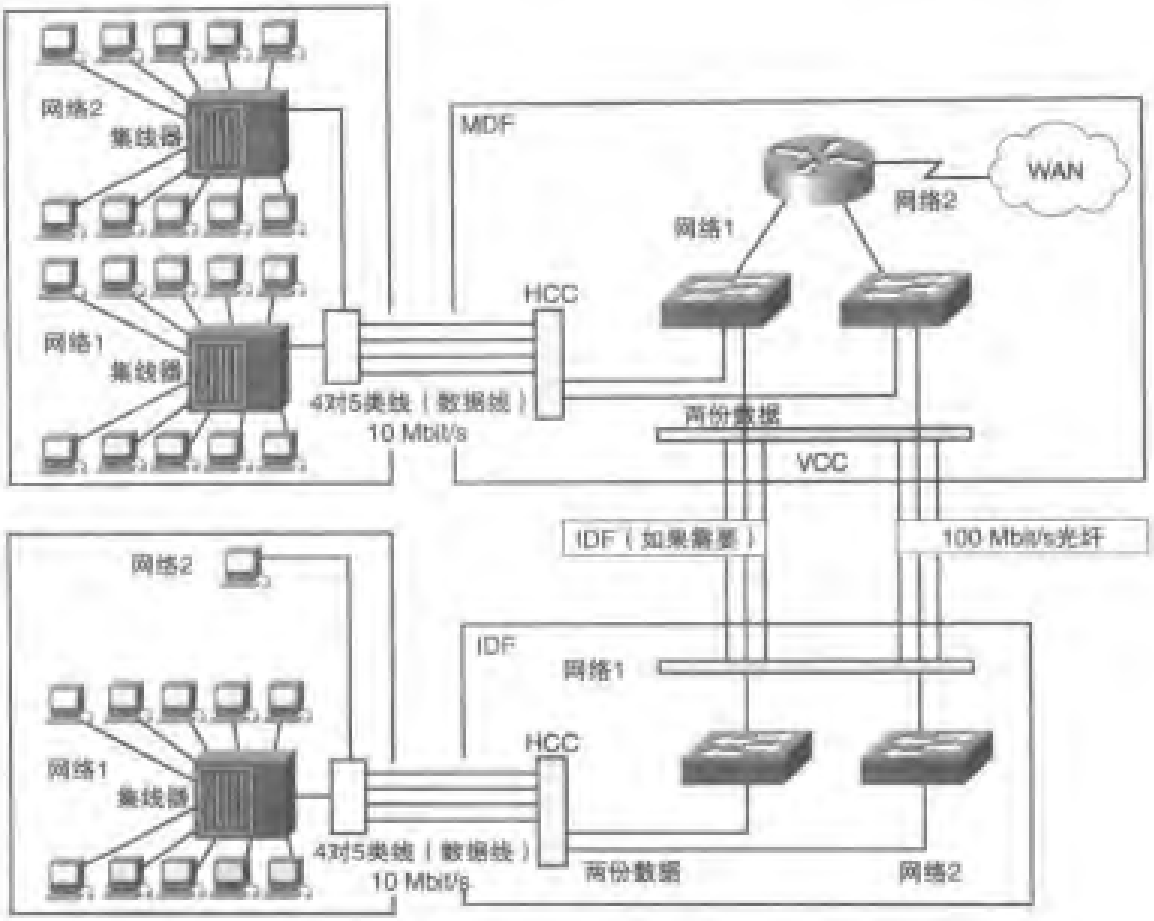


图5-51 第3层分段

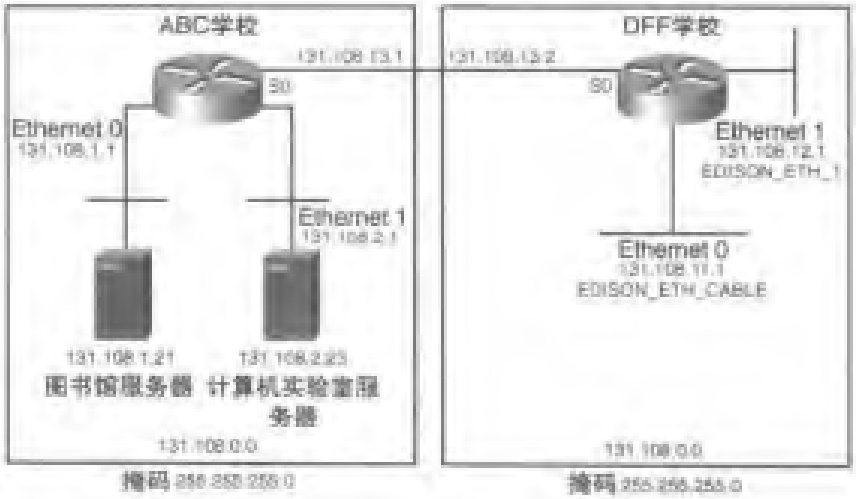


图5-52 寻址图

论交换机发送帧和过滤帧的方式。通过接触交换机和网桥，能帮助用户理解这些设备是如何学习地址的。因为不是每个局域网都必须分段，所以你需要理解局域网分段和冲突域划分的原则。分段技术可以保证网络的性能不会随着局域网规模的增长而降低。

随着网络规模和用户数目的增长，以及用户需要更多的带宽来运行其应用，网络拥塞使网络速度降低到让用户不再信任的程度。当应用程序不能快速运行时，用户对此怨声载道而变得失去耐性。解决网络拥塞最有效的方法之一是把网络分解成更小的网段。可以使用网桥或交换机在合适的物理



图5-53　逻辑网络图

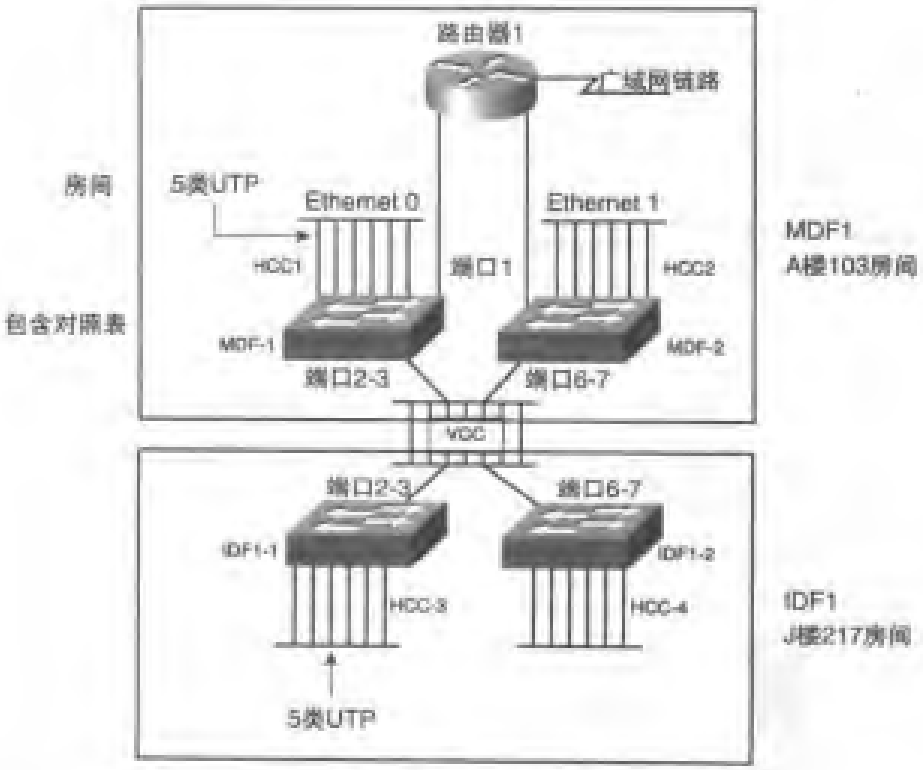


图5-54　物理网络图

位置上进行分段，例如，限制网络网段中的设备数量。

交换机能对连接进行集中，以使数据传输更加有效。帧从输入端口（接口）交换到输出端口。每一个端口给主机提供了全部的连接带宽。

在典型的以太网集线器中，所有的端口连接到一个公共的背板或集线器内的物理连接上，连接到集线器上的所有设备共享网络带宽。如果两个站点之间建立的会话占用了大量带宽，集线器上所有其他设备的网络性能便会下降。

为了减少网络性能的下降，交换机把每一个接口当作一个单独的网段。当不同接口上的站点需要通信时，交换机接近线速地将帧从一个接口转发到另一个接口，以保证每一个会话能使用全部的带宽。

为了在接口之间有效地交换帧，交换机维护一个地址表。当帧进入交换机时，交换机把发送站

（源）的MAC地址与接收该帧的端口关联起来。

以太网交换机的主要功能如下：

- 隔离各网段内的通信。
- 通过建立更小的冲突域为每个用户提供更多的带宽。

第一个功能是隔离网段间的通信，网段是指通过使用类似以太网交换机这样的设备将网络划分成的更小单元。每个网段都使用CSMA/CD访问方法来实现网段内多个用户之间的通信流。这种分段使得不同网段上的多个用户能同时发送信息，而不会降低网络速度。

以太网交换机基于2层MAC地址将数据报文定向到适当的一个或多个端口，以实现对通信的过滤。通过建立更小的冲突域，以太网交换机的第二个功能可以保证每个用户拥有更多的带宽。

快速以太网支持对局域网进行分段（划分为更小的冲突域），为每个网段提供速度最高可达100 Mbit/s的专用网络链路（就像高速路车）。高使用率的服务器可以拥有自己的100 Mbit/s甚至是1,000 Mbit/s的链路。现今网络最平常的情况是：快速以太网或吉比特以太网交换机充当着以太网的“骨干”，10 Mbit/s或100 Mbit/s的以太网交换机在工作组内提供到桌面的连接。随着对桌面多媒体或视频会议等新兴应用的需求逐渐普遍，某些独立台式计算机也拥有自己专用的100 Mbit/s的网络链路。今天的网络是全交换的，使用100 Mbit/s或1,000 Mbit/s作为骨干，10/100 Mbit/s连接到桌面。

5.4.13 交换机和网桥如何过滤帧

网桥有能力根据第2层的数据字段过滤帧。例如，网桥可以被编程为拒绝（不转发）从一个特定网络数据源发送的所有帧。因为数据链路层的信息一般会包括关于上层协议的参考信息，网桥通常可以根据这个参数进行过滤。此外，过滤器也可以帮助处理那些不必要的广播和组播分组。桥接功能一般会内置在路由器中，而不会由一台独立的设备提供。

当网桥建立了本地地址表后，网桥就可以开始工作了。当网桥接收到一个帧，它会检查源地址。如果源地址是本地的，网桥会忽略这个帧。如果这个帧属于另外一个局域网，网桥会复制这个帧到相应的局域网上。忽略帧称为过滤（filtering），复制帧称为转发（forwarding）。

5.4.14 过滤类型

基本的过滤能完成下述功能：

- 将本地帧保留在本地。
- 非本地帧发送到其他网段。

基于特定的源地址或目的地址的过滤包括：

- 阻止一个站向它所在局域网以外的网段发送帧。
- 阻止所有“外部”的帧流向指定的站，从而限制其他站与该站的通信。

两种过滤都对互连网络上的通信进行了某种控制，并且能提供更高的安全性。

大部分的以太网桥都可以过滤广播和组播帧。有些时候，一台设备发生故障，有可能会不停的发送广播帧，会导致大量的帧在网络上持续的被复制。***广播风暴***（broadcast storm），就像它的名字一样，可以导致网络性能下降为0。如果网桥可以过滤广播帧，广播风暴发生的机率就小了。

现在，网桥也可以基于网络层协议进行帧过滤。这一功能模糊了网桥与路由器之间的区别。路由器工作在网络层，通过路由选择协议转发网络通信。实现了高级过滤技术的网桥通常被称为桥式路由器（brouter）。它通过检查网络层信息进行过滤，但是它不使用路由选择协议。桥接功能一般会内置在路由器中，而不会由一台独立的设备提供。

5.5　总结

在本章中，你学习了以下内容：

• 更高性能计算机/工作站和网络密集型应用产生了对带宽的更高要求，这样的要求大大超过了共享以太网/802.3局域网的10 Mbit/s。

• 随着越来越多的用户开始利用网络共享大文件、访问文件服务器、连接Internet，产生了网络络拥塞后退。

• 在分段的以太网LAN上，跨越不同网段的数据通过网桥、交换机或路由器进行交换传递。交换机将局域网划分为很多的微分段，把一个大的冲突域划分为很多无冲突的域。

• 使用交换式以太网拓扑的局域网会产生看起来好像只有两个节点（发送节点和接收节点）的网络。

• 和网桥一样，交换机通过读取分组2层目的MAC地址实现高速传输。

• 通过建立独享的网段（点到点的连接），并将这些独享网段通过交换机连接成为一个虚拟网络，以太网交换技术提高了网络的可用带宽。

• 对称交换是指所有端口都具有相同的带宽。

• 虚拟局域网是指不局限在一个物理交换网段的网络设备或用户的分组。

• 生成树协议的主要功能是在允许复制交换/桥接路径的同时，避免因为在网络中产生环路而引起延迟效应。

• 确保快速而稳定的最关键因素之一是网络设计。如果网络设计不当，一些没有预见到的问题可能会出现，甚至危及到网络的发展。

• 局域网的设计目标包括功能性、扩展性、适应性和可管理性。

设计过程应该包括：

• 收集用户的需求和期望。

• 在分析服务器位置和未来发展的基础上，确定当前和未来的数据通信模式。

• 确定所有第1层、第2层和第3层网络设备，并确定所使用的局域网和广域网技术。

• 编写物理和逻辑网络实施文档。

作为本章内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

5.6 关键术语

网桥（*bridge*） 连接两个网段并在两个网段之间转发具有相同通信协议分组的网络设备。网桥工作在OSI参考模型的数据链路层（第2层）。一般来说，网桥基于帧的MAC地址过滤、转发或者泛洪该帧。

桥接（*bridging*） 用网桥连接两个或多个局域网段的技术。

广播（*broadcast*） 将一个数据分组发送到网络中所有的节点。广播通过广播地址进行识别。参见广播地址、广播域和广播风暴。

广播地址（*broadcast address*） 一个特殊的用于向所有节点发送数据的保留地址。一般来说，广播地址是一个全1的MAC目的地址。参见“广播”。

广播域（*broadcast domain*） 能够收到某台设备发送广播帧的所有设备集合。路由器一般用于限定广播域，因为路由器不转发广播帧。参见“广播”。

广播风暴（*broadcast storm*） 很多的广播在网络上所有网段同时传播，这是一种不希望发生的网络事件。广播风暴占用了大部分的网络带宽，导致网络超时的发生。

总线拓扑（*bus topology*） 一种线型局域网结构，数据通过传输介质传播到网络的所有角落，网络上所有站点都会接收到这一数据。对比“星型拓扑”。

冲突（*collision*） 在以太网中，两个节点同时发送数据所产生的结果。不同节点发出的帧在物理介质中相遇时发生冲突并损坏。

冲突域（*Collision domain*） 在以太网中，数据帧冲突能够传播到的网络区域。中继器和集线器传播冲突；局域网交换机、网桥和路由器不传播冲突。也可称为带宽域。

拥塞（*Congestion*） 通信量超过了网络容量。

带冲突检测的载波侦听多路访问（CSMA/CD）（*Carrier sense multiple access collision detect*） 一种介质访问机制。准备发送数据的设备在发送之前首先检查传输通道上是否有载波。如果在一个特定的时间内没有监测到载波，网络设备可以开始发送。如果两个设备同时开始发送，会发生冲突，两台发送数据的设备都会监测到冲突的发生。冲突导致在随机时间之后的重新发送。以太网和IEEE 802.3都采用CSMA/CD访问控制方式。

对照表（*Cut sheet*） 一种用于标识线缆段走向和房间数量的粗略图表。

贯穿式（*cut-through*） 一种分组交换的技术。当数据流入交换机的时候，数据帧在还未从输入端口接收完毕时，起始部分可能已经开始从输出端口转发出去。使用贯通式技术的网络设备在监测到目的地址，并确定输出端口后立刻开始转发数据帧。又称为飞速分组交换（on-the-fly packet switching）。

企业级服务器（*enterprise server*） 为网络上所有用户提供服务（例如电子邮件服务或者域名服务）的服务器。

以太网（*Ethernet*） 一种基带局域网标准，该标准由施乐公司发明，施乐公司、英特尔公司和DEC公司共同发展完善。以太网络使用CSMA/CD机制，可以在多种线缆上实现10 Mbit/s传输。以太网标准与IEEE 802.3系列标准类似。

快速以太网（*Fast Ethernet*） 100Mbit/s的以太网标准。快速以太网提供了10倍于10BASE-T以太网标准的传输速度，同时保持了相同的帧格式、MAC控制机制和最大传输单元（MTU）。这些一致性保证了在快速以太网的网络环境中可以使用现有的10BASE-T网络应用和网络管理工具。快速以太网是基于

IEEE 802.3标准的扩展。参见“以太网”。

快速转发技术（*fast-forwood switching*）　在收到目的地址之后立刻转发分组，这一交换方式的延迟最低。

吉比特以太网（*Gigabit Ethernet*）　1,000Mbit/s的以太网标准。吉比特以太网提供了10倍于快速以太网标准的传输速度。

IEEE 802.3　IEEE发布的局域网协议，规定了关于物理层和数据链路层MAC子层的一种实现方式。IEEE 802.3采用CSMA/CD机制，在各种物理介质上实现不同的访问速度。IEEE 802.3标准的一个扩展规定了快速以太网的具体实现。最初IEEE 802.3标准的物理层实现包括：10BASE-2、10BASE-5、10BASE-F、10BASE-T和10BROAD-36。快速以太网的物理层实现包括：100BASE-TX 和100BASE-FX。吉比特以太网的物理层实现包括：1000BASE-T、1000BASE-LX和1000BASE-SX。

电气与电子工程师协会（*Institute of Electrical and Electronics Engineers, IEEE*）　一个专业组织，制定和开发通信和网络的相关标准。IEEE局域网标准就是当前网络的主要标准。

局域网（*Local-area network, LAN*）　一种相对较小的地理范围内（最多几公里）的高速、低错误率数据网络。局域网用于连接在一个建筑物或者在一个特定的地理范围内的计算机、外设、终端和其他设备。局域网标准规定了OSI模型中物理层和数据链路层的布线和信号传输的实现。以太网、FDDI和令牌环网是广泛使用的局域网技术。

局域网交换机（*LAN Switch*）　在数据链路层网段之间转发分组的高速交换机。大多数的局域网交换机基于MAC地址转发帧。通常根据局域网交换转发方式的对其进行分类：贯穿式交换和存储转发式交换。Cisco Catalyst 5000就是局域网交换机。

延迟（*Latency*）　网络设备从请求发送到允许发送之间的所耽搁的时间。

MAC（介质访问控制）地址（*MAC address*）　标准化的数据链路层地址。连接到局域网中的任何设备或端口都需要这个地址。网络中的设备通过该地址确定端口的位置、建立并更新路由选择表及相应的数据结构。MAC地址是一个6字节长的地址，由IEEE来控制。也称为硬件地址、MAC层地址或者物理地址。

微分段（*microsegmentation*）　将网络划分成为很小的网段，通常是为了增加网络设备的带宽总和。

网络层（*network layer*）　OSI参考模型的第3层。这一层提供两个端系统之间的连接和路径选择。路由选择发生在网络层。和SNA模型的路径控制层的功能类似。

中继器（*repeater*）　在两个网段之间重新生成并传播电信号的网络设备。

路由器（*router*）　网络层的设备，利用一种或多种度量值来确定通信转发的最佳路径。路由器根据网络层的信息转发分组。有时候，也可以称为网关（尽管网关这个定义已经过时了）。

路由选择表（*routing table*）　存储在路由器或其他连网设备中的一张表，用于跟踪记录特定目的网络的路径。在某些情况下，这些路径有相关的度量值。

生成树协议（*Spanning Tree Protocol*）　一种利用生成树算法的桥接协议，通过建立一个生成树，使得网桥可以绕开网络中的环路，动态地工作。网桥之间通过交换网桥协议数据单元（BPDU）消息来检测环路；通过关闭选定的网桥接口消除环路。生成树协议主要基于IEEE 802.1生成树协议标准和早期的DEC生成树协议标准。IEEE标准支持网桥域，允许网桥在一个扩展的局域网中建立一个无环路的拓扑结构。一般采用IEEE标准做为首选协议，而不选用DEC标准。

星型拓扑（*Star topolagy*） 一种局域网的拓扑结构，所有端节点都通过点到点的方式连接到一个中央节点。环形拓扑的组织采用单向闭合的星型实现，而不用点到点的连接。对比“总线拓扑”。

存储转发（*Store-and forward*） 一种分组交换的技术，数据帧在被转发到相应端口之前要经过完整的处理，这些处理包括计算CRC校验和检查目的地址。在获得可用于转发数据帧的网络资源（如一条未使用的链路）之前，数据帧必须临时存放在网络设备中。

交换机（*Switch*） 基于帧的目的地址过滤、转发或者泛洪的网络设备。交换机工作在OSI参考模型的数据链路层。

交换（*Switching*） 从网络设备的一个接口获取数据帧并从另外一个接口发送出去的过程。

5.7 复习题

1. 以太网的介质采用哪种广播技术在网络节点中传输和接收数据？
   A. 分组
   B. 数据帧
   C. 数据段
   D. 每次一个字节
2. 微分段技术的特点包括？
   A. 发送者和接收者之间的虚路径
   B. 在交换机内有多个传输路径
   C. 网段上的所有通信都是立即可以看见的
   D. A和B
3. 局域网交换机可以被看作下列的哪一项？
   A. 工作在第1层的多端口中继器
   B. 工作在第2层的多端口集线器
   C. 工作在第3层的多端口路由器
   D. 工作在第2层的多端口网桥
4. 非对称式交换最适于以下哪种环境？
   A. 客户/服务器方式的网络通信，“快速的”交换机端口用于连接服务器
   B. 均匀分布的网络通信
   C. 缺少内存缓冲的交换机
   D. A和B
5. 描述全双工和半双工的以太网工作方式。
6. 描述生成树协议的主要功能。
7. 在网络中哪种网段是通过交换机划分的？
   A. 网络
   B. 园区网
   C. 冲突域
   D. 广域网
8. 在全双工的以太网交换机中，哪个是正确的？
   A. 冲突被实质上消除了
   B. 使用了节点间的两个线对和一个交换连接
   C. 节点之间的连接被认为是点到点的
   D. 以上所有的
9. 拥塞会导致下面哪种效果？
   A. 低可靠性和低流量
   B. 高冲突率
   C. 网络不可预知性和高错误率
   D. 降低响应时间，更长时间的文件传输和网络延迟
   E. 以上所有的
10. 主机A要发送数据给主机B。通信过程是这样的，主机A停止发送分组之后，主机B开始发送数据；类似的，主机B停止发送分组之后，主机A开始发送数据。这样的传输类型应该定义为哪种方式？
    A. 全双工

B. 半双工
C. 单工
D. 以上都不是

11. 下面哪种关于数据帧在局域网中转发的描述是错误的?
A. 存储转发式交换是数据帧在转发到相应的端口之前要做完整的处理
B. 存储转发式交换比贯穿式交换慢
C. 贯穿式交换也可以称为快速分组交换
D. 如果网络连接速度慢，贯穿式交换需要缓冲技术

12. 下面哪个关于局域网交换机的描述是正确的?
A. 它修复了网络中段为微分段的碎片
B. 它是一台高速的多端口的网桥
C. 因为低带宽导致了更高的延迟
D. 它需要在连接的机器上添加一块新的网络接口卡

13. 一台16端口的交换机可以产生多少个冲突域?
A. 1
B. 2
C. 14
D. 16

14. 通过局域网交换技术建立虚电路，可以导致?
A. 增加冲突
B. 减少可用带宽
C. 增加广播
D. 增加可用带宽

15. 交换机如何学习连接到其端口的网络设备的地址?
A. 交换机从路由器上得到相应的表
B. 交换机检查从端口流入的分组的源地址
C. 交换机之间交换地址表
D. 交换机不能建立地址表

16. 对称式交换的目的是什么?
A. 为每个端口提供相同带宽的交换式连接
B. 保证网络表是对称的
C. 为每个端口提供不同带宽的交换式连接
D. 交换机只能提供非对称式交换

17. 哪种网络设备可以用于对局域网进行逻辑分段?
A. 路由器
B. 网桥
C. 交换机
D. 集线器

18. 路由器通过哪种方式划分网段?
A. 减少广播域
B. 提供更多的逻辑网段
C. 减少带宽
D. A和B

19. 下面哪种不是在局域网部署第3层设备带来的好处？
    A. 能将局域网划分成独立的物理和逻辑网络
    B. 能提供广域网的连接
    C. 为网络提供逻辑结构
    D. 增加局域网的规模
20. 下面哪个是企业级服务器的例子？
    A. 大公司里的CAD服务器
    B. 校园区的DNS服务器
    C. 学校的管理记录服务器（成绩和文档）
    D. 工资和会计服务器



第6章　交换机

目标

学习完本章后，你将能够：

- 启动交换机。
- 识别交换机的组成部分。
- 描述并识别接入层交换机的应用场合。
- 描述并识别汇聚层交换机的应用场合。
- 描述并识别核心层交换机的应用场合。

本章将简单对比集线器和现代的交换技术，并介绍*交换机*的特点和组成部分，包括LED指示灯及各种指示灯信息的含义。随后将介绍交换机的初始化过程、控制台连接和命令行帮助。本章将集中介绍各种不同类型和不同型号的交换机，分级化的网络设计和交换机在接入层、汇聚层和核心层的应用。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图。光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

6.1　交换机概述

交换机是第2层网络设备，主要是作为工作站、服务器、路由器、集线器和其他交换机的集中点。

与交换机一样，*集线器*（hub）是早期的集中设备，提供*多端口*（ports）的连接。集线器比交换机的功能要差一些，主要是因为连接在集线器上的所有网络设备处于同一个带宽域，会引起冲突。另外，集线器工作在半双工的模式下，这就意味着在一个特定的时刻只能发送或者接收数据。

交换机是一台多端口的网桥，是当前采用星型拓扑结构的以太局域网的标准技术。交换机为所连接的两台的连网设备提供一条独享的点到点的虚线路，因此避免了冲突。交换机可以工作在全双工模式之下，这意味着可以同时发送和接收数据。对于网络支持工作而言，理解并配置交换机是很关键的。

局域网用于连接一个房间、一幢大楼或者靠近的一组大楼。在同一地点的并且由单一组织管理的一组大楼称为一个园区（campus）。较大型局域网的设计需要遵循如下的原则：

- 接入层用于将最终用户连接到局域网。

- 汇聚层在终端用户所在的局域网之间提供基于策略的连接。
- 核心层提供汇聚层节点之间的最快速连接。

当局域网的规模扩大到园区之后，需要不同类型的局域网交换机。每一层需要最适合该层功能的交换机。因为对网络层次的定位不同，所设计的交换机的特点、功能和技术指标也会各不相同。选择一个最适合该层次的交换机可以确保局域网用户获得最佳的网络性能。

因此，理解各层的作用和工作在该层上的交换机的功能对于设计一个高效的交换式局域网是很重要的。

6.2　交换机启动

要将一台刚关闭或刚拆除包装的全新交换机变成一台在网络上管理网络通信的设备需要一些步骤。下一节列出了这些步骤，并将介绍了如何验证交换机已经成功地启动并执行所需的步骤、已经准备就绪，能够被配置并置于生产环境中。

6.2.1　Catalyst交换机的物理启动

交换机是一台专用的特殊的计算机，它包括中央处理器（CPU）、随机存储器（RAM）和操作系统。如图6-1所示，交换机通常会有若干端口用于连接主机，同时还会有几个专用的管理端口。通过连接到交换机构控制台端口，如图6-2，可以对交换机进行管理，并查看和变更交换机的配置。



图6-1　Cisco交换机的端口



图6-2　控制台端口的连接

交换机通常没有用于开启和关闭的电源开关，而是简单地通过连接/断开电源进行控制。例6-1给出了Cisco交换机启动时命令行界面（CLI, Command-Line Interface）的输出。

例6-1 Cisco交换机的启动信息

```
32K bytes of flash simulated non-volatile configuration memory
Base Ethernet MAC address: 00:04:4D:D2:3D:00
Motherboard assembly number:73-3382-08
Power supply part number:34-0834-01
Motherboard serial number: FAB044685H5
Power supply serial number: DAB04283*PL
Model revision number: A0
Motherboard revision number: C0
Model number: WS-C2924 XL-EN
System serial number: FAB0447S0X2
Press RETURN to get started!
00:00:27: %SYS-5-RESTART: System restarted
Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5.2)XU,
    MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2000 by cisco Systems, Inc.
```

6.2.2 交换机的LED指示灯

交换机的前面板有几个指示灯，用于监控系统的活动和性能。这些指示灯称为发光二极管（Light Emitting Diodes, LED）。前面板上的指示灯包括：

- 系统指示灯（system LED）。
- 远程电源供应（RPS）指示灯。
- 端口模式指示灯（Port Mode LEDs）。
- 端口状态指示灯（Port States LEDs）。

1 系统指示灯

系统指示灯（System LED），如前图6-1所示，显示系统是否已经接通电源并且正常工作。表6-1说明了系统指示灯的几种可能的状态。

表6-1 系统指示灯的状态

指示灯颜色	系统状态
关闭	系统未加电
绿色	系统运行正常
琥珀色	系统加电但运行不正常

2 远程电源供应（RPS）指示灯

远程电源供应（RPS, Remote Power Supply）指示灯显示交换机是否由远程电源供电。RPS指示灯表明了交换机的RPS状态。表6-2说明了交换机上RPS指示灯各种颜色的含义。

表6-2　远程电源供应指示灯的状态

指示灯颜色	RPS状态
关闭	RPS关闭或未安装
持续绿色	RPS已连接并可用
闪烁绿色	RPS正在支持堆叠（stack）中的另一台交换机
持续琥珀色	RPS已连接但工作不正常
闪烁琥珀色	交换机内部电源出现故障，正在使用RPS

3　端口模式指示灯

端口模式指示灯（Port Mode LEDs）显示模式（Mode）按钮的当前状态。各种模式用于决定如何对端口状态LED进行解释。如果要选择或改变端口模式，连续地按压Mode按钮直至Mode LED指示在所需的模式。端口状态LED能代表多种含义，取决于Mode LED的当前值，参见表6-3。

位于交换机前面板的Mode按钮用于确定如何对端口状态灯的含义进行解释。

Mode按钮有三种状态：

- STAT（状态，States）。
- UTL（利用率，Utilization）。
- FDUP（全双工，Full Duplex）。

如果交换机的状态灯为闪烁的橙色，一般表明在某一个端口、模块或者交换机有硬件故障。如果端口或者模块状态不正常，状态灯也为闪烁的橙色。

4　端口状态指示灯

每一个端口都有一个端口状态指示灯（Port States LED）。这些灯显示交换机或者单个端口的状态。表6-3说明了交换机各种端口模式的含义。

表6-3　端口模式指示灯的状态

模式LED	端口模式	描述
STAT	端口状态	显示端口状态，这是缺省模式
VTIL	交换机利用率	显示目前该端口被交换机使用的带宽
DUPLX	端口双工模式	可以是半双工或全双工
SPEED	端口速度	端口运行速度（对10/100端口可以是10 Mbit/s或100 Mbit/s）

要选择或改变端口模式，可以通过按压Mode按钮直至需要的模式被选中。表6-4说明了在各种端口模式下端口状态指示灯各种颜色的含义。

表6-4　不同端口模式下端口模式指示灯的状态

模式LED	颜色	描述
STAT 端口状态	关闭 持续绿色 闪烁绿色 绿色/琥珀色交替 持续琥珀色	无链路 链路正常运行 发送或接收数据 链路处于转发状态 端口目前未转发
UTIL 交换机利用率	绿色 琥珀色	当间的背板利用率 最大的背板利率
	绿色和琥珀色	如果所有的LED都是绿色，交换机当前的带宽使用率达到了总带宽的50%或更高随着带宽使用绿的下降，部分LED变为琥珀色
DUPLX 端口双工模式	关闭 绿色	半双工 全双工
SPEED 端口速率（10/100端口）	关闭 绿色	端口运行在10Mbit/s 端口运行在100Mbit/s

6.2.3 在交换机POST阶段检查端口LED

在电源线连接好之后，交换机会启动一系列称为加电自测试（POST，power-on self test）的测试用于检测交换机是否工作正常。“系统指示灯（System LED）”会显示POST成功与否。如果交换机已经加电，系统指示灯是灭的，说明POST正在进行。如果系统指示灯变为绿色，说明POST已经成功。如果系统指示灯为琥珀色，则POST失败。POST失败是一个致命的错误。如果POST检测失败，交换机就不能可靠的工作。

“端口状态指示灯（Port States LED）”也会在POST过程中有所变化。在交换机发现网络拓扑结构并搜索环路时，端口状态指示灯会变为琥珀色并持续大约30秒。如果端口状态指示灯变成绿色，说明交换机的一个端口已经和目标（例如一台计算机）成功建立链接。如果端口指示灯不亮，说明交换机确定没有连接到端口的设备。

6.2.4 观察交换机的初始启动输出

为了配置或检查交换机的状态，需要将一台计算机连接到交换机上，并建立双方之间的通信。使用一根反转线缆（rollover cable）连接交换机背面的“控制台端口（console port）”和计算机背面的串口（COM port）。同样的线缆和操作也适用于连接路由器的控制台端口。

启动计算机的“超级终端（Hyper Terminal）”程序，会显示一个如图6-3所示的对话窗口。第一次建立交换机和超级终端的连接时，首先要为这一连接命名。在下拉菜单中选择连接交换机所使用的COM端口，点击确定按钮，如图6-4所示。第二个对话窗口出现，按照图6-5配置相应的参数，



图6-3 超级终端



图6-4 超级终端会话的命名



图6-5　超级终端的设置

点击确定按钮。

将交换机连接到一个过电保护的电源上。交换机初始化启动输出会显示在超级终端的屏幕上。在交换机加电之后，应该注意检查交换机的初始化启动输出。这一输出显示了交换机的相关信息、POST过程中的详细信息，以及关于交换机硬件的数据。

例6-2到例6-4说明了如标题所示的各种输出。

例6-2　装载和初始化Flash

```
C2950 Boot Loader(CALHOUN-HBOOT-M)Version 12.0(5.3)WC(1), MAINTENANCE INTERIM
SOFTWARE
Compiled Mon 30-Apr-01 07:56 by devgoyal
WS-C2950-24 starting...
Base ethernet MAC Address: 00:08:e3:2e:e6:00
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 162 files, 3 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 2961920
flashfs[0]: Bytes available: 4779520
flashfs[0]: flashfs fsck took 6 seconds.
...done initializing flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:c2950-c3h2s-mz.120-5.3.WC.1.bin" ...
##################################################################
##################################################################
File "flash:c2950-c3h2s-mz.120-5.3.WC.1.bin" uncompressed and installed,
    entry point: 0x80010000
executing...
```

例6-3 POST

```
Initializing flashfs...
flashfs[1]: 162 files, 3 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 7741440
flashfs[1]: Bytes used: 2961920
flashfs[1]: Bytes available: 4779520
flashfs[1]: flashfs fsck took 6 seconds.
flashfs[1]: Initialization complete.
Done initializing flashfs.
C2950 POST: System Board Test : Passed
C2950 POST: Ethernet Controller Test : Passed
C2950 POST: MII TEST : Passed
cisco WS-C2950-12 (RC32300) processor (revision B0) with 22260K bytes of memory.
Processor board ID FOC0605W0BH
Last reset from system-reset
```

例6-4 初始化完成

```
Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:08:E3:2E:B6:00
Motherboard assembly number: 73-5782-08
Power supply part number: 34-0965-01
Motherboard serial number: FOC060502HP
Power supply serial number: PHI05500C5D
Model revision number: B0
Motherboard revision number: B0
Model number: WS-C2950-12
System serial number: FOC0605W0BH
Press RETURN to get started!
C2950 INIT: Complete
```

在交换机完成启动和POST之后，会出现关于系统配置对话（System Configuration dialog）的提示。你可以对交换机进行手工配置，使不使用系统配置对话（System Configuration dialog或setup dialog）均可。交换机的系统配置对话比路由器的要简单很多。你可以在特权EXEC提示符下，通过输入setup命令进入系统配置对话。

6.2.5 查看交换机命令行界面的帮助信息

Cisco交换机的命令行界面与Cisco路由器的命令行界面类似。

通过键入一个问号（?）可以执行帮助命令。当你在命令提示符后执行帮助命令时，当前命令模式下可用命令列表就会显示出来，如例6-5所示。

例6-5 ?（帮助）命令的输出

```
Switch>?
access-enable Create a temporary Access-List entry
access-profile Apply user-profile to interface
clear Reset functions
connect     Open a terminal connection
disable     Turn off privileged commands
disconnect Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
help        Description of the interactive help system
lat         Open a lat connection
lock        Lock the terminal
login       Log in as a particular user
logout      Exit from the EXEC
mtrace      Trace reverse multicast path from destination to source
name-connection Name an existing network connection
pad             Open a X.29 PAD connection
ping            Send echo messages
ppp             Start IETF Point-to-Point Protocol(PPP)
--more--
```

帮助命令很灵活。如果想要得到以特定字符序列开头的命令列表，只需在这些字符后面直接键入一个问号（?）。不用在问号前面再键入空格。这种形式的帮助叫做命令字帮助（word help），因为它可以帮助键入一条命令。在使用上下文敏感的帮助时，问号前面的空格（或不空格）是很重要的。例如，为了获得交换机show命令选项的列表，需要在show命令之后键入空格和问号，如例6-6所示。例6-7显示了这样一个例子：在字母r后面直接键入一个“？”，可以找到以r开头的命令。（在这个例子中，不需要键入空格。）

例6-6 show ?命令的输出

```
Switch>show ?
class-map  Show QoS Class Map
clock      Display the system clock
diags      Show runtime diagnostic info
exception  exception information
flash:     display information about flash: file system
history    Display the session command history
hosts      IP domain-name, lookup style, nameservers, and host table
location   Display the system location
policy-map Show QoS Policy Map
```

```
- more--
Example 6-7Keyword Help Command
Switch>show r?
rmon
Switch>show r_
```

在例6-6中，只要在命令的关键字或参数的位置上键入问号，就可以列出该命令的关键字和参数。问号前面需要一个空格。这种形式的帮助叫做命令语法帮助（cammand syntax help），因为它可以根据已经输入的命令、关键字和参数提醒用户适用的关键字或参数。

和路由器类似，交换机也有几种命令模式。缺省模式是用户EXEC模式，可以通过以大于号结尾的提示符加以识别。在用户EXEC模式中可以使用的命令仅限于修改终端设置，完成基本测试和显示系统信息的命令。

通过enable命令可以从用户EXEC模式切换到特权EXEC模式。特权EXEC模式通过以“#”号结尾的提示符加以识别，如下所示：

```
Switch#
```

特权EXEC模式中的命令集包括在用户EXEC模式中允许使用的命令，另外还有configure terminal、configure memory、configure network命令，通过这些命令可以进入其他命令模式。因为这些模式是用于配置交换机的，所以需要密码才能够进入特权EXEC模式，以防止非授权的使用。如果系统管理员设置了密码，在进入特权EXEC模式之前会提示用户输入密码。密码的内容不会显示在屏幕上，并且密码是大小写敏感的。例6-7中列出了在特权EXEC模式中可以使用的命令。

例6-7 show? 命令的输出

```
Switch#?
Exec commands:
access-enable  Create a temporary Access-List entry
access-profile Apply user-profile to interface
access-template Create a temporary Access-List entry
Archive manage archive files
clear          Reset functions
clock          Manage the system clock
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
disconnect     Disconnect an existing network connection
enable         Turn on privileged commands
erase          Erase a filesystem
--More--
```

注意，这些命令与用户EXEC模式中下的命令是不同的。

6.3　局域网交换机与分级网络设计

分级网络设计模型把一个复杂的网络问题分解为多个小的、更易于管理的问题。分级结构中的每一级或层都负责可以解决一组不同的问题，这使得网络硬件和软件能够为实现特定的任务而进行优化。分级中最低层的设备设计用于接收进入网络的通信，并将其传送给高层。Cisco提供了一种3层的分级作为推荐的网络设计方法。

在3层网络设计模型中，网络设备按照3个层次进行分组：核心层（core）、汇聚层（distribution）和接入层（access），如图6-6所示。同开放系统互连（OSI）参考模型类似，3层设计模型是一个概念上的框架，也就是一个抽象的网络图。

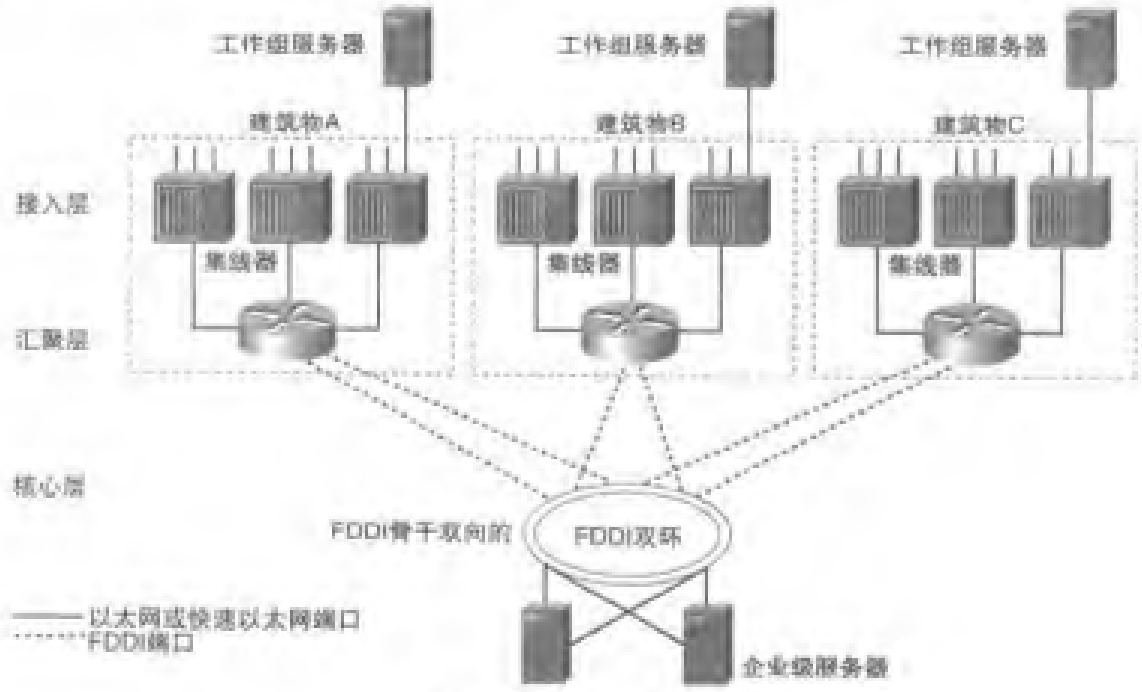


图6-6　分级设计模型

由于分级模型易于模块化，它对于网络设计非常有用。因为每层设备有类似的、明确定义的功能，管理员可以很容易地增加、替换以及去除网络某一部分。这种灵活性和可适应性使得分级网络设计是一种可扩展的网络设计。

分级网络设计模型适合于任何网络设计。需要强调的一点是这3个层次可能位于清晰明确的不同物理实体中，但并非一定如此。定义这3个层次可以帮助完成成功的网络设计，以表现出网络中必须具有的功能。

但是层次模型也可能很难理解，因为每一层的准确构成是因网络而异的。3层设计模型中的每一个层次都可能会包含路由器、交换机、链路或者是这些设备的组合。实际上，有些网络也许把两个层次的功能合并到单一的设备中，或者完全忽略某个层次。

下面3节将对这3个层次进行详细表述。

6.3.1　核心层

网络的核心只有一个用途：通过高速转发通信，提供优化的、可靠的传输结构。换句话说，核心层（core layer）应该尽可能快地交换分组。在该层中的设备不应该承担访问列表检查、数据加密、地址翻译或者其他影响的最快速率交换分组的任务。

6.3.2 汇聚层

汇聚层（distribution layer）位于接入层和核心层之间，它把核心层同网络的其他部分区分开来。该层的目的是通过使用访问列表和其他的过滤器限制进入核心层的通信以提供边界的定义。因而，该层次定义了网络的策略。策略（policy）就是处理某些类型通信的一种方法，这些通信的类型包括路由选择更新、路由汇总、VLAN通信以及地址聚合。可以使用策略来保护网络，并通过阻止不必要的通信来保留网络资源。

如果网络中有两种或多种路由选择协议，比如路由选择信息协议（RIP）和内部网关路由选择协议（IGRP），则各个路由选择域之间的信息共享，或重分配是在汇聚层完成的。

6.3.3 接入层

接入层（access layer）为网络提供通信，并且实现网络入口控制。最终用户通过接入层访问网络的。作为网络的“前门”，接入层使用访问列表以阻止非授权的用户进入网络。通过广域网技术，比如帧中继、ISDN或租用线，接入层也能为远程地点提供网络接入。

6.3.4 交换式局域网、接入层概述

在组建满足中型到大型组织所需要局域网的过程中，使用分级设计模型能帮助建设取得成功。分级设计模型也使得网络随组织发展的变化更加容易。

接入层是用户工作站和服务器连接到网络的入口。在一个园区局域网中，接入层中使用的设备既可以是交换机，也可以是集线器。如果使用集线器，带宽是共享的。如果使用交换机，那么带宽是独占的。如果两台乃至多台用户工作站或服务器直接连接到交换机的端口上，这些计算机都可以使用连接到交换机的全部带宽。而如果两台或多台计算机连接到一台集线器上，那么每一台计算机能够使用的带宽将是总带宽除以计算机数目。

集线器可以接到交换机端口上。这种情况下，通过集线器连接到交换机端口的设备共享带宽。

接入层的功能还包括：

- 共享式带宽（shared bandwidth）。
- 交换式带宽（switched bandwidth）。
- MAC层过滤（MAC layer filtering）。
- ***微分段***（microsegmentation）。

MAC层过滤使得交换机能只将帧传送到连接特定目的设备的交换机端口。交换机能创建很小的第2层网段，称为微分段（microsegmentation）。这些冲突域可以小到只有两台设备（即目的设备和所连接的交换机端口）。接入层使用第2层交换机。

6.3.5 接入层交换机

如图6-7所示，接入层交换机运行在OSI模型的第2层，提供各种服务，如虚拟局域网（VLAN）。接入层交换机的主要目的是允许最终用户连接到网络。接入层交换机应该以低成本和高端口密度提供这种功能。

通常用在接入层使用的Cisco交换机包括：

- Catalyst 1900系列。
- Catalyst 2820系列。
- Catalyst 2950系列。
- Catalyst 4000系列。
- Catalyst 5000系列。

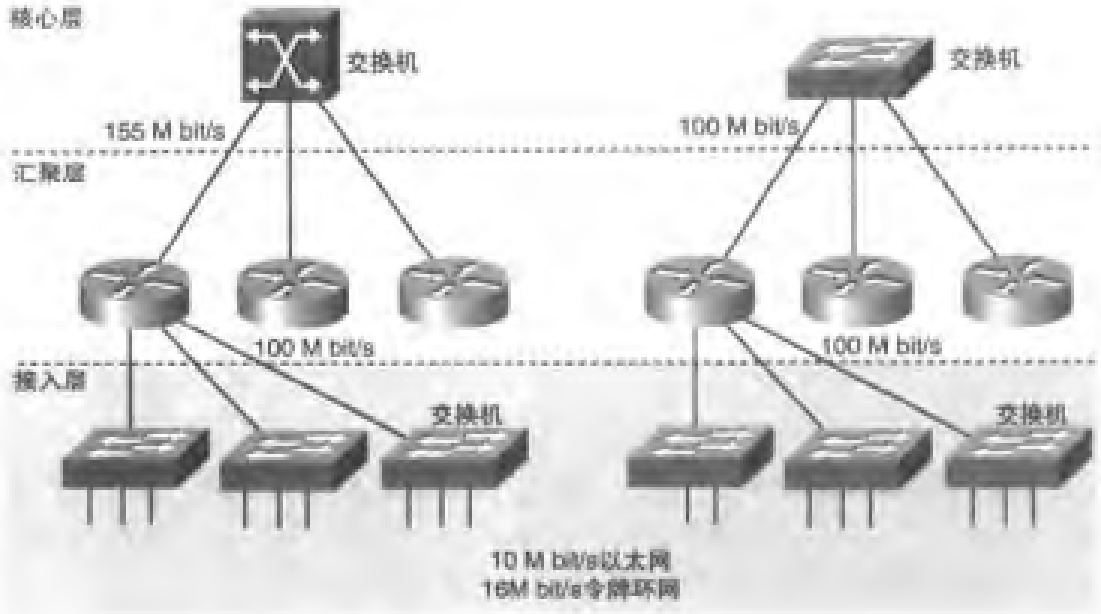


图6-7　接入层交换机

表6-5列出了这些接入层交换机的特征。

在小型或中型园区网中，Catalyst 1900或2820系列交换机有效的接入设备。Catalyst 2950系列交换机适用于为需要更高带宽的服务器或用户提供接入。这是通过提供具有快速以太网交换端口来完成的。Catalyst 4000和5000系列交换机包括吉比特以太网端口，适用于作为大量的用户或大型园区网的接入设备。

在非园区网环境中，接入层可以通过类似帧中继、ISDN、XDSL或租用线路这样的广域技术为远端站点提供到企业网络的接入。

这3层（核心层、汇聚层和访问层）常常被错误地认为必须存在于清楚分明的物理实体中。事实并非如此。定义这些层次的目的是为了帮助成功的网络设计并表示网络中必须存在的功能。这些层次的实现完成取决于所设计网络的需求。然而，重要的是，为了使得网络能优化地工作，并在发展过程中保持扩展性，就必须保持分级结构。

6.3.6　汇聚层概述

网络的汇聚层位于接入层和核心层之间，能帮助定义和分离核心。该层的主要目的是提供一个边界的定义，以在其内进行分组处理。该层将网络分段为多个广播域。访问控制列表可以实施策略并过滤分组。汇聚层将网络问题限制在发生问题的工作组内，防止这些问题影响到核心层。该层的交换机运行在第2层和第3层上。目前，你把第3层交换看作快速路由选择就足够了。在交换式网络中，汇聚层包含很多功能，如：

- 布线间连接的汇聚。
- 定义广播/组播域。
- VLAN路由选择。
- 需要进行的任何介质转换。
- 安全性。

表6-5　接入层交换机

Catalyst	类型	支持的OSI层次	以太网端口	快速以太网端口	吉比特以太网	企业规模
1900系列	固定配置	第2层	12或24	2	0	小到中型
2820系列	模组扩展卡	第2层	24	2	0	小到中型

（续）

Catalyst	类型	支持的OSI层次	以太网端口	快速以太网端口	吉比特以太网	企业规模
2950系列	固定配置	第2层	0	12或24速率可配置	0或2	小到中型
4000系列	每机架有多个模块化插槽	第2层或第3层	0	可配置端口数，共可以到240个	可配置端口数，共可以到240个	中到大型
5000系列	每机架有多个模块化插槽	第2层或第3层	0	根据选择变化	根据选择变化	中到大型

6.3.7 汇聚层交换机

汇聚层交换机是多台接入层交换机的汇聚点。该交换机必须能处理来自接入层设备的所有通信量。

汇聚层交换机需要具备高性能。这是广播域的分界点。汇聚层汇聚了VLAN的通信，成为关于通信流的策略决策的焦点。由于这些原因，汇聚层交换机运行在OSI的第2层和第3层。该层的交换机被称为多层交换机（multilayer switch）。这类交换机在一台设备中组合了路由器和交换机的功能，但其通过对通信进行交换所获得的性能比标准路由器要高。如果这些多层交换机没有一个关联路由器模块，则需要使用外置路由器来实现第3层的功能。

适合汇聚层的Cisco交换机包括：

- Catalyst 2926G。
- Catalyst 5000系列。
- Catalyst 6000系列。

汇聚层设备与核心层设备相比，需要更少的接口（interface）和更低的交换速率，因为他们要处理的通信少。不过，如果汇聚层存在瓶颈，一个光速的核心层也是没有用处的。

汇聚层将网络的接入层和核心层分开，有利于定义和区分核心（参见图6-8）。该层提供了一个边界定义，是对分组进行处理的地方。在园区网环境中，汇聚层可能包括如下几种功能：

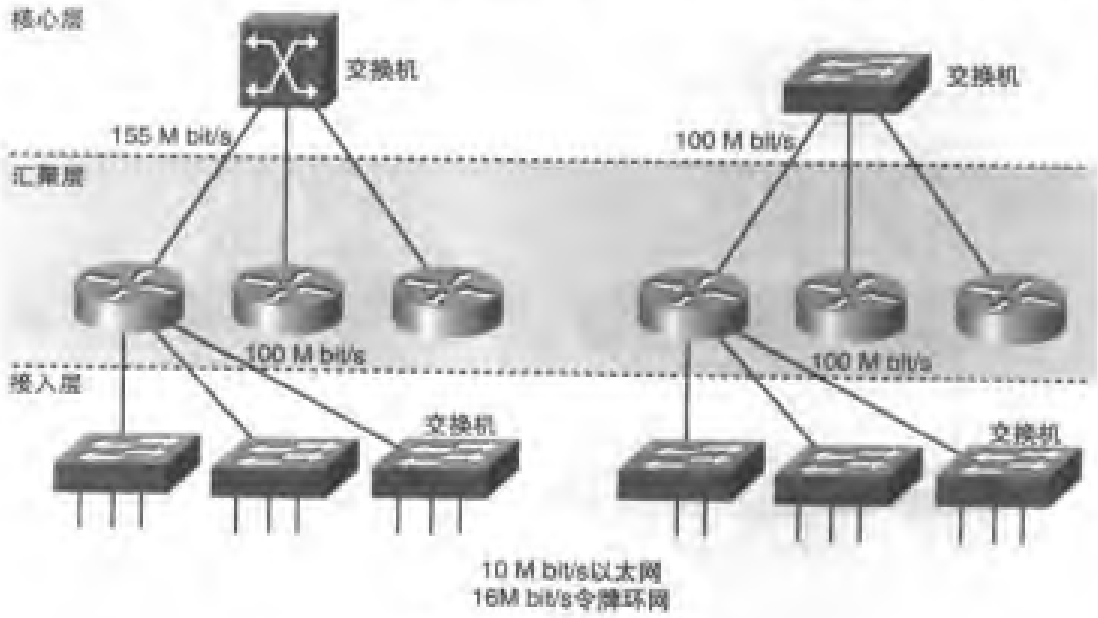


图6-8 汇聚层交换机

- 寻址或区域聚合。
- 部门或者工作组接入。

- 广播域/组播域定义。
- VLAN路由选择。
- 任何需要发生的介质转换。
- 安全性。

在非园区网环境中，汇聚层可以是路由选择域之间的重分配点（redistribution part）或者是静态和动态路由选择协议之间的分界处。也可以是远程站点访问公司网络的接入点。汇聚层可以总结为：提供基于策略的连接的层。

6.3.8　核心层概述

作为网络的中心，核心层被设计成快速而可靠。要避免在核心层使用访问列表，因为它们会增加延迟。此外，最终用户不应该能直接访问核心层。比如吃苹果，如果不先穿过果皮就无法得到苹果核里面的种子。在分级网络中，最终用户的通信只有通过了汇聚层和接入层以后才能到达核心层路由器，而访问列表应该应用在汇聚层和接入层。

由于核心路由选择没有访问列表、地址转换或者其他的分组处理，看起来好像不需要很强大的路由器就可以胜任这样简单的工作。然而，恰恰相反，在核心层使用的是最强大的Cisco路由器，因为它们有最快的交换技术和最大的物理接口容量。

6.3.9　核心层交换机

如图6-9所示，核心层是园区交换网络的骨干。该层的交换机使用一系列第2层技术。如果核心层交换机之间的距离不太远，这些交换机可以通过以太网技术连接。也可以其他的第2层技术，比如异步传输模式（ATM）信元交换。网络设计中，核心层可以是一个被路由核心（routed core）或者说第3层核心（layer 3 core）。核心层交换机被设计用于在需要时提供高效的第3层功能。在做出核心交换机的选择之前，你应该考虑如需求、成本和性能等因素。

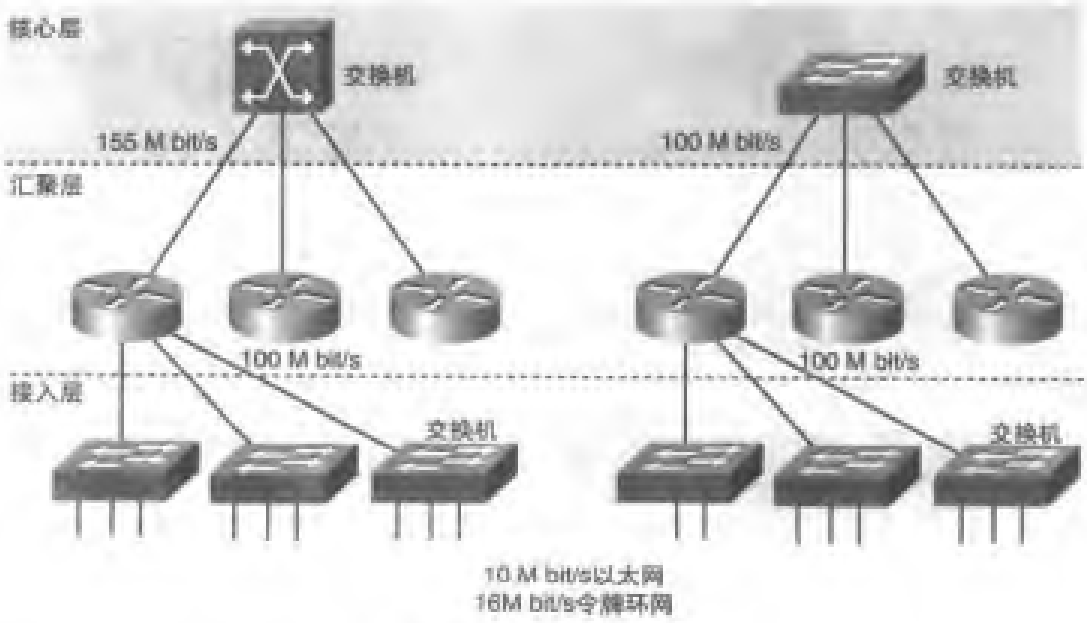


图6-9　核心层交换机

适合在核心层使用的Cisco交换机包括：

- Catalyst 6500系列。

- Catalyst 8500系列。
- IGX 8400系列。
- Lightstream 1010。

被Ciso定位为企业核心路由器的7000、7200和7500系列路由器也使用了最高速的交换模式。12000系列路由器也是核心路由器，但它是为满足Internet服务提供商（ISP）的核心路由的需要而设计的。除非你的公司要为其他公司提供Internet接入业务，否则你不太可能会在你们的电信机柜里看到12000系列的路由器。

与某些路由器（如2500系列）不同，7000、7200和7500系列路由器是模块化的，可以在需要的时候添加接口模块。这些路由器的大机箱可以在多个模块上提供很多接口，并且几乎覆盖了所有的介质类型。这使得这些路由器成为可扩展的、可靠的核心层解决方案。

核心路由器实现可靠性的一种方式是使用冗余链路，通常是同所有其他的核心路由器的连接都使用冗余链路。可能的情况下，这些冗余链路是对称的（即它们有相同的吞吐量），这样就可以使用等值（equal-cost）负载均衡。这就是核心层交换机需要相对较多接口的原因。核心路由器实现可靠性的另一方法是使用冗余电源。核心路由器通常提供两个或者更多的“热插拔（hot-swappable）”电源，单个电源可以被取下并替换而不会使路由器停止工作。

核心层连接应该使用最快、最可靠和广域网中最贵的租用线：T1、T3、OC3或者更高速的。如果在广域网核心层使用冗余的T1，每台路由器需要有4个串口来实现到各站点的两条点到点连接。

由于使用高端路由器和广域网链路，核心层可能会成为一个相当大的花销。有些设计者为了减少花费在核心层不使用对称链路。取而代之的是使用分组交换或者按需拨号技术（比如帧中继和ISDN）来做备份链路。使用这些技术来节省花费的代价是对性能的影响。比如，如果使用ISDN BRI作为备份链路，将会失去进行等值负载均衡的能力。

在广域网中不一定要有网络核心层。在某些情况下，局域网骨干也认为属于核心层。园区网或者跨越复杂办公楼或者临近建筑的大型网络，可能有一个基于局域网的核心层。这种情况下，交换式快速以太网或者吉比特以太网是最常用的核心层技术，它们通常使用光纤连接。企业机级交换机，比如Catalyst 400、5000和6000系列，担负起局域网核心层的任务，因为它们在第2层进行帧交换，所以路由器在第3层进行分组交换要快得多。事实上，作为模块化设备，这些交换机可以在机架上配备路由交换模块（RSM, route switch module）来增加第3层的路由选择功能。

6.4 总结

在本章中学习了分析和设计网络的一般模型。

- 该模型认为较大的网络分为3层。
- 接入层。
- 汇聚层。
- 核心层。

每层都有特定的功能。在交换式网络设计中，每层有其最适合的交换机。你还学习了各层交换机的特性以及改变带宽和性能所需要的技术。当前看来适合的设备可能并不满足未来的需求。作为网络专业人员的职责就是确保你所选择的交换设备最适合自己的网络。

作为本章学习内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

6.5　关键术语

接入层（*access layer*）　该层将通信传入网络并进行网络入口控制。最终用户通过接入层访问网络。

骨干（*backbone*）　网络的核心结构，连接网络中所有部件，使之可以通信。

核心层（*core layer*）　园区交换网络的骨干。该层的交换机可以使用许多第2层技术。

汇聚层（*distribution layer*）　该层定义了进行分组处理的边界。

集线器（*hub*）　通常指在星型拓扑网络中作为中心的设备。

接口（*interface*）　1、两个系统或者设备之间的连接。2、路由选择术语中，指网络连接。

微分段（*microsegmentation*）　将一个冲突域分成两个或者更多冲突域，以减少冲突和网络拥塞的过程。

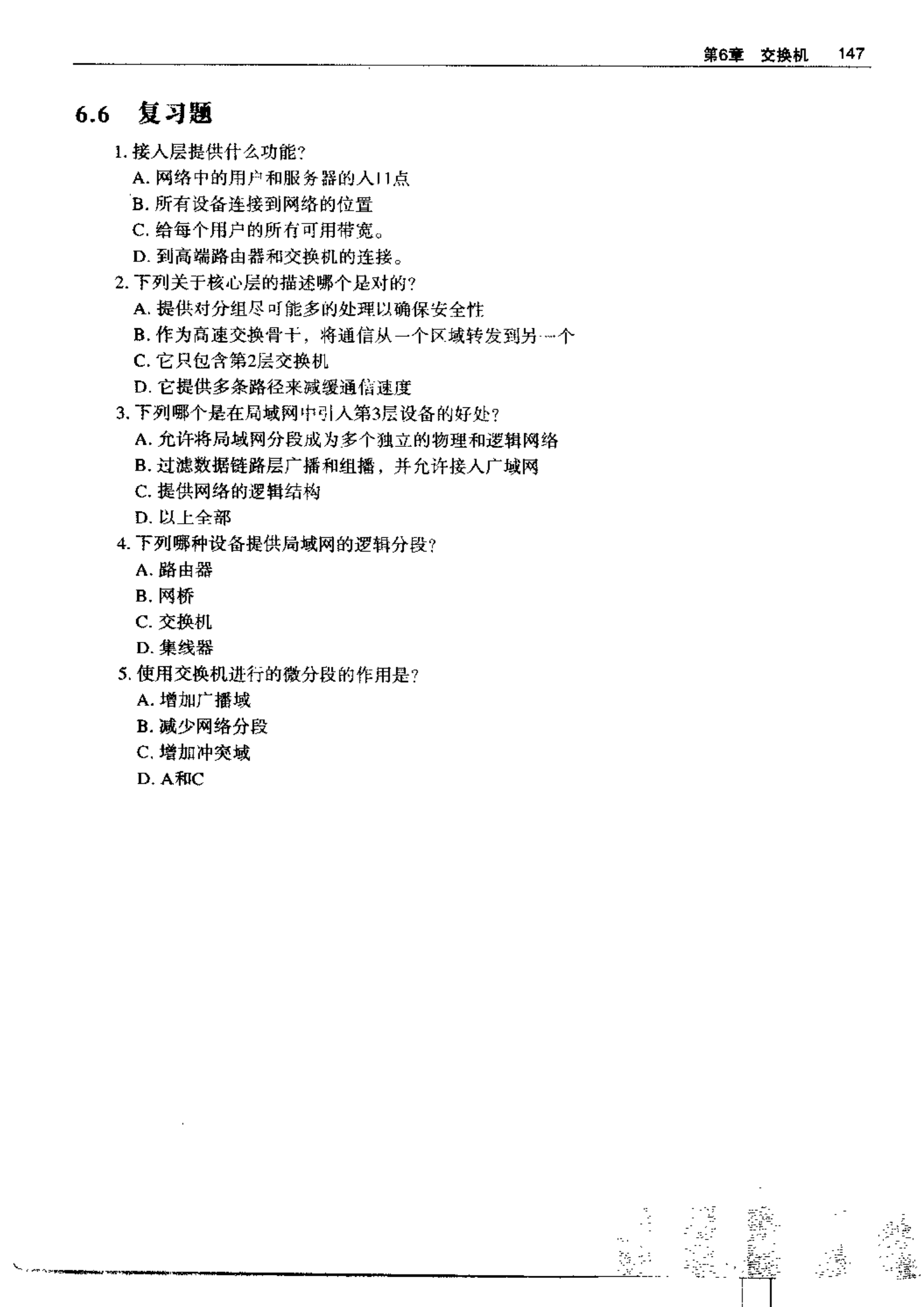
端口（*port*）　网络互连设备（比如路由器）上的接口。在接插面板（patch panel）上像RJ-45插孔那样允许插入具有相同尺寸插头的母口。这些端口使用的跳线（patch cord）用于实现接线面板上的计算机之间交叉互连。正是交叉互连使得局域网能工作。

交换机（*switch*）　根据每个帧上的目的地址进行帧的过滤、转发和泛洪操作的网络设备。交换机工作在OSI参考模型的数据链路层。

交换（*switching*）　将从一个接口传入的帧从另一个接口发送出去的过程。

6.6 复习题

1. 接入层提供什么功能?
   A. 网络中的用户和服务器的入口点
   B. 所有设备连接到网络的位置
   C. 给每个用户的所有可用带宽。
   D. 到高端路由器和交换机的连接。
2. 下列关于核心层的描述哪个是对的?
   A. 提供对分组尽可能多的处理以确保安全性
   B. 作为高速交换骨干，将通信从一个区域转发到另一个
   C. 它只包含第2层交换机
   D. 它提供多条路径来减缓通信速度
3. 下列哪个是在局域网中引入第3层设备的好处?
   A. 允许将局域网分段成为多个独立的物理和逻辑网络
   B. 过滤数据链路层广播和组播，并允许接入广域网
   C. 提供网络的逻辑结构
   D. 以上全部
4. 下列哪种设备提供局域网的逻辑分段?
   A. 路由器
   B. 网桥
   C. 交换机
   D. 集线器
5. 使用交换机进行的微分段的作用是?
   A. 增加广播域
   B. 减少网络分段
   C. 增加冲突域
   D. A和C





第7章　交换机配置

目标

学习完本章之后，你将能够：

- 描述微分段。
- 描述交换机如何学习地址。
- 描述交换机转发。
- 了解交换机和冲突域。
- 了解交换机和广播域。
- 配置LAN交换机。
- 验证LAN交换机配置。
- 管理LAN交换机。

交换机是第2层的设备，它用来解决带宽不足和网络瓶颈问题。交换机能够对LAN进行*微分段*（*microsegment*），使得每个微分段都是两台主机构成的网段（2-host segments），从而在一个较大的区域中创建了多个无冲突的区域。虽然LAN交换机消除了*冲突域*（*collision domain*），但是所有连到交换机的主机仍然是同一个*广播域*（*broadcast domain*）的一部分。因此，所有连接在一台LAN交换机的节点都能收到它们中任一节点发出的广播。

本章复习了交换机的一些基本属性和操作特性，并将重点放在了交换机的基本配置、验证和基于IOS的交换机的管理方面。本章还提供了设置交换机IP地址端口特性和其他配置参数的指南。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图，光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

7.1　微分段

对LAN进行分段有两个主要原因：第一是为了隔离各网段之间的通信，第二是通过创建更小的冲突域从而使每个用户获得更多的带宽。

使用第2层的交换机对LAN进行分段有几个原因，也带来了几个优点。首先，如果没有LAN分段，大于一个小型工作组的LAN将很快会变得拥塞并发生冲突，从而实质上没有任何带宽可供利用。

LAN分段可以通过网桥、交换机和路由器来实现。这些设备都有各自的优点和缺点。

添加这些设备可以将LAN划分成更小的冲突域，如图7-1所示。创建了4个冲突域。

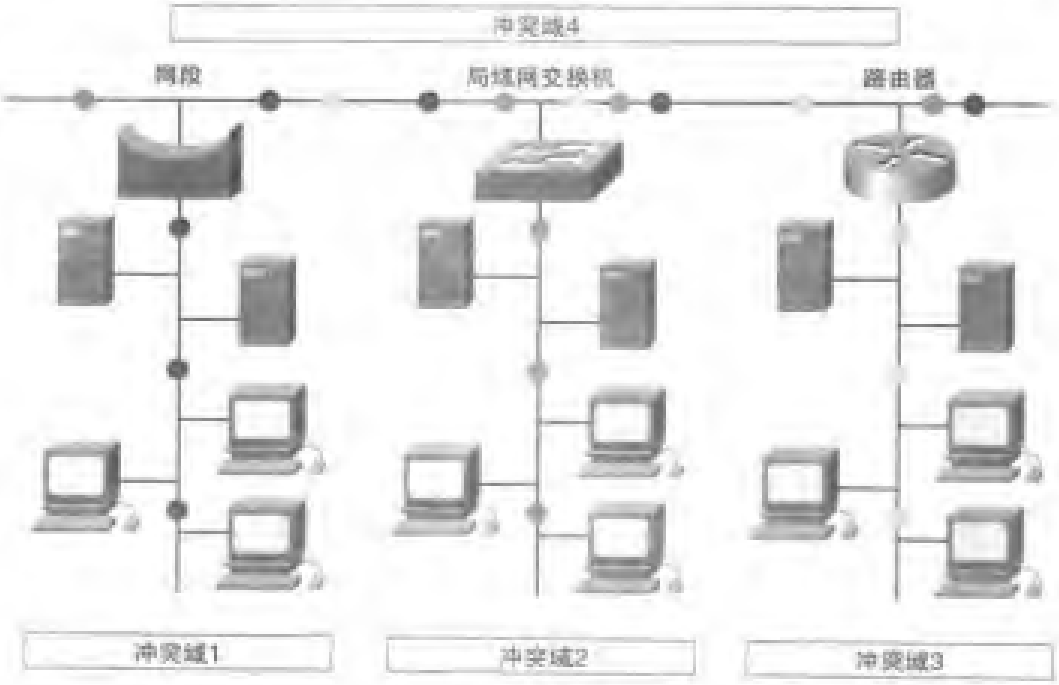


图7-1　冲突域

通过将大网络分成自我包含（self-contained）的多个单元，网桥和交换机能够带来一些优点。因为只转发了一部分通信，所以网桥和交换机减少了设备在所有连接的网段上所能接收到的通信。网桥和交换机增加了冲突域的数目，但减少了冲突域的大小；它们对广播域的大小没有影响。

路由器的每个接口都连接着一个独立的网络，因此在LAN中添加路由器能够产生比较小的冲突域和广播域。这是因为路由器不转发广播，除非对其编程上让它们这么做。

交换机利用微分段来减小LAN中的冲突域。它通过创建专用的网络分段或点到点的连接，并且把这些分段连接成交换机上的一个虚拟网络来实现这一功能。

虚拟网络电路只在两个节点需要通信时才会存在。把它称为虚电路（virtual circuit）是因为只有当需要的时候它才存在，而且它是建立在交换机内部的。图7-2显示了一个在微分段实现前后的网络。

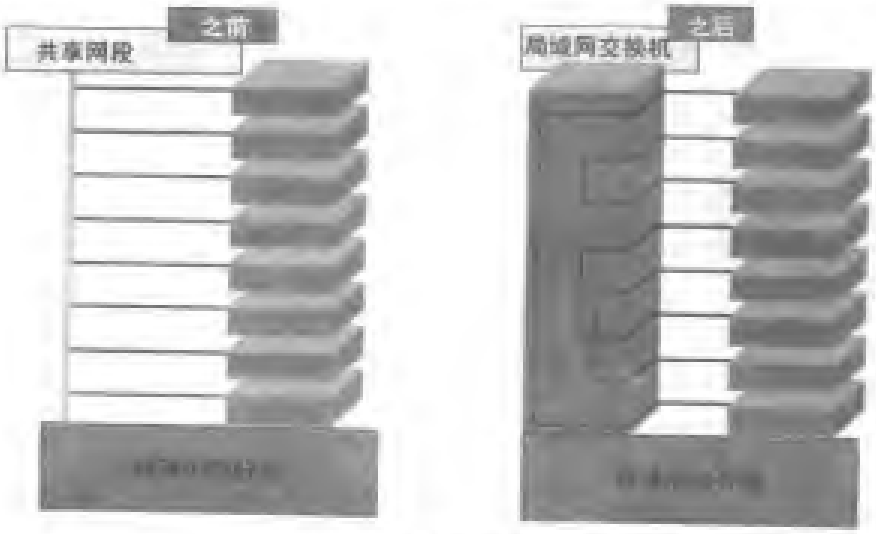


图7-2　网络的微分段

微分段的实现

因为使用了微分段，可以认为LAN交换机是没有冲突域的多端口网桥（multiport bridges）。

通过把帧交换到它的目的端口，数据能够高速地传输。如图7-3所示，通过读取第2层的目的MAC地址信息，交换机可以实现高速的数据传输，这与网桥的工作方式很相似。由于在整个帧进入交换机之前，就可以把帧发送到连接接收工作站的端口，因此帧转发时就可以获得低延迟级别和高传输速率。图7-4显示了一个交换表。

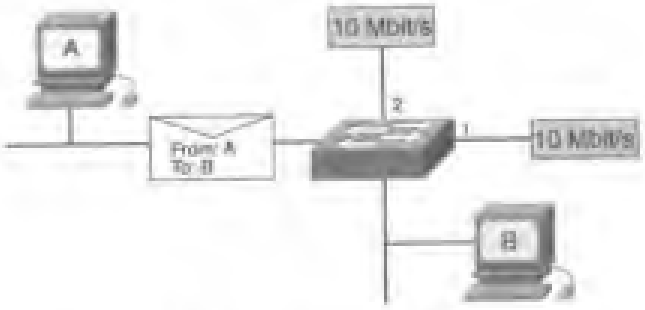


图7-3 LAN交换机操作

以太网交换机增加了网络的可用带宽，它通过创建网络分段或者建立点到点的连接，并在交换机内把这些分段连接成一个虚拟网来实现。这条虚拟的网络电路只在两个节点需要通信时才存在。称它为虚电路是因为只有当需要的时候它才存在，而且该电路是建立在交换机内部的。



图7-4 交换表

尽管LAN交换机减小了冲突域的大小，但是连接到交换机的所有主机仍然处于相同的广播域中。因此，通过LAN交换机连接的所有其他节点都会收到来自这些节点中的任一节点的广播。

交换机是数据链路层设备，它像网桥一样能够把多个物理上的LAN分段连接成一个较大的网络。与网桥相似，交换机基于MAC地址对通信进行转发或泛洪。因为交换是在硬件中而不是在软件中执行的，所以交换速度非常快。交换机的每个端口都能有效地充当微网桥，每个端口都充当一台独立的微网桥（microbridge），为每一台主机提供介质的全部可用带宽。图7-5显示了一个交换机如何能够把一个网络分割成单一广播域的例子。

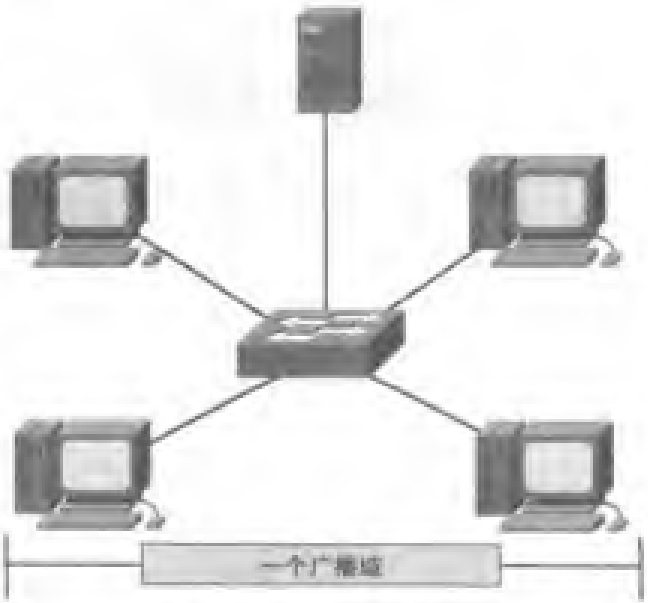


图7-5 LAN交换概述

7.2　交换机如何学习地址

以太网交换机能通过读取所传输的数据帧的源地址和记录帧进入的交换机的端口来学习网络上每台设备的地址。然后，交换机把这些信息添加到它的转发数据库或交换表中。地址是动态学习到的。也就是说当交换机读取到新的源地址时，它就学习到了新地址。交换机就会把该地址存储在*内容可寻址存储器（CAM）*中。如果读取到的源地址在CAM中找不到时，交换机就会学习并存储该地址，以备将来使用。

每次存储地址时，都会打上时间标记（timestamp）。这使得地址只能存储一段时间。每当地址被引用或在CAM中找到时，它们都将接收一个新的时间标记；那些在一段时间内都没有被引用的地址将从列表中删除。通过删除过时的或旧的地址，CAM维护了一个准确和实用的转发数据库。当替换一台工作站的网络接口卡时，这一点就显得尤其重要。

当工作站A需要传送数据到工作站B时，A发送的帧将穿过交换机，如图7-6所示。请记住，交换机是工作在第2层的。因此，当这个帧穿过网络的时候，交换机会查看它的介质访问控制（MAC）地址，以发现源MAC地址并将其存储到地址表中，如图7-7所示。

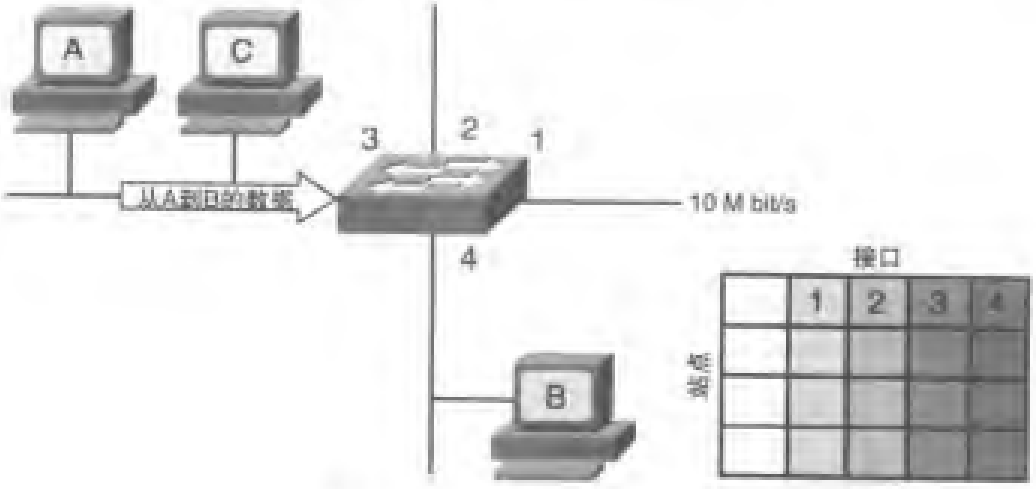


图7-6　LAN交换机操作示例

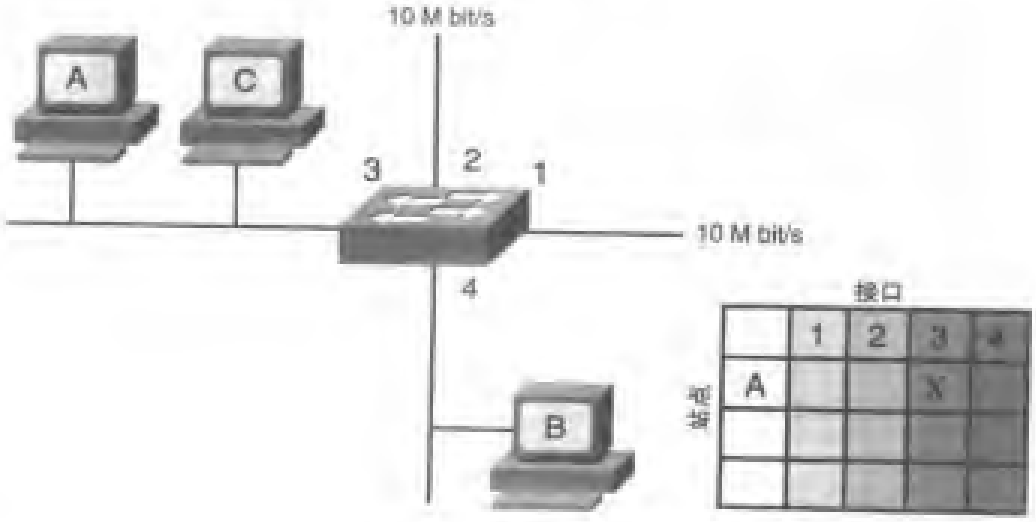


图7-7　更新转发表

当一个分组进入交换机的一个端口时，交换机将在地址表中生成一条记录条目，该条目指出发送分组的站点的MAC地址和分组所经过的端口。

当交换机需要转发帧时，它会检查该帧的目的MAC地址，然后查找CAM以确定哪一个端口能够到达那个目的地。如果交换机的转发表中没有该地址的相应条目，交换机就把该帧泛洪到除接收该帧的端口之外的所有端口上去，如图7-8所示。如果站点A发送一帧给站点B，由于目的地址未知，交换机就把该帧扩散到除端口3以外的所有端口中。当站点B响应站点A的时候，交换机会把站点B的MAC地址当作源地址，并在CAM中为站点B做了一条记录，现在交换机就知道站点B在哪里连接网络了。

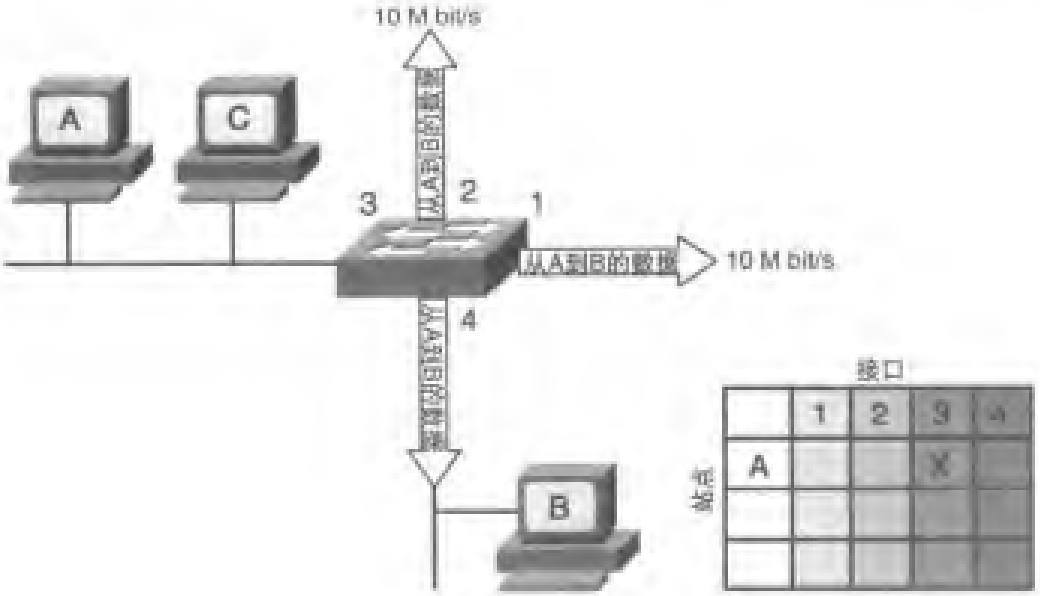


图7-8 MAC泛洪

现在数据可以从站点B经过交换机传送到站点A，但是这次交换机并不对流量进行泛洪。因为交换机知道站点A在网络上的位置（端口3），所以交换机只向端口3发送数据。在图7-9中，站点B将数据传送到交换机；在图7-10中，交换机从B往A传送数据。最初的数据传输已经指示了MAC地址来自于哪里，因此在后续的传输中，交换机能在网络中更有效率地传输流量。

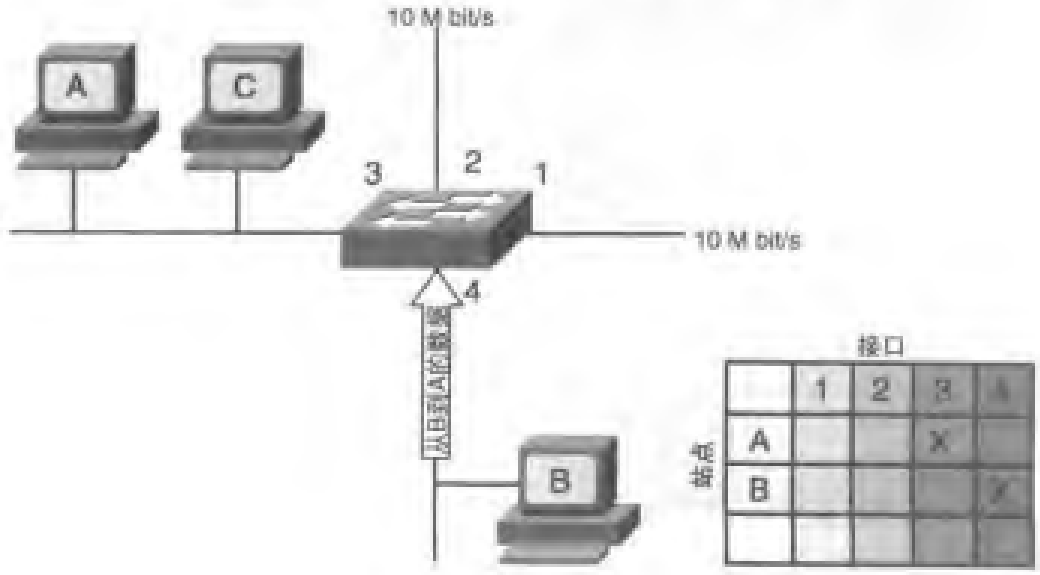


图7-9 数据从B到交换机

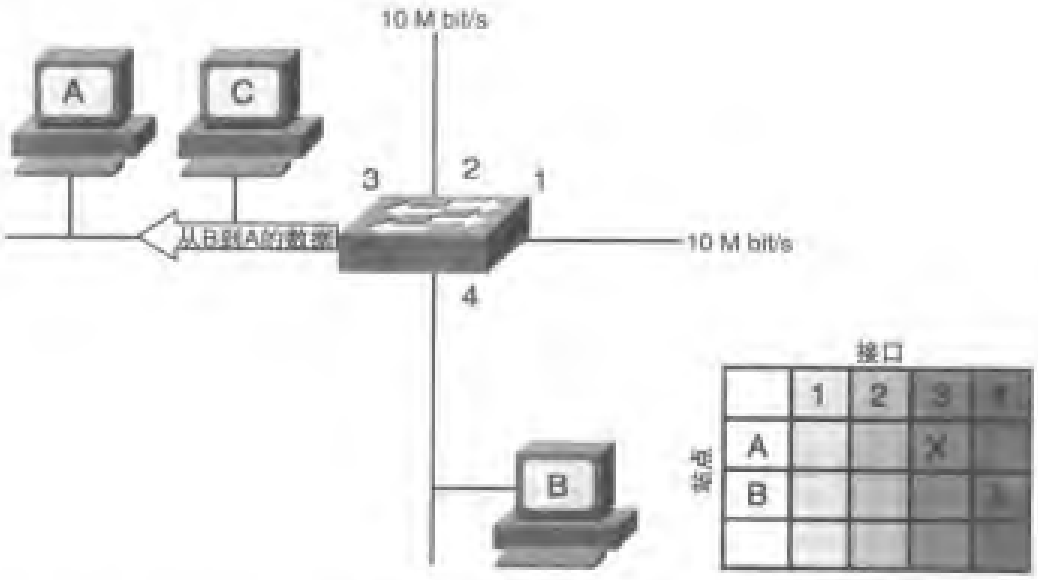


图7-10　数据从B到A

7.3　交换机的各种转发方式

通过交换机转发数据帧有两种交换模式：贯穿式（cut-through）和存储转发（store-and-forward）。

7.3.1　存储转发交换

当交换机执行*存储转发交换（store-and-forward switching）*时，在转发之前必须接收到整个帧。然后，交换机读取目的或源地址，并且在帧发送之前进行过滤。在交换机接收帧的过程中，会发生延迟。帧越大，延迟越长，因为需要更长的时间来读取整个帧。采用这种方式时，错误可以检测出来，因为在交换机等待整个帧接收完成的过程中，它有时间来检查错误，如图7-11所示。

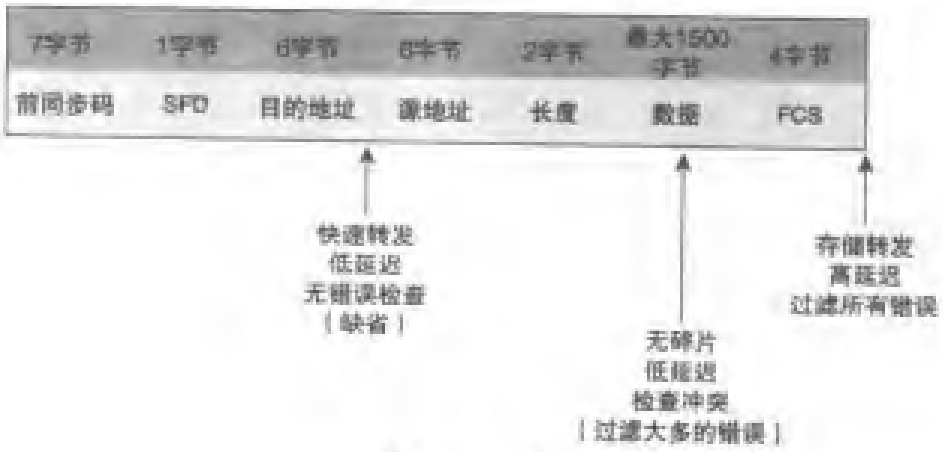


图7-11　帧头

7.3.2　贯穿式交换

交换机在执行*贯穿式交换（cut-through switching）*时，当它接收到帧时，它只读取目的地址。然后，在整个帧到达之前，帧就被转发出去。这种模式减少了传输延迟，但也减弱了错误检测，如图7-12所示。

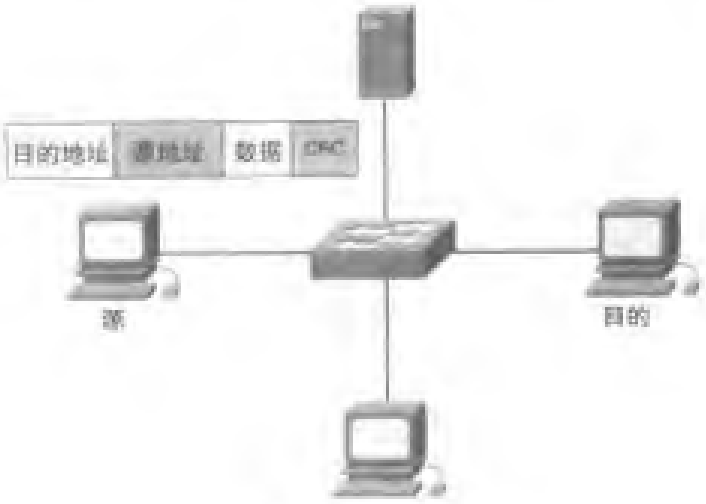


图7-12 存储转发

直穿交换有两种方式：

- **快速转发交换**（Fast-forward switching）——这类交换提供了最小的延迟。它一收到目的地址就立即转发分组来实现。由于快速转发交换在整个分组尚未全部接收到之前就开始转发，因此发生错误的分组可能会继续传播下去。尽管这种情况不经常发生，而且目的网络的适配器会在接收到分组时丢弃这个错误的分组，但是多余的通信在特定的环境中可能被认为是不可接受的。这时可以使用无碎片选项来减少转发出去的有错误的分组的数量。在快速转发模式中，延迟为接收到第1个比特起到开始发送第1个比特为止的时间段，或者是第1个比特进来到第1个比特出去（FIFO）所经历的时间。
- **无碎片交换**（Fragment-free switching）——这种交换方式在转发开始前会过滤掉冲突帧，这些帧大多数都是错误的分组。在正常运行的网络中，冲突帧必须小于64字节。任何大于64字节的分组都是有效的分组，因此通常会无误地接收。在这种方式中，无碎片在转发之前要等待，直到确定接收到的分组不是冲突帧时才开始转发分组。在该模式中，延时按FIFO来量度。

每种交换模式的延迟都取决于交换机转发帧的方式。交换模式越快，交换机的转发延迟就越短。但是为了完成快速帧转发，交换机就会用较短的时间去检查错误。折衷方案是使用较少的错误检查，但这会导致大量的重传。另外，虽然存储转发交换会导致更长的延迟，但是它确保了数据的完整性。

7.3.3 对称交换

*对称交换（symmetric switching）*是根据分配给交换机的每个端口的带宽来描述LAN交换机的一种方法，如图7-13所示。对称交换机在相同带宽的端口之间提供交换连接，例如全部10Mbit/s端口或全部100Mbit/s端口之间的连接。如图7-14所示，非对称LAN交换机则在不同带宽的端口间提供交换连接，例如10Mbit/s与100Mbit/s端口的混合使用的情况。

7.3.4 非对称交换

*非对称交换（Asymmetric switching）*应用于大多数的客户机/服务器网络通信中。在该模型中，当多个客户机同时与一台服务器通信时，要求将更多的带宽分配给与服务器相连接的那个交换机端口，以防止那个端口成为瓶颈。你将在下一节中学到，在非对称交换机中，需要使用存储缓冲技术，以使从100Mbit/s主的通信能够发送到10Mbit/s端口而不会对10Mbit/s 端口造成太大的拥塞。

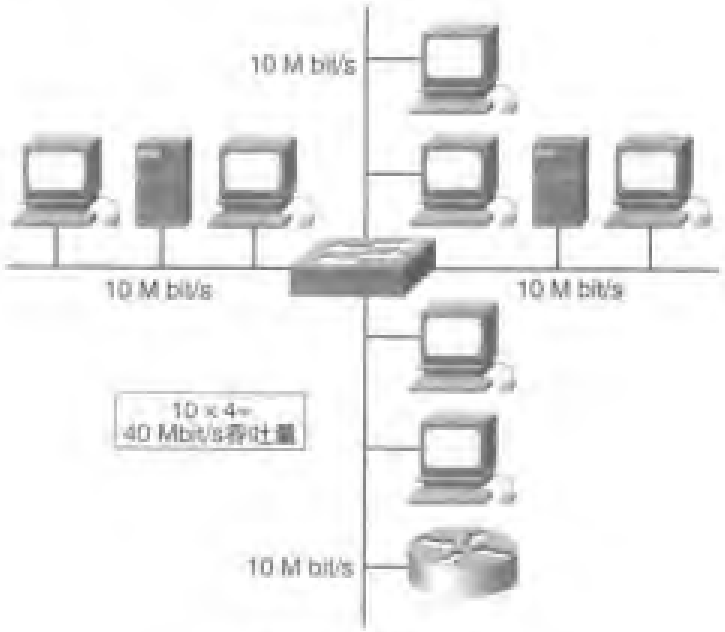


图7-13　对称交换

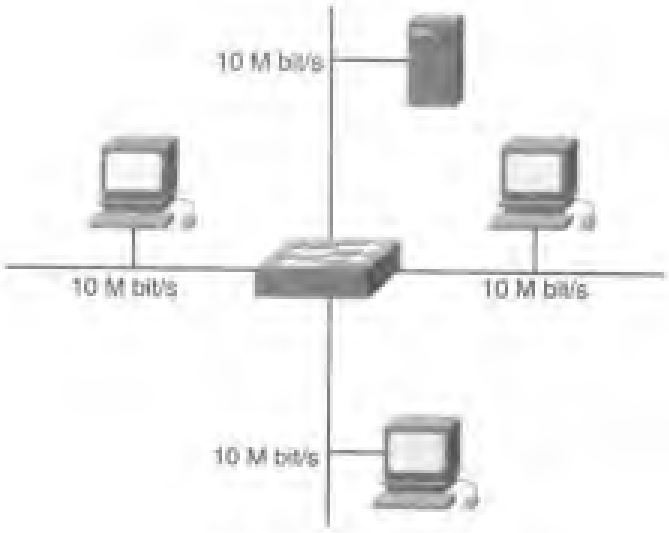


图7-14　非对称交换

7.3.5　内存缓冲技术

以太网交换机可以使用缓冲技术将分组存储和转发到正确的一个或多个端口。当目的端口忙时，也可以采用缓冲技术。交换机用来存储数据的存储器区域称为存储器缓冲区。存储缓冲技术使用两种方法来转发分组：基于端口的*存储缓冲*（port-based memory buffering）和共享式的存储缓冲（shared memory buffering）。

在基于端口的存储缓冲中，分组存储在链接到特定进入端口的队列中。只有当队列中所有在它之前的分组都被成功发送出去时，该分组才发送到外出端口。单一的一个分组就有可能因为目的端口繁忙而延迟存储器中所有分组的传送。这种延迟在即使其他分组能发送到开启的目的端口的情况下也会产生。

共享式存储缓冲把所有分组存入能由交换机上所有端口共享的公共存储缓冲区中。分配给一个端口的存储器数量由每个端口的实际需要而定。这称为缓冲区存储器的动态分配。缓冲区中的分组动态链接到发送端口，链接到为那个端口分配的存储器区域中。这使得分组无需移到不同队列就可

以在某个端口上接收并在另一个端口上发送。

交换机维护一张分组目的端口（分组需要经此到达接收者的端口）的映射表，交换机只有在分组已经成功传送后才清除这个目的端口映射。由于存储缓冲区是共享的，因此分组受整个存储器缓冲区大小的限制，而不是受分配给一个端口的缓冲区大小的限制。这意味着更多的分组能以更低的分组丢失率发送。存储缓冲对于10/100Mbit/s的交换机来说是很重要的，它使得100Mbit/s 端口能把分组转发到10Mbit/s端口。

7.4 交换机和冲突域

以太网/802.3网络的主要缺点是它们容易发生冲突。冲突的发生是由于两台主机同时发送帧所致，在较老的总线和基于集线器的以太网上冲突非常普遍。当冲突发生时，传送的帧会遭到破坏。根据以太网/802.3带冲突检测载波侦听多路访问（CSMA/CD）规则，此时发送主机进入回退阶段，并尝试在一个随机时间段之后再次发送。冲突会导致网络缺乏效率，如图7-15所示。

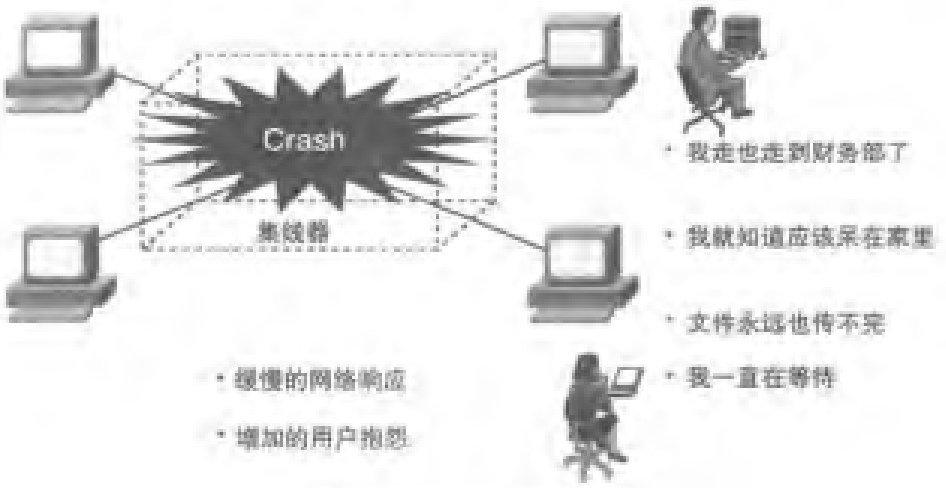


图7-15 交换机和冲突域

冲突域（collision domain）是帧在其中产生并发生碰撞的网络区域。所有的共享介质环境都是冲突域，如图7-16所示。

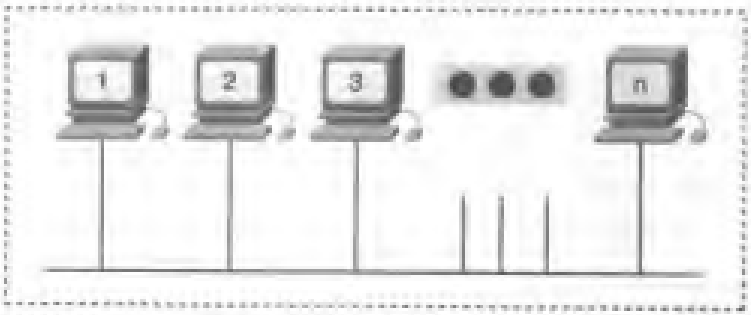


图7-16 基本的共享访问

当一台主机连接到交换机的一个端口时，交换机建立了一个专门的连接，这个连接被认为是一个单独的冲突域。举例来说，如果有一台12个端口的交换机，它的每一个端口都连接有一台设备，这样就创建了12个冲突域。

交换机通过学习连接到它的每个端口的主机的第2层MAC地址来建立一张交换表。当所连接的两台主机想彼此通信时，交换机查找交换表并在端口之间建立虚连接。称它为虚连接是因为该连接

只有在需要的时候才存在。当虚拟线路不再需要时，它将被断开。

这样可以依次创建微分段。微分段运行起来就好像网络中只有两台主机，其中一台是发送主机，另一台是接收主机。这样使得可用带宽得到最大的利用。

由于交换机给每个网段提供专门的带宽，因此，交换机减少了冲突并且增加了网段上的带宽。

7.5　交换机和广播域

网络中的通信以3种方式进行。最常用的方式是通过单播传输。在单播传输中，一个发送帧会尽可能地到达一个接收者。

另外一种通信方式是组播传输。在组播传输中，一个发送帧会尽可能地只到达整个网段里的一个子网或一个组。只有需要接收多播流量的站点才会参与组播组。图7-17显示了交换机和不同的广播域。

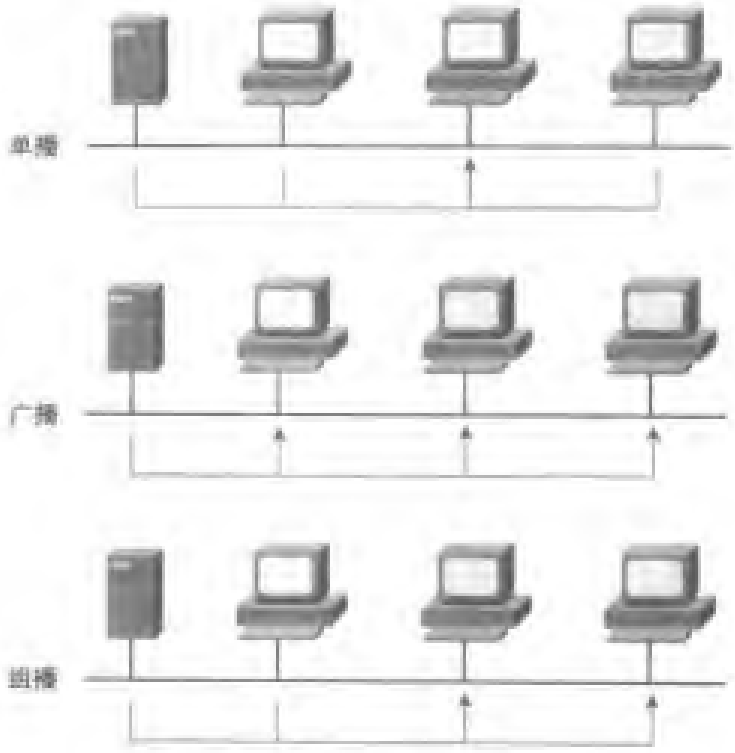


图7-17　交换机和广播域

最后一种通信方式是广播传输。在广播传输中，一个发送帧会到达网络上的所有接收者。在网段上的每台主机都会接收到广播帧，如图7-17所示。

当一台设备想发送第2层的广播时，帧的目的MAC地址设置为最高的可能值——也就是FF:FF:FF:FF:FF:FF。把这个值设为目的MAC地址，保证了所有的设备都会接收并处理广播帧。

第2层的广播域指的是MAC广播域。MAC广播域由LAN中的所有设备组成，这些设备能够接收从一台主机发送给LAN中所有其他设备的广播帧。

交换机是第2层设备，当它接收到一个广播时，它把该广播转发到除广播进入端口之外的所有端口。每台连接交换机的设备都必须处理广播帧。当把可用带宽用于广播时，会降低网络的效率，如图7-18所示。

当两台交换机相连时，广播域的大小会增加。在这个实例中，广播帧被转发到交换机1上的所有已连接的端口中。如果交换机1连接到交换机2，则帧也会广播到连接在交换机2上的所有设备，如图7-19所示。

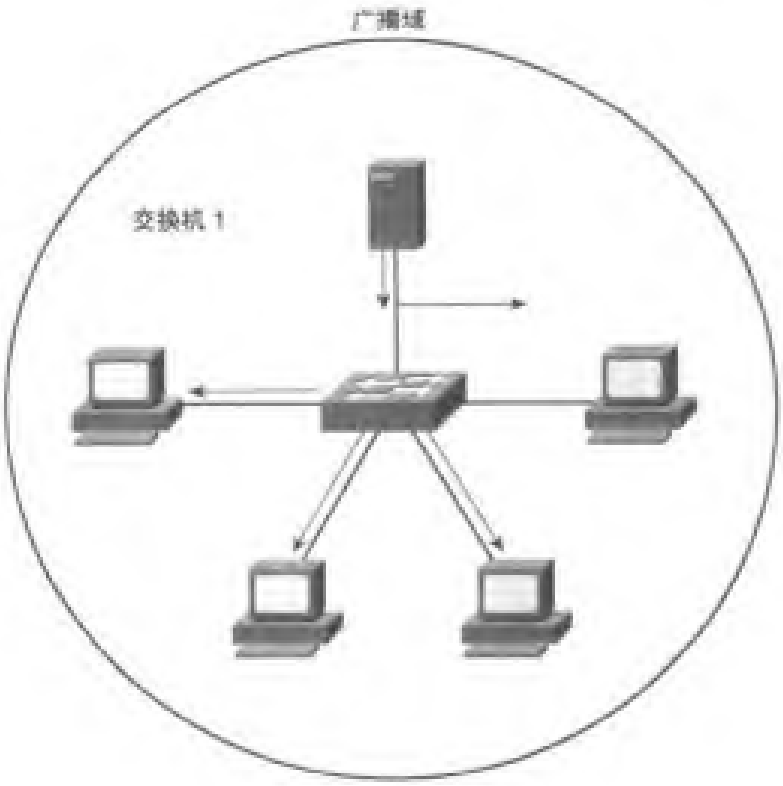


图7-18 单一的广播域

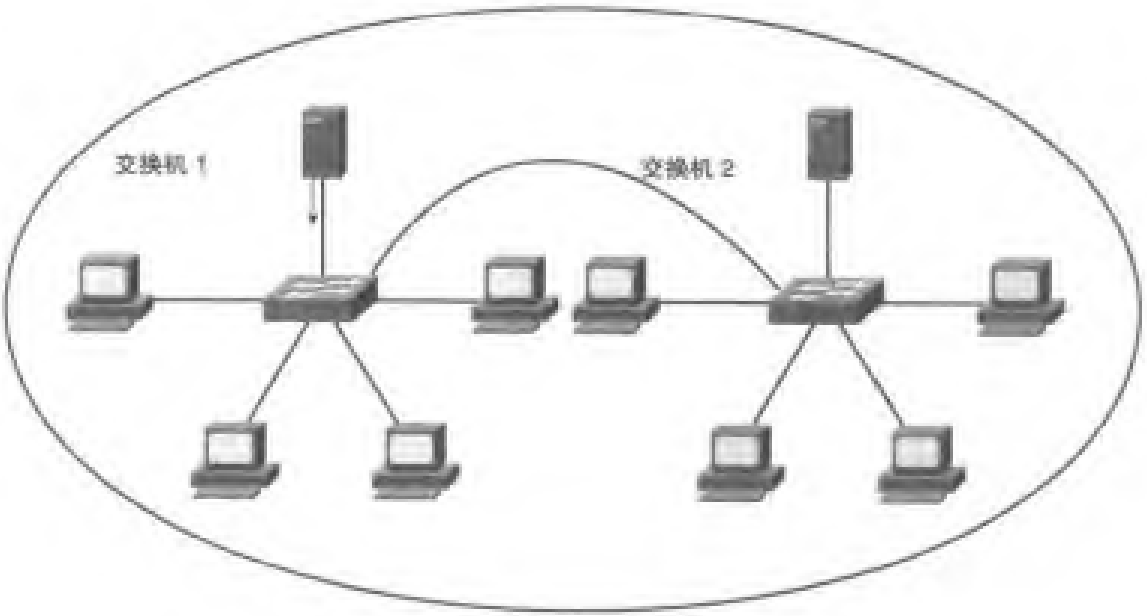


图7-19 多部交换机广播域

因为在广播域中的所有设备都必须接收并处理广播帧，所以广播的全部结果是可用带宽的减少。

路由器是第3层的设备，它不传递广播。因此，它们通常用来分隔冲突域和广播域。

7.6 交换机与PC之间的通信

交换机是第2层设备，它可以智能地学习到连接在交换机端口的所有设备的MAC地址，并把该

信息添加到转发表中。地址信息添加完成以后，交换机读取从某个端口进入的数据帧的目的MAC地址，然后查找它的转发表，找到与目的MAC地址相匹配的出口后把数据帧转发出去。

7.6.1　PC到交换机的传输

当一台PC连接到LAN时，它并不关心连接到LAN传输介质的其他设备，它只是把数据帧从网络接口卡传送到网络介质上。

PC可以通过交叉线连接到另外一台计算机上，也可以通过直通线连接到其他网络设备，例如集线器、交换机或路由器。

注意：连接工作站与交换机时，必需使用直通线（straight-through cable）。

7.6.2　交换机之间的通信

MAC地址为A的主机A发送数据到MAC地址为B的主机B，该数据帧从端口1进入交换机A。交换机A读取进入的数据帧的目的MAC地址，并查找它的转发表。交换机A识别出主机B的MAC地址映射到端口2，于是它把此数据帧交换到该出口。

注意：连接两个交换机时，必须使用交叉线（cross-overcable）。

转发表中允许多个MAC地址映射到一个特定端口。当一台连接着多台工作站的集线器连接到交换机的某个端口或者多台交换机互连时，这种情况非常普遍。

当需要穿过两台交换机进行传输时，会发生与前面传输类似的处理过程。考虑下面这种情况，主机A需要传输数据帧到MAC地址为F的主机F。

首先，主机A把帧发送到交换机A的端口1，但交换机A在它的转发表里面找不到目的主机F的MAC地址。于是，交换机A把该帧向除端口1之外的所有端口扩散。

连接在交换机A上的主机B和主机C接收到该数据帧后，检查该帧的目的MAC地址。由于发现目的MAC地址不是它们自己的MAC地址，于是它们忽略该数据帧。另外，由于泛洪作用，数据帧也被转发到与交换机A相连的交换机B的端口2。交换机B查找它的转发表，并识别出目的MAC地址已映射到端口4。于是，交换机B把数据帧从端口4发送到MAC地址为F的主机F上。

当主机F对主机A进行回复时，需要经过一个相反的处理过程。这时，交换机A就可以把主机F映射到端口4来更新它的转发表，交换机B则把主机A映射到端口2来更新它的转发表。

最终，交换机A将学习到主机D、E、F的MAC地址，并把它们都映射到端口4；交换机B将学习到主机A、B、C的MAC地址，并把它们都映射到端口2。

7.7　检验Catalyst交换机的初始配置

新的交换机会有预先设置好的配置，该配置使用厂家设定的缺省值，但这些设置难以达到网络管理员的要求。我们可以通过命令行界面来配置和管理交换机，越来越多的连网设备也可以通过使用基于Web的界面和浏览器来进行配置与管理。

为了有效地管理含有交换机的网络，网络管理员必须熟悉许多管理任务。这些任务中，一些任务与维护交换机以及它的网络操作系统（IOS）有关，而另外一些任务则是为了获得最优的、稳定的和安全的操作而管理交换机的接口和各种表。

有些时候，用户会忘记密码，此时管理员需要执行密码恢复操作以访问交换机。基本的交换机配置、升级IOS以及密码恢复都是网络管理员必须具备的技能。

7.7.1 检验Catalyst交换机的缺省配置

交换机首次加电启动时，在它的运行配置文件中有缺省的配置数据。交换机的缺省名称为Switch，控制台或虚拟终端（vty）线路都没有设置密码。在例7-1中，对于诸如Cisco 2900系列的基于IOS命令的交换机，可以用show run命令来显示交换机的缺省配置。

例7-1 缺省交换机配置

```
Switch#show run
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!

!
ip subnet zero
!

!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
<OUTPUT OMITTED>
!
line con 0
 transport input none
 stopbits 1
line vty 5 15
!
end
```

7.7.2　交换机端口属性

使用show interface命令可以看到接口的属性，要记得区分插槽号（slot number）和端口号（port number）（如对于0/1，插槽号为0，端口号为1）。缺省情况下，交换机的端口（接口）设置为自动模式（auto mode），如例7-2所示。也就是说，它们会自动探测半双工或全双工操作模式以及端口的速率，如10Mbit/s或100Mbit/s。

例7-2　缺省接口属性

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down
Hardware is Fast Ethernet, address is 0008.e32e.e601 (bia 0008.e32e.e601)
MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Auto-duplex, Auto Speed, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:31:54, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1 packets input, 64 bytes
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast
0 input packets with dribble condition detected
5 packets output, 495 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
```

7.7.3　VLAN属性

交换机的所有端口都属于VLAN 1；VLAN 1作为缺省管理VLAN（management VLAN）。使用show vlan命令可以显示交换机中所定义的VLAN的相关信息。例7-3显示了VLAN 1的缺省属性，注意：交换机的12个端口全都属于VLAN 1。缺省情况下，所有端口初始化时都属于VLAN1。

例7-3　VLAN1缺省属性

```
Switch#show vlan
VLAN Name Status Ports
----------------------------------------------------------------------
```

```
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4,
Fa0/5, Fa0/6, Fa0/7, Fa0/8,
Fa0/9, Fa0/10, Fa0/11, Fa0/12
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1 enet 100001 1500 - - - - - 1002 1003
1002 fddi 101002 1500 - - - - - 1 1003
1003 tr 101003 1500 1005 0 - - srb 1 1002
1004 fdnet 101004 1500 - - 1 ibm - 0 0
1005 trnet 101005 1500 - - 1 ibm - 0 0
```

7.7.4 闪存目录

由于新交换机还没有配置过，它的闪存目录（flash directory）里没有包含任何VLAN数据库文件（vlan.dat），也没有保存的配置文件（config.text）。其中，vlan.dat文件用来储存本地VLAN的信息，交换机使用该文件与其他交换机共享VLAN的信息。缺省情况下，闪存目录里有一个包含IOS映像的文件（以.bin结尾）、一个称为env_vars的文件以及一个称为html的子目录。使用dir flash：命令可以显示闪存目录的内容，如例7-4所示。

例7-4 缺省闪存目录

```
Switch#directory flash:
Directory of flash:/
2 -rwx 1674921 Apr 30 2001 15:09:51 c2950-c3h2s-mz.120-5.3.WC.1.bin
3 -rwx 269 Jan 01 1970 00:00:57 env_vars
4 drwx 10240 Apr 30 2001 15:09:52 html
7741440 bytes total (4780544 bytes free)
```

7.7.5 显示IOS版本信息

你可以用show version命令来验证IOS版本和配置寄存器的设置，如例7-5所示。交换机的其他信息也可以在该输出中看到，例如IOS系统映像文件名、交换机型号、序列号码、内存大小以及端口号码和类型。

例7-5 验证IOS版本和配置寄存器的设置

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-C3H2S-M), Version 12.0(5.3)WC(1),
MAINTENANCE INTERIM SOFTWARE
```

```
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:56 by devgoyal
Image text-base: 0x80010000, data-base: 0x8031A000
ROM: Bootstrap program is CALHOUN boot loader
Switch uptime is 1 hour, 24 minutes
System returned to ROM by power-on
System image file is "flash:c2950-c3h2s-mz.120-5.3.WC.1.bin"
cisco WS-C2950-12 (RC32300) processor (revision B0) with 22260K bytes of memory.
Processor board ID FOC0605W0RH
Last reset from system-reset

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:08:83:26:E6:00
Motherboard assembly number: 73-5782-08
Power supply part number: 34-0965-01
Motherboard serial number: FOC060502HP
Power supply serial number: PHI05500C5D
Model revision number: B0
Motherboard revision number: B0
Model number: WS-C2950-12
System serial number: FOC0605W0RH
Configuration register is 0xF
```

7.7.6　使用缺省配置的好处

在缺省状态下，交换机只有一个广播域，它可以通过控制台端口使用命令行界面来进行管理或配置，生成树协议也被启用。由于没有为交换机分配IP地址，这也就提供了额外的安全措施。

对于小型网络，缺省配置已经足够了。利用交换机对局域网进行微分段，就可以立即获得更好的网络性能。



实验活动　查看交换机的缺省配置

在本实验中，你将查看29xx系列交换机的设置。通过将超级终端连接到交换机的控制台端口，使用不同的show命令以收集交换机当前的配置信息。

7.8　Catalyst交换机的网络设置

对于一台已配置好的交换机，只要求提供密码就可以访问用户EXEC、ENABLE或者特权EXEC模式。交换机的配置模式从特权EXEC模式进入。在命令行界面，缺省的特权EXEC模式提示符为Switch#；在用户EXEC模式，提示符为Switch>。

7.8.1 恢复交换机的缺省配置

如例7-6所示，为了确保新的配置完全覆盖当前存在的配置，需要进行以下的操作：

• 通过删除闪存目录中的VLAN数据库文件vlan.dat来删除现有的VLAN信息。

• 删除配置备份文件startup-config（该例子显示了如何在catalyst2950和1900交换机上执行这个操作）。

• 重启交换机。

例7-6 在2950和1900系列交换机上恢复缺省配置

```
Catalyst 2950
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat?[confirm]
Switch#erase startup-config

<output omitted>
Switch#reload

Catalyst 1900
Switch#delete nvram
```

7.8.2 指定交换机的主机名和密码

安全性、文档和管理对于每一台互连网络设备都是非常重要的。

每台交换机都应该配置一个主机名，都应该在控制台和虚拟终端线路上设置密码，如例7-7所示。

例7-7 设置交换机主机名和密码保护的线路

```
Switch(config)#hostname ALSwitch
ALSwitch(config)#line configuration 0
ALSwitch(config-line)#password
ALSwitch(config-line)#login
ALSWitch(config-line)#line vty 0 4
ALSwitch(config-line)#password
ALSwitch(config-line)#login
```

7.8.3 指定交换机的IP地址和缺省网关

为了使交换机能被Telnet和其他TCP/IP应用所访问，你需要给交换机设置IP地址和缺省网关，例7-8显示了如何为Catalyst2 950和1 900交换机进行这些设置。缺省情况下，VLAN 1是管理VLAN。在基于交换的网络中，所有网络设备都应该属于同一个管理VLAN。这样，仅用一台管理工作站就可以访问、配置和管理所有网络设备。

例7-8 设置交换机的IP地址和缺省网关

```
Catalyst 2950
ALSwitch(config)#interface VLAN1
```

```
ALSwitch(config-if)#ip address 192.168.1.2 255.255.255.0

ALSwitch(config)#ip default-gateway 192.168.1.1

Catalyst 1900
ALSwitch(config)#ip address 192.168.1.2 255.255.255.0
ALSwitch(config)#ip default-gateway 192.168.1.1
```

7.8.4 设置端口属性

交换机快速以太网端口缺省设置为自动速度（auto-speed）和自动双工模式（auto-duplex），这样使得接口可以协商这些设置。当网络管理员需要保证某个接口使用特定的速度和双工模式（半双工或者全双工）时，这些值可以手动设置，如例7-9所示。

例7-9 设置端口速度和双工模式

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#duplex full
Switch(config-if)#
00:34:01: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
00:34:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down
00:34:03: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
00:34:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
Switch(config-if)#speed 100
Switch(config-if)#
00:34:24: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
00:34:25: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down
00:34:27: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
00:34:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
```

另外一个有用的端口设置选项是postfast。

如果交换机的某个端口连接的仅仅是终端用户工作站（并非连接到其他交换机或者网桥），你就应该在这些终端用户端口上启用称为快速端口的Catalyst交换机特性。使用快速端口后，当端口首次启动时，它会自动从阻塞状态变为转发状态。对于在启动时就需要连接并登录Netware服务器的Netware客户而言，设置快速端口非常有用。例7-10显示了如何设置快速端口，在Fast-Start栏中显示了快速端口的状态：

例7-10 如何在端口上启用快速端口并验证配置

```
Switch> set spantree portfast 4/1 enable
Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, etc. to
a fast start port can cause temporary spanning tree loops. Use with caution.
```

```
Spantree port 4/1 fast start enabled.
Switch># show spantree 4/1
Port Vlan Port-State    Cost Priority Fast-Start Group-method
---- ---- ----------    ---- -------- ---------- ------------ --------
4/1  1    blocking      19   20       enabled
4/1  100  forwarding    10   20       enabled
4/1  521  blocking      19   20       enabled
4/1  522  blocking      19   20       enabled
4/1  523  blocking      19   20       enabled
4/1  524  blocking      19   20       enabled
4/1  1003 not-connected 19   20       enabled
4/1  1005 not-connected 19   4        enabled
Switch>#
```

7.8.5 基于Web的界面

智能网络设备可以提供基于Web的界面，以实现配置与管理。在交换机配置了IP地址和网关之后，你就可以用这种方法访问它。网络浏览器可以设置为该IP地址和端口（缺省为80）以获取Web服务。你可以启动或者关闭http服务功能，也可以选择该服务的端口地址，如例7-11所示。

例7-11 启动HTTP服务和端口

```
Switch(config)#ip http ?
access-class   Restrict access by access-class
authentication Set http authentication method
path Set base  path for HTML
port HTTP port
server Enable HTTP server
Switch(config)#ip http server

Switch(config)#ip http port ?
<0-65535> HTTP port

Switch(config)#ip http port 80
Switch(config)#
```

任何附加软件（一个applet）都可以从交换机或其他网络设备上下载到浏览器中。这些设备由基于浏览器的图形用户界面（GUI）来管理。



实验活动 交换机基本配置

在本实验中，你将为交换机配置IP地址并确保对命令行界面访问的安全性。你还将配置交换机端口速度和双工属性，然后保存当前配置。另外，还要查看交换机的浏览器界面。

7.9 管理MAC地址表

交换机通过检查在端口上接收到的帧的源地址就可以学习到连接在该端口的PC或工作站的

MAC地址。然后，交换机把这些学到的MAC地址记录在MAC地址表中。如果帧的目的MAC地址已经记录在该表中，则该帧就能交换到正确的接口上。

为了检查交换机所学到的地址，可以输入特权EXEC命令，如例7-12所示。

例7-12 Show mac-address-table的输出

```
Switch#show mac-address-table
Dynamic Address Count: 2
Secure Address Count: 0
Static Address (User-defined) Count: 0
Syster Self Address Count: 13
Total MAC addresses: 15
Maximum MAC addresses: 8192
Non-static Address Table:
Destination Address Address Type VLAN Destination Port
---- ----------- -- ------------ ---- --------------------
0010.7a60.ad7e      Dynamic      1    FastEthernet0/2
00e0.2917.1884      Dynamic      1    FastEthernet0/5
```

通过在交换机上记录和维护数千条的MAC地址以及在每个端口上记录和维护多个地址，交换机能动态地学习地址。为了保持交换机的适当内存量和最佳操作，有时必须丢弃MAC地址表中一些已学习到的地址条目。为了做到这一点，当分组进入某个端口时，MAC地址表中的所有条目都会打上时间标记。机器可能会从它所相连的端口移走、关机或转移到同一交换机或不同交换机的另一端口上。另外，网络接口卡也可能已经被替换。因此，帧的转发有可能会发生混乱。基于这些原因，对于某条以前学到的地址，如果在300秒内没有再接收到该地址的帧，则该MAC地址条目就会自动地丢弃或者过期。

网络管理员也可以选择使用特权EXEC命令clear mac-address-table来清除这些动态条目，而不是仅仅等待动态条目过期，例7-13显示了clear mac-address-table命令的输出。由管理员所配置的MAC地址条目也可以这种方式删除。按这种方式来清除地址表可以确保立即删除不再有效的地址。

例7-13 Clear mac-address-table的输出

```
Switch#clear mac-address-table
Switch#show mac-address-table
Dynamic Address Count: 0
Secure Address Count: 0
Static Address (User-defined) Count: 0
System Self Address Count: 13
Total MAC addresses: 14
Maximum MAC addresses: 8192
Non-static Address Table:
Destination Address Address Type VLAN Destination Port
------------------- ---------  - -- - -- -----------------
```



实验活动 管理MAC地址表

在这个实验中，建立一个基本的交换机配置并管理交换机的MAC地址表。

7.9.1 配置静态MAC地址

人们可能会希望一个MAC地址永久性地分配给一个接口，交换机也不会自动地将该MAC地址过期。

因为一台特定的服务器或用户工作终端必须连接到交换机的某个端口，所以一个永久的地址可以分配给该接口，从而交换机可以静态地获得MAC地址。这还可以提高安全性。

为了设置交换机接口的静态MAC地址条目，在全局配置模式下使用如下的命令语法：

```
Switch(config)#mac-address-table static mac-address-of-host
Switch(config)#interface FastEthernet ethernet-number vlan vlan-name
```

为了把该条目删除掉，使用no形式的命令。

命令mac-address-table的输出如例7-14所示。

例7-14 配置静态MAC地址

```
Switch(config)#mac-address-table ?
aging-time Set MAC address table entry maximum age
secure Configure a secure address
static Configure a static 802.1d static address
Switch(config)#mac-address-table static 0010.7a60.1884 interface
FastEthernet0/5 vlan VLAN1

Remove Static MAC Address
Switch(config)#no mac-address-table static 0010.7a60.1884 interface
FastEthernet0/5 vlan VLAN1
```



实验活动 配置静态MAC地址

在本实验中，请在交换机端口上设置和删除静态MAC地址。

7.9.2 配置端口安全性

对网络管理员而言，确保互连网络的安全是一项重要的责任。通过办公室或房间里墙上的结构化布线的出口，你可以访问接入层的交换机端口，任何人都可以把PC或膝上型计算机插入到某一个出口上。因此，这是非授权用户访问网络的一个潜在入口。交换机提供了一种称为端口安全的特性。利用该特性，你可以限制能在该接口上学习到的地址的数量，还可以配置交换机在这些数量超过某个值时采取相应的行动，如例7-15所示。你可以静态地设置安全的MAC地址，不过这可能是一种容易出错的复杂的任务。

例7-15 配置端口安全

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#port security ?
action action to take for security violation
max-mac-count maximum mac address count
<cr>
Switch(config-if)#port security action ?
shutdown shut down the port from which security violation is detected
trap send snmp trap for security violation
```

一种替代方法是在交换机的接口上设置端口安全性。这时，交换机动态学习到的第一个地址就成为安全地址。

为去掉接口上的端口安全，使用no命令形式。

为验证端口的安全状态，输入命令show port security。

实验活动　配置端口安全属性

在本实验中，你将为Catalyst交换机上独立的快速以太网端口配置和管理端口安全性。

7.10　实施添加、迁移和改变

当你向网络添加一台新的交换机时，你要配置它的名称、管理VLAN的IP地址、缺省网关和密码。

添加新的交换机时，确保完成以下的任务：

- 配置交换机的名字。
- 出于管理的目的，确定并配置一个IP地址。
- 配置一个缺省的网关。
- 为控制台、辅助端口和虚拟终端（vty）接口配置管理性访问。
- 为该设备配置安全措施。
- 按照实际需求配置交换机的接入端口。

当把一台主机从交换机的某个端口迁移到另一个端口或者从某台交换机迁移到另一台交换机的某个端口时，你应该删除那些配置，以免产生意外的行为。然后，再把所需要的配置添加上去。

当添加、改变或迁移主机时，确保完成以下的任务：

- 添加MAC地址：
  ——配置端口安全。
  ——配置MAC地址。
- 改变MAC地址：
  ——删除MAC地址的限制。
- 迁移MAC地址：
  ——添加MAC地址。
  ——在该端口配置分配给新用户的MAC地址。
  ——删除端口原来的配置。

实验活动　添加、迁移和改变MAC地址

在本实验中，你把PC从交换机的某个端口迁移到另外一个端口上以及向该交换机添加一台新的PC。

7.11　管理交换机操作系统映像和设备配置文件

应该为连网设备的操作配置文件生成文档并进行维护。把最近的running-configuration文件的副本保存在某服务器上，或者保存在一张独立的磁盘上。这些都是必要的文档，在需要进行重新配置时，它们将会很有用。当你正在配置一台相似的交换机时，你也可以用这信息作为一个起点。

实验活动　管理交换机操作系统映像

在本实验中，你将把IOS映像备份到一台TFTP服务器，然后再把它恢复到交换机中。



实验活动 管理交换机启动配置文件

在这个实验中，把启动配置文件备份到一个TFTP服务器上，然后再把它恢复到交换机中。

7.12 恢复1900/2950的密码

任何交换机管理程序都要求确保在控制台和虚拟终端线路上设置了密码，enable密码和enable secret密码也都设置了。这些操作有助于保证只有授权的用户才能访问交换机的用户EXEC模式和特权EXEC模式。

有时候，你可以在物理级别上访问交换机，但是无法访问用户或特权的EXEC模式，原因在于你不知道或已经忘记了该密码。

这种情况下，你就要执行密码恢复步骤。



实验活动 Catalyst 29xx交换机的密码恢复步骤

在本实验中，你将至丢失密码后，重新获得对Catalyst 2900交换机的控制。

7.13 升级1900/2900固件的IOS

随着错漏的修补、新特性的引入和性能的增强，IOS和固件的映像都会周期性地发布。有了IOS的新版本，网络运行起来会更加安全或者操作起来效率更高。在这种情况下，你就应该升级IOS。

为了升级IOS，你需要从Cisco.com软件中心把新的映像文件下载到本地服务器上。

为了下载新的映像[w11]，以客户的用户名和密码登录到该网站。下载完映像后，就可以将它安装到交换机中。



实验活动 Catalyst 29xx交换机的固件升级

在本实验中，你将升级交换机的IOS和HTML文件。

7.14 总结

本章中，你学习了以下内容：

- 用交换机对网络进行分段的概念和优点。
- 交换机如何学习地址。
- 交换机转发帧的不同方式。
- Catalyst交换机的缺省设置。
- 如何设置IP地址和缺省网关使交换机可以连接并管理网络。
- 如何使用Web浏览器查看交换机设置。
- 如何设置接口的速度和双工操作。
- 如何检查和管理交换机的MAC地址表。
- 如何配置端口安全。
- 如何管理配置文件和IOS映像。
- 如何恢复交换机的密码。
- 如何升级交换机的IOS。

作为本章学习内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

7.15　关键术语

非对称交换（*asymmetric switching*）　为端口之间的交换连接提供不同带宽的一种交换方式，例如10Mbit/s和100Mbit/s端口之间的交换。

广播域（*broadcast domain*）　所有设备的集合，这些设备都能接收集合内任一设备发出的广播帧。因为路由器不转发广播帧，所以广播域一般由路由器设定边界。

内容可寻址存储器（*CAM*（*content-addressable memory*））　通过内容而不是通过地址进行访问的存储器。

冲突域（*collision domain*）　在以太网中，冲突域是指传播发生冲突的帧的网络区域。中继器和集线器都会传播冲突，而LAN交换机、网桥和路由器都不会传播冲突。

快速转发交换（*fast-forward switching*）　在交换机尚未收到整个分组之前实际上就开始交换的一种交换方式。

无碎片交换（*fragment-free switching*）　一种交换技术，它在转发之前先过滤掉冲突帧，这些帧大部分是错误的分组。

存储缓冲（*memory buffering*）　在转发之前首先将分组存储在存储器中的一种缓冲方法。

微分段（*microsegment*）　把网络分成更小的网段，其目的通常是为了增加网络设备的带宽总合。

存储转发交换（*store-and-forward switching*）　一种分组交换技术。在这种技术中，帧在转发到合适端口前要经过完整的处理。处理过程包括计算循环冗余校验（CRC）和检验目的地址。此外，这些帧必须暂时存储起来，直到有网络资源（例如一条没有使用的链路）可用时才转发它。

对称交换（*symmetric switching*）为端口之间的交换连接提供相同带宽的一种交换方式，例如全部10Mbit/s或全部100Mbit/s的端口之间的交换。

7.16 复习题

1. 微分段有哪些特点？选择所有正确的答案。
   A. 发送主机和接收主机之间有专线连接
   B. 交换机内部有多条流量路径
   C. 会增加冲突
   D. 为LAN创建了一个广播域
2. LAN交换机的特征是什么？
   A. 工作在第1层的多端口中继器
   B. 工作在第2层的多端口集线器
   C. 工作在第3层的多端口路由器
   D. 工作在第2层的多端口网桥
3. 对称交换为下面哪种情况进行了优化？
   A. 连接到交换机“快速”交换端口上的客户端-服务器间的网络流量
   B. 网络流量的平均分配
   C. 缺少存储缓冲区的交换机
   D. 链路之间负载均衡
4. 在____交换中，交换机检查目的地址后就立即开始转发帧，而在____交换中，交换机接收到完整的帧才转发？
   A. 存储转发；对称
   B. 贯穿式；存储转发
   C. 存储转发；贯穿式
   D. 存储缓冲；贯穿式
5. 无碎片交换和快速转发交换是哪种交换的两种形式？
   A. 存储转发
   B. 存储缓冲
   C. 贯穿式
   D. 对称
6. 工作站与交换机相连时，使用哪种电缆最合适？
   A. 直通
   B. 交叉
   C. 空调制解调器
   D. 标准电话线
7. 一台主机发送，一台主机接收，这是哪种通信方式的特征？
   A. 广播
   B. 单播
   C. 多播
   D. 以上都不是



第8章　生成树协议

目标

学习完本章后，你将能够：

- 描述冗余拓扑的目标。
- 定义生成树协议（STP）。
- 描述生成树端口状态和指定端口选举的步骤。
- 描述根网桥选举步骤。
- 描述路径成本。
- 设置STP计时器。
- 解释STP如何加快收敛。
- 描述快速生成树协议。

本章将介绍冗余拓扑及其在网络维护中的重要性。此外，本章还介绍了生成树协议（STP）和快速生成树协议（RSTP）的功能。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图，光盘上的素材是本章内容的补充能强化本章所介绍的概念。

8.1　冗余拓扑概述

网络中具有冗余是很重要的。冗余使网络具有容错能力，冗余拓扑可使网络不会因为单个链路、端口或连网设备的失效而瘫痪。但是，基于交换机和网桥的冗余拓扑，容易受到广播风暴、帧的反复重传和*介质访问控制（MAC）*数据库不稳定的影响。

8.1.1　什么是冗余

各公司和组织越来越依赖于计算机网络进行工作。访问文件服务器、数据库、因特网、企业内部网和企业外部网对于商业成功有着关键作用。如果网络瘫痪了，生产就会蒙受损失，顾客就会不满。

各公司都在寻找1天24小时，1周7天都能正常运行的计算机网络。达到100%正常运行是几乎不可能的，但是99.999%（即“5个9”）的可靠性则是一些组织设定的目标。这意味着平均每30年才有1天的故障时间，平均每4 000天才有1小时的故障时间，平均每年只有5.25min的故障时间。此外，

对许多企业（金融机构、医院、ISP等等）而言，如果发生这些故障，则会带来巨大的商业损失。许多其他中等可靠性的目标则是降低成本。

达到99.999%的可靠性的目标需要极端可靠的网络。网络的可靠性来源于可靠的设备和可以容忍故障和错误的网络设计。为了屏蔽故障，网络应当设计成能够快速收敛。

容错性通过冗余来实现。冗余指的是多于和大于一般情况和正常情况下所应该有的。冗余如何促进可靠性呢？我们可以用坐小汽车上班来类比。假设上班的惟一方法是坐小汽车，但如果小汽车出故障无法使用了，则除非修好汽车，否则就无法上班。

如果小汽车平均10天会有1天因故障无法使用，那么它有90%的利用率。每10天有9天可以上班。可靠性是90%。

另外买一辆小汽车会增添麻烦，毕竟，没有必要只是为了上班而买两辆小汽车。虽然其中一辆是没有必要的，但是第2辆小汽车会在第1辆小汽车出问题的时候可供使用。这样就增加了可靠性。

8.1.2　冗余拓扑

冗余拓扑（redundant topologies）的目标是消除由于单点故障而引起的网络中断。所有网络都需要冗余来加强可靠性。例如，公路网就是一个冗余拓扑。如果一条路需要封闭检修，则会有另外一条路到达目的地。

假设一个小镇和市中心之间被一条河隔开。如果河上只有一座桥，那么它就是到市中心的惟一路径，因此这个拓扑没有冗余。

如果桥被淹没了或者意外损坏了，就无法通过这座桥到达市中心。但是，如果在河上修建另外一座桥，则可以构成冗余拓扑。即使某一座桥无法使用了，小镇也不会和市中心分隔开来。

8.1.3　冗余交换拓扑

具有冗余路径和设备的网络会有更长的网络正常运行时间。冗余拓扑消除了单点故障，如图8-1表示。如果一条路径或者一台设备失效，冗余路径或冗余设备会接管已失效的路径或设备的任务。

在图8-1中，如果交换机A出现故障，通信仍旧会通过交换机B从网段2流向网段1，最终到达路由器链路。

如果交换机A的端口1失效，流量仍然可以通过交换机B的端口1进行传输。

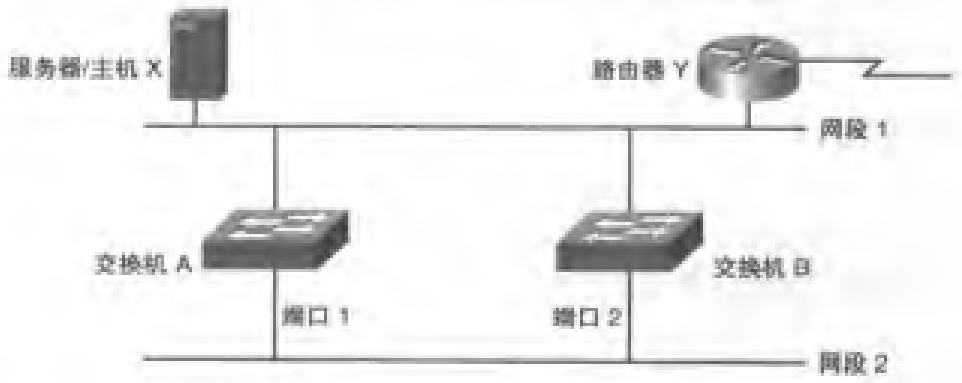


图8-1　冗余交换拓扑

交换机会学习连接到其端口的设备的*MAC*地址，以便数据能够正确转发到目的地。在交换机未获得设备的MAC地址之前，它会把未知目的地的帧泛洪（flood）出去。广播和多播也会被泛洪出去。

冗余交换拓扑（redundant-switched topologing）会导致广播风暴、帧的反复重传和MAC地址表不稳定的问题。

8.1.4 广播风暴

在交换式网络中，广播和多播都会带来潜在的问题。交换机把多播当作广播对待，它对广播和多播都会进行扩散，即把帧发送到除接收到该帧的端口之外的所有端口。

如图8-2所示，如果主机X发送一个广播，例如发送*地址解释协议（ARP）*来请求路由器的第2层地址，交换机A会向所有端口转发广播。因为交换机B与交换机A在同一个网段，所以它也会转发所有广播。交换机B会接收所有由交换机A发送的广播，而交换机A也会接收到所有由交换机B发送的广播。于是，交换机A认为这些广播是新的广播，再次转发它们；交换机B也是如此。

两台交换机都会这样持续不断地传播广播。这称为广播风暴（broadcast storm），它会不断持续下去，直到其中一台交换机从网络上断开为止。所有的交换机和设备都忙于处理这些广播通信，故用户的流量根本无法传送。因此，网络会瘫痪或者显得极慢。

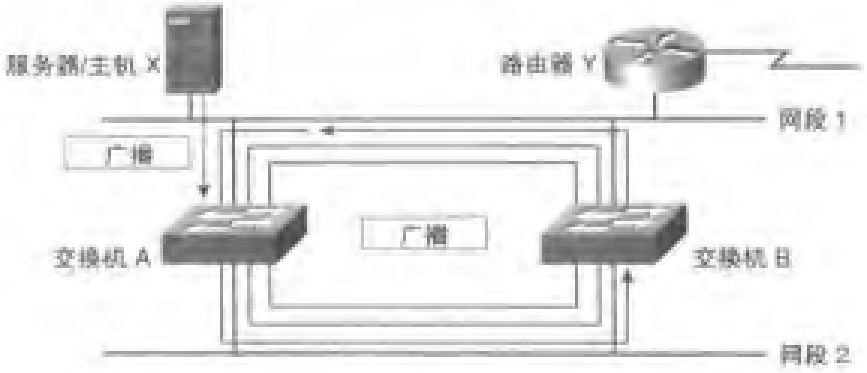


图8-2 广播风暴

8.1.5 帧的重复传送

在冗余交换网络中，一台终端设备可能会接收到同一帧的多个副本（如图8-3所示）。

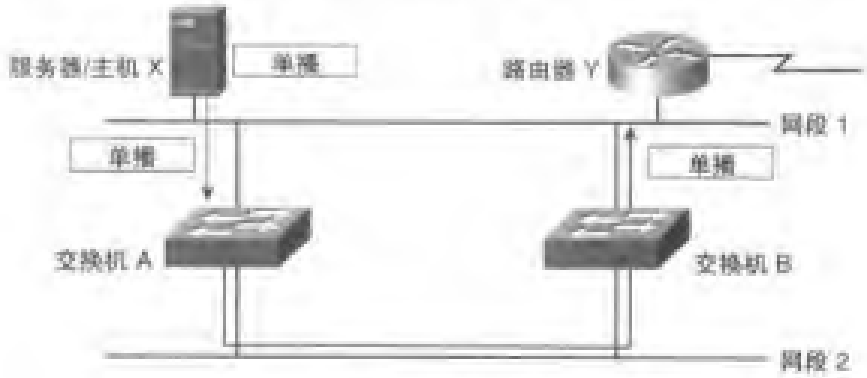


图8-3 帧的重复传送

大部分的协议都设计成忽略或者处理重复传送（duplicate transmissions）。一般来说，在这种情况下，使用序列编号机制的协议会假定许多传输帧已经失效，而且这些序号已经循环使用；其他一些协议则尝试把反复重传的帧留给适合的高层处理，但这可能会带来不可预测的结果。为了说明反复重传的帧是如何产生的，参考图8-3并考虑以下情况：

- 当主机X发送一个单播给路由器Y时，该帧的一个拷贝通过了直接相连的以太网（即网段1）被路由器Y所接收，同时也到达了交换机A。交换机A接收该帧并将其放到缓冲区里面。
- 交换机A检查帧的目的地址字段。如果发现在它的MAC地址表中并没有到达路由器Y的地址条目，则它会向除了接收到该帧的端口之外的所有其他端口泛洪该帧。

• 当交换机B接收到交换机A通过网段2传送过来的该帧的一个拷贝时，如果在它的MAC地址表中也没有路由器Y的地址条目，则交换机B也会向网段1转发该帧的一个拷贝。

• 路由器Y第二次接收到同一个帧的拷贝。

环路防止解决方案可以解决重复传送的问题，它通过逻辑断开环路和禁止这4个接口中的某一个在常规操作的时候发送帧来实现。

8.1.6　MAC数据库的不稳定性

在冗余交换网络中，交换机可能会学习到错误的信息。一台交换机可能会学到某个端口上的MAC地址，而事实上它并不在那个端口上。图8-4是一个MAC数据库不稳定的例子。

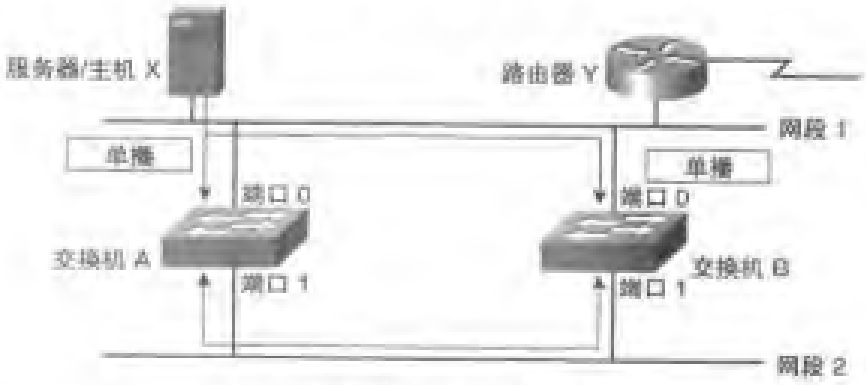


图8-4　MAC数据库的不稳定

在这个例子中，当第一帧到达的时候，交换机B建立了主机X与连接到网段1的端口0之间的MAC地址映射。一段时间之后，经过交换机A转发的该帧的一个拷贝到达交换机B的端口1，这时交换机B必须删除第一个映射，而建立主机X与连接到网段2的端口1之间的并不正确的MAC地址映射。

取决于交换机的内部架构，交换机或许能，也或许不能处理好MAC地址数据库的快速变化。在这个例子中，环路防止解决方案可以消除交换机无法处理好MAC数据库快速变化的问题，它通过在逻辑上断开环路以及禁止这4个接口中的某一个在常规操作中发送帧来实现。

8.2　生成树概述

*生成树协议（STP, Spanning Tree Protocol）*是一种第2层的链路管理协议，它用于维护一个无环路的网络。数字设备公司（DEC，Digital Equipment Corporation）最先提出STP。IEEE 802委员会随后修改了Digital公司的生成树算法，并且在IEEE 802.1d的规范中公布。Digital公司和802.1d的算法并不相同，也不兼容。Cisco的交换机，例如Catalyst 1900和2950，使用IEEE 802.1d 的STP。

STP的目的是为了维护一个无环路的网络拓扑。当交换机和网桥在拓扑中发现环路时，它们自动地在逻辑上阻塞一个或多个冗余端口，从而获得无环路的拓扑。

STP持续探测网络，以便在链路、交换机或网桥失效或增加时都可以获得响应。图8-5显示了一个例子。当网络拓扑改变时，运行STP的交换机和网桥自动重新配置它们的端口，以避免失去连接或者产生环路。

在基于交换机的互连网络中，物理层的环路会导致严重的问题。广播风暴、帧的重复传送以及MAC数据库的不稳定都会导致网络瘫痪。

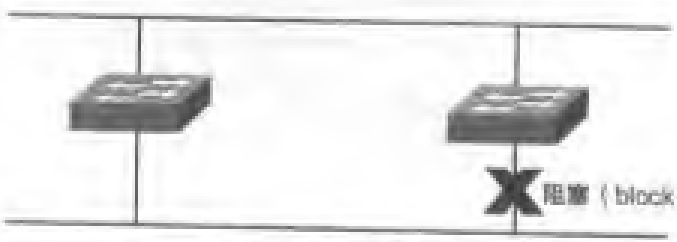


图8-5　生成树协议

交换网络具有较小的冲突域，微分段和全双工操作等优点。简单来说，它的优势在于性能方面。交换式网络使用STP在有环路的物理拓扑上建立无环路的逻辑拓扑。不属于活动的无环路拓扑的那一部分链路，端口和交换机并不真正参与数据帧的转发。

