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（第一、二学期）（第三版）

Cisco Networking Academy Program

CCNA 1 and 2

Companion Guide

Third Edition

The only authorized textbook for the Cisco Networking Academy Program



[美] Cisco Systems 公司
Cisco Networking Academy Program 著

清华大学 | 北京大学 | 北京邮电大学 | 华南理工大学
—— 思科网络技术学院 —— 译

人民邮电出版社
POSTS & TELECOM PRESS

思科华为3COM 让技术不再孤单，思想不再流浪

中国思科华为3COM网络技术站推荐读物 http://www.CiscoH3C.com.com

思科网络技术学院教程（第一、二学期）（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OSI参考模型的各层和路径的确定、关于IP路由选择及寻址和子网划分等主题的配置细节、基本的路由器配置和运行等内容。本教程还介绍了以太网、访问控制列表、TCP/IP协议组，以及铜线、无线和光纤等介质。

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TCP、OSPF路由选择、变长子网掩码（VLSM）和NAT等内容，对路由器配置、Cisco IOS软件和TCP/IP部分的内容进行了较大的改动和强化。
- 在附录中新增了关于结构化布线的内容。
- 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中对应部分的实验。
- 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、具有可自定义考试引擎的300道模拟试题、关于Cisco设备的图片集、覆盖难点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 7-115-12211-3

9 787115 122117 >

ISBN7-115-12211-3/TP·3930
定价：65.00 元（附光盘）

人民邮电出版社网址 www.ptpress.com.cn

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
（第一、二学期）（第三版）

[美] Cisco Systems公司
Cisco Networking Academy Program 著
清华大学|北京大学|北京邮电大学|华南理工大学
——思科网络技术学院—— 译

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1、2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 7-115-12211-3

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059559号

版 权 声 明

Cisco Systems, Inc Cisco Networking Academy Program: Cisco Networking Academy Program CCNA 1 and 2 Companion Guide Third Edition （ISBN 1-58713-110-2）

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

（第一、二学期）（第三版）

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

译 清华大学 | 北京大学 | 北京邮电大学 | 华南理工大学
—— 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：40

字数：1 118千字 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：01-2003-1479号

ISBN 7-115-12211-3/TP·3930

定价：65.00元（附光盘）

本书如有印装质量问题，请与本社联系 电话：(010)67129223

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。

本书为思科网络技术学院第一、二学期的配套书面教程，主要内容包括：网络入门、网络基础、网络介质、线缆测试与局域网和广域网布线、以太网基础、以太网技术和以太网交换、TCP/IP协议集和IP寻址、路由选择基础和子网、TCP/IP传输层和应用层、广域网和路由器、路由器基础、路由器配置、了解邻近和远程设备、管理Cisco IOS软件、路由选择和路由选择协议、距离矢量路由选择协议、TCP/IP差错控制消息、路由器排障基础、中级TCP协议、访问控制列表等内容。每章的最后还提供了复习题。附录A描述了结构化布线的各方面情况；附录B的术语表描述了书中使用的有关网络的术语和缩写；附录C是每章结尾复习题的答案。

本书为思科网络技术学院第一、二学期的指定教材，适合准备参加CCNA认证考试的读者。另外本书也适合各类网络技术人员参考阅读。

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，钱伯斯第二次访华之际，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 让合作更流浪

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。

为满足互联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，掌握这些内容可以帮助你在计算机网络领域从容应聘或接受更高级的教育和培训。

本书的内容比你在思科网络技术学院项目的在线教材中学到的内容更为深入，本书将向你介绍与思科认证网络工程师（CCNA）认证考试相关的主题。本书遵循了思科系统公司应用在教程中的样式及风格。

本书介绍了局域网(LAN)设计、配置和维护方面的知识，并将扩展你在这些方面的实际经验。本书中涵盖的概念将带给你布线、路由选择、IP寻址、路由选择协议和排除网络故障等几个方面的经验和技能。本书介绍了开放系统互联（OSI）参考模型，讨论了冲突（collisions）和网络分段（segmentation），并在以太网技术和以太网交换方面新增加了一章的内容。本书还大大增强了IOS和TCP/IP相关章节的内容，并且增加了访问控制列表一章。

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

本书的目的

这本书的目的是教授你思科所支持的网络技术，帮助你理解如何设计和构建网络，如何配置Cisco路由器。本书设计为与思科网络技术学院项目在线教程配合使用。

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。在课堂教学中，本书可作为在线教程的补充。

本书同样适合于公司的培训人员、公司职员以及一般用户。本书容易掌握的、不枯燥难懂的表述方式，是那些愿意远离专业技术手册的读者们理想的选择。

本书的特点

本书的特点是书中贯穿了可以帮助读者完整理解网络和路由选择的内容。

• **目标**——在每一章的开始都会列出学完这一章后要掌握的内容和要达到的目标。这些目标涉及本章中所包含的各个概念。

• **插图、实例、表格和场景**——本书包含了许多插图、实例和表格，它们可以帮助你加深对理论、概念、命令和安装顺序等内容的理解。它们对概念的补充可以帮助你更形象地体会章节的内容。此外，特定的场景还提供了现实生活中遇到的情形，对问题和解决方案进行了详述。

• **每章总结**——每章的结尾都有关于本章中概念的总结，它提供了本章的纲要，是复习的好帮手。

• **关键术语**——每章还包含了一个关于本章中所涉及关键术语的列表，作为学习的帮助。此外，在学习新的概念之前，这些关键术语能够加深你对本章概念的理解，并理解本章的内容。关键术语将贯穿整章，并在首次出现时用粗体字加以强调。

• **复习题**——每章的结尾都有一些练习题，可作为对每章学习情况的评估。此外，这些问题补充了章节中介绍的概念，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；

• **实验参考**——本书中提到的工作表和实验都可以在《思科网络技术学院教程实验手册（第一、二学期）》（第三版）中找到。这些实验使你能够把理论与实践很好地结合起来。

本书的内容结构

本书分为20章和3个附录。

• **第1章“网络技术入门”**，介绍接入因特网（Internet）的基本知识。同时也介绍了几种不同的数制以及由一种数制转换为另一种数制的方法。本章对应于CCNA 1在线教程中的内容。

• **第2章“网络技术基础”**，介绍了网络工程师们使用的一些术语和各种类型的计算机网络。也描述了OSI参考模型网络体系是如何支持各种网络标准的。此外，本章还介绍了OSI参考模型中各层的基本功能。最后，本章描述了各种网络设备和网络拓扑。本章对应于CCNA 1在线教程Module 2中的内容。

• **第3章“网络介质”**，介绍了基本的电气理论，这些理论是理解OSI参考模型物理层的基础。本章讨论了在物理层上用到的各种不同类型的网络介质，包括屏蔽双绞线、非屏蔽双绞线、同轴电缆、光纤和无线介质。本章对应于CCNA 1在线教程Module 3中的内容；

• **第4章“线缆测试及局域网广域网布线”**，描述了与测试局域网（LAN）中传输介质相关的一些问题，这些介质为局域网提供物理层的连接。网络介质是网络物理上的真正骨干，劣质的网络线缆将会导致网络故障或网络不稳定。用于线缆测试的设备会涉及到一些电子和数学上的概念及术语，例如信号、波、频率和噪声。理解这些词汇有助于你学习关于网络、布线和线缆测试的知识。本章对应于CCNA 1在线教程Module 4和Module 5中的内容。

• **第5章“以太网基础”**，讨论了以太网的运行方式、成帧、错误处理以及以太网络中各种不同类型的冲突。此外，本章还介绍了冲突域和广播域。最后本章描述了网络分段和用于网络分段的设备。本章对应于CCNA 1在线教程Module 6中的内容；

• **第6章“以太网技术与以太网交换”**，介绍了第2层的桥接和交换技术。它介绍了生成树协议（STP），阐明了STP如何工作，还提到了STP交换机端口的状态。本章对应于CCNA 1在线教程Module 7和Module 8中的内容。

• **第7章“TCP/IP协议集与IP寻址”**，概述了TCP/IP协议集。它从TCP/IP的历史和未来讲起，把TCP/IP协议模型与OSI模型相比较，对TCP/IP协议集中的每一层进行了描述。本章对应于CCNA 1在线教程Module 9中的内容。

• **第8章“路由选择基础与子网”**，讨论了与因特网协议（IP）相关的话题。本章也讨论了路由选择协议和被动路由协议之间的区别，并讲述了路由器如何追踪两个位置之间的距离。最后，本章介绍了距离矢量、链路状态和混合型三种方式的路由选择协议，以及每种方式的路由选择协议如何解决路由选择的问题。本章对应于CCNA 1在线教程Module 10中的内容。

• **第9章“TCP/IP传输层与应用层”**，涵括了传输层的相关问题。讨论了传输层如何利用网络层提供的服务（例如最佳路由选择和逻辑寻址）来提供源和目的地之间的端到端连接。本章描述了传输层如何可靠和准确地对从源到目的地的流进行控制。本章对应于CCNA 1在线教程Module 11中的内容。

• **第10章“广域网与路由器”**，介绍了广域网（WAN）的设备、技术和标准。此外，还讨论了路由器在WAN中的作用。本章对应于CCNA 2在线教程Module 1中的内容。

• **第11章“路由器基础”**，描述了如何通过正确的命令和启动顺序来执行初始的路由器配置，从而在第一次使用一台路由器时可以对其进行启动。本章还解释了路由器的启动顺序；解释了在当前使用的Cisco 互联网操作系统（IOS）软件版本下，路由器用于创建初始化配置文件的设置会话（setup dialog）。本章对应于CCNA 2在线教程Module 2中的内容。

• **第12章“路由器配置”**，讨论了路由器的各种模式和更新路由器配置文件的各种配置方法。理解Cisco IOS软件并知道路由器启动的过程是非常重要的。此外，本章还描述了用于路由器密码恢复所必需的步骤。本章对应于CCNA 2在线教程Module 3的内容。

• **第13章“了解邻近和远程设备”**，介绍了如何通过正确的路由器命令来应用、监控和维护Cisco发现协议（Cisco Discovery Protocol）。此外，本章还解释了三个最常用的命令。本章对应于CCNA 2在线教程Module 4中的内容。

• **第14章“管理Cisco IOS软件”**，考察路由器启动所经历的各个阶段。本章也介绍了如何使用各种Cisco IOS 软件源选项，执行命令以加载Cisco IOS软件到路由器，管理备份文件以及升级Cisco IOS 软件。此外，本章还讨论了配置寄存器的作用，讲述了如何确定IOS文件的版本号。最后，本章描述了如何利用TFTP服务器作为软件源。本章对应于CCNA 2在线教程Module 5中的内容。

• **第15章“路由选择和路由选择协议”**，介绍了路由器在执行开放系统互联（OSI）参考模型网络层的关键的网络互联功能时的用途和所进行的操作。此外，本章讨论了路由选择协议和被路由协议的区别以及路由器如何追踪两个位置之间的距离。最后，本章介绍了距离矢量、链路状态和混合型三种路由选择方式，还详细介绍了每种方式是如何解决常见的路由选择问题的。本章对应于CCNA 2在线教程Module 6中的内容。

• **第16章“距离矢量路由选择协议”**，介绍了使路由器的路由信息协议（RIP）和内部网关路由协议（IGRP）生效的初始化配置。此外，本章描述了如何监控IP路由选择协议。本章对应于CCNA 2在线教程Module 7中的内容。

• **第17章“TCP/IP错误消息和控制消息”**，介绍了ICMP、ICMP的消息格式、ICMP错误消息的类型、引起特定ICMP错误消息的潜在原因、当今在网络上使用的各种ICMP控制消息和产生ICMP控制消息的原因等。本章对应于CCNA 2在线教程Module 8中的内容。

• **第18章“路由器故障排除基础”**，对网络检测进行了介绍。它强调要用一种结构化的方法来进行故障排除。最后，本章描述了排除路由器故障的基本方法。本章对应于CCNA 2在线教程Module 9中的内容。

• **第19章“中级TCP”**，描述了TCP/IP如何保证任何互联网络间的通信。此外，本章介绍了TCP/IP协议栈的各个组成部分，例如用于支持文件传送、E-mail、远程登录和其他应用等的协议。本章还介绍了可靠的和不可靠的传输层协议，详细分析了数据报（分组）在网络层的无连接传送。最后，解释了ARP和RARP的工作原理。本章对应于CCNA 2在线教程Module 10中的内容。

• **第20章“访问控制列表”**，包含了关于如何使用ACL的提示、要考虑的因素、建议和常规的使

用指导。本章还介绍了用于创建ACL的命令和配置。最后本章提供了标准ACL和扩展ACL的应用实例，并讲述了如何将ACL应用到路由器的端口上。本章对应于CCNA 2在线教程Module 11中的内容。

• **附录A“结构化布线”**，涵盖了结构化布线体系、标准和编号的内容。此外，本附录还包括了布线安全、布线工具、安装步骤、测试验收以及布线业务的概况方面的内容。本附录还提供了布线的学习实例，介绍如何把本章中所提到的全部内容应用到真实的场景中。本附录的内容并没有收录在在线教程中，但却提供了一些作为一名CCNA必须了解的有用信息。

• **附录B“术语表”**，给出了书中使用的关键术语的汇总列表。

• **附录C“复习题答案”**，给出了每章结尾处的测试问题的答案。

关于光盘

本书所附的光盘能帮助你进一步提高学习效果。光盘中包括了在线教程中没有的额外章节，配有CCNA模拟试题的测验引擎，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模拟。这些材料使得你不在教室也能进行学习和技能培养，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。
• 关于模拟试题的准确简明的答案。
• 学习者主导的练习和学习。
• 适合各个层次学习者的灵活性。
• 本书的术语表。

最后，这些学习工具不仅强调概念，也强调了学以致用的重要性。本光盘能帮助你理解路由和交换技术，达到理论联系实践的效果。

思科系统公司网络图标示例

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。下列的图标示例显示了你在本书中可能遇到的一些最常用的图标。



命令句法表示习惯

本书命令句法的表示习惯与Cisco IOS命令手册（Command Reference）中的表示习惯是一致的。在命令手册中对表示习惯的描述如下：

- 竖线（|）用于分隔可选的、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（比如[{ }]）表示必须在任选项中选择一个。
- **粗体字**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。

第一部分　网络技术基础

第1章　网络技术入门
第2章　网络技术基础
第3章　网络介质
第4章　线缆测试及局域网、广域网布线
第5章　以太网基础
第6章　以太网技术和以太网交换
第7章　TCP/IP协议集和IP寻址
第8章　路由选择基础与子网
第9章　TCP/IP传输层与应用层



第1章　网络技术入门

目标

学习完本章之后，你应该能够：

- 了解Internet连接的要求。
- 了解个人计算机的主要组成部分。
- 了解笔记本电脑的以太网适配器。
- 描述网络接口卡（NIC）的功能。
- 列出安装NIC所需的组件。
- 明白ping命令的功能。
- 明白Web浏览器的特点。
- 描述用来度量数字数据大小的单位。
- 把十进制数转换成二进制数。
- 把二进制数转换成十进制数。
- 把十六进制数转换成二进制数。
- 把二进制数转换成十六进制数。

本章介绍计算机和连接到因特网（Internet）的基础知识。此外，还介绍不同的数制，以及把数字从一种数制转换成另外一种数制的方法。

请务必在本书配套的光盘中查看与本章相关的e-Lab实验活动、视频和插图。这些光盘资料提供了补充材料，能够强化本章中涉及的概念。

1.1　Internet连接的基本原理

为了理解计算机在一个网络系统里面所扮演的角色，让我们来考察一下*Internet*。Internet可以被认为是一棵树，而计算机则是这棵树的叶子。在Internet中，计算机既可以是信息的发送者，也可以是信息的接收者。即使没有Internet，计算机也能正常运行；但是如果没有计算机的话，Internet就无法存在了。Internet正在快速地发展着，而用户则变得越来越依赖于它所提供的众多服务。

作为网络不可缺少的组成部分，计算机在各个领域也扮演着非常重要的角色。企业利用它们的计算机来达到各种各样的目的，同时也以一些共同的方式使用它们。例如，企业利用服务器来存储

用于管理客户和员工的重要信息，利用电子表格软件来管理财务信息，利用文字处理软件来维护记录并保持其一致性，以及利用浏览器来访问内部和外部的网站。

利用诸如电缆调制解调器（cable modem）和数字用户线（DSL）等服务，家庭和小型办公室现在已经可以实现对Internet的高速接入了，而这又使得用户对这些支持服务的需求不断增加。用户现在需要的是能够共享连接的工具，而不再仅仅满足于一台连接到Internet上的电脑了。

Internet是世界上最大的数据网络。Internet由众多互相连接的、大大小小的网络组成。在这个巨大的网络的边缘是那些单独的计算机用户。

与Internet的连接可以被分解成以下几个层次：

• ***物理连接***——通过电缆把一个专门的扩展卡（例如调制解调器或网络接口卡（NIC））与PC连接起来之后，就可以实现与网络的物理连接了。该物理连接用于本地网络内PC间的信号传输，另外还用于Internet上远程设备间的信号传输。

• ***逻辑连接***——逻辑连接使用一些被称为协议的标准。协议是一种关于一系列规则和协定的正式描述，这些规则和约定规定了网络上的设备应如何进行通信。与Internet的连接可能会用到多种协议，其中***传输控制协议/Internet协议（TCP/IP）***集则是用于Internet的最主要的协议。TCP/IP是一套协同工作的协议，通过它们可以进行数据的发送和接收。在第7章“TCP/IP协议集和IP寻址”里面，你可以学到更多关于TCP/IP的知识。

• ***应用程序***——应用程序是连接的最后一部分。它可以解释数据，并且把信息以可理解的形式显示出来。应用程序与协议一起工作，在Internet上发送和接收数据。例如，***Web浏览器***把超文本标记语言（HTML）显示为一个网页，***文件传输协议（FTP）***用于从Internet上下载文件和程序。Web浏览器也可以通过使用一些专有的插件程序来显示特定的数据类型，如视频、音频和动画。

以上的介绍可能会使Internet看起来非常简单。然而，在以后的章节里，随着对这个主题更深入的探讨，你会发现在Internet上传输数据是一项非常复杂的任务。

1.2　PC的基础知识

因为计算机是网络里面非常重要的组成部分，所以能够识别PC的主要部件并知道它们叫什么是非常重要的。你可以把PC的内部组件想象为由各种设备组成的网络——它们全部都连接在系统总线上。在某种意义上，一台PC可以说是一个微型的计算机网络。

很多网络设备（例如路由器和交换机）就是一些具有特定用途的计算机。它们的很多组成部分与普通PC是相同的。计算机要可靠地获得信息，就必须按照正确的流程工作。你应该能认出下面所描述的计算机的各个组成部分（这同样适用于笔记本电脑），叫出它们的名字，并且能说出它们的用途。

1.2.1　电子器件

电子器件用电的形式来传输数据或信号。大多数电子器件都位于主板上或插到主板的扩展卡上。下面是一些常见的电子器件：

• **晶体管**——用于放大信号或者接通、关闭电路的组件。微处理器可能含有数百万个晶体管。

• **集成电路（IC）**——由半导体材料制成的组件。它由许多晶体管组成，用于实现特定的用途。

• **电阻**——由可以阻碍电流流动的材料制成的组件。

• **电容**——以静电场的形式储存能量的电子组件。它由两块用绝缘材料分隔的金属板组成。

• **连接器**——可以插入电缆的端口或者接口。连接器包括串行口、并行口、通用串行总线（USB）和磁盘驱动器接口。

• **发光二极管（LED）**——有电流通过时会发光的半导体组件。它通常被用作指示灯。

1.2.2 PC组件

一般来说，PC组件是为PC提供额外功能的部件，它们可以是预先组装好的，也可以是附加的。这与那些必不可少的电子组件（每一台PC都需要它们）相对而言的。这些PC组件包括：存储介质驱动器、内存、硬盘驱动器、处理器和电源等。以下是一些最常见的PC组件：

• ***印刷电路板（PCB）***——置有芯片（集成电路）和其他电子组件的薄板。PCB包括主板和各种扩展适配器。

• ***光盘驱动器***——可以从光盘里读取信息的光学驱动器。它也可以是CD-RW（可读写光盘）驱动器，也可以是DVD（数字化视频光盘）驱动器，还可以是以上三者的结合。

• ***中央处理单元（CPU）***——计算机的“大脑”，绝大多数的计算都由它完成（如图1-1所示）。

• ***软盘驱动器***——可以对软盘进行读写（如图1-2所示）。



图1-1 中央处理单元

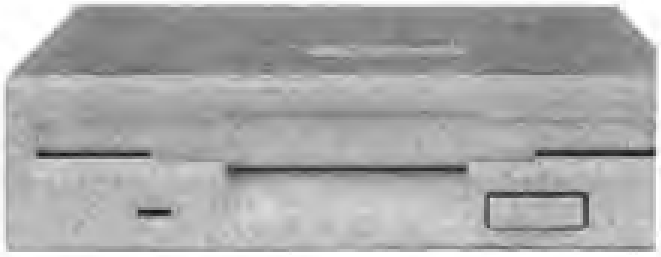


图1-2 软盘驱动器

• ***硬盘驱动器***——负责读写硬盘上的数据，是计算机的主要存储设备。

• ***微处理器***——包含有CPU的芯片。一台典型的PC有许多的微处理器，其中包括主CPU。

• ***主板***——计算机的主电路板（如图1-3所示）。由于主板是计算机的中枢系统，所以它是至关重要的。系统里面的其余一切东西都插在主板上面，由它控制，并依靠它来与系统内的其他设备通信。

• ***总线***——一组电路的集合。通过它，数据可以从计算机的一个部分传输到另一个部分。总线负责把计算机内部的所有组件与CPU连接起来。工业标准结构（ISA）和外部组件扩展接口（PCI）就是两类常见的总线。

• ***随机存取存储器（RAM）***——也被称为可读写存储器。可以把数据写到RAM里面，也可以从RAM里面读取数据。RAM是CPU进行绝大多数计算和操作的主要工作区域。RAM的一个缺点是必须使用电力来维持数据的存储。如果计算机关机或者掉电，存储在RAM里面的所有数据都会丢失——除非它们已经被预先保存到磁盘上。带有RAM芯片的内存条插在主板上。

• ***只读存储器（ROM）***——计算机存储器，上面预先记录有数据。一旦数据写到ROM芯片里面之后，就只能读取，而不能被擦除。但有一种叫做电可擦除可编程只读存储器（EEPROM）的ROM是可以写入数据的，它被称为闪存或固件。绝大多数PC里面的基本输入输出系统（BIOS）都存储在EEPROM里面。

• ***扩展插槽***——计算机的总线接口，通常在主板上。可以把扩展卡插在上面，从而为计算机增加新的功能（如图1-4所示）。

• ***系统单元***——PC系统的主要组成部分。它包括机箱、底座、电源、微处理器、主内存、总线、扩展卡、磁盘驱动器（软盘、CD、硬盘等）和各种端口。系统单元不包括键盘、显示器和其他与计



图1-3　主板

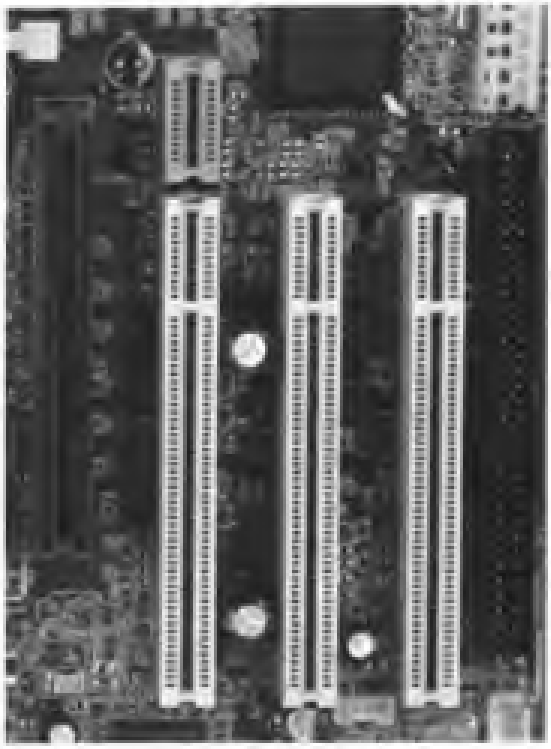


图1-4　扩展插槽

算机连接的外部设备。

- *电源*——为计算机供电。

1.2.3　主板上的组件

主板是计算机的主电路板。由于它是计算机的神经系统，所以至关重要。系统里面的其余一切都插在它上面，由它控制，并依靠它来与系统内的其他设备通信。以下是主板的各个组成部分：

- *底板*——一块大电路板，上面有一些用来插扩展卡的插槽。
- *内存芯片*——内存条上的RAM芯片，被插在主板上。
- *网络接口卡（NIC）*——一块印刷电路板。它为PC提供进行网络通信的能力。很多新近推出的桌面电脑和膝上型电脑都把以太网卡集成到了主板上。
- *视频卡*——一块插到PC里面的板，它使PC具有显示能力。视频卡（也称显卡）通常自带微处理器和内存，以便提高显示图像的速度和能力。
- *声卡*——用于处理所有声音功能的扩展卡。
- *并行端口*——可以同时传输超过1 bit的接口。它用于连接外部设备，例如打印机。
- *串行端口*——进行串行传输的接口，它一次只能传输1 bit。串行端口可以用于连接外置调制解调器、绘图仪或串行打印机。它也可以以控制台连接的方式连接网络设备，例如路由器和交换机。
- *鼠标端口*——用以将鼠标连接到PC。
- *键盘端口*——用以将键盘连接到PC。
- *电源线*——用以将电器设备连接到电源插座，以便为设备供电。
- *通用串行总线（USB）端口*——它可以使你在不重新启动系统的情况下，插拔各种外部设备（例如鼠标、调制解调器、键盘、扫描仪和打印机）。USB端口最终将会取代串行和并行端口。



实验活动　PC硬件

本实验能帮助你熟悉PC系统的各种基本的外部组件以及它们之间的连接，包括网络附件。

你将检查PC的内部结构，识别出主要的组件。你还将观察Windows操作系统的启动过程，并使用控制面板找出与PC硬件有关的信息。

1.2.4 桌面型计算机与笔记本电脑的比较

笔记本计算机正在变得越来越普及。除了笔记本电脑的组件比台式PC组件要小之外，台式PC和笔记本电脑的主要分别在于：笔记本电脑具有更大的灵活性和便携性。笔记本电脑里的扩展插槽称为*个人计算机存储卡国际协会卡（PCMCIA）*插槽，或者PC卡插槽。网卡、调制解调器、硬盘驱动器和其他设备（通常跟厚的信用卡大小差不多）可以插在PC卡插槽上。图1-5显示了一块用于无线局域网（WLAN）的PC卡适配器。



图1-5 PC卡

1.2.5 网络接口卡

如图1-6所示，网卡是一块印刷电路板，它能为PC提供进行网络通信的能力。网卡又称为局域网适配器，它插到主板上后，可以提供一个连接到网络的端口。网卡提供了计算机接入局域网的接口。



图1-6 网络接口卡

网卡通过电缆与网络通信，通过扩展插槽与计算机通信。当网卡安装到计算机里面之后，它需要一个中断请求（IRQ）来向CPU请求服务。中断请求是一个信号，它通知CPU已出现了一个需要CPU注意的事件，它是通过硬件线路传到微处理器中的。键盘上的一个键被按下就是中断产生的一个例子。CPU必须把该字符从键盘传到RAM。另外，网卡还需要一个输入输出（I/O）地址、供操作系统（例如Linux或者Windows）使用的一块内存空间和执行其功能所需的驱动程序。I/O地址是内存里面的一个存储单元。通过一个辅助设备，内存中的I/O地址用于向计算机输入数据，或者从计算机中获得数据。

在为网络选择网卡的时候，要考虑以下几点：

- **网络的类型**——对于不同的网络，使用的网卡是不同的。例如，以太网卡是设计用于LAN的。其他的网络类型包括令牌环网和光纤分布数据接口（FDDI）。目前，以太网是最常见的网络类型。
- **传输介质的类型**——对于特定类型的传输介质（例如双绞线、同轴电缆、光纤或无线），有与之对应的网卡的端口或连接器。其中，同轴电缆现在正变得越来越少见了。
- **系统总线的类型**——系统总线的类型有很多，例如PCI和ISA。由于PCI插槽的速度要比ISA插槽的速度快，所以后者现在已经被逐渐淘汰了。

1.2.6 网卡和调制解调器的安装

要连接到Internet的话，必须有一块适配器卡。这块适配器卡可以是modem或者NIC。*调制解*

*调器（modem）*是一个电子设备，计算机之间通过它可以利用电话线进行通信。它使数据能通过公共交换电话网（PSTN）从一台计算机传输到另一台计算机上。图1-7显示了一个外置modem的例子。通常modem是以字节块的形式发送数据的。每发送完一个块，modem都会进行一些基本的数学运算去分析它，并询问接收端的计算机是否同意这个结果。如果有任何不一致的情况出现，这个块就会重传。发送端的modem先把数字信号转换成模拟信号，然后再把数据发到PSTN上；接收端的modem则把接收到的模拟信号重新转换成数字信号。



图1-7　外置调制解调器

调制解调器（modem）这个名词来源于该设备的用途。把数字信号转换成模拟信号的过程称为调制（modulation），其反过程称为解调（demodulation），因此就有了调制解调器这个名词。Modem可以安装在计算机的内部，也可以在外部通过串行口或USB接口与计算机连接。Modem把计算机与网络相连的方法是：拨打另一台计算机的modem的电话号码——这通常是Internet服务提供商（ISP）的电话号码。

网卡可以使主机连接到网络，因此它被认为是一个关键的组件。网卡有很多类型，这要视具体的设备结构而定。例如，笔记本计算机可以使用内置的接口，或者是一块PCMCIA卡；而台式计算机则可以使用集成的网卡或适配器卡。

下面列出了一些需要进行网卡安装的情形：

- 为一台没有网卡的PC安装网卡。
- 替换一块有问题或损坏了的网卡。
- 从10兆比特每秒（10Mbit/s）的网卡升级到10/100Mbit/s的网卡。

如图1-8所示，要安装网卡，需要具备以下条件：

- 有关网卡配置的知识，包括跳线和即插即用软件。现在绝大多数的网卡都不需要跳线了。它们都是即插即用的，只需要很少的配置，甚至不需要进行配置。当然，如果有必要的话，可以通过网卡附带的软件对其进行配置。
- 网卡诊断软件的使用，包括厂商提供的诊断软件和回环测试（请参考网卡的文档资料）。
- 解决硬件资源冲突的能力，包括IRQ、I/O基地址和直接内存访问（DMA）。DMA可以使数据从RAM直接传输到设备中，而不需要经过CPU。



图1-8　安装网卡

1.3　高速拨号连接概述

上个世纪60年代初期，调制解调器的发明提供了从哑终端到主机的数据通信连接。由于购置一台主机系统的成本太高，所以很多公司都只是租用计算机机时。当时的连接速率非常低——只有300比特每秒（bit/s），相当于每秒钟传输30个字符左右。

上个世纪70年代，随着PC的价格下降到了可以接受的程度，电子公告板系统（BBS）出现了，它使用户可以连接到一块讨论板上进行信息的粘贴或读取。当时300bit/s的速度还是可以接受的，因为它超过了人们读写的速度。到了上个世纪80年代初，BBS才开始被广泛使用，而人们又开始希望

能进行文件和图像的传输了。因此，300bit/s的速度很快变得难以忍受了，于是调制解调器的速度开始增加。到了上个世纪90年代，调制解调器的速度达到了9600bit/s。到1998年，调制解调器的速度达到了现在的水平——56kbit/s（即56000bit/s）。

后来，本来在企业环境里使用的高速服务，例如DSL和cable modem，都迁移到了个人消费市场上。这些服务不再需要昂贵的设备或者额外的一条电话线。同时，它们是*永远在线*（*always-on*）的服务，因此能够提供即时的接入，而无须在每次会话进行的时候都建立连接。这提供了很高的可靠性和很大的灵活性，也使得Internet、小型办公室和家庭网络间的连接共享变得更容易了。

1.4 TCP/IP配置

TCP/IP是一组协议或规则，它使得跨越网络协同操作的计算机之间可以共享资源。为了访问Internet，计算机必须运行TCP/IP协议集。为了在工作站上启用TCP/IP，必须利用操作系统的工具来对它进行配置。PC需要IP地址、子网掩码、默认网关以及域名系统（DNS）信息。这些信息可以手动配置，也可以从动态主机配置协议（DHCP）服务器上获得。在PC机上配置TCP/IP所必需的信息通常都是从网络管理员或ISP那里获得。不管是使用Windows操作系统还是使用Apple Macintosh操作系统，配置过程都是类似的。TCP/IP、DHCP和DNS会在后续的章节中提到。



实验活动 PC TCP/IP网络设置

本实验将向你介绍发现计算机的网络连接、主机名、介质访问控制（MAC）地址（第2层）以及网络地址（第3层）的方法。

1.5 用Ping测试连通性

*Ping*是一个很有用的程序，它用于检验TCP/IP是否成功安装。Ping是以声纳探测命名的，它是用来对水下的物体进行定位和距离测量。Ping的意思是分组因特网探测器（Packet Internet Groper）。

Ping命令通过向某一特定目的地发送多个IP分组来实现。每一个发送出去的分组都会请求目的地作出应答，返回的应答响应中包含到达目的地的成功率和往返时间，根据这些信息就可以断定是否与目的地连通。Ping命令可以用来测试NIC的收发功能、TCP/IP的配置以及网络连通性。Ping命令的一些用法如下：

- ping 127.0.0.1（内部回环测试）——检验TCP/IP栈的操作、NIC的收发功能。图1-9显示了ping 127.0.0.1的测试结果。



图1-9 ping 127.0.0.1

- ping*主机的IP地址*——检验本地主机的TCP/IP地址配置。
- ping*默认网关IP地址*——检验连接本地网络和其他网络的路由器是否可达。
- ping*远端目的地的IP地址*——检验与远端主机的连通性。



实验活动　使用ping和tracert

在本实验中，你将学习使用TCP/IP的ping和tracerout命令来测试网络的连通性。在这一过程中，如果该IP还有对应的名字的话，还会出现名字解析。

1.6　Web浏览器和插件

Web浏览器能为用户实现如下功能：

- 连接Web服务器。
- 请求信息。
- 接收信息。
- 在屏幕上显示结果。

Web浏览器是一种能解析***超文本标记语言（HTML）***的软件。HTML是能用来对Web页面内容进行编码的众多语言中的一种。其他标记语言，如标准通用标记语言（SGML）和扩展的标记语言（XML），在创建动态、交互式Web页面方面，能比HTML提供更高级的特性。HTML——最普遍使用的标记语言——能够显示图形，播放声音、电影和其他多媒体文件。***超级链接（Hyperlinks）***是计算机程序命令，它指向同一文档的其他部分或Web服务器上的其他HTML文件，从而提供了一种访问其他Web页面和文件的捷径。最为流行的两种Web浏览器是Internet Explorer（IE）和Netscape。尽管它们所实现的功能都是相同的，但是它们之间仍然有一定的差别。有些Web站点可能不支持这两种的某一种，因此在计算机上同时安装这两种程序是有好处的。

表1-1比较了这两款浏览器的特性。

表1-1　Microsoft Internet Explorer与Netscape Communicator的比较

IE	Communicator
与其他Microsoft产品整合在一起	最先流行的浏览器
占用较多的磁盘空间	占用较少的磁盘空间
能显示HTML文件，实现e-mail、文件传输及其他功能	能显示HTML文件，实现e-mail、文件传输及其他功能

标准Web浏览器无法显示许多特定的或专有的文件类型。为了打开这些文件，浏览器必须配置使用***插件（plug-in）***应用程序。通过与浏览器一起工作，这些应用程序能够启动观看这些特定文件所需的程序。下面是一些比较流行的专有的插件：

- Flash Player/Shockwave Player——用来播放由Macromedia Flash制作的多媒体文件的插件。
- Adobe Acrobat Reader——允许用户浏览和打印Adobe的便携式文档格式（PDF）文件的软件。
- Windows Media Player——允许用户播放音频和视频文件的软件。
- Quicktime——由苹果（Apple）公司开发的允许用户播放视频和音频文件的软件。
- RealPlayer——允许用户播放音频文件的软件。



实验活动　Web浏览器基础

在本实验中，你将会学习如何使用Web浏览器来访问Internet站点，熟悉统一资源定位符（URL）的概念，以及用搜索引擎在Internet上查找信息。你还将通过访问选定的Web站点来学习网络术语的定义，以及使用超级链接从当前Web站点跳转到另一Web站点。

1.7 其他常用的计算机应用程序

计算机能执行许多其他有用的任务。譬如，在企业中，员工通常会使用一套办公软件包（如Microsoft Office和Lotus Smart Suite）形式的应用程序。办公用的应用程序通常包括下面几种：

- **电子制表软件**——能让用户制作由行和列组成的电子表格的应用程序。它通常使用公式来处理和分析数据。
- **字处理软件**——能让用户创建和编辑文本文档的应用程序。现在的字处理软件都允许用户创建复杂的文档。这些文档中包含图形和多种多样格式的文本。
- **数据库软件**——能让用户存储、维护、组织、分类和过滤记录的应用程序。记录是一组由共同的主题（如客户名）所标识的信息的集合。
- **演示文档软件**——能够让用户设计演讲稿以便在会议、上课和销售中发表演讲的应用程序。
- **个人信息管理程序**——包含诸如e-mail、联系方式列表、日历以及将要做的事情的列表等内容的应用程序。



实验活动 基本的PC/网络故障排除过程

在本实验中，你将在简单和常见的网络问题上运用基本故障排除模型。你还将熟悉更为常见的硬件和软件问题。

1.8 二进制数

本节介绍数据在计算机内部的表现形式和在网络上传输的格式，以及与计算机相关的几种数制和逻辑。

1.8.1 数据的二进制表示

计算机是由电子开关组成的机电设备。在计算机硬件执行运算的时候，计算机依靠这些电子开关进行处理，因此计算机只对电脉冲作出反应。这些脉冲代表“开（on）”或“关（off）”的状态（1或0）。

计算机利用电子开关（on或off）来对数据进行操作和存储。计算机只能理解并使用这种二进制格式的数据，“1”表示“on”，“0”表示“off”。这些“1”和“0”表示计算机的电子组件的两种可能状态，它们称为二进位或比特（bit）

美国信息交换标准码（ASCII）是计算机中表示字符数据最常用的编码方式，它用二进制数表示键盘上的字符。计算机通过网络、电、光及无线电波发送“on/off”状态来表示“1”或“0”。每一字符用一个与之对应的8位二进制数的编码来表示。

1.9 比特、字节和度量单位

比特是二进制数，它们可能是0，也可能是1。在计算机里面，它们用电子开关的通断，电荷、光脉冲和电磁波的有无来表示。

例如：

- 二进制数0用0V电压表示（0=0V）。
- 二进制数1用+5V电压表示（1=+5V）。

计算机把8bit归为一组，这样的8bit称为1字节。在计算机内部，1字节表示一个单独的可寻址存储单元。这些存储单元表示一个数值或者一个字符，例如用ASCII码表示的字符。8个开关通断组合可以表示256（即2^8）个不同的值，所以一个字节可以表达的数值范围是0到255。字节是使用计算机

和网络时所必须理解的一个重要概念。

大多数计算机用8个比特来表示一个数字、字母或者符号。这样的8个比特称为1字节；一个字节对应一个存储单元（见表1-2）。

表1-2　信息单元

Unit	bytes*	bits*
bit（b）	1/8 byte	1bit
byte（B）	1byte	8bit
Kilobyte（KB）	1000 byte	8000bit
Megabyte（MB）	100万byte	800万bit
Gigabyte（GB）	10亿byte	80亿bit
Terabyte（TB）	1万亿byte	8万亿bit

* 表示约等于的字节数或者比特数

注释：KB和Kb、MB和Mb常常会产生混淆。在比较传输速度的时候要注意KB和Kb之间的转换。例如，调制解调器的软件通常以kbit/s为单位来标称连接速度（例如，45kbit/s），而常用的浏览器却用kB/s来显示下载速度。这就是说，一个45 kbit/s的连接，最大的下载速度是5.76kB/s。实际上，由于其他因素消耗了一定的带宽，这个下载速度是无法达到的。此外，文件大小通常以字节来衡量，但是LAN的带宽和WAN的连接却常常用千比特每秒（kbit/s）或者兆比特每秒（Mbit/s）来表示。用文件大小的字节数乘以8就可以得到在传输中所消耗的用bit/s计算的带宽。

以下是计算机常用的度量单位：

• *bit*——计算机最小的数据单位，1比特等于1或者0，是计算机处理、存储、传输数据时使用的二进制格式。

• *byte*——用于描述数据文件大小、磁盘或者其他存储介质空间的容量或者通过网络传输的数据量的单位，1字节相当于8比特。

• *kb（kilobit）*——大约1000比特。

• *kB（kilobyte）*——大约1000字节（精确值为1024字节）。

• *Mb（megabit）*——大约100万比特。

• *MB（megabyte）*——大约100万字节（精确值为1,048,576字节）。megabyte有时记作“meg.”。大多数个人电脑使用MB来计算内存大小，大文件有时也用MB来度量大小。

• *GB（gigabyte）*——大约10亿字节。Gigabyte有时记作“gig.”。大多数的个人电脑使用GB来度量硬盘大小。

• *TB（terabyte）*——大约1万亿字节。一些高端计算机使用TB来度量硬盘大小。

• *kbit/s（kilobits per second）*——1000比特每秒。它是计算通过网络连接传输的数据量的标准单位。

• *kB/s（kilobytes per second）*——1000字节每秒。它是计算通过网络连接传输的数据量的标准单位。

• *Mbit/s（megabits per second）*——100万比特每秒。它是计算通过网络连接传输的数据量的标准单位。基础以太网工作带宽为10Mbit/s。

• *MB/s（megabyte per second）*——100万字节每秒。它是计算通过网络连接传输的数据量的标准单位。

• *Gbit/s（gigabits per second）*——10亿比特每秒。它是计算通过网络连接传输的数据量的标准单位。10G或者10吉比特以太网工作带宽为10Gbit/s。

• *Tbit/s（terabits per second）*——1万亿比特每秒。它是计算通过网络连接传输的数据量的标准单位。一些核心路由器和交换机工作带宽超过1Tbit/s。

• *Hz（hertz）*——频率单位。声波、交流电及其他循环波形的状态转换速度或周期。1Hz表示一秒钟一个循环。

• *MHz（megahertz）*——兆周每秒。它是描述计算机微处理器等处理芯片速度的一个常用单位。许多无线电话工作在这个频段（例如900MHz）。

• *GHz（gigahertz）*——吉（1 000 000 000）循环每秒。它是描述计算机微处理器等处理芯片速度的一个常用单位。许多无线电话和无线LAN工作在这个频段（例如802.11b工作在2.4GHz）。

注释： PC处理器的处理速度在不断提高。在20世纪80年代PC机使用的微处理器工作频率不到10MHz（最初的IBM PC是4.77MHz）。现在，PC处理器的处理速度已经接近3GHz，将来的处理器还会更快些。

因为计算机设计成利用通断开关进行工作，所以使用二进制数字和二进制数码是很自然的事情。然而，在日常生活中，人们使用的是十进制数，而很难像计算机一样去记住一大串1或者0。因此计算机使用的二进制数需要转化成十进制数。

二进制数有时需要转换成十六进制（hex）数，因为十六进制数可以用较少的十六进制位表示一大串二进制数字，易于记忆和操作。

1.9.1 十进制

数制包括符号和使用这些符号的规则。在实际中存在多种数制。最常用的一种是十进制，或者说是基于10的基数制。由于使用10个符号，因此它被称为十进制。这十个符号是数字0、1、2、3、4、5、6、7、8和9。利用这些数字可以表示所有的数值，如表1-3所示。

表1-3 十进制数

符号个数	10			
符号	0、1、2、3、4、5、6、7、8、9			
底指数	10^3	10^2	10^1	10^0
位值	1000	100	10	1
例子：2,134	$2*10^3$	$1*10^2$	$3*10^1$	$4*10^0$

十进制数用基于10的幂来运算。从右到左的每一列数位表示的值都可以通过10（底数）的一个幂（指数）来得到。这个幂取决于它相对于小数点的位数。从右到左读入一个十进制数时，第一个（也就是最右边的一个）数位表示10^0（1），第二个数位表示为10^1（10*1=10），第三个数位表示为10^2（10*10=100）……第七个数位表示为10^6（10*10*10*10*10*10*10=1,000,000）。这样的算法适用于所有的数位。

例如：

2134=（$2*10^3$）+（$1*10^2$）+（$3*10^1$）+（$4*10^0$）

这个例子给出了十进制的用法。在这个数字中，它的个位是4，十位是3，百位是1，千位是2。了解十进制数的工作机制有助于理解二进制数（基数为2）和十六进制数（基数为16），它们都使用和十进制相同的工作机制。为了便于阅读理解，IP地址都是写成十进制数形式的。IP地址172.16.14.188就是由四个由点号隔开的十进制数组成的。

1.9.2 二进制

计算机使用***二进制***，即基数为2的基数制，来识别和处理数据。二进制数使用两个符号（0和1）代替了十进制数（基数为10的基数制）所使用的十个符号。在二进制数中，每个位置都表示不同的

2的幂次，幂的次数由它所在的位置决定（2^0、2^1、2^2、2^3、2^4，如此类推），如表1-4所示。

表1-4　二进制数

符号个数	2							
符号	0、1							
基指数	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
位值	128	64	32	16	8	4	2	1
例子：10110	0	0	0	1	0	1	1	0

例子：

10110=（$1*2^4$=16）+（$0*2^3$=0）+（$1*2^2$=4）+（$1*2^1$=2）+（$0*2^0$=0）

=（16+0+4+2+0）=22

如果二进制数10110从左往右读读，那么它有1个16、0个8、1个4、1个2和0个1，加起来就是22。机器可识别的IP地址用一串32位的二进制数表示。

1.9.3　十六进制

基数制16或十六进制数比二进制数更方便读取，因此在计算机中得到广泛应用。计算机使用二进制数进行计算，但是常常使用十六进制数输出以便于读取。十六进制数采用16个符号，通过它们的组合可以表示所有的数字。因为只有10个符号（0、1、2、3、4、5、6、7、8和9）表示数字，十六进制数还要采用6个其他符号来表示，它们是字母A、B、C、D、E和F。A表示十进制数10，B表示11，C表示12，D表示13，E表示14，F表示15，如表1-5所示。

表1-5　十六进制数

符号个数	16			
符号	0、1、2、3、4、5、6、7、8、9、A、B、C、D、E、F			
基指数	16^3	16^2	16^1	16^0
位值	65536	256	16	1
例子：1A2C	1	A	2	C

在十六进制数中，每位数都表示以16为底数的幂，幂的次数由它所在的位置决定。从右到左，第一位表示16^0（即1），第二位表示16^1（即16），第三位表示16^2（即256），如此类推。网络适配器和NIC地址通常用一串12位的十六进制数表示。

例子：

1A2C=（$1*16^3$=65536）+（10（A）$*16^2$=2560）+（$2*16^1$=32）+（12（C）$*16^0$=12）

=（65536+2560+32+12）=68144

1.9.4　十进制数到二进制数转换

实现十进制数到二进制数的转换有几种方法。图1-10的流程图描述了其中一种方法，这种方法推算出2的幂的组合，使之相加与待转换的十进制数相等。转换方法有许多，读者可以选择其中一种方法并且熟练掌握。

以下是一个例子：

十进制数168转换成二进制数的步骤如下：

步骤1：128比168小，因此二进制数最左边的一位是1，168-128=40。

步骤2：64比40大，因此二进制数第二位是0。

步骤3：32比40小，因此二进制数第三位是1，40-32=8。

步骤4：16比8大，因此二进制数第四位是0。

步骤5：8等于8，因此二进制数第五位是1，余数为0，二进制数其他位为0。

步骤6：结果是，与十进制数168等价的二进制数为10101000。

作为练习，请把十进制数255转换为二进制数。结果是11111111。

这个流程图只适用于不大于255的十进制数，对应于八位的二进制数，它适用于IP地址转换。对于更大的数，只需在左边加入位，每个新位的权值是前一个位的2倍。例如650的转换可以从512开始推算，其结果是一个十位的二进制数。

实验活动 十进制到二进制转换

通过这个练习，你可以练习把十进制数转换为二进制数。

1.9.5 二进制到十进制的转换

正如十进制数到二进制数转换一样，二进制数到十进制数转换也不止一种方法，图1-11的流程图是其中一个例子。

二进制数可以通过二进制数字乘以基数（基数为2）的幂转化为十进制数，幂的次数由对应数位的位置决定。

以下是一个例子：

转换二进制数01110000到十进制数。

$$
\begin{aligned}
& 0*2^0=0 \\
+\ & 0*2^1=0 \\
+\ & 0*2^2=0 \\
+\ & 0*2^3=0 \\
+\ & 1*2^4=16 \\
+\ & 1*2^5=32 \\
+\ & 1*2^6=64 \\
+\ & 0*2^7=0 \\
\hline
& 112
\end{aligned}
$$

（对应位值为1的幂值的和）。

注释：从右向左转换，任何数的0次幂是1，因此$2^0=1$。

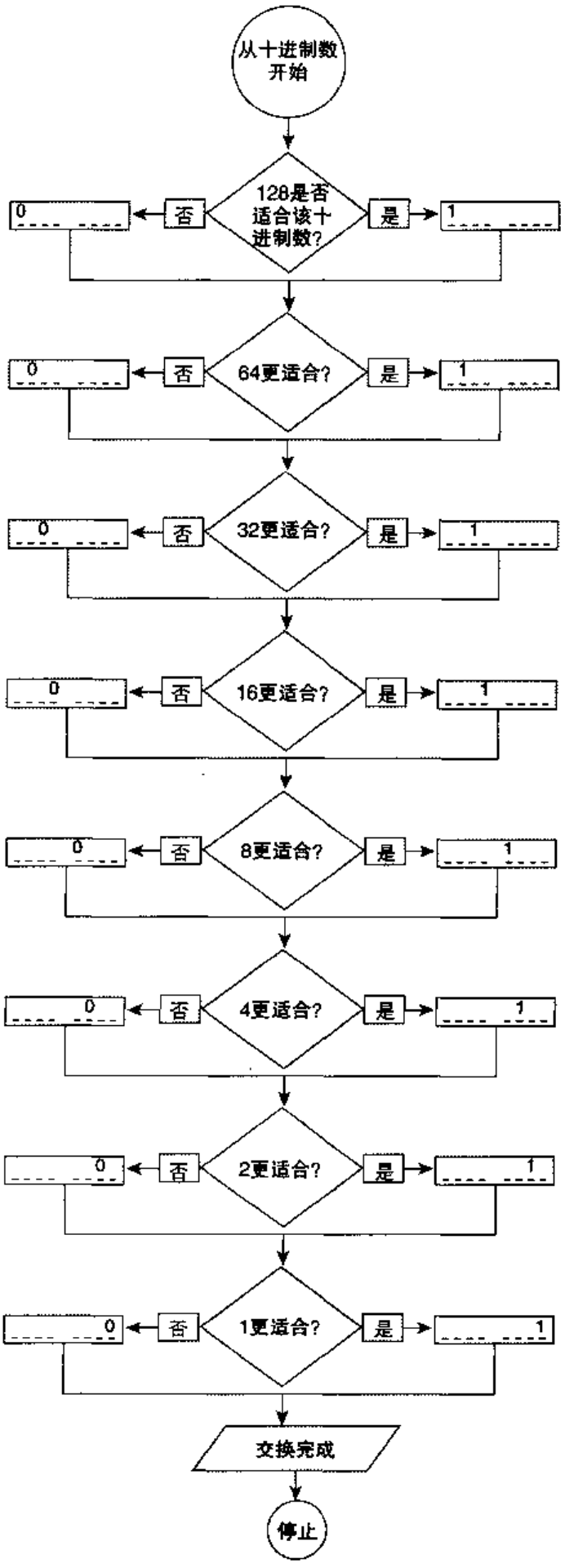


图1-10 十进制数到二进制数的转换过程

和图1-10中的流程图一样，图1-11的流程图也只适用于不大于255的十进制数，对应于8位的二进制数。更大的二进制数可以右边每一位增大2的一次幂来转换。例如，要转换十位的二进制数，如果对应位有效（数值为1），第10位二进制数等价于512，第9位二进制数等价于256。

实验活动　二进制到十进制转换

通过这个练习，你可以练习把二进制数转换为十进制数。

1.9.6　十六进制数和二进制数转换

Cisco路由器进行寄存器配置时，经常要用到十六进制数和二进制数相互转换。Cisco路由器有一个16比特长的配置寄存器，它可以转换成4位的十六进制数。例如，二进制数0010000100000010等于十六进制数2102。

第2层*介质访问控制（MAC）地址*通常用十六进制记录。以太网和令牌环网中，这些地址长度为48比特，也就是6个*octet*（一个octet即一个字节）。（"Oct"源于希腊语中8的单词。）由于这些地址包含了6个字节，因此可以用12个十六进制数表示。每4个比特对应一个十六进制数字（$2^4=16$），如表1-6所示。

二进制数：

10101010.11110000.11000001.
11100010.01110111.01010001

可以表示为较短的等价的十六进制数：

AA.F0.C1.E2.77.51

为了更便于处理这些十六进制数，可以每4个十六进制数采用句点隔开，例如AAF0.C1E2.7751。

计算机和软件输出十六进制数的时候常常以0x开头，因此，看到0x的时候就可以认为紧跟后面的数字是十六进制数。例如0x1234表示16进制的数1234。

与二进制和十进制一样，十六进

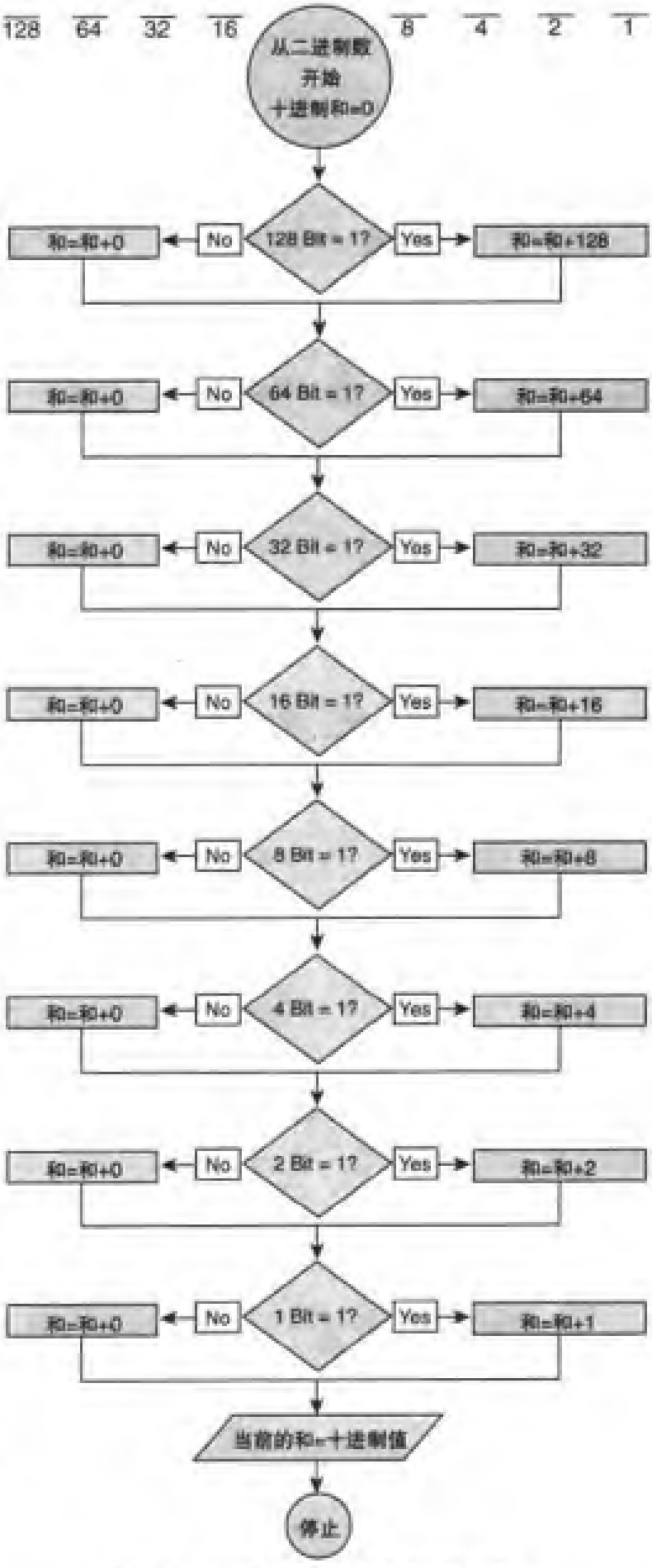


图1-11　二进制数到十进制数的转换过程

制也是基于符号、乘方和数位来使用的。十六进制数使用0到9以及A到E，表1-6显示了与十六进制数码等价的二进制数和十进制数。

表1-6 与十六进制数码等价的二进制数和十进制数

二进制	十六进制	十进制
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

十六进制转换成二进制，每个十六进制数字转换成4位二进制数。例如，转换十六进制数AC（0xAC）为二进制数，首先转换A（即二进制数1010），接着转换C（即二进制数1100），则十六进制数AC对应二进制数10101100。

4个二进制数字的组合对应1位十六进制数，但是对应着2位十进制数。8个二进制数字的所有组合仅需要2个十六进制数字表示（如果用十进制表示，需要4位），这是使用十六进制的原因。此外，使用两个十进制数表示4比特在阅读上会引起误会。例如，8位的二进制数01110011转换成十进制数是115。那么它是表示11-5还是1-15呢？如果看作11-5，对应的二进制数应当是10110101，不等于最初要转换的二进制数。如果使用十六进制数，转换结果是1F，再次转换回二进制数仍旧是00011111。

十六进制数可以看作是二进制数的速记形式，它把8位的数字缩短为2位的十六进制数字，减少了长数字的混乱和书写空间。此外，十六进制数常常会加上0x的缩写，如十六进制数5D会写作0x5D。

十六进制数转换成二进制数，只需要把每一个十六进制数字转换成4比特的二进制数字即可。

实验活动 十六进制转换

通过这个习题，可以练习将十六进制数转换成十进制数和二进制数。

1.9.7 32比特二进制数的四字节点分十进制数表示

现在，Internet上的计算机地址（IP地址）都是32比特的二进制数字。为了便于使用，这些32比特的二进制数字会分割成一系列的十进制数字。首先，将二进制数分割为4组，每组8个比特，然后把这些8比特（一个八位组）转化为对应的十进制数。这种转换已经在“二进制到十进制的转换”这一节中介绍过。

书写的时候，这样的4个十进制数常常会用句点隔开，例如10.15.129.201，称为***点分十进制表示***，它是32位地址的紧凑形式，易于记忆。这种表示方法在后面的教程中会频繁使用，所以必须掌握。当转换这些点分十进制数到二进制数时，要记住这些一位到三位的十进制数对应八位的二进制数，当要转换的十进制数小于128的时候，要在等价的二进制数最左边补0，以得到八位的二进制数。

例如，当转换点分十进制数10.15.129.201到等价的二进制数时，结果应当写作00001010.00001111.10000001.11001001。

1.9.8　布尔逻辑

布尔逻辑起源于数字电路，它描述了通过两个输入的电压得到一个输出电压的概念。在计算机应用中，不同的电压用接通和断开两种状态表示。这两种状态依次用1和0表示，也就是二进制中的表示方法。

布尔逻辑是一种二进制逻辑，通过对比两个数字，然后根据它们来做出处理。这些处理包括与运算、或运算和非运算。除了非运算之外，其他的布尔运算具有同样的运算形式，即输入两个数字（1或0），根据逻辑规则得出结果。

这一小节介绍各种运算。首先介绍的是非运算，下一小节将给出一个网络中直接使用布尔逻辑的例子——子网掩码。这个例子使用的是与运算。

如表1-7所示，非运算只是将所输入的值（0或者1）取反，即1变成0，0变成1。有专门的逻辑电路来实现这种运算，它们遵从以下规则：无论什么输入，输出其相反数。

表1-7　非运算

输入	输出
0	1
1	0

如表1-8所示，与运算需要两个输入值。如果两个输入值都是1，逻辑门输出1；其余情况，输出0。输入值有四种组合，其中三种组合输出为0，一种组合输出为1。与运算在IP寻址和子网掩码中使用十分广泛。

表1-8　与运算

与运算	0	1
0	0	0
1	0	1

如表1-9所示，或运算也需要两个输入值。如果其中有一个或两个值为1，则输出是1。和与运算一样，输入值有四种组合，但是有三种组合输出为1，只有一种输出为0。

子网掩码和通配符掩码这两个网络操作都使用布尔逻辑。网络中的设备用地址来标识，掩码可以对地址进行过滤，它可以对地址进行分类，并提供给其他网络操作使用。

表1-9　或运算

或运算	0	1
0	0	1
1	1	1

1.9.9　IP地址和子网掩码

Internet上使用的32比特地址称为*Internet协议（IP）*地址。这一节介绍IP地址和子网掩码之间的关系，更多关于IP地址的知识参见第7章。

当IP地址分配给计算机的时候，32比特的IP地址最左边的若干位表示网络，具体位数由这个IP的类型决定。IP地址其余部分标识网络中的一部计算机，这样的一部计算机称为主机。因此计算机的IP地址包括网络号和主机号，标识特定网络里面的特定主机。

计算机通过另外的一个称为***子网掩码***的32比特二进制数字来分开IP地址。子网掩码定义了构成IP地址的32位中的多少位用于标识网络。子网掩码对应网络号的位为1，其他标识主机号的位为0。以下是几个子网掩码的例子：

例子1：

11111111.00000000.00000000.00000000，点分十进制表示是：255.0.0.0。

例子2：

11111111.11111111.00000000.00000000，点分十进制表示是：255.255.0.0。

在第一个例子里面，最左面的8位表示网络地址，其余24位表示主机地址。在第二个例子中，左边的16位表示网络地址，其余的16位表示主机地址。

IP地址10.34.23.134转换为二进制是：

00001010.00100010.00010111.10000110

为了确定IP地址的网络号，可以将32位的IP地址和子网掩码对应位作与运算。子网掩码和IP地址的组合中，两个0的结果是0，一个1和一个0的结果是0，两个1的结果是1。更具体的例子如下：

例子1：第一个子网掩码为255.0.0.0

00001010.00100010.00010111.10000110：IP地址

11111111.00000000.00000000.00000000：子网掩码

因此IP地址的网络号是00001010.00000000.00000000.00000000。用点分十进制表示，网络号是10.0.0.0。

例子2：第二个子网掩码为255.255.0.0

00001010.00100010.00010111.10000110：IP地址

11111111.11111111.00000000.00000000：子网掩码

因此IP地址的网络号是00001010.00100010.00000000.00000000。用点分十进制表示，网络号是10.34.0.0。

子网掩码在IP寻址中有重要的作用，现在只需要理解子网掩码的概念就可以了。

1.10 总结

本章学习了以下知识点：

- 计算机是网络的重要组成部分，掌握计算机知识越多，越容易理解网络。
- 了解计算机工作原理，便于理解网络。
- TCP/IP是Internet协议。
- Ping命令是测试网络连通性的简单方法。
- 软件是人和硬件之间的桥梁，Web浏览器和电子邮件是最常用的软件程序。
- 检修PC错误是使用网络的必要技能。
- 熟悉计算机部件和网卡的作用十分重要。学会安装网卡也同样重要。
- 比特是二进制数，8比特称为1个字节。
- 计算机使用二进制来识别和处理数据，二进制数字有0和1。
- 在高层次的计算中常常会使用十六进制，十六进制使用十六个符号：0、1、2、3、4、5、6、7、8、9、A、B、C、D、E和F。
- 布尔逻辑是基于两个二进制输入值的二进制运算，包括与运算、或运算和非运算。
- IP地址是Internet中使用的32比特的地址。

为了补充你在本章所学的知识，请参考本书配套光盘中对应章节的视频、插图和e-Lab实验。

1.11　关键术语

美国信息交换标准码（*American Standard Code for Information Interchange*，*ASCII*）　最常用的计算机文字数字表示代码，使用二进制数表示键盘上的符号。

应用程序（*application*）　是网络连接的终端，解释数据并显示为可理解的信息。应用程序利用协议通过Internet发送和接收数据。

底板（*backplane*）　有许多扩展板卡插槽的电路板。

二进制（*binary*）　以1和0表示的计数系统（1=开，0=关）。

比特（*bit*）　计算机中最小的数据单位。1比特可以是1，也可以是0。计算机采用二进制格式处理、存储、传输数据。在计算机里面，比特用电子开关的通断，电荷、光脉冲和电磁波的有无表示。

布尔逻辑（*Boolean logic*）　是计算机对二进制数值的操作。布尔逻辑可以描述存储单元的电磁充放电状态和电路的通断情况（1表示通，0表示断）。计算机通过与运算或者或运算得到运算结果给后面的处理使用。

总线（*bus*）　数据通过这样的一组电路可以从计算机的一个部分传送到另外一个部分。

字节（*byte*）　用于描述数据文件大小、磁盘或者其他媒质的存储空间大小、通过网络传输的数据量大小的量度单位。一个字节相当于8比特的数据。

CD-ROM驱动器（*CR-ROM drive*）　可以从CD-ROM中读取数据的光学设备。

中央处理单元（*central processing unit*，*CPU*）　计算机的“大脑”，进行最多计算的部分。

点分十进制符号（*dotted-dicimal notation*）　根据法则，32比特的整数写成4个用句点分隔开的八比特的十进制数字，用于表示Internet上的IP地址，例如192.67.67.20。

扩展插槽（*expansion slot*）　计算机的一个开口，通常在主板上。扩展板卡插入扩展插槽之后可以为计算机提供新的功能。

文件传输协议（*File Transfer Protocol*，*FTP*）　应用协议，是TCP/IP协议集的一部分，用于在网络主机间传输文件。

软盘驱动器（*floppy disk drive*）　用于读写软盘。

吉比特（*gigabyte*，*GB*）　大约1古字节。Gigabyte有时记作“gig.”。大多数的个人电脑使用GB来度量硬盘大小。

吉比特每秒（*gigabits per second*，*Gbit/s*）　它是计算通过网络连接传输的数据量的标准单位。10G或者10吉比特以太网工作带宽为10Gbit/s。

硬盘驱动器（*hard disk drive*）　用于读写硬盘，是计算机里面的主存储体。

超级链接（*hyperlink*）　计算机程序命令，用于连接Web服务器上另外的HTML文件或者本文件里面的其他部分，是到其他Web或者文件的快捷方式。

超文本标记语言（*Hypertext Markup Language*，*HTML*）　一种简单的超文本格式语言，它使用各种标记说明用于观看的应用程序（如Web浏览器）应如何解释文档的各个部分。

Internet全球最大的互联网络，由全球范围内上万个网络连接而成，并且包含了一种文化，这种文化集中在基于现实生活的研究和标准化。

Internet协议（*Internet Protocol，IP*） 是TCP/IP集中的网络层协议，提供无连接的互联网服务。

千比特（*kilobit，Kb*） 大约1000比特。

千字节（*kilobyte，KB*） 大约1000字节（精确值为1024字节）。

千比特每秒（*kilobits per second，kbit/s*） 它是计算通过网络连接传输的数据量的标准单位。

千字节每秒（*kilobytes per second，kB/s*） 它是计算通过网络连接传输的数据量的标准单位。

键盘端口（*keyboard port*） 用于将键盘连接到计算机。

逻辑连接（*logical connection*） 通过标准（即协议）建立

兆比特（*megabit，Mb*） 大约1兆比特。

兆字节（*megabyte，MB*） 大约1兆字节（精确值为1,048,576 字节）。megabyte有时记作“meg.”。大多数个人电脑使用MB来计算内存大小。大文件有时也用MB来度量大小。

兆比特每秒（*megabits per second，Mbit/s*） 它是计算通过网络连接传输的数据量的标准单位。基础以太网工作带宽为10Mbit/s

兆字节每秒（*megabyte per second，MB/s*） 它是计算通过网络连接传输的数据量的标准单位。

介质访问控制地址（*MAC address*） 连接LAN的每个设备需要的标准的数据链路层地址。网络中的其他设备用这些地址来确定网络中的特定端口并建立、更新路由表和数据结构。MAC地址的长度为6字节并由IEEE控制。

存储器芯片（*memory chips*） 主板上内存条上的RAM芯片。

微处理器（*microprocessor*） 一种包含CPU的硅制芯片。

调制解调器（*modem*） 转换数字信号和模拟信号的设备。在源端，调制解调器把信号转换成适于传输的形式在模拟线路上传输，在目的端，模拟信号被还原成数字形式。

主板（*motherboard*） 计算机主板。

鼠标端口（*mouse port*） 用于计算机连接鼠标。

网络接口卡（*network interface card，NIC*） 一种印刷电路板，可以为计算机提供网络通信能力。

八位组（*octet*） 在网络中，经常使用octet这个词（而不是byte），因为一些机器结构使用的字节长度不是8位。

并口（*parallel port*） 通过并口，可以同时传输超过一个比特的数据，很多外设，例如打印机，通过并口连接

个人计算机存储卡国际协会（*Personal Computer Memory Card International Association，PCMCIA*）它为信用卡大小的设备（PCMIA卡或PC卡）建立了标准，这个标准最早是为了提计算机扩展存储器设计的，现在已经得到扩展，适用于很多类设备。

物理连接（*physical connection*） 通过特制的扩展卡（例如调制解调器，网卡等）和电缆连接到网络上去。

ping表示分组Internet探测器（*Packet Internet Groper*）。在IP网络中常用它来检验设备的可到达性。

插件（*plug-in*） 可以容易地安装和作为Web浏览器一部分的软件和程序。

电源线（*power cord*）　用于连接电源插座和电气设备，为设备提供电源。

印刷电路板（*printed circuit board，PCB*）　有集成电路和其他电子部件的线路板。

协议（*protocol*）　规定网络设备如何交换信息的规则和约定集合的正式表述。

随机访问存储器（*random-access memory，RAM*）　也称为可读写存储器，可以往里面读写数据。

只读存储器（*read-only memory，ROM*）　计算机的一种存储器，数据写入后不能修改。

串口（*serial port*）　通过它进行串行通信，每次只可以传输一个比特。

声卡（*sound card*）　可以处理声音的扩展板卡。

子网（*subnetwork*）　在IP网络中共享一个特殊子网地址的网络。子网是由网络管理员任意分段的网络，分段的目的是提供多级和分层的路由选择结构，同时消除子网和其所连接网络的寻址复杂度。也称为subnet。

子网掩码（*subnetwork mask*）　IP地址的一部分，它通过子网掩码标明子网。

系统单元（*system unit*）　PC系统的主要部分。

1000吉字节（*terabyte，TB*）　约1万亿字节。一些高端计算机使用TB来硬盘大小。

1000吉比特每秒（*terabits per second，Tbit/s*）　万亿比特每秒。它是计算通过网络连接传输的数据量的标准单位。一些核心路由器和交换机工作带宽超过1Tbit/s。

传输控制协议/Internet协议（*TCP/IP*）　美国国防部在20世纪70年代开发的一套协议的通用名称，支持全球互联网的结构。TCP和IP是这套协议中最著名的两个协议。

通用串行总线（*USB*）　端口它可以实现鼠标、调制解调器、键盘、扫描仪、打印机等外设的热插拔。

视频卡（*video card*）　可以处理图像的板卡。

Web浏览器（*Web browser*）　一种基于用户图形接口（GUI）的超文本客户端应用程序，例如Internet Explorer和 Netscape Navigator 用于处理超文本文档和其他通过万维网和Internet获得的远程服务器上的服务。

1.12 复习题

完成下面的复习题，以考核你对本章主题和概念的理解掌握情况。答案请参见附录C“复习题答案”。

1. 因特网中的连接可以分为以下哪些部分？
   A. 物理连接
   B. 逻辑连接
   C. 应用程序
   D. 以上全部
2. 计算机的主要线路板是指什么？
   A. PC子系统
   B. 主板
   C. 底板
   D. 计算机存储器
3. 什么是PCMCIA插槽？
   A. 膝上型电脑插槽
   B. 所有计算机的扩展插槽
   C. 网卡的扩展插槽
   D. 专门外设的插槽
4. 什么是NIC？
   A. 一种WAN适配器
   B. 一种可以提供网络连接的印刷电路板
   C. 以太网专用的板卡
   D. 数据链路层地址
5. 安装网卡时，以下哪些能力是必须具备的？
   A. 网卡配置知识
   B. 诊断网卡故障知识
   C. 解决网卡冲突能力
   D. 以上全部
6. 什么数制是基于2的乘方的？
   A. 八进制
   B. 十六进制
   C. 二进制
   D. ASCII码
7. 匹配以下短语以及它们的定义
   （1）比特
   （2）字节
   （3）kbit/s
   （4）MHz
   a. 计算机数据的最小单位
   b. 计算通过网络连接传输的数据量的标准单位
   c. 频率单位，用于描述状态转换速度，声波、交流电、其他循环波形的周期
   d. 用于描述数据文件大小、磁盘或者其他存储介质空间、通过网络传输的数据量的单位

8. 1字节可以表示的最大十进制数是多少?

A. 254

B. 256

C. 255

D. 257

9. 十进制数151转化成二进制数的结果是多少?

A. 10100111

B. 10010111

C. 10101011

D. 10010011

10. 二进制数11011010转化为十进制数的结果是多少?

A. 186

B. 202

C. 218

D. 222

11. 二进制数0010000100000000转化为十六进制数的结果是多少?

A. 0x2100

B. 0x2142

C. 0x0082

D. 0x0012

12. 十六进制数0x2101转化为二进制数的结果是多少?

A. 0010 0001 0000 0001

B. 0001 0000 0001 0010

C. 0100 1000 0000 1000

D. 1000 0000 1000 0100

13. 以下关于ping的说法，哪个是正确的?

A. ping命令用于测试网络的连通性

B. Ping是分组互联网探测器。

C. ping 127.0.0.1命令用于判断TCP/IP协议栈的操作和NIC收发功能。

D. 以上全部



第2章　网络技术基础

目标

学习完本章之后，你应该能够：

- 描述网络历史。
- 定义LAN、WAN、MAN、SAN和数据中心技术，并描述其特征。
- 定义和描述VPN的功能、优点和技术。
- 定义物理拓扑和逻辑拓扑。
- 描述OSI参考模型的优点。
- 讨论OSI七层参考模型各层的功能。
- 描述OSI参考模型中的基本通信流程。
- 说出TCP/IP协议模型各层的名字。
- 描述中继器、集线器、NIC、网桥、交换机和路由器的功能。
- 描述语音网关、DSLAM、CMTS和光平台。
- 描述防火墙、AAA服务器、VPN集中器的作用。
- 描述无线适配器、无线接入点、无线网桥的作用。
- 定义总线拓扑，总线拓扑，星形拓扑，扩展星形拓扑，环形拓扑，层次拓扑，网状拓扑和半网状拓扑。

本章介绍了网络专业人员使用的一些网络术语和不同类型的计算机网络，阐明了网络标准如何确保不同类型的网络技术之间具有更好的兼容性和互操作性，还阐述了开放系统互联（OSI）参考模型的网络方案如何支持这些网络标准。此外，本章介绍了 OSI 模型中各层的基本功能。在学习这一章的过程中，你将会学到OSI模型每一层的基本功能，这将是你开始设计、构建以及解决网络故障的基础。

最后，本章还介绍了不同的网络设备以及物理和逻辑布线设计。

请务必在本书配套的光盘中查看与本章相关的e-Lab实验活动、视频和插图。这些光盘资料提供了补充材料，能够强化本章中涉及的概念。

2.1　网络术语

本节介绍数据网络的概念和发展历史，并讨论以下几种网络的基本特征：

- 局域网（*LAN*）。
- 广域网（*WAN*）。
- 城域网（*MAN*）。
- 存储区域网（*SAN*）。
- 数据中心（*Data center*）。
- 企业内部互联网（*Intranet*）。
- 企业外部互联网（*Extranet*）。
- 虚拟专用网（*VPN*）。

2.1.1　数据网络

由于企业和政府办事处之间需要跨越很长的距离进行电子信息的交换，因此数据网络渐渐发展起来了。微型计算机与大型计算机不一样，它们没有连接起来，因此在不同的微型计算机之间缺乏一种共享数据的有效途径。图2-1举例说明了一家拥有多台微型计算机的公司，但是这些电脑之间并没有进行网络连接。

注释：在早些年代，一般的公司机构会购买一些单独的计算机，其中有一些还带有打印机。当那些没有打印机的员工需要打印文档的时候，他们需要把文件复制到软盘上，然后把软盘中的文件拷到一台带有打印机的电脑上，再进行打印。这种笨拙的网络就叫做*sneakernet*（意为“鞋子上的网络”）（如图2-2所示）。

显然，在企业中通过使用软盘来共享数据并不是一种高效、经济的做法。每一次文件修改后，都必须让所有需要该文件的其他人再共享一次。如果两个人同时修改一个文件，并且企图共享它时，

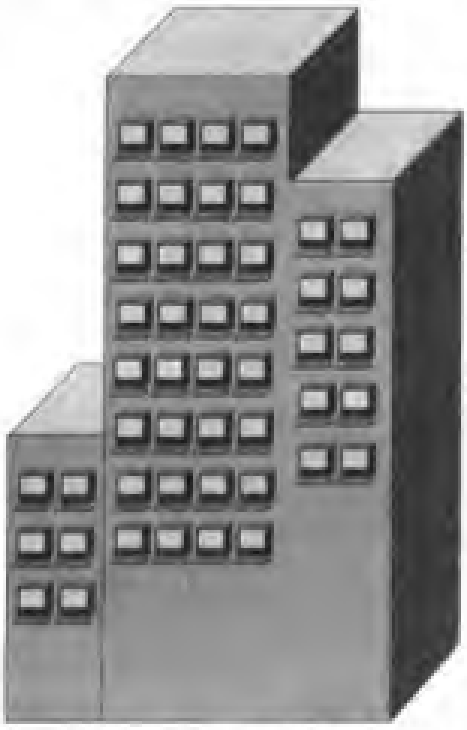


图2-1　拥有多台独立计算机的公司

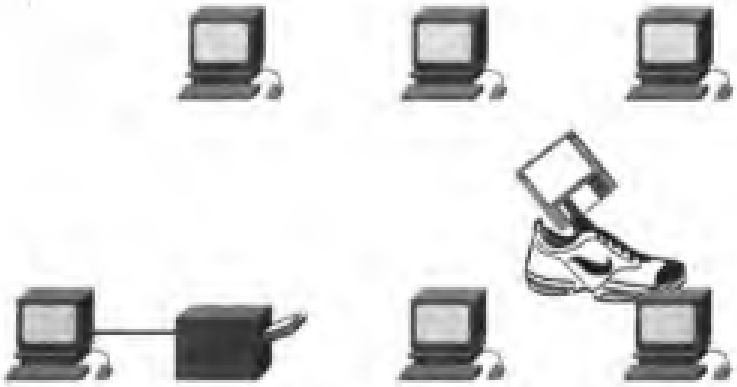


图2-2　Sneakernet

其中一个修改版本将会丢失。企业中需要有解决以下问题的方法：

- 如何避免重复购置设备和资源。
- 如何高效地通信。
- 如何组建和管理网络。

企业已认识到网络技术既能提高生产力又能节省资金。因此，网络的增加和扩展速度几乎跟新网络技术和产品的出现速度一样快。在20世纪80年代初，网络出现了惊人的扩展，尽管早期的网络发展还处于混乱状态。

20世纪80年代中期出现的网络是用许多种不同的软件和硬件创建的。由于不同的公司之间的竞争，每一家公司都使用自己公司开发的标准来生产网络硬件和软件。因此，很多新的网络技术彼此之间都不兼容，使得使用不同规范的网络之间的通信变得越来越困难。正是由于这一点，使得增加新的设备时通常要去掉旧的网络设备。

其中一个较早出现的解决方法是创建*局域网（LAN）*标准。这是因为LAN标准提供了一套生产网络软、硬件的开放性的指导方针，提供了在LAN设备中融合和匹配不同厂家制造的网络设备的能力，从而可以获得稳定性。图2-3显示了一个简单的LAN。随着计算机在商业上的普及，很快局域网又显然不能满足要求了。如图2-4所示，在一个LAN系统中，每个部门或公司都是一座电子岛屿。

在LAN产生之前，就有了信息不仅仅在公司内部而且还要在企业之间进行高效快速传输的要求。这个解决办法就是创建*城域网（MAN）*和*广域网（WAN）*。因为WAN可以在很大的地理区域内连接用户网络，这就使得企业能跨越很长的距离进行彼此通信，如图2-5所示。

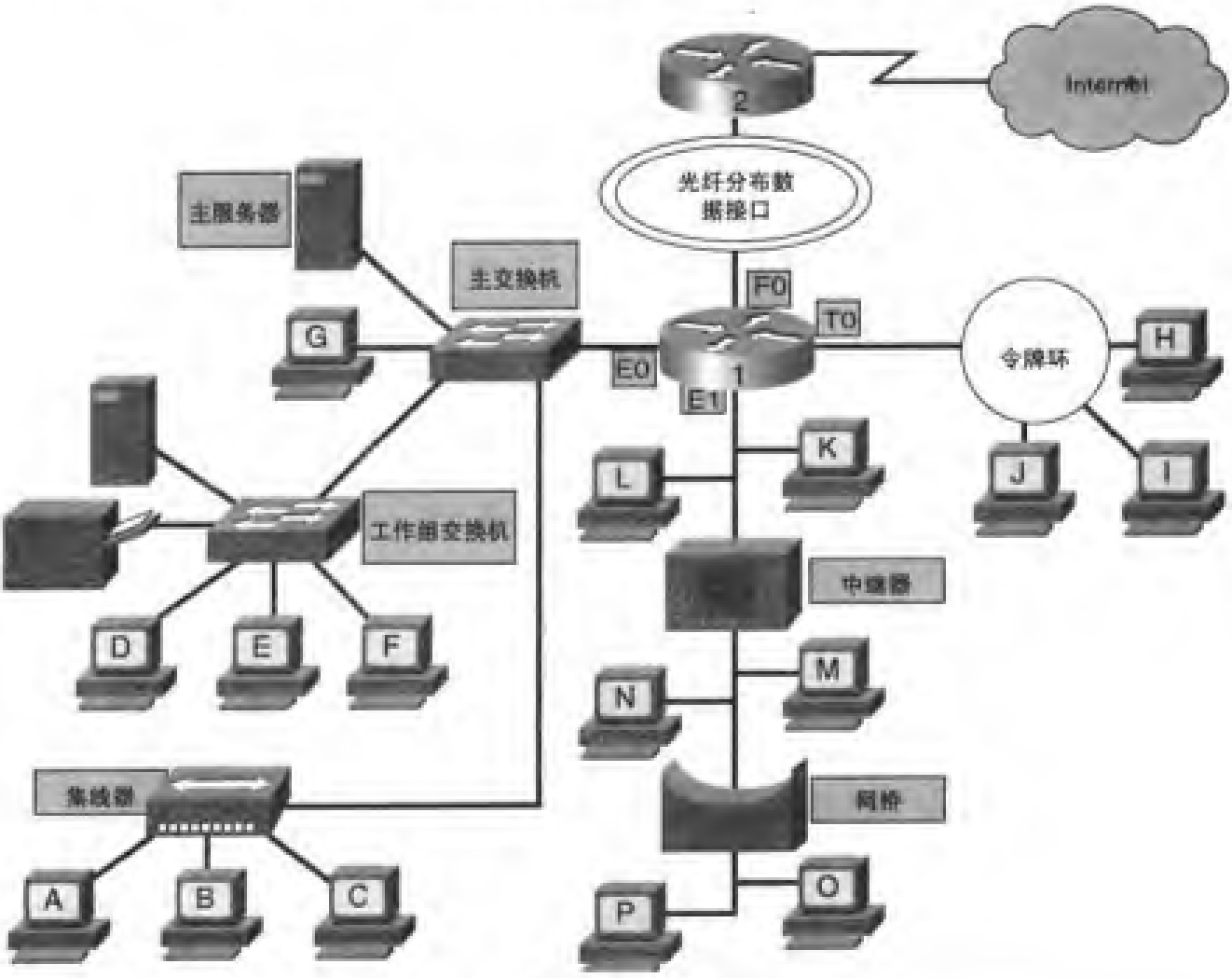


图2-3 简单局域网

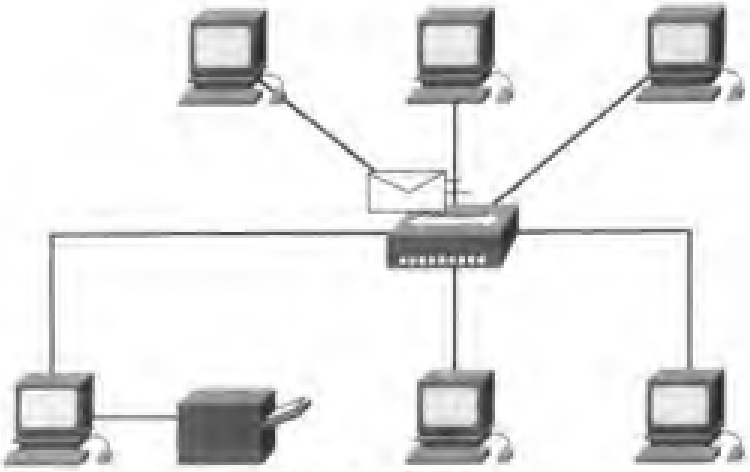


图2-4　局域网

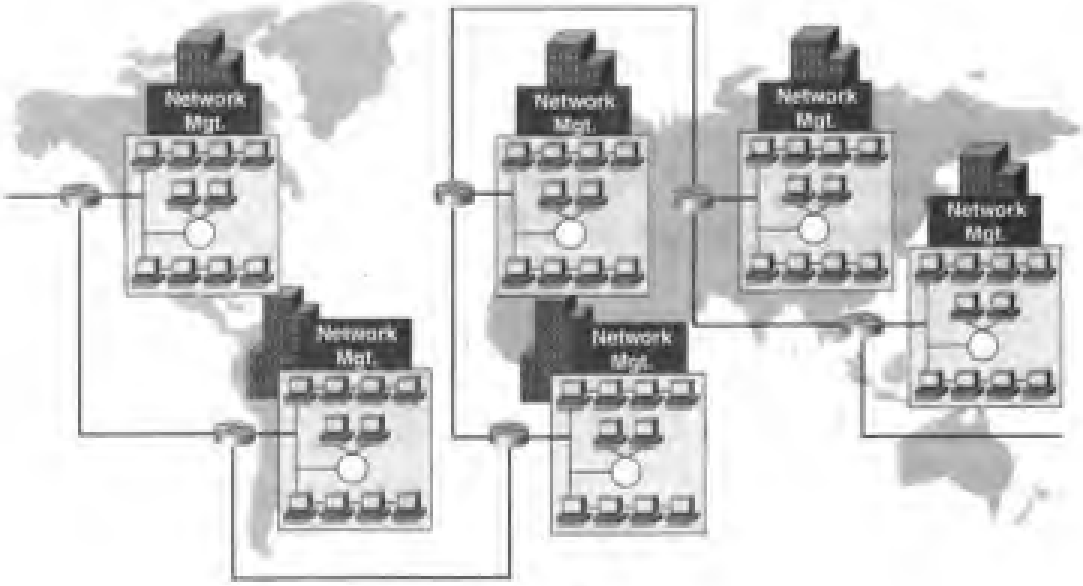


图2-5　广域网

2.1.2　计算机网络的历史

计算机网络的历史很复杂，它涉及过去35年来世界各地许许多多的人，表2-1简单地展示了Internet是如何演进的。技术创新与商业化的过程就更为复杂了，但是了解网络发展的基本知识对我们学习网络课程很有帮助。

表2-1　微型计算机发展历史

时间	发展
20世纪40年代初	大型的机电式设备，现已几乎消失了
1947年	半导体晶体管的发明为制造更为小型、更为可靠的计算机提供了可能
20世纪50年代	集成电路发明出来了，它把几个——稍后是很多个，现在则是上百万个——晶体管集成在一片很小的半导体上面
20世纪60年代	带有终端的大型计算机开始普及，集成电路也得到广泛使用
20世纪60年代后期和70年代	出现了称为“迷你型”计算体积更小型的计算机
1977年	苹果（Apple）公司推出了微型计算机，也就是个人计算机（PC）
1981年	IBM推出它的第一台PC
20世纪80年代中期	使用独立计算机的用户通过使用modem连接到另一台计算机来共享数据（文件），这就称为点到点（point-to-point）或者拨号（dialup）通信

20世纪40年代，计算机是非常大型的电子机械设备，到现在这种计算机几乎消失了。1947年，半导体晶体管的发明为制造更为小型、更为可靠的计算机提供了可能。20世纪50年代，运行打孔卡式程序的巨型计算机开始在一些大型的机构使用。50年代末期，集成电路发明出来了，它把几个——稍后是很多个，现在则是上百万个——晶体管集成在一片很小的半导体上面。60年代，带有终端的大型计算机开始普及，集成电路也得到广泛使用。

在20世纪60年代后期以及70年代，人们又发明了称为“迷你”计算体机的更小型的计算机（尽管它们相对于今天的标准来说仍然是非常庞大）。1977年，苹果（Apple）电脑公司推出了微型计算机，也就是个人计算机（PC）。1981年，IBM推出了它的第一台PC。用户界面友好的苹果Macitonish、开放架构的IBM PC以及集成电路的进一步微型化导致了PC在家庭和商务中的广泛使用。

80年代中期，使用独立计算机的用户通过使用modem连接到另一台计算机来共享数据（文件）。这种方式称为*点到点*（point-to-point）或者*拨号*（dialup）通信。在拨号连接的情况中，某些计算机被用作通信的中心，这个概念也因此而有所扩展。这些作为中心的计算机称为电子公告板（bulletin board）。用户可以连接到电子公告板上发表消息和查看消息，以及上传和下载文件。这种系统的缺点在于缺乏直接的通信，即便有也很少，而且仅仅与知道这个电子公告板的人才能通信；另外一个限制在于电子公告板计算机的每个连接都需要一个modem。假如有5个人需要同时连接到该机器上，则需要用5个modem连接到5个独立的电话线上。我们可以想像一下有500个人想同时与电子公告板建立连接的情形！

从20世纪60年代开始一直延续到90年代，美国国防部（DoD）为了军事与科研的需要，研究出大型、可靠的WAN。这种技术不同于使用在电子公告板中的点到点通信，它允许多台计算机通过不同的途径相互连接。这种网络自身可以决定如何把数据从一台计算机传输到另一台计算机。与一次只能与一台计算机通信不同，它可以使用同一连接访问多台计算机。DoD的WAN渐渐地就发展成为今天的Internet。

2.1.3 网络协议

协议集（protocol suite）是协议的集合，这些协议使得一台主机跨越网络与另一台主机的通信成为可能。***协议（protocol）***是一套规则和协定的正式描述，它们管理设备在网络中通信的某一特定方面。协议规定了数据通信中的格式、定时、后顺序和差错控制。没有协议，计算机就无法把从另一台计算机传过来的比特流组合成为原始的数据。协议控制数据通信的所有方面，它们决定物理网络如何构建，计算机如何连接到网络，数据在传输中采用怎样的格式，以及数据如何发送。这些网络规则由不同的组织和委员会制订与维护：

- 电气和电子工程师学会（*IEEE*）。
- 美国国家标准协会（*ANSI*）。
- 电信工业协会（*TIA*）。
- 电子工业联合会（*EIA*）。
- 国际电信联盟（*ITU*），前身为国际电报电话咨询委员会（*CCITT*）。

2.1.4 局域网（LAN）

LAN由计算机、网络接口卡、外围设备、网络介质以及网络通信控制设备组成。图2-6所示为一LAN。

LAN使得企业可以利用计算机技术有效地共享本地的文件和打印机，并可以进行诸如E-mail之类的内部通信。LAN把数据、本地通信以及计算机设备结合在一起。

LAN主要完成以下工作：

- 在有限的地理范围内运作。
- 允许多个用户同时接入高带宽介质。
- 提供全时的本地服务的连接。
- 互连物理上相邻的设备。

以下是一些常用的LAN技术：

- 以太网。
- 令牌环。
- 光纤分布数据接口（FDDI）。



图2-6　局域网

2.1.5　广域网（WAN）

WAN连接不同的LAN，为位于其他区域的计算机或者文件服务器提供接入服务。如图2-7所示，WAN在一个很大的物理范围内连接网络用户，使得企业能跨越长距离进行通信。

利用广域网可以使LAN中的计算机、打印机以及其他设备被远程共享。WAN在广阔的地理区域内提供直接的数据通信。过去通常只能在同一个办公室才能进行通信，而现在借助于WAN则可以向世界上任何地方的任何人发送即时消息（IM）。协作软件提供了对实时信息和资源的访问，从而使得可以远程召开会议，而不是像以前一样只能坐在会议室里面对面地开会。广域网也创造出新一类工人，即远程办公者（telecommuters），他们上班不用走出家门。



图2-7　广域网

广域网主要完成以下工作：

- 在很大的、地理上分隔的区域之间运作；
- 允许用户之间进行实时的通信；
- 提供远程资源与本地服务器的24小时连接；
- 提供E-mail、万维网、文件传输和电子商务等服务。

以下是一些常用的广域网技术：

- 调制解调器（*modem*）。
- 综合业务数字网（*ISDN*）。
- 数字用户线路（*DSL*）。
- 帧中继（*Frame Relay*）。
- T传输系列（美国）和E传输系列（欧洲）——T1，E1，T3，E3等。
- **同步光纤网**（*SONET*）——第一级同步传输信号（STS-1），即第一级光载波（OC-1）；第三级同步传输信号（STS-3），即第三级光载波（OC-3），等等。

更多信息：不断涌现的家庭网络应用

现在，人们把自己的家设计构建成“Internet家庭”，在家里进行布线以便进行以太网连接。人们将计算机与电话系统、安全系统、家庭影院系统、空调系统、灯光系统和其他电器集成起来，以使能通过点击鼠标甚至通过语音指令进行控制。

服务提供商还建造了基于蜂窝和卫星的通信网，它们能提供丰富的业务，例如无线Internet接入。此外，本地交换运营商（LEC）——通常称作本地电话公司——提供了高速的数据传输业务，例如数字用户线（DSL）业务。这些业务的市场价格已经足够低，家庭用户完全可以承受。

人们还把PC、电话以及传真集成起来，使得通过计算机能实现自动应答、存储和检索消息。此外，使用IP电话技术和VoIP（voice over IP）技术的Internet电话，使得人们可以通过线缆、无线或其他介质接入Internet而完全不用电话线路就可以拨打长途电话，而且还无需付长途话费。

2.1.6 城域网（MAN）

MAN是跨越一个城市的网络，譬如一个市区或者一个郊区。MAN连接远距离分隔开来的处于不同地理位置的LAN，如图2-8所示。例如，一个拥有多个分支机构的银行可能会使用MAN。通常一个服务提供商使用专用传输线或者光纤服务连接两个或者两个以上的LAN，MAN也可以通过在公共区域发射光信号的无线网桥技术来实现。现在已实现的更高的光纤带宽使得MAN可以提供比过去更为有用、更为经济的选择。

以下是MAN与LAN、WAN之间的主要区别：

- MAN所连接的用户跨越的地理范围或区域在范围上介于局域网与广域网之间。
- MAN把一个城市中的多个网络连接成一个更大的网络（也可以提供到广域网的有效连接）。
- MAN也可以通过与骨干线路桥接而互连几个LAN。

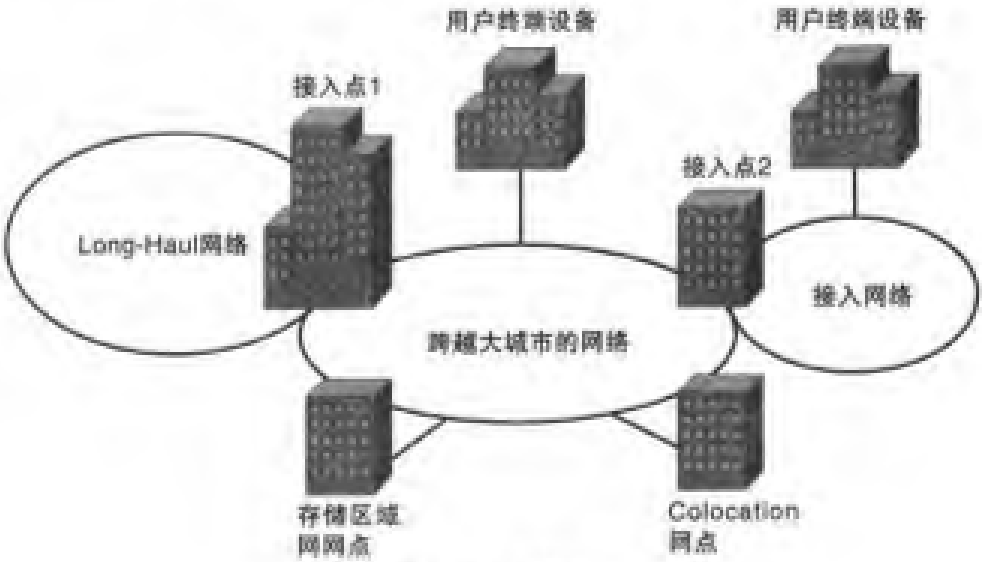


图2-8 城域网

2.1.7 局域网中的专用网络

有时LAN中会存在一些更小的、更专用的网络。值得注意的是，这些专用网络用于访问存储系统、数据中心技术系统和设备、企业内部或外部网以及虚拟专用网（VPN）。本小节将对这些不同类型的专用网络进行介绍。

存储区域网

*存储区域网（SAN）*是专用的、高性能网络，它用于在服务器与存储资源之间传输数据。如图2-9所示，由于SAN是一个独立的专用网络，从而可以避免在客户机与服务器之间的任何传输冲突。SAN技术允许服务器到存储设备、存储设备到存储设备或者服务器到服务器的高速连接。这个存储方案使用独立的网络基础设施，消除了任何由于现有网络连接出现故障而带来的问题。

存储区域网有如下特点：

- **高性能**——SAN允许两个或两个以上的服务器同时高速访问磁盘或磁带阵列，提供增强的系统性能。
- **实用性**——存储区域网具有内在的灾难容错的能力，因为数据可以镜像映射到一个在10km（6.2英里）之外的SAN上。
- **可扩展性**——如同LAN和MAN，SAN也可以使用各种各样的网络技术。这就使得系统间的备份数据操作、文件移动、数据复制能很容易重新定位。

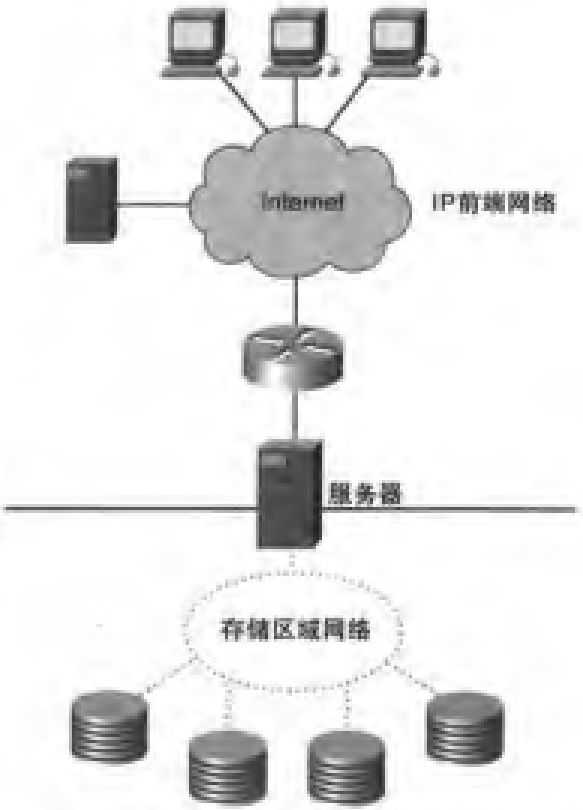


图2-9　存储区域网

数据中心技术

如图2-10所示，*数据中心（data center）*是一个设计用于在网络基础设施之上加速信息传播的全球协作的设备网络。利用核心IP网络的服务，企业和服务提供商可以加速和增强诸如宽带流媒体之类的高容量的应用。数据中心技术提高了网络的性能，同时消除了在网络基础设施上形成流媒体的需要。

数据中心通过在多个内容引擎间分配负载而消除了潜在的拥塞源；这些内容引擎（content engine）放在接近观众的地方。丰富的网页和多媒体内容复制到内容引擎中，用户则被路由到位置最优的内容引擎中。

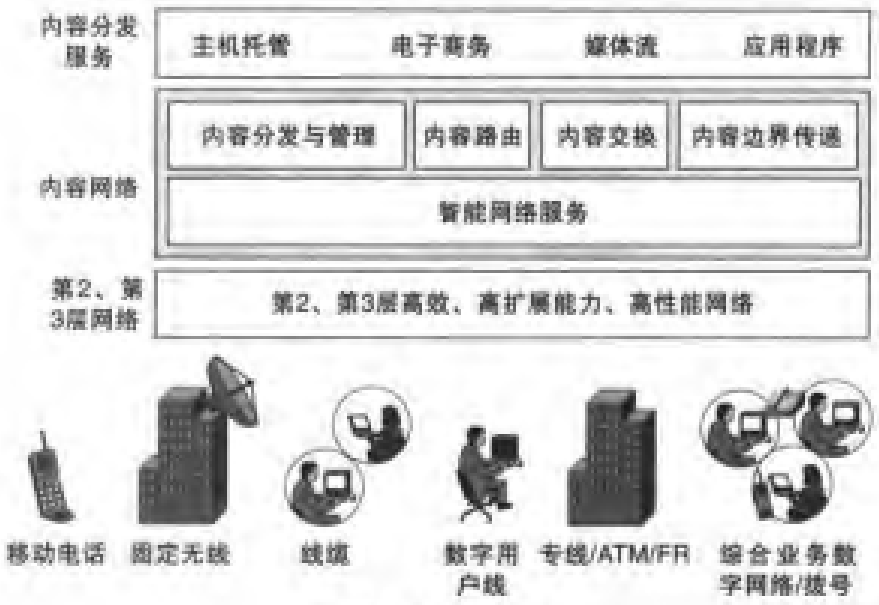


图2-10　数据中心

举例来说，当从ISP那里下载一部电影的时候，如果该ISP使用了数据中心技术，你只需花几分钟就可以下载一部电影，而不用等待数个钟头来下载这部大的电影文件，这是因为数据中心可以加速信息的传递。

企业内部互联网和企业外部互联网

LAN的普通结构就是***企业内部互联网络（intranet）***。企业内部的Web服务器与公众Web服务器的不同在于：如果没有正确的用户名与密码，用户是不能访问一个组织的企业内部网的。Intranet是设计给那些具有访问某个组织内部LAN的权限的用户访问的。在Intranet中，Web服务器安装在网络上，然后使用带有浏览器技术的前台终端就可以访问服务器上的信息，例如那些存放在服务器上的财务数据、图片、文本数据等。

企业外部互联网（extranet）是允许经授权的外部用户访问部分内部网络的企业内部网。Intranet放置在防火墙的后面并仅仅对公司内部员工或者组织开放，而extranet却向外部用户提供不同级别的访问权限。惟有拥有有效的用户名和密码，你才可以访问extranet，而且你的帐号决定了你可以访问的网络范围。

Extranet有助于扩展基于Intranet的应用和服务的使用范围，但是那样就需要引入对外部用户或企业的扩展的、安全的访问机制。这种访问机制通常要通过设置密码、用户ID以及其他应用层安全机制来实现。因此，extranet是带有参与企业和对应的intranet之间的安全交互的两个或两个以上intranet策略的扩展。Extranet在实际操作中控制每一个企业对intranet的访问，它通过使用专有连接的、共享的网络基础设施把客户、供应商、合作伙伴以及对公司intranet有兴趣的公众联系起来。

图2-11 描述了一个intranet和extranet。

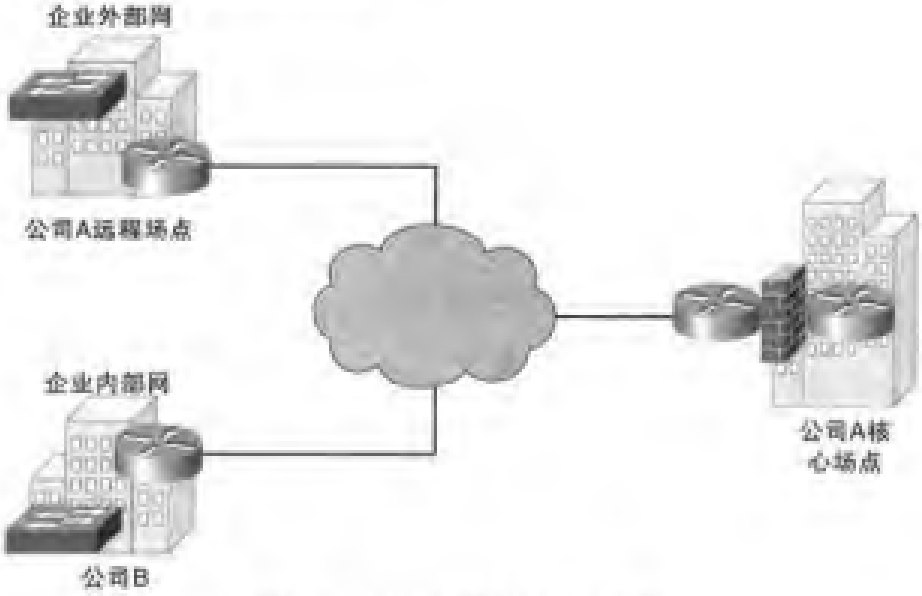


图2-11 企业内部网和企业外部网

2.1.8 虚拟专用网

虚拟专用网（VPN）是在一个公共网络基础设施（例如全球范围的Internet）之上构建的专用网络。例如，利用VPN，一个远程接入用户就可以通过在远程接入的PC与公司总部的VPN路由器之间建立一条安全的隧道，跨越Internet访问公司总部的网络。

Cisco的产品支持最新的VPN技术。VPN在共享的公共基础设施（如Internet）之上提供安全的、可靠的连接服务。VPN采用与专用网络相同的安全和管理方面的策略，它们是在远程用户与企业客

户网络之间建立起点到点连接的最节约成本的方法。

如图2-12所示，主要有下面三种类型的VPN：

• **接入型VPN**——为移动办公人员和小型办公室、家庭办公室（SOHO）提供通过共享的网络基础设施访问公司总部的intranet或者extranet。接入型VPN使用模拟拨号、ISDN、DSL、移动IP和线缆等技术来安全地连接移动用户、远程办公人员和分支机构。

• **Intranet型VPN**——通过使用专用连接的、共享的基础设施把地区和远程办事处与总部的内部网络连接起来。Intranet型VPN与extranet型VPN不同在于：它们只允许企业客户的雇员访问。

• **Extranet型VPN**——通过使用专用连接的、共享的基础设施把企业总部网络与其合作伙伴的网络连接起来。Extranet型VPN与intranet型VPN不同在于：它允许外部用户的访问。

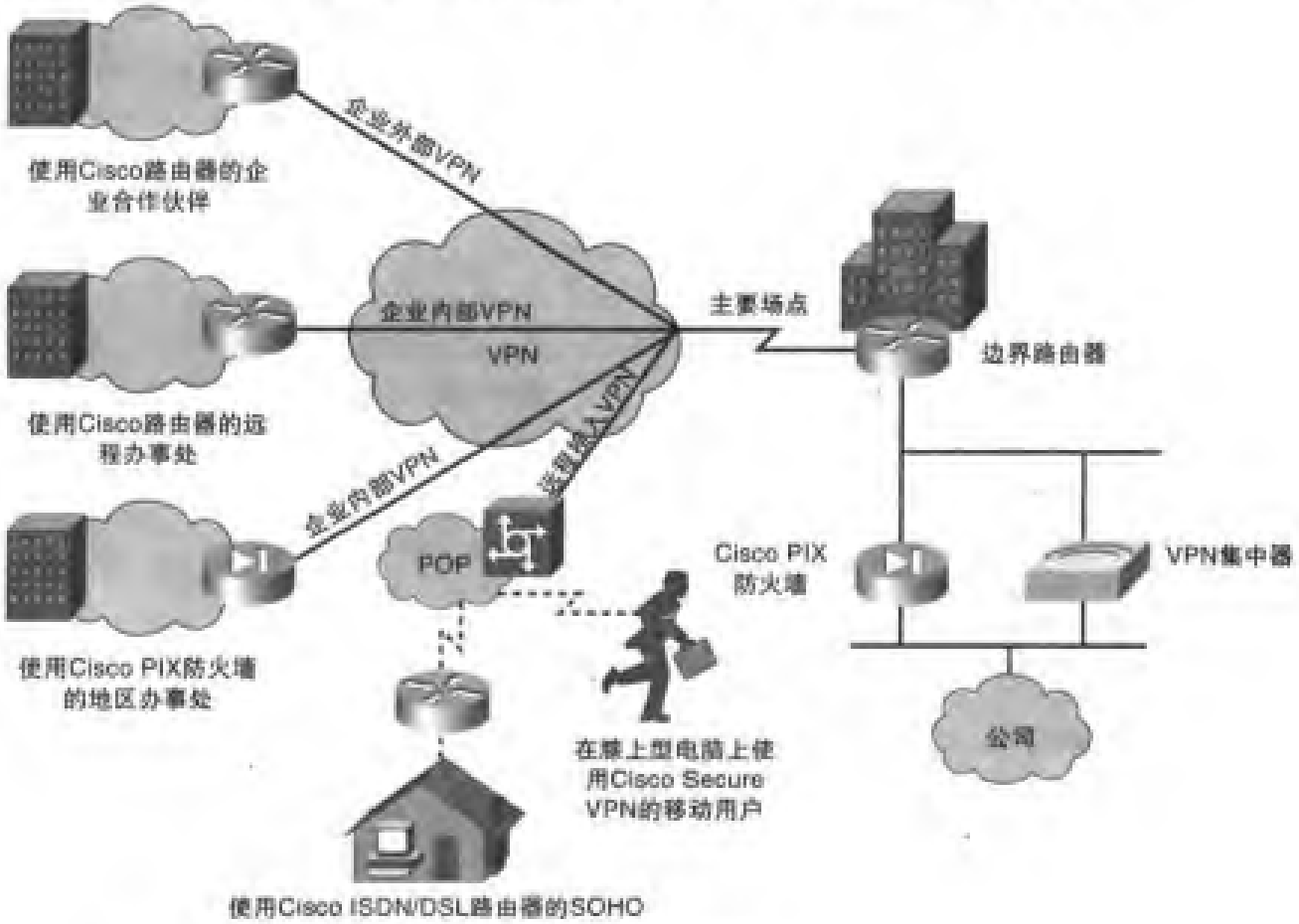


图2-12　VPN技术

VPN有以下的优点：

• 单一VPN技术就能为多个TCP/IP应用提供保密性。当你想为合作伙伴或远程办公人员提供安全访问时，为多种TCP/IP应用提供保密性就显得相当重要。

• 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。这种方案的优点在于对终端用户是透明的，因为只要加密处于开启状态，服务器就可以自动实施加密。

• VPN可以为员工提供移动性，并允许他们安全地访问公司的网络。

2.2　数字带宽

LAN和WAN都有一个共同的特点：它们都使用*带宽（bandwidth）*来描述它们的传输容量。这个术语对于理解网络是至关重要的，但刚开始接触时可能会引起混淆。因此，在深入了解网络之前，本节先详细地讲解一下这个概念。

2.2.1 带宽的重要性

*带宽（bandwidth）*定义为在某给定时间内通过某个网络连接的信息量。这个定义看起来似乎很简单，但是在学习网络课程时，你必须理解带宽的概念。为什么理解带宽这么重要呢？

- **带宽是有限的**——无论采何种介质来组建网络，传输信息的网络容量都是有限的。物理定律和在介质上传输信息的技术都限制了网络带宽。例如，由于双绞电话线的物理性质以及语音调制解调技术的限制，传统modem的带宽一般限制在56kbit/s左右。DSL也采用了双绞电话线，然而DSL能够提供比传统的modem高得多的带宽。这是因为DSL使用的频率范围（bandwidth）比语音（和POTS modem）所使用的频率范围宽得多，这就是为什么你能通过DSL每秒发送更多比特数的原因。光纤的物理性质使之具有能提供有效的无限带宽的潜力。即便如此，在技术发展到可以利用光纤的所有潜能之前，光纤的带宽也不能被完全利用。
- **带宽不是免费的**——为LAN购置一些在很长一段时间里提供几乎接近于无限带宽的设备是可能的。但是对于WAN连接，却几乎总是需要从服务提供商那里购买带宽。不论哪种情况，了解带宽以及了解一定时间内带宽需求的变化都可以为个人或企业节约大量的资金。因此，网络管理员需要对所购买的设备和服务的种类作出正确的决策。
- **带宽是分析网络性能、设计新网络以及理解Internet的关键因素**——网络专业人员必须理解带宽和吞吐量对网络性能和设计的巨大影响。信息以比特流的形式跨越网络从一台计算机传输到另一台计算机。Internet中充斥着几百亿的几百亿次方的比特，瞬间就可以在全球范围内传输大量的信息。在某种意义上，说Internet就是带宽会更加合适。
- **是带宽的需求在不断增加**——新的网络技术和网络基础设施一经创造出来以提供更大带宽，就会产生出新的应用来充分利用这些更大的网络容量。包括视频和音频在内的丰富的多媒体内容需要很大的带宽；IP电话系统取代了传统的语音系统而被广泛地应用，这也进一步增加了对网络带宽的需求。成功的网络专业人员应该预见到日益增加的带宽需求从而相应地做好网络的规划。

2.3 数字带宽的形象化类比

用下面两个也具有流量概念的事物来形象地类比网络带宽，可使带宽的概念易于理解。由于水和交通都可以称为流，所以可以这样比喻：

- **带宽就像水管的粗细，如图2-13所示**——水管网络将新鲜水输送给千家万户，而将废水运走。该网络由许多不同直径的水管组成。城市主干水管的直径可能有2m，而厨房水龙头的直径可能只有2cm。水管的粗细决定了运输水的能力。因此，可以用水来类比数据，而用水管的粗细来类比带宽。当网络专家们需要提高网络信息的运输能力时，他们会说他们需要把这些信息“放入更大的管中”。

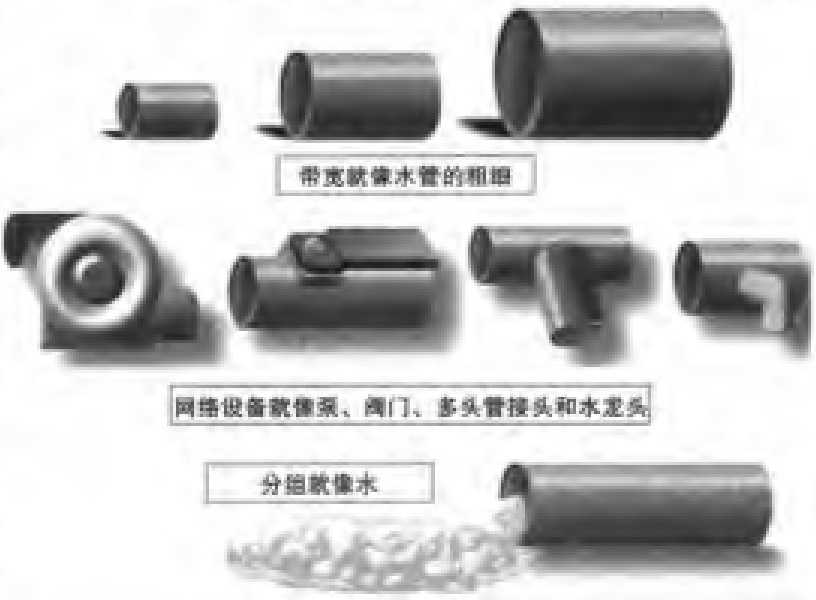


图2-13 带宽的水管类比

- **带宽就像高速公路的车道数，如图2-14所示**——公路网络延伸到每个城市或乡镇。车道数较多的高速公路连接着车道数较少的公路，而这些公路又通向更小、更窄的公路，最终是到达住宅和办公地的车道。当很少几辆车在高速公路上行驶的时候，每辆车都可以行

驶得非常自由。但当车流增加时，尤其是车道数较少时，每辆车行驶都慢了许多。最终，当更多的车不断地进入高速公路时，即使有多个车道的高速公路也会变得拥塞和缓慢。如果将数据网络类比为高速公路系统，则数据分组相当于车，而带宽相当于高速公路的车道数。当将数据网络被视为高速公路系统时，很容易看出为何低带宽会引起整个网络的拥塞。



图2-14　带宽的高速公路类比

请记住，带宽的实际含义是：在某一特定的时间内（在给定的条件下）理论上能通过某一特定区域的最大比特量。上述的那些类比只不过是为了使带宽的概念更易于理解。

2.3.1　数字带宽的度量

在数字体系中，带宽的基本单位是比特每秒（bit/s）。带宽是在一个给定的时间（或多少秒）内有多少信息（或bit）从一个地方流到另一个地方的量度。虽然带宽是以bit/s来描述的，但通常还有一些数倍于bit/s的表示方式。换句话说，网络带宽通常描述为kbit/s、Mbit/s，甚至kMbit/s。

尽管术语*带宽*和*速度*经常交替使用，但它们并不完全是一回事。例如，你可以说以45 Mbit/s传输的T3比以1.544 Mbit/s传输的T1具有更高的速度。然而，如果只用到它们传输能力内的一小部分时，它们传输数据的速率大致相同，就像小量的水在细管和粗管里的流速大致相同的道理一样。因此，通常更为准确的说法是T3的带宽比T1的要大，因为它在相同时间内能够传输更多的信息，而不是它有更高的速率。

表2-2汇总了带宽的各种单位。

表2-2　带宽单位

带宽单位	缩写	等价换算
比特每秒	bit/s	1bit/s=带宽基本单位
千比特每秒	kbit/s	1kbit/s=1000bit/s=10^3bit/s
兆比特每秒	Mbit/s	1Mbit/s=1 000 000bit/s=10^6bit/s
吉比特每秒	Gbit/s	1Gbit/s=1 000 000 000bit/s=10^9bit/s

2.3.2　带宽的限制

带宽的差异取决于介质的类型及LAN和WAN所采用的技术的差异。介质的物理特性决定了这些差异。由于信号在双绞线、铜轴电缆、光纤及空气等介质中传输方式的物理差异，从而导致了信息传输能力受限于介质本身的极限传输能力。然而，网络的实际带宽是由介质的物理特性及所选择的

发送信号和检测网络信号的技术所共同决定的。

例如，最近研究表明无屏蔽双绞线（UTP）、同轴电缆的物理特性使得理论带宽的极限可以超过1Gbit/s，但是实际上带宽还是取决于所使用的特定技术，如10Base-T、100Base-TX、或1000Base-TX以太网。带宽还取决于一些可变因素，如网络的用户数、所用的设备、应用程序及广播量等。换句话说，实际带宽不是由介质的极限带宽所决定，而是由发送信号的方式、NIC及所选择的网络设备所决定。

表2-3列出了一些常用的网络介质类型以及它们的极限带宽和极限距离。

表2-3 最大带宽和长度极限

介质	最大理论带宽	最大物理距离
50Ω同轴电缆（10Base2以太网，细缆）	10Mbit/s	185m
50Ω同轴电缆（10Base5以太网，粗缆）	10Mbit/s	500m
5类非屏蔽双绞线（10Base-T以太网）	10Mbit/s	100m
5类非屏蔽双绞线（100Base-TX以太网）	100Mbit/s	100m
5类非屏蔽双绞线（1000Base-TX以太网）	1000Mbit/s	100m
多模光纤（62.5/125μm）（100Base-FX以太网）	100Mbit/s	2000m
多模光纤（62.5/125μm）（1000Base-SX以太网	1000Mbit/s	220m
多模光纤（50/125μm）（1000Base-SX以太网）	1000Mbit/s	550m
单模光纤（9/125μm）（1000Base-LX以太网）	1000Mbit/s	5000m

表2-4汇总了常用的广域网服务及其带宽。

表2-4 广域网服务和带宽

广域网服务	典型用户	带宽
Modem	个人用户	56kbit/s=0.056Mbit/s
DSL	个人用户、远程办公者、小型办公室	12kbit/s~6.1Mbit/s=0.128Mbit/s~6.1Mbit/s
ISDN	远程办公者、小型企业	128kbit/s=0.128Mbit/s
Frame Relay	小型办公机构（学校）、中型企业	56kbit/s~44.736Mbit/s（美国）/ 34.368 Mbit/s（欧洲）=0.056Mbit/s~44.736Mbit/s（美国）/34.368Mbit/s（欧洲）
T1	大型实体	1.544Mbit/s
T3	大型实体	44.736Mbit/s
STS-1（OC-1）	电信公司、数据通信公司骨干网	51.840Mbit/s
STS-3（OC-3）	电信公司、数据通信公司骨干网	155.251 Mbit/s
STS-48（OC-48）	电信公司、数据通信公司骨干网	2.488Gbit/s

2.3.3 数据吞吐量

带宽是在给定的时间段内可以通过网络的信息量大小的量度。因此，有效带宽是网络性能的一个关键指标。一个典型的LAN可以构建为向桌面工作站提供100Mbit/s的带宽，但这并不意味着每个用户每一秒钟都可以通过网络传输100Mbit的数据，这只有在理想环境下才可能成为现实。吞吐量的概念有助于解释为什么会是这样。

吞吐量（throughout）是指一组特定的数据在特定的时间段经过特定的路径所传输的信息量的实际测量值。不幸的是，由于诸多原因使得吞吐量常常是远小于所用介质本身可以提供的最大数字带宽。下面是一些决定吞吐量的因素：

- 网络互联设备。
- 所传输的数据类型。
- 网络拓扑。
- 网络上的用户数量。
- 用户的计算机。

- 服务器。
- 电源状况。
- 拥塞。

网络的理论带宽是在网络设计中所需要重点考虑的因素，因为网络的带宽从来不会高于所采用的介质和网络技术所决定的极限值。图2-15列出了一些影响吞吐量的因素。然而，对网络设计者和管理者而言，考虑这些可能影响实际吞吐量的因素是非常重要的。通过对吞吐量的定期测试，网络管理员可以意识到网络性能的变化和网络用户需求的变化，从而相应地调整网络。

吞吐量 < = 介质的数字带宽
为什么?
你的PC机（客户机）
服务器
你所在LAN的其他用户
网络云中的路由选择
所有有关的网络设计(拓扑)
所传输的数据类型
一天中的时间段

图2-15　影响吞吐量的因素

2.3.4　数据传输计算

通常要求网络设计者和管理者要基于带宽来作出决策。是否需要增加WAN连接的带宽以适应新的数据库？当前LAN骨干网是否具备足够的带宽以满足视频流培训课程？诸如这类问题的答案并不容易找到，但是可以从数据传输计算着手。

使用公式*T=S/BW*（传输时间=文件大小/带宽）可以帮助网络管理员评估网络性能的几个重要方面。如果给定应用的典型文件大小已知，那么用文件大小除以网络带宽就可以估计出这个文件传输所需的最小时间。

进行数据传输计算时，有两个重要方面需要考虑：

- 结果只是一个估计值，因为文件大小不包括为了使数据能通过网络传输而进行处理所增加的开销。这个处理称为封装，封装在后续的章节有详细的讲解。
- 结果可能是最佳状态下的传输时间，因为可用带宽永远达不到该网络类型的最大理论值（如果用吞吐量取代带宽会更加准确）。

虽然数据传输计算相当简单，但如果你不注意在方程中使用相同单位的话，也会遇到麻烦。换句话说，如果带宽的单位是兆比特每秒（Mbit/s），则文件大小的单位必须是兆比特（Mbit），而不是兆字节（MB）。因为文件大小通常是以MB为单位的，所以你需要将MB乘以8来转换成Mbit。

请使用公式*T=S/BW*来回答下列问题（必要时应进行单位的转换）。

利用ISDN传输一张软盘的数据内容（1.44MB）所花的时间是否比利用OC-48传输一个10-GB硬盘的内容所花的时间少？

图2-16汇总了文件传输时间计算的简单公式。

最小下载时间T=S/(BW)	典型下载时间T=S/P
BW=	源主机与目的主机之间“最慢链路”的最大理论带宽（以bit/s为单位）
P=	传输时刻的实际吞吐量（以bit/s为单位）
T=	文件传输的时间（以s为单位）
S=	文件大小（以bit为单位）

图2-16　文件传输时间计算

2.3.5　数字带宽与模拟带宽的对比

无线电、电视和电话利用电磁波通过空气和电缆进行传输。这些波被称为模拟的，因为它们具有与光和声波一样的波形，而波形是通过发射机产生的。正如光和声波会改变其大小和形状一样，携带传输信息的电信号也会相应地改变其大小和形状。换句话说，电磁波可以类比为光和声波。

模拟带宽是通过每一信号所占电磁波频谱的多少来量度的。模拟带宽的基本单位是*赫兹*（Hz），或周每秒。正如数字带宽的单位一样，模拟带宽也有数倍于基本单位的单位，常用的有千赫（kHz）、

兆赫（MHz）和吉赫（GHz）。这些都是过去用来描述无绳电话（它通常工作在900MHz或2.4GHz频率处）带宽的单位。802.11a和802.11b无线网络的工作频率通常为5GHz和2.4GHz。

虽然模拟信号可以传输各种各样的信息，但它们与数字传输相比有一些很大的缺点。例如，模拟视频信号需要很宽的频带来进行传输，它无法压缩到一个更小的带宽中进行。因此，如果模拟带宽不够时，信号根本就无法传输。虽然数字带宽也有相同的情况，但是数字带宽较少会碰到这种情况，因为数字带宽通常都有更大的可用带宽。

在数字信号中，所有的信息不管它是什么样的信息都是以bit来发送的。当声音、视频和数据准备在数字介质上进行传输时，它们都会形成比特流，这就使得数字带宽具有比模拟带宽更重要的优点。在最小的数字信道（最低带宽）上都可以传输无限的信息。