当活动拓扑的一部分发生故障时，必须重新建立一个新的无环路的拓扑。这时，需要尽可能快地重新计算新的无环路拓扑或者使新的无环路拓扑收敛，以便减少终端用户无法访问网络资源的时间。

802.1d标准定义的STP对于当今的新网络拓扑来说，其收敛太慢。一个新的标准——IEEE 802.1w，即RSTP——已经定义出来了，它用于突破现有的局限性。本章会讨论STP和RSTP。

8.2.1 生成树的运行

当网络稳定时，网络也已收敛，此时，每一个网络都有一棵生成树。因此，对于每一个交换网络，以下陈述都是正确的：

- 每个网络都有一个根网桥（root bridge）。
- 每个非根网桥都有一个根端口（root port）。
- 每个网段都有一个指定端口（designated port）。
- 不使用非指定端口（urdesignated port）。

根端口和指定端口用于转发（F, forwarding）数据流量；非指定端口将丢弃数据流量，它们也称为阻塞（B, blocking）端口或者丢弃（discarding）端口。网桥的根端口是最接近根网桥的端口，每个非根网桥都必须选出一个根端口。图8-6显示了生成树的操作。

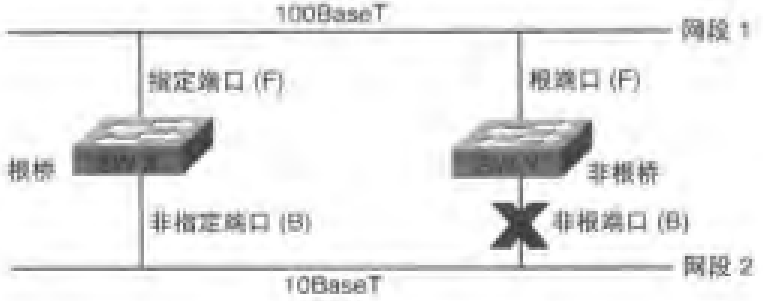


图8-6 生成树的运行

为使采用STP的网络最初收敛为一个逻辑上无环路的网络拓扑，可以通过以下3步实现：

1. **选举一个根网桥**。这个协议有一个选举根网桥的过程。在一个给定网络中，只有一台网桥可以作为根网桥。根网桥中的所有端口都是指定端口，指定端口通常处于转发状态。当端口处于转发状态时，它可以发送和接收流量。在这个例子中，交换机X被选举为根网桥。

2. **在非根网桥上选举根端口**。STP在每个非根网桥上建立一个根端口，这个根端口是从非根网桥到根网桥的最低成本路径。根端口一般处在转发状态。生成树的路径成本是从根网桥到该非根网桥路径上所有成本的一个累加值，这些成本是基于带宽计算出来的。在这个例子中，交换机Y到根网桥的最低成本路径是通过100BaseT快速以太网。

3. **为每个网段选举指定端口**。在每个网段上，STP都会建立一个指定端口。将网桥上到达根网桥有最低成本的端口选为指定端口。指定端口一般处于转发状态，为该网段转发流量。在这个例子中，两个网段的指定端口都在根网桥上，因为根网桥直接连接到这两个网段。交换机Y的10BaseT以太网端口是一个非指定端口，因为一个网段只能有一个指定端口。非指定端口一般处于阻塞状态，以便在逻辑上断开环路拓扑。当一个端口处于阻塞状态时，这个端口不转发流量，但是它仍旧接收到流量。

8.2.2　利用生成树构造无环路拓扑

冗余网络拓扑设计用来确保在出现单点故障的时候，网络仍旧能够继续工作。由于网络持续工作，用户的工作就不会轻易受到中断。所有因故障而引起的中断时间越短越好。

可靠性是通过冗余来增加的。基于交换机或网桥的网络通过在交换机之间或网桥之间引入冗余链路来克服单点故障，但是这些连接会在网络中引入物理上的环路，图8-7展示了一个例子。

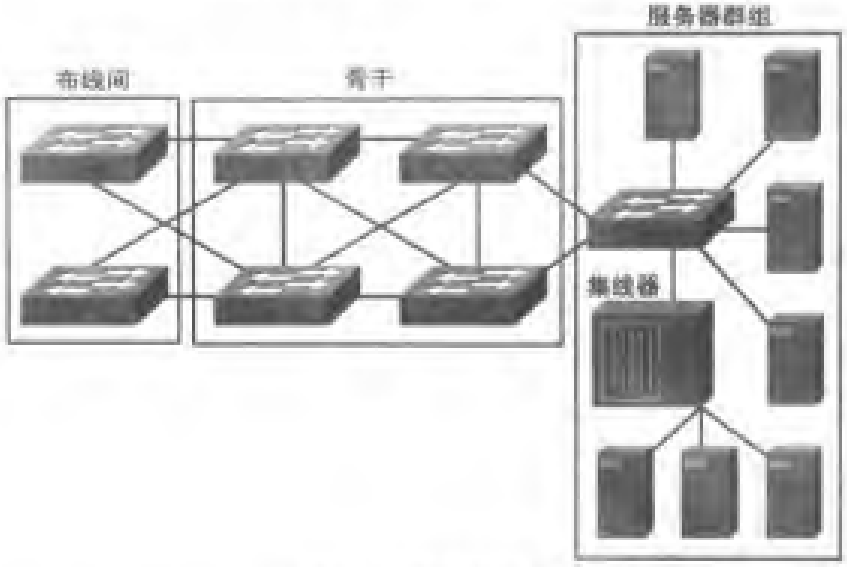


图8-7　桥接环路

创建桥接环路是为了在一旦一条链路出现故障时，另外一条可以接管转发流量的任务。

交换机工作在OSI模型的第2层，转发决定也发生在这一层。正是这一点决定了交换网络中不能存在环路。

当流量的目的地未知时，交换机会把该流量泛洪到所有端口。广播和组播的通信也会向除接收到该流量的端口以外的所有端口转发（泛洪）。因此这些流量会形成一个环。由于第2层的报头中没有*生存期（TTL, time to live）*，如果有帧发送到有第2层环路的交换机拓扑中，它会一直地循环转发下去，从而浪费了带宽，使得网络无法使用。

在第3层中才有TTL。随着TTL值的不断减小，直到为0的时候，分组就会被丢弃。然而，这样就出现了一个两难境地。为了获得可靠性，一个包含交换机或网桥环路的物理拓扑是必需的；但是，一个交换网络却又不允许有环路存在。这种两难境地的解决方法是：允许物理环路存在，但要建立无环路的逻辑拓扑。

构造的无环路逻辑拓扑称为树，它是星形或者扩展星形逻辑拓扑——网络的生成树。这样的拓扑是一棵生成树，因为网络中的所有设备都是可以访问或者可以间接访问的，但是任何两台设备之间都不存在环路。用于构造无环路拓扑的算法称为生成树算法，它可能需要相对较长的时间才能收敛。

8.3　STP的高级功能

STP建立了一个根节点，称为根网桥。并构建了一种拓扑，在这种拓扑中，网络中的每一个节点都只有一条路径可以到达。最终生成的树起源于根节点，不属于最短路径树的一部分的冗余链路会被阻塞。因为这样的路径被阻塞了，所以实现一个无环路的拓扑是有可能的。在阻塞链路上收到的数据帧将会被丢弃。

STP需要网络设备互相交换消息来检测桥接环路，交换机发送的用于构建无环路拓扑的消息称为*网桥协议数据单元（BPDU, bridge protocol data units）*。阻塞端口会不断收到BPDU，以保证当活动路径或设备发生故障的时候，仍然可以计算出一棵新的生成树。

BPDU包含足够的信息，因此所有交换机利用这些信息可以完成以下的工作：

- 选择一台单独的交换机作为生成树的根。
- 计算它自身到根交换机的最短路径。
- 对于每一个LAN网段，指定一台交换机作为最接近根的交换机，称它为指定交换机。指定交换机处理所有从LAN到根交换机的通信。
- 每个非根交换机选择自身的一个端口作为根端口，它是到根交换机路径最短的接口。
- 在每个网段上选择属于生成树一部分的端口作为指定端口。非指定端口将被阻塞掉。

生成树构造一个无环路拓扑时，它总是使用相同的4步来判定：

1. 最低的根*网桥ID（BID, bridge ID）*。
2. 到根网桥的最低路径成本。
3. 最低的发送网桥ID。
4. 最低的端口ID。

网桥使用这4步来保存各个端口中接收到的“最佳”的BPDU的一个副本。当网桥进行评估的时候，它考察该端口已经接收到的所有BPDU以及将要在该端口发送出去的BPDU。每个BPDU到达时，都会按照这个4步判决步骤来进行检查，看它是否比该端口已经保存的现有BPDU更优（即值更小）。如果新的BPDU（或者本地产生的BPDU）更优，就会替换旧的值。

此外，这个“保存最佳BPDU”的流程控制着BPDU的发送。当一个网桥开始变为活动时，它的每个端口都是每2s（使用缺省定时值时）发送一个BPDU。然而，如果一个端口收到另外一个网桥发送过来的BPDU，而这个BPDU比它正在发送的BPDU更优，则本地端口会停止发送BPDU。如果在一段时间（缺省为20s）后它不再接收到邻居的更优的BPDU，则本地端口会再次发送BPDU。

8.3.1 选择根网桥

在STP中，根网桥是具有最低BID的网桥。BID包括优先级和网桥MAC地址。

运行生成树算法的交换机和网桥利用BPDU定期（缺省是每2s）与其他交换机和网桥交换配置消息。包含在BPDU中的其中一个信息是BID。

STP要求每个网桥分配一个惟一的标识（BID）。BID通常由优先级（2 Bytes）和网桥MAC地址（6 Bytes）所构成。根据IEEE 802.1d的规定，缺省的优先级是32,768（二进制数为1000 0000 0000 0000，或者十六进制数0x8000），也就是中值。

在图8-8中，两台交换机都使用相同的缺省优先级，则具有更小的MAC地址的交换机会成为根网桥。在这个例子中，交换机X（SW X）是根网桥，它的网桥ID是0x8000（0c00.1111.1111）。

注意：根据交换机的型号，Cisco Catalyst交换机使用MAC地址池中的一个作为其MAC地址，该地址池分配给背板或管理模块。

图8-9所示的网桥ID由一个缺省为32 768的网桥优先级和交换机的基本MAC地址所组成。

当一台交换机最初启动时，它假定自己就是根交换机，并发送“次优”BPDU，它们的根和发送者BID信息字段中都包含有交换机的MAC地址。所有交换机都会接收到发送者的BID。当交换机收到一个更低的根BID时，它会把自己正在发送的BPDU的根BID替换为这个更低的根BID。所有的网桥都会接收到这些BPDU，并且判定具有最小BID值的网桥作为根网桥。

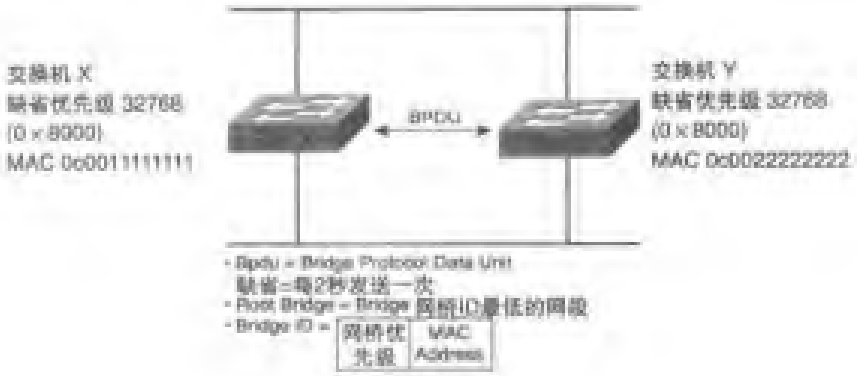


图8-8　根网桥选择

管理员可以通过把交换机的优先级设置为比缺省值更低的值来干预根交换机的选举，这样会使得网桥ID变小。

网络管理员可能希望干预根网桥的选举结果，这通常是在网络管理员非常清楚网络流量的时候才做的事情。

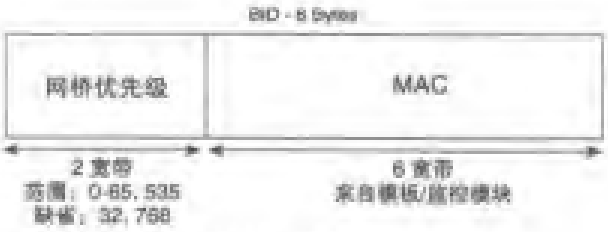


图8-9　网桥ID

实验活动　选举根网桥

在本实验中，将根据出厂缺省设置判断哪一台交换机将会选举为根网桥。然后强制使其他交换机选举为根交换机。

8.3.2　STP端口状态的转换过程

在一个启用了STP的网络中，所有网桥在启动之后都将经历阻塞状态以及侦听和学习这两种过渡状态。正确配置的端口最终会稳定在转发或者阻塞状态。处于转发状态的端口提供了到达根网桥的最低成本路径。当网桥识别出网络拓扑发生变化的时候，交换机端口会进入两种过渡状态。即当拓扑发生变化时，端口会暂时进入侦听状态和学习状态。图8-10显示了生成树的各种状态以及它们之间的转换。

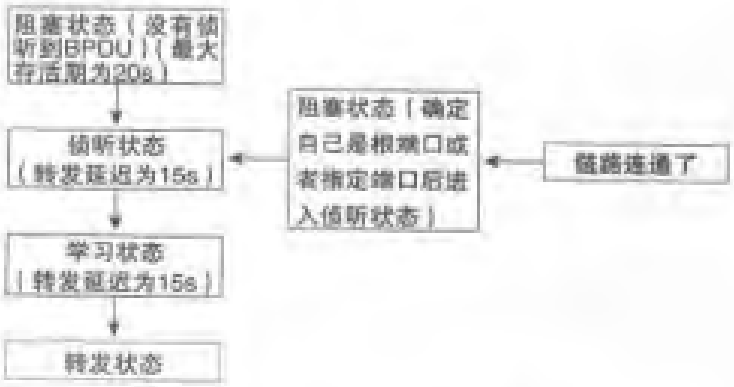


图8-10　生成树端口状态

一开始，所有网桥端口都处于阻塞状态以便侦听BPDU。网桥首次启动的时候，会认为自己是根网桥而转换到侦听状态。另外，如果在指定的时间（最大存活期）内没能收到新的BPDU，网桥

也会从阻塞状态转换到侦听状态。处于过渡性侦听状态的的端口可以发送或者接收BPDU来确定活动的网络拓扑。在侦听状态下，网桥将不传送用户数据。正是在这种状态下，网桥完成以下工作：选举根网桥、选举非根网桥上的根端口以及选举各网段上的指定端口。

15秒（转发延迟）之后，如果端口在选举完成后依然保持为指定端口或根端口，则它将转入学习状态，否则就转入阻塞状态。处于学习状态的端口可以用它侦听到的MAC地址来构成自己的MAC地址表，但它仍然不能转发用户的帧。缺省情况下，学习状态会持续15s（转发延迟）。在这一时期，网桥仍然不能传送用户数据。

STP各状态如下：

- **阻塞状态**（Blocking）——不转发数据帧；接收BPDU。
- **侦听状态**（Listening）——不转发数据帧；侦听数据帧。
- **学习状态**（Learning）——不转发数据帧；学习地址。
- **转发状态**（Forwarding）——转发数据帧；学习地址。
- **禁止状态**（Disabled）——不转发数据帧；不接收BPDU。

学习状态减少了数据转发开始时需要进行泛洪的数量。学习状态结束时，那些依然是指定端口或者根端口的端口将进入转发状态，其他的端口则回退到阻塞状态。处于转发状态的端口可以发送或者接收用户数据。

端口由阻塞状态转换到转发状态通常需要30到50s。这个时间也可以通过配置生成树计时器来调整。一般情况下，计时器值应该设置为缺省值，因为缺省值能给予网络充分的时间来收集所有关于网络拓扑的正确信息。

端口由侦听状态转换到学习状态，或者由学习状态转换到转发状态所需要的时间称为转发延迟，其缺省值为15s。在丢弃BPDU之前，网桥用来存储BPDU的时间称为最大存活期，其缺省值为20s。处于阻塞状态的端口如果在最大存活期内没能收到新的BPDU，它将从阻塞状态转换到侦听状态。

如果交换机端口仅仅是与用户终端连接（没有与其他交换机或者网桥相连），则可以在这些端口启用Catalyst系列交换机的***快速端口（portfast）***特性。启用快速端口后，当该端口首次启动的时候，它就自动从阻塞状态进入转发状态。由于这类端口没有与其他交换机或者网桥相连，因此在这类端口上不会形成环路，所以这种做法是可行的。图8-11是显示网络端口状态的实例。

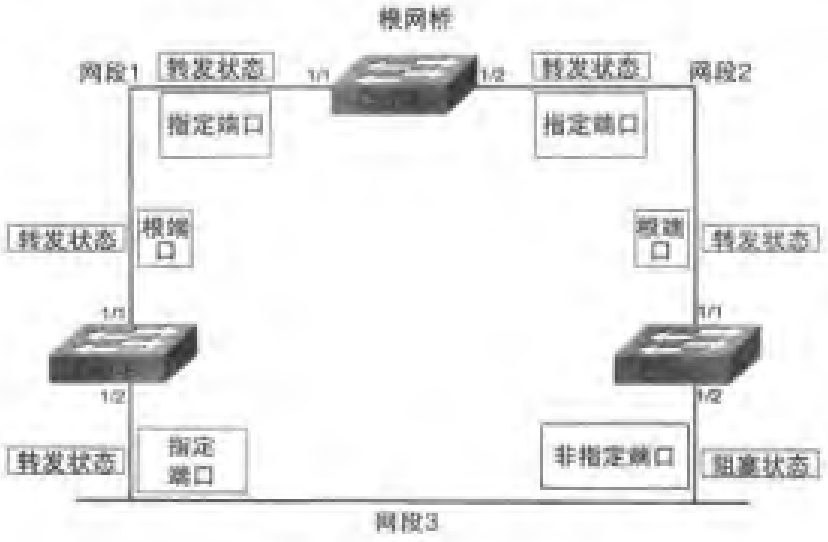


图8-11 网络端口状态实例

8.3.3　选举指定端口

桥接网络中的每个网段都有一个***指定端口***（designated port）。该端口起到单独的桥接端口的作用，也就是负责发送和接收在该网段和根网桥之间流量。这样设置的原因是：如果只用一个端口来处理每一个连接的流量的话，所有的环路都可以打破。包含某一网段指定端口的网桥称为该网段的***指定网桥***（designated bridge）。

在选出根网桥之后，交换机继续下一步工作——选举根端口。网桥上最接近根网桥的端口就是根端口。所有非根网桥都要选出一个根端口。

网桥使用“成本”这个概念作为距离的量度。具体来说，网桥会追踪计算根路径成本，根路径成本就是到根网桥的所有链路的累积成本。图8-12显示了如何选举根端口的一个实例，阐明了在几个网桥之间和根端口选举过程中成本值是如何计算的。

由Cat-A（根网桥）发送的BPDU包含有值为0的根路径成本（步骤1）。当Cat-B接收到这些BPDU的时候，会在BPDU中的根路径成本上增加端口1/1的路径成本。假定该网络是快速以太网，当Cat-B收到成本值为0的根路径，则它加上端口1/1的成本值19（步骤2）。然后Cat-B使用19为内部成本值并以此作为BPDU中的根路径成本值从端口1/2发送出去（步骤3）。

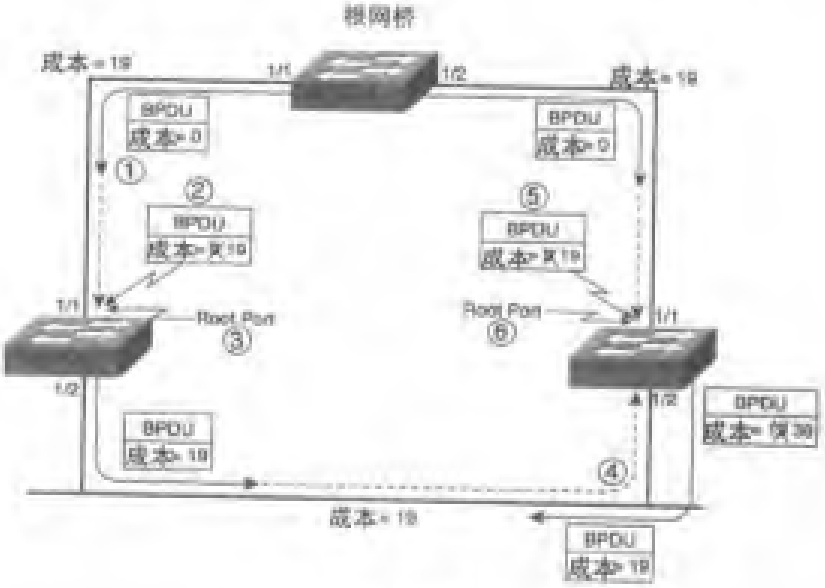


图8-12　选举根端口

Cat-C从Cat-B那里接收到这些BPDU（步骤4），把根路径成本增加为38（19+19）。然而，Cat-C也从端口1/1那里接收到来自根网桥的BPDU。这些BPDU从Cat-C的端口1/1进来的时候成本值为0，然后Cat-C将其增加至19（步骤5）。这个时候，Cat-C要作出一个决定：它必须从中选出一个根端口——距离根网桥最近的端口。Cat-C观察到在端口1/1上的根路径成本是19，而端口1/2上的是38。于是，Cat-C的端口1/1成为根端口（步骤6）。然后Cat-C开始向下游的交换机通告这个值为19的根路径成本（步骤7）。

尽管在图8-12中没有对Cat-B的根端口选举过程进行详细的说明，但它的过程跟Cat-C是相似的，也要经过一系列的计算。Cat-B的端口1/1到达根网桥的成本值是19，而端口1/2的成本计算值是38。所以，端口1/1成为Cat-B的根端口。注意成本值是在接收到BPDU的端口上进行累加计算的。

记住STP成本是在接收BPDU，而不是在发送BPDU的端口上进行累加的。例如，Cat-B在端口1/1接收到成本值为0的BPDU，然后是“在Cat-B内”把成本值增加为19。

在初始化STP收敛的第3步——选举指定端口的过程中，体现出STP防止环路形成的作用。桥接

网络中的每个网段都有一个指定端口。该端口起到了单独的桥接端口的作用，也就是负责发送和接收在该网段和根网桥之间的流量。这样设置的原因是：如果只用一个端口来处理每个连接的流量的话，所有的环路都可以打破，包含某一网段的指定端口的网桥称为该网段的*指定网桥*。

选举根端口的同时，基于到根网桥的根路径成本的累计值的指定端口选择过程也在进行，如图8-13所示。在图8-13中，显示了依次考察各个网段并确定该网段指定端口的过程。首先考察网段1，即Cat-A和Cat-B之间的链路。在该网段上有两个端口：Cat-A的端口1/1和Cat-B的端口1/1。Cat-A的端口1/1的根路径成本值为0（因为Cat-A是根网桥），而Cat-B的端口1/1的根路径成本值为19（从Cat-A那里接收到的BPDU的成本值0加上分配给Cat-B端口1/1的路径成本值19）。因为Cat-A的端口1/1的根路径成本更低，所以它成为这条链路的指定端口。

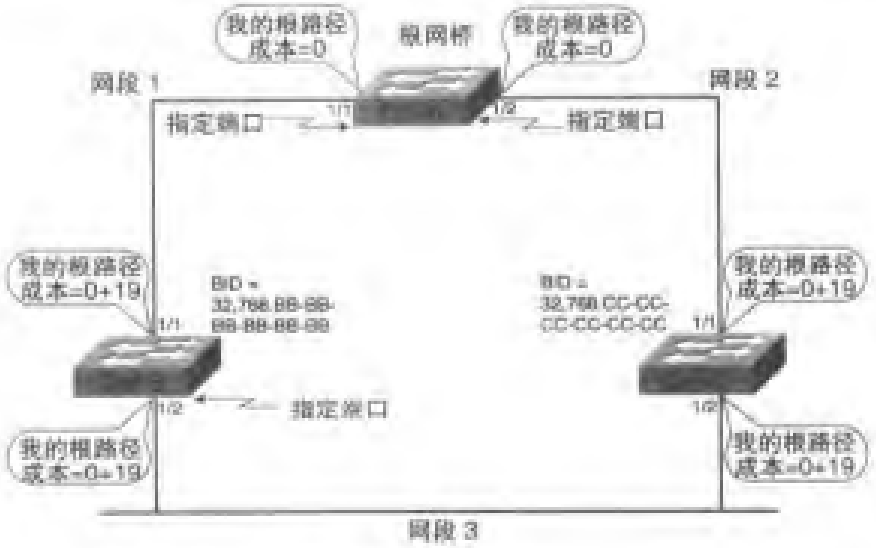


图8-13 选举指定端口

对于网段2（Cat-A和Cat-C之间的链路），也要经历相似的选举过程。Cat-A的端口1/2的根路径成本为值0，而Cat-C的端口1/1的根路径成本值为19。Cat-A的端口1/2的根路径成本更低，于是它成为指定端口。注意根网桥的所有活动端口都成为了指定端口。这条规则的惟一例外是当根网桥自身存在第1层物理环路的情况。例如，根网桥的两个端口连接到了同一台集线器上，或者两个端口通过交叉线连接到了一起。

现在来考察网段3（Cat-B和Cat-C之间的链路）：Cat-B 的端口1/2和Cat-C的端口1/2的根路径成本值都是19。这是一个“平局（tie）”。当STP遇到这种平局（或者其他需要作出判决的情况）时，通常都会用前面“生成树协议”一节中所提到的4步判决步骤来处理。下面是判决的4个步骤：

- 最低根BID。
- 到根网桥的最低路径成本。
- 最低发送BID。
- 最低端口ID。

在图8-13的例子中，3台网桥都承认Cat-A是根网桥，然后再往下对根路径开销进行估计。然而，如在前面的段落中所指出的，Cat-B和Cat-C的成本值都是19。这样就使得第3条判断准则——BID准则成为决定性的因素。因为Cat-B的BID（32,768.BB-BB-BBBB-BB-BB）比Cat-C的BID（32,768.CC-CC-CC-CC-CC-CC）小，所以Cat-B的端口1/2成为网段3的指定端口，Cat-C的端口1/2也就成为非指定端口。

8.3.4　路径成本

生成树路径成本（path cost）是路径上所有链路的带宽的总路径成本累积值。表8-1列出了IEEE 802.1D规定的各种不同网络技术（例如令牌环、以太网和SONET）中的路径成本缺省值。网桥用成本这个概念来对网桥间的距离进行度量。802.1D标准起初是用1000Mbit/s除以链路的带宽（Mbit/s）来定义成本，但随着10吉比特以太网的出现，这条规定就不再适用。表8-2列出了用于各类以太网技术的以前定义的和现在定义的链路成本值。

表8-1　不同连网技术的路径成本

带宽	STP成本
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
45 Mbit/s	39
100 Mbit/s	19
155 Mbit/s	14
622 Mbit/s	6
1 Gbit/s	4
10 Gbit/s	2

表8-2　以太网链路成本的修订

链路速率	成本（修正后的IEEE规定）	成本（以前的IEEE规定）
10 Gbit/s	2	1
1 Gbit/s	4	1
100 Mbit/s	19	10
10 Mbit/s	100	100

从表中你可以看到网桥是如何利用链路成本来估计自己到其他网桥的距离的。例如，10 Bast-T链路的成本是100（1 000/10），快速以太网和光纤分布数据接口（FDDI）的是10（1 000/100）。从1983年Radia Perlman开始使用STP后，这种机制一直工作得很好。然而，随着吉比特以太网和OC-48 ATM（2.4 Gbit/s）的应用，问题也出现了：成本值只以整数的形式储存，不承认小数为合法数据。例如，OC-48 ATM的开销值是1 000 Mbit/s / 2 400 Mbit/s = 0.41 667。0.41 667是非法数据，这就意味着它跟其他1 Gbit/s或者更高带宽的网络技术一起时，成本值才近似为1。因此，一个选择办法是把等于或大于1Gbit/s的链路的路径成本值都设为1。但是这样一来，在吉比特的网络中，STP就不能准确地选出“最佳路径”了。为了解决这个问题，IEEE决定用非线性尺度来修改成本。

8.3.5　STP计时器

Hello时间控制了发送配置BPDU的时间间隔，802.1D标准规定其缺省值为2s。这个值实际上只控制配置BPDU在根网桥上生成的时间，其他网桥则把它们从根网桥收到的BPDU向外通告。换言之，如果在2~20秒内由于网络故障而没有收到新的BPDU，非根网桥在这段时间内就停止发送周期BPDU。如果这种情况持续超过20s，也就是超过缺省的最大存活期，非根网桥就使原来储存的BPDU无效，并开始寻找新的根端口。所谓最大存活期，就是网桥在丢弃BPDU之前用来备份储存它的时间。

转发延迟是网桥在侦听状态和学习状态所花费的时间。只用转发延迟这一个值就控制了侦听和学习这两种状态，它的缺省值为15s。这个值是在假定网络的最大规模为7段网桥跳数、BPDU的最大丢失个数为3以及Hello时间间隔为2s的情况下得到的。这个转发延迟计时器同样可以用来控制网桥表在网络拓扑发生改变后的生存时间。

前面已经提到，每个端口都会把最佳的BPDU做一个备份。只要网桥每两秒不断地收到新的

BPDU，它就会不断地对这些BPDU做备份。但是，如果发送这个最佳BPDU的网桥失效了，就必须有某种机制来保证有其他网桥来接管。表8-3列出了部分STP计时器。

表8-3 STP计时器

计时器	含义	缺省值
Hello时间	根网桥发送配置BPDU的时间间隔	2s
转发延迟	侦听状态或学习状态的持续时间	15s
最大存活期	存储BPDU的时间	20s

在某些情况下，交换机可以通过直接相连的链路监测到拓扑的变化，此时无须等到最大存活期到期就直接转入侦听状态。

例如，在图8-14中，假定网段3的链路使用了集线器，而Cat-B的端口1/2的收发器失效了。由于Cat-C可以继续从集线器那里接收到以太网的“链接”信息，所以不会马上意识到失效情况。Cat-C仅仅知道没有新的BPDU到来了。20秒（最大存活期）之后，Cat-C的端口1/2把记录了Cat-B拥有网段3指定端口的BPDU信息置为无效。这使得Cat-C的端口1/2转入侦听状态并努力成为指定端口。由于这个时候Cat-C的端口1/2是网段3的链接中最接近根网桥的端口，所以它最终进入转发状态。实际上，在Cat-B失效后，Cat-C用了大约50秒（最大存活期20秒+侦听状态15秒+学习状态15秒）来接管Cat-B。

在某些情况下，交换机可以通过直接相连的链接监测到拓扑的变化，无须等到最大存活期到期就可直接转入侦听状态。作为范例，我们来看看图8-15。

在这个例子中，Cat-C的端口1/1失效了。这一失效直接导致根端口上的链路失效，所以无须等待20s，旧信息立即就过期了。于是，Cat-C的端口1/2立即转入学习状态并试图成为新的根端口。这对于把STP的收敛时间由50s降到30s（侦听状态15s+学习状态15s）非常有效。

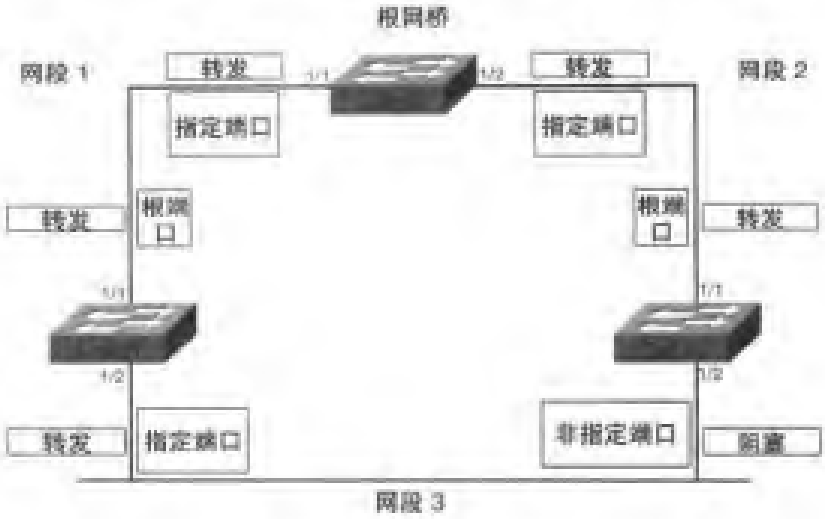


图8-14 已确定端口状态的网络实例

使用STP计时器的时候有两个要点要注意。第一，在没有仔细考虑清楚之前，不要改变计时器的缺省值。当你试图使计时器的数值最大化时，最好只在根网桥上改变STP计时器的值，这是因为根网桥的BPDU的3个字段中包含了计时器的数值，它可以把该计时器值从根网桥通告到网络中的其他网桥上。考虑另外一种情况：如果所有网桥的计时器的值都是在本地配置的，那么在一些网桥还停留在侦听状态的时候，另一些网桥可能已经工作在转发状态了。这种混乱的情况可能会迅速地导致网络进入不稳定状态。作为网络中的惟一一台根网桥，由于它的BPDU中含有定时器字段，所以应该由它指定整个桥接网络的定时器参数。

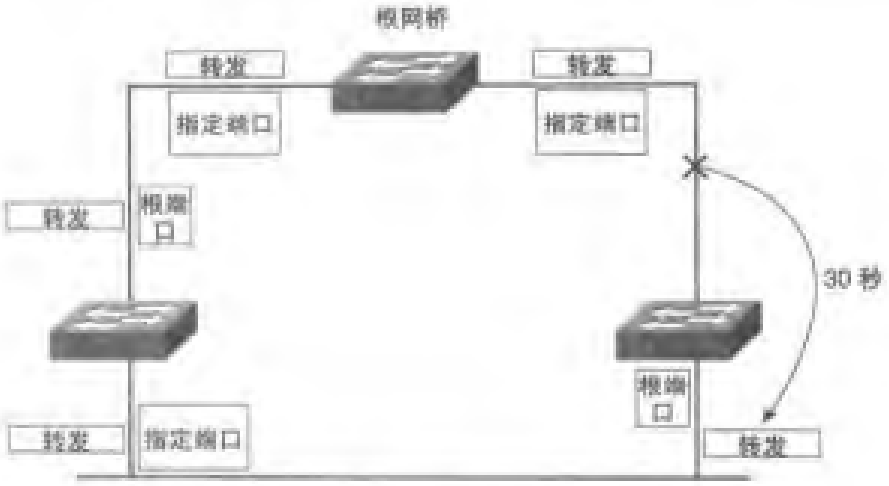


图8-15　已确定端口状态的网络实例

8.3.6　重新计算生成树

网络拓扑发生改变之后，STP通过把一些端口由阻塞状态转为转发状态来保持连通性。如果拓扑的改变是由于网桥或者链路的失效所引起的，生成树通过把一些端口由阻塞状态转为转发状态来重新调整网络拓扑以保证网络的连通。

如图8-16，假如交换机X（根网桥）失效，那么它在最大存活期期间（缺省为20秒，也就是丢失了10个BPDU）就不能向交换机Y发送BPDU，因此交换机Y监测到不能从根网桥得到BPDU的情况。如果交换机Y在其最大存活期期满的时候依然不能从交换机X那里接收到新的BPDU的话，交换机Y就会开始重新计算生成树。交换机Y将它的处于阻塞状态的端口（端口1）从阻塞状态依次转换成侦听、学习最后到转发状态。

大约50秒后网络收敛，交换机Y成为根网桥，并在两个网段之间转发流量。



图8-16　重新计算生成树

实验活动　重新计算生成树

在本实验中，你将观察生成树算法在交换网络的拓扑发生改变之后的处理过程。

8.3.7　收敛

收敛（convergence）对于网络的正常运行来说是很有必要的。对于一个交换式的或者桥接式的网络，一个主要问题是当网络拓扑发生改变之后网络需要多长时间才能收敛。对STP而言，收敛就意味着这样一种状态：所有的交换机和网桥要么处于转发状态，要么处于阻塞状态。

当网桥和交换机的端口处于过渡状态的时候是不能转发用户流量的，而快速收敛正是一种可以缩短这个时间间隔并且合乎我们需要的网络特性。收敛时间通常为30~50s。

8.4　RSTP

为了在网络拓扑发生改变之后，能显著地加快生成树的重新计算过程，快速生成树协议

（RSTP）就应运而生了。RSTP额外为端口定义了替换和备份两种类型，将端口的状态定义为丢弃、学习和转发3种。

当物理拓扑或者它的配置参数发生改变时，RSTP（IEEE 802.1w）可以显著地缩短网络重新收敛的时间。RSTP选出一台交换机作为活动生成树连接拓扑中的根，再根据其上面的端口是否为活动拓扑的一部分来对每个端口配置类型。

在交换机、交换机端口或者LAN失效之后，RSTP能够迅速保持网络的连通性。网桥另一端的端口通过它们之间的显式握手通信转入转发状态，并成为新的根端口和指定端口。当交换机重新启动的时候，RSTP允许交换机端口进行配置，以便端口重新初始化后可以直接进入转发状态。虽然在802.1w中规定的RSTP替换了在802.1d中所规定的STP，但是RSTP与STP却保持着一致性。不过，你的交换机上必须安装增强软件映像（EI）才能使用RSTP。

RSTP定义了以下的端口类型：

- **根端口**（Root）——为生成树拓扑选举出来的转发端口。
- **指定端口**（Designated）——每个交换式LAN网段的转发端口。
- **替换端口**（Alternate）——到根网桥的替换路径，用以替换当前的根端口。
- **备份端口**（Backup）——由指定端口提供的到生成树的叶结点的路径的备份。备份端口只存在于这两种情况下：两个端口通过点到点链路相连成一个环路；网桥与共享LAN网段有两条或两条以上的连接。
- **禁止端口**（Disabled）——在生成树操作中不起作用的端口。

根端口和指定端口包括了活动拓扑中的端口，替换端口或者备份端口则不包括活动拓扑中的端口。

8.4.1 RSTP端口状态

端口状态可以控制转发和学习的过程，它包括丢弃（discarding）、学习（learning）和转发（forwarding）3种状态。表8-4对STP和RSTP端口状态进行了比较。

表8-4 STP和RSTP端口的比较

操作状态	STP端口状态	RSTP端口状态	是否处于活动拓扑中
启用	阻塞	丢弃	否
启用	侦听	丢弃	否
启用	学习	学习	是
启用	转发	转发	是
禁用	禁用	丢弃	否

在一个稳定的拓扑里，RSTP保证所有根端口和指定端口都处于转发状态，而所有的替换端口和备份端口都处于丢弃状态。

8.4.2 转换到转发状态

IEEE802.1w引入了一种非常重要的特性——快速转换（rapid transition）。在802.1w制订之前，生成树算法要被动地等到网络收敛之后才能把一个端口转换成转发状态。新的RSTP确保端口可以不依赖于计时器配置而安全地转换为转发状态。为了实现端口上的快速收敛，协议依赖于这样两个新的变量：边缘端口型（edge port type）和链接类型（link type）。

与终端设备直接相连的端口称为边缘端口（edge ports）。边缘端口不会在网络中形成桥接环路，所以它可以跳过侦听和学习状态直接转换成转发状态。当边缘端口的链接稳定下来后，它不会再引起拓扑的变化。

只有在边缘端口和点到点链接中，RSTP才能完成转发状态的快速转换。在当今的交换式网络中，这并非一条很严厉的约束。链接的类型自动地取决于端口双方的双工模式。全双工模式端口的链接类型为点到点，而半双工模式的则缺省为共享类型。你可以通过外部配置来改变这些缺省设置。图8-17是转发状态快速转换的一个例子。

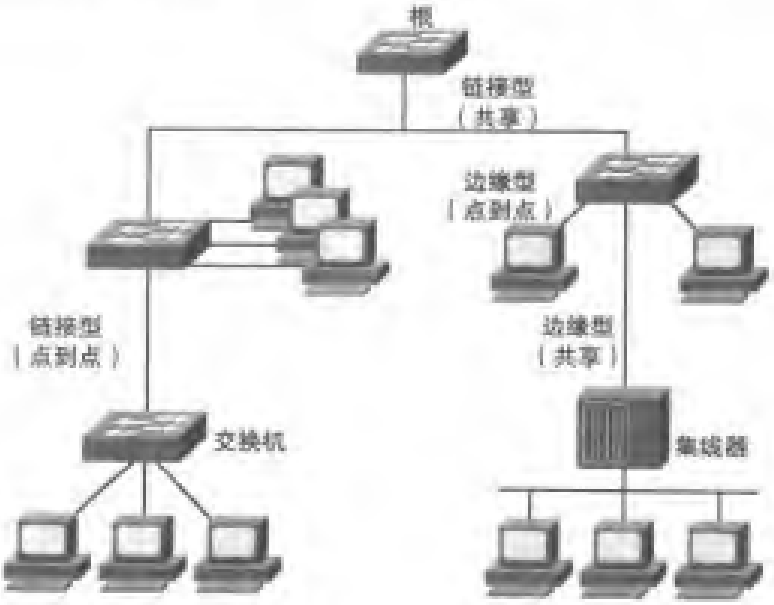


图8-17　转发状态快速转换

RSTP（IEEE 802.1w）最终将取代STP（IEEE 802.1d）。

8.5　总结

本章阐述了如下的STP知识点：

- 阐述了以下问题：冗余拓扑、冗余交换拓扑、广播风暴、帧的重复重传和MAC数据库的不稳定。
- 冗余拓扑可以提供更加可靠和容错性能更好的网络。
- STP和生成树算法可以确保在具有物理环路的拓扑中，形成无环路的逻辑拓扑。
- 阐述了在STP工作过程中比较重要的几个概念：生成树操作、生成树、根网桥选举、生成树端口状态的转换过程、指点端口的选举、路径成本、STP计时器、重新计算生成树以及收敛。
- 讨论了跟RSTP相关的问题、RSTP端口状态以及转发状态的转换。

作为本章学习内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

8.6 关键术语

地址解释协议（*Address Resolution Protocol, ARP*） 将IP地址映射成MAC地址的因特网协议。

网桥ID（*bridge ID, BID*） 网桥或者交换机用来标识优先权和进行根网桥/根交换机选举的数字。拥有最小BID的网桥就是根网桥。

网桥协议数据单元（*bridge protocol data unit, BPDU*） 网桥在可配置的时间里，用来相互之间交换信息的生成树协议Hello分组。

指定网桥（*designated bridge*） 拥有从某一网段到根网桥的帧转发最小路径开销的网桥。

介质访问控制（*Media Access Control, MAC*） IEEE所定义的数据链路层的两个子层中较低的那一个子层。该子层控制对共享介质的访问，例如是进行令牌传递还是使用竞争。

快速端口（*portfast*） 它忽略侦听和学习状态，是使端口立即进入生成树转发状态的一条命令。

快速生成树协议（*Rapid Spanning Tree Protocol, RSTP*） RSTP额外为端口定义了替换和备份两种类型，将端口的状态定义为丢弃、学习和转发3种。

生成树协议（*Spanning Tree Protocol, STP*） 用于维护无环网络的第2层链路管理协议。STP持续监测网络，以便对链路、交换机或者网桥失效或者添加时作出响应。

生存期（*time to live, TTL*） IP中的一个字段，它用于指示一个分组在返回或者被丢弃之前还能经过的最大跳数。

8.7 复习题

1. 冗余拓扑的目的是消除网络的中断故障。这种故障是由几个失效点引起的？
   A. 1
   B. 2
   C. 3
   D. 4
2. 生成树协议的目的是什么？
   A. 维持单一环路
   B. 维持无环网络
   C. 维持多环网络
   D. 维持减少了环路的网络
3. 当网络拓扑发生改变时：
   A. 必须发起重新计算生成树的过程
   B. 必须重新配置生成树的顶结点
   C. 必须重新配置生成树中的所有设备
   D. 生成树协议自动重新配置交换机或者网桥端口
4. 根网桥上的所有端口都是
   A. 根端口
   B. 阻塞端口
   C. 指定端口
   D. 非指定端口
5. 生成树协议如何在非根桥上选出根端口？
   A. 根端口为非根网桥到根网桥的最高成本路径
   B. 根端口为非根网桥到根网桥的最低成本路径
   C. 根端口为非根网桥到备份根网桥的最低成本路径
   D. 根端口为非根网桥到备份根网桥的最高成本路径
6. 以下哪种网桥会被STP选为根网桥？
   A. 拥有最低优先级
   B. 拥有最低BID
   C. 拥有最高BID
   D. 拥有最大MAC地址
7. STP BID包括有：
   A. 网桥优先级和网桥IP地址
   B. 网桥优先级和网桥MAC地址
   C. 网桥MAC地址和网桥IP地址
   D. 网桥MAC地址和以太网端口号
8. 在哪种状态下端口只形成MAC地址表但不转发用户数据帧？
   A. 学习状态
   B. 阻塞状态
   C. 侦听状态
   D. 转发状态

9. 修正后的IEEE规定100 Mbit/s连接的成本是多少?
   A. 4
   B. 10
   C. 19
   D. 100
10. STP收敛的定义是什么?
   A. 所有端口转换到阻塞状态
   B. 所有端口转换到转发状态
   C. 所有端口转换到转发状态或者侦听状态
   D. 所有端口转换到转发状态或者阻塞状态
11. STP缺省的最大存活期是:
   A. 2s
   B. 15s
   C. 20s
   D. 30s
12. 在RSTP中,等效于STP的阻塞状态的状态是:
   A. 阻塞状态
   B. 放弃状态
   C. 丢弃状态
   D. 转发状态
13. RSTP中,每个交换式LAN网段上被选举为转发端口的交换机端口称为:
   A. 根端口
   B. 备份端口
   C. 替换端口
   D. 指定端口
14. STP如何提供无环网络?
   A. 将所有端口置为阻塞状态
   B. 将所有网桥置为阻塞状态
   C. 将部分端口置为阻塞状态
   D. 将部分网桥置为阻塞状态



第9章　虚拟局域网

目标

学习完本章后，你将能够：

- 解释VLAN是什么。
- 引述创建VLAN的原因并描述VLAN的优点。
- 说出VLAN的实施方法的名称并对其进行描述。
- 创建、验证和删除VLAN的配置。
- 描述基本的VLAN故障排除方法。

本章介绍虚拟局域网（VLAN）并讨论使用交换式虚拟局域网体系结构的优点。本章还介绍了VLAN的概念和操作。此外，本章提供了创建、验证和删除VLAN的指南。最后，本章介绍了故障排除的方法，帮助你识别和解决应用VLAN过程中遇到的问题。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图，光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

9.1　VLAN介绍

以太网交换技术的一个主要特征是*VLAN*，它使用交换机将工作站和服务器聚集到逻辑概念上的组中。在一个VLAN中的设备只能够与在同一个VLAN中的设备通信，这样，一个交换式的网络工作起来就像是许多互不相连的单独的LAN一样。很难为VLAN下一个准确的定义，因为各个厂家使用不同的方法来创建VLAN。

很多公司往往使用VLAN来确保把某些特定的用户归到逻辑的分组中。在传统的工作场合，同一个部门常常被组织在一个“本地”的区域中，因此LAN的发展自然适应了这种需求。现在人们的工作地点不再被物理空间所束缚，因此VLAN就发展了“逻辑”区域。例如，在公司市场部工作的人划分在属于市场部的VLAN，而在工程部工作的人则划分在属于工程部的VLAN中。

VLAN的着眼点为网络的可扩展性、安全性和网络管理。VLAN拓扑中的路由器提供广播过滤、安全性和流量控制管理。

一个VLAN是一组网络设备和服务的集合，它不受限于一个物理分段和一台交换机。图9-1显示比较了VLAN中工作站的逻辑分组和传统LAN中工作站的物理分组。

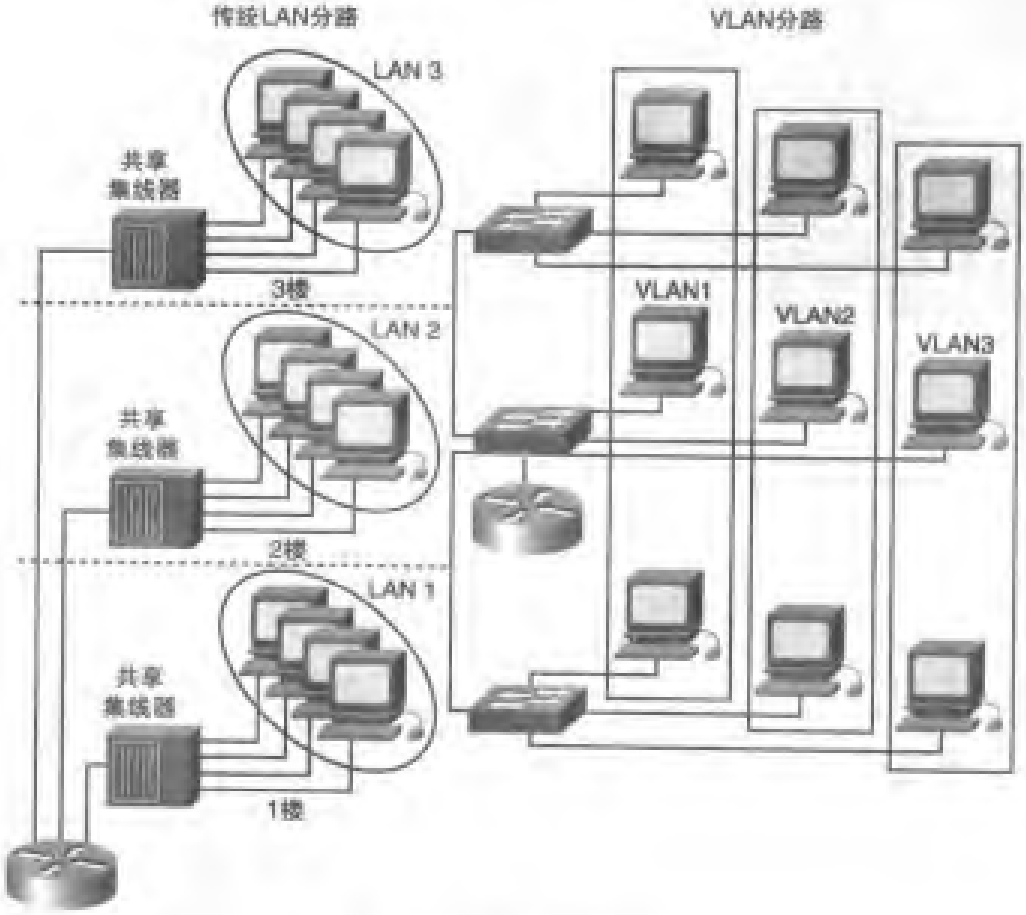


图9-1 VLAN和物理边界

VLAN对交换式网络进行逻辑分段，它根据组织的功能、工程组及应用等因素将这些设备或用户组成群体而无须考虑他们所在的物理位置。例如，一个特定工作组使用的所有工作站和服务器可以连接到同一个VLAN中，而无须考虑它们与网络的物理连接或它们的物理位置。图9-2显示了一个物理VLAN设计的实例，它定义了跨越两台交换机的3个VLAN，VLAN之间由一台路由器互相连接起来。只需要通过软件而无须拔出和移动设备或线缆就可以对网络进行重新配置。

图9-3显示了一个基于公司不同工作组和楼层位置来设计的VLAN。在这个例子中，为每个部门（工程部、市场部和会计部）定义一个VLAN，它分布在3个不同物理位置的3台交换机上。

处于一个VLAN中的客户工作站通常被限制成只能访问处于同一个VLAN上的文件服务器。一个VLAN可以看成是一个在一系列已定义的交换机中的广播域。VLAN由许多终端系

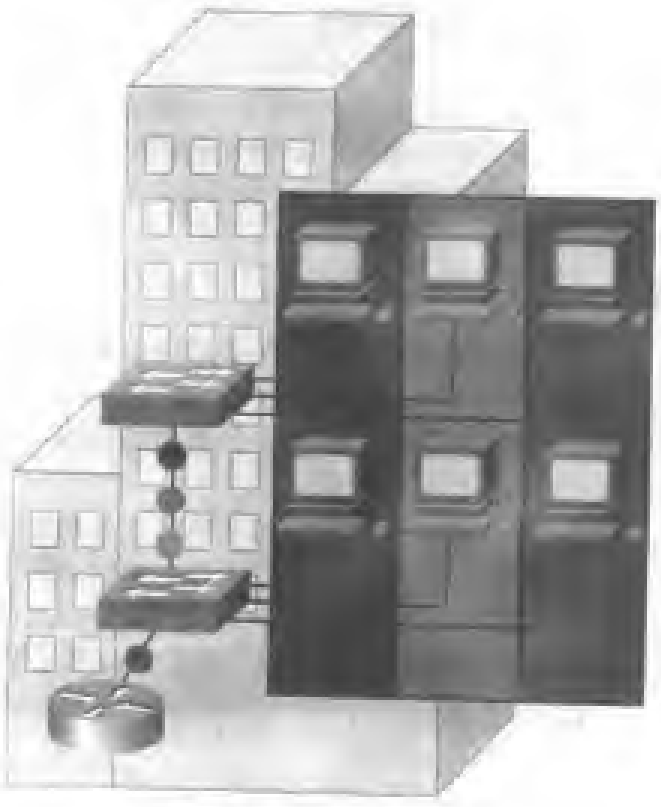


图9-2 VLAN设计

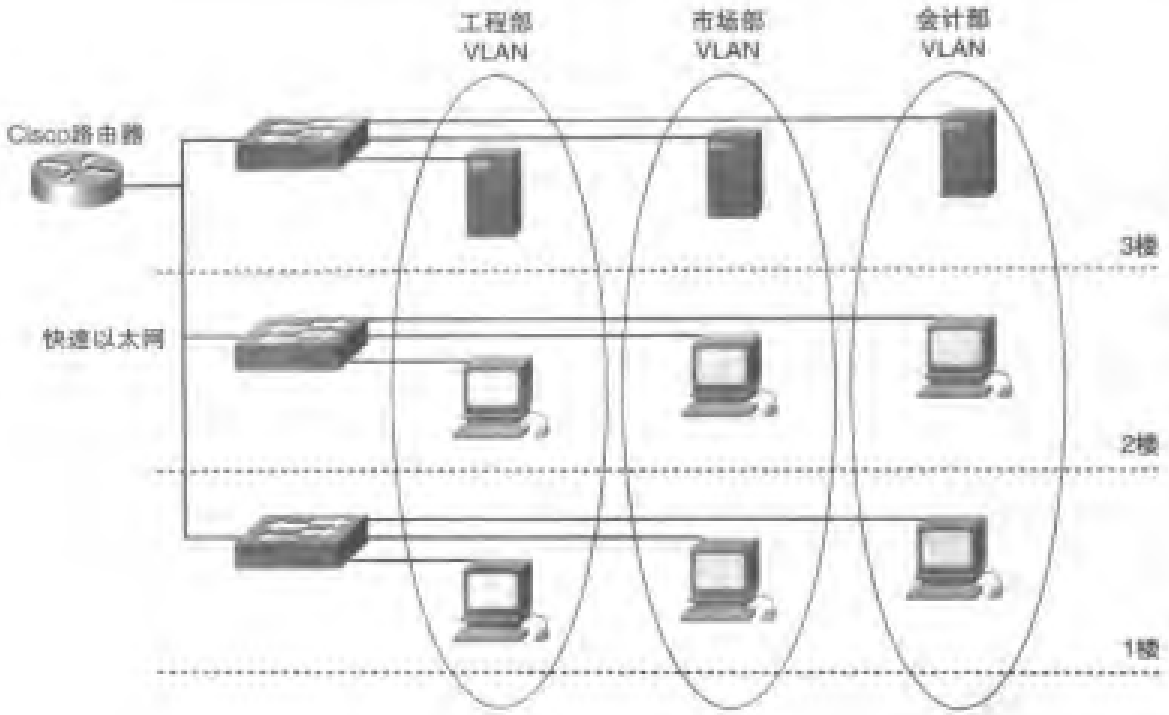


图9-3 VLAN分布在不同的物理位置

统构成，这些终端系统为主机或网络设备（例如网桥和路由器），它们通过一个单独的桥接域相连。桥接域被各种不同的网络设备所支持，例如运行桥接协议的局域网交换机为每个VLAN分配一个独立的网桥组。

VLAN的产生是为了在LAN配置中提供传统上由路由器提供的网络分段服务。在VLAN拓扑中的路由器提供广播过滤、安全和流量管理。交换机可能不会转发VLAN间的流量，因为这样会破坏VLAN广播域的完整性。这些流量应该只能够在VLAN间进行路由。

9.2 用VLAN和路由器构成的广播域

一个VLAN是由一台或多台交换机生成的广播域。

在下面的情形中，该网络设计方案需要两个独立的广播域。在图9-4中，使用了3台单独的交换

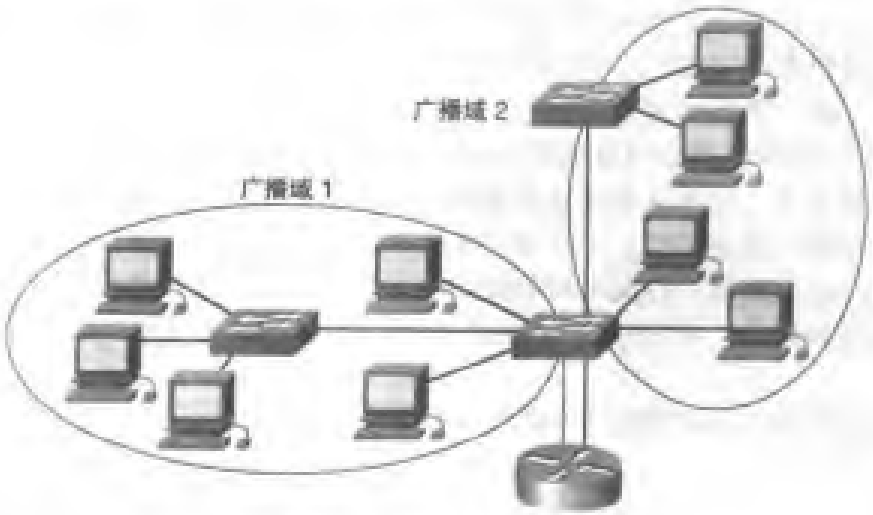


图9-4 VLAN广播分布

机来建立两个独立的广播域——每个广播域一台交换机。请注意，路由器使得分组可以在广播域间进行路由，这些广播域就像独立的第3层的分组（grouping）。这可以通过与路由器的一个或多个连接来实现。

9.3　VLAN的运行方式

一个VLAN构成了一个交换式网络，它根据功能、项目组或应用而无须考虑用户的物理位置来进行逻辑分段。交换机的每个端口都可以分配给一个VLAN。分配到相同VLAN的端口共享广播域，分配到不同VLAN的端口不共享广播域。通过减少不必要且消耗带宽的广播，VLAN全面提高了网络的性能。创建VLAN的方法有两种：

- **静态VLAN**（static VLAN）——这个方法也称为基于端口的成员身份。把端口静态分配给一个VLAN就创建了静态VLAN。当一台设备连接到网络上时，它自动属于这个端口的VLAN。如果用户改变了端口但又想访问同一个VLAN，网络管理员就必须为这个新连接手动添加一个端口到VLAN的分配。如图9-5所示。

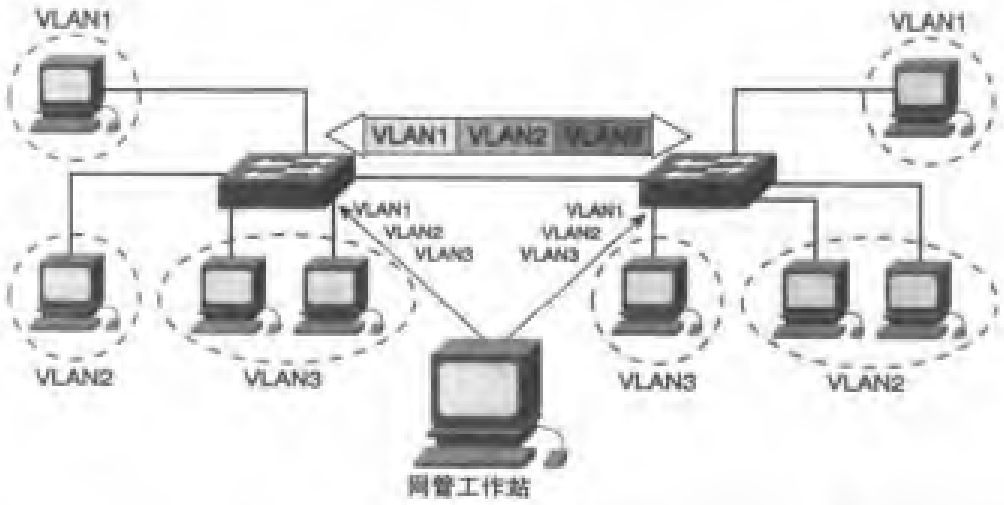


图9-5　静态VLAN

- **动态VLAN**（Dynamic VLAN）——动态VLAN通过使用诸如CiscoWorks 2000之类的软件包来创建。通过VLAN管理策略服务器（VMPS），你可以基于连接到交换机端口上的设备MAC地址动态地为端口分配VLAN。目前动态VLAN能基于设备的MAC地址来建立VLAN成员身份。当一台设备连接到网络时，交换机查询VMPS上的数据库以确定VLAN成员身份。这一过程如图9-6所示，其中每台交换机都有一个惟一的MAC地址。

图9-7显示了基于端口的静态VLAN成员身份。端口被分配到某个特定的VLAN，它与连接到该端口上的用户或系统无关。这意味着连接到该端口上的所有用户应该都是同一个VLAN的成员。一台单独的用户工作站或一台连接多个工作站的集线器可以连接到一个单独的交换机端口。网络管理员通常负责管理VLAN的分配。各端口的配置是静态的，不能够自动改变成另一个VLAN，除非手动地对交换机进行重新配置。在图9-7中，注意每个VLAN都是一个独立的子网，路由器负责VLAN间的通信。

当用户连接到相同的共享网段时，如传统的基于集线器的以太网一样，所有用户将共享该网段的带宽。每当新的用户连接到这个共享介质，每个用户的可用带宽就会变少，因为所有的用户都处于同一个冲突域。如果共享介质的设备太多，冲突就会大量发生，用户应用程序的性能也会随之下降。交换机通过使用微分段为设备间提供独享带宽来减少冲突。然而，交换机依然转发广播，如

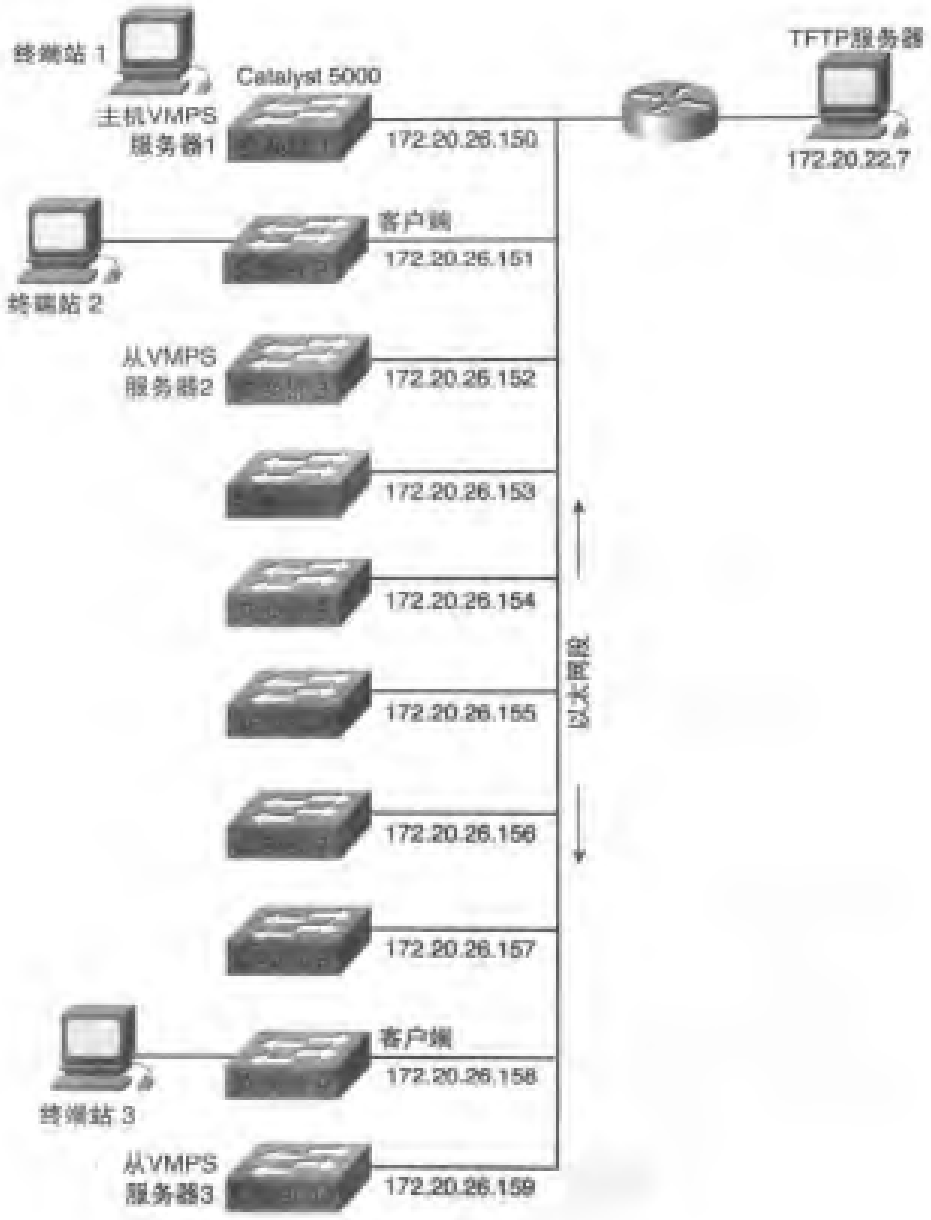


图9-6 动态VLAN

ARP。VLAN通过定义独立的广播域为处于同一共享网络的用户提供更多的带宽。

交换机上每个端口的缺省VLAN为VLAN 1或管理VLAN。不能删除管理VLAN；然而可以创建新的VLAN，也可以重新将端口分配到这些VLAN中。

请记住交换机上的每个接口都像网桥上的端口，因此交换机也基本上被认为是多端口的网桥。网桥会过滤那些无需流向非源网段的其他网段的流量。如果一个帧需要穿过网桥，而且该帧的目的MAC地址是网桥所知道的，那么网桥将会把这个帧转发到正确的接口而不会转发到其他别的接口上；如果网桥或交换机不知道目的地在哪里，它将会把该帧扩散到广播域中（VLAN）除源端口外的所有端口。

每个VLAN都应该分配一个惟一的第3层网络或子网地址。这是为了能够通过路由器在VLAN间交换分组。VLAN可以作为端到端的网络而存在，此时它跨越了整个交换结构；它也可以存在于地理边界内部。

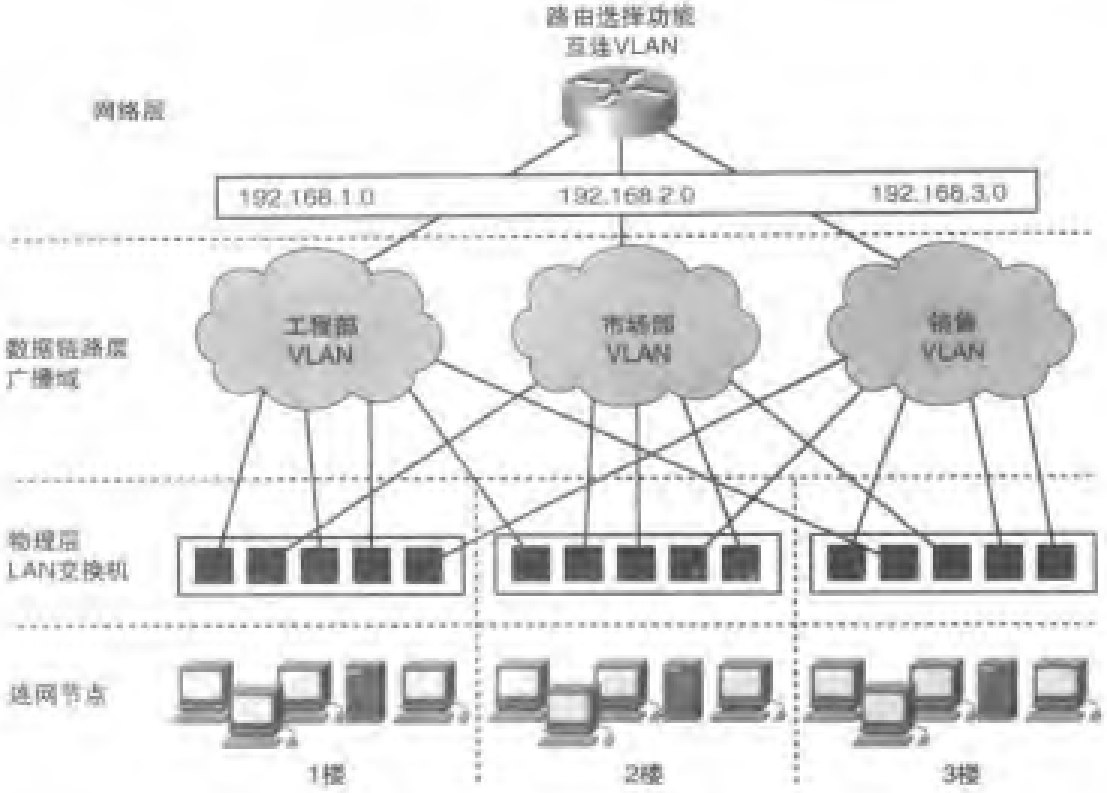


图9-7　端口为中心的静态VLAN

9.4　端到端的VLAN

端到端的VLAN使设备可以基于资源的使用来分组，这包括诸如服务器的使用、工程组和部门之类的参数。端到端VLAN的目标是把80%的流量控制在本地VLAN中，图9-8显示了端到端VLAN的实例。一个端到端的VLAN网络有如下特点：

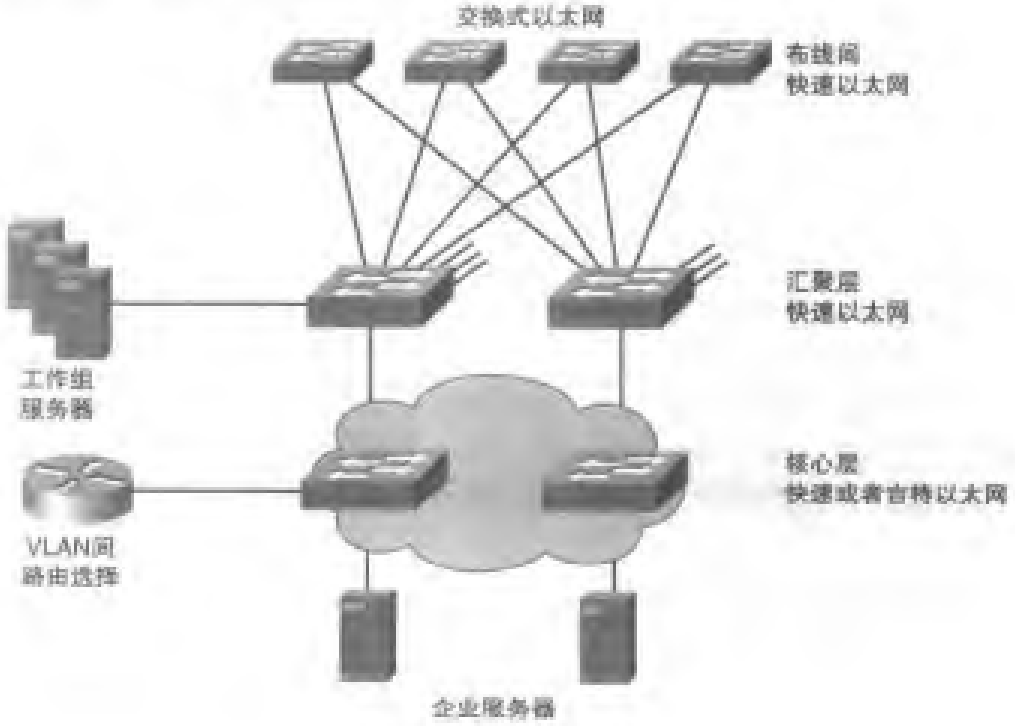


图9-8　端到端的VLAN

- 用户分组是基于工作组或工作职能，而与物理位置无关。
- 同一个VLAN中的所有用户有相同的80/20流量模式。
- 当用户在园区附近移动时，该用户的VLAN成员关系不应该改变。
- 每个VLAN都有所有成员共有的一系列安全性要求。

9.5 地理性VLAN

由于很多公司的网络已经变为以资源为中心，端到端VLAN已变得很难维护；用户要求使用各种不同的资源，而许多资源不再处于他们的VLAN中。由于资源的放置和使用的变化，现在的VLAN更经常地基于地理边界而不是基于公共性边界来创建。

这样的地理位置可以大至整座建筑或小至一间配线间的一台交换机。在地理性VLAN结构中，通常可以发现一种新的20/80模式，其中80%的流量属于远程用户，20%的流量属于本地用户。这正好和端到端的VLAN设计相反。尽管这种拓扑意味着用户必须跨越第3层的设备（路由器）去获取80%的资源，但是这种设计使得网络能提供一种确定的、持续的访问资源的方法。

另外，地理性VLAN比分布在不同地理区域上的VLAN更容易管理和理解。

9.6 VLAN的优点

公司在不停地改组，每年平均有20%~40%的人员在流动。这些移动、增加和改变是网络管理员最头痛的问题之一，也是网络管理的最大开支之一。很多移动都需要重新布线，而且几乎所有的移动都要分配新的工作站地址，需要重新配置集线器和路由器。

9.6.1 变动的管理

VLAN提供了一套有效的机制来控制这些改变并大大降低与集线器、路由器重新配置相关的费用。同一个VLAN中的用户共享相同的网络地址空间（即IP子网），而不管他们的位置如何。当某个VLAN中的用户从一个位置移动到另一个位置时，只要他们仍然处于同一个VLAN而且连接到一台交换机的端口，他们的网络地址就不用改变。位置的变化可以像把一个用户插到一台支持VLAN的交换机的一个端口，再把那个端口配置为所需的VLAN那样简单。在动态VLAN中，当在VMPS中查找到已移动工作站的网络接口卡的MAC地址时，交换机会自动把那个端口配置为相应的VLAN。

9.6.2 VLAN与安全

VLAN是一种把防火墙从路由器延伸到交换机结构并保护网络免受潜在的危险广播破坏的有效机制。此外，VLAN拥有所有交换的性能优点。

通过把交换机的端口或用户分配到特定的VLAN组来创建防火墙；这些VLAN组可以在同一台交换机上，也可以跨越多台交换机。一个VLAN中的广播流量不会传输到该VLAN之外。图9-9显示了一个广播域的例子。相反地，邻近的端口不会接收到别的VLAN产生的广播流量。这种配置充分地减少了整个广播的流量，为真正的用户流量节省出带宽，并完全降低了广播风暴对网络的影响。图9-10显示了路由器如何在VLAN间充当一个防火墙。

共享型LAN的一个缺点是它们相对容易被渗入。只要连接到一个活动的端口上，入侵者就可以访问该网段内的所有流量。组越大，则潜在进入的可能就会越大。

为增加安全性，一种既可以降低成本又可以方便管理的技术是把网络分成多个广播组。它使得网络管理员能完成以下的工作：

- 限制一个VLAN组中用户的人数。

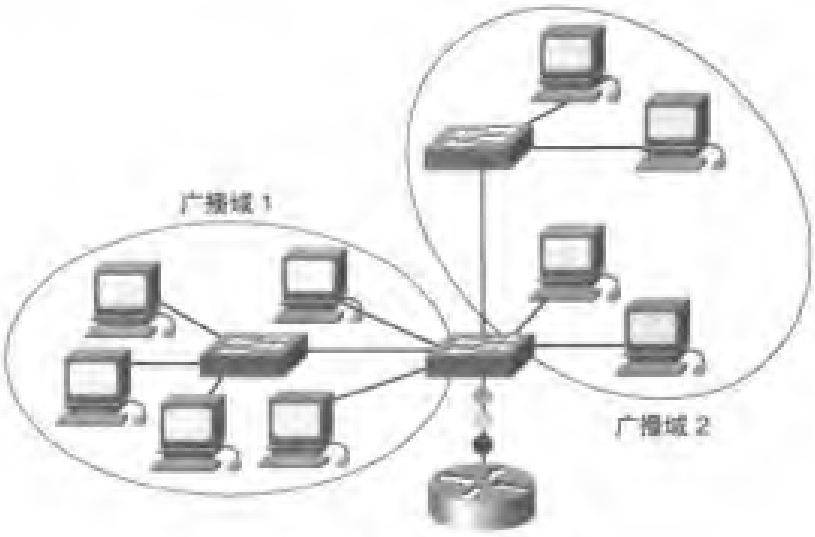


图9-9　广播域

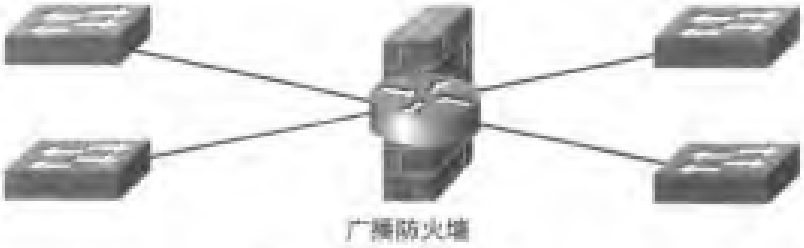


图9-10　广播防火墙

- 防止其他用户在没有得到VLAN网络管理员允许的情况下加入网络。
- 把所有未使用的端口配置为一个缺省的低等级服务的VLAN。

实现这种形式的分组是相对容易的。基于应用和访问特权的类型来对交换机端口进行分组，受限制的应用和资源通常放在一个安全的VLAN中。在安全的VLAN中，交换机限制对该组的访问。可以是基于工作站的地址、应用程序的类型或者协议类型来建立限制。一个VLAN安全性的例子如图9-11所示。

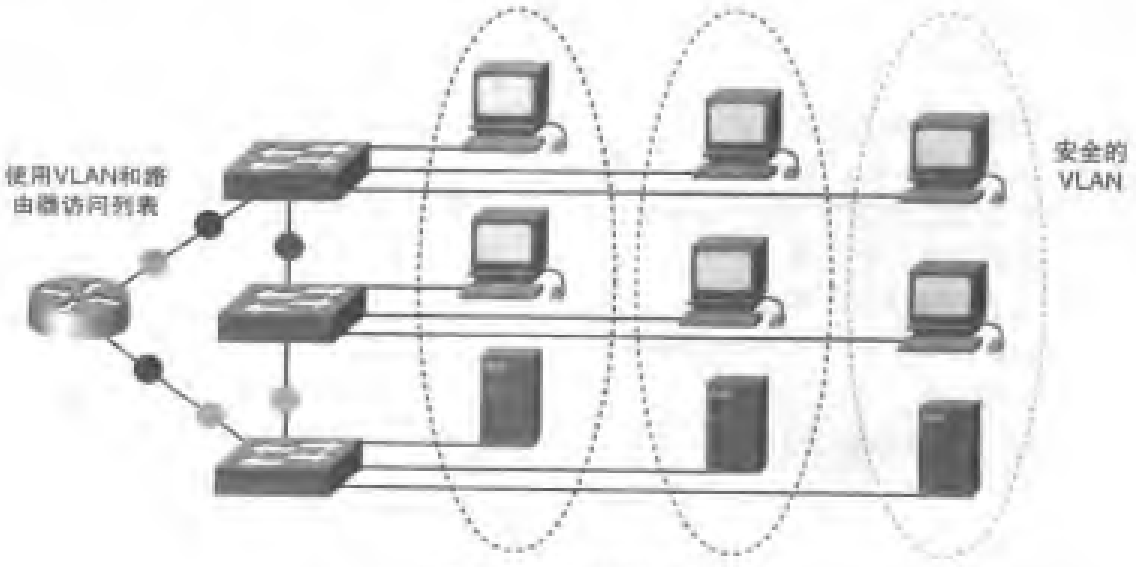


图9-11　安全的VLAN

9.7 在VLAN中使用集线器

在过去的几年，网络管理员安装了大量的集线器，很多这种设备已被更新的交换技术所代替，因为网络应用程序要求为桌面提供更多专用的带宽和更佳的性能。然而这些集线器在很多已安装的场合仍然发挥着作用。因此，网络管理员通过把现有的集线器连接到交换机上来节省开支，图9-12显示了一个例子。

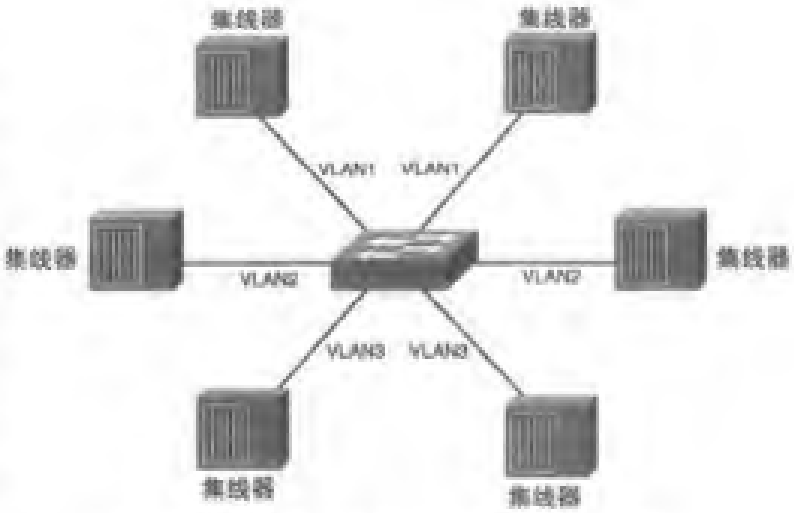


图9-12 在交换式VLAN中使用现有的集线器

每个连接到交换机端口上的集线器网段只能被划分到一个VLAN中，所有共享一个集线器网段的工作站成为同一个VLAN的成员。交换机维护多个MAC地址（每台工作站一个），并把这些地址与集线器所连接的端口相关联。如果一台单独的工作站需要重新分配到另外一个VLAN，则它必须重新定位到相应的集线器中。互连的交换结构处理交换机端口间的通信，并自动决定正确的接收网段。共享式集线器越是能够分为更小的组，微分段就越多，把单独的用户分到VLAN中各组的灵活性就越大。通过把集线器连接到交换机上，你可以把这些集线器配置成为VLAN体系结构的一部分。根据VLAN的分配，也可以共享直接连到交换机端口的流量和网络资源。

9.8 VLAN的类型

3种基本的模型决定和控制了一个分组如何指派到一个VLAN。这3种模型为：

- 基于端口的VLAN（port based VLAN）（静态）。
- 基于MAC地址的VLAN（MAC address based VLAN）（动态）。
- 基于协议的VLAN（protocol-based VLAN）（动态）。

交换机中VLAN的数目依据不同的因素可能会变化很大。这些因素包括流量模式、应用程序的类型、网络管理的需要以及组的共同特点。另外，定义交换机的大小和VLAN数量时需要重点考虑的一个因素是IP寻址方案。

例如，假设用24bit的掩码来定义一个子网。在这种假设下，该子网中一共只有254个主机地址可用。因为强烈建议VLAN和IP子网要一一对应，所以任何一个VLAN上的设备都不应超过254台。

9.9 VLAN帧标识

在由多台交换机构成的VLAN中，数据帧在发送到交换机间的链路上之前，帧头会被封装或者改变，以反映某个VLAN ID。在转发到终端设备前，该帧头还要变换回原来的格式。VLAN的标识逻辑上标记了哪个分组属于哪个VLAN组。

目前存在着多种的中继方法，包括IEEE802.1Q，交换机间链路（ISL），802.10和局域网仿真（LANE）。

9.9.1 IEEE 802.1Q：帧标记

这种协议是IEEE用来标识VLAN的的一种标准方法，它通过在数据帧头插入VLAN标识符来标

记VLAN。这个过程称为帧标记。图9-13显示了一个带有VLAN ID的802.1Q帧格式。每一个802.1Q端口都指派到一个中继线上，而且中继线上的所有端口都属于一个本征VLAN。每一个802.1Q端口都分配一个属于它自己的本征VLAN（缺省是VLAN 1）的标识符值，所有没有标记的帧都指派到在ID参数中规定的LAN中。802.1Q中继线的相关中继线端口都有一个本征VLAN，802.1Q不标记本征VLAN的帧。所以，普通的主机能够读取本征的没有标记的帧，但是不能读取其他帧，因为这些帧都已经进行了标记。在交换机之间交换VLAN的信息时，IEEE 802.1Q帧标记是优先选取的方法。



图9-13　802.1Q帧格式

9.9.2　交换机间链路协议

交换机间链路（ISL）是一种Cisco专有的封装协议，它用来互连多台交换机；它在交换机和路由器上都支持。图9-14显示出了ISL的帧格式。

Catalyst系列交换机使用的ISL帧标记是一种低延迟的机制，它把来自于多个VLAN的流量复用到一条单独的物理路径上。它应用于交换机、路由器以及使用在诸如服务器之类的节点上的网络接口卡之间的连接。为了支持ISL特性，每一台连接的设备都必须配置了ISL。已经配置了ISL的路由器可以用来实现VLAN之间的通信，在第10章的“VLAN中继协议”中会更详细地讨论这个问题。如果ISL帧的报头加上数据帧的大小超过了最大传输单元（MTU），则当一个非ISL设备接收到这个ISL封装的以太网帧后，也许会把它认为是协议错误的帧。管理员利用生成树协议（STP），采用ISL帧标记来维护冗余连接和并行链路间的负载均衡。



图9-14　ISL帧格式

9.9.3　FDDI 802.10

802.10是一种Cisco的专有方法，它在标准IEEE 802.10帧（FDDI）中传输VLAN信息。VLAN信息是写在802.10帧的安全协会标识符（SAID, security association identifier）部分。这种方法通常用来通过FDDI骨干网传输VLAN。

9.9.4 局域网仿真（LANE）

局域网仿真是由ATM论坛定义的一个标准，它为两台通过ATM连接的工作站提供了在传统的LAN（如以太网和令牌环网）中通常所具有的功能。正如该名称所暗示的一样，LANE协议就是在异步传输模式（ATM）网络的顶端仿真LAN。具体来说，LANE协议定义了一种仿真IEEE802.3以太网或者802.5令牌环网的机制。

LANE协议为高层（即网络层）协议定义了一个服务接口，这些接口与现存的LAN中的接口是一样的。通过ATM网络传输的数据会以适当的局域网MAC格式进行封装。换句话说，LANE协议使得一个ATM网络看上去以及行为上都表现得像一个以太网或者令牌环网。图9-15给出了一个LANE网络的例子。

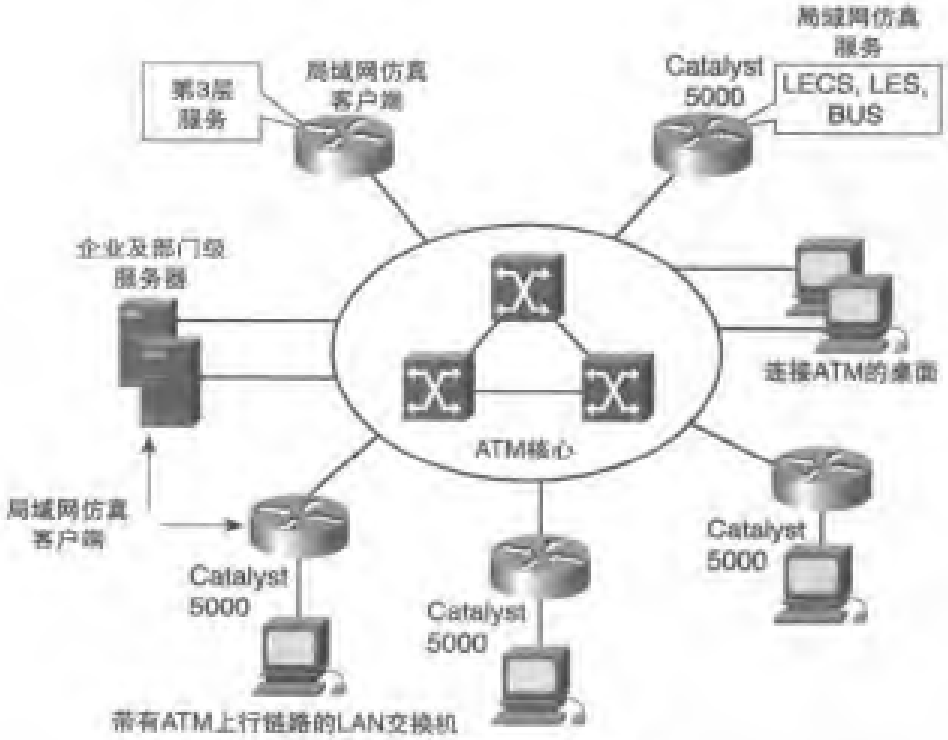


图9-15 LANE网络

表9-1显示了帧标记和封装方法。

表9-1 帧标记和封装的方法

标识方法	封装	标记	介质
802.1Q	否	是	以太网
ISL	是	否	以太网
802.10	否	否	FDDI
LANE	否	否	ATM

9.10 VLAN的配置

起初，网络管理员认为VLAN可以使他们的工作简单化，认为VLAN就意味着不再需要路由器了。不幸的是，这个假设并不正确。VLAN并不能解决第3层的一些问题。它们也许可以使管理员能够更容易执行某些第3层的任务，例如形成一些更为简单的访问列表，但是仍然需要第3层的路由选择。

9.10.1 配置静态VLAN

静态VLAN是在交换机上手动地分配给某个VLAN一些端口，它通过利用VLAN管理应用程序或直接在交换机上面配置来进行分配。除非你改变这些配置，否则这些端口就保持它们已经指定的VLAN配置。尽管静态VLAN需要手动改变条目，但它们安全、易于配置和易于监控。这种VLAN在满足下面几个条件的网络中运行得很好：

- 移动受到控制和管理。
- 有功能强大的VLAN管理软件来配置端口。
- 当维护终端工作站的MAC地址和用户过滤列表时，无需假定会有额外的开销。

相反，动态VLAN并不依靠分配给某个特定VLAN的那些端口，而是基于MAC地址、逻辑地址或者协议类型来进行VLAN分配。

当在Cisco 29xx系列的交换机上配置静态VLAN时，必须记住以下的准则：

- VLAN的最大数目取决于交换机及交换机端口的数目。
- VLAN 1是出厂时定义的缺省VLAN之一。
- VLAN 1是缺省的以太网VLAN。
- *Cisco发现协议（CDP, Cisco Discovery Protocol）*和*VLAN中继协议（VTP VLAN Trunking Protocol）*通告是在VLAN 1上发送的。
- 必须在所有参与到VLAN的交换中继上配置相同的封装协议，例如802.1Q或者ISL。
- 配置VLAN的命令会随着型号的不同而不同。
- Catalyst 29xx系列交换机的IP 地址是在VLAN 1的广播域里。
- 为了创建、添加或者删除VLAN，交换机必须配置为VTP服务器模式。

在交换机上创建静态VLAN是一个直接而简单的任务。如果你正在使用一台基于Cisco IOS命令的交换机，在特权EXEC模式下输入命令vlan database进入VLAN配置模式。创建一个VLAN所必需的配置步骤如下：

```
Switch#vlan database
Switch (vlan) vlan vlan_number[vlan_name]
Switch (vlan) exit
```

如果需要，也可以配置VLAN的名称。

退出时，VLAN会应用到交换机上。下一步是为VLAN分配一个或者多个接口：

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

Catalyst 2900 交换机：

```
Switch (config-if) #switchport access vlan 2
```

Catalyst 1900 交换机：

```
(config-if) #vlan-membership static 2
```

你可以利用show running-configuration命令来验证配置，如例9-1所示。

例9-1 show running-configuration命令

```
Switch#show running-config
Hostname Switch
!
ip subnet-zero
!
interface FastEthernet0/1
!
```

```
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
--- output omitted ---
```



实验活动 配置静态VLAN

在本实验中，你将建立一个交换机的基本配置并进行验证。通过控制台进入交换机，决定固件的版本号，创建2个VLAN，给它们命名以及给它们分配端口。

9.11 验证VLAN的配置

验证VLAN配置的一个好方法是使用show vlan（如例9-2所示）、show vlan brief或者show vlan id id_number命令。

例9-2 show vlan 命令

```
Switch#show vlan
Virtual LAN ID: 300 (IEEE 802.10 Encapsulation)
vLAN Trunk Interface: FDDI 1/1.10
Protocols Configured: Address: Received: Transmitted:
IP 31.108.1.1 642 645
Virtual LAN ID: 400 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.20
Protocols Configured: Address: Received:Transmitted:
IP 171.69.2.2 123456 654321
Bridge Group 50 5190 8234
Virtual LAN ID:500 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.30
Protocols Configured: Address: Received:Transmitted:
IPX 1000 987654 456789
Virtual LAN ID: 600 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.30
Protocols Configured: Address: Received:Transmitted:
IP 198.92.3.3 8114 4508
IPX 1001 2 3
Bridge Group 50 8234 5190
```

VLAN会应用到如下的综述：

- 一个已经创建的VLAN只有当它被映射到交换机的端口时才有用。
- 缺省情况下，所有的以太网端口都属于VLAN 1。
- 不要在端口号之间输入空格。这样交换机会给你一个错误消息，因为一个空格会把空格后面的值定义为另外一个参数，而该参数却不属于此命令结构中的参数。

9.12 保存VLAN的配置

把VLAN配置的副本作为文本文件保留下来是非常有用的，它可以达到备份或审核的目的。

你可以用一张软盘来保存VLAN的配置文件，然后把它传送到不同的计算机上。如果该VLAN配置文件中捕获有一些无关系的字符，则在使用之前将它们删除。

以下的步骤描述如何复制一个VLAN配置：

步骤1 经由交换机控制台的连接，进入到交换机上的特权模式。

步骤2 转到超级终端窗口的“传送”选项。

步骤3 选择“捕获文本”。

步骤4 选择配置文件将会保存的位置（例如桌面）。

步骤5 给文件取名为VLANconfig。

步骤6 选择“开始”。

步骤7 在交换机上，键入show run。

步骤8 当配置文件显示完毕的时候（如果没有显示完毕，则按几下空格键来完成显示），回到超级终端窗口的“传送”选项，再次选择“捕获文本”，“停止”来保存和关闭文件。

步骤9 删除没有关系的字符。



实验活动 检验VLAN配置

在本实验中，你将创建一个基本的交换机配置和两个VLAN。然后为VLAN命名并且给它们分配多个成员端口。最后，通过把一台工作站从一个VLAN移到另一个VLAN来测试它的功能。

9.13 删除VLAN的配置

在一台基于set命令的交换机上删除一个VLAN，可以键入命令**clear vlan** *vlan_number*，如例9-3所示。在这个例子中，通过使用命令clear vlan 2把VLAN 2从该域中删除。需要注意的一点是：你必须在VTP服务器上键入这个命令。你不能从一个VTP客户机上删除VLAN；如果这台交换机配置为透明模式，你可以删除VLAN，然而这个VLAN仅仅是在该Catalyst交换机上被删除了，而不是在整个管理域中被删除。在一台配置了透明模式的交换机上，所有VLAN的创建和删除都只对本地有意义。（VTP域会在第10章介绍）

注意：当你删除了一个VLAN后，任何分配到这个VLAN的端口都会变成非活动状态。这些端口仍然与这个VLAN相关联（所以变得非活动），除非你把它们再分配到一个新的VLAN中。

例9-3 基于Set命令的交换机

```
Console> (enable) clear vlan 2
This command will deactivate all ports on vlan2
In the entire management domain
Do you want to continue (y/n) [n]?y
Vlan 2 deleted
```

从基于Cisco IOS命令的交换机接口上删除一个VLAN，就犹如在一台路由器上删除一条命令一样。在之前的例子中，可用下面的命令在FastEthernet 0/3创建了VLAN 2：

```
Switch (config-if) #switchport access vlan 2
```

为了从这个接口上删除该VLAN，只要在接口Fa 0/3上使用这条命令的no格式即可：

```
Switch(config-if)#no switchport access vlan 2
```



实验活动 删除VLAN配置

在这个实验中，创建一个基本的交换机配置和两个VLAN。然后给它们命名并且给它们分配多个成员端口。接着，删除这些VLAN，并了解为什么你不能删除VLAN 1。

9.14 VLAN故障排除

在交换式网络中，误配一个VLAN是最常见的错误之一。这一部分描述最常见的误配错误，而且提出解决方案以帮助你为交换式网络排除故障。

表9-2显示了一些可能会发生在路由器或者交换机上的高级别的VLAN问题。表中列出的问题的事实或现象及其可能发生的原因和相应的措施也许可以帮助你去识别和解决这些问题。

表9-2 VLAN的问题

问题的现象	可能发生的原因及相应的措施
VLAN的速度慢或者性能不稳定	该设备适配器坏了，此时要检查一下硬件 以太网的全双工或者半双工设置不正确 线缆存在问题。检查连接的LED灯；检查是否适当的连接上正确的线缆以及线缆长度是否超出了最大的线缆距离
所连接的终端或modem连接不能与路由器或交换机通信	终端和控制台端口误配 检查波特率和字符格式是否配对 检查为了到达不同IP子网的交换机，是否需要在路由器上配置缺省路由
本地的VLAN设备不能与远端的、在路由器另一边的VLAN上的设备通信	IP地址或者掩码配置错误 检查CDP和利用show interface命令 缺省网关没有设置或者设置不正确 检查路由器、交换机、服务器和客户机 VLAN配置错误。检查端口的分配是否正确 如果一个端口属于多个VLAN，则去除不必要的VLAN之间的连接 存在VLAN不一致的问题。确认中继线两端的VLAN能相互匹配 存在ISL问题。确认有适当的中继线使用VLAN 1以及要确认没有发生无效的VTP服务器信息更新

当遇到吞吐量很差的问题时，检查看看存在什么类型的错误。有可能是适配器坏了。如果帧校验序列（FCS）、帧对界错误和超短帧都出现了，则通常表明双工模式不匹配。罪魁祸首通常是设备之间的自动协商或者是一条链路两端之间不匹配的设置。要考虑下面这些问题：

- 问题是发生在本地还是链路的远端？记住：一条链路中包括的交换机端口数目是最少的。
- 分组采用哪一条路径？是通过中继线还是通过非中继线到达另一台交换机？

如果你从show interface命令的输出中看到冲突的次数在迅速地增加，问题可能是这条链路已经过载了。有一个错误的说法，即交换式以太网消除了冲突，而事实是：交换机使冲突的次数最小化而已。但是如果交换机运行在半双工模式下，冲突仍然会发生，因为两端的设备同一时间总会试图进行通信。

很多客户机试图同时与新闻服务器进行通信就是一个例子。这些流量穿过路由器和交换机到达直接相连的服务器。同时，服务器也在试图为响应这些客户的请求而进行通信。当服务器正在应答

某个客户时，另外一个客户发送来一个请求，结果就有可能发生冲突。在以太网中解决冲突的惟一办法就是运行在全双工模式下。VLAN故障排除的过程如图9-16所示。

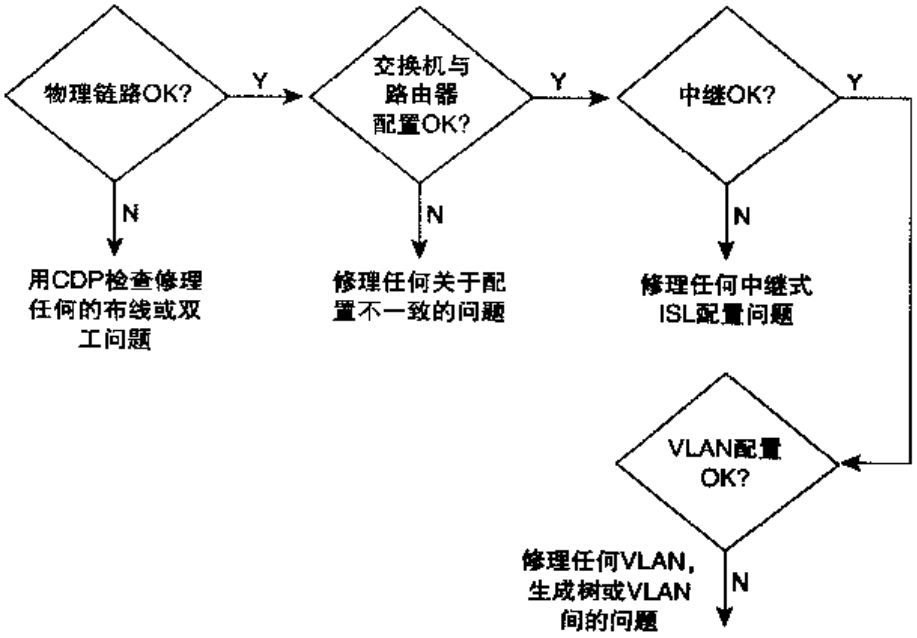


图9-16　VLAN故障排除

作为故障排除过程中的一个实例，我们可以假设一台设备不能与另一台设备通信。以下是解决此问题的建议方法：

• 使用show interface命令来查看，确保IP地址、子网掩码和交换机的接口的VLAN成员身份正确。为了防止冲突，确保接口都配置了不同子网的IP地址和子网掩码。

• 如果主机是跟交换机接口处在同一个子网，就要确保交换机接口和连接那台主机的端口都分配在同一个VLAN中。可以使用show interface和show port来检查。

• 如果主机是在另一个子网，就要确保交换机上已经配置了缺省网关（缺省路由），且该网关的IP地址为与交换机接口位于同一子网的路由器的IP地址。可以使用show ip route命令来检查。

• 用show spantree（Catalyst1900）或show spanning-tree vlan（Catalyst 2950）命令来检查端口的生成树状态。如果端口处于侦听或学习状态，则等到端口进入转发状态，然后再尝试去连接主机。

• 确保主机和适当的交换机端口的速度和双工设置都正确。可以使用show port命令来检查。

• 如果所连接的设备是一台末端工作站：

——在该端口启用生成树的快速端口。可以使用set spantree portfast enable命令。记住，这些命令在2900系列的交换机上并不支持。快速端口把端口立即置于转发状态，而跳过了侦听和学习状态。（不要把这一特性应用在连接非末端工作站设备的端口上。）

——在端口上关闭中继协议。可以使用set trunk命令。

——关闭端口的以太通道。可以使用set port channel命令。你必须为这个命令指定一个有效的端口范围，而不是仅仅指定单独的一个端口。

• 确保交换机正在学习主机的MAC地址。可以利用show cam dynamic命令。

9.15　总结

在这一章里，你学习到了使用VLAN会有如下的好处：

• 使得移动、添加和改变设备的连接更加容易。

- 通过在VLAN间采用第3层路由选择设备，可以获得更好的管理控制。
- 相比于单个广播域的LAN，VLAN可以降低LAN的带宽消耗。
- 通过减少广播的转发，降低了不必要的CPU开销。

对于VLAN故障排除，你学到了以下方法：

- 关于如何为基于VLAN的网络排除故障的更为具体的方法。
- 在VLAN配置和排除故障过程中会碰到的一些最常见的问题。
- 防止广播风暴和环路的方法。
- 故障排除命令的恰当使用方法。

作为本章所学习内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

9.16　关键术语

广播（*broadcast*）　发送到网络中所有节点的数据分组。广播由广播地址所标识。

Cisco发现协议（*CDP, Cisco Discovery Protocol*）　提供单一专有的命令，就能够使网络管理员获得另外一台直接相连的路由器的配置的摘要。

帧校验序列（*FCS, frame check sequence*）　为了进行错误控制而添加到帧上的额外字符。

全双工（*full-duplex*）　具有能够在发送站点和接收站点之间同时进行数据传输的能力。

半双工（*half-duplex*）　在发送站点和接收站点之间，数据的传输在某一时刻只能向一个方向进行。

虚拟局域网（*VLAN, virtual local-area network*）　在一个或多个LAN上的一组设备，经配置（用管理软件）后它们就可以如同连接在同一线路上那样进行通信，而这时它们实际上是位于几个不同的局域网段。

VLAN中继协议（*VTP, VLAN Trunking Protocol*）　在交换式网络中，VTP减少了管理工作量。当你在VTP服务器上配置了一个VLAN时，这个VLAN信息就会分发到这个域内的所有交换机上。这样就无需在其他交换机上都配置同样的VLAN。VTP是Cisco专有的协议，在绝大多数的Cisco Catalyst系列产品中都可以使用。

9.17 复习题

1. VLAN解决什么问题?
   A. 可扩展性
   B. 安全性
   C. 通信流的管理
   D. 以上都是
2. 一个VLAN可以被认为是下面中的哪一个?
   A. 广播域
   B. 冲突域
   C. 广播域和冲突域
   D. 域名
3. 在VLAN拓扑中的路由器能提供什么功能?
   A. 广播过滤
   B. 安全
   C. 通信流管理
   D. 以上都是
4. 短语*可扩展的微分段*（*microsegmentation with scalability*）的含义是什么?
   A. 无须建立冲突域就能够增加网络大小的能力
   B. 将大量的主机连接到一台交换机上的能力
   C. 实时地向多个节点发送广播地能力
   D. 以上都是
5. 交换机作为VLAN的核心元素，提供了哪些智能化的功能?
   A. 基于用户、端口或逻辑地址来分组形成VLAN
   B. 对帧进行过滤和转发
   C. 与其他交换机和路由器进行通信
   D. 以上都是
6. 连接到一个__2__端口的每一个__1__分段只能被分配到同一个VLAN中。
   A. 交换机；集线器
   B. 集线器；路由器
   C. 集线器；交换机
   D. 局域网；集线器
7. 以下哪一项不是静态VLAN的优点?
   A. 安全性
   B. 易于配置
   C. 易于监控
   D. 加入新站点时可以自动配置端口
8. 以下哪一项不是VLAN划分时依据的标准?
   A. 端口号
   B. 协议
   C. MAC地址
   D. 以上都是建立VLAN的标准

9. 以下哪一项是增加VLAN带来的好处？选择所有正确的。
   A. 交换机不需要配置
   B. 广播能够得到控制
   C. 机密数据能够得到保护
   D. 突破了限制用户成为组的物理的边界
10. 下面关于VLAN的陈述哪一个是错误的？
   A. 把用户逻辑分组为明确的VLAN的最常用的方法是帧过滤和帧的标识
   B. VLAN的优点包括通过建立安全用户组而得到的更加严密的网络安全性
   C. 网桥构成了VLAN通信中的一个核心组件
   D. VLAN有助于分发流量负载
11. 交换机上的哪一项第3层功能使你能够轻松地操纵不同IP子网上的设备？
   A. 透明桥接
   B. 分段
   C. 冲突域的减少
   D. VLAN
12. 当分组从一个VLAN传输到另外一个VLAN时，需要以下哪一种设备？
   A. 网桥
   B. 路由器
   C. 交换机
   D. 集线器
13. 帧标记发生在OSI模型的哪一层？
   A. 第1层
   B. 第2层
   C. 第3层
   D. 第4层
14. ___使交换机可以共享地址表，而___向每一帧分配一个用户定义的VLAN ID？
   A. 帧标记（Frame tagging）；帧转发
   B. 帧标识（Frame identification）；帧移动
   C. 帧过滤；帧标记
   D. 帧标记；帧过滤
15. 为什么创建VLAN很重要？
   A. 使得移动、添加和改变更加简单
   B. 需要较少的管理性开销
   C. 路由器能够更快地交换
   D. A和B



第10章 VLAN中继协议

目标

学习完本章之后，你将能够：

- 理解中继（trunking）。
- 理解VTP和VTP配置的基本原理。
- 理解虚拟局域网（VLAN）间的路由选择。
- 配置基本的VLAN间路由选择。

本章将学习中继（trunking）的由来及其操作。还将发现VLAN中继协议（VTP）是如何在一个大型局域网络环境中解决一些与管理和实现虚拟局域网（VLAN）相关的问题的。最后，将介绍VLAN间的路由选择。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图，光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

10.1 中继（Trunking）

中继（Trunking）的历史可以追溯到无线电（radio）和电话（telephone）技术的起源。在无线电技术中，中继线是一条承载多路无线电信号的通信线。

在电话行业，中继的概念与两点间（其中的一点往往是中心局）的电话通信路径或信道相关。图10-1举出了一个例子。

共享的多条中继线（shared trunks）也可以作为中心局（CO, central office）间的冗余（如图10-2所示）。

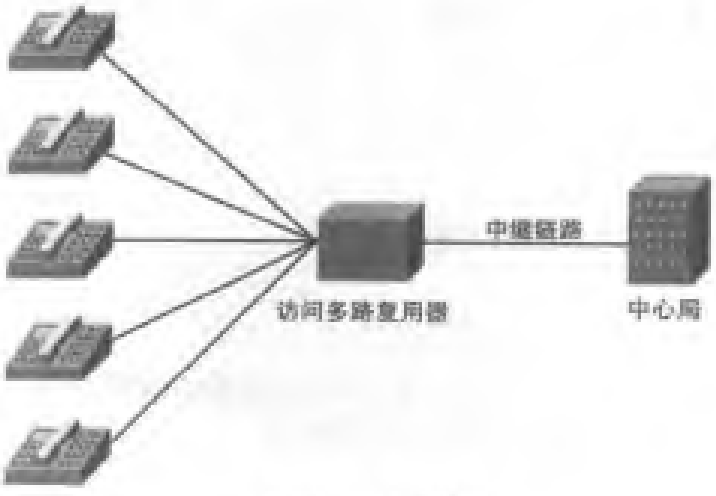


图10-1 中继链路

电话和无线电业中使用的这一概念也是电信硬件一开始便使用的。这种线路的一个例子便是通信网络中集中了多条线路的一段，如图10-3所示。骨干便是由多条中继构成的。

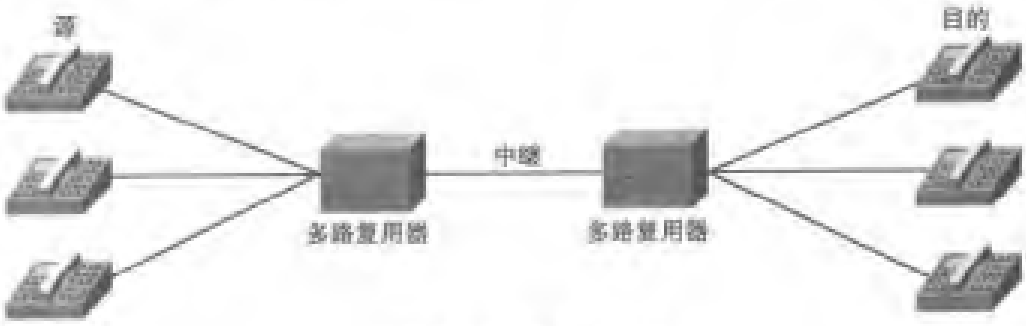


图10-2　中继共享链路

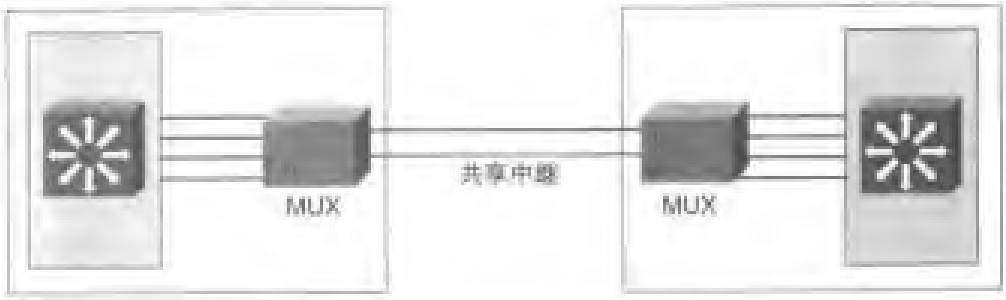


图10-3　使用频分复用（FDM）的中继线

目前，同样的中继原理已经应用于网络交换技术。这里的一条中继线是两台交换机之间的一个物理和逻辑连接，用于传输网络通信。

10.1.1　中继的概念

中继（trunk）是两点间的一条传输信道，这两点通常是交换中心。中继线是承载（或启用）多条逻辑链路的一条物理连接。

对于VLAN交换环境而言，中继是一条支持多个VLAN的点到点链路。中继线的目的是为了在两台实现VLAN的设备（通常是两台交换机）之间创建链路时节省端口。图10-4显示了在两台交换机Sa和Sb上可用的两个VLAN。

图10-4中所示的第一种方法是在设备间建立了两条物理链路，每条链路承载一个VLAN的通信。这种解决方案不易扩展。如果要加入第3个VLAN，就需要再牺牲一个端口。这种设计同样无法胜任负载均衡。而且有些VLAN的通信也被证明不必单独占用一条专门的链路。一条中继多条虚拟（逻辑）链路捆绑在一条物理链路上。

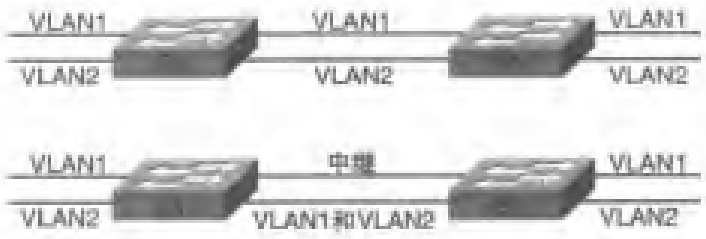


图10-4　为什么进行中继

10.1.2　中继的运行方式

当通过一条中继传输的VLAN数量增加时，在中继两端使用现有的交换表进行基于帧目的MAC地址的端口传输决定的速度会变慢，并且难于管理。交换机所存储的表越大，决定将帧交换到各自端口的过程就越慢。

为了有效地管理两台网络设备之间单条物理线路或链路上来自不同VLAN的帧传输，在这两台设备之间需要一种通信/语言。使用这种通信，或者说协议，能够使设备可以对帧在中继两端相关端

口上的传输和分发达成“共识”。中继协议由此诞生。

中继协议允许来自不同VLAN的帧通过单条物理信道传输；它们对帧的分发进行管理，以将其分发到对应的VLAN端口。目前，存在着两种中继机制：帧过滤（frame filter）和帧标记（frame tagging）。本章使用帧标记，因为这种方法是IEEE推荐的标准中继机制。图10-5显示了一个中继链路的例子。

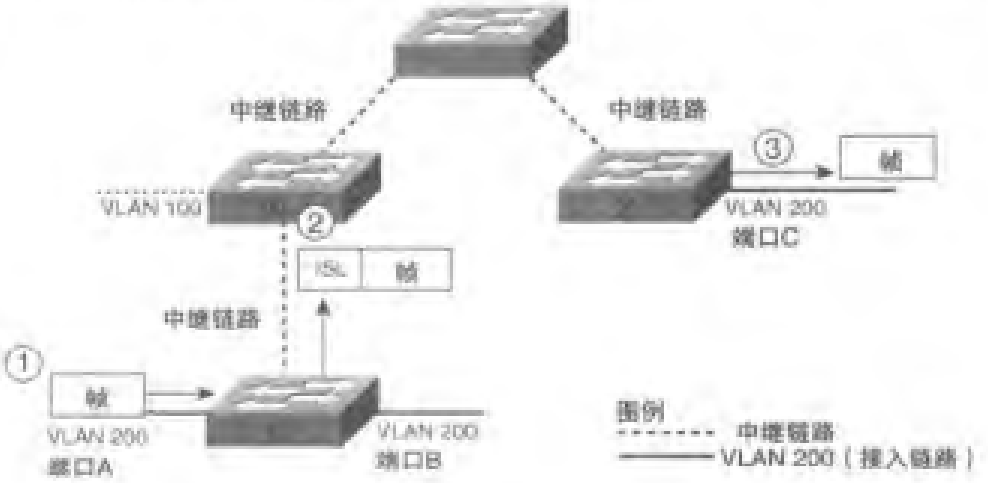


图10-5 中继链路

采用帧标记机制的中继协议为每个帧分配一个标识符，使得管理它们更为容易，从而实现更快捷的帧传送。这些标记在中继线链路的开始处添加并在另一端删除。它们不会被广播。

两台交换机之间惟一的物理链路能够承载任意VLAN的通信。为此，在这条链路上发送的每一个帧都被打上标记来标识它所属的VLAN。存在不同的标记方案。以太网段中最常见的方案如下：

- **交换机间链路**（*Inter-Switch Link, ISL*）——起源于Cisco专有的交换机间链路协议。
- **802.1Q**——这是一种IEEE标准方法，它在以太网帧中插入VLAN成员信息。

10.1.3 VLAN和中继

实现中继需要某些规则或协议。中继机制能帮助VLAN交换网络的扩展。一个VLAN是在一个或多个局域网上的一组设备，通过配置（使用管理软件）这些设备就像速在同一条电缆上一样进行通信，但实际上它们分布在许多不同的局域网网段中。中继提供了一种有效的手段来向其他交换机分发VLAN ID信息，并完成网络中交换机之间的通信，如图10-6所示。



图10-6 VLAN和中继

帧标记（Frame tagging）是一种标准的中继机制；与帧过滤相比，帧标记为VLAN的部署提供了一种更具扩展性的解决方案，使其能够在园区网络范围内实现。IEEE 802.1Q规定帧标记是实现VLAN的方法。图10-7显示了一个帧标记的例子。

VLAN帧标记是专为交换式通信开发的一种方法。在每一帧被转发穿越网络骨干时，帧标记在每一帧的头部设置一个惟一的标识符。每台交换机在向其他交换机、路由器或终端设备进行帧的广播或传送之前，都会理解并检测这个标识符。当帧要离开网络骨干时，交换机会在帧被传输至目标

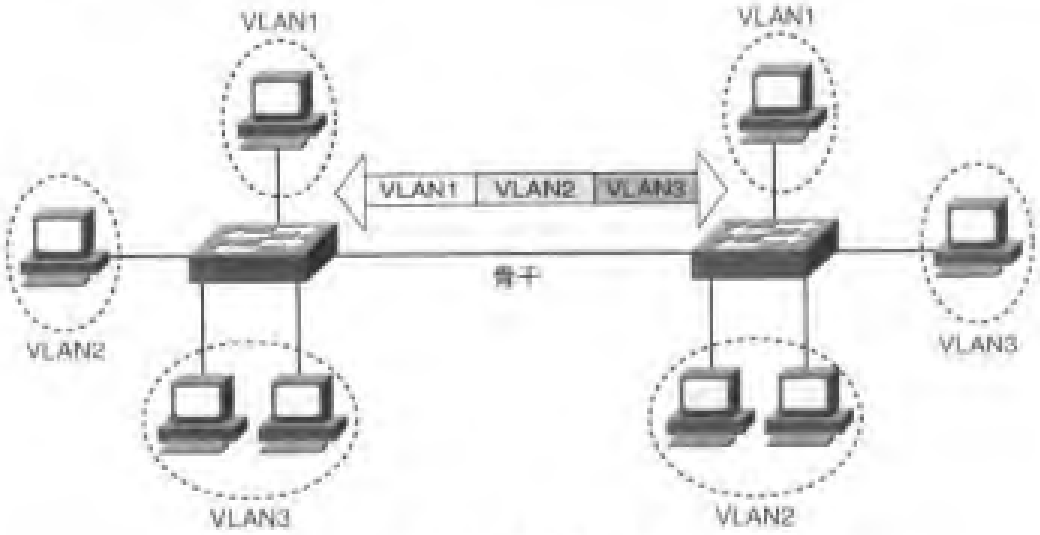


图10-7　帧标记

终端站之前，去掉这个标识符。帧识别是第2层功能，只需要很少的处理或管理开销。

中继链路不属于某一特定VLAN。中继链路的职责是扮演交换机和路由器间的VLAN管道。

图10-6中的交换机使用ISL相互通信，ISL是在交换机间数据流传输时维护VLAN信息的一种协议。在ISL中，以太网帧与一个包含VLAN ID的报头一起被封装。

10.1.4　交换机命令行界面

根据所使用的交换机型号，你会遇到两种不同的命令输入类型。Cisco交换机的命令行界面（CLI）基于IOS命令的或基于set命令。前者使用IOS命令，与Cisco路由器所用的命令类似。后者使用set命令来配置交换机。两种CLI所使用的命令是不同的。下面给出了两种命令类型的配置例子。例如，2900系列的交换机使用基于IOS的命令。4500和6500系列的交换机则使用基于set的命令。型号更老的交换机，比如1900系列，在使用IOS命令的同时还具有一个菜单驱动界面。所有类型的交换机都提供一个基于web的图形化管理界面，用户可以使用浏览器来访问。

下面是基于IOS命令的交换机特权模式提示符和命令实例：

```
Switch# show trunk
```

下面是基于set命令的交换机特权模式提示符和命令实例：

```
Switch>(enable) set vtp v2 enable
```

10.1.5　中继的实现

要在一台基于Cisco IOS命令的交换机上创建或配置一条VLAN中继，首先将端口配置为中继，然后指定中继的封装。中继两端的封装必须一致。为此需要使用如例10-1所示的命令。

例10-1　配置VLAN中继线命令

```
Switch(config-if)# switchport mode trunk?
  allowed          Set allowed VLAN characteristics when interface is in trunking mode
  encapsulation    Set trunking encapsulation when interface is in trunking mode
  native           Set trunking native characteristics when interface is in trunking mode
  pruning          Set pruning VLAN characteristics when interface is in trunking mode
Switch(config-if)# switchport trunk encapsulation?
```

```
dot1q           Interface uses only 802.1q trunking encapsulation when trunking
isl             Interface uses only ISL trunking encapsulation when trunking

Switch(config-if)# switchport trunk encapsulation isl
```



实验活动 用ISL进行中继

在本实验中，你将创建一个基本的交换机配置，然后创建多个VLAN，给它们命名并指定成员端口。在两台交换机之间创建一条ISL中继线线路，然后将一台工作站从一台交换机移到另一台交换机来测试VLAN。

试图在一个端口上配置VLAN中继线之前，要确定该端口所支持的封装类型。对于基于set命令的交换机，可以通过使用show port capabilities命令来实现，如例10-2所示。注意，端口2/1只支持IEEE 802.1Q封装。

例10-2 show port capabilities命令

```
Console> (enable) show port capabilities 2/1
Model                   WS-X4232-GB-RJ
Port                    2/1
Type                    No GBIC
Speed                   1000
Duplex                  full
Trunk encap type        802.1Q
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 2/1-2
Flow control            receive-(off,on,desired),send-(off,on,desired)
Security                yes
Membership              static,dynamic
Fast start              yes
QOS scheduling          rx-(none),tx-(2q1t)
CoS rewrite             no
ToS rewrite             no
Rewrite                 no
UDLD                    yes
SPAN                    source,destination
```

要在一台基于set命令的交换机上创建或配置一条VLAN中继，输入set trunk命令，将链路两端的端口配置为中继端口，并指定在这条中继链路上传输的VLAN。

```
Switch>(enable) set trunk mod_num/port_num|on|off|desirable|auto|nonegotiate} vlan_range
|isl|dot1q|dot10|lane|negotiate]
```

也可以使用set trunk命令来改变中继的模式，如例10-3所示。

例10-3 set trunk命令

```
Console> (enable)
Console> (enable) set trunk 2/1 on dot1q
```

```
Port(s) 2/1 trunk mode set to on.
Port(s) 2/1 trunk type set to dot1q
```

快速以太网和吉比特以太网的中继模式关键字如下：

• on——这个模式使端口成为永久中继模式。即使相邻端口不同意改变，该端口仍将成为一个中继端口。on状态不支持封装类型的协商，因此必须在配置中指定封装。

• off——这个模式使端口成为永久非中继模式，并会通过协商将链路转换成非中继链路。即使相邻端口不同意改变，该端口仍将成为一个非中继线端口。

• desirable——这个模式使端口主动尝试将链路转换成中继链路。当相邻端口被设置为on、desirable或auto模式时，该端口会成为中继端口。

• auto——这个模式使端口愿意将链路转换成中继链路。当相邻端口的状态被设置为on或desirable模式时，该端口会成为中线端口。这是快速以太网和吉比特以太网端口的缺省模式。注意，如果中继链路两端都是缺省设置，它不会成为中继线；任何一端都不会率先询问是否转换成中继。

• nonegotiate——这个模式使端口成为永久中继模式，但禁止端口产生动态中继协议（DTP, Dynamic Trunking Protocol）帧。必须手动配置相邻的端口，使之作为中继线端口才能建立一条中继链路。

使用特权模式下的**show trunk** [*mod_num/port_num*]命令来检看交换机上已经配置的中继及其设置。

10.2　VLAN中继协议

本节将解释VLAN中继协议（VTP）的概念和操作，及其在VLAN交换式局域网环境中的实施。

10.2.1　VTP的历史

VTP的产生为了解决在VLAN交换式网络环境运行中潜在的问题。

例如，考虑一个拥有支持多VLAN的多台互连交换机的域。为了创建和维护VLAN间的连通性，每个VLAN必须手动配置在每台交换机上。随着组织的增长，其他交换机被加入到网络中，每个新加入的交换机必须手动配置VLAN信息。任何一个错误的VLAN分配都可能导致下面两个潜在的问题：

• 由于VLAN配置不一致造成的VLAN交叉连接。

• 在混合介质环境中，例如以太网和光纤分布数据接口（FDDI），VLAN配置发生冲突。

有了VTP，可以在一个公共的管理域中维持VLAN配置的一致性。另外，VTP减少了管理和监控VLAN网络的复杂性。

10.2.2　VTP的概念

VTP的任务是在一个公共的网络管理域中维持VLAN配置的一致性。VTP是一种消息协议，它使用第2层的中继帧来管理一个单独域中VLAN的添加、删除和重命名。而且，VTP还允许向网络中的所有其他交换机集中传达变化。

VTP消息被封装在Cisco特有的ISL或IEEE 802.1Q协议帧中，然后通过中继链路传送给其他设备。在IEEE 802.1Q帧中，添加了一个4字节字段来标记每个帧。两种格式都带有VLAN ID。

尽管交换机端口一般只被分配到一个VLAN中，但是中继端口缺省传输来自所有VLAN的帧。

10.2.3 VTP的好处

VTP可以减少在发生改变时可能产生的配置不一致。这种不一致性了解导致违返安全策略，因为使用重复的命名会造成VLAN交叉连接出现；并且当VLAN从一种局域网类型映射到另一种（例如从以太网到ATM或FDDI）时，也会在内部断开。VTP提供以下好处：

- 整个网络的VLAN配置一致性。
- 与允许跨越混合介质中继一个VLAN的映射方案，例如将以太网VLAN映射到高速骨干VLAN中（如ATMLANE或FDDI）。
- 对VLAN的准确跟踪和监控。
- 关于整个网络中新增VLAN的动态报告。
- 加入新VLAN时的即插即用配置。

在交换机上创建VLAN之前，必须首先建立一个VTP管理域（VTP management domain），在这个域内可以检查当前网络上的VLAN。同一个管理域中的所有交换机彼此共享它们的VLAN信息，并且一台交换机只能参加一个VTP管理域。不同域中的交换机不会共享VTP信息。

使用VTP，每台Catalyst系列交换机会在它的中继线端口通告以下信息：

- 管理域。
- 配置版本号。
- 已知的VLAN及其具体参数。

10.2.4 VTP域

一个VTP域由一台或多台互连设备组成，它们共享同一个VTP域名。一台交换机只能属于一个VTP域中。

当向网络中其他交换机传输VTP消息时，VTP消息被封装在一个中继协议帧中，如ISL或IEEE 802.1Q。域名必须与被传输的信息完全匹配（大小写敏感）。图10-8显示了一个ISL帧中VTP的一般封装。

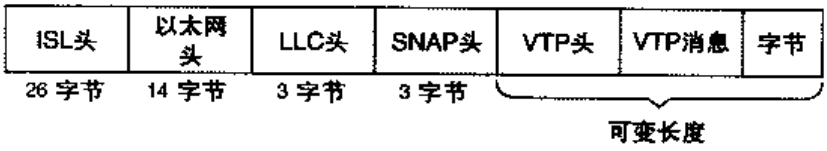


图10-8 用ISL帧封装VTP

VTP头的不同取决于VTP消息的类型，但通常而言，以下4项可以在所有VTP消息中找到：

- **VTP协议版本**——不是版本1就是版本2。
- **VTP消息类型**——指出4种类型之一。
- **管理域名长度**——指出后面的名称长度。
- **管理域名**——指出为管理域配置的名称。

10.2.5 VTP模式

VTP交换机工作在以下3种模式之一：

- **服务器**（Server）。
- **客户端**（Client）。
- **透明**（Transparent）。

1 VTP服务器（缺省模式）

如果一台交换机被配置为服务器模式，你将可以创建、修改和删除VLAN并对整个VTP域指定

其他配置参数（如VTP版本和VTP剪裁）。VTP服务器在Catalyst系列交换机的NVRAM中保存VLAN配置信息。VTP服务器从所有中继端口发送VTP消息。

VTP服务器向同一VTP域中的其他交换机通告它们的VLAN配置信息，并通过中继链路上接收的通告与其他交换机同步VLAN配置。该模式是交换机的缺省模式。

2　VTP客户端

被配置为VTP客户端模式的交换机不能创建、修改或删除VLAN信息。此外，客户端也不能保存VLAN信息。这种模式适用于那些缺乏足够存储器来保存大量VLAN信息表（如VIP服务器所需的）的交换机。VTP客户和服务器一样处理VLAN变化，而且它们也从所有中继线端口发送VTP消息。

3　VTP透明模式

被配置为透明模式的交换机不参与VTP。一台VTP透明模式的交换机不通告它的VLAN配置，也不会基于收到的通告去同步它的VLAN配置。它们转发其中继线端口上收到的VTP通告（版本2），但是却忽略消息中所包含的信息。一台透明交换机既不会在收到更新时修改它的数据库，也不会发送更新以指示其VLAN状态的变化。除了转发VTP通告，VTP在透明交换机上是禁用的。

4　VTP的运行方式

检测通告中VLAN的增加信息作为对交换机（服务器模式和客户模式）的一种通知，使它们可以准备接收中继端口上具有最新定义的VLAN ID、仿真局域网名称或802.10安全组织标识符（SAID, Security association identifiers）的网络通信。

图10-9中，交换机C向交换机A和交换机B传输一条添加或删除的VTP数据库条目。配置数据库有一个修订号等于“通告”+1。配置修订号（configuration revision）越高意味着被发送的VLAN信息比所存储的拷贝数据更新。当一台交换机收到一个具有更高配置修订号的更新时，交换机会用发送来的VTP更新中的新信息覆盖存储的信息。交换机F因为属于另一个域而不会处理更新。

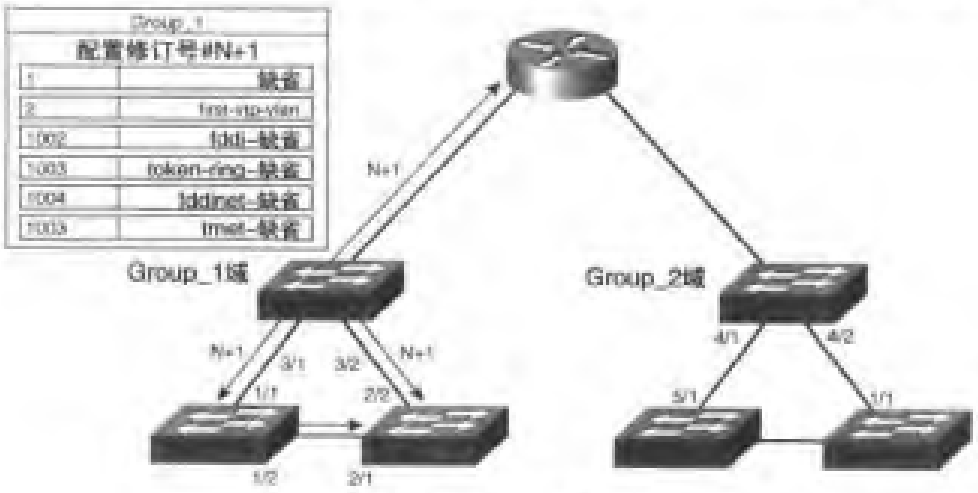


图10-9　VTP操作

在缺省状态下，管理域处于一种不安全模式，也就是说交换机的相互操作无需密码。给管理域添加一个密码将自动使其进入安全模式。必须在管理域中的每一台交换机上配置同一个密码才能使用安全模式。

10.2.6 VTP的实施

使用VTP，每台交换机在它的中继端口上通告其管理域、配置修订号、已知VLAN以及各已知VLAN的具体参数。这些通告帧被发送给一个组播地址，使得所有相邻设备能够收到这些帧，但是这些帧不能通过正常的桥接过程来转发。同一个管理域中的所有设备获知发送设备中目前所配置的所有新VLAN。一个新VLAN必须在管理域中的一台设备上创建并配置。该管理域中的所有其他设备自动获知这个信息。

关于出厂缺省VLAN上的通告是基于介质类型的。用户端口不能配置为VTP中继。每个通告的配置修订号从0开始。当有改变发生时，配置修订号增加1（n+1）。管理域中的修订号持续增加直到2,147,483,648，此后计数器复位回0。

存在两种类型的VTP通告（VTP advertisement）：

- 客户端启动时的信息请求。
- 来自服务器的响应。

VTP消息（VTP message）分为3种类型：

- **通告请求**（*Advertisement request*）——客户端请求VLAN信息。
- **汇总通告**（*Summary advertisement*）——服务器以汇总响应。
- **子集通告**（*Subset advertisement*）——服务器以子集响应。

这3种类型的VTP消息如图10-10所示。

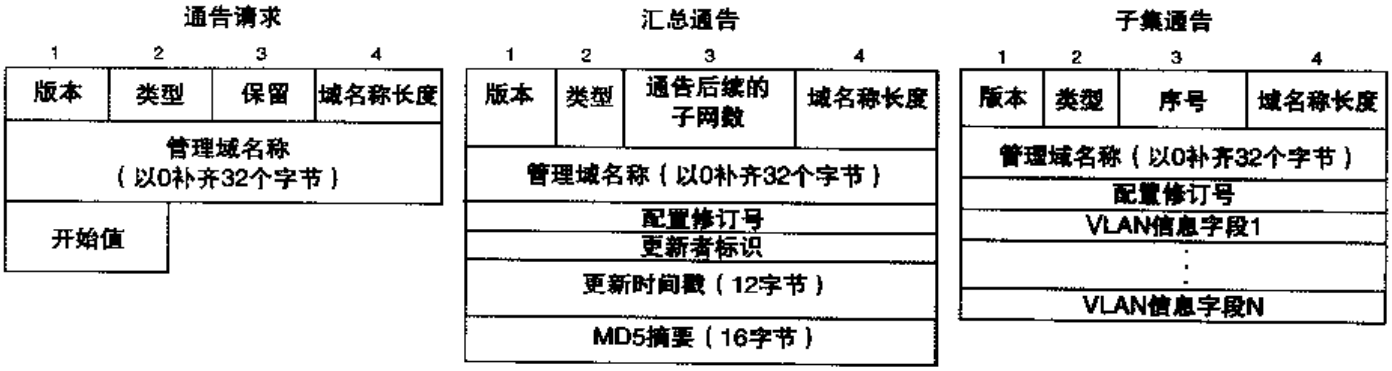


图10-10 通告请求

缺省情况下，服务器和客户端模式的Catalyst交换机每5分钟发布一次汇总通告。它们用当前的VTP修订号通知邻居交换机它们所确信的信息。假定域名匹配，接收服务器或客户比较配置修订号。如果通告中的修订号高于接收交换机上的当前修订号，则接收交换机会发出一个对新VLAN信息的通告请求。一个汇总通告格式的例子如图10-11所示。

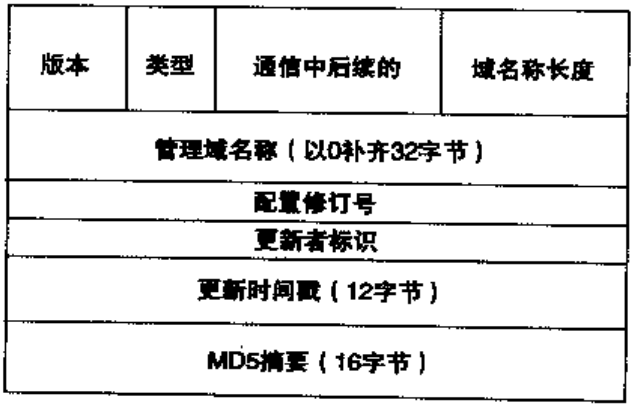


图10-11 汇总通告格式

子集通告包括VLAN的详细信息，如VTP版本类型、域名称及相关字段以及配置修订号。创建或删除一个VLAN、挂起或启动一个VLAN、改变VLAN的名称以及改变一个VLAN的最大传输单元（MTU）都可以触发该通告。一个子集通告格式的例子如图10-12所示。

通告必须包含以下部分或全部信息：

- **管理域名称**（*Management domain name*）——域名不同的通告将省略。
- **配置修订号**（*Configuration revision number*）——越高的数字意味着越新的配置。

• **消息摘要算法5**（*MD5 Message Digest5*）——当分配了一个密码的时候，MD5是VTP发送的密钥。如果密钥不匹配，则忽略更新。

• **更新标识**（*update identify*）——更新者标识是发送VTP汇总通告的交换机的标识。

10.2.7　VTP的配置

以下是在网络上配置VTP和VLAN之前需要考虑的基本任务：

步骤1　确定即将使用的VTP版本号。

步骤2　决定这台交换机是否是一个已存在的管理域的成员或者是否需要创建一个新的域。如果已经存在一个管理域，确定域的名称和密码。

步骤3　为交换机选择一个VTP模式。

版本	类型	序号	域名称长度
管理域名称（以0补齐32Bytes）			
配置修订号			
VLAN信息字段　1			
⋮			
VLAN信息字段　N			

VLAN信息字段包括每个VLAN的信息，它的格式如下

信息长度	状态	VLAN类型	VLAN名称长度
ISL VLAN-id		MTU大小	
802.10索引			
VLAN名称（用0补足4的倍数个字节）			

图10-12　子集通告格式

1　配置VTP版本

在管理域中可以运行两种不同版本的VTP：VTP版本1和VTP版本2。两个版本不能互操作。如果选择把管理域中的一台交换机配置成VTP版本2，则必须把该域中所有交换机都配置成VTP版本2。缺省是VTP版本1。如果需要一些VTP版本2提供但VTP版本1没有提供的特殊特性，需要执行VTP版本2。可能需要的最常见特性是对令牌环VLAN支持。

在一台基于Cisco IOS命令的交换机上配置VTP版本，首先进入VLAN数据库模式（VLAN database mode）。使用以下命令改变一台基于Cisco IOS命令的交换机上的VTP版本号：

```
Switch# vlan database
Switch(vlan)# vtp v2-mode
```

使用以下命令改变一台基于set命令的交换机上的VTP版本号：

```
Switch>(enable)set vtp v2 enable
```

VTP版本1不支持而VTP版本2支持的特性如下：

• **对令牌环的支持**——VTP版本2支持令牌环局域网交换和VLAN。

• **不能识别的类型/长度/值（TLV）支持**——VTP服务器或客户向其他的中继传播配置变化，甚至包括它不能解析的TLV。这些不能识别的TLV保存在NVRAM中。

• **版本相关的透明模式**——在VTP版本1中，一台VTP透明交换机检查VTP消息中的域名和版本，并仅当版本和域名匹配时才转发这个消息。因为监控引擎软件只支持一个域，所以在透明模式下VTP版本2中不需要检查版本就能转发VTP消息。

• **一致性检查**——在VTP版本2中，只有通过CLI或简单网络管理协议（SNMP）输入新信息时，才执行VLAN一致性检查（如VLAN名和值）。当新信息是从一个VTP消息中或得或从NVRAM中读取的，则不执行一致性检查。如果一个收到的VTP消息中的摘要是正确的，则这些信息无需经过一致性检查就被接受。一台能运行VTP版本2的交换机，只要它的VTP版本2处于禁用状态，就可以和运行于VTP版本1的交换机共同运行在同一个域中。

如果一个域中的所有交换机都能够运行VTP版本2，只需要在一台交换机上启用VTP版本2（使用set vtp v2 enable命令）。版本号会传播给该VTP域中其他能运行VTP版本2的交换机。

2 配置VTP域

如果所安装的交换机是网络中的第一台交换机，要创建管理域。否则，验证要加入的管理域的名字。如果管理域被保护，则要为该域配置密码。

使用如下命令创建一个管理域：

```
Switch(vlan)# vtp domain Cisco
```

域名长度可以在1到32个字符之间，并且大小写敏感。密码必须在8到64个字符之间。

在一个现有VTP域中加入新的VTP客户端时，一定要核实该交换机的VTP配置修订号低于VTP域中其他交换机的配置修订号。使用show vtp status命令。一个VTP域中的交换机使用具有最高VLAN配置修订号的交换机的VLAN配置。如果一台新加入的交换机具有一个比VTP域更高的修订号，那么它可以擦除VTP服务器和VTP域中的所有VLAN信息。

在基于set命令的交换机上创建一个管理域或将交换机加入管理域，使用如下命令：

```
Switch>(enable)set vtp domain domain_name
```

3 配置VTP的模式

为交换机选择3种可用VTP模式之一。以下是选择交换机模式的一些基本指导方针。

如果是管理域中的第一台交换机，并且还期望添加其他交换机，那么把模式设为服务器（server）。其他交换机会从这台交换机中获知VLAN信息。你至少要有一台服务器。

如果管理域中有其他交换机，设置交换机模式为客户端（client）以防止新交换机意外地向现有网络传播错误信息。如果希望这台交换机最终成为VTP服务器，那么在它从网络上获知正确的VLAN信息之后将其模式改为服务器。

如果某台交换机不会与网络中的其他任何交换机共享VLAN信息，则将该交换机设置为透明模式（transparent mode）。在透明模式下，可根据意愿创建、删除和重命名VLAN，而该交换机不会把这些改变传播给其他交换机。如果网络中有很多人在配置设备，那么你将面临网络中具有两种不同意义但有相同VLAN标识的重叠VLAN的风险。

使用如下命令设置基于Cisco IOS命令的交换机的正确模式：

```
Switch(vlan)# vtp{client|server|transparent}
```

使用如下命令设置基于set命令的交换机的正确模式：

```
Switch>(enable)set vtp mode server|client|transparent
```

4 验证VTP配置

例10-4显示了show vtp status命令的输出。这条命令可以验证基于Cisco IOS命令的交换机上的VTP配置设置。

例10-4 show vtp status命令

```
Switch# show vtp status
VTP Version                     :2
Configuration Revision          :2
Maximum VLANs supported locally :68
Number of existing VLANs        :6
VTP Operating Mode              :Client
VTP Domain Name                 :Cisco
```

```
VTP Pruning Mode                        :Disabled
VTP V2 Mode                             :Enabled
VTP Traps Generation                    :Disabled
MD5 Digest                              : 0x35 0x84 0x7B 0x04 0x3D
0x55 0x3B 0xDA
Configuration last modified by 0.0.0.0 at 12-23-02 20:24:33
```

例10-5显示了在一台基于set命令的交换机上执行show vtp statistics命令的结果。这条命令显示了发送和接收到的VTP通告消息汇总以及配置错误侦测。使用这条命令可以帮助进行VTP的故障排除。

例10-5　show vtp statistics命令

```
Switch>(enable)show vtp statistics
VTP statistics:
summary advts received          0
subset advts received           0
request advts received          0
summary advts transmitted       0
subset advts transmitted        0
request advts transmitted       0
No of config revision errors    0
No of config digest errors      0
```



实验活动　802.1Q的中继

在本实验中，你将创建一个基本的交换机配置，然后创建多个VLAN，给它们命名并分配成员端口。在两台交换机之间创建一条802.1Q中继线路，然后通过把一台工作站从一台交换机移到另一台交换机上来测试VLAN。



实验活动　VTP客户和服务器配置

在本实验中，你将创建多个VLAN，给它们命名并分配成员端口。在两台交换机之间创建一条802.1Q中继线线路，将其中一台交换机配置为服务器，另一台配置为客户。然后通过把一台工作站从一台交换机移到另一台交换机上来测试VLAN。

10.2.8　VTP剪裁

一个交换机的缺省行为是在网络上传播广播和未知分组。这种行为会导致不必要的数据流穿过网络。

VTP剪裁（VTP pruning）通过减少不必要的通信泛洪，如广播、组播、未知和泛洪的单播分组，来提高网络带宽。VTP剪裁通过限制泛洪通信进入正常通信用来访问网络设备必须使用的中继线，来增加可用带宽。缺省情况下，VTP剪裁是禁用的。如果在一台远端交换机上没有任何来自VLAN3的可用设备，则剪裁可以阻止该交换机将VLAN 3的数据流发送到中继上从而阻止带宽浪费。

在一台VTP服务器上启用VTP剪裁也就在整个管理域的启动剪裁。在启用VTP剪裁后，它需要几秒种才能生效。在缺省情况下，VLAN 2到1,000都（pruning eligible）。VTP剪裁不会剪裁来自不具有剪裁资格的VLAN的数据通信。VLAN 1永远没有剪裁资格（pruning ineligible），因此来自

VLAN 1的数据通信不能被剪裁。可以在设备上有选择地设置特定VLAN具有剪裁资格或不具有剪裁资格。使用如下命令在基于Cisco IOS命令的交换机上设置VLAN具有剪裁资格：

```
Switch(vlan)# vtp pruning
```

在一台基于Cisco IOS命令的交换机上设置某个VLAN不具有剪裁资格，输入如下：

```
Switch(config)#interface fastethernet 0/3
Switch(config-if)# switchport trunk pruning vlan remove vlan-id
```

在一台基于Cisco set命令的交换机上设置某个VLAN具有剪裁资格，输入如下：

```
Console>(enable)set vtp pruneeligible vlan_range
```

在一台基于Cisco set命令的交换机上设置某个VLAN不具有剪裁资格，输入如下：

```
Console>(enable)clear vtp pruneeligible vlan_range
```

10.3 VLAN间路由选择

当一个广播域中的主机想要和另一个广播域中的主机通信时，必须使用路由器。同样的情况也存在于VLAN中。图10-13显示了一个例子。

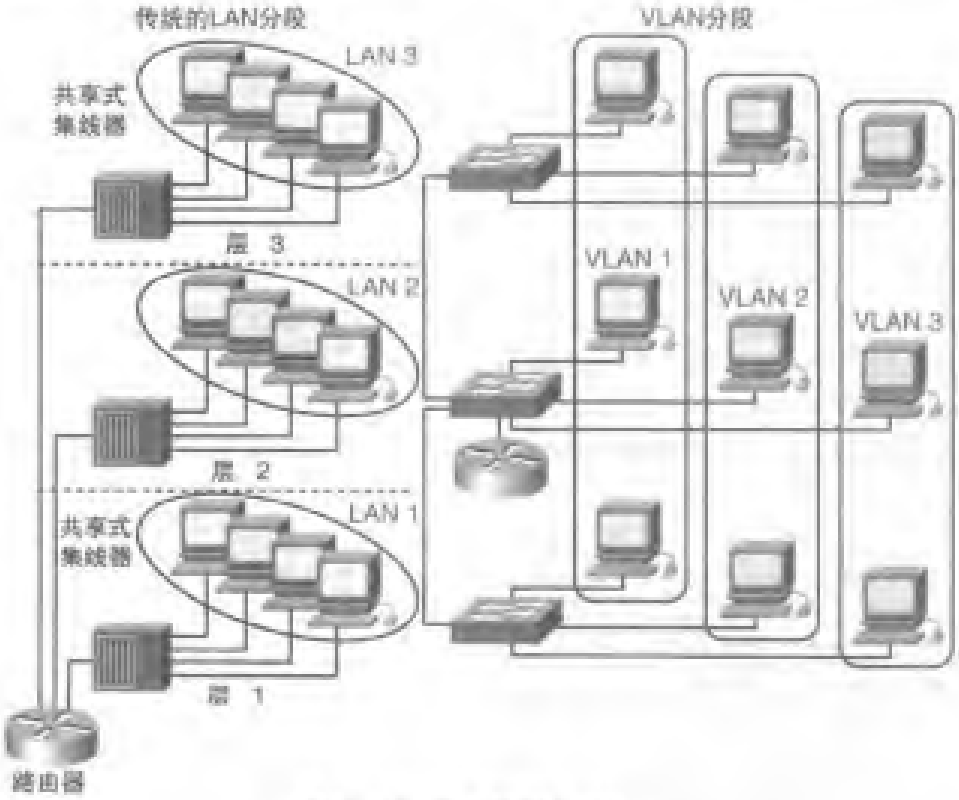


图10-13 路由器和VLAN

交换机的端口1属于VLAN 1，端口2属于VLAN 200。如果交换机的所有端口都属于VLAN 1，那么与这些端口相连的主机就能够相互通信。然而在这个例子中，这些端口属于不同的VLAN：VLAN 1和VLAN 200。如果来自不同VLAN的主机需要通信，则必须使用路由器，如图10-14所示。