理解数字带宽和模拟带宽的差别和相似之处是非常重要的，这两类带宽在信息技术领域中都很容易碰到。然而，因为本课程主要是涉及数字网络，所以涉及到术语*带宽*时就是指数字带宽。

2.4 网络模型

先从理论和概念着手，然后再过渡到比较具体的实现，这样学习网络技术会更容易一些。作为一名网络专业人员，在设计、创建和维护网络之前，你必须先了解网络之间如何进行通信的理论。掌握分层的概念有助于你理解在一台计算机和另一台计算机进行通信时所发生的行为。

本节包括分层的概念以及它如何明确地应用在通信模型上。此外，描述了两种特定的模型（OSI和TCP/IP模型）和对等层通信及其封装。

2.4.1 利用分层在大量的数据中分析问题

分层的概念有助你理解在一台计算机和另外一台计算机进行通信时所发生的行为。以下是关于物理对象（如高速公路交通或电子数据）运动的一些问题：

- 什么在流动？
- 有哪些不同的对象流动形式？
- 用什么规则来管理流动？
- 流发生在什么地方？

对象的这种运动，不管它是物理上的还是逻辑上的，都可以用*流（flow）*来表示。分层有助于描述流动过程的细节问题。流动系统的例子有公共水系统、高速公路系统、邮政系统和电话系统。

现在来考察表2-5：考察的网络是什么？什么在流动？正在流动的对象有哪些不同的形式？流动的规则是什么？流发生在什么地方？表中列举出的网络的类比有助于你理解计算机网络中的数据流。

表2-5 网络比较

网络	什么在流动	不同的形式	规则	地点
水系统	水	热水、冷水、可饮用水、污水	进入规则（打开水龙头），冲洗，不能把某物放到排水管里去	水管
高速公路系统	汽车	卡车、小汽车、自行车	交通规则和公共礼貌	公路与高速公路
邮政系统	物件	信件（已写信息）、包裹	包装和邮资的规则	邮箱、办公室、货车、飞机、邮递员
电话系统	信息	所说语言	接通电话的规则和礼貌习惯	电话系统线路、电磁波，等等

网络通信过程是很复杂的。以电信号形式表示的数据，必须跨越传输介质到达正确的目的计算机，然后再转换为它的最初形式，才能给接收方读取。这一过程由多个步骤组成，因此，实现网络通信最

有效的方法就是进行分层处理。在这个分层通信的处理方式中，每一层都要执行一个特定的任务。

在以下几个小节，你将会看到网络通信的过程如何被一个分层模型划分为若干阶段。你也可以看到数据是如何通过网络发送出去以及它如何到达预定目的地的过程。在学习网络通信的过程中，很重要的一点是要理解网络通信过程的各个步骤、组成和协议。当网络通信的处理并非很顺利的时候，这种理解能够为你提供有用的故障排除信息。

2.4.2 利用分层来描述数据通信

处理网络通信的困难在于它是一个十分复杂的过程。如果只把网络通信当作一个整体来对待，那么理解这个处理过程会特别困难。针对这种情况的解决方法就是把整个网络通信划分为一系列的层，每一层负责网络通信的一个特定部分。这些分层只与它的上下层互相联系，这种互相联系非常精细地定义了一个层的目的。使用分层的两个最常见的网络模型是OSI参考模型和TCP/IP参考模型。

2.4.3 OSI参考模型

局域网、城域网和广域网的早期发展在许多方面都是很混乱的。在20世纪80年代早期，网络的大小和数量都开始迅速地增长。随着各大公司认识到通过使用网络技术可以节省资金和提高生产效率，新网络的增加和现有网络的扩展几乎和新的网络技术、产品出现的速度同样迅速。

到了20世纪80年代中期，各大公司开始感受到盲目扩展网络带来的困难，尤其是那些使用不同的规范和设备来进行相互通信的网络。于是他们意识到必须摒弃先前的*专用（proprietary）*网络系统。专用网络系统只是个别公司自己研发、拥有和控制的。在计算机产业中，专用是开放的反义词。专用意味着一个公司或者一些公司组成的小团体控制着对技术的使用和改进，而*开放（open）*意味着公众可以免费使用这种技术。

为了解决不同网络系统之间互不兼容和不能相互通信的问题，国际标准化组织（ISO）研究了不同的网络方案（例如DECnet、SNA和TCP/IP）以寻找一种标准。基于这些研究，ISO提出了一种网络模型，它能够帮助供应商构建一个与其他网络兼容的、可相互操作的网络。

把一个复杂的网络通信划分为更小的、相对独立的任务的过程可以比作为组装一辆汽车的过程。作为一个整体，一辆汽车的设计、制造和装配是一个极其复杂的过程，单独的一个人不太可能懂得完成从草稿图到制成一辆汽车所需要的全部工作。这也就是为什么需要机械工程师去设计汽车，制造工程师去设计模子来生产部件以及每一个装配技术人员去装配汽车的原因。

1984年发布的***OSI参考模型***，是ISO提出的一个描述性的方案。它为供应商们提供了一套标准来确保全世界各公司提出的不同类型的网络技术之间具有更好的兼容性和互操作性。

OSI参考模型是作为网络通信准则的主要模型。尽管存在其他模型，但大多数网络供应商都把他们的产品和OSI参考模型关联起来，特别是当他们需要培训用户如何使用其产品时，因为他们认为该模型是目前告诉人们关于网络中如何发送数据和接收数据的最好工具。

OSI参考模型定义了每一层的网络功能。更重要的是，它作为一个框架，可以帮助我们理解信息是如何在网络中传输的。另外，即使发送方与接收方使用不同的网络介质，OSI参考模型都可以描述信息或数据分组是如何通过网络介质（比如线缆）把某一台计算机的一个应用程序（比如电子表格和文档）传输到另外一台计算机的另外一个应用程序。

OSI参考模型有7层，每一层都有特定的功能：

- **第7层**——应用层。
- **第6层**——表示层。
- **第5层**——会话层。
- **第4层**——传输层。

- **第3层**——网络层。
- **第2层**——数据链路层。
- **第1层**——物理层。

网络功能的分离叫做*分层*（*layering*）。把网络分成7个层有如下的好处：

- 把网络通信分成更小、更简单的模块。
- 把网络的组成部件标准化，从而可以让许多供应商去进行研发和技术支持。
- 允许不同类型的网络硬件和软件相互通信。
- 防止某一层的变化影响到其他层，从而可以更快地研发。
- 将网络通信分成更小的组成部分，更易于理解。

通过逐层学习OSI参考模型，你会了解到数据分组在网络中的传输过程，以及每一层上有哪些设备在工作。因此，如果数据分组在传输过程中出现问题，你就懂得如何去解决。

2.4.4 OSI各层及其功能

OSI参考模型的每一层都有它必须实现的一系列功能，以保证数据包能从源传输到目的地。下面是OSI参考模型各层的简单介绍。

第7层：应用层

应用层是OSI模型中最靠近用户的一层，它为用户的应用程序提供网络服务。与OSI的其他层不同的是：它不为其他OSI层提供服务，而是只为OSI模型之外的应用程序提供服务。这些应用的例子有电子表格程序和文字处理程序。应用层为想要进行通信的双方建立连接，对错误恢复步骤和数据完整性控制进行协商和同步。第7层应用程序的例子包括远程登录（Telnet）和超文本传输协议（HTTP）。

第6层：表示层

表示层确保一个系统的应用层发送的信息能够被另外一个系统的应用层读取。必要时，表示层会把各种不同的数据格式翻译成一种通用格式。这层中的一个比较重要的任务是加密与解密。第6层常见的图像格式标准有PICT、TIFF和JPEG，表示影音的标准的例子有MPEG和MIDI。

第5层：会话层

顾名思义，***会话层***建立、管理和终止两个通信主机之间的会话。会话层为表示层提供服务，它也同步两台主机表示层之间的对话以及管理它们的数据交换。除了会话规则之外，会话层还为进行高效的用户传输、服务分类以及会话层、表示层和应用层的差错报告提供条件。第5层协议的例子有网络文件系统（NFS）、X-Window系统和AppleTalk会话协议（ASP）。

第4层：传输层

传输层在发送主机系统上对将要发送的数据进行分段，在接收主机系统上完成数据段到数据流的重组。传输层和会话层之间的边界可以认为是应用协议和数据流协议之间的分界。应用层、表示层、会话层需要考虑的是应用方面的问题，而下面4层却只考虑数据传输的问题。

传输层试图提供一种可以向上层屏蔽传输实现细节的数据传输服务。特别地，像如何在两台主机间实现可靠传输这一类的问题就是传输层所需要考虑的。在提供通信服务时，传输层建立、维护和在适当的时候终止虚拟电路。该层利用错误检测和恢复以及信息流控制来提供可靠的服务。第4层

协议的例子有传输控制协议（TCP）、用户数据报协议（UDP）和顺序分组交换（SPX）。

第3层：网络层

网络层是较复杂的一层，它提供两台主机（它们可能位于地理上很分散的网络中）间的连接和路径选择。另外，逻辑寻址是网络层所关心的。第3层协议的例子有Internet协议（IP）、网间分组交换（IPX）、Apple计算机网络协议（AppleTalk）。

第2层：数据链路层

数据链路层提供数据在物理链路上的可靠传输功能。这就涉及到物理寻址（与之相对应的是逻辑寻址）、网络拓扑、网络介质访问、错误检测、帧的顺序传送和流量控制等问题。

第1层：物理层

物理层为激活、维持和释放端系统之间的物理链路定义了电气、机械、规程的和功能的标准。这些特性如电压、电压变化的时序、物理数据速率、最大传输距离、物理连接器和其他在物理层规范中定义的类似特性。

2.4.5　对等层通信

为了使数据分组从源传送到目的地，源端OSI模型的每一层都必须与目的端的对等层进行通信，这种通信方式称为***对等层通信***。在这一过程中，每一层的协议在对等层之间交换信息，该信息称为协议数据单元（PDU）。位于数据源的每个通信层，使用针对该层的PDU同目的地的对等层进行通信，如图2-17所示。

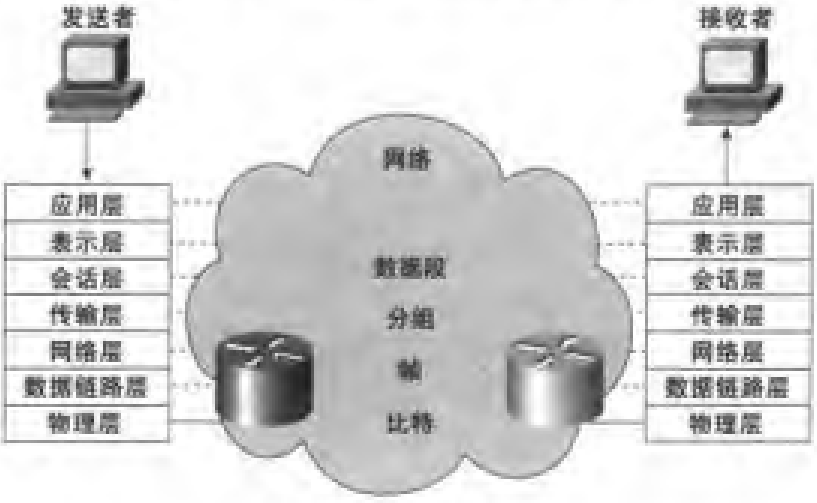


图2-17　对等层通信

网络上的数据分组产生于源，然后被传送到目的地。每一层都依赖于其底层提供的服务。为了提供这种服务，底层将来自上层的PDU封装到它的数据字段中，然后增加为实现该层功能所需的报头。之后，当数据通过OSI模型的每一层时，都会增加相应的报头。第4层PDU中的数据组称为***段（segment）***。

网络层为传输层提供服务。它通过对数据进行封装和增加一个报头来创建一个***分组（packet）***（第3层PDU），从而让数据通过该层进行传输。报头包含为完成传输所需的信息，如源和目的逻辑地址。

数据链路层为网络层提供服务。它将网络层信息封装到***帧（frame）***（第2层PDU）中。帧头包含完成链路功能所需要的物理地址，帧尾包含接收方用来检查数据是否正确的帧校验序列（FCS）。然后，帧就变成将要传送到物理层的数据。

物理层为数据链路层提供服务。物理层将数据链路层帧编码为1和0（比特）的模式，以便在第1层的介质（通常为线缆）上进行传输。

集线器、交换机和路由器这些网络设备工作在最低的3层。集线器工作在第1层，交换机在第2层，而路由器则在第3层。开始处理终端用户之间的端到端传输的层是传输层（第4层）。

2.4.6 DoD（TCP/IP）模型

尽管OSI参考模型得到了普遍的认同，但Internet的历史上和技术上的开放标准却是传输控制协议/Internet协议（TCP/IP）模型。TCP/IP模型及其协议集使得世界上任意两台计算机间进行通信成为可能，并且通信速度接近光速。TCP/IP模型像那些使得电话、电力、铁路、电视以及录像带工业迅速繁荣的标准一样，具有历史性的重要意义。

美国国防部（DoD）拨出巨资开发TCP/IP模型，因为它想要一个可以在任何条件甚至核战争中都可以生存的网络。进一步来说，就是假设一个处于战争的世界，纵横交错着各种不同类型的连接，包括线缆、微波、光纤和卫星链路等。然后假设不管当时互联网络（这时可能已受到战争的破坏）上任何节点或网络的情况如何，你都需要信息或数据（以分组的形式）能够流动。美国国防部想让它的数据分组能在任何时间任何条件下都可以通过，并且从任何一个位置到达任何其他位置。正是这种苛刻的设计要求促使了TCP/IP模型的诞生。从那时开始，TCP/IP模型就成为了Internet赖以发展的实际标准。

当你学习了解TCP/IP模型的各层时，需要记住Internet最初的设计目的，这有助于解释为什么某些事情会是那样的。如图2-18所示，TCP/IP有4层：

- 应用层。
- 传输层。
- Internet层。
- 网络接入层。

OSI	TCP/IP
应用层（第7层）	应用层
表示层（第6层）	
会话层（第5层）	
传输层（第4层）	传输层
网络层（第3层）	Internet层
数据链路层（第2层）	网络访问层
物理层（第1层）	

图2-18 TCP/IP模型

注意，TCP/IP模型中有些层的名字和OSI参考模型中的一样，但是不要混淆这两种模型中的对应层次。即使它们有相同的名字，而且在每一个模型中大多数分层都有着相同的功能，但是某些层却很不一样。



实验活动 OSI模型和TCP/IP模型

本次实验，你将要描述和对比TCP/IP模型和OSI模型的各个分层。你也将要为每一层上的TCP/IP协议以及工作在该层的工具进行命名。

2.4.7 封装过程的细节

网络上所有通信都是产生于源，然后发送到目的地。在网络上传输的信息称为数据或数据分组。如果一台计算机（主机A）想给另外一台计算机（主机B）发送数据，这些数据必须首先要经历一个称为*封装*（*encapsulation*）的过程。

封装

封装（*encapsulation*）就是在网络传输之前为数据附上必要的协议信息。因此，当数据沿着OSI模型的各层向下传递时，OSI的每一层都会在向下传递之前给数据增加上数据报头（在第2层还有数据报尾）。报头和报尾包含对网络设备和接受者的控制信息，以确保数据的正确传送以及接收者能够正确解释数据。例如，可以把报头看作是信封上的地址。信封需要地址，以便信件能够被邮递到所要到达的接收方。

注释：名词*报头*（*header*）是指加到分组前端的信息，正如报尾就是加到分组末端的信息一样。另外，地址是添加的信息中重要的一部分。

要理解封装是如何进行的，可以考察一下数据传输时是如何通过各层的，正如图2-19所示。当数据从源端发出后，它就会从应用层一直向下传递到达其他各层。对所交换的数据进行打包的方式以及这些数据的流动方式都会随着每一层为终端用户所执行的网络服务的变化而变化。

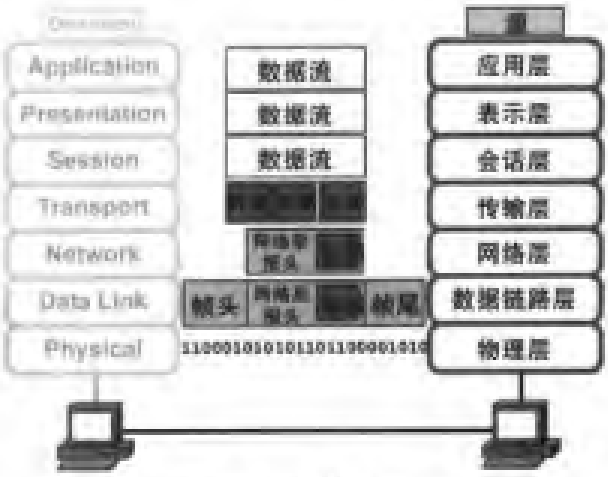


图2-19　封装

以电信号形式表示的数据，必须通过线缆传送到正确的目标计算机中，然后再转化为能够被接收端所能读取的最初形式。正如你所设想的那样，这个过程包括了几个步骤。正因为如此，硬件、软件和协议的开发人员意识到实现网络通信的最有效的方式就是进行分层处理。

如图2-20所示，网络必须执行以下5个转换步骤来封装数据：



图2-20　数据封装的过程

步骤1：创建数据——当用户发送E-mail消息时，消息中的字母和数字字符被转换成可以在Internet上传输的数据。

步骤2：为端到端的传输将数据打包——对数据打包来实现互联网的传输。通过使用分段（segment），传输功能确保e-mail系统两端的主机之间能可靠地通信。

步骤3：在报头上添加网络地址——数据放置在一个分组或数据报中，其中包含了带有源和目的逻辑地址的网络报头。这些地址有助于网络设备沿着已选定的路径发送这些分组。

步骤4：在数据链路报头上添加本地地址——每一个网络设备都必须将分组放入帧中。该帧使得可以传送到该链路上下一个直接相连的网络设备。在选定的路径上的每一个网络设备都必须把帧传递到下一台设备。

步骤5：为进行传输而转换为比特——当这些比特在介质上传输时，时钟同步功能使得设备可以把它们区分开来。物理互联网络上的介质可能随着使用不同的路径而有所不同。例

如，E-mail消息可以起源于LAN，穿过校园骨干网，然后到达WAN链路，直到它到达另一个远程LAN上的目的地。数据通过OSI模型各层向下传送的过程中，会被添加上报头和报尾。

解封装

当远程设备顺序接收到一串比特时，远程设备的物理层把这些比特传送到数据链路层进行操作。数据链路层会执行如下工作：

步骤1：检验该MAC目的地址是否与工作站的地址相匹配或者是否为一个以太网广播地址。如果这两种情况都没有出现，就丢弃该帧。

步骤2：如果数据已经出错了，那么将它丢弃，而且数据链路层可能会要求重传数据。否则，数据链路层就读取并解释数据链路报头上的控制信息。

步骤3：数据链路层剥离数据链路报头和报尾，然后根据数据链路报头上的控制信息把剩下的数据向上传送到网络层。

这个过程称为***解封装***（*de-encapsulation*），每一个后续层都会执行一个类似的解封装过程。可以把解封装过程看作为读取信封上的地址来判断是否是给你的信；如果信上写的是你的地址，你就可以从信封里取出信件。

更多信息：循环冗余校验（CRC）

每个数据分组都有添加到原始数据本身的信息，它们以分组报头的形式出现。报头包含寻址信息，以便分组能到达正确的目标设备。它们还包括排序的信息，因此当所有分组到达接收计算机时，根据这些信息就能正确地重组。

报头信息放置在该分组的头部，即在原始数据前面。分组还可能包含报尾信息，它位于分组的尾部，即原始数据之后。

在报尾中有一个被称为循环冗余校验（CRC）的错误校验部分。在分组离开源计算机之前和到达目的地时，都要对分组进行CRC计算。如果这些计算的结果不同，则表明数据发生了改变。发生这种情况是由于构成数据的用“1”和“0”表示的电信号受到了干扰。如果发现了不一致，就要对分组进行重发。

2.4.8 网络设备

直接连接到网络段的器件叫***设备***（*device*）。这些设备分为两类：

- **终端用户设备**——包括计算机、打印机、扫描仪和其他直接为用户提供服务的设备。
- **网络设备**——包括把终端用户连接起来使他们能进行通信的所有设备。

为用户提供网络连接的终端用户设备也称为*主机*（*host*）。图2-21显示了终端用户设备的一个例子——工作站。

这些设备使用户能共享、创建和获取信息。主机可以脱离网络而存在，但是如果没有网络，它们的能力就会大大降低。主机通



图2-21 终端用户设备：工作站

过一个*网络接口卡（NIC）*与网络介质进行物理连接。它们利用这种连接来完成e-mail发送、报表打印、相片扫描或者数据库访问等工作。NIC是插入到计算机主板上的总线扩展槽中的一种印刷电路板，它也称为网络适配器。膝上型电脑或笔记本电脑的NIC大小通常与PCMCIA卡的大小相当。

每一块网络接口卡都有一个称为MAC地址（后面有更多关于MAC地址的内容）的惟一代码。顾名思义，NIC就是用来控制主机对介质的访问。在网络行业中，没有用于终端用户设备的标准化的符号，但是它们都有相似之处，因而可以很快辨认出来。网络设备为需要在终端用户设备之间传输的数据提供传输服务，它们扩展线缆连接，汇集连接，转换数据格式以及管理数据传送。执行这些功能的设备的例子有中继器、集线器、网桥、交换机和路由器，以下几个部分将概述这些常见的网络设备。

2.4.9　中继器

*中继器（repeater）*是位于第1层（OSI参考模型的物理层）的网络设备。要理解中继器是如何工作的，理解这一点就很重要，即当数据离开源在网络上传送时，它是转换为能够沿着网络介质传输的电脉冲或光脉冲的——这些脉冲称为*信号（signal）*。当信号离开发送工作站时，信号是规则的，而且很容易辨认出来。但是，当信号沿着网络介质进行传送时，随着经过的线缆越来越长，信号就会变得越来越弱、越来越差。中继器的目的是在比特级别对网络信号进行再生和重定时，从而使得它们能够在网络上传输更长的距离。

术语*中继器（repeater）*最初是指只有一个“入”端口和一个“出”端口的设备，然而现在也有了多端口的中继器了。中继器归类为OSI模型的第1层设备，因为它仅仅工作在比特级上，而不查看其他信息。

2.4.10　集线器

*集线器（hub）*的目的是对网络信号进行再生和重定时。它的特性与中继器很相似。如图2-22所示，hub是网络中各个设备的通用连接点，它通常用于连接LAN的分段。Hub含有多个端口。每一个分组到达某个端口时，都会被复制到其他所有端口，以便所有的LAN分段都能看见所有的分组。

由于集线器与中继器有相似的特性，所以集线器也称为*多端口中继器（multiport repeater）*。中继器与集线器的区别在于连接设备的线缆的数量。一个中继器通常只有两个端口，而一个集线器通常有4至20个或更多的端口，如图2-23所示。前者在一个端口上接收到信号，然后再复制到另一个



图2-22　集线器

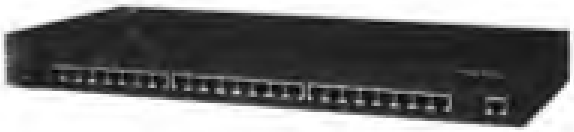


图2-23　有多个端口的集线器

端口；后者在一个端口上接收到信号后，会将该信号复制到其他所有端口。

以下是集线器最为重要的特性：

- 放大信号。
- 在整个网络传播信号。
- 无需过滤。
- 无需路径判定或交换。
- 用作网络汇集点。

集线器通常用于10Base-T以太网或100Base-T网络（你将在第6章的“以太网技术和以太网交换”中学习到更多关于以太网的知识）。集线器为有线传输介质创建了一个中心连接点，它通过使单一电缆出故障而不中断整个网络来增强网络的可靠性。这些特性使得它与总线拓扑区别开来，因为总线拓扑一根电缆出故障就会中断整个网络（网络拓扑在后续的章节中再论述）。由于集线器仅仅是再生信号并复制到其他所有端口（网络线路），所以它被认为是第1层的设备。

在以太网中，所有的主机都连接到同一物理介质上。在这个公共介质上发送的信号都会被所有的设备接收到，因此会发生冲突。*冲突（collision）*就是当2个比特同时在同一网络中传播时发生的一种情形。网络中产生数据分组并发生冲突的区域就称为**冲突域**（collision domain）。所有共享媒质环境都是冲突域或*带宽域（bandwidth domain）*。在第5章的“以太网基础”中，你将会学到更多关于冲突域的知识。正如本节前面所提到的，第1层的功能就仅仅是便于信号的传送，这些设备不能识别信号中的信息模式、地址和数据。当两条电缆用集线器或中继器连接在一起时，所有的互连都是冲突域的一部分。

2.4.11 网络接口卡

网络接口卡（NIC）是第2层的设备，世界上的每一块NIC都带有称为*介质访问控制（MAC）*的惟一编码。MAC地址控制LAN中主机的数据通信，而NIC控制主机对介质的访问。图2-24显示了一块NIC。

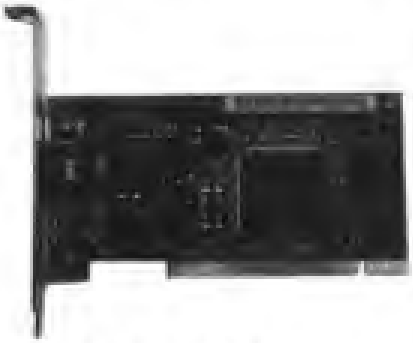


图2-24 网络接口卡

2.4.12 网桥

*网桥*是第2层的设备，它设计用来创建两个或多个LAN分段。其中，每一个分段都是一个独立的冲突域。换句话说，网桥设计用来产生更大可用带宽。它的目的是过滤LAN的通信流，使得本地的通信流保留在本地，而让那些定向到LAN其他部分（分段）的通信流转发到那里去。每一台网络设备在NIC中都有一个惟一的MAC地址。网桥会记录它每一边的MAC地址，然后基于这张MAC地址表作出转发决策。

网桥仅仅通过查看MAC地址来过滤网络通信流，因此，它们能快速地转发代表任何网络层协议的通信流。由于网桥仅仅查看MAC地址，它们并不关心网络层协议，它们关心的只是基于帧的目的MAC地址来决定是否转发它们。以下是网桥的一些重要特性：

- 网桥比集线器更为智能。就是说，它能分析传入的帧，并且能基于第2层信息进行转发或丢弃它们。
- 网桥在两个或多个LAN分段之间收集和转发分组。
- 网桥创建更多的冲突域，使得多个设备能同时无冲突地发送。
- 网桥维护MAC地址表。

图2-25显示了网桥如何使用。网桥的外形会依它们的类型而有很大的变化。

对网桥的定义在于它对帧的第2层过滤以及它如何实现这一点上。为了过滤或者有选择地转发网络通信流，网桥构建位于各个网络分段的所有MAC地址的表，然后把它们与相应的端口关联起来。这一过程如下：

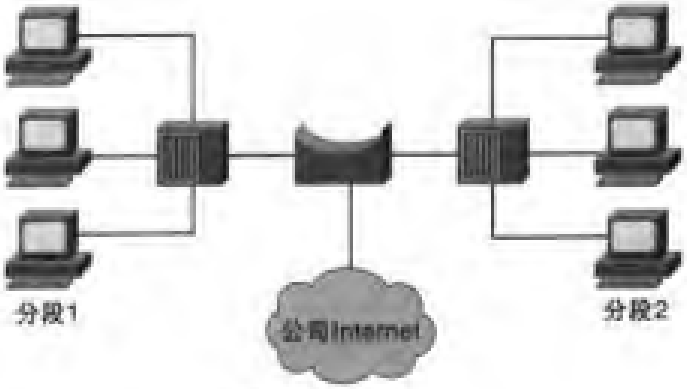


图2-25　网桥

步骤1：当数据帧沿着网络介质到达时，网桥会将该帧中携带的目的MAC地址与包含在它的MAC地址表中的MAC地址进行比较。

步骤2：如果网桥断定数据帧的目的MAC地址与源的MAC地址属于同一网络分段，那么它就不会将该数据帧转发到其他网络分段。这一过程就称为*过滤（filtering）*。通过执行这一过程，网桥就能通过消除不必要的通信流而大大减少网络分段间的通信量。

步骤3：如果网桥断定数据帧的目的MAC地址与源的MAC地址不属于同一网络分段，则把它转发到合适的网络分段。

步骤4：如果目的MAC地址是网桥所不知道的，则把该数据帧广播到网络中除发送该帧的设备以外的所有设备上。这一过程就称为*泛洪（flooding）*。

一个*广播（broadcast）*就是一个发送到网络中所有节点的数据分组。一个*广播域（broadcast domain）*由连接到同一个网络的所有设备组成，它们都会接收由某个节点向同一网络的其他所有节点发送的数据分组广播。由于网络上的每一台设备都必须侦听广播，故网桥总是转发这些广播。因此，在网桥环境中的所有分段都被认为是处于同一个广播域。

正如中继器和集线器的结合一样，另一种称为*交换机（switch）*的设备也是用于多个网桥的连接。下一节将会详细地论述交换机。

2.4.13　第2层交换机

第2层交换机，也称为LAN交换机或工作组交换机，通常替代共享式集线器而与现存的线缆基础设施一起工作，以保证交换机安装后现存网络的中断达到最小。图2-26显示了一台交换机。


图2-26　交换机

像网桥一样，交换机也连接LAN的分段。它利用一张MAC地址表来决定帧需要转发到哪个分段，从而减少通信量。但交换机的处理速度比网桥要高得多。

交换机是数据链路层的设备，它像网桥一样把多个物理上的LAN分段互连成单个更大的网络。与网桥相似，交换机也是基于MAC地址对通信帧进行转发和泛洪。由于交换是在硬件中执行的，所以交换机的交换速度要比网桥中用软件执行的交换快速得多。把每一个交换端口都当作一个微型网桥，则每一个交换端口就充当一个独立的网桥，从而为每一台主机提供介质的全部带宽。这种方法就叫做微分段。

*微分段（Microsegmentation）*允许创建私有的或专用的分段——一台主机一个分段。每一台主机都可以立即获得全部带宽，而不必跟其他主机竞争可用的带宽。在全双工交换机中，由于只有一台设备连到一个交换机的端口，所以不会发生冲突。

然而，跟网桥一样，交换机也是把广播消息转发到交换机上的所有分段。因此，交换机环境中的所有分段被认为是处于同一广播域。

一些交换机——主要是高端的和企业级的交换机——实现了多层交换的功能。例如，Cisco 6500和8500系列实现了一些第3层交换功能。Cisco Catalyst 8500（如图2-27所示）是一台增强型第3层ATM交换机，它无缝地将线速的第3层交换和ATM交换结合在一起。Catalyst 8500系列为校园网和城域网提供了可扩展的、廉价的和基于企业内部互连网络（intranet）应用特性的解决方案，以促进企业生产力的不断增长。第一、二代的ATM交换机对用户而言是一个昂贵的、低效率的以及多系统的解决方案；与它们不同，Catalyst 8500系列在单一机箱上提供了一个综合的ATM和吉比特以太网解决方案。



图2-27 Cisco Catalyst 8500交换机

2.4.14 路由器

如图2-28所示，*路由器（Router）*是一类网络互连设备，它基于第3层地址在网络间传递数据分组。它能为网络上的数据分组选择最佳传递路径。

路由器工作在第3层，这使得它能基于网络地址而不是单独的第2层MAC地址作出决策。它也能连接不同的第2层技术，如以太网、令牌环网和光纤分布数据接口（FDDI）。它通常也连接异步传输模式（ATM）和串行线路。然而，由于基于第3层信息对分组进行路由的能力，路由器已经成为Internet的主要部分，它上面运行IP协议。

路由器的目的是检查每一个进来的分组（第3层数据），为它们选择穿过网络的最佳路径，然后将它们交换到适当的出口。在大型网络中，路由器是最重要的通信调节设备。实际上，路由器可以使任何种类的计算机与世界上任何地方的其他计算机进行通信。

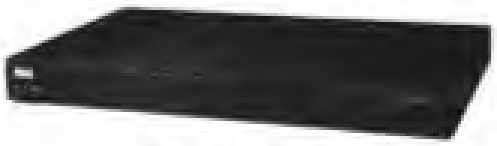


图2-28 路由器

2.4.15 语音、DSL、Cable Modem及光设备

语音网络和数据网络的融合以及终端用户和网络骨干的快速数据传输，这些新近的网络需求已经导致了以下新网络设备的出现：

- 处理汇集的分组语音和数据流的语音网关。
- 服务提供商中心局的数字用户线接入多路复用器（DSLAM），它用于汇集来自许许多多家庭的DSL modem连接。
- 在电缆控制器的头端或中心位置用于聚集来自于众多cable modem用户连接的电缆终端系统（CMTS）。
- 用于在光缆上发送和接收数据的光平台，它能提供高速连接。

语音网关

*网关*是一种特定目的的设备，它把信息从一种协议栈转换到另一协议栈。Cisco的AS5400系列通用访问服务器提供了高投资效益比的平台，它把路由、远程接入、语音网关、防火墙以及数字modem的功能结合在一起。图2-29



图2-29 Cisco AS5400系列通用网关

显示了Cisco AS5400系列通用网关，它提供了能在任何时候任何端口实现通用端口数据、语音、无线以及传真服务的功能。

数字用户线接入多路复用器（DSLAM）

DSLAM（Digital Subscriber Line Access Multiplexer）是用在多种DSL技术中的设备，它充当大量的用户端设备和通信公司网络之间的连接点。图2-30显示了Cisco 6100系列高级DSL接入复用器。



图2-30　Cisco DSLAM 6100

Cable modem终端系统（CMTS）

线缆操作员在各种各样的汇集点采用CMTS（Cable Modem Termination System）或者在电缆网络中采用集线器来为家庭和商业用户提供高速的Internet接入、语音以及其他网络服务。Cisco的通用宽带路由器（uBR）7100 CMTS系列是设计用于诸如公寓建筑物或旅馆等多房客单元（multitenant units，MTU）的。诸如uBR10012系列的高容量设备（如图2-31所示）能处理数千个用户。

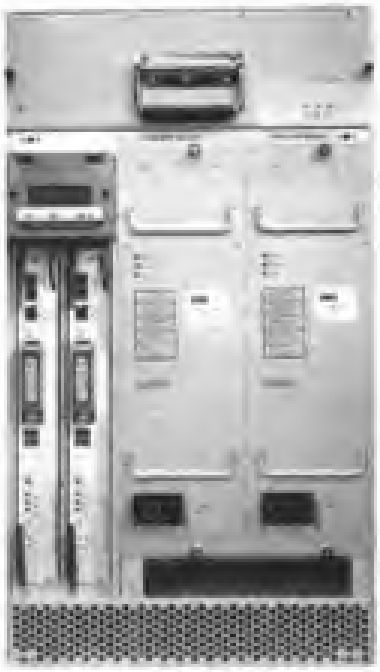


图2-31　Cisco CMTS uBR10012

光平台

有几个光平台可用于光网络中，它们主要是骨干网和广域网中的技术。图2-32显示的Cisco ONS 15454是密集波分多路复用（DWDM）光网络系统。该系统在单一平台上提供了多个网络组件的功能。

2.4.16　安全设备

由于与Internet和企业外部互连网络的连接日益增加，从远端站点接入企业网络的远距离通信用户和移动用户也越来越多，从而使得网络安全日益重要。涉及到网络安全的组件或设备有防火墙、AAA服务器和VPN集中器。

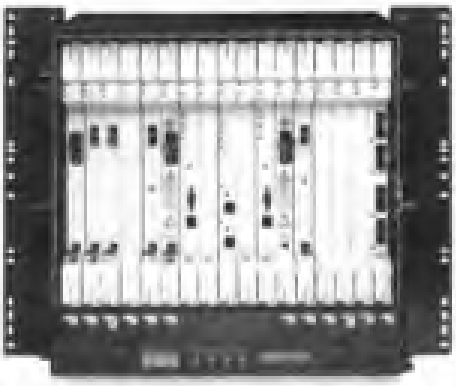


图2-32　光平台——Cisco ONS 15454 DWDM光网络系统

防火墙

术语*防火墙（firewall）*既可以指运行在路由器或服务器上的程序，也可以指特定的、独立的网络硬件。防火墙保护某私有网络的资源不被其他网络的用户访问。它与路由器紧密合作，对每一个网络分组都进行检查以决定是否将它转发到目的地。防火墙的作用就好像交通警察的作用一样，它保证只有有效的通信流才能进入或离开网络。图2-33显示了Cisco 的PIX防火墙535系列，这是一种专用的网络设备。

AAA服务器



图2-33 Cisco的PIX防火墙

AAA服务器是处理用户访问计算机和网络资源的请求的服务器程序。它为企业提供认证、授权和统计服务。AAA服务器保证只有认证了的用户才能进入网络（认证），容许进入的用户只能访问他们需要的资源（授权），并且在他们容许进入后记录他们所做的每一件事（统计）。

AAA服务器就像信用卡系统。为了用信用卡提取现金，信用卡系统必须验证该信用卡确实属于用卡者（认证），必须核对信用卡中剩下的金额足够支付所要求的金额数量（授权），并且必须记录下该用户的帐目（统计）。图2-34显示了AAA服务器在哪里使用的一个例子。

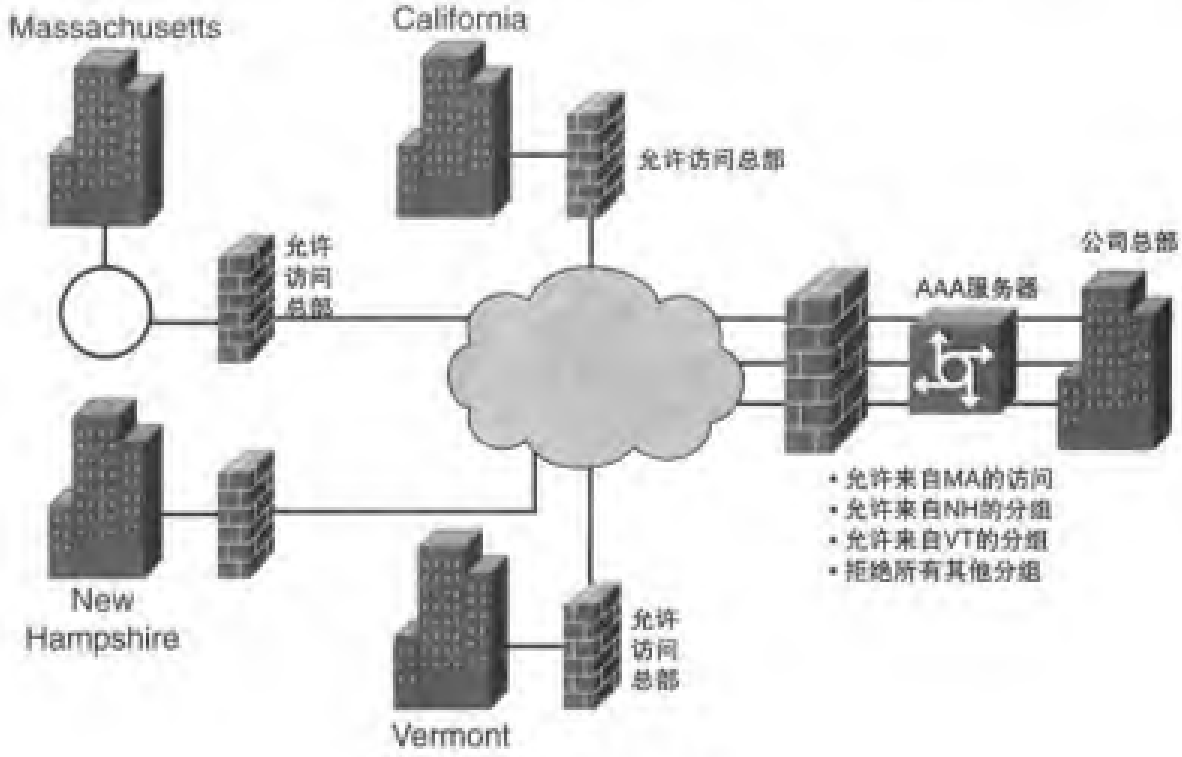


图2-34 AAA服务器

VPN集中器

VPN集中器提供了强大的远程接入和端到端VPN的能力、易于使用的管理接口以及VPN客户程序。Cisco的VPN 3000集中器系列由通用的远程访问VPN平台和将高可用性、高性能和可扩展性与当今最先进的加密和认证技术结合在一起的客户机软件组成。图2-35显示了VPN 3000集中器。



图2-35 Cisco VPN 3000集中器

2.4.17 无线设备

无线局域网（WLAN）具有传统局域网（如以太网）所具有的全部特色和优点，同时又突破了线缆的限制。一些常见的无线网络设备包括无线网卡、无线接入点以及无线网桥。下面的章节将主

要描述这些无线网络器件。

无线网卡

每一个无线客户都需要一块无线网卡或客户端适配器。这些可以是PCMCIA和PCI卡，它们为笔记本电脑和桌上型工作站提供无线接入。装有无线网卡的笔记本电脑或笔记本计算机在保持与网络的连接性的同时，可以在园区环境里自由地移动。无线PCI与ISA适配器（对桌上型工作站而言）可以使终端工作站无需额外的线缆就可以快速、容易、便宜地加到LAN中。所有的适配器都含有天线——PCMCIA卡的天线是内置的，而PCI卡的天线则是外置的。天线规定了数据发送和接收的范围。图2-36显示了无线适配器。



图2-36　无线适配器

无线接入点

一个无线接入点（AP）或基站（见图2-37）是一个无线局域网的收发器，它可以充当集线器（为一个独立的无线网络的中心点）或网桥（为无线与有线网络的连接点）的功能。多个AP能提供漫游的功能，使得无线用户可以自由地四处漫游而不会中断与网络的连接。



图2-37　无线接入点

无线网桥

无线网桥（如图2-38所示）能在以太网络间提供高速（11Mbit/s）、长距离（最远达25英里，约40.2km）及视距的无线连接。Cisco的AP都可以作为无线网络的中继器（扩展点）。



图2-38　无线网桥

实验活动　OSI模型的封装和设备

本实验，你将要描述OSI模型的各层以及它们的特点。你还将识别在各层操作的封装单元和设备。

2.5　网络拓扑

网络拓扑定义了各种计算机、打印机、网络设备和其他设备的连接方式。换句话说，网络拓扑描述了线缆和网络设备的布局以及数据传输时所采用的路径。网络拓扑会在很大程度上影响网络如何工作。

网络拓扑包括物理拓扑和逻辑拓扑。*物理拓扑*是指物理结构上各种设备和传输介质的布局。物理拓扑通常有如下几种：

- 总线型。
- 环型。
- 星型。

- 扩展星型。
- 树型。
- 网状。

图2-39显示了各种不同的物理拓扑。

*逻辑拓扑*定义了发送数据的主机访问传输介质的方式。接下来的几小节将会描述各种不同类型的物理拓扑和逻辑拓扑。

图2-40显示了由网络设备连接起来的各种不同网络拓扑。该图显示了一个中等复杂程度的网络拓扑，它是学校或小型企业中的典型网络。

下面几小节将会详细地描述各种网络拓扑。

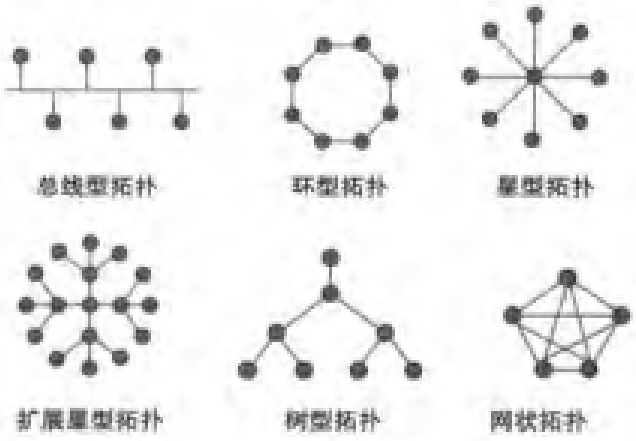


图2-39 各种不同物理拓扑

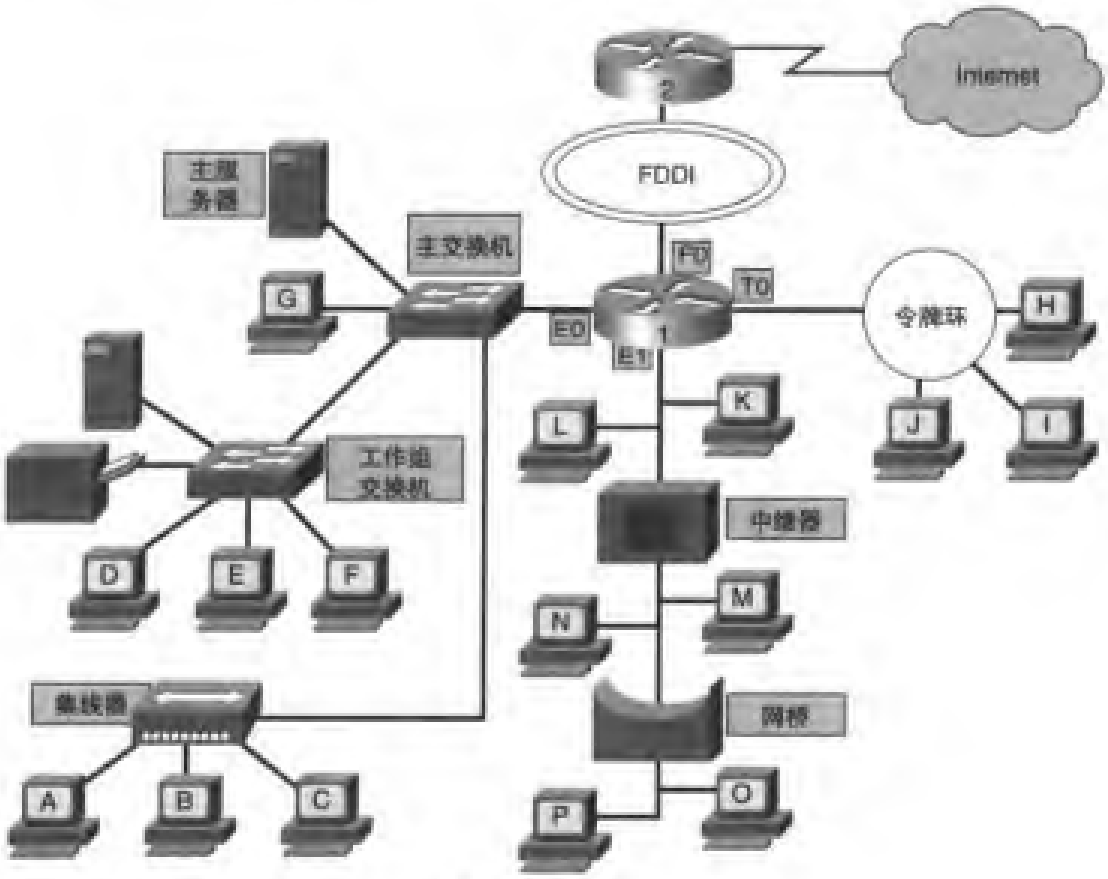


图2-40 网络拓扑

2.5.1 总线型拓扑结构

*总线型拓扑（bus topology）*通常也称为线性总线，它使用一根线缆来连接所有的设备（见图2-41）。线缆相继地连接各台计算机，就像一条公交线路穿过一个城市一样。

使用物理总线型拓扑时，主线缆段必须以终结器结束，因为终结器会吸收已到达线缆末端的信号。如果没有终结器，用来表示数据的电信号就会从线缆末端反射回线缆中，从而在网络中造成误码。

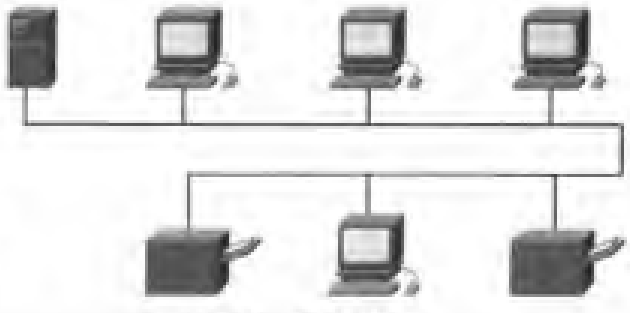


图2-41 总线型拓扑

2.5.2　星型和扩展星型拓扑

*星型拓扑（star topology）*是以太网内最普遍使用的物理拓扑结构，如图2-42所示。安装好了的星型拓扑就像自行车的轮辐。星型拓扑结构有一个中心汇集点（即诸如集线器、交换机或路由器之类的设备），所有的线缆分段都在此汇集。网络中的每个终端都通过独立的线缆连接到中心设备。

虽然构建物理星型拓扑比总线型拓扑的成本要高，但是用这些高出的成本换取星型拓扑结构的优点也是值得的。因为每个终端都是通过独立的线缆接入中心设备，所以当该线缆出问题时，只会影响到该终端而网络中其余终端依然可以正常地工作。这个优点非常重要，这也是为什么事实上所有新建的以太网都使用物理星型拓扑结构的原因。

出于安全性或访问控制的考虑，中心连接点或许正是我们想要的，但是它也是星型拓扑的主要缺点。如果中心连接点出现故障，则整个网络都无法连通。

当星型拓扑扩展到包含连接到其他主要网络设备的额外网络设备时就称为*扩展星型拓扑（extended-star topology）*，如图2-43所示。



图2-42　星型拓扑

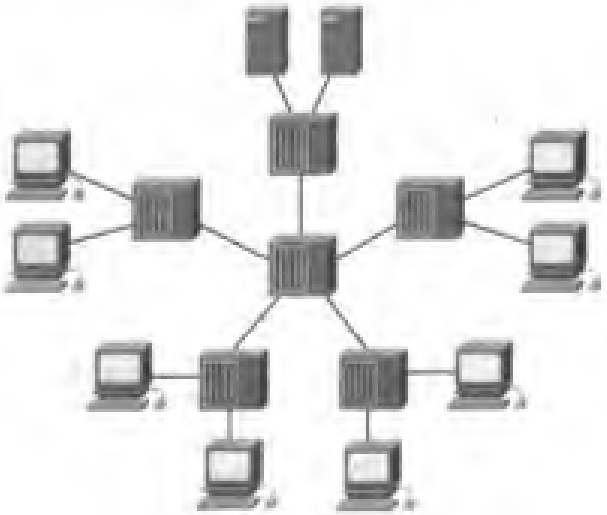


图2-43　扩展星型拓扑

2.5.3　环型拓扑结构

逻辑*环型拓扑结构（ring topology）*是LAN连接中另一种重要的拓扑结构。顾名思义，环形拓扑就是所有主机都连接成一个环或圆。与物理总线拓扑不同，环型拓扑结构没有需要结束的始端和末端。数据的传输方式与逻辑总线结构完全不同。在环形拓扑中，帧沿着环传输，在每个节点处都会停留。如果该节点想要发送数据，它就可以将自己想要传输的数据和目的地址添加到该帧中，然后该帧继续沿着环传输直到它找到目的节点并让目的节点从中获取所需要的数据为止。这种做法的优点是在传输过程中没有任何冲突。

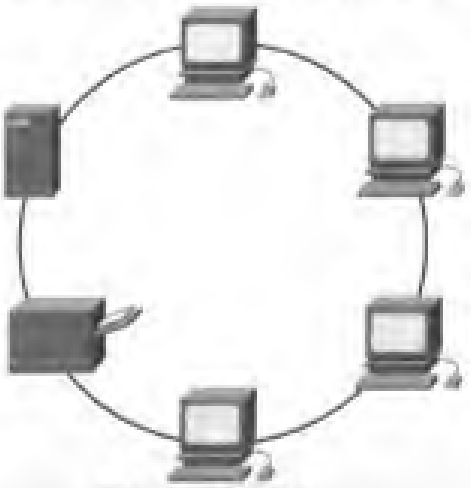


图2-44　环型拓扑

有两种环型结构：

- 单环。
- 双环。

如图2-44所示，单环结构中，网络中所有的设备共享一条线缆，并且数据只沿一个方向传输。每个设备必须等待直到轮到它发送数据的时候，才可以发送数据。大多数的单环

拓扑实际上都连接成星型。

如图2-45所示，双环结构中，数据可以双向传输。双环拓扑具有冗余性（容错性），当其中一个环出现故障以后，数据依然能够在另一个环中传输。如果两个环都出现故障，则故障点的“旁路系统”能自动使双环愈合成单环。

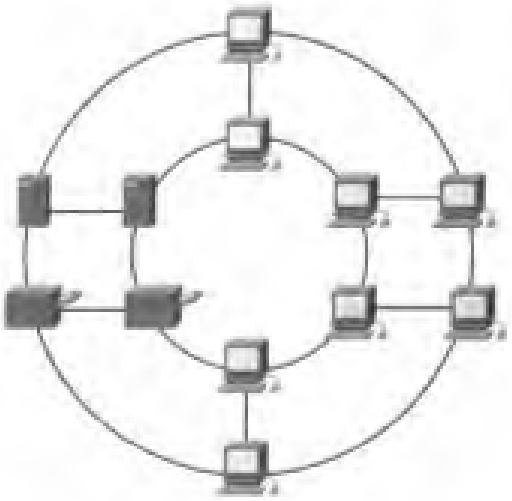


图2-45 双环型拓扑

2.5.4 树型拓扑结构

*树型拓扑结构（Hierarchical topology）*和扩展星型拓扑类似。它们的主要不同之处在于树型拓扑没有使用一个中心节点，而是使用了一个根节点，其他节点再从该节点引出，如图2-46所示。存在两种类型的树型拓扑结构：二叉树（每个节点分成两个分支）以及骨干树（各分支节点都从树干中引出）。

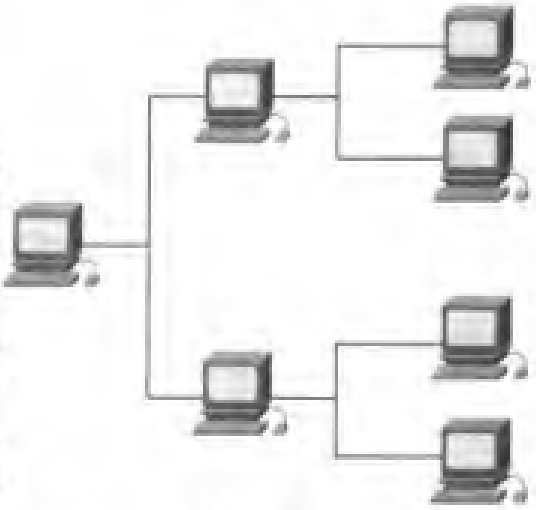


图2-46 树型拓扑

2.5.5 全互连网状和部分互连网状拓扑

*全互连网状拓扑（full-mesh topology）*中，所有设备（节点）都两两相连以提供冗余性和容错性，如图2-47所示。这种布线方式有明显的优点和缺点。优点是每个节点在物理上都与其他节点连接，从而创建了冗余连接。如果某一条线路出了故障，信息仍然可以通过多条其他的链路达到目的地。主要缺点是当网络节点变得较多时，链路介质的数量以及链路间连接的数量就会变得异常之大。因此，实现全互连网状的拓扑是非常昂贵和困难的，通常只在路由器之间的WAN中才采用这种拓扑。

在*部分互连网状拓扑（partial-mesh topology）*中，至少有一个节点与其他所有节点相连，只不过不是所有节点都这样相连，如图2-48所示。由于拓扑中具有几个可替代的路由器，故部分互连网络拓扑仍然具有冗余性。因此，当其中某条路由变得不可用时，数据依然能够采用其他路径，即使该路径可能要长一些。这种拓扑用于许多通信骨干网以

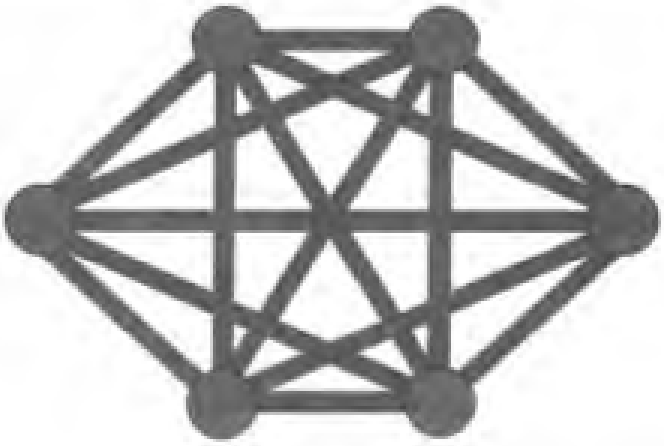


图2-47 全互连网状拓扑

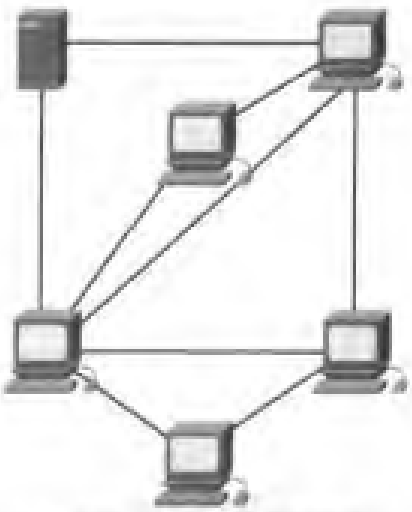


图2-48 部分互连网状拓扑

及Internet中，

2.5.6 逻辑拓扑

网络的逻辑拓扑是指各台主机通过传输介质相互通信的方式。最常见的两种逻辑拓扑形式是广播和*令牌传递（token passing）*。

广播拓扑即是每台主机都把所要发送的数据的目标地址设为网络介质上的某个特定NIC地址、多播地址或者广播地址，然后把该数据发送到传输介质中。每台主机使用传输介质时不必遵循某种次序，即先来先服务。以太网也是采用这种方式来工作的，如后面的课程所阐述。

第二种逻辑拓扑是令牌传递。令牌传递通过向各个节点顺序传递一个电子令牌来控制网络介质的访问。当一个节点接收到令牌时，它就可以把数据发送到网络介质上；如果该节点没有数据要发送，那么就将令牌传递给下一个节点，如此循环下去。使用令牌传递的其中两个例子是令牌环和光纤分布式数据接口（FDDI）。它们也都是物理环型拓扑上使用令牌传递的两个例子。

2.6 总结

本章学习了以下知识点：

- LAN和WAN发展的历史原因。
- LAN由计算机、网卡、外围设备、网络传输介质以及网络设备所组成。
- WAN由两个或多个分布在不同物理区域的LAN所组成。
- MAN跨越一个城市的区域，如市区或郊区。
- SAN增强了系统的性能，具有可扩展性和内在的容许灾难性故障的能力。
- 数据中心是全球协作的设备网络，用来在Internet网络基础设施上加速信息的传递。
- Intranet设计用于让有权访问企业内部网的用户访问企业内部网。Extranet设计用于提供应用和服务，但是需要对外部用户或企业使用扩展的、安全的访问机制。
- VPN是在公共网络基础设施上构建的专用网络。它主要有三类：接入型、企业内部互连型和企业外部互连型VPN。
- 带宽（bandwith）和吞吐量（throughput）是用来衡量网络速度和容量的标准。
- 将复杂的问题拆分成几个小单元有助于理解较大的问题。
- 通信（communication）是一个复杂的问题，可以将它划分为若干层来处理。划分体系有多种。
- 1984年，ISO开发出并公布了OSI参考模型，为众多生产厂商提供了一套标准以确保各种不同类型的网络技术之间有更好的兼容性和互操作性。
- OSI参考模型是一个描述性的网络架构，该标准确保各种不同类型的网络技术之间有更好的兼容性和互操作性。
- OSI参考模型的每一层都有特定的功能和协议。这7层分别是：应用层、表示层、会话层、传输层、网络层、数据链路层和物理层。
- 发送端通信协议的每一层都与接收端的对等层进行通信。
- TCP/IP模型有4层：应用层、传输层、Internet层和网络访问层。
- 网络中的所有通信都是始于源，终于目的地。因此，数据在发送之前必须封装上一些必要的协议信息。
- 网络设备是用来互连各种网络的，集线器、交换机和路由器是用来互连LAN、MAN和WAN的设备。各种网络设备工作在OSI参考模型的不同层上。
- 在把信号发送到网络之前，中继器会对它们进行再生、放大和重定时。
- 当涉及到网络中心点的设备时，就会使用术语*集线器（hub）*而不使用*中继器（repeater）*。

Hub（也可以认为是多端口中继器）工作在第1层，它不对数据作任何判断。只有hub的网络环境是一种共享访问型的网络环境，在其中会发生冲突。添加到这种网络的设备越多，冲突也就越多，从而引起网络性能急剧下降。

- LAN交换机工作在第2层，它基于MAC硬件地址作出有限的决策。交换机提供专用的LAN连接。
- 多层交换机工作在第2、3、4层，它可以实现第3层的服务质量（QoS）和安全功能。多层交换机的许多功能与路由器一样，只不过它们是通过硬件实现的。
- 路由器能为网络中的数据传递选择最佳的路径。
- 多种服务器为计算机和用户提供网络接入的服务。例如，防火墙、AAA服务器和VPN集中器都能为网络提供安全服务。
- 多种无线网络设备为计算机和用户提供了无线网络接入服务。常见的无线网络设备包括无线适配器、无线接入点和无线网桥。
- 物理拓扑描述了各个节点之间是如何通过电缆连接的，而逻辑拓扑则描述了网络中信息是如何传递的。
- 在物理总线型拓扑中，一条电缆连接所有设备。
- 以太网中最普遍使用的是物理星型拓扑。在该拓扑中，网络中每个节点使用各自的线缆连接到中心节点。当星型网络扩展到包括连接到其他主要网络设备的额外的网络设备时，它就称之为扩展星型拓扑。
- 环型拓扑中，所有节点连接成一个环或圆。
- 全互连网状拓扑中，所有的节点都两两相连。

为了补充你在本章所学的知识，请参考本书配套光盘中对应章节的视频、插图和e-Lab实验。

2.7　关键术语

应用层（*application layer*）　OSI参考模型的第7层。这一层为OSI参考模型外的应用程序（例如电子邮件、文件传输和终端仿真）提供服务。

带宽（*bandwidth*）　在一定时间内通过某一网络连接的信息量。

网桥（*bridge*）　第2层设备，设计用于创建两个或两个以上的LAN分段，使得每个分段都是一个独立的冲突域。

广播（broadcast）向网络中的所有节点发送数据分组。它由广播地址所标识。

广播域（*broadcast domain*）　所有能接收到集合内任一节点发出的广播帧的设备的集合。

总线型拓扑（*bus topology*）　通常也称为线性总线，它通过一条线缆连接所有的设备。这根线缆相继地连接各台计算机，就像一条公交线路贯穿整个城市一样。

冲突（*collision*）　冲突是以太网中两个节点同时发送数据所致。当从这两个节点发出的帧在物理介质上相遇时，它们将会发生冲突，而且彼此的数据都会遭到破坏。

冲突域（*collision domain*）　在以太网中，冲突域指的是已发生冲突的帧还能在其中继续传播的网络区域。中继器和集线器都能传播冲突，局域网交换机、网桥和路由器则不会。

数据中心（*data center*）　数据中心是全球协作的特定设备网络，用来在Internet网络基础设施上加速信息的传递。

数据链路层（*data link layer*）　OSI参考模型的第2层，该层提供了通过物理链路的数据传输功能。数据链路层主要考虑的方面有：物理寻址、网络拓扑、线路规程、错误通知、帧的顺序传输以及流量控制。

解封装（*de-encapsulation*）　把数据从特定的协议头中解封出来。

封装（*encapsulation*）　用特定的协议头将数据进行封装。

扩展星型拓扑（*extended-star topology*）　当星型网络扩展到包括连接到其他主要网络设备的额外的网络设备时，就称为扩展星型拓扑。

企业外部互联网（*extranet*）　基于Intranet的应用和服务，它对外部用户和企业实施了扩展的、安全的访问机制。

防火墙（*firewall*）　防火墙是路由器或者接入服务器，用作连接公共网络和私有网络的缓冲器。

泛洪（*flooding*）　交换机和网桥使用的信息传输技术，它指的是把从某个接口接收到的信息，再向除最初接收到该信息的接口以外的所有接口发送出去。

帧（*frame*）　作为数据链路层单元在传输介质上传输的信息逻辑组。

全网状拓扑（*full-mesh topology*）　所有节点都两两连接，具有冗余性和容错性。

树型拓扑（*hierarchical topology*）　与扩展星型拓扑十分相似，主要的区别是它不使用中心节点，而是使用主干（trunk）节点来连接其他分枝节点。

集线器（*hub*）　网络中设备的公共连接点，它通常用于连接LAN的各个分段。一个hub有多个端口。当一个分组到达某个端口时，hub就会将其发送到其他所有端口上，以便该分组能够到达LAN中的所有分段。

企业内部互联网（*intranet*）　一种通用的LAN配置。Intranet用来为那些有权访问企业内部LAN的用户提供接入。

局域网（*local-area network*，*LAN*） 在一个相对小的区域（最大至几千米）内的高速、低误码率的数据网络。LAN连接着一栋楼或者其他有限地理区域内的工作站、外围设备、终端及其他设备。

介质访问控制（*Media Access Control*，*MAC*） 惟一标识网络中每个节点的硬件地址。该地址控制了网络中节点的数据通信方式。

城域网（*metropolitan-area network*，*MAN*） 覆盖一个城市的网络。通常MAN地理覆盖范围比LAN大，而比WAN要小。

微分段（*microsegmentation*） 微分段可以创建专用的网段——一台主机一个分段。每台主机都可以享用全部带宽而不用跟其他主机竞争可用的带宽。

网络接口卡（*network interface card*，*NIC*） 插入计算机主板总线扩展插槽的印刷电路板，也可以是计算机的外围设备。

网络层（*network layer*） OSI参考模型的第3层。该层为两个终端提供连接性和路径选择。网络层也是路由选择所在的层。

开放系统互联参考模型（*Open System Interconnection reference model*） 是由ISO提出的一个网络体系结构模型。该模型分为七层，每一层都有特定的网络功能，例如寻址、流量控制、差错控制、封装和可靠信息传输。OSI参考模型广泛地用作教学和理解网络功能的一种方法。

分组（*packet*） 即信息逻辑组，其中包含有包含控制信息的报头和（通常是）用户数据。它通常指网络层的数据单元。

部分网状拓扑（*partial-mesh topology*） 至少一个节点保持着与其他节点的多个连接，但不是全互连。由于该拓扑中具有可替代的路由，因此它仍然具有冗余性。

对等层通信（*peer-to-peer communication*） 一种通信形式，即位于源的OSI模型的每一层都必须与目的地的对等层进行通信。

物理层（*physical layer*） OSI参考模型的第1层。物理层定义了电气的、机械的、操作规程的以及功能的规范，以便激活、维护和终止系统间的物理链路。

表示层（*presentation layer*） OSI参考模型的第6层。该层确保由某个系统的应用层所发送的信息能被另一个系统的应用层读取。

协议（*protocol*） 控制网络设备如何交换信息的一套规则和约定的正式描述。

协议集（*protocol suite*） 一组通信协议，它们一起工作，在OSI参考模型的某几层或全部7层中作为一个组进行通信。并不是每一个协议栈都包含OSI模型的每一层，通常协议集中的一个协议就涉及到几层。TCP/IP是一个典型的协议集。

中继器（*repeater*） 工作在OSI参考模型的第1层（即物理层）的网络设备。其目的是对信号在比特级别进行再生、重定时和放大，以使得这些信号可以在介质上传输得更远。

环型拓扑（*ring topology*） 一种所有节点连接成一个环或圆的拓扑结构。与物理总线拓扑不同，环型拓扑没有起始点和终结点，因此也不需要终结器。

路由器（*router*） 一种互连网络的设备，它基于第3层的地址来在网络间传递数据分组。

分段（*segment*） TTCP规范中使用的术语，OSI参考模型中传输层的一个逻辑信息单元。

会话层（*session layer*） OSI参考模型的第5层。该层负责建立、管理和终止应用程序间的会话，并管

理表示层实体间的数据交换。

星型拓扑（*star topology*） 以太网中最普遍使用的是物理拓扑。星型拓扑由中心连接点（诸如集线器、交换机或路由器之类的设备）所组成，所有的线缆分段都聚集于此。

存储区域网（*storage-area network*，*SAN*） 在服务器与存储资源间传输数据的专用的、高性能的网络。

交换机（*switch*） 用于连接LAN分段的一种设备，它利用MAC地址表来判断数据帧应该发往哪一个分段，因而减少了通信量。交换机的处理速度比网桥高得多。

吞吐量（*throughput*） 网络中到达或通过某个特定的点的信息速率。

令牌传递（*token passing*） 一种访问介质的方式，即网络设备通过获得一个称为令牌的小帧而按顺序访问介质的方式。

传输层（*transport layer*） OSI参考模型的第4层。这一层负责终端节点之间的可靠的网络通信。它提供了一种建立、维护和终止虚拟链路，以及传输失效检测和恢复、信息流量控制的机制。

虚拟专用网（*virtual private network*，*VPN*） 在公共网络基础设施（如全球性的Internet）之上构建的专用网络。

广域网（*wide-area netowrk*，*WAN*） 一种数据传输网络，它在广阔的地理范围内为用户提供服务，它通常使用公众通信公司提供的传输设备。

2.8 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 下面哪一项是首个实现的微型计算机网络类型？
   A. 城域网
   B. 广域网
   C. 局域网
   D. 个人域网络
   （注：个人域网络（PAN）指的是通过蓝牙支持设备由个人创建的短程网络。当这些设备处于范围之内时，无需线缆就可以自动配对并连接在一起。）
2. 如果使用modem连接10台计算机，需要多少个modem？
   A. 1
   B. 5
   C. 10
   D. 15
3. 写入到网络接口卡上的编码是什么？
   A. 网络接口卡
   B. MAC地址
   C. 集线器
   D. 局域网
4. 哪种物理拓扑结构的所有节点直接连接到一个中心节点且在节点之间没有其他连接？
   A. 总线型
   B. 环型
   C. 星型
   D. 网状
5. TIA和EIA代表什么？
   A. 电视工业协会（Television Industry Association）和电子工业协会（Electronic Industries Association）
   B. 电信工业协会（Telecommunications Industry Association）和电子工业联盟（Electronic Industries Alliance）
   C. 电信工业联盟（Telecommunications Industry Alliance）和电子工业协会（Electronic Industries Association）
   D. 电话国际协会（Téléphonique International Association）和电报工业联盟（Elégraphique Industries Alliance）
6. 局域网完成以下哪些工作？（选择所有正确的项）
   A. 在一个有限的地理范围内运作
   B. 允许多个用户同时接入高带宽物理介质
   C. 连接到Internet
   D. 提供本地服务器的全时连接
7. 下面哪个句子最好地描述了广域网？
   A. 它连接被大的地理区域分割开的局域网络
   B. 它连接一个大城市中的工作站、终端以及其他设备
   C. 它连接一个大的建筑物里面的局域网络

D. 它连接一个建筑物里面的工作站、终端以及其他设备

8. 下面哪个句子正确地描述了城域网？

A. 城域网是在一个建筑物里面连接工作站、外围设备、终端以及其他设备的网络

B. 城域网跨越广阔的地理区域为用户提供服务；它通常使用公众通信公司提供的传输设备。

C. 城域网是跨越一个城市（都市或郊区）的网络

D. 城域网是由路由器和其他设备相互连接起来的网络，它完成一个独立网络的功能

9. 下面哪一项不是存储区域网（SAN）的特征？

A. 存储区域网允许对磁盘或磁带阵列的同时访问，加强系统性能

B. 存储区域网提供可靠的灾难恢复解决方案

C. 存储区域网具有可扩展性

D. 存储区域网使系统和数据的可用性最小化

10. 以下哪个服务在共享的公共网络基础设施上提供安全、可靠的连接？

A. Internet

B. 虚拟专用网

C. 虚拟公共网

D. 广域网

11. 下列哪个在共享基础网络设施上把企业总部、远程办事处以及分支机构连接成一个内部网络？

A. 接入VPN

B. Intranet VPN

C. Extranet VPN

D. Internet VPN

12. 公司网络中可以用来选择诸如雇员、客户和合作伙伴之类的团体的那一部分网络叫什么？

A. Internet

B. 企业外部网

C. 企业内部网

D. 局域网

13. 对象在模型各层间的运动叫什么？

A. 封装（warpping）

B. 流（flow）

C. 移动（traveling）

D. 传输（transmission）

14. OSI参考模型有几层？

A. 4

B. 5

C. 6

D. 7

15. OSI参考模型是什么？

A. 一个规定信息在网络中如何传递的概念框架

B. 一个描述网络中数据如何在应用程序之间传递的模型

C. 一个规定各层网络功能的概念框架

D. 以上全部

16. 下面哪一项是网络各层的正确顺序？

A.
（1）物理层
（2）数据链路层
（3）传输层
（4）网络层
（5）表示层
（6）会话层
（7）应用层

B.
（1）物理层
（2）数据链路层
（3）网络层
（4）传输层
（5）会话层
（6）表示层
（7）应用层

C.
（1）物理层
（2）数据链路层
（3）网络层
（4）会话层
（5）传输层
（6）应用层
（7）表示层

D.
（1）物理层
（2）网络层
（3）会话层
（4）数据链路层
（5）传输层
（6）应用层
（7）表示层

17. OSI模型的哪一层涉及物理寻址、网络拓扑结构、网络介质访问以及流量控制？

A. 物理层
B. 数据链路层
C. 传输层
D. 网络层

18. 以下哪一项最好地定义了封装？

A. 对数据进行分段以便它在网络中连续地流动
B. 对数据进行压缩以使传输得更快
C. 对数据进行分组以便一些数据能放在一起

D. 把数据打包在一个特定的协议报头中

19. 在一个局域网上从主机A向主机B发送一封电子邮件，在开始发送电子邮件以前，必须对数据进行封装。下面哪一项最好地描述了在生成一个分组以后所发生的事情？

A. 分组被沿着介质传送

B. 分组被放到一个帧里

C. 该分组被分段为若干帧

D. 该分组被转化为二进制格式

20. 在TCP/IP模型中，哪一层处理关于可靠性、流量控制和错误校正等问题？

A. 应用层

B. 传输层

C. Internet层

D. 网络接入层

21. 对于下面的哪些问题中继器可以提供一个简单的解决方案？

A. 网络上存在太多类型的不兼容设备

B. 网络上存在过多的流量

C. 收敛速率过低

D. 过多的节点或线缆不足

22. 关于网桥和它的转发决策，下面哪一项是正确的？

A. 它们运行在OSI的第2层而且使用IP地址来做出转发决策

B. 它们运行在OSI的第3层而且使用IP地址来做出转发决策

C. 它们运行在OSI的第2层而且使用MAC地址来做出转发决策

D. 它们运行在OSI的第3层而且使用MAC地址来做出转发决策

23. 关于交换机的功能下面哪一项是正确的？

A. 增加了冲突域的规模

B. 结合了集线器的连接功能和网桥的流量管理功能

C. 结合了集线器的连接功能和路由器的流量传送功能

D. 可执行第4层的路径选择功能

24. 路由器会对什么作出路由选择？

A. 第1层的比特

B. 第2层的帧

C. 第3层的分组

D. 第4层的分段

25. 下面哪一项是正确的？

A. 网关是具有特定目的设备，实现应用层不同协议栈之间的转换

B. CiscoAS5400 系列通用网关提供了通用端口，使得能在任何时候、任何端口上提供数据、语音、无线以及传真服务

C. DSLAM 充当无数用户设备和通信公司网络之间的接口

D. 上述答案都正确

26. 下面哪些是AAA服务器的功能？（选择所有正确的项）

A. 确保只有通过认证的用户才可以进入网络

B. 确保用户只能访问他们所需要的资源

C. 确保对所有授权用户进入网络后的操作进行记录

D. 上述答案都正确

27. 下面哪些是防火墙的功能？（选择所有正确的项）

A. 基于软件的

B. 基于硬件的

C. 过滤通信流

D. 第2层设备

E. 上述答案都不正确



第3章　网络介质

目标

学习完本章之后，你应该能够：

- 描述原子的主要构成。
- 描述测量电流的术语。
- 熟悉制定有线、无线网络标准的组织。
- 描述双绞电缆的主要类型和用途。
- 描述同轴电缆的主要类型和用途。
- 描述光缆的主要类型和用途。
- 描述无线介质的主要类型和用途。
- 描述各种类型的无线数据通信以及它们各自的优点和不足。
- 描述不同的调制技术。
- 描述无线电频率调制。
- 描述扩频技术的优点。
- 描述跳频扩频和顺序扩频。
- 解释无线环境下加密和安全措施的重要性。

物理层的作用是通过在源和目的之间定义电气的、无线的或光的规范来传输数据。到达建筑物后，低压电流通过隐藏在墙体、地板和天花板内的电线输送到工作站、服务器和网络设备。由文字、图片、音频或视频组成的数据，通过线路传送，并以铜导线里的电子脉冲或光纤里的光脉冲的形式表示。

本章将介绍电学基本理论，为理解OSI模型物理层的网络连接打下基础。本章还将讨论物理层中所用到的各种网络介质，包括屏蔽双绞线电缆、非屏蔽双绞线电缆、同轴电缆和光缆，以及无线介质。

请务必看看关于本章的e-Lab实验活动、视频和插图，这些内容可以在本书所附的光盘中找到。光盘中的这些内容用作补充材料，能强化本章中所介绍的概念。

3.1　电学基础

本节将介绍电学的基本理论，这为理解OSI参考模型的物理层（第1层）的网络连接打下了基础。

3.1.1　原子和分子

宇宙万物的基本单元是原子。原子由三个微小部分构成：质子、中子和电子。质子和中子聚集在一个小分组内，称为原子核。电子围绕原子核做自由运动。这三部分结合在一起就构成了一个原子。图3-1所示的元素周期表列出了所有已知类型的原子和它们的属性。原子由三种基本粒子组成：

- **质子**——带正电的粒子。
- **中子**——不带电的粒子。
- **电子**——带负电的粒子。

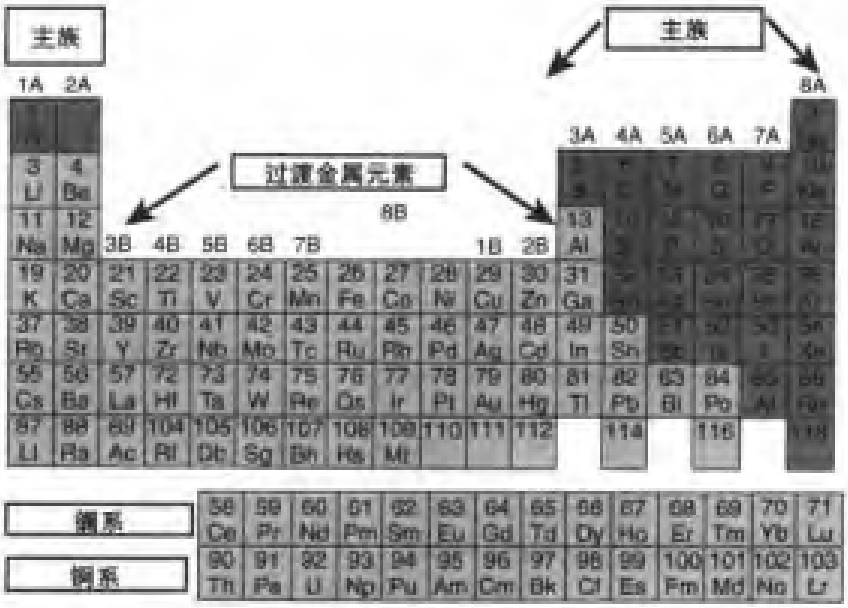


图3-1　元素周期表

原子通常具有同等数量的质子和电子，由于正负电荷相等，所以原子不带电。

丹麦物理学家尼尔斯·玻尔提出一种表示原子的简化模型，如图3-2所示。此图示例了氦原子的玻尔模型，它包含两个质子、两个中子和两个电子。质子和中子在原子中心形成原子核，电子标在围绕原子核的轨道上。此图不是按照比例来画的，不过，如果这个原子的质子和中子的大小如足球场中央的足球的话，电子就只有樱桃大小，并围绕足球场的最外圈的看台旋转。与原子核相比，电子很小，但其运行轨道与这些粒子相比非常大，尽管原子自身也是微观的。

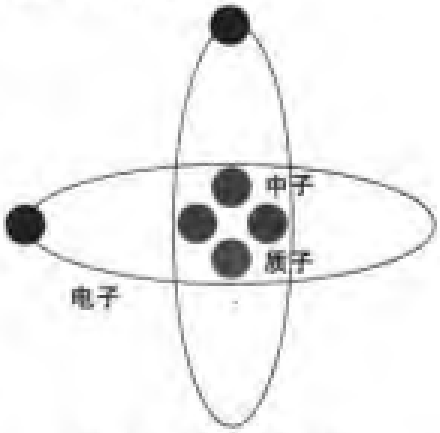


图3-2　氦原子玻尔模型

多种原子以不同的方式组合在一起，就构成了各种物质的分子，比如，氢原子和氧原子结合形成水分子。

3.1.2　物质的电属性

原子的原子核被一股强大的力量束缚在一起，而将电子束缚在原子核轨道上的引力却弱得多。原子中的电子可能脱离原来的轨道而进入临近原子的轨道。电子的这种运动被定义为电流。

如果一个原子失去或得到一个电子，它就不再具有相同数目的电子和质子。这样的原子叫做离子，因为质子、电子数目不同，它带有净电荷。离子的电荷对相邻原子的引力可以使它们得到或失去电子。这样，随着相邻原子的电子移动，电流就通过物质流动。

根据电子脱离轨道的难易程度，原子和分子可以被分为三种类型：绝缘体、导体和半导体。表

3-1中进行了总结。

表3-1 三类主要电材料的总结

物质	流动	例子
绝缘体	电子不流动	塑料，纸张，干木头，空气，纯水，玻璃
导体	电子顺利流动	铜，银，金，焊料，含有离子的水，人的身体
半导体	电子流动可控制	碳，锗，镓，砷化物，硅

绝缘体

绝缘体是由原子或分子构成的材料，其电子需要巨大的力量才能脱离轨道。比如塑料、玻璃、空气、干木头、纸、氮气和纯水（其构成原子不是离子）。

导体

导体是由原子或分子构成的材料，其原子核对电子束缚力很小，很小的力便可使电子脱离轨道。元素周期表将原子分组，按列排出。最好的导体被排在图3-1中特别的一列：铜（Cu），银（Ag），金（Au）。其他导体包括铅焊料（铅（Pb）与锡（Sn）的混合物），带有离子的水。因为人体中近70%都是离子化的水，所以也是导体。

半导体

半导体是由原子或分子构成的材料，其电子的移动可以精确控制。最重要的半导体是硅，其他导体还包括位于元素周期表同一列的碳（C）和锗（Ge）。砷化镓（GaAs）分子也是常见的半导体。

硅很普遍，在沙、玻璃和多种岩石里都可以找到。圣何塞、加利福尼亚一带就以硅谷闻名，因为依靠硅制芯片的电脑产业就是在这里兴起的。微处理器内的开关或门就是由半导体组成的。

3.2 电的测量

与其他的物理过程和概念一样，要使用电就必须能对其进行测量。测量的方法多种多样，本节着重讲述电压、电流、电阻和阻抗。

3.2.1 电压

因为电子和质子带有相反的电荷，它们被一种类似于磁铁南北两极之间引力的力相互吸引。电荷分离时，会在周围产生引力场或压力场，这种力就是电压。所产生的这种力使同种电荷相斥，异种电荷相吸。在电池里就存在这一过程：化学反应使电子通过外部电路而非电池本身从电池的负极向正极移动。这种电荷的间距产生了电压。电压还可以通过摩擦（静电）、磁极（发电机）或太阳能产生。

电压用字母*V*来表示。测量电压的单位是伏特，也用字母*V*来表示（例如，12*V*=12伏特）。

电压分两种：

- **直流（DC）电压**——电池是直流电压源的一个例子。在直流电路里，电子总是沿着相同方向从负极移动到正极。
- **交流（AC）电压**——在交流电路中，电源的正负极定期地变为负极和正极，然后再改变回去，如图3-3所示。这种变化使电子运动的方向随时间变化而

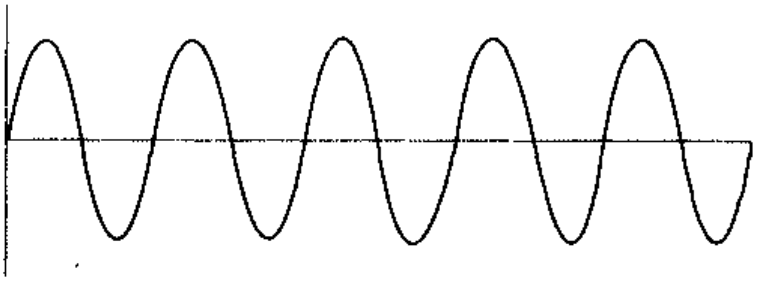


图3-3 交流电

改变或交替。

实验活动　安全使用万用表

在本实验中，学会怎样正确使用万用表。

实验活动　电压测量

在本实验中，学会用万用表测电压。

3.2.2　电流

电流是电荷的移动，在电子移动时产生。只要有电压和电流通过的路径，电子便从负极（负极排斥电子）沿路径向正极移动（正极吸引电子）。

电流用字母*I*表示。测量电流的单位是安培，用字母A或“安培”表示，安培通过每秒通过某一点的电荷量来定义。可以被想像为通过电路的电子数量，通过电路某一点电子数量越多，电流就越大。

直流电压产生的电流总沿着相同的方向从负极流向正极，交流电压产生的电流先沿一个方向流动，然后改变方向，接着又变回原来的方向，周而复始。

3.2.3　瓦特

如果电流可以被看作流动电子运动的数量，电压就可以被看作电子运动的速度。电流（经过某点的电子数量）和电压（电子的压力或速度）的乘积等于*瓦特*或电功。电功的基本单位是瓦特（W）。瓦特等于伏特数乘安培数（W=V×I）。电器，比如灯泡、发动机和计算机电源，所消耗或产生的电能都用瓦特来计量。真正完成这项工作的是电路中的电流或称安培数。比如，静电的电压很高，放电距离可能会超过3cm，但它的电流很小，虽然会使人颤抖一下，但不会造成伤害。汽车里的发动机大概需要12V的低电压，但却要很高的电流以产生足够的能量启动引擎。闪电的电压和电流都很高，能造成严重的破坏或伤害。

3.2.4　电阻和阻抗

导体可以很容易地传导电子，因此不需要太高的电压使电子通过。相反，在绝缘体中，电子被更加牢固地束缚在自己的轨道上，因此，电子移动受到阻碍。***电阻***是物质阻碍电子移动的属性。导体的电阻低，绝缘体电阻高。

电阻用字母R来表示，测量电阻的单位是欧姆，用希腊字母Ω表示，因为Ω的读音与欧姆相似。

术语*电阻*一般用于描述直流电路，交流电路中的电阻叫做***阻抗***，用字母Z表示。与电阻相同，它的计量单位也是欧姆，也用Ω表示。

实验活动　电阻的测量

在本实验中，要求掌握用万用表测量电阻。

3.2.5　电路

电子在导电性材料中运动得最通畅。虽然干燥气候下的空气也可以导电，如静电电击，但是电子无法从电池中穿过空气流动到不相连接的铜线上。电流或者说是电子运动只在完整的环路中发生，这种电路即闭合电路。

图3-4显示了一个简单电路，里面有一盏灯。开关可以看作一条电线的两端，能够打开（或切

断）再闭合（或短路），从而切断或接通电流。

在图3-4上部的图中，灯及其开关都是断开的。电池里的化学过程使电荷分离，产生电压，但是因为没有电子运动的完整路径，所以没有电流，灯泡不亮。

在图3-4下部的图中，开关是接通的，形成电流流动的完整路径，电子流动过程中遇到灯泡的电阻，电流以光的形式释放能量。

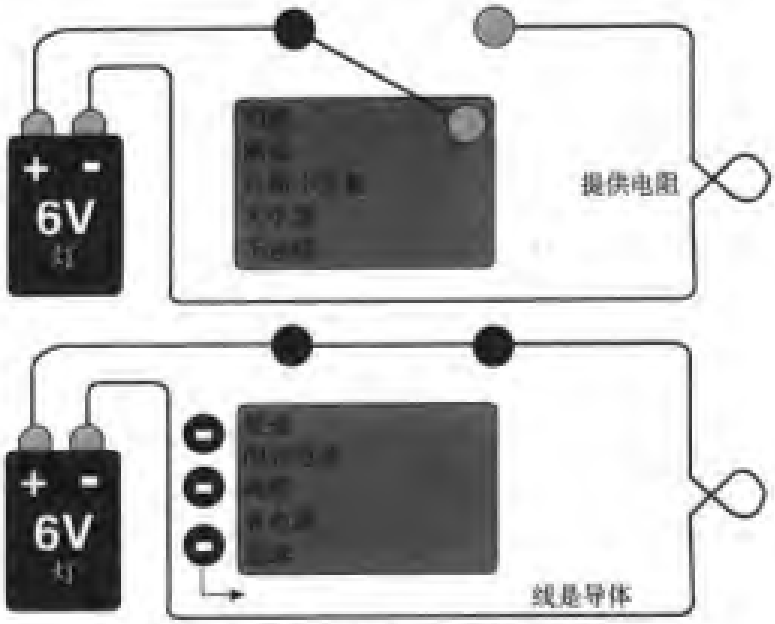


图3-4 串行电路——闪光灯

网络中的电路与这种简单电路原理相同，但复杂得多。当学习一个新概念时，将其与一个熟悉的例子相关联往往很有帮助。前面讨论的电路可以比喻为图3-5所示的水流路线。水箱里水的重量形成压力使水流动，水龙头好比前例中的开关。当龙头关闭时，阻止了水的流动；当龙头打开时，允许水流通过，同时也对水流产生一定的阻力，因为相比大水龙头，小水龙头只能通过较少的水流。最后，管道为水流回水缸提供了一个闭合的通道。

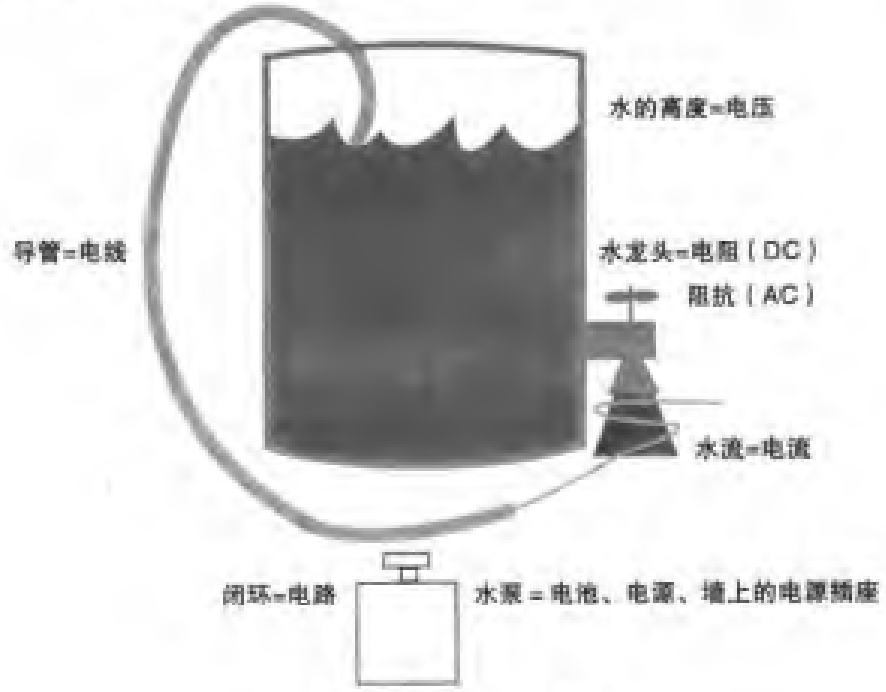


图3-5 水流类比电子流动



实验活动 通信电路

在本实验中，要求建立串行电路并探索其基本特征。

3.3 铜介质

铜是最常用的信号线缆介质。铜线是将信号从源计算机传送到目的计算机的线缆的组成部分。铜的几个重要特征使它很适合用作电缆：

• **导电性**——铜最著名的特征大概就是它对电流的传导性。同时，铜也是热的良导体。这一特征使它广泛用于厨具、散热器和冰箱。

• **抗腐蚀性**——铜不易生锈、不易被腐蚀。较之其他金属，铜的腐蚀如氧化等都慢得多。

• **韧性**——铜的柔韧性很好，可以被拉得很细又不被折断。比如，直径1cm的铜丝可以被加热、碾压，拉得比头发丝还要细。

• **可塑性**——纯铜的可塑性很强（容易定型）。它在被锤、压、锻或被做成不规则形状时不会被折断。铜在冷热状态下都可以被塑造。

• **强度**——冷轧铜的强度是3500~4900kg/cm^2。铜最多可在204℃时保持它的强度和韧性。

本节着重讲述用于网络的两种铜缆：

• **双绞线**——双绞线电缆由一对或多对铜线组成。大多数数据和语音网络均采用双绞线电缆。

• **同轴电缆**——*同轴电缆*以一根或硬或软的铜线作为中心导体。同轴电缆曾经被用作局域网缆线，现在主要用于视频连接、高速连接，比如T3（或E3）线路和有线电视。

3.3.1　美国线规

缆线或导体的直径常用美国线规（AWG）来度量。AWG是主要用于度量铜缆或铝缆直径的美国标准。典型的居民用电线是AWG12或AWG14；电话本地环路（从中心局到家庭或住宅区）的UTP中所用的导体或电线尺寸介于19AWG到26AWG之间。大多数新的电话线都在22AWG到26AWG之间，24AWG最常见。计量数字越低，电线越粗。粗电线的电阻较低，可以传输更多的电流，长距离传送信号的效果更好。24AWG的电线相当于直径1/24英寸（约0.106cm）。

3.3.2　双绞电缆

双绞电缆是用于电话通信和大多数现代以太网的缆线。一对电线形成一个可以传输数据的电路。电线绞合在一起，以防*串话*及相邻电线产生的噪声。

线对被绞合在一起有两个原因。首先，当电线传送电流时，电流在电线周围产生磁场，从而干扰了相邻电线。为解决这个问题，每对电线携带方向相反的两路信号，两个磁场也在相反的方向产生，因此可以相互抵消。这一过程叫做*抵消*。将电线对绞在一起可以使两条电线靠得更紧，从而保证在缆线内有效地抵消干扰。

其次，网络数据通过两条绞在一起的电线传送。每条线上有一份数据的拷贝，两份拷贝互为映像。这对信号被称为*差异信号*。如果两条线绞在一起，一条线上的噪声也会出现在另一条线上。当数据被收到时，一份拷贝被反转，然后将两路信号相比较。此时，接收器可以滤出噪声，因为噪声信号可以相互抵消。

双绞电缆的两种基本类型包括：屏蔽双绞线（STP）和非屏蔽双绞线（UTP）。接下来的一节将讨论UTP电缆和STP电缆的更多细节。

3.3.3　屏蔽双绞电缆

屏蔽双绞电缆（STP）由四对细铜线组成，它们绞在一起，每条线都外裹带色码的塑料绝缘体。每对电线包裹在金属箔片里，然后四对电线又包在另一层金属箔片或编织物中。这一层外面还包有一层塑料外套。图3-6展示了STP的一个例子。

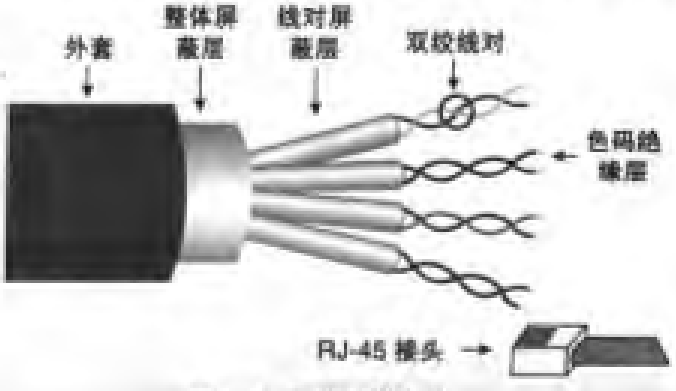


图3-6　屏蔽双绞电缆

外屏蔽双绞线（ScTP），也被称为箔片双绞线（FTP），是STP的一个变种。ScTP只有一层箔片包裹四对电线，如图3-7所示。STP和ScTP内的屏蔽减少了不必要的电子噪声，这成为STP相比非屏蔽电缆的一个主要优点。

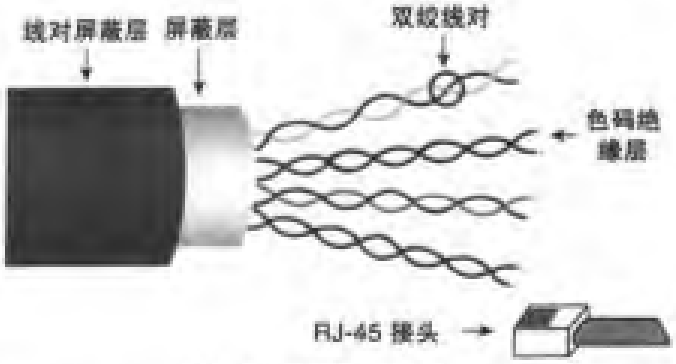


图3-7 屏蔽双绞电缆

然而，屏蔽电缆比非屏蔽电缆更难于安装，因为金属屏蔽需要接地。如果安装不当，STP和ScPT会对噪声问题非常敏感，因为不接地的屏蔽层会起天线的作用，接收各种无用的信号。如果不使用中继器，STP和ScTP电缆无法像同轴电缆和光缆那样进行远距离传输。绝缘层和屏蔽一定程度上增加了缆线尺寸、重量和成本。尽管有这些缺点，屏蔽铜缆线今天仍然用作网络介质，特别是在欧洲。

下面总结了STP缆线的一些特征：

- **速度和吞吐量**——10至100Mbit/s
- **每节点的平均成本**——较高。
- **介质和连接器的尺寸**——中大。
- **最大电缆长度**——100m（短）。

3.3.4 非屏蔽双绞电缆

非屏蔽双绞电缆（UTP）是一种常用的网络*介质*。它由四对细铜线组成，每对铜线都绞合一起，每根铜线都外裹带色码的塑料绝缘层，如图3-8所示。然后，线对外面整体包有一层塑料外套。UTP缆线使用的接头叫做RJ-45接头，如图3-9所示。

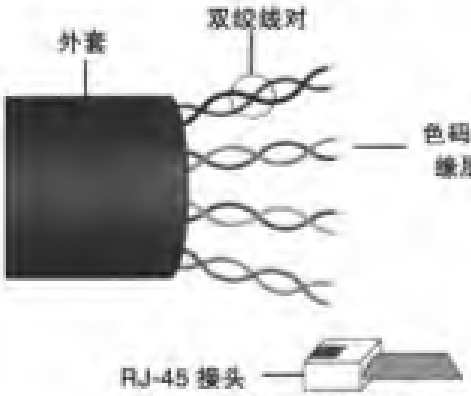
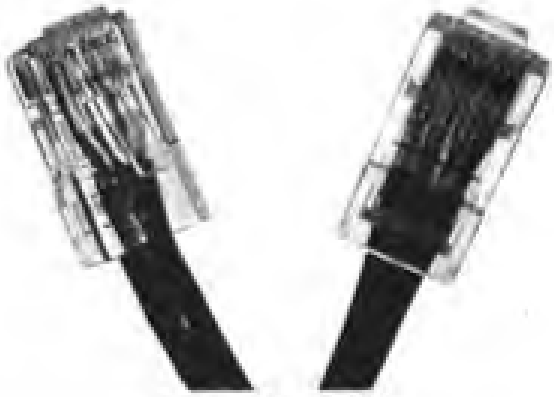


图3-8 非屏蔽双绞电缆


图3-9 RJ-45 接头

UTP缆线的优点很多。它直径小，不需要接地，因而易于安装。它的尺寸也是一个优势，因为在给定的空间内，可安装的UTP缆线数量比其他的铜介质更多。同时它也是最便宜的一种网络介质，接头也更容易安装。与其他铜介质一样，它也支持各种数据传输速率。

UTP的主要缺点在于，相比其他网络介质，它对电子噪声和干扰更为敏感。因为没有屏蔽，它只能靠“抵消”和“差异信号”来减少噪声。另一个主要缺点是它的最大传输距离小于同轴光缆和光纤电缆。

UTP曾经一度比其他电缆传输数据的速度慢，这种情况现在已经不存在了。事实上，UTP现在被看作传输速度最快的铜介质。UTP的几个主要特征如下：

- **速度和吞吐量**——10至1000Mbit/s。

- **每节点的平均成本**——最低。
- **介质和接头的尺寸**——小。
- **最大电缆长度**——100m（短）。

常用的UTP电缆类型如下：

- **1类（CAT 1）**——用于电话通信。不适合传输数据。
- **2类（CAT 2）**——可用于传输数据，最大速度为4Mbit/s。
- **3类（CAT 3）**——用于10BASET以太网，传输数据的最大速度为10Mbit/s。
- **4类（CAT 4）**——用于令牌环网络，传输数据的最大速度为16Mbit/s。
- **5类（CAT 5）**——用于快速以太网，传输数据的最大速度为100Mbit/s。
- **超5类（CAT 5e）**——用于最大传输速度为1000Mbit/s（1Gbit/s）的网络。用于吉比特以太网（GigE）。
- **6类（CAT 6）**——CAT 6的规范是2003年2月3日新提出的，现已可以安装和使用，用于吉比特以太网。

一般而言，5类及以上网络电缆由4对24AWG软铜线组成。旧的布线中3类传输语音，用5类来传输数据。最新的布线中用超5类以上的电缆来传送语音和数据。尽管超5类的成本较高，但从长期来看还是比较划算的。

对比UTP和STP时，关键点如下：

- 二者的传输速度通常适用于局域。
- 二者都是最便宜的数据传输介质。UTP比STP更便宜。
- 因为大多数建筑已经采用了UTP，所以许多传输标准也是根据它来制定，以避免改换其他电缆所耗的高昂成本。应当保证所使用的电缆类型满足带宽要求。比如用3类缆布线的建筑不能支持最低要求5类线缆的快速以太网。

3.3.5　同轴电缆

如图3-10所示，同轴电缆主要由四部分组成：

- 铜导线。
- 塑料绝缘层。
- 编织铜屏蔽层。
- 外套。

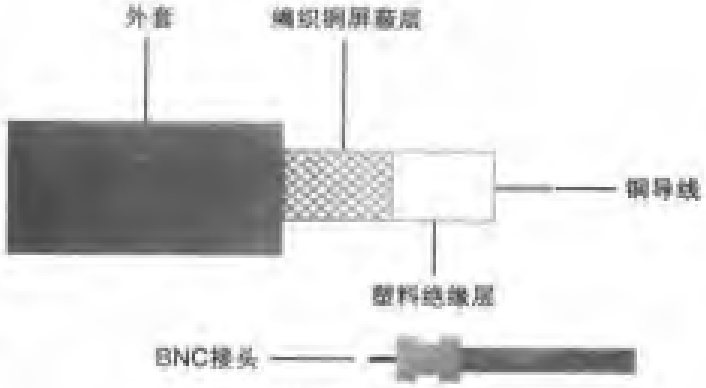


图3-10　同轴电缆

电缆中心是一根硬的铜导线，围绕导线有一层柔韧的塑料绝缘体，一层铜编织物或金属箔片包裹在绝缘体外面。这一层相当于电缆的第二根电线，同时对内部的导线也起到屏蔽的作用，帮助减少外部干扰。包裹这一层的是缆线的外套。用在同轴电缆中的接头叫同轴电缆接插头（BNC），是British Naval Connector或Bayonet Neill Concelman连接器的缩写。

同轴电缆过去曾广泛用于局域网，它有以下几个优点。与STP或UTP电缆相比，它实现长距离传输时所需要的中继器升压更少。它比UTP要贵，但比光缆便宜。这项技术已在多种数据传输中被运用多年，广为人知。比如，同轴电缆广泛用于家庭有线电视信号的传输和高速Internet接入。在有线电视领域，家庭中常用的RG-59电缆使用20AWG的导线。

RG-6最常用于从街边的线架到家的这段距离，因为其屏蔽层更重，中心导线也更大，达到

18AWG。RG-11的中心导线更重，达14AWG，用于将电缆连接到邻近的区域。

使用电缆时应当考虑它的尺寸。电缆的直径越大，使用越困难，因为承载缆线的导管大小是有限的。同轴电缆有多种不同的规格。其中直径最大的一种（1cm）以前曾专用于作以太网骨干电缆，因为相比其他类型的电缆，其传输距离更长，抗噪声的能力也更强。这种同轴电缆通常被称作**粗缆**，如图3-11所示。顾名思义，因为太粗、某些条件下，粗缆会显得太硬，不易安装。一般规律是，安装越困难，网络介质的安装费用越高。同轴电缆与双绞线电缆相比安装成本更高。粗缆只在一些特殊用途中才会使用。

直径为0.35厘米的同轴电缆有时被称为**细缆**，也曾经广泛用于以太网中。图3-12所示，细缆特别适用于需要进行很多扭曲和转向的场合。由于安装相对容易，因此安装费也相对较低。所以，有时被称为*低价缆*（*Cheapnet*）。



图3-11 同轴电缆——粗缆



图3-12 同轴电缆——细缆

然而，两种类型的同轴电缆都要求外传导层妥善接地，这加大了安装难度。正因为如此，虽然有优点，同轴电缆也不再被广泛用于以太网。

尽管全球范围内许多总线拓扑的网络仍然使用同轴电缆，IEEE已经不再鼓励将这种缆线或拓扑作为使用以太网的标准。几乎所有新的局域网都采用了以太网扩展星型拓扑、UTP和光纤的结合。

以下是对同轴电缆特征的一些总结：

- **速度与吞吐量**——10至100Mbit/s。
- **每节点的平均成本**——便宜。
- **介质尺寸**——中等。
- **最大线缆长度**——500m。

更多信息：阻燃电缆

阻燃电缆是在建筑物的通风空间里延展的缆线。在建筑物结构中，通风空间（读作"PLEH-nuhm"源自拉丁语的"充满"）是一个位于建筑天花板与吊顶之间独立的空间，用于暖气、通风装置和空调（有时称为HVAC）的空气流通。在有电脑的建筑里，通风空间往往用于安装用于连接的通信电缆。因为普通电缆在火灾中有致命的危害，所以在通风空间内需要使用特别的阻燃电缆。

阻燃电缆的保护层通常用铁氟龙制成，比普通电缆要贵得多。它的外层材料对火有更强的抵抗性，即使燃烧也比普通电缆产生的烟少。双绞线电缆和同轴电缆都做成了阻燃电缆。

3.3.6 线缆规范和终结头

规范或称*标准*，是指广泛使用并作为完成某项任务公认方法的一套规则或规程。比如，OSI参考模型标准可以保证全球的网络设备相互兼容，协调工作。各种关于电缆的规格，有助于保证电缆

的互操作性、安全性和性能。

电气与电子工程师协会（IEEE）制定了局域网布线规范。IEEE 802.3是针对以太网的标准，IEEE802.5是针对令牌环网的标准。美国保险商实验室发布了主要针对安全性的标准。

电信工业协会（TIA）和***电子工业联合会（EIA）***联合发布的布线标准，通常被称为TIA/EIA标准。以下是该标准的部分内容：

- TIA/EIA-568-B——商业建筑的电信布线标准。
- TIA/EIA-569-B——以前的TIA/EIA-568-A标准，它是商业建筑的电信通道和空间标准。
- TIA/EIA-570-A——住宅和低密度商业建筑的电信布线标准。
- TIA/EIA-606——商业建筑的电信基础设施管理标准。
- TIA/EIA-607——商业建筑的电信接地/连接要求。

这一组织的标准在网络介质标准中的影响最大，其影响力还包括水平布线、骨干（垂直）布线、配线间、设备室、工作区域和进门装置。TIA/EIA使得网络设计者在对局域网设备进行规划和安装时，能自由选择所需要的设备，并确保了局域网设计的可操作性。

TIA/EIA-568-B标准着眼于水平布线，即从工作区墙上的插孔至布线间的电缆。前面介绍过的五种电缆（CAT 1-CAT 5），只有CAT 3、CAT 4和CAT 5符合TIA/EIA-568-B标准。CAT 5最常用。针对CAT 5e和CAT 6的最新标准已经制定，针对CAT 7布线的新标准也在制定中。这些新标准提供了对CAT 5的改进，使用越来越普遍。

TIA/EIA-568-B标准要求每一工作区域的电源插座有两根电缆：

- 传送语音的电话电缆。
- 传送数据的网络电缆。

语音电缆必须是两对UTP电缆，并配有正确的接头或终结器。

网络电缆必须是以下几种之一，并配有正确的接头或终结器：

- 150ΩSTP两对电缆（令牌环局域网）。
- 100ΩUTP四对电缆（以太局域网）。
- 62.5/125μ光缆（以太局域网）。
- 同轴电缆（在新的安装中很少使用，且在下一次的标准更新中可能会被删除）。

尽管不在标准之列，75欧姆的同轴RG-6电缆还是用于有线电视连接，如果需要，该电缆也可以少量地用于语音和数据连接。

这一标准还规定了UTP布线中每根缆线从墙面插孔到配线间的最大长度。从工作站到墙面插孔适用3米长的跳接线。90米的电缆用于从墙面插孔到配线间中的***配线板***。从配线板到布线间的水平交叉连接系统使用6米的跳接线。这一标准保证了整个电缆长度不超过100米。

实验活动　基本电缆测试

本实验要求你用一个简单的电缆测试器检测一根直通缆线或交叉缆线是否良好；同时，用Fluke 620高级电缆测试器检测缆线长度和连通性。

实验活动　制作直通电缆

本实验要求制作一根CAT 5或CAT 5e UTP以太网跳接线，并测试电缆的连通性是否良好和针脚连接是否正确（正确颜色的电缆连接到正确的针脚）。

实验活动　制作反转电缆

本实验要求制作一根CAT 5或CAT 5e UTP控制台反转电缆，并测试电缆的连通性是否良好和针脚连接是否正确（正确颜色的电缆连接到正确的针脚）。

实验活动 制作交叉电缆

本实验要求按照TIA-568-B和TIA-568-A标准制作一根CAT 5或CAT 5e UTP以太网交叉电缆，并测试电缆的连通性是否良好和针脚连接是否正确（正确颜色的电缆连接到正确的针脚）。

实验活动 购买UTP电缆

本实验要求了解市场上的网络电缆的种类和价格，尤其是跳接线和批量电缆。

3.4 光介质

在局域网的骨干和广域网（WAN）的长距离、高带宽、点到点传输中，光纤是最普遍的介质。它之所以流行，原因如下：

- 光纤对闪电、*电磁干扰（EMI）*或*无线电频率干涉（RFI）*不敏感，也不会产生EMI或RFI。
- 光纤的带宽比其他介质更宽。
- 光纤中的信号衰减很低，因此能够保证很长距离的传输和良好的信号质量。
- 光纤比其他介质更安全，因为很难在光纤上插入分接器，即使插入了也容易检测到。
- 为实现更高的传输速率，可以在现有的光纤连接上用更新更快的装置替换现有的光纤发送器和接收器，而不必替换光纤。
- 在长距离通信中，光纤的成本要低于铜线。
- 制成光纤的原材料来自砂子，这是一种丰富的物质。
- 使用光纤不必要像用电信号时一样考虑接地。
- 光纤很轻，易于安装。
- 光纤比铜线更能抵抗类似水这样的环境因素。
- 在长距离缆线中，光纤易于拼接。

基于以上原因，如果需要在超过100m的距离传输大量数据时，往往使用光纤。

本节将介绍*光缆*的基本理论。你将了解光纤是如何引导光进行长距离传输。你还将了解所使用的光缆类型，光纤如何安装、与光纤配合的接头和设备的类型，以及如果对光纤进行测试，保证其能正常工作。

3.4.1 电磁频谱

光纤网络中的光子是电磁能的一种，当电荷向后向前移动或加速时，就会产生一种能量，叫作电磁能。这种能量可以以波的形式穿过真空、空气和玻璃等其他材料。*波长*是任何能量波的一个重要特性，如图3-13所示。

对人类而言，无线电波、微波、雷达、可见光、X射线和伽马射线看起来都是非常不同的，但它们都是电磁能的不同种类。如果将这些电磁波按照波长长短依次排列，就形成了*电磁频谱*，如图3-14所示。



图3-13 波长

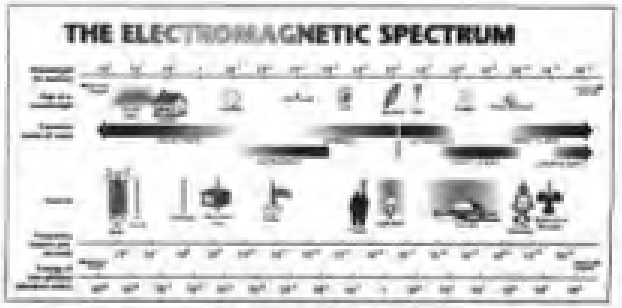


图3-14 电磁频谱

电磁波的波长是由产生电磁波的电子电荷前后移动的频率决定的。比如，如果电荷移动的速度较慢，产生的波长就长。可以把电荷的运动想像成水池里的一根棍子。如果棍子前后移动得慢，产生的涟漪的波峰和波谷之间的波长就长，反之，波长就短。

电磁波产生的原理都是相同的，因此它们之间有许多共同特征。比如，它们在真空中的速度相同，大约是30万km/s或者叫光速。

肉眼可见的电磁能量的波长在700nm至大约400nm之间。一nm（纳米）即十亿分之一米，（0.000000001m）缩写为nm。波长在700nm至大约400nm的电磁能称为***可见光***。波长较长的可见光（大约700nm）为红色，较短的（400nm）为紫色。这部分电磁波谱可在彩虹里看到。

通过光纤传输数据，所用的波长是人眼不可见的。这些波长比红光的波长稍长，叫做红外线。红外线可以用在电视遥控上。光纤中所用光的波长为下列的一种：

- 850nm。
- 1310nm。
- 1550nm。

至所以选择这些波长，是因为它们在光纤中的传输效果比其他波长更好。

3.4.2　光的传播方式

当电磁波（包括光）离开发射源时，都以直线方式传播。这些由源向外的直线称为射线。

可以把光线想象成由激光器产生的细光束。在真空中，光以每秒30万km/s的速度传播，然而，光穿过其他介质，如空气、水、玻璃时的速度要慢一些，且各不相同。当光线（*入射光*）跨越一种介质（比如空气）的边界进入另一种介质（比如玻璃）时，光线的部分能量被反射回来。这便是你可以在镜子中看到自己的原因。被反射回来的光叫*反射光*。入射光中未被反射的光能进入了玻璃。进入的射线往往比原来的路径有一定的角度弯曲。该射线叫*折射光*。入射光线的弯曲角度取决于两个因素：

- 入射光线射到玻璃表面的角度。
- 光在两种介质中传播的速率的比值（本例中为空气和玻璃）。

由于光线在不同介质的边界可以发生弯曲，所以即使光纤弯成曲线时光线也仍然可以传播。

射线的弯曲度由玻璃的光密度决定。光密度是指光线进入一种介质后速度的减慢程度。介质的光密度越大，光在该介质中的速度相比在真空中的速度就慢得越多。光在一种介质中的传播速度与光在真空中的速度的比率就是该介质的折射率（IR），表示如下：

IR=光在真空中的速度/光在介质中的速度

因此，介质光密度的衡量就是介质的折射率。折射率越大，光密度越大，光的传播速度也越小。表3-2列出了空气、玻璃、钻石和水的折射率。

表3-2　折射率

物质	折射率
空气	1.000
玻璃	1.523
钻石	2.419
水	1.333

对于玻璃这样的介质，通过添加化学物质可以增加折射率（光密度）。通过提纯，可以降低玻璃的折射率。

在接下来的两节中，你将学习更多关于***反射***和折射的知识，这将有助于你理解光纤的设计和工作原理。

3.4.3 反射定律

当光穿过一种介质到达另一种介质时，比如从空气到玻璃，或者从表面反射或者折射进第二种介质，如图3-15所示。这取决于光到达介质表面时的角度。入射线与垂直于玻璃表面的直线之间的角度叫***入射角***。当入射角达到一个特定值（称为临界角）时，所有的光都会反射回原介质，如图3-16所示。

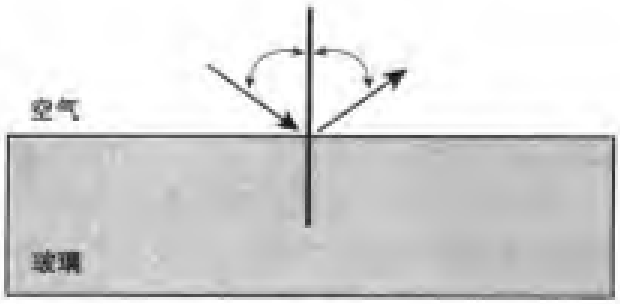


图3-15 反射

这条垂直的直线叫作***法线***，它并不是光线，只是计量角度的一个工具。反射线与法线间的角度叫作反射角。反射定律表明，***反射角***等于入射角。也就是说，光线以多大的角度反射离开介质表面取决于光线入射的角度。

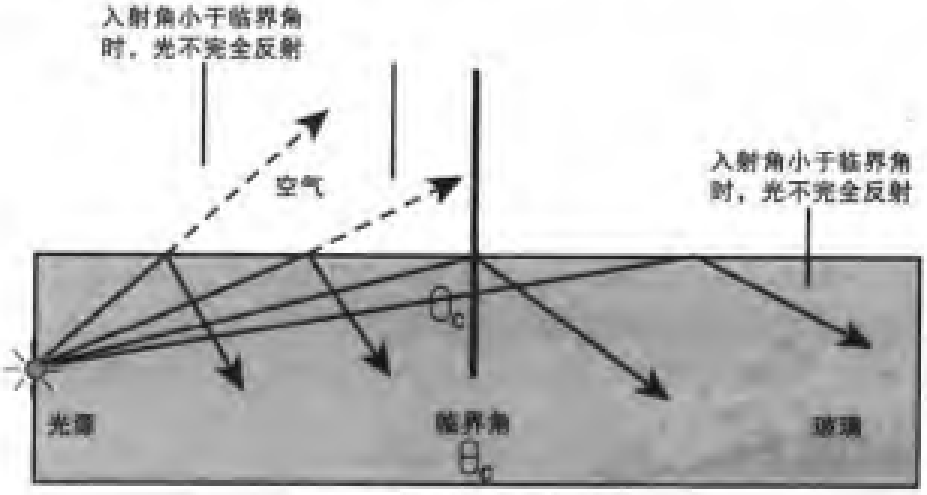


图3-16 临界角

3.4.4 折射定律（斯奈尔定律）

当光到达两种透明介质（如空气和玻璃）的接触面时，光线被分为两部分。一部分光反射回原介质（空气）中，反射角等于入射角。剩余的光线中的能量穿过界面进入第二种介质（玻璃）。

如果入射光线以正好90度角到达到玻璃表面，光线会笔直进入玻璃而不发生弯曲。但如果不是正好90度，就会发生弯曲。我们将这种光线传播方向的改变叫作***折射***。光线的折射度取决于两种介质的折射率。如果光从折射率小的介质进入折射率大的介质，折射线会向法线弯曲，反之则偏离法线。图3-17举例说明折射。

比如，如图3-18所示，光线以非90度角穿过玻璃和钻石的边界。玻璃的折射率大概是1.523，钻石的折射率大概是2.419。因此，进入钻石的光线向法线靠拢。当光线以非90度的角度从钻石进入空

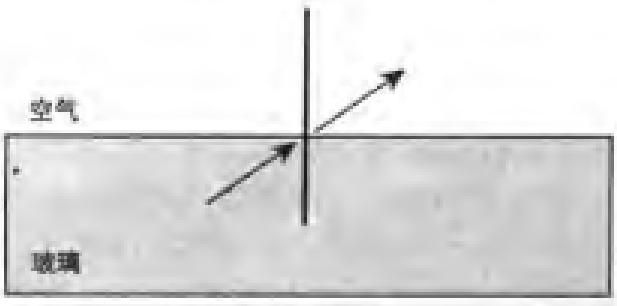


图3-17 折射

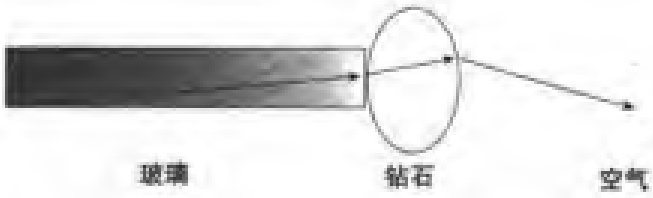


图3-18 折射例子

气时，又偏离法线。因为空气的折射率（约为1.000）小于钻石的折射率。

3.4.5　全反射

如果光线的接通和断开以在光纤内发送数据1和0，那么光线必须停留在光纤内，直到到达远端。

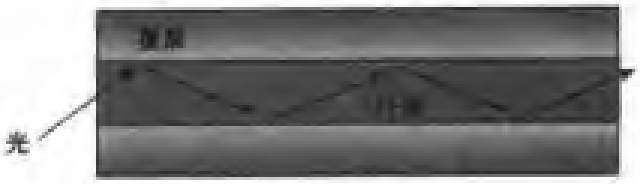


图3-19　全反射

要避免光线折射进包裹光纤的外层材料，因为这样的折射会引起光能量的部分损失。因此，设计时，光纤的外表面对在光纤内部的光线必须好比一面镜子。如果任何试图离开光纤的光线在光纤边界处都被以某个角度反射回光纤内，并向光纤的远端传播，这对光波而言就是好的*管道*或者*波导*。

反射定律和折射定律告诉了我们如何设计光纤，以使得光波在光纤中传输时能量损失最少。要使光纤内的光线被反射回光纤，并且不因为折射而产生能量损失，需要满足两个条件。这两个条件如下：

- 光纤纤芯（内部）的折射率高于其周围的材料。围绕光纤纤芯的材料叫作覆层。
- 入射角大于内层和覆层之间的临界角。

当以上两个条件都满足时，光纤内所有的入射线都会被反射回光纤，这叫作*全反射*，也是光纤制造的基础。全反射使光纤里的光从纤芯和覆层的边界处折回并继续向光纤远端传播。光线在光纤内层沿着一条之字型路线前进。

使光纤符合第一个条件（光纤内部材料的折射率高于周围材料）比较容易。另外，进入内层的光线的入射角可以被控制，控制入射角度的因素有两个：

- 光纤的数值孔径。如图3-20所示，若想使入射光纤完全反射，入射角的范围就是光纤纤芯的数值孔径。
- 光线在光纤中传播时所经过的路径。

可以实现全反射的光纤满足了限制条件1和2后，便可为数据通信提供光波路径。如图3-21所示。

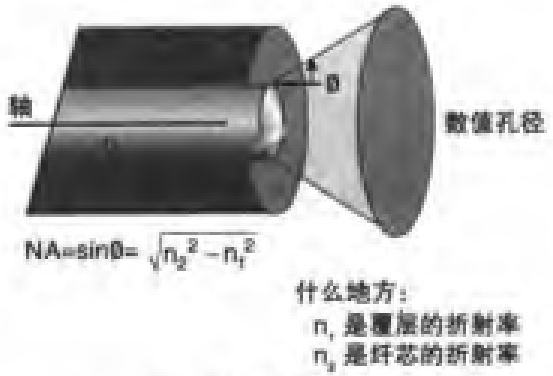


图3-20　数值孔径



图3-21　光波路径

3.4.6　光缆

*光缆*是一种利用调制光在细玻璃束内传输数据的网络介质。代表数据比特的信号被转化为光束。重要的一点是认识到虽然在终端设备上需要用电来产生和翻译光纤信号，但光缆内并不像铜介质那样有电流。事实上，光缆组件是很好的绝缘体。光纤介质的许多特征使它优于铜介质。

每条用于网络连接的光缆都由两条包有独立护套的玻璃光纤组成。一条将数据从设备A传送到设备B，另一条将数据从设备B传送到设备A。每条光纤都沿单一方向传送，正如两条方向相反的单行道。这样的安排提供了全双工的通信链路。正如铜双绞线使用分离的电线对发送（Tx）和接收（Rx）一样，光纤链路用一根光纤传送，另一根接收，如图3-22所示。一般来说，两根光缆包裹在

同一个外套中，一直到连接头处。

此处，两根光纤是分开的。在光纤内，由于没有光逃逸，也就表示没有干扰现象，所以不需要绞合或屏蔽。同一条缆线里有多条光纤是很常见的，这样使得在数据间、地板或建筑物里只需要布一条缆线。一条缆线可以包含2、4、8、12、24、48或更多独立的光纤。如果用铜线，必须为每条电路准备一根UTP缆线。光纤每秒传送的比特数也远远大于铜介质。

如图3-23和图3-24所示，光缆一般由5个部分组成：

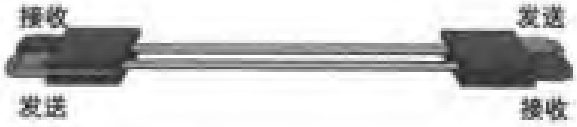


图3-22 全双工光纤



图3-23 光缆的五个组成部分

- 纤芯。
- 覆层。
- 缓冲层。
- 加强材料。
- 外套。

纤芯是光纤中心供光传输的部分，所有的光信号都通过纤芯传送。纤芯主要是由二氧化硅和其他元素制成。围绕纤芯的是覆层，也由二氧化硅制成，但折射率相对要低。穿过光纤纤芯的光线在纤芯与覆层的交界处反射回纤芯，从而保证光线沿纤芯传播。