路由选择最重要的好处是它已被历史证明能促进于网络，特别是大型网络。尽管Internet是一个最明显的例子，但这一点对任何类型的网络，如大型园区骨干也是正确的。因为路由器禁止广播的传播，并使用比网桥和交换机更智能的转发算法。所以路由器能提供更为有效的带宽利用。这也同时带来了灵活和优化的路径选择。比如，在使用路由选择时，很容易在大多数网络中实施多条路径

上的负载均衡。另一方面，第2层的负载均衡难于设计、实施和维护。

如果一个VLAN跨越多台设备，则用一条中继线互连这些设备。一条中继线可以承载多个VLAN的流量。例如，一条中继线可以连接一台交换机和另一台交换机，连接一台交换机和一台VLAN间路由器，或者连接一台交换机和一台具有支持中继的特殊网络接口卡（NIC）的服务器。

记住，当一个VLAN上的主机想和另一个VLAN上的主机通信时，路由器是必需的。

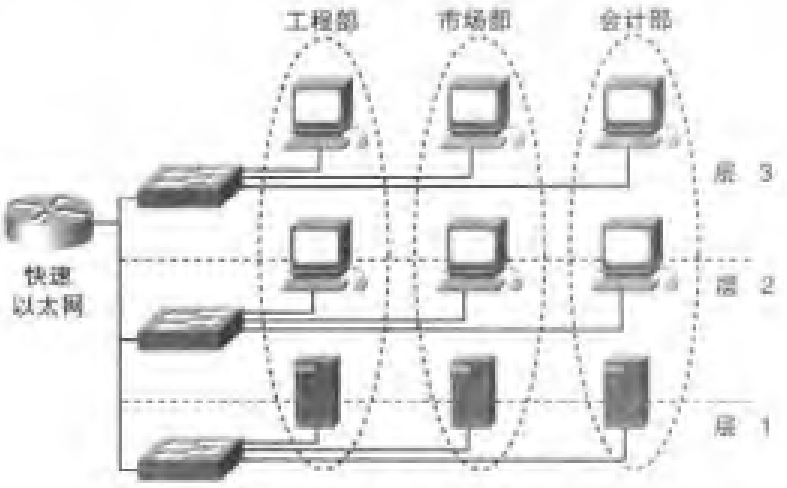


图10-14　去除物理界限

10.3.1　VLAN间的问题和解决方案

连接几个VLAN时，会产生一些技术问题。多个VLAN环境中最常见的两个问题是：

- 终端用户设备到达非本地主机的需要。
- 不同VLAN主机间通信的需要。

当一台设备需要连接一台远程主机时，它会检查它的路由选择表以确定是否存在已知路径。如果这台远程主机属于一个已知如何到达的子网，则系统会检查它能否连接该接口。如果所有已知路径都不成功，系统还有最后一个选择：缺省路由（default route）。该路由是一个特定类型的网关路由，而且通常在系统中是惟一的。在路由器上，一个缺省路由在show ip route命令输出中由一个星号（*）指示。对于局域网上的主机而言，这个网关被设置为与外界直接相连的机器，而且也是工作站TCP/IP设置上显示的缺省网关。如果为一台路由器配置的缺省路由是作为通往公共因特网的网关，那么该缺省路由指向一台Internet服务提供商（ISP）节点的网关机器。使用ip route命令来设置缺省路由，如例10-6所示。

例10-6　ip route命令

```
Router(Config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

例10-6中，192.168.1.1是网关。VLAN间的连通性能够通过逻辑或物理连接实现。逻辑连接包括交换机到路由器的一条单独连接或中继线，该中继线能够支持多个VLAN。这种拓扑被称为“单臂路由器（router on a stick）”，因为到路由器只有一个单独的连接，但是路由器和交换机之间有多个逻辑连接。例如图10-15所示。

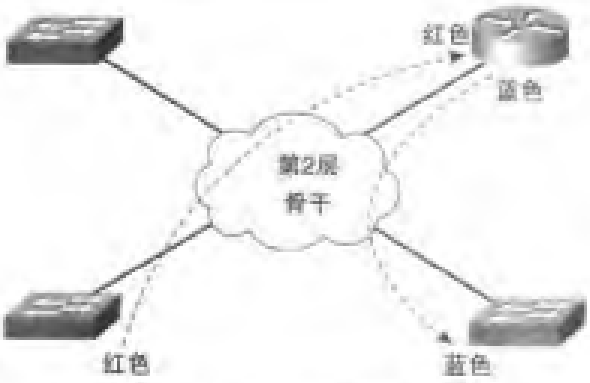


图10-15　单臂路由器

注意：一般而言，在没有其他办法时，用“单臂路由器”作为VLAN间路由选择的方法是最合适的。这并不是说“单臂路由器”设计是一种不好的选择；它只是反映了其他选择能提供更高的吞吐量和功能。并且，因为“单臂路由器”技术用在路由器处于网络边缘（至少连接到第2层网络）的情况下，因此它与园区网的其他部分结合得不太紧。

10.3.2 被隔离的广播域

在交换网络中，路由处理器（Route Processor）负责提供VLAN间的通信。路由处理器通过提供VLAN访问来共享资源以及连接网络中的其他部分。这些部分是用传统子网方式的逻辑网段或者是需要通过广域链路访问的远程站点。路由选择处理器非常像路由器，但它们可以建立在交换机内。它们可以没有物理接口，但它们可以使用与一般路由器相同的IOS命令来配置。

在配置VLAN之间的路由选择之前，必须已经在网络中的交换机上定义了VLAN。与网络设计和VLAN定义相关的问题必须在网络设计阶段得到解决。以下是需要考虑的问题：

- 在VLAN间共享资源。
- 负载均衡。
- 冗余链路。
- 逻辑寻址。
- 使用VLAN对网络进行分段。

图10-16显示了被隔离的广播域。

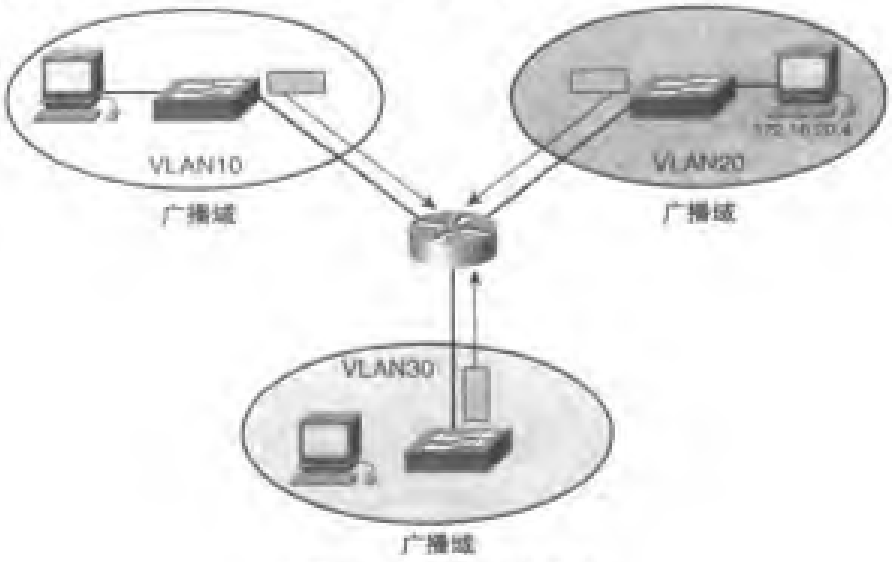


图10-16 隔离的广播域

10.3.3 寻找VLAN间的路由

路由处理器包含大部分的系统存储器部件和主系统处理器。**缺省网关**（default gateway）只是一个路由器接口，通常情况下由一个IP地址来表示。**缺省路由器**（default router）是一台路由器，至少有一个接口作为缺省网关。对DHCP而言，一台缺省路由器就是一台提供一个IP地址池的路由器。图10-17显示了一台缺省网关。

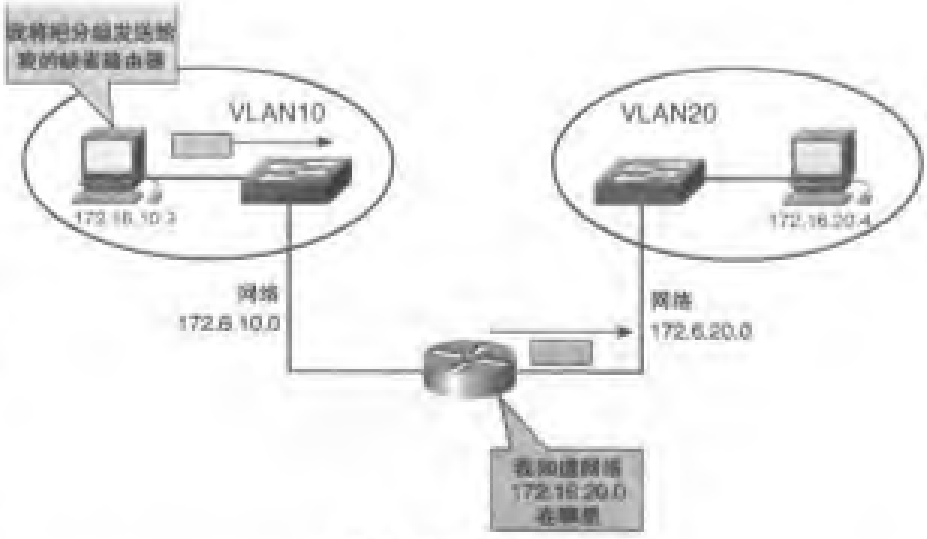


图10-17 缺省网关

在通过路由处理器连接分离的子网时引发了终端用户设备是如何通过多个局域网网段与其他设备通信的问题。有些网络设备使用路由选择表来标识向哪里转发本地网段之外的分组。即使终端用户设备没有责任来路由数据，这些设备仍必须能向子网中的地址而不是它们自己的地址发送数据。

因此，每台终端用户设备不需要管理自己的路由选择表，大多数设备都配置了一个指定路由处理器的IP地址。这个指定路由处理器是发给所有非本地网络分组的缺省路由器。路由处理器再将这些分组转发给相应的目的地。一台网络设备的缺省路由器的IP地址取决于包含这台网络设备的IP子网。

早期的VLAN设计依赖于连接了具有VLAN功能的交换机的外部路由器。在这种方法中，传统路由器通过一条或多条链路连接一个交换网络。“单臂路由器”设计采用一条连接路由器和其余园区网的中继链路。VLAN间的通信必须通过第2层骨干到达路由器，在该处实现VLAN间的移动。然后，

通信通过常规的第2层转发到达要求的终端站点。这种“出路由器再回来”的网络通信是“单臂路由器”设计的特征。

10.3.4　物理和逻辑接口

在传统情况下，一个具有4个VLAN的网络在交换机和外部路由器之间需要4个物理连接。随着像ISL技术的不断普及，网络设计者开始使用中继线链路来连接路由器和交换机。尽管可以使用如ISL、802.1Q、802.10或LAN仿真（LANE）)中任何一种中继技术，基于以太网的方法（ISL和802.1Q）最为常用。Catalyst 2900交换机的缺省方式是802.1Q，而29xx交换机的缺省方式是ISL。

Cisco专有协议ISL在快速以太网链路上中继VLAN。

随着网络中VLAN数量的增加，每个VLAN使用一个路由器接口的物理方法很快变得不可扩展。有多个VLAN的网络必须使用VLAN中继，以为多个VLAN分配单一的路由器接口。

使用中继链路的主要优点是可以节省路由器和交换机端口。不仅节省财力，还可以减少配置的复杂性。因此，用中继线连接路由器的方法比每个VLAN一条链路的设计能扩展到更多数量VLAN。

10.3.5　将物理接口划分为多个子接口

子接口是一个物理接口（如路由器上的快速以太网接口）上的一个逻辑接口。单个物理接口上可以存在多个子接口。

每个子接口支持一个VLAN，并被分配一个IP地址。为了使同一个VLAN上多台设备进行通信，所有设备的IP地址必须在同一个网络或子网中。例如，如果子接口2的IP地址是192.168.1.1，那么192.168.1.2、192.168.1.3和192.1.1.4也是连接到子接口2的设备的IP地址。为了用子接口进行VLAN间的路由，必须为每个VLAN创建一个子接口。

10.3.6　配置VLAN间路由选择

本节主要展示配置路由器和交换机之间的VLAN间路由选择所必需的命令。在实施这些命令之前，要检查每台路由器和交换机分别支持哪种VLAN封装。例如，Catalyst 2950交换机从Cisco IOS 12.0（5.2）WC（1）版本开始支持802.1Q中继，但不支持ISL中继。Cisco路由器从Cisco IOS 12.0（T）版本开始支持ISL和802.1Q中继特性。为了让VLAN间的路由选择正常工作，所有有关的路由器和交换机必须支持相同的封装。

在一台路由器上，一个接口可以被逻辑地划分为多个虚拟子接口（virtual subinterface）。子接口为通过一个物理接口路由选择多个数据流提供了一种灵活的解决方案。要定义一个物理接口上的子接口，执行以下任务：

1. 标识接口。
2. 定义VLAN封装。
3. 为接口分配一个IP地址。

为了标识接口，在全局配置模式下使用interface命令：

```
Router(config)# interface FastEthernet port-number subinterface-number
```

*port-number*标识物理接口，*subinterface-number*标识虚拟接口。路由器必须能够使用标准中继协议与交换机通信。这意味着相连的两台设备都必须理解对方。这个例子中使用了802.1Q。

要定义VLAN封装，在接口配置模式下要输入encapsulation命令：

```
Router(config-if)# encapsulation dot1q vlan-number
```

*vlan-number*标识子接口为之承载流量的VLAN。只有当帧去往非本地网络时，才在帧中加入一

个VLAN ID。每个VLAN分组在分组头中都携带了VLAN ID。

要为接口指定IP地址，可在接口配置模式下输入如下命令：

```
Router(config-if)# ip address ip-address subnet-mask
```

*ip-address*和*subnet-mask*是指定接口的32位网络地址及其掩码。



实验活动 配置VLAN间的路由选择

在本实验中，你将配置一台外部路由器，使之路由一台交换机上的多个VLAN间的流量。

10.4 总结

中继在VLAN网络环境中实施，它允许VLAN在跨越网络的范围内得到扩展。中继一般在交换机之间实施，是通过在参与中继链路的每台交换机上设置至少一个端口为中继模式来实现的。

最常见的两种允许和管理不同VLAN帧通信的中继协议如下：

- ISL
- 802.1Q

VLAN中继协议（VTP）通过维持网络的一致性来减少VLAN网络环境中的一些潜在问题。VTP提供以下好处：

- 整个网络的VLAN配置一致性。
- 允许一个VLAN被中继在混合介质中的映射方案。
- 准确地跟踪和监控VLAN。
- 整个网络中对增加VLAN的动态报告。
- 加入新VLAN时，进行即插即用配置。

当一个VLAN中的一个终端站点需要与另一个VLAN中的终端站点通信时，需要VLAN间的路由选择。

作为本章所学内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

10.5　关键术语

802.1Q　一种中继协议，可以在一根单独的电缆中承载多于一个子网的流量。IEEE 802.1Q委员会定义这种复用VLAN的方法是为了提供多厂商的VLAN支持。

缺省网关（*default gateway*）　一个路由器接口，通常由一个IP地址来表示。

缺省路由器（*default router*）　至少有一个接口作为缺省网关的一台路由器。

交换机间链路（*Inter-Switch Link, ISL*）　Cisco提出的，专有的中继协议，它可以互连多台交换机，并且当流量在交换机间的中继线链路上传输时维护VLAN信息。

路由处理器（*Route processor*）　包含大部分的系统存储器部件和主系统处理器。

子接口（*Subinterface*）　一个物理接口上的众多虚拟接口之一。

中继（*Trunk*）　是两点间（通常是交换中心）的一条独立的传输信道。

中继连接（*Trunking*）　两台交换机之间传输网络流量的一条物理和逻辑连接。一个网络骨干由多条中继线组成。

虚拟局域网（*VLAN, Virtual LAN*）　在一个或多个局域网上的一组设备，它们通过配置（使用管理软件）从而能够像连在同一条电缆上一样进行通信，但实际上它们分布在许多不同的局域网网段上。

VLAN中继协议（*VLAN Trunking Protocol, VTP*）　VTP是一种消息协议，它使用第2层的中继帧来管理一个网络范围中VLAN的添加、删除和重命名。

10.6 复习题

1. 使用中继链路的主要好处是什么?
   A. 为每条中继提供更多的带宽
   B. 有效使用路由器和交换机端口
   C. 允许每个物理端口上有一个单独的VLAN
   D. 降低路由器的开销
2. 哪种协议在一条中继上承载多个VLAN?
   A. 802.2
   B. 802.3
   C. 802.1Q
   D. 802.11B
3. 哪种协议是Cisco专有的并设计用于传输来自多个VLAN的流量?
   A. 802.11A
   B. 802.1Q
   C. VNET
   D. ISL
4. 在一台基于Cisco IOS命令的交换机上创建或配置一条VLAN中继，首先将一个端口配置为中继线，然后指定中继的封装。
   A. 正确
   B. 错误
5. VTP消息是封装在Cisco专有的交换机间链路（ISL）中还是其他类型的帧中?
   A. IEEE 802.1Q协议帧
   B. IEEE 802.1R协议帧
   C. 802.11D协议帧
   D. 802.19协议帧
6. 使用VTP时，Catalyst系列交换机会在其中继端口中通告以下何种信息?
   A. 管理域
   B. 配置修订号
   C. 已知VLAN及其特定参数
   D. 以上所有
7. VTP交换机可以工作在哪种模式下?
   A. 服务器
   B. 客户端
   C. 透明
   D. 以上所有
8. 一个管理域中能运行两种不同版本的VTP：VTP版本1和VTP版本2。这两种版本可以互操作。
   A. 正确
   B. 错误
9. 创建一个管理域，使用哪条命令?
   A. Switch(vlan)# domain Cisco
   B. Switch(vtp)# domain Cisco
   C. Switch(vlan)# vtp domain Cisco

D. Switch(vtp)# vtp domain Cisco

10. 一台交换机的缺省行为是在网络中传播广播和未知的_____？

A. 帧

B. 分组

C. 标记

D. VLAN

11. 在一台VTP服务器上启用VTP剪裁会使得整个_____域启用剪裁？

A. 服务器

B. 透明

C. 管理

D. 用户

12. 在交换网络中，_____是用来提供VLAN间的通信的？

A. 路由处理器

B. 调制器

C. VTP

D. 子网

第三部分　CCNA4：广域网技术

第11章　扩展IP地址
第12章　广域网技术
第13章　点到点协议
第14章　ISDN和DDR
第15章　帧中继
第16章　网络管理介绍



第11章　扩展IP地址

目标

学习完本章之后，你将能够：

- 解释扩展IP地址的必要性。
- 描述NAT术语。
- 描述NAT的特性。
- 区分静态NAT、动态NAT和PAT。
- 配置并验证NAT和PAT。
- NAT和PAT的故障排除。
- 区分BOOTP和DHCP。
- 配置并验证DHCP。
- 描述DHCP术语及其特性。
- DHCP的故障排除。
- 识别并区分公有和私有IP地址。

任何一台连接到因特网的设备都需要一个IP地址。需要IP地址的设备数量在飞速增长，但是可用的IP地址数量是有限的。本章将探讨IP地址空间耗尽的问题，以及已经提出的一些有助于减轻IP地址扩展问题的解决方案。这里介绍的解决方案包括网络地址转换（NAT, Network Address Translation）、端口地址转换（PAT, Port Address Translation）、动态主机配置协议（DHCP, Dynamic Host Configuration Protocol）和私有IP地址的使用。你将学习如何在路由器上配置、验证NAT和DHCP以及如何对它们进行故障排除。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图。光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

11.1　Internet协议（IP）概述

IP协议是一种连接协议的选择。IP的应用发展迅速，这意味着更多的主机可以连接到因特网。在因特网发展初期，PC、工作站、服务器和路由器是连接到因特网的仅有的几种设备。管理员静态分配IP地址。

今天，PDA、便携机、台式机、主机、存储设备、路由器、交换机、视频游戏控制台和安全摄

影机都连接到了因特网。甚至有关于将家庭器具接入因特网的讨论。可以非常明显地看到，如果没有扩展方案，因特网的革命将很快达到其极限。

近几年已经实现了几种扩展方案，包括可变长度子网掩码（VLSM, Variable-length subnet mask）、无类域间路由选择（CIDR, Classless interdomain routing）和IP协议第6版（IPv6）。本章将描述其他3种IP地址扩展问题的解决方案：私有寻址（private addressing）（RFC 1918）、地址转换（address translation）（NAT与PAT）和地址池（address pooling）（DHCP）。

本章描述IP地址扩展问题的解决方案。

今天的因特网面临着两个扩展性挑战：

- 注册IP地址空间将要耗尽，而因特网的规模仍在持续增长。
- 随着因特网的增长，骨干因特网路由选择表中的IP路由数量也在增加。这引发了路由选择算法的扩展问题。

IP扩展解决方案如下：

- NAT
- DHCP
- RFC 1918（私有IP寻址）

NAT是一种节约大型网络中注册IP地址并简化IP寻址管理任务的机制。NAT已经标准化并在RFC 1631中描述。

当一个分组经过一台Cisco IOS NAT的路由器进行路由时，路由器将该分组中的源IP地址从一个私有的内部网络地址转换为一个合法的IP地址，这样该分组就可以在公共的外部网络（例如因特网）上传送。返回通信的地址被转换回来以便在内部网络上传送。本章将在后面详细讨论NAT。

因特网在爆炸性的增长，而且看不出有减缓的迹象。管理员必须给接入因特网的主机分配IP地址、缺省网关和其他一些必要的信息。DHCP帮助管理员动态地为设备分配IP地址。

随着全球因特网的腾飞，很多组织希望使用IP来连接，但又不希望他们所有的主机都暴露给因特网。RFC 1918通过定义公有和私有IP地址空间来处理这一问题。

因特网分配编号委员会（IANA, Internet Assigned Numbers Authority）保留了3块IP地址，如表11-1所示。RFC 1918描述了如何最佳的使用这些地址。

表11-1 RFC1918地址

Class	RFC 1918内部地址范围	CIDR前缀
A	10.0.0.0~10.255.255.255	10.0.0.0/8
B	172.16.0.0~172.31.255.255	172.16.0/12
C	192.168.0.0~192.168.255.255	192.168.0.0/16

这3段范围提供了超过1700万个私有地址（private address）。私有（private）意味着它们不允许被路由到公共的因特网，但在组织内部可以按照需要自由的使用它们。因此，这些地址被认为是不可路由的（non-routable）。

IPv4和IPv6地址都以授权的方式进行分配。Internet服务提供商（ISP）为用户分配IP地址。ISP从本地因特网注册局（LIR, Local Internet Rogistry）或国家因特网注册局（NIR, National Internet Registry）或适当的地区因特网注册局（RIR, regional Internet Registy）获得IP地址。这些机构包括亚太网络信息中心（APNIC）、美洲因特网编号注册局（ARIN）、拉丁美洲及加勒比地区IP地址注册局（LACNIC）或欧洲地区IP地址注册局（RIPE NCC）。

任何人都可以使用保留的私有IP地址。这意味着两个网络或者两百万个网络都可以使用相同的私有地址。在公共的因特网上永远都不会看到RFC 1918地址，一台公共的因特网路由器也决不会路由这些地址，因为ISP一般会配置他们的路由器来阻止转发私有寻址的用户数据流。

如果为一个非公共的企业内连网、一个测试实验室或一个家庭网络寻址，就可以使用这些私有

地址而不是那些全球惟一的地址。全球地址必须花钱从提供商或注册机构那里获得。

RFC 1918地址也已经在产品化网络中找到了位置。通过VLSM，可以将一个C类网络地址空间中剩余的某一子网进一步划分子网。尽管这种解决办法比在一个只有两台主机的广域网链路上浪费掉一个可以容纳30台主机的子网要好得多，但是它仍然花费了一个可用于未来扩展的子网。浪费较少的一种解决方案是在广域网链路中使用私有网络地址。在图11-1中，广域网链路地址使用私有地址空间10.0.0.0/8中的子网来寻址。

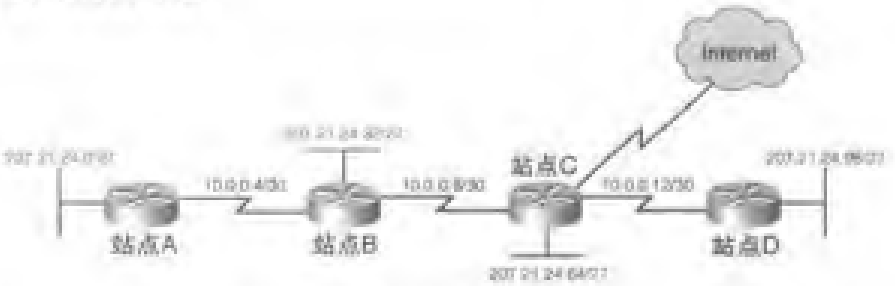


图11-1 在广域网中使用私有地址

如果站点A、B、C和D的局域网用户希望访问因特网，这些路由器如何使用私有地址呢？在这些站点下的终端用户应该没有问题，因为他们使用网络207.21.24.0中的全球惟一地址。路由器仅在转发数据流和交换路由选择信息的时候才使用其串行接口上的私有地址。上游的提供商和因特网中的路由器只看到分组中的源和目的IP地址，他们不在乎分组是否在某个点上经过了使用私有地址的链路。事实上，许多提供商在他们网络的核心中使用RFC 1918网络地址，以避免耗尽他们所提供的全球惟一地址。

在广域网链路上使用私有地址的一个条件是这些串行接口不能是去往因特网的通信的起始源，或者是来自因特网的通信的最终目的。路由器通常不会花时间在web上冲浪，因此这个限制通常只在使用ICMP进行故障排除或使用SNMP，又或者是通过因特网使用Telnet进行远程连接时才会成为问题。在这些情况下，路由器只能通过其全球惟一的局域网接口地址进行寻址。

NAT为单个公司和因特网提供了极大的好处。在NAT之前，一个具有私有地址的主机不能访问因特网。有了NAT后，单个公司可以使用私有地址对他们的部分或全部主机进行寻址，然后使用NAT访问公共的因特网。同时，这些主机连接到因特网并不需要消耗地址空间。

11.2 NAT和IPAT

NAT是对IP分组报头中的地址进行操作的过程，它将IP报头中的目的地址、源地址或这两个地址替换为管理员分配的不同地址。运行专门的NAT软件或硬件的设备执行这一替换过程。Cisco IOS NAT设计用来简化并节约IP地址，因为它允许使用未注册IP地址的私有IP互连网通过将这些地址转换为全球注册IP地址，从而接入因特网。Cisco IOS NAT通过对外部网络隐藏了内部IP地址也增加了网络的秘密性。

采用NAT的设备通常运行在存根网络（stub network）的边界。存根网络是只有一条到其邻居网络连接的网络。图11-2显示了存根网络的一个简单例子。当存根网络中的一台主机想要向外部主机传输

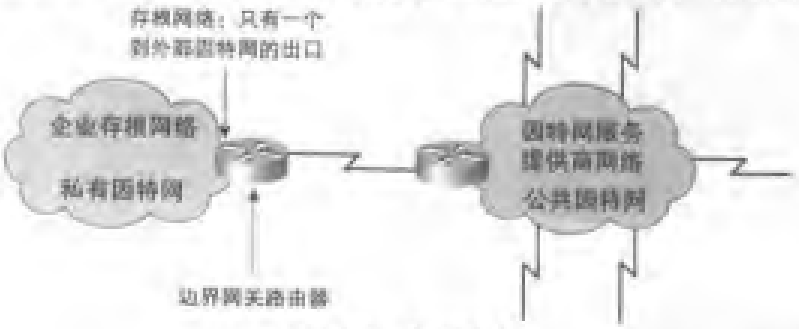


图11-2 存根网络

时，它将分组转发到它的边界网关路由器。在这种情况下，主机的边界网关路由器也是NAT转换器。

NAT运行在一台Cisco路由器上，通常连接两个网络，它在分组被转发到另一个网络之前将内部网络中的私有（内部本地）地址转换为公共（内部全球）地址，如图11-3到图11-5所示。

一台内部主机（10.0.0.2）想与一台外部主机（128.23.2.2）通信。它将分组发送给它的网关RTA，如图11-3所示。

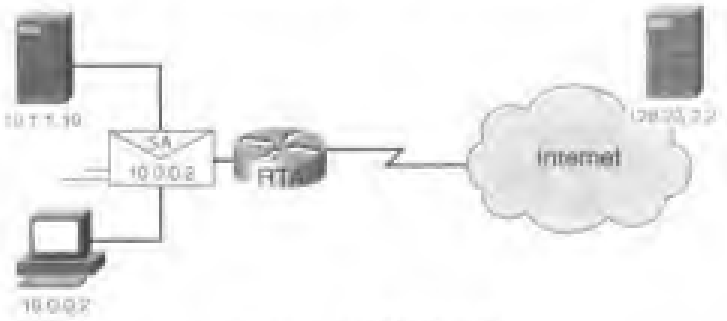


图11-3　NAT如何工作

RTA发现分组要路由到外部的因特网。NAT进程选择一个全球惟一的IP地址（179.9.8.80）替换分组源地址字段中的本地地址。然后将本地到全球地址的映射存储在NAT表中，如图11-4所示。

分组被路由到它的目的地。在这个客户-服务器环境中，服务器可能响应一个分组，该分组将以全球地址（179.9.8.80）返回到RTA，如图11-5所示。

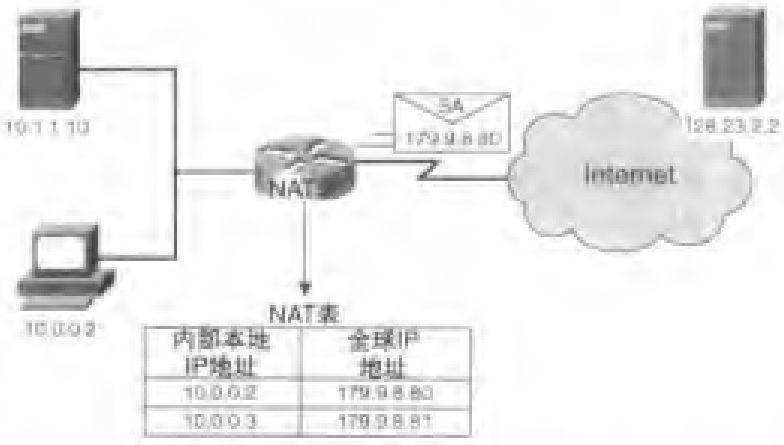


图11-4　NAT如何工作：NAT表

在图11-6中，NAT进程看到一个分组要从外部路由到内部，于是在NAT表中查找该全球地址到本地地址的映射，然后用本地地址替换分组目的地址字段中的全球地址，并将分组转发到内部。

在NAT术语中，内部网络（inside network）是需要被翻译的一组网络。外部网络（outside network）则是所有的其他地址，通常是位于因特网上的合法地址。

NAT的功能之一是其可以配置为将整个网络向外部世界通告为一个地址。这有效的对外部世界隐藏了内部网络，并提高了安全性。NAT的这种特性叫做静态PAT（Static PAT），如图11-7和11-8所示。在Cisco IOS配置中PAT也被称做超载（overload）。使用NAT可以对多个外部地址进行转换，而使用PAT能使用一个或少量的外部地址。在图11-7中，主机10.0.0.2和10.0.0.3使用一个公共IP地址179.9.8.80发送分组到外部世界。路由器通过在外部IP地址后附加一个惟一的源端口号来跟踪每台主机的分组。

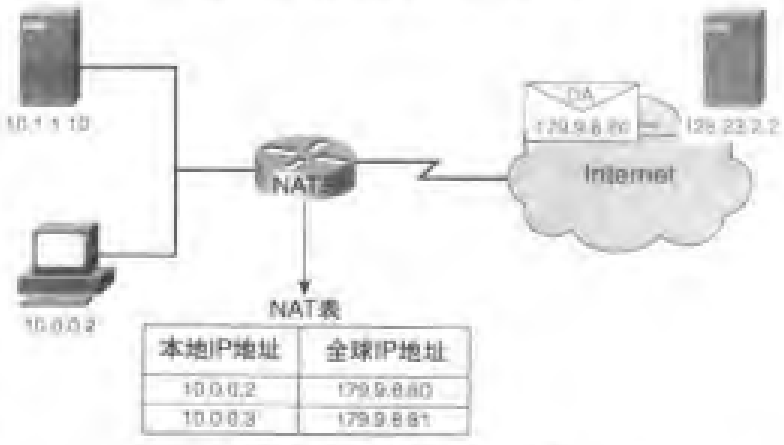


图11-5　NAT如何工作：应答

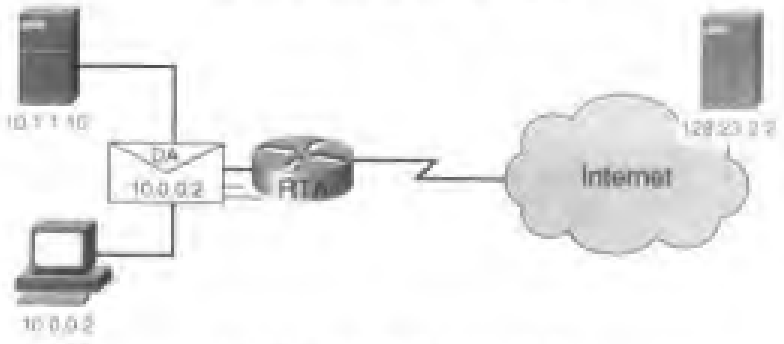


图11-6　NAT如何工作：结果

PAT使用全球IP地址中的惟一源端口号来区分不同的转换。因为端口号是16位编码，所以使用PAT时所有被转换为同一个外部地址的内部地址总数在理论上可以有65,536个。

PAT试图保持原始的源端口。如果这个源端口已经被分配，PAT将试图在适当的端口组0~511、512~1,023和1,024~65,535中从前至后查找第一个可用端口。如果在适当的端口组中没有可用的端口，并且配置了多个外部地址，PAT将移至下一个IP地址，并试图再次分配原始的源端口。这一过程一直持续到PAT用完可用的端口和外部IP地址。

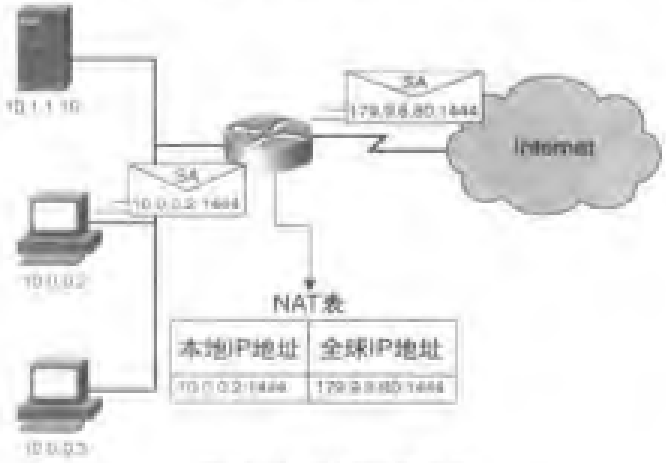


图11-7 PAT如何工作

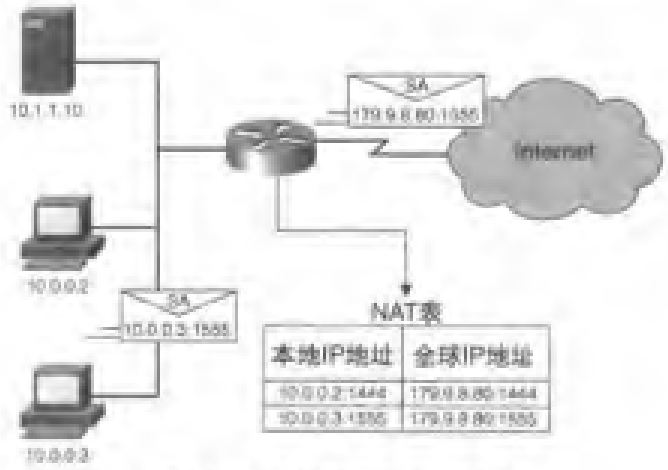


图11-8 PAT如何工作：结果

11.2.1 NAT和PAT的特性

NAT可以动态或者静态的发生，可以因为各种各样的目的来使用它。静态NAT设计用来允许本地和全球地址的一一映射，如图11-9所示。这种方式对于那些必须能够被因特网访问的内部IP主机特别有用，例如DNS服务器或电子邮件服务器。

动态NAT设计用来将一个未注册IP地址映射到一组注册IP地址中的某一个注册IP地址，如图11-10所示。

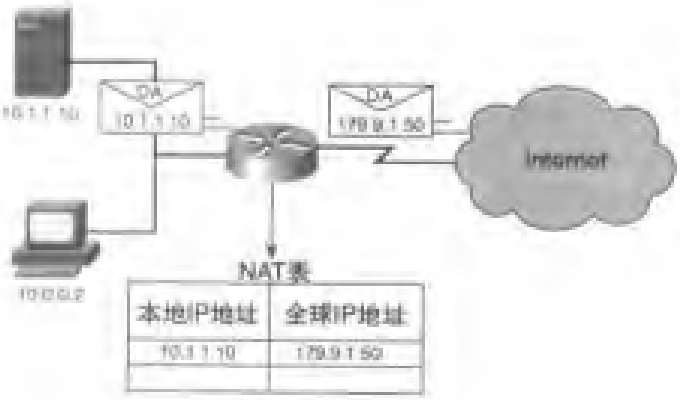


图11-9 静态NAT

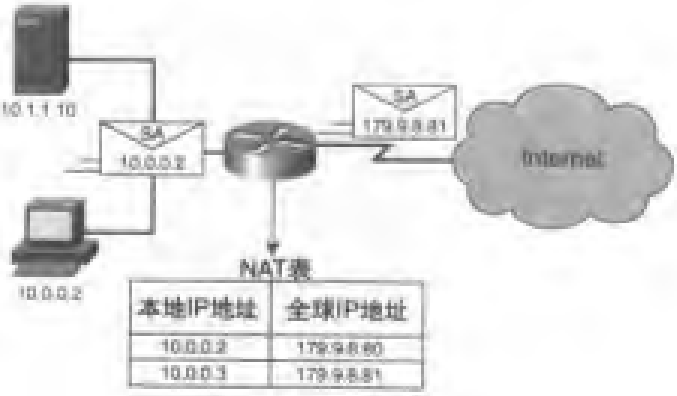


图11-10 动态NAT

Cisco定义了如下的NAT术语：

- 内部本地地址（*Inside local address*）——分配给内部网络中一台主机的IP地址，可以是一个RFC 1918私有地址。
- 内部全球地址（*Inside global address*）——由地区因特网注册局（RIP）或服务提供商分配的一个合法IP地址，它将对外代表一个或多个内部本地IP地址。
- 外部本地地址（*Outside local address*）——为内部网络主机所知的一台外部主机的IP地址。
- 外部全球地址（*Outside global address*）——外部网络的某台主机拥有者分配给该主机的IP地址。

NAT提供了如下好处：

• **消除了重新寻址的开销，例如在更换ISP时**——需要外部访问时不再需要重新分配所有主机的地址，节省了时间和金钱。

• **通过应用端口级的复用节约了地址**——使用NAT，内部主机可以共享一个注册IP地址进行所有的外部通信。在这种配置方式下，只需要相对较少的外部地址就可以支持大量的内部主机，节约了IP地址。

• **保护网络安全**——因为私有网络并不通告它们的地址或内部拓扑，所以当他们与NAT一起使用以获取受约束的外部访问时，仍然保持了相当的安全。

11.2.2　配置NAT和PAT

本小节包含如下配置主题：

• 静态转换。

• 动态转换。

• 超载NAT（PAT）。

1　静态转换

静态转换发生在明确地配置了查找表中的地址时。将一个特定的内部本地地址映射到一个预设的内部全球地址上。内部本地和内部全球地址被静态的一一映射起来。这意味着对于每一个内部本地地址，静态NAT都需要一个内部全球地址。为了配置静态内部源地址转换，执行表11-2中描述的任务。

表11-2　配置静态NAT

步骤	动　作	注　释
1.	建立一个内部本地地址与一个内部全球地址间的静态转换 Router(config)# ip nat inside source static local-ip global-ip	输入全局命令no ip nat inside source static可以取消静态源地址转换
2.	指定内部接口 Router(config)# *interface type number*标记该接口为连接内部网络的接口 Router(config-if)# ip nat inside	输入interface命令后，CLI提示符将由(config)# 变为 (config-if)#
3.	指定外部接口 Router(config-if)# interface type number标记该接口为连接外部网络的接口 Router(config-if)# ip nat outside	

直接将静态转换输入到配置中，它们会显示在转换表中。例11-1给出了Cisco IOS路由器的命令。

例11-1　配置静态NAT

```
Router(config)#ip nat inside source static 10.1.1.2 192.168.1.2
Router(config)#interface s0
Router(config-if)#ip nat outside
Router(config-if)#interface e0
Router(config-if)#ip nat inside
```

图11-11显示了静态NAT的使用。路由器将来自主机10.1.1.2的分组源地址转换为192.168.1.2。例11-2提供了网关的配置。



图11-11 静态NAT实例

例11-2 网关配置

```
hostname GW
!
ip nat inside source static 10.1.1. 2 192.168.1.2
!
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!
interface Serial0
 ip address 192.168.1.1 255.255.255.0
 ip nat outside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

2 动态转换

使用动态NAT，在路由器收到需要转换的通信之前NAT表中不存在转换。（管理员定义这些流量。）动态转换是临时的，它们最终会超时。为了配置动态内部源地址转换，执行表11-3中显示的任务。

表11-3 配置动态NAT

步骤	动 作	注 释
1.	根据需要定义一个供分配的全球地址池 Router(config)# ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}	输入全局命令no ip nat pool删除全球地址池
2.	创建一个访问控制列表来标识要转换的主机 Router(config)# access-list access-list-number permit source [source-wildcard]	输入全局命令no access-list access-list- number删除访问控制列表
3.	配置基于源地址的动态NAT Router(config)# ip nat inside source list access-list number pool name	输入全局命令no ip nat inside source取消动态源地址转换
4.	指定内部接口 Router(config)# interface type number Router(config-if)# ip nat inside	输入interface命令后，CLI提示符将由（config)#变为(config-if)#
5.	指定外部接口 Router(config)# interface type number Router(config-if)# ip nat outside	

动态转换要指定内部地址能被转换成的全球地址池，如例11-3所示。

例11-3 配置动态NAT

```
Router(config)# ip nat pool nat-pool 179.9.8.80 179.9.8.95
netmask 255.255.255.0 255.255.255.240
```

访问控制列表必须只允许那些要被转换的地址。记住，在每个访问控制列表的末尾都存在一条隐含拒绝所有的条目。一个访问控制列表如果有过多的许可将导致不可预料的结果。Cisco强烈建议不要在NAT命令所引用的访问控制列表中使用允许所有（permit any）。使用允许所有会导致NAT消耗过多的路由器资源，从而引起网络问题。

以下命令配置了适当的接口来担当内部和外部接口的角色：

```
Router(config)#interface s0
Router(config-if)#ip nat outside
Router(config-if)#interface e0
Router(config-if)#ip nat inside
```

图11-12中将通过访问控制列表1（源地址来自10.0.0.0/16）的所有源地址转换为地址池nat-pool中的地址。地址池所包含的地址范围从179.9.8.80/28到179.9.8.95/28。

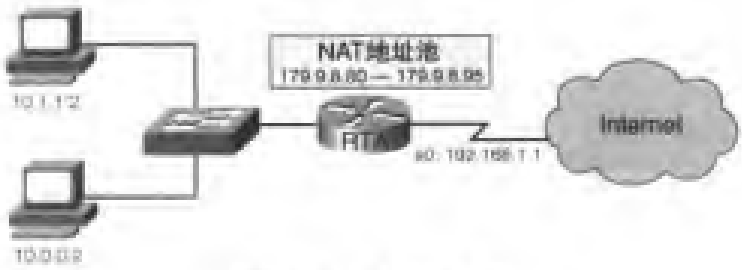


图11-12　PAT的例子

RTA的配置如例11-4所示。

例11-4　RTA的配置

```
<output omitted>
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface fastethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat outside
!
```

注释：NAT不会转换主机10.1.1.2，因为访问控制列表不允许它被转换。

3　超载NAT

NAT路由器最强大的特性之一就是能够使用PAT。这有时被称为“多对一”NAT，或者叫地址超载（address overloading）。使用地址超载，数以百计的私有地址节点可以使用一个全球地址访问因特网。NAT路由器通过对转换表中的TCP和UDP端口号进行映射来区分不同的会话。

为了配置内部全球地址超载，执行表11-4所示的任务。

表11-4　配置NAT复用

步骤	动　作	注　释
1.	定义一个标准访问控制列表来允许那些被转换的地址 Router(config)# *access-list access-list-number* permit *source* [*source-wildcard*]	输入全局命令no *access-list access-list-number* 删除访问控制列表

续表

步骤	动 作	注 释
2.A	建立动态源转换，指定上一步所定义的访问控制列表。 Router(config)# ip nat inside source list *access-list-number* interface *interface* overload	输入全局的no ip nat inside source命令取消动态源转换。关键字overload用来启用PAT
2.B	指定用于超载的全球地址（作为一个池） Router(config)# ip nat pool *name ip-address* {netmask *netmask* | prefix-length *prefix-length*}建立复用转换 Router(config)# ip nat inside source list *access-list-number* pool *name* overload	
3.	指定内部接口 Router(config)# interface *type number* Router(config-if)# ip nat inside	输入interface命令后，CLI提示符将由(config)#变为(config-if)#
4.	指明外部接口 Router(config)# interface *type number* Router(config-if)# ip nat inside	

定义一个标准IP访问控制列表以允许转换内部本地地址，如例11-5所示。

例11-5 标准IP访问控制列表

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255
```

建立超载转换，指定被超载的IP地址为分配给一个外部接口的IP地址，如例11-6所示。

例11-6 接口的超载

```
Router(config)# ip nat inside source list 1 interface serial0/0 overload
```

建立复用转换，指定被复用的IP地址为分配给一个地址池名的IP地址，如例11-7所示。

例11-7 地址池的超载

```
Router(config)# ip nat pool nat-pool2 179.9.8.20 netmask 255.255.255.240
Router(config)# ip nat inside source list 1pool nat-pool2 overload
Router(config)# interface s0
Router(config-if)# ip nat outside
Router(config-if)# interface ethernet 0
Router(config-if)# ip nat inside
```

实验活动 配置NAT

在本实验中，你将配置一台路由器使用NAT将内部私有IP地址转换为外部公共地址。

实验活动 配置PAT

在本实验中，你将配置一台路由器使用PAT将内部私有IP地址转换为外部公共地址。

实验活动 你将配置静态NAT地址

在本实验中，配置一台路由器使用PAT将内部私有IP地址换为外部公共地址。同时配置静态IP映射以允许从外部访问一台内部PC。

11.2.3　验证NAT和PAT的配置

配置完NAT之后，使用clear和show命令验证它是否按期望的那样运行。

在缺省情况下，NAT表中一段时间后不使用的动态地址转换将会超时。没有配置端口转换时，转换表条目的超时时间是24小时，除非用ip nat translation命令重新配置。可以使用表11-5中的命令之一在超时之前清除表的条目。

表11-5　清除NAT表项的命令

命　令	描　述
clear ip nat translation *	从NAT转换表中清除所有的动态地址转换表条目
clear ip nat translation inside *global-ip local-ip* [outside *local-ip global-ip*]	清除一条包含内部转换或内部与外部转换的简单动态转换表条目
clear ip nat translation protocol inside *global-ip global-port local-ip local-port* [outside *local-ip local-port global-ip global-port*]	清除扩展动态转换表条目

在EXEC模式下执行表11-6中所示的任务之一可以显示转换信息。

表11-6　显示转换信息的命令

命　令	描　述
show ip nat translations	显示当前活动的转换
show ip nat statistics	显示转换统计信息

也可选择使用show run命令查看NAT、访问控制列表、接口或地址池命令中的需要值。



实验活动　验证NAT和PAT配置

在本实验中，你将使用clear和show命令验证NAT和PAT是否运行正常。

11.2.4　NAT和PAT配置的故障排除

在NAT环境中出现IP连通性问题时，通常很难确定问题原因。很多时候，NAT被误认为有错，但事实上是下层的问题。

当你试图确定IP连通性问题的起因时，排除NAT是有帮助的。遵循以下步骤检验NAT是否正按预想的运行：

步骤1　根据配置，清楚地定义NAT应该完成的内容。

步骤2　验证转换表中存在正确的转换。

步骤3　使用show和debug命令验证转换的发生。

步骤4　仔细查看对分组的操作，验证路由器具有正确的路由选择信息来传送分组。

使用debug ip nat命令，通过显示由路由器转换的每个分组的信息，来验证NAT特性的操作。debug ip nat detailed命令为每个被认为要转换的分组产生一个描述。这条命令也输出某些错误和意外状况的信息，例如分配一个全球地址失败。

例11-8显示了针对图11-13中的网络使用debug ip nat的输出例子。在这个例子中，调试输出的前两行是域名系统（DNS）的请求和应答过程。调试输出的剩余行是内部网

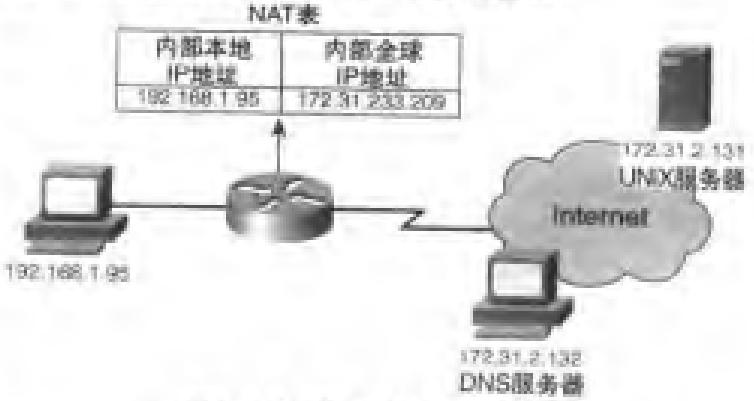


图11-13　使用NAT debug命令

络中一台主机到外部网络中一台主机的Telnet连接。

例11-8 debug ip nat输出

```
Router#debug ip nat

NAT:s=192.168.1.95->172.31.233.209,d=172.31.2.132[6825]
NAT:s=172.31.2.132,d=172.31.233.209->192.168.1.95[21852]
NAT:s=192.168.1.95->172.31.233.209,d=172.31.1.161[6826]
NAT*:s=172.31.1.161,d=172.31.233.209->192.168.1.95[23311]
NAT*:s=192.168.1.95->172.31.233.209,d=172.31.1.161[6827]
NAT*:s=192.168.1.95->172.31.233.209,d=172.31.1.161[6828]
NAT*:s=172.31.1.161,d=172.31.233.209->192.168.1.95[23313]
NAT*:s=172.31.1.161,d=172.31.233.209->192.168.1.95[23325]
```

debug输出信息的解释如下：

- **NAT***——NAT后跟一个星号（*）表示转换是在快速交换路径上进行的。一个会话中的第一个分组总是通过低速路径（也就是处理交换）。如果缓存条目存在，剩余的分组就通过快速交换路径。
- **s=***a.b.c.d*——a.b.c.d是源地址。
- *a.b.c.d* **->***w.x.y.z*——w.x.y.z是源地址被转换到的地址。
- **d=***a.b.c.d*——a.b.c.d是目的地址。
- **[23325]**——方括号中的数字是IP标识号。这些信息对调试非常有用，因为它可以跟踪与之相关的其他分组，例如通过协议分析器。



实验活动 NAT和PAT配置的故障排除

在本实验中，你将使用show和debug命令进行NAT和PAT配置的故障排除。

11.2.5 NAT的优点和缺点

NAT包括以下一些优点：

- NAT通过内部网的私有化来节约合法的注册寻址方案。
- NAT增加了连接到公共网络的灵活性。多个地址池、备份地址池以及负载共享/均衡地址池的实现有助于保证可靠的公共网络连接。
- 网络的非私有化需要对现有网络进行重新寻址；其代价与需要转变到新寻址方案的主机数量相关。NAT允许保留现有方案，并同时支持私有网络以外的新的地址分配方案。

NAT并不是没有缺点。地址转换的代价是失去了一些功能，特别是对那些在IP有效载荷中发送IP地址信息的协议和应用。这需要NAT转换器的附加支持。NAT的缺点如下：

- NAT增加了延迟。交换路径延迟的引入是因为需要转换分组头中的IP地址。由于NAT普遍使用处理交换来实现，因此需要考虑性能。CPU必须查看每个分组以决定是否需要转换，然后改变IP报头——可能还有TCP报头。这一过程不太可能容易进行高速缓存。
- 实现和使用NAT时的一个重大缺点是丧失了端到端的IP追踪能力。当分组在多个NAT跳上经历了许多次的分组地址转换后，要跟踪该分组是非常困难的。当然这种情况也导致了更安全的链路，因为电脑黑客将很难确定分组的源，甚至不可能跟踪或获得初始的源或目的地址。
- NAT也迫使一些使用IP寻址的应用无法工作，因为它隐藏了端到端的IP地址。那些使用物理地址而非符合要求的域名的应用将无法到达那些经过NAT路由器转换的目的地。有时，可以通过实现

静态NAT映射来避免这一问题。

• NAT支持那些在应用数据流中没有携带源或目的IP地址的TCP/UDP流量，例如HTTP、TFTP和Telnet。

尽管下面的通信类型在应用数据流中携带有IP地址，但是Cisco IOS NAT支持这些应用：

• ICMP。
• 文件传输协议（FTP）（包括PORT和PASV命令）。
• TCP/IP上的NetBIOS（数据报、名称和会话服务）。
• Progressive Networks的RealAudio。
• White Pines的CuSeeMe。
• Xing Technologies的Streamworks。
• DNS的“A”和“PTR”查询。
• NetMeeting（2.1、2.11和3.01）。
• H.323v2［除RAS外的H.225/245消息类型——IOS版本12.1(5)T］。
• VDOLive［IOS版本11.3(4)/11.3(4)T以后］。
• Vxtreme［IOS版本11.3(4)/11.3(4)T以后］。
• IP多播［IOS版本12.0(1)T］（只支持源地址转换）。

Cisco IOS NAT不支持以下流量类型：

• 路由选择表更新。
• DNS区传输。
• BOOTP。
• talk, ntalk。
• 简单网经管理协议（SNMP）。
• NetShow。

11.3 DHCP概述

路由器、服务器和其他关键节点通常需要一个特定的IP配置。但是，桌面客户却不需要一个特定的地址，而是一段地址范围中的任意一个。这个范围通常在一个IP子网内。一个特定子网内的桌面客户可以使用该范围内的任意一个地址，其他值则为缺省值。这些缺省值包括该子网或网络的子网掩码、缺省网关和DNS服务器地址。

配置一台连接到TCP/IP因特网的主机需要以下几个值：

• 一个IP地址。
• 一个子网掩码。
• 一个缺省网关。
• 一个DNS服务器地址。

这个列表是最小配置，也许根据网络环境还需要其他变量。这些变量一般可以手动配置到每台IP主机里。它们通常存储在一个配置文件中，计算机启动时访问该文件。

另外，有些客户是没有磁盘的；操作系统和软件存储在ROM中。ROM芯片制造厂商在生产时并不知道IP配置值；因此，你不能配置这些值。这些配置必须在启动后提供。在这种环境下，可以在IP主机启动时动态分配这些IP值。DHCP设计用来执行这个特殊任务。因为桌面客户通常包含大量的网络节点，DHCP对系统管理员来讲是一个好消息。

11.3.1 DHCP介绍

DHCP工作在客户/服务器模式中，允许一个IP网络上的主机（DHCP客户）从一台服务器上（DHCP服务器）获得它们的配置。这减轻了管理一个IP网络所需的工作。客户从服务器接收到的最重要的配置选项是它的IP地址。RFC 2131描述了DHCP协议。

DHCP客户是大多数现代操作系统的一部分，包括Window 9x/NT/2000/XP，Solaris，Linux和MAC OS。客户部分从网络上请求配置值。网络中必须有一台DHCP服务器，用来管理IP配置值的分配并响应来自客户的请求。DHCP服务器可以负责响应多个子网的请求。DHCP并非打算用来配置路由器、交换机和服务器，因为这些主机需要静态IP地址。

DHCP的工作是通过配置一台服务器来为客户分配IP信息。客户在管理定义的周期内租用来自服务器的信息。当租用期满时，客户必须请求另外一个地址，尽管该客户通常又会重新分配到相同的地址。

管理员通常喜欢使用Microsoft NT/2000/XP服务器或UNIX计算机来提供DHCP服务，因为这些解决方案可扩展，并且相对容易管理。虽然如此，Cisco IOS的一个特性集（Easy IP）提供了可选的，用一台路由器作为具有全部特性的DHCP服务器。它的缺省租用配置为24小时。这个特性在小型办公室和家庭办公室中非常有用，这些办公室可以利用DHCP和NAT，而不需要一台基于计算机的服务器。

管理员设置DHCP服务器从预定义的池中分配地址。DHCP服务器还可以提供其他信息，例如DNS服务器地址、WINS服务器地址和域名。另外，大多数的DHCP服务器允许管理员明确定义可以服务的客户MAC地址，并每次自动为它们分配相同的IP地址。

DHCP客户发送一条携带有DHCP请求分组的直接IP广播。在最简单的情况下，位于同一网段中的一台DHCP服务器会接收这个请求。图11-14、11-15和11-16图示了DHCP的请求/应答过程。服务器注意到GIADDR字段为空，所以客户在同一网段中。服务器还注意到请求分组中的客户硬件地址，如图11-14所示。

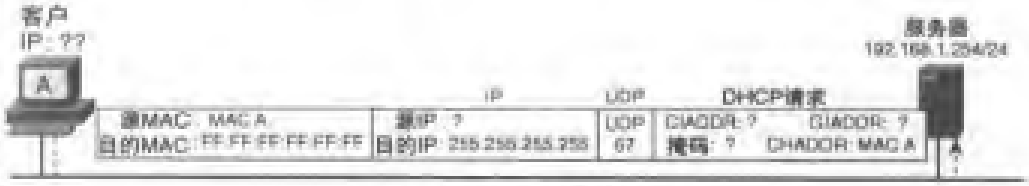


图11-14 DHCP启动过程

DHCP服务器从该网段的可用池中挑选一个IP地址和全局参数。然后，DHCP服务器把它们放入DHCP分组中的适当字段。服务器使用硬件地址A（在CHADDR中）来构建一个合适的帧，将其返回给客户，如图11-15所示。

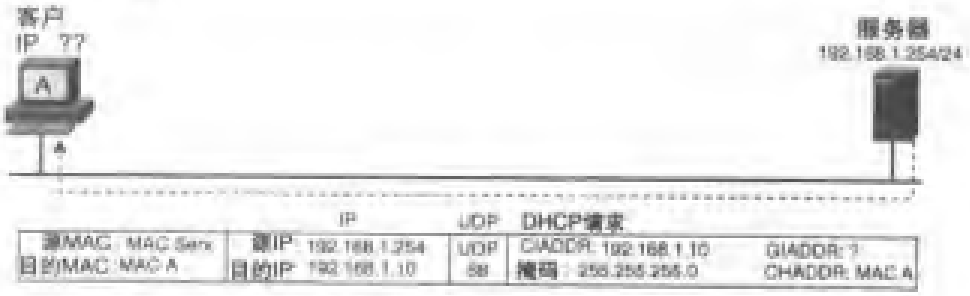


图11-15 DHCP服务器应答

DHCP客户操作系统使用DHCP应答中的值来配置客户的IP协议栈，如图11-16所示。

DHCP使用UDP作为它的传输协议。客户在端口67上向服务器发送消息，而服务器在端口68上

向客户发送信息。



图11-16 DHCP完成

11.3.2 BOOTP和DHCP的区别

因特网团体首先开发了自举协议（BOOTP, Bootstrap Protocol）来配置网络上的无盘客户。BOOTP最初定义在1985年的RFC 951中。作为DHCP的前身，BOOTP具有一些与DHCP相同的操作特点。两种协议都是基于客户-服务器的，都使用UDP端口67和68，它们被称为BOOTP端口，因为BOOTP出现在DHCP之前。

BOOTP提供先前提及的4个基本IP参数。但是，BOOTP不是动态的。当一个客户请求一个IP地址时，BOOTP服务器搜索一个预先定义的条目，查找和客户MAC地址匹配的条目。如果该条目存在，该条目对应的IP地址便会返回给客户。这意味着IP地址和MAC地址间的绑定必须已经在BOOTP服务器上配置好了。

DHCP定义了一种机制，该机制允许为客户分配一个具有有限租期的IP地址，允许稍后将该IP地址重新分配给另外一个客户，或者在客户移动到另一个子网中时为其进行重新分配。客户可以更新租期来保持相同的IP地址。

DHCP为客户提供一种收集其运行在TCP/IP网络上所需的其他IP配置参数（WINS和域名）的机制。表11-7提供了DHCP与BOOTP之间的区别总结。

表11-7 DHCP和BOOTP

BOOTP	DHCP
静态映射	动态映射
永久分配	租借分配
只支持4个配置参数	支持超过30个的配置参数
用于向主机发送一个可引导的操作系统	不能用于向主机发送一个可引导的操作系统

11.3.3 DHCP的特性

DHCP使用了3种机制来为客户分配IP地址：

- **自动分配**（*Automatic allocation*）——DHCP为客户分配一个永久IP地址。
- **手工分配**（*Manual allocation*）——管理员分配客户的IP地址，DHCP将地址传递给客户。
- **动态分配**（*Dynamic allocation*）——DHCP为客户分配一个有限时间（租期）内使用的IP地址。

本节关注的重点是动态分配机制。一些可用的配置参数列举在IETF RFC 1533文档中。其中一些参数如下所示：

- IP地址。
- 子网掩码。
- 路由器（缺省网关）。
- 域名。
- 域名服务器（一个或多个）。
- 名称服务器（例如WINS）。

请看图11-17。DHCP服务器创建IP地址池和相关的参数。地址池针对一个单独的逻辑IP子网，

允许多台DHCP服务器响应一个子网。同样的，IP客户是可以移动的。如果多台服务器都能够响应，一个客户便可以获得多台服务器提供的参数。但是，一个客户只能选择一台服务器。例11-9显示了DHCP服务器发送给DHCP客户的信息。

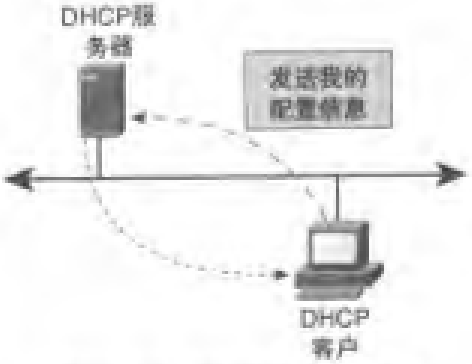


图11-17 DHCP客户和服务器

例11-9 DHCP配置文件

```
IP Address:192.204.18.7
Subnet Mask:255.255.255.0
Default Routers:192.204.18.1, 192.204.18.3
DNS Servers:192.204.18.8, 192.204.18.9
Lease time:5 days
```

DHCP客户可用于多个厂商的多种操作系统上，包括Windows 3.1、Windows 9x、Windows NT、Windows 2000、Windows XP、Solaris、Linux、MAC OS、Novell NetWare、FTP Software、NetManage和Cisco。

11.3.4 DHCP的运行方式

DHCP客户配置过程如图11-18所示。



图11-18 DHCP发现过程

该过程遵循5个步骤：

1. **客户向所有节点发送一个DHCPDISCOVER广播**——一个客户预先设置使用DHCP，该客户向一台服务器发送一个请求来要求得到一个IP配置（通常在启动时）。作为一种选择，客户可以建议它所希望使用的IP地址，比如在请求延长租期的时候。客户通过在本地网段内发送一个被称为DHCPDISCOVER的广播（255.255.255.255）来查找DHCP服务器。

2. **服务器向客户发送一个DHCPOFFER单播**——当服务器接收到广播时，它将确定是否可以用自己的数据库来为该请求提供服务。如果它不能为该请求提供服务，该服务器会将这个请求转发给其他DHCP服务器，这决定于它的配置。如果它可以为该请求提供服务，DHCP服务器就以单播DHCPOFFER的形式为客户提供IP配置信息。DHCPOFFER是一个提议配置，可能包括IP地址、DNS服务器地址和租期。

3. **客户向所有节点发送一个DHCPREQUEST广播**——如果客户发现适合的提议，它将发送另一个广播DHCPREQUEST，明确地请求那些特殊的IP参数。为什么客户广播请求而不是向服务器单播请求？使用一个广播是因为第一个消息，DHCPDISCOVER，也许到达了多台DHCP服务器。如果有多台服务器产生提议，那么广播的DHCPREQUEST就可以让大家知道接受的是谁的提议。被接受的提议通常是第一个收到的提议。

4. **服务器向客户发送一个DHCPACK单播**——收到DHCPREQUEST的服务器通过发送一个单播确认，即DHCPACK，来进行正式的配置。注意，服务器可能但也未必不发送DHCPACK，因为它可能已经临时将信息租借给了另外一个客户。收到DHCPACK消息后，客户立刻开始使用所分配的地址。

如果客户检测到该地址已经在本地网段中使用，它就会发送一个DHCPDELCLINE消息，并重新开始申请过程。如果客户在发送DHCPREQUEST之后从服务器收到一个DHCPNAK，它也会重新开始申请过程。

5. **客户释放IP地址**——如果客户不再需要它的IP地址，客户会向服务器发送一个DHCPRELEASE消息。

根据一个组织的策略，一个终端用户或一个管理员静态地为主机分配一个属于DHCP服务器地址池中的IP地址也是有可能的。为了以防万一，Cisco IOS DHCP服务器总是在将IP地址提供给客户之前检查该地址，以确保它没有在使用中。服务器向一个客户发送DHCPOFFER之前，先发出ICMP回应请求（ping）到一个池的地址。尽管是可配置的，用来检查潜在的IP地址冲突的缺省ping的个数是2。

如果服务器在另外一个网段上，可以使用路由器中的BOOTP中继代理将请求传输到那个网段。

11.3.5　配置DHCP的操作

就像NAT一样，DHCP服务器需要管理员定义一个地址池。ip dhcp pool命令定义了将哪些地址分配给主机。该命令的语法如下：

```
Router(config)#ip dhcp pool name1
Router(dhcp-config)#network ip-address mask
```

第一条命令，ip dhcp pool *name1*，创建了一个名为*name1*的池，并且将路由器置于一个特定的DHCP配置模式下。在这个模式下，使用network声明来定义要租借的地址范围。如果网络上有特殊地址需要被排除在外，返回全局配置模式，使用ip dhcp exclude-daddress命令。输入exit退出DHCP配置模式。

ip dhcp excluded-address命令配置路由器在为客户分配地址时排除一个单独的地址或一段地址。可以使用这个命令来保留那些静态分配给关键主机的地址，例如路由器的地址。该命令的语法如下：

```
Router(config)#ip dhcp excluded-address ip-address[end-ip-address]
```

通常，一台DHCP服务器被配置为分配多个IP地址。可以在DHCP配置模式下设置其他的IP配置值。IP客户在没有缺省网关的情况下访问不了多远。可以使用default-router命令来设置缺省网关。还可以配置DNS服务器的地址（dns-server）和WINS服务器（netbios-name-server）。IOS DHCP服务器实际上可以为客户配置任何TCP/IP信息。

在DHCP池配置模式下输入的一系列关键的IOS DHCP服务器命令如表11-8所示。

表11-8　DHCP池命令

命令	用途
Router(config)# ip dhcp pool *name*	为DHCP服务器地址池创建一个名字，进入DHCP池配置模式（由config-dhcp# 提示符标识）
Router(config-dhcp)# network *network-number* [*mask* | */prefix-length*]	指定DHCP地址池的子网号和掩码 前缀长度指明组成地址前缀的位个数。前缀是指定客户网络掩码的一个可选方法。前缀长度之前必有一个反斜杠（/）
Router(config-dhcp)# domain-name *domain*	为客户指定域名
Router(config-dhcp)# dns-server *address* [*address2...address8*]	指定DHCP客户可用的DNS服务器的IP地址。需要一个IP地址；但是也可在一条命令行中最多指定8个IP地址
Router(config-dhcp)# netbios-name- server *address* [*address2...address8*]	指定Microsoft DHCP客户可用的NetBIOS WINS服务器。需要一个地址；但是也可在一条命令行中最多指定8个地址
Router(config-dhcp)# default-router *address* [*address2...address8*]	为DHCP客户指定缺省路由器的IP地址。需要一个IP地址，但是也可在一条命令行中最多指定8个地址
Router(config-dhcp)# lease {*days* [*hours*] [*minutes*] | infinite}	指定租用的持续时间。缺省租期为一天

尽管在支持DHCP的Cisco IOS版本中缺省启用DHCP服务器进程，但仍然可以使用service dhcp全局配置命令来重新启用它。no service dhcp命令可以禁用该服务器。

11.3.6　验证DHCP的操作

表11-9列出了需要时可在EXEC模式下显示DHCP服务器信息的命令。

表11-9 显示DHCP服务器信息的命令

命令	用途
Router> show ip dhcp binding [*address*]	显示在特定DHCP服务器上创建的所有绑定列表
Router> show ip dhcp conflict [*address*]	显示在特定DHCP服务器上记录到的所有地址冲突列表
Router# show ip dhcp database [*url*]	显示DHCP数据库中的最近活动
	在特权EXEC模式下使用该命令
Router> show ip dhcp server statistics	显示服务器统计和发送与接收消息的计数信息

11.3.7 DHCP配置的故障排除

要启用DHCP服务器的调试功能，使用debug ip dhcp server特权EXEC命令。表11-10列出了调试DHCP服务器信息的命令。

表11-10 调试DHCP服务器的命令

命令	目的
debug ip dhcp server events	报告服务器事件，例如地址分配和数据库更新
debug ip dhcp server packets	译解DHCP的接收和传输的信息
debug ip dhcp server linkage	显示数据库连接信息（例如radix树中的父子关系）

为了对DHCP服务器的操作进行故障排除，可以使用命令debug ip dhcp server events，如例11-10所示。

例11-10 DHCP调试命令