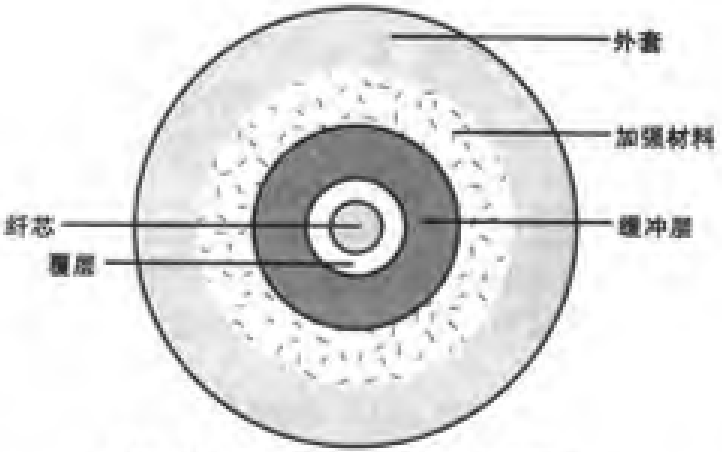


图3-24 光缆五个组成部分的截面图

围绕覆层的是缓冲材料，通常是塑料，用来保护纤芯和覆层不受破坏。

围绕缓冲材料的是加强材料，保护光缆在安装时不被拉坏。所用的材料通常是Kevlar，与防弹背心的材料相同。最后一部分是缆线外面的外套，用来保护光纤不被磨损、溶解或受到其他损害。外套根据缆线的用途而有所差别。

光纤中光线通过的部分被称之为光纤的纤芯。不是所有角度的光都能进入纤芯的，要进入纤芯，光线的入射角必须在光纤的数值孔径范围内。类似地，一旦光线进入了光纤的纤芯，其在光纤内可以使用的光路数也是有限的。这些光路被称为模式。如果光纤的纤芯很大，光线穿越光纤时可以使用的路径很多，光纤就称为*多模*光纤。*单模*光纤的纤芯小得多，只允许光线沿一条路径（一个模式）在光纤中通过。图3-25解释了多模光纤和单模光纤的差异。

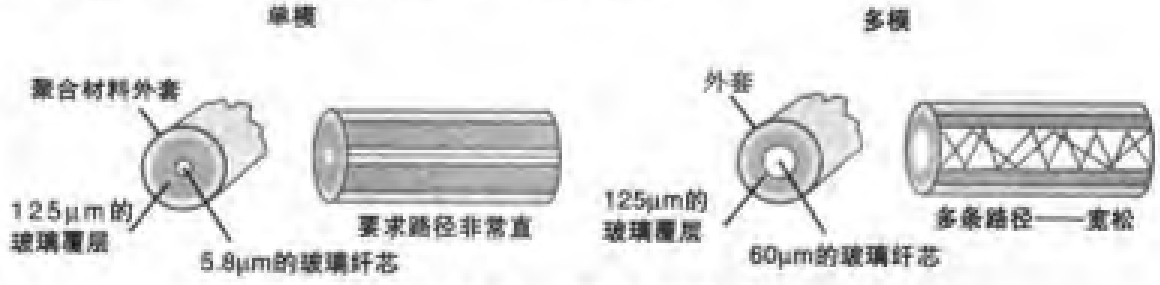


图3-25 单模与多模的对比

表3-3比较了单模光纤和多模光纤的特征。

表3-3　单模光纤和多模光纤的特性

	单模光纤	多模光纤
纤芯特性	小芯（10μm或更小）	大芯（50，62.5μm或更大）
散射特征	很少散射	允许散射，所以存在信号丢失
距离特征	适用于长距离的应用（最长3km,9842英尺）	支持长距离应用，但距离比单模短（最多2km 6560英尺）
光源	用激光作光源，通常用于园区骨干，距离达数km	用发光二极管作光源，通常用于局域网内或园区网中数百米的距离

接下来的两节将更详细地介绍光纤的两种基本类型：多模和单模。

3.4.7　多模光纤

相对于单模光纤来说，多模光纤允许在同一个纤芯里面同时传送多种模式（路径）的光。根据入射角度的不同，各种模式的光在光纤中实际经过的距离可能不同。入射角的问题会使得不同模式的光到达目的地（线缆接收端）的时间略有差异——这种现象称为**模式色散**。多模光纤采用一种特殊的玻璃，称为*渐变折射率玻璃*，其朝纤芯外缘方向的折射率更小。这种玻璃使得光在通过纤芯中心时速度放慢，通过纤芯中心以外的区域时速度加快，这就保证了所有模式的光能几乎同时到达终点。采用这种设计是因为，从光纤中心部分通过的光线相比在光纤内不断反射传递的光线，所经过的路径更短。所有的光线应该同时到达光纤末端。这样，光纤接收端的接收器就能收到一个强闪的光，而不是一个很长很模糊的脉冲。

标准的多模光纤（局域网中最常用的光缆）一般采用62.5μm或50μm的纤芯，再加上直径125μm的覆层。这种光缆一般表示为：62.5/125或50/125。1μm是百万分之一米。

由于覆层的直径比所传送光的波长大得多，所以光在沿传输线传播的过程中，在纤芯内部不断地反射。

红外发光二极管（LED）与直腔面发射激光器（VCSEL）通常用作多模光纤的光源。相比激光，发光二极管的造价便宜一些，需要注意的安全问题也更少。但是，发光二极管所发射的光在光缆中传输的距离没有激光长。多模光纤（62.5/125）传送数据的距离最远可达2km（6560英尺）。多模光纤主要在局域网的应用中，也包括骨干的布线。



实验活动　采购光纤

本实验中，你来介绍市面上光纤和相关部件的种类及价格。本实验主要针对光纤跳线和大批量的光纤。

3.4.8　单模光纤

在单模光纤的纤芯中只传播一种模式的光。在单模光纤中，纤芯小得多，直径只有8~10μm。9μm的纤芯是最常见得。单模光纤上9/125的标记表示纤芯的直径为9μm，环绕纤芯的覆层直径为125μm。

单模光纤几乎没有空间供光线进行来回反射。而且，单模光纤还使用非常汇聚的红外激光作为光源。激光光源所产生的光纤以90度进入纤芯。因此，单模光纤中，承载数据的光线脉冲基本上是沿直线在纤芯中传输，如图3-26所示。这大大提高了数据传送的速度和距离。

基于这种设计，单模光纤相比多模光纤，传送数据的速率（带宽）更高，距离更远。单模光纤可以将局域网数据传递3km的距离。多模光纤最多只能传送2km。激光和单模光纤比发光二极管和多模光纤更贵。由于这些特性，单模光纤通常用作楼间的连接或广域网连接（例如，电话公司的网络连接）。

图3-27用多个截面图比较了两种类型光缆的纤芯和覆层的相对尺寸。单模光纤的纤芯更小更精密，这就是单模光纤相比多模光纤，带宽更高，传送距离更长的原因，尽管这也必然造成更高的制造成本。

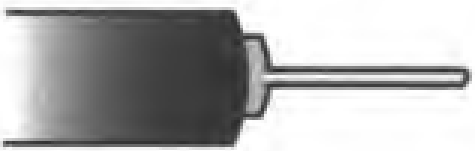


图3-26 单模光纤

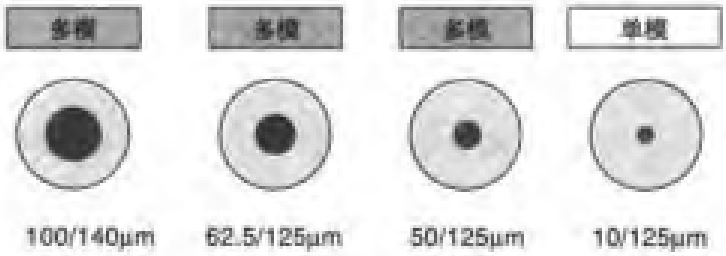


图3-27 单模和多模光纤

警告：用作单模光纤光源的激光器发出的激光要比可见光的波长更长，由于光太强，因此会对人眼造成伤害。不要去看一端连接到设备上的光纤的末端。不要向网卡、交换机或路由器的传送端口里看。其实，什么也看不到。记住，要在光纤的末端盖上保护盖，并将保护盖插入交换机和路由器的光纤端口。要非常小心！

下面总结了光缆的特征：

- **速度与吞吐量**——大于1Gbit/s。
- **每节点平均成本**——昂贵。
- **介质和接头尺寸**——小。
- **最大传输距离**——单模大于10km，多模最多可达2km。

3.4.9 线缆的设计

如图3-28所示，有两种基本类型的线缆设计：

- 松套型（Loose-tube）。
- 紧密缓冲型（Tight-buffered）。

紧密缓冲型光纤在覆层与纤芯之间有一些缓冲材料，而松套型则没有。两种设计最实际的主要差别在于应用的不同。松套型光纤一般用于楼外的铺设中，而紧密缓冲型光纤一般用于楼内。大多数局域网多用紧密缓冲型多模光纤。

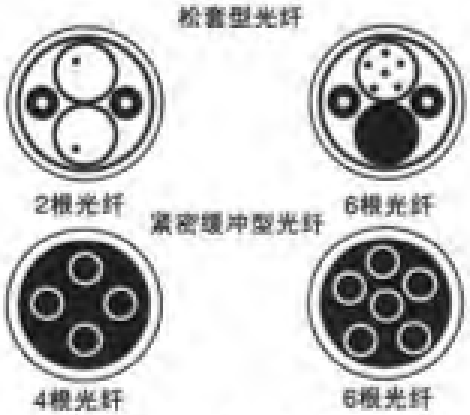


图3-28 松套型与紧密缓冲型的对比

3.4.10 光纤网络的其他组件

局域网上大多数数据都是以电信号的形式传送的。但是，光纤链路使用光来发送数据。所以，需要某种装置将电转换为光，并在光纤的另一端，将光转换为电。这就意味着需要两种设备：发送器和接收器。

除了发送器和接收器，本节还讨论了光网络连接中使用的各种类型的光缆连接器和设备。

发送器

发送器从交换机和路由器接收需要传输的数据。这些数据是以电信号的形式存在的，发送器将电信号转换为相应的光脉冲。通常采用以下两种光源对数据进行编码并通过线缆发送：

- **发光二极管（LED）**——二极管可以产生出波长为850或1310nm的红外光，它们在局域网中一般用于多模光纤。在光纤的一段用透镜对红外光进行聚焦。发光二极管的安全性不高。

• 激光（Laser）——激光光源可以产生细的，强烈的红外光束，波长通常为1310nm或1550nm。多用于广域网上长距离的单模光纤或园区骨干。但要特别小心，防止对眼睛造成伤害。

每种光源都是通过明与暗的快速交替以每秒很高的比特率来发送数据的1和0。

接收器

光纤的另一端就是接收器。其功能类似太阳能供电计算器的光电管。当光到达接收器时，就产生电。它的任务首先是检测光纤上的光脉冲，然后将光脉冲转换回在发送端初始进入光纤的初始电信号。现在，信号已经又恢复为电压改变的形式。这时的信号可以通过铜线传送到任何的设备，比如计算机、交换机或路由器。通常用作接收器，与激光链路配合使用的半导体设备被称为PIN光电二极管（PIN photodiode）。

PIN光电二极管被制造成对光纤远端的发送器所产生的特定波长的光（850nm、1310nm和1550nm）敏感。当接收到适当波长的光脉冲时，PIN光电二极管很快产生适当网络电压和电流。没有光时，立刻停止产生电压。这个过程在铜缆上产生了表示数据1和0的电压变化。

接头

接头连接在光纤末端，以使得光纤能与发送器和接收器上的端口进行连接。在多模光纤中，最常用的接头类型为用户接头（subscriber connector，SC），如图3-29所示。单模光纤的接头类型为直插式接头（straight tip，ST），如图3-30所示。对于SC和ST，都是每根光纤一个连接器。新型的连接器将发送和接收光纤组合成了一个模块化的接头，尺寸类似RJ-45，以节省空间。



图3-29　SC连接器



图3-30　ST连接器

光学扩大器与光纤配线板

在光纤网络中，除了必需的发送器、接收器、接头和光纤以外，有时你还看到一些其他的设备。

中继器是就是光放大器，接收经过长距离传输发生了衰减的光脉冲，使之恢复为原始的形状、强度和定时。恢复后的信号可以传送到光纤远端的接收器。

光纤配线板，如图3-31所示，类似于铜缆配线板。配线板允许通过各种可用的光纤（线缆链路）来快速改变交换机和路由器这样的设备之间的连接。



图3-31　光纤配线板

3.4.11　光纤中的信号和噪声

光纤不会受到能在铜介质上造成问题的外部噪声源的影响。为什么？因为除了在发送端，外部光是无法进入光纤的。覆层外的缓冲层和外套阻止了光进入和离开光缆。

而且，光缆中一条光纤上的传输不会对其他光纤的传输造成干扰。事实上，光纤链路的质量非常好，这使得最近的吉比特以太网和10G以太网中规定的传输距离远大于原始以太网传统的2km传输距离。（在第6章“以太网技术和以太网交换”中，你将学习到更多关于以太网技术的内容。）光

纤传输使得以太网协议可以用在城域网和广域网中。

尽管光纤是用作大数据量的远距离传输介质中最好的，但也不是没有问题。当光通过光纤时，一部分光能会损失。光信号在光纤中传播的距离越长，损失的能量就越多。这种信号的**衰减**是由多种因素引起的，包括光纤的自身属性。最重要的原因是**散射**。光纤里的散射是由光纤中微小的不一致（扭曲）造成的，它们会发射和散射部分的光能，如图3-32所示。

吸收是导致光能损失的另一个原因。当光触到光纤里的某些化学杂质时，这些杂质会吸收部分能量。这部分光能转化成少量的热能。吸收使光信号变得有些模糊。

导致光信号衰减的另一原因是纤芯-覆层边界处制造时的不规则或粗糙。由于在光纤的粗糙部分不能做到全反射，光信号的一部分能量受到损失。如果光纤的厚度或对称性上有任何小瑕疵，就会影响全反射，部分光能就会被覆层吸收。

光的**色散**限制了通过光纤的传输距离。色散是一个术语，用于描述光脉冲在通过光纤时的扩散，如图3-33。

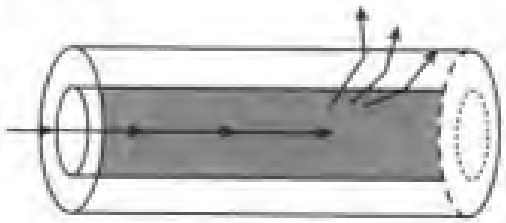


图3-32 离散

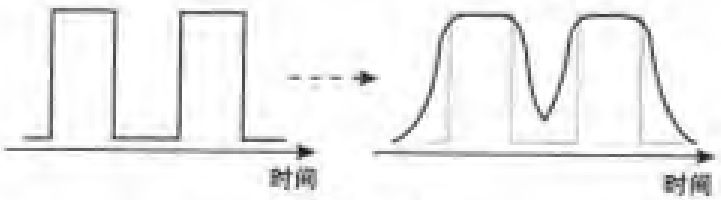


图3-33 分散

为了弥补在大直径的纤芯中，不同模式光所通过实际距离的不同，设计了渐变折射率多模光纤。单模光纤中不存在光信号可以走多条路径的问题。但是，色散却是多模和单模光纤共同的特征。某种波长的光穿过玻璃时的速度与其他波长的光稍有差别。这便是棱镜分离不同波长光的原理。理想状况下，发光二极管和激光源只产生一个频率的光。这样，色散就不再是问题了。

不幸的是，激光，尤其是LDE，会产生一系列的波长，这样色散就限制了光纤传输的距离。如果你试图将信号传得太远，光能亮脉冲在到达接收器时将会变得扩散、分离、模糊。接收器无法区分1和0。

3.4.12 光纤的安装、保护和测试

光纤中衰减过多的一个主要原因是不恰当的安装。如果光纤被拉伸或弯曲得太紧，就会引起纤芯的小裂缝，对光线进行散射。将光纤弯曲的角度太大，会改变光纤接触到纤芯-覆层交界处的入射角。使得光线的入射角小于全反射的临界角。在弯曲处，某些光纤不是被反射，而是折射进入覆层并损失掉了。

有两种类型的弯曲：

- **宏曲**（Macrobending）——宏曲是肉眼可见的弯曲。当你将光纤弯曲时，一部分光线超过了临界角，使得光漏出纤芯，进入覆层。光一旦进入覆层，就很难再次返回纤芯。它会通过缓冲层向外泄漏，如图3-34所示。
- **微曲**（Microbending）——微曲与宏曲的影响是一样的。它使光超过临界角并泄漏出纤芯，如图3-34所示。它的发生幅度很小，肉眼不可见。

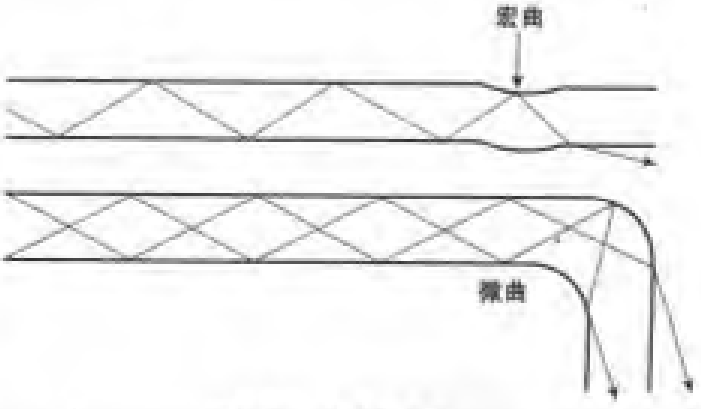


图3-34 宏曲和微曲

注释：当缆线结构中的不同材料以不同程度膨胀或收缩时，缆线里的超高温振幅也可以产生微曲。这种膨胀或收缩使得光纤挤压或伸展，由此产生了微曲。

为防止光纤过分弯曲，通常用一种叫内管（interducting）的管材拉伸。内管比光纤硬得多，不容易被过度弯曲，因此，内管中的光纤不容易弯曲。内管可以保护光纤，使之易于拉伸，并保证弯曲半径不至于过大。

光纤被拉好后，其末端必须劈开（切割），并仔细抛光保证末端光滑。图3-35显示了光纤末端抛光不当所导致的问题，图3-36演示了恰当的光纤末端表面抛光技术。

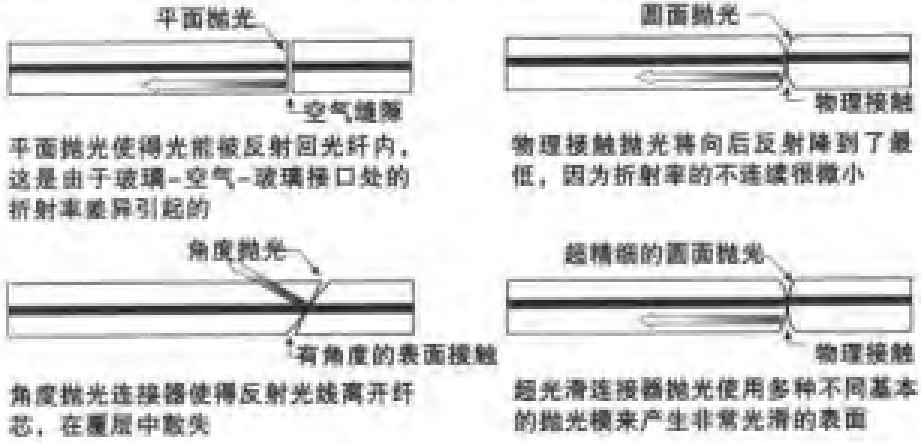


图3-35　光纤端面抛光

要用显微镜或内置放大仪器检测光纤末端，以确认它被恰当地抛光和成型。然后，在光纤末端仔细地安装接头。接头的不恰当安装、不恰当的拼接，或将两条纤芯尺寸不一致的光缆拼接在一起都会大大降低光信号的强度。图3-37展示了将62.5μm的光纤与50μm的光纤的拼接。

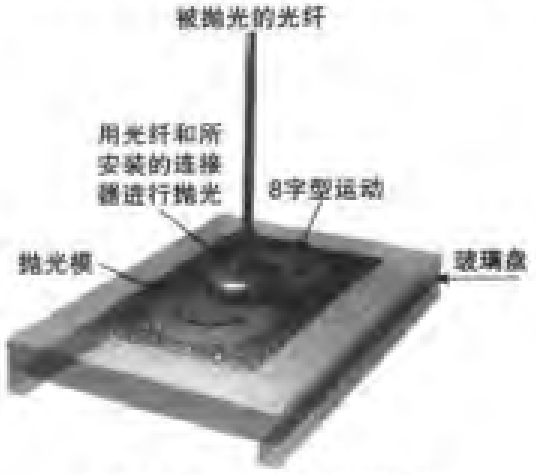


图3-36　光纤端面抛光技术

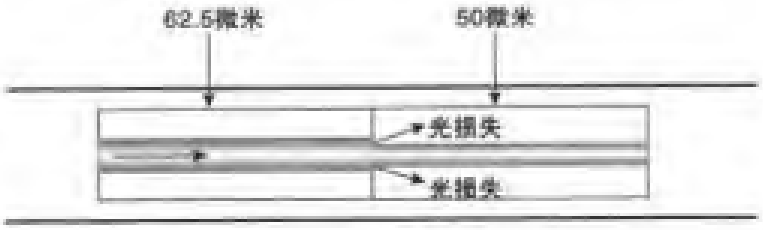


图3-37　不同类型光纤的接合

光缆和接头安装完毕后，接头和光纤的末端一定要保持洁净。光纤的末端要盖上保护盖以防损坏。将光纤连接到路由器或交换机的端口上时，光纤末端一定要进行清洁。清洁光纤末端应该用蘸有异丙醇的无棉镜头纸。交换机和路由器的光纤端口在不使用时需要盖上，并在进行连接前用蘸有异丙醇的镜头纸清洁。末端不洁净会导致光在到达接收器时产生很大的衰减。

所有这些因素：散射、吸收、色散、不当安装、光纤末端不洁，都会影响光信号的传输距离，因此被称为光纤噪声。在使用光缆之前，一定要经过测试，以保证能够有足够的光到达接收器，以便在信号中检测出0和1。

设计好光纤链路后，一定要计算所忍受的光能损失。这种忍受能力称为*光链路损失预算*。它和

每月的财政预算很类似。当你将所有的花费（衰减）从最初的收入中减去后，必须剩下足够的钱，以使得你能度过这个月。

*分贝（dB）*是衡量能量损失数量的单位。它表明发送器发出的能量有百分之多少实际到达了接收器。

测试光纤链路是极其重要的，测试的结果一定要保留。所用的光纤测试设备有多种，其中最重要的两种是光损失计量器（Optical Loss Meter）和光时域反射计量器（Optical Time Domain Reflcometer，OTDR）。

这些计量器均用来对光缆进行测试，以保证缆线符合光纤的TIA标准。也是为了通过测试确保链路能量损失没有超过光链路损失预算。OTDR可以提供关于光纤链路的很多详细的诊断信息，以用于在出现问题时对链路进行故障排除。

实验活动 购买光纤

本实验中，你需要了解市场上的缆线以及相关部件的种类和价格，尤其是光跳线和批量光缆。

3.5 无线通信

无线信号是能在外层空间的真空中或类似空气这样的介质中传播的电磁波。无线信号不需要铜或光纤等物理介质，因而在网络中的应用十分灵活。通过使用高频信号，无线传输可以跨越很远的距离。每个信号都使用不同的频率（以赫兹为单位），因此相比其他的信号都是独特的。

无线技术已经使用多年，卫星电视、AM/FM广播、手机、遥控设备、雷达、警报系统、天气广播、无绳电话和扫描仪都已经融入了我们的日常生活。今天，无线技术是商业和个人生活的基本组成部分。

3.5.1 无线数据通信

无线电频谱是电磁频谱的一部分，用于传送语音、视频和数据。它所用的频率从3千赫（kHz）到30万兆赫（GHz）之间。本节只涉及支持无线数据传送的无线电频谱部分。

无线数据通信的种类很多，如图3-38所示。

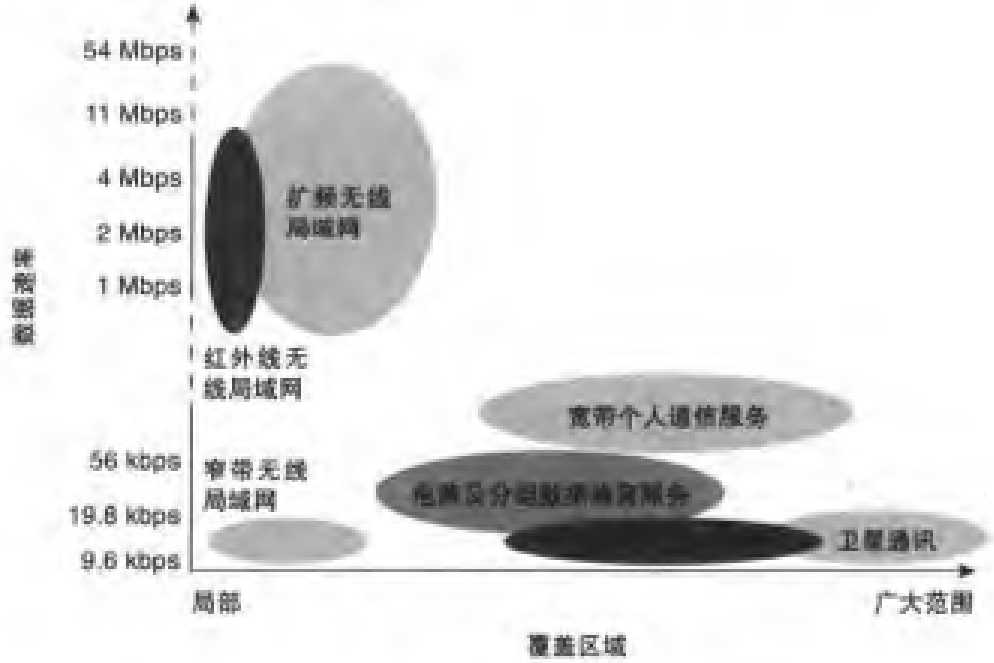


图3-38 无线数据网络

每种类型的无线数据通信都有各自的优点和缺点，如下所示：

- **红外线（IR）**——数据传输率很大，成本较低，但传送距离短。
- **窄带**——数据传输速率低，中等成本，需要许可证，传输距离有限。
- **扩频**——数据传输速率高，中等成本，限于园区范围，思科的Aironet产品就采用了扩频技术。
- **宽带个人通信服务（PCS）**——低数据传输率，中等成本，覆盖城域网。Sprint是一个例外。Sprint PCS覆盖全国和世界范围。
- **电路和分组数据（蜂窝数据和蜂窝数字分组数据[CDPD]）**——低数据传输率，高包装费，覆盖全国范围。
- **人造卫星**——低数据传输率，高成本，覆盖全国和全球范围。

3.5.2　无线信号

信号以数据形式传送时，要考虑以下三个参数：

- **多快**——数据传输速率可达多少？
- **多远**——在保持最大的数据传输速率的前提下，无线局域网（WLAN）单元能被放置多远。
- **多少**——不降低数据传输速率的情况下，能够容纳多少用户？

这些参数都与尽可能远地接收高质量信号的能力有关。增加数据量需要使用更多的频率，或通过其他的方法将数据放在无线电（RF）信号上。

无线电的效率受以下三个因素的影响，如图3-39所示：

- **所采用的调制类型**——调制技术越复杂，吞吐量越大。
- **距离**——信号传输得越远，信号越弱。
- **噪声**——电子噪音和障碍物会对无线电产生负面影响。

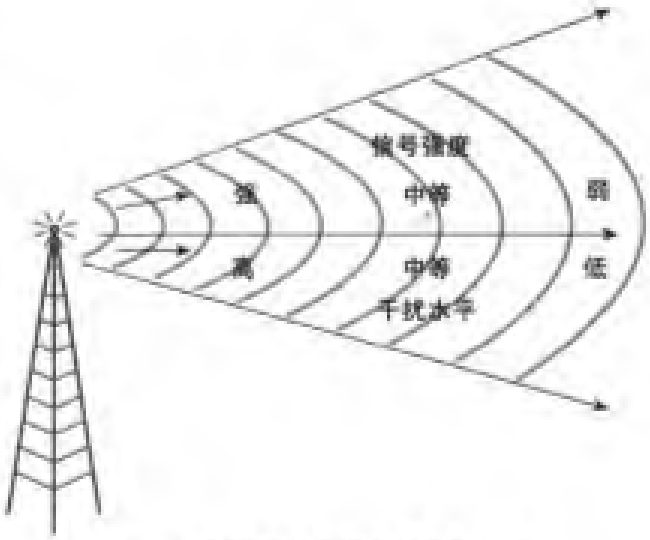


图3-39　影响无线电频率效率的因素

下面的几小节将具体介绍这三个因素。

调制

调制是调节振幅、频率，以及无线电或光波的相位，进行数据传送的过程。载波的性质可以即时地被另一种调制波形所改变。调制将数据信号（文本、声音等）混合到载波中以完成网络传送。

最常见的调制方式如下（见图3-40）：

- **调幅（AM）**——调制载波的幅度。
- **调频（FM）**——调制载波的频率。
- **调相（PM）**——调制载波的相位。

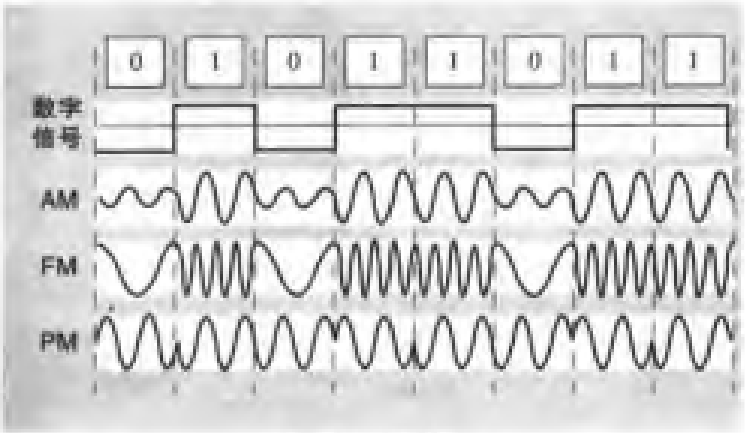


图3-40　调制

距离对信号的影响

接收器离发送器越远，信号变得越弱，信号和噪声的区别也越小。逐渐地，就无法区分信号和

噪声，这便产生了通信损失。信号发送时压缩（或调制方案）的量决定了需要从噪声中区分出的信号量。传输方式或调制方案（压缩）越复杂，数据传输速率越高，抗噪声的能力越弱。因此，传输距离也越短。

噪声对信号的影响

电子噪声和障碍物会对无线电的效率产生不利影响。在没有到达现场并实际进行测试之前，无法提供WLAN产品的具体传输距离。例如，带有内置金属结构的墙面会大大限制无线电的传送范围。

注释：要正确接收信号，复杂的调制方案需要最佳的信号-噪声比（信号更多而噪声更少）。如果信道上有噪声，速度就会降低。噪声、速度和距离是相互联系的。

3.5.3 无线频段

大多数无线频率是由政府机构，比如美国联邦通信委员会（FCC），授权使用的。要在这些频率上进行广播，你需要获得许可证并付费。

不需要许可证的频段更容易实施，成本也较低。如图3-41所示，有三个不需要许可证的频段。

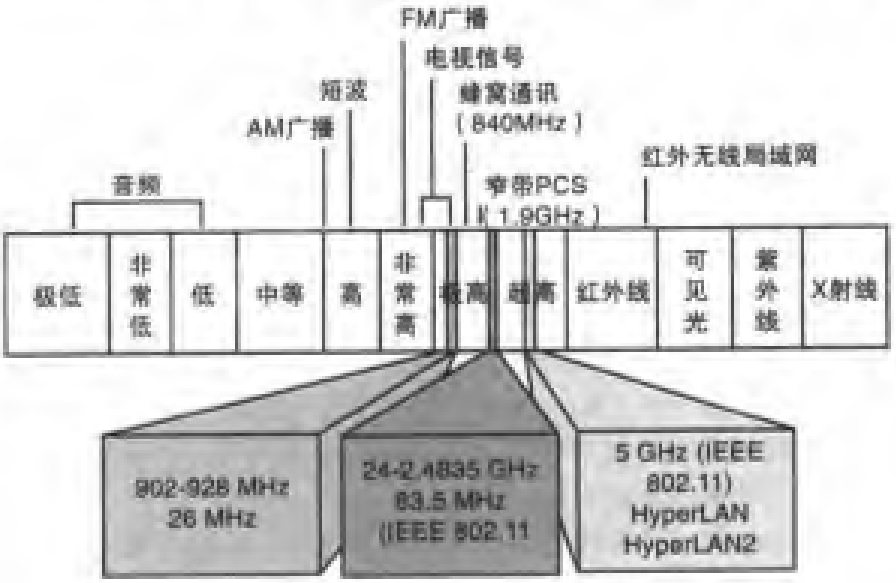


图3-41 无许可证频率波段

- **900兆赫（MHz）**——900MHz波段用于传送无绳和蜂窝电话。
- **2.4吉赫（GHz）**——最广泛部署的无线标准，802.11b标准就工作在2.4GHz无限制无线电频段，能提供最高11Mbit/s的数据速率。
- **5吉赫（GHz）**——最近，FCC开放了5GHz的频段用于无许可证高速数据通信装置。Cisco已经拥有5GHz的技术，并把这一频率用于新产品，如Cisco Aironet 1200系列，一种双波段产品，同时支持2.4GHz（802.11b）和5GHz（802.11a）标准。802.11a标准的最大数据传输速率为54Mbit/s。

频率和可传送的数据量之间存在着联系。这好比管子的概念。带宽越宽，可用的频率就越多。频率越宽，数据传输率越高。可用频率的数量决定了数据传输速率。

因为900MHz波段支持了蜂窝电话和其他消费品，波段已经变得十分拥挤。造成的结果是，用户经常受到干扰或无法接入网络。900MHz的一个优点是比2.4GHz传送距离更远（同样的天线）。它的一个缺点在于，由于频段有限，最快最可靠的数据传送速率只有1Mbit/s。

2.4GHz频段范围比900MHz更宽，支持更高的数据速率，可靠的传输距离可达25km。Cisco

Aironet 340无线局域网系列产品就工作在2.4-GHz，能提供11Mbit/s的吞吐量。

Cisco已经拥有了5-GHz技术并提供5-GHz频段的产品，因为这个频段的高带宽将支持更高的数据吞吐量。Cisco Aironet 5GHz 54Mbit/s无线局域网客户适配器是兼容IEEE 802.11a标准的CardBus适配器，工作在UNII-1和UNII-2频段。客户适配器配合Cisco Aironet 1200系列802.11a接入点，提供了结合企业所需的性能、移动性、安全性和可管理性的解决方案。5GHz频率的缺点在于，传输距离有限。5GHz产品的室内传输距离约为15m，室外大约在762m以内。

3.5.4　扩频技术

与个人汽车上备有的AM和FM波段一样，其他无线电也使用特定的波段、频率和调制类型。*扩频（SS）*是20世纪40年代开发的一种调制技术，能将信号扩展到更宽的无线电频率上。术语"扩频"描述了这是一种用带宽的消耗获得更高信噪比的调制技术。这种技术对于数据通信是很理想的，因为它对无线噪声不太敏感，所产生的干扰也少。

如图3-42所示，在扩频系统中，发送的信号所扩展的频率范围远远宽于传输该信号所需要的最小带宽。一个基本前提是，在有窄带噪声的信道中，增加发送信号的带宽，能使得信号被正确接收的可能性增大。

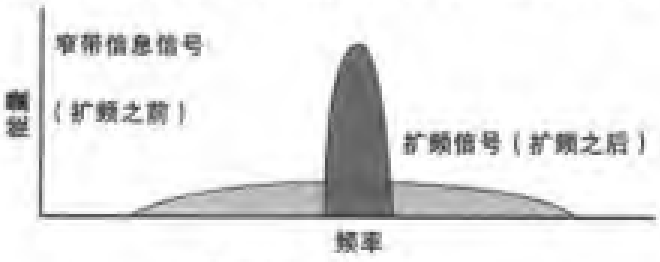


图3-42　扩频技术

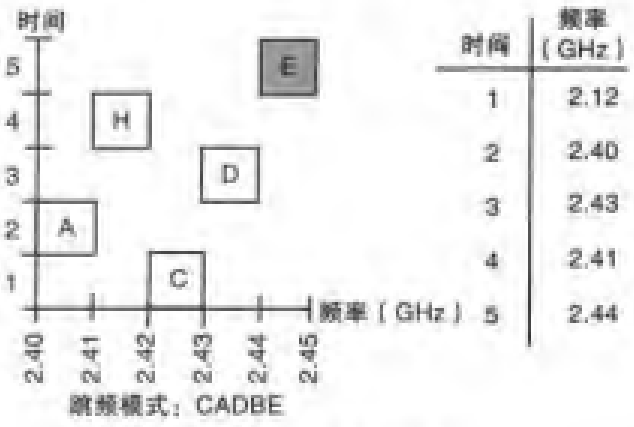
使用无许可证无线电频段就需要扩频技术。扩频的两种方式是跳频扩频（FHSS）和顺序扩频（DSSS）。这些扩频技术使无线电能量在可用的波段上传输。接下来的一节更详细地介绍了FHSS和DSSS。

3.5.5　FHSS和DSSS

作为调制技术，*跳频扩频（FHSS）*和*顺序扩频（DSSS）*都存在着优点和缺点。

对于FHSS技术，传输波随机地从一个频率跳到另一个频率。图3-43展示了FHSS的一个例子，其中，传输波从C（2.42Hz）跳到A（2.40GHz），到D（2.43GHz），再到B（2.41GHz），最后到E（2.44GHz）。这种技术可以使传输波跳过窄带干扰，使信号更清晰，传输更可靠。然而这种技术速度较慢，接收器也必须使用相同的解码方式。

如图3-44所示，DSSS技术的可靠性更高，因为每个比特（1或0）都是用一串1和0表示，叫做*碎片序列（chipping sequence）*。即使丢失的串达到了40%，原始的传输内容也可以重建。DSSS技术支持远距离的大吞吐量数据传输。



时间	频率（GHz）
1	2.12
2	2.40
3	2.43
4	2.41
5	2.44

图3-43　跳频扩频

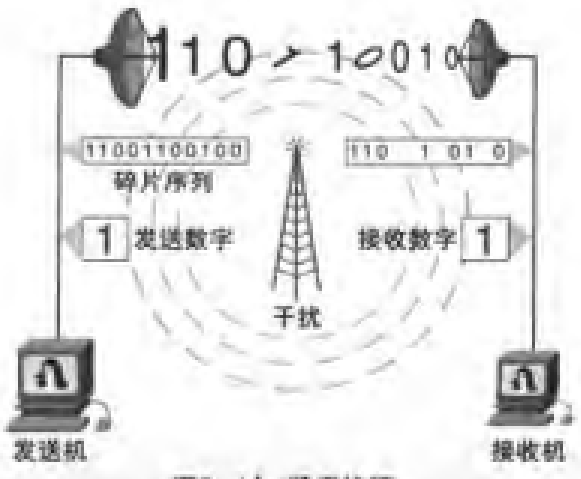


图3-44　顺序扩频

受最高数据传送速率2Mbit/s的限制，FHSS只在某些特定的应用中推荐使用，比如某些类型船只的通信。对于所有其他的无线局域网应用，DSSS都是更好的选择。最新发布的IEEE标准——802.11b，通过DSSS提供了与以太网类似的数据速率——11Mbit/s。FSSS不支持超过2Mbit/s的数据速率。

3.6 无线网络

计算机刚出现时，只有大公司、政府和大学才能买得起。从起初房屋大小但计算能力很低的设备，到能放在手掌中的设备，技术已经发生了巨大的飞越。这样的飞跃同样也发生在这个产业的网络连接领域。

本章前面部分提到的各种类型的网络连接都需要物理连接。其优点体现在速度、可靠性和某种程度的便利性上。物理连接支持共享打印机、服务器和软件以提高生产力。然而，联网的系统，要求工作站保持静止，只能提供介质和办公室范围内的移动。

无线技术的引进消除了这些限制，将真正的可移动性引入了计算机世界。虽然目前的无线技术还不能像有线网络那样提供高速传输，也不能实现有线网络的安全性和工作时间可靠性，但其灵活性弥补了这些不足。

考虑在现有的设施上安装网络时，无线是很多管理员的首选。一个简单的无线网络在工作站开启后几分钟就能运转。到Internet的连接通过有线、路由器、基带调制解调器或数字用户线（DSL）调制解调器提供，对于各个无线节点，无线接入点起集线器的作用。在住宅或小型办公室环境中，这些设备可以被合并到一个单元中。

3.6.1 无线局域网组织和标准

掌握无线技术的规定和标准才能确保所部署的网络的兼容性和互操作性。与有线网络一样，IEEE也是无线网络标准的主要发布者。这些标准是在美国联邦通信委员会以前制定的规定的框架下创立的。

IEEE 802.11标准中的关键技术是DSSS。DSSS适用于工作在1至2Mbit/s范围的无线设备。DSSS最高速率可达11Mbit/s，但高于2Mbit/s时被认为是不兼容的。已通过的下一个标准是IEEE 802.11b，它的传输能力可达11Mbit/s。尽管DSSS WLAN能与FHSS WLAN实现互操作，但所产生的问题促使制造商对设计进行了改变。这样，IEEE的任务就只是制定与厂商解决方案相匹配的标准。

IEEE 802.11b，也叫Wi-Fi，或高速无线，指的是运行在1、2、5.5和11Mbit/s的DSSS系统。所有的802.11b系统都向后兼容，支持802.11中速率为1Mbit/s和2Mbit/s的DSSS。向后兼容性非常重要，因为它使得对无线网络的升级不需要替换网卡或接入点。

IEEE 802.11b设备通过使用与IEEE 802.11不同的编码技术，实现了更高的数据吞吐量，支持在同一个时间帧内传输更大量的数据。大部分的802.11b设备仍然达不到10Mbit/s有线以太网的吞吐量，通常工作在2至4Mbit/s的范围。

802.11a覆盖了工作在5-GHz传输频段的WLAN设备。使用5-GHz频段使得802.11b设备不能与工作在2.4GHz的设备实现互操作。802.11a设备能提供54Mbit/s的数据吞吐量，并且通过*双倍速率*技术能达到108Mbit/s。在生产网络中，更为标准的速率是20至26Mbit/s。

802.11g与802.11a的吞吐量是一样的，但由于采用了正交频分复用（OFDM）调制技术，因此具备向后兼容性。Cisco已经开发了支持802.11b和802.11a设备在WLAN上共存的接入点。接入点提供的网关服务使得本来不兼容的设备可以相互通信。

3.6.2 无线设备和技术

无线网络最少可以只包含两台设备，即两个带有无线网卡的节点。图3-45展示了内置的无线网

卡。图3-46展示了外置USB无线网卡。这两个节点可以是桌面工作站，也可以是笔记本电脑。安装了无线网卡，就建立了一个专门的网络，相当于有线网络中的对等体。在这个环境中，两台设备都可以作为服务器和客户端，尽管提供了连接，但吞吐量和安全性都是最低的。这种网络的另一问题是兼容性，不同厂家的网卡往往不能兼容。



图3-45　内置无线网卡



图3-46　外置USB无线网卡

如图3-47，一般情况下，接入点（AP）作为WLAN基础设施模式的中心集线器而安装。AP通过固定线路连接到有线局域网中，以提供Internet访问和到有线网络的连接。AP是装有天线，在某个特定区域内提供无线连接的设备，这个区域称为一个蜂窝（cell）。

根据安装接入点位置的结构，以及天线的尺寸和增益，蜂窝的大小可以从数英尺到25英里。更常见的距离范围是91.4~152.4m。为了服务更大的区域，可以安装多个AP，覆盖范围有一定程度的交叠，以支持在蜂窝间漫游，如图3-48所示。这种漫游与移动电话公司提供的漫游服务类似。多个AP网络的交叠对于支持设备在WLAN中的移动是至关重要的。尽管在IEEE标准中没有规定，但20~30%的交叠率是所期望的。这样交叠率能支持蜂窝间的漫游，支持无缝地实现断开/重连接而不造成服务中断。



图3-47　接入点

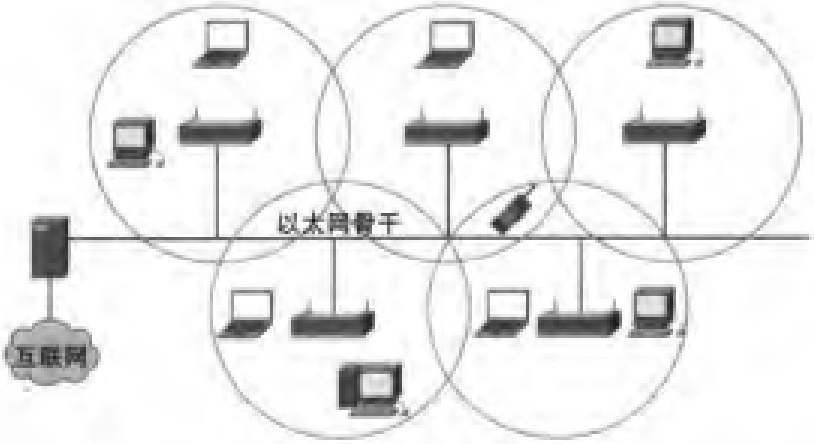


图3-48　漫游

当无线局域网中的客户端被激活后，它便开始监听可以关联哪个兼容的设备。这个过程叫*扫描*，可以是主动的，也可以是被动的。

主动扫描方式下，无线节点发出探测请求，寻找可以加入的网络。探测请求包含了所希望加入网络的服务设置标识符（Service Set Identifier，SSID）。如果遇到使用相同SSID的AP，AP就发出探测回应，身份验证和关联步骤就完成了。

被动扫描节点监听由AP（基础设施模式）或对等节点（临时）发出的信号管理帧（beacons），当一个节点接收到包含自己希望加入网络的SSID的信号管理帧时，便尝试加入该网络。被动扫描是一个持续不断的过程，随着信号强度的变化，节点可以与AP建立或消除关联。

3.6.3 无线局域网间如何通信

建立到WLAN的连接后，节点会像其他802网络一样传送帧。WLAN不使用标准的802.3帧。因此，使用*无线以太网*这一术语是一个误导。帧的类型有三种：控制、管理和数据。以下是每种类型所包含的帧：

- 管理帧
  - —— 关联请求帧。
  - —— 关联响应帧。
  - —— 探测请求帧。
  - —— 探测响应帧。
  - —— 信号帧。
  - —— 身份验证帧。
- 控制帧
  - —— 请求发送（RTS）。
  - —— 清除发送（CTS）。
  - —— 确认。
- 数据帧

只有数据帧与802.3帧相似，然而无线802.3帧的有效载荷是1500字节，以太网帧不能超过1518字节。另一方面，无线帧最大可达2346字节。通常，WLAN帧被限制在1518字节内，因为通常它都与有线以太网相连。

因为无线频率是一个共享介质，因此也会发生冲突，与有线共享介质一样。一个重要的差别在于源节点没有办法检测到冲突的发生。因此，WLAN使用载波侦听多址/冲突避免（CSMA/CA）。这一功能类似载波侦听多址/冲突检测（CSMA/CD）。第5章“以太网基础”中将详细讨论CSMA/CD。

当源节点发送帧时，接收节点返回正确确认（ACK），这会导致50%可用带宽的连续消耗。这种开销，再加上冲突避免协议的开销，使得11Mbit/s的IEEE 802.11b无线局域网实际数据输出降低为5.0~5.5Mbit/s。

网络的运行也会受到信号强度和由于距离和干扰造成的信号质量降低因素的影响。随着信号减弱，可以激活自适应速率选择（ARS），传输单元将速率降低，从11Mbit/s到5.5Mbit/s，从5.5Mbit/s到2Mbit/s，或从2Mbit/s到1Mbit/s，如图3-49所示。



图3-49 自适应速率选择

3.6.4 身份验证和关联

WLAN的身份验证发生在第2层，所验证的是设备而不是用户。记住这一点对于考虑WLAN的安全性、故障排除和整体管理非常重要。

对于使用缺省配置的新AP和NIC，身份验证过程可能是一个空过程。客户端向AP发送身份验证请求帧，该帧被AP接受或拒绝。客户端通过身份验证响应帧获得AP验证结果。也可以配置AP将身份验证任务转交给验证服务器完成，以便进行更彻底的身份验证。

身份验证后的关联允许客户使用AP的服务来传送数据。

身份验证和关联的类型

身份验证和关联的类型如下：

- **未验证和未关联**——节点与网络断开，未与接入点关联。
- **已验证和未关联**——节点与网络相连，尚未与接入点关联。
- **已验证和已关联**——节点与网络连接并可以通过接入点发送和接收数据。

身份验证方法

IEEE 802.11列出了两种验证过程：

- **开放系统**——这一过程是只有SSID能匹配的开放连通标准。尽管低级网络嗅探器保证无线局域网中SSID的能力很高，它可以用于安全或非安全环境。
- **共享密钥**——这一过程要求使用有线对等密钥（WEP）加密。WEP是一种使用64和128字节密钥的简单算法。接入口配有一把加密密钥，通过接入口接入网络的节点必须配有一把配套的密钥。静态WEP密钥比开放系统的安全性要求更高，但不能防黑客。

现在出现了许多安全技术以解决未经验证而进入无线局域网的敏感性。

3.6.5　无线电波/微波频谱

计算机以电的方式传送数据信号。无线电发射器将这些电信号转换为无线电波，这可以通过将电流在发射器天线里的转换完成。这些无线电波从天线里以直线发出，但随之便会减弱。在无线局域网里，发射天线10m以外的无线电信号只有原始强度的1/100。与光一样，无线电波可以被某些材料吸收或被某些材料反射。当从一种材料进入另一种材料时，比如从空气进入塑料墙体，无线电波会发生折射，它还可以被空气中的水滴散射和吸收。

为大楼或园区设计WLAN时，无线电波的质量是很重要的。对安装WLAN的场所进行评估的过程被称为“场所调查”。

因为无线电信号会在传播过程中减弱，接收器就必须配有天线，当无线电波接触到接收器的天线时，天线里会产生弱电流，这些由接收的无线电波引起的电流与发射器天线里最初产生的电流相同。接收器将这些弱电信号的幅度增强。

在发射器里，来自计算机或局域网的电（数据）信号不是直接发送到发射器的天线，这些信号被用来改变另一个更强的信号，称为载波信号。

接收器将天线接收到的承载信号解调。接收器分析承载信号的周期变化并重现原来的电数据信号。

3.6.6　无线局域网上的信号和噪声

在有线以太网上，通常用一个非常简单的过程来诊断干扰的原因。使用无线频率技术时，必须考虑多种类型的干扰。

- **窄带**——一种与扩频相反的技术。顾名思义，窄带不影响无线信号的整个频谱。解决窄带干扰问题的一种方式是改变接入点使用的信道。实际上，检测窄带干扰原因的成本很高，又很费时。检测干扰源需要一台频谱分析仪，即使是很便宜的型号，也需要3000至4000美元。窄带干扰的例子

包括CB无线电波和ham无线电波。

• **全波段**——全波段干扰影响着整个频谱范围。蓝牙技术每秒在2.4GHz范围内跳频多次，对802.11b网络产生很大的干扰。常常可以看到在无线网络设施中有要求进入之前关闭所有蓝牙设备的标牌。在家庭和办公室里，微波炉常被看作制造干扰的东西。1W微波泄到无线频谱就可以导致对网络的严重干扰。2.4GHz频谱内的无线电话也可以构成对网络的干扰。

• **天气**——一般来讲，无线信号即使在极端恶劣的天气里也不会受到影响，然而，雾或太潮湿的环境会影响到无线网络。闪电也可以使空气带电从而改变传输信号的路径。

信号范围问题

首要的也是最明显的信号问题来自于发送站和天线类型。容量更大的发送站将信号发送得更远，抛物面天线也可以集中信号，增加传输距离。

在小办公室和家庭办公室（SOHO）里，大多数接入点都采用两条全方位天线来向各个方向传输数据，从而降低了通信范围。图3-50展示了全方位天线。

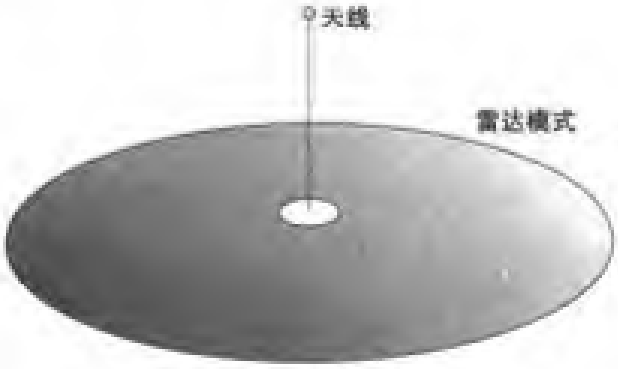


图3-50 全方位天线

3.6.7 无线安全

以指数速度发展的网络，包括无线技术，也伴随着日益严重的安全风险。增加安全性意味着增加管理系统的时间。

无线局域网安全性的第一层次是保护无线电波本身。无线接入点在很广的区域内发射无线电波，这一区域不局限在物理建筑物内，这会使无线电波被偷听而易受影响。在无线网桥中，无线电波被集中为一束激光，窃听者要想中途拦截通信，必须进入激光路径。因此，无线接入点比无线网桥对安全性的要求更高。

3.6.8 WEP

有线对等保密（WEP）是802.11标准下定义的一种安全机制，设计用于保护无线局域网接入点和网卡之间通过空气进行的传输。IEEE 802.11b要求一个40位的密钥。然而，很多厂商，比如Cisco，都支持128位的标准。

WEP的主要目标如下：

• 拒绝没有适当WEP密钥的未经授权用户接入网络。

• 阻止没有WEP密钥者对所捕获的经过WEP加密的通信进行解密。

WEP使用RSA数据安全公司（RSADSI）RonRivest发明的RC4流密码。RC4加密算法是一种支持变长密钥的对称流加密方法。对称加密方法中加密解密使用相同的密钥。这种密钥必须被加密解密双方共享。

近来，加密分析员已经报告IEEE 802.11 WLAN标准下的身份验证和WEP加密方案的弱点。WEP已经进行了一些改进来弥补加密分析员找出的这些弱点。然而，在WLAN中不推荐使用WEP作为惟一的安全机制。应该用其他的高级别安全机制，比如VPN或防火墙，作为WEP的补充。

3.6.9 VPN、EAP和LEAP

一些新的安全解决方案和协议也在不断发展，比如虚拟专用网（VPN）和可扩展身份验证协议

（EAP）。使用EAP时，接入点不提供对客户端的身份验证，而是将这个职责转交给专门完成该功能的更高级的服务器完成。使用综合的VPN服务器时，VPN技术会在现有的协议，比如IP，之上创建一个隧道。隧道是一个3层连接，而不是AP和发送节点之间的2层连接。

以下简要描述了EAP和LEAP：

• **EAP-MD5质询**——EAP是最早的一种身份验证手段，与有线网络上的质询握手验证协议（CHAP）密码保护非常类似。EAP使得无线客户端的适配器能用不同的身份验证类型与不同的后端服务器进行通信，比如远程验证拨入用户服务（RADIUS）。

• **轻量级可扩展验证协议（LEAP）**——Cisco已经开发出了一种基于相互验证的EAP派生协议，称为LEAP。相互验证意味着，在被许可进入企业网络之前，用户和其所试图连接的接入点必须都经过身份验证。相互验证保护了企业不会将未授权的AP作为一个可能的网络入口。LEAP是主要用于Cisco WLAN接入点的一种身份验证技术。通过用动态的WEP密钥加密，LEAP 提供了证件交换过程的安全性，并支持相互验证。

VPN的安全级别包括下列几种：

• **用户验证（User authentication）**——只允许授权用户在网络上进行连接，并发送和接收数据。

• **加密（Encryption）**——提供加密服务，更进一步地保护不受入侵者侵入。

• **数据验证（Data authentication）**——保证数据的完整性，对源和目的设备进行验证。

VPN技术有效地封闭了无线网络，因为无限制的WLAN会自动地在看起来位于相同无线网络上的节点间自动地转发数据。WLAN常常会扩展到其所安装的家庭或办公室边界以外，并且，如果没有安全措施，入侵者可以轻易地渗透到网络中。另一方面，对网络管理员而言，要在WLAN中提供低级的安全措施，所花费的努力是最小的。

3.7　总结

本章学习了以下知识点：

• 电是某种类型原子的电子从限制它的原子分离或流出的能力。

• 异性电荷相吸，同性电荷相斥。在电路中，电流从负极流向正极。

• 根据材料允许电子流动的能力，可以将其分为绝缘体、导体和半导体。

• 电压、电流、电阻和阻抗这些概念提供了一种对电进行测量的手段，这是设计和制造电子设备所需要的。

• 交流电和直流电是电流的两种类型。交流电为我们的家庭、学校和工作场所提供能源。直流电供依靠电池工作的用电设备使用。

• STP电缆综合了屏蔽、抵消和金属线的绞合等技术。ScTP从本质上是包裹在金属箔片屏蔽层内的一个双绞线对。

• UTP电缆是一种用在多种网络中的四线对介质。

• 同轴电缆由四个主要部分组成：铜导线、塑料绝缘层、铜屏蔽编织层和外套。

• 规范或标准是一组广泛使用的规则或规程，用作完成某项任务的公认方法。

• 经过适当的安装、测试和维护，光纤是一种良好的传输介质。

• 光能是电磁能量波的一种，用于在较长距离上安全地传送大量数据。

• 光线在玻璃光纤中传播时遵守反射和折射定律，因此可以制造能产生全反射的光纤。全反射使得光信号能完全保留在光纤中，即使光纤不直也一样。

• 对于长距离线缆传输，尤其是多段缆线是通过配线板连接或结合在一起的时，光信号衰减都是一个问题。因此，在使用之前，线缆和连接器必须安装恰当，并且经过高质量光测试设备的充分测试。

• 在无线数据通信中，无线电频率是用于传送语音、视频和数据的电磁频谱的一部分。

• 调制是对无线电频率或光波的幅度、频率或相位进行改变以实现数据传送的过程。

• 为了利用不需要许可证的无线电频段，必须使用扩频技术。跳频扩频（FHSS）和顺序扩频（DSSS）是两种重要的调制技术。顺序扩频的可靠性和吞吐量都高于跳频扩频。

• 无线信号随着距离的增加而衰弱，如果位于最优范围以外，无线设备只能以更低的速度进行连接。

• 建筑物（带有金属的墙）或用电设备都可能引起噪声。这都会对无线通信的范围造成不良影响。

• 无线标准包括IEEE 802.11、IEEE 802.11a、IEEE 802.11b和IEEE 802.11g。

• 有线对等保密（WEP）是802.11标准中定义的一项安全机制，设计用于保护无线局域网中AP和网卡之间通过空气的传输。

• --些新的安全解决方案和协议，比如VPN、EAP和LEAP正不断涌现。

作为对本章中你所学内容的补充，请参考本书所附CD中针对本章的视频、插图和e-Lab实验。

3.8　关键术语

调幅（*amplitude modulation，AM*）　对载波的高低进行调节。

入射角（*angle of incidence*）　光线接触玻璃表面的角度。

反射角（*angle of reflection*）　反射光线和法线直接的角度。

衰减（*attenuation*）　通信信号的能量损失。

骨干（*backbone*）　网络中主要用作来自或发往其他网络通信的主要路径的部分。

同轴电缆（*coaxial cable*）　由一个中空的外层圆柱型导体和包裹在其中的一条内部导线组成的电缆。

串话（*crosstalk*）　某条线缆上对邻近线缆的电磁信号的不必要接收。

散射（*dispersion*）　光信号沿着光纤范围加宽。

顺序扩频（*direct-sequence spread spectrum，DSSS*）　使得传输更可靠的一种技术，因为每个比特（1或0）都用一串1和0标识，称为碎片序列（chipping sequence）。

电子工业协会（*Electronic Industries Association，EIA*）　一个制定电传输标准的团体。EIA和TIA已经制定了许多著名的通信标准。

电磁干扰（*electromagnetic interference，EMI*）　可造成邻近的电子部件、设备和系统运行中断的电磁场。

跳频扩频（*frequency-hopping spread spectrum，FHSS*）　传输信号随机地从一个频率跳到另一个频率的技术。该项功能使得传输信号能跳开窄带干扰，从而提高了信号的清晰度和传输的可靠性。

光缆（*fiber-optic cable*）　一种能传导调制光信号的物理介质。相比其他的传输介质，光缆更贵，但不受电磁干扰的影响。有时也称为光纤（optical fiber）。

调频（*frequency modulation，FM*）　对波的频率进行调制。

电气与电子工程师协会（*Institute of Electrical and Electronic Engineers，IEEE*）　主要负责制定通信和网络标准的专业机构。IEEE的局域网标准是占主导地位的局域网标准。

阻抗（*impedance*）　交流电路中对电子运动的阻力。

介质（*media*）　单词“介质（medium）”的复数形式。介质指的是传输信号所经过的各种物理环境。常用的网络介质包括双绞线、同轴电缆、光缆和空气（微波、激光和红外可以在空气中传输）。

模式色散（*modal dispersion*）　由于不同模式光入射角的不同，造成其各自在光纤中传输距离不同，从而引起它们到达目的地的时间（在线缆的另一端接收）略有差异。

多模（*multimode*）　光缆的一种，能传送多条光路。

噪音（*noise*）　线路上的一种不需要的电信号，它通过改变信号波形来影响信号质量。

配线板（*patch panel*）　引脚位置和端口的集合装置，能被安装在布线间的架子或墙支架上。配线板起着类似接线总机的作用，实现工作站的线缆的相互连接以及与外界的连接。

调相（*phase modulation，PM*）　对波的极性（相位）进行调制。

反射（*reflection*）　光量子击打表面并以相同的角度但相反的方向离开表面。

折射（*refraction*）　光线进入另一种介质时方向的改变。

无线频率干扰（*radio frequency interference，RFI*） 无线电信号在线路上引起的噪音。

扩频（*spread spectrum，SS*） 19世纪40年代开发的一种调制技术，将传输信号扩展到一个更宽的频率上。术语“扩频”描述了牺牲带宽来获得更高信噪比的调制技术。

标准（*standard*） 广泛使用或正式规定的一组规则或规程。

非屏蔽双绞线（*shielded twisted-pair，STP*） 在多种网络实现中使用的一种两对接线介质。STP线缆有一层屏蔽绝缘层，能减少EMI。

粗网（*thicknet*） 早期的一种同轴电缆，用在10BASE5网络连接中。粗网曾经是很理想的，因为它的信号传输距离可以达到500m。

细网（*thinnet*） 一种简单的细同轴电缆，用于10BASE2系统中。细网的信号传输距离为185m，但使用起来比粗网容易得多。

电信工业协会（*Telecommunications Industry Association，TIA*） 发布电信标准的一个标准协会。

非屏蔽双绞线（*unshielded twisted-pair，UTP*） 用在多种网络中的一种四对线介质。

波长（*wavelength*） 一个波的长度，用一个波的任何一点到与之相应的下一个波的同一点之间的距离度量。光的波长，通常以纳米（nm）为单位。

有线对称保密（*wired equivalent privacy，WEP*） 802.11标准中定义的一种安全机制，用于保护无线局域网AP和网卡之间通过空气的传输。

3.9　复习题

通过完成所有的复习题可以测试你对本章所涉及的主题和概念的理解程度。答案列在附录C“复习题答案”中

1. 搭配左右两列：

1）中子　A）带负电荷的粒子

2）质子　B）不带电荷（中性）的粒子

3）电子　C）带正电荷的粒子

A. 1-C，2-B，3-A

B. 1-A，2-C，3-B

C. 1-B，2-C，3-A

D. 1-B，2-A，3-C

2. 下列关于电的描述哪项不正确？

A. 相反电荷以一种使之相互吸引的力相互作用。

B. 相同电荷以一种使之相互排斥的力相互作用。

C. 对于相反和相同电荷，相互作用力随电荷距离的接近而增加。

D. 以上都不是。

3. 搭配下列的度量和其各自的单位：

1）电压　A）欧姆

2）电流　B）安培

3）电阻　C）伏特

A. 1-C，2-B，3-A

B. 1-B，2-C，3-A

C. 1-A，2-C，3-B

D. 1-C，2-B，3-A

4. 电子在_____环路里流动，叫作_____。

A. 开放；电压

B. 闭合；电压

C. 开放；电路

D. 闭合；电路

5. STP的最大缆线长度是多少？

A. 100英尺

B. 150英尺

C. 100米

D. 1000米

6. 多少对线组成一条UTP电缆？

A. 2

B. 4

C. 6

D. 8

7. UTP使用哪种接头？

A. STP

B. BNC

C. RJ-45

D. RJ-69

8. 同轴电缆相比STP或UTP的优点是什么?