```
Router#debug ip dhcp server events
Router#
00:22:53:DHCPD: checking for expired leases.
00:23:23:DHCPD: assigned IP address 172.16.13.11 to client 0100.10a4.97f4.6d.
00:27:49:DHCPD: returned 172.16.13.11 to address pool remote.
00:29:59:DHCPD: assigned IP address 172.16.13.11 to client 0100.10a4.97f4.6d.
```

该例显示，服务器周期性地检查是否有租用已经过期的IP地址。同样，还可以查看地址何时被收回以及何时被分配。

11.3.8 DHCP中继

DHCP客户使用IP广播来寻找网段上的DHCP服务器，就像前面看到的一样。当服务器和客户不在同一个网段，而是被路由器分隔开的时候又会发生什么呢？路由器不会转发这些广播。

DHCP并不是惟一使用广播的关键服务。Cisco路由器和其他设备可以使用广播来查找简单文件传输协议（TFTP）服务器。有些客户可能需要利用广播查找一个终端访问控制器访问控制系统（TACACS）服务器。通常，在一个复杂的分层网络中，客户和关键服务器往往不在同一个子网中。远程客户通过广播来查找这些服务器，但是在缺省的情况下，路由器不会将客户的广播转发到的它们子网之外的网络。

有些客户在没有诸如DHCP这类服务时将不能工作，所以必须实现以下两种选择之一：在所有子网中都放置服务器，或者使用Cisco IOS帮助地址特性。在几台计算机上运行诸如DHCP或DNS这类服务会产生开销，并令管理员头疼，所以第一种选择不是很吸引人。如果可能，管理员使用ip helper-address命令为那些关键的UDP服务中继广播请求。

通过使用帮助地址特性，路由器可以配置为接受UDP服务的广播请求，然后将其以单播方式转

发给某个特定的IP地址。缺省情况下，ip helper-address命令转发以下8种UDP服务：

- Time
- TACACS
- DNS
- BOOTP/DHCP服务器
- BOOTP/DHCP客户
- TFTP
- NetBIOS名称服务
- NetBIOS数据报服务

在DHCP这种特殊情况下，客户在本地网段广播一个DHCP发现分组。图11-19显示了DHCP消息的格式。网关获得这个分组，如果配置了帮助地址，就将DHCP分组转发到特定地址。

在转发这个分组之前，路由器在分组的GIADDR字段填入路由器在该网段的IP地址。这个地址将在DHCP客户得到IP地址之后成为DHCP客户的网关地址，如图11-20所示。

操作码	硬件类型	硬件地址长度	跳数
事务ID（XID）			
秒		标记	
客户端IP地址			
你的IP地址（YIADDR）			
服务器IP地址（SIADDR）			
网关IP地址（GIADDR）			
客户硬件地址（CHADDR）			
服务器名称（SNAME）——64Bytes			
文件名——128Bytes			
DHCP选项			

图11-19 DHCP消息格式

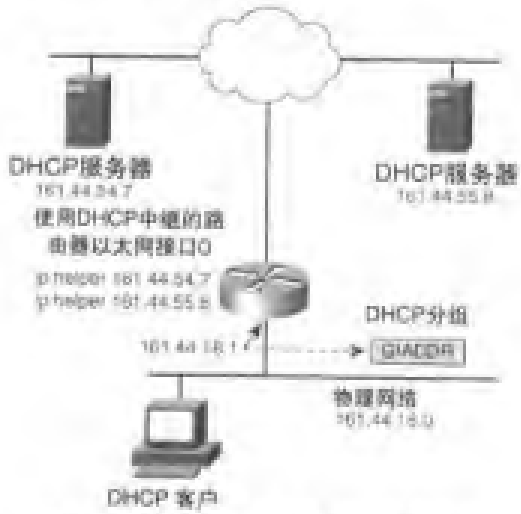


图11-20 DHCP客户得到一个IP地址

DHCP服务器收到发现分组后使用GIADDR字段来对地址池列表进行索引，它搜索网关地址设置和GIADDR值相匹配的地址池。这个地址池随后用来为客户提供其IP地址。图11-21显示了一个DHCP客户的广播，图11-22显示了一个DHCP服务器的单播。

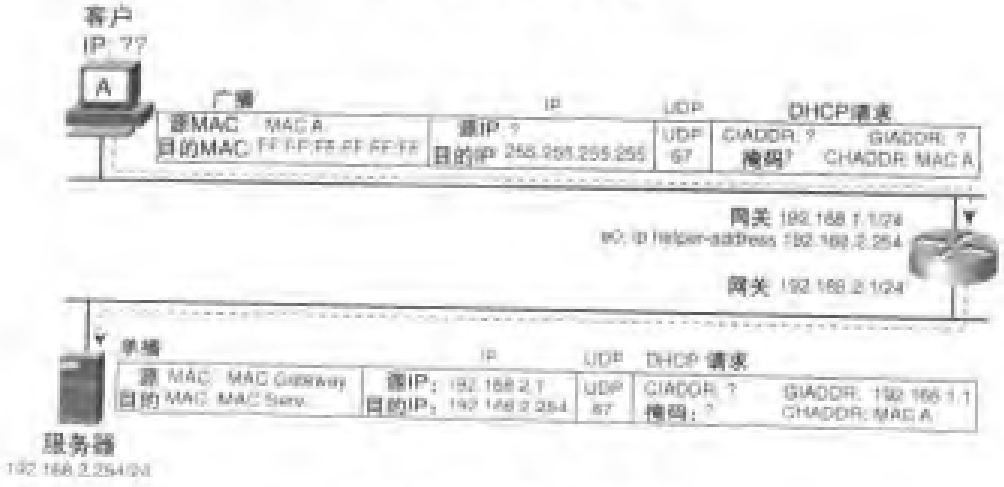


图11-21 DHCP客户广播



图11-22 DHCP服务器单播

实验活动 配置DHCP

在本实验中，你将配置路由器的DHCP，使其随后可以为接入的主机动态分配地址。

实验活动 配置DHCP中继

在本实验中，你将配置路由器的DHCP，随后为工作站添加能够远程获取DHCP地址并为接入的主机动态分配地址的能力。

11.4 总结

本章包含以下内容：

- 随着因特网的增长，主干因特网路由选择表中的IP路由数量也在增加。这引发了路由选择算法的扩展问题，于是提出了IP扩展问题的3种解决方案。
- FRC 1918为私有网络分配IP地址提供了背景。它也为那些想要部署IP但又不想与因特网完全连通的公司提供了实现指导方针。
- NAT允许将私有地址转换为公共可用的地址，以便在因特网中使用。本章展示了NAT配置和验证的实例。
- PAT允许一组内部主机同外部主机通信，并共享NAT配置中的复用地址。本章展示了PAT配置和验证的示例。
- DHCP提供了一种动态分配IP地址的机制，因此地址在主机不需要它们时可以自动重新使用。本章展示了相关的配置和故障排除实例。

作为本章所学内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

11.5 关键术语

自举协议（*Bootstrap Protocol, BOOTP*） 最初定义在1985年的RFC 951中。作为DHCP的前身，BOOTP具有一些与DHCP相同的操作特点。两种协议都使用UDP端口67和68，这些端口被称为BOOTP端口，因为BOOTP出现在DHCP之前。

无类域间路由选择（*classless interdomain routing, CIDR*） 允许路由器将路由聚合在一起，减少核心路由器所携带的路由选择信息数量。有了CIDR，若干个IP网络对外部网络呈现为一个以单独的更大的实体。

动态主机配置协议（*Dynamic Host Configuration Protocol, DHCP*） 提供了一种动态分配IP地址的机制，因此地址在主机不需要它们时可以自动被重新使用。

内部全球地址（*inside global address*） 在一个NAT配置中，内部本地地址被转换成的那个IP地址。

内部本地地址（*inside local address*） 在一个NAT配置中，被转换的IP地址。

网络地址转换（*network address translation, NAT*） 仅在公共网络上全球惟一。一种将私有地址转换为公共可用地址以便在因特网中使用的机制。一种有效的隐藏私有网络中真实设备地址的方法。

外部全球地址（*outside global address*） 外部网络的某台主机拥有者分配给该主机的IP地址。

外部本地地址（*outside local address*） 为内部网络主机所知的一台外部主机的IP地址。

超载（overloading，也被称为PAT） 使用TCP端口号允许一组内部主机与外部主机通信，并“共享”NAT配置中的超载地址。

11.6 复习题

1.私有地址通过什么进行分配?

A. RFC 1918的网络管理员

B. ARIN

C. RIPE

D.任何地址都可以作为私有地址

2.下面哪一个是有效的RFC 1918私有地址?

A. 10.0.0.0/7

B. 10.0.0.0/8

C. 192.168.0.0/16

D. 172.16.0.0/12

3. BOX公司维护它自己的公共web服务器，并打算实现NAT。应该为该web服务器使用哪一种类型的NAT?

A. 动态

B. 静态

C. PAT

D. 根本不使用NAT

4. 下面哪一项应用是Cisco IOS NAT所支持的?

A. ICMP

B. DNS区传输

C. BOOTP

D. FTP（包括PORT和PASV命令）

5. 下面哪一种流量类型是Cisco IOS NAT不支持的?

A. ICMP

B. DNS区传输

C. BOOTP

D. FTP（包括PORT和PASV命令）

6. BOOTP支持_____而DHCP支持_____

A. 静态映射

B. 动态映射

C. PAT

D. NAT

7. 将下列DHCP消息按其在过程中出现的正确顺序排列。

A. DHCPACK

B. DHCPREQUEST

C. DHCPOFFER

D. DHCPDISCOVER

8. DHCP代表什么?

A. Dynamic Host Configuration Protocol

B. Dynamic Hosting Configuration Protocol

C. Dynamic Host Computer Protocol

D. Dynamic Host Computer Port

9. NAT通过允许内部网私有化来保存合法注册的寻址方案。

A. 正确

B. 错误

10. DHCP并非打算用于配置路由器、交换机和服务器，因为这些主机需要静态IP地址。

A. 正确

B. 错误



第12章 广域网技术

目标

学习完本章之后，你将能够：

- 理解局域网（LAN）和广域网（WAN）的区别。
- 识别WAN中使用的设备。
- 列举WAN的标准。
- 描述WAN的封装。
- 对多种可选WAN链路分类。
- 分组交换和电路交换WAN技术的区别。
- 描述WAN设计的步骤。

当一个企业增长到超过单一的地理位置的时候，就需要互连各个部门的LAN，形成一个企业广域网（WAN）。本章将讨论互连的一些可用选项、实现互连所需的硬件以及讨论这些内容时所用的术语。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图。光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

12.1 广域网技术概述

广域网（WAN）是一种运行的地域超过局域网（LAN）的数据通信网络。广域网和局域网主要区别之一在于一个公司或组织需要向外部的广域网服务提供商申请订购使用广域网电信网络服务。广域网通常使用电信运营商提供的数据链路在广域范围上访问网络带宽。广域网将组织位于各地的多个部分连接起来、并与其他组织连接、与外部服务（比如数据库）连接以及与远程用户连接。广域网通常可以传输各种各样的通信类型，比如语音、数据和视频。电话和数据服务是最常用的广域网服务。

放置在用户端的设备，如图12-1所示，被称为客户端设备（CPE, Customer Premises Equipment），这种设备属于用户所有或者由服务提供商租用给用户。使用铜线或者光纤将CPE连接到服务提供商的最近的交换或中心局（CO）。这段线缆通常被称做本地环路（local loop）或“最后英里”（last-mile）。一个呼叫被本地连接到其他本地环路，或者是通过中继非本地连接到一个主中心，再到一个区域中心，再到一个地区或者国际电信中心，该呼叫传输了很长距离后才到达它的目的。图12-2图示说明了广域网服务提供商。

如果本地环路要传输数据，就需要类似调制解调器之类的设备用于数据传输。那些在本地环路上传输数据的设备叫做数据电路端接设备或者数据通信设备（DCE，data circuit-terminating equipment）。而那些将数据传输给DCE的客户设备就叫做数据终端设备（DTE，Data Terminal Equipment）。图12-3显示了DCE和DTE设备的实例。DCE主要为DTE提供了一个进入广域网云中通信链路的接口。DTE/DCE接口使用各种各样的物理层协议［比如高速串行接口（HSSI）和V.35］，用来创建设备间彼此通信的编码。如图12-4所示。

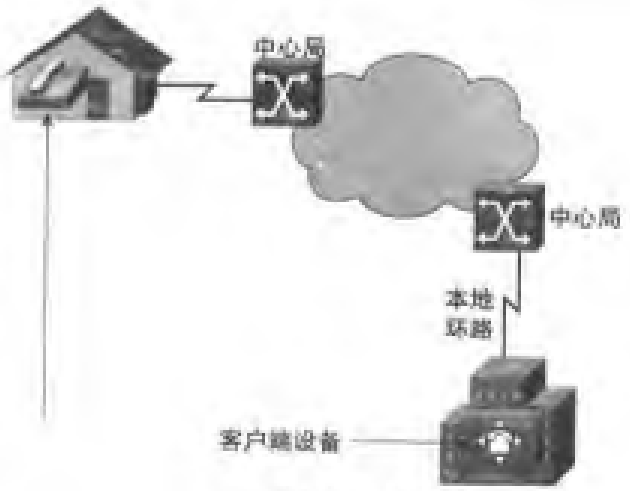


图12-1　CPE

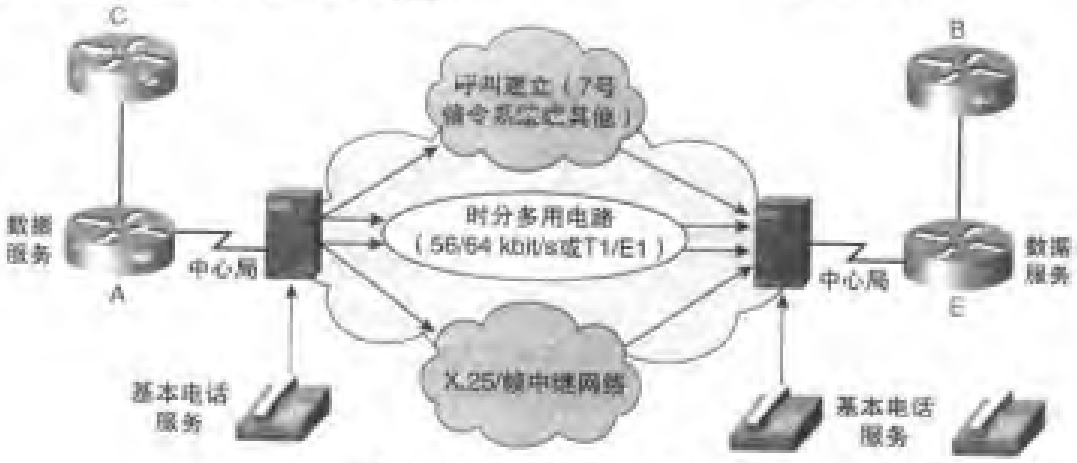


图12-2　广域网服务提供商

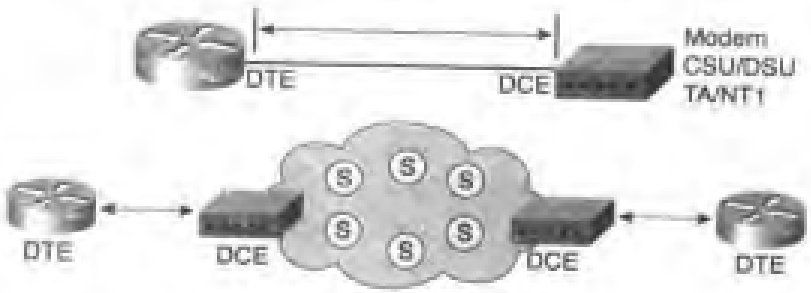


图12-3　DTE/DCE

广域网提供商可以提供各种速率的广域网链路，单位可以是比特每秒（bit/s）、千比特每秒（kbit/s，1,000bit/s）、兆比特每秒（Mbit/s，1,000kbit/s）或吉比特每秒（Gbit/s，1,000Mbit/s）。bit/s描述一般指全双工，所以同时地，一条E1线路双向都是2Mbit/s，或T1线路双向都是1.5Mbit/s。需要注意的是1kbit/s就是1,000bit/s，而kB是1024个字节。数据传输的衡量单位K是十进制含意的，而数据存储的K是二进制含意的。从技术上讲，kbit/s应该用小写字母k表示它是十

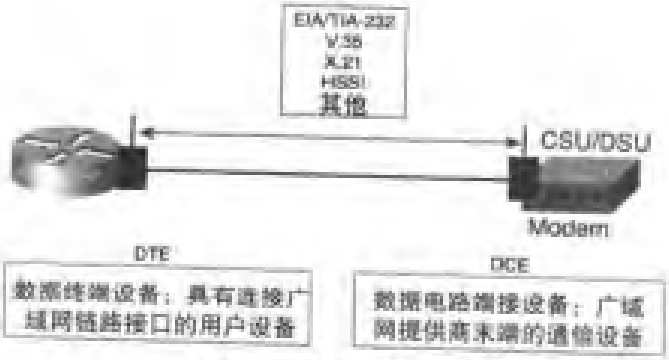


图12-4　广域网的物理层

进制的，但几乎人人都用大写字母K。表12-1中列出了常用的广域网电路类型和带宽。

表12-1 广域网电路类型和带宽

类型	信令标准	比特流速率
56	DS0	56kbit/s
64	DS0	64kbit/s
T1	DS1	1.544Mbit/s
E1	ZM	2.048Mbit/s
J1	Y1	2.048Mbit/s
E3	M3	34.064Mbit/s
T3	DS3	44.736Mbit/s
OC-1	SONET	51.840Mbit/s
OC-3	SONET	155.520Mbit/s
OC-9	SONET	466.560Mbit/s
OC-12	SONET	622.08Mbit/s
OC-18	SONET	933.12Mbit/s
OC-24	SONET	1244.16Mbit/s
OC-36	SONET	1866.24Mbit/s
OC-48	SONET	2488.32Mbit/s
OC-96	SONET	4976.640Mbit/s
OC-192	SONET	9953.280Mbit/s

12.2 广域网设备

广域网本质上是由服务提供商的通信链路连接起来的一组局域网。由于通信链路不能直接插入局域网中，所以需要各种接口连接设备。

基于局域网的计算机把数据传输给一台具有局域网和广域网接口的路由器。如图12-5所示。路由器根据地址信息把数据传送到适当的广域网接口。由于路由器是主动的、智能的网络设备，所以它可以参与管理网络。路由器通过提供动态控制资源和支持网络的任务和目标来管理网络。它们的目的就是实现连通性、可靠的性能、管理控制和灵活性。

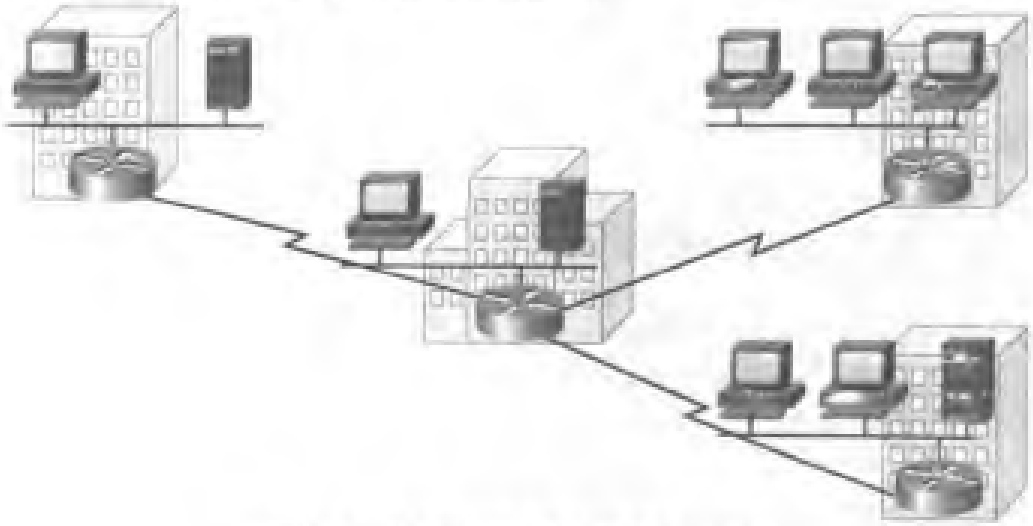


图12-5 通过路由器连接广域网和局域网

通信链路需要信号具有适当的格式。对于数字线路，需要一个信道服务单元（CSU, Channel Service Unit）和一个数据（或数字）服务单元（DSU, data (or digital) service unit）。在实际中这两个单元通常都合并在一台设备中，即CSU/DSU，如图12-6所示。有时候CSU/DSU就内建于路由器的接口卡中。

如果本地环路是模拟线路，而不是数字线路，就需要一台调制解调器，如12-7图所示。调制解调器在话音级的电话线路上通过调制和解调信号来传输数据。数字信号被调制为模拟话音信号进行传输。打开调制解调器中的内部扬声器可以听到被调制的信号，所听到的是一连串的嘟叫和嘶嘶的声音。在接收端，模拟信号被还原为数字信号形式，这个过程被称为解调。



图12-6　广域网CSU/DSU

当使用综合业务数字网（ISDN）作为通信链路时，所有连接到ISDN总线上的设备必须是ISDN兼容的。一般而言，这种兼容性被集成到用于直接拨号连接的计算机或用于局域网到广域网连接的路由器的接口上。比较老的设备可能没有ISDN的接口，在这种情况下就要使用ISDN终端适配器（TA, terminal adapter）。



图12-7　广域网和调制解调器

通信服务器用于远程访问局域网，它集中了拨号用户的通信。这种设备可能具有模拟和数字（ISDN）混合接口，并且支持数十或者上百个用户同时接入。

12.3　广域网标准

广域网仍然使用OSI分层参考模型，类似于局域网。但是广域网主要关心下两层。广域网标准通常描述了物理层的传送方式和数据链路层的要求，包括寻址、流量控制和封装。广域网标准由多个公认的权威机构定义和管理。

广域网的物理层协议描述了如何提供电气、机械、操作和功能的连接到通信服务提供商所提供的服务。连接到广域网的设备，通常是一台路由器，它被认为是一台DTE。而连接另一端的设备为服务提供商提供接口，这就是一台DCE。表12-2中列举了图12-8所示的常用物理层标准和它们的连接器。

表12-2　广域网物理层标准

标准	描述
EIA*/TIA*232	在近距离范围内，允许25针D连接器上的信号速度最高可达64kbit/s。以前被称为RS-232。ITU-T v.24规范中也是一样
EIA/TIA 449 EIA-530	EIA/TIA 232的高速版本（最高可达2Mbit/s），它使用36针D连接器，传输距离更远 有几个版本，也被称为RS-422和RS-423
EIA/TIA 612/613	高速串行接口（HSSI），在50针D连接器上提供速度高达52Mbit/s的访问服务

续表

标准	描述
V.35	用于高速同步数据交换的ITU*标准。在美国，V.35是大多数路由器和连接到T1线路的DSU的接口标准
X.21	用于同步数据通信的ITU-T*标准。它使用15针D连接器。这种类型的连接器主要用于欧洲和日本

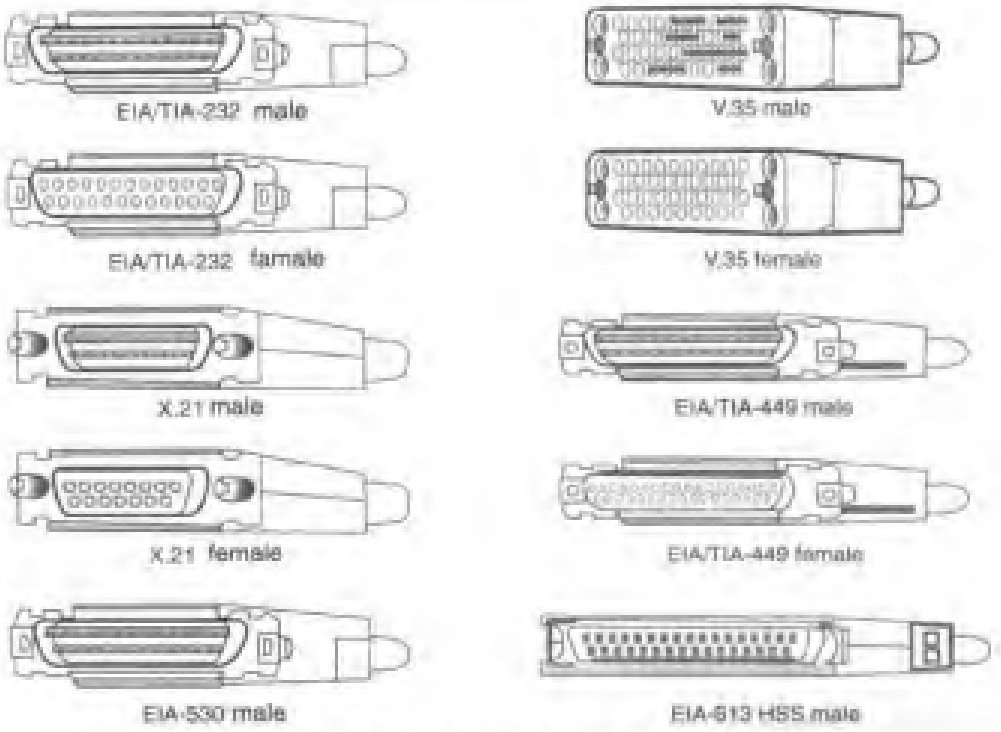


图12-8 广域网连接器

*EIA = 电子工业联合会（Electronic Industries Association）

*TIA = 电信工业协会（Telecommunications Industry Association）

*ITU = 国际电信联盟（International Telecommunication union）

*ITU-T = 国际电信联盟-电信标准部（International Telecommunication union Telecommunications Standardization sector）

数据链路层协议定义如何将数据封装以传输到远程站点，以及传输这个封装帧的机制。使用了多种不同的技术，比如ISDN、帧中继和异步传输模式（ATM），但是它们几乎都使用相同的基本成帧机制——高级数据链路控制（HDLC），这是一个ISO标准，或者是HDLC的一个子集或变体，如图12-9所示。

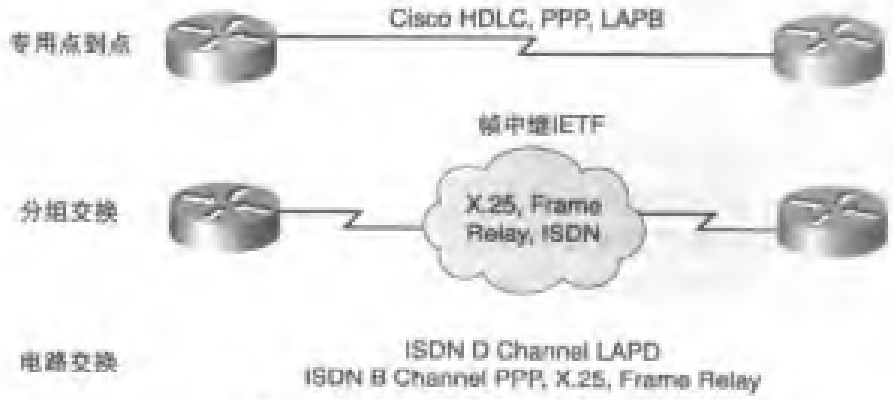


图12-9 广域网数据链路层协议

12.4　广域网封装

为了在一般是点到点的物理链路上进行传输，数据要从网络层传递到数据链路层。数据链路层构造一个帧来封装网络层数据，以便进行必要的检查和控制。每种广域网连接类型都用第2层协议封装穿越广域网链路的流量。为了确保使用正确的封装协议，在路由器上必须为每个串行接口配置所使用的第2层封装类型。封装类型的选择取决于广域网技术和通信设备。大多数的成帧都基于HDLC标准。

HDLC成帧设计用于在不可靠线路上可靠地传输数据，因此包括了用于流量和错误控制的信令机制。帧通常以一个8比特标志字段开始和结尾：比特模式01111110或7E16（16进制）。由于实际数据中也可能出现这种形式，所以发送HDLC的系统通常在数据字段中每5个1后插入1个0比特，这样实际上标志序列只会出现在帧尾。接收系统剔出插入的比特。当一个帧紧接在一个帧之后发送时，前一个帧的结尾标志被用做下一个帧的开始标志。

几乎总是点到点的广域网链路不需要地址字段，但帧结构中仍然保留这个字段。它的长度为1或2字节。控制字段指示帧的类型，可以是信息帧、监控帧或无编号帧。无编号帧携带线路建立消息，信息帧携带网络层数据，监控帧控制信息帧的流动和请求在出错时的数据重传。控制字段一般是1字节，但扩展的滑动窗口系统是2字节。地址字段和控制字段合起来称为帧头（frame header）。

控制字段后面的就是封装的数据，然后是使用循环冗余校验机制的帧校验序列（FCS），它是一个2或4字节长的字段。目前有几种数据链路层协议正在使用，包括HDLC的子集和专有版本，如图12-10所示。PPP和Cisco版本的HDLC在帧头部都有一个额外字段，用来标识封装数据的网络层协议。



图12-10　广域网帧的封装格式

12.5　广域网链路的选择

以下小节讨论常用于广域网连接的各种技术。有助于对这些选择有一个总的看法和分类。

12.5.1　电路交换连接

电路交换（circuit switch）用于建立两个不同地域点间的语音或数据连接。在有用的通信开始之前，需要通过设置交换来建立连接。这由电话系统通过在普通的语音级线路和ISDN数字线路上拨号来完成。

为了避免建立连接所产生的延迟，电话服务提供商在他们的系统上也提供永久式电路。这种专用或租用线提供比交换式电路更高的可用带宽。下面列举了一些电路交换连接的实例：

- 公共交换电话网（*PSTN, Public Switched Telephone Network*）。
- ISDN基本速率接口（*BRI, Basic Rate Interface*）。
- ISDN基群速率接口（*PRI, Primary Rate Interface*）。

12.5.2　分组交换连接

很多广域网用户没有有效使用专用电路所提供的固定带宽，无论是交换式电路还是永久式电路，因为数据流是突发的。为了更好地服务这些用户，通信提供商着手提供可用的数据网络，也就是数据在标记的信元、帧或分组中穿越分组交换网络。由于很多用户共享交换机间的内部链路，所以分组交换（packet switching）的代价比电路交换低。又由于链路是共享的，一台交换机必须在开始将分组发送给下一台之前完整接收该分组，这样分组交换网络中的延迟（等待时间）和延迟的不定性（抖动）大于电路交换网络。尽管共享网络中的延迟和抖动是固有的，但是现代技术允许在这种网络上进行令人满意的语音甚至视频通信。

分组交换网络可以为特定的端到端连接建立通过交换的路由。如果在交换开始时就已经建立了路由，这些路由被称为永久虚电路（PVC, Permanent Virtual Circuits）；如果它们是根据需要建立的，就称为交换虚电路（SVC, Switched Virtual Circuits）。如果路由选择不是预先建立，而是每个分组独自交换，这样的网络被称为无连接网络。

为了连接到一个分组交换网络，用户需要一条本地环路以连接到服务提供商提供服务的最近位置，即服务的接入点（POP, Point of Presence）。通常，这是一条专用租用线，它比租用线更短，用来直接连接用户，并且常常承载几条虚电路（VC）。因为并不是所有的VC同时都会有它们最大的需求量，所以租用线的容量要小于所有单条VC之和。下面列举了几种分组或信元交换连接：

- 帧中继（Frame Relay）
- X.25
- ATM

12.5.3 分组和电路交换

分组交换网络的发展克服了公共电路交换网络的高额费用，并提供了更有效的广域网技术。

用户进行一次电话呼叫时，呼叫的号码用来在交换中沿呼叫路由设置交换，所以从呼叫方电话机到被呼叫方形成一条连续的电路。由于用交换操作来建立电路，电话系统也称为一个电路交换网络。如果用连接计算机的调制解调器替代电话机，那么交换电路就可以传输计算机数据。图12-11显示了电路交换的一个例子。

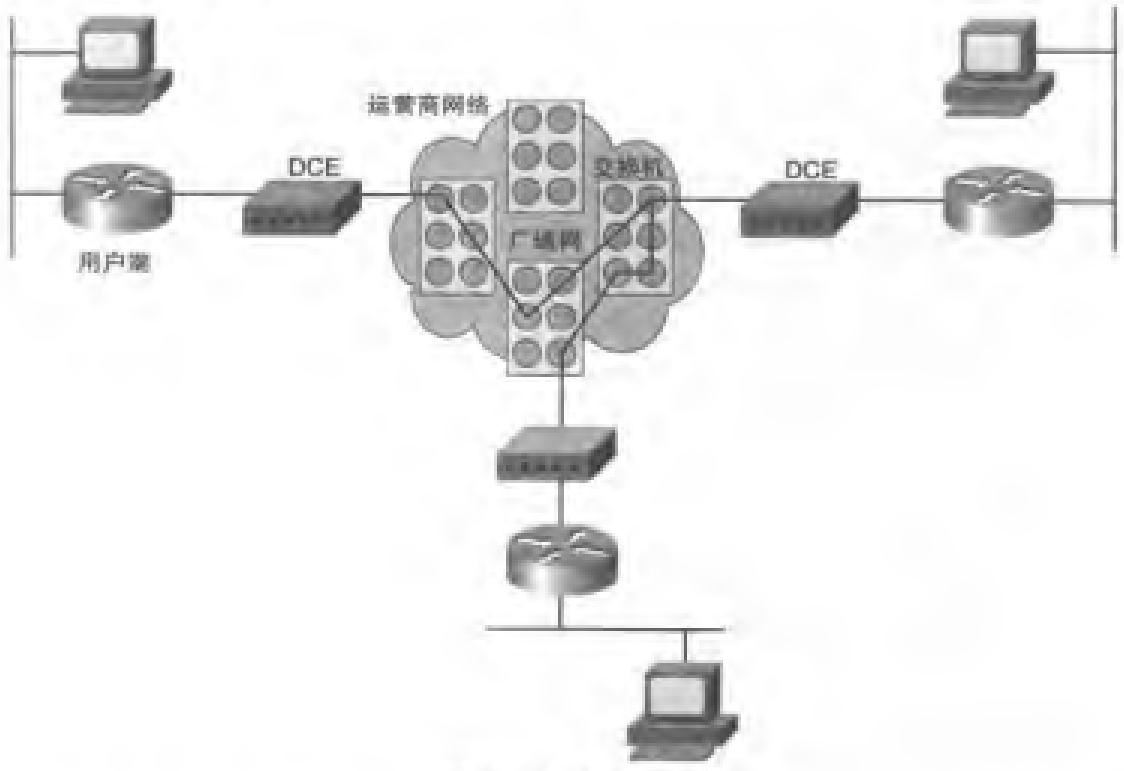


图12-11 电路交换

实际中的电路有些介质可能不是铜线，比如光纤或微波。其中交换局之间的内部电路路径会被多个会话共享，所以使用时分多路复用（TDM, Time-Division Multiplexing）技术让每个会话轮流使用共享的连接。TDM确保给每个用户提供固定容量的连接。

如果电路用于传输计算机数据，这种固定容量的用法就不太有效。如果电路用于访问因特网，比如传输网页时在电路上产生了突发流量，随后在用户看网页时没有流量，然后传输下一页时又产

生了突发流量。这种在没有和最大之间的使用变化是典型的计算机网络流量。由于用户单独使用固定容量分配，因此交换电路对于传输数据来说是一种昂贵的方式。

一种可供选择的办法就是仅在需要时才为流量分配带宽，并且让多个用户共享可用的带宽。在电路交换连接中，由于电路已经建立好，所以放到电路上的数据比特自动传输到远端。如果电路是共享的，就需要一些机制来标记比特，让系统知道把它们发送到哪里。由于很难标记单个比特，所以把这些比特按不同方式组合在称为信元、帧或分组中，最终被标记的包或分组就可以在提供商网络的交换局之间进行传递。实现这种系统的网络被称为分组交换网络。图12-12显示了分组交换的一个实例。

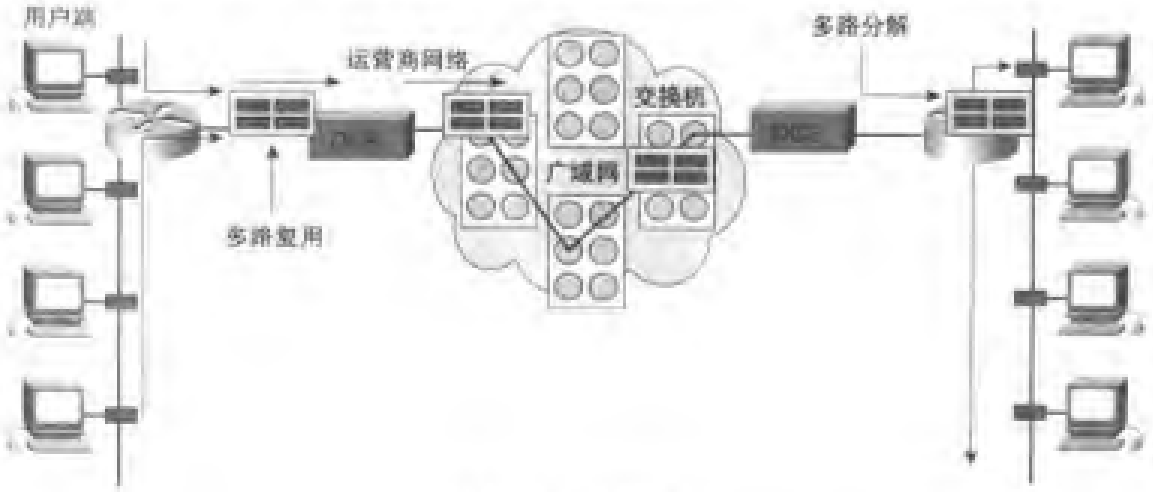


图12-12　分组交换

由于在提供商网络中连接交换局或交换机的链路仅在有数据从用户来的时候才分配给该用户，这样许多用户可以共享链路，每个用户的花费明显低于专用电路交换连接。另一方面，由于每个分组必须在交换机上等待其他用户的分组离开链路，所以分组交换网络中的数据具有不可预知的延迟。

分组交换网络中的交换机必须能够根据每个分组中的地址信息来决定分组必须发送的下一条链路。这种链路决定有两种方法：无连接或面向连接。无连接系统，比如因特网，在每个分组中都带有完整的地址信息。面向连接的系统预先为分组确定路由，每个分组只需要携带一个标识符。在帧中继环境下，这些标识符被称为数据链路连接标识符（DLCI, Datalink Connection Identifiers）。交换机通过查找其内存表中的标识符来确定向前的路由。所有表中的一组条目标识了通过系统的一条特定路由或电路。如果这条“电路”只在分组传输时才物理存在，就被称为虚电路（VC）。

建立VC的条目可以通过在网络上发送连接请求来建立，这种情况建立的电路被称为交换虚电路（SVC）。在SVC上传输的数据必须等待直到表的条目建立好。尽管建立一条SVC可能操作数小时、数天或者数周。在需要一直有可用电路的地方可以建立一条永久虚拟电路（PVC）。交换机在启动时加载这个表条目，使得PVC一直可用。

12.6　广域网技术

以下小节讨论了一些用于建立广域网连接的广域网技术，比如模拟拨号、ISDN、租用线、X.25、帧中继、ATM、DSL和电缆调制解调器。这些小节中还包括这些广域网技术的优点、缺点和特定的使用环境。

12.6.1　模拟拨号

当需要间歇的少量数据传输时，调制解调器和模拟拨号电话线提供了低容量、交换式的专用连

接（如图12-13所示）。

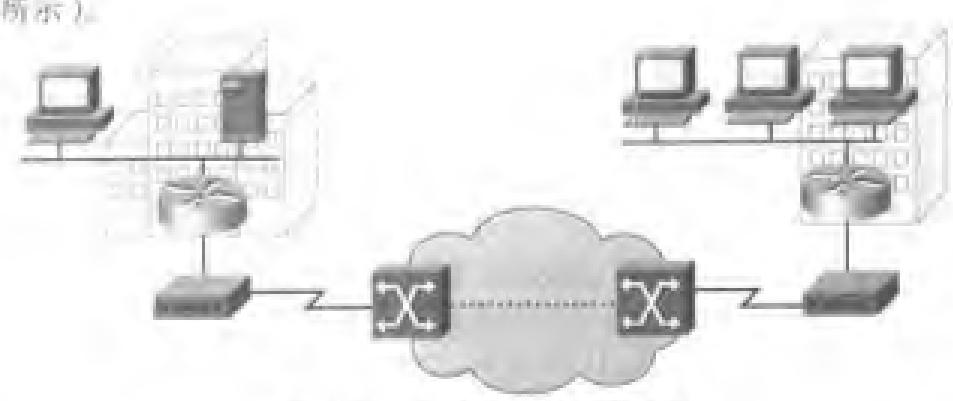


图12-13 广域网调制解调器技术

传统电话系统使用称为本地环路的铜线线缆将用户端的电话机连接到PSTN。呼叫过程中本地环路上的信号是用户语音的电子拷贝，是一个持续变化的信号。

本地环路不适于直接传输二进制计算机数据，但是调制解调器可以在语音电话网上传输计算机数据。一台调制解调器将二进制数据调制为模拟信号，并把模拟信号解调为二进制数据。

信号传输的速率受本地环路的物理特性限制，连接到PSTN的最高速率限制是33kbit/s左右。如果信号来自数字连接，速率可以增加到56kbit/s左右。

对于一些小的公司，模拟拨号足够满足一些交换活动，如销售图表、价格、日常事务报道和邮件。用户可以在晚上或者周末使用自动拨号来进行大文件的传输和数据备份，这样可以节省费用。价格取决于端点间的距离、每天的时间和呼叫的持续时间。

调制解调器和模拟线路的优点是简单和实现代价低。缺点是低速率和相对较长的连接时间。调制解调器在经常使用的情况下，较长的连接建立时间也不是问题。持续的专用电路在点到点流量上不会有延迟和抖动。但是语音和视频流量在低速上是无法操作的。

12.6.2 ISDN

PSTN的内部连接或中继线已经发生了变化，从以前承载的模拟频分多路复用信号转变为现在所承载的时分多路复用数字信号。很明显，下一步是让本地环路能够承载数字信号，从而实现高容量的交换式连接。

综合业务数字网（ISDN, Integrated Services Digital Network）将本地环路转化为TDM数字连接。该连接有用来传输语音或数据的64 kbit/s承载（B）信道和一条用来进行呼叫建立和其他用途的信令（D）信道。

基本速率接口（BRI）用于家庭和小型企业，提供2条B信道和1条16kbit/s的D信道。对于大型企业，ISDN的基群速率接口（PRI）可以满足。在北美，PRI提供23条B信道和1条D信道，总比特率达到1.544Mbit/s。（这包括用于同步的额外开销。）在欧洲、澳大利亚和其他国家，ISDN PRI提供30条B信道和1条D信道，总速率达到2.048Mbit/s（包括同步开销）。PRI的D信道是64kbit/s，如图12-14

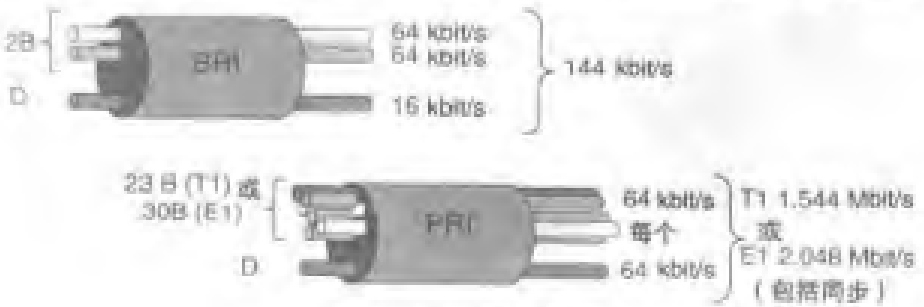


图12-14 ISDN信道

所示。注意，北美的PRI速率对应于T1连接。国际的PRI速率对应于E1连接。

BRI的D信道没有充分使用，因为只有两条B信道可以控制。有些提供商允许使用D信道进行低速数据传输，比如9.6kbit/s的X.25连接。

对于小型广域网，BRI ISDN可以提供理想的连接机制。BRI具有较短的呼叫建立时间（通常低于秒），并且64kbit/s的B信道提供比模拟调制解调器链路更高的带宽。图12-15显示了广域网使用ISDN技术。如果需要更多的带宽，第2条B信道就被启动，提供128kbit/s的速率。尽管这对于视频传输还不够，但是它允许在传输数据时还可以同时有几个语音会话。

ISDN另外一个常见的应用是为一条现有的租用线连接提供所需的额外的容量。租用线适合传输平均流量负载，高峰期则加入ISDN。当租用线突然中断，ISDN又可以作为备份线路。

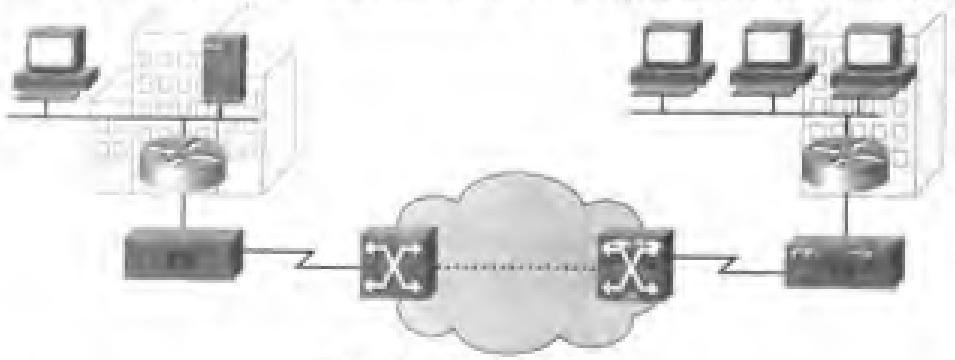


图12-15　广域网ISDN技术

ISDN在每条B信道的价格类似于模拟语音连接。也就是说，两条同时的64kbit/s连接的价格是一条连接的两倍。

在ISDN PRI上，两个端点间可以连接多条B信道，从而允许无延迟或抖动的视频会议和高带宽数据连接。长距离上的多条连接会变得非常昂贵。

12.6.3　租用线

当需要永久专用连接（permanent dedicated connecting）时，可以使用租用线（leased lines），它的最高带宽可达2.5Gbit/s。

点到点链路可以提供一条预先建立的广域网通信路径，该路径从用户端通过运营商网络，比如电话公司，到远程网络。点到点线路一般可以从运营商处租用，因此经常被称为租用线。租用线可以提供各种不同的容量。这些专用电路的价格通常基于所需带宽和两个连接点间的距离。点到点链路一般比共享的服务（比如帧中继）贵。当要连接很多地方时，就不得不考虑租用线方案的价格。专线容量提供端点间的无延迟或无抖动、持续的可利用性是类似电子商务等应用的基本保证。

每条租用线连接都需要一个路由器串行接口，同样也需要CSU/DSU和服务提供商提供的实际电路。租用线广泛用于建设广域网，如图12-16所示，可以提供永久的专用容量。传统上这种应用已

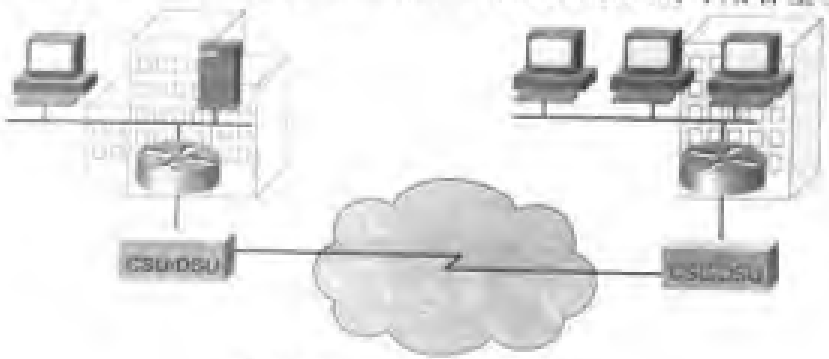


图12-16　广域网租用线技术

经广泛使用，但是它仍然存在很多缺点。由于广域网的流量经常变化而租用线容量又是固定的，这就造成了带宽很少被完全使用。此外，每个端点都需要路由器的一个接口，这样位于多点星型中心的路由器将会非常昂贵。租用线的任何变化一般都需要运营商对站点的容量进行改变。

租用线能够用来提供企业局域网间的直接点到点连接。租用线也可以用来把不同的部门连接到一个分组交换网络中。多条连接可以复用在一条链路上，从而缩短链路并让中心路由器需要较少的接口。

12.6.4 X.25

对应于租用线的昂贵，电信提供商引入了分组交换网络中的共享线路来降低成本。第一个分组交换网络标准就是X.25协议族。X.25提供了交换式或者永久式的低比特率、共享和可变带宽的服务。图12-17显示了一个X.25广域网。

X.25要给用户提供一个网络地址。随着呼叫请求分组到达目的地址，可以建立穿越网络的VC。所建立的SVC用信道号来标识。被标记了信道号的数据分组被发送到对应地址。在一条连接上可以启动多条信道。

用户使用租用线或拨号连接接入X.25网络。X.25网络也可在用户间预先建立好信道，提供一条PVC。

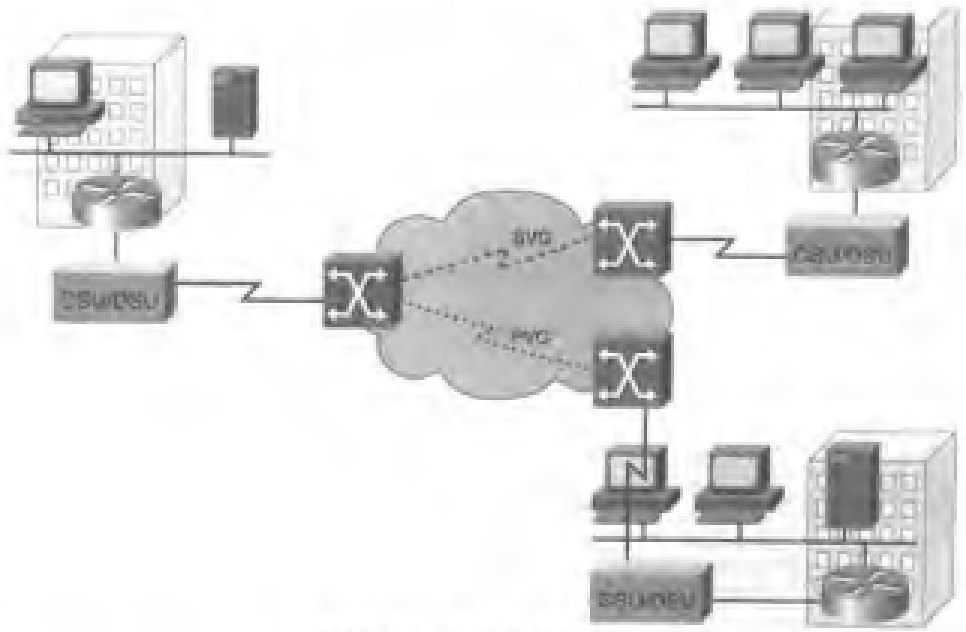


图12-17 广域网X.25技术

由于X.25的计费不是基于连接时间和距离而是基于传输的数据量的，所以它非常经济。数据可以任何的速率来发送，最高达到连接的容量。这提供了一定的灵活性。X.25网络通常只有最高48kbit/s的低带宽。除此之外，数据分组将受到通常是共享网络的传输延迟影响。

12.6.5 帧中继（Frame Relay）

随着对高带宽和低延迟分组交换需求的增加，电信提供商又引入了帧中继（FR）。尽管其网络布局与X.25类似，但是可用的数据传输速率一般达到4Mbit/s，有些提供商还可以提供更高的带宽（如图12-18所示）。

帧中继在某些方面与X.25不同。最重要的是，它是运行在数据链路层上的一种更为简单的协议。术语帧（frame）用于描述数据链路层的数据单元。

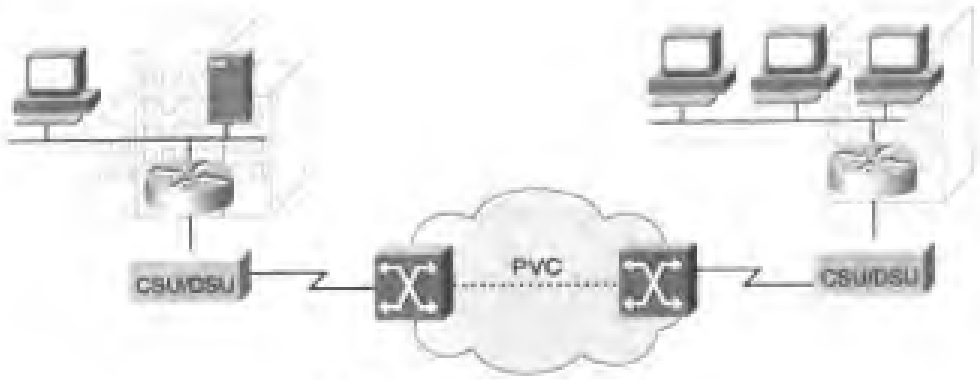


图12-18　广域网帧中继技术

帧中继没有实现差错或流量控制。简化了的帧处理减少了延迟。用来避免中间交换机重组帧的方法有助于减少抖动。

大多数的帧中继连接基于PVC而不是SVC。到达网络边界的连接通常是租用线。ISDN的D信道用来建立一条或更多B信道上的SVC。帧中继的价格基于网络边界处的连接端口容量和协定容量或端口上不同PVC的承诺信息速率（CIR）。

帧中继为承载语音和数据流量提供了永久的、共享的中等带宽的连接。帧中继是连接企业局域网的理想方式。即使用了多条PVC，LAN上的路由器也只需要一个接口，而且连接到FR网络边界的较短的访问线路，或本地环路都允许广泛分散的LAN之间建立经济的连接。

12.6.6　ATM

在发展FR的同时，电信提供商又看见对一种比以前能提供更高带宽的低延迟和低抖动的永久共享式网络技术的需求。解决方案就是异步传输模式（ATM，Asynchronous Transfer Mode）。ATM数据传输速率最高可以达到155Mbit/s。类似于其他共享式技术，X.25和FR，他们的广域网结构看起来都一样，如图12-19所示，但是ATM提供了更高流量水平的连接解决方案。当流量，比如视频，具有不能容忍延迟的本性时，ATM尤其有效。

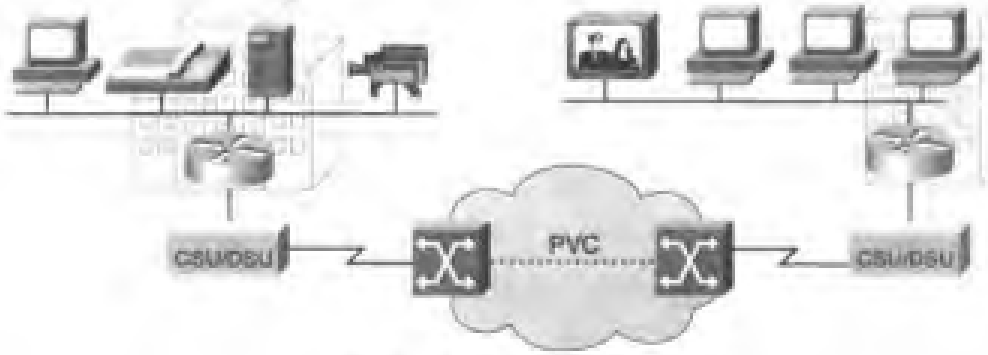


图12-19　广域网ATM技术

异步传输模式（ATM）是能够在私有和公共网络上传输语音、视频和数据的技术。它建立了一种基于信元的体系结构而不是基于帧的体系结构。ATM的信元都是固定的53个字节长度。这53字节的ATM信元中包含5字节的ATM头和48字节的ATM有效载荷。这种又小又是固定长度的53字节的信元非常适合传输语音和视频流量，因为语音和视频流量是不能容忍延迟的。语音和视频流量不需要等待大数据分组的传输。

53字节的ATM信元不如帧中继和X.25的较大帧和分组有效率，因为一个48字节的有效载荷至少有5Bytes的开销。当信元传输被分解的网络层分组时，开销更高，因为目的端的ATM交换机必须要

对分组进行重新组合。一个典型的ATM线路需要比FR高20%的带宽才能传输相同数量的网络层数据。

ATM提供PVC和SVC，尽管广域网一般使用PVC。类似其他共享技术，ATM允许在一条租用线上有多条连接到网络边界的虚电路。

12.6.7 数字用户线（DSL）

电话系统限制了本地环路上的带宽。从系统上对本地环路进行去耦就可以提供更高的带宽而无需安装新的线缆。图12-20图示了一条DSL连接。



图12-20 DSL

数字用户线路（DSL, Digital Subscriber Line）技术断开来自于CO或本地交换局的交换机的本地环路。连同其他DSL用户的本地环路一起，用DSL替代连接到CO中的数字用户线接入多路复用器（DSLAM, Digital Subscriber Line Access Multiplexor）。为了维护日常的电话服务，DSLAM又连回电话交换机。一般也可用ATM连接回DSL提供商的因特网服务。

DSL提供全天候的连接。一旦用户打开他们连接到DSL调制解调器的电脑，他们就被连接了。这种建立方式去除了建立连接的拨号时间和努力。

两种基本类型的DSL技术是非对称（ADSL asymmetric DSL）和对称（SDSL symmetric DSL）。所有形式的DSL服务都可以归类为这一种或另一种类型，并且每种类型有很多变化。术语xDSL有时泛指现有的各种形式的DSL。非对称服务提供的下载或下行速率（到用户）高于上行速率（到提供商）。对称服务在这两个方向上提供相同速率。

不同的DSL类型提供不同的带宽，大多数超过了T1或E1租用线。实际中所获得的速率主要取决于本地环路的实际长度和布线的类型与环境。为了能提供满意的服务，本地环路必须要小于5.5公里（3.5英里）。DSL不是全球适用，因为DSL具有众多的类型、标准和正在形成的标准，所以对于企业计算机部门的家庭办公支持并不是一种流行的选择。此外，用户不能选择直接连接到企业网络，而是必须先连接到一个ISP，然后再通过因特网建立到企业的IP连接。这种限制具有安全隐患。

12.6.8 电缆调制解调器（Cable Modem）

在城市，同轴电缆被广泛地应用于传输电视信号。有线电视网络也可以用于网络访问，可以比传统的电话本地环路提供更高的带宽。图12-21显示了电缆调制解调器的连接。

电缆调制解调器可以使用传输有线电视的同轴电缆进行双向、高速的数据传输。有些电缆服务提供商承诺提供6.5倍T1线路的数据传输速率。这个速度使得电缆可以作为快速传输大量数字信息，包括视频片段、音频文件和大量数据的诱人的介质。使用ISDN的BRI需要花2分钟来下载的信息用电缆调制解调器连接只需要2秒钟即可下载。

电缆调制解调器访问提供高于租用线的速度，价格更低，更易安装。电缆调制解调器提供全天候的连接。一旦用户打开了他们的计算机，就已经连接到因特网上了。这种建立方式去除了建立连接的拨号时间和努力。但是，这样一直在线的电缆连接意味着被连接的计算机随时都易受黑客攻击，需要安装防火墙来保证计算机的安全。

电缆调制解调器能够在一条6MHz的电缆信道上提供高达30到40Mbit/s的数据传输。这个速度要比56Kbit/s的调制解调器快500倍。

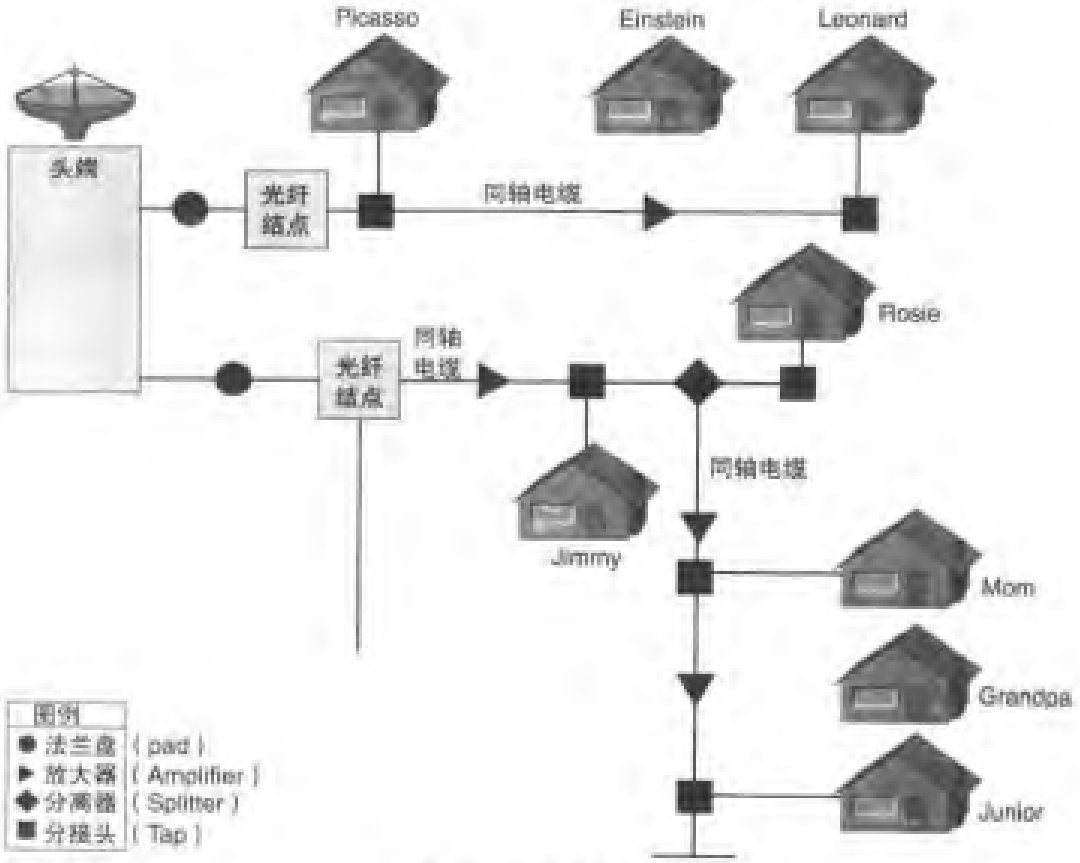


图12-21　电缆调制解调器

使用电缆调制解调器，用户能够在接收有线电视服务的同时接收送往个人计算机的数据。当然要实现这种方式还需要一个简单的1转2分离器，如图12-2所示。

类似于DSL，用户只有使用电缆调制解调器连接到因特网服务提供商（ISP），再通过一个TCP/IP应用，比如Telnet，才能连接到企业网络中。另一个更大缺点是所有本地用户共享电缆的带宽，就像使用同轴电缆的以太网连接的情况。当更多的用户使用这种服务时，实际的带宽可能比预期的要低。一个更加严重的问题就是安全：家庭计算机不仅受到来自因特网的攻击，还会受到自己电缆上用户的攻击。因此一些本地防火墙模式的保护是基本的。

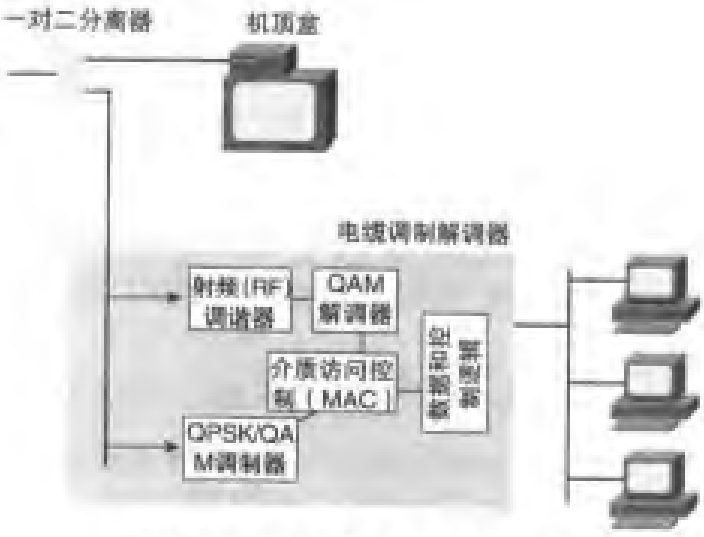


图12-22　电缆调制解调器两路分离器

为了解决安全的问题，电缆调制解调器服务提供使用虚拟专用网（VPN）连接到通常放置在公司网上的VPN服务器的能力。

12.7　广域网通信

当今的网络管理员必须管理复杂的广域网，来支持大量增长的围绕着因特网协议（IP）和Web所构建的软件应用。这些广域网需要大量的网络资源和高性能的连网技术。广域网环境混合了多种

介质和多种协议，并互连了诸如因特网之类的其他网络。复杂的协议和特性交互完成了这种网络环境的发展和管理。

无论设备性能和介质能力如何改进，广域网设计都变得更加困难。谨慎设计广域网可以减少与连网环境增长相关的问题。为了设计可靠的、可扩展的广域网，网络设计者必须记住：每个广域网都有特殊的设计需求。以下章节对广域网通信和设计方法论的利用进行了概述。

广域网被认为是连接到LAN上路由器的一组数据链路。在LAN上的用户终端站点和服务器间交换数据。路由器根据需要在LAN之间通过数据链路传输数据。

广域网通信发生在分隔的地域之间。当一台本地终端站点想与一台远程终端站点（也就是位于不同地点的一台终端站点）通信时，其信息必须经过一条或多条广域网链路。广域网中的路由器是网络的连接点。这些路由器为那些需要穿越网络的数据流确定其最合适的路径。

通常情况下，由于代价和法律的原因，构成一个广域网的数据链路由通信提供商或通用运营商所拥有，并按一定费用提供给企业使用。

电路交换技术和分组交换技术是两种广域网服务类型，有其各自的优缺点。例如，电路交换网络为用户提供专用的带宽，这个带宽不能被其他用户占用。与之相反，分组交换是网络设备共享一条点到点链路，将分组从源经过运营商网络传输到目的的方式。传统上，分组交换网络提供比电路交换网络更高的灵活性，并能更有效的使用网络带宽。这些互连LAN或连接LAN到其他网络的链路通常提供远低于100Mbit/s的数据传输速率（带宽），而100Mbit/s是LAN的普通速率。提供链路费用是一个广域网的主要花费，广域网的设计目的必须以合理的代价提供合理的带宽。在要求以更高的速率提供更多的服务访问的用户压力和控制代价的管理压力下，决定最佳的广域网配置不再是一件简单的任务。

广域网可以承载不同类型的流量，例如语音、数据和视频，并且所选用的设计必须提供足够的容量和传输时间来满足企业的需求。这包括指定不同站点间的连接拓扑、这些连接的特性和容量以及其他的事情。

早期的广域网常常由直接连接位于不同地域的大型计算机的数据链路组成，而现今的广域网则连接位于不同地域的局域网。端用户站点、服务器和路由器位于局域网中，广域网数据链路则在路由器处终结。路由器通过交换所连接局域网的信息，为所需的数据流确定通过网络的最适合的路径。路由器还能对不同的流量给与不同的优先级，从而提供服务质量（QoS）管理。

与当前的广域网相比，新的广域网体系结构必须更复杂，必须基于新技术，能处理有服务级别的要求和保证的持续增长（且快速改变）的应用。此外，预计在下一个5年中会有300%的流量增长率，这使得企业对控制广域网的费用感到越来越大的压力。

网络设计者正在使用广域网技术来支持这些新需求。广域网连接一般处理重要的信息，并对带宽的价格和性能进行优化。例如，连接园区网的路由器通常需要应用流量优化、多条冗余路径、用于灾难恢复的拨号备份和针对关键应用的QoS。表12-3总结了支持这些广域网需求的各种广域网技术。

表12-3 广域网技术总结

广域网技术	典型应用
租用线	租用线可用于点到点协议（PPP）的网络和中心和轴辐拓扑（hub-and-spoke），或者用于备份另一种类型的链路
综合业务数字网（ISDN）	ISDN可用于经济的远程访问企业网。它提供对语音和视频的支持，也作为另一种类型链路的备份
帧中继	帧中继为远程站点之间提供一种经济、高速和低延迟的网状拓扑。它可用于私有网络和运营商提供的网络

因为广域网只是一组基于局域网的路由器间的互连，广域网上没有服务，所以广域网技术功能在OSI参考模型的下3层中实现：物理层、数据链路层和网络层，如图12-23所示。路由器根据网络

层分组头确定数据的目的，并将该分组向下传送给适当的数据链路连接，然后传送到物理连接上。

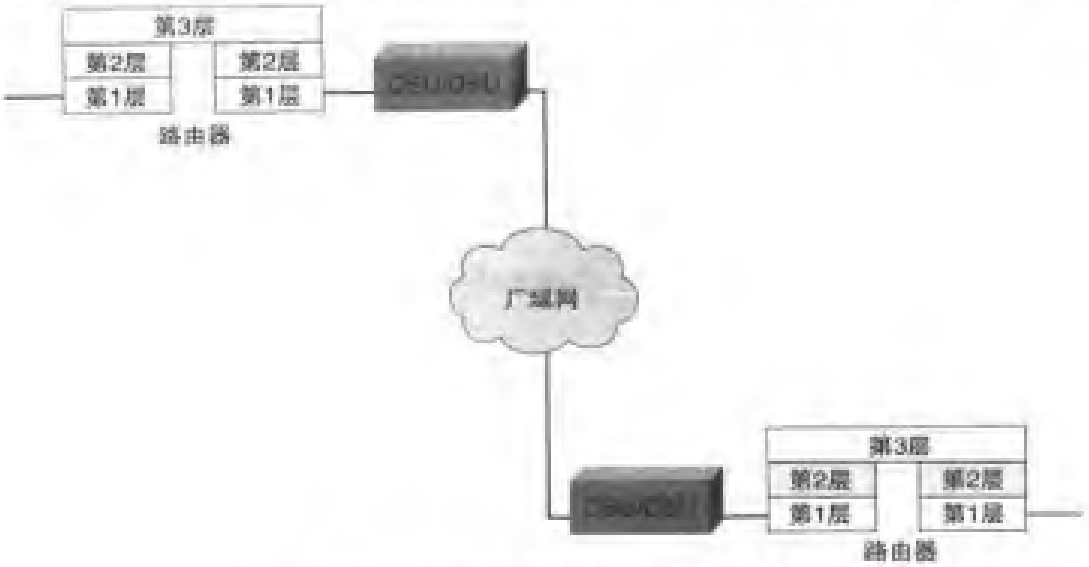


图12-23　运行在第1、2、3层的广域网

一般说来，广域网通信具有相对较低的吞吐量、高延迟和高差错率的特点。从服务提供商处花钱租用介质（也就是线路）将两个或多个园区网连接在一起也是广域网连接的一个特征。由于广域网的基础设施经常从服务提供商处租用，因此广域网的网络设计必须优化带宽的费用和效率。例如，所有用于广域网的技术和特性的开发应满足以下设计需求：

- 优化广域网带宽。
- 最小的成本。
- 为终端用户提供最有效的服务。

目前，传统的共享介质网络由于以下新的网络需求而负担过重：

- 由于企业使用客户/服务器、多媒体和提高生产率的其他应用，使得网络的使用率不断增长。
- 应用需求的更换速率在不断提高，并将继续下去（例如因特网的“推动”技术）。
- 应用程序的不断增加，需要给终端用户提供更好的网络服务质量。
- 各种规模的部门、远程用户、移动用户、国际站点、顾客/供应商和因特网之间正在建立空前数量的连接。
- 爆炸性增长的公司内部网（intranets）和外部网（extranets）产生更高的带宽需求。
- 服务于企业商务需求的企业级服务器的使用持续增加。

12.7.1　局域网/广域网集成

分布式应用不断地需要更多的带宽，而因特网使用的爆炸性增长使得许多局域网的体系结构达到了极限。语音通信已经显著增长，目前正更多地依赖于集中的语音邮件系统以实现口头通信。网络是信息流动的关键性工具，需要花费更少，但要支持新兴应用和大量用户的性能增长需求。

直到现在，局域和广域的通信仍然只是逻辑上的区分。在局域网中，带宽是免费的，连通性只受限于硬件和实现的费用。在广域网中，带宽比费用更重要，延迟敏感的流量（如语音）仍旧与数据区分开。

因特网应用，如语音和实时视频需要更好的、更可预知的局域网和广域网性能。这些多媒体应用很快会成为商业生产力工具的实质部分。当公司开始考虑实现新的基于内连网的、带宽敏感的多媒体应用时，例如视频培训、视频会议和基于IP的语音，这些应用将对已有的网络体系结构产生严

重的影响。

举例来说，如果一个公司的关键商业性IP流量依赖于它的企业网，并且希望集成一个在线的视频培训应用，那么它的网络必须能提供QoS保证。这个QoS必须能传输多媒体流量，但又不能干扰关键商业流量。因此，网络设计者需要更大的灵活性以解决多个网络互连问题，而又不会创建多个网络或取消现有的数据通信投资。

12.7.2 识别和选择网络能力

在了解网络需求之后，必须要识别并选择适合计算环境的特定性能。下面一节帮助完成这些任务：选择一个互连模式或不同位置间的链路布局，以及选择价格合理的链接技术来满足企业需求。

许多广域网常常因为历史原因而使用星型拓扑。当企业增长并添加新的分支部门时，这些分支部门被接回总部，呈现传统的星型布局。有时，因为可靠性或延迟或者其他原因，一些星型端点会交叉连接，导致一种网状或部分网状拓扑。在星型结构和全网状结构之间，还有许多可能的互连布局。在设计一个新的广域网时，或者更普遍的是重新评价或修改一个已有广域网时，必须选择能满足设计需求的拓扑。

在选择布局时，有几个因素需要考虑。链路越多花费越大，但目的间有多条路径提高了可靠性。目的间数据传输必须经过的节点或路由器越多，所花费的时间越长，因为通常的情况是：一台网络设备必须完整接收到数据的每一块或每个分组后才能将其转交给下一台网络设备。

表12-4显示了用于数据链路的不同技术和不同特性。

表12-4 广域网技术

数据链路类型	提供商费用	带宽	连接类型
专线	距离，容量	不限	永久/固定的容量
电话线	距离，时间	33~56kbit/s	拨号、低速连接
ISDN	距离，容量	64~128kbit/s	拨号、中速连接
X.25	数量	小于48kbit/s	交换式/固定的容量
帧中继	容量	小于4Mbit/s	永久/固定的容量
ATM	容量	小于155Mbit/s	永久/固定的容量

有些技术需要在传输数据之前建立一条连接，例如基础的电话、ISDN或X.25，它们不适合用于需要低响应时间或低延迟的广域网（尽管一旦连接建立之后，ISDN和电话都是低延迟和低抖动的电路）。ISDN特别适用于将小型或家庭办公（SOHO, small or home office）接入企业网络，提供快速连接和能改变的带宽。ISDN还可作为主要连接的备份链路，并提供与主要连接并行的按需带宽连接。这些技术的一个特性就是它们仅在使用时才会产生费用。

企业的另一部分可能直接用租用线连接起来，或者用一条到最近一个共享网络接入点（POP）的接入链路连接起来。X.25、帧中继和ATM都是共享网络的例子。租用线通常比接入链路长而且贵，但实质上可得到任意的带宽，并且提供低延迟和低抖动。

ATM、帧中继和X.25网络在同一条内部链路上承载若干用户的流量。企业不能控制数据穿越共享网络时必须经过的链路的数量或者跳数，又或者是数据在每台网络设备中等待转发至下一条链路所必须等待的时间。这种延迟和抖动的不确定性使得这些技术不适合于某些类型的网络流量。但是，共享网络的费用共享特点远远胜过它的这个缺点。因为多个用户共享一条链路，所以每个用户的费用远小于具有相同容量的直接链路费用。

尽管ATM是一个共享网络，但是它的设计目的是提供最小的延迟和抖动，通过使用高速内部链路来发送易于处理的数据单元，即信元。ATM信元有53字节的固定长度，其中数据48字节，头部5字节，广泛用于承载对延迟敏感的流量。帧中继也可以用于对延迟敏感的流量，它通常使用QoS机

制为敏感度更高的数据赋予优先级。

一个典型的广域网使用根据流量类型和数量所选择的多种技术组合。ISDN、帧中继或租用线用来将单独的部门接入一个区域；帧中继、ATM或租用线用来将这些区域接入骨干；ATM或租用线则组成广域网骨干。

12.7.3 识别和选择连网模型

网络设计的层次模型允许按层次设计网络。要理解分层的重要性，可以思考一下OSI参考模型，它是了解计算机通信的一个分层模型。OSI参考模型使用层次来简化两台计算机的通信任务。网络设计的层次模型也同样使用层次来简化网络互连。每一层都专注于特定的功能，从而允许连网设计者为本层选择合适的系统和特性。

使用层次设计易于改变。网络设计的模块化允许创建设计元素，这些元素可以随着网络的增长而被复制。同样，因为网络需要升级，升级的费用和复杂程度也被限制在整个网络的一小部分中。在大型的平面或网状网络体系结构中，改动将会影响到大多数系统。将网络分割成小而易于理解的元素，可以较为容易地发现网络中的故障点。网络管理者可以容易地理解网络的转换点，从而帮助识别故障点。

12.7.4 分级网络设计模型

网络设计趋向于以下两种常规设计策略之一：网状或层次。在网状结构中，网络拓扑是平面的，所有路由器完成本质相同的功能，通常没有明确定义何处应完成何种特定功能。网络的扩展往往是偶然面又任意进行的。在层次结构中，网络按层次来组织，每一层有一个或多个特定功能。使用层次模型的好处如下：

- **可扩展性**——层次模型的网络因为其局部功能性和潜在问题易于发现，所以可在不牺牲控制或可管理性的情况下大幅增长。大规模层次网络设计的一个例子就是公共交换电话网（PSTN）。
- **易于实现**——层次设计为每层指定了清楚的功能，从而使得网络实现更容易。
- **易于故障排除**——由于每层的功能定义良好，所以网络中的问题隔离并不复杂，也易于临时将网络分段以缩小问题的范围。
- **可预测性**——使用功能层次的网络，其行为是可以预测的，这使得增容计划相当容易。这种设计方法也有助于为分析目的而建立网络性能模型。
- **协议支持**——在遵循层次设计原理的网络中更容易混合当前和未来的应用与协议，因为底层基础设施已经被逻辑的组织起来了。
- **易管理**——这里所列举的所有好处都使得网络更易于管理。

12.7.5 3层设计模型

层次网络设计包括以下3个层次：

- **核心层**（*core layer*），提供站点间的最优传输。
- **汇聚层**（*distribution layer*），提供基于策略的连通性。
- **接入层**（*access layer*），为工作组和用户提供网络接入。

图12-24显示了一个层次网络设计各方面特征的高级视图。

想象有一个企业，可能是一个在欧洲每个国家都运行的金融机构，在所有人口超过10,000的城镇中都有一个分支机构。每个分支机构都有一个局域网，并且决定将这些分支机构互连到一个广域网中。一个网状网络显然不可行，因为900个中心需要将近50万条链路。而一个简单的星型网络也很

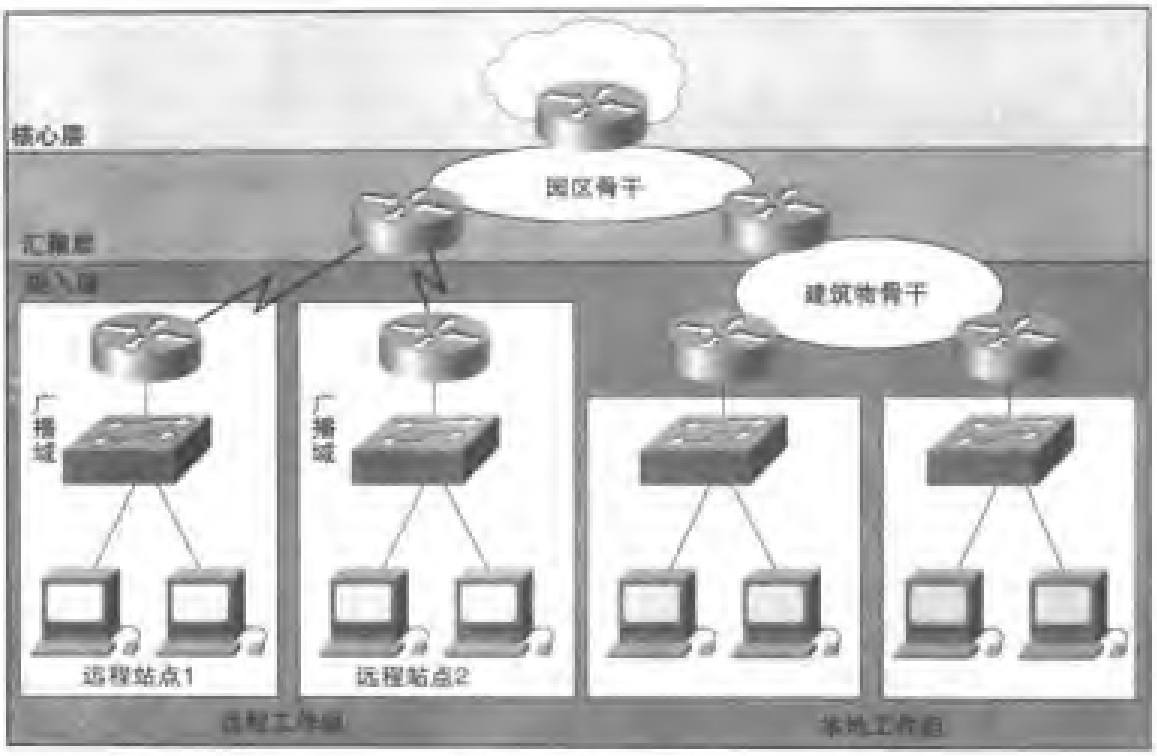


图12-24 层次网络设计

难实现，因为在中心处需要一台具有900个接口的路由器或者需要一个接口上要具有900条用于分组交换网络中的虚电路。

考虑更换为一种层次设计模型，将一个区域中的一组局域网互连起来，再互连这些区域从而形成一个地区网络，最后将这些地区互连在一起形成广域网的核心。

每个区域可以根据连接的地点数目（最多30~50个）或按照传统的地理边界来划定。区域网络的拓扑可以是如图12-25所示的星型拓扑，并由这些星型的中心形成相应的地区网络，可能还是星型结构。一个地区可以地理上连接3到10个区域，每个地区的中心又可以被点到点的链接起来，如图12-26和图12-27所示。

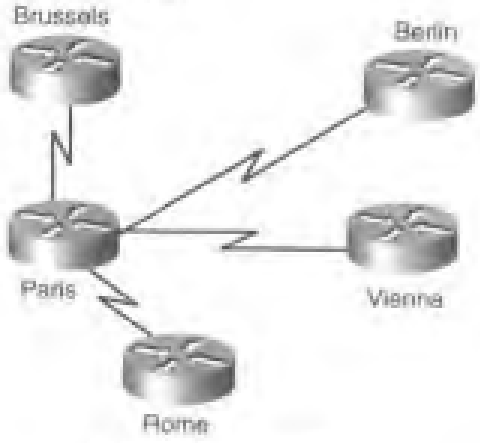


图12-25 层次网络

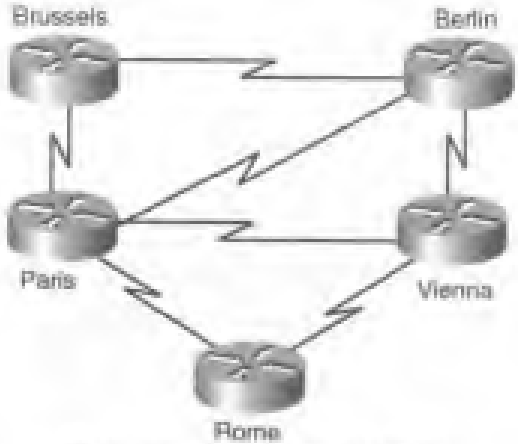


图12-26 连接多个区域的网络1

这种遵循上述层次体系的3层模型用在电话系统中。连接一个区域中不同站点的链路被称为广域网的接入链路或接入层，它将这些站点接入到企业网络中。区域间的流量由分发链路分发，并在需要的时候移送至核心链路，从而传送到其他地区。

这种分层结构常被证明是有用的，网络流量反映一个企业分支结构，它被划分成地区、区域和分支机构。这种分层结构在下面这种情况中也被证明是有用的：所有分支机构必须访问一些重要服

务，但是此时无法从流量上充分证明某个分支机构与这些服务的直接连接。

区域中心的局域网中可以具有提供区域级和本地服务的服务器。根据流量的大小和类型，接入连接可以是拨号（例如ISDN）、租用线或帧中继。帧中继易于实现冗余的网状化，而无需额外的物理连接。分布链路可以是帧中继或ATM，网络核心则是ATM或租用线。

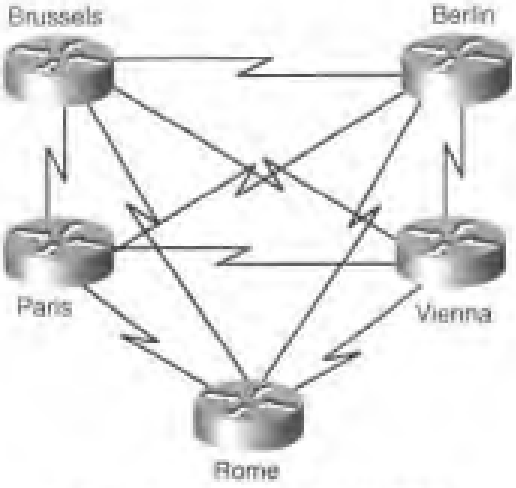


图12-27　连接多个区域的网络2

12.7.6　3层模型组件

每一层作为网络中的一个点由OSI参考模型的第3层（网络层）来界定：由第3层设备或分隔网络广播域的其他设备来界定这3个层次。3层模型由核心层、汇聚层和接入层组成，每层都有特定的功能：

- **核心层**——核心层提供地理上远距离站点间的快速广域连接，将许多园区网络和公司或企业广域网连接在一起。核心链路通常是点到点的，并且在核心层很少有主机。核心服务（例如T1/T3、帧中继、SMDS）主要从自电信服务提供商处租用。
- **汇聚层**——汇聚层在广域网环境中为多个局域网提供网络服务。本层是园区网的骨干网络，通常基于快速以太网。本层在大型站点中实现，用于建筑物间互连。
- **接入层**——接入层通常是一个局域网或一组局域网，典型的如以太网或令牌环网，直接为用户提供接入网络的服务。接入层几乎是所有主机接入网络的地方，包括各种服务器和用户工作站。第5章“交换原理和局域网设计”中详细介绍了接入层的设计。

3层模型可以满足大多数企业网络的需要，但并不是所有的环境都需要完整的3层结构。在某些情况下，两层设计甚至是一层的平面网络就足够了。在这些情况中，层次结构设计允许一层或两层的网络随着需要的增长扩展为3层结构。以下章节将讨论这3层的详细功能，然后再讨论一层和两层结构。

1　核心层功能

核心层的功能是在远程站点之间提供一条快速路径，如图12-28所示。网络的核心层不应该执行任何的分组处理，例如使用访问控制列表来完成过滤，这会降低分组交换的速度。核心层通常作为广域网实现。广域网需要冗余路径，使网络能经受住单电路故障而继续工作。负载共享和快速收敛的路由选择协议也是重要的设计特征。有效利用核心层的带宽总是至关重要的。

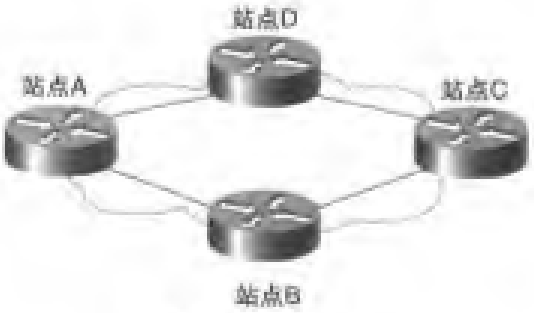


图12-28　核心层

2　汇聚层功能

网络的分发层是接入层与核心层的分界点，帮助定义和区分核心。本层的目的是提供界限定义，并且在本层处理分组。在广域网环境中，分发层可以包括如下一些功能：

- 地址或区域聚合。
- 将部门或工作组接入核心层。
- 广播/多播域的定义。

- 虚拟局域网（VLAN）路由选择。
- 需要出现的任何介质转换。
- 安全。

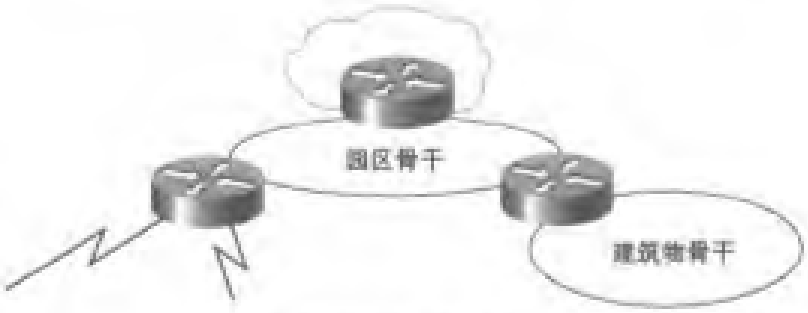


图12-29 分发层

分发层包括园区网骨干和所连接的路由器，如图12-29所示。由于策略通常在这一层实现，因此可以说分发层提供了基于策略的连通性。基于策略的连通性是指园区网骨干上的路由器被编程设定只允许可接受流量。注意，好的网络设计实例不会将末端站点（如服务器）放在骨干网上，这缓解了骨干网，使其严格的作为工作组间或园区服务器间的流量传输路径。

在非园区环境中，分发层可以是远程站点接入公司网络的一个点。分发层可以被概括为提供基于策略的连通性的一个层次。

3 接入层功能

接入层是允许本地终端用户进入网络的地点，如图12-30所示。本层可同样使用访问控制列表或过滤来进一步优化特殊用户的需要。在园区环境中，接入层包括以下功能：

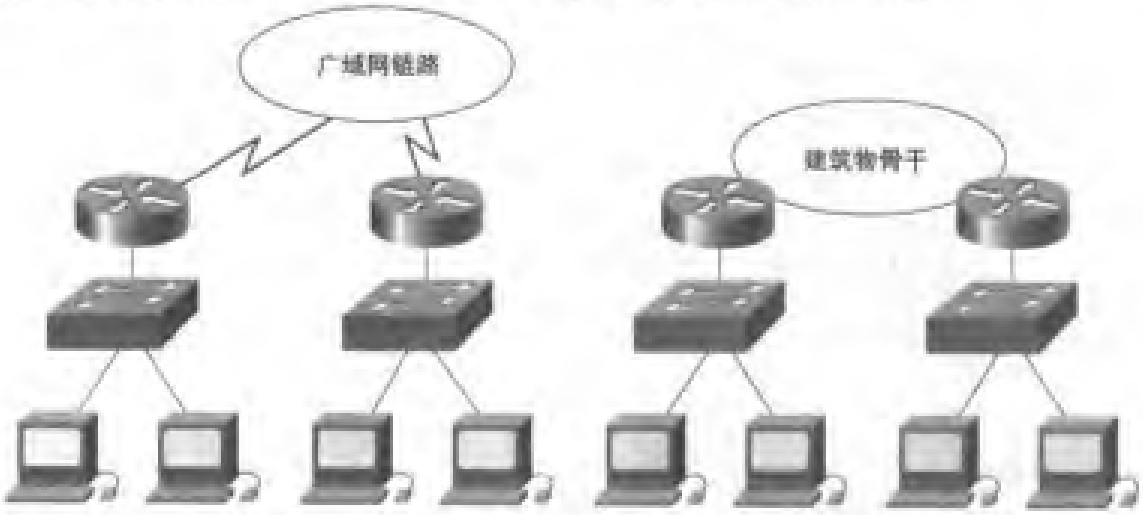


图12-30 接入层

- 共享式带宽。
- 交换式带宽。
- MAC层过滤。
- 微分段。

接入层将用户接入局域网，并将局域网接入广域网骨干或广域网链路。这种方法允许设计者分发运行在本层设备的服务。接入层允许网络的逻辑分段和基于功能的用户分组。传统上，这种分段是基于组织边界的（例如市场部门、行政部门或工程部门）。但是，从网络管理和控制的观点来看，接入层的主要功能是将广播流量隔离在单个工作组或局域网。在非园区环境中，接入层可以通过广域技术（例如帧中继、ISDN或租用线）将远程站点接入公司网络。

12.7.7 分级广域网设计的优点

层次广域网设计的一个优点是提供了一种通过在整个网络放置第3层路由选择点来控制数据流

量模式的方法。因为路由器具备根据第3层的寻址来确定从源主机到目的主机的路径的能力，所以数据流量只沿着分层结构向上流动直至发现需要的目的主机，如图12-31所示。

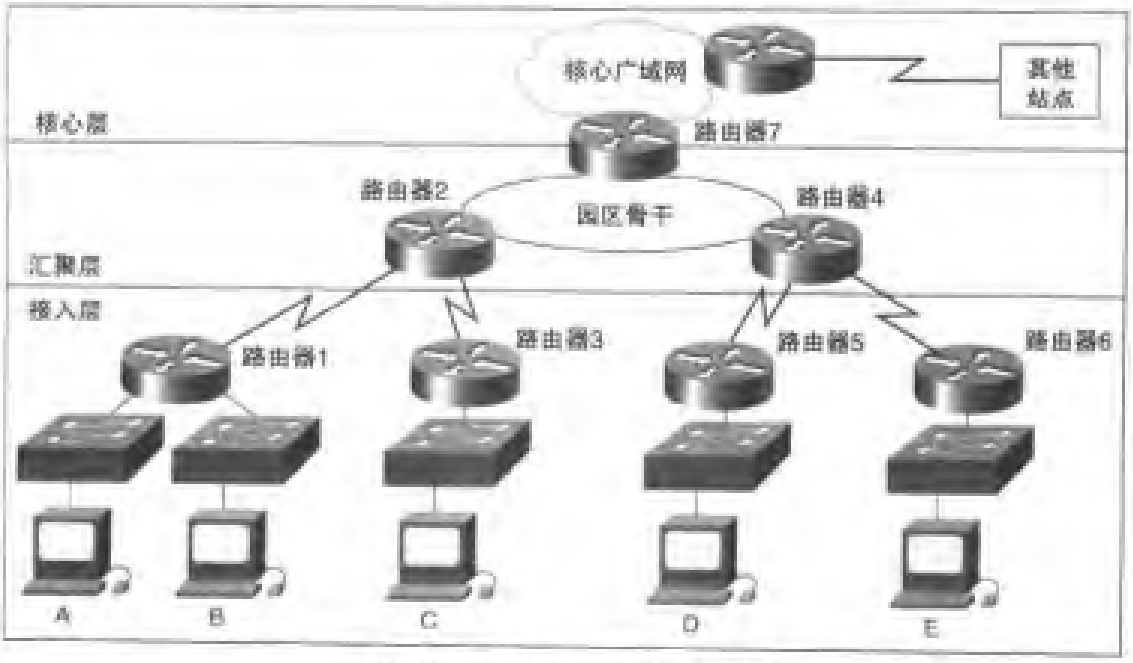


图12-31　路由器是数据路径的决策点

如果主机A建立了到主机B的一个连接，那么这个连接上的流量会到达路由器1，然后向下转发至主机B。注意图12-32中这个连接不需要在路由器1和路由器2之间的链路上产生任何流量，这保留了那条链路上的带宽。

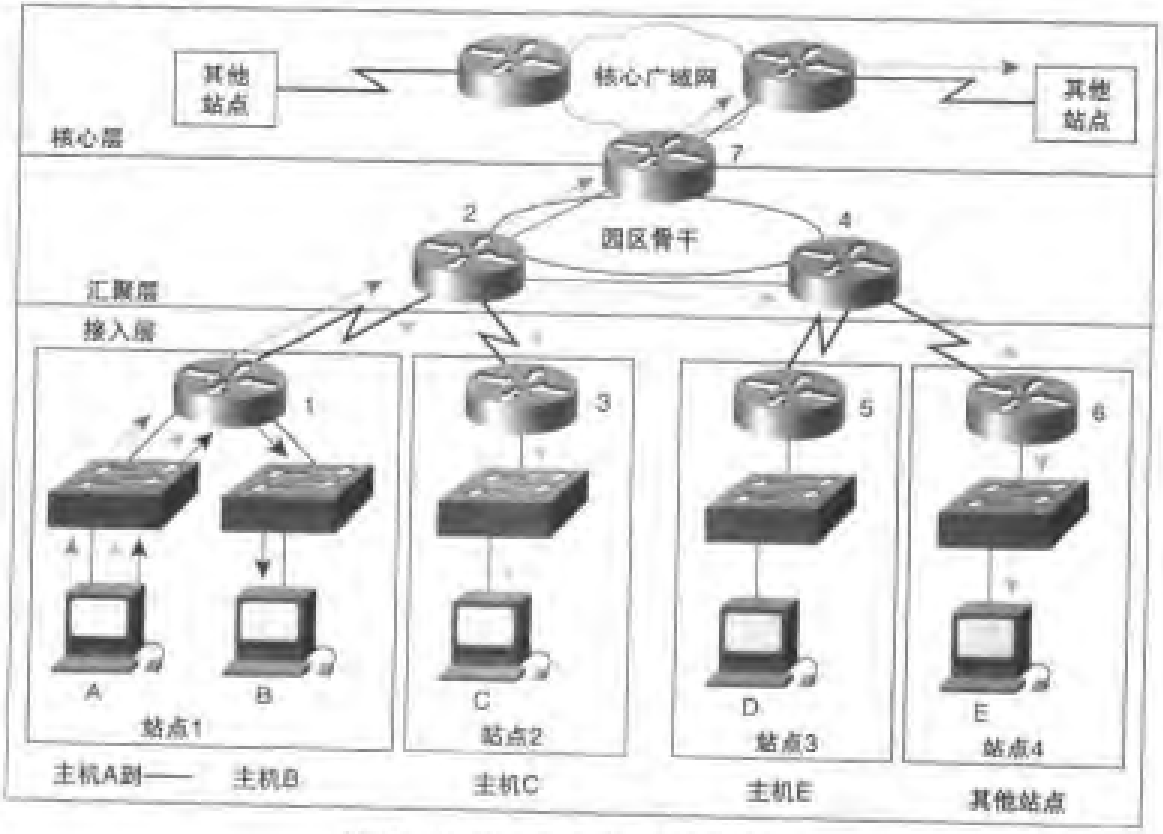


图12-32　基于源/目的寻址的数据流动

在两层的广域网结构中，如图12-33所示，流量仅沿分层结构向上流动直到目的地，这保留了

给其他广域网链路的带宽。

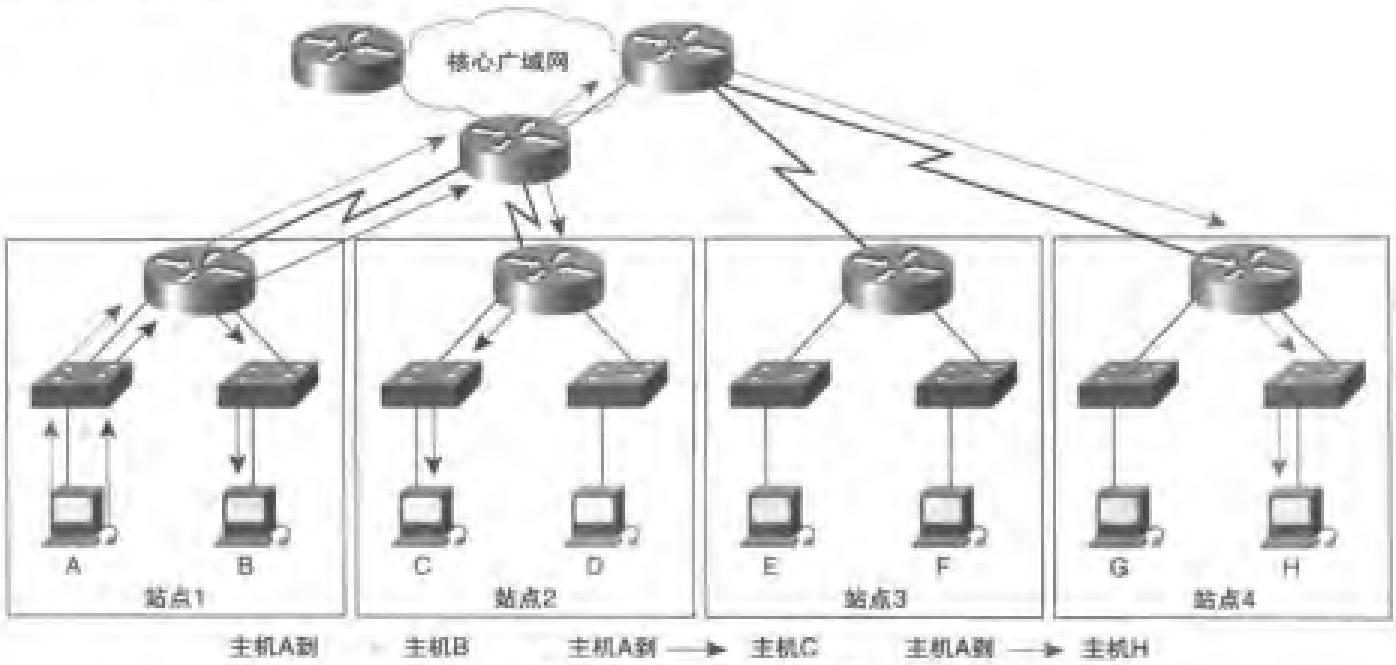


图12-33 两层广域网结构

12.7.8 服务器的放置

需要访问的服务器的放置会影响广域网中的流量模式。如果将企业服务器放在站点1的接入层，如图12-34所示，那么所有去往该服务器的流量必须通过路由器1和路由器2之间的链路。这会消耗站点1的大量带宽。

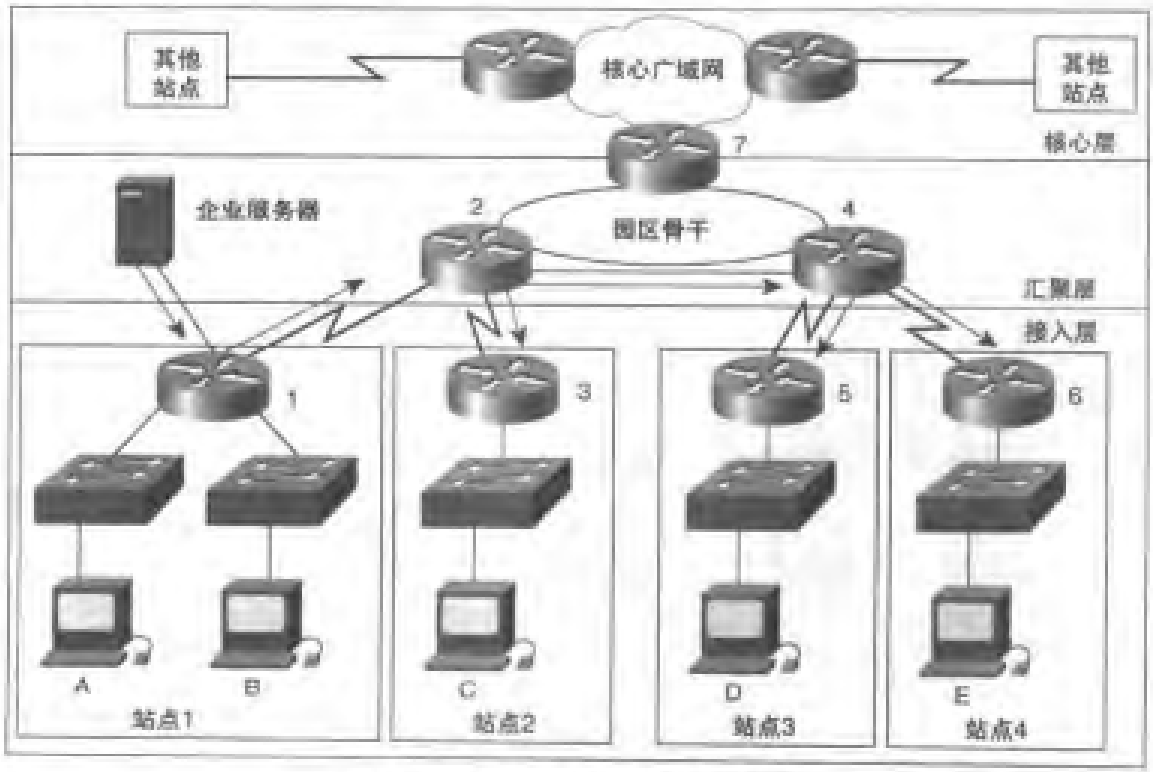


图12-34 将企业服务器放置在接入层

如果将企业服务器放在分层结构的更高一层上，如图12-35所示，会减少路由器1和路由器2之

间链路上的流量，站点1的用户就能够访问其他服务。在图12-36中，一台工作组服务器被放置在用户大量集中的站点接入层，并限制了通过广域网链路访问服务器的流量。这样一来，更多的带宽可以用来访问该站点之外的资源。

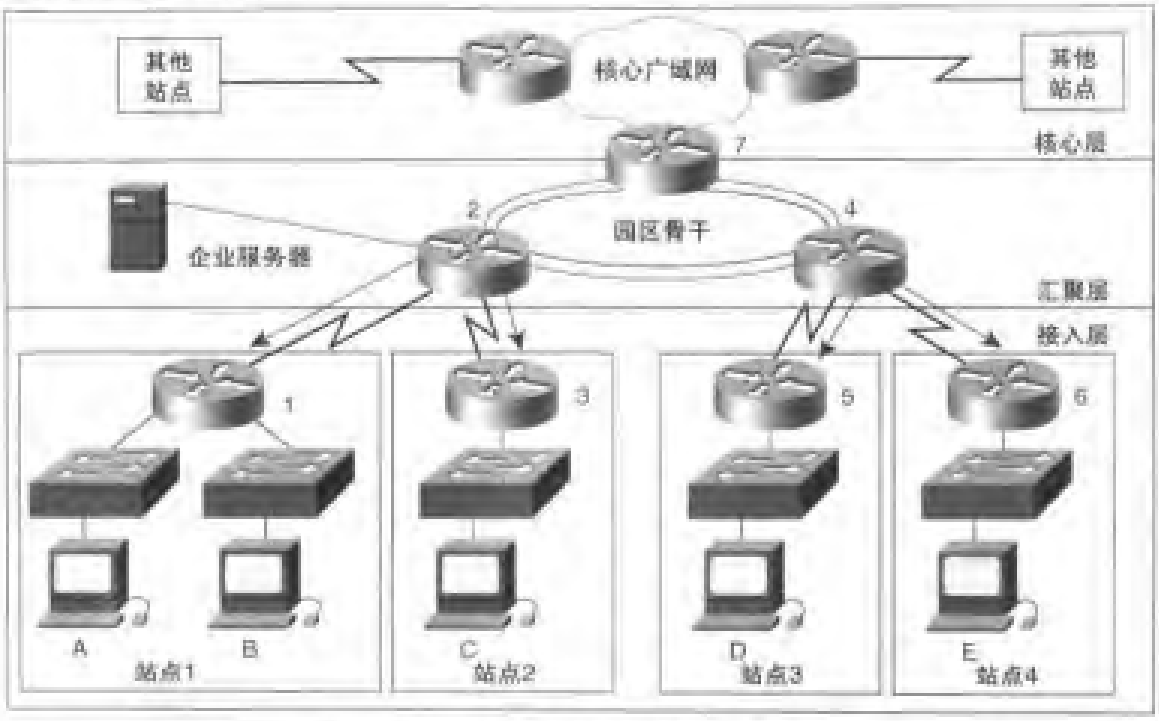


图12-35　将企业服务器放置在更高的一层上

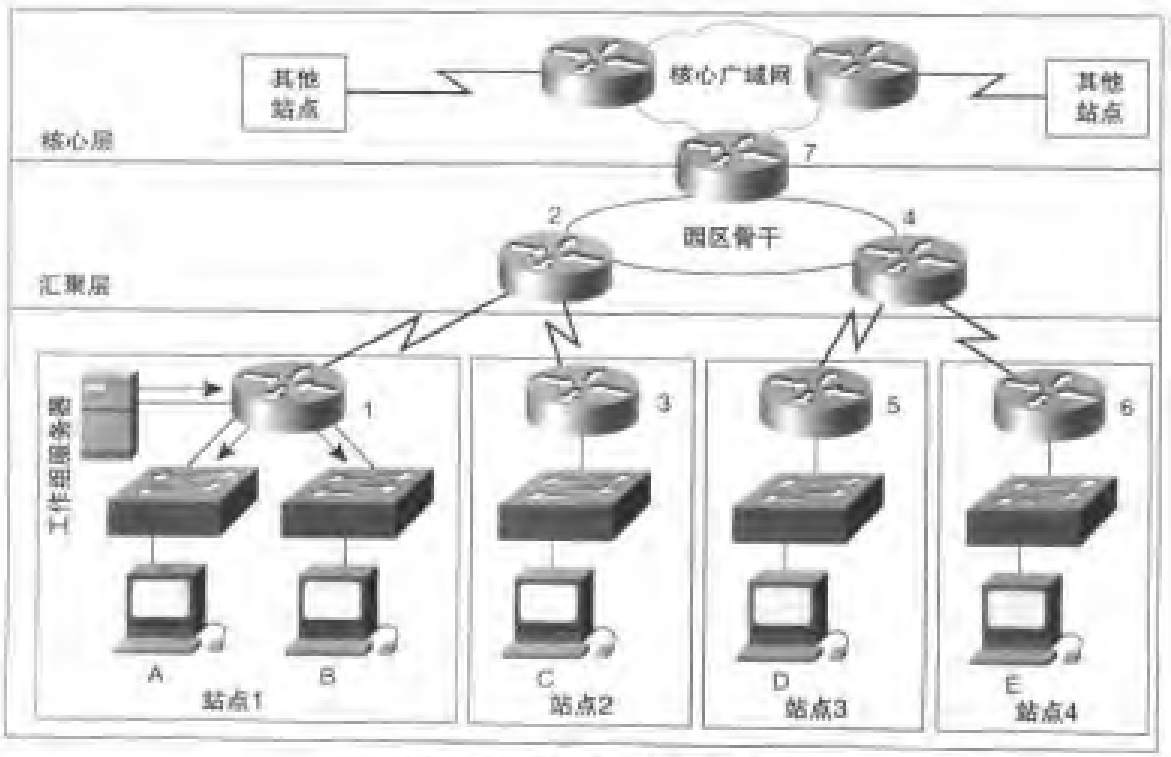


图12-36　工作组服务器的放置

12.8　广域网设计

如果企业中所有的数据流都在一座建筑物中，那么可以使用局域网来承载这些流量。如果一些

数据必须在一个园区的建筑物之间流动，那么可以使用高速的数据链路来互连这些建筑物，从而形成一个园区局域网。单个的远程接入局域网以及将局域网连入因特网是单独的研究课题，不在这里考虑。如果数据必须在不同地域间传输，就需要用一个广域网来承载这些数据。

大多数学生不会有机会去设计一个新的广域网，但是很多学生将会参与现有广域网的扩展和升级设计，并会用到这里所学的技术。

12.8.1 设计广域网的步骤

设计一个广域网是一项具有挑战性的任务。以系统的方式来设计可以产生优良的性价比。许多广域网随着时间而发展，已经不是遵循这里所讨论的指导方针的最初设计了。但是，每次考虑修改现有广域网时，就应该使用这里所概括的步骤。广域网的修改可能因为一些变化，例如广域网所服务的企业扩张或者是为了适应工作习惯或商业方法的改变。

商行和公司建立广域网的原因是他们需要在企业的多个分支机构间及时传送数据。满足这种商业需求会产生数据链路的费用、主要供应和管理问题。

为了设计广域网，就必须知道承载哪些数据流量、从何处以及到何方。广域网根据不同带宽、延迟和抖动需求承载不同的流量类型。对每对端点和每种流量类型来说，需要各种流量的特征信息。要确定这些信息可能需要进行广泛的学习并咨询各种各样的网络用户。设计通常包括对现有广域网的升级、扩展或修改。大部分所需的信息都可以从现有网络管理统计中获得。

需要知道不同的端点允许选择广域网的拓扑或布局。地理上的考虑将影响拓扑，而诸如可用性之类的需求也将对拓扑有所影响。例如，高可用性需求需要额外的链路来提供备选的数据路径。

通过选择端点及其链路，可以用一部分运载自己流量的带宽和另一部分运载来自其他源的聚合流量的带宽来估算链路的必需带宽。

链路上的流量对延迟和抖动有不同的需求，这些需求与已经确定的带宽一起允许为链路选择适当的技术。广域网的安装和运行费用可以测定，并与驱动广域网供应的商业需要相对比。

在计划一个广域网实现时，要谨慎考虑以下所讨论的几个要点。这里所描述的步骤可以帮助改进广域网的费用和性能。在计划过程中综合这些步骤可以使商行持续改进其广域网。

驱动广域网设计和实现的两个主要目标是：

- **应用的可用性**——网络承载计算机之间的应用信息。如果网络用户无法使用这些应用，那么网络就没有用。
- **所有者的总费用**——信息系统（IS）部门的预算经常是几百万美元。当大公司日益依赖电子数据来管理其商业活动时，与计算资源有关的费用就会持续增长。一个设计良好的广域网有助于平衡这些目标。正确实施的广域网基础设施可以优化应用的可用性，并允许经济地使用现有的网络资源。

通常，广域网设计需要考虑3个实际因素：

- **环境变量**——环境变量包括主机、服务器、终端和其他端节点的位置；该环境中的计划流量以及提供不同服务级别的预计成本。
- **性能约束**——性能约束包括网络的可靠性、流量吞吐量和主机/客户计算机的速度（例如，网络接口卡和硬盘访问的速度）
- **连网变量**——连网变量包括网络拓扑、线路容量和分组流量。网络流量的特征是广域网规划的成功关键，但是几乎没有几个规划者做好这关键的一步。

广域网设计中没有比广域网所承载的流量类型更关键的特征了。

流量类型包括：

- 语音/传真。
- 事务数据（如SNA）。

- 客户/服务器数据。
- 消息传递（如E-mail）。
- 文件传输。
- 批量数据。
- 网络管理。
- 视频会议。

分析和分类流量是关键设计决策的基础。流量影响容量，而容量又影响着成本。测量和估计流量的时间检验方法是针对传统网络的，并不适用于广域网。

流量特性包括：

- 峰值和平均流量。
- 连通性和吞吐量。
- 连接方向。
- 延迟的容忍度，包括长度和可变性。
- 网络可用性的容忍度。
- 差错率的容忍度。
- 优先级。
- 协议类型。
- 平均分组长度。

由于许多网络规划者不具有设计和规划流量复杂的和不定性的广域网技术，他们通常是猜测带宽的容量，结果导致了昂贵的超设计要求的网络，或者是低性能的低于设计要求的网络。

广域网设计的总体目标是以最少的成本提供不损害既定的可用性需求的服务。这需要面对两个主要问题：可用性和成本。它们在本质上是对立的。任何在可用性方面的提升必然反映到成本的增加。因此，必须谨慎估量资源可用性和总体成本的相对重要性。

设计过程的第一步是了解业务需求，这将在随后的小节中介绍。广域网需求必须反映其运行的目标、特性、业务过程和业务策略。

12.8.2 收集需求

设计一个广域网时，需要从收集关于业务结构和过程的数据开始。然后需要确定有助于设计网络的重要人员。需要与重要人员商谈并获得他们的地理位置、目前的应用以及他们的计划需要。最终的网络设计应能反映用户的需求。

一般而言，用户首先希望他们网络中的应用具有可用性。应用可用性的主要组件是响应时间、吞吐量和可靠性：

- 响应时间是从输入一条命令或按键开始，主机系统执行该命令或传送应答的时间。认为快速响应时间是关键的应用包括交互式在线服务，例如自动播音员和销售点的机器。
- 高吞吐量的应用一般涉及文件传输活动。但是，高吞吐量应用通常也有低响应时间的需求。实际上，可以在响应时间敏感的流量较少时调度这些应用（例如在常规的工作时间之后）。
- 尽管可靠性一直很重要，一些应用的实际需求还是要超出典型需要。组织机构需要近100%的正常运行时间来进行所有在线或经由电话来实施的业务活动。例如金融业务、证券交易、急救中心、警察局和军事行动，它们需要高级的硬件和冗余。确定停机时间的代价就是确定网络可靠性的重要性。

评估用户需求有很多方法。在过程中越接近用户，评估就越准确。一般而言，可以使用以下方法来获取信息：

- **用户团体的简介**——不同用户群需求的概要。这是确定网络需求的第一步。尽管许多用户有

相同的电子邮件需求，但是他们仍然会有不同的需要，例如在区域中需要共享本地打印服务器。

会谈、集中用户群和调查，这些确立了网络实施的基线。了解一些群体可能需要访问公共服务器，而另一些群体则可能希望允许从外部访问特定的内部计算资源。一些机构可能需要IS支持系统以一种特殊的方式依照一些外部标准来进行管理。

获取信息的非正式方法是与关键的用户群会谈。也可以使用集中用户群的方法来收集信息，并在具有相似（或相异）兴趣的不同机构间开展讨论。最后，正式调查可以用来获得用户对具体服务水平意见的有效统计数据。

• **人力因素测试**——最昂贵、最消耗时间以及评估用户需求的可能方法是在实验室环境下测试具有代表性的用户。这在估算响应时间需求时是十分可行的。例如，可以建立工作系统并让用户从实验网络执行普通的远程主机活动。通过评测用户对主机响应的反应，可以创建可接受性能的基准阈值。

在收集了关于公司结构的数据以后，需要确定公司内的信息流向。找出共享数据的放置处以及使用者。确定外部数据能否接入公司。

要确信已经了解了现有网络的所有性能。如果时间允许，分析现有网络的性能。

12.8.3 分析需求

网络的需求需要进行分析，包括客户的业务和技术目标，将要实施哪些新应用？有没有基于因特网的应用？将要接入哪些新网络？什么是成功的标准？（怎么知道新设计是否成功？）

可用性度量了网络的有效性。许多事件都会影响可用性，包括吞吐量、响应时间和访问资源。每个客户对可用性的定义都不同。可以通过添加更多的资源来提高可用性，但是资源会抬高成本。网络设计所寻求的是以最少的成本提供最大的可用性。

分析需求的目的是确定每个源在一段时间内数据率的均值和峰值。尝试着根据经过流量的类型、流量级别、主机的响应时间以及执行文件传输的时间来描绘一个普通工作日的活动吞吐量。还可以观察测试阶段中现有网络设备的使用情况。

根据流量类型，使用以下4种技术之一来分析和测量流量：

• **网络管理软件**——对某些流量，可以使用网络管理软件来分析流量的统计信息。

• **现有的测量**——可以在服务器上放置网络分析设备，根据路由器的统计分析现有网段的分组传送。

• **估算方法**——当现有的测量无法完成时（例如应用根本不存在），可以使用估算过程。即与应用开发商和网络管理员一起估算事务处理速度、时间长度和传送，从而推导出流量的统计信息。

• **比较来源**——可以找到已知的具有相似特性的来源，从而调整流量统计信息。

如果所测试网络的特性接近新网络的特性，就可以根据计划的用户数、应用和拓扑估算出新网络的需求。这是在缺乏测量详细流量行为的工具时估计流量的最佳推测方法。

除了监控现有网络之外，还可以测量一个典型测试网络上已知数量的用户所产生的活动和流量，然后根据结果推算出预期人数的活动和流量。

定义网络工作载荷的一个问题是由于用户数量、应用类型和地理位置，很难精确地确定流量负载和网络设备性能。在没有真实的网络时，这个问题尤为突出。

考虑以下影响动态网络的因素：

• **网络接入的时间相关特性**——峰值阶段不同，测量必须反映包含峰值要求在内的观测范围。

• **流量类型的差异**——被路由和桥接流量对网络设备和协议有不同的要求，有些协议对丢弃分组敏感，有些应用类型需要更多的带宽。

• **网络流量的随机特性**——流量的精确到达时间和特定结果是不可预知的。

每个流量源有自己的量度标准，必须将这些量度值转换成比特每秒（bit/s）。还应该标准化流量

来获得每个用户的流量。最后，应该用一个因子来计算协议开销、分组碎片、流量增长和安全冗余。通过因子的变化，可以进行假设分析。例如，在一台服务器上运行微软的Office软件，然后分析网络上共享该应用的用户所产生的流量。这个流量值可以帮助确定在网络上带宽的需求和安装微软Office软件的服务器需求。

12.8.4　敏感性测试

从实践的角度来看，敏感性测试包括中断稳定链路并观察发生的事件。当在一个测试网络中工作时，这相对容易一些。可以删除一个活动的接口来扰乱网络，然后监视网络如何处理这种变化：如何重新路由流量、收敛速度、是否有连接丢失以及在处理指定类型流量时是否出现问题。还可以改变网络的流量级别，来确定当流量级别接近介质的饱和度时对网络的影响。

12.8.5　广域网拓扑

网络的拓扑是指互连的布局。尽管可能有许多不同的拓扑，但它们都基于几种简单布局。

一条链路连接两个局域网的拓扑称为点到点拓扑，如图12-37所示。还可以连接其他局域网并保持点到点的拓扑。这很容易实施，但是具有一个缺点，那就是从一端到另一端的流量必须经过所有的中间节点。优点就是总的互连距离最短。如果线路是租用的这很重要。

为了缩短从某个局域网到另一个局域网的延迟，可以重新互连成一个星型拓扑。此时的链路数量不变，但是星型中的每个叶节点到其他叶节点只需要两跳。链路的长度可能会增加，因此成本也更多。位于星型中心的路由器需要为每一个叶节点提供一个接口，而作为叶节点的路由器则只需要一个广域网接口。

如果需要冗余度或最小延迟，还可以增加多条链路形成一个网状拓扑，如图12-38所示。此时，每个局域网到其他局域网只需要一跳，而网络也更加健壮，因为不会有单节点故障来阻止其他节点的通信。低延迟和健壮性是要付出一些代价的，因为需要更多的接口和链路。

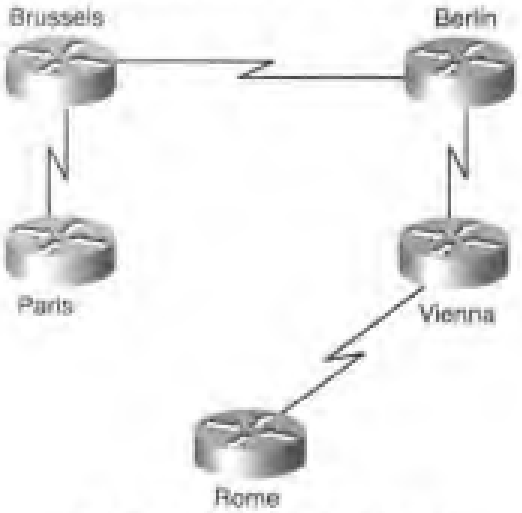


图12-37　广域网的点到点拓扑

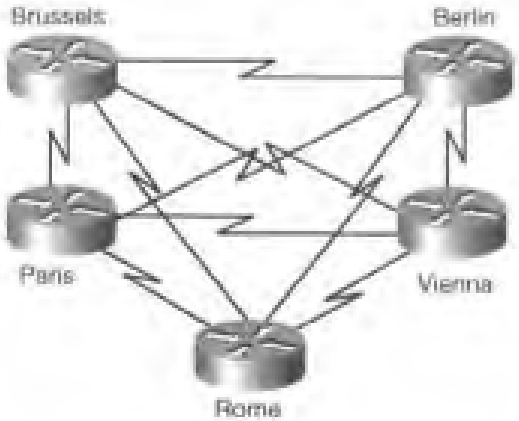


图12-38　全网状的广域网

点到点或星型广域网的链路数量比节点数少1，所以N个节点需要（N-1）条链路。而网状广域网的公式则是$N \times (N-1)/2$。一个具有50个节点的广域网，其星型拓扑需要49条链路，而网状拓扑则需要1,225条链路。对规模较大的广域网来说网状拓扑未必是一种经济的拓扑结构。

这些拓扑可以任意组合。通常基本配置会是星型，但是部分叶节点可以交叉连接，形成一个局部网状的拓扑，如图12-39所示，如果故障发生则能提供一定的冗余。随着网络的增长，这些基本

的拓扑不太具备扩展能力，更大的网络需要一个更具结构化的方案。在随后的小节中将考虑一种层次拓扑。

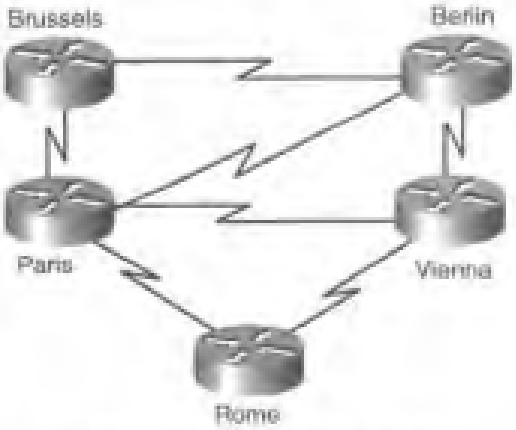


图12-39 局部网状的广域网

12.8.6 如何识别和选择连网能力

设计一个广域网基本上包括选择互连模式或不同位置间的链接布局，以及为链路选择价格合理的技术来满足企业需求。

除电话、ISDN、DSL和电缆之外的其他所有技术都需要一条专用租用线。租用线可以将企业的不同部分直接连接在一起，或者将它们连接到最近的诸如X.25、帧中继或ATM之类的共享网络的接入点（POP）。直接连接的距离通常较长，因此也比较贵，但是它们能获得实际的所有带宽。直接的专线连接具有较低的延迟和抖动。

ATM、帧中继和X.25网络在同一条内部链路上承载若干客户的流量。企业不能控制数据穿越共享网络时的链路数量或跳数，或者是数据在每台网络设备中等待移动到下一条链路的时间。这种延迟和抖动的不确定性使得这些技术不适合于某些类型的网络流量。但是，共享网络的成本共享特点远远胜于它的这个缺点。因为多个客户共享一条链路，所以每个客户的成本远小于具有相同容量的直接链路成本。

尽管ATM是一个共享网络，但是它的设计目的是提供最小的延迟和抖动，主要通过使用很小的数据帧（信元）和高速内部链路来实现。ATM广泛用于承载对延迟敏感的流量。帧中继也可以用于对延迟敏感的流量，它通常使用QoS机制为更敏感的数据赋予优先级。

一个典型的广域网使用通常根据流量类型和容量所选择的多种技术组合。ISDN、帧中继或租用线用来将单独的分支部门接入一个区域；帧中继、ATM或租用线用来将这些区域接入骨干；ATM或租用线则用来构成广域网骨干。

12.8.7 广域网设计的其他考虑事项

许多企业的广域网要连接到因特网。这造成了安全问题，但是也为其分支机构间的流量提供了另一种方法。

必须设计的部分流量是去往或来自于因特网的。因为具有局域网的企业的任何地方都有可能要访问因特网，所以这些流量主要以两种方式承载：每个局域网可以有一条到本地ISP的连接，或者核心路由器单一连接到一个ISP。第一种方式的优点是因特网流量由因特网承载，而不是企业网，因此可能只需要较低的广域网链路带宽。缺点是有多条链路使得整个企业广域网公开在基于因特网的攻击之下，并且难于监控和保护众多的连接点。单个连接点容易管理和保护，即使企业广域网将承载那些本应由因特网所承载的流量。

如果企业中的每个局域网有各自独立的因特网连接，另一种可能是对企业广域网开放。在流量相对较少时，可以将因特网作为企业广域网，所有分支机构间的流量都通过因特网传输。保护各种局域网将成为一个问题，但广域网连接的节省可以补偿这些额外的安全措施。

尽可能将服务器放置在使用量较大的地方。服务器的频繁复制以及非高峰期时服务器间的更新安排都可以减少链路容量的需求。因特网可访问服务的位置取决于该服务的特性、预期的流量、安全问题等等。这是一个专门的设计课题，不在这里考虑。

12.9 总结

本章讨论了以下关键知识点：

- 连接广域网有许多的选择。
- 广域网在不同地域的局域网之间传送数据。
- 通常，广域网所有的数据链路由通信提供商或普通运营商拥有，并按一定费用提供给企业使用。
- 广域网承载多种类型的流量，例如语音、数据和视频；因此广域网设计必须提供足够的容量和传输时间来满足企业的需求。
- 因为广域网只是基于局域网的路由器互连集合而没有业务，所以广域网技术运行在OSI参考模型的下3层。
- 广域网设计通常包括对现有广域网的升级、扩展或修改。
- 存在有许多不同的广域网拓扑，例如点到点、星型和网状拓扑。
- 一个典型的广域网使用多种技术的组合，例如ISDN、帧中继、ATM和租用线。
- 对大型广域网来说，3层的层次设计方案能够提供许多优点。
- 将广域网接入因特网为分支机构间的流量提供了一个备选方案。
- 从家庭办公室远程接入企业网络可以使用模拟调制解调器、ISDN、DSL或电缆调制解调器。
- 一条模拟拨号、ISDN或DSL连接使用现有的电话线，而电缆调制解调器则使用同轴电缆网络。
- 模拟拨号和ISDN仅在需要时拨号并提供连接。DSL和电缆调制解调器则是在计算机开机时一直连接。
- 不同的技术其带宽也不同，DSL和电缆调制解调器的传输速率远远超过模拟拨号和ISDN。

作为本章所学内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

12.10 关键术语

异步传输模式（*Asynchronous Transfer Mode, ATM*） 多种服务类型（如语音、视频或数据）在固定长度（53Bytes）的信元中传输的信元中继的国际标准。固定长度的信元允许信元的处理可以通过硬件完成，因此减少了传输延迟。ATM设计利用高速传输介质，例如：E3、SONET和T3。

电路交换（*circuit switching*） 在“通话”期间发送方和接收方之间存在一条专有的物理电路路径的交换系统。广泛应用于电话公司网络。

中心局（*Central Office, CO*） 本地电话公司局，是所有本地环路连接到的地方，以及用户线路发生电路交换的地方。

客户端设备（*Customer Premises Equipment, CPE*） 电话公司提供的终端设备，比如终端、电话和调制解调器，它被安装在客户端并连接到电话公司的网络。

信道服务单元（*Channel Service Unit, CSU*） 将终端用户设备连接到本地数字电话环路的数字接口设备。通常与DSU一起提及，称为CSU/DSU。

数据电路端接设备（*DCE*） data circuit-terminating equipment（EIA扩充）或data circuit-terminating equipment（ITU-T扩充）通信网络的连接设备，包含用户到网络接口的网络端。DCE提供到网络的一条物理连接、转发流量并提供用于同步DCE和DTE设备间数据传输的时钟信号。调制解调器和接口卡就是DCE的实例。

数字服务单元（*Digital Service Unit, DSU*） 用于数字传输的设备，使DTE设备的物理接口适配于一个传输设备，比如T1或E1。DSU也提供诸如信号时钟的功能。通常与CSU一起提及，称为CSU/DSU。

数据终端设备（*Data Terminal Equipment, DTE*） 用户网络接口的用户端设备，作为一个数据源、目的或两者都有。DTE通过DCE设备（例如调制解调器）连接到数据网络，并且使用由DCE产生的时钟信号。DTE包括的设备有计算机、协议转换器和多路复用器。

分组交换（*packet switching*） 在发送分组时节点间彼此共享带宽的连网方式。

永久虚电路（*Permanent Virtual Circuits, PVC*） 永久建立的虚电路。由于指定的虚电路任何时候都必须存在，所以PVC节省了电路建立和拆除所需的带宽。在ATM术语中被称为永久虚连接。

交换虚电路（*Switched Virtual Circuits, SVC*） 根据需要动态建立并在传输完成后拆除的虚电路。SVC用于间断的数据传输情况中。在ATM术语中被称为交换虚连接。

时分多路复用（*Time-Division Multiplexing, TDM*） 在一条独立的线路上基于预先分配的时隙给多条信道分配带宽的技术。无论工作站有无数据传输，带宽都固定分配给每条信道。

12.11 复习题

1. 模拟拨号的连接不适合于下面哪些通信类型？
   A. E-mail
   B. 低量的文件传输
   C. 报告
   D. 视频
2. 下面关于ISDN的描述哪一个是正确的？
   A. ISDN BRI提供两条B信道和一条D信道。
   B. D信道，工作在16kbit/s，用来传输用户数据。
   C. 在北美，ISDN BRI提供23条B信道和1条D信道。
   D. ISDN BRI的总速率是2.533Mbit/s。
3. 租用线是一条_____链路，它提供了一条单一的从客户到远程网络的预先建立的广域网通信链路。
   A. 点到点
   B. 点到分点
   C. 模拟
   D. 数字
4. 下面关于X.25网络哪一个是正确的？
   A. 比特速率很低。
   B. 数据分组不会造成延迟。
   C. 广泛用于EDI应用。
   D. 费用与数据量有关。
5. 帧中继如何在同一物理连接上处理多个会话？
   A. 帧中继多路复用电路。
   B. 不允许多个会话。
   C. 帧中继双向会话。
   D. 帧中继把它们转换为一个ATM信元。
6. 下面关于ATM技术哪一个是不正确的？
   A. 能够传输语音、视频和数据。
   B. ATM提供比帧中继更高的带宽。
   C. 基于信元体系结构而不是基于帧体系结构。
   D. ATM信元是35Bytes的固定长度。
7. 连接到服务提供商中心局的位于用户端的设备是：
   A. DTE
   B. DCE
   C. CPE
   D. 以上都不是
8. 将数据发送到本地环路上的设备是：
   A. DTE
   B. DCE
   C. CPE
   D. 以上都不是

9. 将数据传输到DCE的客户设备是：
   A. DTE
   B. DCE
   C. CPE
   D. 以上都不是
10. 数字线路需要一个_____和一个_____。
   A. CSU和DSU
   B. DTE和DCE
   C. T1和E1
   D. 以上都不是
11. 对于模拟广域网服务，一个_____是必需的？
   A. DCE
   B. DTE
   C. 调制解调器
   D. NIC
12. 下面除了_____以外都是电路交换连接？
   A. 公共交换电话网（PSTN）
   B. ISDN基本速率接口（BRI）
   C. ISDN基群速率接口（PRI）
   D. SONET
13. 在分组交换网络中，交换开始时已经建立的路由被称为：
   A. 永久虚电路（PVC）
   B. 交换虚电路（SVC）
   C. 永久虚服务（PVS）
   D. 交换虚服务（SVS）
14. 在分组交换网络中，根据需要才建立的路由被称为：
   A. 永久虚电路（PVC）
   B. 交换虚电路（SVC）
   C. 永久虚服务（PVS）
   D. 交换虚服务（SVS）
15. 下面哪种服务是ISDN连接的特点？
   A. 异步拨号
   B. 异步租用线
   C. 同步拨号
   D. 同步租用线
16. 下面哪一个是DCE设备？
   A. 路由器
   B. 调制解调器
   C. 交换机
   D. 集线器
17. PPP运行在OSI的哪一层？
   A. 网络层

B. 数据链路层
C. 应用层
D. 传输层

18. 帧中继运行在OSI的哪一层？
A. 第1层
B. 第2层
C. 第3层
D. 第4层

19. ISDN BRI由以下哪一个组成？
A. 2条B信道和2条D信道
B. 2条B信道和1条D信道
C. 23条B信道和1条D信道
D. 30条B信道和1条D信道



第13章　点到点协议

目标

学习完本章后，你将能够：

- 识别和描述点到点协议（PPP）通信的基本组件。
- 定义和描述PPP协议中链路控制协议（LCP）数据帧和网络控制协议（NCP）数据帧的用途。
- 了解配置和验证PPP的过程。
- 描述和解释PPP验证。
- 定义和描述密码验证的用途。
- 定义和描述质询握手验证协议（CHAP）的用途。

你在本章中将学到定义PPP通信的基本组件、处理流程和操作。另外，还将学习PPP中LCP帧和网络控制协议（Network Control Protocol）帧的使用。最后，将学习到如何配置和验证PPP的配置。还将连同PPP身份验证一起学习PAP协议和CHAP协议的使用。

PPP在REC 1661中描述，是针对拨号Internet连接（包括ISDN）的良好解决方案。PPP是一种分层的协议，最初由LCP发起对链路的建立、配置和测试。在LCP初始化后，通过一种或者多种“网络控制协议（Network Control Protocol）”来传送特定协议族的通信。在RFC1332文档中描述的IP控制协议（IPCP IP Control Protocol）允许在PPP链路上传输IP分组。其他一些NCP为下列协议提供服务，AppleTalk（RFC 1378）、OSI（RFC 1377）、DECnet Phase IV（RFC 1762）、Vines（RFC 1763）、XNS（RFC 1764）和透明以太网桥接（RFC 1638）。

下面所列出的是本章将要讨论的PPP关键特征：

- **地址通知**（*Address notification*）——它允许服务器通知拨号客户在连接时使用的IP地址。这种机制对于需要请求IP地址且支持备用配置的客户而言是足够强大的。SLIP则要求用户手动配置这些信息。RFC 1877中指定的PPP选项也可以通知名称服务器地址，包括因特网和NetBIOS名称服务器。
- **身份验证**（*Authentication*）——这里可用到的选项是PAP或CHAP。这两者在RFC 1334文档中被描述。
- **多协议支持**（*Multiple protocol*）——反通过的运行附加的NCP，可以在同一链路运行多种协

议。例如IP和IPX的流量可以共享一条PPP链路。

• **链路监控**（*Link monitoring*）——这些工具包括一个链路级回应装置，可以周期性的检查链路操作。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图。光盘上的素材是本章内容的补充，能强化本章所介绍的概念。

13.1　PPP分层体系结构

PPP提供了同步和异步电路上的路由器到路由器、主机到网络的连接。图13-1显示了PPP在广域网中的应用。PPP是目前使用得最为广泛的广域网协议，这是因为它具有以下特征：

• 能够控制数据链路的建立。
• 能够对IP地址进行分配和管理。
• 支持多种网络协议的复用。
• 能够配置链路并对链路进行质量测试。
• 错误检测



图13-1　广域网中的点到点协议

PPP使用分层体系结构。体系结构就是一个的逻辑模型、设计或蓝图。分层体系结构有助于相邻层之间的通信。在网络中应用的OSI模型就是分层的体系结构。PPP提供了在一条点到点链路上封装多种协议数据报的方法，并且还可以利用数据链路层来测试连接。因此，PPP使用了OSI分层体系结构中的3层。图13-2显示了PPP在OSI模型中所处的位置。图13-3显示了PPP各层的功能。



图13-2　PPP与OSI模型

• 物理层用来实际的点到点连接。
• 数据链路层用来建立和配置连接。
• 网络层用来配置不同的网络层协议。

你可以在以下类型的物理接口上配置PPP：

• 异步串行接口。
• 同步串行接口。
• 高速串行接口（HSSI）。
• 综合业务数字网（ISDN）。

PPP使用它的LCP在广域网数据链路上协商和设置控制选项。PPP使用网络控制程序组件对多种网络层协议进行封装及选项协商。



图13-3　PPP各层功能

LCP位于物理层之上，用来建立、配置和测试数据链路连接。PPP也通过使用LCP来自动的匹配链路两端设备之间如下面列出的封装格式选项：

• **身份验证**（*Authentication*）——身份验证选项需要建立链路的呼叫方输入信息，用以确保呼叫者发起呼叫时拥有网络管理员的许可（见图13-4）。对等路由器之间相互交换身份验证消息。下列所示的是可供选择的两种验证方式：



图13-4 身份验证

—— PAP。

—— CHAP。

• **压缩**（*Compression*）——压缩选项通过减少链路中数据帧所含的数据大小，来提高PPP线路的吞吐量。当到达目的地后，协议对数据帧进行解压缩（见图13-5）。Cisco路由器支持两种压缩算法，它们是Stacker和Predictor。



图13-5 压缩

• **错误检测**（*Error-Detection*）——PPP的错误检测机制使进程能够识别错误的情形。Quality和Magic Number选项用来确保实现一条可靠的、无环路的数据链路。

• **多链路**（*Multilink*）——Cisco IOS 版本11.1及以后的版本支持PPP的多链路捆绑。这个选择为PPP使用的路由器接口提供了负载均衡的功能。（见图13-6）

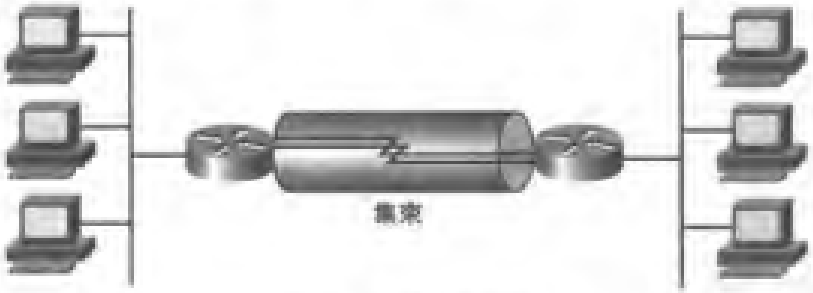


图13-6 多链路捆绑

• **PPP回拨**（*PPP callback*）——它被用来进一步提高安全性，Cisco IOS版本11.1提供了在PPP中的回拨功能。在这个LCP选项的作用下，一台Cisco路由器可以扮演回拨客户或回拨服务器的角色。客户发起一个初始呼叫，请求回拨，并且终止初始的呼叫。回拨路由器依照配置语句回应初始呼叫，并向客户返回呼叫。

LCP还可以处理分组大小变动的限定、侦测一般的配置错误、终止链路以及确定链路功能是否正常。

PPP允许在同一条通信链路上运行多种网络层协议。对每一种使用的网络层协议，PPP都提供了单独的网络控制协议。例如因特网协议（IP）使用IPCP，互连网络分组交换（IPX）使用IPXCP。NCP中包含了一些功能字段，这些字段中含有用来标明PPP所封装的第3层协议类型的标准代码。

如图13-7所示，PPP帧中包括以下字段：

• **标志（Flag）字段**：指示一个帧的开始和结束，它是由二进制数序列01111110组成。

• **地址（Address）字段**：该字段包含二进制数序列11111111，这是一个标准的广播地址。PPP并不会指定单台设备的地址。

• **控制（Control）字段**：该字段长度为1字节，由二进制数序列00000011组成，表示用户数据采用无序帧方式传输。它提供的无连接链路服务类似于逻辑链路控制（LLC，Logical Link

Control）类型1所提供的方法。

• **协议（Protocol）字段**：长度为2字节，用于标识被封装在帧中数据字段里的协议类型。表13-1列出了一些PPP字段中的协议代码。

表13-1　PPP字段编号

值（16进制）	协议名称
8021	IPCP
8023	OSI Network Layer Control Protocol
8029	AppleTalk Control Protocol
802b	Novell IPX Control Protocol
c021	LCP
c023	PAP
c223	CHAP

信息提示

你会发现有一些PPP字段的代码并没有包含到表中，详细情况请查询网站http://www.iana.org/assignments/ppp-numbers。

• **数据（Data）字段**：长度为0或多个字节，它包含符合协议字段中指定协议的数据报。通过确定帧序列的结尾，为FCS留出2个字节，便可确定数据字段的结尾。该字段的最大长度缺省值是1,500字节。

• **帧校验序列（FCS）字段**：通常为16位（2字节）。PPP帧中包含这些额外的字符来进行差错控制。

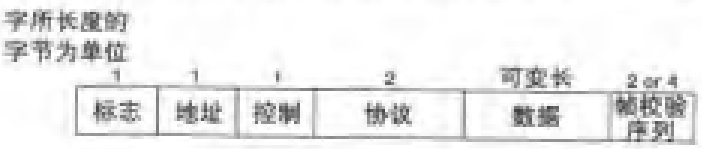


图13-7　PPP帧格式

13.2　建立PPP会话

PPP提供了建立、配置、维护和终止点到点连接的方法。PPP经过以下4个阶段在一条点到点的链路上建立通信连接。

1. **链路的建立和配置协商**——通信的发起方发送LCP帧来配置和检测数据链路。

2. **链路质量检测**——链路将被检测，从而判断链路的质量是否能够携带网络层信息。

3. **网络层协议的配置协商**——通信的发起方发送NCP帧，用以选择和配置网络层协议。在这一阶段选定的网络层协议，比如TCP/IP、Novell IPX和AppleTalk，被配置完毕，通信双方可以发送各自的网络层协议分组。

4. **链路终止**——通信链路将一直保持到LCP或NCP帧关闭链路或者是发生一些外部事件（如空闲时间超长或用户干预）。



图13-8　PPP链路协商

有3类LCP帧：

• 链路建立帧（Link-establishment frame）用来建立和配置链路。

• 链路终止帧（Link-termination frame）用来终止链路。

• 链路维护帧（Link-maintenance frame）用来管理和调试链路。

图13-8是一个PPP链路协商的例子。

表13-2中描述了PPP会话建立的4个阶段。

表13-2 PPP会话建立阶段

阶段	描述
1. 链路建立阶段	在这个阶段中，每一台运行PPP的设备都发送LCP帧来配置和测试数据链路。LCP帧中包含有一些配置选项字段，这些字段可以使设备之间协商一些选项的使用，比如最大传输单元（MTU），压缩PPP的某些字段和链路验证协议。如果一个配置选项没有被包含在LCP的分组内，那么这些配置字段将会使用一些缺省的值 在网络层分组交换之前，LCP必须首先打开一条连接并协商配置参数。在配置确认数据帧发送并且接收后，这一阶段就宣告完成了
2. 链路质量检测阶段	在链路建立和确定身份验证协议之后，对等的两端可以相互鉴别。如果使用身份验证的话，那么验证过程发生在网络层协议阶段开始之前
3. 网络层协议阶段	在这个阶段中，使用PPP的设备发送NCP分组来选择和配置一种或多种网络层协议，比如IP。在每一种选择的网络层协议被配置后，每一个网络层协议的数据分组就可以通过链路发送了 如果LCP关闭链路，它会向网络层协议发出通告，以使网络层协议做出适当的反应。当PPP协议配置完成后，你可以使用show interface命令来检查LCP和NCP的状态
4. 链路终止阶段	LCP可以在任何时间终止链路。这经常是由用户的请求（关闭）而发生的，也可因物理层事件而发生，比如失去载波或超时

13.3 PPP身份验证协议

对于一个PPP会话来讲，身份验证功能是可选的。在链路已经建立并且身份验证协议被选择以后，对等的两端可以相互鉴别。如果启用了验证功能，验证过程将发生在网络层协议配置阶段开始之前。

身份验证功能需要呼叫的发起方输入验证信息，这个信息用来确定用户拥有网络管理员赋予的呼叫许可。对等的路由器之间相互交换身份验证消息。

当你在配置PPP验证的时候，你可以选择PAP或者是CHAP。一般来讲，CHAP是首选的验证协议。

13.3.1 PAP

密码验证协议（PAP, Password Authentication Protocol）通过使用两次握手机制，为建立远程节点的验证供了一个简单的方法。在PPP链路建立阶段完成后，远程节点将不停地在链路上反复发送用户名/密码，直到身份验证通过或者连接被终止。如图13-9中所示的例子。



图13-9 PAP身份验证

PAP不是一种健壮的身份验证协议。身份验证时密码在链路上以明文发送，而且由于验证重试的频率和次数由远程节点来控制，因此不能防止回放攻击和重复的尝试攻击。

13.3.2 CHAP

质询握手验证协议（CHAP, Challenge Handshake Authentication Protocol）使用3次握手机制来启动一条链路和周期性的验证远程节点。CHAP作用在初始链路建立之后，而且在链路建立后的任

何时间都可以进行重复验证。

在PPP链路建立阶段完成之后，本地路由器发送一个“质询（Challenge）”消息到远程节点。远程节点使用一个数值来回应挑战，这个数值是由单向哈希函数（典型为MD5 Message-Digest algorithm）基于密码和挑战消息计算得出的。本地路由器依靠由它自己计算得出的期望值来检查回应。如果数值匹配，身份验证将被通过。否则连接将立即终止。如图13-10中所示的例子。



图13-10　CHAP身份验证（应为3次握手）

CHAP通过使用惟一的，不可预知的，可变的挑战消息来防止回放攻击。因为挑战消息是惟一且随机的，作为结果的散列值也是惟一且随机的。利用重复进行挑战验证过程，可以限制暴露给任何单次攻击的时间。CHAP是由本地路由器或者一台第3方的验证服务器来控制挑战的频率和次数的。

13.4　PPP封装与验证过程

当你在配置PPP身份验证时，你可以选择PAP或CHAP中的一种验证方式。在你输入encapsulation ppp命令时，系统根据配置选择验证方式。如果没有配置验证，则PPP进程就会立即启动。否则PPP进程就会进行到下一个步骤。图13-11中所示的是身份验证的过程。

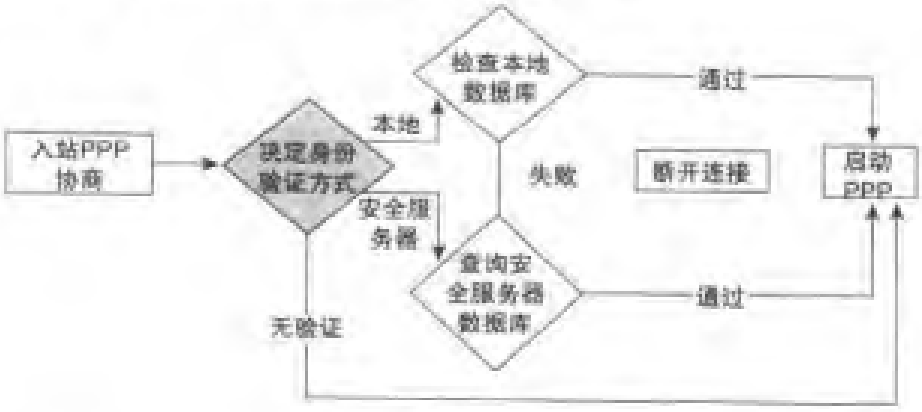


图13-11　身份验证过程

验证进程然后确定身份验证的方法。

身份验证进程检索本地数据库或安全服务器（通过使用命令username password建立），以检查用户所提供的用户名和密码是否匹配CHAP或PAP验证方式中指定的信息。

身份验证进程检查由本地数据库返回的验证查询响应。如果响应是一个肯定的答复，PPP进程就启动。如果是一个否定的答复，用户将被立即拒绝。

如果选择PAP验证方式，在PPP链路建立阶段完成以后，远程节点重复向路由器发送用户名和密码信息，直到验证通过或者链路终止。

如果选择CHAP验证方式，在PPP链路建立阶段完成之后，本地路由器发送一个挑战消息到远程节点。远程节点使用一个数值来回应挑战，这个数值是由单向哈希函数（典型为MD5）基于密码和

挑战消息计算得出的。本地路由器依靠由它自己计算得出的期望值来检查回应。如果数值匹配，身份验证将被通过。否则连接将立即终止。

下面列出的步骤和图显示了在两台路由器之间进行CHAP验证时所发生的连续事件。这里没有列出在使用debug ppp negotiation命令时所显示的实际信息。要得到更多的信息，请查阅www.cisco.com/warp/public/471/debug_ppp_negotiation.html上的"Understanding debug ppp negotiation Output"文档。

下列步骤是图13-12显示的过程：

步骤1 远端设备向3640-1发起连接呼叫。在呼叫进入的接口上已经配置了ppp authentication chap命令。



图13-12 CHAP身份验证过程步骤1

步骤2 LCP协商使用CHAP和MD5。

步骤3 在这次呼叫中，3640-1需要向发起呼叫的路由器发送一个CHAP挑战消息。

图13-13中所示的步骤为两台路由器之间进行CHAP验证时的过程：



图13-13 CHAP身份验证过程步骤2

步骤1 一个CHAP挑战分组由以下特征构成：

- 01 = 质询分组类型标识符。
- id = 标识该挑战分组的序列号。
- random = 随机数。
- 3640-1 = 质询方的认证名。

步骤2 该质询分组的id号和随机数值由被叫路由器（3640-1）保存。

步骤3 质询分组被发往发起呼叫的路由器。被叫路由器会维护一个已发出挑战消息的列表。

图13-14表示了对被叫路由器发出的质询分组的接收和MD5的处理过程。

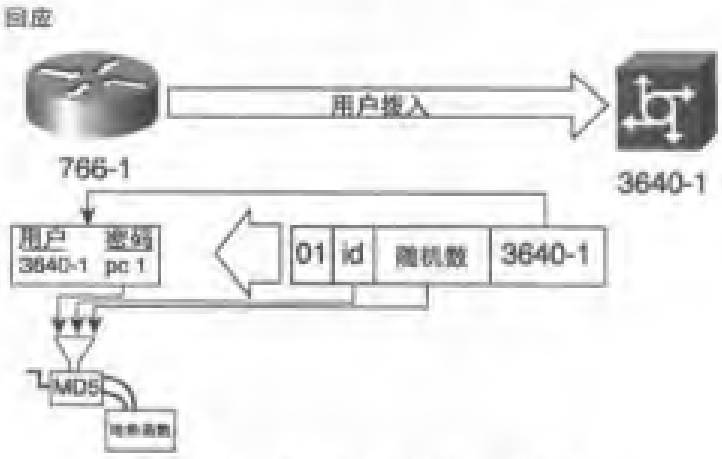


图13-14 CHAP身份验证过程步骤3

发起呼叫的路由器用下面的方式对CHAP挑战分组进行处理：

步骤1 将序列号放入MD5哈希生成器。

步骤2 将随机数放入MD5哈希生成器。

步骤3 质询者的认证名"3640-1"用来查找密码。发起呼叫的路由器查找匹配用户名为3640-1的条目，这个条目用于CHAP验证。在这个例子里，这个条目如下所示：username 3640-1 password pc1

步骤4 将口令放入MD5哈希生成器。这个结果是一个单向MD5哈希数值，这个数值将会被放到CHAP回应中，发回挑战验证方。

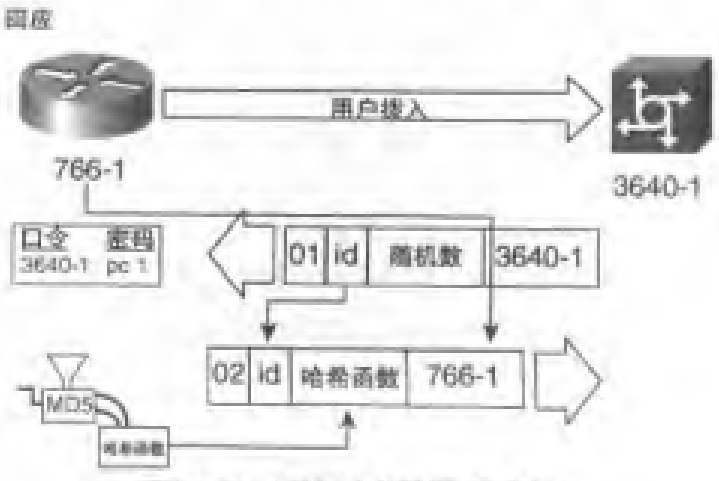


图13-15 CHAP身份验证过程步骤4

图13-15所示为发回验证方CHAP回应分组的建立过程。过程如图所示：

步骤1 回应分组由下面各部分组成：

• 02 = CHAP回应分组类型标识符。

• id = 序列号，直接从挑战分组复制过来。

• hash = MD5哈希生成器的输出结果。

• 766-1 = 本设备的认证名。这是为了挑战方的需要，质询方用这个认证名查找核对验证时所需的用户名和密码。（我们将在后面看到更详细的内容）

步骤2　回应分组被发回质询方。

图13-16给出了挑战方对回应分组的处理过程。

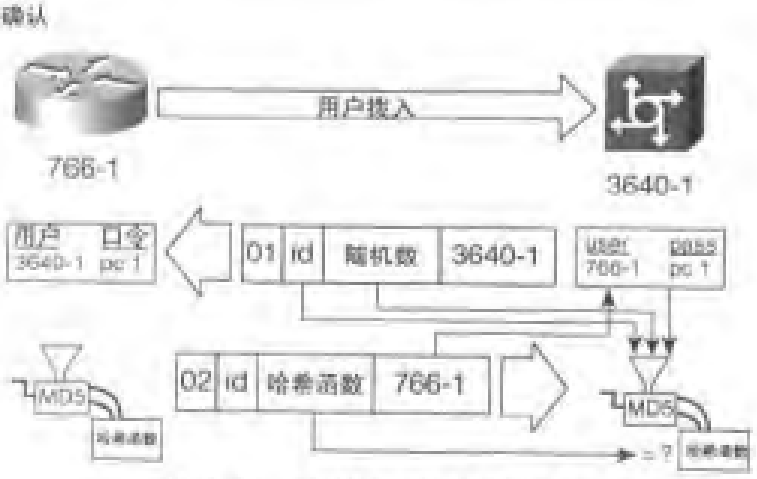


图13-16　CHAP身份验证过程步骤5

在认证方，CHAP回应分组是按下列方式进行处理的：

步骤1　用序列号找出原始的挑战分组。

步骤2　把序列号（id）放入MD5哈希生成器。

步骤3　把原始质询分组中的随机数放入MD5哈希生成器。

步骤4　使用发起呼叫路由器的认证名766-1从下面的来源之一查找口令：

• 本地用户名和密码数据库。

• 远程验证拨入用户服务（RADIUS）或者一台终端访问控制器访问控制系统（TACACS+）服务器。

步骤5　将口令放入MD5哈希生成器。

步骤6　将回应分组中收到的哈希值与自己所计算出来的MD5散列值进行比较。如果自己计算出的结果与所收到的MD5哈希值是一致的，那么CHAP验证就成功了。

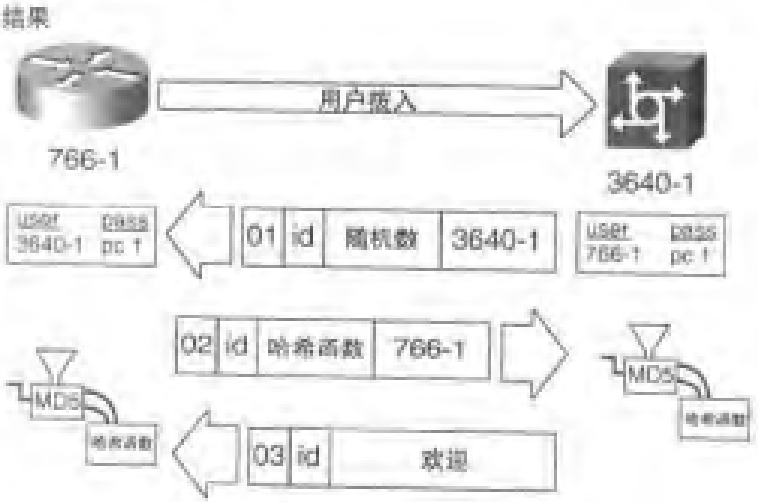


图13-17　CHAP身份验证过程步骤6

图13-17显示了发送给发起呼叫路由器的成功消息。

如果验证成功，一个CHAP验证成功分组将会由以下几部分组成：

• 03 = CHAP验证成功消息类型标识符。

• id = 序列号，直接从回应分组中复制过来。

• "Welcome in" 某种简单的文本消息，为了让用户可读。

如果验证失败，一个CHAP验证失败分组将会由以下几部分组成：

• 04 = CHAP验证失败消息类型标识符

• id = 序列号，直接从回应分组中复制过来。

• "Authentication failure" 或其他类似的文本消息，为了让用户可读。

这时验证成功或验证失败的分组就发送到发起呼叫的路由器。

注意：这个例子描述了一个单向的验证过程。在双向验证中，将重复以上整个过程，只是由呼叫路由器发起最初的"质询"。

13.5 串行点到点连接

几乎所有的广域网技术都是基于物理层中的串行传输。这就意味着数据帧里的比特在物理介质上传输时，一次只传送一个比特。

构成第2层数据帧的比特被物理层处理，一次一个的发送到物理介质上。信号发送方法（NRZ-L、HDB3、AMI）和一些其他的因素，都把一种串行通信方法和另外的通信方法区分开来。下面所列的是一些不同的串行通信标准：

- RS-232-E。
- V.35。
- HSSI。

13.6 时分多路复用

时分多路复用（TDM, Time-division multiplexing）技术可以使几台源设备发出的信息经过一条通信信道或者使用同一个信号传输，这些信息到达远程端点后能够被重构为原来的数据流。

如图13-18中所示，有3台源设备发出信息流，这些信息被携带并转换到输出信道。首先，从每一台输入信道取一个信息块，这些信息块的大小可能不等；但是通常情况下，在一个时间单位中传输的信息块大小为1比特或者是1字节。依据传输时是以比特为标准还是以字节为标准，TDM的类型可分为比特交错或者字节交错两种。

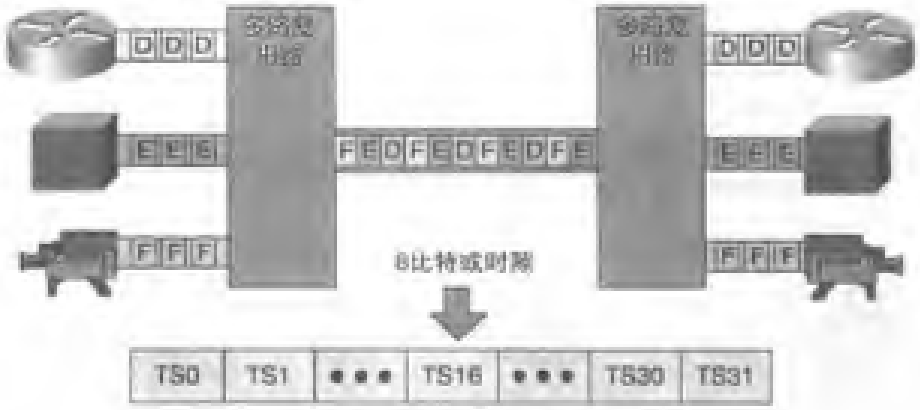


图13-18 TDM源信息流

这3条输入信道中的每一条信道都拥有自己的容量。要使输出信道可以容纳来自于3条输入信道的信息，输出信道的容量不能小于几条输入信道带宽的总和。

在TDM中，无论是否发送输入信息，TDM总是输出固定的时隙。TDM的输出数据结构和火车很相似。例如，有32辆运送货物的拖车，不同的船公司都用有自己的拖车。每天火车都拖着32辆拖车离开。如果船公司有货物装船，他们会将货物装入集装箱，并把集装箱放置到拖车上。由火车带动拖车。如果船公司没有货物运输，属于他们的拖车是空置的，但是空置的拖车依然保持在随火车运输的行列中。

总之，TDM是一个物理层中的概念，它从来不关心复用到输出信道中的信息是什么。因此，TDM可以独立于输入信道所使用的第2层协议。

ISDN就是一个TDM应用的好例子。ISDN的基本速率接口（BRI）由3条信道构成，它们是2条64-kbit/s的B信道（B1和B2）和一条16-kbit/s的D信道。在图13-19中，TDM有9个时隙，这些时隙被反复发送。这可以使电话公司对网络终端装置后的分界点-也就是本地环路进行有效的管理和故障排除。

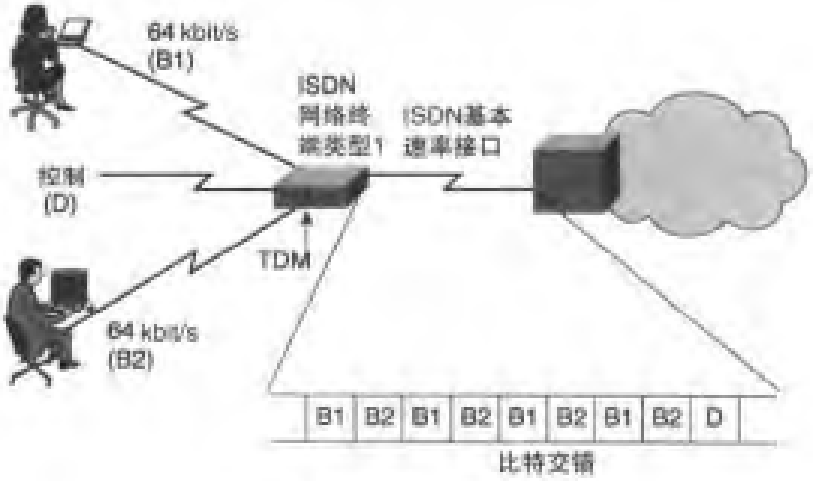


图13-19　TDM

13.7　分界点

分界点（demarcation point），也就是通常所说的demarc，这个点标识了服务提供商或电话公司所负责的网络最终点。分界点对于美国和非美国的电话公司来讲，其界定是不同的。在美国，电话公司提供本地环路连接到消费者的建筑物，由消费者提供活动设备（CSU/DSU）作为本地环路的终止点，这些设备通常放置在电信配线间中。因此，当这些设备故障时，消费者有责任对它进行维护和更换。

在北美地区，网络终端类型1（NT1）设备属于用户室内设备（CPE）。在世界上大部分地区，NT1属于由服务商提供和管理的网络部分，这样可以使电话公司对本地环路进行主动的管理和排错。分界点位于NT1设备之后。用户把CPE设备——通常为一台路由器或一台帧中继接入设备与NT1相连，在连接时，一般使用诸如V.35或RS-232之类的串行接口。图13-20所示为分界点的例子。

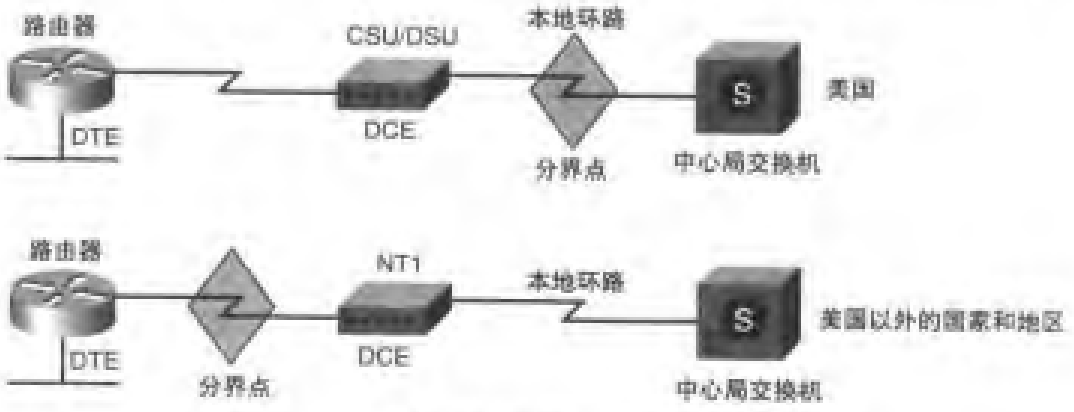


图13-20　分界

13.8　数据终端设备（DTE）与数据通信设备（DCE）

在广域网连接中，设备通常被放置在连接的两端。DTE设备和数据通信设备放置在连接的一端，相应还有另外的DTE设备和数据通信设备放在另一端，如图13-21所示。广域网服务提供商的传输网络将两台数据通信设备连接起来。用户室内设备，通常为路由器，是DTE设备。其他终端设备还有计算机、打印机和传真机。

DCE设备，通常是一台调制解调器（modem）或一个信道服务单元/数据服务单元（CSU/DSU），它们用来把由DTE设备发送过来的用户数据转换成广域网服务提供商的传输链路所能接受的格式。

这些信号由远端的DCE设备接收，解码为原来的数据比特序列，发送给远端DTE。两台DCE设备必须配置为可以相互理解。换句话说，它们之间必须采用一致的编码方案和数据传输速率。

为了使DTE设备和DCE设备之间能够通信，开发了一些标准。一些像电子工业联合会（EIA）和国际电信联盟-电信标准部（ITU-T）这样的组织在这些标准的发展过程中起到了积极的作用。图13-22中所示为CSU/DSU网络连接类型。

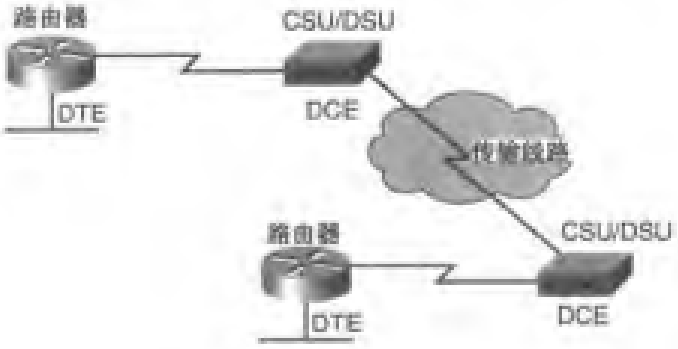


图13-21 数据通信设备

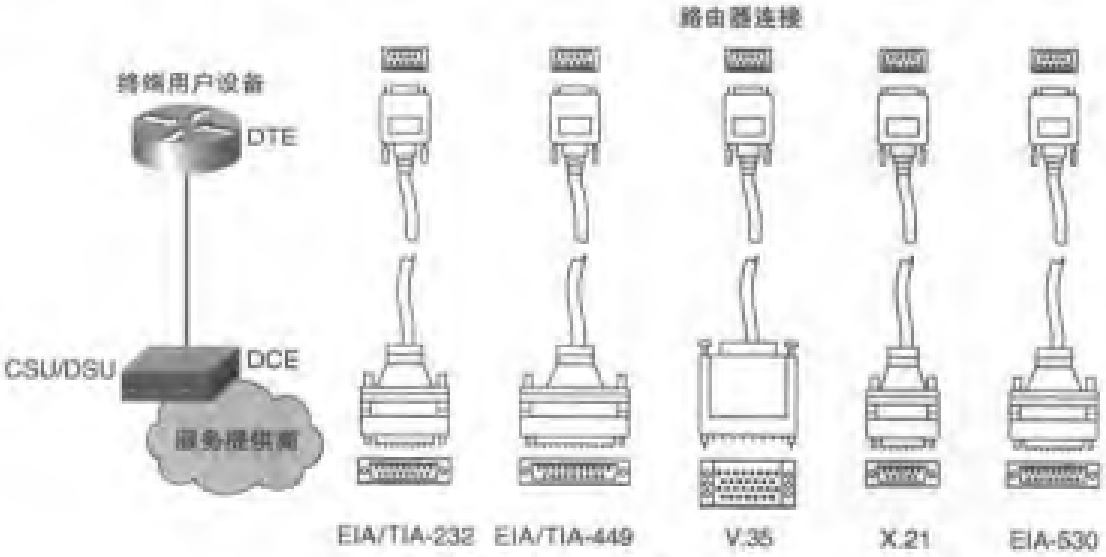


图13-22 CSU/DSU网络连接

DTE-DCE接口的特定标准由下面的规范构成：

- 机械的（*Mechanical*）——定义物理上的——如插脚的数量、连接器的类型等等。
- 电气的（*Electrical*）——为表示0/1定义电压标准。
- 功能的（*Functional*）——指定接口中每一条信号线路在工作时所执行的功能。例如在EIA/TIA-232和DB-25标准中，2号线——传输DTE-DCE的信号；3号线——在DTE接收来自于DCE的信号；15号线——传输时钟信号。
- 规程的（*Procedural*）——指定数据传输时事件产生的次序。

假设有两台DTE设备必须连在一起，就好像在试验中两台计算机或两台路由器连接在一起那样。这时要使用一种被称为“空调制解调器”的线缆，用以消除对DCE设备的需要。当同步线路传输需要时钟时，一台外部设备或者其中的一台DTE设备必须要产生时钟信号，通常这个功能是由DCE设备提供的。

在这种情况下，路由器上的同步串行端口要根据连在本端口的线缆类型被配置为DTE或者DCE，匹配路由器配置的线缆的类型不是DTE就是DCE。如果端口类型被设置成DTE，这是默认配置，这时它就需要从CSU/DSU或其他DCE设备那里获得外部时钟。

DTE设备连接到DCE设备时所用到的线缆是一条屏蔽的串行转换线缆。屏蔽串行转换线缆连接路由器的一端可能是一个DB-60连接器，这个连接器用来连接路由器的串行广域网接口卡上的DB-

60端口。串行转换线缆的另一端的连接器类型与所使用的标准相适应。广域网供应商或者CSU/DSU一般都要求使用这种线缆类型。Cisco设备支持EIA/TIA-232, EIA/TIA-449, V.35, X.21和EIA/TIA-530串行标准。

为了支持在有限的空间接入更多的连接器，Cisco采用了一种灵巧的串行线缆。这种灵巧线缆的末端是一种比DB-60连接器小巧的26针连接器。

13.9　HDLC封装

最初的串行通信都是基于面向字符的通信。面向比特的通信方式效率更高一些，但是最初的面向比特的协议都是专有的。在1979年，国际标准化组织（ISO）使HDLC标准化，它作为一种标准的面向比特的数据链路层协议用来封装同步串行数据链路中的数据。这次标准化使得其他的委员会采用了HDLC，并且扩展了该协议。自1981年以来，ITU-T发展了一系列的HDLC派生协议，称为链路接入协议。X.25使用的平衡式链路接入过程（LAPB）、ISDN使用的D信道链路接入过程（LAPD）、调制解调器链路接入过程（LAPM）、调制解调器使用的PPP和帧中继链路接入过程（LAPF）都是这些派生协议的例子。

HDLC使用同步串行传输，它在并不可靠的物理层链路上为两点间提供无差错通信。HDLC定义了第2层帧结构，通过使用确认和窗口操作方案进行流量控制和差错控制。不管是数据帧还是控制帧，格式都相同。

标准的HDLC原本不支持在单一链路中传输多种协议，这是因为HDLC无法标识所携带的是哪一种协议。Cisco提出了一种专有的HDLC版本。Cisco的HDLC帧中使用了一个专有类型字段，这个字段等同于一个协议字段，使HDLC在同一链路中传输多种网络层协议数据成为可能。HDLC是Cisco路由器串行接口默认的第2层封装协议。

HDLC定义了三种类型的帧，如图13-23所示，每一种帧类型都拥有不同的控制字段格式：

- **信息帧**（*I-帧*）——为站点携带传输的数据。附加了可以由信息帧捎带的流量控制和错误控制数据。
- **监控帧**（*S-帧*）——在没有使用捎带信息时，为通信提供了请求/响应机制。
- **无编号帧**（*U-帧*）——提供了补充的链路控制功能。如连接设置。代码字段标识了无编号帧的类型。

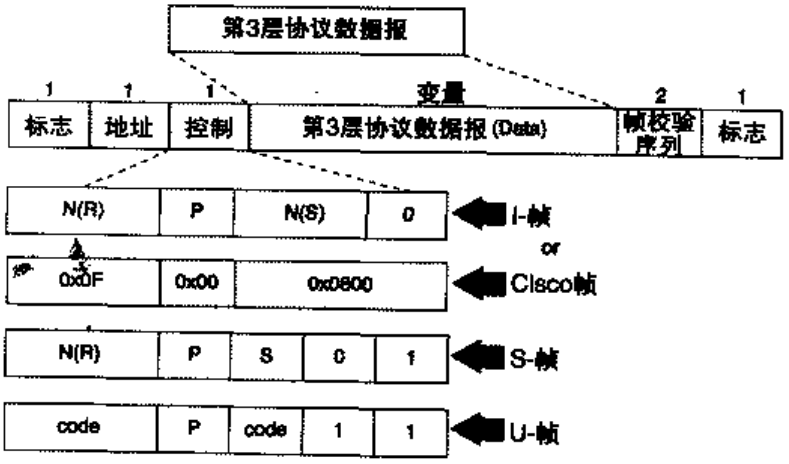


图13-23　HDLC帧

控制字段中的首个或前两个比特用于标识帧类型。在信息帧（I）的控制字段中，发送序列号指出了下一个要发送帧的编号。接收序列号提供了下一个要被接收的帧的编号。发送方和接收方都维护着发送和接收的序列编号。

13.10　配置HDLC封装

默认情况下，Cisco设备在同步串行线路上采用Cisco HDLC 串行封装方法。可是，如果串行接口被配置成其他的封装协议，而且接口的封装协议必须要改回HDLC，此时应进入串行接口的接口配置模式。然后输入**encapsulation hdlc**这条接口配置命令，指定接口的封装为HDLC:

```
router(config-if)# encapsulation hdlc
```

Cisco的HDLC是一个点到点协议，可以在两台Cisco设备之间的租用线上使用它。当与一台非Cisco设备通信时，同步的PPP协议是一个更为可行的选择。

13.11 串行接口的故障排除

show interface serial命令输出的显示内容列出了关于串行接口的详细信息。通过使用show interface serial命令可以验证有关HDLC或PPP封装的正确配置。当配置HDLC，“Encapsulation HDLC”将出现在show interface serial命令的输出信息当中。

当配置PPP时，你可以通过使用show interface serial命令检查PPP的LCP和NCP的状态，如例13-1中显示的那样。

第一个例子显示的是HDLC封装，第二个例子显示的是PPP封装。

例13-1 show interface s0/0命令

```
Router#show interface s0/0
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 131.108.156.98, subnet mask is 255.255.255.240
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters never
--  output omitted ---

Router#show interface s0/0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
--  output omitted ---
```

表13-3中列出的是在使用show interface serial命令后，你可能见到的接口故障状态：

```
Serial x is down, line protocol is down
Serial x is up, line protocol is down
Serial x is up, line protocol is up (looped)
Serial x is up, line protocol is down (disabled)
Serial x is administratively down, line protocol is down
```

表13-3 可能的故障状态

状态行	可能的故障	故障的排除方法
Serial *x* is up, line protocol is up（DTE模式）	这是正常线路的状态	不需要采取任何操作
Serial *x* is down, Line Protocol is down（DTE 模式）	通常表明路由器没有检测到CD（carrier detect）信号。（也就是说CD信号为无效状态） 电话公司故障：线路断开或者线路没有连接到CSU/DSU上 线缆故障 硬件故障（CSU/DSU）	1. 查看CSU/DSU上的LED指示灯确定CD信号是否有效，或者在线路上接入一个断接盒，检查CD信号的状态 2. 确保使用的是正确的线缆及接口。（参阅硬件安装文档） 3. 在线路上接入一断接盒，并检查所有的控制信号 4. 与专线或其他载波服务的供应商联系，确定线路是否存在故障 5. 更换出现故障的部件 6. 如果怀疑路由器硬件出现问题，可以将串行线路连接到其他的接口上。如果线路能够正常工作，这就说明原先的接口存在问题
Serial *x* is up, Line protocol is down（DTE模式）	本地或远程路由器配置错误 远程路由器没有发送keepalive信号 专线或其他载波服务故障。（线路噪音过大，交换机配置错误或出现故障） 线缆上的定时故障。（CSU/DSU上没有设置SCTE） 本地或远程CSU/DSU出现故障 路由器硬件故障。（本地或远程）	1. 让调制解调器、CSU或DSU工作在本地回送方式，然后利用show interface serial命令确定线路协议是否工作正常 如果线路协议正常工作了，这可能是电话公司或一台有故障的远程路由器的问题 2. 如果远端也存在着同样的问题，那么可以在远端调制解调器、CSU或DSU上重复第1步的操作 3. 查看所有线缆，确保线缆都连接在正确的接口、CSU/DSU以及电话公司的网络端结点上。利用show controllers命令确定线缆是分别接在哪些接口上的 4. 运行debug serial interface命令 5. 如果在本地回送方式下线路协议仍旧没有正常工作，并且debug serial interface命令的输出信息表明keepalive计数器并没有逐步递增，那么说明路由器硬件可能出现了故障。可以更换路由器的接口硬件 6. 如果线路协议工作正常，并且keepalive计数器在逐步递增，这说明问题不在本地路由器 7. 如果怀疑路由器硬件出现问题，可以将串行线路连接到其他的接口上。如果线路能够正常工作，这就说明原先的接口存在问题
Serial *x* is up, Line protocol is down（DCE模式）	没有使用clockrate接口配置命令 DTE设备不支持或没有设置SCTE模式（终端定时） 远程CSU或DSU出现故障	1. 为串行接口增加clockrate接口配置命令： clock rate *bit/s* *bit/s*是需要设定的时钟率（bit/秒）：1,200, 2,400, 4,800, 9,600, 19,200, 38,400, 56,000, 64,000, 72,000, 125,000, 148,000, 250,000, 500,000, 800,000, 1,000,000, 1,300,000, 2,000,000, 4,000,000，或8,000,000 2. 如果允许的话，将DTE设备设置为SCTE模式。如果CSU/DSU不支持SCTE，那么就需要在Cisco路由器接口上禁用SCTE功能

（续表）

状态行	可能的故障	故障的排除方法
		3. 确保使用正确的电缆 4. 如果线路协议仍旧没有正常工作，那么说明可能出现了硬件故障或线缆故障。在线路上接入断接盒，并查看线路上的信号 5. 如果需要的话，可以更换出现故障的部件
Serial *x* is up, line protocol is up（looped）	电路上存在环路。当检测到回路存在时，就将keepalive分组中的序列号改为一个随机数。如果具有相同随机数的分组沿链路返回，那么说明存在回路	1. 利用show running-config特权命令查看路由器的配置信息中是否存在loopback接口配置命令的条目 2. 如果路由器配置信息中存在包含loopback接口配置命令的条目，那么应该利用no loopback接口配置命令删除环路 3. 如果路由器配置信息中没有包含loopback接口配置命令的条目，那么可以检查CSU/DSU并确定其是否被设置为手动回送模式，如果是这样的话，应当禁用手动回送模式 4. 复位CSU或DSU，并检查线路状态。如果线路协议工作正常，那么就不需要进行其他的操作 5. 如果CSU或DSU没有被设为手动回送模式，这时可以与租用线或其他载波服务的供应商联系，确定线路是否存在故障
Serial *x* is up, line protocol is down（disabled）	电话公司服务故障所导致的高误码率 CSU或DSU硬件故障 路由器硬件故障	1. 利用串行分析仪及断接盒检查线路故障。查看CTS（Clear to Send）和DSR（data set ready）信号的切换 2. 让CSU/DSU构成回路（DTE回路）。如果问题依旧存在，那么可能是硬件故障。如果问题不再出现，那么故障可能源于电话公司 3. 如果需要的话，更换损坏的硬件（CSU、DSU、交换机、本地或远程路由器）
Serial *x* is administratively down, line protocol is down	路由器配置信息中含有shutdown接口配置命令 IP地址重复	1. 查看路由器配置信息中是否包含shutdown命令 2. 利用no shutdown接口配置命令消除shutdown命令的作用 3. 利用show running-config特权命令或show interface命令确定是否存在相同的IP地址 4. 如果存在相同IP地址的话，就需要对IP地址进行修改

show controllers命令是解决串行线路故障的另一重要的诊断工具。根据设备类型的不同，这一命令的语法形式有所不同，如下所列：

- 对于Cisco 7000系列路由器上的串行接口来说，应该使用show controllers cbus命令。
- 对于Cisco接入服务器产品来说，应该使用show controllers命令。

对于像Cisco 1700、2000、2500、2600、3000和Cisco 4000系列访问服务器与路由器来说，应该使用show controllers命令。例13-2显示了在Cisco 2621访问服务器上对串行接口使用show controllers命令时的输出信息。

例13-2 show controllers命令

```
Router#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
idb at 0x81414E2C, driver data structure at 0x8141753C
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x06
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
```

在show controllers命令的输出显示信息上，包括了接口信道的状态和线缆连接是否正常的信息。注意在此例当中，串行接口0/0连接的是v.35线缆。

如果电气接口的类型显示为UNKNOWN（而不是v.35、EIA/TIA-449或其他的电气接口类型），可能是由于线缆连接不正确导致的。接口卡内部的配线问题也有可能导致这种情况。如果不能识别电气接口类型，那么show interface serial命令的输出信息可能显示为串行接口及线路协议工作不正常。

下面将介绍一些在解决串行线路及广域网故障时非常有用的debug命令：

• debug serial interface——验证接收到的HDLC keepalive分组的数量是否在不断增加。如果接收到的keepalive分组不再增加，那么可能是因为网络或串行接口中存在时钟同步问题。例13-3为网络中的debug输出信息。

• debug arp——指出路由器是否在利用ARP分组发送或学习关于WAN云图中另一端路由器的信息。当TCP/IP网络中的某些节点有响应面其他节点没有响应的时候，可以利用这一命令检测故障。

• debug frame-relay lmi——获取本地管理接口（LMI）的信息，可以用于确定帧中继交换机及路由器是否正在发送或接收LMI分组。

• debug frame-relay events——确定路由器与帧中继交换机之间是否有数据交换。

• debug ppp negotiation——显示PPP启动过程中进行协商PPP选项时所传输的PPP分组。

• debug ppp packet——显示发送和接收的PPP分组。这个命令显示了下层分组内容。

• debug ppp errors——显示与PPP连接的协商及操作过程有关的错误信息（如非法帧或错误帧）。

• debug PPP chap——显示PPP CHAP和PAP的分组交换过程。

警告 由于在CPU的任务处理过程中，debug命令的信息输出具有很高的优先级，会导致系统不可用。因此，应该只有在解决特定问题或与Cisco技术支持人员进行交流时才使用debug命令。此外，最好是在网络通信流量很低、用户人数很少的情况下使用debug命令。这样才能尽量降低debug命令对系统带来的负面影响。

例13-3 debug serial interface命令

```
Router#debug serial interface
Serial network interface debugging is on
Router#
00:06:47: Serial0/0: HDLC myseq 29, mineseen 29*, yourseen 29, line up
00:06:57: Serial0/0: HDLC myseq 30, mineseen 30*, yourseen 30, line up
```

```
00:07:07: Serial0/0: HDLC myseq 31, mineseen 31*, yourseen 31, line up
00:07:17: Serial0/0: HDLC myseq 32, mineseen 32*, yourseen 32, line up

Router#undebug all
All possible debugging has been turned off
Router#
```



实验活动 串行接口故障排除

在这个试验中，对两台相连路由器的串行接口进行配置。然后利用show命令来对它们之间的连通性问题进行故障排除。

13.12 配置PPP

PPP有很多可以配置的方面，包括身份验证、压缩和错误检测以及是否支持多链路功能。本章主要描述不同的PPP配置选项。

表13-4中所列为可供PPP封装的Cisco路由器配置的LCP选项。

表13-4 LCP配置选项

选项	功能	协议	命令
身份验证 Authentication	身份验证选项需要链路建立的呼叫方输入信息，用以确保呼叫者发起呼叫时拥有网络管理员的许可。对等路由器之间相互交换身份验证消息。下列所示的是可供选择的两种验证方式： -PAP -CHAP	PAP CHAP	ppp authentication pap ppp authentication chap
压缩 Compression	压缩选项通过减少链路中数据帧所含的数据大小，来提高PPP线路的吞吐量。当到达目的地后，协议对数据帧进行解压缩。（见图13-5） Cisco路由器支持两种压缩算法，它们是Stacker和Predictor	Stacker或 Predictor	ppp compress stacker ppp compress predictor
错误检测 Error-Detection	PPP的错误检测机制使进程能够识别错误的情形。Quality式Magic Number用来确保实现一条可靠的、无环路的数据链路	Quality式 Magic Number	ppp quality *number_1-100*
多链路 Multilink	Cisco IOS版本11.1及以后的版本支持PPP的多链路（MP）。这项功能有时也被称为Multilink PPP。这个选项为使用PPP的路由器端口提供了负载均衡的功能。MP利用把分组分段并排序来分割PPP的负载，然后在多条并行电路上发送数据段。在一些方案中，MP可以将多条物理线路组合成一条逻辑链路，这样就能提高两台路由器之间的吞吐能力而且降低了系统的延时	MP	ppp multilink

13.13 配置PPP封装

下列操作可在接口serial 0上启动PPP封装：

```
Router# config terminal
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

在启动PPP封装的串行接口上可以配置点到点软件压缩功能。执行软件压缩功能可能会显著地影响系统性能。如果传输的数据大多数为已经压缩的文件，则这时不推荐使用压缩功能。

要配置PPP的压缩功能，应在接口配置模式下执行下列的操作：

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# compress [predictor | stac]
```

输入下列命令可以监控链路上丢弃的数据，以防止数据帧环：

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp quality number_1-100
```

下列命令可配置多链路负载平衡：

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink
```



实验活动 配置PPP封装

在本试验中，请在两台相连的路由器的串行接口上启动PPP封装，然后测试它们之间的链路。

13.14 配置PPP身份验证

表13-5中的过程概要描述了如何配置PPP封装及PAP/CHAP身份验证协议。

表13-5 配置PAP/CHAP

步骤	操作	结果及注意事项
1.	通过在全局模式下使用hostname命令为主机赋予主机名： Router（config）#hostname SantaCruz	这里指定的名称必须和链路另一端路由器中username所使用的主机名相匹配 注意-hostname命令对大小写敏感
2.	定义验证时远端路由器需要的用户名和密码，应在全局模式下使用username *name* password *password* Router（config）#username HQ password cisco	在Cisco路由器中，两台路由器必须具有相同的密码 在IOS11.2版本以前，这个密码是加密的，是secret密码。要在基于IOS的路由器上加密密码，应在全局配置模式下输入password-encryption命令
3.	通过使用接口配置命令encapsulation PPP在接口上启动PPP封装： Router（config-if）#encapsulation ppp	要在异步串行接口上启动PPP封装还需要其他的附加命令
4.	配置PPP身份验证功能时使用接口配置命令ppp authentication {chap | chap pap | pap chap | pap}： router（config-if）#ppp authentication chap	如果同时启动了这两种验证协议，则配置中指定的第一种验证方式在链路协商过程中将被请求使用。如果另一端设备建议使用第二种验证方法，或简单的拒绝了第一种验证方法，那么这两台设备之间就开始尝试使用第二种验证方法
5.	利用show interface命令来验证配置是否正常工作： router#show interface s0	当PPP被配置后，可以用这个命令查看LCP和NCP的状态

正确的掌握这些配置是绝对有必要的，因为PAP和CHAP要依靠这些参数来实现验证功能。

图13-24中描述了一个两次握手的PAP验证配置的例子。这两台路由器之间彼此验证，所以在每一台路由器上都要配置PAP验证命令。而且每一台路由器发送的PAP验证用户名和密码必须与其他路由器上的用户名和密码相匹配，这些用户名和密码是用命令username *name* password *password*建立的。

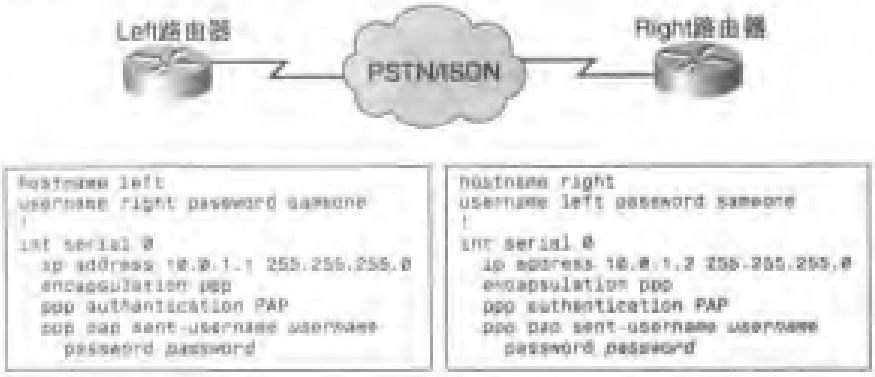


图13-24 PAP配置

图13-25所示为CHAP验证中出现的双向验证过程。在这种情况下，路由器的主机名必须和另一台路由器配置中的username命令指定的名称相匹配，密码必须一致。

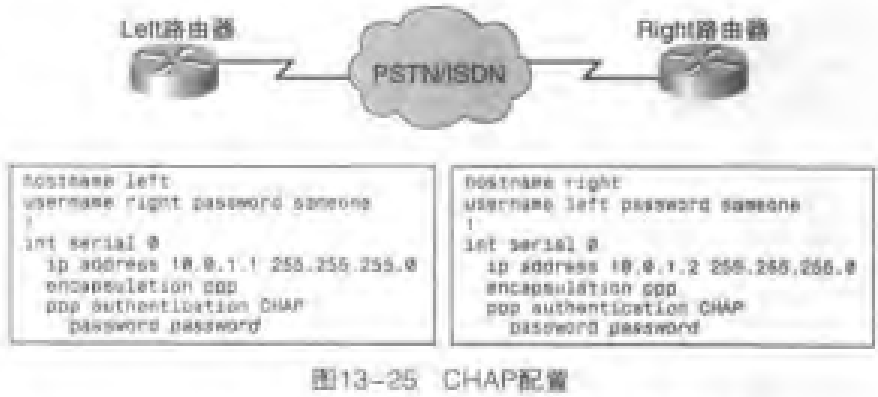


图13-25 CHAP配置

使用下面的方法可以使你更简单的在路由器上进行CHAP的配置任务：

- **你可以在多台路由器上使用相同的主机名**——当你想让远程用户在验证过程中认为他们连接的是同一台路由器时，可以在每一台路由器上利用下列命令配置相同的主机名：

```
router(config-if)#ppp chap hostname hostname
```

- **你可以通过一个口令来验证一台未知主机**——这样做可以限制路由器中保存的用户名/密码的条目数量。通过使用下面的命令，你可以配置一个密码，当任一主机对路由器进行验证时，路由器将向验证主机发送这个密码：

```
router(config-if)#ppp chap password secret
```



实验活动 配置PPP身份验证

在本试验中，请在两台路由器之间配置CHAP身份验证。

13.15 检验串行PPP封装配置

使用show interface命令来检验HDLC或PPP封装正确的配置，正如例13-4中所示。当HDLC被配置后，“Encapsulation HDLC”将会显示在show interface的输出信息中。当PPP被配置后，你可

以使用这条命令检查PPP的LCP和NCP状态。

例13-4 检验串行PPP封装配置

```
Router#show interface s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
 -- output omitted ---
```

表13-6列出了在PPP的建立，配置和检验过程中所使用的命令。

表13-6 PPP命令

命令	描述
encapsulation ppp	在接口上启用PPP封装
ppp authentication pap	在接口上启用PAP身份验证方式
ppp authentication chap	在接口上启用CHAP身份验证方式
username *username* password *password*	建立一个基于用户名的验证系统
show interface	显示路由器或访问服务器上所有配置过的接口的状态
debug ppp authentication	对PAP或CHAP的验证过程进行调试
undebug all	关闭所有调试信息的显示



实验活动 验证PPP配置

在本试验中，把两台相连路由器的串行口配置为PPP协议，并且检验它们之间的链路。

13.16 对串行PPP封装配置进行故障排除

使用debug PPP authentication命令可以显示验证过程中验证信息的交换顺序。例13-5图示了左面路由器和右面路由器进行验证时使用debug ppp authentication命令输出信息。当配置双向验证后，每一台路由器彼此验证对方，并且显示的信息为所有验证过程和被验证过程的情况。CHAP定义为一种单向验证的方法，然而我们仍然可以使用CHAP在全部的链路方向上创建双向验证。因此，CHAP双向验证的双方都发起独立3次握手过程。这条命令可以显示验证过程中所发生的验证信息交换顺序。

例13-5 串行PPP故障排除

```
4d20h: %LINK-3 UPDOWN: Interface Serial0, changed state to up
4d20h: Se0 PPP: Treating connection as a dedicated line
4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from "left"
4d20h: Se0 CHAP: I CHALLENGE id 3 len 28 from "right"
```

```
4d20h: Se0 CHAP: O RESPONSE id 3 len 28 from "left"
4d20h: Se0 CHAP: I RESPONSE id 2 len 28 from "right"
4d20h: Se0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0 CHAP: I SUCCESS id 3 len 4
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
```

表13-7汇集了左面路由器的双向PAP验证输出信息。

表13-7 PAP身份验证

输出显示	描述
Se0 PPP: Phase is AUTHENTICATING, by both	双向验证
Se0 PAP: O AUTH-REQ id 4 len 18 from "left"	输出的验证请求
Se0 PAP: I AUTH-REQ id 1 len 18 from "right"	进入的验证请求
Se0 PAP: Authenticating peer right	验证进入
Se0 PAP: O AUTH-ACK id 1 len 5	输出的确认信息
Se0 PAP: I AUTH-ACK id 4 len 5	进入的确认信息

Debug ppp命令用来显示与PPP操作有关的信息。在这条命令前加上no就可以关闭相应的调试信息输出。表13-8列出了可供debug ppp命令使用的不同选项。

```
debug ppp {packet | negotiation | error | chap}
no debug ppp {packet | negotiation | error | chap}
```

表13-8 debug ppp 命令选项

命令选项	说明
packet	使用debug ppp packet显示发送和接收的PPP分组
negotiation	使用debug ppp negotiation显示PPP启动过程中进行协商PPP选项时所传输的PPP分组
error	使用debug ppp error命令显示与PPP连接的协商及操作过程有关的协议错误和错误统计
chap	使用debug ppp chap命令显示PPP CHAP和PAP的分组交换过程



实验活动 PPP配置故障排除

在本试验中，你将在两个路由器上配置PPP协议，并使用show和debug命令对连通性问题进行故障排除。

13.17 总结

在本章中，你学习了以下的内容：

- PPP是一种被广泛使用的广域网协议。
- PPP通过使用LCP（链路控制协议）和一组NCP（网络控制协议）来协商可选的配置参数和程序，解决了因特网的连通性问题。
- PPP会话有4个阶段：
  - —— 链路建立。
  - —— 链路质量检测。
  - —— 网络层协议配置协商。
  - —— 关闭链路。
- 当配置PPP验证时可以选择PAP或CHAP。
- PAP不是一种健壮的验证协议。

• CHAP使用一个惟一的、不可预测的挑战值来防范回放（playback）攻击。

• 用encapsulation ppp命令来配置接口以使用PPP进行封装。

• 当PPP配置完成后，使用show interface命令可以检查LCP（链路控制协议）和NCP（网络控制协议）的状态。

13.18 关键术语

质询握手验证协议（*Challenge Handshake Authentication Protocol*, CHAP） 质询握手验证协议是指在使用PPP封装的线路上支持的安全特性，它阻止未授权的访问。CHAP本身不阻止未授权的访问，它只标识远程终端。路由器或接入服务器决定是否允许用户访问。

链路控制协议（*Link Control Protocol*, LCP） 链路控制协议是建立、配置、保持和终止点到点连接的协议。

逻辑链路控制（*Logical Link Control*, LLC） 逻辑链路控制是数据链路层的两个子层中较高的子层，它是由IEEE定义的。LLC子层处理错误控制、数据流控制、成帧和MAC子层寻址。最普遍的LLC协议是IEEE802.2，它包括无连接和面向连接两个变体。

网络控制程序（*Network Control Program*） 网络控制程序是一种路由并控制通信控制器和其他网络资源间的数据流动的程序。

密码验证协议（*Password Authentication Protocol*, PAP） 密码验证协议是允许PPP对等实体之间进行相互验证的一种验证协议。试图连接到本地路由器的远程路由器需要发出一个验证请求。与CHAP（挑战握手协议）不同，PAP以明文方式（非加密方式）传送密码和主机名或用户名。密码验证协议本身不能防止未授权的访问，只是能鉴别远程终端。然后由路由器或接入服务器决定该用户是否有权访问。只有在PPP线路上才支持PAP。

点到点协议（*Point-to-Point Protocol*, PPP） 点到点协议是SLIP（串行线路因特网协议）的后继，它提供了在同步和异步电路上的路由器到路由器和主机到网络的连接。

13.19 复习题

1. 在PPP链路上建立连接的第一步包括：
   A. 初始的PPP节点向最近的PPP邻居发送一个会话启动消息
   B. 在PPP链路激活以前，路径上的路由器与身份验证程序进行协商
   C. PPP节点为动态地址分配进行通告或查询服务器为地址分配进行通告
   D. 初始节点为配置数据链路而发送链路控制协议（LCP）帧
2. 在PPP中，如果链路控制协议（LCP）终止了一条链路，会发生什么？
   A. 目的节点将尝试建立一条新链路
   B. NCP（网络控制协议）发送一个链路维持帧
   C. 初始节点重新建立连接会话过程
   D. 链路控制协议（LCP）通知网络层协议
3. PPP支持以下哪种网络层协议？
   A. Novell IPX
   B. IP
   C. AppleTalk
   D. 以上全部
4. PPP中的NCP（网络控制协议）实现以下哪种功能？
   A. 建立链路
   B. 封装多种协议
   C. 把分组转变成信元
   D. 建立连接
5. 在PPP的帧里，哪个字段标识封装的是IPX还是TCP/IP？
   A. 标识字段
   B. 控制字段
   C. 协议字段
   D. 帧检验序列
6. PPP在什么情况下最可能会被本地工作站用于建立到因特网的连接？
   A. 工作站直接连到局域网内
   B. 工作站直接连到路由器上
   C. 工作站需要拨号连接到因特网
   D. 永远不会被工作站使用
7. 当使用PPP时，LCP负责：
   A. 建立、保持和中断点到点的连接
   B. 保持多条链路
   C. 路由器的更新
   D. 压缩
8. PPP会话的建立包括几个阶段？
   A. 2
   B. 3
   C. 4
   D. 1
9. 当选择PAP作为PPP的验证协议时，将使用哪种类型的握手？

A. 1次握手
B. 2次握手
C. 3次握手
D. 4次握手

10. 检查LCP（链路控制协议）和NCP（网络控制协议）的状态可以使用以下哪条路由器命令？
A. router>show interfaces
B. router（config）# show interface
C. router# show interfaces
D. router（config-if）# show interfaces

11. 你将会使用哪种协议在ISDN上建立一个远程连接？
A. PPP
B. SLIP
C. PAP
D. CHAP

12. 当PPP在几条链路上进行负载均衡时，利用了什么特性？
A. PAP
B. 栈式存储器（stacker）
C. 压缩
D. 多链路

13. PPP链路的建立需要链路控制协议（LCP）开启一个连接，然后：
A. 协商配置参数，发送和接收一个配置确认帧
B. 测试链路，并且判断链路质量是否适合网络协议
C. 对PPP节点进行轮询，并且决定是否存在一个到达NCP（网络控制协议）服务器的路径
D. 向最近的上传PPP邻居发出查询，以获取路由选择的度量值（比如跳数）



第14章 ISDN和DDR

目标

学习完本章后，你将能够：

- 描述综合业务数字网（ISDN）的体系结构。
- 描述ISDN协议层。
- 配置ISDN。
- 配置按需拨号路由选择（DDR）。
- 验证并排除ISDN故障。
- 验证并排除DDR故障。

本章介绍并描述了一组称为*ISDN*的技术，首次提出该技术是在30多年前。开发者们认识到公共交换电话网（PSTN）所固有的局限性，预想ISDN可以提供一系数字管道，该管道通提供多种服务的综合通道。这些服务包括语音，分组交换甚至视频。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图，光盘上的素材与本章内容的补充，能强化本章所介绍的概念。

14.1 ISDN标准

这些年来通过了许多ISDN标准。这些标准承诺为家庭和商业提供高速的数字服务。尽管ISDN有广泛的标准，但电信公司并没有实施所有这些技术。因此ISDN的配置和价格随地区的不同变化也很大。

现在，用户使用ISDN主要用于广域网备份技术以及向远程办公者和小型办公室提供远程接入服务，如图14-1所示。服务商和大公司采用基群速率接口（PRI）来提供对多种POTS的支持（模拟modem）或ISDN基本速率接口（BRI）拨号。虽然ISDN与POTS相比有连接建立速度快和吞吐量大的优点，但许多潜在的BRI用户还是转向了数字用户线（DSL）和有线技术。这些大都是吞吐量大且成本低廉的技术。

尽管有这些新技术出现，ISDN依然是一种远程接入的可行方案，因为：

- 有条件使用ISDN的地方比DSL或有线技术的地方更广泛。
- 许多大公司和服务提供商在ISDN设备和培训上进行了大规模的投资，并计划继续平衡投资。

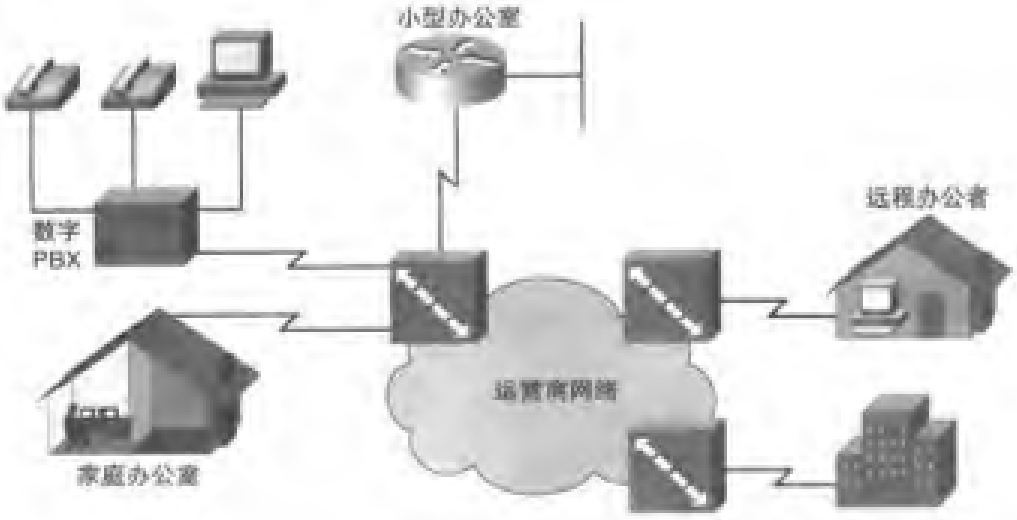


图14-1　综合服务

• 使用ISDN的远程办公室可以直接连接到中心局（CO）而不用穿越公用因特网。多数DSL技术和有线技术的实施都需要远程主机通过跨因特网的虚拟专用网（VPN）与中心站点通信。

14.2　ISDN概述

许多广域网技术都可以用于远程网络接入。本章讲述的是ISDN通信的服务、标准、组件、运行以及配置。ISDN专门设计用来解决小型办公室或拨号用户使用传统电话拨号服务时带宽较低的问题。

传统的公共交换电话网是基于用户端设备与本地交换机之间的模拟连接，也称为本地环路（local loop），如图14-2所示。这种模拟信号使得从本地环路可以获得的带宽受到限制。带宽限制不允许模拟数据以高于3,000Hz的速度传播。通过在本地环路上使用数字信号就可以去除带宽的限制，从而使远程用户得到更快的接入速度，如图14-3所示。而使用模拟调制解调器拨号的用户仍旧使用模拟语音本地环路系统的3kHz的带宽，这就限制他们使用大约56kbit/s的下载速率和33kbit/s的上传速率。

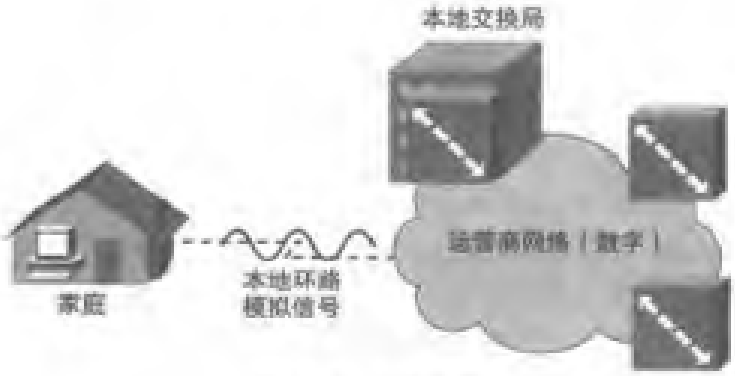


图14-2　本地环路

电话公司开发ISDN意在创建一个完整的数字网络。ISDN允许在现有的电话线上传递数字信号。当电话公司的交换机升级为可以处理数字信号时，这才成为可能。ISDN通常用于远程办公以及将小型或远程办公室接入公司局域网中。

电话公司开发ISDN也是标准化用户服务的一部分。这包括用户-网络接口（UNI，User-Network Interface），通常称为本地环路（Local Loop）。ISDN标准定义了端到端数字连接所需的硬件和呼叫建立方案，这对达到通过保证ISDN网络之间便利通信从而实现世界范围连通性的目标也有帮助。在ISDN网络中，数字化功能是在用户端完成的，而不是在电话公司完成的。

正如其名字所示，ISDN使用的是数字技术。ISDN以高速数字设备来替代传统模拟电话设备，从而向用户提供一条数字的本地环路。图14-4是模拟通信与数字通信的对比。因此，ISDN端到端的传输都是数字的。因为普通老式电话服务（POTS）使用模拟的本地环路，电信运营商必须使用脉码

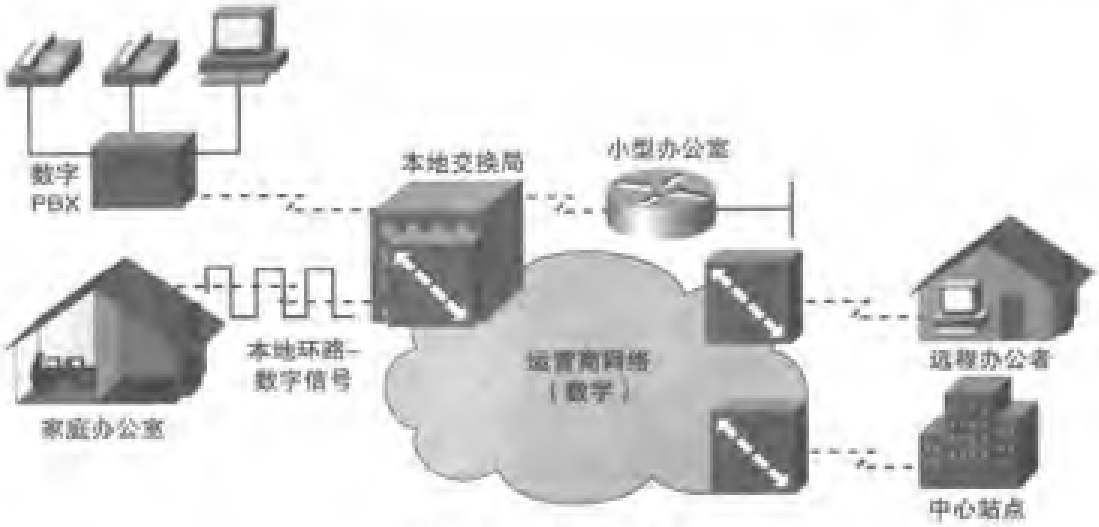


图14-3 ISDN数字通信

调制（PCM）来对模拟信号进行编码以进行数字传输。这种类型的模拟到数字转化就引入了我们所不希望的延时以及潜在的噪声。

ISDN使本地站点可以进行数字连接，数字连接有很多好处，包括：

- 可以承载多种类型的网络流量（如数据，语音和视频）。
- 呼叫建立过程比普通电话服务快。
- 数据传输速率比传统调制解调器快。

用户可以通过两种不同的物理接口连接到ISDN网络：BRI和PRI。单一的BRI或PRI接口提供一组复用的B信道和D信道，如图14-5所示。

ISDN的B信道称为承载信道（bearer

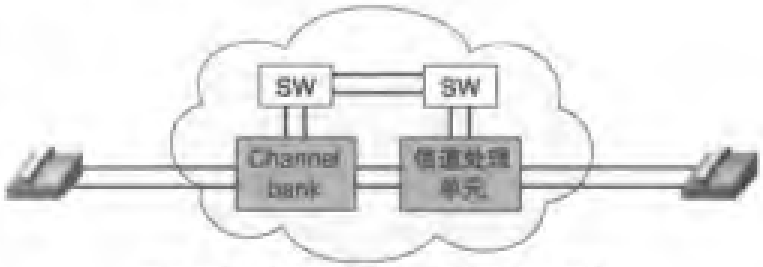


图14-4 模拟与数字的对比

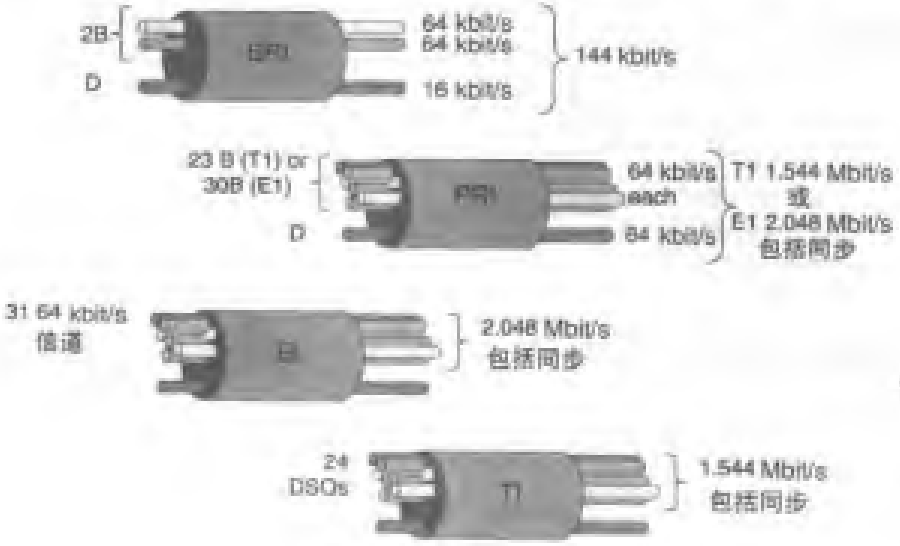


图14-5 ISDN服务

channels），因为它们传送语音，数据和传真。B信道以帧的形式运载信息，使用高级数据链路控制（HDLC）和点到点协议（PPP）作为第2层协议。

D信道，或称为delta信道，用于带外信令（out-of-band signaling）。D信道运载控制信息，如呼叫建立和拆除。通常D信道在第2层使用D信道链路接入过程（LAPD, Link Access Procedure on the D Channel）。

BRI服务通过一条本地铜线环路来提供，此环路用于承载传统模拟电话服务。在北美，大多数ISDN本地环路的最大长度大约为18,000feet（约5.5km）。

BRI有以下特点：

- 2条64kbit/s的承载信道。
- 1条16kbit/s的delta信道。
- 48kbit/s的成帧和同步信息。
- 总速率为192kbit/s。

论及BRI的带宽时，了解所指的是ISDN的哪种特征是非常重要的。如果指的是用户数据的带宽，BRI可以提供128kbit/s（2条64kbit/s的B信道）。如果所指的带宽是B信道和D信道的，BRI可以提供144kbit/s。如果所指的带宽是ISDN BRI的总带宽，包括成帧和同步，那么其带宽将为192kbit/s，但我们很少这样说。

ISDN PRI通过客户内部设备（CPE）与ISDN交换机之间的T1和E1租用线来提供。ISDN交换机通常是中心局的一台5类Telco交换机，它也可以处理语音呼叫。

T1参考DS1（第1类数字信号），DS1由24条DS0（第0类数字信号）组成，每条DS0信道的带宽为64kbit/s，如表14-1所示。一条单个的ISDN B信道是一个DS0。基于T1的PRI的特点：

- 23条64kbit/s的承载信道。
- 1条64kbit/s的D信道，位于第24时隙。
- 8kbit/s的成帧和同步信息。
- 总速率为1.544Mbit/s。

基于E1的PRI的特点：

- 30条64kbit/s的承载信道。
- 1条64kbit/s的D信道，位于第16时隙。
- 64kbit/s的成帧和同步信息。
- 总速率为2.048Mbit/s。

表14-1 数字信号级别

数字信号级别	速率	T名称	信道或DS0数
DS0	64kbit/s	-	1
DS1	1.544Mbit/s	T1	24
DS2	6.312Mbit/s	T2	96
DS3	44.736Mbit/s	T3	672
DS4	274.176Mbit/s	T4	4032

DS0 = 数字服务（0）

14.3 ISDN标准及接入方式

ISDN的标准化工作开始于20世纪60年代后期。1984年发布了一整套ISDN建议，其后一直由国际电信联盟-电信标准部（ITU-T）[原国际电报电话咨询委员会（CCITT）]进行更新。ISDN是一套围绕数字电话和数据通信的协议。ITU-T依照以下几个常用主题对ISDN协议进行分组和组织：

• E协议——推荐使用的ISDN电话网络标准。例如，E.164协议描述了ISDN全球寻址。

• I协议——涉及概念、术语和一般方法。I.100系列包含了一般ISDN概念及其他I系列建议的结构。I.200是关于ISDN服务方面。I.300描述了网络方面的建议。I.400描述了如何提供用户网络接口（UNI）。

• Q协议——包含了交换以及信令的运行部分。术语信令在这里表示ISDN呼叫的建立过程。

ISDN标准定义了两种主要的信道类型，每一种都有不同的传输速率。承载信道（B信道）定义为64kbit/s的完全数字路径。称为“完全”是因为它可以传输任何类型的数字化数据，比如一个全双工模式的数字化语音呼叫。另一条信道称为delta信道（D信道），其速率为16或64kbit/s。BRI的D信道为16kbit/s，PRI的D信道为64kbit/s。ISDN的接入选项如图14-6所示。D信道用来为B信道传输控制信息。记住：当一个TCP连接建立时，有一个信息交换的过程，称为连接建立（Connection Setup）。信息沿最终数据传输时所使用的路径进行交换。控制信息和数据共享同一条路径，这称为带内信令。ISDN的控制信息使用一条独立的信道：D信道，这称为带外信令。

信道	容量	主要用于
B	64 kbit/s	电路交换的数据
D	16/64 kbit/s	信令发送信息

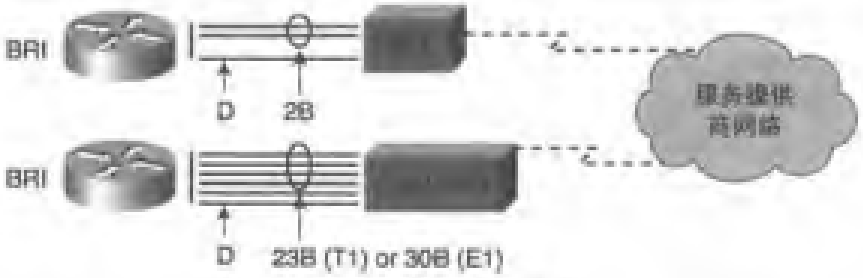


图14-6 ISDN接入选项

ISDN指定两种标准的接入方法：BRI和PRI。单一的BRI或PRI接口提供一组复用的B信道和D信道。

BRI使用2条64kbit/s的承载（B）信道加上1条16kbit/s的delta（D）信道。B信道传输用户数据，D信道用于发送信令和控制信息。许多Cisco路由器都支持BRI。因为BRI使用2条B信道和1条D信道，有时也被写成2B+D。

B信道可用于数字化语音传输。这时就需要使用专用的语音编码方法。同样B信道也可以用于相对高速的数据传输。在这种模式下，信息在数据帧中传输，帧格式使用第2层HDLC或PPP协议。PPP与HDLC相比更健壮，因为它提供了很好的验证、链路协商和协议配置的机制。

窄带ISDN是电路交换的连接。B信道就是电路交换的成分。

D信道运载信令信息，如呼叫建立和拆除，以控制B信道。D信道的数据流使用LAPD协议。LAPD是基于HDLC的数据链路层协议。在北美和日本，PRI提供23条64kbit/s的B信道和1条64kbit/s的D信道。

在欧洲和世界其他大多数地区，PRI提供30条B信道和1条D信道，因此它能提供与E1电路相同级别的服务。PRI将DSU/CSU用于T1/E1连接。

14.4 ISDN3层模型及协议

ISDN使用一套ITU-T标准生成OSI参考模型的物理层、数据链路层和网络层，如表14-2所示：

• ITU-T I.430和I.431分别定义了ISDN BRI和PRI物理层规范。

• ISDN 数据链路层规范是基于LAPD的，在ITU-T Q.920、ITU-T Q.921、ITU-T Q.922以及ITU-

T Q.923中正式定义。

• ISDN网络层在ITU-T Q.930（也称为I.450）和ITU-T Q.931（也称为I.451）中定义，定义了用户到用户的、电路交换和分组交换的连接。

表14-2　ISDN协议

OSI层	D信道	B信道
3	Q.931——终端和交换机之间的ISDN网络层	IP
2	Q.921——D信道链路接入过程	PPP HDLC
1	I.430/I.431——ISDN物理层接口： I.430用于基本接口 I.431用于基群接口	

BRI服务是通过传统模拟电话服务使用的本地铜线环路来提供的。传统模拟电话服务只有一条物理路径，但对于BRI，有3条独立的信息路径（2B + D）。3条信道的信息复用到一条物理路径上。

ISDN物理层（第1层）的帧格式取决于该帧是出站（从终端到网络——TE帧格式）还是入站（从网络到终端——NT帧格式），两者格式不同，如图14-7所示。每一个帧包含16比特B1信道数据，16比特B2信道数据，4比特D信道数据和12比特开销，总长度为48比特。每秒钟可传送4,000个这样的帧，这样，B1和B2信道的容量就是16 × 4,000=64kbit/s，D信道的容量就是4 × 4,000=16kbit/s。

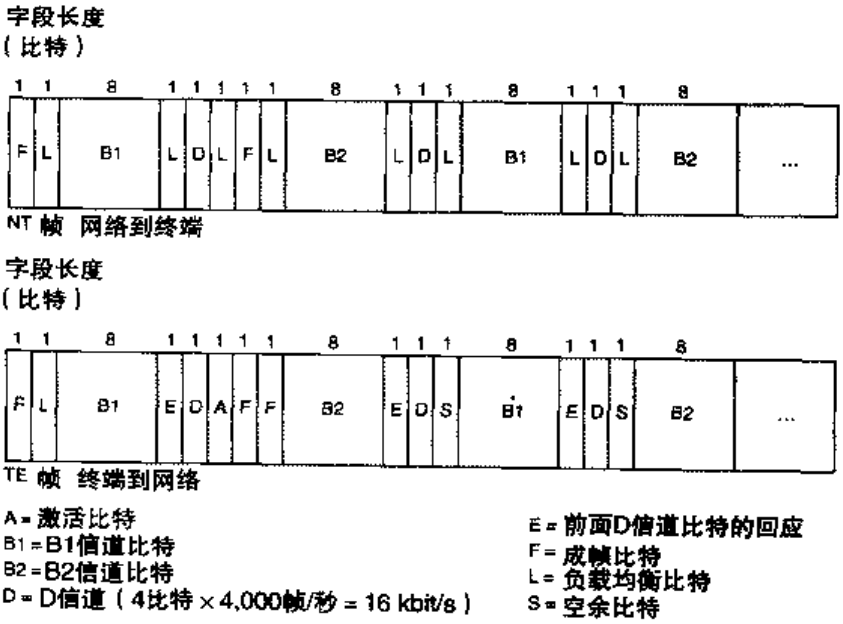


图14-7　ISDN物理层帧格式

ISDN物理层数据帧的开销部分用于以下用途：

• **成帧比特**（*Framing bit*）——提供同步。

• **负载均衡比特**（*Load Balancing bit*）——调整平均位值。

• **前面D信道比特的回应**（*Echo of Previous D Channel bit*）——当几台位于同一被动总线的终端竞争同一条信道时，用于解决竞争问题。

• **激活比特**（*Activation bit*）——激活设备。

• **空余比特**（*Spare bit*）——未指定。

• **8个附加信道比特的累计比特**（*8 added Channel bit conuts bits*）。

注意：BRI接口的物理比特速率是4,000 × 48=192kbit/s。有效比特速率是4,000 × 36 = 144kbit/s =

64kbit/s + 64kbit/s + 16kbit/s（2B + D）。

ISDN第2层的信令协议是LAPD。LAPD与HDLC相似。LAPD用在D信道上，用于确保控制信息和信令能够发送和正确接收。

如图14-8所示，LAPD的标记和控制字段与HDLC相同。LAPD地址字段长2bytes。地址字段的第1字节包含服务接入点标识符（SAPI, Service access point idemifer）。SAPI标识了LAPD向第3层提供服务的入口。命令/响应（C/R）比特表示数据帧包含的是一条命令还是一个响应。第2个字节包含了终端终点标识符（TEI）。每个用户端的终端设备都需要一个惟一的标识符。TEI可以在设备安装时静态指定（0-63），或是在呼叫时由交换机动态分配（64-126）。TEI字段全为1（127）表示广播。



图14-8 ISDN数据链路层

TEI与SAPI一起组成完整的第2层地址。SAPI是一个6bit的数字，用于标识和管理连接到ISDN网络上的同一设备的不同数据类型。记住：一些ISDN消息用于呼叫建立和拆除，而另外一些是实际数据。因此，TEI代表特定的ISDN设备，而SAPI代表此设备上运行的特定进程。例如，SAPI值为0表示呼叫控制进程，而SAPI值为63表示第2层管理功能。

正如以太网II数据帧包含目的介质访问控制（MAC）地址和协议类型信息一样，LAPD数据帧也包含一个TEI和一个SAPI值。

14.5 ISDN呼叫建立

一台路由器要通过ISDN连接到另一台路由器，需要进行一些数据交换。要建立一个ISDN呼叫，需要在路由器和ISDN交换机之间使用D信道，并且在服务提供商网络中的ISDN交换机之间使用7号信令系统（SS7）。

路由器和ISDN交换机之间的D信道总是激活（UP）的。Q.921描述了ISDN数据链路层LAPD的进程，其功能与开放系统互连（OSI）参考模型第2层的过程相似。D信道用于呼叫控制功能，例如呼叫建立，信令发送和呼叫终止。Q.931协议实施了这些功能。Q.931详细说明了OSI参考模型第3层的功能。Q.931标准对终端终点和本地ISDN交换机之间的网络层连接作了建议，但没有强加端到端的建议。因为一些ISDN交换机是在Q.931标准制订之前开发的，所以不同的服务商和交换机类型对Q.931的实施也不同。因为交换机类型不是标准的，就需要在路由器的配置中用命令指定他所连接的ISDN交换机的类型。

可以通过多种方式发起ISDN呼叫。在ISDN呼叫中，呼叫方请求建立一个呼叫，如图14-9所示。在真正进行连接和呼叫之前，可以看到许多不同的消息，例如一个处理消息。这个可选的消息显示了呼叫是如何处理的。



图14-9 ISDN Q.931呼叫建立

警告消息也是一样的，它是一个典型的电话消息，但也不是必需的消息。警告消息也不是数据传输消息。大多数情况下，见到的是数据呼叫的连接消息。

不同的ISDN交换机类型使用不同的呼叫建立和拆除程序。根据交换机类型不同，有的需要图14-9中所显示的所有步骤，有的只需要其中一些步骤。但最基本的呼叫建立、呼叫处理、连接和连接确认消息是必须要交换的。

在BRI和PRI呼叫建立期间，会陆续发生下列事件：

- 通过D信道将被叫电话号码发送到本地ISDN交换机。
- 本地交换机通过SS7信令发送协议建立一条路径并将被叫电话号码发送到远端ISDN交换机。
- 远端ISDN交换机通过D信道向目的地发送信令。
- 在远端路由器表示它将接收这个呼叫之后，远端ISDN交换机使用SS7向本地交换机发回一个呼叫连接消息。
- 一条B信道建立端到端的连接，而另一条B信道还可以用来建立新的会话或数据传输。也可以同时使用两条B信道。

与呼叫建立相似，呼叫拆除不是端到端的功能，而是由ISDN交换机处理的。呼叫释放的过程基于一种3次消息（Three message）方法：

- 挂断（Disconnect）消息。
- 释放（Release）消息。
- 释放完成（Release Complete）消息。

释放消息在网络上以尽可能快的速度传输。图14-10假定由被叫方发起的释放。整个过程是由呼叫方与被叫方之间的D信道上的一个断开消息激发的。接到这个消息之后，用来释放交换路径的信息交换就开始了。交换路径支持着B信道电路。同时也会向下一台交换机发送一个释放消息。这个消息会穿过整个网络，从所有的中间交换机到终端交换机。



图14-10　ISDN Q.931呼叫拆除

在相关的交换机释放呼叫时，一个释放消息最终会传递到最终的交换机。这个传输过程导致以下情况发生：

- 向呼叫方发送一个挂断消息。
- 启动一个计时器以保证对方收到释放消息。
- 断开到交换机的路径。
- 当从前一台交换机收到一个已释放的消息后，向前一台交换机发送一个释放完成消息。

14.6　ISDN功能和参考点

ISDN标准定义了使用户接入BRI或PRI服务的设备或硬件的功能。厂商可以生产支持一种或多种功能的硬件。ISDN规范定义了连接一台ISDN设备和另一台设备的4个参考点。每一台ISDN网络中的设备都执行一种特定任务以促进端到端的连通性。

要连接执行特定功能的设备，两台设备之间的接口需要进行适当的定义。这些接口称为参考点，如图14-11所示。一个参考点就定义了两功能间的一个连接类型。对ISDN连接用户端有影响的参考点有：

- R——非ISDN兼容设备（TE2）和终端适配器之间连接的参考点，如RS-232串行接口。
- S——连接到用户交换设备（NT2）上的参考点，使不同类型的CPE之间能够进行呼叫。
- T——其电子特征与S接口相同，为从NT2到ISDN网络或NT1的出站连接的参考点。

• U——NT1到电话公司提供的ISDN网络之间连接的参考点。

因为S和T参考点电子特征相似，所以一些接口被标成S/T接口。虽然执行的功能不同，但端口电子特征相同并且可以用于任一功能。

面对所有ISDN的缩略语和首写字母缩写词，你可能已经彻底混乱了。要建立ISDN并对其进行故障排除，就需要了解所有这些组件和参考点在现实中是什么样子的。

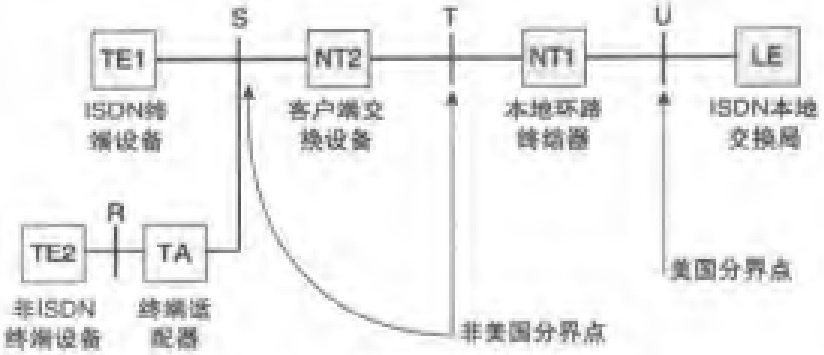


图14-11 ISDN参考点

如图14-12所示，从墙上插座出来的标准两线电缆连接到NT1上，再将从NT1上出来4线电缆连接到ISDN电话、终端适配器、Cisco ISDN路由器和ISDN传真机上。S/T接口采用8线的连接器，可以为NT或TE设备供电。

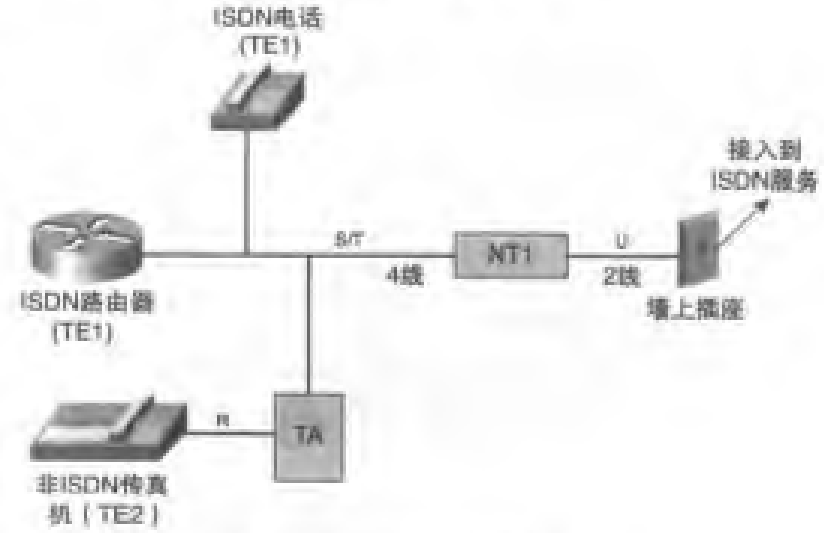


图14-12 ISDNBRI物理参考点

因为所有这些连接器看上去都很相似（例如RJ-11、RJ-45等等），连接时必须注意是什么样的插头和插到什么地方。S/T参考点是一个4线接口（TX和RX）。它可以是点到点连接或多点［被动总线（passive bus）］连接。它采用ITU I.430规范。S/T接口定义了TE1或终端适配器（TA）与NT之间的接口。

U接口定义了NT和ISDN网云之间的两线接口。R接口定义了TA和与之相连的非ISDN设备（TE2）之间的接口。

NT1和NT2合并在一起的设备有时称为NTU。

规范的ISDN S接口可以由多台不同性能的终端设备占有同一条总线（“S”总线）。当交换机可以与多台设备通信时，就称为“多点连接”。不幸的是，这样给设备设置和呼叫处理都增加了难度。解决这个困难需要使用服务配置文件标识符（SPID）和端点标识符（EID）。

选择ISDN设备时，了解参考点类型是非常重要的，因为参考点决定着所需要的ISDN接口类型。在美国，一般需要通过U接口连接到服务提供商。这表示如果购买了一台带有S/T接口的ISDN路由器，就需要另外再购买设备（一台NT1）来连接服务商的网络。同样，如果将一台带有U接口的路由器连接到NT1上，将会导致设备永久性的损坏。因此，弄清楚ISDN的参考点是正确选择和安装ISDN设备的关键。

14.7 确定路由器的ISDN接口

在美国，用户需要提供NT1。在欧洲和许多其他国家，电话公司提供NT1的功能并向用户提供一个S/T接口。这种情况下，用户不需要提供单独的NT1或集成NT1功能的终端设备。像路由器的ISDN模块或接口之类的设备需要按照前面所述来订货。

要选择带有合适ISDN接口的Cisco路由器，需要做以下工作：

步骤1 确定路由器是否支持ISDN BRI。

步骤2 确定NT1的提供者。NT1是到ISDN服务提供商中心局的本地环路的终点。在美国，NT1是CPE（用户室内设备），表示是由用户负责。在欧洲，服务商一般都提供NT1。

步骤3 如果NT1是CPE，要确保路由器具有U接口。如果路由器带有S/T接口，需要外置的NT1连接到ISDN服务提供商。

如果路由器有一个标注“BRI”的接口，表示它支持ISDN。本身已经内置ISDN接口的路由器是TE1。如果路由器有U接口，那它还内置了NT1。

如果路由器没有标注“BRI”的接口并且它是固定结构（非模块化）的路由器，那就必须使用已有的串口。使用像串口之类非真正的ISDN接口时，必须在串口上连接一个TA设备以提供连通性。

对于模块化路由器，如果有可用的插槽，它可以升级具有ISDN接口。注意：不要将一台带有V接口的路由器直接到NT1上，否则可能会损坏接口。

14.8 ISDN交换机类型

需要配置路由器使其识别与其通信的交换机的类型。ISDN交换机的种类很多，部分取决于使用交换机的国家。这是对Q.931的不同实施造成的结果，Q.931是不同供应商制造的交换机所使用的D信道信令协议。

ISDN服务商提供的服务随国家和地区不同，变化也很大。与调制解调器相似，每种交换机的操作与其他的都有轻微差别，并且有一套特定的拨号建立需求。因此，在路由器可以连接ISDN服务之前，必须为它配置中心局所用的交换机的类型。必须在配置时就对路由器指定这些信息，以便路由器可以正确地与交换机通信并进行网络级ISDN呼叫和发送数据。表14-3列举了一些国家所用的ISDN交换机类型。

表14-3 世界各国使用的ISDN交换机的类型

国家	交换机类型
美国和加拿大	AT&T 5ESS和4ESS；北方电信DMS-100
法国	VN2，VN3
日本	NTT
英国	Net3和Net5
欧洲	Net3

除了了解服务商使用的交换机类型之外，了解电信指定的SPID也是必需的。SPID是ISDN服务提供商用于标识ISDN线路配置的数字。SPID允许多台ISDN设备，如语音和数据设备，共享本地环路。National ISDN-1交换机和DMS-100需要用SPID。

SPID只在北美和日本用。ISDN服务商提供一个SPID来标识ISDN服务的线路配置。很多情况下，当配置路由器时，必须要配置SPID。

每个SPID指向一个链路建立和配置信息。SPID通常是一系列类似于电话号码的字符。SPID标识了每一个连接到中心局交换机的B信道。标识之后，这条交换链路就可以为连接服务了。记住：ISDN通常使用拨号连接。在路由器初始连接到ISDN交换机上时，SPID就需要被处理。如果需要SPID，但没有正确配置，初始化过程就会失败，ISDN服务也就不能使用。

14.9 ISDN配置

ISDN定义了ISDN CPE和服务商交换机之间传输的数据和控制信息。ISDN服务商使用多种类型的交换机来提供服务。每种不同类型的交换机在操作上有少许差异，并且有一套明确的呼叫建立需求。必须依照与之通信的中心局交换机的类型对ISDN CPE进行配置。要使路由器能够进行呼叫和发送、接收数据，就必须为路由器配置这些信息。本节主要侧重讲述ISDN的配置。

共有两种ISDN接入类型：BRI和PRI。为了配置起见，我们分别讲述BRI和PRI。本节将会检查用于验证配置的命令是否正确。这部分主要包含以下方面：

- 配置ISDN BRI。
- 配置ISDN PRI。
- 验证ISDN配置信息。
- ISDN配置故障排除。

必须先指定全局和接口参数，为路由器在ISDN环境中运行做好准备。这部分主要讲述接入路由器BRI配置。

在全局配置模式下，必须指定ISDN服务提供商使用的交换机的类型。根据建立连接的国家不同，大约有10种不同的交换机类型可供选择。

ISDN接口配置命令包括指定IP地址、拨号组（为了DDR）以及ISDN服务配置文件标识符（SPID号）。还必须使用dialer map命令将静态映射的目的地与目的IP地址、主机名和ISDN拨号号码关联在一起。

14.9.1 配置ISDN BRI

可以在全局模式或接口模式下配置isdn switch-type *switch-type*命令来指定服务提供商的交换机类型。

在全局配置模式下配置isdn switch-type命令会将所有的ISDN接口设置成相同的交换机类型。全局命令配置之后，可以为单独的接口配置交换机类型。表14-4列举了ISDN BRI交换机类型。

表14-4 ISDN BRI交换机类型

交换机类型	描述
basic-5ess	AT&T基本速率交换机（美国）
basic-dms 100	NT DMS-100（北美）
basic-ni	National ISDN（北美）
basic-1tr6	德国1TR6ISDN交换机
basic-nwnet3	挪威Net3交换机
basic-nznet3	新本兰Net3交换机
basic-ts013	澳大利亚TS013和TS014交换机
basci-net3	英国和欧洲
Ntt	NTT ISDN交换机（日本）

不同的ISDN服务提供商使用的交换机类型不同。实际上，一些服务提供商用一种类型的交换机在软件上模拟另外类型的交换机。服务提供商会告诉你正确的交换机类型信息。如果没有给路由器配置正确的交换机类型信息，路由器就不能使用第3层的Q.931与ISDN交换机通信。换句话说，路由器就不能进行拨出或接收ISDN呼叫。

交换机类型可以通过isdn switch-type命令来设置。但需要确定是在全局配置模式还是接口配置模式下输入此命令。

在全局模式下输入isdn switch-type命令会将路由器的所有接口都配置成相同的交换机类型：