A. 能达到10Mbit/s至100Mbit/s的速率。

B. 便宜。

C. 在不增压的情况下能传输更远的距离。

D. 以上都不是。

9. 双绞线电缆中电线相互绞合的作用是什么?

A. 使线缆更细。

B. 使线缆更便宜。

C. 减弱噪声问题。

D. 使得6对线能装入原本只能装4对线的空间中。

10. EIA/TIA的标准的重要性是什么? 选择所有适合的。

A. 为OSI参考模型的实现提供了框架。

B. 为制造商保证兼容性提供了可以遵守的指导原则。

C. 提出了多产品和多厂商环境下最低的介质要求。

D. 以上都不对。

11. _____光缆传输多束发光二极管产生的光。

A. 多模

B. 多信道

C. 多相位

D. 以上都不对。

12. 在网络中使用光缆的一个优点是什么?

A. 便宜。

B. 易于安装。

C. 是一项行业标准，任何电子商店可以获得。

D. 相比同轴或双绞线电缆，传输速率更高。

13. 哪种光缆通常用于室外安装?

A. 紧密缓冲型。

B. 紧套型。

C. 松散缓冲型。

D. 松套型。

14. 通常用于单模光纤的光源是哪种?

A. 光晶体管

B. 激光

C. 光电阻器

D. 发光二极管

15. 哪一个术语描述了光线射到玻璃表面的角度?

A. 反射角

B. 折射角

C. 入射角

D. 击打角

16. 调制是改变振幅、频率或周期的过程。哪一个缩写代表一种调制类型？

A. AM

B. FM

C. PM

D. RM

17. 下列哪一个范围没有正确标识一个无许可证的频率？

A. 2.4GHz

B. 5GHz

C. 9GHz

D. 900MHz

18. 哪一项不是关于扩频技术优点的描述？

A. 扩频传输的速率高。

B. 扩频技术不易受无线电噪声干扰。

C. 扩频技术使得正确接收的概率更高。

D. 扩频技术产生的干扰很少。

19. 以下哪一项没有描述顺序扩频（DSSS）的特征？

A. DSSS是可靠的，因为每位都用位串1和0表示。

B. 即使丢失的位串达到40%，原始的传输信号仍可以恢复。

C. DSSS技术的数据吞吐量低，接入范围小。

D. 最新发布的IEEE标准，802.11b，支持用DSSS实现完全类似以太网的数据速率11Mbit/s。

20. 下列哪一项不是有线对等保密（WEP）的特征？

A. WEP使用RC4流加密机制。

B. WEP是在802.3标准中定义的的安全机制。

C. WEP的一个目标是拒绝没有适当WEP密钥的未经授权用户接入网络。

D. 以上都不对。



第4章　线缆测试及局域网、广域网布线

目标

学习完本章之后，你应该能够：

- 熟悉基于频率的线缆测试所用的基本术语。
- 理解影响网络介质的信号和噪声。
- 恰当地进行局域网布线。
- 恰当地进行广域网布线。

本章将讲述对局域网物理层连接所用介质进行测试的相关问题。为了使得局域网和广域网能正常运转，物理层介质必须符合针对以太网上传送信号所用各种数据速率的产业标准（10、100、1000或10 000Mbit/s）。本章中，“信号（signals）”一词指的是从发送方向接收方移动的数据信号。在沿物理介质传送的过程中，信号会衰减；然而，接收方必须仍能清楚地确定数据中每个比特的状态（1或0）。否则，就会由于网络中的错误率过高而导致局域网或广域网连接失效。

无论从字面上看还是从物理上看，网络介质都是网络的骨干。劣质的网络布线会导致网络故障和网络性能不可靠。所有三类网络介质（铜线、光纤和无线）都需要进行测试和度量以确定其质量，而这些测试就是本章的主要内容。

请务必看看关于本章的e-Lab实验活动、视频和插图，这些内容可以在本书所附的光盘中找到。光盘中的这些内容用作补充材料，能强化本章中所介绍的概念。

4.1　学习基于频率线缆测试所需的背景知识

测试基于铜线、光纤和无线网络介质所用的设备涉及到一些电子和数学的概念和术语，如信号、波、频率和噪声等。理解这些词汇有助于学习网络连接、布线和线缆测试。

4.1.1　波

*波（Wave）*是从一个位置传播到另一个位置的一种能量。波有很多形式，但都可以用类似的词汇描述。

可以将波看作为扰动（disturbance），一桶完全静止没有扰动的水中是不存在波的。相反，由于

存在风和潮汐这样的扰动，海洋中总是存在某种形式的可检测的波。

海洋波可以用其高度或振幅来描述，度量单位是米。也可以用波到达海岸的频繁程度来描述。这一特征可以用两种类似的方式来描述：周期（period）和频率（frequency）。波的周期是各个波浪之间的时间间隔，度量单位是秒。*频率（frequency）*是每秒到达海岸的波浪数量。

与海洋波一样，电子信号的*振幅（amplitude）*也表示其高度，但其度量单位是伏特而不是米。与海洋波的周期是一个波浪完成的时间一样，如果信号有规律地重复，那么信号的一个完整循环所用的时间便是信号周期，度量单位是秒。电子信号的频率是每秒完整的循环数（波数），度量单位是*赫兹（hertz）*。

如果扰动是故意产生的，并且持续时间固定并且可预测，就称其为*脉冲（pulse）*。在电子信号中，脉冲很重要，因为它们决定了所传送的数据值。

图4-1显示了振幅和频率两个概念的表示方法。

网络专业人员们感兴趣的是特定类型的波：

- 铜介质上的电压波。
- 光纤上的光波。
- 无线环境中使用的，被称为电磁波的电磁场交替。

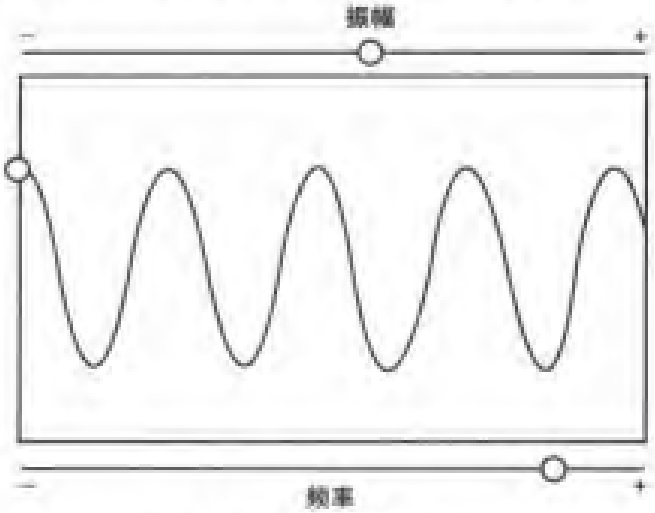


图4-1　振幅和频率

4.1.2　正弦波和方波

如图4-2所示，*正弦波*，或正弦曲线，是一种数学函数图形。

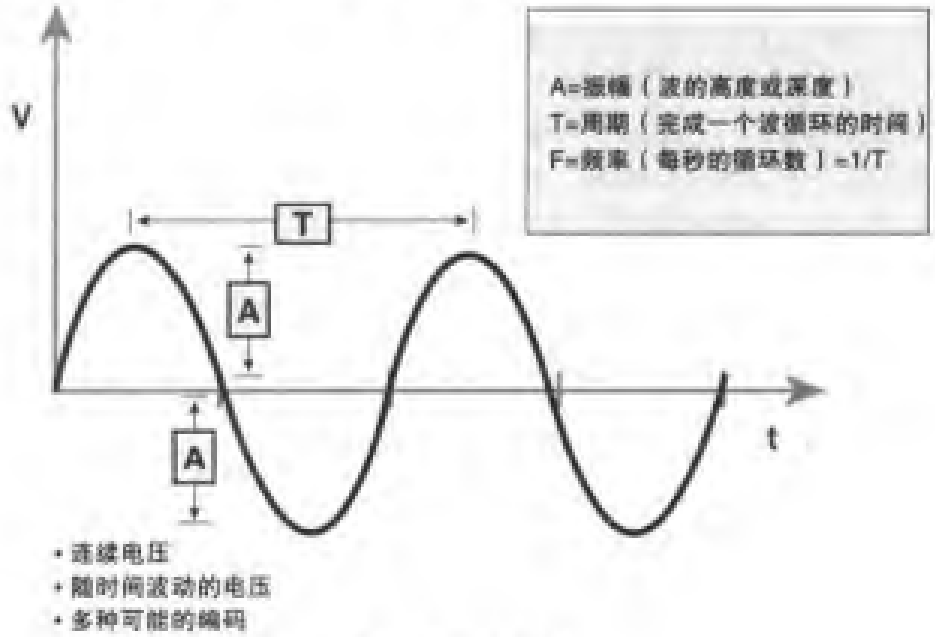


图4-2　模拟信号

正弦波有某些特征：

- **周期性**（定期重复相同的模式）。
- **连续变化**（相邻的两点的数值各不相同）。

正弦波是许多随时间作规律性变化的自然现象的图示，例如地球到太阳的距离，乘坐大观缆车时距离地面的距离，以及一天中太阳升起的时间。由于正弦波是连续变化的，因此属于模拟波。

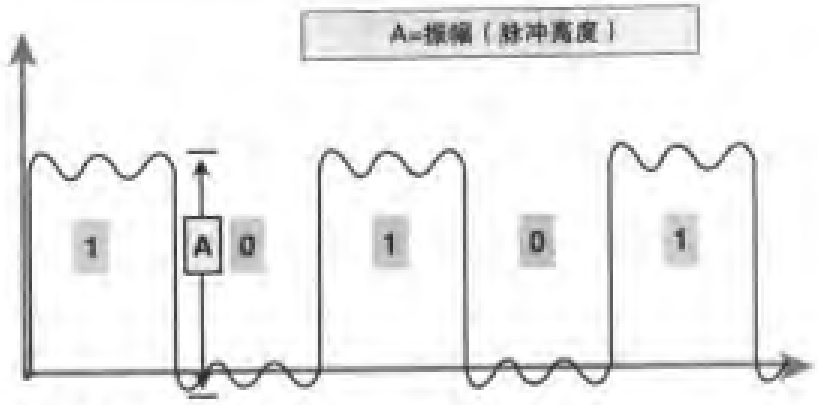


图4-3 数字信号

与正弦波类似，*方波*也是周期性的。然而，方波图形不随时间作连续变化，它的波值在一定时间内保持不变，然后突然变化，再保持不变，最后又突然恢复到初始值，如图4-3所示。方波代表数字信号或脉冲。与所有的波一样，方波也可用振幅、周期和频率来描述。

4.1.3 指数和对数

如第1章“网络入门”中所述，在网络中需要记住三种重要的计数体制：

- **2为底数**（二进制）。
- **10为底数**（十进制）。
- **16为底数**（十六进制）。

计数体制的底数指的是占据一位的不同符号数。例如，二进制计数只有两个不同的占位符（数字0和1），十进制有十个不同的占位符（数字0-9），十六进制有十六个不同的占位符（数字0-9和字母A到F）。

10×10可写作10^2（即10的平方、10的二次方或10自乘两次）。$10 \times 10 \times 10$可写作10^3（即10的立方、10的三次方或10自乘三次）。用这种方式表示时，你可以说10是底数，数字2和3是指数。下面的例子示例了这一概念。

$Y=10^1$	$Y=10^1$
X:2	X:3
Y:100	Y:1000

计数体制的基数也与每位的值有关。最低位的值为*底数*的0次方（基数的0次方），或者1。下一位的值为*底数*。在二进制中等于2，十进制中等于10，十六进制中等于16。

指数形式能更方便地表示非常大的数字。用来表示十亿，比用1 000 000 000来表示更简单，并且更不容易出错。线缆测试中的很多计算都涉及很大的数字，因此指数形式是首选的表示方式。

4.1.4 分贝

描述网络信号的一种重要方式是使用*分贝（dB）*作为度量单位。分贝与上一节描述的指数和对数有关。计算分贝的公式如下：

$dB=10 \log_{10}(P_{out}/P_{in})$

或

$dB=20 \log_{10}(V_{out}/V_{in})$

通常，光纤中的光波和空气中的无线电波用能量公式度量，铜缆上的电磁波用电压公式度量。在这些公式中：

- dB度量了波能量的损失或增加。分贝通常是负数，表示波传播过程中能量的损失，但如果信号被放大，则为正数，表示能量的增加。
- $\log_{10}$表示括号中的数字用以10为底的对数进行了转换。
- P_{final}是以瓦特（watts）为单位的提交能量值。
- P_{ref}是以瓦特（watts）为单位的初始能量值。
- V_{final}是以伏特（volts）为单位的提交电压值。
- V_{ref}是以伏特（volts）为单位的初始电压值。

下面的例子展示了如何计算dB值：

$$P_{final}=P_{ref}\times 10^{(dB/10)}$$

$$dB=20$$

$$P_{ref}=2kW$$

$$P_{final}=200kW$$

当你输入dB和P_{ref}值时，所产生的能量值会随之变化。这种计算能用于查看无线电波通过不同的材料和各种电子系统，传送一定距离后所剩余的能量。

4.2　从时间和频率观察信号

“信息时代”最重要的证据之一便是表示字符、词语、图像、视频或音乐的数据能在线路和电子设备中电子化地表示为电压模式。这些电压模式所表示的数据可以转换为光波或无线电波，并反向转换回电压波。以模拟电话为例。呼叫者声音所产生的声波进入电话的麦克风。麦克风将声能的模式转换为表示声音的电能的电压模式。

如果随时间作出电压模式的图像，就能看到表示声音的各种模式。*示波器（oscilloscope）*是一种重要的电子设备，用于观察电信号，比如电压波和脉冲。显示屏上的X轴表示时间，Y轴表示电压或电流。通常有两个Y轴输入，因此能同时观察和测量两路波。

用示波器分析信号被称为时域分析（time-domain analysis），因为X轴或数学函数的域代表时间。工程师们也用频域分析（frequency-domain analysis）来研究信号。在频域分析中，X轴代表频率。一种称为*频谱分析仪（spectrum analyzer）*的电子设备能产生用于频域分析的图像。图4-4演示了示波器和频谱分析仪上显示的一些信号。

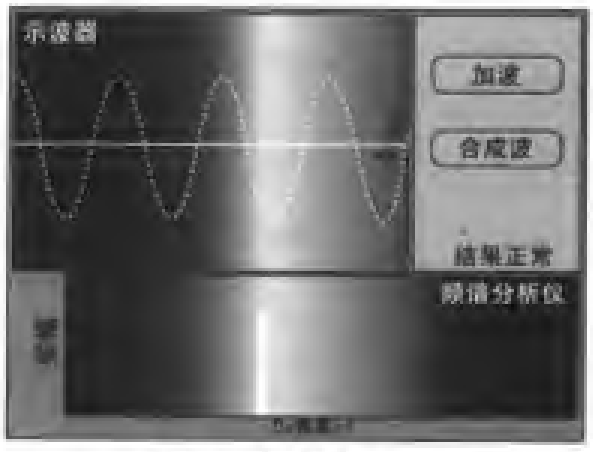


图4-4　傅立叶变换

电磁信号使用不同的频率进行传输，以使得不同的信号不会相互干扰。例如，调频（FM）无线信号所使用的频率与电视或人造卫星信号不同。当听众改变收音机的电台时，他们改变的是收音机的接收频率。

4.3　时间和频率上的噪声

*噪声（noise）*是通信系统（包括局域网）中的一个重要概念，如图4-5所示。尽管噪声通常表示不需要的声音，但通信中噪声的定义是不需要的信号。噪声可能是由自然或技术原因产生的，并附加到通信系统的数据信号中。

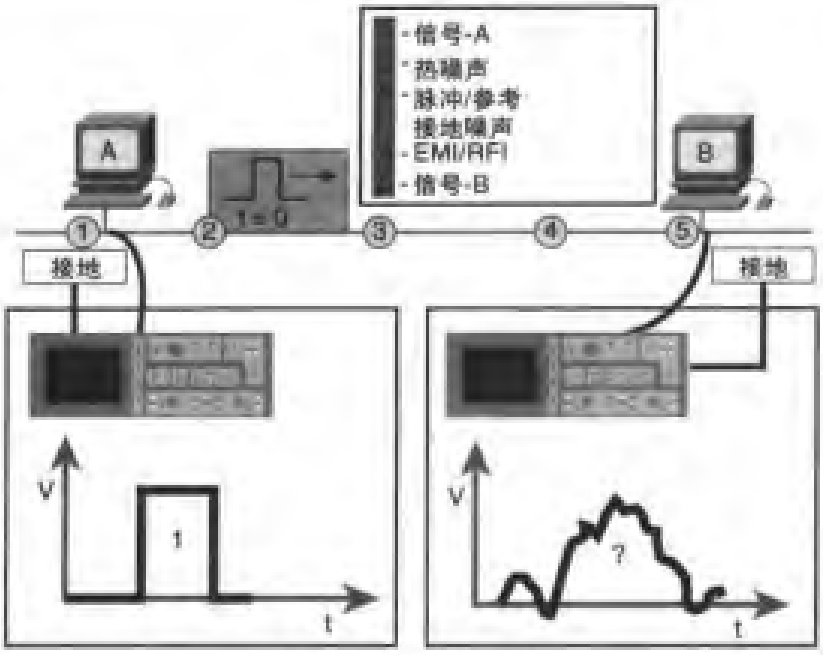


图4-5 识别并定义噪声

所有的通信系统都有噪声。尽管噪声不能完全去除，如果能理解噪声源，就能将噪声的影响降到最低。噪声源包括：

- 邻近的传送数据信号的电缆。
- ***无线频率干扰***（*Radio frequency interference，RFI*），由邻近的其他传送信号产生的噪声。
- ***电磁干扰***（*Electromagnetic interference，EMI*），由邻近的源（比如发送机或光）产生的噪声。
- 光信号的发送端或接收端的激光噪声。

对所有传输频率产生同等影响的噪声称为***白噪声***（*white noise*）。只影响较小频率范围的噪声称为***窄带干扰***（*narrowband interference*）。在无线电接收器上，白噪声干扰所有的电台，而窄带干扰只干扰频率靠近的一些电台。在局域网上，白噪声影响所有的数据传输，而窄带干扰可能只破坏某些信号。然而，如果窄带干扰所影响的频段包括局域网上传送的所有频率，整个局域网的性能就会受到损害。

4.4 模拟带宽与数字带宽

在通信系统中，带宽是一个极为重要的概念。对于学习局域网来说，有两种看待带宽的方式很重要：模拟带宽和数字带宽。

模拟带宽（*analog bandwidth*）通常指的是一个模拟电子系统的频率范围。模拟带宽可以用于描述一个无线电台或电子放大器所发送的频率范围。模拟带宽的单位就是频率的单位：每秒循环数或赫兹。模拟带宽的一个例子是电话使用的3kHz，听觉范围信号的20kHz，调幅广播电台的5kHz和调频广播电台的200kHz。

数字带宽（*digital bandwidth*）用于度量在给定时间内能从一处传递到另一处的信息量。数字带宽的基本度量单位是比特每秒（bit/s）。然而，由于局域网能以数百万比特每秒的速度传输，所以通常用千比特每秒（kbit/s）或兆比特每秒（Mbit/s）作为度量单位，如表4-1所示。带宽受物理介质、当前的技术和物理规律的限制。

在线缆检测过程中，用模拟带宽来确定铜介质的数字带宽。在一端发送模拟频率，在对端接收。然后将发送和接收信号进行对比，计算出信号的衰减量。通常，支持更高模拟带宽并且衰减不高的介质也支持更高数字带宽。

表4-1　数字带宽的各种单位

带宽的数字单位	缩写	换算
比特每秒	bit/s	1bit/s=带宽的基本单位
千比特每秒	Kbit/s	1Kbit/s=1000bit/s=10^3bit/s
兆比特每秒	Mbit/s	1Mbit/s=1,000,000bit/s=10^6bit/s
吉比特每秒	Gbit/s	1Gbit/s=1,000,000,000bit/s=10^9bit/s

4.5　网络介质上的信号和噪声

噪声指的是物理介质上使得接收方检测数据信号更困难的任何干扰。铜缆容易受到多种噪声的干扰，而用光纤作为传输介质时，可能的噪声源就少得多。介质上出现一定级别的噪声是不可避免的，但应使得可接受的噪声级别越低越好。正如当房间的背景噪声与谈话者的声音相比太大时进行交谈会很困难一样，数字信号也可能被噪声淹没，以至无法理解希望得到的信号。

恰当的线缆安装技术和线缆两端接头的恰当连接是至关重要的。如果遵循标准，数据信号的衰减就会更小，噪声级别也会被控制在最低。

一旦完成线缆安装，就必须对其进行测试，以确保其达到电信工业协会/电子工业协会TIA/EIA 568-D标准。在进行下一步的网络硬件安装前，必须找出存在的问题并进行纠正。完成安装后也应该对线缆进行定期测试，以确定其是否仍满足规范。随着时间的推移，线缆和接头会出现磨损和老化，为了保证网络的可靠运行，应该找出潜在的问题并进行纠正。对于所有的线缆测试和故障排除，都必须正确地使用合格的线缆测试仪器。

4.5.1　铜缆和光缆的信号传输

在铜缆上，用二进制的0和1电压变化来表示数据信号。发送方和接收方都根据信号地对电平进行测量。信号地（signal ground）提供了零电压参考值。发送和接收设备必须正确接地，以保证零电压参考点是准确的。

为了使得局域网能正常工作，接收设备必须能准确地将所发送的二进制1和0转换为电平。信号使用的电压很低，低于5伏。由于目前的以太网技术支持每秒数十亿的数据速率，所以必须对每个比特进行识别，即使其持续时间非常短。在接收端不能通过对电平进行放大、或对比特持续时间进行延长来识别数据。因此，当信号经过电缆和接头进行传输时，要尽可能地保持原始信号的强度。面对一直快速发展的以太网协议，新安装的电缆应该使用目前可获得的最优质5类（CAT5）非屏蔽双绞线（UTP）或更高速率的电缆、接头和互联设备，比如压线板（punch-down block）和配线板（patch panel）。

铜缆分为两种基本类型：屏蔽（shielded）和非屏蔽（unshielded）。对于屏蔽电缆，某些类型的屏蔽层保护着数据信号不受外来噪声的干扰。其他类型的屏蔽层保护电缆中的每一对线不受同一电缆内其他线对上电子信号产生的噪声的干扰。

同轴电缆是屏蔽电缆的一种，如图4-6所示。它的构成包括实心的铜导线，导线外覆的绝缘材料和绝缘材料外的网状导电屏蔽层。在局域网中，网状屏蔽层是接地的，以保护内部的导线不受外部电子噪声的干扰。通过将所传送的信号限制在电缆内，屏蔽层还有助于消除信号损失，这使得同轴电缆相比双绞线更不“嘈杂”；然而，同轴电缆更贵。屏蔽层接地的要求和同轴电缆的大体积都使得

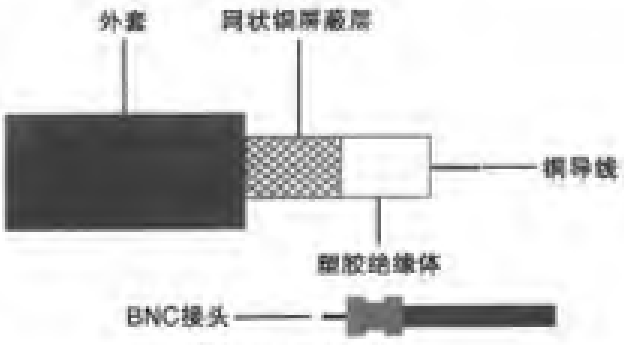


图4-6　同轴电缆

它相比其他类型的铜缆更难安装。

双绞线电缆分为两种类型：

• 屏蔽双绞线（STP）（见图4-7）。

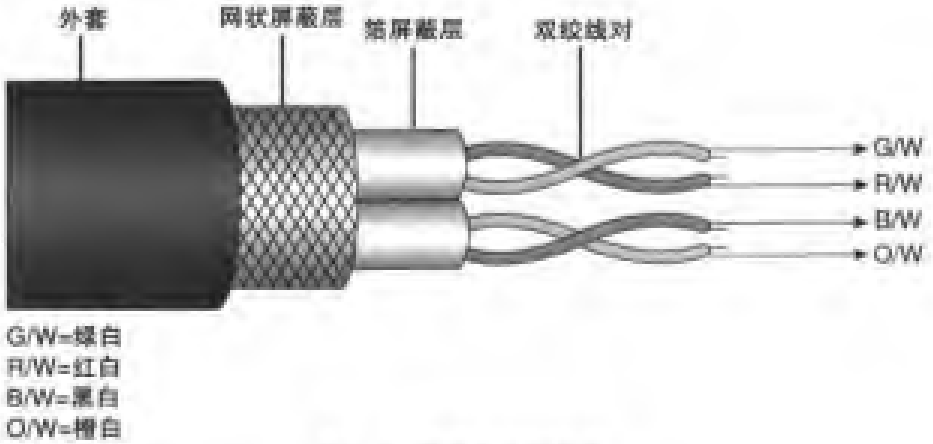


图4-7　屏蔽双绞线电缆

• 非屏蔽双绞线（UTP）（见图4-8）。

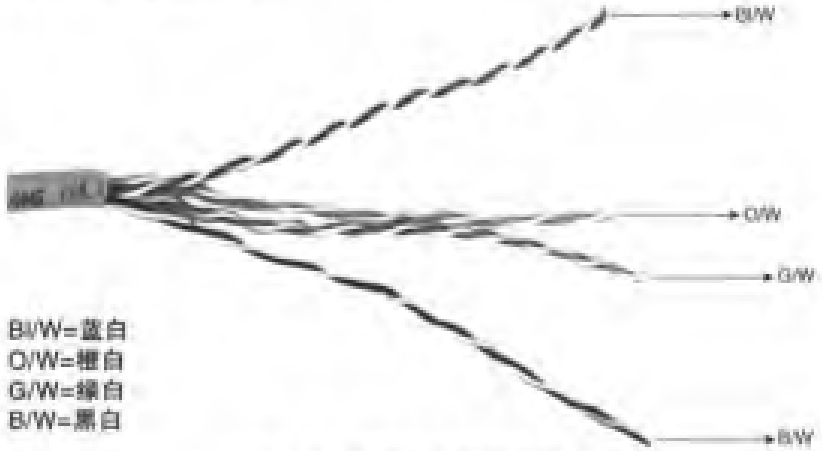


图4-8　非屏蔽双绞线电缆

STP电缆也称为屏蔽双绞线（ScTP）或箔片双绞线（FTP），包含一个外部的带电屏蔽层，该屏蔽层接地以隔绝外部电子噪声信号。STP还使用内部的箔片屏蔽层来保护每个线对不受其他线对所产生噪声的影响。STP电缆更贵、安装更困难，因此不如UTP常用。UTP不包含屏蔽层，是最嘈杂的铜缆，但由于便宜而且容易安装，所以最常用。

如图4-9和4-10所示，光缆通过增强或减弱光强以表示二进制1和0来实现数据信号传送。在相同的传输距离上，光信号强度不会像电信号强度那样减弱。光信号不受电子噪声的影响，因此光纤



图4-9　光纤连接器



图4-10　光纤

不需要接地。所以，光纤通常用在建筑之间或建筑内的楼层之间。随着光纤成本的下降和对带宽需求的增加，光纤可能成为一种更为常用的局域网介质。

4.5.2　铜介质上的衰减和插入损耗

*衰减（attenuation）*是指信号振幅随链路长度的增加而减少，如图4-11所示。线缆越长，信号频率越高，则信号衰减越大。因此，用线缆测试仪测试线缆衰减时所使用的信号是该线缆所支持的最高频率。

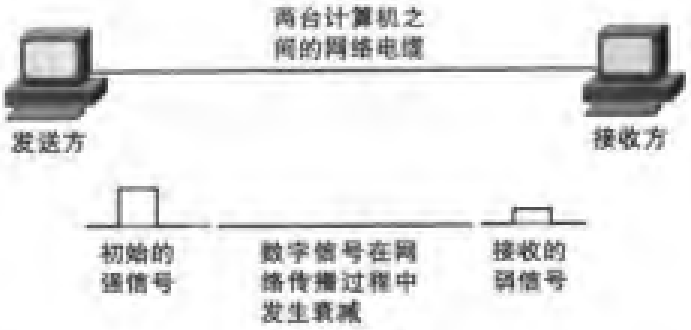


图4-11　衰减

衰减用负的分贝（dB）值来表示。负分贝值越小，表示链路的性能越好。

导致衰减的一些因素：

- 铜缆的电阻将信号的部分电能转换为热能。
- 当信号通过线缆的绝缘层漏出时会造成信号能量损失，不合格接头所造成的阻抗也会导致信号能量损失。

*阻抗（impedance）*是衡量电缆对交流电（AC）阻力的度量，单位是欧姆（Ω）。CAT 5电缆的通常（特征）阻抗是100欧姆。如果CAT 5线缆上的接头安装不当，其阻抗值就会同线缆有差异。这种差异被称为*阻抗不连续（impedance discontinuity）*或*阻抗不匹配（impedance mismatch）*。

阻抗不连续会造成衰减，因为部分的传送信号被反射回了发送设备，而不是继续向接收方传递，这与回声类似。如果多处的不连续造成剩余信号的另外部分被反射回发送方，这种影响就是复合的。当返回的反射信号遇到第一处不连续时，信号的一部分会沿着原始信号的方向回弹，造成多重回声影响。回声到达接收方时间间隔的不同使得接受方很难准确地检测信号的数据值。这种影响被称为抖动（jitter），会造成数据错误。

在一条通信链路上，信号衰减和阻抗不连续的组合影响被称为*插入损耗（insertion loss）*。网络的正常运行依赖于所有线缆和接头特征阻抗的恒定，在整个线缆系统中不存在阻抗不连续。

4.5.3　铜介质上的噪声源

噪声指的是物理介质上使得接收方理解发送方所发送数据更困难的任何电子能量。对于线缆的TIA/EIA-568-B认证现在要求对各种类型的噪声进行测试。UTP对外界的噪声源（比如附近的发送机或荧光灯）或线缆内部的噪声源都没有任何的屏蔽措施。

*串扰（crosstalk）*是指信号从一个线对传送到邻近的线对。当一个线对上的电压发生变化时，便会产生电磁场能量。这种能量会像发送方发出广播信号一样从发送线对向外放射。线缆中的相邻线对像天线一样向邻近的线对产生很弱但类似的电子信号。串扰可能干扰邻近线对上的数据。串扰也可能由邻近的完全分离的线缆引起。当串扰是由另外一条线缆上的信号引起时，被称为*外部串扰（alien crosstalk）*。串扰对于高频传输的破坏更大。

线缆测试工具在测量串扰时首先发送一个测试信号到一个线对上，然后测量在线缆的其他线对上所引起的不必要的串扰信号的振幅。随着传输频率的增加，串扰也会增加，对数据信号的破坏也更大。

如图4-12所示，当各线对被分开时会出现不希望产生的串扰，会受到其他线对数据串扰的影响。因此，可以通过将线对绞合在一起来将串扰降到最低。UTP线缆的类别越高，线缆中所需的绞合数就越多，以便能将串扰降到最低，并且在高频传输时也能达到这一目标。要保证可靠的局域网通信，分开的线对数必须控制在绝对最低。在将接头连接到UTP线缆的末端时，这一点非常重要。



劣质接头，电线拆开部分的距离过长。

优质接头，电线拆开的程度正好够连接接头。

图4-12 接头容易产生串扰

串扰分为三种类型：

- 近端串扰（near-end crosstalk，NEXT）。
- 远端串扰（far-end crosstalk，FEXT）。
- 综合近端串扰（power sum near-end crosstalk，PSNEXT）。

如图4-13所示，*近端串扰*是根据从链路的相同端测量到的测试信号和串扰信号间电压振幅的比率计算得出的。这种差异都用负的分贝（dB）值表示。负值低表明噪声多，负值高表面噪声少，正如负温度，低值所表示的热量比高值更多。依照传统，线缆测试仪不会显示符号来表示负的NEXT值。读出30dB（实际为-30）的NEXT值，相比读出10dB（实际为-10）的NEXT值，表示NEXT噪声更少，线缆更好。

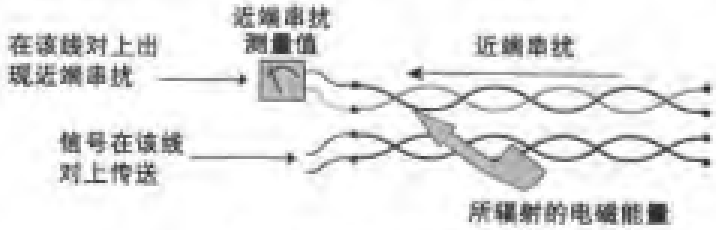


图4-13 近端串扰

在UTP链路中，需要对每个线对对其他线对的近端串扰进行测量，并且在链路的两端都要进行测量。为了缩短测试时间，某些线缆测试仪器支持用户使用比TIA/EIA-568-B更大的频率跨度值来测试链路的近端串扰性能。所得到的测量值可能不符合TIA/EIA-568-B，而且可能忽略了一些链路故障。要验证链路性能是否合格，应该用高质量的测试仪器从链路两端测量近端串扰值。为了完全符合高速电缆规范，这种验证也是需要的。

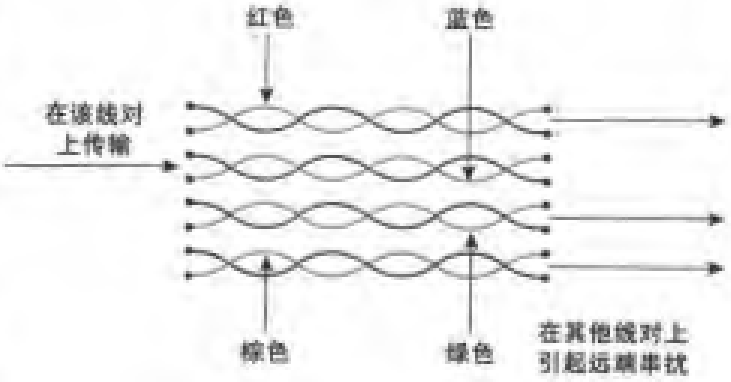


图4-14 远端串扰

由于衰减，在远离发送者的地方出现的串扰（*远端串扰*）在线缆上所产生的噪声相比近端串扰更少，如图14-4所示。远端串扰所引起的噪声仍然会传播回信源，但噪声在回程过程中也会衰减。因此，远端串扰没有近端串扰那样问题严重。

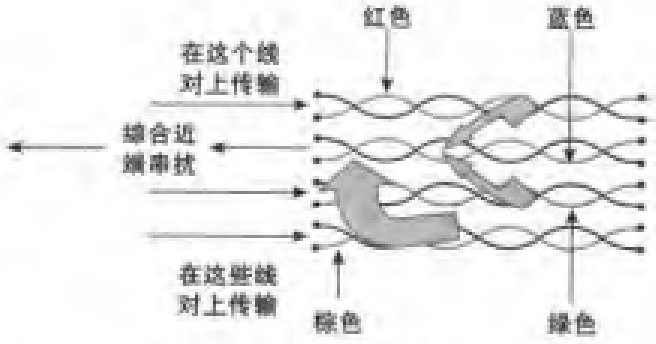


图4-15 综合近端串扰

如图4-15所示，*综合近端串扰（PSNEXT）*测量了来自线缆中所有线对的近端串扰的累积效果。对于四对线缆中的每个线对，PSNEXT是通过三个对-对NEXT测试结果计算的。同时来自多个传输源串扰的综合效应可能对信号是非常有害的。TIA/EIA-568-B认

证现在要求这种PSNEXT测试。

某些以太网标准，例如10BASE-T和100BASE-TX在每个方向上只从一个线对接收数据。然而，对于类似1000BASE-T这样在单个方向上也需要从多对线缆同时接收数据的新技术，综合测量就是非常重要的测试。

4.5.4　线缆测试标准

*TIA/EIA-568-B*标准中规定了铜缆要用于调制解调器或高速以太局域网时所必须通过的十项测试。线缆中的所有链路都要经过该线缆所属分类所适用的最高数据速率测试。

线缆链路要符合TIA/EIA-568-B标准必须检验的主要测试参数如下：

- 接线图（Wire map）。
- 插入损失（Insertion loss）。
- 近端串扰（NEXT）。
- 综合近端串扰（PSNEXT）。
- 等效远端串扰（ELFEXT）。
- 综合等效远端串扰（PSELFEXT）。
- 回波损耗（return loss）。
- 传输延迟（propagation delay）。
- 线缆长度（cable length）。
- 时延偏差（delay skew）。

以太网标准规定，RJ-45接头的每个引脚都有专门的用途，如图4-16所示。网卡在引脚1和2上发送信号，在引脚3和6上接收信号。UTP线缆中的各条导线在线缆两端都必须被连接到适当的引脚上。接线图测试确保了在线缆中不存在断路和短路。如果在接头处导线没有恰当地连接，就会出现断路。如果两条导线被连到一起，就会导致短路。

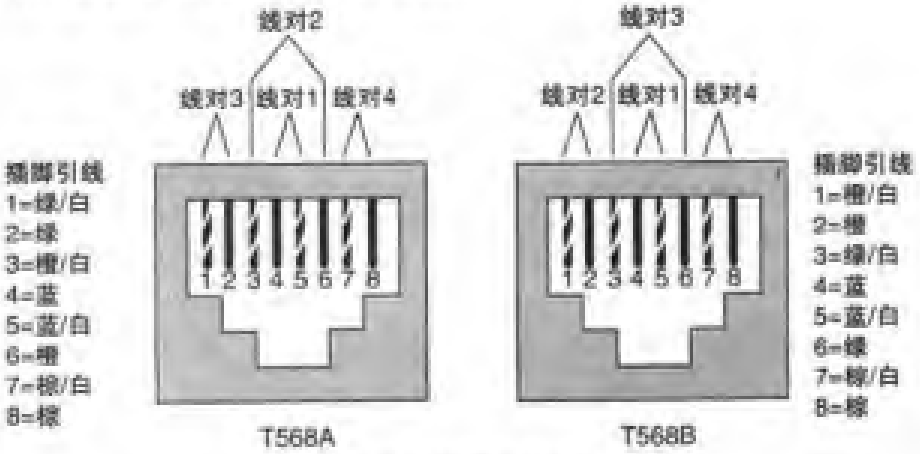


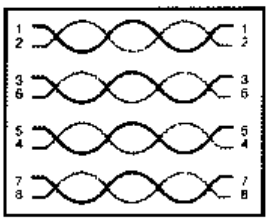
图4-16　RJ-45接头的以太网标准

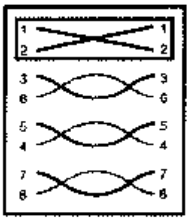
接线图测试也能验证所有八条导线在电缆的两端都连接到了正确的引脚。接线图测试能检测多个不同的接线错误。当在一端的接头上线对安装正确，在另一端的接头上线对颠倒时就会出现颠倒线对（reversed-pair）错误。如果在一端将带橙色条纹的导线放在引脚1，橙色导线放在引脚2；而在另一端将带橙色条纹的导线放在引脚2，而将橙色导线放在引脚1，电缆就会出现颠倒线对错误，如图4-17所示。

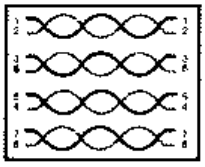
当来自不同线对的两条导线在电缆的两端都连接到了错误的引脚，就会导致分离线对（split-pair）错误。仔细观察图4-17中的引脚编号，以发现接线错误。分离线对会造成各由两条未绞合在

一起的导线构成的发送或接收线对。

当一个线对在两端所连接的引脚完全不同时，就会导致交叉线对（transposed-pair）错误。请对比在两端使用相同引脚对的颠倒线对错误。在同一条链路的不同位置使用下插块（punch-down blocks）上的两种不同颜色的导线（分别表示T568A和T568B）时也会产生交叉线对错误。


正确的T568B接线


颠倒线对接线错误


分离线对接线错误

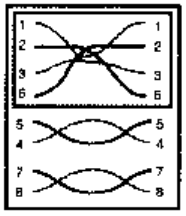

交叉线对接线错误

图4-17 线缆接线图问题

实验活动 Fluke 620 Cable Tester：接线图

本实验中，你将学习Fluke 620 LAN Cable Meter的接线图测试功能。

实验活动 Fluke 620 Cable Tester：错误

本实验中，你将学习Fluke 620 LAN CableMeter的线缆错误测试——合格/失败功能。

实验活动 Fluke 620 Cable Tester：长度

本实验中，你将学习Fluke 620 LAN CableMeter的线缆长度测试功能。

实验活动 Fluke LinkRunner：局域网测试

本实验中，你将使用Fluke LinkRunner来确定线缆的一段电缆是否是活动的，并确定其速度、双工能力和服务类型。你也可以用ping来检验网络层连接性。

实验活动 Fluke LinkRunner：线缆与网卡的检测

本实验中，你将使用Fluke LinkRunner来检验线缆长度和完整性，并确定线缆的终结处。你还将检验PC网卡的功能。

4.6 其他测试参数

在通信链路上，信号衰减和阻抗不连续的综合效果被称为***插入损耗（insertion loss）***。插入损耗随数据传输速率和频率的提高而增加。插入损耗用分贝衡量。TIA/EIA-568-B标准要求，线缆在用作局域网通信链路之前，必须通过插入损耗测试。

串扰通过四个分离的测试进行测量：

- **近端串扰**（NEXT）。
- **等效远端串扰**（ELFEXT）。
- **综合等效远端串扰**（PSELFEXT）。
- **回波损耗**（return loss）。

线缆测试仪测量NEXT时，先在一个线缆对上施加一个测试信号，然后测量在其他线缆对上接收到的串扰信号的振幅。NEXT值用分贝表示，通过在线缆同一端获得的测试信号与串扰信号振幅的差值来计算。记住，由于线缆测试仪所显示的分贝数实际是负值，因此，数越大，NEXT越低。

等效远端串扰（equal-level far-end crosstalk，ELFEXT）测试用于测量远端串扰（FEXT）。对与对之间的ELFEXT以dB为单位，表示所测量的FEXT与信号被FEXT干扰的线对的插入损失之间的差值。在使用1000BASE-T技术的以太网中，ELFEXT是一种重要的测量手段。

*综合等效远端串扰（power sum equal-level far-end crosstalk，PSELFEXT）*是来自各个线对的ELFEXT的综合影响。

回波损耗以分贝为单位，度量由链路上各处的阻抗不连续所引起的信号反射。回忆一下，回波损耗的主要影响不是信号能量的损失，重要的问题是由于来自阻抗不连续处的反射波所引起的信号回波以不同的时间间隔冲击发射器而造成的信号抖动。

4.6.1　时基参数

*传输延迟（propagation delay）*是关于信号通过所测试电缆所用时间的简单度量。线对的延迟依赖于其长度、绞率（twist rate）和电气特性。延迟的单位是纳秒（nanosecond），一纳秒等于十亿分之一秒，或0.000000001s）。TIA/EIA-568-B标准为各种类别的UTP电缆设定了传输延迟的上限。

传输延迟测量值是线缆长度测量的基础。TIA/EIA-568-B-1中规定链路的物理长度的计算选用电气延迟最短的线对。测试器根据时域反射计（Time Domain Reflectometry，TDR）测试所得的电气延迟，而不是线缆外套的物理长度，来测量线缆长度。由于线缆内的导线是绞合在一起的，信号实际传输的距离比线缆的物理长度更长。当线缆测试仪进行TDR测量时，它会沿一个线对发送一个脉冲信号，然后测量在该线对上脉冲返回所需的时间。

TDR测试不仅用于确定线缆长度，也用于确定到发生类似短路或断路故障处的距离。当脉冲遇到断路、短路或劣质连接时，部分或全部的脉冲能量就会反射回测试仪，据此便能计算距连线故障处的大概距离。在定位线缆中的故障连接点（比如墙上插孔）时，这种计算是很有用的。

由于各个线对在绞数和电气特性上的差别，同一条线缆内不同线对的传输延迟可能略有差异。线对间的延迟差异被称为*延迟偏差（delay skew）*。在类似1000BASE-T以太网这样的数据沿多个线对同步传输的高速网络中，延迟偏差是一个关键参数。如果线对间的延迟偏差过大，数据比特到达的时间就不同，数据就无法正确地重新组合。即使一条电缆链路不用作这种类型的数据传输，测试延迟偏差也有助于确保链路能支持今后向高速网络的升级。

局域网中的所有线缆链路必须通过前文所述的TIA/EIA-568-B标准所规定的全部测试，以确保其能在高速和高频时可靠工作。在线缆安装完成时要进行线缆测试，然后定期测试以确保局域网布线满足工业标准。正确地使用高质量的线缆测试仪能确保测试的准确性。对于测试结果要仔细存档。

4.6.2　光缆测试

光纤链路由两条单独的用作分离独立数据路径的玻璃光纤构成。一条光纤承载一个方向的传输信号，另一条承载反向的信号。每条玻璃光纤都包裹有光线无法通过的外套，因此在光缆中不存在串扰问题。外套、外部EMI或噪声对光缆布线都没有影响。在光纤链路上也存在衰减，但相比铜缆要小。

光纤链路容易受到光学中类似UTP阻抗不连续情况的影响。当光遇到光学不连续时，部分光信号沿相反的方向反射，只剩下部分的原始信号继续沿光纤向接收者传送。这导致到达接收端的光能量减少，使得信号识别更加困难。与UTP电缆一样，接头安装不当也是光纤中光线反射和信号强度损耗的主要原因。

由于在光纤传输中噪声不是问题，对于光纤链路主要关心的问题是到达接收端光信号的强度。如果衰减导致接收端光信号的减弱，就会导致数据错误。光缆测试主要就是沿光纤发射一束光，然后测量是否有足量的光到达接收端。

在光纤链路上，需要根据接收端的需求计算可接受的光能损失。该计算也称为光纤链路损耗预算（optical link loss budget）。光纤测试仪器能检查实际的损失是否超过了光纤链路损耗预算。如果光纤未通过测试，线缆测试仪会指出在光缆链路上哪里出现了光学不连续。通常，问题都是由一个

或多个连接不当的接头引起的。线缆测试仪指出了必须更换的连接错误所发生的位置。错误纠正后，缆线需要重新测试。

4.6.3 一项新的布线标准

2002年6月20日，TIA-568标准的6类（CAT6）补充正式发布。这个标准的官方名称是ANSI/TIA/EIA-568-B.2-1。新标准列出了原来的以太网布线十项测试和每项测试的通过分数。通过CAT 6类认证的线缆必须通过全部十项测试。

尽管CAT 6测试内容本质上与CAT 5标准所规定的一样，但是CAT 6线缆通过认证所要求的分数更高。CAT 6线缆必须能承载最高达250MHz的频率，并且串扰和回波损失要更小。

类似Fluke DSP-4000系列或Fluke OMNIScanner2这样的高品质线缆测试仪能完成CAT 5、CAT 5e和CAT 6线缆认证（既包括永久链路也包括信道链路）所需的全部测试测量。

4.7 局域网布线

局域网布线问题属于OSI参考模型的第1层。要理解连接各种网络设备的线缆类型，你需要理解以太网在局域网中的物理层实现，这是在数据链路层中规定的局域网技术。

确定各种不同类型线缆的用途，并区分以太网中使用的各种接头是很重要的。

本节主要介绍局域网的物理层实现和在园区局域网中实现以太网技术的主要原则。本章还会讨论规定用于以太网的各种接头间的差异，以及各种UTP布线标准。

4.7.1 局域网的物理层

以太网是广泛使用的局域网技术。以太网最初是由一个称为DIX（Digital、Intel和Xerox）的团体实现的。DIX创造并实现了首个以太局域网规范，这被用作1980年发布的电气与电子工程师协会（IEEE）802.3规范的基础。此后，IEEE将802.3委员会扩展为三个新的委员会，称为802.3u（快速以太网）、802.3z（光纤上的吉比特以太网）和802.3ab（UTP上的吉比特以太网）。

局域网布线问题属于OSI参考模型的第1层。很多拓扑结构和物理介质都支持局域网。图4-18显示了你可以部署用于支持以太网的各种物理层实现的一个子集。

介质的表示符号各不相同。例如，表示串行线路的符号看起来像一个拉长的字母z或一道闪电；以太网的符号通常是一条直线，带有很多从直线上伸出的垂直线条；令牌环网络的符号是一个连接多个主机的圆圈；对于FDDI，符号是两个连有设备的同心圆圈，如图4-19所示。



图4-18 局域网的物理层实现

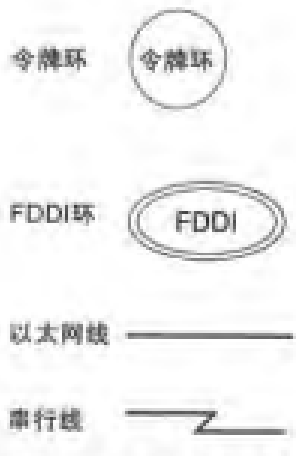


图4-19 局域网物理层介质的符号

介质的基本功能就是在局域网中，以比特或字节的形式承载信息流。除了无线局域网（使用大气或空间作为介质），网络介质都将网络信号限制在导线、线缆或光纤范围内。网络介质被看作局域网第1层的组件。

计算机网络可以用多种不同类型的介质搭建。每种介质都有各自的优势和劣势。一种介质的优势（比如CAT 5的成本）可能是另一种介质的劣势（光纤的成本）。主要的优势和劣势种类如下：

- 线缆长度。
- 成本。
- 易于安装性。

同轴电缆、光缆，甚至是自由空间都能传送网络信号。然而，我们所要研究的主要介质是5类非屏蔽双绞线（CAT5 UTP）。

4.7.2　园区内的以太网

有了可以在园区部署的各种以太网速率，你需要确定在何时（如果需要的话）以及何处升级到一种或多种快速以太网实现。使用正确的硬件和线缆基础设施，10或100Mbit/s以太网可以在网络中的任何地方运行。如表4-2所列，10-Mbit/s以太网通常用在终端用户级的桌面连接，而更快的技术则用于连接服务器或类似路由器和交换机这样的网络设备。

表4-2　推荐的以太网连接

	以太网10BASE-T的用途	快速以太网的用途	吉比特以太网的用途
终端用户级（终端用户设备到工作组设备）	提供终端用户设备和用户级交换机之间的连接	提供高性能PC工作站到服务器的100Mbit/s访问	通常不用在该层
工作组级（工作组设备到骨干）	通常不用在该层	提供终端用户与工作组间的连接。提供工作组到骨干的连接。提供服务器块到骨干的连接	提供从工作组到骨干的高性能连接。提供到企业服务器块的高性能连接
骨干级	通常不用在该层	为中低网络使用量的应用提供连接	提供高速骨干和网络设备的连接

在现今的安装中，尽管部分客户正在提供从骨干到终端用户的吉比特以太网连接，然而布线和交换机端口的开销可能使之无人问津。在作出决定之前，你必须确定网络的需求。例如，一个运行在传统以太网10Mbit/s的网络很容易就被新一代的多媒体、视频和数据库产品所击跨。

通常，可以用下列几种不同的方式在园区局域网中使用以太网技术：

- 以太网或快速以太网可以在用户级提供良好的性能。同样，快速以太网或吉比特以太网可以用于消耗带宽高的客户端或服务器。
- 快速以太网通常用作用户级和网络设备间的连接，以支持从接入链路各个以太网段上汇聚的通信。
- 很多客户/服务器网络都遇到这个问题，即太多的客户端试图访问同一个服务器，这会在服务器所连接的局域网上造成瓶颈。为了增加整个园区局域网的客户/服务器访问性能，并避免在服务器端出现瓶颈，可以使用快速以太网或吉比特以太网链路连接企业服务器。快速以太网或吉比特以太网提供了一种用于避免慢速网络的高效解决方案。
- 也可以用快速以太网链路提供工作组级和骨干之间的连接。由于园区局域网模型支持在各个工作组路由器和骨干交换机之间使用双重链路，因此可以对链路上来自多个接入交换机的聚集通信实现负载均衡。
- 可以在交换机和骨干之间使用快速以太网（或吉比特以太网）。在骨干交换机之间使用价格可

承受的最高速率介质。

• 也可以使用快速以太网连接提供工作组和骨干之间的连接。园区局域网模型可以支持每个工作组和骨干交换机间的双连接，因此可以平衡连接间多接入交换机的加速传输。

• 可以在交换机和骨干间使用快速以太网或吉比特以太网。在骨干交换机之间采用可支持的最快介质。

4.7.3 以太网介质和接头的要求

除了网络的需求，在选择以太网实现方案之前，还必须考虑各种实现所需的介质和接头。用于支持以太网实现的线缆和接头都源自“电子工业协会/电信工业协会（EIA/TIA）”这个标准组织。关于以太网布线分类的定义源自EIA/TIA-568（SP-2840）商用大楼通信布线标准。EIA/TIA规定了UTP使用*RJ-45*接头。字母RJ代表“注册插孔（registered jack）”，编号45指的是有8个传导器的物理接头。

表4-3比较了针对最流行的以太网实现的线缆和接头规范。需要关注的重要区别是分别用于10Mbit/s以太网、100Mbit/s以太网和1000Mbit/s以太网的不同介质。在今天的网络中，你会看到10Mbit/s和1000Mbit/s混合的需求，你必须清楚需要改变到UTP CAT 5上，以支持快速以太网。

图4-20演示了物理层实现所使用的一些不同的连接类型。

表4-3 以太网介质需求比较

	介质	分段的最大长度	拓扑	接头
10BASE2	50Ω同轴电缆（细缆）	185m（606.94英尺）	总线型	英国海军接头（British Naval Connector，BNC）
10BASE5	50Ω同轴电缆（粗缆）	500m（1640.4英尺）	总线型	附属单元接口（Attachment unit interface，AUI）
10BASE-T	EIA/TIA CAT 3、4、5 UTP，两对	100m（328英尺）	星型	ISO 8877（RJ-45）
10BASE-TX	EIA/TIA CAT 5 UTP，两对	100m（328英尺）	星型	ISO 8877（RJ-45）
10BASE-FX	62.5/125多模光纤	400m（1312.3英尺）	星型	全双工介质接口连接器（media interface connector，MIC）直通式（straight tip，ST）接头或用户接头（subscriber connector，SC）
10BASE-CX	STP	25m（82英尺）	星型	ISO 8877（RJ-45）
10BASE-T	EIA/TIA CAT 5 UTP，四对	100m（328英尺）	星型	ISO 8877（RJ-45）
10BASE-SX	62.5/50μm多模光纤	62.5μm光纤为275m（853英尺）；50μm光纤为550m（1804.5英尺）	星型	SC
10BASE-LX	62.5/50μm多模光纤；9μm单模光纤	62.5μm光纤为440m（1443.6英尺）；50μm光纤为550m（1804.5英尺）；单模光纤为3至10km（1.86至6.2英里）	星型	SC

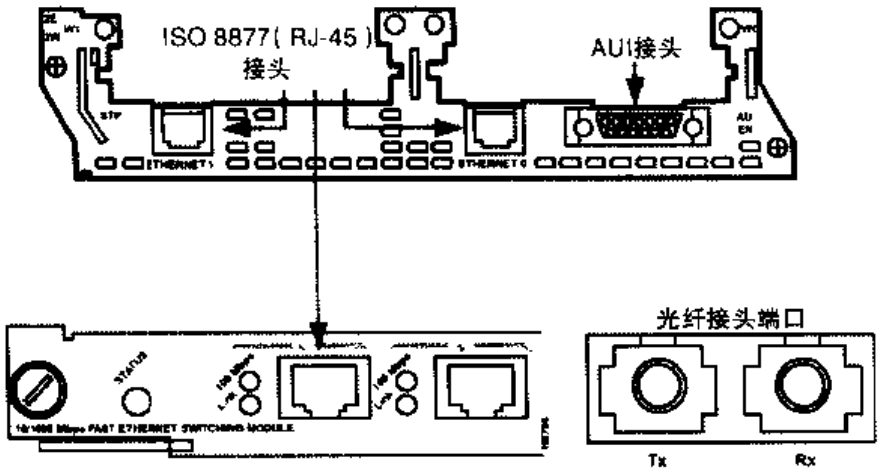


图4-20　区分各种连接

4.7.4　连接介质

本节简单讨论了用于局域网实现的各种连接类型和用于以太网和光纤系统间的一种接口设备——吉比特接口转换器（GBIC）。本章介绍下列主题：

- RJ-45——通常用于终结双绞线电缆的接头。
- AUI——计算机网卡或路由器接口与以太网线缆间的接头。
- GBIC——一种用作以太网和光纤系统间接口的设备。

RJ-45

RJ-45接头和外套是最常用的。在本章的“UTP实现”一节中将更详细地讨论RJ-45接头。

附属单元接口

在某些情况下，网络上的接头类型与所需连接的介质类型不匹配。AUI接头便用作这个接口。AUI是位于计算机网卡和以太网电缆之间的一个15针的物理连接器接口。在10BASE5（粗网）以太网中，用一根短线缆连接计算机上的AUI和主电缆上的发送接收器。在10BASE2（细网）以太网中，计算机上的NIC直接连接到以太网同轴电缆上。

吉比特接口转换器（GBIC）

*吉比特接口转换器（Gigabit Interface Converter，GBIC）*是插入到吉比特以太网端口中的热插拔的输入/输出设备。使用GBIC的一个主要优点是GBIC是可以互换的。这一功能为用户提供了部署其他1000BASE-X技术，而无需改变路由器或交换机上物理接口/模块的灵活性。

光纤GBIC是一个发送接收器，负责将串行电流转换为光信号，也负责将光信号转换为数字电流。下列是一些类型的光纤GBIC：

- 短波长（1000BASE-SX）。
- 长波长/长距离（1000BASE-LX/LH）。
- 扩展距离（1000BASE-ZX）。

通常，GBIC用作以太网和光纤系统间的接口，例如光纤通道和千兆以太网间。图4-21展示了一个GBIC，图4-22展示了GBIC拔出的Cisco WS-X2931 吉比特以太网模块。



图4-21 吉比特接口转换器



图4-22 GBIC拔出的Cisco WS-X2931 吉比特以太网模块

4.7.5 UTP实现

如果仔细观察RJ-45透明端接头，你会看到八条彩色导线。这些导线被绞合为四对。四条导线（两对）传输正或真电压，被称作“顶（tip）”（T1到T4）；其他的导线传输负或假的接地电压，被称为“环（ring）”（R1到R4）。“顶”和“环”源自早期的电话。今天，这些术语分别指线对中的正负电线。线缆中第一个线对中的导线或接头被标为T1和R1，第二对被标为T2或R2，依此类推。

RJ-45是凸型部件，压在线缆的末端。当你从前端观察凸型接头，切面朝下时，引脚的位置从左向右被编号为8到1，如图4-23所示。如图4-24所示，外套是网络设备、墙面或隔间插孔或配线板上的凹型组件。当你观察设备端口时，相应的凹引脚位置自左往右是1到8。



图4-23 RJ-45接头的引脚位置



图4-24 RJ-45插孔和线序

为了使得电流在接头和插孔间流动，线序必须遵守EIA/TIA-568-A和EIA/TIA-568-B标准，如前面的图4-16所示。

除了使用正确类型的EIA/TIA电缆连接设备（这依赖于网络设备插孔使用的标准类型），还需要确定使用下列哪一种电缆：

- **直通线缆**（straight-through cable）——一直保持引脚连接不变的电缆。因此，线缆两端连接到引脚1的导线是相同的。
- **交叉线缆**（crossover cable）——交叉关键线对，以使之在设备和线路连接之间适当地排列、发送和接收信号的线缆。

如果将线缆两端的RJ-45接头按照相同的方向并排，会在每个接头端看到彩色导线（或彩条或引脚）。如果两端彩色导线的顺序相同，电缆就是直通的。图4-25展示了两端RJ-45接头中所有导线顺序相同的情况。

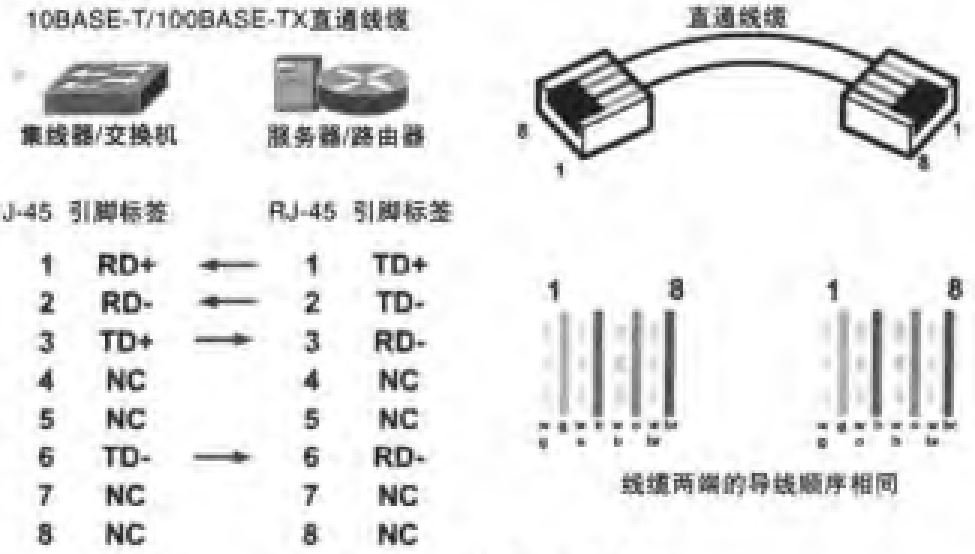


图4-25　UTP实现：直通线缆

以太网中规定，只使用CAT 5 UTP线缆的线对1、2、3和6来发送（TD）和接收（RD）信号。另外四对导线未使用。如图4-25左边所示，在直通线缆中，一端的RJ-45引脚1、2、3和6连接到了线缆另一端的引脚1、2、3和6。但是，吉比特以太网使用全部八对导线。

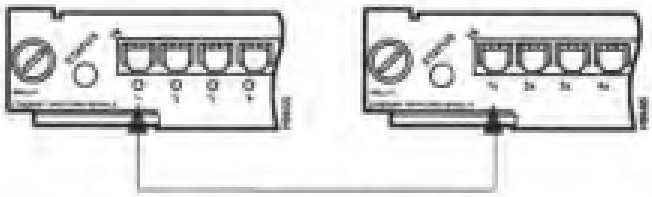


图4-26　用直通线缆进行设备互联

直通电缆可以用于将类似PC或路由器这样的设备连接到其他用作集线器或交换机的设备上。如图4-26所示，只有当端口标识有x时，才应该使用直通线缆。

对于交叉线缆，观察两端的RJ-45接头发现，线缆一端的某些导线交叉到了线缆另一段的其他引脚中。以太网中规定，一端的RJ-45引脚1应该连接到另一端的引脚3。一端的引脚2应该连接到另一端的引脚6，如图4-27所示。

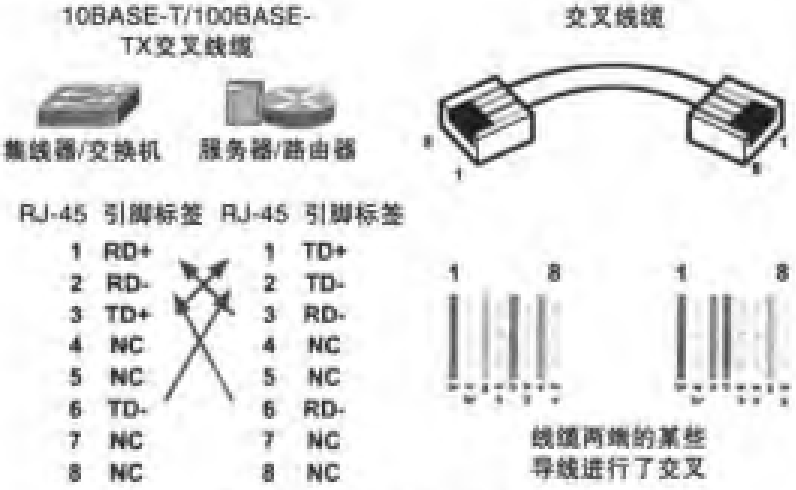


图4-27　UTP实现——交叉线缆

可以用交叉线缆来连接类似的设备，交换机到交换机或交换机到集线器。图4-28显示了当两端的端口都标有x，或都未标x时，应该使用交叉电缆。

下列是在互联网络设备时选择线缆类型的指导原则。

用直通线缆进行下列的连接：

- 交换机到路由器。
- 交换机到PC或服务器。

- 集线器到PC或服务器。

用交叉线缆进行下列的连接：

- 交换机到交换机。
- 交换机到集线器。
- 集线器到集线器。
- 路由器到路由器。
- PC到PC。
- 路由器到PC。

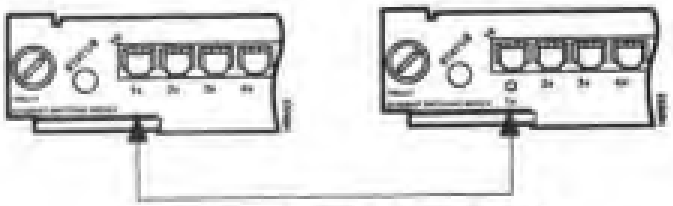


图4-28 用交叉线缆进行设备互联

实验活动 为插孔压线

本实验中，你将学习使用压线工具（punch-down tool）完成安装在墙面的RJ-45数据插孔的连线。

4.8 局域网连接设备

多种类型的设备相互连接构成了局域网。这些设备被称作局域网硬件组件。本节将讨论局域网环境中使用的通用硬件组件。局域网设备包括中继器、集线器、网桥、交换机和路由器，其中交换机是现代局域网中最普遍的设备。

4.8.1 中继器

如在“局域网的物理层”一节所提到的，以及图4-19所示，存在多种类型的介质，它们各自都有其优势和劣质。CAT 5 UTP最常被提及的缺点之一是线缆长度。网络中，UTP线缆的最大长度为100m（大约333英尺）。如果你已经对网络进行了扩展，超出了这个限制，就需要增加中继器（repeater）。在多数以太网络中，中继器通常以集线器（hub）的形式出现，也就是一个多口中继器；也会以使用更新技术的交换机（switch）形式出现。

术语*中继器（repeater）*源于早期的可视通信，当时，站在某座山上的人将重复前一座山上的人传来的信号，从而将信号传达给下一座山上的人。电报、电话、微波和光通信都使用中继器在长距离传输中对信号进行增强。

如图4-29和4-30所示，中继器的目的是在比特级对网络信号进行再生（regenerate）和重定时（retime），以使其能在介质上传输更长的距离。如果存在太多的网络节点，或线缆数量不足时，通常使用中继器。在扩展局域网段时，以10Mbit/s总线型以太网的“4中继器规则（Four Repeater Rule）”，也称为“5-4-3规则”，作为标准。该规则规定，使用4个中继器最多只能实现5个网段的端到端连接。

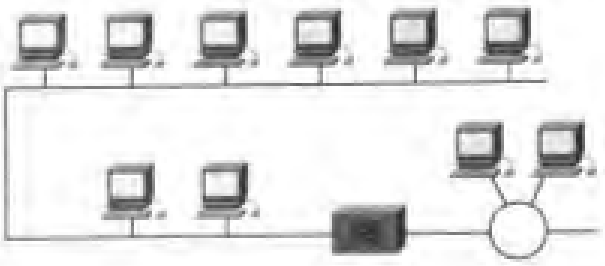


图4-29 中继器

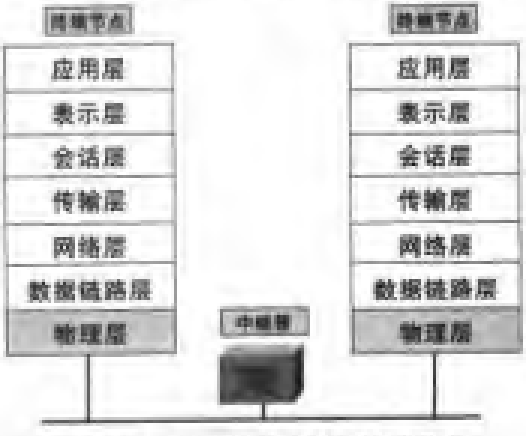


图4-30 用中继器连接两终端节点

但其中只有3个网段中能连接主机（计算机）。尽管在应用到总线型网络上时，5-4-3规则很重要，但对于交换机和扩展星型拓扑就而言不太有效了。

4.8.2　集线器

集线器实际上就是多端口中继器。在很多情况下，这两种设备间的差别只是各自提供的端口数量不同。典型的中继器只有2个端口，集线器则通常有4口到24口，如图4-31所示。另外，集线器通常用在以太网10BASE-T或100BASE-T网络中，尽管在其他的网络体系结构中也可以使用集线器。



图4-31　八端口集线器

利用集线器，网络拓扑从所有设备都直接插入线缆的直线型总线结构，转变为星型结构。利用集线器，通过线缆进入一条集线器端口的数据在连接到相同网段的所有其他接口（除去数据发送的端口）上被进行电气中继。

集线器分为两种基本类型：

- **有源型**（*Active*）——***有源集线器***必须插到电插座中，因为它需要能量将进入的信号放大，然后从其他的端口发送出去。
- **智能型**（*Intelligent*）——***智能集线器***有时也被称为*聪明集线器*（*smart hubs*）。这些设备的工作方式基本上与有源集线器类似，但还包括一个微处理器芯片并具备诊断能力。相比有源集线器，智能集线器更贵，但在故障排除时也更有用。

所有连接到集线器上的设备都能接收全部的通信。因此，集线器是单个冲突域。冲突（collision）是指两个终端工作站同时在网络线路上发送数据的情况。

有时，集线器也被称为集中器（concentrators），因为对于以太局域网，它们起一个中央连接点的作用。



实验活动　购买集线器

本实验中，你要了解市场上的各种网络组件及其各自的价格。主要关注的是以太网集线器和网卡。

4.8.3　网桥

有时需要将一个大型的局域网分解为多个更小、更易于管理的网段。这种策略减少了单个局域网内的通信量，能将网络的地理区域扩展为超过单个局域网所能支持的范围，如图4-32所示。用于将各个网段连接在一起的设备包括网桥、交换机、路由器和网关。交换机和网桥都工作在OSI模型的数据链路层。网桥的功能是作出关于是否将信号传递到网络中下一个网段的智能决定。网桥也可以用于连接不同的协议和介质，好比在城域中用无线网桥互联以太局域网。

网桥从网络上接收到数据帧后，会在网桥表中查找目的MAC地址以确定是过滤该数据帧，对其进行泛洪，还是复制到另一个网段。决策过程如下：

- 如果目的设备所在的网段与数据帧相同，网桥

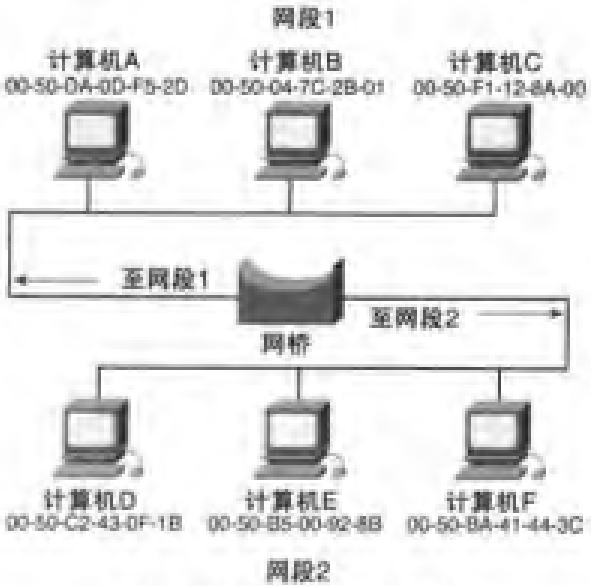
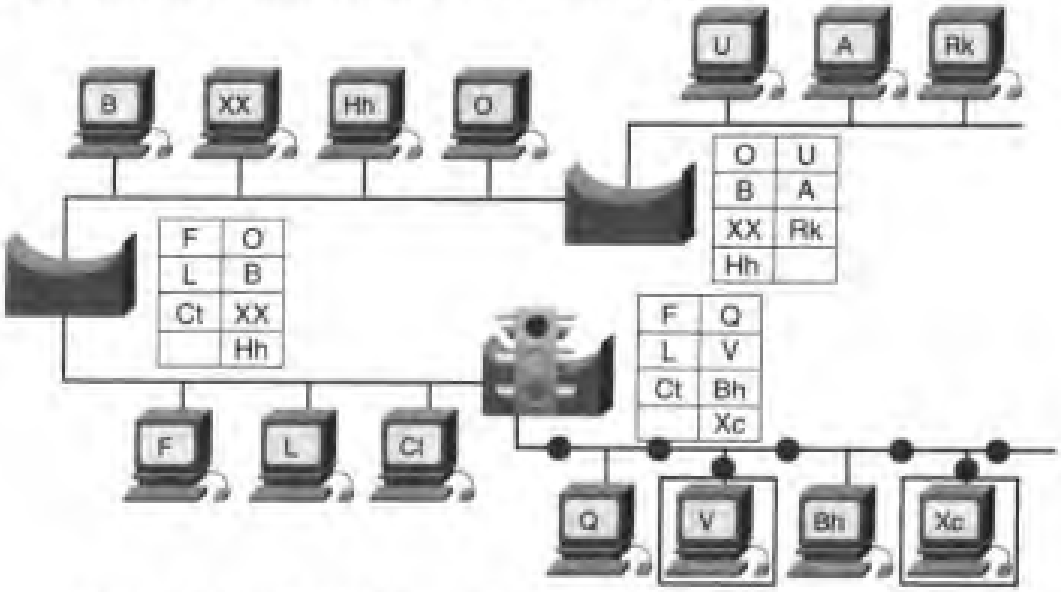


图4-32　用网桥对网络进行分段

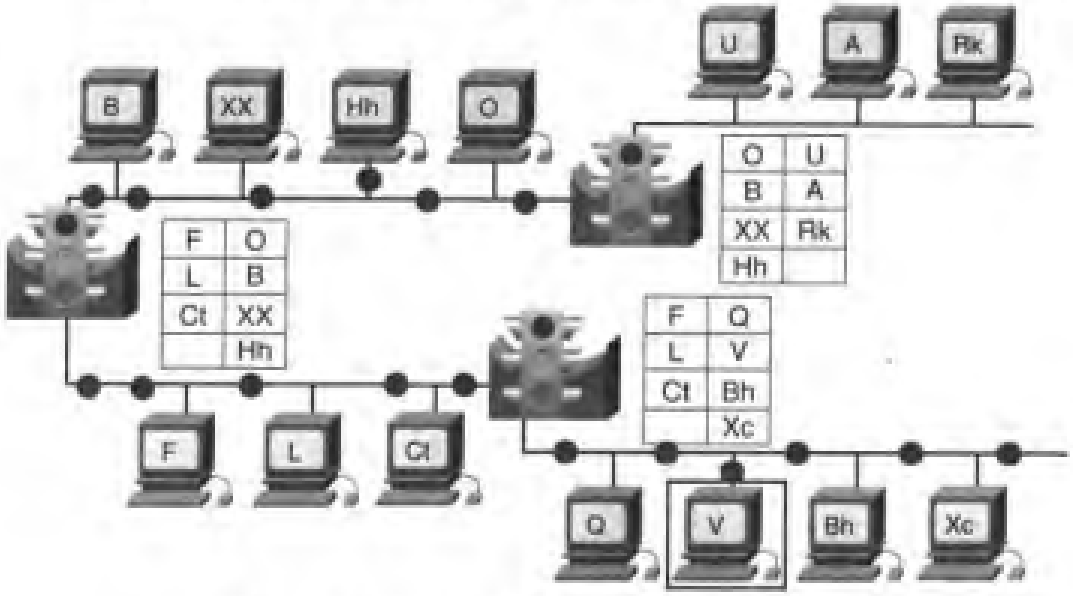
会阻止帧进入其他的网段，如图4-33所示。这个过程称为*过滤（filtering）*。



本例中，数据分组源自计算机V，目的地为计算机Xc。数据分组到达了最终的目的地，并且没有广播到网络中的其他网段上。

图4-33 用网桥对网络进行分段：过滤

• 如果目的设备位于不同的网段上，网桥则将帧转发（forward）到适当的网段，如图4-34所示。



本例中，数据分组源自计算机V，目的地为计算机Hh。
网桥检查自己的网桥表以确定是否允许信号继续向网络中的其他网段传送。

图4-34 用网桥对网络进行分段：转发

• 如果目的地址对网桥是未知的，网桥会将数据帧转发到除接收该帧的端口以外的所有端口。该过程称为*泛洪（flooding）*。

如果作战略性地放置，网桥能大大提高网络性能。

4.8.4 交换机

交换机有时也被称为多口网桥。典型的网桥可能只有两个端口（连接两个网段），而交换机可能有多个端口，这取决于所需要连接的网段数量。与网桥一样，交换机也会学习关于接收自网络上各

个计算机的数据分组的特定信息。交换机用这些信息来构建转发表，以确定从一台计算机发往其他计算机数据的目的位置，如图4-35所示。

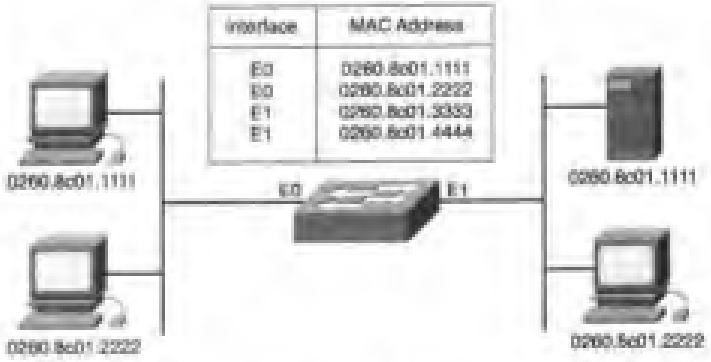


图4-35　交换表

尽管交换机作为一种比网桥更高级的设备，但与网桥有某些相似性。网桥是根据目的MAC地址来确定是否将帧转发到其他的网段。交换机有多个端口，分别连接多个网段。交换机会选择目标设备或工作站所连接的网段。以太网交换机正成为越来越流行的解决方案，因为与网桥一样，它们也能提高网络的性能（速度和带宽）。

交换技术通过减少通信量和增加带宽，缓解了以太局域网中的拥塞问题。由于能在现有的线缆基础设施上工作，交换机常常替代共享集线器，这样既能提高性能，对现有网络的影响又最小。

当今，在数据通信中，所有的交换设备都完成两种基本操作：

- **交换数据帧**——从输入介质上接收帧，然后从输出介质上发送出去的过程。
- **交换操作的维护**——交换机构建和维护交换表并查找环路。

交换机的运行速度远高于网桥，并且可以支持其他功能，比如虚拟局域网。

以太网交换机有很多优点，比如允许多个用户在一个虚拟的无冲突环境中利用虚拟电路和专用网段实现并行通信，如图4-36所示。这种安排实现了共享介质上可用带宽的最大化。另一个优点是迁移到交换式局域网环境是很划算的，因为现有的硬件和布线可以重用。

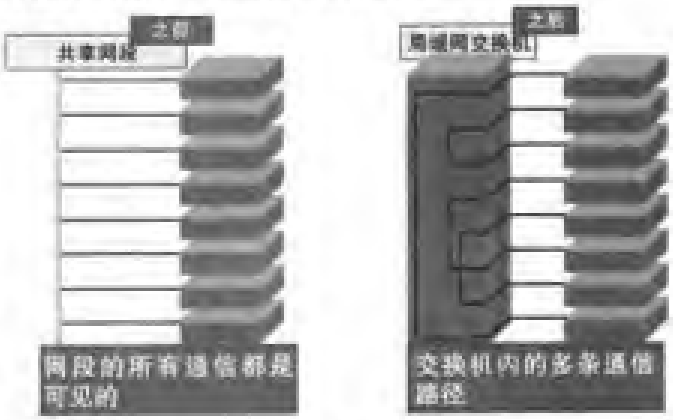


图4-36　通过交换机实现网络的微分段



实验活动　购买局域网交换机

本实验中，你要了解市场上的各种网络组件及其各自的价格。主要关注的是以太网交换机和网卡。

4.8.5　无线网络介质

无线网络是连接局域网的另一种方法。你不需要任何的线缆，并且可以很容易地移动计算机。无线网络使用无线电频率（radio frequency，RF）、激光、红外线（infrared，IR）或卫星/微波来传送信号，完成从一台计算机到另一台计算机的信号传送，没有永久的线缆连接。无线信号是通过空气传送的电磁波。由于不需要物理介质，无线信号成了构建网络的万能方式。

无线数据通信的一个常见应用是移动应用。移动应用的例子包括，经常往返者、飞机、卫星、外层空间探测器、航天飞船和空间站。

无线通信的核心是被称为发送器和接收器的设备。信源与发送器交互，将数据转换为电磁（electromagnetic，EM）波，然后由接收器进行接收。然后，接收器将这些电磁波转换回数据，提交给目的方。为了实现双向通信，每台设备都需要一个发送器和一个接收器。很多的网络设备制造商将发送器和接收器制造成一单个的单元，称为发送接收器（transceiver）或无线网卡。无线局域网（wireless LAN，WLAN）中的所有设备都必须恰当地安装无线网卡。

用于网络的两种最常见的无线技术是红外线和无线电频率。红外线技术有自己的弱点。工作站

和数字设备必须位于发射器所发射光线的直线上才能工作。基于红外线的网络环境适用于所有需要网络连接的数字设备都位于同一个屋内的情况。IR网络技术可以很快地安装，但是数据信号可能受屋内人走动或空气中湿气的影响而减弱或被阻挡。然而，一种新的能在视距外工作的红外线技术正在研发之中。

无线电频率技术允许设备位于不同的房间甚至不同的建筑内。无线信号最大距离的有限性仍限制了这类网络的应用。无线电频率技术可以工作在一个或多个频率上。单个无线电频率容易受到外界干扰和地理的阻碍。而且，单个频率很容易被他人监听，这会造成数据传输的不安全。扩频技术通过使用多个频率增加了抗噪声的能力，并且使得外来人员很难破解数据传输，从而解决了数据传输不安全的问题。

无线环境下的安全问题

网络连接以及无线技术的指数增长导致了安全风险的增加。增强安全性意味着增加花费在系统管理上的时间。

无线局域网安全性的第一级是保护无线电频波本身。无线接入点所发射的无线电波能到达很大的范围，不仅仅局限在物理建筑内，这使得无线电波可以被偷听者访问，因此增加了攻击的可能。无线网桥使用的无线电波集中为一个波束。偷听者需要在波束的路径上才能截取通信。因此，无线接入点通常比无线网桥所要求的安全性更高。

如果你认为某些人可能在你的局域网无线链路上进行偷听，那加密就是关键。

下面几节讨论了两种无线安全方案：***有线等效保密（wired equivalent privacy，WEP）***和IEEE 802.1 X或可扩展身份验证协议（Extensible Authentication Protocol，EAP）。

WEP

WEP是解决客户安全担心的第一步。WEP是802.11标准中定义的一种安全机制，设计用于保护无线局域网接收点和网卡间通过空气的传输。IEEE 802.11b 需要40位的密钥。然而，很多厂商，比如Cisco，都支持可选的128位标准。

WEP的主要目标是：

- 拒绝没有适当WEP密钥的未经授权用户接入网络。
- 阻止没有WEP密钥者对所捕获的经过WEP加密的通信进行解密。

WEP使用RSA数据安全公司（RSADSI）RonRivest发明的RC4流密码。RC4加密算法是一种支持变长密钥的对称流加密方法。对称加密方法中加密解密使用相同的密钥。这种密钥必须被加密解密双方共享。

近来，加密分析员已经报告IEEE802.11 WLAN标准下的身份认证和WEP加密方案的弱点。WEP已经进行了一些改进来弥补加密分析员找出的这些弱点。然而，在WLAN中不推荐使用WEP作为惟一的安全机制。应该用其他的高级别安全机制，比如VPN或防火墙，作为WEP的补充。

802.1X/EAP

IEEE 802.1X/可扩展身份验证协议（Extensible Authentication Protocol，EAP）是可替代IEEE 802.11所规定的WEP的一种安全方案，IEEE 802.1/EAP 主要着眼于提出一个用于进行集中式认证和动态密钥分配的框架。IEEE 802.1 X是一个基于端口的网络访问控制标准。EAP允许可支持不用身份验证类型的无线客户端适配器与不同的后台服务器，比如远程身份验证拨入用户服务（Remote Authentication Dial-In User Service, RADIUS）。

Cisco Systems公司已经开发出了一种基于相互验证的EAP派生协议，称为轻量EAP

（Lightweight EAP，LEAP）。相互验证意味着，在被许可进入企业网络之前，用户和其所试图连接的接入点必须都经过身份验证。相互验证保护了企业不会将未授权的接入点作为一个可能的网络入口。

Cisco LEAP身份验证的主要优点如下：

- 集中式验证和密钥分配。
- 由于支持多种操作系统并且动态产生密钥，因此适用于大规模的企业WLAN部署。

4.8.6　主机的局域网连接：网卡和接口

顾名思义，如图4-37和4-38所示，网卡（NIC）是安装在计算机主板或外设的总线上的一个扩展槽内的一块印制电路板。也可以叫网络适配卡（network adapter）。在膝上型/笔记本电脑中，网卡通常是信用卡大小。网卡的功能是将主机设备连接到网络介质。



图4-37　网络接口卡（电路板）

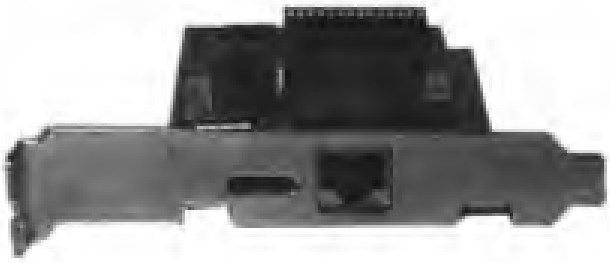


图4-38　网卡（介质连接）

网卡工作在OSI模型的第1层和第2层。网卡被看作2层设备是由于全世界的每块网卡上都有一个惟一代码，称为介质访问控制（Media Access Control，MAC）地址。这个地址用于控制主机在网络上的数据通信。第2层设备，比如网桥或交换机，都使用各个网卡的MAC地址。在本章的后续部分，你会了解更多关于MAC地址的信息。顾名思义，网卡控制着主机对介质的访问。因此，网卡也工作在第1层，因为它只关注比特，不关注任何的地址信息和高层协议信息。网卡通常内置发送接收器。

某些情况下，网卡上接头的类型与所需要连接的介质类型不匹配。Cisco 2500路由器就是一个很好的例子。在这款路由器上，以太网接口是一个AUI接头，需要连接的是UTP CAT 5以太网电缆。为了完成连接，需要使用一个发送接收器（transceiver，即transmitter/receiver）。以太网发送接收器提供发送/接收功能（因为任何一项都没有内置到以太网接口中），并且同时将一种类型的信号或接头转换为另一种类型（例如，连接15针的AUI接口到RJ-45插孔）。

在图示中，网卡没有标准化的符号。当联网设备连接到网络介质时，就隐含了网卡或类似网卡设备的存在。当拓扑图上出现小点时，就代表一个网卡或起网卡作用的接口（端口）。

4.9　工作站和服务器

通过使用局域网和广域网技术，很多计算机被互联在一起，为用户提供各种服务。为了完成这项任务，联网的计算机扮演着不同的角色，起着不同的功能。某些类型的应用要求计算机像均等的伙伴那样工作。其他类型的应用对任务进行分配，一台计算机以一种不对等的方式为很多其他的计算机提供服务。无论哪种情况，两台计算机通常都使用请求/响应协议进行相互通信。一台计算机发出针对某项服务的请求，另一台计算机接收并响应该请求。请求方扮演客户端的角色，响应方扮演服务器的角色。

4.9.1 对等网络

在*对等网络（peer-to-peer network）*中，联网的计算机相互之间像平等的伙伴，或对等体一样。对等网络也被称为*工作组（workgroups）*。作为对等体，每台计算机都可以起客户端的作用，也可以起服务器的作用。例如，某个时刻，计算机A可能向计算机B发送关于某个文件的请求，作为响应，计算机B提供文件给计算机A。计算机A起客户端的作用，计算机B起服务器的作用。在此之后，计算机A和计算机B可以交换角色。B作为客户端，向连有共享打印机的A发出打印请求，而A作为服务器，响应来自B的请求。A和B相互之间是互惠或者对等关系。

在对等网络中，各个用户控制自己的资源。它们可以决定与其他用户共享某些文件，如图4-39和图4-40所示。在允许其他用户访问自己的资源之前，可能要求输入密码。因为由各个用户作出这些决定，所以网络中不存在控制或者管理中心。此外，各个用户必须对自己的系统进行备份，以便在出现故障时能从数据损失进行恢复。当计算机充当服务器时，会为其他系统的请求提供服务，服务器的用户可能会感受到机器性能下降。



图4-39 共享文件



图4-40 被共享的文件

相对而言，对等网络容易安装和运行。除了在每台计算机上安装适当的操作系统外，不需要额外的设备。多数现代的桌面操作系统都支持对等网络。由于用户负责控制自己的资源，因此不需要专职的管理员。当计算机数量少时，大概小于等于10台时，对等网络能良好地工作。由于扩展性不强，对等网络的效率随着网络中计算机数量的增加而快速下降。另外，各个用户控制对其计算机上资源的访问，也就意味着安全性可能难以保证。客户/服务器网络模型可以用于克服对等网络的这些局限性。

实验活动 建立一个对等网络

本实验中，你将在两台PC之间创建一个简单的对等网络。你需要选择适当的电缆并进行安装，配置工作站的IP地址，并用ping命令测试连接。你还需要在一台PC上共享一个文件夹，在另一台PC上对共享文件夹进行访问。

4.9.2 客户/服务器网络

在客户-服务器（client-server）方案下，网络服务位于专用的被称为服务器（server）的计算机上，服务器负责响应客户端的请求，如图4-41所示。服务器是一台中央计算机，能持续响应客户端

关于文件、打印、应用程序和其他服务的请求。大多数网络操作系统（NOS）都采用了客户-服务器模型。典型地，桌面计算机作为客户端，有额外处理能力、内存和专用软件的计算机作为服务器。

服务器设计用于处理多个客户端同时发起的请求，如图4-42所示。在客户端能访问服务器资源之前，需要对用户进行身份验证和使用资源的授权。处理授权的方式是为每个用户分配一个帐号和口令，以便充当网络接入哨兵的身份验证服务对其进行检验。通过对用户帐号、安全性和访问控制进行集中、基于服务器的网络简化了网络的管理任务。



图4-41　客户-服务器模式

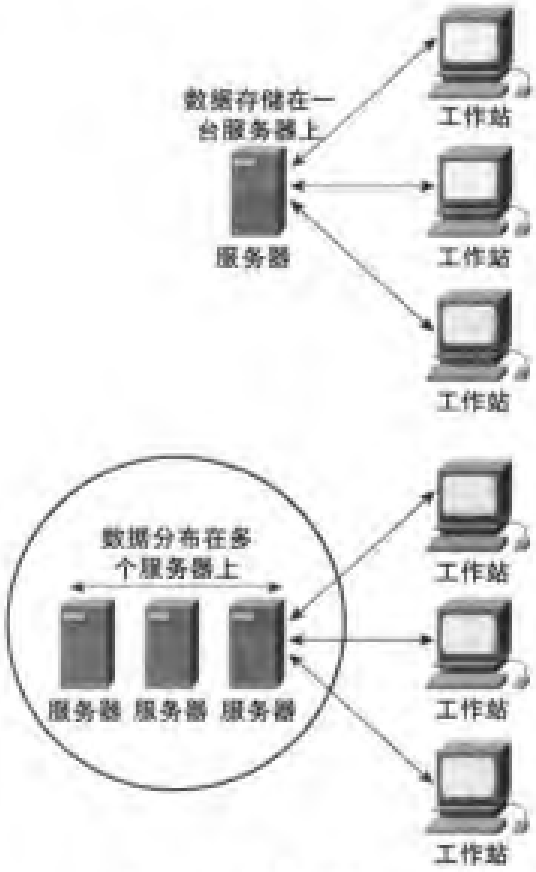


图4-42　服务器资源

将文件、打印机和应用程序等网络资源集中在服务器上，也使得更容易备份和维护所产生的数据。这些资源位于专用的、专职的服务器上，而不是分散在单个的计算机上，这使得访问更容易。大多数的客户-服务器系统还包括用于增强网络功能的各种工具，通过增加新的服务以扩展网络的用途。

客户-服务器网络中的分工带来了实实在在的好处，但也会带来某些成本。尽管将资源集中在服务器系统上带来了更高的安全性，使得访问更简单，并且能对控制进行协调，服务器也引入了网络中的单个故障点。一旦服务器不能运行，整个网络就根本无法工作。服务器的管理和维护需要由经过培训的内行完成。这样的要求增加了运行网络的开销。服务器系统还要求额外的硬件和专用的软件，这些都增加了成本。

表4-4和4-5总结了对等网络与客户-服务器网络各自的优点和缺点。

表4-4　对等网络与客户-服务器网络各自的优点

对等网络的优点	客户-服务器网络的优点
实现更便宜	安全性和可扩展性更高
无需NOS服务器软件	由于管理集中化，在大型网络中更便于管理
无需专门的网络管理者	所有的数据可以在一个中央位置进行备份

表4-5　对等网络与客户-服务器网络各自的缺点

对等网络的缺点	客户-服务器网络的缺点
不能很好地扩展到大型网络，会变得难以管理	需要NOS软件，比如Windows NT/2000/XP、Novell NetWare或UNIX
必须对每个用户进行培训以完成管理任务	服务器要求昂贵的、功能强大的硬件
安全性较低	要求专业的管理员
所有共享资源的机器性能会受到影响	如果只有一台服务器则存在单点故障，如果服务器失灵，所有的用户数据都不可用

实验活动　构建一个基于集线器的网络

本实验中，你将用一个以太网集线器在两台PC之间构建一个简单的网络。你需要选择适当的网线并安装，配置工作站的IP地址，并用ping命令测试连接。

实验活动　构建一个基于交换机的网络

本实验中，你将用一个以太网交换机在两台PC之间构建一个简单的网络。你需要选择适当的网线并安装，配置工作站的IP地址，并用ping命令测试连接。

4.10　广域网布线

要将一个网络与其他的远程网络进行连接，有时必须使用广域网（wide-area network，WAN）服务。广域网服务提供了不同于局域网的各种连接方法和布线标准。因此，需要理解连接这些服务所需的布线类型。

本节讲述了在局域网或广域网中用于互联交换机和路由器的线缆和接头。本节还讨论了如何连接路由器，以实现串行连接、综合业务数字网基本速率接口（ISDN BRI）连接、数字用户线（DSL）连接和有线电视连接，以及如何建立控制台连接。

4.10.1　广域网的物理层

很多物理实现都在广域间传送通信。根据设备距离服务的不同、速度的不同和实际服务的不同，需求也有很多差异。图4-43列出支持目前某些更突出的广域网解决方案的数据链路层和物理层实现。所选择的物理层类型需要根据距离、速度和所需要的接口类型确定。

Cisco的高级数据链路控制（HDLC）	PPP	帧中继	ISDN BRI（使用PPP）	DSL调制解调器	线缆调制解调器
EIA/TIA-232 EIA/TIA-449 X.21 V.24 V.35			RJ-45 注意：ISDN BRI 线缆的引脚与以太网引脚不同	RJ-11 注意：与电话线配合工作	F 注意：与有线电视线路配合工作

图4-43　广域网物理层的实现

串行连接用于支持类似运行点到点协议（PPP）或帧中继的专线这样的广域网服务。连接的速度范围从2400bit/s到T1（1.544Mbit/s）。

其他的广域网服务，比如ISDN，提供按需拨号连接或拨号备份服务。一个ISDN BRI有两个用于传送数据的64kbit/s的承载信道（B 信道），以及一个用于信令和其他链路管理任务的delta信道（D信道）。PPP通常用于在B信道上传送数据。

住宅宽带（高速）服务需求的不断增长增加了DSL和线缆调制解调器（cable modem）的流行程度。DSL服务能在现有的电话线上实现T1/E1速率。工作在现有同轴有线电视线路上的有线服务，也能提供与DSL相匹配或更高速率的连接。

4.10.2　广域网串行连接

串行传输是一种数据比特在单个信道上串行发送的数据传送方式。这种"每次一个（one-at-a-time）"的传输方式与每次传输多个比特的并行数据传输相对比。对于长距离通信，广域网使用串行传输。为了传送用比特表示的能量，串行信道使用特定的电磁或光频率范围。

频率用每秒的循环数（hertz）描述，用作通信的波段或频谱。例如，在语音级电话线上传送的信号使用最高达3kHz（千赫兹）。频率范围的大小称为*带宽（bandwidth）*。

表示带宽的另一种方法是指出串行信道每秒传送的数据比特数。

表4-6比较了EIA/TIA-232和EIA/TIA-449, v.35, X.21，EIA-530等多种用于广域网串行连接的物理层标准。

表4-6　物理层标准比较

数据（bit/s）	距离（m） EIA/TIA-232	距离（m） EIA/TIA-449,v.35,X.21，EIA-530
2400	60	1250
4800	30	625
9600	15	312
19,200	15	156
38,400	15	78
115,200	3.7	—
T1（1.544Mbit/s）	—	15

可用于连接串行广域网服务的物理连接类型有几种。必须选择正确的串行电缆类型，以配合路由器使用，这依赖于所选择的物理层实现方式，或服务提供商使用的实现方式。图4-44显示了可选的各种串行接头。串行接头用于连接终端用户设备和服务提供商。注意，Cisco路由器上的串行端口使用专用的60针接头，或者体积更小的"智能串行（smart serial）"接头，它能在一块广域网接口卡上支

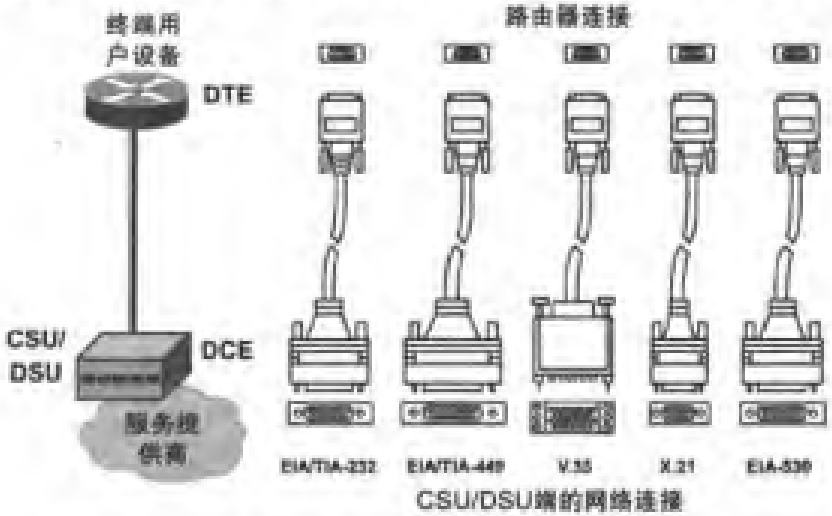


图4-44　广域网串行连接选项

持两个串行连接。线缆另一段的接头类型依赖于服务提供商或者终端设备的需求，但常用的是V.35。

4.10.3 路由器与串行连接

除了确定线缆类型，还需要确定自己的设备是否需要数据终端设备（DTE）或数据通信设备（DCE）接头。在广域网链路上，DTE是用户设备的终端点。DCE是用于将来自DTE的用户数据转换为提供广域网服务的设备所能接收的形式。

如图4-45所示，如果直接与服务提供商或完成信号定时（比如信道服务单元/数据服务单元[CSU/DSU]）的设备相连，路由器是DTE因此需要DTE串行线缆。这个例子是关于路由器的典型案例。

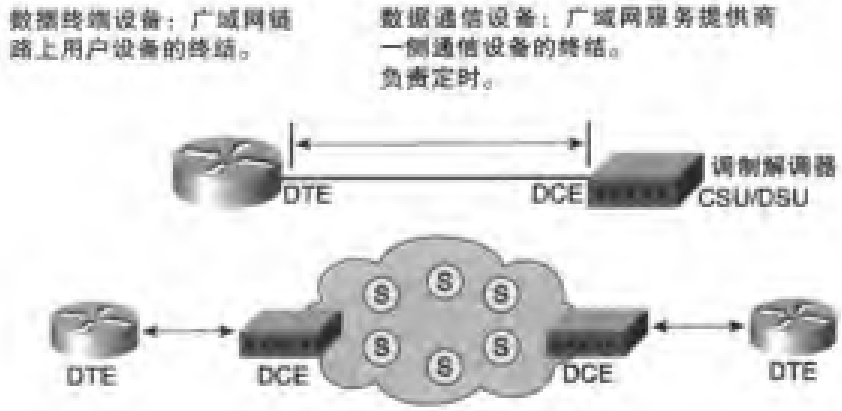


图4-45 DTE和DCE的串行连接

注释：定时（clocking）是在设备间实现数据传输同步的一种方法。在一个广域网串行连接中，CSU/DSU控制所传输数据的定时。

然而，某些情况下，路由器必须充当DCE，如图4-46所示。例如，如果在测试环境中进行背靠背（back-to-back）路由器连接（即在连接的两端都使用路由器），一台路由器是DTE，另一台是提供时钟的DCE。



图4-46 背靠背串行连接

如果对路由器进行串行连接，路由器必须有固定的或者模块化的端口。所使用的端口类型会影响你以后用于配置各个接口的语法。

图4-47显示了带有固定串行端口（接口）的路由器示例。每个端口都指定了一个关于端口类型和端口编号的标号——例如，串口0。为了配置一个固定端口，需要按照端口类型和端口编号惯例指定接口——例如，串口0。

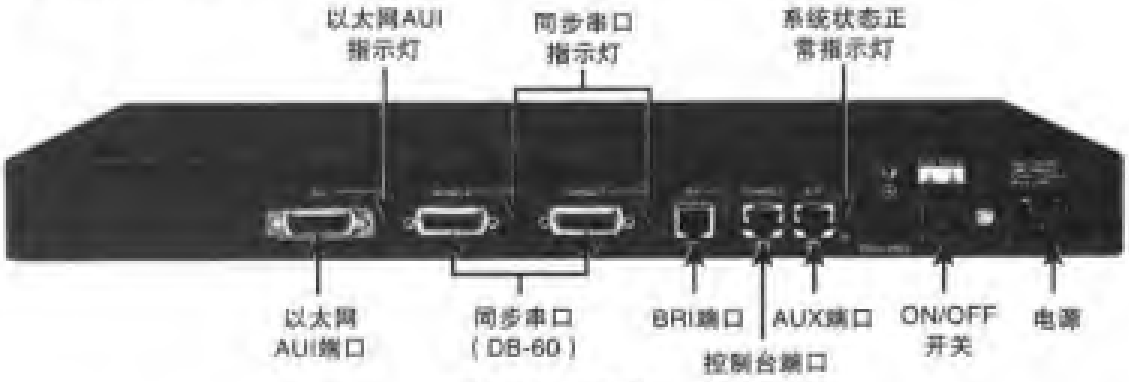


图4-47 固定接口

图4-48示例了带有模块化串行端口的路由器。通常，每个端口都分配一个标号，由端口类型、

插槽（模块的位置）和端口编号构成。为了配置模块卡上的端口，需要用“端口类型 插槽编号/端口编号”这样的惯例来指定接口——例如，串口1/0，其中接口类型为“串口”，串口模块所在的插槽编号是“插槽1”，你所指的串口模块上的特定端口是“端口0”。

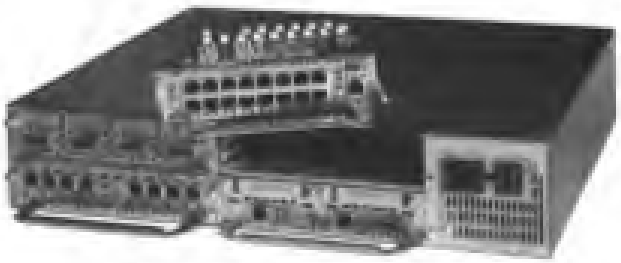


图4-48　模块化串行端口接口

实验活动　连接路由器的局域网接口

本实验中，你将识别路由器上的以太网或快速以太网接口。然后选择用于将路由器连接到集线器或交换机的适当线缆。最后，使用线缆将路由器连接到集线器或交换机。

实验活动　构建一个基本的被路由广域网

本实验中，你将连接两个简单的局域网，每个局域网都包含一台工作站和一台交换机（或集线器），从而形成一个基本的路由器——路由器广域网。

4.10.4　路由器与ISDN BRI 连接

使用ISDN BRI时，你可以选用两种类型的接口：BRI S/T和BRI U。在ISDN BRI服务中，用户（U）接口是用于从用户到网络终结器1（Network Termination 1，NT1）设备双绞线对连接的电气接口。终端（terminal，T）接口是NT1设备与NT2设备（通常是一台专用分支交换机（PBX））间的电气接口。系统（system，S）接口是NT1与ISDN设备（比如计算机或电话）之间的电气接口。在BRI中，T接口在电气上与S接口完全相同。因此，两个接口通常合并为一个接口，称为S/T接口。

要确定所需要的接口类型，必须确定是由你还是你的服务提供商提供NT1设备。NT1设备是位于路由器和服务提供商ISDN交换机（网云）之间的中间设备，用于将四线的用户线路连接到常规的两线本地环路。在北美，NT1通常由客户提供；在世界的其他地方，则由服务提供商提供NT1设备。

如果NT1设备需要由客户提供，则需要使用带U接口的ISDN BRI。U接口内置NT1。如果使用外置的NT1设备，或者服务提供商使用NT1设备，则路由器需要一个ISDN BRI S/T接口。因为路由器可以带有多种类型的ISDN接口，所以在购买路由器时必须确定所需要的接口。某些路由器同时带有U和S/T接口。路由器所带的ISDN接头类型可以通过查看端口的标签确定。图4-49显示了ISDN接口的各种不同的端口类型。

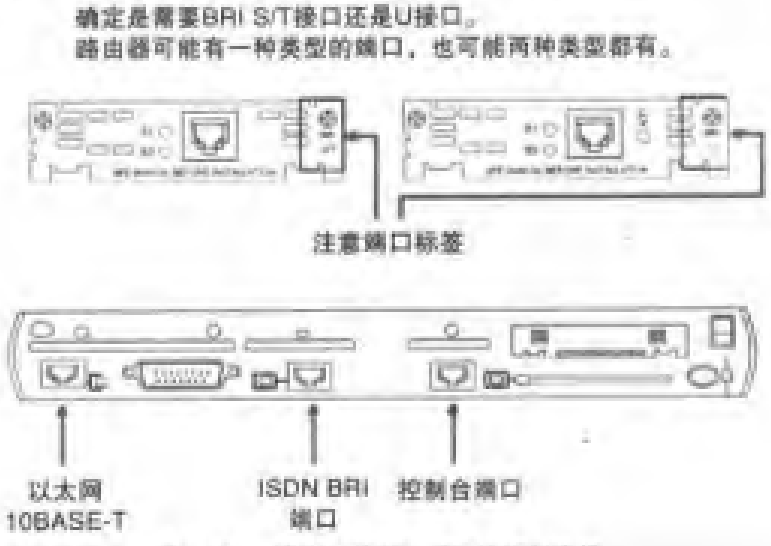


图4-49　路由器连线，实现ISDN连接

警告： 来自ISDN BRI端口的线缆只能插到ISDN插孔或ISDN交换机中。ISDN BRI使用的电压可能对非ISDN设备造成严重破坏。

要将路由器上的ISDN BRI端口互连到服务提供商的设备上，需要使用带有RJ-45接头的UTP CAT 5直通线缆。注意，ISDN BRI线缆的引脚与以太网不同。表4-7显示了ISDN BRI S/T接口的接头引脚。

表4-7 ISDN BRI S/T接口的接头引脚

引脚	信号
1	未用
2	未用
3	发送（Tx+）
4	接收（Rx+）
5	接收（Rx-）
6	发送（Tx-）
7	未用
8	未用

4.10.5 路由器与DSL连接

DSL技术是一种调制解调器技术，支持在双绞电话线上进行便宜的高速数字传输。当今，对绝大多数的小办公室或家庭办公室，DSL技术都是针对很多商业应用的良好选择，比如文件传输和对企业内部网的访问。异步数字用户线（Asymmetric digital subscriber line，ADSL）是最常见的，它是一个更大的，通称为xDSL的技术家族的一部分。

Cisco 800系列固定配置DSL路由器提供了更强的安全性、更低的购置成本、经过验证的可靠性，并通过为专门的小办公室和远距离工作者量身定制的CISCO IOS软件实现了投资保护。

Cisco 827-4V ADSL路由器有一个ADSL接口，如图4-50所示，该接口能通过DSL将用户连接到Internet或企业局域网。



图4-50 Cisco 827-4V路由器

要将一条ADSL线路连接到路由器上的ADSL端口，需要完成下列步骤：

步骤1 将电话线连接到路由器的ADSL端口上。

步骤2 将电话线连的另一端连接到墙上的外部电话插孔上。

要连接路由器实现DSL服务，需要使用带有RJ-11接头的电话线。DSL工作在标准的电话线上，它只使用RJ-11接头中的两个引脚，如表4-8所示。

注释： 如果你将非DSL设备上接到开通了DSL服务的电话线，则需要安装一个过滤器，以防止数据和语音业务间的相互干扰。

表4-8 电话接头的引脚（RJ-11）

引脚	信号
1	未用
2	未用
3	发送（Tx）
4	接收（Rx）
5	未用
6	未用

4.10.6　路由器与有线电视电缆的连接

线缆调制解调器支持在传送有线电视的同轴线路上实现双向、高速的数据传输。某些有线服务提供商允诺所提供的速度最高可达T1租用线的6.5倍。随着对宽带服务需求的增长，线缆调制解调器连接正变得越来越流行。

Cisco uBR905线缆接入路由器，在有线电视系统上为住宅、小型办公室和家庭办公室（SOHO）用户提供了高速的网络接入。Ubr905路由器带有一个用于连接有线电视系统的同轴电缆接口（F接头）。同轴电缆和F接头用于连接路由器和有线电视系统。同轴电缆可以是无线级（radio grade）59（RG-59）或RG-6，推荐使用RG-6。

注释：RF同轴电缆用于将无线电频率连接到天线。大多数的有线电视系统使用同轴电缆作为自己的布线系统。从有线电视提供商到邻近用户的分线盒的主要中继线路可能使用光纤，但分线盒与用户之间很可能使用的是同轴电缆。

将Cisco uBR905有线电缆接入路由器连接到有线系统中，需要执行下列步骤：

步骤1　确定路由器未连接电源。

步骤2　定位从同轴电缆CATV墙插孔上引出的RF同轴电缆。

步骤3　如果需要，安装一个分线器/定向耦合器（cable splitter/directional coupler），以分离供电视和计算机使用的信号。如果需要，也可以安装一个“高通滤波器（high-pass filter）”来阻止电视和计算机信号间的干扰。

步骤4　将同轴电缆连接到路由器的F接头，如图4-51所示。用手将接头插紧，确保已经达到手所能插到得很紧的程度，然后用扳手拧1/6圈。

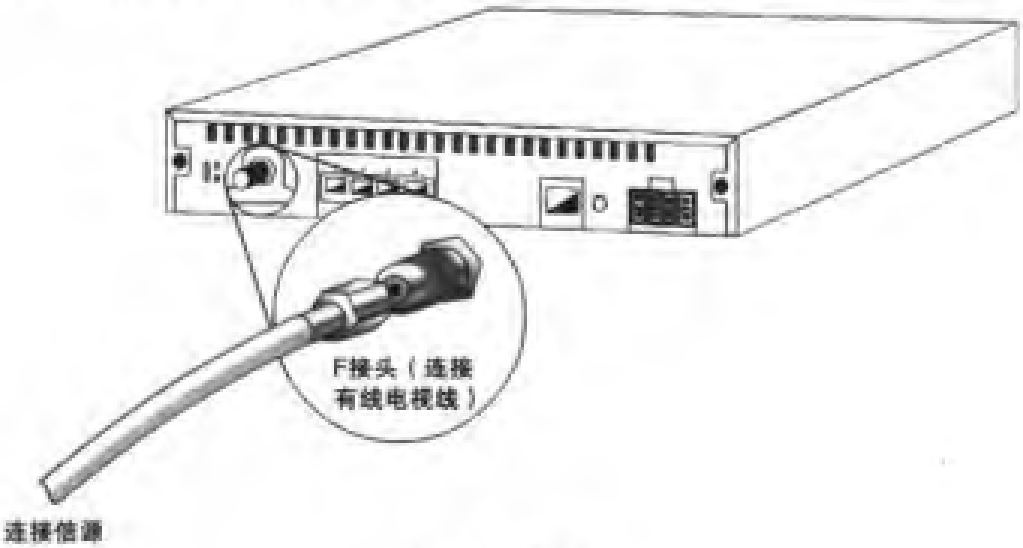


图4-51　F接头

警告：不要将接头插得过紧，否则会损坏接头。不推荐使用扳手，因为在已经用手插紧后，这样可能存在将接头拧过推荐的1/6圈的危险。

步骤5　确保从分配接头（distribution tap）到Cisco uBR905路由器的所有同轴电缆接头——所有中间的分线器、耦合器或接替模块——都被安全地拧紧。

4.10.7　建立控制台连接

为了完成对Cisco设备的初始配置，需要提供一个直接到设备的管理连接。对于Cisco设备，这

个管理附件称为*控制台端口*（*console port*）。控制台端口使得你能监视并配置Cisco的集线器、交换机或路由器。

用在终端和控制台端口间的线缆是带有RJ-45接头的*反转线缆*（*rollover cable*），如图4-52所示。

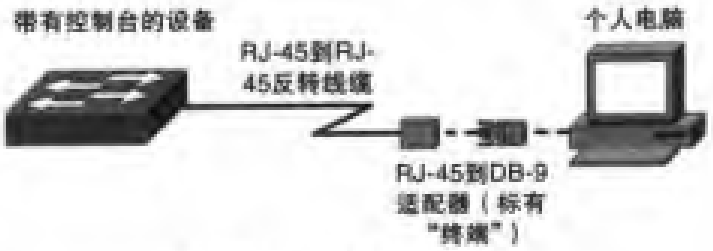


图4-52 建立控制台连接

反转线缆（也称为控制台线缆）的引脚图与以太网或ISDN BRI所使用的直通或交叉RJ-45线缆不同。反转线缆的引脚图如下：

1至8
2至7
3至6
4至5
5至4
6至3
7至2
8至1

为了在终端和Cisco控制台端口间建立连接，必须执行下列步骤：

步骤1 用反转线缆连接设备。你可能需要为你的PC或终端使用一个RJ-45到DB-9或RJ-45到DB-25适配器。

步骤2 用下列的通用设备（COM）端口设置配置终端模拟程序：

- 9600 bit/s。
- 8数据位。
- 无奇偶位。
- 1停止位。
- 无流量控制。

注释：路由器上的辅助（AUX）端口用于提供通过调制解调器的远程管理。在可以使用之前，必须用控制台端口对AUX端口进行配置。AUX端口也使用9600bit/s、8数据位、无奇偶位、1停止位并且无流量控制的设置。速度可达38,400bit/s。



实验活动 建立一个到路由器或交换机的控制台连接

本实验中，你将连接一台PC到路由器或交换机，以建立一个控制台会话并观察用户接口。



实验活动 对互联设备进行故障排除

本实验中，你将用两台PC、两台交换机（或集线器）和两台路由器建立一个简单被路由的广域网。你需要配置工作站的IP地址。然后正确地找出与线缆和工作站IP地址相关的网络问题。

4.11 总结

本章学习了以下知识点：

- 波（Wave）是从一个位置传播到另一个位置的一种能量，是由扰动产生的。所有的波都有类似的属性，如振幅、周期和频率。
- 正弦波是周期性的、连续变化的函数。模拟信号类似正弦波。
- 方波是周期性的函数，其值保持恒定一段时间，然后突然改变。数字信号类似方波。

• 指数用于表示非常大的数字。将底数增大到一个特定的指数等于将底数自己与自己相乘指数次（例如，10^3=10*10*10=1000）。

• 对数与指数类似。某个数以10为底的对数等于使10到达该数值的指数。（例如，$\log_{10}1000=3$，因为$10^3=1000$）。

• 分贝用于度量信号能量的增加或损失。负值表示损失，正值表示增加。

• 时域分析是用示波器作出电压或电流关于时间的图像。频域分析是用频谱分析仪做出电压或能量关于频率的图像。

• 噪声是通信中不需要的信号。噪声源自其他的线缆、RFI和EMI。白噪声影响所有的频率，窄带干扰只影响某些频率。

• 模拟带宽是与特定模拟传输相关联的频率范围，比如电视或FM光波。

• 数字带宽用于度量在给定时间内能从一处传递到另一处的信息量。其单位是每秒传送的比特数。

• 为了理解后面要介绍的线缆测试的概念，对前面的这些主题有基本的理解是很重要的。

• 局域网中，大多数的问题都发生在OSI的物理层。对这些大多数的问题，要预防或者进行故障排除。惟一的方法是通过使用线缆测试仪。为了正确地安装线缆和接头，关于局域网介质上噪声源的概念是很重要的。

• 网卡为PC提供了发送和接收网络通信的能力。

• 以太网、令牌环和FDDI是三种常见的局域网协议。

• 术语*以太网*通常用于代表普遍符合以太网规范的所有CSMA/CD局域网。

• 局域网实现中的以太网家族包括四个主要分类：以太网和IEEE 802.3、快速以太网、吉比特以太网和10G或10000-Mbit/s以太网。

• 使用交叉线缆来连接两台类似的设备（比如交换机到交换机、路由器到路由器、PC到PC，以及集线器到集线器）。

• 用直通线缆连接两台不同类的设备（比如交换机到路由器、交换机到PC、集线器到路由器，以及集线器到PC）。

• 存在两种主要类型的局域网：对等网络和客户-服务器网络。

• 路由器通常是DET，因此需要使用DTE串行线缆来连接类似CSU/DSU这样的DCE设备。

• ISDN BRI有两种类型的接口：S/T和U。要连接ISDN BRI端口到服务提供商的设备，需要使用UTP CAT 5直通线缆。

• 对于DSL服务，电话线和RJ-11接头用于连接路由器。

• 对于有线电视服务，同轴电缆和F接头用于连接路由器。

• 反转线缆用于连接终端和路由器的控制台端口。

作为对本章中你所学内容的补充，请参考本书所附CD中针对本章的视频、插图和e-Lab实验。

4.12 关键术语

有源集线器（*active hub*） 必须插到电插座中，因为它需要能量将进入的信号放大，然后从其他的端口发送出去。

外部串扰（*alien crosstalk*） 由线缆外的信号引起的串扰。

振幅（*amplitude*） 电信号的振幅表示其高度，但是以电压为单位而不是米。

模拟带宽（*analog bandwidth*） 通常指的是一个模拟电子系统的频率范围。模拟带宽可以用于描述一个无线电台或电子放大器所发送的频率范围。

衰减（*attenuation*） 信号振幅随链路长度的减小。

附属单元接口（*attachment unit interface, AUI*） 计算机网卡或路由器接口与以太网线缆间的15针的接头。

交叉线缆（*crossover cable*） 交叉关键线对，以在设备和线路连接之间适当地排列、发送和接收信号的线缆。

串扰（*crosstalk*） 是指信号从一个线对传送到邻近的线对。当一个线对上的电压发生变化时，便会产生电磁场能量。这种能量会像发送方发出广播信号一样从发送线对向外放射。

分贝（*decibel*） 描述网络信号的一种重要方式，描述波能量损失或增加的一个单位。分贝通常是负数，表示波传播过程中能量的损失，但如果信号被放大，则为正数，表示能量的增加。

延迟偏差（*delay skew*） 由于各个线对在绞数和电气特性上的差别，同一条线缆内不同线对的传输延迟可能略有差异。线对间的延迟差异被称为时延偏差。

数字带宽（*digital bandwidth*） 度量在给定时间内能从一处传递到另一处的信息量。

等效远端串扰（*equal-level far-end crosstalk, ELFEXT*） 测量FEXT的一种测试。

电磁干扰（*electromagnetic interference, EMI*） 来自邻近信源（比如马达和灯）的噪声。

远端串扰（*far-end crosstalk, FEXT*） 当一个双绞线对上的信号到达一个多线对线缆系统的远端，被耦合到另一个线对时发生的串扰。

频率（*frequency*） 每秒完整的波数。

吉比特接口转换器（*Gigabit Interface Converter, GBIC*） 插入到吉比特以太网端口中的一种热插拔的输入/输出设备。

赫兹（*hertz*） 频率的单位，频率是每秒完整的循环数（波数）。

IEEE 802.1X/可扩展身份验证协议（*IEEE 802.1X/Extensible Authentication Protocol, EAP*）可替代IEEE 802.11所规定的WEP的一种安全方案，IEEE 802.1/EAP主要着眼于提出一个用于进行集中式认证和动态密钥分配的框架。

阻抗（*impedance*） 衡量电缆对交流电（AC）阻力的度量，单位是欧姆（Ω）。

插入损耗（*insertion loss*） 在通信链路上，信号衰减和阻抗不连续的综合效果。

智能集线器（*intelligent hub*） 有时也被称为“聪明集线器（smart hubs）”。这些设备的工作方式基本上与有源集线器类似，但还包括一个微处理器芯片并具备诊断能力。相比有源集线器，智能集线器更贵，但在故障排除时也更有用。

对数（*logarithms*） 等于给定的一个数字被增大到一个特定值时所用的指数值。

窄带干扰（*narrowband interference*） 只影响小频率范围的噪声。

近端串扰（*near-end crosstalk，NEXT*） 根据从链路的相同端测量到的测试信号和串扰信号间电压振幅的比率计算得出的。

噪声（*noise*） 在通信中，噪声是指不需要的信号。噪声可能是由自然或技术原因产生的，并附加到通信系统的数据信号中。

示波器（*oscilloscope*） 一种重要的电子设备，用于观察电信号，比如电压波和脉冲。

对等网络（*peer-to-peer network*） 联网的计算机相互之间像平等的伙伴，或对等体一样。作为对等体，每个计算机都可以起客户端或服务器的作用。

传输延迟（*propagation delay*） 信号通过所测试电缆所用时间的简单度量。

综合等效远端串扰（*power sum equal-level far-end crosstalk，PSELFEXT*） 来自所有线对的ELFEXT的综合效果。

综合近端串扰（*power sum near-end crosstalk，PSNEXT*） 综合来自线缆中所有线对的NEXT的累积效果。

脉冲（*pulse*） 确定被传送的数据值。如果扰动是故意产生的，并且持续的时间固定且可预测，那么这样的扰动就是脉冲。

中继器（*repeater*） 在比特级对网络信号进行再生和重新定时，使之能在介质上传输更长距离的设备。

无线频率干扰（*radio frequency interference，RFI*） 来自邻近传送信号的噪声。

RJ-45一种通常用于终结双绞线电缆的接头。

正弦波（*sine waves*） 许多随时间作规律性变化的自然现象所对应数学函数的图示，例如地球到太阳的距离，乘坐大观缆车时距离地面的距离，以及一天中太阳升起的时间。由于正弦波是连续变化的，因此属于模拟波。

频谱分析仪（*spectrum analyzer*） 能产生频域分析所用图像的设备。工程师们也使用频域分析来研究信号。

方波（*square waves*） 图像不随时间连续变化，它的波值在一定时间内保持不变，然后突然变化，再保持不变，最后又突然恢复到初始值。

直通线缆（*straight-through cable*） 在整个线缆中保持各个针脚连接不变的线缆。因此，线缆两端连接到引脚1的导线是相同的。

交换机（*switch*） 有时也被称为多口网桥。典型的网桥可能只有两个端口（连接两个网段），交换机可能有多个端口，这取决于所需要连接的网段数量。

TIA/EIA-568-B标准（*TIA/EIA-568-B standard*） 规定了铜缆要用于调制解调器或高速以太局域网所必须通过的十项测试的标准。

波（*wave*） 从一处传播到另一处的能量。

有线等效保密（*wired equivalent privacy，WEP*） 是802.11标准中定义的一种安全机制，设计用于保护无线局域网接收点和网卡间通过空气的传输。