```
Router(config)# isdn switch-type type
```

如果在接口配置模式下输入isdn switch-type命令，则只有正在配置的接口才采用所配置的交换机类型：

```
Router(config-if)# isdn switch-type type
```

注意接口配置模式下的命令会覆盖全局级别的命令。

一般情况下，需要在全局配置模式下使用isdn switch-type命令来设置交换机类型。但有时也需

要指定两种交换机类型。如果一台路由器同时连接BRI和PRI时就需要这样。因此，从IOS版本11.3（T）之后，Cisco将此命令扩展到接口配置模式下。

interface bri *interface-number*命令用于指定本身就支持ISDN的路由器（TE1）上的一个ISDN接口。因此要将第一个ISDN接口配置成AT&T基本速率交换机类型，就需要输入例14-1中所示的命令。

例14-1 ISDN Interface BRI命令

```
RTA(config)#interface bri 0
RTA(config-if)#isdn switch-type basic-5ess
```

如果路由器本身没有BRI接口（如果是TE2设备），就必须使用外置的ISDN终端适配器。在TE2路由器上，使用interface serial *interface-number*命令。

安装ISDN服务后，服务提供商会告知交换机类型和SPID的信息。SPID用于指定每个ISDN申请者可用的服务，跟交换机的类型有关，有的交换机就必须要配置SPID。National ISDN-1和DMS-100 ISDN交换机需要配置SPID，而AT&T 5ESS交换机就不需要。在使用Adtran ISDN模拟器时必须指定SPID。Adtran ISDN模拟器是用于实验室和测试环境中模拟ISDN连接的设备，使用时不需要接入提供商建立真正的账号。

SPID的格式取决于ISDN交换机的类型和服务商的需求。在接口配置模式下使用isdn spid1和isdn spid2命令来指定路由器向本地ISDN交换机初始化一个呼叫时ISDN网络所需要的SPID。表14-5描述了这两条命令。

表14-5 isdn spid1和isdn spid2命令参数

命令参数	描述
spid-number	标识所申请的服务的数字。由ISDN服务提供商指定其值
ldn	（可选）。本地拨打目录号。若要在大多数交换机使用2条B信道，这个号码必须与来自ISDN交换机的被叫方信息一致

参数switch-type指定服务提供商的交换机类型。要将ISDN接口禁用交换，指定isdn switch-type none。例14-2显示National ISDN BRI交换机在全局配置模式下的配置。

例14-2 National ISDN BRI配置

```
Router(config)#isdn switch-type basic-ni
```

要指定SPID，在接口配置模式下使用isdn spid#命令来指定已分配给B信道的SPID号：

```
Router(config-if)#isdn spid1 spid-number [ldn]
Router(config-if)#isdn spid2 spid-number [ldn]
```

可选参数ldn指定了本地拨打目录号。对于大多数交换机，此号码必须与来自ISDN交换机的被叫方信息相匹配。SPID信息在接口配置模式下指定。

要进入接口配置模式，在全局配置模式下输入interface bri命令：

```
Router(config)#interface bri slot/port
```

slot/port参数表示端口适配器槽号/端口号。此号码是在工厂安装时或新添加到系统上时指定的。此号码可以通过show interfaces命令显示。

要为BRI 0/0的2条B信道都配置SPID，使用例14-3中的命令。

例14-3 配置BRI接口的SPID

```
Router(config)#interface bri0/0
Router(config-if)#isdn spid1 51055540000001 5554000
Router(config-if)#isdn spid2 51055540010001 5554001
```



实验活动 配置ISDN BRI

在本实验中，你将配置一台ISDN路由器使之能成功的拨通本地ISDN交换机。使用一台Adtran Atlas550 ISDN模拟器来模拟交换机 / ISDN网云。

14.9.2 配置ISDN PRI

ISND PRI通过租用T1或E1线路传输。主要的PRI配置步骤如下：

步骤1 设置ISDN交换机类型。指定路由器连接到运营商中心局PRI交换机类型。

步骤2 选择控制器。指定T1/E1控制器、成帧类型和线形编码，便于运营商实施传输。

步骤3 建立用作PRI的端口。为T1/E1实施设定PRI组的时隙并指定所使用的速率。

因为路由器通过T1/E1连接PRI，所以没有PRI接口。相应的，路由器连接租用线的物理接口一般称为T1控制器（或者，如果使用E1线路，则叫做E1控制器）。控制器配置必须和接口连接的运营商网络一致。从控制器中通过interface serial命令，对于PRI B信道和PRI D信道要分开配置。

通过使用isdn switch-type命令，指定PRI所连接的ISDN交换机的类型。和BRI一样，这条命令可以在全局或者接口模式下使用。表14-6列出了可用于ISDN PRI配置的交换机类型。

表14-6 ISDN PRI交换机类型

Switch Type	Description
primary-5ess	AT&T basic rate switches (USA)
primary-dms100	Northern Telecom DMS-100 (North America)
primary-ni	National ISDN (North America)
primary-net5	Switch type for Net5 in United Kingdom, Europe, and Australia
primary-ntt	NTT ISDN switch (Japan)

配置T1或者E1控制器需要完成如下4步：

步骤1 在全局配置模式下，指定控制器和路由器上PRI卡位于的槽位/端口。

```
Router(config)#controller {t1 | e1} {slot/port}
```

步骤2 配置成帧、线路编码和时钟，这些由服务提供商指定。framing命令用于选择PRI服务提供商使用的帧的类型。如果是T1，使用以下的命令法：

```
Router(config-controller)#framing {sf | esf}
```

如果是E1线路，使用framing命令加上如下参数：

```
Router(config-controller)#framing {crc4 | no-crc4}[australia]
```

使用linecode命令在运营商数字设备上指定物理层信令方式：

```
Router(config-controller)#linecode {ami | b8zs | hdb3}
```

在北美，使用B8ZS信令方式实施T1载波。每条ISDN信道可以达到全64kbit/s。欧洲一般使用hdb3编码方式。

步骤3 为PRI运行配置特定的接口。并在运营商数字设备上指定分配给PRI的固定时隙：

```
Router(config-controller)#pri-group [timeslots range]。
```

如果是T1，时隙使用范围是1-24；如果是E1，使用范围是1-31。

步骤4 给PRI D信道指定接口。这个接口是路由器上连接T1/E1的串行接口：

```
Router(config)#interface serial { slot/port: | unit:} {23 | 15}。
```

在E1和T1的实施中，信道编号从1开始（E1为1-31，T1为1-24），而Cisco路由器上的串行接口编号从0开始。因此，第16信道，即E1的信令信道，对应串行子接口15；第24信道，T1的信令信道，对应串行子接口23。这样，interface serial 0/0:23表示T1 PRI的D信道。

子接口（一般在帧中继中使用）用点（或句点）表示。举个例子，S0/0.16是子接口。不要混淆

使用子接口表示的T1或E1的信道。信道使用冒号（不是点）指定信道编号，区别列举如下：

- S0/0.23指子接口。
- S0/0:23指信道。

在DDR（或者用户）通过ISDN创建了端到端的路径之后，需要指定数据传送所需的数据报封装方式。ISDN可用的封装方式如下：

- PPP。
- HDLC。
- 帧中继。
- 平衡式链路接入过程（LAPB）。
- Combinet私有协议（CPP）。

LAPB也用于D信道上数据报的传输。

正如本章前面所提到的，一般喜欢采用PPP作为第2层的封装协议。

在ISDN接口上，使用encapsulation命令配置封装格式：

```
Router(config-if)#encapsulation [ppp | labp | hdlc | x25 | cpp]
```

如果配置了PPP封装，在需要同时接收多于一个拨号发起者的呼叫时，必须使用PAP或者CHAP认证。例14-4列举了具有CHAP的PPP的典型BRI封装配置。

例14-4　BRI封装的例子

```
Router(config)#interface bri 0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
```

14.9.3　验证ISDN配置

show命令用来确认ISDN的配置是否工作正常：

```
Router#show isdn status
Router#show interfaces bri0/0
Router#show isdn active
```

为了检验BRI的工作，使用show isdn status命令检查BRI接口的状态。在配置ISDN BRI之后，可以使用这条命令检查TE1（路由器）和ISDN交换机之间通信是否正常。在例14-5中，显示输出表明TE1协商成功，ISDN第3层（端到端）已准备就绪，可以开始拨出和接收呼叫。

例14-5　show isdn status命令

```
Cork#show isdn status

Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface

    dsl 0, interface ISDN Switchtype = basic-ni

    Layer 1 Status:
    ACTIVE

    Layer 2 Status:
```

```
    TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED

    TEI = 65, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED

    Spid Status:
    TEI 64, ces = 1, state = 5(init)

        spid1 configured, no LDN, spid1 sent, spid1 valid
        Endpoint ID Info: epsf = 0, usid = 70, tid = 1

    TEI 65, ces = 2, state = 5(init)

        spid2 configured, no LDN, spid2 sent, spid2 valid

        Endpoint ID Info: epsf = 0, usid = 70, tid = 2

    Layer 3 Status:
    0 Active Layer 3 Call(s)

    Activated dsl 0 CCBs = 0

    The Free Channel Mask: 0x80000003
    Total Allocated ISDN CCBs = 0
```

配置ISDN BRI需要混合使用全局和接口命令。为了配置ISDN交换机类型，进入全局配置模式，并使用isdn switch-type *switch-type*命令。如例14-6所示：

例14-6 ISDN部分配置

```
Router(config)# isdn switch-type basic-ni
!
<Output Omitted>
!
interface BRI0/0
   isdn switch-type basic-ni
   isdn spid1 51055540000001 5554000
   isdn spid2 51055540010001 5554001
```

确认显示第1层的状态是ACTIVE，第2层状态是MULTIPLE_FRAME_ESTABLISHED。这条命令也会显示活跃的呼叫数量。

show isdn active命令显示当前所有呼叫信息，包括被呼叫号码、呼叫持续的时间（直到连接撤消）、计费通知（AOC advice of charge）、呼叫中使用的计费单元，但在呼叫中或者在呼叫之后都不提供AOC信息。

show dialer显示关于拨号器接口的信息。这些信息包括：当前呼叫的状态、拨号计时的值、拨号的原因以及所连接的远程设备。

show interfaces bri0/0命令显示路由器上所配置的BRI接口的统计信息。如果在命令后面加上信道编号，会显示信道相关信息。show interfaces bri0/0:1命令显示B信道使用PPP封装，LCP已协商并开启，两种网络控制协议在运行：IP控制协议（IPCP）和CDP控制协议（CDPCP）。例14-7显

示BRI接口的输出结果：

例14-7　show interfaces bri0/0命令

```
BranchF#show interface bri0/0: 1 2
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations 0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     82 packets input, 2844 bytes, 0 no buffer
     Received 82 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     82 packets output, 2838 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     5 carrier transitions
(output omitted)
```

14.9.4　ISDN配置的故障排除

下面的命令用于调试和对ISDN配置进行故障排除：

• debug isdn q921——显示路由器和ISDN交换机之间D信道的链路状态信息（第2层）。如果show isdn status命令显示第1层和第2层不是工作状态，则使用此调试命令。

• debug isdn q931——显示ISDN网络连接（第3层）建立和撤消呼叫的交换信息。

• debug ppp authentication——显示PPP认证协议信息，包括CHAP分组交换和PAP信息交换。

• debug ppp negotiation——显示关于PPP流量的信息和PPP组件的协商交换信息，包括链路控制协议（LCP）、验证和网络控制协议。成功的PPP协商过程是：开启LCP状态、验证和协商网络控制协议。

• debug ppp error——显示协议错误以及与PPP连接协商和操作相关的错误统计信息。

14.10　DDR路由

DDR涉及一系列Cisco特性，它允许两台或更多路由器之间通过一个简单拨号网络建立动态的连

接。DDR用于通过ISDN网络或PSTN的低流量、周期性的网络连接。DDR允许在需要的基础上交换路由选择更新信息，但更多的时候都使用静态路由选择。

一般来说，如果两个站点之间每天都需要长时间的连接，那么使用专用WAN线路比较有价值。DDR则用于满足通过电路交换WAN服务提供周期性连接的需求。DDR非常灵活，能连接不同的终端节点并按需使用WAN连接，减少WAN费用。

DDR是一个过程：当流量发送时，路由器通过拨号网络建立连接；当数据传输完成时，中断连接（见图14-13）。DDR一般用于如下情形：

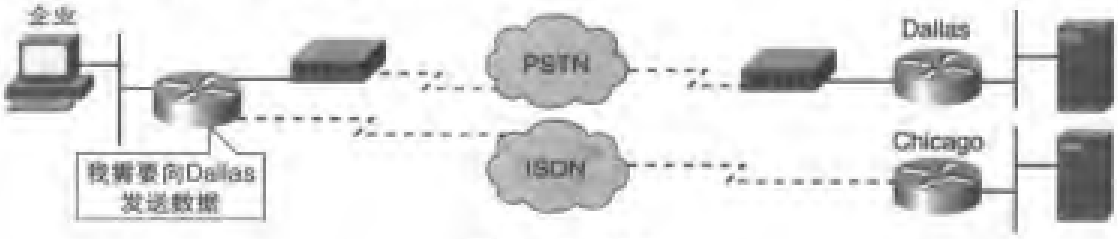


图14-13 DDR

- 远程通信者需要每天周期性地连接到公司的网络。
- 远程办公室需要发送小量的数据，比如销售处理或存货状态查询，周期性的访问中心局的主计算机。
- 客户使用自动订购系统。
- 按照预定周期性地从ISP获取电子邮件。

14.11 DDR运行方式

在配置了DDR的接口上接收到流量会触发DDR。如果流量是期望的，则初始化呼叫。可以按特定协议类型的IP流量进行定义，比如特定源和目的地址的分组，或者按其他标准。由网络管理员定义期望流量。在期望流量传送完成并且相应的空闲超时周期过去后，呼叫被中断。

有效利用DDR操作的关键在于期望流量的定义。定义期望流量有几种机制，包括拨号器和访问列表。在到达目的地的连接激活之后，即使非期望流量也会被转发。

在Cisco路由器上实施DDR包括如下步骤：

步骤1 路由器接收流量，执行路由表查询以决定到达目的地的路由，确定相应的出站接口。

步骤2 如果出站接口配置了DDR，路由器执行查询以决定流量是否是所期望的。网络管理员必须预先定义期望流量。

步骤3 路由器鉴别发起拨号所必需的拨号信息（这些通过拨号器映射来完成）以接入到下一跳路由器。

步骤4 然后，路由器检查拨号器映射是否在使用中。如果接口正连接到期望的远程目的地，流量允许转发。在连接建立之后，任何发往此目的流量都被允许；但是，只有期望流量能重置空闲计时器。如果接口当前没有连接到远程目标，路由器通过BRI的D信道发送呼叫建立信息。在链路开启之后，路由器传送期望流量和非期望流量。非期望流量可能包含数据和路由选择更新。

步骤5 没有期望流量出现时，空闲计时器开始计时进入空闲超时周期，按照所配置的空闲计时器的值中断连接。

这个过程在图14-14中显示。



图14-14　DDR工作的一般过程

14.12　传统DDR

传统DDR是指：具有基本的DDR配置，在接口上应用单个拨号器参数。如果在单独接口上需要多个拨号器配置，那么就需要使用拨号原型。

要配置传统DDR，执行如下步骤：

步骤1　定义静态路由。

步骤2　指定期望（Interesting）通信。

步骤3　配置拨号器信息。

14.13　为DDR定义静态路由

为了转发流量，路由器需要了解到达特定目的使用什么路由。如果采用动态路由选择协议，在路由选择更新信息或者hello信息被定义为期望流量的情况下，DDR接口会触发到远端的拨号。为了阻止经常或者频繁地激活DDR链路（配置了支持动态路由选择协议），可以配置必要的静态路由。

为IP配置静态路由，使用如下命令：

```
Router(config)# ip route net-prefix mask { address | interface} [ distance] [permanent]
```

图14-15中，在路由器Central上定义了一条指向路由器Home所连的LAN（10.40.0.0）的静态路由。同时，在Home上定义了两条指向Central上两个LAN子网的静态路由。如果路由器Home连接在末节网络上（非本地路由），所有的流量都应该被送往Central，所以最好在路由器Home上配置缺省路由：

```
Home(config)# ip route 0.0.0.0 0.0.0.0 10.1.0.2
```

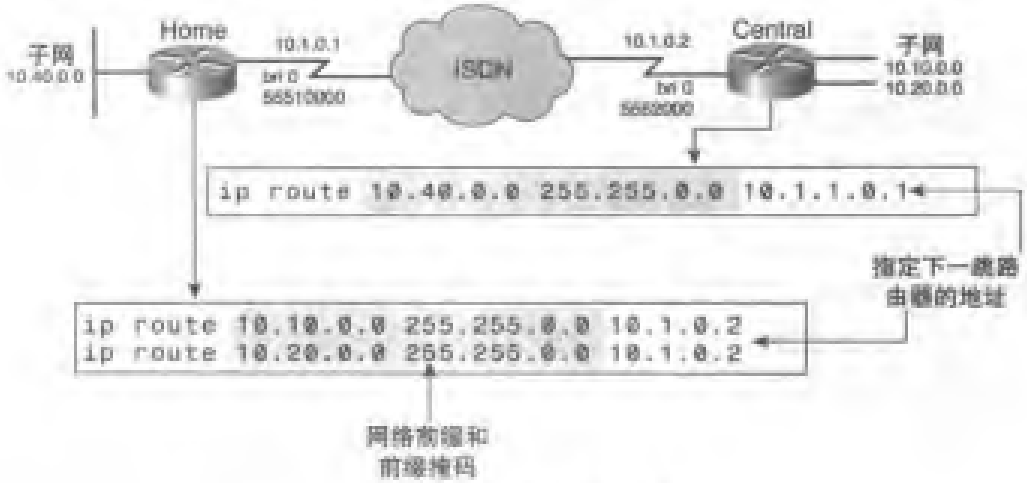


图14-15　定义静态路由

在配置静态路由时，请考虑如下因素：

- 定义的静态路由总是优于动态路由。关于同一网络，如果静态路由在路由选择表出现，所有

相应的动态路由将被忽略。

• 为了减少静态路由条目的数量，可以定义汇总或缺省静态路由。

14.14 为DDR指定期望流量

DDR呼叫由期望流量来触发。这些流量可以定义为特定协议类型的IP数据，或者按照特定的源和目的以及其他标准来定义。网络管理员定义期望流量。

使用全局命令dialer-list定义期望流量：

```
Router(config)#dialer-list dialer group-num protocol protocol-name {permit | deny |
list access-list-number}
```

在例14-8中，dialer-list 1 protocol ip permit命令允许所有IP流量触发呼叫。在例14-8中，有两个指定期望流量的例子：一个没有结合访问列表，另一个使用了访问列表。在第一个例子中（没有使用访问列表），dialer-list命令允许所有的IP流量触发呼叫。在第二个例子中（有访问列表），FTP和Telnet流量被认为是非期望流量，这些流量不能激活DDR链路。其他IP分组都可以触发DDR链路。

例14-8 dialer-list 1 protocol ip permit命令

```
dialer list 1 protocol ip permit

dialer-list 1 protocol ip list 101

access-list 101 deny tcp any any eq ftp
access-list 101 deny tcp any any eq telnet
access list 101 permit ip any any
```

14.15 配置DDR拨号器信息

配置DDR接口需要用几步来完成。在拨号器接口上配置PPP和在串行接口上配置PPP类似。PPP是运行在D信道上的链路层协议。例14-19显示了如何在DDR接口上配置PPP。

例14-9 在DDR接口上配置PPP

```
Home(config)#username Central password cisco
Home(config)#interface bri0/0
Home(config-if)#encapsulation ppp
Home(config-if)#ppp authentication chap
Home(config-if)#ip address 10.1.0.1 255.255.255.0

Home#show running-config
hostname Home
!
isdn switch-type basic-5ess
!
!
username Central password cisco
interface BRI0
```

```
  ip address 10.1.0.1 255.255.255.0
  encapsulation ppp
  dialer idle-timeout 180
  dialer map ip 10.1.0.2 name Central 5552000
  dialer-group 1
  no fair-queue
  ppp authentication chap
!
router rip
network 10.0.0.0
!
no ip classless
ip route 10.10.0.0 255.255.0.0 10.1.0.2
ip route 10.20.0.0 255.255.0.0 10.1.0.2
!
dialer-list 1 protocol ip permit
```

使用dialer-list为DDR接口指定期望数据以后，还需要和DDR接口关联起来。可以使用dialer-group group-number命令完成关联，如例14-10所示：

例14-10 dialer-group group-number命令

```
Home(config-if)#dialer-group 1

Home#show running-config
hostname Home
!
isdn switch-type basic-5ess
!
username central password cisco
interface BRI0
  ip address 10.1.0.1 255.255.255.0
  encapsulation ppp
  dialer idle-timeout 180
  dialer map ip 10.1.0.2 name Central 5552000
  dialer-group 1
  no fair-queue
  ppp authentication chap
!
router rip
network 10.0.0.0
!
no ip classless
```

```
ip route 10.10.0.0 255.255.0.0 10.1.0.2
ip route 10.20.0.0 255.255.0.0 10.1.0.2
!
!
dialer-list 1 protocol ip permit
```

在这条命令中，*group-number*指定接口所属的拨号器组编号。组编号的范围是从1到10的整数。这个编号必须和dialer-list *group-number*命令指定的编号一致。每个接口只能属于一个拨号器组。但同一个拨号器列表可以应用到多个接口（通过使用dialer-group命令）。

同时，必须为远程DDR接口指定正确的拨号信息。可以通过dialer map命令完成，如图14-16所示：

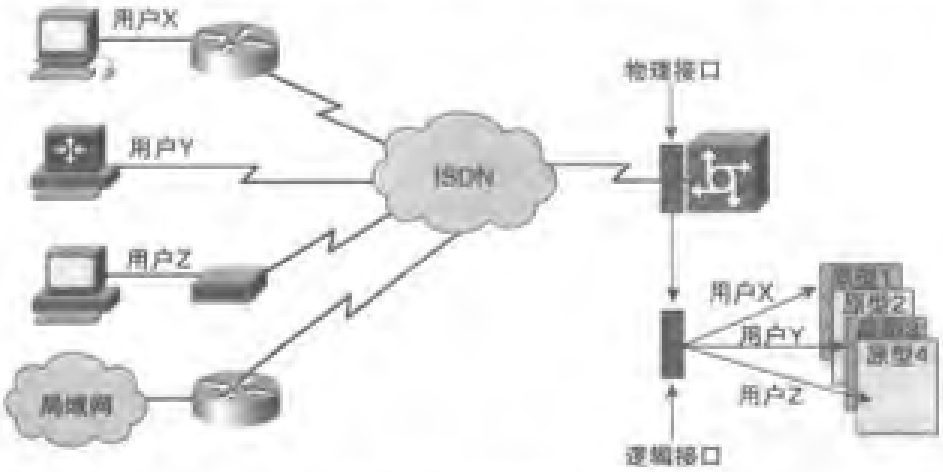


图14-16 拨号器映射

dialer map命令把远程协议地址映射到电话号码。这条命令在需要拨多站点的场合是必需的。

```
Router(config-if)#dialer map protocol next-hop-address [name hostname] [speed 56 | 64]
[broadcast] dial-string
```

如果只需要拨单个站点，可以使用无条件的拨号字符串命令，这使得不管流量发往何处都拨同一个号码；对于传统的DDR来说是必须且惟一的步骤。在采用拨号原型而不用传统DDR的情况下，虽然必须配置这些信息，但配置目的信息的步骤是不同的。

利用dialer idle-timeout *seconds*命令指定在中断连接之前等待的空闲时间（秒数）。秒数代表的是自从最后一个期望分组通过之后经过的时间。缺省值为120秒。

实验活动 配置传统DDR

在本实验中，你将配置一台ISDN路由器，利用传统DDR呼叫另一台ISDN路由器。一台Adtran Atlas550 ISDN模拟器用来模拟交换/ISDN云。这里，只有HTTP能初始建立呼叫。

14.16 拨号器原型（Dialer Profiles）

因为配置直接应用在接口上，使得传统DDR具有很多局限性。这就意味着在链路两端的DDR接口之间形成了一对一的对应关系。如果IP地址直接应用在接口上，那么只有配置在相应IP子网的DDR接口才能与之建立DDR连接。

拨号器原型把配置从接收和发送呼叫的接口移除，以每次呼叫为基础把配置绑定到接口上。这使得物理接口可以根据入站或者出站的呼叫请求，动态的采用不同的特性建立连接。拨号器原型可

以定义封装、访问控制列表、定制最小和最大呼叫数以及特性的开启或关闭。

拨号器原型设计和实施的目标是应用在复杂和可扩展的电路交换互连网络中，这些通过在Cisco路由器和接入服务器上实施新的DDR模型来完成。拨号器原型把逻辑部分从放置或接收呼叫的物理接口分离开来，包括网络层、封装和拨号参数。

使用拨号器原型，可以完成如下任务：

- 在ISDN接口的B信道上配置不同的IP子网。
- 在ISDN接口的B信道上配置不同的封装。
- 为ISDN接口的B信道配置不同的DDR参数。
- ISDN BRI接口属于多个拨号器池，减少了ISDN B信道的浪费。

拨号原型包含如下组成元素：

- **拨号接口**（*Dialer interface*）——使用按目的拨号原型的逻辑实体。
- **拨号器池**（*Dialer pool*）——每个拨号器接口对应一个拨号器池，这样把一组单个或多个物理接口和拨号器原型关联起来。
- **物理接口**（*Physical interface*）——拨号器池中的接口，该拨号器池配置了封装参数并且标识了拨号器池下属的接口。在物理接口上需要配置封装类型、PPP验证和多链路PPP。

“期望分组（interesting packet）”被路由到远程DDR IP地址。路由器检查配置的拨号接口，查找和远程DDR IP地址属于同一子网的接口。如果存在，路由器在拨号器池中查找未用的物理DDR接口。然后，拨号器原型的配置将会应用到此接口上，开始尝试创建DDR连接。当连接中断以后，这个接口回到拨号器池中，等待下次呼叫。

14.17　配置拨号器原型

在路由器上可以配置多个拨号器接口。每个拨号器接口都有到达目的地的完全配置。全局命令interface dialer创建拨号器接口并进入接口配置模式。

为了配置拨号器接口，执行如下任务：

步骤1　利用所有的基本DDR命令配置一个或多个拨号器接口，比如，IP地址、封装类型、认证、空闲计数器以及期望流量的dialer-group。

步骤2　配置拨号字符串、对应远程路由器名称的拨号remote-name以及要拨的电话号码。拨号器池把池中的物理接口和逻辑接口关联起来。

步骤3　配置物理接口并利用dialer pool-member命令分配给拨号器池。使用这条命令指定多个拨号器池编号，可以将接口分配给多个拨号器池。如果有多个物理接口存在于拨号器池中，使用dialer pool-member命令的优先级选项指定物理接口在池中的优先级。优先级只在拨出时有用。

在拨号器池中，可以使用同步、串行、BRI或PRI接口的组合。

14.18　验证DDR配置

Show dialer interface命令可以显示入站和出站呼叫的统计信息，和传统DDR的显示格式相同。

“Dialer state is data link layer up”信息表明拨号器正常工作，“interface bound to profile Dialer0”信息指示bri0接口绑定到拨号原型Dialer0。例14-11显示了这些信息。

例14-11　show dialer interface命令

```
Router# show dialer interface bri 0
BRI0 - dialer type = ISDN
```

```
Dial String Successes Failures Last called Last status
0 incoming call(s) have been screened.
BRI0: B-Channel 1
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ip (s=10.1.1.8, d=10.1.1.1)
Interface bound to profile Dialer0
Time until disconnect 102 secs
Current call connected 00:00:19
Connected to 5773872 (wolfman)
BRI0: B-Channel 2
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

show isdn active命令显示当前活动的ISDN呼叫信息。（例14-12显示了输出结果）在输出结果中，可以看到ISDN呼叫是连接远程名为Seattle的路由器的出站呼叫。

例14-12 show isdn active命令

```
Phoenix#show isdn active
------------------------------------------------------------------------------
                                ISDN ACTIVE CALLS
------------------------------------------------------------------------------
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
------------------------------------------------------------------------------
Call  Calling  Called Remote       Seconds Seconds Seconds Charges
Type  Number   Number  Name         Used    Left    Idle    Units/Currency
------------------------------------------------------------------------------
Out            5551000  Seattle    87      41      78      0
------------------------------------------------------------------------------
```

show isdn status命令显示BRI接口3层的信息。在显示输出中，ISND第1层是激活的，在第2层建立了具有SPID1和SPID2的连接，在第3层有活动的连接。

可以利用debug命令帮助解决DDR配置的问题。



实验活动 配置拨号器原型

在这个实验中，需要在路由器上配置拨号器原型。这使得可以在两台远程路由器上同时发起到中心ISDN BRI路由器的DDR呼叫。利用Adtran Atlas550 ISDN模拟器来模拟交换/ISDN云。

14.19 总结

在本章中，你学习了以下内容：

- ISDN通过公众交换网络提供集成语音/数据的传输。
- ISDN组件包括终端、TA、NT设备和ISDN交换机。
- ISDN参考点（R、S、R和U）定义功能组之间的逻辑接口，比如TA和NT1。
- 一个ITU-T协议组负责定义ISDN，跨越OSI参考模型的物理层、数据链路层和网络层。
- 常用的ISDN封装是PPP和HDLC。
- ISDN有多种用途，包括远程访问、远程节点和SOHO连接。
- 有两种ISDN服务：BRI和PRI。
- ISDN BRI把144kbit/s的带宽分成3个分离的信道，可用的带宽为128 kbit/s。
- BRI的配置包括BRI接口、ISDN交换机类型和ISDN SPID。
- DDR按需建立和释放电路交换连接。

作为本章所学习内容的补充，请参阅本书所附光盘中关于本章的视频、插图和e-Lab实验。

14.20 关键术语

2B + D

2条B信道和1条D信道。参考ISDN BRI服务。

基本速率接口（*Basic Rate Interface, BRI*） ISDN接口，由2条B信道和1条D信道组成，用于语音、视频和数据的电路交换通信。

客户端设备（*Customer Premises Equipment, CPE*） 电话公司提供的终端设备，比如终端、电话、调制解调器，它安装在用户所在地，并和电话公司的网络相连。

综合业务数字网（*Integrated Services Digital Network, ISDN*） 由电话公司提供的通信协议，它允许电话网络传送数据、语音和其他来源的业务流量。

平衡式链路接入过程（*Link Access Procedure, Balanced, LAPB*） 它是X.25协议栈中的数据链路层协议。LAPB不同于HDLC协议，它是一个面向比特的协议。

D信道链路接入过程（*Link Access Procedure on the D channel, LAPD*） 用于D信道上的数据链路层协议。LAPD不同于LAPB，它主要用来满足ISDN基本接入的信号需求。在ITU-T Q.920建议和Q.921建议中有定义。

网络终端类型1（*Network Termination type 1, NT1*） 一种用来连接4线ISDN用户和传统的2线本地环路的设备。

网络终端类型2（*Network Termination type 1, NT2*） 在不同的用户设备和NT1间传输流量的设备。它是一种负责交换和集中的智能设备。

基群速率接口（*Primary Rate Exchange, PRI*） ISDN的基群速率访问接口。基群速率访问包含一条64kbit/s的D信道和23条（T1）或30条（E1）语音或数据的B信道。

Q.931 推荐在终端与本地ISDN交换机间使用的网络层协议。该协议并不采用端到端的建议。不同的ISDN供应商和交换机类型可使用Q.931的不同实现。

参考点（*reference point*） 参考点是用于定义ISDN不同接口特性的规范。这些规范在ITU建议I.411（V、U、T、S、R参考点）中定义（物理特性和电气特性）。

服务配置文件标识（*Service Profile Identifier, SPID*） 服务提供商使用的数字，用来定义ISDN设备预定的服务。当访问交换机时，ISDN设备使用SPID初始化与服务提供商的连接。

终端适配器（*Terminal Adapter, TA*） 一种用来连接ISDN基本速率接口到一个现有接口的设备，如EIA / TIA-232。实际上，TA就是一台ISDN调制解调器。

终端设备类型1（*Terminal Equipment 1, TE1*） 一种与ISDN网络兼容的设备。TE1连接网络终端类型1（NT1）或网络终端类型2（NT2）。

终端设备类型2（*Terminal Equipment 2, TE2*） 一种与ISDN网络不兼容的设备，需要使用终端适配器才能与ISDN网络相连。

14.21　复习题

1. ISDN中使用哪条信道进行数据传输？
   A. 16kbit/s的B信道
   B. 16kbit/s的D信道
   C. 64kbit/s的B信道
   D. 64kbit/s的D信道
2. 哪条信道用于ISDN带外信令？
   A. 数据
   B. B信道
   C. 本地环路
   D. D信道
3. 首先动态分配的TEI值是多少？
   A. 64
   B. 127
   C. 0
   D. 1
4. 在两台交换机之间使用以下哪种机制来传递呼叫控制信息？
   A. D信道
   B. SS7
   C. B信道
   D. Q.921
5. 在处理ISDN呼叫的过程中，D信道的主要功能是什么？
   A. 传送数据通信
   B. 传送语音通信
   C. 传送视频通信
   D. 传送呼叫信令
6. 在北美使用ISDN BRI将一台路由器用作拨入服务器，需要用到哪个ISDN接口？
   A. ISDN PRI E1
   B. ISDN BRI U
   C. ISDN PRI T1
   D. ISDN BRI S/T
7. 如果路由器有一个U接口，这意味着什么？
   A. 它有内置的TA
   B. 它有内置的TE1
   C. 它有内置的NT1
   D. 它有内置的BRI
8. 下列哪种交换机类型用于欧洲BRI连接？
   A. Net3
   B. Net5
   C. Northern Telecom公司的DMS-100
   D. VN3
9. 由以下谁来提供SPID？

A. 路由器厂商
B. ISDN交换机
C. ISDN服务提供商
D. 网络管理员

10. DDR用于什么？
A. 帧中继网络中低容量、周期性的网络连接
B. ISDN中低容量、周期性的网络连接
C. ISDN中低容量、永久性的
D. ISDN中高容量的连接

11. 下列有关DDR的叙述中错误的是哪些（选4个）？
A. DDR将路由器连接到一个拨号网络
B. DDR在两个站点之间创建永久连接
C. DDR允许路由器只连接一个端点
D. 如果使用频率低，DDR可减少广域网的成本
E. 如果希望有一台永久的WWW服务器，配置DDR是正确的选择
F. DDR仅应用于ISDN

12. 使用传统DDR的主要局限性是什么？
A. 不支持PPP认证
B. 必须使用拨号器映射（dialer map）
C. 将配置直接应用到物理接口
D. 传统DDR受到IP应用的限制



第15章 帧中继

目标

学习完本章后，你将能够：

- 描述帧中继的服务、标准以及组件。
- 理解本地管理接口（LMI）的特性。
- 描述帧中继子接口的用途。
- 配置基本的帧中继。

我们已经学习了点到点协议（PPP）和综合业务数字网络（ISDN）两种类型的广域网技术。这两种技术可以用来解决地理上相距很远的地点间的连接问题。在本章中，将学习另一种广域网技术——帧中继，帧中继技术也可以为用户提供地理上相距很远的地点间的连接方案。

在本章中，将学习到帧中继的服务、标准、组成和操作。另外，本章也描述了帧中继服务的配置工作以及监控和维护帧中继连接的相关命令。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图。光盘上的素材与本章内容的补充，能强化本章所介绍的概念。

15.1 帧中继概述

帧中继是国际电信联盟—电信标准部门（ITU-T，它的前身是CCITT，国际电报电话咨询委员会）和美国国家标准协会（ANSI）制定的标准，定义了在公共数据网络（PDN）上发送数据的流程。帧中继属于高性能、高效率的数据链路技术，在世界范围内的网络中广泛使用。帧中继通过将数据划分成分组，在广域网上传送信息。每个分组到达目的地要途经多台帧中继网络中的交换机。帧中继工作在OSI参考模型的物理层和数据链路层，但依赖于诸如TCP等上层协议来进行纠错控制。

帧中继最初是作为一种在综合业务数字网（ISDN）接口上使用的协议来设计的。如今，帧中继已经成为一种交换式数据链路层协议的工业标准，它使用高级数据链路控制协议（HDLC）封装，在互连设备之间管理虚电路（VC）。帧中继使用虚电路，通过面向连接的服务方式建立连接。

提供帧中继接口的网络可以是电信运营商提供的公用通信网络，或是服务于企业的专有企业网络。帧中继网络在用户端设备（例如路由器、网桥、主机）和载波网络设备（例如帧中继交换节点）之间提供分组交换的数据通信功能。正如以前学到的，用户设备通常指数据终端设备（DTE），而与

DTE设备接口相连的网络设备通常指数据电路终端设备（DCE），如图15-1所示。

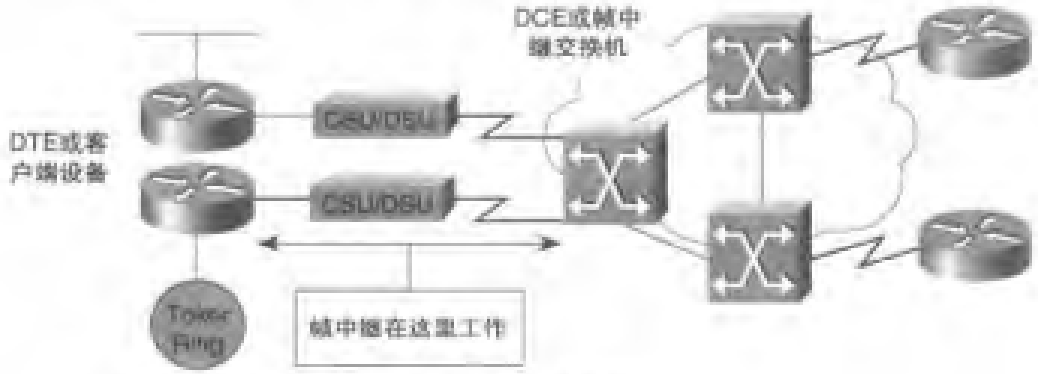


图15-1　用户设备

15.1.1　帧中继术语

帧中继网络中两台DTE设备之间的连接称为逻辑连接或虚电路（VC）。通过向网络发送信令消息动态地建立虚电路。这种情况，称为交换虚电路（SVC），但这并不常用。一般地，永久虚电路（PVC）由所使用的运营者预先配置。虚电路的交换信息存储于交换机的内存中。

因为帧中继是设计运行在高质量的数字线路上的，所以它不提供差错恢复机制。在以太网这种局域网技术中，如果数据帧中有错误，会丢弃该帧，而不会发送通知。

一台有帧中继接口的设备，也称为帧中继组合/拆分设备（assembler / diassembler）或一台连接帧中继网络的路由器，可以有多条虚电路连接不同的端点。它成为一种很划算的租用线的替代品，因为每个端点仅需一条较短的租用线和接口。此外，帧中继可以节省成本，因为租用线的容量是基于虚电路所需带宽的平均值，而不是最大带宽。

因为每条虚电路都有一个数据链路连接标识符（DLCI, data-link assembler identifier），所以可以在一条单一的物理接入线路上区分不同的虚电路。DLCI存储于每个所传输的数据帧的地址字段中。DLCI仅具有本地意义，虚电路每一端的DLCI值可能不同。

下面是本章讨论帧中继过程中所用到的一些术语（参见图15-2）：

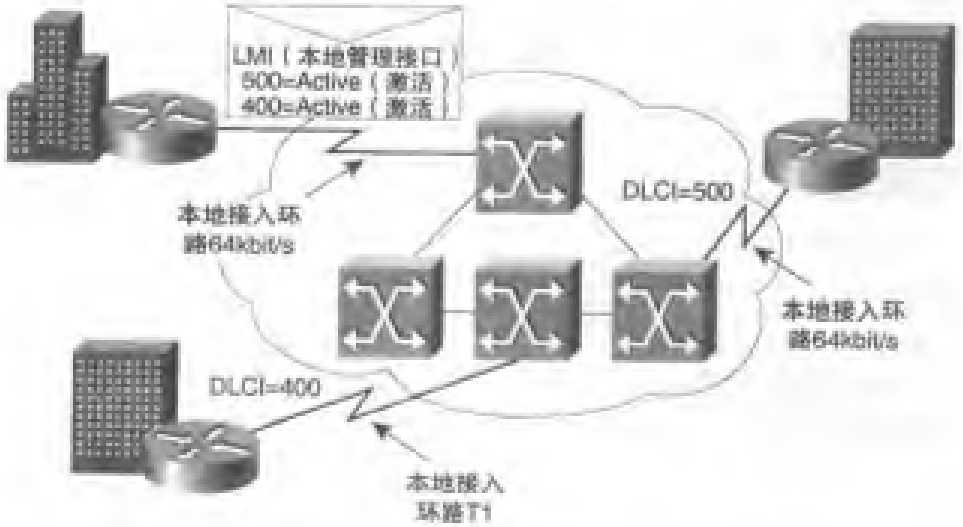


图15-2　DLCI值

- **本地访问速率**（*Local Access Rate*）——连接到帧中继网云（本地环路）的时钟速率（端口速率）。该速率是数据流入网络或流出网络的速率。

• **数据链路连接标识符**（*Data Link Connection Identifier，DLCI*）——它是源设备和目的设备之间标识逻辑电路的一个数值。帧中继交换机通过在一对路由器之间映射DLCI来创建永久虚电路。

• **本地管理接口**（*Local Management Interface，LMI*）——它是用户端设备（CPE）和帧中继交换机之间的信令标准，负责管理设备之间的连接，维护设备之间的连接状态。LMI包括对维持机制的支持，维持机制验证数据是否正在传输。LMI还包括对多播机制的支持，多播机制向网络服务器提供本地DLCI。LMI还支持多播寻址，多播寻址可以使用几个DLCI作为多播（多个目的地）地址，并可以给予DLCI在帧中继网络中的全局意义而不是局部意义（DLCI仅在本地交换中使用）。LMI也包括对状态机制的支持，状态机制向交换机报告已知DLCI的现行状态。共有几种类型的本地管理接口，路由器需要被告知正在使用的本地管理接口类型。Cisco支持的3种LMI类型为：cisco、ansi、q933a。

• **承诺信息速率**（*Committed Information Rate，CIR*）——承诺信息速率是服务提供商承诺要提供的有保证的速率，以bit/s为单位。

• **承诺突发**（*Committed Burst，Bc*）——在承诺速率的测量间隔内，交换机准许接收和发送的最大数据量，以bit/s为单位。

• **超量突发**（*Excess Burst，Be*）——在承诺信息速率之外，帧中继交换机试图发送的未承诺的最大额外数据量，以bit/s为单位。超量突发依赖于厂商可以提供的服务，但是一般来说它要受到本地接入环路端口速率的限制。一般来说，发送超量突发数据（Be）的概率要小于承诺突发数据（Bc）。网络把超量突发数据（Be）看作可丢弃的数据。

• **前向显式拥塞通知**（*Forward Explicit Congestion Notification，FECN*）——当一台帧中继交换机意识到网络上发生拥塞的时候，会向目的设备发送FECN分组，告知网络上发生了拥塞。

• **后向显式拥塞通知**（*Backward Explicit Congestion Notification，BECN*）——如图15-3所示，当一台帧中继交换机意识到网路上发生拥塞的时候，会向源路由器发送BECN分组，指示路由器降低分组的发送速率。如果路由器在当前的时间间隔内接收到任何BECN，它会按照25%的比例降低分组的发送速率。

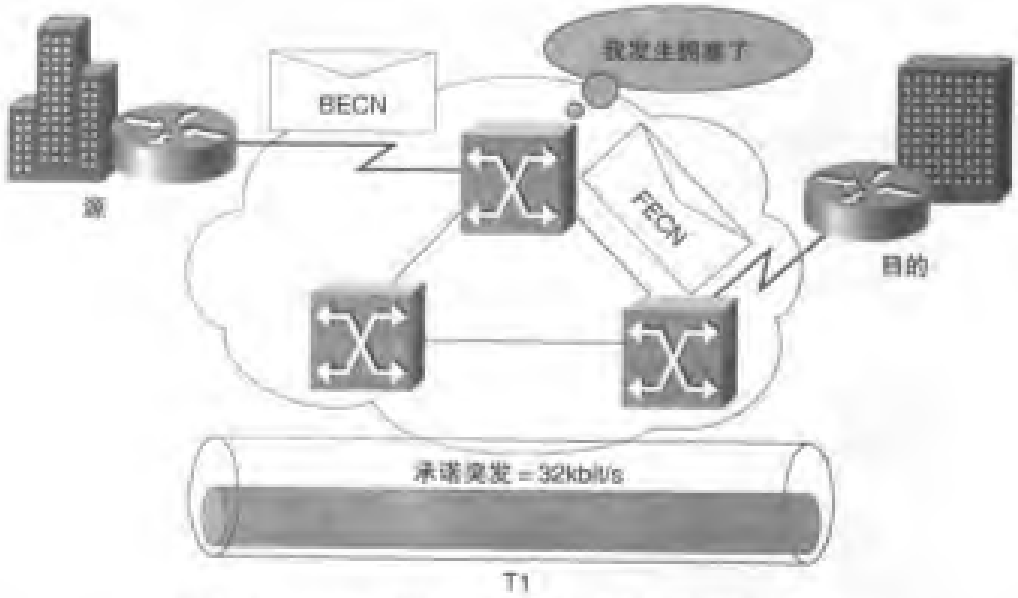


图15-3 帧中继交换机发送后向显式拥塞通知（BECN）

• **允许丢弃**（*Discard Eligibility，DE*）——当路由器检测到网络拥塞时，帧中继交换机将首先丢弃那些DE位设置为“1”的分组。DE位设置在那些超量的通信流量上（也就是那些在CIR之后所接收到的通信流量）。

15.1.2　帧中继运行方式

帧中继可以用作一种接口，连接电信运营商的公用通信网络，或者是专有企业网络。只要在电信运营商的中心局（Central Office，CO）安装帧中继交换设备，就可以进行公用帧中继服务。这样，用户可以按照网络的使用情况交费，从而得到经济实惠的好处。此外，还不用花时间和经历来管理和维护帧中继网络的设备和服务。

在现有的帧中继网络中，还没有专门为帧中继互连设备制定的标准。因此，支持帧中继的接口不是必须指定在网云中的网络设备之间使用帧中继协议。于是，像传统的电路交换、分组交换或者这两种技术的混合交换都可以使用，如图15-4所示。

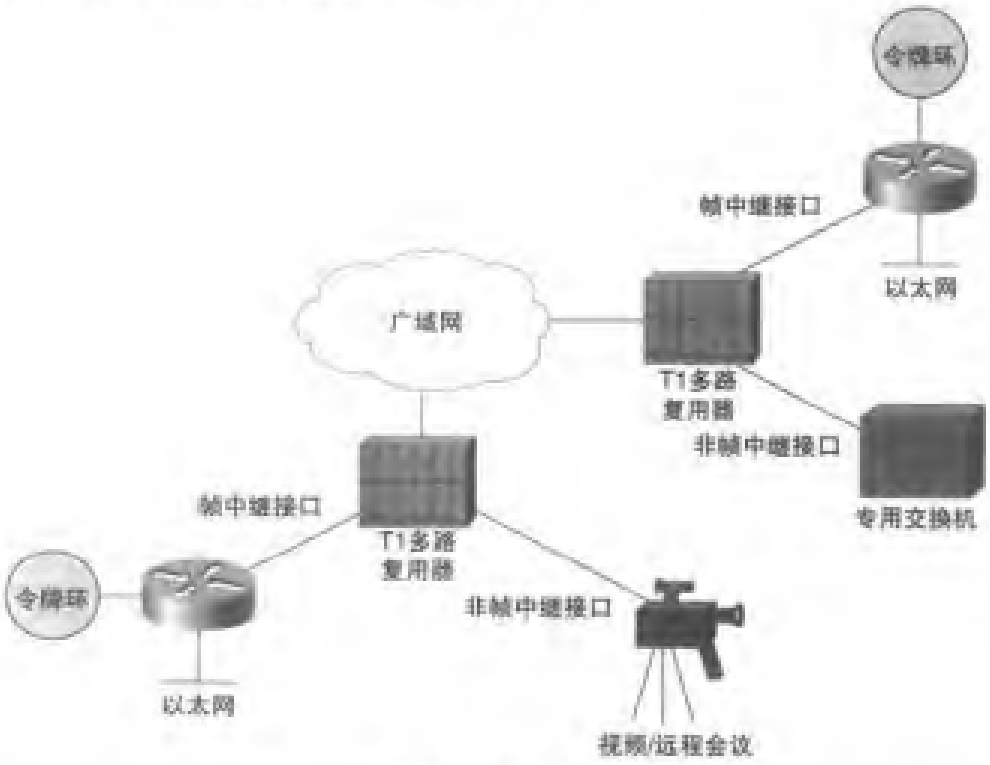


图15-4　互连设备

连接用户设备和网络设备的线路，可以在一个很广的范围之内选择数据传输速率。一般来说，帧中继支持的数据传输速率在56kbit/s到2Mbit/s之间，当然，帧中继还可以支持比这更低或更高的传输速率。

帧中继作为用户和网络设备之间的接口，如图15-5所示，它提供一种多路复用的方法，通过为

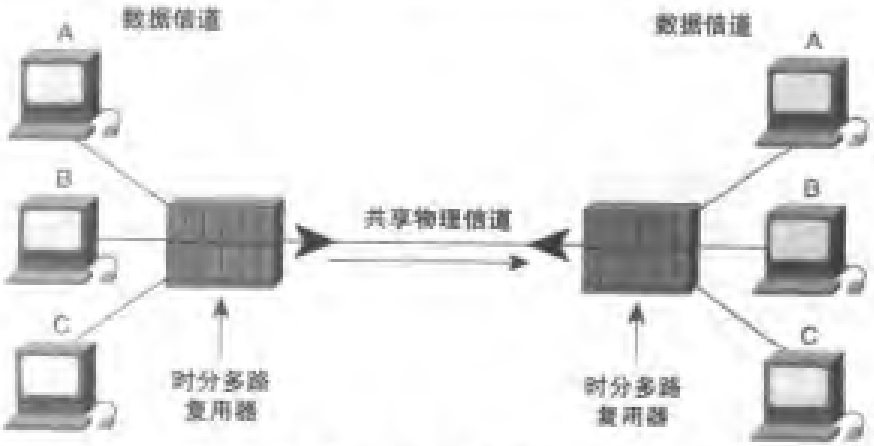


图15-5　单一的物理连接

每对数据终端设备（DTE）分配不同的DLCI，利用共享物理介质来建立多个逻辑数据会话过程（称为虚电路）来实现。

帧中继的多路复用提供了更多的灵活性，可以更加有效地利用现有的带宽。因此，帧中继允许用户以更低的成本共享网络带宽。例如，一个采用帧中继的广域网，等同于多条路径。电话公司通常拥有和维护这些路径。用户可以花较多的钱为公司租一条专用的路径，也可以花较少的钱和他人共享一条路径。当然，也可以在一个专有网络中采用帧中继。但我们很少采用这种方式。

帧中继的标准可以为帧中继网络中可配置和管理的永久虚电路（PVC）进行编址。帧中继永久虚电路由数据链路连接标识符（DLCI）来标识，如图15-6所示。帧中继的DLCI具有本地意义；也就是说，DLCI的值在整个帧中继广域网上并不是惟一的。由虚电路连接的两台数据终端设备可能使用不同的DLCI值来指定同一个连接。

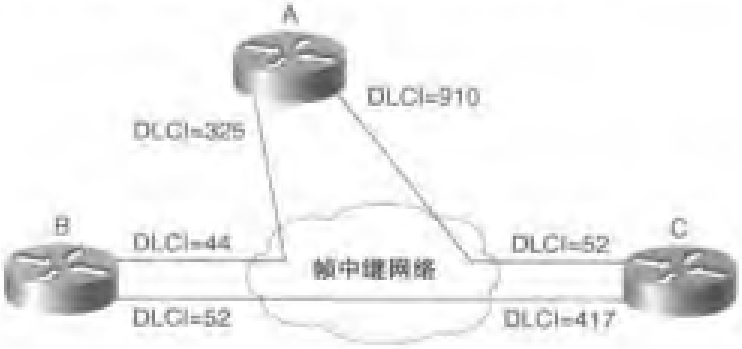


图15-6 终端设备

当帧中继为多个逻辑数据会话提供多路复用时，服务供应商的交换设备首先要建立一个表，该表用来将不同的DLCI值映射到出站端口。其次，当接收到一个数据帧时，交换设备分析其连接标识符并将该数据帧发送到相应的出站端口。最后，在第一个数据帧发送之前，将建立一条通往目的地的完全路径。

图15-7显示了帧中继的帧格式。标志字段指示了帧的开始和结束，其后的2个字节为地址信息，2Bytes中的10bits组成了实际的电路ID（也就是DLCI）。

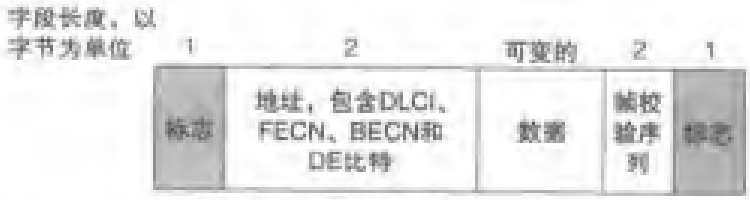


图15-7 标志字段

以下是帧中继帧格式的各字段：

- **标志**（*Flag*）——指示帧中继数据帧的开始和结束。
- **地址**（*Address*）——指示地址字段的长度。尽管帧中继的地址实际上有2Bytes，但也包括了为将来地址长度扩充而预留的地址比特。地址字段中每个字节的第8比特被用来指示地址。地址字段包括以下信息：
  - —— DLCI值（*DLCI value*）：指示DLCI的值，包含地址字段的前10比特。
  - —— 拥塞控制（*Congestion Control*）：地址字段的最后3比特，用来实现帧中继的拥塞通知机制，包括前向显式拥塞通知（FECN）、后向显式拥塞通知（BECN）以及允许丢弃位（DE）。
- **数据**（*Data*）——是一个可变长度的字段，包含封装的上层协议数据。
- **帧校验序列**（*FCS*）——（Frame Check Sequence）用来保证传输数据的完整性。

举例来说，如图15-8所示，假设有两条永久虚电路（PVC），一条连接Atlanta和Los Angles，另一条连接San Jose和Pittsburgh。Los Angles使用DLCI 22来标识它到Atlanta的PVC，而Atlanta使用DLCI 82来标识同一条PVC。类似地，San Jose使用DLCI 12来标识它到Pittsburgh

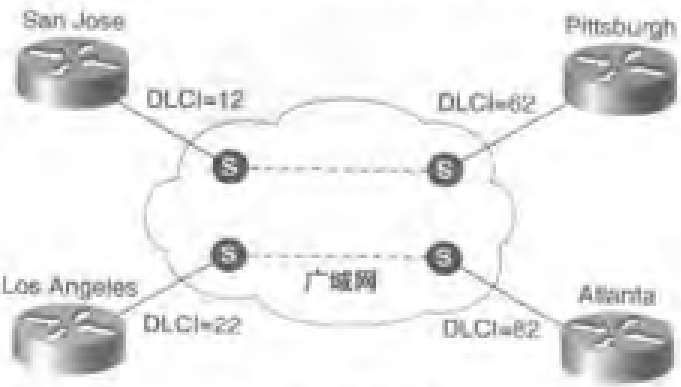


图15-8 使用DLCI

的PVC，而Pittsburgh使用DLCI 62来标识同一条PVC。网络使用内部机制来区分这两个具有本地意义的PVC标识符。Los Angles和San Jose使用不同的DLCI值，所以不需要使用内部机制来区分这两个标识符。

帧中继地址空间局限在10bits，可以创建1,024个DLCI地址。根据本地管理接口（LMI）类型来确定这些地址的可用部分。Cisco本地管理接口类型使用从16~1007的DLCI取值范围来携带用户数据。厂商保留使用余下DLCI地址，包括LMI消息和多播地址。

接口描述块（IDB interface descriptor blocks）的数量，是由用户使用的Cisco IOS版本支持的，它限制了每个系统接口和子接口的总数。一个接口描述块是内存的一部分，存储包含接口的信息，诸如计数器、接口状态等。IOS为每个接口维护一个IDB，并为每个子接口也维护一个IDB。高速接口比低速接口需要更多的内存。每个平台IDB的最大数量不同，随着Cisco IOS版本的不同而变化。

15.1.3　帧中继本地管理接口（LMI）

在帧中继历史上，1990年曾有过一次重大的发展。当时，Cisco公司、StrataCom公司、Northern Telecom公司、DEC公司成立了一个小组，一方面致力于帧中继技术的开发，另一方面加速互操作的帧中继产品的推广。该小组不仅为基本帧中继协议开发了配套的规范，而且还扩展了帧中继的一些特性，以便在复杂的互连网络环境中提供额外的功能。这里的帧中继扩展就是指本地管理接口（LMI）。

15.1.4　LMI的运行方式

LMI过程的主要目标是：

- 确定路由器所知的多条PVC的操作状态。
- 发送维持分组，以确保PVC处于激活状态，不会因休止状态而失效。如图15-9所示。

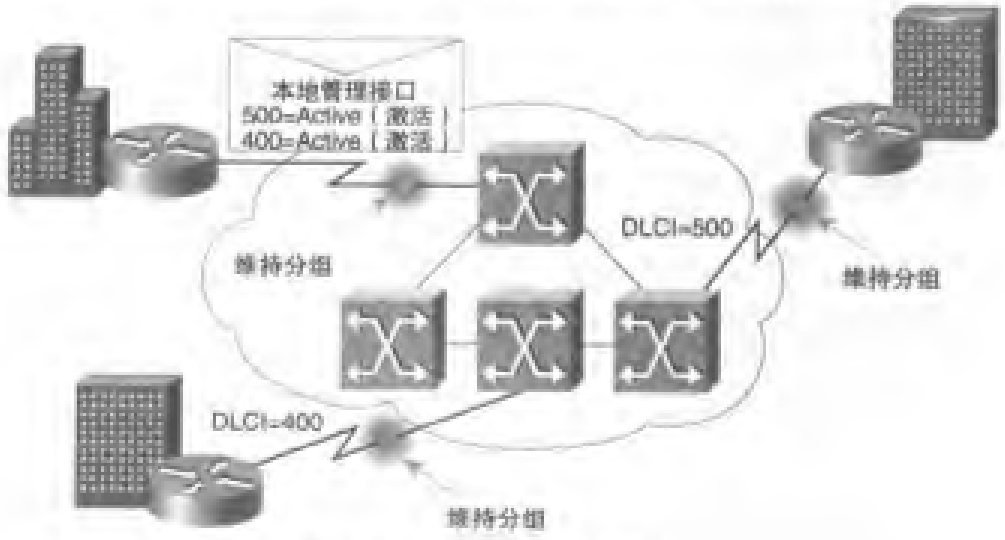


图15-9　本地管理接口（LMI）

- 通知路由器哪些PVC是可以使用的。
- 通过路由器上的命令可以调用3种LMI类型：ansi、cisco、q933a。

帧中继规范还包括LMI过程。LMI消息用特定的LMI数据链路标识符（DLCI）（在合作规范中指定，DLCI＝1,023）标识的帧发送。LMI帧格式如图15-10所示。

在标志字段和LMI DLCI字段之后，LMI帧包含4个必须的字节。第1字节是非数字信息（Unnumbered Information，UI）指示符，与平衡式链路接入过程（LAPB）中非数字信息帧指示符具

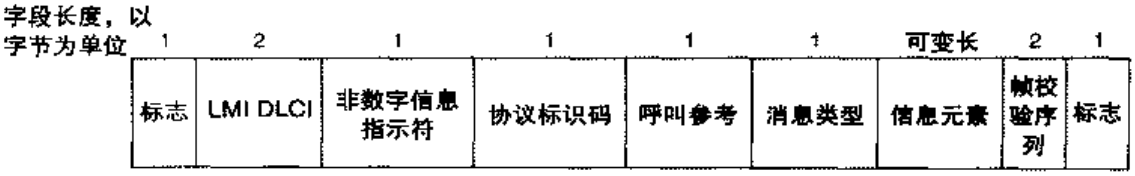


图15-10 LMI帧

有相同的格式，其中的轮询／结束（poll／final，P／F）位都设为0。接下来的1字节是协议识别码，设置为一个标识该帧是LMI帧的值。第3个必须的字节是呼叫参考，总是全置为0，目前还未使用。

最后1个必须的字节是消息类型字段。帧中继中定义了两种消息类型字段：状态查询消息和状态消息。状态消息是对状态查询消息的响应。维持消息（keepalive，在连接上发送消息以保证连接的两端继续认为该连接有效）和PVC状态消息是两个典型的例子，它们都有普通LMI的特性，符合帧中继规范。

状态消息和状态查询消息一起作用，以验证逻辑链路和物理链路的完整性。这些信息在路由选择环境中是很关键的，因为路由选择协议需要根据链路完整性及其他因素来决定选择哪一条路由。

下一个字段是信息元（Information Element，IE）字段，是可变长度的字段（以字节为单位）。消息类型字段后面可以接多个信息元，每个信息元由1字节的IE标识符、1个IE长度字段以及1字节或多个字节的实际数据组成。

15.1.5 LMI的扩展

除了为传输数据定义基本帧中继协议功能之外，帧中继规范还包括LMI扩展。它使得对大规模的复杂互连网络的支持变得更容易。一些LMI扩展被认为是基本的，即任何采用帧中继规范的人都应该实施这些扩展。另外一些LMI功能则是可选的。LMI扩展的概要如下：

- **虚电路状态消息**（*基本的*）——在用户设备和网络之间提供通信和同步功能。周期性报告新的PVC的加入以及已经存在的PVC是否删除之类的相关信息，还概括性地提供有关PVC完整性的信息。虚电路状态消息防止数据被发送到已经不存在的PVC上。
- **组播**（*可选项*）——允许发送端发送单个的帧，并可以通过网络把该帧传输到多个接收端。因此，组播提供了路由选择协议消息和地址解析协议的高效传输，通常这些协议必须能够被同时发送到多个目的地。
- **全局寻址**（*可选项*）——使得连接标识符具有全局性，而不仅局限于本地意义。从而允许它们用来标识帧中继网络中的一个特定接口。全局寻址使得一个帧中继网络因为有地址可寻而类似于一个本地局域网；地址解析协议ARP也因此能够像局域网上那样在帧中继网络中运行。
- **简单流量控制**（*可选项*）——提供XON／XOFF的流量控制机制，该机制可应用到整个帧中继接口。这意味着那些高层不能使用拥塞通知比特的设备也可以实现一定级别的流量控制。

15.2 全局寻址

除了基本的LMI特性之外，几个可选的LMI扩展特性在网络互连环境下也尤为重要。其中最重要的一个可选LMI扩展特性就是全局寻址（global addressing）。有了这个扩展特性，一个帧中继帧的DLCI字段的值代表了每台终端用户设备（如路由器等）的全局有效地址。具体实现参见图15-8。

正如以前提到的，基本（非扩展的）帧中继规范所支持的用来标识PVC的DLCI仅在本地有效。在这种情况下，地址不能用来标识网络接口以及跟接口相连的节点。因为这些地址并不存在，它们不能被传统的地址解析和发现技术所发现。这意味着，使用基本帧中继寻址，必须要创建一个静态的映射来告知路由器使用哪个DLCI可找到一台远程设备以及和它相关联的互连网络地址。

在图15-8中，每个接口都有各自的标识符。假设Pittsburgh需要发送一个数据帧到San Jose。因为到San Jose的DLCI标识符是22，所以Pittsburgh就把DLCI字段设为22，并把该帧发送到帧中继网络。在出口端，网络将DLCI字段所包含的值改为62，以便标识该帧的源节点。每台路由器的接口都要用一个惟一的值来作为它的节点标识符，每台单独的设备因而能够相互区分。这使得复杂环境下的路由选择成为可能。全局寻址为大规模的复杂网络带来了明显的便利，带有全局寻址的帧中继网络对于它周边的路由器来说，就像任何一个局域网一样。

15.2.1　组播

组播是另一个有价值的可选LMI特性。为多播组特意分配了4个保留的DLCI值（1019-1022）。采用这4个保留DLCI值标识的数据帧，网络将对其进行复制，以把它们发送到指定集合中的每个所在地。组播扩展还定义了LMI消息，用来通知用户设备有关添加、删除的情况以及多播组的当前状况。在那些使用动态路由选择的网络中，路由选择信息必须在多台路由器之间进行交换。对于这种情况，可以通过使用带有组播DLCI的数据帧来提高发送效率。这样，组播允许把消息发送到一组指定的路由器。

15.2.2　反向ARP

反向ARP（Inverse ARP）机制允许路由器自动建立帧中继映射，该映射将DLCI和路由器的网络地址相关联，如图15-11所示。在初始LMI交换的过程中，路由器可以从交换机上学到正在使用的DLCI。然后路由器向配置在接口上的每种协议的DLCI发送一个反向ARP请求，前提是每个接口都需要支持该协议。从反向ARP返回的信息将用来创建帧中继映射。



图15-11　反向ARP

15.2.3　反向ARP和LMI运行的各个阶段

LMI状态消息和反向ARP消息结合在一起使用，允许路由器将网络层地址和数据链路层地址相关联。

当连接到帧中继网络的路由器启动时，会向网络发送一条LMI状态请求消息。网络使用LMI状态消息应答，该消息中包含每条在接入链路上配置的虚电路的详细信息。

路由器定期地重复发送状态请求，但仅当状态改变时进行应答。在一系列简短的应答后，网络发送完全状态消息。

如果路由器需要将虚电路映射到网络层地址（在大多数情况下是IP），它给每条虚电路发送一个反向ARP消息。反向ARP消息中包括路由器自己的网络层地址，以便远程DTE设备（路由器）也可以执行映射。反向ARP应答允许路由器在地址和DLCI的映射表中建立映射条目。如果链路上支持多

种网络层协议（例如IP和IPX），则为每种网络层协议发送反向ARP消息。

15.2.4 帧中继映射

路由器可以从路由选择表决定下一跳地址，但该地址必须被解析到一个帧中继DLCI，如图15-12所示。这个解析过程是通过一个称为帧中继映射（Frame Relay Map）的数据结构来完成的。路由选择表用来提供出站通信流量的下一跳协议地址或DLCI。该数据结构可在路由器中静态配置，或使用反向ARP功能特性来自动建立映射。



路由选择表

网络	下一路由器的地址	接口
10.0.0.0	172.16.1.2	S0

主存

帧中继映射

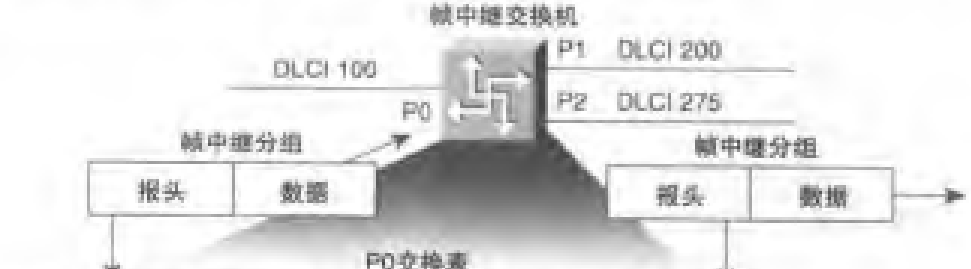
下一路由器的地址	DLCI
172.16.1.2	100

物理接口

图15-12 反向ARP请求的应答

15.2.5 帧中继交换表

帧中继交换表由4个条目组成：两个用来表示流入的端口和DLCI，两个用来表示流出的端口和DLCI，如图15-13所示。因此，经过每台交换机时，DLCI要被重新映射；访问端口可以改变。这正是即使访问端口能够改变时而DLCI却不可以改变的原因。



P0交换表

DLCI=100	入站端口	入站DLCI	出站端口	出站DLCI	DLCI=100
	P0	100	P1	200	
			P2	275	

图15-13 帧中继交换表

15.3 帧中继运行总结

现在已经学习了帧中继操作的基本概念，可以按照以下步骤来实现帧中继，如图15-14和图15-15所示。

步骤1 从服务提供商那里订购帧中继服务，或者创建一个专用的帧中继网络。

步骤2　将每台路由器连接到相应的帧中继交换机上，对于路由器的连接可以直接相连，也可以通过信道服务单元/数字服务单元（CSU/DSU）进行连接。

步骤3　当CPE路由器启动后，它向帧中继交换机发送状态查询消息。该消息一方面通知交换机远程路由器的状态，另一方面也向交换机询问其他远程路由器的连接状态。

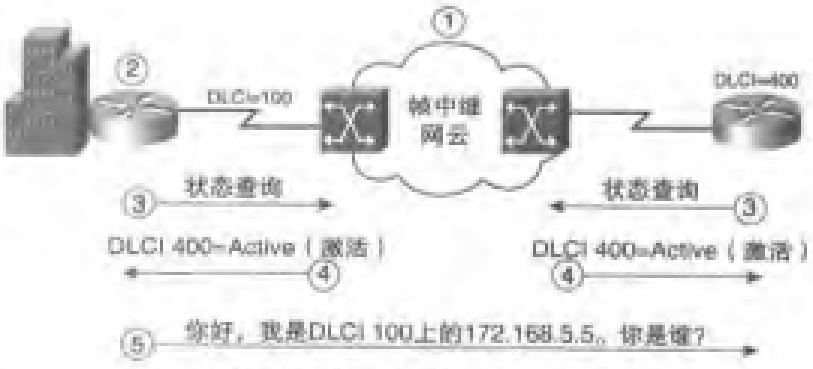


图15-14　配置远程路由器的路由

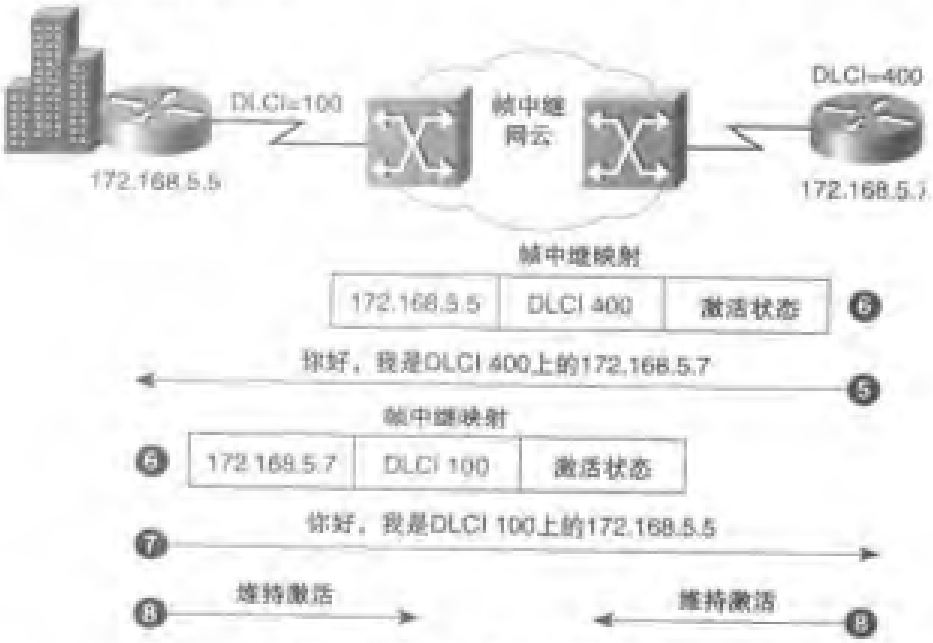


图15-15　改变每个DLCI的状态

步骤4　当帧中继交换机接收到请求时，它通过一条带有远程路由器DLCI的状态消息来响应请求，告知本地路由器能否发送数据。

步骤5　对于每一个激活状态的DLCI，每台路由器都发送一个反向ARP请求分组，用来介绍它自己的当前状态，同时也请求每台远程路由器通过发送各自的网络层地址来标识自身。

步骤6　当路由器收到反向ARP消息的时候，它在帧中继映射表中创建一条映射条目，该映射表包含本地DLCI和远程路由器的网络层地址以及连接的状态信息。注意：这里的DLCI是路由器在本地配置的DLCI，而不是远程路由器正在使用的DLCI。在帧中继映射表中可能出现3种连接状态。

- **激活状态**（*active state*）：表示连接是有效的，路由器可以交换数据。
- **未激活状态**（*inactive state*）：表示本地到帧中继交换机的连接是有效的，但是远程路由器到帧中继交换机是失效的，没有正常工作。
- **删除状态**（*delete state*）：表示没有本地管理接口可以接收帧中继交换机的信息，或者在CPE路由器和帧中继交换机之间没有服务发生。

步骤7　每隔60秒，路由器之间相互交换反向ARP消息。

步骤8　每隔10秒（此间隔是可以配置的），CPE路由器向帧中继交换机发送一条维持消息。维持消息的作用是验证帧中继交换机是否处于激活状态。

15.4 帧中继子接口

在帧中继网络中，为了能够发送完整的路由选择更新，可以为路由器配置逻辑划分的接口，这些接口称为子接口。子接口是物理接口的逻辑划分块。在子接口的配置过程中，每条PVC可配置为一个点到点的连接，从而允许子接口像专线那样工作，如图15-16所示。



图15-16 路由选择更新

早期运行帧中继时需要路由器（也就是一台DTE设备）为每条PVC都要有一个广域网串行接口，如图15-17所示。通过把单个广域网串行物理接口逻辑地划分成多个虚拟的子接口，可以将实现帧中继的总体成本大大降低。如图15-18所示，单个路由器接口通过使用不同的子接口可以为多个远程地点提供服务。

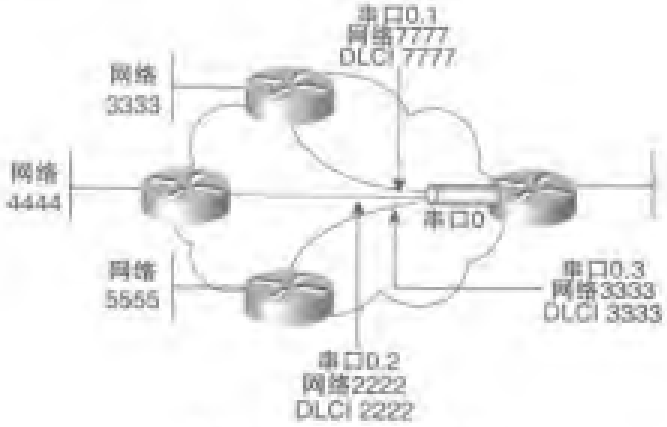


图15-17 惟一的DLCI号

15.4.1 水平分割路由选择环境

在水平分割路由选择环境（split horizon routing environments）中，从一个子接口学习到的路由，可以通过其他子接口通告。当一个物理接口接收到路由选择更新之后，会拒绝在相同的物理接口上通告该路由选择更新，因此，水平分割可以避免路由选择环路的发生，如图15-19所示。水平分割的结果是，如果一台远程路由器向中心路由器发送路由选择更新，而且中心路由器通过单一的物理接口连接着多条PVC，那么中心路由器就不能通过同一物理接口向其他远程路由器通告该路由选择更新消息，如图15-20所示。

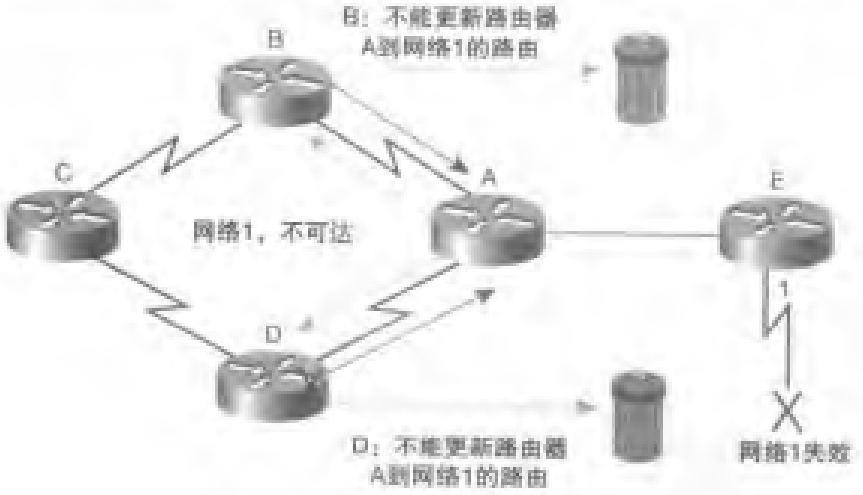


图15-18 水平分割

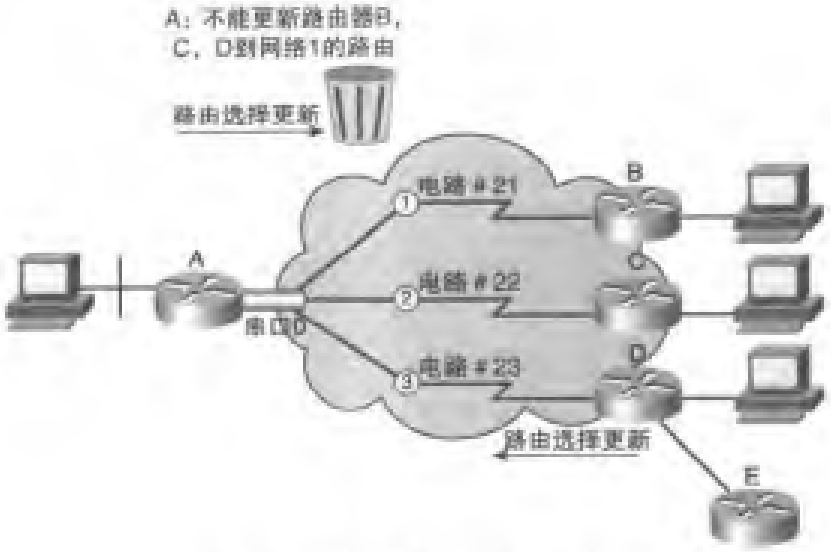


图15-19　水平分割路由更新

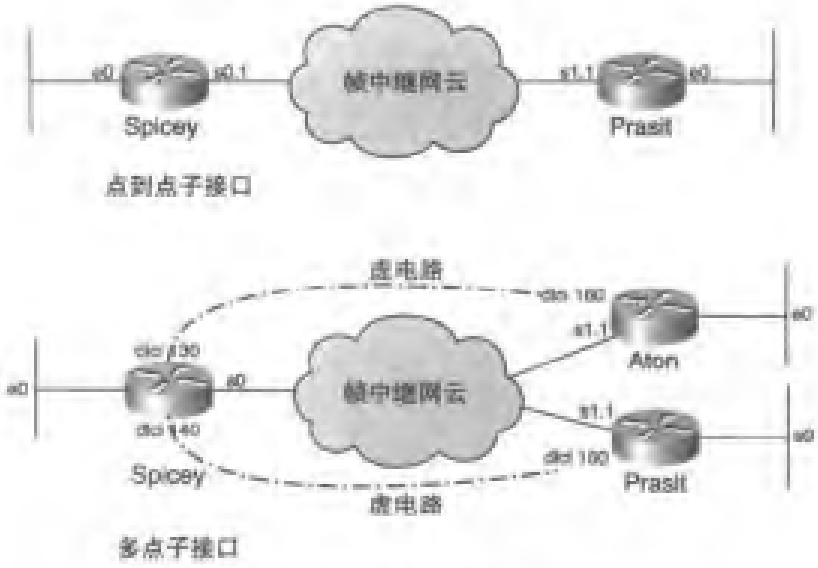


图15-20　可靠的连接

15.4.2　使用子接口解决可达性问题

可以将子接口配置成支持下列连接类型：

点到点（Point-to-Point）：使用一个单独的子接口来建立一条PVC，该PVC连接到一台远程路由器的子接口或者物理接口。在这种情况下，这些接口都在同一子网，并且每个接口都有它自己单独的DLCI。每个点到点连接所连接的是其本身的子网，因此在这样的环境下，广播是没有问题的，因为对路由器来说点到点连接就像专线一样。

多点类型（Multipoint）：使用一个单独的子接口来建立多条PVC，这些PVC连接到远程路由器的多个子接口或物理接口。这种情况下，所有加入的接口都处于同一个子网，并且每个接口都有自己的本地DLCI。因为子接口按常规的帧中继网络运行，所以路由选择更新要受到水平分割的限制。

15.5　基本帧中继配置

基本帧中继配置是指：在远程路由器支持LMI和反向ARP机制时，想在一个或多个物理接口上

配置帧中继。在这种环境下，本地管理接口告知路由器可以使用的DLCI。缺省情况下，逆向ARP机制功能开启，所以它不会显示在配置输出中。使用下列步骤可以进行基本帧中继配置：

步骤1 选择一个接口，并进入接口配置模式：

```
router(config)# interface serial 0
```

步骤2 配置网络层地址，如IP地址：

```
router(config-if)# ip address 192.168.38.40 255.255.255.0
```

步骤3 选择用来封装端到端的数据流量的封装类型：

```
router(config-if)# encapsulation frame-relay [cisco | ietf]
```

如果连接到另一台Cisco路由器，可以使用缺省值cisco。

ietf参数用来连接一台非Cisco路由器。

步骤4 如果Cisco IOS的版本是11.1或更早的版本，需要为帧中继交换机指定LMI类型：

```
router(config-if)# frame-relay lmi-type { ansi | cisco | q933a }
```

cisco是缺省值。如果IOS的版本是11.2或更新的版本，LMI类型可以自动适应，不需要进行该步骤的配置。

步骤5 为链路配置带宽：

```
router(config if)# bandwith kilobits
```

这条命令会影响路由选择操作，如IGRP协议，因为它用于定义链路的度量值。

步骤6 如果路由器禁止反向ARP，需要重新开启。（缺省情况下，反向ARP开启）。

```
router(config-if)# frame-relay inverse-arp [protocol][dlci]
```

*protocol*指所支持的协议类型，包括IP、IPX、AppleTalk、DECnet、VINES和XNS。

*dlci*是指交换反向ARP消息的本地接口的DLCI值。

现在我们已经大致了解了基本帧中继配置的步骤，可以利用这些知识在一台Cisco 1600路由器的串行接口上配置帧中继。

15.5.1 配置串行接口

使用下列步骤为串行接口配置帧中继分组封装：

步骤1 进入接口配置模式：

```
1600(config)# interface serial 0
```

步骤2 将该接口的封装方式设置为帧中继：

```
1600(config-if)# encapsulation frame-relay
```

步骤3 使该接口的配置改变生效：

```
1600(config-if)# no shutdown
```

15.5.2 检验串行接口的配置

可以通过确认PVC在帧中继线路上已被激活来验证接口的配置：

步骤1 键入encapsulation frame-relay命令之后等待60秒。

步骤2 进入特权EXEC模式，键入show frame-relay pvc命令。

步骤3 确认在命令输出中有PVC STATUS=ACTIVE消息（下例中的粗体字部分）：

```
1600# show frame-relay pvc

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 17, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0.1
```

```
input pkts 45 output pkts 52 in bytes 7764
out bytes 9958 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
pvc create time 00:30:59, last time pvc status changed 00:19:21
```

步骤4 记录DLCI = 消息中的DLCI值。（本例中，该值是17）。使用该值来完成帧中继接口的配置。

步骤5 如果键入命令之后没有输出结果，使用show interfaces serial 0命令来确定串行接口是否处于激活状态。命令输出的第1行应为：

```
Serial0 is up, line protocol is up
```

如果命令输出的第1行为Serial0 is up，line protocol is down，那么应该确认帧中继交换机的LMI类型配置正确，可以在同一命令输出中检查LMI type is CISCO消息来确认。

步骤6 返回全局配置模式，继续有关配置。

15.5.3 检验帧中继运行并确认连通性

配置帧中继之后，可以使用表15-1中的Show命令来验证连接是否激活。

表15-1 show命令

命令	描述
show interfaces serial	显示多播DLCI的信息，该DLCI用在运行帧中继配置的串行接口上，而LMI的DLCI用于相应的LMI
show frame-relay pvc	显示每个已配置连接的状态信息和流量统计。该命令也用来查看路由器接收到的BECN和FECN分组的个数
show frame-relay map	显示与本端路由器相连的远程设备的网络层地址信息和相应的DLCI值。该命令不适用于点到点子接口，仅用于多点接口和子接口
show frame-relay lmi	显示LMI流量统计信息。例如，显示本地路由器和帧中继交换机之间交换的状态消息的数量

15.5.4 确认线路的连通

完成下列步骤，可以确认线路是否连通。

步骤1 在特权EXEC模式下，键入show interfaces serial 0命令，显示如下信息：

```
1600# show interfaces serial 0
Serial0 is up, line protocol is up
Hardware is QUICC Serial
MTU 1500 bytes, BW 1544 Kbit,
DLY 20000 usec, rely 255/255, load 1/255
Encapsulation FRAME-RELAY,
loopback not set, keepalive set (10 sec)
LMI enq sent 163, LMI stat recvd 136,
LMI upd recvd 0, DTE LMI up
LMI enq recvd 39, LMI stat sent 0, LMI upd sent 0
LMI DLCI 1023 LMI type is CISCO frame relay DTE
Broadcast queue 0/64, broadcasts sent/dropped 27/0,
interface broadcasts 28
```

```
Last input 00:00:01, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops);
    Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/64/0 (size/threshold/drops)
Conversations 0/1 (active/max active)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1813 packets input, 109641 bytes, 0 no buffer
Received 1576 broadcasts, 0 runts, 0 giants
13 input errors, 0 CRC, 13 frame, 0 overrun,
    0 ignored, 0 abort
1818 packets output, 117260 bytes, 0 underruns
0 output errors, 0 collisions, 32 interface resets
0 output buffer failures, 0 output buffers swapped out
29 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

步骤2 确认在命令输出内容中有下列信息：

- Serial0 is up, line protocol is up——表示帧中继连接处于激活状态。
- LMI enq sent 163, LMI stat recvd 136——表示该连接正在发送和接收的数据，在输出中的数值有可能不同。
- LMI type is CISCO——路由器的LMI类型配置正确。

步骤3 如果命令的输出内容中没有出现上述消息，则执行下列步骤：

- 向帧中继服务提供商确认你所租用的线路是否正确配置了LMI。
- 确认设置了维持机制，并且路由器正在接收LMI更新信息。

步骤4 返回全局配置模式，继续有关配置。

15.5.5 确认帧中继映射

完成以下步骤，以实现对帧中继映射的检验：

步骤1 在特权EXEC模式下，键入show frame-relay map命令。查看输出内容中，每个串行子接口是否存在status defined, active这样的信息：

```
1600# show frame-relay map
Serial0.1 (up): point-to-point dlci, dlci 17 (0x11, 0x410),
    broadcast,
status defined, active
```

步骤2 如果命令的输出内容中没有步骤1中的信息，则执行以下步骤。

- 确认中心站点路由器连通并进行了正确配置。
- 与帧中继运营商联系，检验线路是否运行正常。

步骤3 返回全局配置模式，继续有关配置。

15.5.6　确认到中心站点路由器的连通性

完成以下步骤，以检测到中心站点路由器（HQ）的连接是否正常：

步骤1　在特权EXEC模式下，键入ping命令，之后键入中心站点路由器的IP地址。

步骤2　注意在Success rate...这一行中的百分比（用粗体字显示）：

```
1600# ping 192.168.38.40

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.38.40,

timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5),

round-trip min/avg/max = 32/32/32 ms

1600#
```

如果成功率在20%以上，说明本次检验是成功的。

步骤3　返回全局配置模式，继续有关配置。

实验活动　配置帧中继

在本实验中，你要配置路由器与本地帧中继交换机建立成功的连接。可以使用Adtran Atlas550帧中继仿真器来模拟交换机/帧中继网云。

实验活动　配置帧中继PVC

在本实验中，你要配置两台背对背的路由器，使其成为帧中继PVC。在没有帧中继交换机和LMI的条件下，这是由手动完成的。

15.5.7　配置子接口

如图15-22所示，为了在物理接口上配置子接口，可以通过下列步骤实现：

步骤1　选择想要在上面创建子接口的物理接口，进入接口配置模式。

步骤2　删除已经分配给该物理接口的所有网络层地址。只要物理接口还有一个地址，本地子接口就无法接收数据帧。

步骤3　按照“基本帧中继配置”部分内容的介绍，配置帧中继封装。

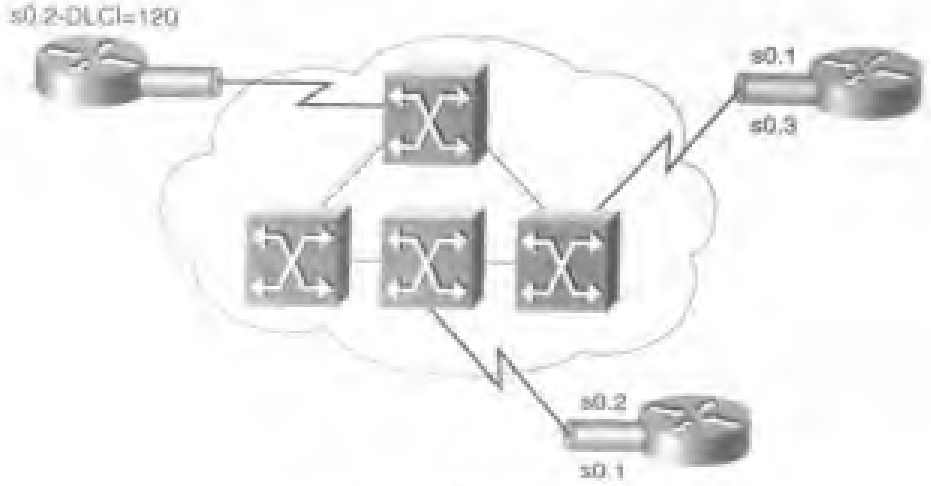


图15-21　点到点子接口

步骤4 选择想要配置的子接口：

```
router(config-if)# interface serial number. subinterface-number
(multipoint | point-to-point)
```

这里，参数number. subinterface-number是指子接口号，取值范围在1到4,294,967,293之间。句点前面的接口号必须与该子接口所属的物理接口的接口号一致。

multipoint用于路由器转发接收到的广播和路由选择更新的情况。如果希望对IP进行路由选择并希望所有的路由器在同一个子网内，可以选择multipoint，如图15-22所示。

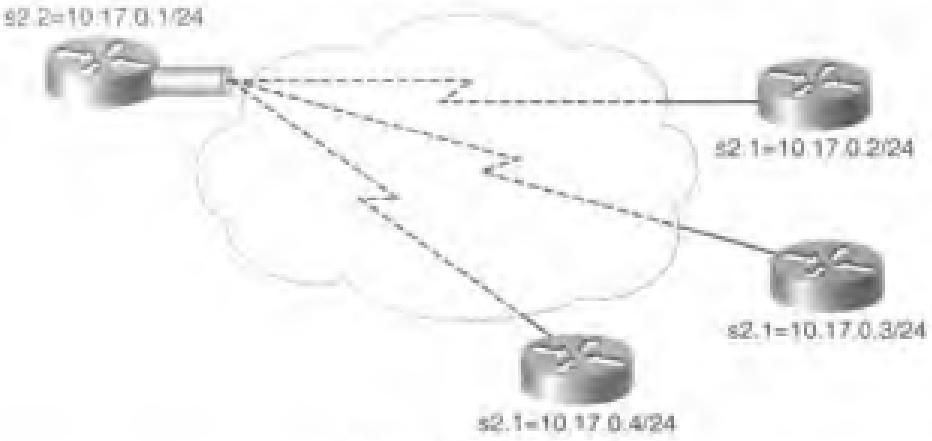


图15-22 多点配置

point-to-point用于以下情况：如果不希望路由器转发接收到的广播信息或路由选择更新，而是希望每对点到点的路由器都有自己的子网，就选择point-to-point，如图15-23所示。

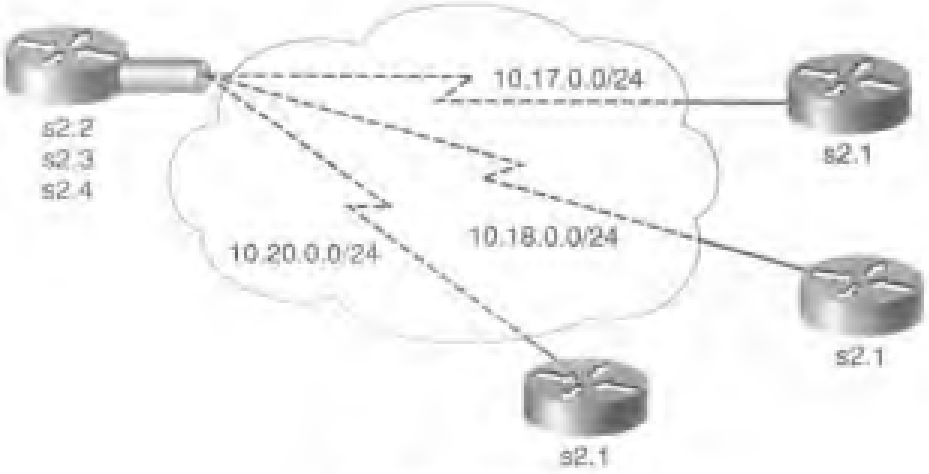


图15-23 子接口配置

必须选择multipoint参数或point-to-point参数，没有默认值。

步骤5 为子接口配置网络层地址。如果子接口是点到点的，使用的协议是IP，那么可以使用ip unnumbered命令来实现配置。

```
router(config-if)# ip unnumbered interface
```

如果使用该命令，推荐使用环路（loopback）接口。因为如果指向一个不是完全可行的接口，帧中继链路不能正常工作；而且环路接口一般不可能失效。

步骤6 如果把子接口配置成多点类型，或者点到点类型，必须为子接口配置一个本地DLCI，以便和物理接口区分开来。

```
router(config-if)# frame-relay interface-dlci dlci-number
```

这里，参数dlci-number定义了连接到子接口的本地DLCI号。这也是把通过LMI学习到的PVC关联到子接口的惟一途径，因为LMI不能识别子接口。

所有点到点的子接口都需要使用该命令。同样地，对于支持反向ARP的多点子接口也需要使用该命令。对于配置静态路由映射的多点子接口就不需要使用该命令。

此外，不要对物理接口使用该命令。

实验活动　配置帧中继子接口

在本实验中，你将使用Adtran Atlas550帧中继仿真器模拟交换机／帧中继网云，将3台路由器配置成全网状帧中继网络。

15.5.8　配置可选命令

在路由器的扩展操作过程中，如果必要的话可以使用以下命令：

```
router(config-if)# frame-relay map protocol protocol-address dlci [broadcast][ietf |
cisco | payload-compress packet-by-packet]
```

表15-2　表15-2描述了该命令的句法格式。frame-relay map命令句法

参数	描述
protocol	定义所支持的协议、桥接或逻辑链路控制
protocol-address	指定目的路由器接口的网络层地址
dlci	指定用于连接远程协议地址的本地DLCI
broadcast	（可选的） 当禁止多点传送时，用来向该地址转发广播信息。如果希望路由器转发路由选择更新，可以使用该参数
ietf | cisco	（可选的） 选择使用的帧中继封装类型。只有在远程路由器是非Cisco路由器时使用ietf参数，否则使用cisco参数
payload-compress packet-by-packet	（可选的） 使用模式存储器方式逐个分组对有效载荷进行压缩

一般来讲，反向ARP用于为某个特定的连接请求下一跳协议地址。反向ARP的应答信息保存在地址和DLCI的映射表（即帧中继映射）中，如图15-24所示。该映射表可以用来进行出站流量的路由选择。如果远程路由器不支持反向ARP，又希望在帧中继网络上配置OSPF时，或者在使用路由选择时又希望控制广播流量时，必须静态指定地址和DLCI的映射表。这些静态的条目称为静态映射。

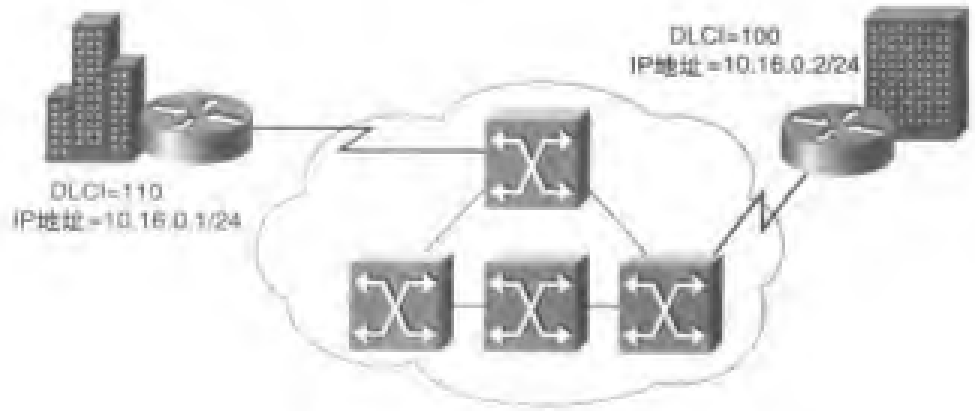


图15-24　反向ARP应答

使用帧中继过程中，可以增加或减少维持间隔，也可以延长或缩短路由器接口向帧中继交换机发送维持数据包的时间间隔。缺省的时间间隔为10秒，下面是命令的格式：

```
router(config-if)# keepalive number
```

这里参数*number*是一个以秒为单位的数字，该值通常比帧中继交换机设定的时间短2到3秒（很短的时间间隔），以保证正确的同步。

如果网络没有指定LMI类型或者在路由器之间进行背对背测试时，必须要使用以下命令为每个本地接口指定DLCI：

```
router(config-if)# frame-relay local-dlci number
```

这里参数*numbe*是指本地接口使用的DLCI值。

15.6 总结

在本章中，你学习了以下内容：

- 帧中继广域网技术提供了一种灵活的方法，用来在帧中继广域网上连接不同的局域网。
- 帧中继提供了一种分组交换的通信能力，在用户设备（如路由器、网桥和用户主机）和网络设备（如交换节点）之间进行数据通信。
- 帧中继使用虚电路在广域网上建立连接。
- 本地管理接口（LMI）的主要目的是：
  - —— 决定路由器所知的众多PVC的运行状态。
  - —— 发送维持分组，确保PVC一直保持连通状态，不会因为一段时间没有使用而失效。
  - —— 通知路由器哪些PVC是可用的。
- 反向ARP机制允许路由器自动建立帧中继映射。
- 根据路由选择表决定的路由器下一跳地址，必须能够被解析为帧中继的DLCI。
- 帧中继可以把单独的一个广域网物理接口划分成多个子接口。
- 水平分割通过不允许从一个物理接口接收的路由选择更新通过相同的物理接口被通告，减少了路由选择环路。

作为本章所学习内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

15.7 关键术语

承诺突发（*committed burst, Bc*） 承诺突发是在帧中继互连网中所协商的一个业务度量值。它是帧中继网络承诺的以CIR接收和传输的最大数据量（以比特计）。

超量突发（*excess burst, Be*） 超量突发是在帧中继互连网络中所协商的一个业务度量值。它是帧中继互连网络在超过承诺突发后所试图传输的比特数。因为超量突发数据可以被网络标志为DE（Discard Eligible，可丢弃），所以一般成功传输超量突发数据的可能性要低于承诺突发数据。

后向显式拥塞通知（*backward explicit congestion notification, BECN*） 后向显式拥塞通知是由帧中继网络设置的标志比特，存在于与拥塞路径的传输方向相反的数据帧中。当DTE接收到了带有BECN比特设置的帧时，它可以请求高层协议采取适当的流量控制措施。

承诺信息速率（*committed information rate, CIR*） 承诺信息速率（以bit/s为单位）是在帧中继网络中入站干线接口和出站干线接口上，帧中继网络承诺的在一般条件下向帧中继终端系统传输信息的速率。该速率是指在最小时间间隔Tc内的平均值。

数据链路连接标识符（*data-link connection identifier, DLCI*） 数据链路连接标识符是在帧中继网络中标识永久虚电路（PVC）或交换虚电路（SVC）的值。在基本的帧中继规范中，DLCI具有本地意义。（也就是说，被连接设备可能使用不同值来指定同一个连接。）在本地管理接口（LMI）扩展规范中，DLCI具有全局意义。（也就是说，DLCI指定各个终端设备。）

帧校验序列（*Frame Check Sequence, FCS*） 帧校验序列采用标准16bits的循环冗余校验码（CRC），它适用于HDLC和帧中继数据帧。FCS在开始标志和FCS之间检测数据帧中发生错误的比特，它只能检测长度不超过4,096字节的数据帧中的错误。

前向显式拥塞通知（*forward explicit congestion notification, FECN*） 前向显式拥塞通知是由帧中继网络设置的标志比特，用来通知接收该数据帧的DTE设备，在从源到目的地的路径上发生了拥塞。DTE设备接收带有前向显式拥塞通知位的数据帧，它可以请求更高层的协议采取适当的流量控制措施。

帧中继（*Frame Relay*） 是业界标准的交换式数据链路层协议，在所连接的设备之间采用HDLC封装，可以处理多条虚电路。帧中继比X.25更为有效，目前一般都使用帧中继取代X.25。

本地访问速率（*local access rate*） 连接到帧中继网云（本地环路）的时钟速率（端口速率）。该速率是数据流入网络或流出网络的速率。

本地管理接口（*Local Management Interface, LMI*） 本地管理接口是基本帧中继规范的增强集。LMI包括对维持机制的支持，该机制用于检验数据是否能够在链路上流动；对多播技术的支持，该技术可为网络服务器提供其本地DLCI和多播DLCI；对全局寻址技术的支持，该技术可在帧中继网络中给DLCI以全局意义而不仅是本地意义；以及对状态机制的支持，该机制向交换机报告已知DLCI的现行状态。

永久虚电路（*permanent virtual circuit, PVC*） 永久虚电路是指永久建立的虚电路。PVC节省了与电路建立和撤消相关的带宽，满足了某些虚电路必须始终存在的情形。

公共数据网（*public data network*） 公共数据网是由政府（如在欧洲）或私营公司运作的，为公众提供计算机通信的网络，通常是营利的。公共数据网使小型组织可以在不必为远距离电路设备投资的情况下创建一个广域网。

15.8 复习题

1. 在同一个物理连接中，帧中继是如何处理多个会话过程的？
   A. 采用双工会话方式
   B. 采用多路复用电路
   C. 它将数据转换成ATM信元
   D. 不允许进行多个会话过程
2. 帧中继采用以下哪种协议进行纠错处理？
   A. 物理层和数据链路层协议
   B. 上层协议
   C. 下层协议
   D. 帧中继不进行纠错处理
3. 帧中继采用以下哪种方式使得DLCI具有全局性？
   A. 广播DLCI
   B. 发送单播信息
   C. 发送组播信息
   D. DLCI不具有全局性
4. 以下哪个是帧中继交换机为进行数据传输而同意的数据速率？
   A. 承诺信息速率（CIR）
   B. 数据传输速率
   C. 定时速率
   D. 波特率
5. DLCI号是由谁来分配的？
   A. 终端用户
   B. 网络根
   C. DLCI服务器
   D. 服务提供商
6. 帧中继报头格式中的哪个字段包含DLCI信息？
   A. 标志字段
   B. 地址字段
   C. 数据字段
   D. 校验和字段
7. 帧中继使用以下哪一项来保持PVC一直处于连通状态？
   A. 点到点连接
   B. Windows Socket
   C. 维持机制
   D. PVC不可能一直保持连通状态
8. 帧中继如何使用反向ARP请求？
   A. 它把IP地址映射成MAC地址
   B. 它把MAC地址映射成IP地址
   C. 它把MAC地址映射成网络地址
   D. 使用IP地址到DLCI的映射表
9. 帧中继采用什么来决定下一跳？

A. ARP表
B. RIP路由选择表
C. 帧中继映射
D. IGRP路由选择表

10. 帧中继采用水平分割的目的是什么？
A. 增加路由器更新
B. 防止路由选择环路
C. 缩短收敛时间
D. 帧中继不使用水平分割

11. 帧中继运行在哪一层？
A. 第2层
B. 第3层
C. 第4层
D. 第1层

12. 下面哪一条叙述是正确的？
A. DTE设备的目的是在网络中提供时钟业务和交换业务
B. 关于帧中继的标准化建议最早是由国际电话与电报顾问委员会（CCITT）提出的
C. 帧中继的较早版本是和本地管理接口（LMI）共同涉及的
D. 交换式的虚电路是永久性的连接，适用在帧中继上的DTE设备之间只需少量数据传输的情况

13. 使用下列哪条命令（在配置模式提示符下）进入配置模式，在这个模式下可以为串口进行帧中继分组封装？
A. # Configure terminal
B. # encapsulation frame-relay
C. # frame-relay interface dlci *number*
D. # interface serial0

14. 如果执行了show interface serial 0命令而且出现了消息“Serial line is up，line protocol is up”，对于这条消息的正确解释是什么？
A. 链路正在接收和发送数据
B. 路由器已经正确配置了本地管理接口（LMI）
C. 帧中继的连接处于激活状态
D. 中心站点路由器开通并处于连接状态

15. 命令show interfaces serial的作用是什么？
A. 显示关于多播的DLCI信息、已配置串口上的帧中继所使用的DLCI信息以及由本地管理接口（LMI）使用的DLCI信息
B. 显示每一个配置的连接状态以及流量的统计信息。该命令还适用于查看路由器所接收的BECN（后向显式拥塞通知）和FECN（前向显式拥塞通知）分组的个数
C. 显示关于与每台本地路由器相连的远程目的设备的网络层地址及相关的DLCI信息
D. 显示本地管理接口（LMI）流量的统计信息。比如，它显示在本地路由器以及帧中继交换机之间交换的状态消息的数量

16. FECN和BECN是什么？
A. 错误校验机制
B. 拥塞通知机制

C. 流量控制机制
D. 维持机制

17. 下面哪项对帧中继虚电路的描述是正确的？
A. 需要会话的建立阶段和拆除阶段
B. 仅适用于有少量数据传输时
C. 在帧中继网络上提供永久的通信路径
D. 在网络设备之间提供一条逻辑的、双向的通信路径

18. 帧中继使用循环冗余校验码（CRC）的目的是什么？
A. 在虚电路上执行流量控制
B. 执行错误校验功能
C. 管理地址解析功能
D. 管理FECN和BECN的操作

19. 下面关于帧中继本地管理接口（LMI）扩展的描述，哪条是不正确的？
A. 通过计算产生了MAC地址
B. 组播组
C. 全局寻址
D. 虚电路状态消息



第16章　网络管理介绍

目标

学习完本章后，你将能够：

- 解释Windows、UNIX和Linux工作站的重要特性。
- 解释网络服务器的功能。
- 理解网络操作系统。

“网络管理（network management）”一词涵盖了在你进行计算机网络管理工作时候的许多内容和细节。本章着重于讲解管理桌面/网络系统的一些主要任务以及提供了在部署企业网络资源时对一些常用服务器选项的比较。本章还讲述了一些可选硬件和软件的优缺点，以及在何种环境下这些不同选项的组合可以达到性能的最优化。对于怎样使用开放系统互连（OSI）模型和简单网络管理协议（SNMP）来帮助管理网络，本章也做了一定的阐述。

请注意参阅本书所附光盘中有关本章的e-Lab实验、视频及插图，光盘上的素材与本章内容的补充，能强化本章所介绍的概念。

16.1　桌面和服务器操作系统简介

第一台个人计算机（PC）是为孤立的桌面系统设计的。它的操作系统软件允许单个用户在某一时间访问文件和系统资源。用户必须坐在PC前进行操作。当基于PC的计算机网络在工作中逐渐普及起来时，软件公司开发了各种专用的网络操作系统（NOS, Network operating system）。他们开发的NOS可以提供文件安全、用户权限管理以及多个用户之间的资源共享。因特网的爆发性增长迫使这些NOS的开发者们开发出来的NOS和当今的因特网相关技术和服务息息相关，如World Wide Web（WWW）。

最近10年以来，连网（networking）已经成为桌面计算的核心内容。配备了连网特性和服务的现代桌面操作系统和它们对应的网络操作系统（NOS）之间的区别正在逐步消失。现在，最流行的操作系统，如Microsoft Windows 2000和Linux，既能安装在高性能的网络服务器上，也能安装在个人用户的PC上。

16.1.1　工作站

工作站（workstation）是运行某些应用程序的客户计算机，它连接到服务器上，从服务器上获

得与其他工作站共享的数据。服务器（server）是运行NOS的计算机。工作站运行一些特别的软件，如网络外壳程序（network shell program）来执行下面的操作：

- 获取用户数据和应用程序命令。
- 决定命令是由本地操作系统响应还是发给NOS。
- 将命令发到本地操作系统或者发给网络接口卡（NIC）处理以传输到网络。
- 从网络上获取发送到运行在本地工作站上的应用程序的数据。



图16-1　典型的工作站

Window NT、Window 2000、Windows XP Professional等操作系统能够运行在个人计算机上。所有运行这些系统的计算机既可以当作是工作站（如图16-1），也可以当作服务器（如图16-2）。PC是指运行其他一些专门为PC设计的操作系统的计算机，如DOS、Windows 95、Windows 98、Windows ME或Windows XP Home。



图16-2　典型的服务器

UNIX和Linux能够做为桌面操作系统来使用，但它们主要是用在高端计算机上。这些工作站主要用于工程与科学计算，因此需要专用的高性能计算机来实现。经常在UNIX工作站上运行的应用有：

- 计算机辅助设计（CAD）。
- 电子电路设计。
- 气象数据分析。
- 计算机图像动画。
- 电信设备管理。

许多现在的桌面操作系统都包括网络功能和支持多用户访问。由于这个原因，根据计算机完成的应用类型来区分计算机和操作系统已经变得非常普遍。这种区分是根据计算机来完成的功能或担当的角色来划分的，如工作站或者服务器。典型的桌面或低端计算机应用包括文字处理、表格处理和财务管理。高端工作站应用包括图像设计、设备管理和其他上面已经列出的内容。

无盘工作站（diskless workstation）是一种专门为运行在网络上设计的计算机类型。正如它的名字所示，无盘工作站没有磁盘驱动器，但有显示器、键盘、内存，包含在只读存储器（ROM）芯片里的引导指示以及网络接口卡。用来建立网络连接的软件从网络接口卡上的可引导ROM芯片中被加载。

因为无盘工作站没有磁盘驱动器，所以你不能从无盘工作站上载或者下载任何数据。这样，无盘工作站不能往网络上传播任何计算机病毒，也不能从网络上拷贝任何数据到它本地磁盘。因此，无盘工作站比普通工作站提供更好的安全性，无盘工作站应用在在安全问题极为重要的网络环境中。

便携式电脑也能用作局域网（LAN）上的工作站。它能通过扩展坞（docking station）、外部LAN适配器或者PCMCIA卡来接入网络。扩展坞（图16-3）是一种将便携式电脑转变为桌面计算机的附加装置。

16.1.2 服务器



图16-3 扩展坞

在一个NOS环境中，许多客户端系统要访问和共享一台或多台服务器上的资源。桌面客户系统配备了他们自己的内存和外围设备，如键盘、显示器和磁盘驱动器等。服务器系统必须提供处理来自客户端的多个并发用户提交的资源请求的能力。

NOS设计了特定的网络管理工具和特性来支持多个用户的并发访问。在一些比较小的网络上，NOS安装在高性能的服务器上，多个用户——也就是客户端，共享这些服务器。服务器必须有高容量/高转速的磁盘驱动器，数量极大的内存（RAM）和高速网络接口卡。在某些情况下，还有多个中央处理单元（CPU），而且它们一般都配置了TCP/IP协议，提供一个或多个TCP/IP服务。

运行NOS的服务器也用于对用户进行身份验证并提供对共享资源的访问，如图16-4。他们能够同时处理多个用户的并发请求。在一个客户能够访问服务器资源之前，客户必须先得到验证并且被授权使用这些资源，这可通过分配给每个客户一个帐户和密码来实现。帐户和密码则被认证服务来确认。验证服务就像哨兵一样，监控着对网络资源的访问。通过帐户管理、安全和访问控制的集中化处理，这种基于服务器的网络简化了网络管理的工作。

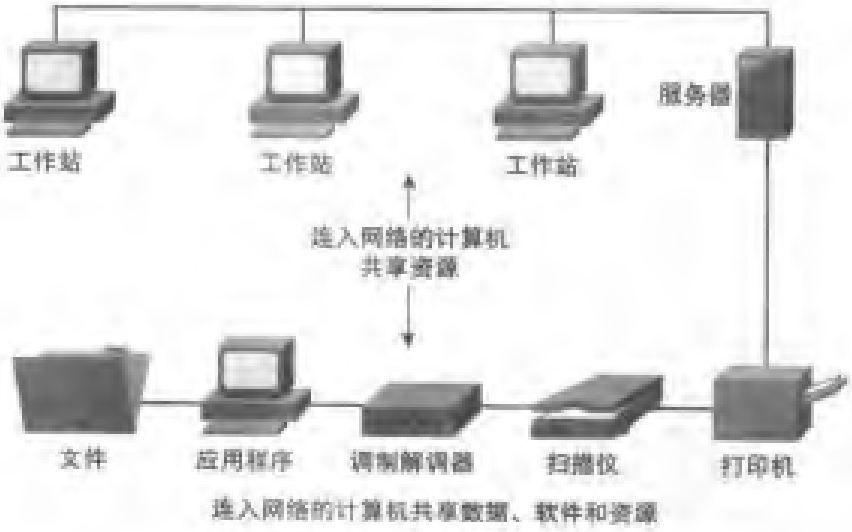


图16-4 共享资源

服务器一般都有相当大的内存来支持多个任务的同时运行，有相当大的磁盘空间来存储共享文件以及作为系统内存的扩展。服务器也一般需要在系统主板上有多个扩展插槽以连接一些共享设备，如打印机和多块网络接口卡。

作为服务器运行的计算机系统所需要的另外一个特性是有很高的处理能力。一般的，计算机只有一个CPU，来执行一个给定任务或进程的指令。为了有效的和快速的对客户提交的请求进行响应，网络服务器需要强大的CPU来执行任务和程序。拥有一个CPU的单处理系统如果处理速度足够快的

话，也是可以满足要求的。但是为了达到更高的处理速度，一些服务器系统需要配置多个处理器。这样的系统称为多处理器系统，他们具备了同时执行多个任务，并且将不同的任务分配给不同处理器执行的能力。多处理系统在一定时间内执行任务的数量得到了极大的提高。

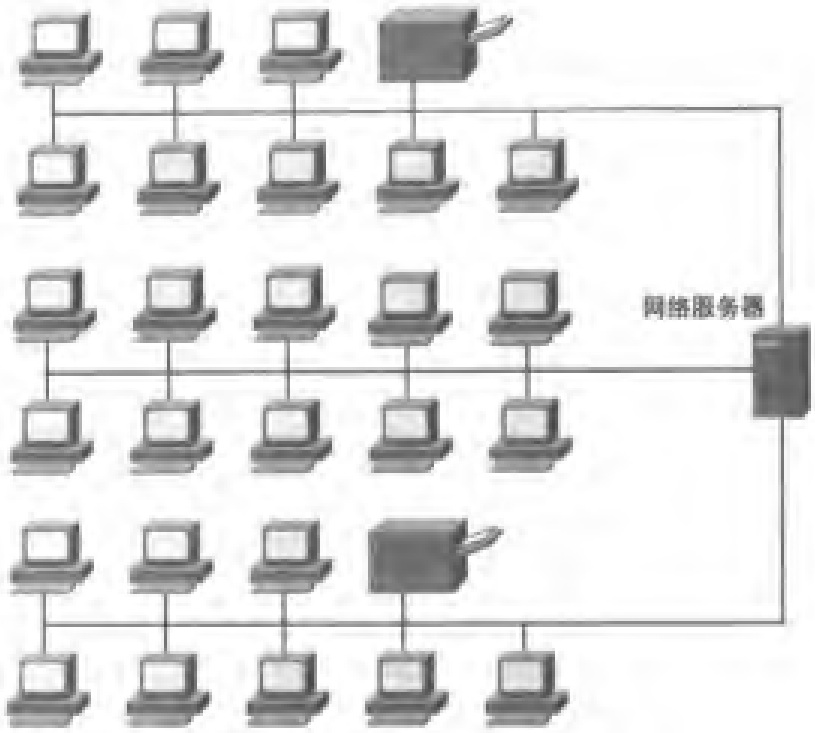


图16-5　支持多个客户端系统的服务器

因为服务器处于网络操作系统的中心位置，上面有着一些对客户端系统至关重要的资源，如图16-5，所以服务器不仅仅需要高性能，而且需要健壮性。“健壮性”是指服务器系统在负载非常大的情况下能够有效工作的能力。这也意味着服务器系统能够在一个或多个处理器或组件发生故障时而不终止服务。这个要求可以通过在服务器系统中构建冗余部件来实现。冗余是指一些特定的硬件，它们在正常组件发生故障后代替它们的工作。冗余是容错系统的一个特性，冗余的引入满足了服务器系统甚至在配件维修的时候都不中断服务的要求。因为NOS依靠服务器的不间断工作，所以额外的冗余配件意味着额外的费用。

服务器应用和功能包括使用超文本传输协议（HTTP）的WEB服务、使用文件传输协议（FTP）的文件传输服务和使用域名系统（DNS）的主机名字服务等。网络服务器支持标准的电子邮件协议，如简单邮件传输协议（SMTP）、邮局协议（POP）和因特网消息访问协议（IMAP）。它还包括一些文件共享协议，如SUN公司的网络文件系统（NFS）协议和Microsoft公司的服务器消息块（SMB）协议。

网络服务器通常也提供打印服务，它也能够提供动态主机配置协议（DHCP）服务，这用来给网络上的客户计算机自动分配IP地址。除了为网络上的客户端运行上述这些服务以外，服务器还能被设置为网络上的一个简单防火墙，这是通过代理服务器软件或网络地址转换（NAT）功能来实现的，这两种方法的共同点是对外部因特网隐藏内部私有地址，从而达到一定程度的安全性。服务器的这些应用一般都不在LAN工作站上实现。

一台运行NOS的服务器当它为较少数量的客户机服务时，可能会运行良好。然而，当网络发展到一定程度时，大多数组织发现他们必须配置多台服务器才能提供可以接受的性能，如图16-6所示。一个典型的服务分流设计是一台服务器负责电子邮件服务，另外一台服务器



图16-6　客户机/服务器环境

负责文件共享服务，第三台服务器负责FTP服务。

服务器上的网络资源，如文件、打印机、应用程序的集中，如图16-7所示，也使得备份和维护它们产生的数据更为方便。将这些网络资源集中地配置在特殊的、专门的服务器上，而不是大范围的PC机上，更有利于用户访问和资源备份。

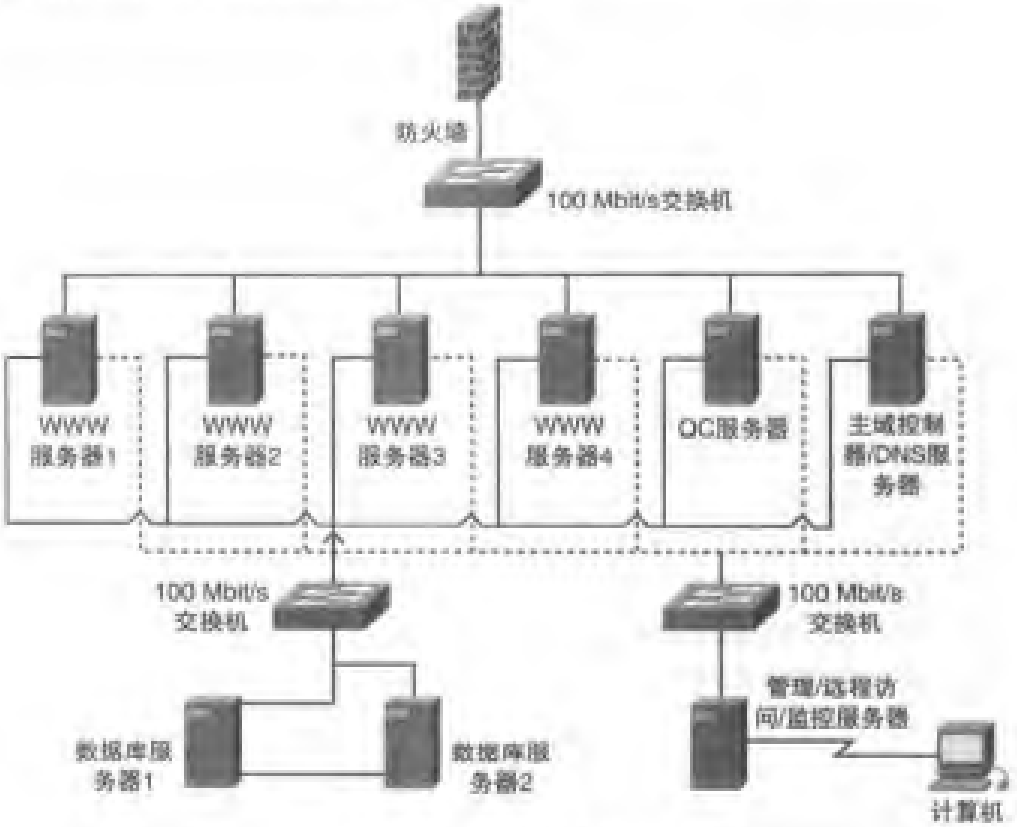


图16-7 服务器群

16.1.3 客户机/服务器关系

客户机/服务器（Client/Server）计算模型实现了在多台计算机上的分布式处理。分布式处理（distributed processing）能够很方便的访问远程系统，从而达到共享信息和网络资源的目的。在一个客户机/服务器环境中，客户机、服务器共享或分担处理任务。大多数NOS都是基于客户机/服务器模式来设计，以给客户提供网络服务。网络上的计算机可以被看作一台主机、一台工作站、一台客户机或者一台服务器。一台运行TCP/IP协议的计算机，不管是工作站还是服务器，都可以被看作是一台网络主机。以下列出了客户机/服务器关系中的一些要点：

- 本地主机是指用户当前工作者的主机。
- 远程主机是指用户正在访问的另外一个系统。
- 服务器通过网络给一台或多台客户机提供资源。
- 客户机是从网络上的一台或多台服务器接受服务的计算机。

客户机/服务器关系一个简单例子是FTP会话。FTP协议是把文件从一台计算机传输到另外一台计算机的工业标准。为了使客户机能够从服务器下载或上传文件，服务器必须运行FTP后台进程或服务。如图16-8所示，在这个例子中，客户端发出一个文

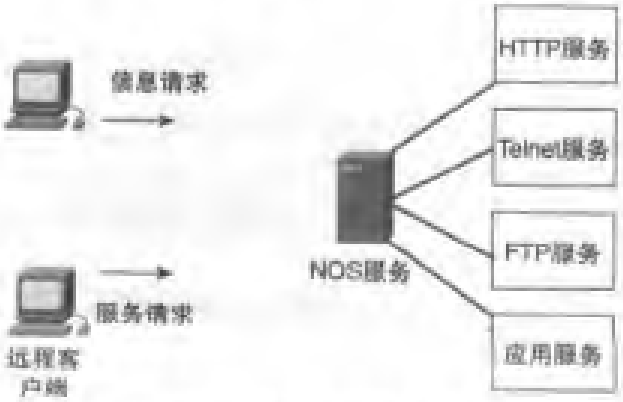


图16-8 客户机/服务器交互

件传输请求，服务器则提供传送或接收文件所需要的服务。

因特网也是一个客户机/服务器分布式处理关系的很好的例子。客户机或前台负责用户表达功能，如屏幕格式、输入窗口和数据编辑，这些是通过浏览器，如Netscape或Internet Explorer来完成的。网页浏览器向网站服务器提交请求，当浏览器向服务器请求数据时，服务器作出响应，浏览器程序就从服务器得到回复数据，然后浏览器就把它收到的HTTP数据显示在窗口中。服务器或者后台程序负责处理客户机发出的页面请求并提供HTTP或WWW服务。

客户机/服务器关系的另外一个例子是LAN上的数据库服务器和数据输入或查询客户端。客户端或前台可能运行一个由C语言或Java语言编写的程序，服务器或后台可能运行Oracle或者其他的数据库管理软件。这样，客户机负责用户的格式表达任务，服务器提供给用户数据存储和数据查询服务。

在一个典型的文件服务器环境中，客户机可能不得不把一个非常大的数据库文件下载到本地然后在本地进行处理工作，这样，大量的文件传输可能会导致网络流量过载。而采用客户机/服务器模式，客户机提交请求给服务器，服务器的数据处理引擎可能会处理10万条记录，然后只将少量满足客户需求的结果传回给客户，而且服务器一般比客户计算机的处理能力强大得多，因此也更适合于处理大量的数据。这样，通过客户机/服务器计算模型，大量的数据存储和处理发生在服务器端，而客户机只需要产生查询即可，网络上只通过非常少的数据或结果，这就既满足了客户机的数据查询和所需结果又减少了网络流量。

客户机/服务器网络的功能分布具有众多优点，同时也导致成本的上升。虽然将资源会聚到服务器系统中带来了更高的安全性、更简单的操作和更协调的控制，但服务器为网络引入了单点故障。另外，服务器需要训练有素的专业人员进行管理和维护，这也会增加网络运营的开销。服务器系统需要的额外的硬件和特定的软件也增加了成本。

16.1.4 NOSs

计算机的操作系统是运行在这台计算机上的应用软件和服务的软件基础。同样的，NOS使得网络上的多台设备之间可以通信和共享资源。NOS一般是指运行在网络服务器上的操作系统，如UNIX server、Microsoft Windows NT server或Windows 2000 server。表16-1列出了不同公司提供的各种操作系统。

表16-1 常用的网络操作系统

Novell	UNIX	Windows	Linux
NetWare	HP-UX	NT	Red Hat
IntraNetWare	Sun Solaris	2000 Server	SCO
GroupWise	BSD	.NET Server	SuSE
	SCO		Debian
	AIX		Mandrake
			Xandros

工作站上的操作系统的功能主要是控制计算机硬件、控制程序执行环境和为用户提供操作界面，工作站上的操作系统有为单个用户或按顺序的为多个用户执行这些功能的能力，但却不能同时为多个用户执行上述功能。管理员也能给多个用户建立多个帐号，但他们只能分别，而不能同时登录这个工作站。

相反的，NOS将它的上述功能分布给网络上的计算机来共同完成，NOS的实现取决于运行在每台计算机上的本地操作系统，因此，NOS将多个用户同时访问共享资源的能力加入到了它的特性集中。

工作站在单独运行的时候，它执行本地操作系统提供的功能：如用户能够访问本地资源，包括

应用程序、文件和直接相连的设备，如打印机等。当工作站成为NOS环境中的客户机后，它执行一些特定的软件，使得本地用户能够访问非本地（远程）资源，并且那些资源就像在本地一样。NOS通过实现远程访问服务，扩展了本地操作系统，从而增强了客户机工作站的可达性。

尽管工作站上的多个用户能拥有自己的帐号，但在一个给定的时间，只能有一个帐号能访问系统。相反的，NOS支持多台客户机上的用户在任何时间同时访问系统资源。服务器必须支持多用户，并且要作为一个被多个用户所共享的资源库来运行，因此，服务器需要特别的硬件和软件的支持。

NOS执行一些特别的功能来允许多个用户同时访问共享资源，客户机系统也包含特定的软件，允许它们向服务器请求被服务器控制的共享资源，服务器则响应客户的资源请求。

系统要想运行为NOS 服务器，它必须能同时为多个用户提供服务。网络管理员为每个用户创建一个帐号，允许这些用户连接和登录服务器系统。服务器上的用户帐号使得服务器能够验证用户，并且为这些用户分配系统资源。能够提供这样功能的操作系统称为多用户系统，像UNIX、Linux、Windows NT/Windows 2000/Windows XP都支持多用户功能。

NOS服务器也是一个多任务操作系统。NOS必须能够同时执行多个任务或进程。操作系统是通过嵌入到执行环境的调度软件来完成此功能的。调度软件为不同的任务分配处理器时间、内存和其他系统资源，从而使它们能够共享系统资源。多用户系统服务器为每个登录用户都运行着一系列进程，这些进程当用户登录服务器的时候被建立，当用户注销的时候则被终止。

当选择NOS的时候，主要考虑的因素有性能、管理和监控工具、安全性、可扩展性和健壮性/容错性等方面。下面对这些因素做一个简单的介绍：

1 性能（Performance）

NOS在客户机/服务器通过网络进行文件读写的时候必须性能良好，它必须在许多用户——有可能是数百个用户，同时提交请求的时候维持良好的性能，当用户访问服务器数据库时，它必须负责处理用户的请求，例如，从驻留在本地服务器系统中的数据库提取数据。分析数据，因此，在负载量很大的情况下的持续性能的好坏是衡量NOS的最重要的指标。

2 管理和监控工具（Management and Monitoring Tools）

NOS的管理界面提供了如服务器监控、客户管理、文件和打印管理和磁盘存储管理等工具。它也提供了安装和配置其他新服务的工具，此外，服务器还需要定期的监控和调整。

3 安全（Security）

NOS必须保护在它控制下的共享资源。安全包括对进行访问服务的用户进行身份验证，防止非授权用户访问网络资源；同时也包括对客户机和服务器之间在网络上传输的信息进行加密等保护措施。

4 可扩展性（Scalability）

可扩展性是指NOS能够扩展但又不影响其性能的能力。NOS必须在加入新的用户或加入新的支持NOS的服务器时保持一致的良好性能。

5 健壮性/容错性（Robustness/Fault Tolerance）

衡量健壮性的标准是NOS在高负载的情况下提供一致服务性能的能力和在组件或处理器发生故障时保持服务的能力。使用冗余磁盘设备和在多台服务器之间进行负载均衡能够提高NOS的健壮性。

16.1.5 Window NT、Window 2000和Windows .NET

接下来讨论微软公司（Microsoft）提供的各种NOS，Windows NT工作站系统是Microsoft为企业市场开发的第一个桌面操作系统。Windows NT 4.0版本有着和Windows 95相似的用户界面，它与Windows95不同之处在于，它是为关键任务设计的，因此有着更为可靠的稳定性。

1 Windows 2000操作系统

Windows 2000 Professional是微软公司为企业桌面系统开发的新的操作系统。跟Windwos 2000 Server一样，Windows 2000也是基于NT核心的，并且包含了很多加强特性。例如，Windows 2000 Professional提供了高级别的安全性和执行关键任务的稳定性。

Windows 2000支持即插即用（Plug and play）技术。它能安装在使用FAT32分区格式的磁盘上，并且它还有对机密数据进行文件加密的功能。即插即用技术是一个很有用的工具，它允许管理员快速简单的在系统中加入新的组件，操作系统能够自动识别它们并且为它们安装驱动程序。即插即用的基本含义是：当一个组件被“插入”到系统中，它不需要额外的配置就能使用。在此之前，当你加入一个新的组件时，你不得不自己安装驱动进行配置。Windows 2000本身附带了一个支持通常即插即用设备的庞大驱动库。

Windows 2000 Professional作为一个桌面操作系统和网络客户端的其他优点包括：

- 它通过高级电源管理（APM, advanced power management）和高级配置与电源接口（ACPI, Advanced Configuration and Power Interface）提供了对移动用户的更好支持。Windows NT不支持ACPI。
- 它通过第2层隧道协议（L2TP, Lager 2 Tunneling Protocol）和IP安全协议（IPSec, IP Securing）来支持更安全的虚拟局域网。Windows的早期版本只支持基于点对点隧道协议（PPTP, Pont-to-Point Tunneling Protocol）的VPN。
- 离线文件夹功能使得用户能够从网络上拷贝和同步文档到本地系统，所以即使他们的计算机没有连到网络上的时候，网络数据一样能够被访问。
- 因特网打印协议（IPP, Internet Printing Protocol）使得用户能打印到统一资源定位器（URL）并且通过WEB浏览器来管理打印机。
- 嵌入的磁盘管理器和其他工具能帮助用户维护和管理操作系统，而Windows NT用户必须向第三方购买这些软件。
- 它支持Kerberos安全（为认证网络用户开发的标准）以及将Windows 2000域看作一个活动目录客户端的特性。
- 它提供了更为容易有效的帐号管理。

Windows 2000的管理任务使用一个统一的框架：Microsoft管理控制台（MMC）。这个工具使用一些包含特别管理功能的嵌入式模块来进行管理。用户和组的建立和管理可以用活动目录用户（ADU）和计算机MMC模块。你可以通过选择**“开始”→“管理工具”→“活动目录用户和计算机”**来进入MMC。Windows 2000和Windows NT 4.0不同的是，Windows 2000将用户和资源这些对象放入一些名为组织单元（OU）的容器对象中。每个OU的管理权限可以被授予给一个用户或组，这个特性允许Windows2000提供比Windows NT 4.0更精确的对象控制。

2 Windows 2000和.NET Server操作系统

Windows 2000和.NET Server操作系统包括Windows 2000 Server、Windows 2000 Advanced Server和最新的Windows .NET Server。网络的特定需要决定了你该选择哪个版本的Windows 2000服务器。

Windows 2000 Server

Windows 2000 Server包括很多新的服务器功能，对中小型网络来说，是一个理想的选择。Windows 2000 Server能提供很多服务器功能，如文件、打印和WWW服务以及应用服务器服务。Windows 2000 Server和以前的Microsoft服务器操作系统的区别是：Windows 2000 Server有一套基于活动目录的服务框架。活动目录被完全集成进了Windows 2000 Server，并且为用户、组、安全服务和网络资源的管理提供中心服务。Windows 2000 Server能够支持4路对称多处理器（4-way SMP），能够最大支持4GB物理内存。因为这些原因，Windows 2000 Server非常适合于中小型网络环境。Windows 2000 Server的其他组件还包括对现今网络上流行的协议的支持，如TCP/IP，因特网分组交换（IPX）/序列分组交换（SPX）。

Windows 2000 Advanced Server

Windows 2000 Server和Windows 2000 Advanced Server基本上是一样的，除了Windows 2000 Advanced Server提供了一些系统管理员在管理较大型网络时需要的一些特别的硬件和软件功能。Advanced Server是一个更加强大的、部门级的应用服务器操作系统，它包括了Windows 2000 Server所提供的所有功能，并且增强了较大型网络运行所需要的高可靠性和可扩展性。Windows 2000 Advanced Server支持8路SMP（8-way SMP），这对运行数据库服务应该是个不错的选择。Windows 2000 Advanced Server还提供了*企业级网络*（enterprise network）所需的高端硬件的支持，如Windows 2000 Advanced Server支持超过4GB的物理内存。

Windows .NET Server

Microsoft开发Windows .NET Server的目的是给运行企业级WEB和FTP服务的站点提供更好的安全性和可靠性，并且在这一领域与Linux和UNIX服务器操作系统进行竞争。然而，Windows .NET Server确实提供了一些独特的性能，例如，随着电子商务的高速发展，基于WEB的公司和那些将他们的服务扩展到互连网的公司，需要一种能提供安全可靠的WEB服务和FTP服务的服务器操作系统，Windows .NET Server，尽管其核心是基于Windwos 2000 Server的，却针对这些需要的服务做了量身定制的修改。Windows .NET Server提供了XML Web服务以满足那些WEB服务流量较大的公司的需要。这个特性为：允许公司直接通过他们的服务器运行所有的软件和服务，而终端用户桌面系统仅作为一个“哑终端”通过互连网来使用这些软件和服务，这样更加增强了安全性和可靠性。.NET Server对那些刚刚开始应用新一代电子商务的公司和那些已经稳定运行于因特网的电子商务解决方案公司都提供了统一的支撑平台。

16.1.6 UNIX和Linux

UNIX和Linux服务器操作系统，尽管相似，但也有一些显著的差别。下面介绍一下不同版本的UNIX和Linux的区别以及举例说明它们分别适合什么样的环境。特定的网络需要决定你应该选择哪个最合适的版本。

1 UNIX的起源

UNIX是一组操作系统的名字，它们的起源可以追溯到1969年的贝尔实验室。在它诞生之初，UNIX就是按支持多用户和多任务来进行设计的，UNIX是最早支持因特网协议的操作系统。UNIX的历史，到现今已经有30多年了，因为多个公司和组织对它做出的不同的贡献，因此它的历史变的很复杂。

UNIX最早是用汇编语言编写的，汇编语言是一种控制计算机内部指令的低级语言。因此，UNIX只能在某些特定的计算机上运行。1971年，D.Richie发明了C语言，1973年Ritchie和他的贝尔实验室的同事K.thompson用C语言重写了UNIX，因为C语言是一种高级语言，所以UNIX能非常方便的移植到其他的计算机上。当初他们这个开发方便移植的操作系统的决定，后来被证明是UNIX能

够取得如此成功的关键。在70年代，UNIX因为贝尔实验室和一些大学——特别是加州大学伯克利分校的努力，得到了长足的发展。

UNIX在80年代开始进入商业市场，它主要是运行在高端网络服务器上，而不是桌面计算机。如今，已经有上十种不同的UNIX版本，包括：

- HP-UX（Hewlett Packard的UNIX）。
- BSD UNIX（也被称为FreeBSD）。
- Santa Cruz Operation（SCO）UNIX。
- Sun Solaris。
- AIX（IBM的UNIX）。

一般来说，各种不同版本的UNIX，在那些运行关键任务以及对安全性和可靠性要求非常高的公司和组织中一直占有领先地位。UNIX也和TCP/IP协议紧密连接，实际上TCP/IP协议就是随着UNIX的发展，LAN和广域网（WAN）上的通信需要而发展起来的

SUN公司的Solaris操作环境和它的核心操作系统SunOS是高性能、通用的、64位的UNIX。Solaris广泛运行在各种类型的计算机上，从基于Intel芯片的个人PC到大型主机系统，甚至超大型计算机。Solaris是运行在大型网络和网络站点的最为流行的UNIX版本。SUN公司同时也是“一次书写，随处运行”（“Write Once，Run Anywhere”）的Java技术的开发者。

除了各个公司LAN上主要运行Microsoft Windows操作系统以外，大多数因特网上都运行强大的UNIX系统。尽管UNIX通常和昂贵的硬件联系在一起，以及给人用户界面不友好的印象，但最近的一些发展，包括Linux的开发，已经逐渐在改变人们对UNIX的看法。

2 Linux的起源

1991年，一个名叫Linus Torvalds的芬兰学生在一台基于Intel 80386的计算机上开始了他的操作系统研发工作。考虑到当时桌面操作系统DOS的失败状态以及商业UNIX的昂贵费用及许可证问题，Torvalds决定开发一种“类UNIX”的操作系统，但是这个操作系统的源代码是公开的并且完全免费的。

Torvalds当初没有想到，他一时的决定导致了一场世界范围内的为开发Linux而进行的协作劳动。到了90年代，Linux已经成为在服务器领域取代UNIX以及在桌面领域取代Windows的一种可选方案。Linux在桌面系统上的普及还带动了人们在桌面PC上对其他UNIX的兴趣，如FreeBSD和Sun Solaris。Linux的不同版本几乎能运行在所有的32位处理器上，如Intel 80x86、Motorola 68000、Alpha和PowerPC。

和UNIX一样，Linux也有许多版本。它们中的一些是可以从网页上免费下载的，另外一些通过商业方式进行发布。下面是一些常见的Linux版本：

- RedHat Linux——RedHat软件公司发布。
- SCOLinux——SCO公司发布。
- Xandros Linux。
- Slackware。
- Debian GNU/Linux。
- SuSE Linux。

Linux是当今世界上最为强大，最为稳定的操作系统。正因为如此，Linux已经在企业服务器领域给传统UNIX服务器带来很大的冲击。Linux很少配置成公司的桌面操作系统，尽管图形用户界面（GUI）的引入已经使得Linux具有很好的用户友好性，但是大多数的初用者觉得Linux比MacOS或Windows难用。现在，许多公司（如RedHat、SuSE、SCO和Xandros）正开始努力让Linux成为一个

真正可选的桌面操作系统。

当把Linux作为桌面操作系统运行时，应用程序的支持是必须考虑的。和Windows相比，Linux上的商业应用程序非常有限。然而，一些开发商提供了Windows模拟软件，它们能够让运行在Windows上的程序也能够运行在Linux上。此外，一些公司，如Corel，正在开发运行在Linux上的办公套件和其他常用的软件包。

3 利用Linux连网

最近发布的Linux版本都配置了连接LAN或者拨号接入因特网和远程网络的网络组件。事实上，TCP/IP协议已经集成进了Linux的内核，而不是作为一个单独的子系统来运行。

Linux作为桌面操作系统和网络客户端的优点有：

- 它是一个真正的32位操作系统。
- 它支持抢占式多任务和虚拟内存。
- 它的源代码是公开的，任何人都可以加强和改进。
- Linux在GNU的通用公共许可（GPL）规则下，可以像其他UNIX（如FreeBSD和NetBSD）一样免费使用。Linux是一个开放源代码软件，这意味着源代码可以公开使用，可以根据需要进行修改。这个概念和商业软件是对立的，商业软件的源代码是保密的，并且每个用户必须为使用它支付许可费用。商业软件依靠版权法律来寻求限制用户对源代码的分析和发布，而Linux可以从不同的网站上不需任何费用的下载。

4 Linux的发布

许多赢利性公司和非赢利性组织都将Linux跟许多应用软件和其他一些功能软件绑定在一起进行销售。这种将操作系统和应用软件绑定在一起的方式称为发布。举一个例子，Red Hat公司将Linux CD、源代码、使用手册以及一些应用软件结合在一起销售，而收取非常少的费用，就是发布。这些额外的应用软件包括办公套件、一个可以选择的图形化桌面、WEB服务器软件等。还有一定级别的客户支持。RedHat还包括了SUN StarOffice办公集成软件。

任何发布的主要组件都是Linux内核。除了内核之外，其他的组件包括安装工具、系统引导工具和应用软件。一些发布为了更方便新用户的使用而更加图形化，另外一些发布则是针对有UNIX经验的开发人员的，因而显得更加原始。下面是一些常用的Linux发布和它们的网址：

- SCO OpenLinux——www.sco.com
- Xandros Desktop Linux——www.xandros.com
- Debian GNU/Linux——www.debian.org
- Mandrake Linux——www.mandrakelinux.com
- Red Hat Linux——www.redhat.com
- Slackware Linux——www.slackware.com
- SuSE Linux——www.suse.com
- Turbo Linux——www.turbolinux.com
- United Linux——www.unitedlinux.com

5 Linux/UNIX图形用户界面

UNIX和Linux都能够运行图形用户界面。因为有很多的UNIX和Linux的不同版本，所以至少有上十种不同的流行的图形界面供你选择使用。例如，Red Hat 8.x就缺省安装了GNOME桌面环境，并且将GNOME设置为所有用户的缺省图形用户界面，如图16-9所示。

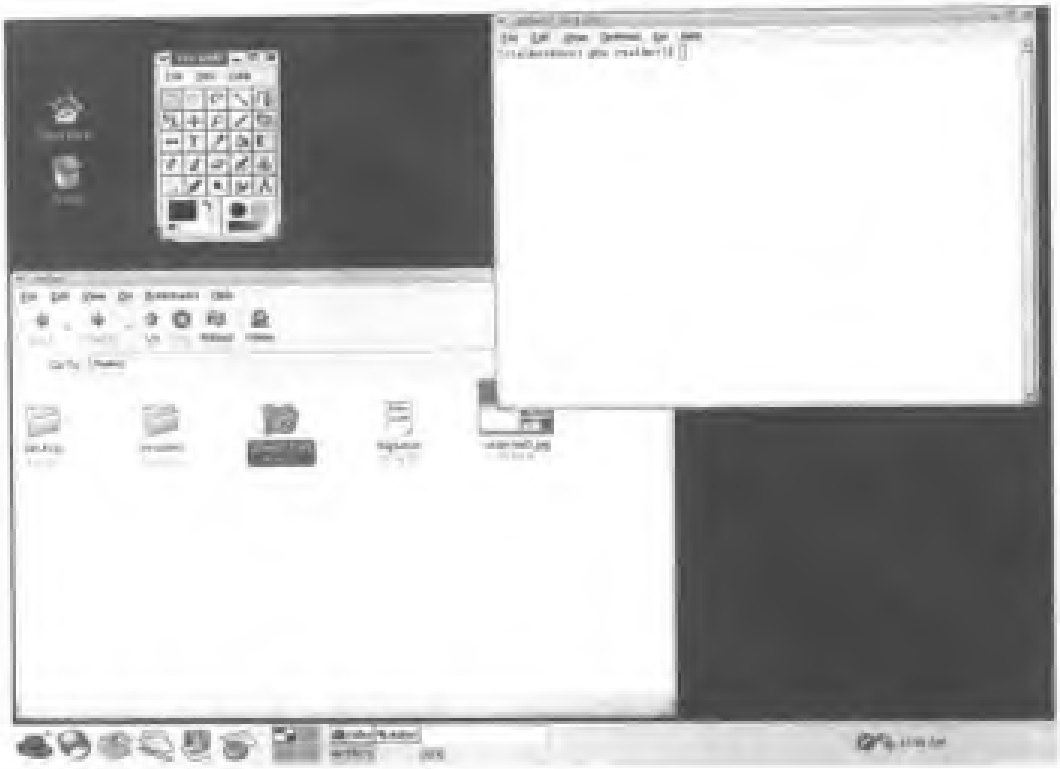


图16-9　Gnome桌面环境

尽管一些其他的桌面环境，如K桌面环境（KDE），如图16-10所示，也能被Linux配置使用，但GNOME迅速得到了业界的承认而成为“标准”的UNIX和Linux图形用户界面。



图16-10　KDE桌面环境

UNIX和Linux都依靠X Window系统来运行图形用户界面。X Window是一个与系统硬件、图形应用和窗口管理等系统一起协同工作的软件。窗口管理是负责管理程序运行的窗口的，如窗口尺寸，

窗口定位以及窗口的绘图工作。

16.1.7 Macintosh OS X

苹果电脑的设计目的是在对等体—对等体（工作组）网络环境下，方便计算机连网。事实上，网络接口作为硬件的一部分和其他网络组件已经集成进了Macintosh操作系统。Macintosh系统中可以使用以太网和令牌环网络适配器。

Macintosh或者Mac，广泛应用于教育领域和企业的图形图像部门。在工作组中，Mac机器能够用网络连接起来，并且能访问AppleShare文件服务器。Mac机器也能够连入包扩Microsoft、NetWare或者UNIX服务器的计算机局域网中。Macintosh操作系统——Mac OS X有时也被称为苹果系统10。

Mac OS X的一些特性存在于名叫Aqua的图形用户界面中，Aqua图形用户界面结合了Mcirosoft Windows XP和Linux图形用户界面的一些特点。Mac OS X被设计为向家庭计算机提供如因特网浏览、视频和照片编辑和游戏等功能。同时，它还向IT专业人员提供强有力的、客户化的工具。

Mac OS X完全兼容于以前老的MAC操作系统，Mac OS X提供了一个新的功能，从而解决了AppleTalk和Windows之间的可连接性。Mac OS X的核心操作系统是被称做“Darwin”的基于UNIX的强大系统，它提供了高稳定性和高性能。Mac OS X在一些功能方面得到了加强，如受保护内存、抢占式多任务、高级内存管理和对称多处理器。这些使得Mac OS X成为操作系统领域一个强有力的竞争者。

16.2 服务器上的服务

NOS被设计为向客户端和对等体提供网络服务。网络服务包括WWW、文件共享、邮件转发、目录服务、远程管理和打印服务等。远程管理是一个很有用的服务，它使得管理员能够在千里之外管理网络系统。值得指出的是，这些网络服务在Windows 2000环境下被称为“服务”，而在UNIX和Linux环境下被称为“后台进程”。它们的基本功能是一样的，但是在不同的操作系统下，它们被载入执行的方式以及和NOS的交互是不同的。

对一些NOS来说，这些关键的网络服务可能在缺省安装的时候就启动了。大多数的网络进程都依靠于TCP/IP协议分组。因为TCP/IP是公开的、众所周知的协议，所以基于TCP/IP的服务有可能会受到非法扫描和恶意攻击。拒绝服务（DoS, Denial-of-Service）攻击、计算机病毒以及快速传播的因特网蠕虫（Worms）病毒使得NOS的设计者们必须重新考虑应该自动运行哪些网络服务。

一些现在流行的NOS的最新版本，如Windows 2000，Red Hat Linux 8.X对自动运行的网络服务作出了限制。当配置一个NOS时，关键的网络服务必须要手动启动。

当用户准备在一个网络打印环境中打印时，打印任务被送到指定打印机的打印队列。打印队列接收打印任务，并对它们进行先进先出（FIFO）的服务。这就是说，当一个打印任务被加到队列中时，它被放置在等待打印的任务的最后面，等所有前面的任务完成之后，它才被打印。打印任务的等待时间长短，决定于在它之前打印任务的多少。网络打印服务提供给网络管理员一些必要的工具，使网络管理员可对在网络上传送的大量打印作业进行管理，这些工具包括给打印任务指定优先级、暂停打印任务甚至删除打印任务。

16.2.1 文件共享

通过网络共享文件是一项重要的网络服务。如今，有很多种文件共享协议和应用正在使用。在一个公司或者家庭网络环境下，文件共享一般通过Windows文件共享协议或网络文件共享（NFS）协议来实现。在这样的环境下，终端用户有可能不知道一个给定的文件到底是在本地还是在远程服

务器。Windows文件共享协议或网络文件共享协议使得用户能够方便的在远程目录中移动、创建和删除文件。

16.2.2 FTP和文件传输

许多公司通过FTP来让远程的员工、客户和普通公众来进行文件访问。FTP服务与WEB服务一起开放，可以使FTP服务更加有效。例如，用户可以浏览一个站点，在网页上看到有关一个软件更新的通知，然后使用FTP来下载那个软件。规模小的公司可以用一台服务器来同时提供FTP和HTTP服务，规模大的公司可能需要专门的FTP服务器。

尽管FTP客户必须登录，但很多FTP服务器都被配置成允许匿名登录。当用户匿名访问FTP服务器的时候，他们不需要在系统上拥有账号。FTP协议允许用户上载、更名和删除文件，所以管理员必须很小心的配置FTP服务器以控制访问级别。

FTP是面向连接的协议。客户必须和服务器打开一个应用层的会话、验证然后执行下载或上载。如果客户会话处于一定时间长度的非激活状态，服务器就会断开这个连接。这个非激活时间称为闲置时间，FTP的闲置时间长度因为软件的不同而不同。

16.2.3 Web服务

World Wide Web（WWW）服务是网络上最常见的服务类型。最近10年来，WWW已经成为一个全球化的信息、商业、教育和娱乐的网络方式。上百万的公司、组织还有个人将他们的网站放到因特网上。网站是指存储在一台服务器或一个服务器群上的网页的总称。

WWW是基于客户机/服务器模型的。客户必须和服务器建立一个TCP会话。在这个会话建立之后，客户才能向服务器请求数据。HTTP用来管理客户的请求和服务器的传输。Web服务已经发展到不仅仅只将HTML文件传输给Web浏览器供用户浏览，而且可以产生XML脚本来供用户的计算机使用。前面在讨论Microsoft .NET Server的时候已经提到过服务器怎样让XML和Web服务协同工作。Web客户软件有基于图形用户界面的 Web浏览器，如Netscape Navigator和Internet Explorer（IE）。

网页存放在提供Web服务的计算机上。两种最常见的Web服务器是Microsoft的因特网信息服务器（IIS）和Apache Web服务器。前者只能运行在Windows平台上，而后者则通常可以运行在UNIX和Linux平台上。其他还有上十种可供使用Web服务器，并且还在开发一些适合于通用操作系统平台的Web服务器。

16.2.4 DNS

DNS将因特网名字（如www.cisco.com）解析为IP地址。许多应用程序都依靠DNS服务来完成它们的工作，如Web浏览、电子邮件程序和文件传输程序都使用远程系统的名字，所以需要DNS服务。DNS协议允许客户端应用程序向DNS服务器请求将这些名字转化为IP地址，如果转换成功了，这些应用程序就可以用这些地址来发送信息。如果没有DNS的名字解析服务，因特网几乎不可能被正常使用。

16.2.5 DHCP

DHCP的目的是让IP网络上的单台计算机能够从一台或多台DHCP服务器上得到它们的TCP/IP配置信息，它的真正目的是减少管理员在管理大型网络时的工作量。通过DHCP来发布的配置信息中，最重要的是主机在网络上的标志——IP地址。DHCP也可以通过租约的形式来恢复或自动更新客户的IP地址。这个机制是给客户分配一个一段时间内可以使用的IP地址，到租约期满则释放它，

然后再分配一个新的IP地址。DHCP允许DHCP服务器完成这些工作，从而减少了网络管理员很大的工作量。

16.3 网络管理

随着网络的发展成长，它渐渐成为了一个组织（公司）的关键的、不可或缺的资源，如图16-11所示。然而，随着网络提供给用户的资源越来越多，它的复杂程度就会变得越来越高，网络出错的机会就会越来越多。但是，让网络半死不活的运行着，提供非常少的资源，对用户来说显然是不可接受的。因此，网络管理员必须积极主动的管理网络、诊断问题、防患于未然，给用户提供最好的网络性能。在某种意义上说，如果没有切实可行的网络管理，网络将会变得无法运行。

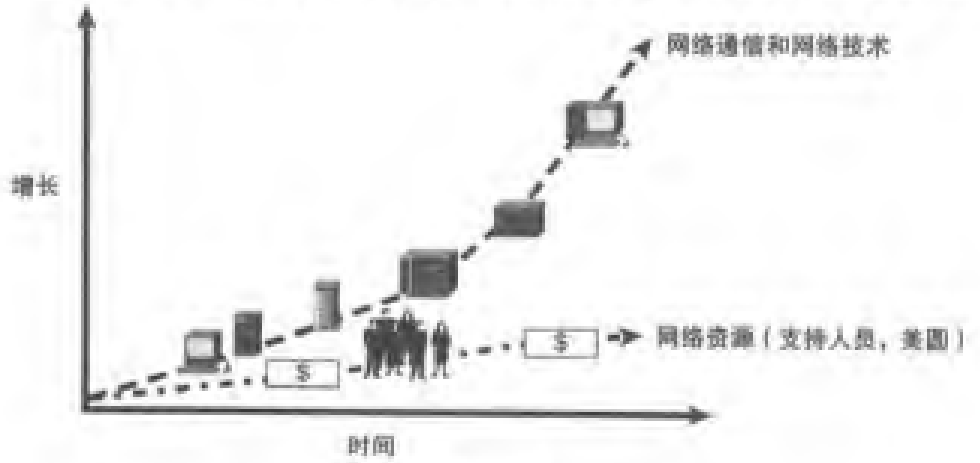


图16-11 网络发展

网络管理包括下面一些内容：

- 网络可用性监控。
- 更多的自动化程序。
- 响应时间监控。
- 安全功能。
- 通信重路由选择。
- 错误恢复能力。
- 用户登记。

加强网络管理的推动力如下：

- **控制企业资产**——没有切实有效的网络资源控制，网络资源将不会给管理者带来所期望的回报。
- **控制复杂性**——随着网络产品、网络用户、网络界面、网络协议和网络设备厂商的大幅度增长，管理者对网络和网络资源的失控倍感担心。
- **改进服务**——随着网络的增长，更多的网络资源被发布，用户希望能享受更好的服务。
- **平衡各种需求**——必须给用户提供具有服务支持级别的不同应用服务，并且要在服务性能、服务可行性和安全等领域权衡考虑。
- **减少当机时间**——要通过冗余设计来确保资源的高可靠性。
- **控制成本**——监控网络资源的使用率，可以用较经济的成本满足用户的需求。

16.3.1 OSI和网络管理模型

对OSI的网络管理模型作一个较深入的分析是很有必要的。国际标准化组织（ISO）成立了一个

委员会，提出了一个在开放系统互连（OSI）管理之下的网络管理模型。

这个模型由4个部分组成：

- 组织（Organization）。
- 信息（Information）。
- 通信（Communication）。
- 功能（Functional）。

下面是被OSI标准采纳了的网络管理模型，它由上至下被分为4个子模块，如图16-12所示。

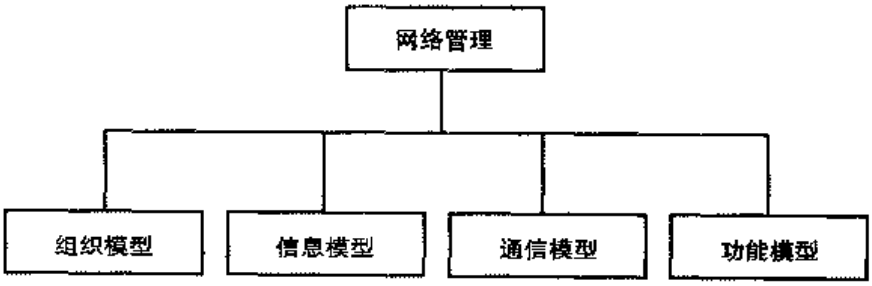


图16-12　网络管理模型

组织模型描述了网络管理的组件（管理者、代理等）以及它们之间的关系。这些组件的不同安排导致了不同的网络管理体系结构，这将在后面说明。

信息模型主要考虑网络对象里管理信息的结构和存储。管理信息存储在一个数据库中，称为管理信息库（MIB, Management Information Base）。网络管理的工业标准着重于管理信息结构（SMI, Structure of Managemet Information），并且定义了存储在MIB中的管理信息的语法语义。MIB和SMI将会在后面的章节中着重讲述。

通信模型负责管理代理和管理员进程之间的数据如何通信的问题。它考虑传输协议、应用协议和对等体之间的命令与响应。

功能模型着重于基于网络管理系统（NMS, network management System）上的网络管理程序。OSI的网络管理模型将功能模型分为5部分（有时被称为FCAPS模型）：

- 错误管理（Fault）。
- 配置管理（Configuration）。
- 记帐管理（Accounting）。
- 性能管理（Performance）。
- 安全管理（Security）。

这样的网络管理模型，描述了大多数网络管理系统所需要的一般内容，因此在世界范围内被大多数厂商所认可。

16.3.2　标准：SNMP和CMIP

为了实现跨网络平台的管理，就需要建立一个网络管理标准，从而厂商能够遵循这些标准生产自己的设备。已经出台了两个标准：

- SNMP——IETE社区。
- 通用管理信息协议（*CMIP*）——电信社区。

SNMP实际上是关于网络管理的一系列标准，包括一种协议、一个数据库结构说明和一系列数据对象。1989年，SNMP作为TCP/IP协议的一个标准被正式采用后，应用越来越普遍。它的升级版本，SNMP版本2（SNMPv2）于1993年通过，SNMPv2能提供集中式、分布式的网络管理机制，并且在SMI、协议操作、管理结构和安全方面作了改进，它还既能运行于基于TCP/IP协议的网络上，

又能运行在基于OSI模型的网络上。不久，SNMPv3发布了，SNMPv3通过管理用户认证和对网络上的分组进行加密实现了对MIB的安全访问和传输，从而解决了SNMPv1和SNMPv2在安全方面存在的缺点。CIMP是由ISO创建的并对分层网络结构进行监控的标准化网络管理协议。

16.3.3 SNMP操作

SNMP是一个应用层的协议，它的设计目的是使网络设备之间的管理信息交互更加方便。通过SNMP来访问每秒钟在接口或多条开放TCP连接上传送的管理信息数据分组，网络管理员能够更加容易的管理网络性能和解决网络问题。

如今，SNMP是对各种各样的商业、大学和科研网络进行管理时用得最普遍的协议。尽管不同的厂商不断开发出了各种不同的基于SNMP的精妙绝伦的网络管理程序，但就SNMP协议而言，它的标准化进程却从未停止过。事实上，SNMP是一个相对简单的协议，但它的特性集却非常强大。足够处理分层网络中出现的层出不穷的困难问题。

基于SNMP的网络管理组织结构包括下面4个组成部分：

- 管理工作站（Managemet Station）。
- 管理代理（Managemet agent）。
- MIB。
- 网络管理协议（Network Managemet Protocol）。

NMS一般而言是一台单独的工作站，但它也能在多个系统上实现。NMS包括一组被称为网络管理应用的软件。网络管理应用包括一个图形用户界面来允许授权的网络管理员管理网络。它对管理员的命令作出响应并把这些命令通过网络提交到管理代理。管理代理是网络设备的关键部分。配置了SNMP协议的主机、路由器、网桥和集线器可以通过代理来被管理。代理对来自NMS的信息请求作出响应［轮询（Polling）］，并且还主动向NMS提交重要信息报告［自陷（trap）］。代理的所有管理信息都存放在它的MIB中。代理应该跟踪下面这些信息：

- 设备的虚电路的数目和状态。
- 代理收到的各种报错消息。
- 设备接收到和发送的分组数目和字节数目。
- 最大输出队列长度（对路由器和其他网络互连设备）。
- 接收到和发送的广播数。
- 网络接口的激活和失效。

NMS通过从MIB获得管理数据来执行监控功能。NMS能设置代理对某种情况作出反应，还能更改代理的配置。管理者和代理之间的通信通过应用层的管理协议来实现。SNMP协议运行在UDP协议的161/162端口，协议的实现是通过下面3种消息交换来完成的：

- Get——管理工作站获取管理代理的MIB对象中的值。
- Set——管理工作站设置管理代理的MIB对象中的值。
- Trap——管理代理向管理工作站报告重要事件。

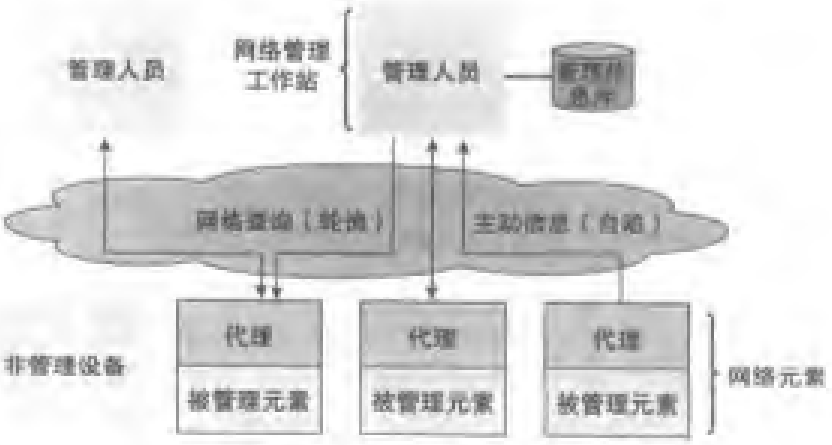


图16-13 组织模型的组成部分

这种模型一般是一个2层结构，

如图16-13所示。这种2层结构模型的前提是假设所有的网络元素都支持SNMP协议。某些情况下，有一些设备可能有着特有的管理界面，这时就需要一个3层结构模型了，如图16-14所示。网络管理员需要和一台网络管理代理服务器进行通信，才能对一个运行特有管理协议的网络节点进行管理。网络管理代理服务器将来自管理员的SNMP请求转化为目的系统能够理解的特有网络管理协议，然后又将目的系统的特有协议响应转换为标准的SNMP消息回送给管理员。

另外一种网络管理应用是将网络管理的部分功能转移到一个称为远程监控（RMON）的探针上去，让它来收集本地管理信息，然后管理员再周期性的获取它收集到的信息。

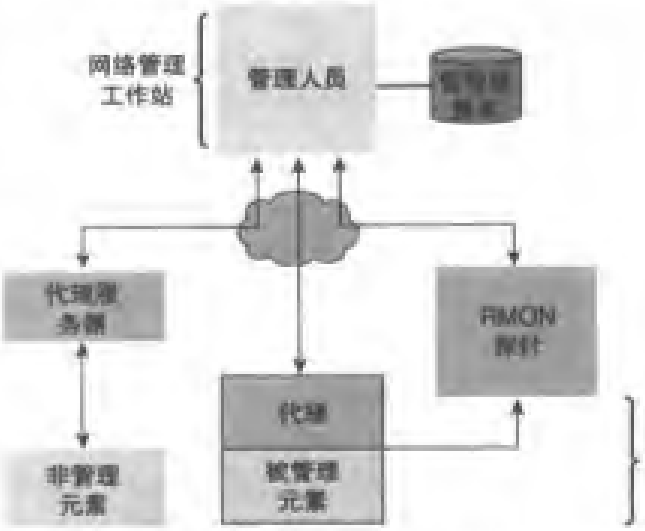


图16-14　组织模型的组成部分

NMS是一台运行某种操作系统的普通工作站，如图16-15所示。它通常有很大的RAM，允许多个管理程序同时运行。NMS一般运行典型的网络协议，如TCP/IP。决定使用何种网络管理应用程序应依靠主机操作系统和通信结构。常用的网络管理应用程序有CiscoWorks 2000、HP OpenView和SNMPc。



图16-15　组织模型

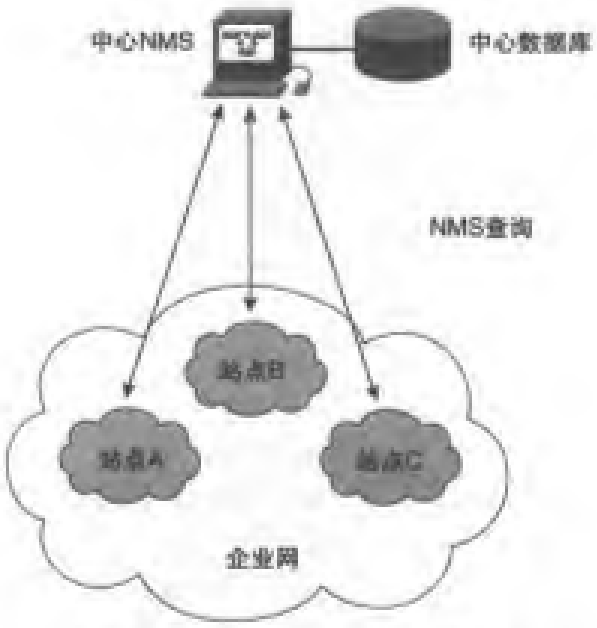


图16-16　中心化的网络管理结构

如前面所述，管理站可能是一台独立的、中心化的工作站，向所有的代理——不管它们的位置在什么地方发送信息请求，如图16-16所示。但在分布式网络中，每台站点一个NMS的分散化结构也许更合适。这些分布式的NMS能作为客户机/服务器的结构来运行，其中一个NMS作为主服务器，其他的作为客户机，客户机将它们的数据传送到主服务器来进行中心端存储，如图16-17所示。另外一个可选的方案是，分布式的NMS有着平等的地位，每一个都有自己的数据库，因此管理信息分布在这些对等的NMS上，如图16-18所示。

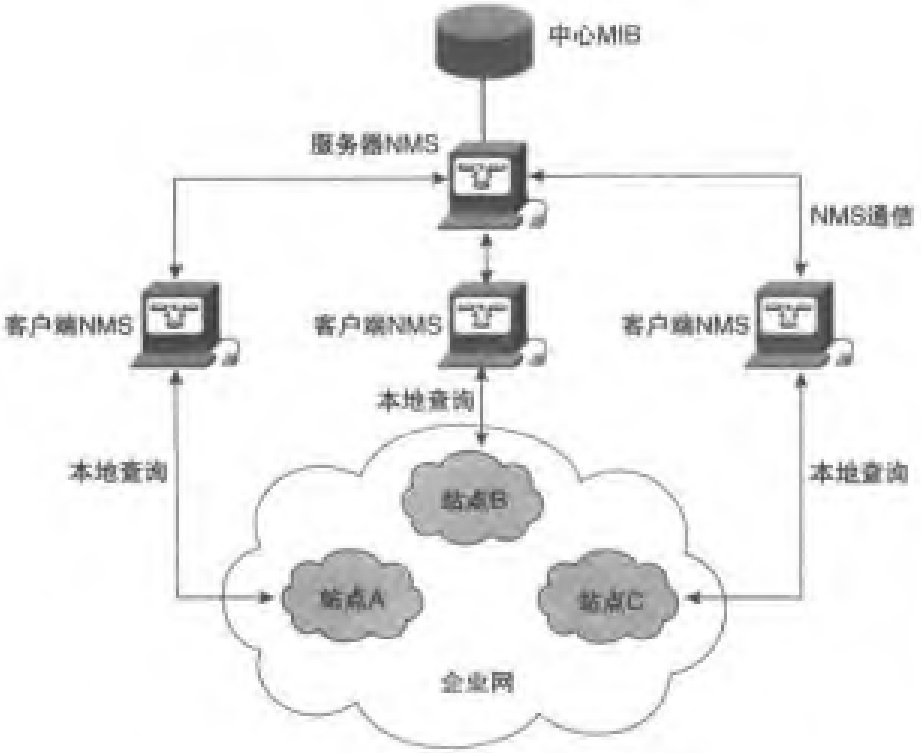


图16-17 分层的网络管理结构

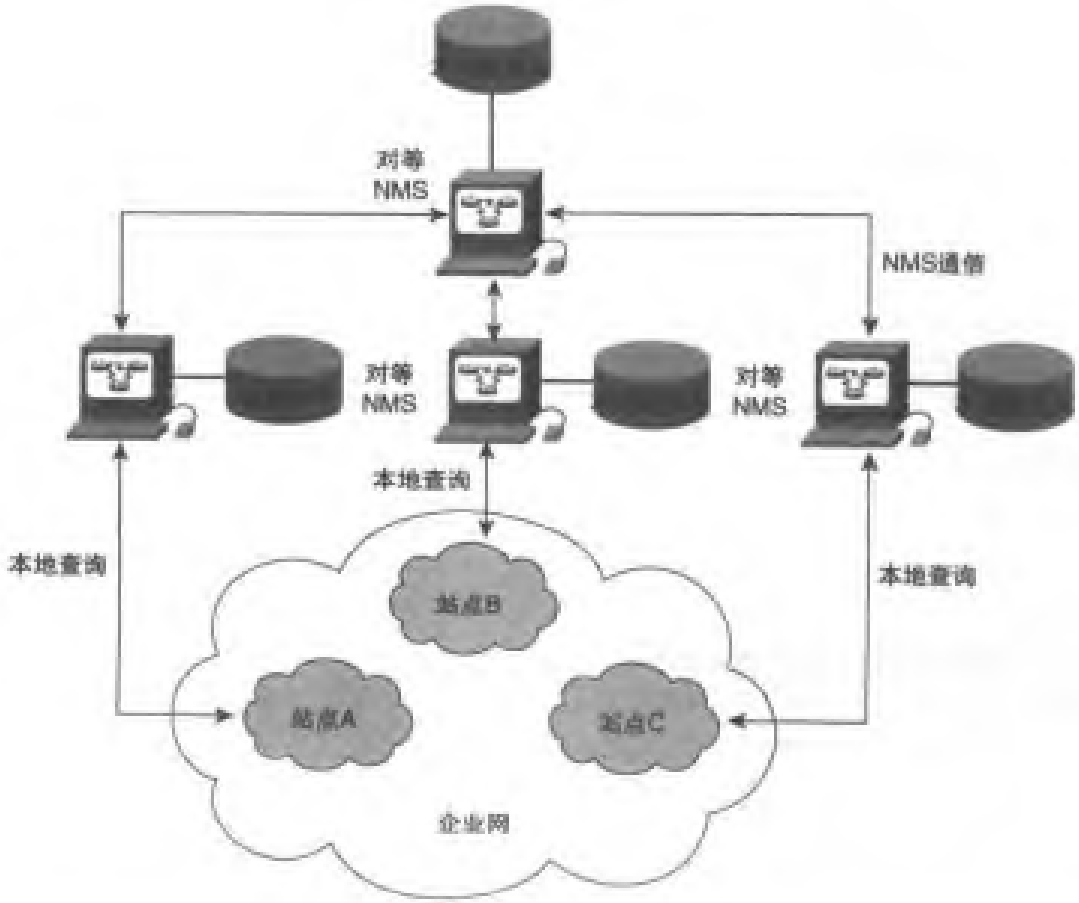


图16-18 分布式网络管理结构

16.3.4　管理信息和MIB结构

MIB是用来存储网络元素及他们属性的结构化信息的。MIB的结构是由SMI定义的，SMI还定义了用来存储对象的数据类型、对象是如何命名以及如何编码以在网络上传输。

MIB以非常好的结构体系来存放设备的管理信息。已经有许多标准的MIB了，但还有更多的专有MIB来分别管理不同厂商的设备。最初的SMI MIB被分为8个不同的组，总共114个被管理对象，正在取代MIB-I的MIB-II中加入了更多的组和对象。

SNMP环境中的所有被管理对象被安排进一个分层或树状结构中，如图16-19所示。树的叶对象是正在被管理的对象，每一个都代表着设备的某个资源、活动和相关管理信息。每一个对象都由一个惟一的对象标志符标志，标志符是用点符号分隔的经过SMI树的数字来表示的。每一个对象标志都定义在ASN.1（抽要语法符号）中。



图16-19　对象标志符

SNMP使用这些对象标志符来标识它们要获取或修改的MIB变量。公共范围内的对象由RFC来定义。人们鼓励厂商们将它们的专有MIB公共化，当他们得到一个被分配的SMI树值时，他们有责任去创建和维护其下的子树。

16.3.5　SNMP协议

代理是嵌入到大多数网络设备中一个软件，这些网络设备包括路由器、交换机、集线器、打印机和服务器等，如图16-20所示。代理负责处理来自管理员的SNMP请求，它也负责维护它所支持的MIB中的对象变量。

管理员和代理之间的交互由“请求和回答协议（question and answer protocol）”，也就是SNMP来完成。“简单（Simple）”一词来自于协议建立之初，只定义了非常少的消息类型。它的设计思想是让设备生产者将管理功能非常容易的加入到他们生产的网络设备中去。这个最初的协议规范称为SNMPv1（版本1）。

SNMP的3种消息类型是NMS发起的：“GetRequest”、“GetNextRequest”和“SetRequest”，如图16-21所示。代理以“GetRequest”这种消息形式确认以上三种消息。另外，当代理遇到影响MIB的底层资源的事件时，会发出诱捕信息。

针对SNMPv1的局限性立即进行了SNMPv2c（版本2c）的开发，SNMPv2c显著的优点是引入了

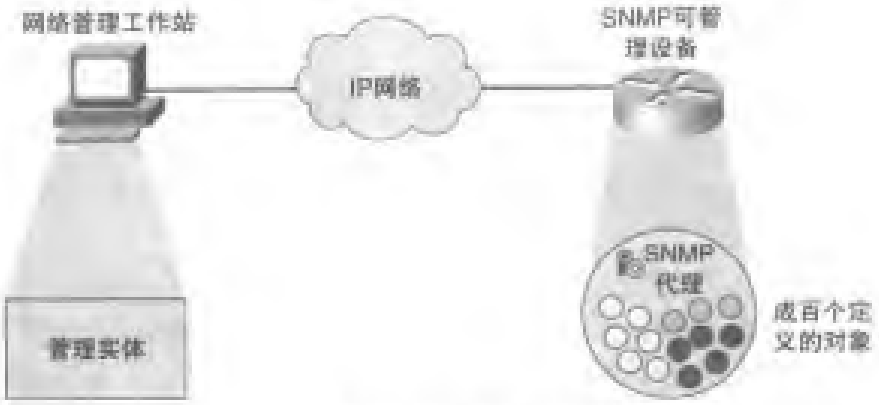


图16-20 对象标志符



图16-21 对象标志符

"Get Bulk"消息类型和总共64位的计数器。"GetRequest"和"GetNextRequest"在从MIB呈表格状结构的设备中获取信息时效率不高，因为它每次只能请求一个变量。"GetBulk Request"针对这个缺点作了修改，它能用一个请求获得一"块"信息。此外，MIB的64bit的计数器弥补了原先计数器在吉比特以太网这样的高速链路上很快就溢出的问题。

管理实体也被称为管理员或NMS，如图16-22所示。它负责向代理发出请求信息，然后通过不同的形式来处理从代理那获得的信息。它可以形成记录以便今后分析、可以通过图像形式显示出来或者跟预先设置好的值进行比较，看是否超过某个阈值，以便决定采取下一步的行动。

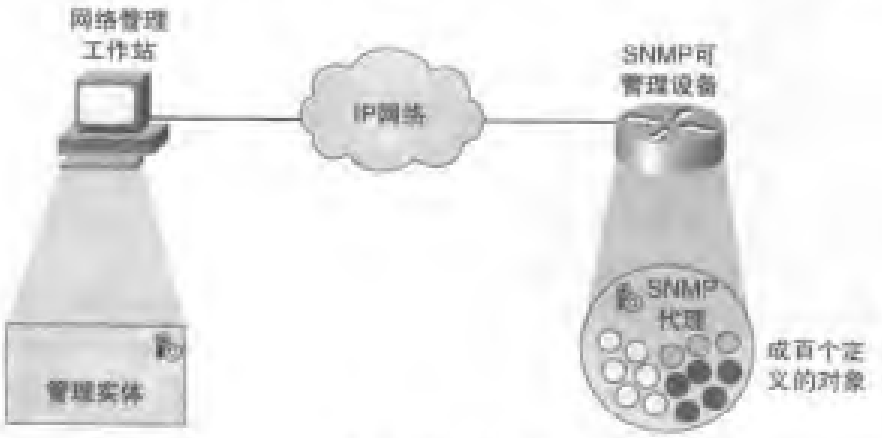


图16-22 对象标志符

管理功能不只局限于获得管理数据，它也有改变被管理设备上的数据的能力，这就可以通过改变被管理设备的配置来控制被管理设备。

管理员和被管理设备之间的交互给网络带来了额外的流量，所以当你决定在网络上进行网络管理时需要小心处理。具有攻击性的监控策略可能影响网络性能。在WAN环境下，带宽的利用率更是需要注意的问题。另外一个要考虑的问题是被监的设备——它必须处理管理员请求，并且这种处理不应影响它自己的正常服务。

一个好的设计原则应该是用尽可能小的频度去获取尽可能少的信息。因此，你需要决定哪些设备和*链路*是最关键的，因而需要被很好的监控以及这些关键设备上关键的管理数据又是什么。

SNMP用用户数据报协议（UDP）来作为传输协议。因为UDP是一种不可靠的传输协议，所以，SNMP可能会丢失信息。SNMP不能保证数据传输的可靠性，因此，使用SNMP的上层应用程序应该负责处理协议数据单元（PDU）的丢失。

每一个SNMP消息都包括一个社区串（community string）——跟密码一样，以限制对被管理设备的访问，如图16-23所示。尽管这个想法是好的，但是因为团体字符串是明文的，所以安全性成了一个问题。现在，SNMPv3（版本3）在安全方面取得了更大的成功。

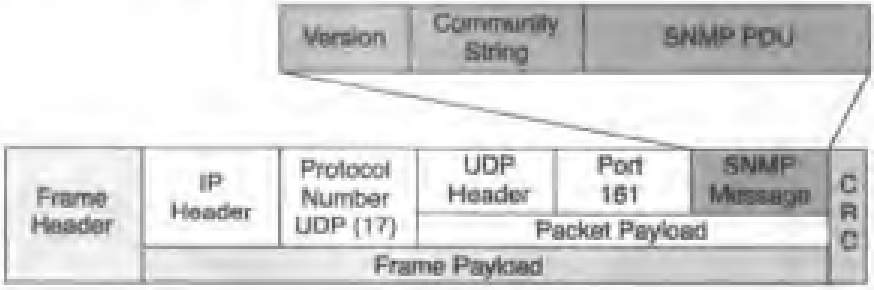


图16-23　对象标志符

SNMPv2消息格式如图16-24所示。有关协议的详细信息，请参看RFC 1157。

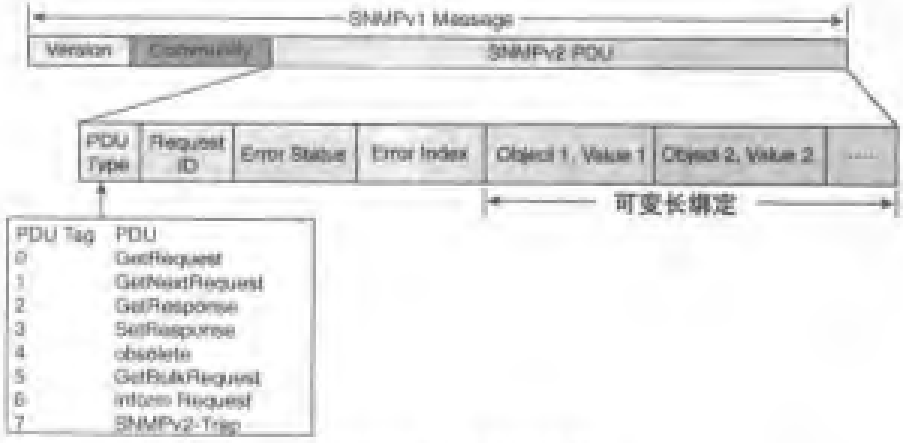


图16-24　对象标志符

团体字符串采用明文方式！这对那些学习过IP协议族的人来说，应该不会引起太多的惊讶。IP协议族的所有协议，除了涉及安全验证和加密以外的，都是明文显示的。

在SNMPv2工作组能够批准新的安全机制以前，团体字符串一直是作为基本的安全策略来运行的，这种在安全机制方面的努力随后被延续到SNMPv3工作组中。正因为要考虑网络管理安全因素，所以，所有基于SNMP的管理应用都需要配置合适的团体字符串。此外，一些组织还经常改变他们的团体字符串值，以减少SNMP非授权用户恶意攻击的风险。

尽管有着基于团体字符串认证的缺点，还是有很多管理应用是基于SNMPv1的。Cisco设备支持

SNMPv3消息类型，因此提升了安全性，但更多的管理软件不支持SNMPv3，如图16-25所示。

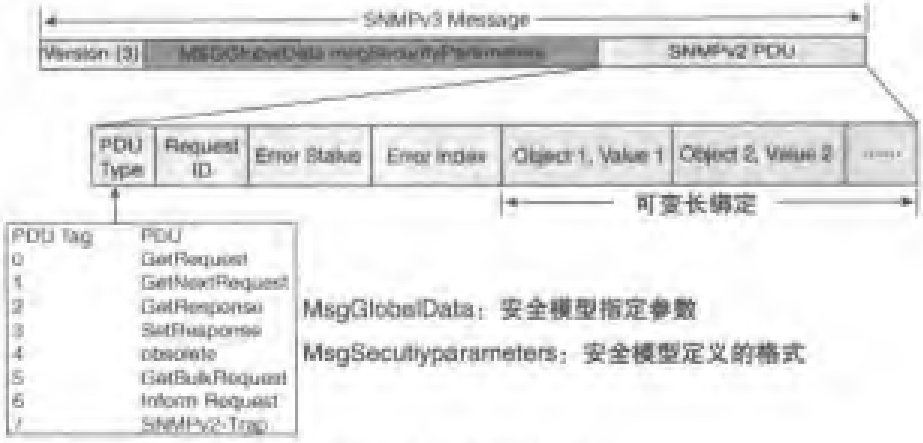


图16-25 配置SNMP

16.3.6 配置SNMP

为了能让NMS和网络设备进行通信，必须在网络设备上启动SNMP，并且配置合适的SNMP团体字符串。下面是对配置这些设备的命令行语法的概述。

Cisco设备可支持多个只读字符串。在大多数系统上，默认只读字符串是public。在企业网络中使用这样的默认值是很不明智的。用下面的命令来给代理设置一个只读团体字符串：

```
Router(config)#snmp-server community string ro
```

*String*就是跟口令一样的，允许访问SNMP协议的团体字符串。

ro（可选）指定了只读访问。授权的管理工作站只能获得MIB对象数据。

Cisco设备也支持多个读/写字符串，所有的SNMP对象都可以被写访问。在大多数系统上，默认的写字符串是private。管理员不应该在企业网络下使用这个默认值。用下面的命令来给代理设置一个读/写团体字符串：

```
Router(config)#snmp-server community string rw
```

rw（可选）指定了读/写访问。授权的管理工作站能获得和修改MIB对象数据。

还可以设置一些参数，如被管理设备所在的位置和主要联系人等：

```
Router(config)#snmp-server location text
Router(config)#snmp-server contack text
```

*text*是描述系统位置的字符串，这些值存放在SysLocation和SysContact MIB对象中。

16.3.7 RMON

RMON的出现是互连网管理方面的一大进步。它定义了一个叫RMON的MIB来补充MIB-II，并且向管理员提供有关网络的至关重要的信息。RMON的特点是：尽管它只是一个简单的MIB规范，没有对承载它的SNMP协议做任何修改，但它却极大的增强了SNMP的功能。

网络管理员能够借助MIB-II来获得单台设备的纯本地信息。考虑一个接入多台设备的LAN，每个设备上都有一个SNMP代理，SNMP管理员能够根据MIB-II得到每台设备接收和发送的数据流量总数，但是仅仅依靠MIB-II，还不能很容易的得到将LAN作为一个整体看待时它上面的流量。为了对这种互连的网络环境进行管理，一般情况下，每个子网都需要一个监控器。

RMON标准最早是IETF RFC 1271定义的（现在被RFC 1757取代），它的设计目的是对基于LAN的分布式网络进行主动监控和诊断。关键网段上的监控设备，称为代理或探针，分析网段上的每个帧来产生用户定义的报警信息和大量的重要统计数据。

RMON标准将监控功能分为了支持以太网拓扑的9个组，后来在RFC 1513加入了支持令牌环特性的第10个组。RMON标准也是按照分布式计算结构设计的，代理或探针通过SNMP与中心的管理工作站（客户）进行通信。这些代理已经在SNMP MIB结构中定义了所有的9类/10类（以太网/令牌环）RMON组，并且提供了不同厂商的基于RMON的诊断工具之间的互操作性。RMON的组包括：

- **统计组**（*Statistics group*）——记录被监控子网/网段的带宽利用率和错误统计数据。（例如，统计带宽利用率、广播包、多播包、CRC错误包和碎片包的数量等）。
- **历史组**（*History group*）——从统计组中周期性的获得统计样本以供今后分析。（如带宽利用率、错误数和包数等）。
- **报警组**（*Alarm group*）——允许管理员为代理记录的任何项目设置一个取样频率和阈值（如绝对值或相对值、上升阈值或下降阈值），当统计值超过阈值后，可以触发报警事件。
- **主机组**（*Host group*）——定义接入网络的某台主机接收或发送的各种分组类型的流量值。（如接收到的或发送的分组数、字节数、错误分组数、广播分组数和组播分组数）。
- **最前列（TopN）主机组**（*Host TopN group*）——提供一个基于主机组统计数据的最前面的N个主机的报告。
- **通信矩阵组**（*Traffic matrix group*）——保存网络上的每对通信节点间的通信错误和带宽利用率。（包括错误数、字节数和分组数）。
- **过滤组**（*Filter group*）——从帧中产生符合用户定义模式的分组流。
- **包捕获组**（*Packet capture group*）——定义怎样将满足过滤模式的包存储在内部缓冲区。
- **事件组**（*Event group*）——将事件记录（产生的trap信息）——连同事件产生的时间和日期，发送给管理员（如根据报警的类型而产生定制化的报告）。

16.3.8　系统日志（Syslog）

Cisco的系统记录功能是基于UNIX的系统记录功能的。系统信息一般都会显示到系统控制台——如果这个功能没有被取消的话。系统记录功能是指应用程序或进程以及Cisco设备的操作系统报告系统可用性和错误信息的机制。Cisco设备使用Syslog协议将这些信息主动发往网络管理工作站。

每个sylsog消息都包括它被记录的时间（时间标记）、功能、严重级别和记录消息文本。有些时候，这些消息是管理员查明设备为什么会发生错误的惟一方法。

严重级别表明了错误消息的危险状况，如图16-26所示。总共有8个严重级别（0—7），0表示最



安全级别	描述
0	Emergencies
1	Alerts
2	Critical
3	Errors
4	Warnings
5	Notifications
6	Informational
7	Debugging

图16-26　系统记录工具

为严重的错误，7最轻，这些级别是：

0——严重紧急（Emergencies）。

1——告警（Alerts）。

2——危急（Critical）。

3——错误（Errors）。

4——警告（Warnings）。

5——通知（Notifications）。

6——信息（Informational）。

7——调试（Debugging）。

功能（facility）和严重级别是用来进行消息处理的。Local 0到Local 7是提供给客户记录消息处理而使用的功能类型。Cisco IOS的缺省严重级别是6，这可以通过配置来更改。

为了能让NMS接收和记录设备的系统消息，必须要对设备进行配置。以下是进行这些配置的命令行句法：

启动记录进程，将记录发送到所有支持的目的地，用如下命令：

```
Router(config)#logging on
```

把记录消息送到syslog服务器主机，如CiscoWorks 2000，用下面的命令：

```
Router(config)#logging hostname | ip address
```

将严重级别设为级别6（informational），用下面的命令：

```
Router(config)#logging trap informational
```

将时间标记包含在syslog消息中，用下面的命令：

```
Router(config)#service timestamps log datetime
```

16.4 总结

这一章包括了以下的主要内容：

- 工作站和服务器的主要功能。
- 客户机/服务器环境中不同设备的功能。
- NOS的发展。
- 各种Windows平台的概述。
- 一些能够取代Windows操作系统的平台的概述。
- 识别网络管理的原因。
- OSI的分层结构和网络管理模型。
- 网络管理工具类型和应用。
- SNMP和CMIP在网络管理中的功能。
- 管理软件怎样收集信息和记录问题。
- 怎样收集关于网络性能的报告。

作为本章所学习内容的补充，请参考本书所附光盘中关于本章的视频、插图和e-Lab实验。

16.5 关键术语

电路（*circuit*） 两个或多个网络节点之间的通信路径。

企业网（*enterprise network*） 一个公司、办事处、学校和其他组织的网络环境以及与它相联系的数据、通信、计算和文件服务器的总称。

帧中继（*Frame Relay*） 一个符合工业标准的数据链路层协议，它采用HDLC封装把多台设备用虚电路的方式连接起来。帧中继比X.25效率更高，并且通常被认为是X.25协议的替代者。

链路（*link*） 由电路或传输通道以及发送者和接收者之间的所有设备组成的网络通信信道。链路通常指的是WAN连接，它有时候又被称做线路或传输线路。

16.6 复习题

1. 网络的基准性能（baseline）是用来衡量网络的什么方面的？
   A. 安全
   B. 设计
   C. 结构
   D. 性能
2. 对等体—对等体网络在终端之间建立起了何种关系？
   A. 客户机—客户机
   B. 客户机—服务器
   C. 服务器—服务器
   D. 服务器—因特网
3. Window NT为了安全目的采用了什么文件系统？
   A. FAT 16
   B. FAT 32
   C. NTFS
   D. NFS
4. 在客户机/服务器网络中，一个用户能够访问某些文件、不能访问另外一些文件。这是用户的什么属性？
   A. 访问
   B. 权限
   C. 能力
   D. 安全性
5. 内部环路IP地址是什么？
   A. 10.10.10.1
   B. 255.255.255.0
   C. 127.0.0.1
   D. 192.0.0.1
6. 防止静电损害的方法有哪种？
   A. 当你在计算机上工作时，关闭电源
   B. 带橡胶手套来绝缘设备
   C. 使用塑料工具
   D. 使用接地腕套
7. 哪种协议支持网络管理？
   A. SMTP
   B. NFS
   C. SNMP
   D. FTP
   E. IPX
8. 列出你的Windows NT计算机上的IP配置。你应该使用什么命令？
   A. ip
   B. ipconfig
   C. winipcfg

D. show ip
E. config

9. 下面哪种是用来进行网络故障排除的方法？
A. 环地址显示
B. 分块征服
C. ping测试
D. Trace错误
E. 重起服务器

10. 如果服务器被设置为使用IP协议，那么客户机必须使用哪种协议和它进行通信？
A. IPX
B. UDP
C. IP
D. Telnet
E. HTTP

11. RMON是哪种协议的扩展？
A. SNMP
B. UDP
C. IPX
D. PING
E. SMTP

12. ping命令中-n选项表示什么？
A. ping区域的网络号
B. 不重复选项
C. ping的次数
D. 不要停止，除非中断
E. 没用

13. RMON中，远程数据是怎样被收集到的？
A. 命令
B. 表
C. 列
D. 探针
E. 用户的交互

14. 对于关键应用业务，_____设备的成本需要加入到网络维护成本中去？
A. 冗余
B. 昂贵
C. 机械
D. 安全
E. 焊接

第四部分 CCNA：额外资料

第17章 光网络基本原理
第18章 网络管理
第19章 Network+认证考试复习
第20章 CCNA认证考试复习
第21章 关于融合型网络技术的介绍
第22章 制定网络安全和网络管理策略
第23章 虚拟专用网



第17章 光网络基本原理

目标

学习完本章后，你将能够：

- 了解光网络的关键的商业推动力。
- 描述光纤系统的特性。
- 描述光通信系统中的通信组件。
- 区分用于光传输中的光发生设备的特性。
- 描述光纤的重要设计特征和折射率。
- 识别光缆的主要组件。
- 描述多模和单模光纤的特性。
- 解释可能存在的光几何学问题。
- 描述光纤中的光损耗因素。
- 区别不同类型的散射的结果。
- 描述光过滤技术和光放大器的功能。
- 描述掺铒光纤放大器（EDFA）的工作原理。
- 描述同步光纤网（SONET）技术。
- 描述SONET/同步数字系列（SDH）。
- 描述密集波分复用（DWDM）系统。
- 解释电/光/电（E/O/E）转换器（收发机）是如何转换的。
- 描述光纤数据传输。
- 描述DWDM的优点和城域DWDM的特性。

本章较深入地讨论了光网络基本原理。光网络在很多方面，如可靠性和安全性，比传统网络要强得多。可靠性和安全性是政府部门和商业机构所期望达到的两个最重要的指标，这也是为什么光技术能成为计算机网络产业内的领导者和标准的原因。

17.1 光网络基础

因特网上通信的增长速度大大超过了传统语音通信的增长速度。网络骨干上的IP带宽需求将服

务提供商的网络容量推向极限，有时甚至超过了它的容量。

服务提供商们需要尽快的提供新的服务，以尽可能少的时间和费用交付高附加值的应用，还要用少量的操作成本构建可扩展的、安全的网络体系。所有这些需求的答案就是光技术。光网络是用来传输各种数据，如文本、视频和声音的极其有效的方式。

本章描述了光网络的商业推动力和光系统的特性，还讨论了光传输的相关组件和特性。

17.1.1　光技术的商业推动力

网络必须有能力快速、有效并且廉价地传输数据和视频信号。与其他任何传输资源比较起来，光纤是最有效的传输介质。光纤为网络通信提供了最高的带宽容量。随着高带宽容量和高传输速度的需求不断增长，可以预见，光纤的使用也将快速增长。

因特网经济的高速发展和数据通信的爆炸性增长需要有一种可扩展的、多服务平台，并且能够支持下一代、基于IP的服务和安全。如今，服务提供商对它们的网络提出的需求，如表17-1所示：

表17-1　光的商业推动力

关键推动力	描述
容量/可扩展性	有效的满足在城域网和长距离网络体系中对容量和可扩展性的需求
可靠性	随着因特网的高速发展而扩展的同时，提供非常好的可靠性
利润增长点	减少成本和促进新的增值服务
大范围覆盖	长距离通信
端到端的灵活性	提供构建可伸缩性的、端到端的光解决方案，并且满足运营商级的可靠性需求
可适应性	通过开放式系统结构来快速适应
空间高效性	减少接入点（POP）的物理空间需求
安全	支持基于IP的安全特性。

17.1.2　光纤系统

光纤技术是当今高速网络的核心技术。在城域内连接远端的城市和其他地点。光纤网络是由细小的玻璃纤维组成的，用来承载比铜缆更快、更可靠的光脉冲，最高速度能达10G bit/s。正在进行将速度提升至40G bit/s的研究工作。

信息在光纤中以光速传播。用来衡量光的时间单元非常之小。尽管光纤很小，但它们能够延续很长的距离。在大约人的头发大小的直径上，光纤能够承载巨大的信息量。

17.1.3　光纤传输系统

所有的通信系统都有3个共同点：一个信号源（Signal Source），一个信号传输的介质（medium）和一个接收器（receiver）。这个系统能简化为用一根绳子连接两个罐头瓶来供朋友交谈。在光系统中，光发生器是光源，介质是光导体（光纤），接收器是光感应器（如图17-1）。

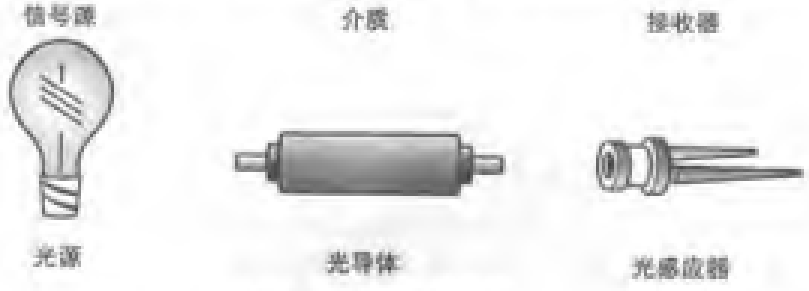


图17-1　光纤传输系统

1　光发射机

光发射机（transmitter）是一个简单的光源，如一个电灯泡（如图17-2）。激光和发光二极管（LEDs）都能用作光发射机。电子信号，如声音、数据或图像被转化为光信号，对数字的电子信号而言对应着光的明或灭；对模拟的电

子信号而言则对应着光的强度的大小。在数字信号中，有光为1，没有则为0；在模拟信号中，光的强度对应着电子信号的级别。

2 光接收器

接收器（receiver）是一个半导体，它将光转变为对应的电信号。它通常被称为“光电转化器（optical-to-eletrical converter）”，或O-E转化器（O-E converter）。在数字信号中，光的出现产生一个某种高级别的电信号，光的消失产生一个低级别的电信号（如图17-3）。在模拟系统中，O-E转化器将光的（能量）级别转化为对应的电级别。

即使没有任何光信号达到O-E转化器的时候，一个电子信号也有可能会产生。存在于所有检波器电路的暗电流产生了这个信号。暗电流是理论上存在于所有电路中的电子噪音。

一些接收电路有着比较低的噪音级别。接收器的噪音级别取决于它的设计。低噪音级别通常是良好设计的结果（如图17-4）。

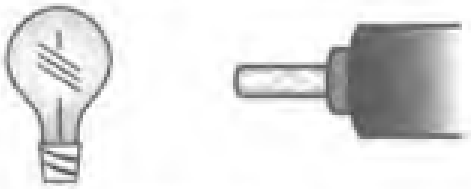


图17-2 光发生器



图17-3 高级别和低级别信号

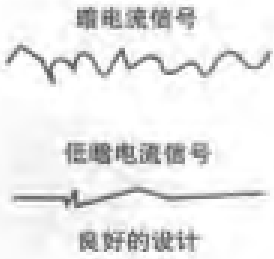


图17-4 暗电流

17.1.4 光

光能用多种方法来描述。如电灯泡能用60W或100W来区分。在光纤中，瓦特数是瓦的千分之一、百万分之一或十亿分之一：毫瓦（mW）、微瓦（uW）或纳瓦（nW）。通常，用分贝（dB）——一个与瓦特数相关的单位，来衡量更为方便。描述语“相对于1毫瓦的分贝（dBm）”定义了在电报和电线中的无线电频率和声音频率的信号强度。

光也能由它的颜色来描述，颜色决定于电磁信号的波长。蓝色波长大约是300纳米（nm），红色是700nm。光纤系统有3个波长值：850，1300，1550nm。多模系统只使用850和1300nm，而单模系统只使用1300和1550nm（如图17-5）。

光的能量决定了它的亮度。瓦特数越高，光就会越亮。在光纤系统中，基准能量是1毫瓦（mW），也是0dBm。高一点的值，如4mW，就应该是+6dBm。3dB的改变意味着瓦特数的加倍；负的3dB（-3dB）的改变意味着瓦特数的减半，如，0.250mW等于-6dBm（如图17-6）。

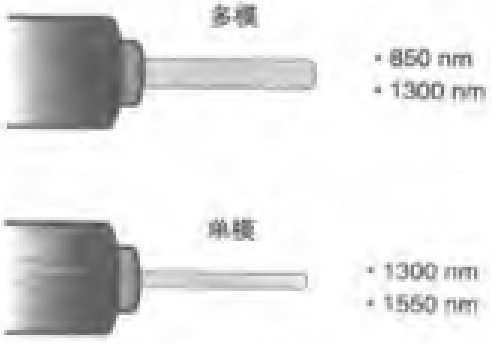


图17-5 光的波长



图17-6 光的能量

光纤系统中的能量级别能够从+20dBm——热激光的输出能量，到大约-70dBm——在100英里长的光纤中走了一个来回的光能量的大小。

1　光传输

在光纤中，信息是通过对光能量的调制进行传输的，而不是光的波长或频率。因此，波长在传输过程中保持不变，这就有可能将两种不同波长的光混合在一根光纤中传输而互不干扰，这被称为*波分复用*（WDM），它允许多于一个的波长通过一根光纤传输，从而增加光纤的容量（如图17-7）。WDM在以后的章节将被详细介绍。

采用何种光源是在系统设计中需要重点考虑的地方，因为它是系统中最昂贵的因素之一。光源的特性常常是光链路最终性能好坏的决定性因素。用于光传输系统中的光发生设备应该是紧凑的、单色的、稳定的和长持久性的。

光传输系统中常用的有3种：LED、激光二极管（laser diodes）和半导体激光（Semiconductor lasers）（如图17-8）。LED是相对发射速度较慢的设备，比较适合于速度低于1G bit/s的场合。LED能以一个相对宽的频谱范围和以一个相对大的角度来传输光。



图17-7　波分复用



图17-8　光发生设备

LED和激光二极管是比较便宜的设备，通常用于多模光纤通信。相反的，半导体激光，有一些性能特性，使之较适合于单模光纤应用环境。

2　反射与折射

光有时被描述为以光线方式传输。*反射*（reflection）是指光线在两种材质的界面以它射入的相同角度反弹回去。反射发生在当一道手电筒光照到窗户或镜子上时反弹回去（如图17-9），光线以它射入的角度被反射回去。

折射（refraction）是光线从一种材质进入到另一种材质时由于传输速度的变化而产生的弯曲。当光线以一个足够陡的角度进入另一种材质时，光的大部分将穿过界面进入到另一种材质（如图17-10）。如果材质有不同的密度，光线就会发生弯曲，或者以一个固定的角度发生折射。折射的

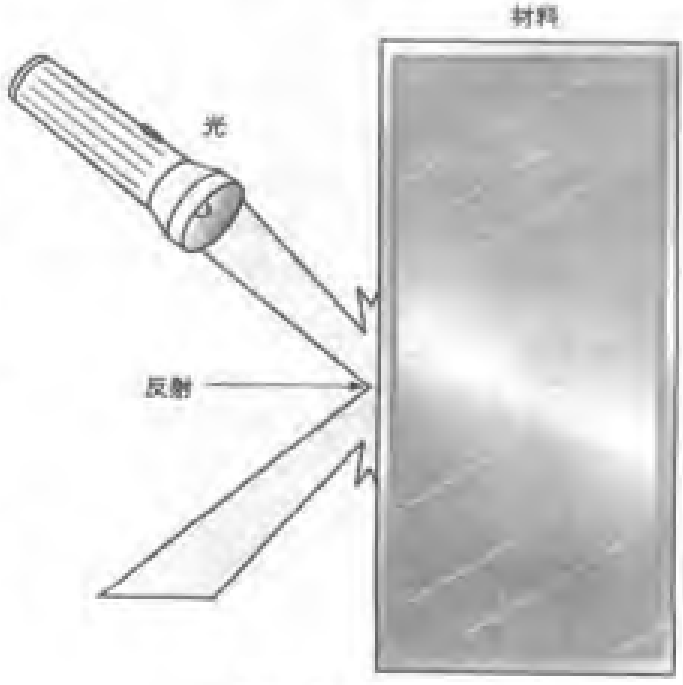


图17-9　反射

角度取决于两种材质的不同密度。如，当光线从水中进入空气中时，发生弯曲。当你把鱼竿插入水中时，鱼竿看起来好像弯的。然而，鱼竿并没有弯，而是照在鱼竿上的光线发生了弯曲。

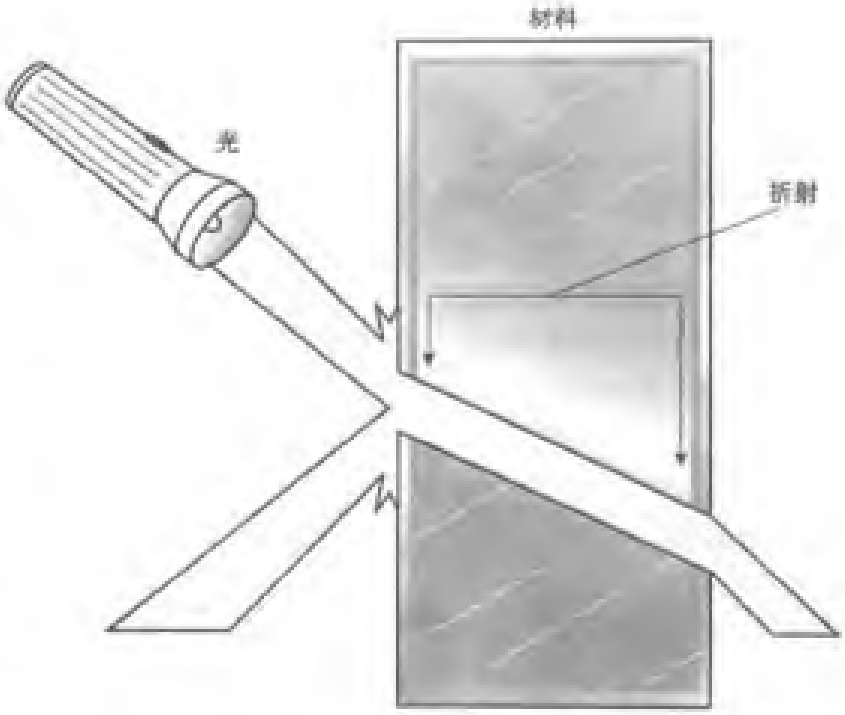


图17-10 折射

3 折射率（IOR）

光纤最重要的设计性能之一是它的IOR，这是光在真空中的传播速度和在光纤中的传播速度的比值。IOR是光纤密度的一个衡量值，因为较密的材质（较高的IOR）导致光在其中传播较慢。对光纤来说，典型的IOR值在1.4和1.5之间。

每个光纤厂商因为他们制造光纤的工艺不同，所以他们的产品的IOR也有细小的差别。即使对同一根光纤来说，IOR也有可能会改变。厂商报告的IOR值是一个平均值。两个有不同IOR值的光纤也能在一起工作。记住，不同的IOR在传输距离上也有所不同，较密的材质导致光传输的较慢。

17.2 光纤

光缆是使用经过调制的光，通过细的玻璃束来进行数据传输的网络介质。代表数据位的信号被转化为光。光纤的许多特性使得这种传输介质比铜缆要更为高级。光纤不用考虑电频干扰（EMI）或射频干扰（RFI）、有着更高的传输速率、极长的传输距离、不用关心接地性、对环境因素有更好的适应性等等。这些因素使得在很多场合中，光纤对铜缆而言是一个更有吸引力的选择。

为了理解光纤介质是如何工作的，你首先应对光的重要特性以及它是怎样在介质中（如玻璃）传输的有一个基本的了解。本节讲述了两种类型的光纤：单模和多模。还讨论了光几何学的一些问题、光损耗以及它产生的原因。此外，还介绍了两种光过滤技术：光纤布拉格光栅（FBG）和绝缘滤波。

17.2.1 光纤类型

光缆由3部分组成，如图17-11所示：

- **保护外套**（protective outer coating）——也被称为缓冲外套（butfer coating）。
- **内覆层**（Inner Cladding）——内包层有着和内核不同的密度，所以光在它上面能发生全反射。
- **纤芯**（Fiber Core）——用化学工艺提炼而成，加强了它的传输特性。

通信光纤分为多模和单模，它们惟一的物理区别在于它们芯纤的直径大小（如图17-12）。因为内核的大小不同，它们的性能特性也不同。单模光纤——因为有着比较小的内核，能够处理比多模光纤多得多的信息



图17-11 光缆的组成部分

量，并且能传输很长的距离。单模光纤也有着比多模光纤小得多的损耗。

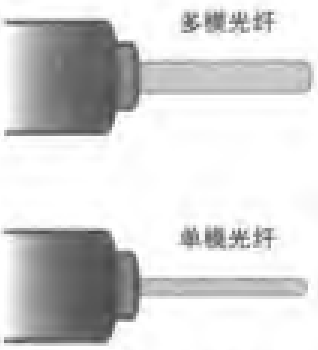


图17-12　光纤类型

1　多模

多模光纤（multimode fiber）用于在每根光纤里传输多路信号。多模允许光以很多路径或模式来传输。多模光纤的较大的内核允许光被分为许多种不同的模式，在一些模式下它到达另一端的时间比在另外的模式下短得多，这就导致源信号在传输时间上被扩散开了。在时分复用（TDM）数字信号中，光速的变化限制了信息位之间的幅长，从而限制了位传输的速率，这就是**色散**（dispersion）。通常，多模速率是几百兆比特/秒（Mbit/s）。

2　单模

单模光纤（single-mode fiber）被用作每根光纤传输一个信号。单模光纤只允许信号采用一条路径通过光纤的中间部位，整个信号以同样的速率通过光纤，这就允许了更高的数据传输速率。单模光纤的传输速率通常是几百兆和几十亿比特/秒（bit/s）。

17.2.2　光纤的几何问题

光纤厂商持续提高生产工艺，使得光纤越来越便宜，质量越来越好。然而，光纤的物理结构上也有一些允许的差异。其中关于焊接（和测试）的最重要的一个特性是在内包层之内的光核心的形状和位置。

因为光只在光纤的核心中传播，所以当焊接光纤时，有必要把核心连接起来。有些时候，光纤核心并不是匹配得非常好。它们也许对内包层中心有轻微的偏差，或它们的大小有所不同，或者它们不是非常规则的圆。（如图17-13）。在某些情况下，由于这些光纤特性的不匹配，可能会导致一个焊接的损耗不能低于0.20dB。

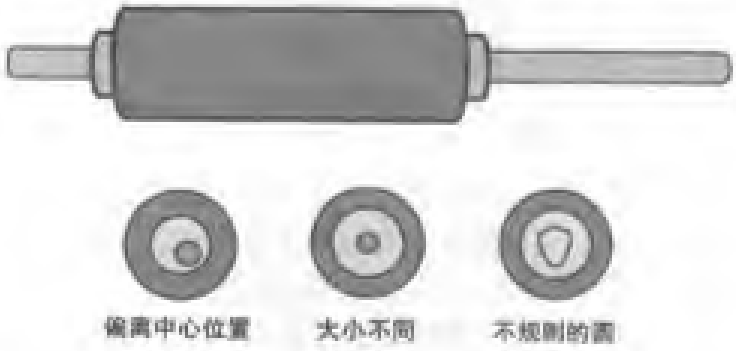


图17-13　光纤的几何问题

1　损耗因素

当光被射入光纤时，你需要考虑它传输的质量有多高，它是否在到达终点之前会被丢失。光纤中信号损失的多少是最为重要的性能特征。如果从接收端出来的光非常的弱，那么，整个系统不可能正常工作。接下来的部分讲述了光纤中损耗的主要因素，它们包括：

- 连接器损耗。
- 宏弯曲。
- 微弯曲。
- 吸收。

2　连接器损耗

连接器损耗存在于将光从一个内核传往另一个内核时。因为连接器依赖于将两个光纤终端连接起来的连接头的性能，所以它允许一些不同于焊接的损耗。如果两个光纤终端连接头被分开了，损耗就会产生，

因为当光从第一个内核出来时会发生散射，这被称为*终端界面分离*（end-face separation）。

即使两个界面之间的距离非常小，也会有一些光被丢失。距离越大，损失也就越大。如果连接头磨损了，在接头处引起松动，那么因为两个内核没有连接紧密也会导致光的损耗。这被称为*角度分离*（angular separation）。内核的位置不匹配在焊接时也会造成同样的问题。

图17-14显示了本章描述的连接器损耗的3种原因。

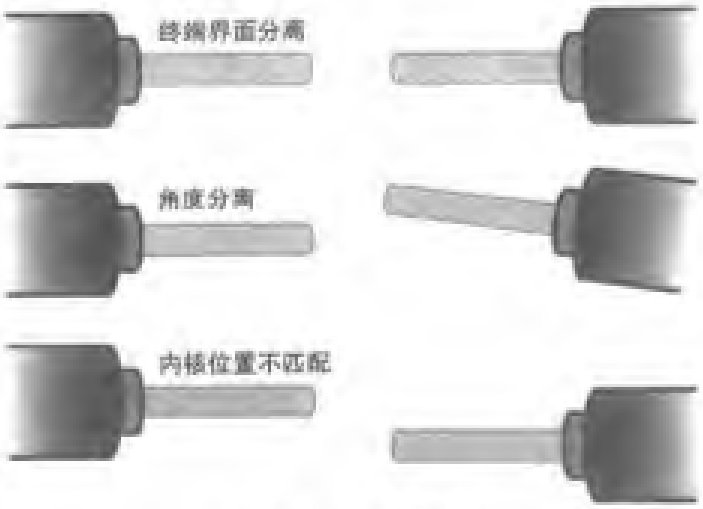


图17-14 连接器损耗

3 宏弯曲

宏弯曲（microbending）是你能够看见的弯曲。当你弯曲光纤时，可能会造成一些光线超过它的临界角度，这样就使这些光泄露出核心层而进入内包层。当光进入内包层后，一般是不容易再回到内核层的，它一般会最终通过缓冲外鞘泄露出去。（如图17-15）。

宏弯曲造成的损耗在波长较长时更为严重。（例如，一个大头针大小的弯曲会造成波长为1310纳米的光0.5dB的损耗，但对1550纳米的光来说可能是2.0dB）。可以通过减少光纤和光缆中过紧弯曲来减少宏弯曲。

4 微弯曲

微弯曲（microbending）造成和宏弯曲同样的影响，它导致光线超过临界角而泄露出纤芯。（如图17-16）。微弯曲发生在微观范围上，人眼不可见。

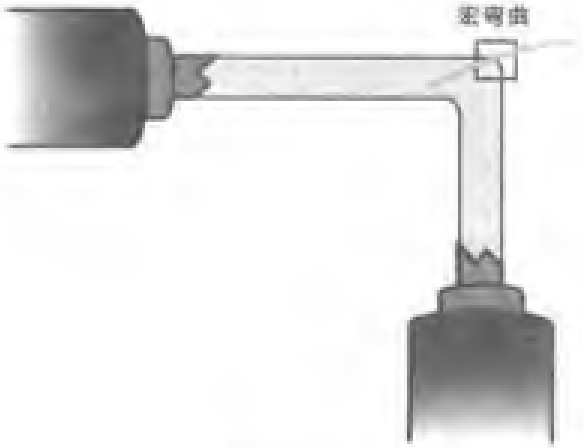


图17-15 宏弯曲

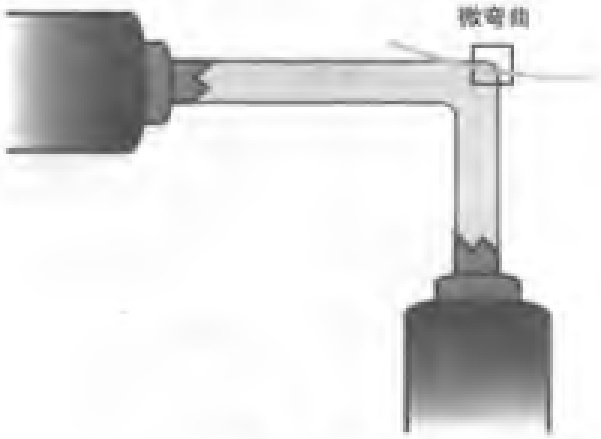


图17-16 微弯曲

微弯曲表现为光纤在生产过程中由于温度的变化而造成的细小皱纹。它也会因为已经安装好的光缆在外界温度急剧变化时，由于光纤各个组成部分热胀冷缩率不同，使得光纤会收缩或拉伸而造成微弯曲。

5 吸收

光也经常被玻璃结构所吸收。某种波长的光可能比其他波长的光被吸收的厉害一些。用户既不能改变也不能控制这种吸收。吸收（Absorption）是光纤的本征损耗特性（如图17-17）。

玻璃中，最为严重的吸收发生在靠近操作波长窗口1310nm和1550nm之间。这个区域经常表现出高级别的吸收性是因为光纤生产过程中产生的氢氧根（OH-）。这个吸收峰值在某些情况下可能会增加，并且导致在操作波长窗口内衰减的增加。

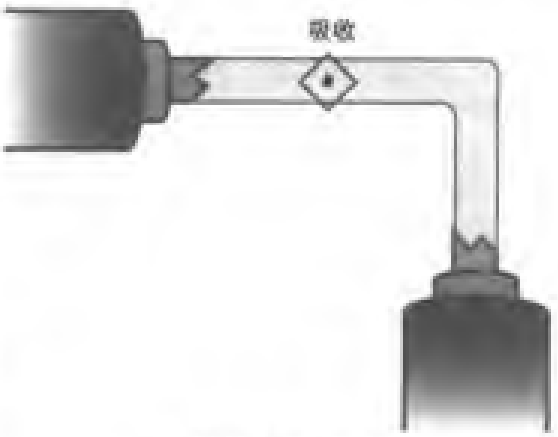


图17-17　吸收

17.2.3　衰减

衰减（attenuation）指的是传输过程中信号强度的减少。衰减是信号长距离传输后的自然结果。光纤系统中的衰减是由多种外在因素造成的，包括生产过程中的压力、环境和物理弯曲。光纤系统中的衰减也是有内在因素的，最主要的是散射（scattering）和吸收（absorption）。

最普通的散射形式为瑞利散射（Rayleigh scattering），它是由于玻璃处于冷却状态时各部分密度的微小差别引起的。散射对较短波长的影响比对较长波长的影响大，这就限制了对波长小于800nm的光波的使用。

由于吸收而造成的衰减是由材质的本征属性引起的。玻璃中的杂质或原子异变都能引发吸收。杂质吸收了光的能量，导致光变得暗淡。与瑞利散射对较短波长影响较大相反，本征吸收对较长波长影响较大。

下面是影响光纤衰减的两个主要因素：

- 光纤的长度。
- 光的波长。

图17-18显示了由瑞利散射、本征吸收（intrinsic absorption）和全衰减（total attenuation）引起的每公里分贝损失（dB/km）。基于这个衰减反应，两个操作波长为1310nm或1550nm。1550nm窗口因为有比较小的衰减，较适合长距离应用。

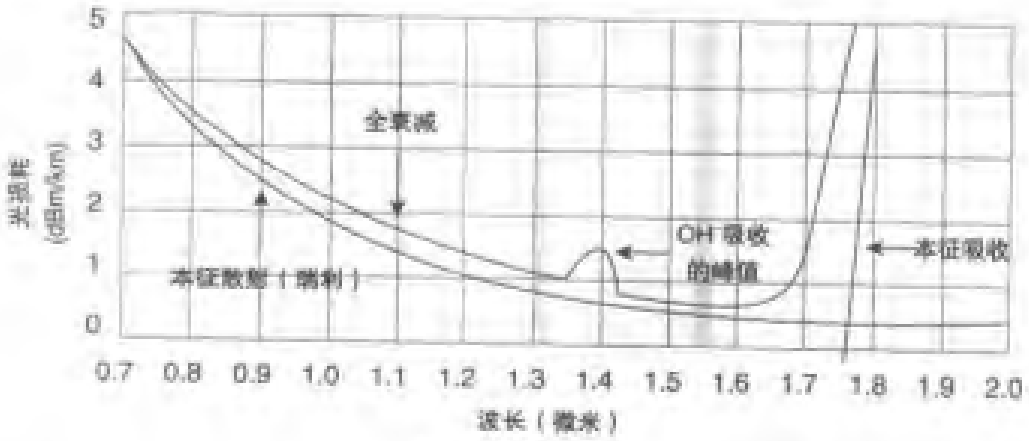


图17-18　衰减

17.2.4　光滤波器

光滤波器（optical filter）是用来区分不同的波长的。光纤布拉格栅格（Fiber bragg grating）和绝缘过滤器（dielectric filter）是光滤波器的两个例子（如图17-19）。

光纤布拉格栅格是光谱滤波器，它反射一个比较窄的波长范围的光而通过所有其他波长的光。光纤布拉格栅格是一种比较廉价的过滤方法，是因为栅格被直接写入标准的单模光纤。这些栅格的

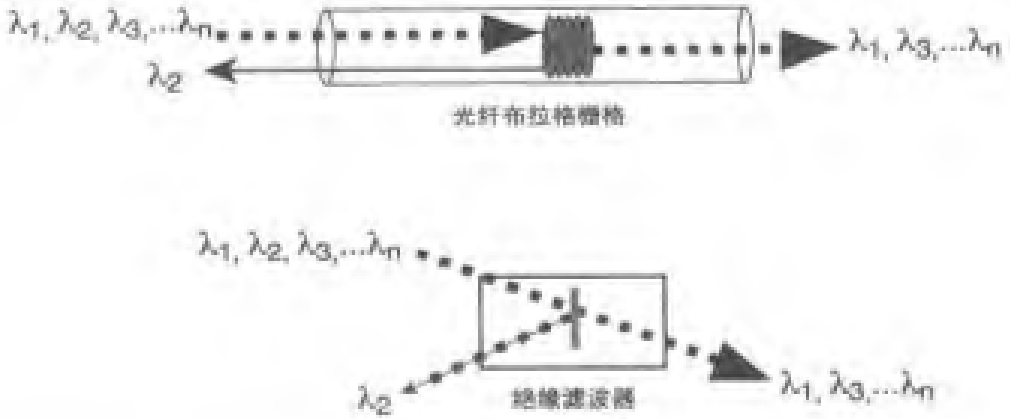


图17-19 光纤过滤技术

优点是能变得非常窄，但使用光纤布拉格栅格想控制滤波器的形状就变的非常困难了。

绝缘滤波器是基于半导体处理的，在它表面涂着一层厚度为波长1/4的绝缘介质。绝缘滤波器反射一种或多种光而通过其他的。与光纤布拉格栅格不同，绝缘滤波器很容易控制滤波器的形状。

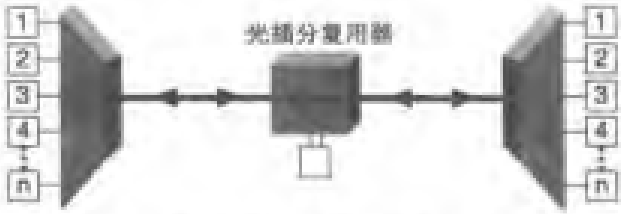


图17-20 光插分复用器

光滤波器用于光插分复用器（OADM, optical add drop multiplexers）中，通过反射一定波长的光而分出适当的光通道（如图17-20）。

17.2.5 光放大器

光放大器（OA, optical amplifier）是用来放大输入光信号的设备，它主要工作在1550nm波长附近，这个波长区域有着比较理想的噪声性能、比较低的信号失真和色扰和高输出饱和度。OA也很简单和高效（如图17-21）。

光脉冲在经过远距离传输之后，其质量降低。为了补救这种影响，可以用电子再生器用来执行3R操作：恢复信号级别，脉冲整形和脉冲重定时。电子再生器很昂贵，并且在传输中引入了延时，而且还要对指定光通道进行操作。

EDFA与电子再生器不同，它不用为了放大光信号而先将光信号转化回电信号。EDFA是由下面4个部分组成的一个设备：

- **掺铒光纤**（Erbium-doped fiber）。
- **光泵**（Optical pump）。
- **耦合器**（Coupler）。
- **分离器**（Isolator）。

EDFA的光通道整个都是被动的，光泵激光是惟一的主动部分。



图17-21 光放大器

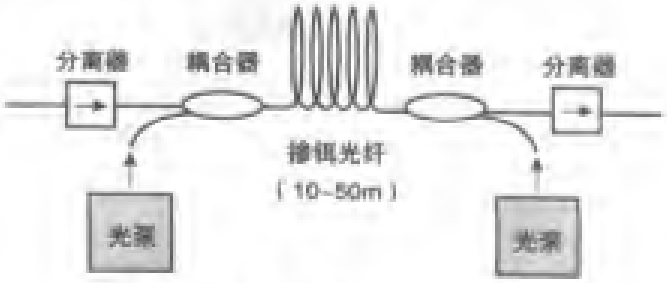


图17-22 掺铒光纤放大器

EDFA中，光纤被掺入了铒，铒是一种在外界激光的触发下能对1550nm范围内的光进行放大的稀有元素。（如图17-22）

17.3　光传输和复用

*SONET*是北美地区在光介质上进行同步数据传输的标准。SDH是SONET的国际标准等同体。使用环状拓扑的服务提供商主要配置SONET。现今的网络有2种比较流行的环状类型：单向路径交换环（UPSR）和双向线路交换环（BLSR）。

*DWDM*是同时传输不同波长的光信号的技术，它允许单根光纤像多根光纤一样工作。DWDM和光网络协同工作使得数据传输更快、价格更低。DWDM是提升现存光纤信息承载量的可扩展的解决方案。

这部分介绍了SONET/SDH技术，SONET的负载结构和SONET/SDH的复用体系。此外，本节还讲述了DWDM的工作原理和DWDM系统的好处。

17.3.1　SONET技术

SONET是美国国家标准委员会（ANSI）的交互运营商标准协会（ECSA）提出的关于光传输的标准，它规定了美国电信通信和其他产业的工业标准。Bellcore代表区域贝尔运行公司（RBOC）和其他一些公司发起了SONET标准，它保证了所有遵从midspan meet标准的公司生产的产品的兼容性。midspan meet指的是能够在通信网络中连接不同厂商的设备并使他们相互正常运行的能力。

SONET还被设计成对同步网络的运行、经营、管理和规定（OAM&P）来进行标准化，以及基于标准的冗余环。SONET还定义了光载波（OC, Optical Carrier）级别和基于光传输体系的电子等价同步传输信号（STS）。

SDH是SONET的国际标准等同体。SONET和SDH是一系列让各不同厂商的设备能协同工作的全球化标准。SONET使用可靠的负载信息来达到简单复用和扩展OAM &P能力的目的。下面介绍一下SONET的负载结构。

SONET负载结构

SONET有几层负载信息，如图17-23所示。负载中包含了足够的信息以使网络正常运行并允许网络控制器和节点间的OAM&P通信。下面描述了SONET负载结构的3层信息：

- 片段负载（*SOH, Section overload*）——片段（section）是两个网络元素之间的链路。片段负

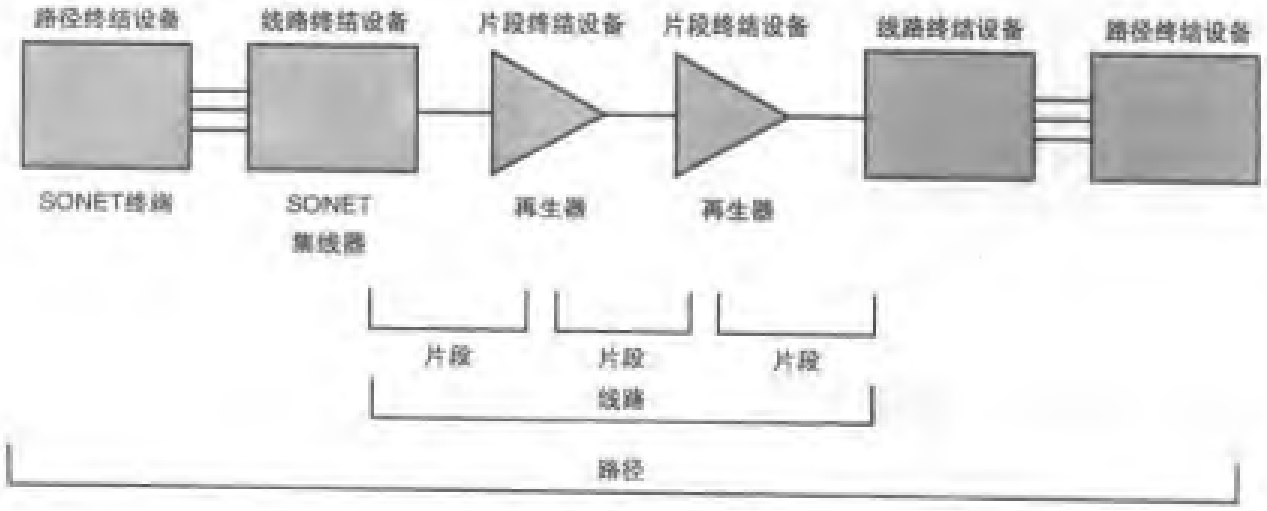


图17-23　SONET负载结构

载用来在相邻网络元素之间通信，如再生器。

- **线路负载**（*LOH, line overload*）——线路是连接两个网络元素、复用和解复用SONET STS信号的一个或多个片段。线路负载负责STS-N复用器之间的STS-N信号。
- **路径负载**（*POH, Path overload*）——路径是指连接两个网络元素、组合和分解流量的一个或多个线路，路径负载包括路径状态等信息，是端到端被携载的。

片段终结设备（STE）通常是再生器。STE能够产生、访问、修改或终结片段负载。线路终结设备（LTE）是能够产生、访问、修改或终结线路负载的网络元素。路径终结设备（PTE）产生、访问、修改或终结路径负载。

17.3.2 SONET复用分级结构

多数运营商提供两种类型的SONET服务：点到点的专线SONET和SONET环。它们都可进行高速度的数据传输，但是只有双光纤环保证自动重路由选择，从而实现冗余。有许多种类型的环，但当今最流行的是UPSR和BLSR（如图17-24）。

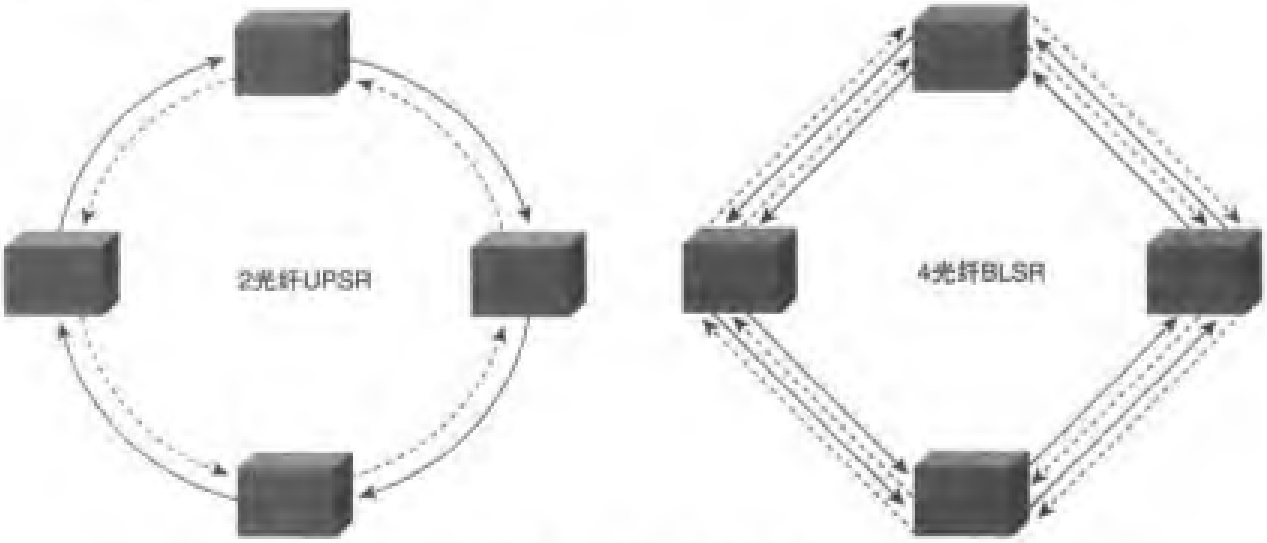


图17-24 UPSR和BLSR配置

在单向环中，所有的网络流量都沿着环的一个方向传输。在双向环中，两个节点间的流量在两个方向上（顺时针方向和逆时针方向）传输。

UPSR一般配置在城域网中（MAN），它有两根光纤（两个方向相反的环）。一根被保留为工作流量的自动保护。BLSR，一般配置在WAN或骨干上，它有两对光纤，一对用作工作流量，一对用作保护目的。在BLSR中，一个环上的每个方向上的一半带宽用作另外一个方向上的所有流量的共享保护。

1 SONET自动保护转换

SONET线路自动保护转换（APS）保证线路层的整个设备。一个网络元素能够监视工作线路，当有错误发生时，能自动转换到备用线路上去。一个1：1的APS为每条工作线路提供一条保护线路，一个1：N的APS为每N条工作线路提供一条保护线路。

2 基于SONET/SDH的TDM传输

基于SONET/SDH的TDM提供了一个可以接受的传输体系，它提供了性能监控，它在物理上是环状，在逻辑上是点到点的（如图17-25）。在TDM上可以进行多服务传输，尽管在带宽利用上不是

最优，但它提供了良好的保护措施。

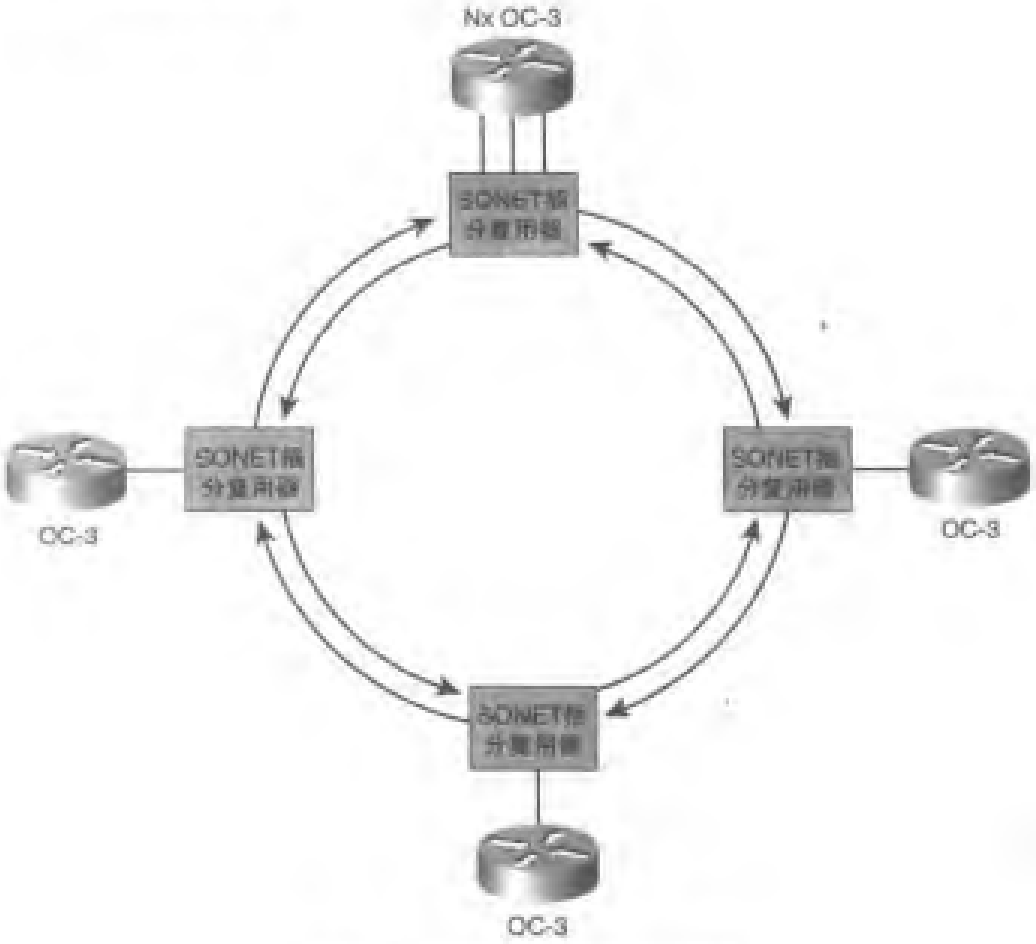


图17-25　基于SONET/SDH的TDM传输

3　SONET复用分级结构

SONET有一个分层的复用结构。SONET定义了一个通过同步的、灵活的、光的传输体系来承载许多不同容量信号的技术。这是通过字节交错复用机制的方法来实现的。

SONET复用过程的第1步是确定最低级别或者叫基信号。SONET中，基信号也被称为同步传输信号级别1，或简称为STS-1，它的工作速率为51.84Mbit/s。高级别的信号是STS-1的整数倍，这样就构成了STS-N家族和同步传输模块（STM）-N信号。（STS-N是SONET体系，而STM-N是SDH体系）。STS-N信号的光传输对等体被称为光传输级别N，或OC-N（如表17-2）。

表17-2　SONET/SDH复用层次

SONET/SDH复用层次光传输级别	SONET/SDH信号	比特速率	容量
OC-1	STS-1	51.84Mbit/s	28 DS1或1 DS3
OC-3	STS-3/STM-1	155.52Mbit/s	84 DS1或3 DS3
OC-12	STS-12/STM-4	622.08Mbit/s	336 DS1或12 DS3
OC-48	STS-48/STM-16	2488.32Mbit/s	1344 DS1或48 DS3
OC-192	STS192/STM-64	9953.28Mbit/s	5379 DS1或192 DS3

17.3.3　DWDM系统

光网络的开始阶段是和WDM联系在一起的，它的兴起是为了给已存的光纤提供额外的容量。

通过WDM，运行在不同波长（或颜色）的多个光传输信号能够组合进一根光纤里进行传输。WDM和DWDM的区别仅仅在于复用的程度不同。DWDM的波长间隔幅度比WDM更小，因此，DWDM比WDM有着更高的容量。

DWDM将来自不同源的数据导入一根光纤中，每一路信号承载于它自己的波长上。使用DWDM，超过200个不同的波长或数据通道能够复用进一个光流，通过单根光纤进行传输。（如图17-26）。

大多数DWDM系统都支持标准的SONET/SDH短距离光接口，兼容的客户设备能够通过这种接口连接到DWDM系统中。在长距离WDM系统中，这种接口通常是运行在1300nm波长的OC-48/STM-16接口。客户端设备可以是SONET/SDH终端或插分复用器（ADM），ATM交换机或路由器。

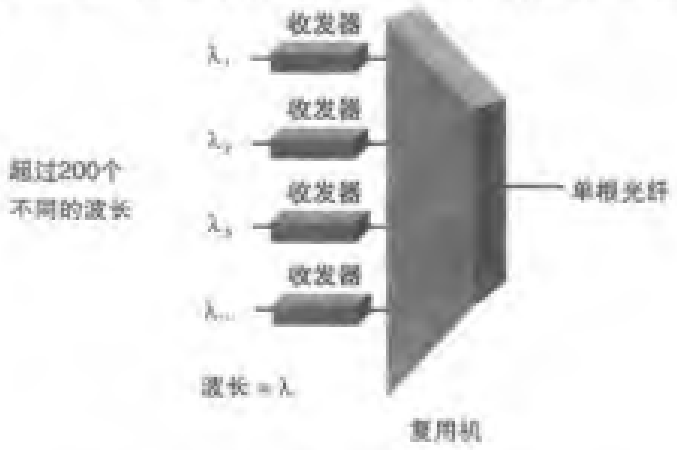


图17-26 DWDM系统

1 E/O/E转换

光能够通过不是百分之百由光纤组成的网络。E/O/E转换发生在数据流量以电信号的形式从光网络边缘进入运行在光网络上的网络核心，然后光信号穿过网络，又在某个传输点转化回电信号。

在DWDM系统中，一个称为收发机的设备将从客户来的SONET/SDH兼容光信号转化回电信号，这个电信号则用来驱动WDM激光发生器。WDM激光发生器是工作在1500nm波长附近的精确的激光发生器。每一台收发器将它从客户那里收到的信号转化为有细小波长差别的光，然后将这些不同波长的光用光学方法复用进单根光纤。在DWDM系统的接收方向上，运行相反的过程，从复用的光纤中分离出单独的波长，输入进分别的收发机，收发机将这些信号转化为电信号，然后驱动连接着客户的标准SONET/SDH界面。（如图17-27）。

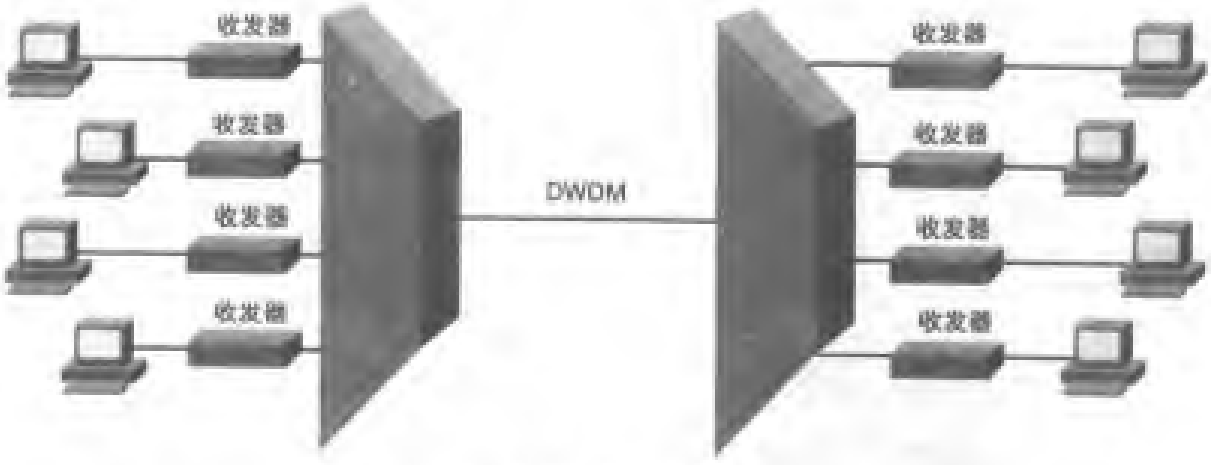


图17-27 电/交/电转化

2 数据传输

在DWDM系统中，每一条通道可以承载10Gbit/s（100亿bit/s），单根光纤最大能传输2万亿bit/s（如图17-28）。因为每一条通道在传输的终点处都会解复用为最初的源信号，所以不同的数据格式能够以不同的数据速率一起传输。

3　DWDM的优点

不管从技术还是经济的角度来看，能够提供潜在的、几乎是没有限制的带宽容量是DWDM技术最明显的优势。光纤的已有投资能够得到保护和优化。当需求改变时，新的容量能够不用很昂贵的升级就能加入到系统中去，这可以通过简单的设备升级或通过提高光纤中的波长复用数来实现。

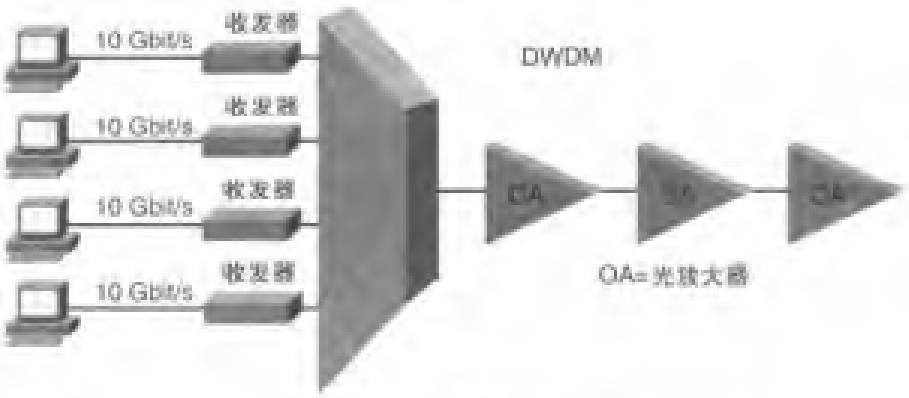


图17-28　数据传输

除了带宽以外，下面还列出了DWDM最具竞争力的优点：

- **可适应性**——DWDM具有非常好的可适应性，特别是IP、SONET和ATM数据都能在光纤中同时传输。
- **透明性**——因为DWDM工作在物理层，所以它能够透明的支持TDM和其他的数据格式，如ATM、吉比特以太网、企业系统互连（ESCON）和在普通物理层上的开放接口光纤通道。
- **可扩展性**——DWDM提供了经济的、可扩展的带宽增长。DWDM能够利用许多城域网和企业网络中已有的丰富的"暗光纤"。DWDM能迅速的满足点对点链路和跨越已有的SONET/SDH环的带宽容量需求。
- **动态提供带宽**——快速而简单的提供动态网络连接使得服务商能够用几天而不是几个月的时间来提供高带宽服务。

传统提升带宽的方法包括采用昂贵的、更快的电路，或者使用更多的光纤。后者的缺点包括对市场需求的滞后、昂贵的工程代价、有限的方法和资源枯竭等等。WDM在保持光纤兼容性的同时既提升了带宽又没有上述各种问题。DWDM提供了更大的光纤容量、对市场需求的快速反应、低成本以及保持了现有TDM设备的利用率。

4　城域DWDM

城域DWDM（metro DWDM），通过支持子波长TDM服务和波长服务，最大的提高了每根光纤的服务密度或增值潜力。如吉比特以太网、光纤连接（FICON）、ESCON等等。城域DWDM和长距离DWDM的基本区别在于城域DWDM是由快速提供服务的需求来驱动的，而不是光纤容量过载的压力（如图17-29）。表17-3对城域DWDM和长距离DWDM作了比较。



图17-29　城域DWDM与长距离DWDM的比较

表17-3 城域DWDM与长距离DWDM

	城域DWDM	长距离DWDM
连通性	本地接入、网状和中心点配置	城市间的连接
距离	中心局之间的距离小于50km	中心局之间的距离大于50km
设计原则	成本考虑优先，采用低成本的SONET/DWDM设备	容量考虑优先，配置昂贵的DWDM技术
光纤使用	一般用来出租，乐意被使用	非常严格的限制使用，安装额外的光纤非常困难

17.4 总结

在本章中，你学习了以下内容：

- 信息在光纤中以光速传输。
- O/E转换器将光转换为相对应的电信号。
- 多模光纤系统使用850nm和1300nm的波长，单模光纤系统使用1300nm和1550nm的波长。
- 光纤传输中，信息是通过对光的能量调制来传输的，光的波长保持不变。
- IOR是光纤最重要的设计性能。
- 光缆由3部分组成：一个保护外套、一个内覆层和一个纤芯。
- 通信光纤分为两类：单模和多模。
- 一般的多模光纤传输速率为几百兆bit/s；一般的单模光纤的传输速率为几百兆bit/s和几十亿bit/s。
- 光的损耗因素有：连接头损耗、宏弯曲、微弯曲和吸收。
- 光的衰减原因有：散射、吸收、生产过程中的压力、环境和物理弯曲。
- 色散导致光脉冲在沿着光纤传播时扩散开。
- OA是不需要将光转化为电就能实现对输入光信号进行放大的设备。
- EDFA不需要将光转化为电就能对输入光信号进行放大。
- SONET/SDH是光传输的标准。SONET在北美地区使用，SDH是SONET的国际标准对等体。
- DWDM将来自不同源的数据合并入一根光纤中。
- 收发机是将SONET/SDH兼容光信号和电信号进行相互转化的设备。
- DWDM能够对不同的数据格式以不同的传输速率进行传输。
- DWDM最具竞争力的优点在于它的灵活性、透明性、可扩展性和动态提供带宽。
- 城域DWDM通过支持子波长TDM和波长服务来最大地增加了每波长的服务密度。
- 城域DWDM受快速提供新服务的需求的驱动，而不是光纤容量过载的压力。

17.5 关键术语

角度分离（*angular separation*） 由于连接头磨损了，在接头处引起松动，而造成两个内核没有连接紧密而导致光的损耗的情况。

衰减（*attenuation*） 衰减指的是传输过程中信号强度的减少.衰减是信号进行长距离传输时的自然结果。

色散（*disperson*） 在时分复用（TDM）数字信号中，光速的变化限制了信息位之间的幅长，从而限制了位传输的速率的情况。

密集波分复用（*dense wavelength division multiplexing, DWDM*） DWDM是同时传输不同波长的光信号的技术，它允许单根光纤像多根光纤一样工作。

终端界面分离（*end-face separation*） 如果两个光纤终端被分开了，当光从第一个内核出来进入另一个内核时会产生损耗的一种情况。

折射率（*index of refration, IOR*） 光在真空中的传播速度和在光纤中的传播速度的比值。

宏弯曲（*macrobending*） 宏弯曲是你能够看见的弯曲。当你弯曲光纤时，可能会造成一些光线超过它的临界角度，这样就使这些光泄露出核心层而进入内包层

微弯曲（*microbending*） 由于某种细小的弯曲造成一些光线超过它的临界角度，从而这些光泄露出核心层而进入内包层。微弯曲发生在微观范围上，人眼不可见。

中跨接合（*midspan meet*） 指的是能够在通信网络中连接不同厂商的设备并使他们正常运行的能力。

多模光纤（*multimode fiber*） 一种光纤类型，用于在每根光纤里传输很多信号。多模光纤允许光以很多路径或模式来传输。多模光纤的较大的内核允许光被分为许多种不同的模式。

光放大器（*optical amplifier, OA*） 光放大器是用来放大输入光信号的设备，它主要工作在1550纳米波长附近，这个波长区域有着比较理想的信噪比、比较低的信号失真和色扰和高输出饱和度。

光过滤器（*optical filter*） 是在光纤网络中用来区分不同波长的过滤器。

光电转换器（*optical-to-electrical converter*） 半导体接收端将光信号转变为相应的电信号的过程。

反射（*reflection*） 反射是指光线在两种材质的界面以它射入的相同角度反弹回去。当一道手电筒光照到窗户或镜子上时被反弹回去，反射就发生了。

折射（*refraction*） 是光线从一种材质进入到另一种材质时由于传输速度的变化而产生的弯曲。

同步数字系列（*Synchronous Digtal Hierarchy, SDH*） SONET的国际标准等同体。

单模光纤（*single-mode fiber*） 单模光纤是一种光纤标准，它被用作每根光纤只传输一个信号。单模光纤只允许信号采用一条路径通过光纤的中间位置，整个信号以同样的速率通过光纤，这就允许了高的多的数据传输率。

同步光网络（*Synchronous Optical Network, SONET*） 是北美地区在光介质上进行同步数据传输的标准。

波长复用（*wavelength division multiplexing, WDM*） 在同一根光纤中将两种不同波长的光混合传输而互不干扰。

17.6 复习题

1. 下列各条中哪一条不是光网络的关键推动力？
   A. 有效的满足城域网和长距离网络结构中对容量和可扩展性的需求
   B. 减少成本的同时实现新的增值服务
   C. 能够进行长距离传输
   D. 能够适应封闭系统结构
2. 下面哪条关于IOR的描述是正确的？
   A. 它的意思是折射率
   B. 它是指光线在两种材质的界面反射回来
   C. 它是指光在真空中的传输速度和在光纤中的传输速度的比值
   D. 两种不同IOR的光纤不能一起工作
3. 判断对错：光流是电路中自然产生的电子噪音。
   A. 正确
   B. 错误
4. 下面哪个波长值没有在光纤中使用？
   A. 850nm
   B. 1300nm
   C. 1450nm
   D. 1550nm
5. 下面哪一（几）条正确描述了光纤？
   A. 高速度传输
   B. 长距离传输
   C. 比铜缆更可靠
   D. 以上都对
6. 下面哪种方法能够放大光纤中的光信号？
   A. OADM
   B. SONET
   C. ROL
   D. EDFA
7. 多模光纤的一般传播速度为：
   A. 几百Mbit/s
   B. 几百Kbit/s
   C. 几百Gbit/s
   D. 上面都不对
8. 关于单模光纤的描述正确的是：
   A. 信号以不同的速率通过单模光纤
   B. 单模光纤的传输速度比多模光纤低
   C. 单模光纤允许多种模式的光在其中传输
   D. 单模光纤允许一种模式的光在其中传输
9. 下面哪些是关于纤芯的可能发生的问题？
   A. 纤芯可能轻微的偏出内包层的中心位置
   B. 纤芯的大小可能有轻微的差别

C. 纤芯的形状可能不是规则圆
D. 以上都对

10. 下面哪个不是光缆的组件？
A. 纤芯
B. 内覆层
C. 外覆层
D. 保护外套

11. SONET被设计为对下列哪些进行标准化？
A. 同步网络操作、管理、维护和设备
B. 异步网络操作、管理、维护和设备
C. 在应用层对SONET功能提供保护
D. ATM的传输标准

12. 下面哪个不是关于维护的3个级别的负载通道？
A. SOH
B. COH
C. LOH
D. POH

13. 下面哪种设备可能是DWDM系统的客户端设备？
A. LAN交换机
B. 网桥
C. 路由器
D. HUB

14. 下列DWDM系统中的哪台设备是用来转化SONET/SDH兼容光信号的？
A. 收发器（Transceiver）
B. 变压器（Transformer）
C. 转换器（Converter）
D. 应答机（Transponder）

15. 从技术和经济的角度，下面哪条是DWDM技术最明显的优点？
A. 在同一时间传输有限数量数据的能力
B. 提供潜在的无限传输容量的能力
C. 安装方便
D. 低成本



第18章　网络管理

目标

学习完本章后，你将能够：

- 描述怎样建立网络的文档。
- 描述网络安全的主要组成部分。
- 描述怎样处理影响网络的环境因素。
- 描述怎样测量网络的基准性能。
- 描述网络管理的可管理方向。
- 描述怎样监控一个网络。
- 描述怎样对一个网络进行查错。

如果你已经知道怎样去设计和构建网络，那么你应该能完成下面的工作了，如决定配线室在什么地方，怎样选择、安装和测试线缆等等。然而，网络的设计和实现只是你必须了解的内容的一部分，你还需要知道怎样去维护和管理网络，让它能在一个可以接受的水平上正常运行。网络管理包括许多不同的领域，如网络文档、网络安全、网络维护、服务器管理和服务器维护，而且，还不仅仅是这些内容，但是对本书来讲，这些已经足够了。上面列出的每个主题都有着同等的重要性，你不应该忽视它们中的任何一条。

许多管理员认为当他们的网络运行起来时，工作就结束了，这种观点是大错特错。当网络安装完成、运行起来的时候，恰恰正是网络管理员真正工作开始的时候。这暗示着，你必须知道怎样去排查网络运行中产生出来的各种问题，此外，你还必须知道什么时候有必要去扩展网络或改变网络配置以满足新的网络需求。本章中，你会学习使用一些技术性手段，如文档建立、监控和故障排除，来管理网络。

18.1　网络文档

一个运行良好的网络首先也是最重要的组成部分是文档。文档是我们平时谈的最多的，然而也是在网络实施中做的最少的。文档代表着网络管理员的思路，它包括工程进度，但不仅仅是，它还包括下面这些组件：

- 标明物理配线规划路径的图表。
- 线缆类型。

- 每一条线缆的长度。
- 线缆的终端类型。
- 每个墙上插座或配线架的物理位置。
- 区分的每一条线缆的标记。

18.1.1 主配线架（MDF）和中间配线架（IDF）规划

文档应该包括网络中的主配线设备和所有中间配线设备的物理和逻辑布局。IDF是连接和管理MDF与工作站设备间的通信的线缆架。线缆通过一个处于中心位置的MDF进入大楼，然后通过每个IDF，最后到达指定的工作站。例如，一个有若干层楼的企业可能在第一层有一个MDF，然后每一层都有一个连接到MDF的IDF。因此，它建立的文档中就应包括线缆架的物理规划、各种辅助设备和服务器，还包括配线架标志来标明线缆的终结点，还有安装在配线间的其他设备的详细规格和配置信息等等。

18.1.2 服务器和工作站配置详细资料

必须注明连入到网络的服务器和工作站的详细配置信息。这些记录信息还应该标准化，应包括

计算机硬件配置工作表
每台计算机一页

文件服务器或工作站：	
物理位置：	
厂商和型号：	
序列号：	
公司名称：	

可移动磁盘驱动器：

厂商	驱动器号	容量	内部/外部	内部驱动器插槽

固定磁盘驱动器：

厂商	驱动器号	容量	内部/外部	内部驱动器插槽

内存现有/最大	现存	最大

外围设备卡：

厂商：	型号：	类型：	中断请求	直接内存访问	基本内存地址

网络接口卡

厂商：	节点地址	型号：	LAN驱动	中断请求	直接内存访问	基本内存地址

注释：	

图18-1 计算机硬件配置工作表

计算机的厂商和型号、序列号、软盘驱动器、硬盘驱动器、DVD/CD-ROM驱动器、声卡和网卡、RAM的数量以及其他物理信息；如图18-1和18-2。它还应包括计算机的配置信息，如中断请求（IRQ）、直接内存访问（DMA）、外围设备卡的基本内存地址。把下面这些信息也包括到文档中去是个很好的习惯，如计算机的物理位置、用户、网络标志（IP地址介质访问控制（MAC）地址）、子网掩码和拓扑图。还有计算机的购买日期和保修信息。

打印机配置工作表 每台打印机一页						
物理位置:						
厂商和型号:						
序列号:						
公司名称:						
打印机名称:						
内存现有/最大:						
进纸箱:	一号进纸箱类型		二号进纸箱类型		三号进纸箱类型	
打印机配置:						
串口	端口	波特率	停止比特	奇偶校验	Xon/Xoff	中断
并口	端口	轮询				中断
网络	IP地址	轮询	MAC 地址			
打印队列:						
打印机操作员::						
注释:						

图18-2 打印机配置工作表

18.1.3 软件列表

为了将每个软件包的标准配置和安装信息文档化，有必要将网络上每台计算机使用的标准的或专门的软件进行列表，这些软件应包括操作系统和应用软件（如图18-3）。

18.1.4 维护记录

对网络中的哪些设备做了哪些维护应该做一个列表（如图18-4）。这能帮助你预测将来可能会发生的硬件和软件问题。

18.1.5 安全性评估

文档不仅仅只包括“软”安全性，如用户权限、密码定义和防火墙，它也应该注意物理安全性。物理的或硬件安全性包括标明MDF和IDF是如何上锁的，谁能够、为什么需要进入这些房间，主机

计算机软件配置工作表 每台计算机一页					
计算机名字：					
操作系统					
厂商	版本	服务更新	网络能力	安全性	
应用软件					
厂商	版本	服务更新	网络能力	安装目录	数据目录

图18-3　计算机软件配置工作表

计算机维修工作表 每台计算机一页				
计算机名字：		日期：		
问题类型：	硬件	软件		
问题描述：				
是否在保修范围：	是：	否：	维修点：	
维修说明：				
付费部门：				
审批者：				
何时维修好： 注释：				

图18-4　计算机维修工作表

是如何被保护的（线缆的安全性和报警），谁能够物理的接触这些系统等等（如图18-5和18-6）。

18.1.6　用户策略

用户策略（User police）是文档中最重要的也是对网络管理员最有用的部分。它们记录了用户如何与网络进行交互的信息。这些策略包括了网络上什么是允许做的、什么是不允许做的，还应包

网络安全房间表格 每个房间一页					
物理位置：				日期：	
物理安全：	门锁	窗户	天花板	防火	抽屉
服务器磁带备份：					
服务器名称：	类型	备份介质	办公室位置	磁带库名	备份日期(星期)
服务器1					
服务器2					
服务器3					
授权访问：	名字		部门	职能	
注释：					

图18-5 网络安全房间表格

网络安全用户表 每个用户一页				
物理位置：			日期：	
用户：			User ID：	
部门： 密码长度：			部门经理： 本地目录：	
ID有效期：			本地访问：	
访问时长：			打印访问：	
远程访问：			管理访问：	
所属组：	组名	组权限	本地/全局	限制性
网络职责/优先级				
注释：				

图18-6 网络安全用户表

括违反用户策略后造成的后果如何。用户策略的其他方面还包括用户ID和密码的最短长度、密码内容等规定。用户策略应该在公司的管理下制订并且保证它们能被接受和被执行。作为网络管理员，你可能想把公司的网络设计为尽可能的安全，但你也应该确保你制订的网络策略和公司的政策不冲突，并且不会限制用户对必要资源的访问。

上面提到的各种文档信息为你的系统创建了一个网络文档集，这个文档集帮助你以一种相对正规的方式来维护和升级你的网络。这些文档信息也给了网络管理员在升级网络出错或从网络错误中恢复时重新配置网络的一个出发点。关于网络文档的最后一点说明是它需要随着网络升级和配置的改变而连续更新，否则，文档就会和你当前的网络环境没有多少相关性了。

18.2　网络安全

网络安全包括两个主要方面：首先保护你的网络防止非授权访问；其次，确保你在发生灾难性事件后能够恢复数据。

网络安全的第一个部分可以回溯到本章已介绍的网络文档小节中，它涉及到网络尽可能的安全以防止非法访问。你可以通过建立安全策略来达到此目的，如最短密码长度、最长密码有效期、密码惟一性（不允许在不同的系统上使用同样的密码）和只允许用户在某天的特定时间或一个星期的某天登录到网络。你可以直接设置这些参数，然后网络操作系统会执行这些设定。

安全也包括确认用户了解公司的安全政策并且遵守这些政策。这些政策如不允许用户用他的名字或宠物名字来做密码以及当用户离开计算机时需要退出登录或激活一个有密码保护的屏幕保护程序等。只有用户了解并遵守公司的网络安全政策，这些政策才能真正被执行。

18.2.1　数据恢复

数据恢复（Data recovery）是网络安全的第二部分，它的任务是保护数据免于丢失。有多种方法达到此目的，而且一般情况下，也会同时采取多种不同方法来保护数据。如图18-7所示，常用的数据保护方法是用磁带设备或容错磁盘来备份数据和使用不间断电源（UPS）来防止设备因电力中断而导致的非正常关机。下面先讨论前两种方法，第3种方法将在“环境因素”一节中讨论。

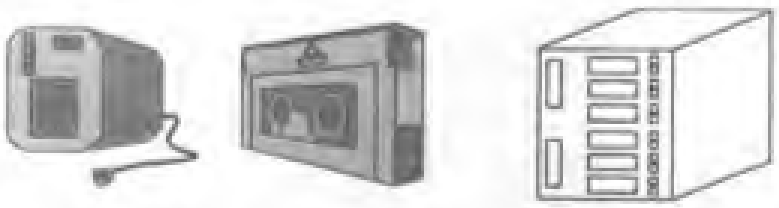


图18-7　UPS、磁带备份器和磁盘阵列

数据备份（Data backup）是指把储存的数据复制到磁带或其他存储介质上，如可移动硬盘、CD-ROM或DVD-ROM。磁带之所以经常被采用，在于它的低价格和大容量。磁带库比起相应的可移动硬盘来说，便宜得多，容量也大得多。磁带也有它的缺点：它是按顺序存储数据的，就跟音乐记录在录音带上一样。这就意味着，和在录音带上想查找一首歌曲一样，你很难迅速的在记录数据的磁带上找到一个特定的文件。但是，因为备份的数据是按顺序记录的，恢复的时候又是按同样的顺序恢复，所以，这并不影响它的使用。磁带对服务器来说也许是最好的备份方法，对工作站来说，CD和DVD刻录器是比较简单和便宜的备份方法。

尽可能完全和快速的进行磁带备份是非常重要的，因为它极大的消耗系统资源（网络带宽和服务器处理能力）。为了达到尽可能高效的完全备份，发明了多种备份方法。大多数备份类型都使用一个叫*归档位*（archive bit）的标志或开关，归档位和文件一起存储，当文件创建或修改时，标志就被置为“开”，这个标志就会告诉备份进程要对那些文件进行备份；如果文件被备份进程存储到了磁带，则标志就被置为“关”，告诉系统当前文件已经备份好了。大多数公司都建议将磁带和备份存放在防火防盗的安全位置，来避免火灾或水灾等其他危险。

18.2.2 备份操作

下面列出了常见的5种备份操作：

• **全备份**（*Full bacup*）——硬盘上所有的文件都被存储在磁带上，所有文件的归档位都设置为“关”。

• **增量备份**（*Incremental backup*）——这种备份类型是对所有上次备份后新建或修改过的文件进行备份。关于增量备份，需要注意两点：首先，增量备份只对那些归档位为“开”的文件和目录进行备份，做完备份之后，再把归档位设置为“关”。其次，在进行完备份之后，如果建立或修改了任何文件，则将它的归档位设置为“开”，这样在下次增量备份的时候，它们就能够被备份到磁带上去。

• **差异备份**（*Differential backup*）——这种备份是对最后一次全备份之后所有建立的或被修改的文件进行备份。这听起来和增量备份是一样的，但它们的区别在于：即使文件已经被备份到磁带上去了，也不会将归档位设置为“关”，这就意味着，每进行一次区别备份，那么所有在最后一次全备份之后建立的或被修改的文件都要被重新存储一遍。

• **拷贝备份**（*Copy backup*）——这种备份是对用户选择的文件进行备份，它不会重置归档位为“关”。

• **每日备份**（*Daily backup*）——这种备份是对每天修改的文件进行备份，同样，它也不会重置归档位为“关”。

前3种备份方法使用得最为广泛。这里举一个进行增量备份和区分备份的例子。为了进行增量备份，首先在星期一进行一次全备份，这样做的结果是所有文件的归档位都被置为“关”；星期二，进行一次增量备份，备份到另外一个磁带上去，这样所有在星期二被修改的文件都存储起来了并且归档位又都恢复为“关”；在每一个工作日都进行同样的操作，备份到不同的磁带上去。这样就为这一个星期所有修改过的文件进行了完备份。在下个星期一，又开始上面的整个备份过程。这种备份的好处是每天需要备份的工作量很小，所以对网络资源的压力很小，缺点是当你需要数据恢复时，先要恢复全备份磁带，然后按照先后次序恢复所有增量备份，这将花费大量时间，此外，如果任何一个磁带损坏了，那么它上面的信息也就丢失了。

为了进行区别备份，首先在星期一进行一次全备份，这样做的结果是所有文件的归档位都被置为“关”。星期二，进行一次区别备份，备份到另外一个磁带上去，这样所有在星期二被修改的文件都被存储起来了，但是并没有将归档位设置为“关”。在每一个工作日都进行同样的操作，备份到相同的磁带上去。这种备份方式也提供了网络数据的完全备份。它的优点是：如果必要的话，只需要两盘磁带就可以进行备份工作了。缺点是：采用这种方法进行备份，你以前已经备份了的数据每天又要重新存储一遍，这就增加了每天的网络资源需求，还有，如果区别备份磁带损坏了，而你又需要在星期五恢复数据的话，那么前面4天的数据就都丢失了，需要重新输入！

> **注意**：如果你每天都进行全备份，那么你只需要1盘磁带就足够了，但是，每天都进行大容量的全数据备份需要消耗大量时间，因而是不现实的。拷贝备份和日常备份都不重置归档位，它们都用来对特定文件进行备份。

进行数据备份时另外一个需要重点考虑的问题是用户工作站上的数据备份。工作站的数据备份了吗？是怎样备份的？工作站上的数据也是同等重要的，如果说不重要的话，那也只是没有服务器上的数据重要。工作站的备份方法取决于实际情况，接下来将讨论工作站备份的问题。

第一种备份方法适合于那些产生大量只为自己使用的数据的工作站。在这种情况下，给那台工作站装一台单独的磁带驱动器也许是最好的方法，因为它允许大量数据的备份又不影响网络流量，但这种方法的缺点是它把备份的责任推给了用户。

第二种备份方法是将所有数据文件拷贝到可移动存储设备，如软盘或ZIP磁盘驱动上去。这种方法相比磁带备份起来减少了费用、时间和复杂度。但是它同样也把备份的责任推给了用户。

第三种备份方法是为所有的用户在服务器上创建供他们存储数据的目录。这种方法使得用户不用依靠特定的设备来自行做备份了，而是当服务器完成备份的时候也就同时完成了所有用户工作站的备份。它的缺点是：必须明确规定什么样的用户数据才能上载到服务器上去，用户必须清楚他们应该把数据上载到什么地方以及上载是否成功。还有，如果网络通信出了问题，那么在问题解决之前，用户将不能使用服务器上的数据。

你可以看到，所有的备份方法都有其潜在的问题，然而，每一种方法又是在特定环境中最合适的方法。惟一错误的方法是忽略系统数据备份的重要性。

18.2.3 冗余技术

保护数据的第2种方法是通过容错存储设备（fault-tolerant storage device）。这种设备可以分为廉价冗余磁盘阵列（RAID）级别0到级别10。RAID类型说明如下：

- RAID 0——将数据同时跨磁盘写入，没有奇偶校验，所以没有冗余性。
- RAID 1——使用磁盘镜像（磁盘复制）来将数据同时写入不同硬盘的同一分区，因此，实现了自动备份。磁盘复制和磁盘镜像一样，都是使用两块硬盘控制器和两块硬盘来防止系统硬盘控制器的单点故障。
- RAID 2——将数据跨磁盘写入，带有奇偶校验。这种系统因为需要昂贵的磁盘修正器来工作，所以应用很少。
- RAID 3——将数据以字节的方式写入，并且具有专门的奇偶校验驱动器，这是一种很好但很昂贵的冗余方法，正因为它的昂贵，所以也很少被采用。
- RAID 4——将数据以扇区的方式写入，并且具有专门的奇偶校验驱动器，这也是很昂贵的冗余方案，并且数据写入磁盘的速度很慢。因为它的费用不菲和写数据较慢的原因，也很少被使用。
- RAID 5——将数据和奇偶校验都跨磁盘写入（至少需要3块磁盘）。通过将奇偶校验写入所有的磁盘，就不需要单独的奇偶校验磁盘了，但是仍然可以达到整个数据的冗余性。数据写入磁盘的速度依然慢，但费用却低了很多。另外一个关于RAID 5的重要事实是：在Windows NT系统下，引导区和系统区不能位于RAID 5磁盘阵列上。

还存在着其他的RAID级别，但超过了这里讲述的必要。事实上，不是所有的网络操作系统都支持上面提到的RAID级别。大多数操作系统都支持RAID 0，RAID 1，RAID 5这3种RAID级别。需要记住的是：RAID 0的写入速度快，但没有提供数据冗余（备份）；RAID 1提供了完全数据冗余但需要2倍于存储数据的空间，因为所有的数据都写入2块单独的硬盘，RAID 1同样有着磁盘控制器的单点失效问题。这个问题被RAID 1的一些变种方法解决了，它们采用磁盘复制方法——磁盘控制器也是2个。

RAID 5需要至少3块磁盘（因为在Windows NT系统中，引导区和系统区不能位于RAID 5磁盘阵列上），并且每块硬盘上的分区大小必须完全一致。RAID 5现在很流行的原因是它提供了快速的数据读取速度——这就给了网络更好的吞吐量。在Windows NT系统中使用RAID 5需要重点指出的是：为了满足完全冗余性，必须对磁盘阵列进行分类，而且必须要有5块硬盘来完成，前两块采用RAID 1（磁盘镜像）来备份系统和引导分区，剩下的3块用来做RAID 5，这就既有了RAID 5的速度优势又满足了全冗余要求。

当和硬盘存储打交道时，一个需要理解的术语是**卷**（volume）。卷指的是存储器的物理单元，卷的一个好的类比例子是百科全书集，百科全书集中的每本书都可以称作一个卷，这些书可能还有多个卷（如X、Y、Z卷），最后，把整个百科全书集看作一个单元。硬盘上的卷集也有同样的概念，多个硬盘上的存储空间可以看作一个单元，被分配一个卷名。为什么强调卷这个概念？这是因为卷在网络系统中用得非常频繁。卷集并没有提供数据冗余，它们仅仅是将大的存储区域看作一个单元而已。

18.3 环境因素

好的网络管理工作的另一部分是处理影响网络的环境因素。只有控制好这些因素才能构建更稳定、更可靠的网络。

当你安装一台新设备时，必须要按照使用手册上的安装过程来进行，这能够防止发生许多因你“率性而为”而产生的问题。当你需要搬动设备的时候，要确保电源开关处于“关”状态，当你买了一块外围设备卡，需要装入计算机内部时，也要确认计算机的电源开关已经关闭并且在接触计算机内部之前要将身体上的静电放掉。使用接地腕带能让你接地良好，如果没有正确的接地，可能会产生出2万V的静电，不要以为这是耸人听闻——当你穿着皮鞋在人造地毯上走动或者坐在塑料椅子上稍微调整一下坐姿时，都有可能产生出这样高的静电。

静电产生的另外一个原因是空气过于干燥，因此，要确保存放设备的房间有着良好的温度和湿度。静电是非常隐蔽的，你可能只有到它产生放电、造成危害时才知道它的存在。静电放电能烧坏网络和计算机设备中的很多电子元件（IC）。为了消除这个隐患，可以考虑购买防静电地板和接地腕带。

让键盘、磁盘驱动器和设备空气流通口不要有灰尘和污垢，要做到这点，就要保持放置设备的房间干净且没有污染物。香烟的烟雾中含有焦油和烟碱等粘性污染物，所以，在计算机设备旁吸烟肯定会对设备最终产生危害；不要把咖啡、饮料和其他液体放在网络或计算机设备旁边或上边，如果液体不小心被碰翻而进入机器内部，几乎可以肯定，设备会被烧坏。

不要让设备过热，计算机和其他网络设备有内置的风扇进行冷却，所以不要挡住设备的通风出口。此外，确保将计算机放置在坚固的地方，震动和突然的打击都会使计算机内部的组件松动而发生故障。

18.3.1 电源条件

要保护你的设备免于不规律电流的破坏。最简单的方法就是对网络和计算机设备采用单独的电路，这样做能够解决一些电源产生的问题，但不是全部。下面列出了其他一些能够控制不规律电流的设备：

- **隔离变压器**（*Isolating transformer*）——控制电压穿刺和高频噪音。
- **稳压器**（*Regulators*）——不管线路电压如何变化，在长时间内维持一个恒定的电压。稳压器能解决诸如电压过低和浪涌等问题。
- **线路调节器**（*Line conditioner*）——有着内置隔离变压器的稳压器。
- UPS——先给电池充电，然后给计算机供电。这种设备允许计算机在电源失效的情况下也能工作。注意，有两种UPS：在线式和后备式。大多数不很昂贵的设备配置的都是后备式UPS，它们只在电压低于80~90V的时候才提供电源。价格比较昂贵的在线式UPS是真正意义上的UPS，它们实时监控电源线路状况，并给计算机供电。

18.3.2 EMI和RFI

网络通信的另外一个问题的根源实际上是设备本身。计算机部件，如电源和监视器，还有荧光、大的电机和电缆都能产生电磁干扰（EMI, electromagnetic interference）和无线电频率干扰（RFI, radio frequency interference），其他的设备或没有良好屏蔽的线缆能够吸收它们。它们造成的问题是：有些时候，设备的一些部件会失效，但那些部件的失效看起来又是由于其他部件引起的，像这样的问题很难诊断，并且需要专门的诊断软件和硬件来检测。

18.3.3 软件病毒

前面讲述的影响网络性能的因素都是物理方面的。影响网络性能的另一个因素是软件——特别是那些存在的惟一目的就是干扰网络正常运行的软件。下面介绍了几种这样的软件。

蠕虫（worm）是通过计算机来繁殖自己的程序，通常是在一台计算机的内存里复制它自己。蠕虫可以非常快的速度来复制自己从而导致计算机崩溃。蠕虫由不同的“片段”组成，它有时仅仅出于“好玩”的目的，有时是恶意攻击，在你不知不觉中就进入计算机或网络系统。*蠕虫*一词来自一本科幻小说，现在一般被术语*病毒*（virus）替代。

病毒是能将自己复制进其他文件从而“感染”计算机文件的程序（通常是一些可执行程序）。它通常是采用如下的方法：当一个被感染的文件被调入内存时，它其中的病毒代码就被执行，病毒代码就能够去感染其他的文件，并且继续下去。病毒通常都有破坏性的结果。最新的病毒变种可以通过因特网以电子邮件附件的方式传播。

特洛伊木马（trojan horse）是伪装成游戏或者应用软件的破坏性程序。当它运行时，特洛伊木马偷偷的对计算机做一些隐蔽操作，然而看上去却像是对计算机做一些有用的工作。

后门是设计者或维护人员故意在系统中留下的安全漏洞。一些操作系统出厂的时候就设置了一些特权帐号以便他们的技术支持人员和厂商维护程序员使用。一个较安全的方法是删除掉系统存在的缺省帐号。后门并不是病毒（也不是特洛伊木马），但它也有着跟它们一样的安全问题。

下面几个提示能够帮助你的计算机或网络防止感染病毒：

- 小心从不明渠道得到的软件。很多时候，通过非法渠道发布的软件是病毒的主要载体，这是因为没有任何系统来检查这些软件。
- 防止别人在你的计算机上使用他们的软盘。任何类型的文件都能够携带病毒——并不需要是可执行文件，即使是一个数据文件，也有可能里面包含着病毒。
- 在所有计算机上使用最新的病毒检测软件，许多公司都出售或提供这样的病毒检测软件。

还有许多检测和防止病毒感染的方法，不在这里一一赘述了，如果你担心病毒问题，可以通过因特网获得其他的说明和报告。

18.4 网络性能

网络管理中，与网络安全和冗余一样，网络性能也是需要重点考虑的另外一个因素。网络性能是对网络速度和可靠性的衡量。为了说明这点，我们拿汽车来和网络进行一个很好的比较：你需要你的汽车锁的很牢靠（安全）和有宽大的空间（冗余），但这还只是一部分，你还需要考虑你的汽车从0加速到60km/h需要多长时间（速度），还有它的刹车工作怎么样（可靠性）。

需要经常对网络性能进行检测，以判别网络性能是否维持在一个可接受的水平。继续我们上面的对比，如果你的汽车性能不是很好了，你可以对它进行维修。网络和汽车的区别在于汽车是从同一个汽车模型里出来的，它们有着相同的性能指标；但网络不是这样：计算机和网络硬件、软件以及线缆的每一种不同组合都会产生不同的网络性能。为了判别网络性能何时较差，需要一个进行性能比较的标准值。这个标准称为*基准*（baseline）性能。基准性能是在网络安装良好并且配置正确的时候测量的。

为了测量基准性能，你可以使用一些网络监控软件包或工具，如Fluke的LANMeter和Windows NT的网络监视器程序。这些工具能够记录几种类型的网络性能数据，如网络带宽使用率、冲突数、错误帧数和广播流量。有了网络系统在最优情况下记录的基准性能，你就可以用它来与网络的实际性能做对比，从而判断网络的“健康”状况。

当网络发展或改变时，你也需要像更新其他文档一样，随之更新基准性能。当升级硬件时，需要升级控制硬件的软件驱动程序。如果你进行软件升级或安装一个新的程序，可能需要重新安装某种服务或安装软件公司提供的补丁包。安装了新的硬件，旧的软件驱动程序有可能无法利用新硬件的特性或者根本就不能兼容，这会造成性能严重下降，这时，你应该重新安装驱动软件来解决这种问题。

当你对网络做出改变时，比如说把某台设备的一部分移到另一台设备上去（如图18-8），那么

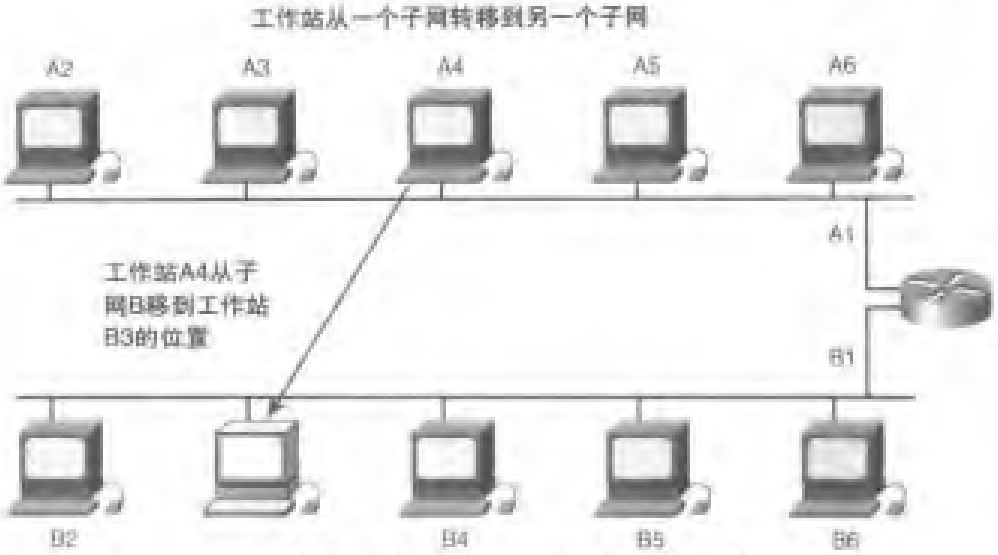


图18-8 PC从一个网段迁移到另一个网段

在进行新的基准性能测量之前，必须先要确认这部分设备在新的网段运行正常。当你要对某个网段进行更改以减少网络流量时，这一点非常重要。因为即使某台设备在它原来的网段运行正常，当它换到一个新网段之后也可能出问题，这样就会对网络性能产生严重影响。所以，在设备迁移之后，一定要确认设备工作正常——包括网络功能的正常和所有关键应用程序运行的正常。

18.4.1 服务器管理

网络管理员需要了解两种类型的网络：对等体到对等体网络和客户机/服务器网络。图18-9显示了对等体到对等体网络，它也称为工作组网络。对等体到对等体网络是为数量较少的工作站设计的，Microsoft建议在对等体到对等体网络中不要超过10个用户。

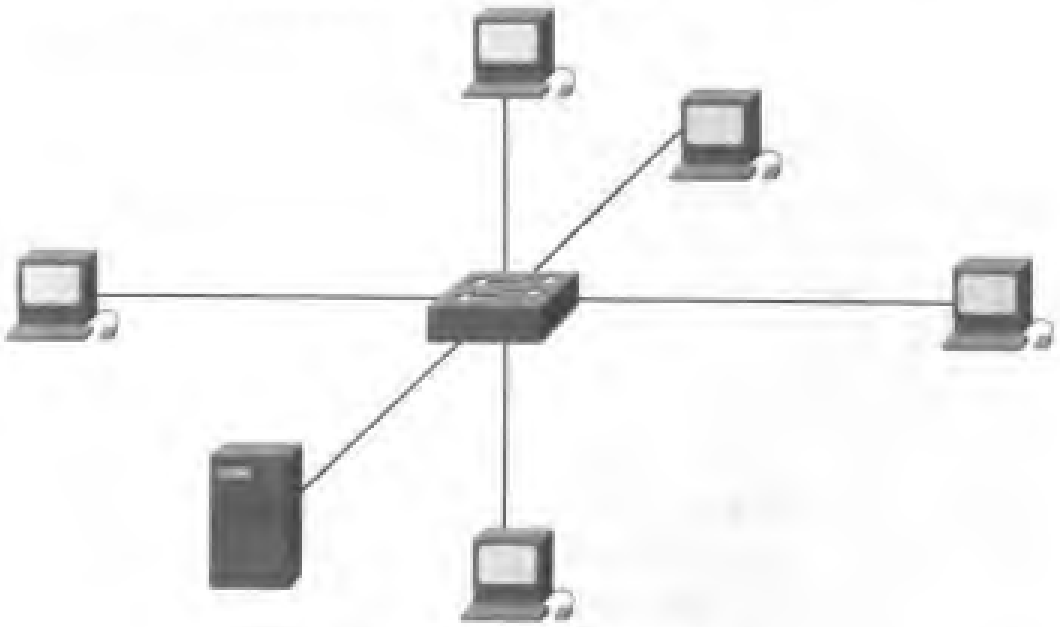


图18-9 对等体到对等体网络

对等体到对等体网络的优点是建立和运行费用比客户机/服务器网络便宜，它允许用户控制它们自己的资源，并且它不需要专用的服务器以及除了一个合适的操作系统之外的其他专门软件。它的缺点是：没有提供一个管理中心点，每个用户必须为访问他的资源的其他用户建立ID；每当一个用

户改变了密码，你必须改变共享资源上的所有密码；如果一个共享工作站关机了或者因为其他原因不可访问，那么它上面的资源就不可用了。最后一个缺点是上面已经提到过的：如果现在的用户已经超过了10个或者马上就要超过10个，对等体到对等体网络就不是一个好的选择。对等体到对等体网络操作系统有Windows fro Workgroups、Window 95、Windows 98和LANtastic。

18.4.2 客户机/服务器网络

另一种网络类型是客户机/服务器网络，如图18-10所示。网络操作系统是客户机/服务器网络的核心，这些系统控制LAN上面的资源和管理。

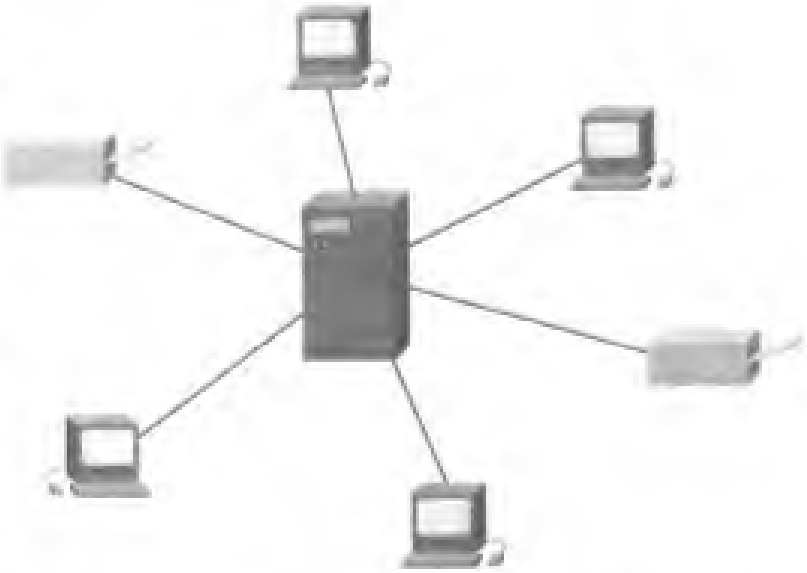


图18-10 客户机/服务器网络

客户机/服务器网络的优点有：用户、资源和管理的集中性；专门的服务器能够更有效的向客户机提供特定的资源；此外，网络能够用一个网络ID和密码提供所有的可允许的资源访问。

客户机/服务器网络的缺点是网络中存在单点故障问题：如果服务器关机了，就没有可供客户机使用的资源了。事实上，客户机如果没有服务器的支持的话，有可能根本就不能运行；网络操作和维护需要经过专门培训的人员来承担；特殊的网络软件和硬件也提高了网络运行的成本。即使有这些缺点，但客户机/服务器网络仍然是超过10个用户的公司的惟一选择。客户机/服务器网络操作系统有AppleTalk、UNIX、Novell NetWare和Windows 2000/XP。

UNIX操作系统有着许多变种，每种都由不同的公司来设计开发。如Sun Microsystems、IBM、Hewlett-Packard和Santa Cruz Operation（SCO）等公司都有着自己的UNIX操作系统。UNIX也有免费版本，如FreeBSD和Linux，后者在当今很流行。

UNIX是一个多用户操作系统，并且支持多进程、多任务和多线程技术。UNIX是基于内核的，内核把计算机硬件层和上层应用程序分离开。UNIX一般采用网络文件系统（NFS，由Sun Microsystems开发），NFS提供了服务器上的文件和目录安全访问。UNIX也提供了用户和资源的集中控制。因为有许多不同的UNIX版本，很难对这些所有的版本做一个对比。上面介绍的一些内容都是UNIX共有的特点。能和UNIX配合良好的客户端软件一般也是由操作系统开发者自行开发的。

在讨论NetWare和Windows NT前，很有必要介绍一下这些年来它们的不同版本。NetWare经过了3.X版本、4.X版本和5.X版本的发展，这些版本的主要区别在于对目录服务的处理不同。

NetWare 3.12版本使用一个名为"*装订所*"（bindery）的对象来管理用户和资源。装订所服务的缺点在于它虽然建立了一个服务器中心网络，但它把每台作为控制点的服务器单独看待。这就产生了多服务器网络问题：每一台服务器仍然为每一个用户单独建立一个帐号，即使这些密码可以被同步并且可以实现改变一台服务器上密码就能改变所有服务器上的密码。正是这个缺点使得集中性管理变得复杂起来。公平的讲，它的这个缺点是有它的时代烙印的，3.12版本发行的那个年代，多服务器网络还没有快速发展起来。并且，NetWare 4.11版本对这个问题做了很大的改进。

NetWare 4.11版本和5.0版本使用名为*Novell 目录服务*（NDS，Novell Directory Serives）的对象来管理用户和资源。它们比起3.12版本的优势在于Novell 目录服务建立了一个服务器中心网络，而且它把整个网络当成一个控制点来看待。这样就加强了单点管理，并且只把服务器仅仅当作网络

内容中的一个对象，这就允许用单个帐号和密码就能授权用户访问网络上的所有资源，使得网络组织和管理更为简单。

所有的NetWare版本都使用两种文件系统的组合：一种是文件分配表（FAT），这也是DOS使用的文件系统；另外一种是目录项表（DET），这是Novell专有的文件系统，它提供了服务器上的文件和目录安全。NetWare的客户端软件非常广泛，包括所有版本的Windows、DOS、Macintosh和OS2。NetWare的强大之处在于它的用户和文件资源管理。

Windows NT是我们最后讨论的操作系统，它包括两个Windows NT版本：Windows NT 4.0和Windows 2000（也被称为Windows NT 5.0）。Windows NT 4.0服务器版本和工作站版本是和Windows 95一起开发的，因而有着相似的用户界面，这也给Windows家族产品提供了一致的“视听感觉”。Windows NT通过“域”的使用来进行用户和资源管理（如图18-11）。域是受服务器控制的用户和资源的一个逻辑组，也被称为主域控制器（PDC）。域也支持一个名为*备份域控制器*（backup domain controllers，BDC）的辅助服务器，它平衡PDC的工作负载并且给用户和资源对象管理提供冗余。

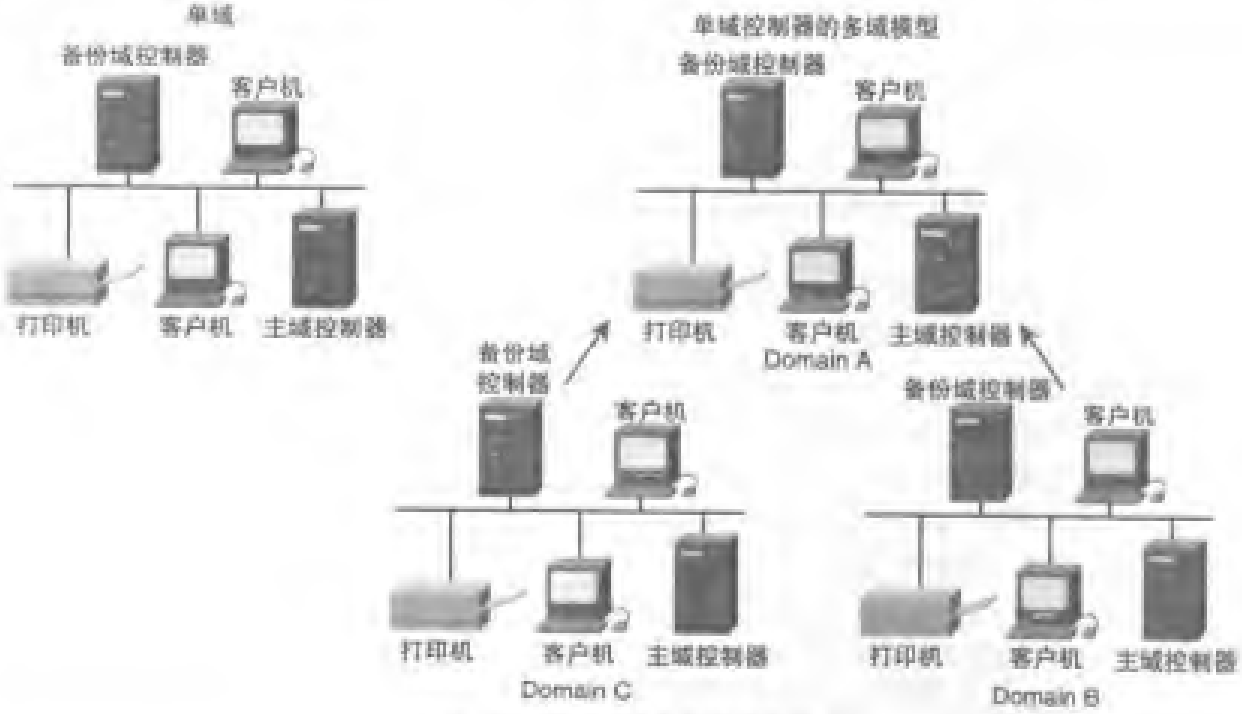


图18-11 NT 4.0版本和多域布局

第3种类型的服务器，称为*独立服务器*（standalone server），也可以存在于域中。这种服务器的建立是为了支持某种特定的应用，并专门为那种应用来提供它的资源。域的另外一个变种是*多域模型*（multidomain model），在这个模型里，几个不同的域由信任/被信任关系连接起来，这使得用户能够跨域使用资源。

Windows 2000服务器也是基于NT技术的，但是，管理结构从域转变为活动目录结构。活动目录是基于网络中心模型的，而不是基于域中心模型，这点跟NDS一样。

Windows NT和UNIX一样：它是支持多进程、多任务和多线程的多用户操作系统，也是基于内核的，由内核将底层硬件和上层应用软件隔离开。它使用FAT16文件系统和NT专有的文件系统——新技术文件系统（NTFS）。采用FAT16，Windows NT只能提供目录（也称为文件夹）级别的安全，不能提供单独的文件安全性。NTFS提供了文件级别和目录级别上的安全性。

Windows NT提供这些文件系统的原因是它要能和其他的不同操作系统共存于同一台机器——这并不意味着两种操作系统能够同时运行。为了能让别的操作系统访问NT自己的文件，NT上的文

件系统必须为FAT16。需要指出的是，Windows 95和Windows 98支持FAT32，但Windows NT不支持。因此，在同一台计算机上运行Windows NT和Windows 95时文件系统的选择应该是FAT16。Windows NT和它自己的客户端——Windows NT工作站，运行起来配合最为良好，但它也能和其他一些客户端操作系统良好运行，如Windows for Workgroups，Windows 95，Windows 98和Macintosh。

不管采用何种网络操作系统，NOS的主要功能都是对网络进行控制。这可通过建立用户权限、帐号（用户ID）、密码和组以及系统配置文件和策略来实现。这些术语将会在下面的章节分别讲述。

18.4.3 网络控制

登录帐号用来鉴别网络系统上的网络用户。帐号和用户密码一起用来识别用户并且授予他访问网络系统资源的权力。账号也决定着用户应对其在网络上的活动负责，这应该在本章前面的安全性文档中规定网络用户有了一个帐号并不意味着网络资源对这个用户完全可用，用户的权限决定了用户的资源可用性。

管理员为用户设置权限，允许或拒绝他访问网络上的特定资源。例如，即使一个用户已经连上了网络，一台打印机也连上了网络，但这个用户也有可能不能使用打印机来打印——如果管理员没有为该用户设置允许使用那台打印机的权限的话。相反，如果管理员为这个用户设置了*允许*使用的权限，那么该打印机就是可用的了。跟打印机一样，数据和应用程序以及所有网络上的其他“资源”，都有着上面所讲述的权限设置问题。给用户分配权限的时候还有一个可管理性问题：如果有大量的用户，那么给每个用户分配或修改权限将会占用管理员大量的时间，那么怎么解决这个问题呢？答案是使用“组”。

组是网络用户的一个逻辑集合，管理员给组设置权限和许可而不是直接给单独的用户进行设置，如果用户需要这些权限，则只需将他指定到这个组即可，这样用户就被授予了那个组的权限。当某个用户的权限需要修改时也是一样，组的权限的改变意味着所有组成员的权限的改变。需要指出的是：不是说不能单独为用户进行权限设置，而是说在大型的网络环境中，使用组效率更高一些。

策略和***配置文件***（profile）对系统资源没有任何影响，它们只负责用户如何与工作站进行交互。配置文件允许用户自定义他的计算机使用界面，并允许网络上的任意计算机使用该配置文件，这称为漫游配置文件。还有一种配置文件，它的特点是对每一个用户提供相同的用户界面，不允许做出改变，这称为***强制配置文件***（mandatory profile），它主要用于许多用户都要物理的使用同一台计算机的场合。如果用户所有的工作都是在一台计算机上完成，不需要使用别的计算机，那么，他可能只需要一个本地配置文件。本地配置文件存放在本地计算机上，而不是像上面两种那样存放在网络上。

策略负责控制本地计算机上的资源。如一个防止用户在本地工作站的硬盘或软盘上存储数据的策略可以提升系统的安全性，因为它可以防止数据被泄露出去。策略也可以防止用户无意中更改他们的系统设置。如工作站的显卡设置、硬盘设置和网卡设置，对大多数用户来讲，都是不需要更改的，如果这些属性被改变了，那么就会给网络维护人员带来很多不必要的工作。

上面我们讨论过的所有内容现在可以来个小结：网络权限、登录帐号、密码和组，还有配置文件和策略给系统管理员提供了一个控制访问、限制网络服务和控制本地用户工作站的方法。网络管理员实际上也是一个权限集，并被授予了网络上的最高特权。不是所有的用户都有权限去改变其他用户的权限的，这样的权限只保留给具有管理员权限的组。如果你是这样组中的一个成员，那么可以告诉你，你也是一名管理员了。

18.5 网络管理中行政管理的一面

网络到底是什么？这是个很重要的问题。网络是一系列相互作用和通信的设备构成的统一系统。当一个网络管理员审视他的网络时，他应当把它看成一个整体，而不是一些单独部分组成的集合。

换句话说，网络中的每台设备都影响着其他的设备，因而网络是一个整体。如图18-12所示，没有什么设备在连入网络后还是孤立的。



图18-12 基本网络架构

网络的一个好的对比例子是汽车。汽车是一些零件的组合，来提供运输功能。发动机提供汽车的动力，但是如果供油系统出问题或轮胎没气，那它也不能运转良好。刹车是一个重要的部件，但反过来，如果没有液压系统，刹车就不能工作，汽车也就不能停下来。总而言之，没有所有零部件的一起工作，汽车就不能完成它指定的任务——运输。

网络系统也是这样。如果网络服务器安装了IPX/SPX协议，而主机没有安装，那么它们就没法通信。同样，假设系统原本工作良好，但网络管理员更改了一端的协议，那么系统就会停止运行。一台设备影响了其他设备的功能。另外一个例子，有一台DNS服务器，IP地址是192.150.11.123，所有的主机都设置了这台DNS服务器，但如果某个技术人员更改了DNS服务器的IP地址，但没有改变主机上的设置，那么，主机就不能再拥有DNS服务了。

在处理网络问题的时候，需要记住一个重要的观点：把网络看成一个整体，而不是一系列被连接起来的设备。这个观点也同样适用于连接因特网的广域网连接：当你对本地路由器做出修改时，将会直接影响你的整个系统通信的效率和可靠性。

18.5.1 理解和建立网络的管理界限

在一个企业网络中，网络管理人员知道他们的责任是很重要的。给用户的桌面系统进行查错是网络管理人员的责任吗？网络管理人员是不是只需要判断用户的问题与通信是否有关就行了？网络管理人员的责任是只延伸到用户接线面板呢，还是延伸到网络接口卡？

这些责任的定义对网络部门来说是很重要的，因为它影响到每个人的工作强度和企业网络服务的成本。网络部门的责任越大，那么它的资源成本也就越大。想象一个餐馆，它的所有者和运营者都是一个人，他负责所有的工作，包括烹饪、上菜、洗碗和结帐。那么这个餐馆的人力资源成本是相当低的，但是它的成长和扩张的机会也是有限的——除非餐馆的所有者雇佣专门的厨师、服务员、杂工和结帐员。当这些责任被细分后，餐馆就能更有效的为更多的客人服务了。当然，随着它的发展和扩张，资源成本也会上升。

跟上面餐馆的例子一样，网络支持的工作可能包括网络的所有方面，或只限定于某一部分。

这些责任的划分应该是基于部门—部门之间的关系来定义和执行的。正确的定义这些关系的重要性在于：如果你把某个部门的责任域划分的很大，那么会给那个部门的资源带来极大的压力，但

如果你把责任域划分的太小，那么又很难高效的解决网络上的问题。

18.5.2　网络成本

网络管理员还需要承担很多责任，其中包括成本分析。成本分析不仅仅包括网络设计和实现的成本分析，还包括网络维护、升级和监控的成本分析。决定网络安装的成本对大多数网络管理员来说并不是件很困难的工作：所需设备的成本马上就可以计算；人力成本也可以用一个固定的价格来算出。然而，搭建网络的成本仅仅是成本分析的开始，其他一些你必须考虑的成本因素包括：

- 网络今后的发展所需的成本。
- 技术和用户培训。
- 维修。
- 软件配置。

这些成本因素的计算比起搭建网络的成本计算要困难的多。网络管理员必须能够看到公司网络的历史和成长趋势，以决定出网络发展的成本。而经理必须衡量新软件和硬件的价格来决定公司是否需要安装它们（和什么时候安装）；还要决定如果要支持这些新的技术，还需要什么样的员工培训；那些运行关键业务所需的冗余设备的成本也应当加入到网络维护的成本中去。考虑一个使用一台路由器接入因特网的公司，如果那台路由器坏了，在它没有被更换之前，公司就没有生意可做，公司也许会因此损失上千美元，所以，一个明智的网络管理员会准备一个备用路由器来尽量减少公司断网的时间。

18.5.3　错误报告文档

有效的网络管理还需要通过文档来实现。当一些问题出现时，应该生成一个错误文档报告，如图18-13。这个错误文档用来收集出错的基本信息，这对尽快判别网络问题是很有必要的；文档还提供了跟踪问题解决进度和问题的最终解决方案；文档报告也为高级管理人员决定是否雇佣新员工、购买新设备和向员工提供培训提供了参考。此外，文档也提供了已解决问题如果再次发生时的解决方法。本章中上面所讲述的所有内容都是关于网络管理中的非技术性因素的。下面将讲述一些用于广域网（WAN）中监控和诊断问题的工具。

计算机维修工作表 每计算机一份		
计算机名字：		日期：
问题类型：	硬件：	软件：
问题描述：		
是否在保修范围：	是：	否：　维修点：
维修说明：		
技术人员：		
付费部门：		
审批者： 注释：		

图18-13　错误报告文档

18.6　网络监控

存在着很多需要对网络进行监控的理由，其中最主要的两个是：预计网络将来的发展和检查网络状态的异常变化。异常变化包括路由器或交换机的失效、黑客试图非法入侵网络或链路通信失败。如果没有对网络进行监控的能力，管理员就只能被动的在这些问题发生后做出反应而不是主动防止这些问题的发生。

在前一节中，网络管理主要集中在LAN，监控一个广域网的很多基本管理技术与管理LAN相同。一个主要的区别就是设备的物理位置。监控工具的位置和使用是保证城域网不间断运行的关键。

18.6.1 连接监控

网络上每天都在进行一些最基本的连通性监控，用户登录到网络的过程就是确认连通性是否正常的过程，如果不能正常登录，网络部门马上就接到报告。但是，这不是连通性监控的最有效的或最可取的方法。还有一些简单的程序能够让管理员输入一串IP地址，程序然后就周期性的对这些地址发ping分组，如果没有得到响应，程序就向管理员发出警告。这也是一种低效的、原始的网络监控方法，但有总比没有好。这种网络监控方法的另外一个缺点是：它只能确定在监控工作站和目的设备间的某个地方出了问题，可能是交换机、路由器或其他任何网络设备，但它不能告诉你到底是哪个地方出了问题。在WAN上，采用这种方法监控所有的主机会耗用很大的资源，如果网络有3,000台主机，那么对所有的主机和设备发ping分组，将会使用大量的网络资源，所以比较好的方法是只对一些关键主机、服务器、路由器或交换机发ping分组以检测它们的连通性。还有，Ping测试方法当主机关机的时候就不能给出真正的连通性结果，所以，这种监控方法只有当别无选择时才被采用。

18.6.2 通信监控

通信监控（traffic monitoring）是一种更复杂的网络监控方法。它检查网络上的实际分组通信并基于这些网络通信来给出报告。如Microsoft Windows NT的网络监控程序和Fluke的网络分析器程序都是这类软件的例子。这些软件不仅仅可以检查出失效了的设备，而且还可以发现哪些设备负载过度或配置错误。它们的共同缺点是：在某个时候只能工作在一个网段上，如果需要收集其他网段上的数据，那么监控软件就要转移到那个网段上去，这一点可以通过在远程网段上使用代理来解决（如图18-14）。像交换机、路由器这些设备的操作系统本身就能够产生和传输流量统计数据，但这些数据怎样被收集和组织到一个中心位置而供网络管理员分析呢？答案是：*简单网络管理协议*（Simple Network Management Protocol—SNMP）。

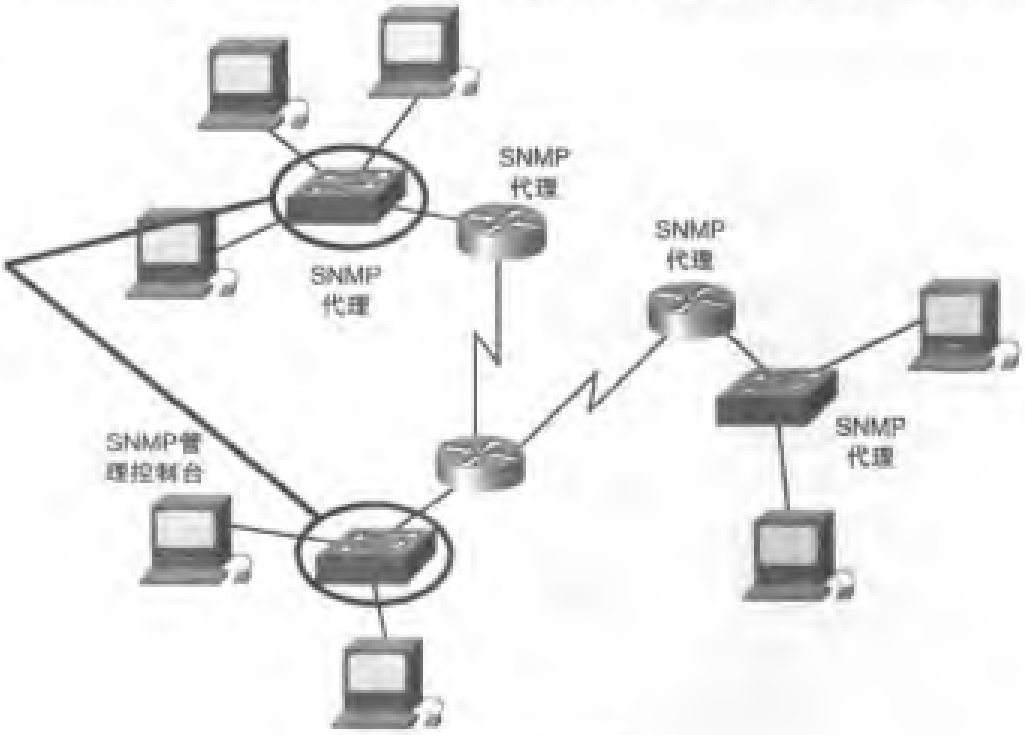


图18-14 SNMP结构

18.6.3 SNMP

SNMP是允许被管理设备通过网络将统计数据传输到中心管理控制台的协议。SNMP是网络管

理体系一个组件，它包括如下4个主要组成部分：

- **管理控制台（站）**（*management console (station)*）——这是网络管理者进入网络系统的界面。它运行着处理数据和控制网络的程序。管理工作站也维护着一个从被管理的设备那获取的管理信息数据库（MIB）。
- **管理代理**（*management agent*）——这是包含在被管理设备内的组件。网桥、路由器、集线器和交换机都可能包含SNMP代理来允许管理工作站控制它们。网络代理对管理工作站的响应方式有两种：首先，通过轮询的方式，管理工作站向管理代理请求数据，然后代理以应答数据作出响应。其次，代理向管理工作站主动汇报数据（诱捕信息），这种方法可以减少网络上的流量和被监控设备上的处理过程，因为它不是依靠管理工作站以一定间隔持续的向代理查询数据，而是在被管理设备上设置阈值（最大或最小值）。如果超过了这些阈值，被管理设备就向管理工作站发送报警信息。这就避免了管理站向网络上的被管理设备进行连续的轮询。诱捕非常适合需要管理大量设备的场合，它因减少了网络上的SNMP的流量而给数据传输提供了更多的带宽。
- **MIB**——这是驻留在每台被管理设备上的数据结构。这个数据结构包含一系列对象，它们是被管理设备收集到的资源数据。MIB中包括如端口界面数据、TCP数据和ICMP数据等信息类别。
- **网络管理协议**（*Network management protocol*）——这是SNMP使用的协议。SNMP是一个应用层的协议，它设计为在管理工作站和管理代理之间进行数据通信。它有3个关键功能：一，从被管理设备获得管理数据的能力；二，把管理工作站对被管理设备进行设置的数据发送到代理的能力；三，接收被管理设备发出的重要事件信息（诱捕信息）。在简单网络管理协议中最需要理解的关键词是*简单*（Simple）一词：当SNMP开发出来的时候，它只是作为一个马上就要被取代的短期系统来设计的，但是结果跟TCP/IP协议一样，SNMP发展成了因特网/内网网络管理的主要标准。在过去的这些年里，SNMP经过了许多改进，监控和管理能力得到了很大的提高。SNMP最重要的功能扩展是*远程监控*（Remote Monitoring，RMON）。RMON的引入使得SNMP可以真正将网络看成一个整体而不是一系列单独的设备的集合。

18.6.4　远程监控

在RMON中是由探针来收集远程数据。探针有着和SNMP中的代理相同的功能，但探针有RMON特有的能力，网络代理没有。当你使用RMON的时候，也跟SNMP一样，中心管理控制台是数据收集中心。RMON探针位于每个被监控的网段，这些探针可能是专门的主机、或位于一台服务器内、或嵌入在网络设备内——如路由器或交换机。探针从每个网段收集指定的数据并把它中继到管理控制台。冗余的管理控制台能给网络管理过程带来两个主要好处：第一，能够给在不同地方的多个管理员（如一个在纽约，一个在盐湖城）提供监控和管理同一网络的能力；第二，冗余的真正意义所在是，如果一个控制台失效了，那么第二个控制台仍然能够来监视和控制网络，直到第一个控制台修复为止（如图18-15）。

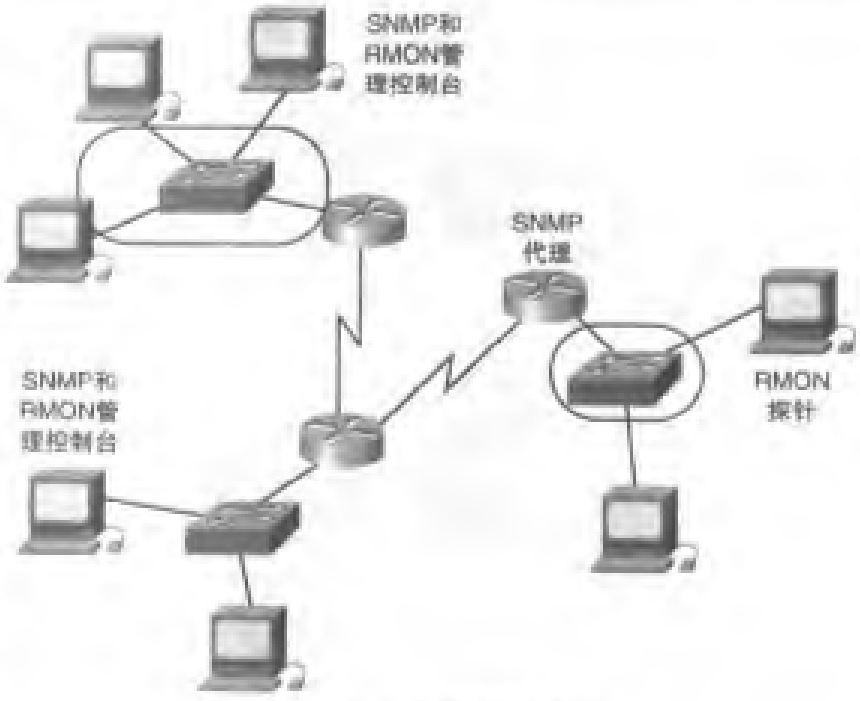


图18-15　双管理控制台网络

SNMP协议的RMON扩展创建了新的数据类。这些数据类给MIB数据库加入了新的分支。这些新的数据类如下：

• **统计组**（*Statistics Group*）——包含对每一个监控网络收集到的统计数据。这些统计数据包括字节、分组、错误和帧大小的计数器（从零开始增长）。另外一种数据类型是索引表，索引表能够区分被监控的以太网上的设备，这就可以为每一台以太网设备分别保存一个计数器。统计组通过对以太网上各种错误的统计，如循环冗余校验（CRC）错误、冲突和过大、过小分组，提供子网的总体负载情况和运行情况。

• **历史组**（*History Group*）——在一个指定的时间段内，对统计组的计数器进行取样并记录的一个数据表格。默认的取样时间是30分钟（1,800秒），默认的表大小是50个条目，能够进行25小时连续不断的监控。因为历史组是为某个特定的计数器创建的，在每一个取样间隔，只要条目数到达50，当新的条目创建时，旧的条目就会删除。因此，这种取样形式提供了网络的基准性能，它可以用来与原始基准性能作对比来解决问题或当网络调整时来进行基准性能更新。

• **报警组**（*Alarm Group*）——使用用户指定的界限，称为阈值（thresholds）。如果被监控的数据计数器超过了阈值，那么就向指定人员发送消息或警告。这个过程，也叫做错误捕捉，它能够使网络监控的许多工作自动完成，而不需要有人经常的、直接的监控网络或等用户来发现网络中的问题。网络进程能在发生错误，特别是更严重、更紧迫的错误的时候，自动向网络人员发送消息。这是抢先式故障排除的一个重要组成部分。

• **主机组**（*Host Group*）——对子网段上发现的每台主机维护着的一个计数器集合。计数器类别有分组、字节、错误和广播等。每一种类别又有不同的计数器类型，如分组计数器有总分组数、接收到的分组和发送的分组，还有一些和特定的项目相关的计数器类型。

• **主机前N位组**（*Host TopN Group*）——提供一组基于某个测量参数的前N台主机的报告。对这个组进行说明的最好方法是举例。例如，可以提供一个每天产生的广播数最多的前10台主机列表和每天发送分组最多主机是哪台。这样，就可以很容易的判断是谁、是什么样的数据流量占用了于网络带宽。

• **矩阵组**（*Matrix Group*）——记录子网段上的两个主机间的数据通信。数据以矩阵（多维表格）的形式存放。从中可以产生哪台主机被用作服务器等结果。重新组织这些数据还能产生其他的报告，如可以显示一台指定服务器的所有用户的报告，或一个指定的用户使用的所有服务器的报告。

• **过滤组**（*Filter Group*）——提供给管理控制台一种指示RMON探针收集特定网段上特定数据的方法。这种选择是基于两种过滤器的：数据过滤器和状态过滤器。数据过滤器设计为符合或不符合特定的数据模式，这就允许选择特定的数据。状态过滤器是基于分组表现出来的类型进行过滤的，如CRC错误分组或合法分组。这两种过滤器能够通过逻辑“与”和“或”来组成复杂的判别条件。过滤组能够使网络管理员得到不同类别的分组的数据，从而更好的对网络进行分析和故障排除。

• **分组捕获组**（*Packet Capture Group*）——允许网络管理员使用过滤组设置的方法来捕获特定的分组。通过捕获分组，网络管理员能分析捕捉到的、满足过滤器条件的分组内容的细节信息。这个组记录了捕获到的单个分组的数量，也记录了总共捕获到的分组的数量。

• **事件组**（*Event Group*）——在MIB数据库中记录其他的组产生的事件。如在报警组中，某个计数器超过了阈值，这个事件就可以在事件组中产生一个事件。基于这个事件，就可以产生相应的反应，如给所有列于报警组中的人员发送消息或在事件表中创建一个记录条目。RMON MIB扩展中的所有对比操作都产生一个事件。

• **令牌环扩展**（*Token Ring Extension*）——令牌环网络上的特定计数器。尽管在RMON扩展中的大多数计数器是与数据链路协议无关的，但统计和历史组却是相关的。它们和特定的以太网协议组合在一起。令牌环组产生使用RMON监控和管理令牌环网络的计数器。

记住RMON是SNMP协议的扩展，这就意味着，尽管RMON加强了SNMP的操作和控制功能，但RMON仍然需要SNMP才能工作。最后指出一点，SNMP和RMON都有了新的版本，如SNMPv2c、

SNMPv3和RMON2，上面所讲述的内容并没有包括这些新版本中的新特性。

18.7 网络故障排除

问题出来了！即使网络处于监控状态、设备是可靠的、人员也很小心，但问题还是出来了。衡量一个网络管理员是否称职的标准是：在导致公司业务中断的网络错误的压力之下，是否有能力去分析、查错并且尽快解决错误。本节中介绍了网络上的一些故障排除技术并提供了一些故障排除工具。对先前提到的故障排除技术和一些其他技术进行概述。如先前所述，这些技术能够成为解决网络问题的最好工具。

网络故障排除的第一步，也是最重要的是使用你的工作日志来作好记录。一个好的记录能为诊断问题理出一个清晰的思路：它能告诉你你已经做了哪些工作，结果怎样？这些对故障排除者来说是极其重要的，它能保证你前面所做的尝试不会在以后无休止的被重复。记录副本对其他的技术人员来说也是很有价值的，它防止当这个问题又出现的时候，他又要重做所有的工作。这份记录还应该包括这个问题出来的时候网络上呈现出来的各种异常迹象，这可以为以后可能发生的相似问题提供参考。

抢先式故障排除的另外一个基本要素是标记。标记所有的东西，包括水平线缆的每一端。标记不应该只包括线缆的数量，还要包括另外一端在什么地方，用途是什么，是用作声音、数据还是影像。这种标记在故障排除时比布线对照布还要有价值，因为它指出了设备单元的具体位置，而不只是图上的某个地方。还要标记集线器、交换机或路由器的位置、每个端口、连接点等等，这些都能够加快网络问题的解决。

最后，所有连入网络的组件都需要标记它们的位置和目的。有了这种标记，所有组件的位置，和它们的用途都可以很容易的定义。正确的标记，配合网络创建之初或更新时建立的网络文档，给出了网络的一个完整图像。另外一个重要的提示是：文档只是对它代表的现在有用，如果网络有了改变，那么有关设备和布线的文档一定要随之改变。

18.7.1 故障排除过程

网络故障排除的第一步是定义问题。问题的定义可能是来自不同的信息源。其中之一可能是系统维护部门的报告，它只是大概的描述了问题的情况；接着，你可能要和发生问题的用户进行电话交谈，和他讨论问题，收集更多的信息。网络监控工具能提供关于你要解决的问题的更全面的信息，其他的用户和你自己的观察也能提供一些信息。分析所有的这些信息，而不是某一个，可能会给你一个更明确的故障排除出发点。网络故障排除是一个系统的在网络上解决问题所应用的过程，一个好的查错技术是使用科学的方法，如下所示：

步骤1 确认网络/用户问题。
步骤2 收集网络/用户问题数据。
步骤3 分析数据，提供一个解决问题的可能方案。
步骤4 实现这个方案，试着解决问题。
步骤5 如果问题没有解决，恢复到解决问题前的网络和数据情况。
步骤6 回到步骤3，进行下一轮。

18.7.2 故障排除的各种技术

排除和隔离是实现科学的查错方法最为有效的技术。
下面介绍这两种技术：

1 排除法的过程

假设你网络上的某个用户呼叫系统维护中心，报告他的计算机上不了因特网了。维护中心填写

好错误报告，提交到你——网络支持部门。

你打电话找那个用户，他告诉你，他什么也没做，就是上不了因特网。你检查一下网络硬件记录，发现那个用户的计算机昨晚进行过升级。于是，你首先联想到可能是他的计算机网络驱动配置有问题。于是，你到他那里检查他的网络配置信息，但是，这些信息看上去是正确的，于是，你ping那个网段上的服务器，结果不正确，如例18-1所示：

例18-1 错误的ping输出（请求超时）

```
C:/ping 110.0.1.1
Pinging 110.0.1.1 with 32 bytes of data:
Request timed out.
Request timed out
Request timed out
Request timed out
Ping statistics for 110.0.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

下一步是检查工作站的网线是否插好，你检查了网线的两端，连接没有问题，试着再ping服务器，还是错误。接着，你ping 127.0.0.1，这是计算机的环路地址（如例18-2），ping成功了，这就排除了计算机、驱动配置和网络接口卡出错的可能。

例18-2 回环ping输出

```
C:/ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Ping statistics for 110.0.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

你怀疑该网段上的服务器可能有问题，另外一台连网的计算机就在旁边，于是你到它上面去ping服务器的地址，结果成功了（如例18-3）。这就排除了服务器、主干和服务器到主干的连接性问题。

例18-3 成功的ping输出

```
C:/ping 110.0.1.1
Pinging 110.0.1.1 with 32 bytes of data:
Reply from 110.0.1.1 bytes=32 time=1ms TTL=128
Reply from 110.0.1.1: bytes=32 time=1ms TTL=128
Reply from 110.0.1.1: bytes=32 time=1ms TTL=128
Reply from 110.0.1.1: bytes=32 time=1ms TTL=128
Ping statistics for 110.0.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

现在，你到了IDF，把那台工作站接到另外一个端口上去，还是ping不通（如例18-4）。这就把

错误限定在水平线缆上了，接下来，更换一条水平线缆，再ping，这次成功了（如例18-5）。现在，你成功了，问题解决了！最后的工作是把问题文档化，填写问题报告表，并返回给系统维护部门，他们会使它更加完整。记住，在你的工作日记里也要记录下问题解决过程以便将来参考。

例18-4 不成功的ping输出

```
C:/ping 110.0.1.1
Pinging 110.0.1.1 with 32 bytes of data:
Request timed out
Request timed out
Request timed out
Request timed out
Ping statistics for 110.0.1.1:
Packets: Sent = 4, Received = 0, Lost =  4 (100%loss)
```

例18-5 成功的ping输出

```
C:/ping 110.0.1.1
Pinging 110.0.1.1 with 32 bytes of data:
Reply from 110.0.1.1 bytes=32 time=1ms TTL=128
Reply from 110.0.1.1: bytes=32 time=1ms TTL=128
Reply from 110.0.1.1: bytes=32 time=1ms TTL=128
Reply from 110.0.1.1: bytes=32 time=1ms TTL=128
Ping statistics for 110.0.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

你可以看到，这个例子说明了一步一步排除网络问题可能性的过程。每一个可能出问题的地方都要考虑进来，然后分别加以排除。如果你马上进行多项改变，问题就很难分析清楚，解决方法也就很难精确实施。当一个解决方法实施后，发现问题仍然没有解决，那么就重新进行分析，提出新的解决方法。这个过程一直延续到问题被发现并得到解决，最后形成文档以便将来使用。不管在网络系统中遇到什么样的问题，解决它们的过程是一样的。

2 隔离技术

你将原本工作良好的两个网络连在一起（如图18-16），但当它们连接起来之后，整个网络却出问题了（如图18-17）。纠正这种问题的第一步是将这个网络再分成以前的两个，确认它们是否分别工作正常。如果是，则除掉一个连接路由器上的所有子网，再连接起来，看是否工作正常。

如果网络工作正常，那么就分别将这两个子网再加入到网络中去，直到问题出现（如图18-18所示）。除掉最后加入的那个子网，看整个网络是否恢复正常。

如果网络又正常运行了，那么把那个存在问题的网段中的所有主机都隔离开（如图18-19所示），然后每次连接回一台（如图18-20所示），直到网络出错。当你发现“捣蛋”的设备后，隔离它，确认网络是否又恢复正常了。

如果网络恢复正常了，那么你就找到出了出错的设备。你现在就可以对这台单独的设备进行故障排除，找出它造成整个网络失效的原因。如果通过分析，找不出任何问题，那么，这台设备有可能与另外那个网络上的某台设备一起造成网络失效。为了发现另外一端的问题，你不得不重复你刚

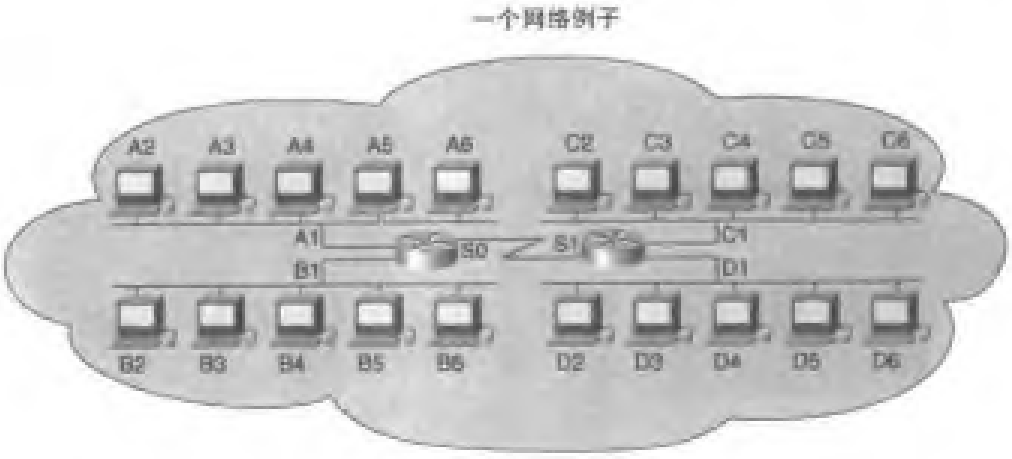


图18-16 一个网络例子

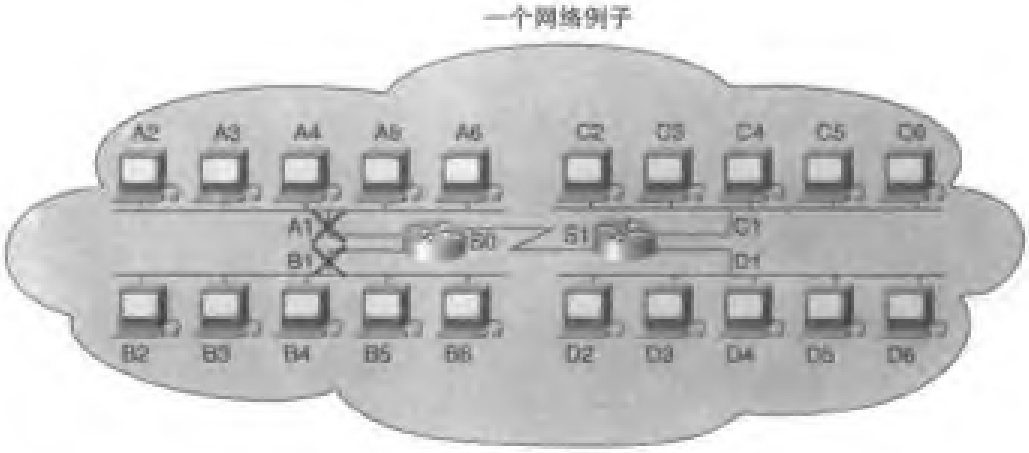


图18-17 去掉子网A和子网B的网络

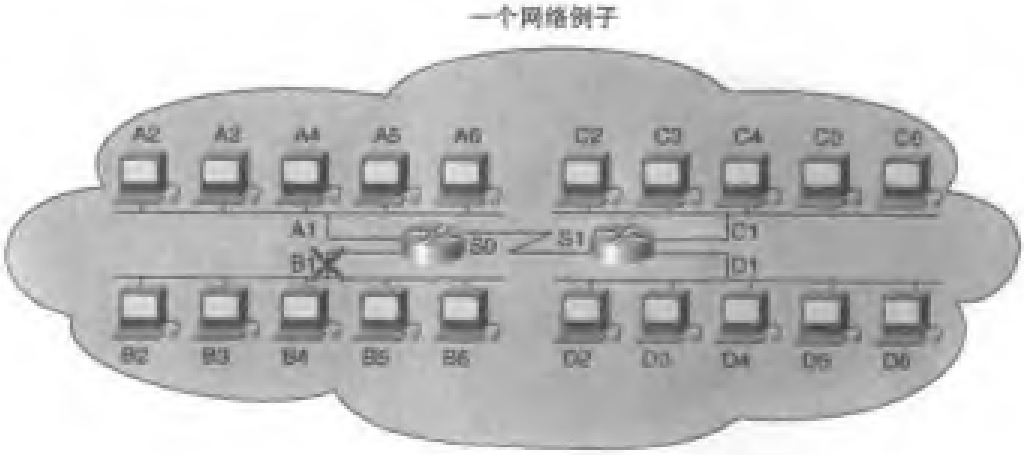


图18-18 去掉子网B的网络

才做的工作。首先，将那台找到问题的设备连到网络中去，然后将另外一端路由器上的所有子网隔离开（如图18-21所示），检查网络是否工作正常，如果是，则分别加入每个子网，直到问题出现。隔离最后加入的子网，检查网络是否恢复正常。

如果网络又正常运行了，那么把那个存在问题的网段中的所有主机都隔离开（如图18-22所示），

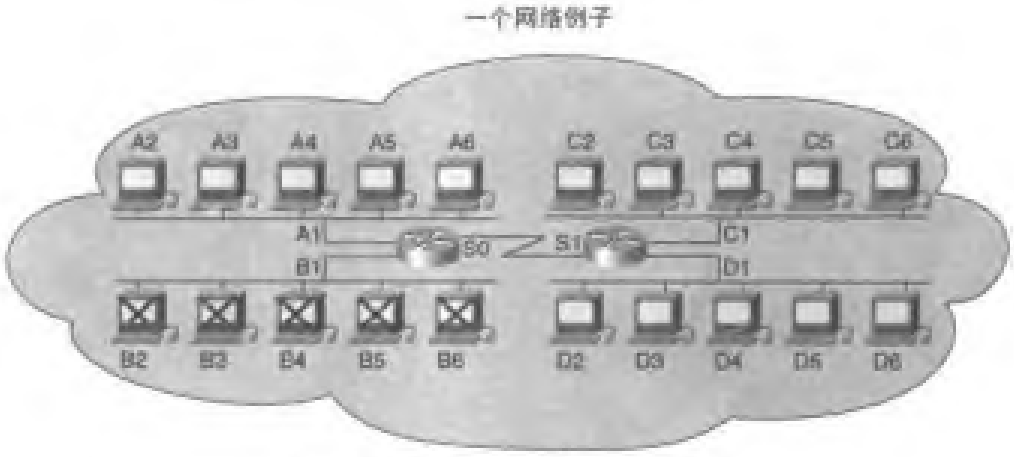


图18-19　去掉B上所有主机的网络

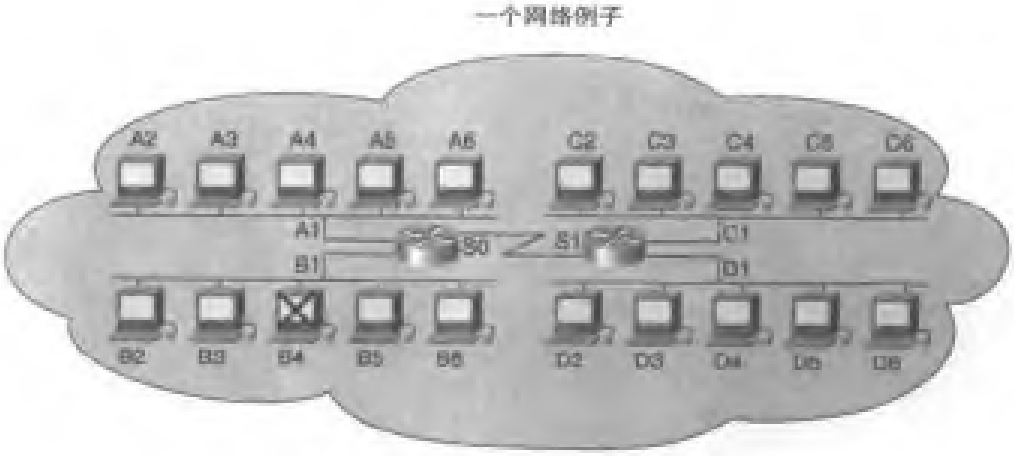


图18-20　去掉B上的一个主机的网络

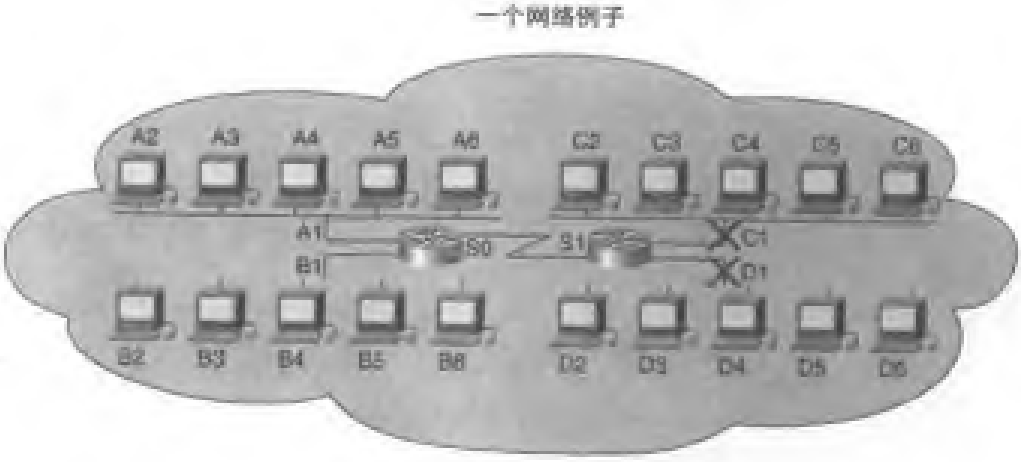


图18-21　去掉子网C和子网D的网络

然后每次连接回一台（如图18-23所示），直到网络出错。当你发现“捣蛋”的设备后，隔离它，确认网络是否又恢复正常了。

如果网络恢复正常了，那么你就找到出了出错的另外一台设备。你现在就可以对这台单独的设备进行故障排除，找出它造成整个网络失效的原因。如果通过分析，找不出任何问题，那么，就将

这两台出错的主机进行对比，找到它们冲突的原因。通过解决这种冲突，你能够将所有的设备连入网络，并且使整个网络工作正常（如图18-24所示）。

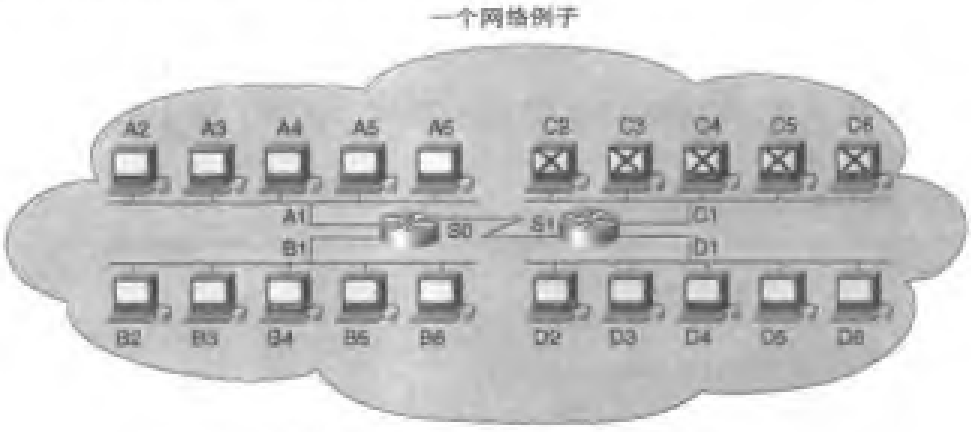


图18-22 去掉C上所有主机的网络

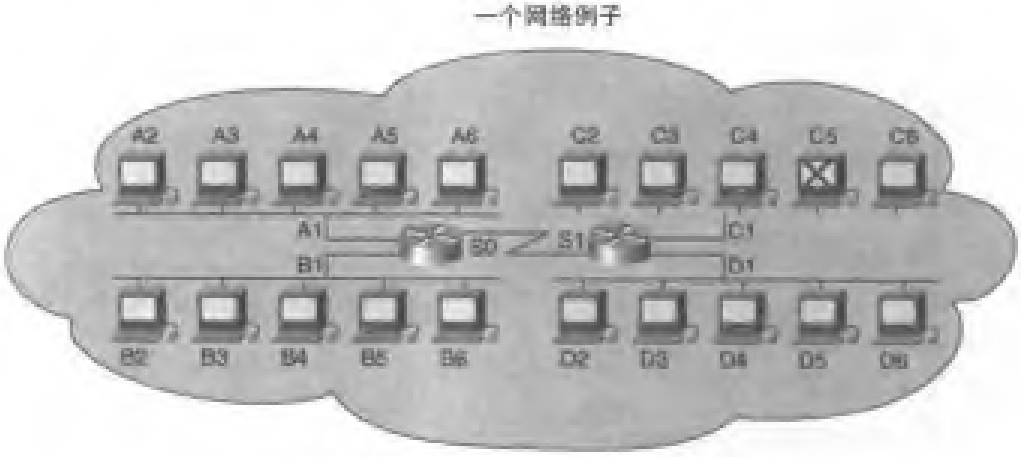


图18-23 去掉C上一个主机的网络

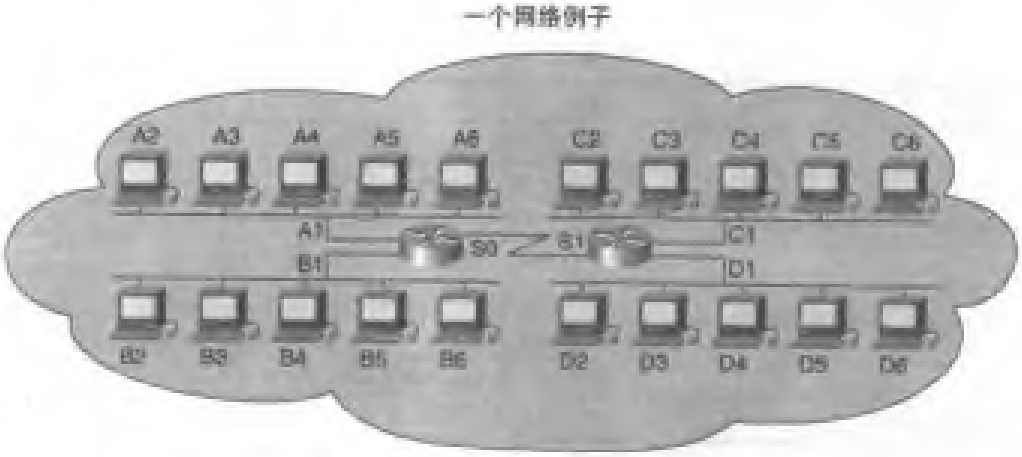


图18-24 完整的正常运行的网络

18.7.3 各种软件工具

如上面所描述的故障排除过程，软件工具对于网络管理员解决网络连通性问题来说是很有用的。

这些工具能帮助解决LAN中的问题，但在WAN故障排除中特别有用。有些命令在大多数客户端软件包中都可用，如ping、tracert（traceroute）、telnet、netstat、arp和Ipconfig（WinIPcfg）。

1　ping命令

Ping命令发送ICMP请求分组来确认远程主机的连接性。在例18-6中显示了ping是否成功。输出显示了回应分组的个数以及返回时间。

例18-6　对ping命令响应的分组个数

```
C:/ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Ping statistics for 110.0.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

C:/ping 110.0.1.1
Pinging 110.0.1.1 with 32 bytes of data:
Request timed out
Reply from 140.189.8.65: Destination Unreachable
Request timed out
Request timed out
Ping statistics for 110.0.1.1:
Packets: Sent = 4, Received = 1, Lost = 3 (75% loss)
```

Ping命令的句法如下，在表18-1中进行了解释：

```
Ping[-t][-a][-n count][-l length][-f][-i ttl] [-r count] destination
```

表18-1　ping命令选项

语法	描述
-t	Ping直到中断
-a	解析主机名并ping这个地址
-n	解析主机名并ping这个地址
-l	指定长度，发送指定大小的请求回应分组
-f	向网关提交“DO NOT FRAGMENT”命令
-i	设置TTL域值
-r	这里的count是记录发送和返回的分组所经过的路径
destination	指定要ping的远程主机，通过域名和IP地址给出

2　tracert（Traceroute）命令

tracert（Traceroute）命令显示了分组到达它的目的地所经过的路径。例18-7显示了tracert的输出。

例18-7 tracert命令输出

```
C:/tracert cisco.com

Tracing route to Cisco.com [192.31.7.130]
over a maximum of 30 hops:
1 1 ms <10ms <10ms 198.150.221.254
2 2ms 1ms 2ms 198.150.15.252
3 4ms 2ms 2ms 198.150.12.1
4 23ms 4ms 4ms ArizonaStateUniversity -s1 -0 -1.core.azst.net
[140.189.64.9]
5 4ms 5ms 5ms ArizonaStateUniversityISP -atm1 -0 -3.core.azst.net
[140.189.8.65]
6 8ms 14ms 8ms APhoenix1.core0.nap.net [207.227.0.201]
7 9ms 10ms 10ms 4.0.5.233
8 64ms 64ms 67ms p2-1.paloalto-nbr2.bbnplanet.net [4.24.7.18]
9 67ms 65ms 69ms p0-0-0.paloalto.cr18.bbnplanet.net [4.0.3.86]
10 66ms 75ms 75ms h1-0. cisco bbnplanet.net [4.1.142.238]
11 66ms 68ms 70ms Sty.cisco.com [192.31.7.39]
12 67ms 77ms 76ms CISCO.COM [192.31.7.130]
```

它的句法如下，表18-2做了解释：

tracert[**-d**][**-h** *maximum-hops*][**-j** *host-list*][**-w** *timeout*]*target_name*

表18-2 tracert命令选项

句法	描述
-d	IP地址不需要解析为主机名
-h	*maximum_hops*给出了最大跳搜索数
-j	*host_list*指定了宽松源路由
-w	指定对每个回答所等待的最长时间（毫秒）
targe_name	进行trace的远端主机，由域名或IP地址给出

3 telnet

这是一个终端仿真程序，使你可以和远程登录服务器之间进行交互命令。除非连接可以建立，否则没有数据能够通过；如果连接断开，telnet也能够通知你。这对测试远程主机的登录配置参数是一个很好的工具。

4 netstat

netstat命令显示了协议统计数据和当前的TCP/IP网络连接（如例18-8）。

例18-8 netstat 命令输出

```
C:\netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    matc-tag-phx:epmap     matc-tag-phx:0         LISTENING
  TCP    matc-tag-phx:microsoft-ds  matc-tag-phx:0     LISTENING
  TCP    matc-tag-phx:1028      matc-tag-phx:0         LISTENING
  TCP    matc-tag-phx:1041      matc-tag-phx:0         LISTENING
  TCP    matc-tag-phx:1073      matc-tag-phx:0         LISTENING
  TCP    matc-tag-phx:1074      matc-tag-phx:0         LISTENING
  TCP    matc-tag-phx:netbios-ssn   matc-tag-phx:0     LISTENING
  TCP    matc-tag-phx:1036      matc-tag-phx:0         LISTENING
  TCP    matc-tag-phx:1073      64.12.28.63:5190       ESTABLISHED
  TCP    matc-tag-phx:1074      64.12.27.164:5190      ESTABLISHED
  TCP    matc-tag-phx:1121      baym-cs39.msgr.hotmail.com:1863  ESTABLISHED
  TCP    matc-tag-phx:2025      currdev1.cisco.com:netbios-ssn   ESTABLISHED
  UDP    matc-tag-phx:epmap     *:*
  UDP    matc-tag-phx:microsoft-ds  *:*
  UDP    matc-tag-phx:isakmp    *:*
  UDP    matc-tag-phx:1030      *:*
  UDP    matc-tag-phx:1034      *:*
  UDP    matc-tag-phx:1046      *:*
  UDP    matc-tag-phx:1900      *:*
```

这个命令的句法如下，在表18-3中进行了解释：

netstat[**-a**][**-e**][**-n**][**-s**][**-p** *proto*][**-r**][*interval*]

表18-3 netstat命令选项

语法	描述
-a	显示所有的连接和监听的端口（服务器端的连接一般不显示）
-e	显示以太网统计数据，这个选项可以和-s选项一起使用
-n	以数字形式来显示地址和端口数
-p	Proto显示指定协议的连接数；proto能够是tcp或者udp,如果和-s选项结合使用以显示不同协议的统计数据，proto能够是tcp、udp或ip
-r	显示路由选择表的内容
-s	显示不同协议的统计数据。缺省的，显示TCP、UDP和IP的统计数据；-p选项能用来指定一个特定的协议子集
Interval	重复显示选择的统计数据，每两次显示间隔为interval秒。按Ctrl+l停止重复显示统计数据如果这个参数被省略，则netstat显示一次当前的配置信息

5 arp

ARP收集本地主机的硬件地址和缺省网关。你能通过查看ARP缓冲区来检测非法的或重复的条目（如例18-9）。

例18-9 arp命令输出

```
C:arp -a
Interface: 192.168.1.101 --- 0x2
Internet Address Physical Address Type
192.168.1.1 00-04-5a-2f-28-29 dynamic
C:\
```

arp命令的语法如下，并在表18-4中进行了解释：

```
arp -a [inet_addr][-N[if_addr]]
arp -d inet_addr [if-addr]
arp -s inet_addr ether_addr[if_addr]
```

表18-4 arp命令选项

语法	描述
-a或-g	显示当前ARP缓冲区的内容
-d	删除由*inet_addr*指定的条目
-s	在缓冲区中加入一个静态条目
-N	显示指定硬件地址的ARP条目
inet_addr	给出IP地址，用点分隔的10进制格式
if_addr	给出需要进行缓冲区修改的IP地址
eth_addr	以连字符分隔的16进制格式显示MAC地址

6 ipconfig (Windows NT) /WinIPcfg (Windows 95/98)

这些Windows实用程序用来显示本地网络适配器或指定网络接口卡的IP地址信息。

命令的句法如下所示，在表18-5中进行了解释：

```
ipconfig[/all | /renew[adapter] | /release[adapter]]
```

表18-5 ipconfig 命令选项

语法	描述
/all	显示适配器的所有信息
/renew	如果没有指定适配器，则更新所有本地适配器的DHCP租用信息
/release	释放这个适配器上的DHCP租用信息，使TCP/IP协议失效

以上这些是网络管理员能够用来对网络进行远程监视和控制的工具。还要注意一点，在使用SNMP和RMON的时候，一定要实现正确的安全管理，以防网络被非法入侵。

18.8 总结

学习完本章后，你应该对下面的内容有了很好的理解：

- 网络管理的可管理性。
- 建立网络管理的管理界限。
- 网络的成本。
- 错误报告文档。
- 监控网络。
- 监控连接性。

- 监控数据流量。
- SNMP。
- RMON。
- 故障排除方法。
- 故障排除的软件工具。

18.9 关键术语

归档位（*archive bit*） 和文件一起存储，记录从上次备份以来，文件是否被修改的信息。当文件创建或修改时，标志就被置为“开”，这个标志告诉备份进程是否要对这个文件进行备份。

基准性能（*baseline*） 基准性能是网络安装好并且配置正确的时候测量的一个性能指标。基准性能可以用来与将来的网络性能做对比。

备份域控制器（*backup domain controllers, BDC*） 平衡PDC的工作负载并且给用户和资源对象管理提供冗余的辅助服务器。

装订所（*bindery NetWare*） 3.12版本用来管理多用户和资源的对象。它的缺点在于它虽然建立了一个服务器中心网络，但它把每台作为控制点的服务器单独看待。

数据备份（*data backup*） 是指把储存数据复制到磁带或另外的存储介质上的过程，这些存储介质有可移动硬盘、CD-ROM或DVD-ROM等。

强制用户文件（*mandatory*） 对每一个用户提供相同的用户界面，不允许用户做出改变，主要用于许多用户都要使用同一台物理计算机的场合。

多域模型（*multidomain model*） 几个由信任/被信任关系连接起来不同的域，使用户能够跨域使用资源的模型。

Novell目录服务（*Novell Directory Services, NDS*） Novell Netware服务器使用这种目录服务来管理用户和资源。它比起3.12版本的优势在于NDS建立了一个以网络为中心的网络，将整个网络当作为控制点。

配置文件（*profile*） 允许用户自定义他的计算机使用界面，使用户不管从哪台计算机连入网络都有着一样的用户界面。

远程监控（*Remote Monitoring, RMON*） SNMP协议的扩展，支持将网络看成一个整体而不是一系列单独的设备。

简单网络管理协议（*Simple Network Management Protol, SNMP*） SNMP是允许被管理设备通过网络将统计数据传输到中心管理控制台的协议。

独立服务器（*standalone server*） 一种主要为了支持某种特定的应用，并将它的资源专门提供给那个应用而建立的服务器。

流量监控（*traffic monitor*） 流量监控是一种复杂的网络监控。它检查网络上的实际分组流量并基于这些网络流量来给出报告。

特洛伊木马（*Trojan horse*） 伪装成游戏或者应用软件的破坏性程序。当它运行时，特洛伊木马偷偷的对计算机做一些破坏操作，然而看上去好像是对计算机做一些有用的工作。

用户策略（*user policies*） 记录用户怎样和网络进行交互的信息。这些策略包含了网络上什么是允许的，什么是不允许的。

病毒（*virus*） 是能将自己复制进其他文件从而“感染”计算机文件的程序（通常是一些可执行程序）。通常是用如下的方法来完成的：当一个被感染的文件被调入内存时，它其中的病毒代码就被执行，它就能够去感染其他的文件，并且接着继续下去。

卷（*volume*） 存储器的物理单元。

蠕虫（*worm*） 是通过计算机来传播它自己的程序，通常是在每台计算机的内存里复制它自己。蠕虫可以非常快的速度来复制自己从而导致计算机崩溃。



第19章 Network+认证考试复习

本章内容见随书附盘。



第20章 CCNA认证考试复习

目标

学习完本章之后，你将能够：
- 理解CCNA考试所包含的主题。
- 了解为了通过CCNA考试需要学习和特别注意的主题。

本章作为你准备CCNA认证考试的复习。准备该考试的第一步就是复习考试大纲和课程的主题。本章对CCNA认证考试所包含的主题提供了一个复习，这将帮助你准备该考试。

20.1 OSI模型

通信协议的总体目标是在不考虑两台计算机上的操作系统和硬件平台的情况下，允许一台计算机上的应用程序和另外一台计算机上的应用程序相互通信。CCNA考试涉及了OSI模型的全部7层，因此你需要了解它们。

20.1.1 应用层

应用层负责确定通信伙伴，并为特定的应用程序服务提供功能，比如文件传输和虚拟终端。
典型的TCP/IP应用包括：
- Telnet。
- 文件传输协议（*FTP*）。
- 简易文件传输协议（*TFTP*）。
- 简单邮件传输协议（*SMTP*）。
- 简单网络管理协议（*SNMP*）。
- 超文本传输协议（*HTTP*）。
- 自举协议（*BOOTP*）。
- 动态主机配置协议（*DHCP*）。

20.1.2 表示层

表示层通过透明地完成各种不同的数据、视频、声音和图像格式与适当传输格式之间的相互转换来提供通信服务。该层还负责数据的压缩、解压缩、加密和解密。

尽管这些功能都可以由专门的协议完成，但通常都将其嵌入到现有的应用层协议中。

下面所列举的都是一些表示层的标准：

- **文本**——ASCⅡ和EBCDIC。
- **图像**——TIFF、JPEG、GIF和PICT。
- **声音**——MIDI、MPEG和QuickTime。

20.1.3 会话层

会话层负责控制设备或主机之间的会话。它负责在应用程序之间建立、管理和终止会话。

下面是一些会话层协议的例子：

- **网络文件系统**（*NFS*）。
- **结构化查询语言**（*SQL*）。
- **远程过程调用**（*RPC*）。
- X Window系统。
- AppTalk会话协议（*ASP*）。
- DNA会话控制协议（*SCP*）。

20.1.4 传输层

传输层负责端到端的信息传递，包括错误恢复和流量控制。

传输层协议可以是可靠的，也可以是不可靠的。不可靠的协议在建立连接、确认、排序和流量控制方面有较少的责任或没有责任。不可靠的传输层协议会把这些责任留给其他层的协议。可靠的传输层协议可以具有以下的责任：

- 建立连接和关闭连接，比如三次握手。
- 传输数据。
- 确认所接收的数据或未接收的数据。
- 确保对到达顺序不正确的分组能够按照正确的顺序排序。
- 进行流量控制，比如调整窗口的大小。

TCP/IP中可靠的传输层协议是传输控制协议（TCP）。使用TCP的协议包括FTP、Telnet和HTTP。

TCP/IP中不可靠的传输层协议是用户数据报协议（UDP）。使用UDP的协议包括TFTP、SNMP、NFS、域名系统（DNS）和路由选择协议RIP。

下列是传输层协议的例子：

- TCP/IP——TCP和UDP。
- Novell——顺序分组交换（SPX）。

20.1.5 网络层

网络层负责在两个端系统（最初源系统和最终目的系统）之间提供连通性和路径选择，这两个端系统可能处于不同的网络上。网络层寻址为最初源系统和最终目的系统提供地址——在TCP/IP中是IP地址。这些地址不会随路径的变化而改变。

下列是网络层协议的一些例子：

- Internet协议（*IP*）。
- Novell的互联网分组交换（*IPX*）。
- 地址解析协议（*ARP*）。
- 反向地址解析协议（*RARP*）。
- Internet控制消息协议（*ICMP*）。

20.1.6 数据链路层

数据链路层在物理链路上提供可靠的数据传输。在这个过程中，数据链路层主要关心以下一些问题：物理（相对于网络或逻辑）寻址、网络拓扑结构、线路规范（终端系统如何使用网络链路）、错误通知、有序帧传输和流量控制。

数据链路层将帧从一个节点传送到另一个节点，比如从主机到主机、主机到路由器、路由器到路由器或路由器到主机。数据链路层地址通常是会改变的，它们代表当前的数据链路地址和下一跳的数据链路地址。在以太网术语中，这将会是源MAC地址和目的MAC地址。

数据链路层协议包括以下这些：

- 以太网。
- IEEE 802.3。
- 令牌环。
- IEEE 802.5。
- 高级数据链路控制（HDLC）。
- 点对点协议（PPP）。

20.1.7 物理层

为了在终端系统之间激活、保持和释放物理链路，物理层定义了电气、机械、程序和功能规范。物理层规范定义的特性包括电平、电压变化时限、物理数据速率、最大传输距离和物理连接以及其他类似的属性。

物理层标准包括：

- 10BaseT。
- 10BaseTX。
- V.35。
- RS-232。

20.2 桥接/交换

本节复习局域网交换，将帮助你回忆减少网络拥塞的一个方法就是尽可能地用交换机替代集线器。此外，为了提高交换机的工作效率，你可能需要利用下列交换特性的部分或全部：

- 快速以太网（100Mbit/s）交换机端口和主机网络接口卡。
- 全双工通信。
- 贯穿式交换。

20.2.1 全双工和半双工以太网的运行方式

存在两种类型的以太网通信方式：

- 半双工。
- 全双工。

半双工通信方式允许两台或更多的设备彼此之间进行通信，但一次只与一台设备进行通信（参见图20-1）。如果多台设备试图同时进行通信，就会产生冲突。这些设备将会退避，然后，每块网络接口卡中的随机算法会决定哪台设备首先发送。

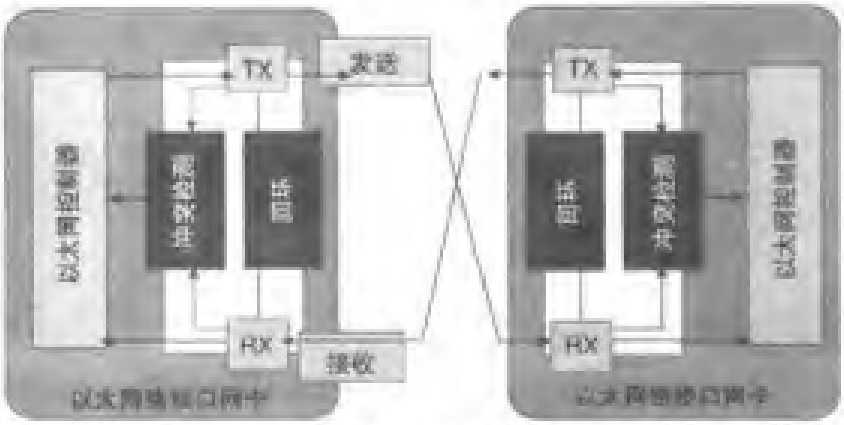


图20-1　半双工以太网设计（标准以太网）

连接到集线器的主机必须工作在半双工模式，因为它们必须能够检测何时发生了冲突（以停止传输）。

全双工通信使两台设备相互之间能同时进行通信（见图20-2）。全双工以太网有一个局限性，即只能有一台设备连接到交换机的端口上，这台设备可以是一台计算机、打印机、路由器或者另外一台交换机。如果所有连接到交换机端口的都是单台设备（不使用集线器），则让它们工作在全双工模式下是一个好主意。

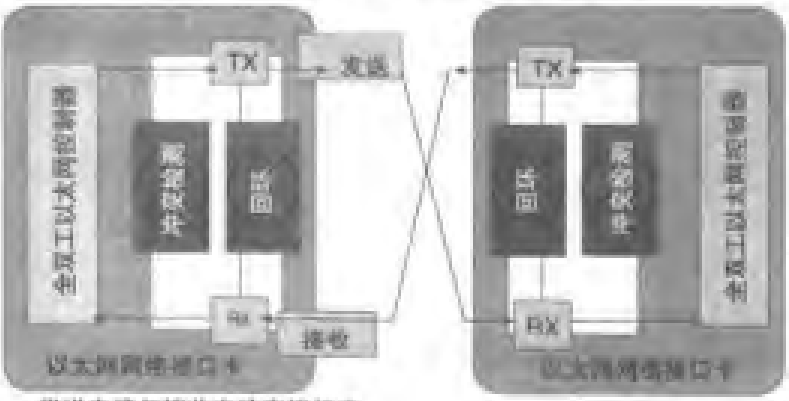


图20-2　全双工以太网设计

全双工方式能够将链路的吞吐量增加一倍。例如，在一条标准的10Mbit/s以太网链路上，吞吐量会是20Mbit/s——10Mbit/s的发送速率加上10 Mbit/s的接收速率。实际上，在一条全双工连接上不会发生冲突，因为冲突域内只有两台设备。

20.2.2　贯穿式交换和存储转发交换的区别

贯穿式交换和存储转发交换是两种主要的交换方式。在某些交换机中，这是在每个端口上都可以配置的参数。

1　存储转发交换（Store-and-forward switching）

存储转发交换通常是绝大多数交换机所采用的缺省方式。在交换机将一个以太网帧从另外一个接口转发出去之前（通过在交换机的源地址表中查找目的MAC地址），它首先把整个帧复制到自己的缓冲区中，并把帧校验序列（FCS）与自己的计算结果进行核对。如果FCS与它自己的计算结果相匹配，则该帧将从适当的端口转发出去。如果FCS和它自己的计算结果不匹配，该帧将被丢弃。检验FCS需要时间——也就是说会引起交换机的额外延迟——但是对所有的错误进行了过滤。

2　贯穿式交换（Cut-Through Switching）

大多数的Cisco交换机都提供两种类型的贯穿式交换：

- **快速转发方式**（*Fast-forward*）。

- 无碎片方式（*Fragment-free*）

在快速转发方式下，交换机读取第2层的目的地址并在源地址表中找到该地址后，立即把帧通过适当的端口转发出去。在帧的剩余部分还没进入交换机之前，帧已经开始被转发到这个接口上。快速转发方式不检查FCS，因此不进行错误检测。

无碎片交换方式与快速转发交换方式类似，但是它要等到帧的前64Bytes被接收到以后，才开始把帧向交换机的出站端口转发出去。根据以太网和802.3规范，冲突应该在帧的前64Bytes内检测到。与快速转发交换方式一样，无碎片交换方式也不检查FCS，因而不进行错误检测。无碎片交换方式比存储转发交换方式快（延迟更小），但比快速转发交换方式慢（延迟更大）。

20.2.3 虚拟局域网（VLAN）的运行方式和好处

使用虚拟局域网（VLAN）的原因很多，包括在一个交换型网络中创建多个分离的广播域。在不同的VLAN之间传送信息必须使用路由器。

可以将VLAN视为一个子网。有几种实现VLAN的方式，但是最常见的一种方式是把多个子网划分为多个分离的VLAN。

如果没有VLAN，2层广播，比如ARP请求，会被交换型网络中所有的主机接收到。在一个大型的交换型网络中，这些ARP请求将消耗不必要的网络带宽和主机处理周期。通常，只有路由器才会阻止2层广播的传送，比如这些ARP请求。

注意，在图20-3中，尽管主机位于不同的子网中，但是ARP请求仍然能够被所有的计算机接收到。这可能是个问题，尤其是当网络中的计算机使用Windows时。使用Windows的计算机只将ARP表的条目保持120秒。因此，如果计算机在120秒内没有与一台设备进行通信，有关该设备的IP地址-MAC地址映射就会从ARP表中删除。在主机下次需要与同一台设备进行通信时，它必须发出另一个ARP请求。另一方面，使用UNIX的计算机通常都将ARP表中的条目保留大约20分钟。



图20-3 全交换网络—两个网络

注意：在一个交换型网络中，要形成多个分离的子网，VLAN不是必需的。然而，你会看到，对于降低强制路由层（2层）的广播，VLAN具有更多的优势。

20.3 被路由协议

对被路由协议的复习包含以下主题，它们都可能在CCNA考试中出现：

- IP地址的不同类别，包括子网划分和私有地址。
- 配置IP地址。
- 对IP地址方案进行故障排除。
- 开发符合需求的IP寻址方案。
- 确定各种TCP/IP应用层协议的基本用途。
- 十进制、十六进制和二进制间的转换。
- 定义流量控制并描述网络中使用的3种基本流量控制方法。
- 解释TCP/IP网络的功能和传输层协议。

20.3.1 IP地址的不同类型，包括子网划分和私有地址

用户如何确定地址中的哪部分标识网络，哪部分标识主机？答案来自因特网的设计者，他们认为，根据网络所包含计算机（主机）数量的不同，网络的大小也是不同的，如表20-1所示。

表20-1 IP地址分类

地址分类	网络数量	每个网络的主机数量
A	126	16,777,216
B	16,384	65,535
C	2,097,152	254
D（多播）	–	–

这里的假设是存在相对较少的大型网络，其中可能有数百万台计算机。设计者们预想到有大量中型的网络，每个网络中可能有数千台计算机。最后，他们看到有大量只包含数百台或更少量计算机的网络。因此，设计者们决定将可用的IP地址划分为多个类别，以定义大型网络（A类）、中型网络（B类）和小型网络（C类），如表20-2所示。了解一个IP地址所属的类别，是确定地址的哪部分标识网络，哪部分标识主机的第一步。

表20-2 识别地址类别

地址分类	高次比特	首个8位位组的地址范围	网络地址所包含的比特数量
A	0	0-127*	
B	10	128-191	
C	110	192-223	
D（多播）	1110	224-239	

*A类所包含的网络地址书写成二进制时，最左边的比特为0。尽管网络127的开始比特为0，但它已经被预留作特殊用途。因此，A类只包含126个可用的网络，不是127个。

IP的任务之一是将分组从其产生的网络转发到目的网络。因此，这种寻址方案必须包含源和目的网络的标识。通过使用目的网络标识，IP可以将一个分组传递到目的网络。当分组到达连接目的网络的路由器时，IP必须接着确定连接在该网络中的特定计算机。这与美国邮政系统的工作方式非常类似。当邮件被路由时，它首先必须通过邮政编码传送到目的地的邮局，然后，邮局必须通过街道地址确定邮件在该城市中的最终目的地。这是一个两步的过程。

相应地，每个IP地址都包含两部分。一部分标识系统所连接的网络，另一部分标识网络中的特定系统。这种类型的地址被称为分层地址，因为它包含多个层次。一个IP地址将这两个标识符结合成了一个数字。这个数字必须是惟一的，因为不允许有重复的地址。第一部分标识系统的网络地址。第二部分，称为主机部分，标识网络中的特定主机。

因特网最初的两层分层假设每个地点都只有一个单独的网络。因此，每个地点都只需要一条到因特网的连接。最初，这些假设是可靠的。然而，随着时间的推移，网络计算不断成熟和扩展。到1985

年，假设一个组织只有一个单独的网络已经不再可靠，组织也不再满足于一条单独的因特网连接。

随着很多地方开始发展多个网络，很明显，IETF需要制定某种机制来区分以因特网第2层子网方式出现的多个逻辑网络。否则，在有多个网络的地方，就没有高效的办法将数据路由到指定的终端系统中。

20.3.2 子网划分

为了创建子网结构，必须通过划分主机字节，将主机比特重新分配为网络比特。这个过程通常被称为“借入比特（borrowing bits）”，但更准确的术语是“借出比特（lending bits）”。这一过程的开始点总是根据IP地址类型确定的最靠左的主机比特。

除了局域网管理功能，子网络划分还使得网络管理员能实现“防广播泄漏（broadcast containment）”和局域网的低层安全性。通过在局域网中划分子网能实现安全性，是由于对其他子网的访问是通过路由器的服务提供的。网络管理员可以配置访问控制列表，根据各种标准来允许或者拒绝对某个子网的访问，从而提供了安全性。某些A类和B类网络的所有者也发现子网划分为该组织创造了一个利润源，这便是出租或者销售以前未使用的IP地址。

在这样的多网络环境中，各个子网络到因特网的连接都通过一个共同点——路由器，如图20-4所示。内部网络环境的实际细节对因特网并不重要。内部网络构成一个私有网络，该网络能够（或者应该能够）传送自己的数据报。因此，因特网只需要关心如何到达网络连接因特网的网关路由器。在私有网络内，可以对IP地址的主机部分进行子划分，以创建子网络。

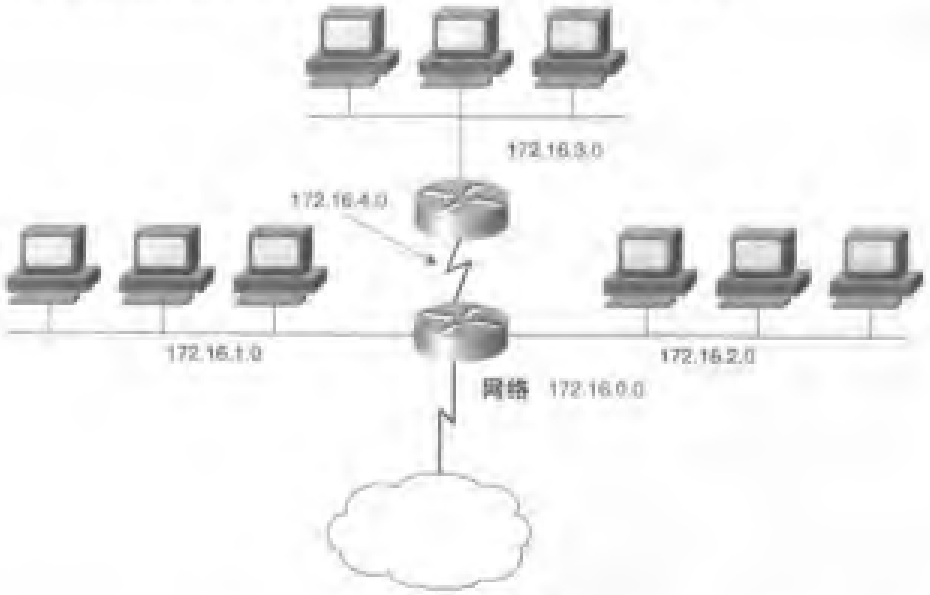


图20-4 子网络

由于子网地址是从A类、B类和C类地址的主机编号部分取得的，因此通常由网络管理员在本地进行分配。与IP地址的其他部分一样，在其所属的网络范围内，每个子网地址也必须惟一，如图20-5所示。

与无类域间路由选择（CIDR）、IPv6和私有地址一样，子网划分提供了另一种节约IP地址的方法。这种方法将完整的网络地址类划分为多个小块，以防止IP地址全部耗尽。图20-6显示了将一个B类网络（131.108.0.0）划分为了3个子网。讲到TCP/IP时，不可能不谈子网划分。作为系统管理员，理解子网划分是一种分割和标识局域网中不同网络的方法是很重要的。对一个小网络而言，进行子网划分不一定必要的；然而对于大型或超大型网络，子网划分是必需的。简而言之，对网络进行子网划分意味着使用子网掩码对网络进行分割，将一个大型网络分解为更小、更高效、更易管理的网

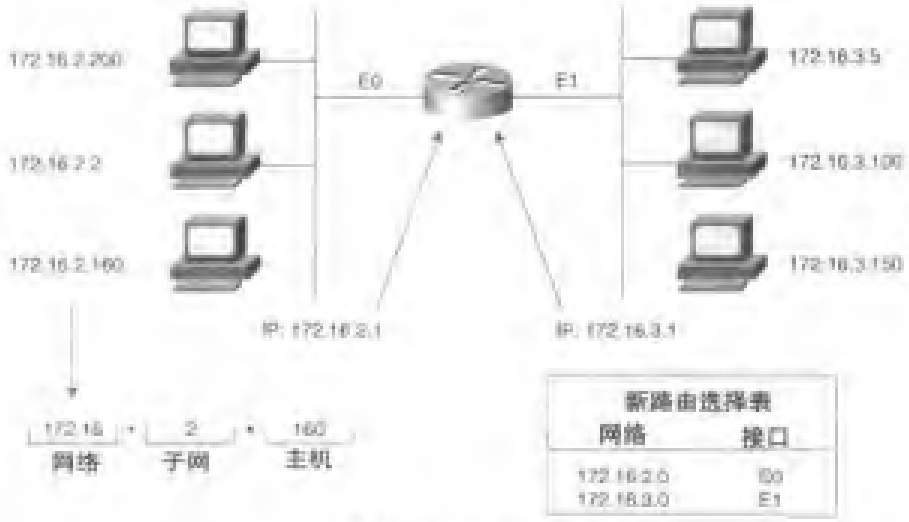


图20-5 子网地址

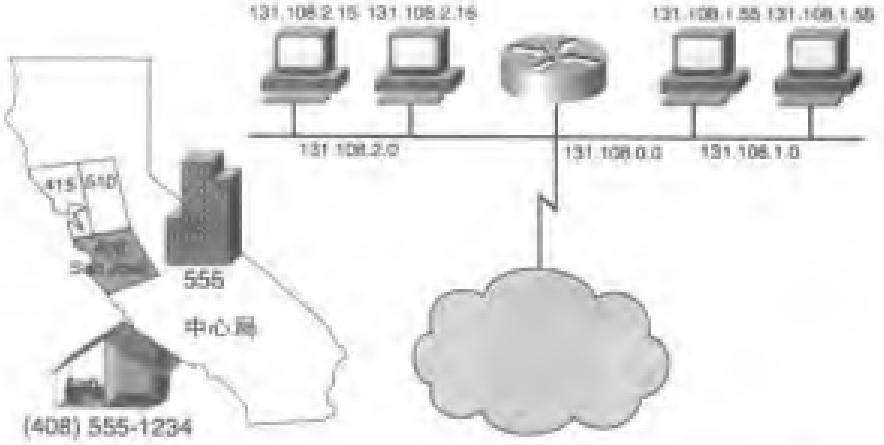


图20-6 子网的寻址

段或子网，如图20-7所示。这与美国的电话系统类似，首先将整个系统分解为地区号码，然后是交换区号码，最后是本地号码。电话系统中的这些元素可以和IP互连网络中的网络编号、子网地址和单个主机地址相类比。

系统管理员必须在增加和扩展网络时解决这些问题。重要的是知道需要多少个子网/网络，每个网络上允许有多少台主机。通过子网划分，网络就不是局限于标准的A、B或C类网络掩码，管理员在网络设计中有了更大的灵活性。

子网地址包含A类、B类或C类的网络部分，增加了一个子网字段和一个主机字段。子网字段和主机字段是为整个网络从原来的主机部分创建得来的。网络管理员在编址上的灵活性在于可以决定如何将原来的主机部分划分为新的子网字段和主机字段。

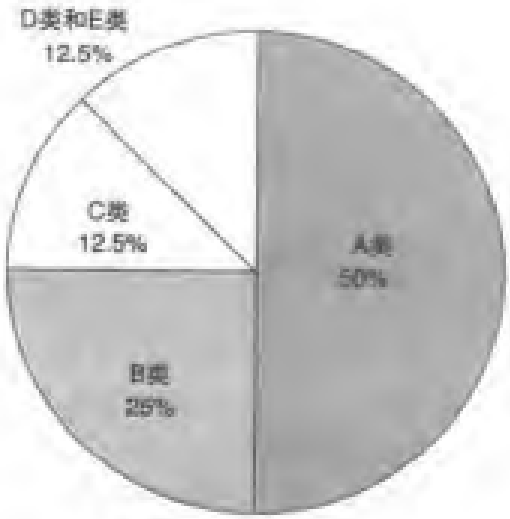


图20-7 子网地址

要创建一个子网地址，网络管理员需要从主机字段借位，然后将其指定为子网字段，如表20-3所示。最少借2位。如果只借1位来创建子网，你只能得到一个网络号——0网络和广播号——.255网络。所能借的最大位数是至少留下2位作为主机编号。在这个C类IP地址的例子中，从主机字段中借

了不同的位数来用于子网字段。

表20-3 子网地址

首字节的十进制表示	子网数	每个子网内A类地址主机数	每个子网内B类地址主机数	每个子网内C类地址主机数
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

20.3.3 十进制、十六进制和二进制之间的转换

解决某个数学问题的方法通常不止一种，十进制到二进制转换也不例外。本节介绍一种方法，但如果别的方法更简单也可以随意使用。

将一个十进制数转换位二进制，首先需要找到适合该十进制数的2的最大幂，如表20-4所示。如果你用计算机完成这个过程，最合乎逻辑的开始点是1个或2个字节所能表示的最大值。

表20-4 2字节/16比特数

2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
32678	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

如前所述，最常见的比特分组是8，构成1字节。然而，某些时候，一个字节所能容纳的最大值（255）不够用。在这种情况下，你必须结合多个字节，因此你可用一个16bits数，而不是两个8bits数；或者一个24bits数而不是3个8bits数。同样的规则也可用于8bits数：将前一个位置的值乘2，得到当前列的值。表20-5记录了这些值（从一个2Bytes/16bits数开始，它对于学习子网划分机制是非常重要的）。

由于经常与计算机打交道的人熟悉字节，因此最容易的方法是从字节的边界开始，并从那里开始计算，如表20-5所示。现在计算一些例子，第一个是6,783。由于这个数比单字节的最大值255大，我们使用2字节,从2^{15}开始计算。因此，6,783 = 00011010 01111111$_2$。

表20-5 2Bytes/16比特数

位的幂	十进制值	位的值	二进制数	余数
2^{15}	6783	32,678	0	6783
2^{14}	6783	16,384	0	6783
2^{13}	6783	8,192	0	6783
2^{12}	6783	4,096	1	2687
2^{11}	2687	2,048	1	639
2^{10}	639	1,024	0	639
2^{9}	639	512	1	127
2^{8}	127	256	0	127
2^{7}	127	128	0	127
2^{6}	127	64	1	63
2^{5}	63	32	1	31
2^{4}	31	16	1	15
2^{3}	15	8	1	7
2^{2}	7	4	1	3
2^{1}	3	2	1	1
2^{0}	1	1	1	0

第二个例子是104。由于这个数比255小，可以用一个字节表示，如表20-6所示。

表20-6 1Bytes/8bits数

位的幂	十进制值	位的值	二进制数	余数
2^7	104	128	0	104
2^6	104	64	1	40
2^5	40	32	1	8
2^4	8	16	0	8
2^3	8	8	1	0
2^2	0	4	0	0
2^1	0	2	0	0
2^0	0	1	0	0

因此，$104=01101000_2$。

该方法对任何的十进制数都有效。考虑十进制数1百万。因为1百万比2Bytes所能标识的最大值65,535大，所以你至少需要3Bytes。一直乘2，直到24比特（3字节）为止，所得值是8,388,608,这表明24bits所能表示的最大值为16,777,215。因此，从第24比特开始，按照前面所讲的过程，直到得到0。使用前面描述的过程，确定十进制数1百万等于二进制数。

$00001111\ 01000010\ 01000000_2$。

二进制到十进制转换正好相反。只要将二进制数放在表中，如果某个位置的值为1，将该位对应的十进制值加入总数。表20-7演示了一个例子，将00000100 00011101转换为十进制，得到1,053。

表20-7 2Bytes/16bits数

位的幂	十进制值	位的值	二进制数	余数
2^{15}	0	32678	0	0
2^{14}	0	16384	0	0
2^{13}	0	8192	0	0
2^{12}	0	4096	0	0
2^{11}	0	2048	0	0
2^{10}	0	1024	1	1024
2^9	1024	512	0	1024
2^8	1024	256	0	1024
2^7	1024	128	0	1024
2^6	1024	64	0	1024
2^5	1024	32	0	1024
2^4	1024	16	1	1040
2^3	1040	8	1	1048
2^2	1048	4	1	1052
2^1	1052	2	0	1052
2^0	1052	1	1	1053

本章的内容，甚至本书的内容，都集中在CCNA考试的根本性主题上。因此，请记住本节的内容与通过该考试所要求掌握的主要目标明确相关，并准备好证明对该内容的完全掌握。

20.4 路由选择协议

协议就是基于多个标准的一组规则，它确定计算机如何穿越网络进行通信。协议也作为不同应用程序、主机或系统通信所使用的共同特征或介质。当计算机之间相互通信时，他们交换数据消息。要接受并对这些消息进行处理，计算机必须在消息的定义和含义上达成一致。示例的消息类型包括与一台远程的机器建立一条连接，发送或接收电子邮件，并传送文件和数据。

协议描述了下列内容：

- 消息必须使用的格式。
- 在某个特定的活动中，计算机交换消息所必须使用的方式，比如穿越网络发送消息。

由于名称上的相似性，被路由协议和路由选择协议常常引起混淆。下面进行了一些澄清：

- **被路由协议**（*Routed protocol*）——任何在网络层地址中提供足够信息，使分组能根据寻址方案，从一台主机转发到另一台主机的网络协议。被路由协议定义了分组中字段的格式。分组通常由一个端系统传递到另一个端系统。被路由协议使用路由选择表来转发分组。图20-8的路由选择表中列出了被路由协议或可路由协议（routable protocols）的例子，包括：
  - ——Internet 协议（IP）。
  - ——Internet分组交换（IPX）。
  - ——AppleTalk。
  - ——Digital DECnet。
- **路由选择协议**（*Routing Protocol*）——通过提供共享路由选择表信息的机制来支持被路由协议。路由选择协议的消息在路由器之间传送。路由选择协议允许路由器通过与其他路由器进行通信来更新和维护自己的路由选择表。TCP/IP中路由选择协议的例子包括：
  - ——路由选择信息协议（RIP）。
  - ——内部网关路由选择协议（IGRP）。
  - ——增强型内部网关路由选择协议（EIGRP）。
  - ——开发式最短路径优先（OSPF）。

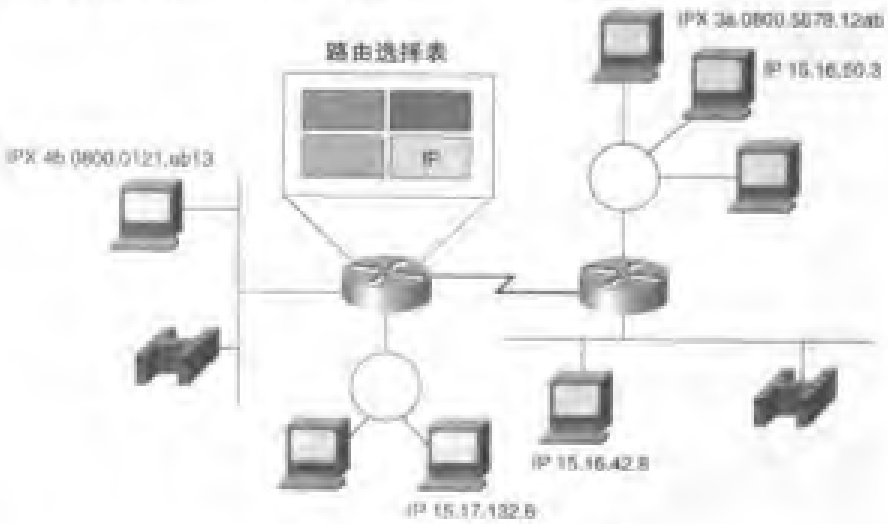


图20-8 路由选择协议

为了使一个协议可路由(routable)，必须使管理员能为每台设备分配一个网络编号和一个主机编号。某些协议，比如IPX，只要求管理员分配一个网络编号，因为他们使用主机的介质访问控制地址（MAC地址）作为物理编号。其他的协议，比如IP，要求提供一个完整的地址和一个网络掩码。

要形成一个被路由的网络，需要IP地址和网络掩码。网络掩码用于分离32bitsIP地址的网络和主机部分。IPX通过连接MAC地址与管理员分配的网络地址来产生完整的地址，不使用网络掩码。对于IP地址，网络地址通过比较地址和网络掩码获得的。

网络掩码的使用使得一组连续IP地址可以作为一个单元看待。如果不允许这样的分组，每台主机都必须为路由选择单独映射，这对于目前因特网中数百万台主机而言是不可能的。从192.168.10.1到192.168.10.254的序列中，所有254个地址都可以用网络地址192.168.10.0表示。因此，只要定位到了网络地址，数据就能发送到这些主机中的任何一台，按照因特网软件联盟（www.isc.org）的建议，路由选择表中只需要保存一个条目192.168.10.0，而不是254个单独条目。要使路由选择能起作用，

必须使用这个分组过程。

路由选择是OSI第3层的功能。作为一种分层的组织的方案，它允许许多单个地址聚合起来，作为一个单元来对待，直到需要单个地址以实现数据的最终传递时为止。路由选择是一个发现从一台设备到另一台设备的最高效路径的过程，如图20-9所示。完成这一过程的主要设备是路由器。

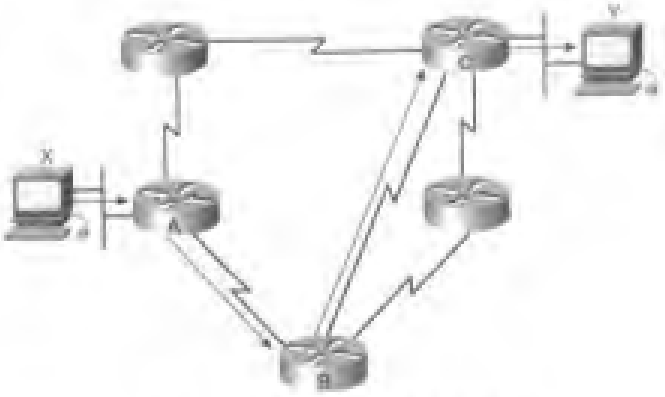


图20-9　网络层协议的工作原理

路由器有两项关键功能：

- 维护路由选择表并确保其他路由器知道网络拓扑的变化。这项功能是通过路由选择协议将网络信息传达给其他的路由器来实现的。
- 当分组到达一个接口时，路由器必须使用路由选择表来确定向哪里发送分组。路由器将分组交换到适当的接口，添加该接口需要的帧格式，然后真正将帧传送出去。

路由器是一种网络层的设备，使用一个或多个路由选择度量值来确定转发网络流量应该使用的最优路径。路由选择度量值是一个用于确定路由优良程度的值。路由选择协议使用各种标准的组合来确定路由选择度量值，如图20-10所示。

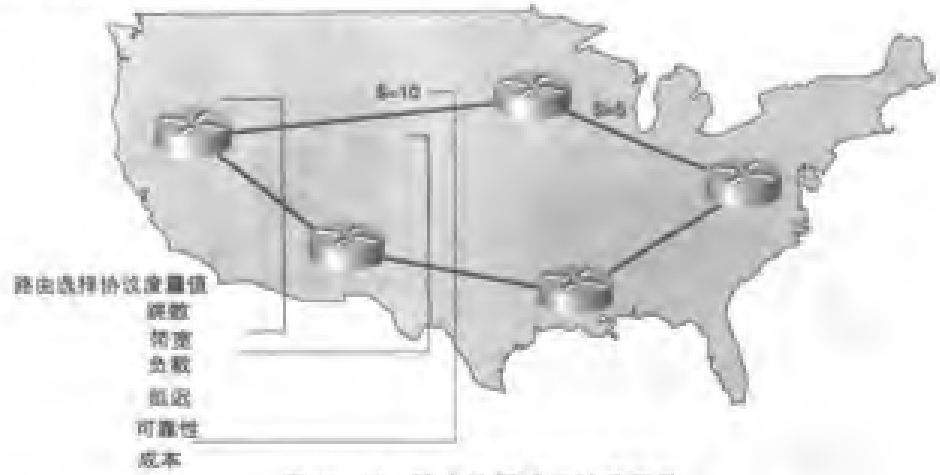


图20-10　路由选择协议的度量值

包含跳数（hop）、带宽（bandwidth）、延迟（delay）、可靠性（reliability）、负载（load）和成本（cost）在内的多个度量值一起计算，形成了确定网络间最优路径的不同组合值。路由器互连多个网段或完整的网络。它们根据第3层信息在网络间传送数据帧。路由器逻辑上决定在互连网络中传送数据的最佳路径，然后将分组送到适当的输出端口，完成针对传输的封装。分组每次经过路由器时，都会发生这种封装和解封装的过程，如图20-11所示。从一台设备发送数据到另一台设备涉及封装和解封装的过程。封装指的是将数据流分解为多个段，添加适当的头和尾，然后发送数据。解封装指的是相反的过程：去处头和尾，然后重新将数据组合成无缝的流。路由器

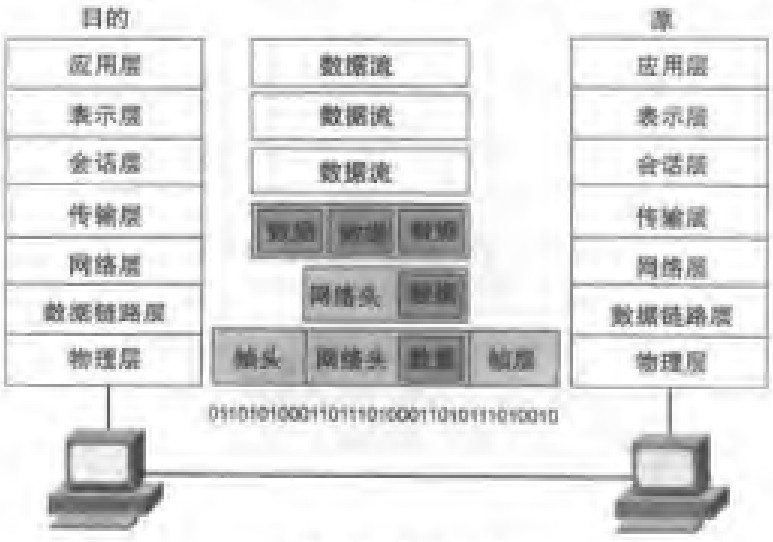


图20-11　数据封装

从局域网设备处（比如工作站）取得帧，然后根据第3层信息，将它们在网络上进行转发。

本节集中介绍了最常用的可路由（或者被路由）协议——IP。尽管重点集中在IP上，你应该知道还有其他的可路由协议（比如IPX/SPX和AppleTalk）。

像IP、IPX/SPX和AppleTalk这样的协议提供了第3层支持，因此是可路由的。然而，某些协议不支持第3层，它们被归为不可路由协议（nonroutable protocols）。最常见的不可路由协议是NetBEUI。NetBEUI是一个小型、快速并且高效的协议，仅限于在一个网段上运行。

20.4.1 外部和内部路由选择协议

路由器使用路由选择协议交换路由选择信息。换句话说，路由选择协议决定如何对被路由协议进行路由。如图20-12所示，内部网关协议（IGP）和外部网关协议（EGP）是路由选择协议的两个家族。家族的划分依据它们对自治系统的处理方式。

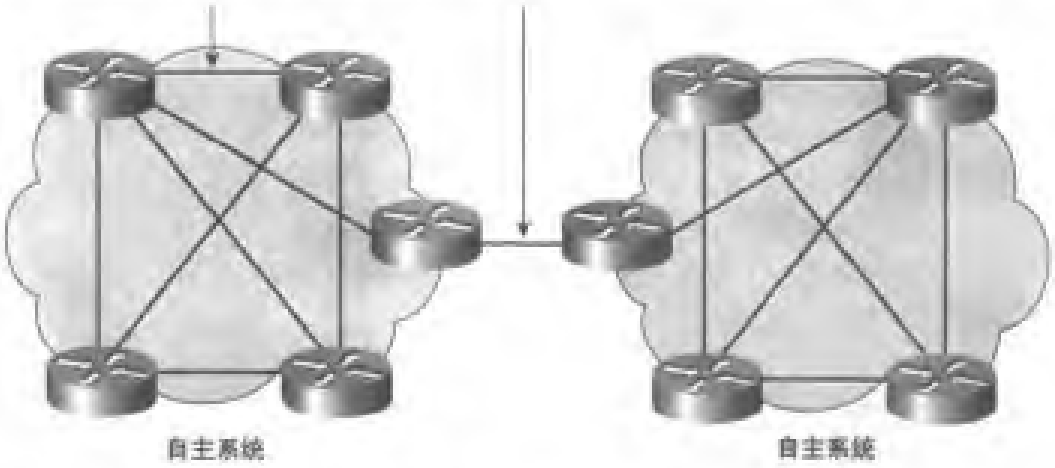


图20-12 IGP和EGP

自治系统（autonomous system）是由单个实体进行管理控制的一个或一组网络，比如cisco.com域。一个自主系统由对外呈现一致路由选择方式的多台路由器构成。因特网地址授权协会（IANA，Internet Assigned Numbers Authority）向各个区域登记处分配自治系统编号。这些登记处是负责美洲、加勒比海和非洲的ARIN(hostmaster@arin.net)；负责欧洲的RIPE-NCC(ncc@ripe.net)；负责亚太区的AP-NIC(admin@apnic.net)。自主系统编号是一个16bits的数字。某些路由选择协议，比如边界网关协议（BGP），要求你在配置中指定该惟一分配的自主系统编号。

IGP在自主系统内对数据进行路由。IGP的例子包括：

- 路由选择信息协议版本1和2（RIPv1）和RIPv2。
- 内部网关路由选择协议（IGRP）。
- 增强内部网关路由选择协议（EIGRP）。
- 开发式最短路径优先（OSPF）。
- 中间系统到中间系统协议（IS-IS协议）。

EGP在自主系统之间路由数据。BGP是EGP应用最为普遍的例子。

20.4.2 在路由器上启用RIP和IGRP

距离矢量路由选择方案确定了到互连网络中任何链路的方向（矢量）和距离（跳数）。距离矢量算法周期性地（如每30秒）发送其全部或者部分的路由选择表给相邻的邻居。即使网络中没有变化发生，运行距离矢量路由选择协议的路由器也会周期性发送更新。通过接收邻居的路由选

择表，路由器可以检验所有已知的路由，并根据从邻居路由器接收到的更新信息来对本地的路由选择表进行修改。这个过程也称为“按传闻进行路由选择（routing by rumor）”，因为某台路由器对网络的理解是根据邻居对网络拓扑的看法得出的。距离矢量协议使用Bellman-Ford算法来计算最佳路径。

距离矢量协议的例子包括：

- **路由选择信息协议**（*RIP*）——因特网上最常用的IGP。RIP使用跳数作为自己的路由选择度量标准。
- **内部网关路由选择协议**（*IGRP*）——Cisco开发这种IGP来解决大型异构网络中的路由选择问题。

20.4.3　IGRP和RIP使用的路由选择度量标准

当路由选择算法更新路由选择表时，其首要目标是确定路由选择表中需要包含的最优信息。路由选择算法使用不同的度量标准来确定最佳路由。每种路由选择算法都用自己的方式解释“最佳”。路由选择算法为网络中的每条路径生成一个数，称为度量值。复杂的路由选择算法可以根据多个度量标准进行路由选择，将它们结合成一个综合度量标准。如图20-13所示。通常，度量值越小，路径越优。

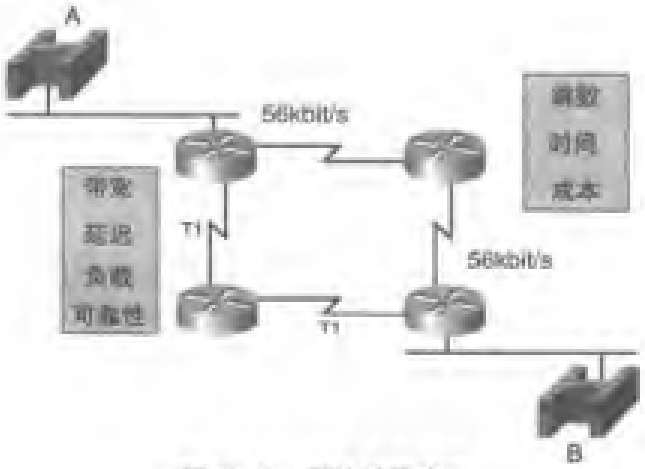


图20-13　路由选择度量

度量标准可以基于路径的单个特征，也可以基于多个特征。路由选择协议最常用的度量标准如下：

- **带宽**（*Bandwidth*）——链路的数据容量。（通常，10-Mbit/s的以太网链路比64-kbit/s的租用线路更优。）
- **延迟**（*Delay*）——分组沿各条链路从源到目的所需的时间。延迟的多少取决于中间链路的带宽、每台路由器的端口队列、网络拥塞和物理距离。
- **负载**（*Load*）——网络资源（比如路由器或链路）上的活动数量。
- **可靠性**（*Reliability*）——通常参考各条网络链路上的错误率。
- **跳数**（*Hop count*）——分组要到达目的地所必须经过的路由器数量。数据通过的每台路由器都被看作一跳。跳数为4的路径表示数据经过该路径到达最终目的地之前需要通过4台路由器。如果到达目的地有多条路径，路由器会选择跳数最少的路径。
- **成本**（*Cost*）——网络管理员指定的任意值——通常基于带宽、金钱花费或其他的计量标准。

20.4.4　比较和对比区分距离矢量、链路状态和混合协议的关键操作

链路状态协议设计用于克服距离矢量协议的局限性。链路状态路由选择协议对网络变化快速响应，只在网络改变发生时才发送触发式更新，并以很长的时间间隔，比如每隔30分钟，发送周期性更新（称为链路状态刷新）。

当链路状态改变时，检测到该变化的设备会产生一个关于该链路（路由）的链路状态通告（LSA），该LSA会传播到所有邻近的设备。每台路由选择设备都会获得该LSA的一份拷贝，然后更新其链路状态（逻辑）数据库，并将该LSA转发给所有邻近的设备。这种LSA的洪泛是必需的，目

的是保证所有的路由选择设备，在创建一个反映网络新拓扑的更新后的路由选择表之前更新其数据库，如图20-14所示。

链路状态数据库用于计算经过网络的最佳路径。通过在链路状态数据库上应用Dijkstra最短路径优先（SPF）算法构建SPF树，链路状态路由器就能确定到达目的地的最佳路径。然后，从最短路径优先树中选择最佳（最短）路径放入路由选择表。

链路状态协议的例子包括开发式最短路径优先（OSPF）和中间系统到中间系统（IS-IS），如图20-15所示。

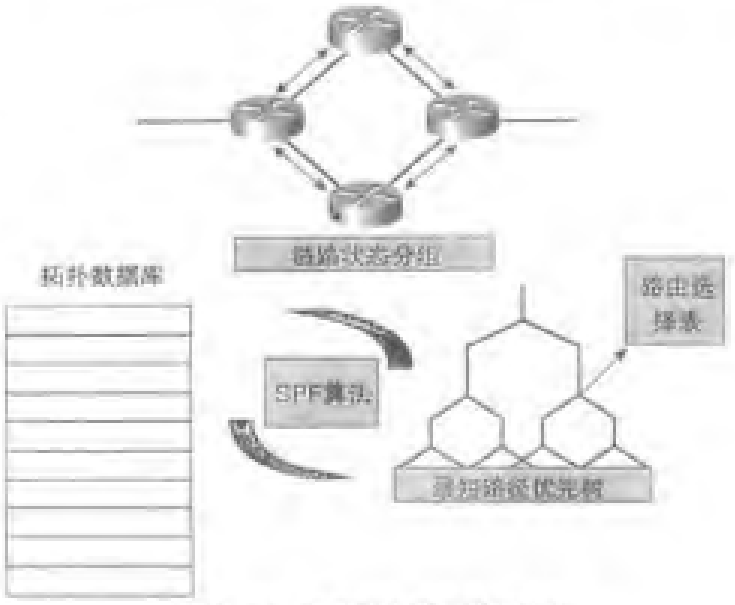


图20-14 链路状态路由选择协议

RIP使用跳数来确定互连网络中任意链路的方向和距离，如图20-16所示。如果到一个目的地有多条路径，RIP会选择跳数最少的一条路径。然而，由于跳数是RIP使用的惟一路由选择度量标准，因此所选的路径不一定是到达目的地的最快路径。RIP版本1（RIPv1）只使用分级路由选择，意味着网络上的所有设备都必须使用相同的网络掩码，因为RIPv1在路由选择更新中不包含子网信息。



图20-15 链路状态路由选择协议



图20-16 RIP使用跳数作为其度量标准

RIP

RIP版本2 (RIPv2)提供了被称为前缀路由选择（prefix routing）的机制，在路由更新中发送子网掩码信息，通过这种方式来支持无类路由选择（classless routing）。对于无类路由选择协议，同一网络中的不同子网可以用不同的子网掩码。在同一个网络中使用不同的子网掩码，称为可变长度子网掩码（VLSM）。

IGRP

IGRP作为一种距离矢量协议，是Cisco专门针对大型网络中路由选择相关问题的，这些问题是

类似RIP这样协议无法解决的。IGRP可以根据延迟、带宽、负载和可靠性选择最快的路径。缺省时，IGRP只使用带宽和延迟度量标准并使用一个24bits的度量值。IGRP对最大跳数的限制比RIP大得多，因此允许网络的扩展。IGRP仅使用有类路由选择（classful routing）。

EIGRP

和IGRP一样，EIGRP也是Cisco专有的协议。EIGRP是IGRP的高级版本，使用32位的度量值。明确要指出的是，EIGRP提供了更高的运行效率，比如更快的收敛性和更小的带宽开销。它被称为一种高级的距离矢量协议。EIGRP也使用链路状态协议的某些功能，因此，也用术语“混合(hybrid)”来描述EIGRP。

OSPF

Internet工程任务组（IETF）于1998年开发的OSPF，是一种链路状态技术。RFC 2328描述了最常用的版本：OSPF 版本2。OSPF是一种IGP，这意味着它在属于同一个自主系统的多台路由器间分发路由选择信息。OSPF是为了满足RIP无法处理的大型、可扩展互连网络的需求而编写的。

IS-IS

中间系统到中间系统（IS-IS）协议是OSI协议栈中的动态链路状态路由选择协议。因此，它负责在ISO无连接网络服务（CLNS）环境下，为无连接网络协议（CLNP）的数据分发路由选择信息。集成式IS-IS（Integrated IS-IS）是IS-IS协议的一种实现方式，能完成对多种网络协议的路由选择。集成式IS-IS为CLNP路由标记上关于IP网络和子网的信息。在IP世界中，它提供了替代OSPF的另一种选择，将ISO CLNS和IP路由选择混合在一种协议中。它可以仅用子IP路由选择，仅用于ISO路由选择，或者两者的结合。

注意：CLNP指的是OSI的网络层协议，它不要求在传送数据之前建立电路。

BGP

边界网关协议（BGP）是外部网关协议（EGP）的一个例子。BGP在自主系统之间交换路由选择信息，同时保证无环路的路由选择。这是因特网上的大公司和因特网服务提供商们使用的首要路由通告协议。BGP版本4（BGPv4）是BGP的第一个版本，支持无类别域间路由选择（CIDR）和路由聚合。与常用的RIP、OSPF和EIGRP这样的内部网关协议（IGP）不同，BGP不使用类似跳数、带宽或者延迟这样的度量标准。BGP基于网络策略（或者叫规则），使用不同的BGP路径属性来法定路由选择。

本章的内容，甚至本书的内容，都集中在CCNA考试的根本性主题上。因此，请记住本节的内容与通过该考试所要求掌握的主要目标明确相关，并准备好证明对该内容的完全掌握。

20.5 广域网协议

对广域网协议的复习包含下列主题，都是CCNA考试中可能出现的：

- 解释帧中继的关键术语和特征。
- 配置帧中继LMI、映射和子接口。
- 识别ISDN协议、功能分组、参考点和信道。
- 区分下列WAN服务：LAPB、帧中继、ISDN/LAPD、HDLC、PPP和DDR。
- 识别在Cisco路由器上封装WAN数据所用的PPP操作。

- 使用show命令显示网络运行参数，以便检测异常。
- 配置ISDN BRI和传统的按需拨号路由选择（DDR）。
- 用PPP封装配置一条串行连接。

20.5.1 帧中继的关键术语和特征

随着对更高带宽和更低延迟分组交换（packet switching）需求的不断增长，通信服务商引入了帧中继（Frame Relay,FR）。尽管从网络布局上看起来其与X.25类似（见图20-17），可用的数据速率通常最高为4Mbit/s，某些服务商还提供更高的速率。

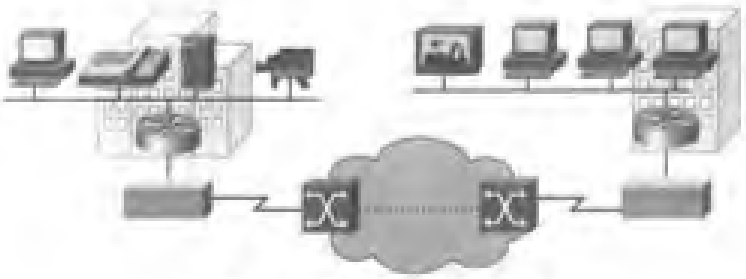


图20-17 使用帧中继的广域网

帧中继在几个方面与X.25不同。最重要的，它在数据链路层而不是网络层运行一个简单得多得协议。术语帧（frame）用于表示数据链路层的单元。

帧中继不实现差错或流量控制。对帧的简化处理减小了延迟。采用了避免中间交换机上帧累积(buildup)的措施，从而减少了抖动。

大多数的帧中继连接都基于*永久虚电路*（PVC），而不是*交换虚电路*（SVC）。到网络边缘的连接通常都是租用线路。从某些服务提供商那里也可以获得拨号连接（使用ISDN线路）。ISDN的D信道用于在一条或更多B信道上建立一个SVC。帧中继的费率基于网络边缘所连接端口的容量和经过协商的容量，或者通过该端口的各个PVC的承诺信息速率（CIR）。

帧中继提供永久的、共享的、介质带宽连接，以承载语音和数据流量，是将企业局域网连接在一起的理想选择。局域网的路由器只需要一个接口，即使使用了多条虚电路（VC）也不例外，到FR网络边缘的租用（短期租用）线路能在非常分散的多个局域网之间提供非常经济的连接。

20.5.2 区分LAPB、帧中继、ISDN/LAPD、HDLC、PPP和DDR

来自网络层的数据被传送到数据链路层，以便能在通常是点对点的物理链路上传送。数据链路层将网络层数据封装成帧，以便能进行必要的检查和控制。每种广域网连接都使用一种第2层协议在通信经过广域网链路时对其进行封装。为了确保使用正确的封装协议，必须对路由器上每个串行接口的第2层封装类型进行配置。封装协议的选择取决于所采用的广域网技术和通信设备。多数的成帧方式都基于HDLC标准。

HDLC成帧方式设计用于在不可靠的线路上提供可靠的数据传输，因此包括了用于流量和差错控制的信令机制。帧总是以一个8比特标志字段开始和结束，该字段的比特模式为01111110，或者是7E16(以16为基数的7E，16进制)。由于这种模式可能出现在实际的数据中，因此发送方的HDLC系统总是会在数据字段的每5个1后面插入一个0，所以实际上标志序列只会出现在帧的两端。接收系统会去除插入的比特。当一个帧紧接着另一个帧传送时，第一个帧的结束标志会用作下一个帧的起始标志。

WAN链路通常是点到点的，不需要地址字段，但地址字段仍然存在。其长度可能是1或2Bytes。控制字段标明了帧的类型，可能是信息帧、监控帧或者无编号帧。无编号帧承载链路建立消息，信息帧承载网络层数据，监控帧控制信息帧的流动，并根据需要在发生错误时请求数据重传。控制字段通常是1Bytes，但对于扩展的滑动窗口系统是2Bytes。地址字段和控制字段一起

称为帧头。

控制字段后面是封装的数据，然后是帧校验序列（FCS），是使用循环冗余校验机制生成的2Bytes或4Bytes的字段。

如图20-18，目前有多种数据链路层协议在使用，包括HDLC的子集或者专用版本的HDLC。图中所包括的PPP协议将在后面进行详细介绍。PPP和Cisco版本的HDLC都在帧头有一个额外的字段，用来标识封装数据所使用的网络层协议。

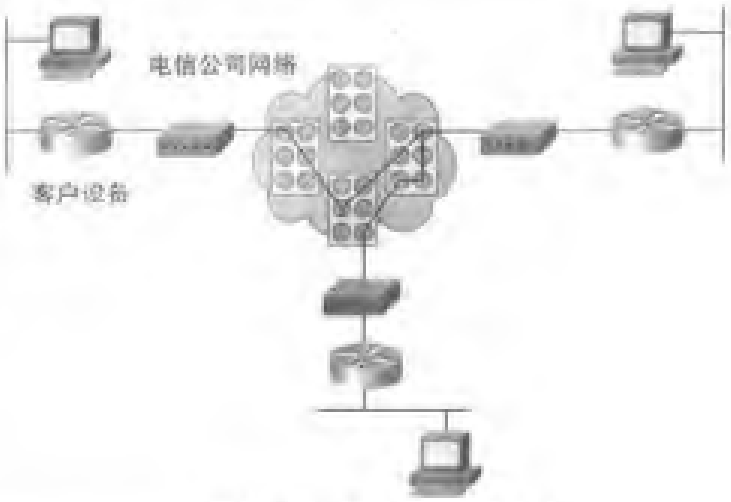


图20-18　广域网帧封装格式

20.5.3　配置ISDN BRI和传流的按需拨号路由选择（DDR）

公共交换电话网（PSTN）的内部连接或者中继线路都已经从承载模拟的频分多路复用信号，转变为承载*时分多路复用*（TDM）数字信号。很明显，下一步就是让本地环路承载数字信号，以实现更高容量的交换式专用连接。

综合业务数字网（ISDN）将本地环路转变为TDM数字连接。该连接上有速率为64-kbit/s的用于传送语音或数据的承载信道（B），以及用于呼叫建立和其他用途的信令信道（delta或D）。

基本速率接口（BRI）ISDN针对家庭和小型企业，提供2条B信道和一条16-kbit/s的D信道。对于更大规模的应用，可以采用基群速率接口（PRI）ISDN。在北美，PRI提供23条B信道和1条D信道，总共的比特速率为1.344Mbit/s（这包括用于同步的一些额外开销）。在欧洲、澳大利亚和世界上其他地区，ISDN PRI提供30条B信道和1条D信道，总共的比特速率为2.048Mbit/s(包括同步开销)。PRI的D信道为64kbit/s，如图20-19所示。注意，北美的PRI速率对应T1连接。国际的PRI速率对应E1连接。

只有两条B信道用于控制，BRI的D信道利用率很低。某些服务提供商支持将D信道用于传送低速率的数据，比如9.6kbit/s的X.25连接。

对于小型的广域网，BRI ISDN是一种理想的连接机制。BRI的呼叫建立时间短（通常小于1秒），并且其64-kbit/s的B信道提供了比模拟调制解调器链路更大的容量。图20-20示例了使用ISDN的广域网。如果需要更大的容量，第二条B信道也可以激活，提供128kbit/s的带宽。尽管这还达不到视频的要求，但带宽的增加使得除了数据流量外还能允许多路同时发生的语音会话。



图20-19　ISDN信道

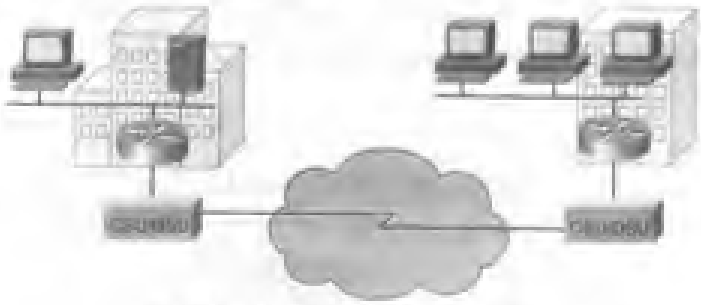


图20-20　使用ISDN的广域网

ISDN另一种常见的应用是提供租用线路连接所需要的额外容量。租用线路的容量用于承载平均的流量负载，ISDN在峰值时使用。当租用线偶尔发生故障时也需要使用ISDN。

ISDN的费率与以每条B信道的模拟语音连接类似。也就是说，两条同时的64-kbit/s连接的花费是一条连接的两倍。

通过PRI ISDN，你可以在两个端点之间连接多B信道，以支持没有延迟或抖动的视频会议和高带宽数据连接。如果跨越长距离，多条连接可能会很昂贵。

20.5.4 通过TFTP进行配置文件管理

在Cisco路由器或交换机中，活动的配置存放在随机访问存储器（RAM）中。Cisco路由器或交换机上存放启动配置的缺省位置是非易失性RAM(NVRAM)。为了防止配置丢失，需要对启动配置进行备份。这些备份拷贝中的一个可以存放在TFTP服务器上。命令copy running-config tftp允许你对配置进行备份。下列的步骤用于该备份过程，如例20-1所示。

- 输入copy running-config tftp。
- 在提示符下输入存放配置文件的TFTP服务器的IP地址。
- 输入配置文件的名称或接受缺省名称
- 每次输入yes表示确认选择。

例20-1 *copy running-config tftp命令*

```
Cougar#copy running-config tftp
Address or name of remote host [ ] 192.168.119.20
Destination file name [Cougar-confg]?
!!!
```

前上传到TFTP服务器上的映像。如例23-8所示，输入了copy tftp flash命令后，系统提示你输入TFTP服务器的IP地址（或名称）。TFTP服务器可能是另一台提供ROM或者Flash存储器软件映像的路由器。然后系统会提示你输入软件映像的文件名。例20-3显示了将名称为C4500-I的系统映像文件复制到Flash存储器过程的示例输出。

如果试图向Flash存储器中复制一个已经存在的文件，系统会提示你同名的文件已经存在。当你将新文件复制到Flash存储器中时，现有的文件会被删除。如果Flash存储器中有存放两个拷贝的空间，第一个拷贝仍然会存放在Flash存储器中，但会置为不可用，以支持最新的版本。当你使用show flash命令时，会看到第一份拷贝显示有[deleted]标记。

如果你中止复制过程，较新的文件会被标记为(deleted)，因为没有完成整个文件的复制，所以该文件是无效的。在这种情况下，最初的文件仍存在于Flash存储器中，供系统使用。

例20-3　copy tftp flash命令

```
Router#copy tftp flash
ILP address or name of remote host [255.255.255.255]? 117722..1166..1133..111111
Name of tftp filename to copy into flash []? c4500-I
copy C4500-I already exists; it will be invalidated!
Copy C4500-I from 172.16.13.111 into flash memory? [confirm] <Return>
xxxxxxxx bytes available for writing without erasure.
erase flash before writing? [confirm] <Return>
Clearing and initializing flash memory [please wait] ####...##
Loading from 172.16.13.111: ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
!!!!!! [text omitted] [OK-324572/524212 bytes]
Verifying checksum...
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvv (text omitted)
Flash verification successful. Length = 1204637, checksum = 0x95D9
```

20.5.6　配置文件管理

捕获show running-config 命令的输出是生成配置备份的另一种方式。你可以通过将输出复制，粘贴到文本文件，并保存文本文件来实现从终端会话上创建这样的备份配置。在可以使用该文件恢复路由器的配置之前，该文件需要一些编辑。图20-21显示了剪切和粘贴配置的示例。



图20-21　剪切和粘贴

要将超级终端中显示在屏幕上的配置文本捕获到文本文件中，需要遵从下列步骤：

步骤1　选择传送（Transfer）。

步骤2　选择捕获文字（Capture Text）。

步骤3　指定用于捕获配置的文本文件的名称。

步骤4　选择启动（Start）开始捕获文本。

步骤5 通过输入show running-config，将配置显示到屏幕上。

步骤6 每次出现“——More——”提示符时，按下空格键，继续显示配置，直到末尾。

步骤7 当配置显示完毕后，用下列步骤停止捕获：

- 选择传送（Transfer）。
- 选择捕获文字（Capture Text）。
- 选择停止（Stop）。

捕获完毕后，你必须对配置文件进行编辑，去除多余的文本。要将文件创建成能复制并粘贴到路由器中去的形式，需要去除所捕获配置中任何不必要的信息。你也可以在文本中添加注释，来对配置的各个部分进行解释。注释行以感叹号（!）开头。

你可以在类似“记事本”这样的文本编辑器中对配置进行编辑。要从记事本中编辑文件，需要下列步骤：

1. 点击文件（File）=>打开（Open）。
2. 找到捕获文件并选择它。
3. 点击打开（Open）。

你需要删除的行包括以下这些：

- Show running-config
- Building configuration . . .
- Current configuration:
- -More-
- Any lines that appear after the word “End”词后的所有行。

在每个接口部分的末尾，添加no shutdown命令。点击文件（File）=>保存（Save），保存删除不必要信息后的配置版本。

你可以从超级终端会话中恢复备份配置。恢复配置以前，在“enable router”提示符下通过erase startup-config命令删除路由器上保留的所有配置，然后输入reload，重新启动路由器。

你可以通过超级终端来恢复配置。要将编辑好的配置备份复制到路由器中，需要下列步骤：

1. 进入路由器的全局配置模式。
2. 在超级终端中，点击Transfer/Send/Text File。
3. 选择用于保存备份配置的文件名称。
4. 文件的各行被输入到路由器中，就好像被键入一样。
5. 查找任何的错误。
6. 输入配置后，按下Ctrl+Z，退出全局配置模式。
7. 用copy running-config startup-config 恢复启动配置。

20.5.7 通过TFTP管理IOS映像

有时候，路由器需要对IOS进行升级或者恢复。当首次使用路由器时，应该对IOS进行备份。你可将IOS映像存放在一台中央服务器上，用其他的IOS映像来恢复或者升级互连网络中路由器或者交换机上的IOS。

服务器上应该运行一个TFTP服务。你可以在特权exec模式下通过copy tftp flash命令启动IOS升级，如例20-4所示。

例20-4 copy tftp flash

```
Cougar# copy tftp flash
Address or name of remote host []? 192.168.119.20
```

```
192.168.119.20 C2600-js-l_121-3.bin
Destination filename [C2600-js-l_121-3.bin]?
Accessing tftp://192.168.119.20/ C2600-js-l_121-3.bin
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue? [confirm]
Erasing device eeeeee…eeeeeeeeeeeee...erased
Loading C2600-js-l_121-3.bin from 192.168.119.20 (via FastEthernet 0/0):
     ! ! ! ! ! ! ! ! ! ! ! ! ! . . . ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
Verifying Check sum. . . . . .OK
[OK-8906589 bytes]
8906589 bytes copied in 277.45 secs
Cougar#
```

路由器提示你输入TFTP服务器的IP地址。当提示输入服务器上IOS映像的文件名时，接下来路由器可能会提示“erase flash”。提示erase flash存储器通常发生在Flash的容量不够容纳新映像的情况下。在映像从Flash存储器中擦除的过程中，会显示一系列的字母“e”来表示擦除的过程。

在下载IOS映像文件的每个数据极时，都会显示一个惊叹号（!）。这个IOS映像的长度是数兆字节，因此可能会花一些时间下载。

新的Flash存储器映像下载完毕后会被检验。现在，路由器已经做好了重新加载以使用新的IOS映像的准备。

20.6 因特网控制消息协议

IP是一种不可靠的网络数据传送方式。IP是一种“尽力的(best-effort)”传输机制。IP没有内置的过程来保证当网络通信存在问题时数据仍能传送。如果每台中间设备，比如一台路由器发生了故障，或者如果目的设备断开了网络连接，都无法完成传送。

另外，在IP的基本设计中，没有告诉发送方数据在传输中发生故障的通知机制。因特网控制消息协议（ICMP）是TCP/IP协议栈的一个组件，解决了IP的这一根本局限性。ICMP没有克服IP不可靠的局限。ICMP给数据发送方发送错误消息，指出在数据传送时发生了问题。图20-22显示了ICMP在TCP/IP模型中的位置。

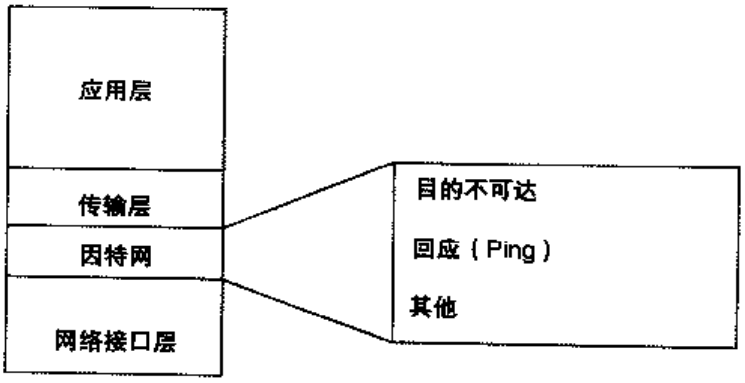


图20-22 ICMP

路由器C没有注意到中间设备传送失败。因此，路由器C没有给路由器A和路由器B，或是给数据发送源设备发送ICMP消息。路由器C也不知道数据报到达那里的路径。数据报只包含源和目的IP地址。数据报中不包含关于所有中间设备的信息。发出报告的设备。只知道发送方的IP地址，并用此地址进行通信。尽管路由器A和路由器B没有直接被通知，但仍可能知道路由器C的接口发生了故障。然而，将该信息分发给邻居路由器不是ICMP的功能。ICMP向发送方报告已传送分组的状态。它的功能

不是传播关于网络变化的信息。

20.6.1 ICMP消息传送

ICMP消息使用IP协议进行传送。ICMP消息作为数据封装到数据报中，封装方式与其他通过IP传送的数据的封装方式相同。表20-8显示了封装在IP分组内的ICMP分组。

表20-8 ICMP封装

帧头	数据报头	ICMP头	ICMP数据
帧头	数据报头	数据报数据域	
帧头	帧数据域		

数据到达网络层后就被封装在一个数据报中。然后，数据报和它所封装的数据又被进一步封装为数据链路层的帧。ICMP消息有其自己的头部信息。但是，该信息和ICMP数据一起进行封装，就和数据报中的任何其他数据一样。ICMP消息的传送方式和任何其他的数据一样，因此，也同样受传送故障的影响。这就产生了这样一种情况：故障报告又会产生更多故障报告，这会在状况已经很差的网络上引起更强的拥塞。因为这个原因，ICMP消息引起的错误不产生自身的ICMP消息。因此，有的数据报传送错误可能永远无法报告给数据的发送方。

20.6.2 错误报告和错误纠正

ICMP是一个针对IP的错误报告协议。当发生数据报传送错误时，ICMP用于将这些错误报告给数据报的发送者。例如，图20-23中的工作站1正在给工作站6发送一个数据报。当路由器C上的相应端口发生故障时，路由器C就会利用ICMP给工作站1发送消息，指出数据报可能无法传送。ICMP不负责纠正所遇到的网络故障。在图20-23的例子中，ICMP不会尝试去纠正阻止数据报传送的路由器C的接口问题。ICMP惟一能做的就是向工作站1报告错误。

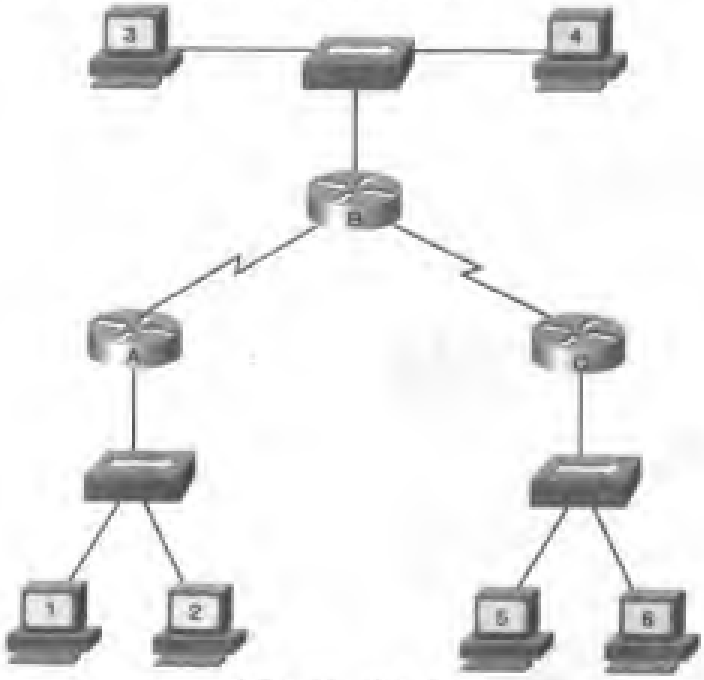


图20-23 错误报告

20.6.3 不可达网络

实现网络通信需要满足某些基本条件。首先，必须在发送和接收设备上正确地配置了TCP/IP协

议栈，包括TCP/IP协议的安装和IP地址以及子网掩码的正确配置。如果数据报要传送到本地局域网以外，还需要配置一个缺省网关。其次，必须有适当的中间设备将数据报从源设备及其网络路由到其目的网络。路由器完成该功能。另外，路由器的接口上必须适当地配置TCP/IP协议，并且路由器必须使用适当的路由选择协议。

如果满足不了这些条件，网络通信就不能完成。例如，发送方可能将数据的地址标为一个不存在的IP地址，或者目的设备没有与网络连接。如果连接接口发生故障，或者路由器没有找到目的网络所必需的信息，则路由器也可能成为故障点。如果目的网络不可到达，就称为不可达网络（unreachable network）。

目的不可达消息包含下列几种：

- **网络不可达**（*Network unreachable*）——这种消息通常意味着路由选择或者寻址故障。
- **主机不可达**（*Host unreachable*）——这种消息通常意味着传送故障，比如错误的子网掩码。
- **协议不可达**（*Protocol unreachable*）——这种消息通常意味着目的网络不支持分组中指定的上层协议。
- **端口不可达**（*Port unreachable*）——这种消息通常意味着TCP端口［套接字(socket)］不可用。

图20-24和图20-25显示路由器接收了一个无法将其传送到最终目的地的分组的过程。可能是由于没有到目的地的已知路由，所以分组不可传送。由于没有已知路由，路由器给数据源发出一条ICMP主机不可达消息。

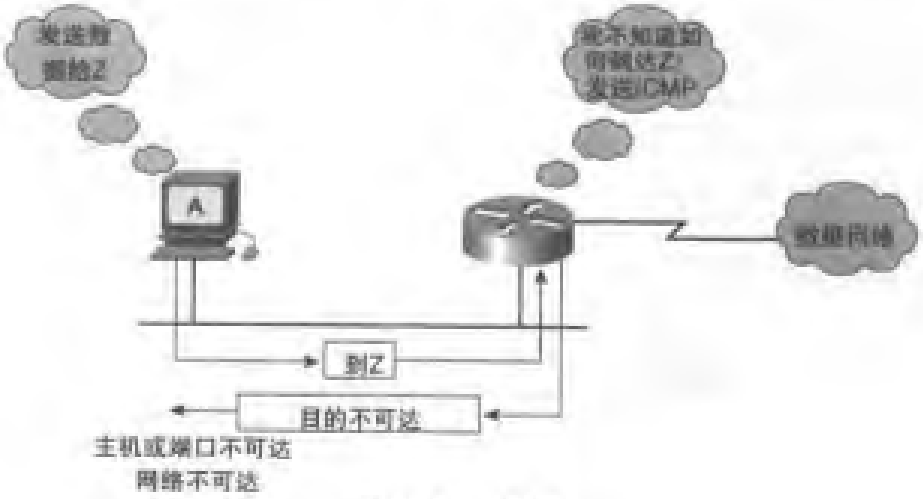


图20-24　ICMP

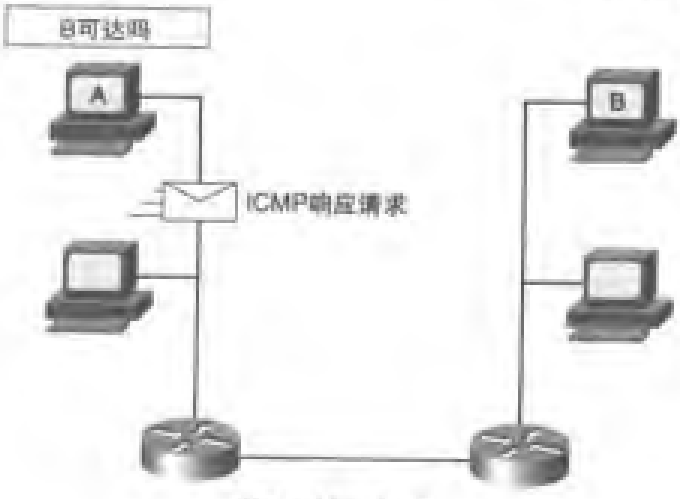


图20-25　ICMP

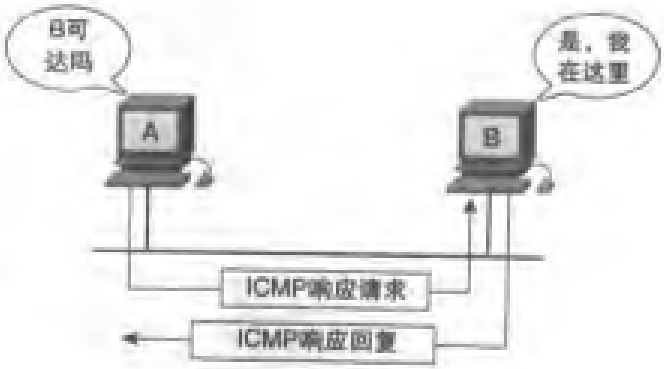


图20-26　回应请求（Echo Request）

20.6.4 用ping测试目的地的可达性

ICMP协议允许你测试某个特定目的地的可达性。图20-26显示了用ICMP向目的设备发送了一条回应请求(echo request)消息。当目的设备接收到ICMP回应请求时，它生成一条回应回复（echo reply）消息，并将其发送给发出回应请求消息的设备。如果发送方收到了回应回复消息，就确认了目的设备可以通过IP协议到达。

如例20-5所示，回应请求消息通常用ping命令发出。本例中，该命令与目的设备的IP地址一起使用。

例20-5 ICMP ping 命令的输出

```
C:\>ping 198.133.219.25

Pinging 198.133.219.25 with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=30ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247

Ping statistics for 198.133.219.25:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 20ms, Maximum = 30ms, Average = 22ms


C:\>
```

也可以如例20-6那样使用ping命令，使用目的设备的DNS名称（假设DNS是可用的）。在这些例子中，ping命令发出4条回应请求，并接收到4条回应回复，从而确认了两台设备之间的IP连接。表20-9显示了Cisco ping 命令的返回代码。

例20-6 ping 命令的输出

```
C:\>ping www.cisco.com
Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:
Reply from 198.133.219.25: bytes=32 time=30ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
Ping statistics for 198.133.219.25:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 20ms, Maximum = 30ms, Average = 22ms
C:\>
```

表20-9 Cisco的 ping返回代码

代码	含义	可能原因
!	每个惊叹号表示收到一个ICMP回应回复	ping 成功完成
.	每个句号标识网络服务器在等待回复的过程中超时	该消息可能意味着很多问题 ping 被访问控制列表或者防火墙阻塞 路径上的路由器没有到达目的地的路由并且没有发送ICMP目的地不可达消息 路径上的某处出现了物理连接问题
U	收到了一个ICMP不可达消息	路径上的某台路由器没有到达目的地址的路由
C	收到了一个ICMP源抑制消息	路径中的设备——可能是目的方——也许接收到了太多的流量；检查输入队列
&	收到了一个ICMP超时消息	可能出现了路由选择环路

20.7 访问列表

网络管理员必须解决如何拒绝对网络不必要的访问，同时允许适当的访问。尽管各种安全工具，比如口令、回叫设备和物理安全设备都很有帮助，它们通常都缺乏对基本流量进行过滤的灵活性和大多数管理员都愿意采用的具体控制。例如，网络管理员可能希望允许用户访问因特网，但不希望外部用户使用Telnet访问局域网。

路由器通过*访问控制列表*（ACL）提供基本的流量过滤功能，比如阻塞因特网流量。一个ACL是连续多个应用于地址或上层协议的permit或deny语句的集合。在本章中，你会学习使用标准或者扩展ACL作为控制网络流量的手段，并了解ACL是如何用作安全解决方案的一部分的。

此外，本章还包含关于如何使用ACL的技巧、考虑事项、建议和通用指导方针，以及创建ACL所需的命令和配置。最后，本章提供了标准和扩展ACL的例子，并介绍了如何将ACL应用到路由器的接口上。

正确配置ACL，并知道在网络中哪里放置ACL是很重要的。ACL在网络中有多种用途。常见的ACL功能包括在网络内部对分组进行过滤，保护内部网络不受非法的因特网访问，以及限制对虚拟终端端口的访问。

20.7.1 ACL概述

ACL是应用到路由器接口上的指令列表。这些列表告诉路由器接受哪些类型的分组，拒绝哪些类型的分组。接受和拒绝都基于某些规范，比如源地址、目的地址和TCP/UDP端口号。

ACL使你能对流量进行管理，并通过将ACL 应用到路由器接口来扫描特定的分组。按照ACL中的某些条件对经过接口的任何流量进行检测。

ACL的创建可以针对所有被路由网络协议，比如IP和IPX，以过滤通过路由器的分组。可以在路由器上配置ACL来控制对网络或子网的访问。

ACL通过控制对路由器接口上的被路由的分组进行转发还是阻塞来过滤网络流量。路由器检查每个分组，根据ACL中指定的条件来确定是转发还是丢弃。ACL条件可能是流量的源地址、目的地址、上层协议或者其他信息。

ACL必须基于每种协议来定义。换句话说，在每个你希望控制的接口，对每种你希望控制的协议，你都必须定义一个在该接口上启用该协议的ACL。（注意，某些协议将ACL称为过滤器。）如果路由器接口上同时配置了IP、AppleTalk和IPX，你就需要至少定义3个ACL。如图20-27所示，通过增加对流入和流出路由器接口的分组进行过滤的灵活性，ACL可以作为一种网络控制工具。

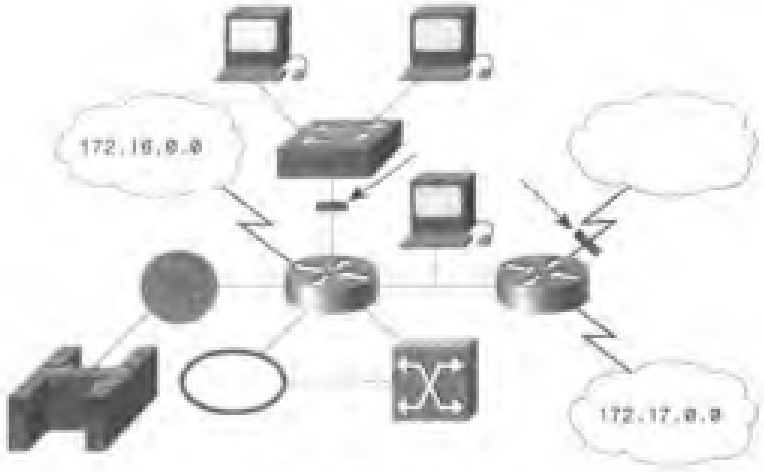


图20-27 ACL示例

20.7.2 创建ACL的原因

创建ACL的原因很多。例如，你可以用ACL完成下列任务：

- 限制网络流量并提高网络性能。例如，ACL可以指明，根据一种协议，某类分组被路由器处理时优先于其他的流量。这被称为队列（queuing）。队列确保路由器不处理不需要的分组。结果是，队列限制了网络流量并减少了网络拥塞。
- 提供流量控制。例如，ACL可以限制或者减少路由选择更新的内容。这些约束能用于限制特定网络的信息在网络中传播。
- 针对网络访问提供基本的安全级别。ACL可以允许一台主机访问网络的一部分，并阻止其他的主机访问相同的区域。
- 确定在路由器的接口上转发或阻塞哪种类型的流量。例如，你可以允许对电子邮件流量进行路由，同时阻塞所有的Telnet流量。

本章的内容，甚至本书的内容，都集中在CCNA考试的根本性主题上。因此，请记住本节的内容与通过该考试所要求掌握的主要目标明确相关，并准备好证明对该内容的完全掌握。

20.8 Cisco设备、IOS与网络基础

对于Cisco设备、IOS和网络基础的复习，CCNA考试中会覆盖下列的主题：

- 描述路由器的组成元素（RAM、ROM、Flash、NVRAM、配置寄存器）。
- 配置路由器口令、身份认证和标记。
- 使用上下文敏感的帮助工具。
- 使用命令历史和编辑功能。
- 完成路由器的初始配置（包括使用setup模式）。
- 使用show命令显示基本的网络运行参数。
- 描述路由器的启动序列。
- 从某台主机建立到特定网络设备的连接并完成配置任务。
- 依照开放的标准互连网络设备。

20.8.1 路由器初始启动输出

路由器每次加电时，都会经过下列的启动序列：

1. 路由器经过加电自检诊断程序来检查CPU、内存和接口的基本运行情况。

2. 系统对软件进行引导，启动映像执行并搜索有效的Cisco IOS映像（路由器操作系统软件）。Cisco IOS映像的来源，无论是Flash存储器或是TFTP服务器，都由配置寄存器的设置确定。配置寄存器的出厂缺省设置是0x2102。这表明路由器应该尝试从Flash存储器加载Cisco IOS映像。

3. 如果经过5次尝试都没有在Flash存储器中找到一个有效的Cisco IOS映像，路由器会回到boot ROM模式。这种模式用于安装或者升级Cisco IOS映像。

4. 如果找到了一个有效的Cisco IOS映像，路由器接着会寻找一个有效的配置文件。

5. 如果在NVRAM中没有找到有效的配置文件，路由器会打开系统配置对话框，以便你能手工生成配置文件。对于路由器的正常运转，Flash存储器中必须有一个有效的Cisco IOS映像，NVRAM中必须有一个配置文件。

在例20-7和例20-8中，所显示的消息根据路由器接口和Cisco IOS版本的不同而有所差别。输出中所显示的内容仅供参考，可能无法准确地反映控制台的屏幕显示。

例20-7 NVRAM无效

```
System Bootstrap, Version X.X(XXXX) [XXXXX XX], RELEASE SOFTWARE
Copyright (c) 1986-199X by Cisco Systems
2500 processor with 4096 Kbytes of main memory

Notice: NVRAM invalid, possibly due to write erase.

--- output omitted ---
```

例20-8 自举和IOS版本

```
--- output omitted ---
IOS (tm) X000 Software (XXX-X-X), Version XX.X(XXXX) [XXXXX XXX]
Copyright (c) 1986-199X by Cisco Systems, Inc.
```

注意： *在第一个例子中，非易失性RAM(NVRAM)是无效的，这可能是由于写擦除。这告诉读者该路由器尚未完成首次配置，或者NVRAM被擦除了。只有经过了配置，路由器才能使用。*

在第二个例子中，用户可以确定路由器上运行的自举程序和IOS的版本。用户还可以确定路由器的型号、处理器和路由器所包含内存的大小。输出中列出的其他信息包括：

- 路由器有几个接口。
- 路由器接口的类型。
- NVRAM的大小。
- Flash存储器的大小。

20.8.2 建立一个超级终端会话

所有Cisco路由器都包含一个EIT/TIA-232异步串行控制台端口（RJ-45）。需要线缆和适配将控制台终端（一台ASCII终端或者运行终端模拟软件的PC）连接到控制台端口。要将ASCII终端连接到控制台端口，需要使用RJ-45到RJ-45反线和RJ-45到DB-25母头适配器 。要将运行终端模拟软件的PC连接到控制台端口，需要使用RJ-45到RJ-45反线和RJ-45到DB-9母头适配器。

控制台端口的缺省参数是9,600波特率、8数据比特、无奇偶校验、1停止毕特并且无流量控制。控制台端口不支持硬件流量控制。

要将一台终端连接到路由器的控制台端口，需要按照下列步骤：

步骤1 用RJ-45到RJ-45反线和一个RJ-45到DB-9或者RJ-45到DB-25的适配器连接终端。

步骤2 按照9,600波特率、8数据比特、无奇偶校验、1停止比特并且无流量控制来配置终端或者运行终端模拟软件的PC。

表20-10列出了操作系统和可以使用的终端模拟软件。

表20-10 终端模拟软件

PC操作系统	软件
Windows 95, Windows 98 Windows 2000, Windows XP	超级终端（Windows自带软件），ProComm Plus
Windows 3.1	终端（Windows自带软件）
Macintosh	ProComm、VersaTerm、ZTerm (单独提供)

20.8.3 登录进入路由器

要配置Cisco路由器，必须通过一台终端或者远程接入来访问路由器上的用户界面。访问路由器时，用户在输入其他的任何命令之前必须首先登录进入路由器。

出于安全的目的，路由器对命令有两种访问级别，如例20-9所示：

- **用户exec模式**——典型的任务包括检查路由器状态。在该模式下，不允许改变路由器配置。
- **特权exec模式**——典型的任务包括改变路由器配置。

登录进入路由器时，会显示用户exec模式提示符。此用户级别下可用的命令是特权exec级别下可用命令的一个子集。大多数情况下，这些命令允许用户显示信息，但不能改变路由器的设置。

例20-9 *路由器模式*

```
Router
!User Mode
Router>enable
Password:
Router#
!Privileged-Mode
Router>disable
Router>
```

20.8.4 键盘帮助

在用户exec模式提示符或者特权exec模式提示符下输入问号（?）会显示常用命令列表。注意示例输出底部显示的——More——。屏幕一次显示22行。底部的——More——提示符指出输出有多屏，如例20-10所示。

例20-10 键盘帮助

```
Router#?
Exec commands:
access-enable      Create a temporary Access-List entry
access-profile       Apply user-profile to interface
access-template    Create a temporary Access-List entry
```

```
archive             manage archive files
bfe                 For manual emergency modes setting
cd                  Change current directory
clear               Reset functions
clock               Manage the system clock
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
disconnect          Disconnect an existing network connection
elog                Event-logging control commands
enable              Turn on privileged commands
erase               Erase a filesystem
exit                Exit from the EXEC
help                Description of the interactive help system
--More-
isdn                Make/disconnect an isdn data call on a BRI interface
lock                Lock the terminal
login               Log in as a particular user
logout              Exit from the EXEC
more                Display the contents of a file
mrinfo              Request neighbor and version information from a multicast router
mrm                 IP Multicast Routing Monitor Test
mstat               Show statistics after multiple multicast traceroutes
mtrace              Trace reverse multicast path from destination to source
name-connection     Name an existing network connection
no                  Disable debugging functions
pad                 Open a X.29 PAD connection
ping                Send echo messages
ppp                 Start IETF Point-to-Point Protocol (PPP)
pwd                 Display current working directory
reload              Halt and perform a cold restart
resume              Resume an active network connection
rlogin              Open an rlogin connection
rsh                 Execute a remote command
send                Send a message to other tty lines
setup               Run the SETUP command facility
```

```
show                Show running system information
--More-
slip                Start Serial-line IP (SLIP)
start-chat          Start a chat-script on a line
systat              Display information about terminal lines
telnet              Open a telnet connection
terminal            Set terminal line parameters
test                Test subsystems, memory, and interfaces
traceroute          Trace route to destination
tunnel              Open a tunnel connection
udptn               Open an udptn connection
undebug             Disable debugging functions (see also 'debug')
verify              Verify a file
where               List active connections
write               Write running configuration to memory, network, or terminal
x28                 Become an X.28 PAD
x3                  Set X.3 parameters on PAD
```

当出现——More——提示符时，你可以通过按下Spacebar看下一屏。如果只要显示下一行，按下Return或Enter。按其余的任意键回到提示符状态。

要访问特权exec模式，输入enable。输入enable会使路由器提示用户输入密码。在特权exec模式提示符下输入问号（见例20-11），会显示比用户exec模式下更长的一个命令列表。

例20-11 Exec模式命令

```
Cisco#?
Exec commands:
access-enable       Create a temporary Access-List entry
access-profile      Apply user-profile to interface
access-template     Create a temporary Access-List entry
archive             manage archive files
bfe                 For manual emergency modes setting
cd                  Change current directory
clear               Reset functions
clock               Manage the system clock
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
disconnect          Disconnect an existing network connection
```

```
elcg                Event-logging control commands
enable              Turn on privileged commands
erase               Erase a filesystem
exit                Exit from the EXEC
help                Description of the interactive help system
  -More -
```

注意：此处所显示的命令列表是大小写敏感的。当你处于用户模式和enable模式以及处于全局配置模式和接口配置模式时，所看到的列表都是不同的。

根据Cisco IOS软件级别和路由器配置不同，屏幕的输出也不相同。

20.8.5 IOS编辑命令

用户界面包括一个增强编辑模式，该模式提供一套关键编辑功能，用户能像输入命令一样对命令行进行编辑。使用表20-11中列出的组合键，可以将光标在命令行中左右移动，以进行修正或者更改。尽管在当前的软件版本中，增强编辑模式是自动启用的，但如果写成的脚本在增强编辑功能启用时交互不当，该功能也可能被禁用。要禁用增强编辑功能，在特权exec模式提示符下输入terminal no editing。

表20-11 编辑命令

命令	描述
Ctrl+A	移至命令行开头
Ctrl+E	移至命令行末尾
Esc+B	后移一个词
Ctrl+F	前移一个字符
Ctrl+B	后移一个字符
Esc+F	前移一个词

对于屏幕显示超过一行的命令，编辑命令集提供了水平滚动的功能。当光标到达右边界时，命令行会左移10个空格。行首的10个字符将看不见，但是用户可以回滚，以检查命令行开头部分的语法。

要回滚，可以按下Ctrl+B，或者重复按下**左箭头键**，直到命令输入的开头。Ctrl+A直接返回行首。

20.8.6 路由器命令历史

用户界面提供了已经输入命令的历史，或者叫记录。这项功能对于找回较长或者复杂的命令或条目特别有用。命令历史功能使你能完成下列任务：

- 设定命令历史缓冲区的大小。
- 找回命令。
- 禁用命令历史功能。

缺省情况下，命令历史功能是启用的，系统会在其历史缓冲区中记录10条命令。要改变某个终端会话过程中系统记录中的命令行数，需要使用terminal history size或者history size命令，命令最多为256。表20-12显示了关于命令历史的命令。

要在历史缓冲区中找回命令，需要从最近的命令开始，按下Ctrl+P。不断按下Ctrl+P和向上箭头键，可以接连找出更早的命令。使用Ctrl+P或向上箭头键后，要返回命令缓冲区中最近的命令，可以重复按下Ctrl+N或向下箭头键来接连返回最近的命令。

表20-12 路由器命令历史

命令	描述
Ctrl + P（或者仅仅是向上箭头键）	找回上一条（前一条）命令
Ctrl + N（或者仅仅是向下箭头键）	找回最近的命令
show history	显示命令缓冲区的内容
terminal history [size *number-of line*]	设置命令缓冲区的大小
terminal no editing	禁用高级编辑特性
terminal editing	重新启用高级编辑特性
Tab	完成命令行

输入命令时，作为一种快捷方式，你可以输入某个命令起始的惟一性字符串。当你按下Tab键时，用户界面会将输入补齐。当输入的字符串能惟一标识某条命令时，Tab键只是可视地表明路由器已经理解了用户想输入的某个命令。

在多数的计算机上，还有其他的选择和复制功能可用。可以复制以前的命令串，然后将其作为当前的命令条目粘贴或者插入。

20.8.7 对命令错误进行故障排除

本实验介绍了Cisco互连网络操作系统（IOS）命令行用户界面。任务是登录进入路由器并使用用户模式和特权模式这两种不同的访问级别来输入命令。无论是用户模式还是特权模式，你都需要熟悉相应模式下可用的命令。还可以使用路由器帮助工具、历史功能和编辑功能。IOS命令界面是对Cisco路由器进行配置的最常用的方法。尤其是在特权模式下，有很多命令可用。不要被大量的命令所吓倒。很多命令平时是不常用的。

20.8.8 Cisco IOS的目的

与任何的计算机一样，路由器或者交换机没有操作系统也无法工作。Cisco将自己的操作系统称为Cisco互连网络操作系统，或者简称为Cisco IOS。这是所有Cisco路由器嵌入的软件体系结构，也是Catalyst交换机的操作系统。一台路由器只有加载了IOS才能工作。离开了操作系统，硬件就无法发挥作用。Cisco IOS提供了下列网络服务：

- 基本的路由选择和交换功能。
- 对连网资源可靠和安全的访问。
- 网络的可扩展性。

20.8.9 Cisco IOS的运行

Cisco IOS 设备有三种不同的运行环境或者模式：

- ROM monitor。
- Boot ROM。
- Cisco IOS。

路由器启动进程通常会加载到RAM中，并建立上面3种之一的运行环境。系统管理员可以使用配置寄存器设置来控制路由器加载的是哪种模式。

ROM monitor完成自举过程并提供低层的功能和诊断。ROM monitor用于从系统故障中恢复和恢复丢失的口令。你不能通过任何网络接口访问ROM monitor，只能通过控制台端口会话。

当路由器运行在boot ROM模式中时，只有Cisco IOS功能集的一个有限的子集是可用的。Boot ROM模式允许对Flash存储器进行写操作，因此主要用于修改存储在Flash存储器中的Cisco IOS映像。

你可以通过在boot ROM模式下使用copy tftp flash命令，将存放在TFTP服务器上的IOS映像复制到路由器的Flash存储器中，对Cisco IOS映像进行修改。

路由器的正常运行需要来自Flash存储器的完整的Cisco IOS映像。在某些设备中，该IOS直接在Flash存储器中运行。然而，多数的Cisco 路由器要求将IOS的一个拷贝装载到RAM中，并在RAM中执行。某些IOS映像在Flash存储器中以压缩格式存储，因此在复制到RAM中时必须解压缩。

要查看当前运行的IOS映像和版本，可以使用show version命令，该命令还能指出配置寄存器的设置。在例20-12中，show flash命令使你能检验系统是否有足够的内存来装载一个新的Cisco IOS映像。

例20-12 IOS映像

```
Cisco>show flash

System flash directory:
File  Length      Name/status
  1    8022152     /c2500-i-1.121-16.bin
[8022216 bytes used, 366392 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

20.8.10 Cisco IOS的特征

Cisco为范围很广的网络产品平台提供了IOS映像。为了优化不同产品平台所需要的Cisco IOS软件，Cisco正致力于开发很多不同的Cisco IOS软件映像。每个映像都代表了一个不同的特征集，针对于不同的设备平台、可用的存储器资源和客户需求。

针对不同的Cisco设备型号和特性集，有数量众多的IOS映像。然而，这些映像的基本配置命令结构是相同的。在任何一种设备上所获得的配置和故障排除经验，可以应用到很大范围的产品上。

不同Cisco IOS版本的命名习惯包含下列3部分：

- 映像所运行的平台。
- 映像所支持的特定功能。
- 映像运行的位置以及它是否已经被压缩过。

Cisco IOS命名习惯、名字中各个字段的含义、映像的内容和其他细节是容易改变的。

选择了满足网络需求的选项后，就可以选择该硬件平台所能支持的Cisco IOS软件版本。每种设备的软件需求在文档CD的“Cisco 产品文档”部分列出。“Cisco软件顾问（Cisco Software Advisor）”是一个交互式工具，能提供最新的信息。

20.8.11 show version命令

show version命令显示关于当前正在路由器上运行的Cisco IOS软件版本的信息，包括配置寄存器和启动字段的设置。

- IOS版本和描述性信息。
- 自举ROM版本。
- 启动ROM版本。
- 路由器正常运行时间。
- 上次重新启动的方式。
- 系统映像文件和位置。

- 路由器的平台。
- 配置寄存器设置。

20.8.12 路由器用户界面

Cisco IOS软件使用命令行界面（CLI）作为其传统的控制台环境。IOS是扩展到多数Cisco产品线的核心技术。在不同的网络互连设备上，它的运行细节是不同的。

你可以通过多种方式访问CLI。一种访问方式CLI的方式就是通过控制台会话。控制台使用一种从计算机或者终端直接到路由器上控制台连接的低速串行连接。访问CLI会话的另一种方式是通过调制解调器，或者连接到路由器AUX端口的零调制解调器产生的拨号连接。这两种方式都要求在路由器上配置网络服务。访问CLI会话的另一种方式就是Telnet到路由器上。要建立到路由器的Telnet会话，必须至少为一个接口配置IP。

还必须为虚拟终端会话配置登录和密码。

路由器用户界面和各种模式

Cisco CLI使用了一种分层的结构。这种结构要求进入各种不同的模式以完成各种特定的任务。例如，要配置一个路由器接口，必须进入接口配置模式。在接口配置模式下，输入的所有配置都只对该接口有效。每种命令模式都用自己独特的提示符标识，也只允许使用适于该模式的命令。

IOS提供了被称为“命令执行者（command executive，exec）”的命令解释服务。每条命令输入后，exec都验证并执行该命令。

作为一种安全特性，Cisco IOS软件将exec会话分成两种访问级别：用户exec模式；特权exec模式，也称为enable模式。

用户exec模式只允许使用有限数量的基本监控命令，因此通常被称为只读模式。用户exec级别不允许使用任何可能改变路由器配置的命令。提示符“>”指出你目前正处于用户exec模式下。

20.8.13 Cisco IOS故障排除

某些情况可能阻碍路由器正常启动，包括：

- 配置文件丢失或者boot system语句不正确。
- 不正确的配置寄存器值。
- 受损的Flash存储器映像。
- 硬件故障。

路由器启动时，会在配置文件中查找boot system语句。Boot system 语句可以强迫路由器从Flash存储器中IOS映像以外的其他映像启动。要确定启动映像的来源，可以键入show version命令，查找标明映像启动来源的行，如例20-13所列。

例20-13 映像启动来源

```
Cisco>show version
--- output omitted ---

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTLDR: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), RELEASE SOFTWA
RE (fc1)
```

不正确的配置寄存器设置可能使IOS无法从Flash存储器中加载。配置寄存器的值会告诉路由器

从哪里获得IOS。对于该信息，你可以使用show version命令，并查找最后一行关于配置寄存器的信息来确认，如例20-14所示。

例20-14 配置寄存器

```
Cisco>show version
---- output omitted ----

Configuration register is 0x2102
```

表12-13描述了其他有用的路由器状态命令。

表20-13 路由器状态命令

命令	描述
show version	显示有关系统硬件、软件版本、配置文件的名称来源和启动映像的配置，还显示系统最近一次重启的原因
show processes	显示关于活动进程的信息
show protocols	显示所配置的各种协议。该命令显示了所配置的任何一种第3层（网络层）协议的状态
show memory	显示关于路由器内存的统计信息，包括针对空闲内存池的统计信息
show stacks	监视进程和中断例程的堆栈使用情况
show buffers	提供路由器上缓冲池的统计信息
show flash	显示关于Flash存储器设备的信息
show running-config（Cisco IOS 软件版本10.3 及以前的版本中使用write term）	显示活动配置文件
show startup-config（Cisco IOS软件版本10.3及以前的版本中使用show config）	显示备份配置文件
show interface	显示配置的所有接口的统计信息

正确的配置寄存器值随硬件平台的不同而不同。Cisco IOS文档中应该包含一份打印版的show version 输出。如果没有文档，你可以检查Cisco文档CD或Cisco.com上的资源，来确定正确的配置寄存器值。通过在配置中改变配置寄存器的值并保存为启动配置可以纠正错误值。

如果问题依然存在，则路由器上的Flash存储器映像文件可能受损。在这种情况下，启动过程中会显示一个错误信息。显示的错误信息如下：

```
open: read error...requested 0x4 bytes, got 0x0
trouble reading device magic number
boot: cannot open "flash:"
boot: cannot determine first file name on device "flash:"
```

如果Flash存储器映像损坏，你应该向路由器中上传一个新的IOS。如果通过这部分的检查没有找到问题，路由器可能有硬件故障。如果是这样，请联系Cisco技术支持中心（TAC）。尽管硬件故障很少见，但的确会发生。

20.9 总结

本章提供了CCNA考试中所强调的主要目标和主题的一些内容。尽管本章不是面面俱到，没有包含你在考试中会遇到的所有内容，但的确对主要的主题进行了简要的总结。记住，为了全面准备CCNA考试，你需要学习很多命令、概念和示例。

20.10 关键术语

访问控制列表（*access control list*，*ACL*） 控制或者限制网络流量的一种手段。ACL会根据预先定义的规则集来对比各种标准。

自举协议（*Bootstrap Protocol*，*BOOTP*） 网络节点用该协议来确定其以太网接口的IP地址，以影响网络的启动过程。

扩展ACL（*extended ACL*） 将源IP地址、目的IP地址、TCP/UDP端口号和其他的标准与标准ACL定义的规则进行比较。

防火墙（*firewall*） 在已连接的公共网和专用网之间作为缓冲的路由器或接入服务器（一台或多台）。用作防火墙的路由器一般采用访问控制列表和其他方法来保证专用网的安全性。

Flash存储器（*Flash memory*） 一种特殊类型的EEPROM（可电擦除可编程只读存储器），它可以一次性被全部擦除和重写，而不是一次一个字节。许多现代的PC都具有存储在Flash存储器芯片上的BIOS，以便在需要时可以很容易地更新。这种BIOS有时也称为FlashBIOS。Flash存储器在调制解调器中也是很常见的，因为它能够使调制解调器制造商们在新协议成为标准时支持这些新协议。

非易失性随机访问存储器（*nonvolatile RAM*，*NVRAM*） 断电后仍能保存其内容的随机访问存储器。

永久虚电路（*permanent virtual circuit*，*PVC*） 永久建立的虚电路。由于特定的虚电路任何时候都必须存在，它节省了电路建立和拆除所需的带宽。在ATM术语中，称为永久虚连接。

排队（*queuing*） ACL指定某些分组被路由器处理时优先于其他流量的过程，所基于的是某些可配置的参数，比如指定某种协议。

随机访问存储器（*RAM*） 可由微处理器读写的易丢失存储器。

交换虚电路（*switched virtual circuit*，*SVC*） 按需求动态建立，并在数据传输完成后拆除的虚电路。它用于数据传输间歇性的情况中。在ATM术语中称为交换虚连接。

时分多路复用（*time-division multiplexing*，*TDM*） 可以根据预先指定的时隙为来自多条信道的信息分配单条线路上带宽的技术。不管工作站是否有数据要传输，都会为每条信道分配带宽。

简易文件传输协议（*trivial file transfer protocol.TFTP*） FTP的简化版，允许文件从一台计算机通过网络传输到另外一台计算机上，而且通常不需要使用客户端身份验证（例如用户名和密码）。



第21章　关于融合型网络技术的介绍

目标

学习完本章之后，你将能够：

- 描述语音、视频和数据网络传统上是如何实现的。
- 比较和对比数据语音（voice-over-data）技术。
- 描述语音、视频和数据网络。
- 描述Cisco AVVID的特征和主要组成部分。
- 识别新兴的关于融合网络的应用及其功能。
- 描述QoS在语音、视频和数据集成网络中的影响。

本章描述了传统的语音、视频和数据网络是如何实现的，并解释了各种类型的数据语音技术。此外，本章还介绍了对融合型语音、视频和数据网络的需求和Cisco集成化语音、视频和数据体系结构(AVVID)以及针对融合网络的新应用。本章还讨论了关于服务质量（QoS）的常见问题。

21.1　传统网络

传统上，企业为数据、语音和视频应用提供分离的网络。这些传统网络都是自主部署、独立运行，通常由不同的团队实现和管理。

这些分离的网络构成了企业的局域网和广域网，并分别用于连接专用用户交换机（PBX）设备、H.320视频会议设备和路由器。这些网络中，在专线、租用线路上提供PBX和H.320视频服务，并通过租用线、帧中继和ATM的组合提供数据服务。图21-1描述了这些分离网络的典型部署。

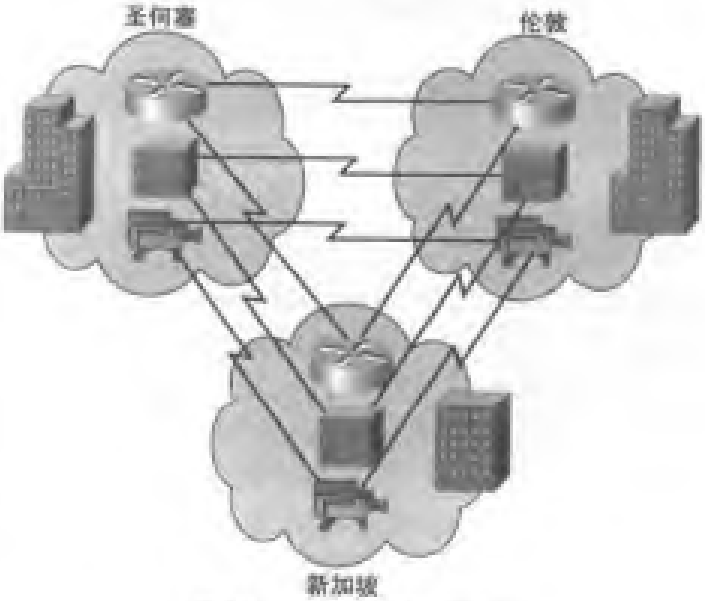


图21-1　典型的传统网络

21.2　关于语音和数据网络的介绍

集成化语音和数据网络支持多种应用，这些应用都是为了以更低的成本替代租用线路。支持语音的路由器可以作为针对办公室内部呼叫的本地电话系统。在图21-2中，用户拨叫了一个位于相同办公室的电话分机。这台支持语音的路由器将呼叫路由到适当的目的地。支持语音的路由器可以作为针对办公室内部呼叫的电话系统，也可以在企业网内对呼叫进行路由。

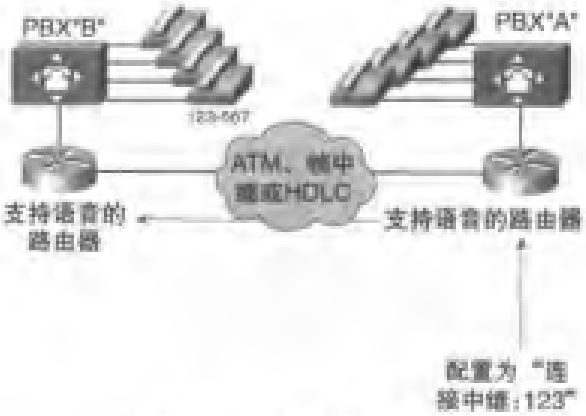


图21-2　语音和数据网络

21.2.1　帧中继语音

帧中继语音（Voice over Frame Relay，VoFR）技术将语音和语音频带数据（包括传真和模拟调制解调器）与帧中继网络上的数据服务进行了合并。VoFR支持PBX使用帧中继永久虚电路（PVC）进行连接。其目的是以更低的成本替代租用线路。通过VoFR，客户可以更容易地增加其帧中继服务的链路速度或者其承诺信息速率（CIR），以支持额外的语音、传真和数据流量。

注意：CIR是帧中继网络所承诺在一般条件下传输信息的速率，它是在最小时段内的平均值。承诺信息速率（以bit/s为单位）是重要的协商式资费标准之一。

支持语音的路由器同时将PBX和数据网络连接到公共帧中继网（见图21-3）。支持语音的路由器包括一块帧中继适配器（Voice Frame Relay Adapter，VFRAD）或者一个在数据网上支持语音流量的语音/传真模块。

复杂的排队技术保证了帧中继语音的QoS。帧中继的优点如下：

- 由于帧中继网络在很多区域很常见，因此作为多服务网络的传输很受欢迎。
- 很经济的服务，并能很好地支持突发流量。
- 为语音帧分配比数据帧更高的优先级，以保证QOS。



图21-3　VoFR网络

21.2.2　ATM语音

ATM语音（Voice over ATM，VoATM）是多服务网络的理想传输方式，特别是对于已经安装了ATM网络的客户。ATM对语音、视频和数据的处理都令人满意。ATM的一项主要好处在于其内在的针对语音、视频和数据流量网络传输特殊需求的设计（见图21-4）。

ATM支持多种控制延迟和延迟变化的机制，包括：

- 服务质量（*QoS*）——使得通信能获得特定的带宽和延迟变化保证。
- 虚电路排队——区分对待各个流量。例如，分配给语音流量的优先级比对延迟不敏感的流量更高。
- 固定长度的小信元——53Bytes的ATM信元减少了变长分组所带来的排队延迟和延迟变化，也减少了经过中间交换机时的延迟。

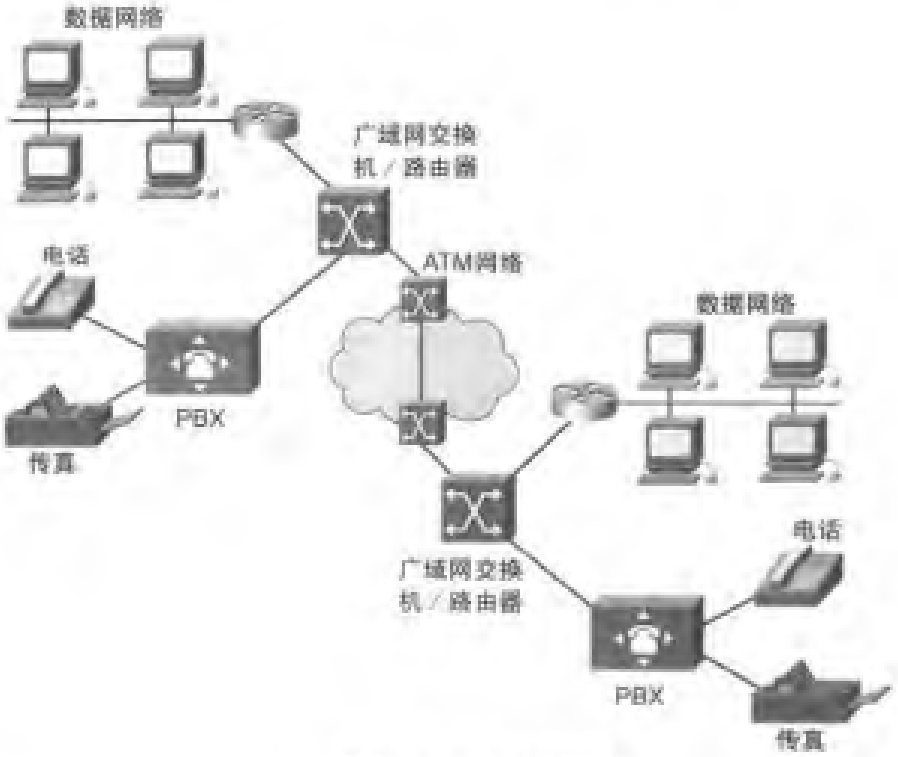
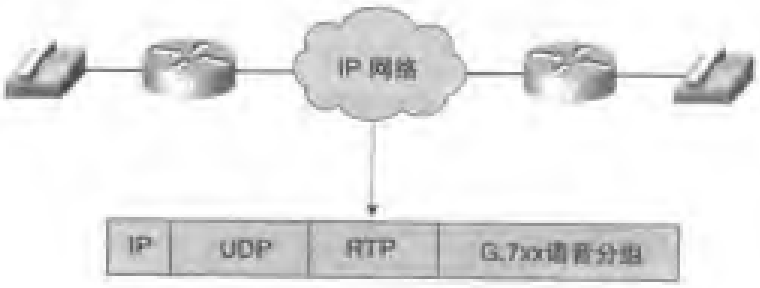


图21-4 VoATM网络

21.2.3 IP语音

IP语音（Voice over IP，VoIP）应用和其他应用一样运行在IP之上。当语音信息穿过IP栈时，封装了IP/用户数据报协议/实时传送协议（IP/UDP/RTP）头；这些信息在接收端进行解封装。在UDP之外使用RTP来提供额外的传输功能，例如时间标记和VoIP分组的排队，这都是UDP不提供的。在数据链路层，VoIP分组可以采用第2层的封装，包括点到点协议（PPP）、高级数据链路控制（HDLC）、帧中继、ATM、以太网等等（见图21-5）。

当用户需要一个易于实施的解决方案，以提供语音和传真功能并处理电话到计算机的语音通信时，可以选择VoIP作为其语音传输介质。



VoIP分组

图21-5 VoIP

21.2.4 比较各种数据语音技术

帧中继、ATM和IP都是流行的数据语音技术，它们一直处于发展之中以满足目前不断扩大的数据语音应用。如表21-1所示，每种技术都有自己的优势和局限性。

表21-1 各种数据语音技术的优点和缺点

数据语音技术	优点	缺点
帧中继	确定的标准；服务普遍	最高速率为T1/E1
ATM	确定的细粒度的服务分类	服务尚不普遍；设备过去很昂贵
IP	由于节约潜力最大，因此广泛部署；特殊的服务类技术	无连接 最不确定

21.3　语音、视频和数据网络

供应商们快速地采用和移植到利用IP作为数据、语音和视频应用的传送方式进一步认可了到融合型网络构架的转换。历史上使用时分复用（TDM）基础设施并依赖“旧世界”惯例的服务提供商（比如电话公司），现在正依赖于IP。

融合网络（Converged networks）是一种持续的趋势，数据、语音和视频的合并是多服务网络自然进化的结果。使用IP作为普遍的传输方式提供了下列好处：

- 企业带宽使用效率的显著提高。
- 降低了整体的带宽需求。
- 易于管理。
- 快速部署新应用的能力。
- 在局域网上，数据、语音和视频共享相同的基础设施。

融合网络使企业网络能融合到一个共同的IP传输上。广域网设施以及针对这些设施所需的终接设备的数量都减少了。带宽可以逐步增加，并且可以通过统计复用的方式在多个应用之间共享，提高了效率，降低了复杂性。当没有语音通信时，数据可以利用所有可用的带宽；当出现语音和视频应用时，它们可以保证根据需求获得带宽。

21.3.1　Cisco AVVID

Cisco集成化语音、视频和数据体系结构（Architecture for Voice,Video and Integrated Data AVVID）是针对融合网络的基于标准的开放系统体系结构。Cisco AVVID是针对在普通IP传输上集成数据、语音和视频的企业创新。Cisco AVVID由下列独立的构建块组成（如图21-6所示）：

- 客户端，例如电话、PC、PDA、固定和无线IP电话、H.323视频会议设备。
- 网络平台（局域网交换机、路由器、网关和其他设备）。
- 智能网络服务（QoS、安全、计费和管理）。



图21-6　Cisco AVVID框架

- 因特网中间件（分布式客户联络套件、消息传送方案、多媒体和协同工作工具）。
- 因特网业务集成（集成商、战略合作伙伴和客户）。
- 因特网业务解决方案（通过Cisco AVVID启用、加速并提供Oracle、Siebel和Ariba的服务）。

AVVID要求采用恰当的基础设施和设计。图21-7描述了一个融合型网络，其中所有的数据、语音和视频都以IP作为传输方式；IP广域网是不同地点之间主要的互连方式，公共交换式电话网（PSTN）被用作次要的备份拨号连接方式。

采用开放标准、促进多厂商协同工作和互操作性是Cisco AVVID的主要优点。由于如图21-7所示的网络是基于标准的，因此保证了与其他应用的开放式竞争和互操作性。

AVVID降低了开销，并为语音网络提供了增强的质量选择。它提供了一个具有高度扩展性、可靠性和适应性的网络，并且支持新的和创新应用的快速部署。AVVID允许通过不同厂商产品的集成来提供一个客户化的解决方案。没有哪个厂商能单独提供一个满足所有数据、语音和视频需要的解

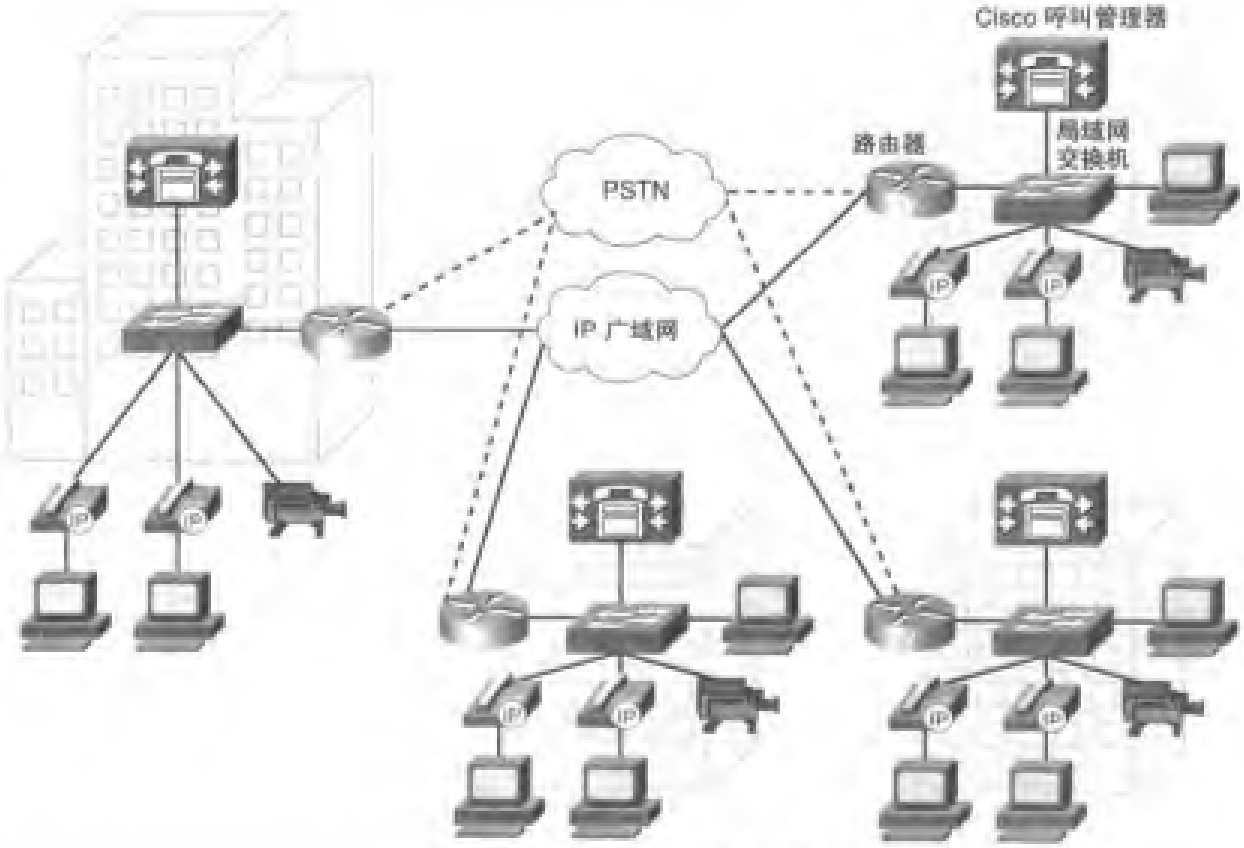


图21-7 语音、视频和数据网络

决方案。特定的应用通常由某个公司设计和实施，并需要集成到整体解决方案中。

21.3.2 融合网络的各种应用

融合网络的一个重要方面便是支持新应用。比如台式IP电话、统一消息传送和*Cisco IP联络中心*这些新兴的应用。融合网络提供了一个框架，许可这些新技术的快速部署。

21.3.3 IP PBX

通过使用Cisco 呼叫管理器（CallManager），可以在融合网络中用IP电话技术替代PBX。Cisco呼叫管理器提供了呼叫控制功能，并且在与IP电话结合使用时，设置了软电话应用，能以一种分布式和可扩展的方式提供PBX功能。语音网关负责连接VoIP网络和其他类型的网络，比如PSTN，或者连接PBX。

21.3.4 统一消息传送

今天，用户有了多种可用的通信和消息传送媒体：电话、手机、呼机、传真、语音邮件和电子邮件。每种方式都需要不同的硬件和软件组件才能工作。***统一消息传送***（Unified messaging）将语音邮件、电子邮件和传真结合成单个应用套件。

有了统一消息传送，单个应用可以存储并检索整套消息类型。语音邮件消息以WAV文件的方式存储，在你旅行时可以作为电子邮件附件下载，响应可以记录并回复到发送方，所有的接受者或者一个扩展的用户列表。电子邮件可以通过电话用户界面（TUI）从文字转换为讲话以进行检索，能通过机场休息室的电话或者手机阅读。由于单个应用可以提供语音、电子邮件和传真，因此所需要

的基础设施减少了。由于以前分散的各类消息现在可以通过最方便的、或者用户最喜欢的界面检索，生产率获得了提高。

通过Cisco GateServer系列产品，Cisco提供了统一消息传送。这些产品为服务提供商和企业提供了开放的、基于标准的接口，从而提供了可扩展的解决方案。图21-8描述了统一消息传送模型。



图21-8　统一消息传送

21.3.5　Cisco IP联络中心

Cisco IP联络中心（IP Contact Center，IPCC）解决方案将数据和语音技术结合，提供了与地域无关的多媒体客户交互。包含了源自多种不同联络渠道的客户交互，包括IP语音、TDM语音、web、电子邮件和传真。无论传输方式是因特网还是传统的PSTN，Cisco IPCC这个完全集成的联络中心体系结构能服务于所有的媒体类型。（见图21-9）。Cisco IPCC体系结构还提供了从传统的呼叫中心到基于IP技术的多媒体联络中心的无缝移植。

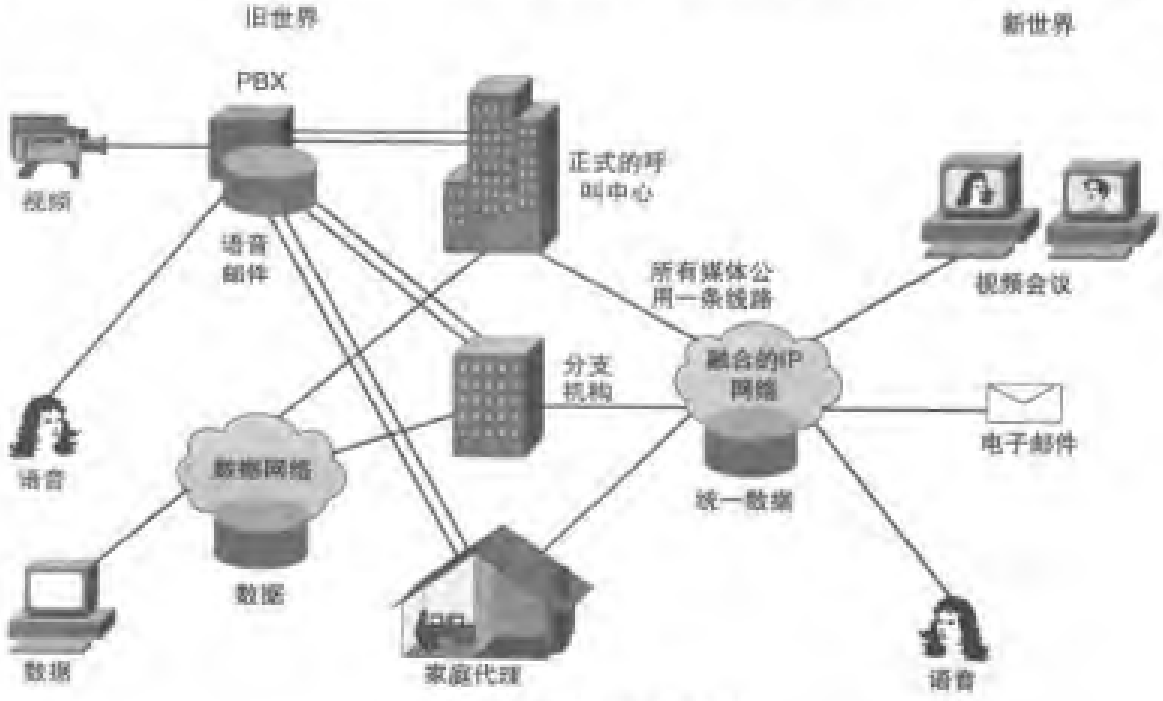


图21-9　Cisco IP 联络中心

Cisco IPCC 解决方案还使服务器和代理级的IP电话能与传统的基于TDM的网络、现有的自动呼叫分配器/专用用户交换机（ACD/PBXs）以及已经安装的桌面系统共存。Cisco IPCC解决方案使一个组织能利用新的基于IP的应用，同时保留不同种类的遗留投资，并利用现有的IP数据基础设施。Cisco IPCC的部署可以是增量式的，以符合企业需求的速率增加IP电话、新的媒体通道和新的基于IP的服务。

Cisco IPCC 在业务上的优点包括：

- 集成式的多媒体排队。
- 基于单一的一套业务规则提供企业范围的联络管理，并为规格化综合报告功能所支持。
- 通过个性化的客户交互增加了客户的满意度。
- 通过普遍存在的IP传输，在代理资源和基于IP的应用服务器两方面都实现了地域无关性。
- 电信级的容错性和系统可靠性。
- 可以从单个站点扩展到多个站点，再到网络服务提供商的多种服务。
- 快速的方案部署，比传统的TDM解决方案速度高数倍。
- 单一网络，消除了多个不同的数据、语音和视频网络所存在的开销。

21.4 QoS的常见问题

分组语音（Voice-over-packet）网络能减少开销并节省带宽；然而，这些网络也存在你必须考虑的独特的QoS问题。在电路交换或者时分复用（TDM）环境中，带宽式专用的，这使得QoS是固有的。在分组交换环境中，所有类型的流量都混合在存储转发方式中。因此，在分组交换环境中，需要设计能提高实时流量优先级的方案。

在一个融合型语音和数据网络中，QoS对于保证与传统电路交换环境中同样高质量的语音传输是至关重要的。语音的QoS问题可以通过VoIP、VoATM或者VoFR标准，或者网络互连设备解决。

21.4.1 延迟（Delay）

延迟（Delay）是分组在两个端点之间传送所需要的时间。在传统的数据网络中，延迟是可以忍受的，对网络用户没有影响或者影响很小；然而，在承载语音通信的网络中，延迟是非常重要的，因为它可能影响用户进行电话交谈的能力。例如，延迟可能导致会话过程中的暂停和中断，增加了一方在另一方完成之前开始说话的可能性。

受网络链路的速度和很多设备有限处理能力的限制，有些延迟是已预料的。电话用户通常可以接受大概150毫秒（ms）的单程延迟而不察觉到任何的问题。你可以在一天中的不同时间和不同网络流量负载的情况下使用ping测量延迟（见图21-10）。如果网络延迟过大，你应该在部署一个承载VoIP流量的网络之前减少它。

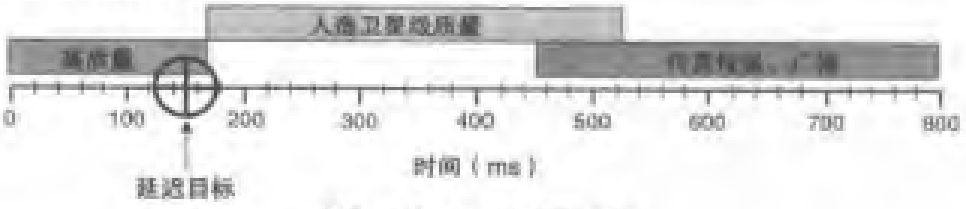


图21-10 QoS问题：延迟

在今天的电话网络中最常见的延迟类型如下：

- **传播延迟**（*Propagation delay*）——传播延迟是由光纤介质或铜介质中光的传播速度特性引起的。
- **处理延迟**（*Handling delay*）——处理延迟（有时也称为Processing delay）定义了各种可能的原因，例如压缩延迟、分组交换延迟和成包延迟。
- **串行处理延迟**（*Serialization delay*）——串行处理延迟是将比特实际放到接口上所花费的时间。

你可以用各种Cisco IOS软件的各种QoS工具来将延迟降到最低，比如低延迟排队和PPP协议分片（PPP fragmentation）。

21.4.2 抖动（Jitter）

抖动（Jitter）与分组所穿越网络中存在的分组间隔时间的变化有关。简言之，抖动就是分组间

隔时间的变化。消除抖动需要聚集分组并将其保持足够长的时间，以使最慢的分组能及时到达并以正确的序列放置。这会引起额外的延迟。

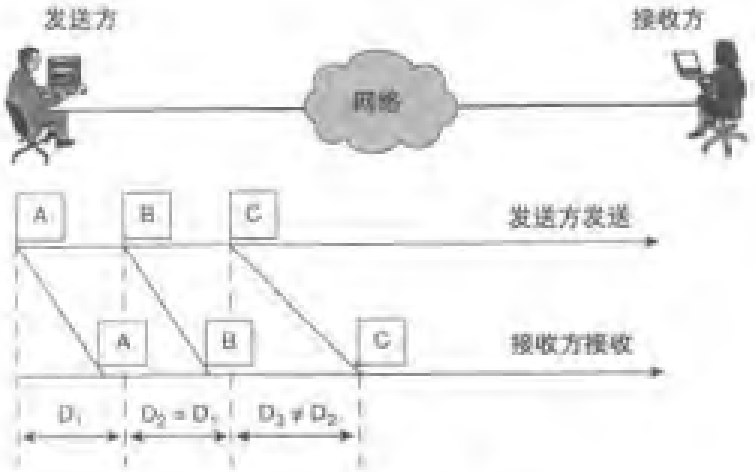


图21-11　QoS问题：抖动

图21-11显示了分组A和B发送和接收所需的时间是相等的（D1=D2）。分组C在网络中遇到了更大的延迟（D3≠D2），接收到的时间比预期晚。这就是为什么抖动缓冲区是必要的，其作用是隐藏分组达到之间延迟的变化。

在Cisco IOS软件中，抖动缓冲区被看作一个动态的队列。这个队列可以根据语音分组之间到达延迟的变化以指数方式增长或收缩。尽管许多厂商选择使用静态抖动缓冲区，但Cisco认为对于基于分组的语音网络，一个设计良好的动态缓冲区是最佳机制。静态抖动缓冲区迫使抖动缓冲区要么太小，要么太大，由于分组的丢失或者太大的延迟会引起声音质量的下降。

21.4.3　丢包（Lost Packets）

丢包可能是一个重要的问题，这需要视分组网络的类型而定。由于IP网络的服务没有保证，因此所表现出的语音分组丢失的发生率比ATM网络更高。

理想地，对于语音和交互视频这样的应用，网络所提供的分组丢失应该为0。对于传真和调制解调器流量，很低的丢失是可以接受的。两个连续的丢失分组会导致一个调制解调器或传真呼叫掉线。对于人与人之间的VoIP呼叫，允许出现的分组丢失就高多了，但这并不是让人满意的。为了进行弥补，分组语音软件可以发送冗余信息，代价是带宽的消耗。

21.4.4　回声（Echo）

即使在传统的电路交换电话网络中，*回声*（Echo）也是存在的。由于网络中往返的延迟小于25毫秒（ms），并且回声通常被每个电话所产生的普通侧音所掩盖，因此通常是可接受的。回声是由于从两线（本地环路）到4线的转换和阻抗不匹配所引起的。

在分组语音网络中，回声是个问题，因为穿越网络的往返延迟通常大于25毫秒。25毫秒后在接收器中听到自己的声音会引起会话中断并破坏节奏。由于这个原因，回声消除技术是必须使用的。

回声消除技术将从分组网络中接收到的语音数据与发送到分组网络中的语音数据进行对比。例如，假设用户A正在和用户B谈话。用户A对B的讲话称为G。当G以回声方式返回用户A时，用户A在实际讲话后的数毫秒内听到了延迟的声音。

为了从线路中消除回声，回声消除器将用户A讲话的翻转图像保留一定的时间；每个回声消除器都收听来自用户B的讲话，并通过减去G以消除任何回声。在基于分组的网络中，回声消除器起可以建入数字信号处理器（DSP）中，也可以作为软件存在。Cisco的所有回声消除都包含在DSP中。

21.4.5　Cisco IOS软件的QoS技术

Cisco IOS软件提供了解决语音、视频和数据应用不同需求的QoS特性和解决方案。Cisco IOS QoS技术支持复杂的网络控制，并能为多种类型的网络应用和流量提供可预知的服务。

各种QoS特性在保证高质量VoIP服务的同时，为关键业务应用提供了高效率和可预知的服务。如图21-12所示，启用了QoS特性，在不同网络负载情况下，语音质量持续保持在高水平上。与之形成对比，未实施QoS会使语音质量随网络负载的增加而下降。

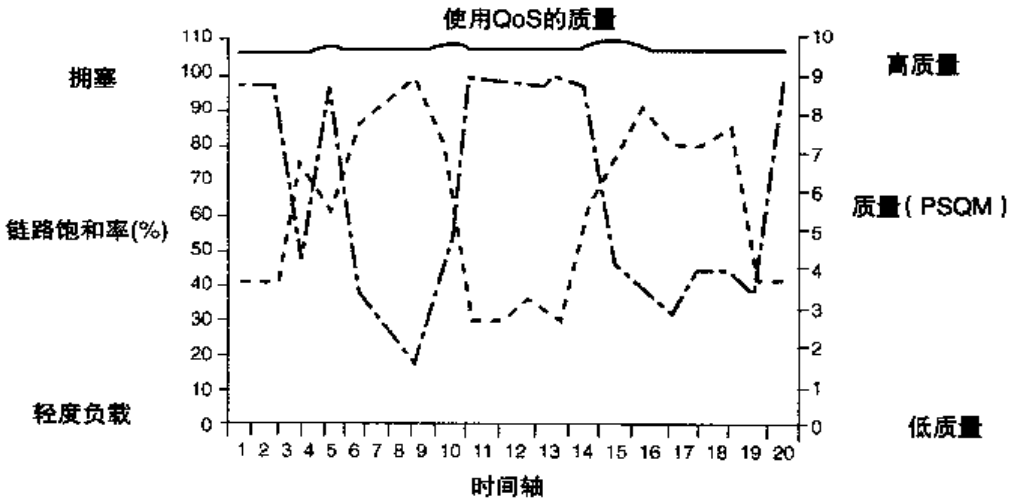


图21-12　VoIP流量-启用QoS

21.5　总结

本章中，你学习了下列关键点：

- 传统上，企业有针对数据、语音和视频应用的分离网络。这些网络通常以相互隔离的方式运作，并且通常由不同的团队实施和管理。
- 集成的语音和数据网络支持多种应用，这都是为了以更低的成本替代租用线路而设计的。
- VoFR是廉价和易于部署的服务，因为帧中继服务是广泛可用的。
- VoATM是多服务网络的理想传输方式，特别是对于已经安装了ATM网络的客户而言。
- VoIP提供了容易地集成高级IP电话功能的能力。
- 语音、视频和数据融合网络降低了成本，并为语音网络提供了更高质量的选择。
- Cisco AVVID是一项针对在普通IP传输上集成数据、语音和视频的企业创新。
- 融合网络的一个重要方面是允许新应用，比如桌面IP电话、统一消息传送和Cisco IP联络中心。
- Cisco IP联络中心（IPCC）解决方案结合了数据和语音技术，以提供地域无关的多媒体客户交互。
- 在整个网络中使用QoS技术能提高分组语音交换网络的传输效率。通过对QoS技术的小心使用，网络设计者能克服质量问题，并以小部分的开销实现电路级别的话音。

作为本章你所学内容的补充，参考本书所附CD-ROM中针对本章的视频、插图和e-Lab实验。

21.6 关键术语

Cisco集成化语音、视频和数据体系结构（*AVVID*） AVVID是一个针对融合网络的基于标准的开放系统体系结构。Cisco AVVID是在普通IP传输上实现集成数据、语音和视频的企业创新。

Cisco IP联络中心（*Cisco IPCC*） IPCC解决方案结合了数据和语音技术，以提供地域无关的多媒体客户交互。这包括源自多种不同联络渠道的客户交互，包含IP语音、TDM语音、web、电子邮件和传真。无论传输方式是因特网还是传统的PSTN，Cisco IPCC的完全集成是联络中心体系结构都能服务于所有的媒体类型。Cisco IPCC体系结构提供了从传统的呼叫中心到基于IP技术的多媒体联络中心的无缝移植。

融合网络（*converged network*） 企业中通过单个网络提供数据、语音和视频应用。

延迟（*delay*） 分组在两个终端点之间传送所需的时间。

回声（*echo*） 由于从两线（本地环路）到4线的转换和阻抗不匹配引起的。

抖动（*jitter*） 与分组所穿越网络中存在的分组间隔时间的变化有关。简言之，抖动就是分组间隔时间的变化。

服务质量（*QoS*） 在确保高质量IP语音服务的同时，用于保证关键业务应用高效和可预知性的各种特性。启用了QoS功能，在不同网络负载情况下，语音质量持续保持在高水平。与之形成对比，未实施QoS意味着语音质量随着网络负载的增加而下降。

传统网络（*traditional network*） 在企业中为数据、语音和视频应用提供分离的网络。这些网络是自主部署的，并且分离运行，通常由不同的团队实施和管理。

统一消息传送（*unified messaging*） 将语音邮件、电子邮件和传真结合为一个应用套件。

帧中继语音（*VoFR*） 将语音和语音频带数据（包括传真和模拟调制解调器）与帧中继网络上的数据服务进行了合并的技术。

IP语音（*VoIP*） 语音应用和其他应用一样运行在IP之上。当语音信息穿过IP栈时，封装了IP/用户数据报协议/实时传送协议（IP/UDP/RTP）头；语音在接收端进行解封装。



第22章　制定网络安全和网络管理策略

目标

学习完本章之后，你将能够：

- 描述网络安全设计。
- 描述网络安全机制。
- 选择安全解决方案。

安全性是网络逻辑设计中最重要的方面之一。但在网络设计过程中它经常被忽视，因为安全性通常被认为是运行中的问题而非设计问题。然而，如果在设计网络之前考虑了安全性，就可以避免在已经完成的设计中加入安全措施性时所带来的扩展性和性能方面的问题。此外，可以当网络仍在逻辑设计阶段就考虑折衷方案，就能够设计出满足安全目标的解决方案。

应该在物理设计阶段开始之间就完成安全性设计，因为安全性设计可能会影响物理设计。本章帮助你和你的网络设计客户一起制定出有效的网络安全策略，并且帮助你选择恰当的工具和产品以实施这些策略。

22.1　网络安全性设计

对于企业网络设计者而言，安全问题现在成了特别热门的话题。这是由于因特网和外连网连接数的增加，因特网上电子商务活动的增加和需要从远端接入企业网络的远程办公者和移动用户的增加。

为了帮助解决与日益增长的安全性需求相关的问题，本章讨论了制定安全策略的各个步骤。本章还包括了针对典型安全挑战的通用安全技术及解决方案，比如保证因特网连接、拨号网络访问、网络服务和用户服务的安全性。在RFC 1244中可以找到这些技术和解决方案。

下列步骤帮助你在设计网络时考虑安全性：

步骤1　确定网络的资产。

步骤2　分析安全风险。

步骤3　分析安全需求和折衷方案。

步骤4　制定安全方案。

步骤5　定义安全策略。

步骤6　制定应用安全策略的过程。

步骤7 制定技术实施策略。

步骤8 得到用户、管理人员和技术人员的认可。

步骤9 对用户、管理人员和技术人员进行培训。

步骤10 实施技术策略和安全过程。

步骤11 对安全性进行检测，如果发现问题就进行更新。

步骤12 通过下列措施来维护安全性：安排定期的独立审核、研读审核日志、对事件做出反应、研读文档和经销商发出的警告信息、持续不断的进行测试和培训以及更新安全方案和策略。

22.1.1 确定网络资产并分析风险

RFC 1244中声明，***网络资产***（network assets）包括网络主机（包括主机的操作系统、应用程序和数据）、网络互连设备（比如路由器和交换机）以及穿越网络的网络数据。网络资产还包括一些不明显但仍然很重要的部分，比如知识产权、商业机密和一个公司的声誉。

从恶意的入侵者到未受过训练的用户下载含病毒的因特网应用程序，这些都是风险。恶意入侵者能够偷窃数据、改变数据并且使合法用户不能得到网络服务（近几年来，这种拒绝服务（或DoS）的攻击已经变得日益普遍了）。

22.1.2 分析安全需求和折衷方案

与绝大多数技术设计需求一样，要达到安全性的目标就意味着要做一些折衷。必需在安全性目标和可承受性、可用性、性能和实用性之间做出折衷。而且，安全性会增加管理工作量，因为需要维护用户登录ID、密码和审核日志。

安全性还会影响网络的性能。一些安全特性，如分组过滤和数据加密，会消耗主机、路由器和服务器的CPU处理能力和内存。

加密会占用路由器或服务器上多达15%的CPU可用资源。可以在专用设备而不是在共享路由器和服务器上实施加密，但这仍对网络性能有影响，因为对分组进行压缩和解压缩会引起延迟。

加密可以减少网络的冗余性。如果所有的流量必须通过一台加密设备，这台加密设备就成了一个单故障点。这便使可用性目标很难实现加密使提供负载均衡也更加困难了。为了最大限度地提高性能，并且把安全措施的复杂性降到最低，负责加密的路由器不应该提供负载均衡。仍然可以使用负载均衡，但必须对提供加密的路由器是透明的。提供加密服务的路由器之间的设备可以提供负载均衡。

22.1.3 制定安全方案

RFC 1244中声明，安全设计的起始步骤之一就是制定***安全方案***。安全性方案是一个高层的文档，它包括了组织需要采取哪些措施才能达到安全性要求。方案中详细说明了制定安全策略以及策略的技术实现中所需要的时间、人力和其他资源。作为一个网络设计者，你可以帮助客户制定一个适当而且符合实际的方案。该方案应该基于客户的目标以及对网络资产和风险的评估。

安全方案应该参照网络的拓扑结构并包含所有将要提供的网络服务列表（比如FTP、web、E-mail等等）。这张列表必须详细说明谁提供了这些业务、谁能访问这些业务、如何提供接入以及谁来管理这些服务。

作为网络的设计者，你会帮助客户根据其业务目标和技术目标评估哪些服务是明确需要的。有时，可能仅仅由于新潮而增加了并不需要的新服务。增加服务可能需要在路由器和防火墙上进行新的分组过滤以保护这些服务，或者需要额外的用户身份验证过程以限制对这些服务的访问，两者都

会增加安全策略的复杂性。应该避免过度复杂的安全策略，因为它们有时会弄巧成拙。过于复杂的安全策略是很难正确实施的，而且很容易引人意想不到的安全漏洞。

安全方案中最重要的一个方面就是明确哪些人会参与安全策略的实施。因此弄清楚下列问题是很重要的：

- 是否需要雇用专门的安全管理员？
- 最终用户和他们的管理者如何参与安全策略的实施？
- 如何对最终用户、管理人员和技术人员进行安全策略和安全保障过程的培训？

为了使安全方案起作用，它必须得到组织内部各级雇员的支持。让公司管理层完全支持安全方案是尤为重要的。总部和远端的技术人员以及最终用户都应该接受这个安全方案。

22.1.4 定义安全策略

RFC 1244中声明，***安全策略***是关于访问组织的技术和信息资产的人员所必须遵守的规则的正式描述。安全策略通知用户、管理员和技术人员关于他们在保护技术资产和信息资产方面的职责。该策略必须明确完成这些职责的机制。与安全方案一样，雇员、管理人员和行政人员以及技术人员必须接受这个安全策略。

制定安全策略是安全管理员和网络管理员的工作。管理员从管理人员、用户、网络设计人员和工程师甚至法律顾问那里得到信息。作为一名网络设计者，你必须与安全管理员紧密合作，以理解这些策略是如何影响网络设计的。

在用户、技术人员和管理层的参与下制定出安全策略后，应该由高层管理人员把它向每个人进行解释。（许多企业要求员工签订声明，以表明他们已经阅读、理解并同意遵守某项安全策略。）

注意： 安全策略不是一成不变的。由于组织在不停地变化，必须对安全策略进行定期的更新以反映新的业务方向和技术变化。

22.1.5 安全策略的组成部分

通常，一项安全策略需要至少包含以下内容：

- **访问策略**（*access policy*）——规定了访问权利和特权。应该提供有关连接外部网络、连接设备到网络中以及给系统添加新软件的指导方针。
- **责任策略**（*accountability policy*）——定义了用户、操作人员和管理人员的责任。应该明确审核能力并为报告全问题提供指导方针。
- **身份验证策略**（*authentication policy*）——通过有效的密码策略建立信任机制并制定远程身份验证的指导方针。
- **计算机技术购买的指导方针**（*computer-technology purchasing guideline*）——明确指定关于购买、配置和审核计算机系统和网络的要求，以便与安全策略保持一致。

22.1.6 制定安全过程

安全过程用来实现安全策略。安全过程定义了配置、登录、审核以及维护的过程。对终端用户、网络管理员和安全管理员，都应写明安全过程。安全过程还应该指定如何处理事件（如检测到入侵应该做什么并与谁联系）。可以通过教员指导和自修培训课程让用户和管理员了解安全规程。

22.2 安全机制

本节描述了网络安全设计的一些典型的组成部分。当你为普通的安全性挑战设计解决方案时，

可以从中进行选择。

22.2.1 身份验证（Authentication）

身份验证（authentication）负责确认请求网络服务的人。术语“*身份验证*”通常指对用户进行验证，但它也可以指对一个软件过程的核实。比如，在某些支持路由验证（route authentication）的路由选择协议中，路由器必须达到某些标准后，它所发出的路由选择更新才能被另一台路由器所接受。

绝大多数安全策略都规定，为了访问网络及其服务，一个用户必须输入登录ID和密码，以提供安全服务器进行身份验证。为了尽可能地提高安全性，还可以使用一次性（动态）密码。在一次性密码系统中，用户的密码总是变化的，这通常由安全卡来完成。*安全卡*（security card）是一个信用卡大小的物理装置。用户向卡中输入了一个*个人识别号*（Personal Identification Number，PIN）。（PIN只是一个允许用户使用该卡的初级安全措施。）该卡提供了在一个限定时间内供访问公司网络的一次性密码。密码与在网络上的中心安全卡服务器同步。安全卡通常由远程办公人员和移动用户使用（在局域网访问中通常不使用安全卡）。

22.2.2 授权（Authorization）

身份验证控制着谁可以访问网络资源，*授权*（authorization）则规定了用户或进程在获得对资源的访问以后能够做什么。授权使安全管理员能控制网络的各个部分，比如服务器上的目录和文件。

对于不同的用户，授权是不同的，差异部分地取决于用户所在部门或其工作职责。比如，一项安全策略可能规定只有人力资源部门的雇员可以查看不归其管理的人员的工资记录。很难明确地列出每个用户在每项资源上所具有的经过授权的行为，因此需要通过技术手段来简化这个过程。比如，网络管理员可以为具有相同特权的用户创建用户组。

22.2.3 记帐（审核）（Accounting（Auditing））

为了有效地分析网络的安全性并对安全事件作出响应，应该建立相应的过程以收集网络活动的数据。收集数据称为*记帐*（accounting）或*审核*（auditing）。

对于有着严格安全策略的网络，审核数据应该包括任何人所做的试图通过身份验证和获得授权的尝试。记录以“匿名”(anonymous)或“guest”身份对公共服务器进行的访问是尤为重要的。审核数据还应包括对用户所作的改变访问权限尝试的记录。

所采集的数据都应该包括试图登录和注销的用户名和主机名和访问权限改变前后的权限。并且，审核日志中所有的数据都应该打上时间标记。

> **警告：**审核过程不应该收集密码。收集密码会引起潜在的安全问题，如果审核记录被不恰当地访问，安全性就会被破坏。（正确和不正确的密码都不应该收集，因为不正确的密码与有效密码的差别通常仅仅是一个字符或字符位置的交换。）

安全性评估（security assessment）是审核的进一步扩展。在安全性评估中，经过训练的专业人员对网络中容易受到网络入侵者攻击的薄弱部分进行内部检查。对网络的薄弱部分进行定期评估应该是网络安全策略和审核过程的一部分。审核的结果应该产生一个改正缺陷的具体计划，也许仅仅是对人员进行再培训。

22.2.4 数据加密（Data Encryption）

加密是将数据编码的过程，目的是为了防止预期接收方以外的人读取数据。加密设备在将数据放入网络之前先对其进行加密。解密设备在将数据传送到应用之前先对其进行解密。路由器、服务器、终端系统或者专用设备都可以作为加密和解密设备。

> 注意：经过加密的数据称为密码数据（ciphered data）（或者简单地称为经过加密的数据（encrypted data））。未经过加密的数据称为明文（plain text或clear text）。

加密是一项非常有用的安全特性，因为它提供了数据的保密性。它也可以用来确认数据发送者的身份。虽然身份验证和授权应该保护数据的保密性并且确认发送者的身份，但是加密仍是可以实施的有效安全特性，主要是为了预防其他安全特性失败的情况。

如果客户通过安全性分析发现，数据不保密或是对数据发送方的身份无法得到保证会带来安全风险严重的后果，那就应该使用数据加密。在内部网络以及用户仅仅使用因特网进行web浏览、E-mail和文件传输的网络中，数据加密通常是不必要的。对于使用虚拟专用网（VPN）技术，通过因特网连接私有地点的组织，推荐使用加密来保护组织数据的保密性。

加密由两部分组成：

- **加密算法**（*Encryption algorithm*）——一组将数据编码和解码的指令。
- **密钥**（*Encrytion key*）——供算法使用的对数据进行编码和解码的代码。

孩子们有时也用一种简单的算法来玩加密，比如“找到上一行的字母，然后用下一行的字母替换”。一个密钥可能看起来就像这样：

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
I N B Y G L S P T A R W Q H X M D K F U O C Z V E J

在本例中，LISA被加密为WTFI。这里的密钥只显示了大写字母，但是也可能包括小写字母和数字。

加密的目的在于，即使已经知道所用的加密算法，如果没有恰当的密钥，入侵者也不能对信息进行解释。这种类型的密钥称为安全密钥（secret key）。当发送方和接收方使用相同的安全密钥时，这称为***对称密钥***（Symmetric Key）数据加密标准（DES）是众所周知的对称加密系统示例，在绝大多数的路由器和服务器中都实施对称加密。

尽管安全密钥在两台设备之间是容易实施的，但是随着设备数量的增加，安全密钥的数量也要相应地增加，这样就难以管理了。比如说，工作站A和工作站B间的会话使用的密钥与工作站A与工作站C间的会话使用的密钥是不同的等等。使用非对称的密钥可以解决这个问题。

公钥/私钥加密（Public/private key Encryption）

公钥/私钥加密是众所周知的非对称密钥系统的例子。在公钥/私钥系统中，网络上的每个安全工作站都会有一个公开的或者容易确定的公钥，所有设备都可以使用一台工作站的公钥来对数据加密，并把数据发送给工作站。

接收工作站使用它自己的私钥对数据进行解密。由于没有其他的设备拥有该工作站的私钥，所有没有其他设备能够对数据进行解密，因此就保持了数据的保密性。（数学家和计算机学家已经写出计算机程序，用来确定用作密钥的特殊数字，这样发送者和接收者就可以使用相同的算法，即使他们使用了不同的密钥。）图22-1显示了用于数据保密性的公钥/私钥系统。



图22-1 确保数据保密性的公钥/私钥系统

公钥/私钥系统同时提供了保密性和身份验证两项特性。通过使用非对称密钥，接受者可以确认文件是否真正来自它所标识的用户或主机。比如说，您现在正在向美国国务局（IRS）发送自己的所得税申报表。IRS需要确认这份所得税申报表是来自您而不是一个想让您缴纳更多税款的恶意第3方。

使用私有密钥可以对自己的文档或文档的一部分进行加密，这就形成了*数字签名*（Digital signature）。IRS通过使用你的公钥对文件进行解密，如图22-2所示。如果解密成功，那么文件必然来自你，因为没有其他人知道你的私钥。



图22-2　用于发送数字签名的公钥/私钥系统

非对称密钥的数字签名特性可以与数据保密性特性一起使用。当你用私钥对文档进行加密后，你还可以使用IRS的公钥对数据进行加密。IRS对文件进行两次解密。如果经过解密得到了明文数据，那么IRS便知道该文档来自你，并且你只想把该文档发送到IRS。

非对称密钥系统的一些其他例子包括Rivest、Shamier和Adleman(RSA)标准、Diffie-Hellman公钥算法和数字签名标准（DSS）。Cisco Systems使用DSS标准对建立加密会话的路由器对等体进行身份验证。路由器对等体使用Differ-Hellman算法来发送关于加密数据用的安全密钥信息。真正的数据是通过DES算法和密钥进行加密的。

22.2.5　分组过滤器（Packet Filter）

可以在路由器和交换机上建立*分组过滤器*（packet filter），以接受或拒绝来自特定地址或服务的分组。分组过滤器扩充了身份验证和授权机制。它们能保护网络资源免受非授权的使用、盗用、破坏和拒绝服务（DoS）攻击。

安全策略应该规定分组过滤器是否实施了下列两种策略的一种：

- 拒绝特定类型的分组而接受所有其他的。
- 接受特定类型的分组而拒绝所有其他的。

第一种策略需要对特定的安全威胁有透彻的理解，因此比较难实施。第二种策略容易实施而且更加安全，因为安全管理员不必通过预测未来的攻击以决定需要拒绝哪些分组。第二种策略也更容易测试，因为网络所接受的使用是有限的。为了很好实施第二种策略，你必须对网络的需求有透彻的理解。网络设计者应该和安全管理员一起决定应该接受哪种类型的分组。

Cisco在对其分组过滤器中实施了第二种策略。Cisco称之为*访问控制列表*（access control lists，ACL）。在运行Cisco互连网络操作系统（IOS）软件的路由器或交换机上，每个ACL在最后都有一条隐含的deny-any语句。所指定的Permit和deny语句在该隐含deny-any语句之前处理。（该语句是隐含的，因为管理员不需要实际输入它；然而，为了使列表的行为更加明显，最好输入该语句。）

ACL允许控制通信流量在路由器或交换机接口上是转发还是阻塞。ACL定义了应用于进入或离开接口分组的准则。典型的标准包括分组的源地址、目的地址和分组内的上层协议。

由于Cisco IOS软件会根据列表中的每一条语句的标准对分组进行检测，直到发现一个匹配的为止，所以应该谨慎地设计ACL，以提供良好的性能。通过研究流量的传送，你可以设计出使绝大多数分组与靠前的条件相匹配的列表。对每个分组需要检查的条件越少，则意味着吞吐量越大。关于

ACL的一条很好的建议：列表的顺序是在顶部设置最通用的语句而在下面设置最具体的语句，最后一个语句为通用的、隐含的deny-any语句。

22.2.6 防火墙（Firewalls）

防火墙（firewall）是在两个或多个网络的边界处用于加强安全策略的一个系统或若干个系统的组合。防火墙可以是一台配有ACL的路由器、一个专用的硬件盒或者是运行在PC或UNIX系统上的软件。在企业网和因特网的边界处设立防火墙尤为重要。

22.2.7 入侵检测（Intrusion Dctection）

*入侵检测*是指对网络活动的实时监测和对数据的分析，以发现潜在的薄弱环节和正在进行的攻击。在网络内部，授权用户在网络上进行的非授权活动——比如，试图通过因特网传送机密文件或非法修改网络的访问特权——都可以被实时地监测到并立即被阻止。对于企图闯入网络的外部入侵者也可以用同样的方式处理。

实时能力（与定期查看日志文件相对）能够通过消除网络入侵者来显著地减少潜在的损害和恢复的代价。一个良好的入侵检测系统有如下特性：

- 必须能在无人监管的情况下连续运行。系统必须十分可靠，以便它能够在被监测的系统后台运行。
- 必须具有容错能力，也就是必须能经受系统崩溃，并且在重启时不用重建它的知识库。
- 必须能够防止被破坏。系统能够对自身进行监测以确保它未受破坏。
- 所带来的系统开销必须小。一个会使得计算机慢到爬行的系统是没有人会使用的。
- 必须能够监测到偏离正常行为的活动，并且当非正常行为发生时能立即警告。
- 当系统随着时间的推移增加新应用时，必须能够对不断变化的系统状态应付自如。

为专门的目的制定客户化检测规则的能力可能也是你感兴趣的。你也许希望制定客户化的检测规则，以防止那些标有“保密”的文档以E-mail的方式传到网络外部，或者解决客户系统或遗留系统中的脆弱环节。这样的定制化使得系统通过修改能在几乎任何环境中应用，尽管这些应用还不普遍，也还没有成为商业产品的标准特性。

22.2 8 物理安全性（Physical Security）

RFC 1244中声明，***物理安全性***（physical security）是指通过将资源置于上锁的房间内来限制对关键网络资源的访问。物理安全性还指保护资源免受自然灾害的侵害，比如洪水、火灾、风暴和地震。由于物理安全性的需求是显而易见的，以至于很容易忘记对其进行计划，但是绝不要忽视它或者认为它的重要性比其他的目标更低。

根据你网络设计的特定客户，物理安全措施应该设置用于保护核心路由器、分界点、线缆、调制解调器、服务器、主机、备份存储等设备。在网络设计工程的早期与你的客户共同工作，以确保设备都放置在有卡钥匙或安全警卫的计算间中。计算间应该配有不间断电源、火警、灭火装置和除水系统。为了保护设备不受地震和暴雨天的强风影响，设备应该安装到固定到底板或墙的机架上。

22.3 选择安全解决方案

前一节描述了网络安全设计的一些典型要素。本节提供了一些方法，能把这些要素组合到一起，以满足以下的安全性挑战：

- 保护因特网连接。

- 保护拨号访问。
- 保护网络服务。
- 保护用户服务。

22.3.1 保护因特网连接

应该用一组交叠的安全机制，包括防火墙、分组过滤器、物理安全措施、审核日志、身份验证和授权，来保护因特网连接。公共服务器，比如WWW服务器以及文件传输协议（FTP）服务器，可以允许未经身份验证的访问，但是所有其他的服务器都应该要求身份验证和授权。公共服务器应该置于一个自由贸易区（free-trade-zone）网络上，该网络通过防火墙和其他网络隔离。

如果客户能购买两台分离的服务器，安全专家建议不要把FTP服务与Web服务放在同一台服务器上运行。FTP用户比Web用户有更多的机会读文件，并且可能修改文件。一名黑客可能使用FTP来破坏一个公司的网站，从而破坏该公司的形象，并可能损坏基于Web的电子商务应用和其他应用。安全专家建议你绝对不要提供对TFTP服务器的因特网访问，因为TFTP不支持身份验证特性。专家还建议禁用那些不使用或非必需的端口和服务。

向web服务器中添加通用网关接口（CGI）脚本或其他类型的脚本时一定要十分谨慎。应该对脚本的安全漏洞进行彻底的测试。只有当电子商务应用与安全套接字层（SSL）标准兼容时，才能在Web服务器上安装电子商务应用程序。

长久以来，E-mail服务器一直是入侵者侵入的一项资源，这可能是由于E-mail协议及其实施已经流传了相当一段时间，因而黑客很容易理解它们。此外，就本质而言，E-mail服务器必须允许外部的访问。为了保护E-mail服务器，网络安全管理员应该订阅专门关于安全信息的邮件列表，不断地安装安全补丁也是很重要的。如果Microsoft SQL Server安装了关于该服务器的安全补丁，就可以避免SQL Slammer蠕虫造成的因特网中断，这个补丁在病毒爆发前6个月就已经可用了。

22.3.2 保护因特网域名系统服务

对域名服务系统（DNS）服务器应该进行仔细的控制和监测。名称到地址的解析对于任何网络的运行都是至关重要的。入侵者如果控制了域名服务器，或者假扮成域名服务器，就能在网络上实施大规模的破坏活动。应该通过路由器上的分组过滤器以及DNS软件自带的安全特性来保护DNS服务器免受安全攻击。

传统上，DNS不具备安全能力。尤其是没有方法就DNS对某个请求的响应进行验证。黑客可以截获查询，并返回一个假冒的名称到地址映射。通过在协议中加入数字签名和其他的一些安全特性可以解决这个问题和其他的安全隐患。

22.3.3 逻辑网络设计和因特网连接

企业网络的一个好的规则就是应该定义恰当的退出点和进入点。与有多条因特网连接的组织相比，只有单条因特网连接的组织更容易管理因特网安全性问题。然而，一些大型的组织由于性能和冗余性的原因需要不止一条的因特网连接。只要这些连接是可以管理和监测的，就没有问题。但是不能容忍某些部门或用户未与公司的网络工程师协商就私自增加因特网连接。

为因特网连接挑选路由选择协议时，为了提供最高的安全性，你应该选择提供路由身份验证的协议（比如RIP版本2、OSPF或BGP4）。静态和缺省路由选择也是不错的选择方案，因为使用静态和缺省路由选择就不会有路由选择更新信息受到损害。接入因特网的路由器应该装备有分组过滤器，以防止DoS攻击。

在保护Internet连接时，可以使用网络地址转换（NAT）来保护内部网络的寻址方案。NAT对外部网络隐藏了内部网络号。当需要进行外部访问时，NAT就对内部网络号进行转换。

通过因特网，使用VPN服务连接多个私有地点的组织应该使用NAT、防火墙和数据加密。在VPN拓扑结构中，私有数据在公共Internet上传送，因此加密是必须的。第2层隧道协议（L2TP）是因特网工程任务组（IETF）针对在公共网络上用隧道传送私有数据而制定的标准。

22.3.4 IP安全协议

IP安全协议（IPSec）是一组提供数据保密性、数据完整性和对IP层的参与对等体进行身份验证的开放标准。随着IPSec获得行业的认可，客户也要求所购买的连网产品中包含对它的支持。(在RFC 1825和1829中对IPSec进行了描述)。

IPSec允许系统选择安全性协议和算法并创建加密密钥。Internet密钥交换协议提供IPSec对等体身份认证和协商IPSec密钥以及安全性关联。IKE使用以下的技术：

- DES——对分组数据进行加密；
- Diffie-Hellman——建立一个共享的、保密的会话密钥。
- **消息摘要算法5**（*Message Digest 5，MD5*）——一种产生128bits 散列值，对分组内数据进行身份验证的单向散列算法。在IPSec框架中，Cisco使用散列值进行身份验证。同样的方法也用在SNMPv2的消息身份验证中。MD5用于验证通信的完整性、对数据源进行身份验证并核查及时性。
- **安全散列算法**（*SHA，Secure Hash Algorithm*）——通过截取少于264bits的消息并生成一个160bits的消息摘要来完成对分组数据的身份验证。该算法采用了更大的消息摘要，提供了针对强行攻击冲突和逆向攻击（inversion attacks）的安全性。
- **RSA 加密惟一值**（*RSA encrypted nonces*）——提供否认（repudiation）功能。
- **RSA签名**——提供不可否认（nonrepudiation）功能。

注意：否认(Repudiation)是一项安全特性，能防止第3方证明另两方之间发生了通信。如果你不希望自己的通信是可跟踪的，这是一项理想的特性。不可否认（Nonrepudiation）正好相反：第3方可以证明另两方之间发生了通信。如果你想跟踪自己的通信并证明其的确发生了，这是一项理想的特性。

22.3.5 保护拨号访问

安全性对于拨号访问是至关重要的。这应该包括防火墙技术、物理安全措施、身份验证和授权机制、记帐功能，还可能包括加密技术。身份验证和授权对于拨号访问安全性而言是最为重要的功能。对于拨号访问，用安全卡提供一次性密码也是很有意义的。

使用点到点协议（PPP）的远程用户和远程路由器应该使用挑战握手验证协议（Challenge Handshake Authentication Protocol，CHAP）进行身份验证。密码验证协议（Password Authentication Protocol，PAP）与CHAP相比安全性要低，因此不推荐使用。

实现身份验证、授权和记帐等功能的另一种选择是***远程身份验证拨入用户服务器(RADIUS)协议***。Livingston公司几年前开发出了RADIUS，它已经作为一项行业标准并记录在RFC 2138和RFC2138中。RADIUS使得管理员可以拥有一个包含用户信息的中心数据库。该数据库包含了身份验证和配置信息，并且指定了允许用户使用的服务类型（例如PPP、Telnet和rlogin等等）。RADIUS是一种客户机/服务器协议。接入服务器作为RADIUS服务器的一台客户机。

对于拨号服务应该进行严格的控制。不应该允许用户把调制解调器和模拟线连接到自己的工作

站或服务器上。（某些公司实际上会解雇这样做的员工。）只设单一的拨入点（比如，一个大型的调制解调器池或者接入服务器）是很有益处的，这样能对所有的用户都以相同的方式进行身份验证。拨出服务应该使用另一组调制解调器。所有的拨入和拨出服务都应该进行身份验证。

如果调制解调器和接入服务器都支持*回拨*（callback）（大多数是支持的），那么就应该使用回拨。使用回拨时，在一个用户拨号进入并且通过了身份验证后，系统将断开该呼叫并且回拨一个特定的号码。回拨是很有用的，因为系统回拨了实际的用户，而不会回拨一个冒充该用户的黑客。然而，回拨机制很容易受到破坏，因此不应该作为惟一的安全机制。

拨号网络运行中的很多安全性考虑，已经超出了一本介绍网络设计的书的范畴。能够说的是，需要对调制解调器和接入服务器进行仔细配置，并防止黑客对它们进行重新配置。应该对调制解调器进行编程，使它能够在每一个呼叫开始和结束时都重新恢复标准配置，调制解调器和接入服务器应该能够完全终止呼叫。当用户意外地挂断时，服务器应该能够强行注销。

22.3.6 保护网络服务

许多关于保护因特网连接的建议同样适用于保护内部企业网。内部网络服务也可以利用身份验证、授权、分组过滤、审核日志、物理安全措施和加密等手段。

要保护内部网络服务，保护网络互连设备是很重要的，比如路由器和交换机。无论用户是通过控制台端口还是通过网络来访问这些设备，都应该要求输入登录ID和密码。那些仅仅需要检查设备状态的管理员可以使用一级密码。那些允许查看或更改配置的管理员应该使用二级密码。

如果允许通过调制解调器访问互连网络设备的控制台端口，必须对端口上的调制解调器采取同标准拨入用户调制解调器一样的安全措施，并且所使用的电话号码不应该列在组织的主要电话号码中，也不应与组织的主要电话号码相关。当发生人员变动时，也应该改变电话号码。

对于拥有许多路由器和交换机的客户而言，像*终端访问控制器访问控制系统*（TACACS）这样的协议，可以用来在一个中央数据库中管理大量的路由器和交换机的用户ID和密码。最新版本的TACACS包括XTACACS和TACACS+。同时TACACS还提供审核特性。

在安全目标比管理目标更为重要时，就应该考虑在企业网络中限制使用简单网络管理协议（SNMP）了。SNMP的一个主要问题是它有一个允许远程工作站改变管理和配置数据的set操作。SNMP版本3(SNMPv3)支持对使用set操作和其他SNMP操作的人进行身份验证。

与Internet连接一样，内部网络应该运行最安全的DNS、FTP和Web软件版本。此外，在实施网络信息服务（NIS）和其他类型的命名和寻址服务器时，也应该根据其所提供的安全级别进行仔细的选择。

尽管网络中的服务（比如文件服务器）需要身份验证和授权是显而易见的，但容易忽视的是，网络本身也需要这些安全机制。在用户登录进入服务器之前，用户应该首先需要登录到网络上。

22.3.7 保护用户服务

用户服务包括了终端系统、应用程序、主机、文件服务器、数据库服务器和其他服务。文件服务器和其他的服务器应该提供身份验证和授权特性。如果用户关心他人对自己系统的使用情况，终端系统也能够提供这些特性。应该鼓励用户在离开办公桌较长时间时注销会话，并在下班时关闭计算机，以防止非授权的人员进入系统并访问服务和应用程序。可以部署自动注销机制来实现长时间没有活动时自动注销会话的功能。保护工作站的另一种方式是使用带有密码保护的屏幕保护程序。某些屏幕保护程序允许用户输入口令来取消屏幕保护并返回到桌面。

安全策略和过程应该规定密码的使用准则：何时应该使用密码、密码如何构成以及如何改变密码。一般来说，密码应该包括字母和数字，并且至少有6个字符，不应该是一个“普通”词，而且应该经常变化。

在服务器上，root密码（或者非UNIX系统上类似的密码）应该只有几个人知道。如果可能，应该避免使用guest账号。对于支持“受信任其他主机”概念的协议，应该小心使用。（例如，UNIX系统上的rlogin和rsh。）如果可能的话，那些允许guest账号和支持受信任主机（trusted hosts）的主机应该与其他的主机相分离。

*Kerberos*是一个身份验证系统。它可以为应用层协议，比如FTP和Telnet，提供用户到主机的安全性。如果一个应用程序要求，Kerberos还可以提供加密功能。Kerberos依赖于在Kerberos服务器上使用密钥发布中心（KDC）的对称密钥数据库。要了解关于Kerberos的最新信息，可参见Kerberos常见问题解答（FAQ）文档（通过www.ov.com/misc/krb-faq.html可以获得）。

安全策略应该规定允许哪些应用程序在连网的PC上运行，并且应该提出关于限制从互连网或者其他的站点下载未知应用程序的指导方针。安全过程也应该规定用户如何安装和更新防病毒软件。防病毒是用户服务安全性中最为重要的方面之一。

根据网络的拓扑结构，用户服务的安全性还可能结合加密。有时加密在服务器和终端系统上进行，而不是在网络内部进行。包括Microsoft、Netscape和Sun Microsystem在内的厂商都为终端系统、工作站和服务器提供加密软件。

为了保证用户服务级的安全性，应该明确应用程序和网络操作系统中已知的安全性漏洞并对其进行修复。网络管理员必须了解最新的黑客进攻手段和病毒信息。

22.4 总结

作为一名网络设计者，你的目标是帮助客户制定实施安全性的策略和过程。你还应该帮助客户选择实施这些策略和过程的工具和产品。由于因特网连接和因特网应用程序的增加，并且更多的用户从远程站点访问企业网络，安全性是绝大多数客户所关心的问题。

本章所提供的内容有助你选择恰当的工具和过程以满足客户关于网络安全性的目标。安全设计与网络总体设计所包含的任务是并行的：分析需求和目标、作出折衷、给出网络流量传送的特征并制定出一种合适的拓扑结构。

网络设计中经常忽略安全性，因为通常将其视为一个运行中的问题而不是设计问题。但是，预先考虑安全性问题，而不是在设计过程结束时或网络运行时再考虑，将会使你的设计更具备可扩展也更加健壮。

22.5 关键术语

记账（审核）（*accounting*（*auditing*）） 在用户访问网络资源时记录用户活动的过程。所记录的信息包括用户在网络上停留的时间、所访问的服务以及会话过程中传送的数据量。

访问控制列表（*Access Control List*，*ACL*） 用于通知计算机操作系统，各个用户或组对特定系统对象（比如一个目录或文件）的访问权限的一组数据。

身份验证（*authentication*） 识别某个人的过程，通常根据用户名和密码。

授权（*authorization*） 同意或拒绝对某项网络资源访问的过程。

回拨（*callback*） 回拨是进行身份验证的一种方法，当用户拨入并通过了身份验证时，由系统断开呼叫并回拨某个号码。

密码数据（*ciphered data*） 经过加密的数据。

解密设备（*decryption device*） 负责在将数据传递给应用之前使之可读的设备。路由器、服务器、终端系统或专用设备都可以作为加密和解密设备。

数字签名（*digital signature*） 一个对类似文档或电子邮件这样的软件用你的私钥进行加密的系统。

加密（*encryption*） 是将数据编码的过程，防止其被预期接收方以外的任何人读取。

加密设备（*encryption device*） 将数据放到网络以前使之不可读的设备。

防火墙（*firewall*） 在两个或多个网络的边界处用于加强安全策略的一个系统或若干个系统的组合。

入侵检测（*intrusion detection*） 对网络活动的实时监测和对数据的分析，以发现潜在的薄弱环节和正在进行的攻击。

IP 协议安全（*IPSec*） 一组提供数据保密性、数据完整性和对IP层的参与对等体进行身份验证的开放标准。

Kerberos 一个身份验证系统。它可以为应用层协议，比如FTP和Telnet，提供用户到主机的安全性。

网络资产（*network assets*） 包括网络主机（包括主机的操作系统、应用程序和数据）、网络互连设备（比如路由器和交换机）以及穿越网络的数据。网络资产还包括一些不明显但仍然很重要的部分，比如知识产权、商业机密和一个公司的声誉。

不可否认（*nonrepudiation*） 第3方可以证明另两方之间发生了通信的系统。如果你想跟踪自己的通信并证明其确发生了，这是很理想的。

分组过滤器（*packet filters*） 可以在路由器或服务器上建立过滤器，以允许或拒绝来自特定地址或服务的分组。分组过滤器扩充了身份验证和授权机制。

物理安全性（*physical security*） 通过将资源置于上锁的房间内来限制对关键网络资源的访问。物理安全性还指保护资源免受自然灾害的侵害，比如洪水、火灾、风暴和地震。

个人识别号（*Personal Identification Number*，*PIN*） 许可用户使用安全卡的初级安全策略。该卡提供了在一个限定时间内访问公司网络的一次性密码。

明文（*plain text*（*clear text*）） 未加密的数据。

远程身份验证拨入用户服务器（*RADIUS*，*Remote Authentication Dial-In User Server*）协议 一种身份验证协议，允许管理员建立中心用户信息数据库。数据库包含身份验证和配置信息，并规定了允许用

户使用的服务类型（比如PPP、Telnet、rlogin等等）。

否认（*repudiation*） 一项安全特性，能防止第3方证明另两方之间发生了通信。如果你不希望自己的通信是可跟踪的，这是一项理想的特性。

路由身份验证（*route authentication*） 一种身份验证类型，路由器必须通过某种标准，其发送的路由选择更新才能被其他的路由器所接受。

安全密钥（*secret key*） 通过使用加密算法保护加密数据，使得入侵者没有适当的密钥便不能读取消息的一种机制。

安全性评估（*security assessment*） 由受过训练的专业人员对网络中容易受到入侵者攻击的薄弱环节进行内部检查的过程。

安全卡（*security card*） 信用卡大小的物理装置，能用于限制对房间或者计算机的访问。

安全方案（*security plan*） 一个高层的文档，提出了某个组织要满足安全性要求所必须完成的工作。

安全策略（*security policy*） 一种策略，规定了分组过滤器是否拒绝特定类型的分组，并接受所有其他的分组，或者接受特定类型的分组，拒绝其他所有分组。

对称密钥（*symmetric key*） 一种公钥/私钥方法，发送方和接受方使用相同的安全密钥。

终端访问控制器访问控制系统（*Terminal Access Controller Access Control System，TACACS*） 一种安全协议，针对拥有众多路由器和交换机的客户，可以用来在一个中央数据库中管理大量的路由器和交换机的用户ID和密码。TACACS也提供审核特性。



第23章 虚拟专用网

目标

学习完本章后，你将能够：

- 描述VPN的工作原理。
- 描述VPN的实施。
- 描述Cisco公司的VPN。
- 描述隧道（tunneling）技术。
- 描述Cisco的第2层隧道协议（L2TP）的实施。
- 描述端到端的虚拟拨号过程。
- 描述虚拟拨号服务的要点。

网络发展的动力是促使应用之间和个人之间的通信能更快捷、更廉价并且更稳定。在大多数情况下，保证通信的安全性并不是网络发展的驱动力。作为实现“使用公共网络实现专用通信”这一全新的、与众不同的目标的基本机制，虚拟专用网为保证通信的安全性提供了一个明确的案例。

23.1 VPN的运行方式

虚拟专用网（VPN）是一种通信环境，其中的访问受到控制以允许只在预先定义好的共同利益社区内进行对等连接。VPN是通过对普通下层通信介质进行某种形式的划分来组建的。这些通信介质基于非独占的方式为网络提供服务。关于VPN的一个更简单、更准确但不太正式的定义是：

VPN是一个在公共网络基础设施（比如全球因特网）上构建的专用网技术。

构建VPN可能是为了满足许多特定的商业和技术需求。一个全面的VPN解决方案可以提供：

- 支持拨入和其他远程访问。
- 支持通过租用线路（或其他的专用方式）连接多个远程站点。
- VPN服务提供商能为VPN客户提供各种服务（比如web主机）。
- 所支持的连接也不局限于VPN内，还支持VPN之间的连接，包括与全球因特网的连接。

23.1.1 VPN的优点

与先前形式的信道加密技术和其他候选技术相比，VPN有很多明显的优点，一些优点包括：

• 仅依靠VPN技术就能为多个TCP/IP应用提供保密性。应用级的加密需要对不同的服务采取不同的方法。通过使用点到点隧道协议（PPTP）、L2TP或第2层转发（L2F）协议实现的IP隧道，也能实现多种协议的支持。在你希望为伙伴或远程办公人员提供安全访问时，为多种TCP/IP应用提供保密性是相当重要的。

• 可以为信任的客户端与VPN服务器之间的所有TCP/IP通信提供加密服务，这样做的优点在于对于终端用户是透明的。只要加密处于开启状态，服务器就可以强迫执行加密。

23.1.2　VPN的类型

VPN被定义为部署在共享基础设施上，使用与专用网络相同策略的客户连接（见图23-1）。共享基础设施可以利用服务提供上的IP、帧中继、ATM等骨干网络，或Internet。根据企业和组织使用VPN的情况，有三种VPN与之相适应：



图23-1　VPN的逻辑拓扑视图

• *接入VPN*（*Access VPN*）——通过一个与专用网络有着相同策略的共享基础设施提供对公司内部网或外部网的远程接入。访问VPN使得用户能够在任何时间、任何地点、以任意方式访问公司资源。访问VPN包括了模拟、拨号、综合业务数字网（ISDN）、数字用户线（DSL）、移动IP和线缆技术，能够安全地联接移动用户、远程办公用户或分支机构。

• *内部网VPN*（*Intranet VPN*）——通过使用专用连接上的共享基础设施，把公司总部、远程办公室和分支机构连接起来。企业能享有与专用网一样的策略，包括安全性、服务质量（QoS）、可管理性和可靠性。

• *外部网VPN*（*Extranet VPN*）——通过使用专用连接上的共享基础设施将客户、供应商、合作伙伴或有一定共同利益的团体连接到公司的内部VPN上。企业能享有与专用网一样的策略，包括安全性、服务质量（QoS）、可管理性和可靠性。

23.1.3　服务水平协议

部署VPN时，很有必要简要地看看*服务水平协议*（Service-Level Agreements，SLA）的重要性。SLA是VPN提供商与用户协商的合同。它包含了用户的期望特定服务达到的标准。要确保VPN服务提供商按照约定的服务质量和服务水平提供服务，SLA是用户所能支配的惟一的约束性工具。最符合用户利益的做法是对VLA所规定标准的执行情况进行监测。然而，SLA对服务提供商和用户都提出了一些技术上的挑战。

对用户而言，SLA的挑战在于设计和运行一个服务评估工具，该工具可以提供关于服务提供商对SLA履行程度的合理指标。注意，用户可能用同一个SLA来约束一个或多个服务提供商所提供的合约约定服务的水平，但是如果这个用户的VPN跨越了多个服务提供商的区域，SLA必须包括有关服务提供商之间互连互通和端到端服务性能的规定。

对于服务提供商而言，SLA所提出的挑战在于需要制定来自许多不同服务提供商的SLA。对一个因特网公共数据网提供商而言，由于主机资源分配机制自身的不可预见性，通常的尽力的服务（best-effort）级质量保证是不能满足SLA要求的。在这种环境中，服务提供商要么保证在网络建设

时就已经在用户接入容量和内部交换容量的比率方面留下了充分的余地；要么可以部署服务区分结构，以确保为每个SLA用户分配了最低限度的资源级别。需要注意的是，第一种方法趋向于减少流量聚集所带来的优点，会对成本造成影响；第二种方法会增加网络运行管理的复杂性，也会影响网络的可扩展性。

23.1.4 VPN示例

在图23-2所描述的例子中，网络A的各站点已经在服务提供商的骨干网上建立了VPN（虚线表示），而网络B则完全不知道VPN的存在。网络A和网络B和谐地共同存在于相同的骨干网基础设施上。

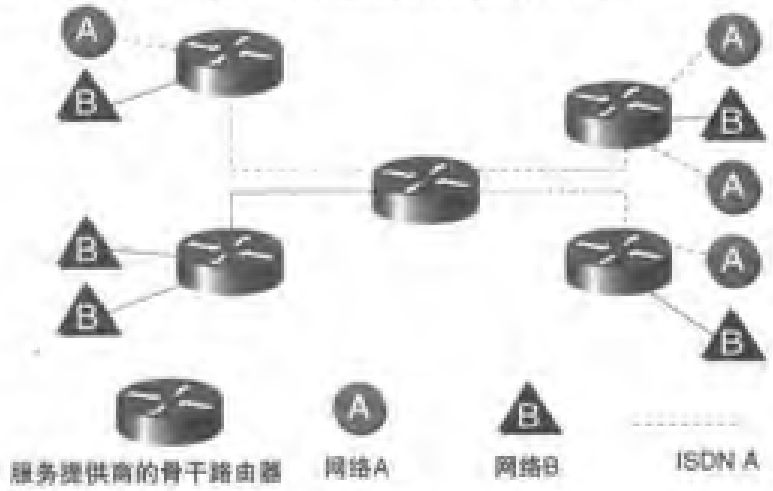


图23-2 连接网络A各站点的VPN

注意：在一个共同的基础设施上同时部署研究性和生产性服务时，也考虑到了网络中虚拟化的概念。教育和研究领域所面临的挑战是如何同时满足网络的研究性需求和生产性需求。

23.1.5 网络A各站点间的VPN

最常见的VPN包含多个子网，它们处于不同地理位置，但归属于同一个管理域，相互之间通过其管理控制范围之外的共享基础设施相互连接（比如全球因特网或单个服务提供商的骨干网）。建立这种VPN的根本动机在于：在VPN社区内，设备之间的通信内容可能是机密的。（再次强调，所需要的保密水平的确定完全依赖于VPN管理员所做的风险分析。）然而，通信系统总的价值又决定了投资于采用独立传输部件的完全专用通信系统是不合理的。

要注意的相关内容是，一个VPN的保密级别很大程度上取决于构建VPN所使用的技术。比如，如果VPN子网之间（或VPN主机之间）的通信在通过公共通信基础设施时进行了安全加密，那么VPN的保密性就相对比较高了。

事实上，VPN实施的粒度可以分解到单个的端到端或一对一的连接。这种类型的一对一VPN例子包括：与安全应用（比如在线银行服务）建立VPN连接的单个拨号用户，或者在桌面电脑和应用服务器（比如在因特网上进行的购买交易）之间建立安全的加密会话的单个用户。随着安全电子商务应用的成熟和其在因特网上进一步的部署，这种一对一的VPN会变得更加流行。

VPN还被当作一种分隔网络流量的方法，这样，研究性流量和生产性流量就好比在黑夜里行驶的轮船，它们彼此之间都不能发现对方的存在。VPN之间如此互不在意，以至于某个共同利益社区内发生的主要事件，比如较大的故障或不稳定事件，对另外一个共同利益社区是完全透明的。

VPN可以跨越超过一个的主机通信网络构建。因此，VPN的状态可能需要一个或多个VPN提供

商网络的支持。当所有的服务提供商都明确地支持由此产生的分布式VPN环境时，这种应用方式的健壮性可以达到最高。然而，偶尔也会采用不需要涉及“覆盖式VPN（overlay VPN）”知识的解决方案，这样会产生混合的结果。

23.2 VPN的实施

当你决定要实施VPN后，就必须采取措施以保证基础设施足够安全，并且保证在实施之前明确地定义了所支持的应用及其目标。

23.2.1 安全审核

运行安全审核能确保防火墙、远程访问应用或身份验证手段中所存在的薄弱环节，在VPN实施以后不会暴露给更多的人。出于这些安全性的考虑，至少需要在网络的边界处进行全面的安全审核，因为这里可能受到来自内部或外部的攻击。这种评价方法应该审查所有进入内部网的人站连接，包括远程接入服务器、基于路由器的辅助连接和外部网连接。就外部网VPN而言，审查的范围还应该包括企业的合作伙伴组织的边界。

23.2.2 范围和应用的需求

完成审核后，你必须通过确定那些会访问VPN和应用的终端用户群（比如合作伙伴、订约人或远程办公用户）来规定VPN的范围。这个步骤还包括对委托人将会使用的应用进行评估，以及这些应用所传送数据机密性的评估。有了对应用的这些评估，就能选择恰当的安全服务和足够安全的加密技术。

接下来，必须定义并测试VPN所支持的所有应用在延迟和QoS方面的需求。即使被认为是存储转发方式的应用，在某些配置中也会有延迟敏感性。这些敏感性影响到该应用是否适合VPN，并且帮助确定了下层网络的性质。

23.2.3 文档编制

对于外部网VPN，企业应该为外部VPN用户草拟一个理解声明。对于远程访问VPN，企业应该更新它的远程访问策略，以确保其中包括了这种新形式的访问技术。

23.2.4 安全策略

以外部VPN为例，虚拟专用网策略规定了身份验证和授权。

授权应该基于参与企业所定义的通用角色（这些角色应该与参与企业中的个人映射）。通用角色应该有一些基本特权，包括针对供应商货物存量的网络访问和web服务器访问。这些角色还应该映射到一组已定义的数据上，并通过VPN加以执行。在所涉及的用户理解声明中，应该包括外部网的策略。

虚拟专用网的远程访问策略不应该与已经建立的远程接入策略有太大的区别。与传统的远程访问策略的主要区别应该是针对合适的因特网访问的“可接受使用”。与任何基于因特网的访问应该有两个因素一样，除了应该有一个适当的基于令牌的身份验证外，这个策略还应包括一个关于这些令牌如何能最安全使用的声明。

23.3 Cisco的VPN设计

包括Cisco端到端硬件和Cisco IOS软件在内的网络产品为在公共基础设施上进行机密的专

用传输提供了复杂的安全措施，通过对流量区分保证了QoS，为关键任务的应用提供了可靠性，为支持宽带数据提供了扩展性，并提供全面的网络管理功能，这一切便构成了完备的访问VPN解决方案。

下一节讨论如何使用Cisco的网络接入服务器（NAS）和路由器，并配合Cisco IOS软件为虚拟拨号服务提供新功能。该功能是基于L2F协议的，该协议已经被因特网工程任务组起草为RFC(RFC2431)。L2F为传输高层协议的数据链路层帧提供了一种基于标准的隧道机制。这些数据链路层协议包括高级数据链路控制协议（HDLC）、异步的点到点协议（async PPP）、串行线路因特网协议（SLIP）或PPP ISDN。现在，L2F已经与PPTP合并，而且已经基本上被L2TP所取代。L2TP是PPP协议的扩展，使得ISP可以运行VPN。L2TP融合了其他两种隧道技术的优点：来自Microsoft的PPTP和来自Cisco Systems的L2F。与PPTP一样，L2TP也要求ISP的路由器支持该协议。通过使用这些隧道技术，可以使得最初的拨号服务器的位置、拨号协议连接终结的位置以及接入网络的位置（通常是公司的网关）相互分离。

> **注意：** 目前，没有关于VPN的软件和硬件组件的标准。每个VPN服务提供商都使用最适合自己的硬件平台和软件应用程序来实现VPN。

23.3.1 隧道概述

虚拟拨号服务的一个关键组件便是**隧道**（tunneling）。一种能将分组封装在某种协议中，并在给定网络的出入点对协议进行解释的传递手段。这些入口点和出口点被定义为隧道接口（tunnel interface）。隧道接口与硬件接口类似，但它是在软件中进行配置的。

下面一节提供了关于网络互连和Cisco关于L2TP实施的额外详细信息。使用L2TP隧道，Internet服务提供商（ISP）或者其他的接入服务商能创建一条虚拟隧道，以实现客户的远程站点或远程用户与公司网络的连接。L2TP访问集中器（LAC）位于ISP的接入点（POP），负责与远程的用户交换PPP消息，并通过L2TP请求和响应的方式与客户的L2TP网络服务器（LNS）通信，以建立隧道。L2TP通过虚拟隧道在点到点连接的两个终端点之间传送协议层的分组。来自远程用户的帧被ISP的POP所接收，剥去任何所链接的帧结构或透明字节后，封装为L2TP，并转发到适当的隧道。客户总部的网关接受到这些L2TP帧，剥去L2TP封装，并处理进入的帧，转发到适当的接口。图23-3显示了L2TP隧道的细节，并显示了用户“lsmith”如何连接到LNS以访问指定公司的内部网。

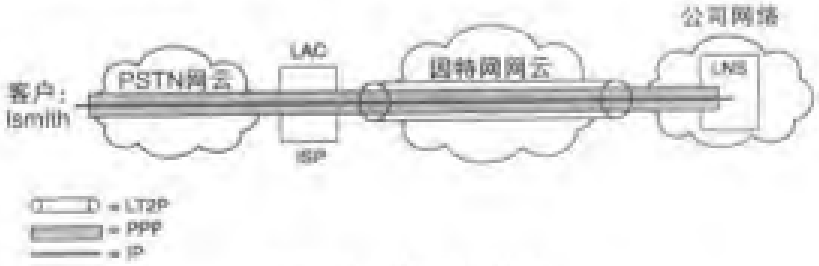


图23-3 L2TP隧道结构

隧道技术包含下列3种类型的协议，如图23-3所示：

- **旅客协议**（*Passenger protocol*）——被封装的协议。在拨号环境中，该协议可能是PPP、SLIP或文本对话。
- **封装协议**（*Encapsulation protocol*）——负责创建、维护并且拆除隧道。Cisco支持几种封装协议，包括用于虚拟拨号服务的L2TP协议。
- **载体协议**（*Carrier protocol*）——承载经过封装的协议。由于其强大的路由选择能力、对各种介质的普遍支持以及在因特网上的部署，IP成了L2TP协议首选的载体协议。

隧道已经发展成为定义和使用VPN的关键组件之一。Cisco IOS通过VPN的远程办公形式提供了虚拟拨号服务。

23.3.2 Cisco的虚拟拨号服务

以下的定义全面地描述了Cisco公司在其Cisco IOS软件中所提供的虚拟拨号服务。

- **远程用户**(*Remote user*)——从家中或者其他的远程地点拨号ISDN/公众交换电话网（PSTN）的客户端。
- **网络接入服务器**（*NAS*）——在模拟电路（基本电话服务）或数字（ISDN）电路上终止拨号呼叫的电信设备。
- **因特网服务提供商**（*ISP*）——提供拨号服务的提供商，既可以通过网络接入服务器（NAS）自己提供业务，有可以把远程拨号用户的服务请求传送到指定的公司网关。
- **公司网关**（*Corporate gateway*）——负责提供针对远程用户请求服务访问的目的路由器。这些服务可能由公司提供，或者甚至由另一家ISP提供。

远程用户（使用异步PPP或ISDN）访问公司局域网时就好像他们直接拨号进入公司网关一样（尽管他们的物理拨号是通过ISP的NAS来进行的）。图23-4显示了一个关于这些连接如何部署在虚拟拨号服务中的拓扑视图。

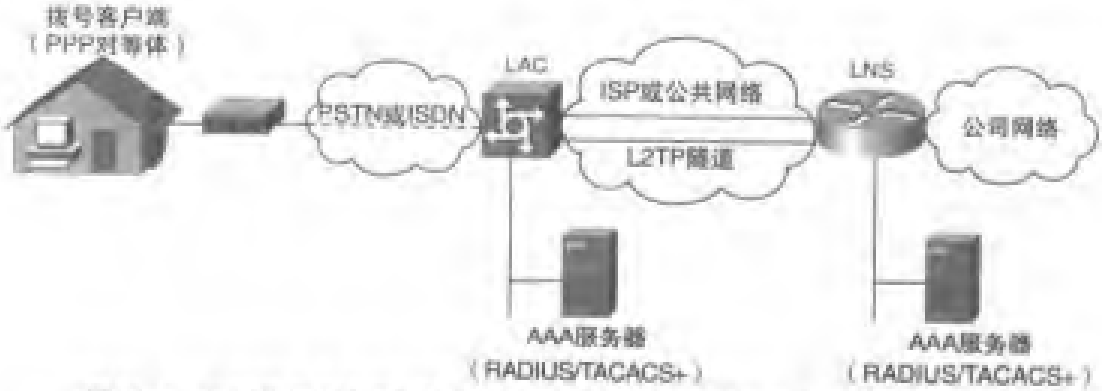


图23-4 远程用户通过建立到公司网络的PPP连接来实现完整的虚拟拨号拓扑

23.3.3 Cisco L2TP的实施

下面是实施Cisco L2TP后所提供的关键管理服务需求。

- 无论是远程端系统还是公司主机，都需要特殊的软件以安全的方式使用该服务。
- 拨号PPP、质询握手验证协议（CHAP）或口令验证协议（PAP）提供的身份验证——包括终端访问控制器访问控制系统（TACACS+）和远程身份验证拨入用户服务器（RADIUS）解决方案，以及对智能卡和一次性口令的支持。身份验证由用户进行管理，与ISP无关。
- 寻址问题将像专用拨号解决方案那样进行管理；远程用户各自所属的公司，而不是ISP，将负责分配地址。
- 公司的远程用户将管理授权，因为它将处于一个直接的拨号解决方案中。
- 记账功能由ISP（出于计费目的）和用户（出于拒付和审核目的）同时完成。

采用L2TP协议，使用隧道把远程用户直接连到公司所在地，就可以实现上述目标的大部分。对于PPP，所有的链路控制协议（LCP）和网络控制协议（NCP）的协商都发生在远程用户所属公司的所在地。允许使用PPP来实现远程用户到企业网关的信息传递。

L2TP是一项新兴的IETF标准，它结合了两种现存隧道协议最好的特性：Cisco L2F和Microsoft PPTP。L2TP作为对PPP的扩展，是VPN的一个重要组件。VPN允许用户和远程办公用户连接其企业内部网或外部网。VPN是很经济的，因为用户可以在本地连接到因特网，然后通过隧道连回到公司资源。这不仅减少了与传统远程访问方式相关的开销代价，而且也提高了灵活性和可扩展性。

传统的拨号网络服务只支持已经注册的IP地址，这限制了在VPN上所实施应用的类型。L2TP支持

多种协议，并在因特网上支持未注册和私有方式管理的IP地址。这使得现有的接入基础设施——比如因特网、调制解调器、接入服务器和ISDN终端适配器（TA）——仍旧可用。也允许企业客户能将拨出支持进行外包，以减少硬件维护成本的开销和800号的费用，并允许它们在公司网关资源处进行集中。图23-4显示了L2TP基础和一个典型的拨号环境。

23.3.4 端到端虚拟拨号过程

为了举例说明虚拟拨号服务是如何工作的，下列的例子描述了当一个远程用户发起访问时可能发生的情况。图23-5提供了关于这个端到端过程各步的详细信息。

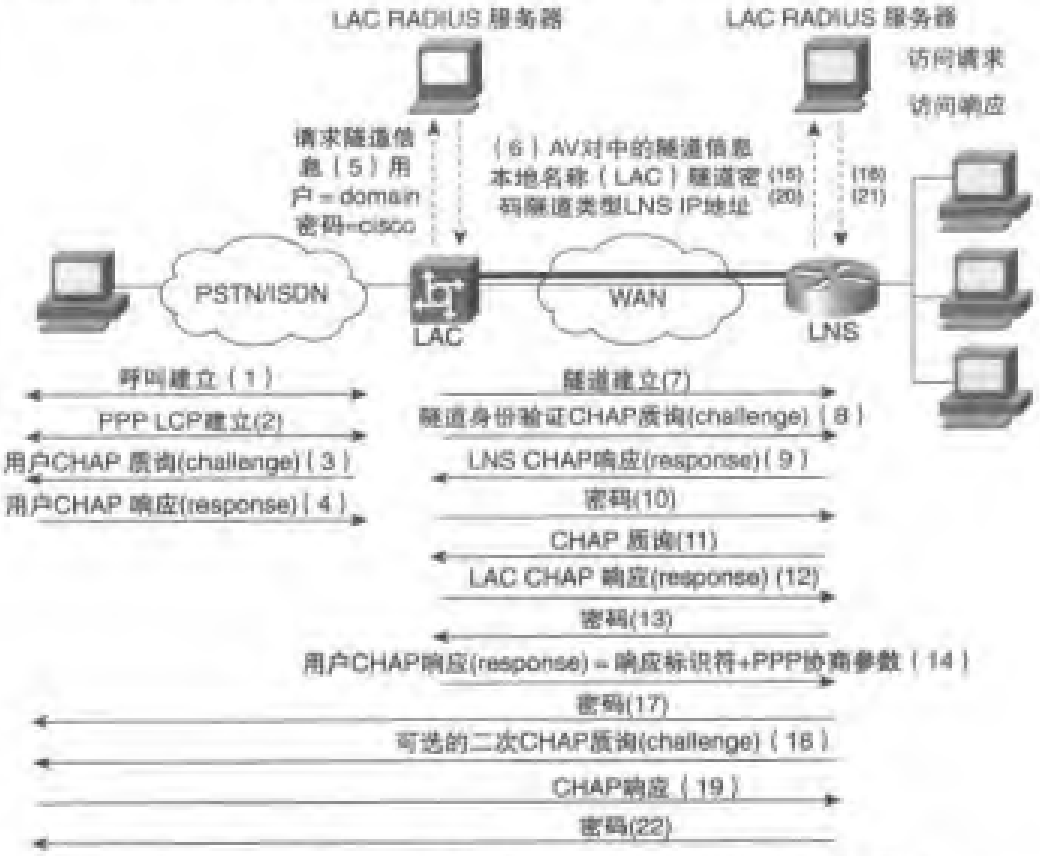


图23-5 远程VPN客户端与企业局域网进行通信所需要的步骤

远程用户、ISP接入点（POP）的LAC以及本部局域网的LNS之间，采用L2TP隧道的虚拟专用拨号网络（VPDN）连接是通过下列的步骤建立的：

1. 远程用户通过模拟电话系统或ISDN，发起一个到ISP的PPP连接。

2. ISP网络的LAC在POP接受该连接，PPP链路建立。

3. 终端用户与LNS完成LCP协商后，LAC用CHAP或PAP对终端用户完成部分的身份验证。用户名、域名或拨号身份验证服务（DNIS）确定用户是否是一个VPDN客户端。如果用户不是VPDN客户端，身份验证继续进行，用户可以访问因特网或其他的所签订的服务。如果用户名是一个VPDN客户端，名称与指定端点进行映射（即LNS）。

4. 隧道和端点（LAC和LNS）在隧道内尝试建立会话之前相互进行身份验证。或者，LNS可以接受隧道创建，而不对LAC进行隧道身份验证。

5. 隧道存在后，便为每个终端用户建立一个L2TP会话。

6. LAC负责传播经过LCP协商的选项，并对LNS部分地验证CHAP/PAP信息。LNS将经过协商的选项和身份验证信息直接传送到虚拟访问接口。如果虚拟访问接口上所配置的选项与LAC的经过

协商的选项不一致，连接会失效，并向LAC发送一个断开消息。

最终结果是，在拨号客户端和远程LNS之间建立了专用的交换过程，就好像没有涉及到中间设备（LAC）一样。图23-5提供了关于L2TP入站呼叫序列的图形化描述，并标明了其自己的相应详细序列号，该编号与上述步骤编号无关。

23.4 虚拟拨号服务要点

下面一节讨论了标准因特网接入服务和虚拟拨号服务两者在身份验证、授权、地址分配和记账方面的一些显著差别。

23.4.1 身份验证与安全机制

在传统的拨号情景中，ISP使用NAS和安全服务器，通过对远程用户的用户名和密码进行质询（challenging）来进行身份验证过程。如果远程用户顺利通过了身份验证，紧接着就进入了授权阶段。

注意：Cisco NAS所提供的功能趋向于既有虚拟拨号服务，也有传统拨号服务。

对于虚拟拨号服务而言，ISP通过身份验证来明确用户的表面身份（并由此隐含地获得用户要访问的企业网关）。在这时，不发生密码交互过程。一旦确定了公司网关，便发起连接，并附带有ISP收集的用户身份验证信息。公司网关通过接受连接和拒绝连接来完成身份验证（比如说，在PAP请求中，如果用户名和密码不正确，连接就会被拒绝）。接受连接后，公司网关在PPP层上就可以进行另一个阶段的身份验证。这些额外的身份验证活动已经超过了规范的范围，但可能包括专用的PPP扩展或者TCP/IP Telnet会话中使用的文本质询(textual challenges)。

针对每个已经建立的L2TP隧道，L2TP隧道安全机制会产生一个惟一的随机密钥，以防止欺骗式攻击。在L2TP隧道内，每个多路复用会话都会维护一个序列号以防止分组重复。Cisco 提供了允许在客户终端上实施压缩的灵活性。此外，隧道的加密可以通过IP安全协议（IPSec）实现。

23.4.2 授权

在提供传统拨号服务时，ISP都维护着定义了授权情况的每个用户配置文件。这样，安全服务器能够与网络接入服务器（NAS）相互作用来提供基于策略的应用，从而在身份验证的基础上连接用户。这些策略的范围很广，从针对小部分站点的简单的源/目的过滤器，到能决定特定应用、日常接入以及允许和拒绝访问目的地的长列表复杂算法。这个过程对于ISP会成为一个负担，尤其是在ISP必须代表公司为远程用户提供接入服务，而公司又要求服务策略经常改变时。

在虚拟拨号服务中，直接由远程用户的公司来提供基于策略的详细授权。通过在远程用户和公司网关之间提供端到端的联机，所有授权的进行跟远程用户直接拨号到公司一样。这个建立过程就能使ISP不必再维护包含许多不同公司的个人用户信息的大型数据库了。更重要的是，虚拟拨号服务对于使用它的公司也更安全。虚拟拨号服务能够使公司对于它们远程用户社区的变化进行迅速的反应。

23.4.3 地址分配

对于传统的因特网服务，用户都接受IP地址是从服务提供商的地址池中动态分配的。这个模型意味着由于防火墙和安全策略拒绝外部IP地址访问公司网络，远程用户几乎不能访问本公司的网络资源。

对于虚拟拨号服务，公司网关可以存在于公司防火墙之后并分配内部地址（事实上，可以是预留给专用网络的RFC 1597地址或非IP地址）。由于L2TP隧道仅工作在数据链路层，这些地址管理的实际策略与正确的虚拟拨号服务是彼此不相关的。为了PPP协议的处理，所有拨号接入的用户都假

装已经连接到公司的网关上了。

23.4.4 记帐

NAS和公司网关都需要提供记帐数据，这意味着它们可以记录分组数、8位位组、每次连接的起始时间和终止时间。由于虚拟拨号是一项接入服务，对于连接尝试（尤其是失败尝试）进行记帐是很有意义的。公司网关可以根据ISP收集的身份验证信息拒绝新的连接，并记录相应的日志。当公司网关接受了一个连接，并进一步进行身份验证时，公司网关有可能会断开与客户的连接。这种情况下，向ISP发回的断开连接指示中也可以包括断开的理由。

由于公司网关可以根据ISP收集的身份验证信息来拒绝某个连接，记帐可以很容易地区分一系列的失败连接尝试和短暂的成功连接尝试。如果没有这项功能，公司网关必须总是接受连接请求，并必须与远程系统交换大量的PPP分组。

23.5 总结

什么是VPN？正如你所学到的，VPN有几种形式。它可以存在于两个端系统之间，也可以存在于两个或更多的网络之间。可以通过使用隧道、加密或其任何一种虚拟路由器的方法来创建VPN。VPN可以由许多网络组成，这些网络通过租用线、帧中继或ATM连接到服务提供商的网络中；VPN也可以由许多拨号用户组成，这些用户连接到服务集中点或其他的拨号用户。

VPN是一个非常多变的主题；没有单个定义的产品，甚至在各个VPN厂商之间没有关于VPN构成的统一意见。因此，人人都知道VPN是什么，但要建立惟一的定义可能非常困难。

每个组织都有自己必须解决的问题，本章中提到的每种工具都可以用于构建特定类型的VPN，以达到一组特定的功能目标。解决这些问题的工具不止一个，网络工程师应该认识到，在VPN这个领域内，许多人都一般性地使用术语——这个涉及范围很广的问题由很多可行的解决方案。每种方案都有很多的优点、缺点和薄弱环节。在未来的数月或数年中，没有单个的VPN机制能排挤掉其他的机制。实际情况反而是，VPN领域的可供选择的各种技术将会不断涌现。

23.6 关键术语

接入VPN（*access VPN*） 通过一个与专用网络有着相同策略的共享基础设施提供对企业内部网或外部网的远程访问的VPN。

载体协议（*carrier protocol*） 承载经过封装的协议。由于其强大的路由选择能力，对各种介质的普遍支持以及在因特网上的部署，IP成了L2TP协议首选的载体协议。

公司网关（*corporate gateway*） 负责提供针对远程用户请求服务访问的目的路由器。这些服务可能由公司提供，或者甚至由另一家ISP提供。

封装协议（*encapsulating protocol*） 负责创建、维护并且拆除隧道。Cisco支持几种封装协议，包括用于虚拟拨号服务的L2TP协议。

外部网VPN（*extranet VPN*） 通过使用专用连接上的共享基础设施，将客户、供应商和有一定共同利益的团体连接到公司内部网的一种VPN。

内部网VPN（*intranet VPN*） 通过使用专用连接上的共享基础设施，将公司总部、远程办公室和分支机构链接在一起的一种VPN。

因特网服务提供商（*Internet Service Provider，ISP*） 提供拨号服务的提供商。它可以通过NAS自己提供服务，也可以把远程拨号用户的服务请求传送到指定的公司网关。

第2层隧道协议（*Layer 2 Tunneling Protocol，L2TP*） PPP协议的扩展，使得ISP可以对VPN进行运营。L2TP融合了其他两种隧道技术的优点：来自Microsoft的PPTP和来自Cisco Systems的L2F。与PPTP一样，L2TP要求ISP的路由器支持该协议。

网络接入服务器（*Network Access Server，NAS*） 在模拟（基本电话业务）或数字（ISDN）电路上终止拨号呼叫的电信设备。

旅客协议（*passenger protocol*） 被封装的协议。在拨号环境中，该协议可能是PPP，SLIP或文本对话。

远程用户（*remote user*） 从家中或其他的远程地点拨叫ISDN/PSTN的客户端。

服务水平协议（*Service-Level Agreement，SLA*） VPN提供商与其用户之间经过协商的协议。SLA保护用户对特定服务所期待的服务标准。

隧道接口（*tunnel interface*） VPN隧道的进出点。隧道接口与硬件接口类似，不过是在软件中配置的。

隧道（*tunneling*） 一种能将分组封装在某种协议中，并在给定网络的出入点对协议进行解释的传递手段。

虚拟专用网（*Virtual Private Network，VPN*） 在公共网络基础设施，比如全球因特网上构建的专用网络。

第五部分　附录

附录A　术语表
附录B　复习题答案



附录A　术语表

术语表见随书附盘。



附录B 复习题答案

本附录中包含了各章末尾“复习题”中问题的答案。

第1章

1. OSI模型的哪一层最恰当地描述了10BaseT标准？

   C. 物理层

2. 下列哪一项最恰当地描述了OSI模型中传输层的功能？

   A. 它通过流量控制来发送数据

3. 下列哪一个功能是路由器用来在网络中转发数据分组的？

   B. 路径选择和交换

4. 下列哪两项是动态路由选择的基本类型？

   C. 距离矢量和链路状态

5. 当网络中的所有路由器都使用着相同的知识时，下列哪一项可以用来描述这个网络？

   A. 收敛

6. 描述数据封装的用途。

   OSI模型的每一层都依赖于其下一层所提供的服务。为了提供该服务，下一层通过封装，将来自上一层的协议数据单元（PDU）放到数据字段中；然后，添加本层用于完成自身功能的各种头部和尾部。

7. 描述OSI模型中传输层的主要功能。

   传输层的服务允许了主机和目的地之间可靠地进行数据传输。为了获得可靠的数据传输，需要在通信终端系统之间建立一种面向连接的关系。

8. 描述ICMP的用途。

   ICMP在所有的TCP/IP主机上都实施。ICMP消息承载在IP数据报中，用于发送错误消息和控制消息。ICMP消息的例子包括ping和“目的不可达”。

9. 描述TCP/IP实现中的窗口操作。

   窗口操作（Windowing）是一种控制端到端信息传送量的方法。窗口操作是发送方和接收方关于在两个确认之间传送多少数据的协议。

10. 描述OSI模型中网络层的主要功能。

    网络层提供了尽力的端到端分组传送。网络层基于IP路由选择表将分组从源网络发送到目的网络。

11. 哪一条命令用来为一个网络配置RIP路由选择进程?
    B.router rip
      network *network-number*
12. 下列哪一项最恰当地描述了TCP/IP协议栈?
    B. 支持所有的物理标准和数据链路协议
13. 哪一项最恰当地描述了经过封装的数据分组的结构?
    C. 帧头部，网络头部，数据，帧尾部
14. 哪一项技术使用了窗口操作来保证一台电脑发送的数据流通过数据链路发送到另外一台电脑时不出现数据重复和丢失?
    A. 确认和重传
15. 动态路由选择的一个优点是什么?
    C. 当拓扑结构和流量发生改变时可以自动调整
16. 下列哪些项最恰当地描述了传输层的主要功能?
    A. 使用TCP协议对数据流进行分段或重组
17. 在RIP路由选择协议中，发送路由选择更新的频率是多少?
    A. 每30秒
18. 下列哪一项是正确的?
    C. MAC地址应用在数据链路层，并在硬件上编码写进网络接口卡
19. 网络分层模型的好处是什么?
    D. 以上答案均正确
20. 路由器为分组进行路径选择执行了下列哪一种功能?
    B. 参照路由选择表，决定使用哪一个端口来发送数据到目的网络

第2章

1. 当172.17.15.0/24用额外的4位进行子网划分时，以下哪两个地址是合法的子网地址?（选择2个答案）
   A. 172.17.15.0
   D. 172.17.15.96
2. 点到点的WAN链接中最有效的子网掩码是什么?
   C. 255.255.255.252
3. 下列哪项是CIDR的特性?（选择所有正确的答案）
   B. 超网
   D. 路由聚合
4. 网络172.21.136.0/24和172.21.143.0/24的汇总地址是什么?
   B. 172.21.136.0/20
5. 哪种路由选择协议在它的路由选择更新中不包含子网掩码信息?
   C. RIPv1
6. 下列哪种方法在一个单一的IP地址内表示一个IP地址集合?
   D. 路由汇总

第3章

1. 在DR和BDR选举出来后，OSPF网络处于哪种状态?

A. ExStart

2. 哪种类型的OSPF分组可以建立和维持邻居路由器的比邻关系?
   C. Hello分组
3. OSPF缺省的成本度量值只基于下列哪一项?
   B. 带宽
4. 下面哪个组播地址代表所有的OSPF路由器?
   D. 224.0.0.5
5. 下面哪条命令可以改变接口的OSPF优先级?
   B. ip ospf priority number
6. 下面哪个组播的地址用于将LSU发送给所有DR/BDR路由器?
   A. 224.0.0.6
7. 下面哪种特性是NBMA网络有的?
   B. 支持两台以上的路由器
8. 下面的哪条命令允许路由器交换路由选择更新信息而不使用组播?
   A. ip ospf neighbor
9. 下面哪条命令所显示路由器所知道的路由，以及它们各自是如何学到的?
   B. show ip route

第4章

1. 如何配置IGRP和EIGRP之间的自动重新分配?
   C. 用同样的自主系统号配置两个协议
2. 哪种协议结合了链路状态和距离矢量路由选择协议二者的优点?
   D. EIGRP
3. 哪个算法用来获得快速的收敛?
   B. 扩散更新算法
4. EIGRP可以通过使用PDM支持哪种协议?
   C. IPX
5. 哪张表包含了路由器所学到的到达各个目的地的路由项，并且为所配置的每种被路由协议维护一个单独的表?
   B. 路由选择表
6. 在EIGRP中下列哪一个建立邻接?
   B. Hello分组
7. 下列哪一项保证了到达所有邻居的EIGRP分组的有序传送?
   D. 可靠传输协议
8. DUAL在跟踪所有路由、比较它们、保证它们无环路后做什么?
   A. 向路由选择表中插入多达4条最低成本路径
9. EIGRP如何防止外部路由发生路由选择环路?
   D. 存储所有在路由表中标为“有环路”的邻接路由
10. 在高带宽的连接中，如点到点的串行连接和多点电路，EIGRP使用多长的Hello间隔?
    A. 5秒

第5章

1. 以太网的介质采用哪种广播技术在网络节点中传输和接收数据?

   B. 数据帧

2. 微分段技术的特点包括?

   D. A和B

3. 局域网交换机可以被看作下列哪一项?

   D. 工作在第2层的多端口网桥

4. 非对称式交换最适于以下哪种环境?

   A. 客户/服务器方式的网络通信，“快速的”交换机端口用于连接服务器

5. 描述全双工和半双工的以太网工作方式。

   对于半双工以太网，发送（TX）和接收（RX）电路竞争使用单个共享介质的权利。对于全双工以太网，发送（TX）和接收（RX）是分离的电路；因此，不需要竞争通过介质传送数据的权利。

6. 描述生成树协议的主要功能。

   生成树协议的主要功能是支持冗余的交换/桥接路径，并且不会受到网络中环路的影响。

7. 在网络中哪种网段是通过交换机划分的?

   C. 冲突域

8. 在全双工的以太网交换机中，哪个是正确的?

   D. 以上所有的

9. 拥塞会导致下面哪种效果?

   E. 以上所有的

10. 主机A要发送数据给主机B。通信过程是这样的，主机A停止发送分组之后，主机B开始发送数据；类似的，主机B停止发送分组之后，主机A开始发送数据。这样的传输类型应该定义为哪种方式?

    B. 半双工

11. 下面哪种关于数据帧在局域网中转发的描述是错误的?

    D. 如果网络连接速度慢，贯穿式交换需要缓冲技术

12. 下面哪个关于局域网交换机的描述是正确的?

    B. 它是一台高速的多端口的网桥

13. 一台16端口的交换机可以产生多少个冲突域?

    D. 16

14. 通过局域网交换技术建立虚电路，可以导致?

    D. 增加可用带宽

15. 交换机如何学习连接到其端口的网络设备的地址?

    B. 交换机检查从端口流入的分组的源地址

16. 对称式交换的目的是什么?

    A. 为每个端口提供相同带宽的交换式连接

17. 哪种网络设备可以用于对局域网进行逻辑分段?

    A. 路由器

18. 路由器通过哪种方式划分网段?

    D. A和B

19. 下面哪种不是在局域网部署第3层设备带来的好处?

D. 增加局域网的规模

20. 下面哪个是企业级服务器的例子?

B. 校园区的DNS服务器

第6章

1. 接入层提供什么功能?

A. 网络中的用户和服务器的入口点

2. 下列关于核心层的描述哪个是对的?

B. 作为高速交换骨干将通信从一个区域转发到另一个

3. 下列哪个是在局域网中引入第3层设备的好处?

D. 以上全部

4. 下列哪种设备提供局域网的逻辑分段?

A. 路由器

5. 使用交换机进行的微分段的作用是?

C. 增加冲突域

第7章

1. 微分段有哪些特点? 选择所有正确的答案。

A. 发送主机和接收主机之间有专线连接

B. 交换机内部有多条流量路径

2. LAN交换机的特征是什么?

D.工作在第2层的多端口网桥

3. 对称交换为下面哪种情况进行了优化?

A.连接到交换机“快速”交换端口上的客户端 – 服务器间的网络流量

4. 在_____交换中，交换机检查目的地址后就立即开始转发帧，而在_____交换中，交换机接收到完整的帧才转发?

B. 贯穿式；存储转发

5. 无碎片交换和快速转发交换是哪种交换的两种形式?

C. 贯穿式

6. 工作站与交换机相连时，使用哪种电缆最合适?

A. 直通

7. 一台主机发送，一台主机接收，这是哪种通信方式的特征?

B. 单播

第8章

1. 冗余拓扑的目的是消除网络的中断故障。这种故障是由几个失效点引起的?

A. 1

2. 生成树协议的目的是什么?

B.维持无环网络

3. 当网络拓扑发生改变时：

D. 生成树协议自动重新配置交换机或者网桥端口

4. 根网桥上的所有端口都是
   C. 指定端口
5. 生成树协议如何在非根桥上选出根端口？
   B. 根端口为非根网桥到根网桥的最低开销路径
6. 以下哪种网桥会被STP选为根网桥？
   B. 拥有最低BID
7. STP BID包括有：
   B. 网桥优先级和网桥MAC地址
8. 在哪种状态下端口只形成MAC地址表但不转发用户数据帧？
   A. 学习状态
9. 修正后的IEEE规定100Mbit/s连接的开销是多少？
   C. 19
10. STP收敛的定义是什么？
    D. 所有端口转换到转发状态或者阻塞状态
11. STP默认的最大存活期是：
    C. 20秒
12. 在RSTP中，等效于STP的阻塞状态的状态是：
    C. 丢弃状态
13. RSTP中，每个交换式LAN网段上被选举为转发端口的交换机端口称为：
    D. 指定端口
14. STP如何提供无环网络？
    C. 将部分端口置为阻塞状态

第9章

1. VLAN解决什么问题？
   D. 以上都是
2. 一个VLAN可以被认为是下面中的哪一个？
   A. 广播域
3. 在VLAN拓扑中的路由器能提供什么功能？
   D. 以上都是
4. 短语*可扩展的微分段*（*microsegmentation with scalability*）的含义是什么？
   A. 无须建立冲突域就能够增加网络大小的能力
5. 交换机作为VLAN的核心元素，提供了哪些智能化的功能？
   D. 以上都是
6. 连接到一个_____端口的每一个_____分段只能被分配到同一个VLAN中。
   A. 交换机；集线器
7. 以下哪一项不是静态VLAN的优点？
   D. 加入新站点时可以自动配置端口
8. 以下哪 一项不是VLAN划分时依据的标准？
   D. 以上都是建立VLAN的标准
9. 以下哪一项是增加VLAN带来的好处？选择所有正确的。
   B. 广播能够得到控制

C. 机密数据能够得到保护

D. 突破了限制用户成为组的物理的边界

10. 下面关于VLAN的陈述哪一个是错误的?

C. 网桥构成了VLAN通信中的一个核心组件

11. 交换机上的哪一项第3层功能使你能够轻松地操纵不同IP子网上的设备?

D. VLAN

12. 当分组从一个VLAN传输到另外一个VLAN时，需要以下哪一种设备?

B. 路由器

13. 帧标记发生在OSI模型的哪一层?

B. 第2层

14. _____使交换机可以共享地址表，而_____向每一帧分配一个用户定义的VLAN ID?

C. 帧过滤；帧标记

15. 为什么创建VLAN很重要?

D. A和B

第10章

1. 使用中继链路的主要好处是什么?

B. 有效使用路由器和交换机端口

2. 哪种协议在一条中继上承载多个VLAN?

C. 802.1Q

3. 哪种协议是Cisco专有的并设计用于传输来自多个VLAN的流量?

D. ISL

4. 在一台基于Cisco IOS命令的交换机上创建或配置一条VLAN中继，首先将一个端口配置为中继线，然后指定中继线的封装。

A. 正确

5. VTP消息是封装在Cisco专有的交换机间链路（ISL）中还是其他类型的帧中?

A. IEEE 802.1Q协议帧

6. 使用VTP时，Catalyst系列交换机会在其中继端口中通告以下何种信息?

D. 以上所有

7. VTP交换机可以工作在哪种模式下?

D. 以上所有

8. 一个管理域中能运行两种不同版本的VTP：VTP版本1和VTP版本2。这两种版本可以互操作。

B. 错误

9. 创建一个管理域，使用哪条命令?

D. Switch(vtp)# vtp domain Cisco

10. 一台交换机的缺省行为是在网络中传播广播和未知的_____?

A. 帧

11. 在一台VTP服务器上启用VTP剪裁会使得整个_____域启用剪裁?

C. 管理

12. 在交换网络中，_____是用来提供VLAN间的通信的?

A. 路由处理器

第11章

1. 私有地址通过什么进行分配?
   A. RFC 1918的网络管理员。
2. 下面哪一个是有效的RFC 1918私有地址?
   B. 10.0.0.0/8
   C. 192.168.0.0/16
   D. 172.16.0.0/12
3. BOX公司维护它自己的公共web服务器，并打算实现NAT。应该为该web服务器使用哪一种类型的NAT?
   B. 静态
4. 下面哪一项应用是Cisco IOS NAT所支持的?
   A. ICMP
5. 下面哪一种流量类型是Cisco IOS NAT不支持的?
   B. DNS区传输
   C. BOOTP
6. BOOTP支持静态映射而DHCP支持动态映射
7. 将下列DHCP消息按其在过程中出现的正确顺序排列。
   D. DHCPDISCOVER
   C. DHCPOFFER
   B. DHCPREQUEST
   A. DHCPACK
8. DHCP代表什么?
   A. Dynamic Host Configuration Protocol
9. NAT通过允许企业内连网私有化来保存合法注册的寻址方案。
   A. 正确
10. DHCP并非打算用于配置路由器、交换机和服务器，因为这些主机需要静态IP地址。
    A. 正确

第12章

1. 模拟拨号的连接不适合于下面哪些流量类型?
   D. 视频
2. 下面关于ISDN的描述哪一个是正确的?
   A. ISDN BRI提供两条B信道和一条D信道。
3. 租用线是一条_____链路，它提供了一条单一的从客户到远程网络的预先建立的广域网通信链路。
   A. Point-to-point
4. 下面关于X.25网络哪一个是正确的?
   B. 数据分组不会造成延迟。
5. 帧中继如何在同一物理连接上处理多个会话?
   A. 帧中继多路复用电路。
6. 下面关于ATM技术哪一个是不正确的?

D. ATM信元是35Bytes的固定长度。

7. 连接到服务提供商中心局的位于用户端的设备是：

C. CPE

8. 将数据发送到本地环路上的设备是：

B. DCE

9. 将数据传输到DCE的客户设备称为：

A. DTE

10. 数字线路需要一个_____和一个_____。

A. CSU和DSU

11. 对于模拟广域网服务，一个_____是必需的？

C. 调制解调器

12. 下面除了_____以外都是电路交换连接？

D. SONET

13.在分组交换网络中，交换开始时已经建立的路由被称为：

A. 永久虚电路（PVC）

14. 在分组交换网络中，根据需要才建立的路由被称为：

B. 交换虚电路（SVC）

15. 下面哪种服务是ISDN连接的特点？

C. 同步拨号

16. 下面哪一个是DCE设备？

B. 调制解调器

17. PPP运行在OSI的哪一层？

B. 数据链路层

18. 帧中继运行在OSI的哪一层？

B. 第2层

19. ISDN BRI由以下哪一个组成？

B. 2条B信道和1条D信道

第13章

1. 在PPP链路上建立连接的第一步包括：

D. 初始节点为配置数据链路面发送链路控制协议（LCP）帧

2. 在PPP中，如果链路控制协议（LCP）终止了一条链路，会发生什么？

D. 链路控制协议（LCP）通知网络层协议

3. PPP支持以下哪种网络层协议？

D. 以上全部

4. PPP中的NCP（网络控制协议）实现以下哪种功能？

B. 封装多种协议

5. 在PPP的帧里，哪个字段标识封装的是IPX还是TCP/IP？

C. 协议字段

6. PPP在什么情况下最可能会被本地工作站用于建立到因特网的连接？

C. 工作站需要拨号连接到因特网

7. 当使用PPP时，LCP负责：

A. 建立、保持和中断点到点的连接

8. PPP会话的建立包括几个阶段?

C. 4

9. 当选择PAP作为PPP的验证协议时，将使用哪种类型的握手?

C. 2次握手

10. 检查LCP（链路控制协议）和NCP（网络控制协议）的状态可以使用以下哪条路由器命令?

C. router# show interfaces

11. 你将会使用哪种协议在ISDN上建立一个远程连接?

A. PPP

12. 当PPP在几条链路上进行负载均衡时，利用了什么特性?

D. 多链路

13. PPP链路的建立需要链路控制协议（LCP）开启一个连接，然后：

A. 协商配置参数，发送和接收一个配置确认帧

第14章

1. ISDN中使用哪条信道进行数据传输?

A. 16kbit/s的B信道

2. 哪条信道用于ISDN带外信令?

D. D信道

3. 首先动态分配的TEI值是多少?

A. 64

4. 在两台交换机之间使用以下哪种机制来传递呼叫控制信息?

D. Q.921

5. 在处理ISDN呼叫的过程中，D信道的主要功能是什么?

C. 传送呼叫通信

6. 在北美使用ISDN BRI将一台路由器用作拨入服务器，需要用到哪个ISDN接口?

B. ISDN BRI U

7. 如果路由器有一个U接口，这意味着什么?

C. 它有内置的NT1

8. 下列哪种交换机类型用于欧洲BRI连接?

A. Net3

B. Net5

D. VN3

9. 由以下谁来提供SPID?

C. ISDN服务提供商

10. DDR用于什么?

B. ISDN中低容量、周期性的网络连接

11. 下列有关DDR的叙述中错误的是哪些（选4个）?

B. DDR在两个站点之间创建永久连接

C. DDR允许路由器只连接一个端点

E. 如果希望有一台永久的WWW服务器，配置DDR是正确的选择

F. DDR仅应用于ISDN

12. 使用传统DDR的主要局限性是什么？
C. 将配置直接应用到物理接口

第15章

1. 在同一个物理连接中，帧中继是如何处理多个会话过程的？
B. 采用多路复用电路
2. 帧中继采用以下哪种协议进行纠错处理？
B. 上层协议
3. 帧中继采用以下哪种方式使得DLCI具有全局性？
C. 发送组播信息
4. 以下哪个是帧中继交换机为进行数据传输而同意的数据速率？
A. 承诺信息速率（CIR）
5. DLCI号是由谁来分配的？
D. 服务提供商
6. 帧中继报头格式中的哪个字段包含DLCI信息？
B. 地址字段
7. 帧中继使用以下哪一项来保持PVC一直处于连通状态？
C. 维持机制
8. 帧中继如何使用反向ARP请求？
D. 使用IP地址到DLCI的映射表
9. 帧中继采用什么来决定下一跳？
C. 帧中继映射
10. 帧中继采用水平分割的目的是什么？
B. 防止路由选择环路
11. 帧中继运行在哪一层？
A. 第2层
12. 下面哪一条叙述是正确的？
B. 关于帧中继的标准化建议最早是由国际电话与电报顾问委员会（CCITT）提出的
13. 使用下列哪条命令（在配置模式提示符下）进入配置模式为串口进行帧中继分组封装？
D.#interface serial0
14. 如果执行了show interface serial 0命令而且出现了消息“Serial line is up，line protocol is up”，对于这条消息的正确解释是什么？
C. 帧中继的连接处于激活状态
15. 命令show interfaces serial的作用是什么？
A. 显示关于多播的DLCI信息、已配置串口上的帧中继所使用的DLCI信息以及由本地管理接口（LMI）使用的DLCI信息
16. FECN和BECN是什么？
B. 拥塞通知机制
17. 下面哪项对帧中继虚电路的描述是正确的？
D. 在网络设备之间提供一条逻辑的、双向的通信路径
18. 帧中继使用循环冗余校验码（CRC）的目的是什么？
B. 执行错误校验功能

19. 下面关于帧中继本地管理接口（LMI）扩展的描述，哪条是不正确的？
A. 通过计算产生了MAC地址

第16章

1. 网络的基准性能（baseline）是用来衡量网络的什么方面的？
D. 性能
2. 对等体—对等体网络在终端之间建立起了何种关系？
A. 客户机—客户机
3. Window NT为了安全目的采用了什么文件系统？
C. NTFS
4. 在客户机/服务器网络中，一个用户能够访问某些文件、不能访问另外一些文件。这是用户的什么属性？
B. 权限
5. 内部环路IP地址是什么？
C. 127.0.0.1
6. 防止静电损害的方法有哪种？
D. 使用接地腕套
7. 哪种协议支持网络管理？
C. SNMP
8. 列出你的Windows NT计算机上的IP配置，你应该使用什么命令？
B. ipconfig
9. 下面哪种是用来进行网络故障排除的方法？
B. 分块征服
10. 如果服务器被设置为使用IP协议，那么客户机必须使用哪种协议和它进行通信？
C. IP
11. RMON是哪种协议的扩展？
E. SMTP
12. ping命令中-n选项表示什么？
A. ping区域的网络号
13. RMON中，远程数据是怎样被收集到的？
D. 探针
14. 对于关键应用业务，_____设备的成本需要加入到网络维护成本中去？
A. 冗余

第17章

1. 下列各条中哪一条不是光网络的关键推动力？
D. 能够适应封闭系统结构
2. 下面哪条关于IOR的描述是正确的？
C. 它是指光在真空中的传输速度和在光纤中的传输速度的比值
3. 判断对错：光流是电路中自然产生的电子噪音。
B. 错误
4. 下面哪个波长值没有在光纤中使用？

C. 1450nm

5. 下面哪一（几）条正确描述了光纤？

D. 以上都对

6. 下面哪种方法能够放大光纤中的光信号？

D. EDFA

7. 多模光纤的一般传播速度为：

A. 几百Mbit/s

8. 关于单模光纤的描述正确的是：

D. 单模光纤允许一种模式的光在其中传输

9. 下面哪些是关于纤芯的可能发生的问题？

D. 以上都对

10. 下面哪个不是光缆的组件？

C. 外覆层

11. SONET被设计为对下列哪些进行标准化？

A. 同步网络操作管理维护和设备

12. 下面哪个不是关于维护的3个级别的负载通道？

C. COH

13. 下面哪种设备可能是DWDM系统的客户端设备？

C. 路由器

14. 下列DWDM系统中的哪台设备是用来转化SONET/SDH兼容光信号的？

D. 应答机（Transponder）

15. 从技术和经济的角度，下面哪条是DWDM技术最明显的优点？

B. 提供潜在的无限传输容量的能力