白噪声（*white noise*） 等效影响所有传送频率的噪声。

4.13 复习题

通过完成所有的复习题可以测试你对本章所涉及的主题和概念的理解程度。答案列在附录C“复习题答案”中

1. 下列哪一项属于802.3u的规范?
   A. 10BASE-F
   B. 10BASE-T
   C. 100BASE-TX
   D. 1000BASE-CX
2. 下列哪一项是关于以太网连接的最恰当描述?
   A. 在服务器和局域网之间使用10Mbit/s以太网作为连接。
   B. 在用户级使用吉比特以太网作为链路以提供高性能。
   C. 在用户级与网络设备间使用快速以太网作为链路，以支持接入链路上来自各个以太网段的聚集通信。
   D. 以上都不是
3. 下列哪个标准组织制定了用于支持以太网实现的线缆和接头规定?
   A. ISO
   B. ANWI
   C. TIA/EIA
   D. IETF
4. 下列关于介质接头的描述，哪项不正确?
   A. RJ-45连接接头是一个主要用于终结同轴电缆的8针接头。
   B. AUI是用在网卡和以太网电缆间的15针接头。
   C. GBIC是将串行信号电流转换为光信号，或实现反向转换的发送接收器。
   D. 以上都不是
5. 以下哪一项不需要配备交叉线缆?
   A. 交换机间的级联链路
   B. 连接路由器和交换机
   C. 连接集线器和交换机
   D. 以上都不是
6. 哪项技术不属于无线通信?
   A. 蜂窝
   B. 宽带
   C. 红外线
   D. 扩频
7. 下列哪项不是有线对等保密（WEP）的特征?
   A. WEP使用RC4算法加密。
   B. WEP是在802.3标准中定义的安全机制。
   C. WEP的一个目标是拒绝没有适当WEP密钥的非授权用户访问网络。
   D. 以上都不是
8. 以下哪项不属于广域网实现?
   A. DSL
   B. ISDN

C. 帧中继
D. 以太网

9. 广域网使用哪种类型的数据传输方法?
A. 并行
B. 串行
C. 单个
D. 以上都不是

10. 哪一项对DCE的描述最恰当?
A. 网络末端的用户设备
B. 作为数据源或目的的设备
C. 类似协议转换器或多路复用器的物理设备
D. 组成用户-网络接口中网络端的设备

11. 下列哪种介质用于连接ISDN BRI端口到服务提供商的设备?
A. CAT 5 UTP直通线缆
B. CAT5 UTP交叉线缆
C. 同轴
D. 光纤

12. 哪种接头用于DSL连接?
A. RJ-45
B. RJ-11
C. F
D. DB-9

13. 哪种接头用来连接路由器和有线电视系统?
A. RJ-45
B. RJ-11
C. F
D. AUI

14. 哪种线缆用来连接终端和控制台端口?
A. 直通
B. 反转
C. 交叉
D. 同轴



第5章　以太网基础

目标

学习完本章之后，你应该能够：

- 简述以太网的历史。
- 识别IEEE标准。
- 理解MAC寻址。
- 识别数据链路层中帧的常见字段。
- 描述介质访问控制（MAC）。
- 描述载波侦听多址/冲突检测（CSMA/CD）。
- 理解以太网的工作原理。
- 识别不同类型的冲突。
- 解释冲突、冲突域和广播域。
- 识别产生冲突域和广播域的第1、2、3层设备。
- 讨论数据流和广播问题。
- 理解冲突和冲突域。
- 理解广播和广播域。
- 理解网络分段和用于建立分段的设备。

*以太网（Ethernet）*是使用最广泛的局域网（LAN）技术，它有很多形式。以太网的设计填补了远距离、低速网络和专用的、短距离高速数据传输网络之间的空缺。

以太网特别适合在本地通信介质上高速传送零星、不定时大流量数据的应用场合。以太网是为了在本地工作组级网络中资源共享而设计的。以太网的设计目标包括简洁性、低成本、兼容性、公平性、低延时以及高速度。

本章将学习以太网历史和IEEE以太网标准。我们将讨论以太网的工作原理、帧结构、错误处理以及以太网中不同类型的冲突。另外，本章将介绍冲突域和广播域的概念。最后本章会对网络分段（segmentation）和用于建立分段的设备予以描述。

请务必在本书配套的光盘中查看与本章相关的e-Lab实验活动、视频和插图。这些光盘资料提供了补充材料，能够强化本章中涉及的概念。

5.1　以太网发展历史

局域网是高速、低错误的数据网络，它覆盖相对小的地理范围（几千米以内）。在独立的建筑物中或者地理范围有限的区域内，局域网可以连接工作站、外设、终端和其他设备。

以太网在当今的局域网技术中占据统治地位。Internet中的大部分流量都是通过以太网的连接而开始和结束的。从上个世纪70年代开始，以太网不断发展以满足日益增长的高速局域网需求。当新的介质——光纤制造出来后，以太网就予以采纳，充分利用了光纤的巨大带宽和低错误率。使用相同的基本协议，1973年以3兆比特每秒（Mbit/s）速率传输数据，现在却可以以10吉比特每秒（Gbit/s）速率传输数据。

以太网的成功在于它的简洁性和易于维护、它结合新技术的能力、它的可靠性以及低的安装和升级成本。随着吉比特以太网的推出，以局域网技术起家的以太网在传输距离方面已经得到了充分的延伸，使得以太网成为城域网甚至广域网的标准。本节对以太网技术进行了回顾，包括以太网的历史、以太网命名规则以及以太网帧格式。

5.1.1　以太网介绍

以太网的最初概念源自这样一个问题：允许两个或多个用户使用同一个传输介质而又互不干扰。早在上个世纪70年代初，夏威夷大学就开始研究多个用户共享传输介质的问题。由此开发出一个叫作Alohanet的系统，该系统可以让夏威夷群岛上的各种工作站彼此之间通过共享无线电频段实现有组织的互访。以太网最初是基于无线电技术的。这部分工作成为日后著名的以太网MAC方法的基础，也就是***载波侦听多址访问/冲突检测（CSMA/CD）***。本章后面将详细讨论CSMA/CD。

以太网最初的版本是世界上最早的局域网。它是30多年前由Robert Metcalfe和他的同事在施乐（Xerox）公司设计的。1980年，由数字设备公司（DEC）、Intel和施乐（Xerox）组成的联盟（DIX）发布了以太网最早的标准。Metcalfe希望以太网成为大众受益的共享标准。因此，DIX让新的标准成为了开放标准，也就意味着以太网对任何公司来说都是开放的。这对计算机工业来说是件不同寻常的事情。上个世纪80年代早期，采用以太网标准开发的首批产品开始销售。这些产品在2公里长的粗同轴电缆（大约是最小手指的直径粗细）上能以10Mbit/s速率传输数据。以太网立即获得成功。

电气与电子工程师协会（IEEE）是一个定义网络标准的专业组织。1985年，IEEE负责局域网和城域网的标准委员会发布了自己的局域网标准。IEEE局域网标准是当今世界上最有影响、广为流传的局域网标准。这些标准是以数字802开头的。基于以太网的标准是802.3。IEEE力图确保它的标准兼容并能适合国际标准化组织（ISO）的OSI参考模型。IEEE将OSI数据链路层分成两个独立的子层：介质访问控制（MAC）和逻辑链路控制（LLC）。

最终，802.3标准对最初的以太网标准作了一些小的修正。DIX的以太网标准与802.3规范之间存在一些差异。然而，这些差异很细微，以至于任何以太网接口卡（NIC）都可以传输、接收以太网和802.3的分组和帧。从本质上讲，以太网和IEEE的802.3是相同的标准。需要记住的一点是，目前802.3是IEEE正式的以太网标准。

在上个世纪80年代中期，以太网的10 Mbit/s传输速率对于那个年代的PC机来说是足够的。到上个世纪90年代早期，PC机速度越来越快，人们开始抱怨由于以太网带宽不足带来的瓶颈。1995年，IEEE宣布了100 Mbit/s以太网标准，随后就是1998和1999年期间推出的吉比特（十亿比特每秒）以太网标准。2002年6月，IEEE通过了10 Gbit/s以太网标准。这些最新的标准还是以太网（802.3）。

所有新的以太网标准从本质上与最初的以太网标准兼容。以太网分组（帧）可以从PC机中老的10 Mbit/s NIC上发送出来，然后被路由器传送到10Gbit/s的以太网光纤链路上，然后传送到一个100 Mbit/s以太网卡为止。只要分组停留在以太网中，它就不会被改变。这展示出以太网获得巨大成功

的一个主要原因——非凡的伸缩性。也就意味着网络带宽可以不断地增长，而无需底层以太网技术的改变。

最初的以太网（IEEE 802.3）已经增补了很多次，以结合新的传输介质和允许更高的传输速率。然而，更重要的是以太网的本质被保留了下来。以太网802.3众多标准属于同一家族。标准之间虽然存在差异，但是相似性大于差异性。在每一个新标准中都保留了最初的标准，也就意味着802.3家族中的所有协议是兼容的。

5.1.2 IEEE以太网命名规则

“以太网”这个术语实际上指的是一组网络技术，包括最初的以太网、***快速以太网***、***吉比特以太网***（Gig-E）和***10Gbit/s以太网***（10-G）。这些不同类型的以太网会在第6章的“以太网技术和以太网交换”中予以详细讨论。

以太网接口的价格在10美元到100,000美元之间。以太网的速度可以是10、100、1000或者是10,000 Mbit/s。本节将从更加细节的角度探讨最初的以太网（10BASE-T）、快速以太网（100BASE-T和100BASE-FX）、吉比特以太网（1000BASE-T和1000BASE-X）以及10 Gbit/s以太网。所有形式的以太网都保留着两个特性：基本帧格式和OSI第2层中的IEEE子层。

一旦以太网需要对新的介质或传输能力扩展时，IEEE会对802.3标准发布新的增补。新的增补通过一个或两个字母来标示——例如，802.3u表示快速以太网。同时，也会给新的增补分配一个缩写描述（标识符）。下面是一些增补的例子：

- 10BASE2（IEEE 802.3a）。
- 10BASE5（IEEE 802.3）。
- 10BASE-T（IEEE 802.3i）。
- 10BASE-TX（IEEE 802.3X）。

如上所示，缩写描述由若干部分组成：

- 表示兆比特每秒传输的数字。
- BASE一词表示基带信号。
- 数字2和5表示同轴电缆分段长度（185米取整为200，用2代表）。
- 一个或多个字母表示所用介质类型（F表示光缆，T表示铜制非屏蔽双绞线）。

基带信号传输是最简单的信号传输方法。在基带信号传输中，整个传输介质的带宽都被信号占用。数据信号（UTP上的电压或者光纤上的闪光）直接在传输介质上传输，不需要其他特殊的信号（载波信号）。以太网使用基带信号传输。

另一种信号传输方法是宽带信号传输，以太网并没采用。在宽带信号传输中，数据信号并非直接在传输介质上传输。相反，载波信号（模拟信号）要经过数据信号的调制才能传输。无线广播和有线电视都使用宽带信号传输。

与国际标准化组织（ISO）一样，IEEE是一个标准制订组织。网络设备制造商不需要完全遵守标准中的所有规范。IEEE的目标如下：

- 提供制造符合以太网标准的设备所需的工程信息。
- 不压制制造商的创新。

对于建立或维护一个小的局域网来说，如果从同一个信誉良好的制造商那里购买所有的设备，那么可以保证这些设备是兼容的。可是对于一个由许多小以太网组成的大局域网来说，网络设备可能来自多个供货商，这时面临的情况就有所不同了。来自不同供货商的网络设备，它们之间的可靠互操作能力是一个非常重要的问题。不幸的是，没有这样一个工业或政府机构能够测试并证明一个网络设备是完全符合IEEE标准的。然而，这可以让你明白标准和工业是两回事。事实上，你需要做

的就是根据自己的了解和同事的意见来做出网络设计和采购方面的决策。

5.1.3　IEEE 802.3/以太网和OSI模型

局域网标准定义了物理介质和连接器，连接器把设备连接到OSI参考模型中物理层的介质上。局域网标准同时定义了设备在数据链路层中通信的方式。此外，局域网标准定义了特定协议流量的封装方式，也就是说传递给不同高层协议的流量可以使用相同的通道，该通道历经OSI模型的各个层次。为了提供这些功能，IEEE以太网数据链路层分成两个子层：

- *介质访问控制（MAC）（802.3）*——顾名思义，MAC子层定义了如何在物理线路上传输帧。它处理每一个相关设备的物理寻址、网络拓扑定义以及线路规程。
- *逻辑链路控制（LLC）（802.2）*——顾名思义，LLC子层负责从逻辑上识别不同的协议类型，然后加以封装。类型编码或者是服务访问点（SAP）标识符实现逻辑识别。一个端工作站使用的LLC帧类型取决于高层协议（例如IP）期望的标识符。尽管*IEEE 802.2*代表了数据帧*封装*的标准类型，但还有其他类型，例如Ethernet II（主要用于基于TCP/IP的以太局域网），后面会进行讨论。

如图5-1所示，*IEEE 802.3*标准定义了物理层（第1层）和数据链路层（第2层）中的MAC部分。

图5-2把各种技术映射到OSI第1层和第2层的下半部。在本书中，我们主要针对的是以太局域网技术。第1层（即物理层）涉及介质、信号、比特流、发送信号部件的接口，以及各种拓扑结构。物理层在计算机之间的通信中扮演关键角色，但是光有物理层是不够的。物理层的每一个功能都有自己的限制。第2层克服了这些限制。



图5-1　802.3以太网和OSI模型



图5-2　局域网规范和OSI模型

对于第1层中的每一个限制，第2层都有一个解决办法，如表5-1所示。

表5-1　第1层限制同第2层解决办法的对照

第1层限制	第2层解决办法
第1层不能和高层通信	第2层通过LLC子层与高层通信
第1层不能标识计算机	第2层使用MAC寻址方案标识计算机
第1层只能描述比特流	第2层使用帧来对比特进行组织或分组（这个过程最终提供了一种让比特具有含义的方法）
当一组计算机同时开始传输时，第1层无法确定到底哪一个计算机要传输二进制数据	第2层使用MAC子层来实现这一点

第2层子层LLC和MAC是活跃的、至关重要的协议，它们使得技术的兼容和计算机的通信成为可能。MAC子层关系到用于传递信息的物理部件。同其他层类似，LLC同通信过程中的物理部件保持着相对的独立性。LLC允许多种第3层协议，例如IP和IPX，能够与多种帧类型得到同步支持。

图5-3将各种以太网技术映射到OSI第2层的下半部和整个第1层。尽管还有各种其他类型的以太网，这里所描述的则是使用最普遍的以太网，也是本课程的中心。



图5-3 以太网技术和OSI模型

5.1.4 MAC寻址

为了在以太网上局部传输帧，必须有一个寻址系统，也就是对计算机和网络接口命名的方法。每一个计算机本身有一个唯一的标识办法。网络上的每一个计算机有一个物理地址。在网络上不允许出现两个相同的物理地址。这个地址叫做*介质访问控制（MAC）地址*，它存在于网络接口卡中。MAC地址的其他术语还包括：硬件地址、NIC地址、第2层地址和以太网地址。

以太网使用MAC地址惟一地标识单独的设备。带有以太网接口的任一设备（PC机、路由器、交换机）都必须有一个MAC地址，否则，其他设备就不能与之进行通信。一个MAC地址长48比特，表示成12个十六进制数字。前6个十六进制数字是由IEEE管理的，用于识别制造商、供货商，构成*组织惟一标识符（OUI）*。剩下的6个十六进制数字由接口序列号或者是特定供货商管理的编号组成。MAC地址有时候也叫做预烧录（burned-in）地址（BIA），因为它是被事先烧录到只读存储器（ROM）中，当NIC启动时，才被拷贝到随机存储器（RAM）中。图5-4展示了MAC地址的格式。



图5-4 MAC地址格式

没有MAC地址，局域网只是一组没有标识符的计算机，而且不可能传输以太网帧。因此，在数据链路层中，需要给高层数据添加*帧头*和*帧尾*。帧头和帧尾包含了控制信息，以便提供给目的系统中的数据链路层通信实体。来自高层实体的数据被封装到数据链路层的帧头和帧尾中。

以太网和802.3局域网都是广播网络。所有的工作站都可以看到所有的帧。每个工作站必须检查每一个帧，以确定是否自己就是目的地。

在以太网络中，如果一个设备希望给另一个设备发送数据，它可以通过使用自己的MAC地址来打开一个通向该设备的路线。当源设备向网络发出数据时，该数据中也承载着目的MAC地址。一旦数据沿着网络介质传播开来，网络上每个设备中的NIC都会检查数据帧中包含的物理地址是否与自己的MAC地址相匹配。如果不匹配，NIC丢弃此数据帧。

如果匹配，NIC验证在帧头中的目的地址以确定这个分组的寻址是否是正确的。当数据到达目的工作站时，该站的NIC对其进行一次拷贝，并把数据从信封中取出送给计算机，由IP和TCP这样高层协议来进行处理。

5.1.5 成帧的基本内容

在物理介质上对比特流进行编码意味着技术上的巨大成就，但仅此一项并不足以实现通信。将数据封装成帧有助于获得一些基本信息，而这是对比特流编码所不能获得的。这些信息如下：

- 哪些计算机在和其他计算机通信。
- 计算机个体之间何时开始通信、何时结束通信。
- 对通信中出现的错误进行识别。
- 在计算机的“会话”中，下一个该轮到谁“讲话”。
- 数据在帧中的位置。

在有了标识计算机的方法后，可以开始封装数据帧。成帧是第2层的封装过程。帧是第2层的协议数据单元。图5-5展示了比特和帧的概念。

当你形象化地展示比特时，使用最准确的图表是电压时间对照图。但是，因为经常要处理更大的数据单位、寻址以及控制信息，这种类型的图会变得出奇的庞大，很容易令人糊涂。可以使用的另一种图表是帧格式图表，它也是以电压时间对照图为基础的。这种图是按照从左到右的顺序查看，就像示波器图一样。帧格式图显示出不同的比特组（字段）；不同的字段具有不同的功能。

许多不同类型的帧通过各种标准进行表述。一个帧中通常有一些叫做字段的部分，每个字段由字节组成（如图5-6所示）。经常在数据链路层帧中碰到的字段名字包括：

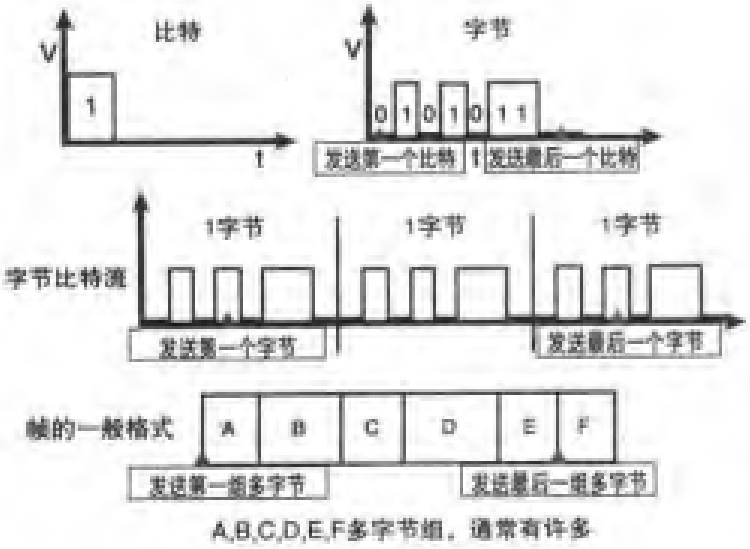


图5-5　从比特到帧

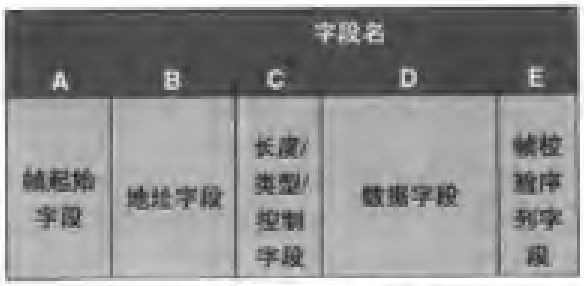


图5-6　帧的一般格式

- 帧起始字段。
- 地址字段。
- 长度/类型/控制字段。
- 数据字段。
- 帧校验序列（FCS）字段。

下面将对帧中不同字段予以详细描述。

帧起始字段

当计算机连接到物理介质时，必须有一种方法发出一条消息，就像是“帧来了！”，以引起其他计算机的注意。各种技术都有不同的方法处理这个过程，但是，如果不考虑技术的话，所有的帧都有一个以字节序列表示的起始信号。

地址字段

所有的帧都包含标识信息，比如源计算机的地址（MAC地址）和目的计算机的地址（MAC地址）。

长度和类型字段

大多数帧都有一些特殊字段。在有些技术里，长度字段指明了帧的确切长度。有时还会有一个类型字段，指定产生发送请求的第3层协议。当然也有一些技术无需使用这些字段。

数据字段

发送帧的原因是要获取高层数据，最终是为了把用户的应用数据从源计算机发送到目的计算机。需要传输的数据分组包括你希望发送的消息（数据）。有时通过填充字节来保证帧的最小长度。在IEEE标准帧中，逻辑链路控制（LLC）字节也包含在数据字段中。值得注意的是，LLC子层在网络协议数据（第3层分组）中增加了控制信息，目的是帮助分组能够被送达目的地。第2层通过LLC与高层协议通信。

帧校验序列字段

所有的帧（包括其中的比特、字节以及帧里面的字段）都会由于各种原因而容易产生错误。帧校验序列（FCS）字段包含一个根据帧中数据计算的数字；这个数字是源计算机计算出来的。一旦目的计算机接收到帧，它将重新计算FCS数字，并同帧中的FCS数字进行比较。如果两个数字不同，就被认为出现错误，帧被丢弃。

通常，帧校验序列数字是通过循环冗余校验（CRC）计算的，该技术对数据执行多项式计算。

5.1.6 以太网帧结构

在MAC子层，对于所有速率（10/100/1,000/10,000 Mbit/s）的以太网来说，帧的结构几乎相同。半双工的吉比特以太网1000BASE-T和10Gbit/s以太网的“W”版本有某些定时问题，因而在MAC子层处理帧隙的过程中存在细微差别，但这些与其他速率不那么一样。然而，在物理层中，几乎所有版本的以太网彼此之间都存在相当大的差异，并且每种速率都有自己的一套结构设计规则。

IEEE 802.3以太网帧

除了前面讨论的802.2帧类型，还有一个更简单的IEEE 802.3帧类型，它是由IEEE最先规划出的。然而，和802.2类似，它并没有被当今的以太局域网所广泛采用。图5-7展示了基本的IEEE 802.3以太网帧的格式。

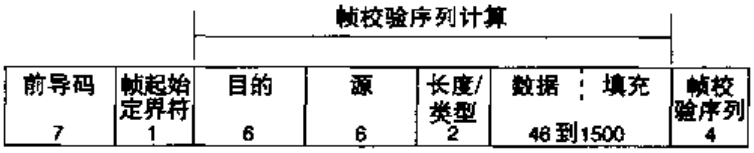


图5-7 IEEE 802.3以太网帧结构

表5-2列出了字节数目和802.3以太网帧字段的名字。

表5-2 IEEE 802.3以太网帧字段

每一个帧字段的字节数	帧字段
7	前导码
1	帧起始定界符（SFD）
6	目的MAC地址
6	源MAC地址
2	长度/类型字段（如果小于十六进制的0600时就代表长度，否则代表类型）
46至1500	数据和填充
4	帧校验序列（CRC校验和）

Ethernet II 帧格式

以太网的DIX版本是在IEEE采纳802.3版本以太网之前开发的，在DIX版本中，前导码和帧起始定界符（SFD）字段组合成一个单独的字段，尽管从二进制模式上来看是相同的。长度/类型字段在早期IEEE版本中只作为长度，而在DIX版本中只作为类型。由于该字段的两种用法在整个工业界都非常通用，所以在后期的IEEE版本中将这两个用法正式合并。早期的DIX以太网帧格式也叫做以太网 Version2或Ethernet II，它是在基于TCP/IP的以太局域网中使用最广泛的帧类型。图5-8展示了Ethernet II帧格式。

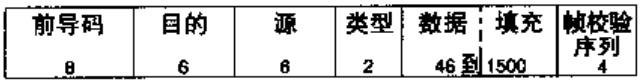


图5-8　Ethernet II帧格式

表5-3列出了字节数目和Ethernet II帧字段的名字。

表5-3　Ethernet II帧字段

每一个帧字段的字节数	帧字段
8	前导码（以10101011模式结束，等同于802.3的SFD）
6	目的MAC地址
6	源MAC地址
2	类型字段（数据长度范围是46至1500，如果小于46个字节，必须在数据后面填充）
46至1500	数据和填充
4	帧校验序列（CRC校验和）

正如表5-3所指出的，Ethernet II类型字段的使用已经合并到当前的802.3帧定义中。在接收到帧的时候，工作站必须确定相应的高层协议是否存在。首先尝试检查长度/类型字段。如果两个字节的值等于或大于十六进制的600，则按照所指出的Ethernet II类型编码来解释帧。如果小于十六进制的600，则将帧作为802.3帧解释，并且帧长度就是字段指出的。接下来需要进一步检查以确定如何继续进行。从这里开始检查802.3数据字段的前4个字节。这4个字节通常分成两个惟一的值来检查；如果这些值不存在，帧被假设成一个802.2逻辑链路控制（LLC）子层封装，并且被根据所指出的802.2 LLC封装来解码。如果被检测的值中有一个是十六进制的AAAA，就表明是一个802.2/802（子网访问协议[SNAP]）封装。另一个被检测的值如果是十六进制的FFFF，就表明是一个老式的Novell网间分组交换（IPX）“原始”封装。

5.1.7　以太网帧字段

下面列表显示了大部分在802.3以太网帧中允许或需要的字段。参考前面图5-8中的802.3以太网帧的图示：

- **前导码**——这个字段包含由1和0交替出现的模式，在异步10Mbit/s和更低速率的以太网中，该字段用于时钟同步。以太网的快速版本是同步的，所以这个时钟信息是多余的，但出于兼容的考虑而保留了下来。前导码是7个字节长，可以表示成下面的二进制模式：

10101010 10101010 10101010 10101010 10101010 10101010 10101010

- **帧起始定界符（SFD）**——该字段是单字节，标志时钟信息的结束。它的二进制模式表示成10101011。在早期的DIX以太网版本中，该字节是8字节前导码的最后一个字节。尽管老DIX以太网对前八个字节的描述不同于IEEE以太网，但二进制模式和用法是相同的。同样，由前导码和SFD所代表的时钟信息已被放弃，并且没有计算到帧的最小和最大长度中。

- **目的地址**——该字段包含了一个6字节的MAC目的地址。目的地址可以是单播（单个节点）、组播（一组节点）或者广播（所有节点）地址。

• **源地址**——该字段包含了一个6字节的MAC源地址。源地址是发送以太网帧的工作站的唯一单播地址。然而，随着虚拟协议使用的不断增长，有时会共享一个特定的源MAC地址作为虚拟实体的标识。

在早期的以太网规范中，MAC地址是可选的2个或6个字节，只要在整个*广播域*中地址的大小是固定的就可以。2个字节的寻址首先是在1998版的802.3规范中的第3.2.3段中明确排除的，并且802.3以太网不再予以支持。

• **长度/类型**——如果这个值小于十进制的1536（十六进制的0600），则代表长度。在LLC层中被用作提供协议标识。

— **类型（以太网）**——在以太网处理过程结束后，类型用来指定接收数据的高层协议。

— **长度（IEEE 802.3）**——长度用来指明紧跟在后面的数据字节的数目。如果该值等于或大于十进制的1536（十六进制的0600），则表示类型，并且数据字段的内容由相应的协议进行解码。常见的以太网类型的协议在RFC 1700中罗列出来，大约是从第168页开始的。

• **数据和填充**——该字段只要不超过最大帧的大小即可。以太网的*最大传输单元（MTU）*是1500字节，数据不能超过此大小。数据可以是任何类型。如果用户数据小于最小帧长度，就会在用户数据后面立即进行数据填充。

帧的结构图显示数据字段介于46和1500字节之间。实际上，以太网并没有规定该字段的大小。只是帧的大小不能小于64字节或者大于1518字节。用户可以从帧的大小中减去其他字段的大小，计算出数据字段的大小。假设使用4字节的MAC地址，数据字段的大小处于46（必要时予以填充）和1500字节之间。

— **数据（IEEE 802.3）**——在物理层和数据链路层处理结束后，根据数据字段中定义的协议信息，数据将被送往相应的高层协议。如果帧的大小不够64字节的最小长度，将会插入填充字节以保证帧至少是64字节长。

• **帧校验序列（FCS）**——该序列包含4字节的CRC值，该值由发送设备产生，并且被接收设备重新计算用来检查帧是否被损坏。循环冗余检查（CRC）算法的数学结果被放置在这个4字节的字段中。发送方对每一个发出的帧计算校验和，4字节的计算结果被追加到数据/填充字段后面。接收方执行同样的计算，将计算结果同接收帧中的校验和进行比较。如果两者匹配，证明帧是完好的。校验计算中涉及的字段包括从目的地址开始到数据/填充字段为止（如图5-7所示）。图5-8中的前导码意味着SFD和扩展字段不在校验计算之内。在以太网帧的字段中，FCS是惟一采用非常规顺序（MSB优先）来传输的。

在目的地址到FCS之间如果出现任意一位比特的破坏，都会产生出不同的校验和，帧校验也包括FCS自身。FCS受到破坏还是前面字段出现破坏是不可能区分出来的。

5.2 以太网工作原理

当多个工作站（节点）要访问物理介质和其他网络设备时，可以采用各种介质访问控制策略。本节简要回顾了访问控制策略，集中讨论以太网的访问控制方法-CSMA/CD。

需要注意的是，尽管CSMA/CD在最初的以太网中具有历史和实践两方面的重要性，但是重要性在实现过程中有所减弱。原因有两个：

• 使用4对线的UTP时，传输（Tx）和接收（Rx）各自占用一对线，铜制UTP能够避免碰撞，并且可以全双工的方式工作，但是要看它是否被用于共享（hub）还是交换的环境。

• 类似的逻辑适用于光纤连接，传输和发送分别使用独立的光纤。

一种新的以太网形式——1000BASE-TX，即通过铜制线缆传输信号的吉比特以太网，在两个方向上同时使用全部4对线，导致持续的冲突。在以前老版本的以太网中，这些冲突妨碍系统的工作。而在1000BASE-TX中，复杂电路可以调节持续的冲突，这类冲突是由于试图在UTP上得到尽可能多

的数据而引起。

5.2.1　介质访问控制

介质访问控制（MAC）是指一些用来确定在共享介质环境（冲突域）中哪个计算机允许传输数据的协议。MAC和LLC组成第2层的IEEE版本。MAC和LLC都是第2层的子层。两类主要的MAC是：

- 确定性的（轮流）。
- 不确定性的（先来先服务）。

令牌环和FDDI是确定性的，以太网/802.3是不确定性的（也叫做随机性的）。

确定性的MAC协议

确定性的MAC协议使用轮流的形式。传递令牌是确定性MAC协议的一个例子。有些美国当地的部落在聚会的时候有传递“发言棒”（talking stick）的风俗。只允许持有“发言棒”的人讲话。当讲话结束后，他/她把“发言棒”传给其他人。

在这个类比中，共享介质是空气，数据是发言人的话语，协议是拥有“发言棒”，“发言棒”也可以叫做令牌。与此类似的数据链路协议叫做令牌环。在令牌环网络中，单个主机被排列成环，如图5-9所示。一个特殊的数据令牌在环中循环。当主机想要通信时，它抓取一个令牌，在有限时间内传输数据，然后把令牌放回环中，令牌可以继续传递下去，直到被另一个主机抓住。



图5-9　令牌环网

非确定性的MAC协议

非确定性的MAC协议使用先来先服务（FCFS）的方法。CSMA/CD是这类协议的一个例子。

为了使用这种共享介质技术，以太网允许网络设备任意传输。在CSMA/CD网络上的工作站监听网络是否空闲，也就是可以传输的时刻。然而，如果两个工作站同时传输，就会发生碰撞，双方都不能成功传输。网络上的所有其他工作站也会听到碰撞并等待网络再次空闲。想要传输数据的工作站依次等待一个随机的时间周期（延后周期）后，才可以再次进行传输，这样可以尽量减少二次碰撞的可能。

三种特殊的拓扑实现以及它们的介质访问控制

令牌环、FDDI和以太网是众所周知的第2层技术。当然，以太网是最为常见的；但是这三种技术服务于针对LAN的各种需求的不同领域。这三种技术都规定了第2层的要素（例如，LLC，命名，成帧和MAC），以及第1层的信号的构成和所用的介质。

- **以太网**——逻辑拓扑是总线型结构（信息流在线性总线上传递），物理拓扑是星型或扩展星型结构（星型布线）。
- **令牌环**——逻辑拓扑是环型结构（信息流沿环传递），物理拓扑是星型结构（星型布线）。
- *FDDI*——逻辑拓扑是环型结构（信息沿环传递），物理拓扑是双环结构（双环型布线）。

5.2.2　以太网MAC

以太网是一种共享介质的广播技术。以太网使用的CSMA/CD访问方法具有以下三种功能：

• 传输和接收数据分组。

• 将数据分组传输到上一层OSI模型之前，解码数据分组，并检测地址的有效性。

• 检测数据分组和网络中的错误。

在CSMA/CD访问方式中，想要在网络介质上传输数据的网络设备采用“先侦听后传输”（listen-before-transmit）的工作方式（CS指载波侦听）。在共享的以太网络中，这意味着一个设备想要传输数据时，首先必须检测网络介质是否忙。这个设备必须检查在网络介质上是否有任何信号。在检测到网络介质不忙的时候，设备开始传输数据。在数据以信号的方式传输的过程中，设备仍然需要侦听，以确保没有其他设备在同时向网络介质传输数据。如果两个设备同时向网络介质传输数据，就如图5-10上半部分显示的那样出现冲突。在设备完成数据传输后，自动进入侦听状态。如果采用传统的以太网络，在一个时间段内只能有一个设备可以传输数据。而交换型以太网就不是这样的，我们将在第6章详细阐述。

网络设备能够检测到网络冲突，这是因为网络介质上的信号的振幅增加了（CD指冲突检测）。当冲突产生时，正在传输数据的设备依然会传输一段很短的时间，以便确保所有的设备都能探测到冲突的产生。当网络中所有传输设备都探测到冲突的产生，每个传输设备都会进行一种运算，也就是*后退*算法。当网络中所有传输设备都后退一段时间后（随机的，每个设备的后退时间都不一致），任一设备就可以再次接入网络介质。当数据在网络上传输时，因冲突而被阻断的传输设备并不具有数据传输的优先权。图5-11大体说明了CSMA/CD过程。

以太网是一种*广播*传输技术。这就是说网络上所有的设备都可以检测到所有沿着网络介质传输的帧。然而，不是网络中的所有设备都可以传输数据。只有MAC地址和帧所携带的MAC地址匹配的设备才能将帧复制到设备自身的缓冲器。以太网与第3层网络地址（如IP或者IPX）并无关系。如果MAC地址匹配，帧就可以被复制和传输到第3层，并检测目的IP或者IPX是否匹配。

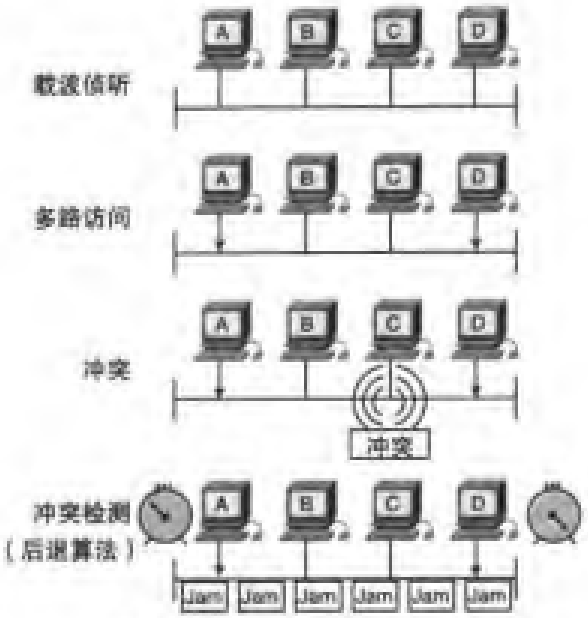


图5-10 载波侦听多路访问/冲突检测

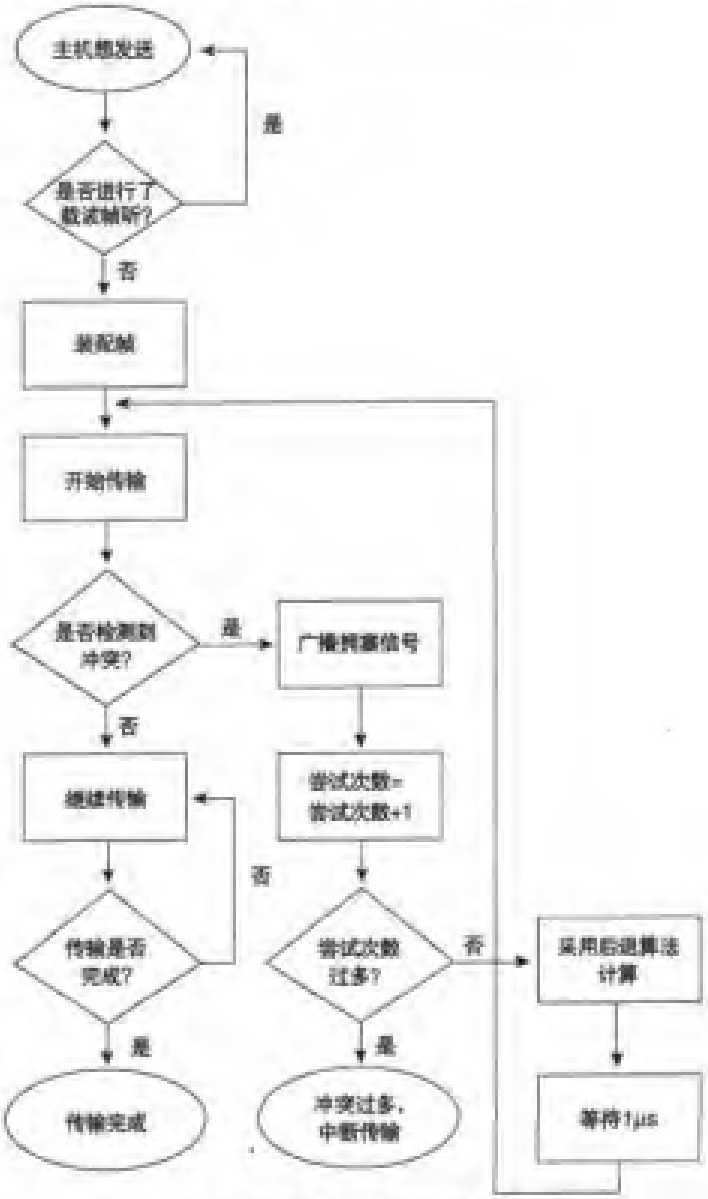


图5-11 载波侦听多路访问/冲突检测过程

当设备验证了数据所带的目的MAC和IP地址后，设备会检测所传递的数据分组是否有错误。如果设备检测到错误，数据分组将被丢弃。不管数据分组是否成功到达，目的设备都不会通知源设备。以太网是一种*无连接的*网络结构，即一种*尽力而为传送系统（best-effort delivery system）*。

5.2.3　单工、半双工、全双工的操作

用于信号传输的数据信道可以按下面三种方式之一运转：单工、半双工、全双工。三种方式的主要区别在于信号的传输方向不同。

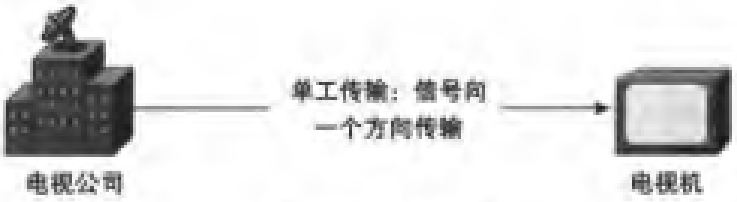


图5-12　单工传输

单工传输是一种简单的传输方式，也被称为单向传输。所有的信号传输都是单向的，就像在单行路上的车流。电视和收音机信号的传输就是一种单工的传输，如图5-12所示。

半双工传输从技术上说是单工传输的一种提高，其传输是双向的。半双工传输确保信号可以双向传输，但这个双向传输并非同时进行，如图5-13所示。半双工以太网，就像开始的802.3以太网标准所定义的，只使用一根线，数据信号在线路上进行双向传输。这样，信号在发送站和接收站之间的数据传输每次只能是单向的。半双工传输使用CSMA/CD协议阻止冲突的产生以及冲突发生时重传数据。

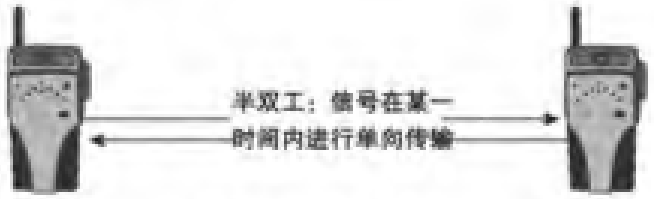


图5-13　半双工传输

全双工传输，如图5-14所示，像一个双向双车道的街道一样运转。数据传输能在两个方向同时进行。以太网全双工操作使交换技术成为可能，这将在第6章里详细论述。因为数据的接收和发送可以同步进行，全双工交换网络技术提高了网络性能。全双工以太网使用两对双绞线，使数据能在发送站和接收站之间同时传输。实际上，全双工以太网是没有冲突发生的，这是因为当两个工作站需要通信时，交换技术在两个站之间建立了一个点到点的虚链路，或称为微分段（microsegment）。全双工以太网理论上可以在双向传输上提供100%的效率。这意味着10Mbit/s以太网如果操作在全双工模式下能达到20Mbit/s。一个100Mbit/s交换潜在地能提供200Mbit/s给一个工作在全双工模式下的工作站。

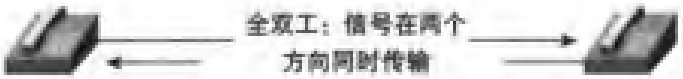


图5-14　全双工传输

5.2.4　以太网定时

以太网被设计运行在总线结构上，这种总线结构使每一个工作站几乎在同一时间都可以听到所有的信息。正式名称是CSMA/CD，CSMA/CD可以这样简单解释，即当两个工作站认识到它们在同时通话时，它们会停止通话并且在重新开始通话之前等待一定的时间。

虽然有一些快速的物理层运行比较复杂，但以太网运行的基本规则和规范并不是很复杂。尽管基本原理简单，但当以太网出现问题时，隔离问题源通常是十分困难的。这是因为以太网是总线结构的（也可以称为分发式的单点故障），问题的范围包括连接到区段上的冲突域内的所有工作站。当使用中继器时，这个范围可以包括四个区段内的工作站。

遵循此规则，以太网内的任何一个工作站想传输信息前，首先要侦听确保当前没有其他工作站正在传输。如果线路上安静，该工作站立刻开始传输。但因为电子信号通过线路传输会花费一定时间（称为***传播延迟***），同时每一个中继器在从一个端口向另一个端口转发帧时也会产生很小的延迟，这样就可能同时或几乎同时有超过一个站开始传输。冲突就这样产生了。

如果这个工作站以全双工模式工作，这个工作站可以同时发送和接收数据，冲突不会出现。全双工操作也改变了对定时的考虑，并且消除了时隙（Slot time）的概念。全双工操作由于没有了对冲突检测的时间限制，而使得设计更大网络结构成为可能。

在半双工操作模式下，假定没有冲突产生，数据发送站传输64比特的定时同步信息，这些信息叫做前导码。后面的传输内容如下：

- 目的和源MAC地址信息。
- 固定的其他帧头信息。
- 实际数据有效负荷。
- 校验和（帧校验序列-FCS）以确保消息在传输过程中没有受到破坏。

接收到帧的终端将重新计算帧校验序列，以便确定入站的消息是否有效，并将有效消息传递给协议栈中的更高一层。

对于10 Mbit/s的以太网以及速率更低的版本来说，采用的是异步传输方式，每一个接收终端采用8字节的定时信息同步接收电路，接收入站数据，而不是丢弃。而100Mbit/s更高速以太网是同步的，所以不需要定时信息。然而，因为某些兼容性的原因，前导码和SFD是存在的。所有在定时信息末尾SFD后面的信息将被传递到上一层。收到帧的时候，需要重新计算校验和，并与接收帧末端的校验和进行比较。如果帧是完整无缺的，它将按照长度/类型字段中指示的协议，或者数据前几个字节中指示的LLC层协议来解释。

以太网基本结构的一些显著变化已经包含在1998版和2000版的标准中。最显著的变化是双字节地址已经被排除在外，尽管在以前的所有版本中都包含在内。当使用长度字段时，802.3长度/类型字段的最大值是1536（十六进制的600），它和先前设定的MTU数据最大值1500（十六进制的5DC）相匹配。

对于所有1000Mbit/s或低于该速率的以太网传输，标准阐明了一个传输不能小于*时隙*。10Mbit/s和100Mbit/s以太网的时隙是512个比特时间（64个字节）。而1000 Mbit/s以太网络的时隙是4096个比特时间（512个字节，包括扩展部分）。时隙并不是为10Gbit/s以太网定制的，因为它并不允许半双工操作。在最大的合法网络结构中使用最长的电缆，并且所有的硬件传播延迟时间都达到合法最大值的时候，回路延迟时间最长，而时隙比这个时间还要长；当检测到冲突的时候，就会使用32位的阻塞信号。换句话说，时隙所需时间，比最大合法以太网冲突域中的两个最远端之间传输所需的理论时间还要长，可能在最后时刻与另一传输发生冲突，然后产生的冲突碎片将返回发送站并被检测出来。为保障系统的正常运行，第一个工作站必须在最小合法帧传输完成之前检测到冲突。如果允许1000Mbit/s以太网工作在半双工的模式，在传输小帧的时候，会添加扩展字段，主要是为保持传输有充裕的时间来确保冲突碎片的回传。这个字段只会在1000Mbit/s的半双工链路中出现，它允许最小为64字节的帧延长足够长的时间来满足时隙的需求。扩展比特将被接收站丢弃。

对这一结果进行大体检测，考虑如下事情：在一个10Mbit/s的以太网上，MAC子层上传输1比特需要用去100纳秒（ns）。在100Mbit/s以太网上，传输1比特需要10ns，而在1000Mbit/s以太网上，只需要1ns时间。表5-4概括了不同类型以太网所需的比特时间。

作一个大概估计，8英寸（约20.3cm）/纳秒通常用于计算在非屏蔽双绞线电缆中的传播延迟。以100m非屏蔽双绞线为例，这就意味着一个10BASE-T的信号在100m非屏蔽双绞线上的传输时间为5个比特时间（大约4.92个比特时间）。简单换算一下，在100Mbit/s的以太网络上需要49.2比特时间，在1000Mbit/s以太网络上需要492比特时间。

表5-4　比特时间

以太网速度	比特时间
10Mbit/s	100ns
100Mbit/s	10ns
1000Mbit/s = 1Gbit/s	1ns
10,000Mbit/s = 10Gbit/s	0.1ns

要使CSMA/CD以太网能操作，发送站必须在一个最小单位的帧传输完成之前就监测到冲突的产生。对于100Mbit/s以太网，系统定时几乎不可能适应100m的电缆。而1000Mbit/s以太网需要专门的（效率很低）调整，因为在第一个比特到达第一个100m非屏蔽双绞线的终点之前，一个几乎完整的最小单位的帧已经被传送完毕。这就很容易解释为什么10Gbit/s的以太网不采用半双工模式。

5.2.5　帧间间隔和后退

表5-5列出的是确保两个分组不冲突的最小间隔，称为帧间间隔（interframe spacing），也就是从前一个帧的FCS字段的最后一位到下一个帧的前导码第一位之间的间隔。

表5-5　帧间间隔

网络速度	帧间间隔	时间
10Mbit/s	96比特时间	9.6μs
100Mbit/s	96比特时间	0.96μs
1 Gbit/s	96比特时间	0.096μs
10Gbit/s	96比特时间	0.0096μs

当一个帧被发送出去之后，10Mbit/s以太网上的所有点至少要等待96比特时间（9.6μs），才能开始下一个帧的传输。即使在速度更快的以太网上，这个间隔也保持相同：96比特时间。但是，网速越快，该间隔的时间就越短，请参见表5-6。这个时间间隔称为帧间间隔（interframe spacing）、帧间间隙（interframe gap）和分组间隙（interpacket gap），目的是确保速度较慢的工作站有时间处理前一个帧，同时为接收下一帧做好准备。

表5-6　时隙参数

网络速度	时隙	时间间隔
10Mbit/s	512比特时间	51.2μs
100Mbit/s	512比特时间	5.12μs
1Gbit/s	4096比特时间	4.096μs
10Gbit/s	不适用	-

* 时隙只适用于半双工的以太网链路

然而，即便是帧的某些前导位面临丢失的可能，从而造成同步减速，中继器的预期作用是在任何一个帧的前面，重新产生出完整64比特定时信息（前导码和SFD）。由于这种强制性定时比特的再引入，我们非常期望尽可能降低帧间间隙。有些以太网芯片组对帧间间隔的缩短非常敏感，只要该间隙降低，系统就看不见这些帧。随着桌面处理能力的提高，个人计算机上的流量更容易充满以太网的网段，并且可以在间隔延迟到来之前开始再次传输帧。近年来，有些厂商故意对帧间间隙设定值进行少许干扰，以便在和竞争产品对比时吞吐量的测试结果有所改善。大多数情况下，这种小把戏没有引起麻烦，但是有出现问题的可能。

工作站之间发生冲突后，所有站的电缆都将空闲，因为每个站都在等待全帧间间隔（full interframe spacing），冲突站必须多等一会儿，也许是更长的一段时间，才能再次重发冲突的帧。设置等待周期（waiting period）的目的是达到半随机的效果，因此在帧重发之前，两个冲突工作站具有不同的延迟时间；否则，将导致更多的冲突。可以通过扩大每次尝试的随机重发时间，部分实现

上述效果。等待时间是以参数时隙的增量进行调节的。

重发由以下公式控制：

$0 = r < 2k$

其中r是时隙的随机数值，k是试图后退的次数（最大的后退次数是10）。后退时间的定义如下：

r*时隙

尽管后退数值对于最后几次重发尝试都是10，但是总共最大的重发尝试是16次。上述公式指定了每次重发尝试等待的最短时间。对一个工作站来说，引入额外的延迟会降低其吞吐量，尽管不是令人满意，但却可以接受。

例如，经历了五次连续的冲突后还不能发送现有的10BASE-T帧，那么等待时间将是0到32 时隙之间的一个随机延迟间隔（0 = r < 25）。需要重申的是，延迟时间是以51.2 微秒为单位的任意值，可以是立即重试，最迟可以在1638.4微秒后重试。

如果在16次重试后，MAC 子层还不能发送帧的话，它将放弃重试并向上一层发送错误信息。此种情况很少发生，只出现在网络负载压力极大或者网络上存在物理问题的情况下。

尽管存在16次发送尝试，但在特殊情况下，MAC子层会遭受更频繁的发送失败，这通常出现在交换链路上。此种现象叫做捕获效应（capture effect）或分组饥饿效应（packet starvation effect）。当两个设备（交换机、端设备或这两种设备）都以半双工方式运行时，各自都试图发送大批流量，这时必然会发生冲突。不论哪个工作站“赢得”首次重发的机会，在传输中极有可能伴随后续的冲突。假设发生了第二次冲突。首先发送帧的第一个工作站，在0到1个时间间隔之间重新选择随机延迟时间，而第二个工作站可以在0、1、2、3个时间间隔中选择。第一个工作站非常有可能再次选择一个更短的延迟时间，然后传输。在接下去的16个连续尝试中，第一个工作站很可能赢得重发的机会。而第二个工作站有可能放弃重试，选择丢弃该帧。第二个工作站将记录下这些过量的冲突错误信息。这类错误通常可以通过*简单网络管理协议*（SNMP）质询交换机端口的方法显露出来，而且经常出现在只有单个设备连接的端口上。由于以太网固有的突发特性，错误信息应该在平均利用率很低的端口上报告。

5.2.6 差错处理

以太网上最常见的错误（一般为良性的）就是冲突。冲突是解决网络访问出现争执的一种机制。有些冲突为网络节点提供一种流畅的、简洁的、低消耗的方法，仲裁网络资源的竞争问题。一旦网络因为各种问题不能正常运作时，冲突可以成为阻碍网络正常运行的重要手段。冲突只出现在半双工网段中。

冲突在两个方面消耗时间。第一，网络带宽的损耗与初始传输和阻塞信号相等，这被称作消耗延迟，影响所有的网络节点。消耗延迟显著地降低了网络的吞吐量。每一个成功或失败的传输尝试对于所有的终端来说，都是一种强制性的闲置时间（后退周期），被称为帧间间隔（或者帧间间隙），这些将直接影响吞吐量。第二类延迟是冲突后退算法带来的后果。后退延迟的效果通常并不显著。

绝大多数的冲突在帧传输的早期出现，并且通常是在SFD之前。在SFD之前产生的冲突一般不向高层次协议报告，就好像冲突并未发生。一旦检测到冲突，发送终端将传输一个32比特的阻塞信号，强制产生冲突。这样，任何正在传输的数据将被完全破坏，所有的工作站都有机会检测到冲突。

在图5-15中，两个工作站都是先监听，确保电缆是闲置的，才开始传输数据。802.3标准对于系统中每个部件的延迟时间给出了一个最低标准限制。对于一个10Mbit/s冲突域，往返延迟时间的最大值为512个比特时间，该值决定了最小帧的长度。工作1最先发起传输，在冲突被检测到之前已经传输了大部分的数据。而工作站2在冲突被检测到之前只传输了少量比特。

仔细观察一下图5-15就会发现，就在信号到达最后一段电缆时，工作站1已经传输了一个帧的大

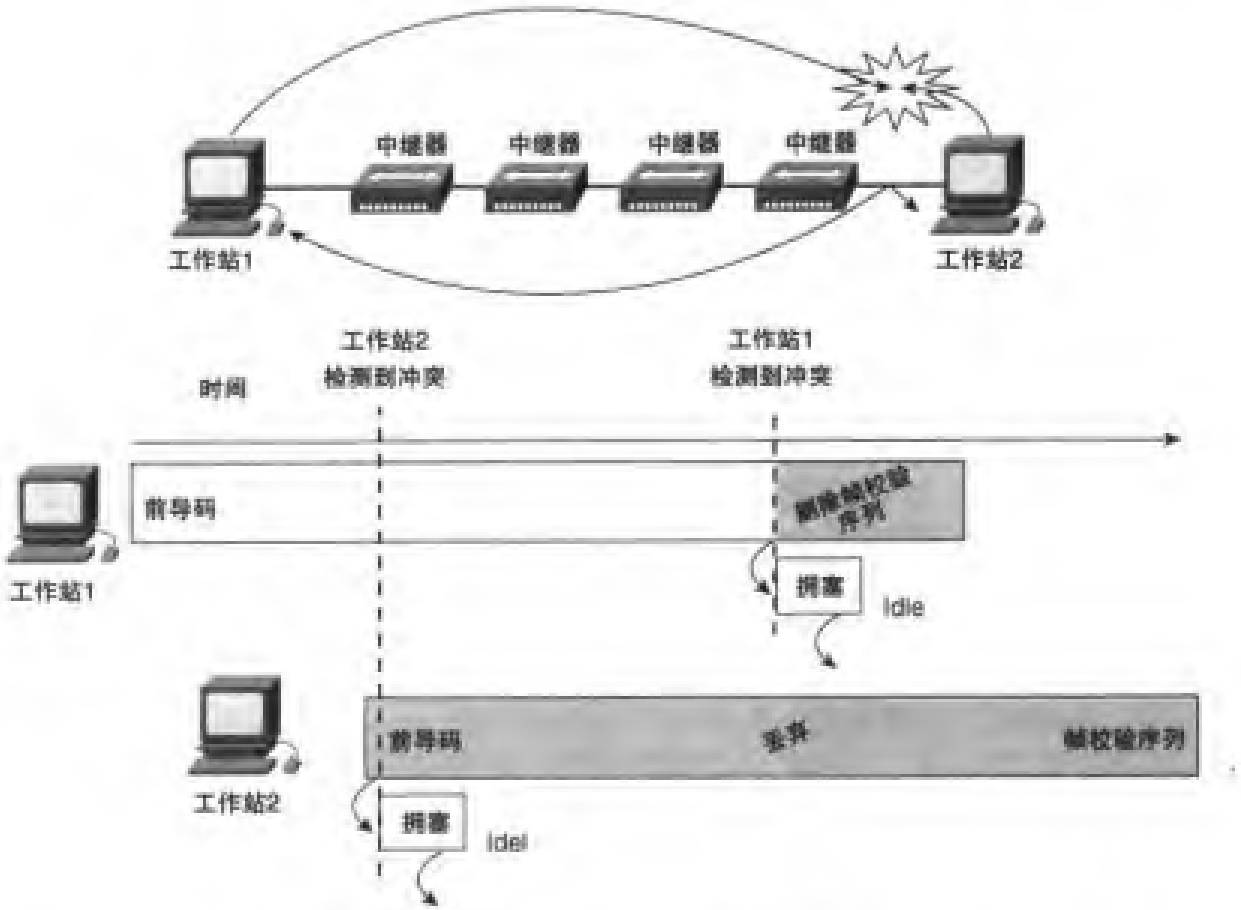


图5-15　10Mbit/s冲突域中的日常错误处理

部分内容。而工作站2在开始自身传输之前，没有接收任何数据。在NIC察觉到冲突之前，站2只能传送几个比特。工作站2立即中断现有的传输，进而开始传输32比特的阻塞信号。然后工作站2中断所有的传输。在发生冲突和阻塞事件期间，工作站2是亲身参与的，冲突域中的冲突碎片传回给工作站1。工作站2完成32比特阻塞信号的传输，在冲突被工作站1接收到之前，呈现闲置状态。此时，工作站1并未检测到冲突，仍然在传输数据。当冲突碎片最终到达工作站1时，工作站1将中断现有的传输，进而开始传输32比特的干扰信号。在传递干扰信号的过程中，工作站1中止了其他的各种传输。

5.2.7　冲突的类型

当位于同一冲突域中的两台或者两台以上的以太网工作站同时发送数据的时候，会发生冲突。冲突一般会被大多数的诊断工具检测出来，利用SNMP查询交换机或者其他设备的时候，冲突可能被报告为单点冲突或者多点冲突。单点冲突是指试图发送一个帧时检测到了冲突，但是在下一次发送尝试时，帧可以成功地发送出去。多点冲突是指在一个帧成功地发送之前发生了多次冲突。这与推迟发送的帧不同，因为推迟发送的帧没有发生冲突。当一台交换机或者工作站试图发送数据时，如果传输介质处于繁忙状态，那么需要等待直到可以发送。当一个帧连续发生冲突后，该帧或许根本就没有被发送，可能会因为发生了过多的冲突而终止发送。

冲突的结果——具有FCS校验错误、小于64字节不完整的或被破坏的帧——称为冲突碎片。一些协议分析和网络监控工具称这样的帧为残帧（runt），但是这样的说法并不确切。

可以通过协议分析会话捕捉到的以太网帧错误类型一般可以分为本地冲突（local collision）、远程冲突（remote collision）和后期冲突（late collision）。图5-16说明了这三种冲突类型。以下几小

节简单介绍各种帧错误类型。

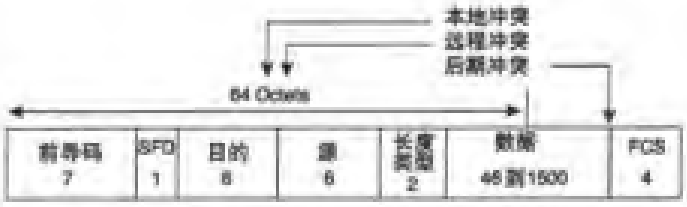


图5-16 冲突类型汇总：本地、远程和后期冲突

本地冲突

在同轴电缆上（10BASE2和10BASE5），信号在单一的传输介质上传播直到遇到另外一台工作站产生的信号，发生本地冲突。信号交叠在一起，减弱了部分信号同时又增强了（加倍）部分信号。加倍的信号使得信号的电压水平超出了最大限度。这种电压过高的情况被这一电缆上的工作站感应为冲突。网卡上有专门的线路负责检测电压超载。在同轴电缆上，一般在-1.5伏附近检测到过载电压。图5-17显示了一段被数字示波器捕捉到的10BASE2/10BASE5冲突的部分帧信号。



图5-17 10BASE2/10BASE5本地冲突

在图5-17中，信号的开始表示的是正常的曼彻斯特编码。增加了其他的信号之后，原信号幅度增加了一倍。这就是冲突的开始，两个波形互相叠加在一起。在这个例子的最后，波形恢复正常，其中一个发送站检测到了冲突并停止了发送，另一个冲突站点发送的拥塞信号（Jam）被检测到。

在无屏蔽双绞线上（比如10BASE-T、100BASE-TX和1000BASE-T），当一个工作站在利用TX线对发送数据时从RX线对上检测到信号，就会发生本地冲突。因为两个信号使用不同的线对，信号实际上没有类似于图5-17那样的信号特征变化。在无屏蔽双绞线上，只有工作在半双工状态下的工作站可以检测到冲突。全双工和半双工在功能上的惟一差别在于是否允许在传送线对和接收线对上同时进行信号传递。如果一个工作站没有进行传输，它就不可能检测到本地冲突。相反，线缆的故障，例如过强的串扰（Crosstalk），可以导致工作站把自己发送的信号检测为本地冲突。

远程冲突

远程冲突的特征是帧长度小于最小帧长度，同时FCS校验码错误。远程冲突并没有本地冲突那样的电压过载或者RX/TX能够同时检测到有信号传送。这种类型的冲突通常是由发生在中继器远端发生的冲突造成的。中继器不会转发过载电压，也不可能发生TX和RX线对同时工作的情况。工作站将进行传输以使两对线都激活，这将导致本地冲突。在无屏蔽双绞线网络里，这是最常见的冲突类型。几乎所有的可以报告冲突的监测工具，例如软件协议分析器和远程监控（RMON）探针，都只能检测到远程冲突，因为他们都是被动监听设备。

后期冲突

在发送站发送了64个字节之后，正常的和合法的冲突就不可能发生了。理论上讲，正常的网络传播一定会在此之前就完成了。在前64个字节传输完成之后发生的冲突成为后期冲突。后期冲突和发生在前64个字节的冲突的最明显区别是网卡会自动重新传输正常的冲突帧，但不会自动重新传输后期冲突引起的冲突帧。从网卡的角度看，一切已经工作正常，协议栈的高层一定要设法减少这样

的帧丢失。除了不进行重新传输之外，工作站在检测到后期冲突后的处理应该和正常的冲突一样。

一个例外是802.3标准，在发生后期冲突时，它允许工作站尝试重新传输，但没有规定必须重新传输。千兆以太网明确禁止发生后期冲突的帧重新传输。

后期远程冲突发生在时间超时并且发生在中继器的远端。无论如何，因为中继器会妨碍发现过载电压和TX/RX线对同时工作这样的本地冲突特征，监测硬件必须能够在远端检测到后期冲突并且报告给监测站点。通过检查一个错误帧的最后几个字节，如果表现出来的模式与JAM信号相关，分析可知一定在中继器的另外一端发生了后期远程冲突。一般而言，这样的冲突一般在本地网段会简单地判断为一个FCS校验错误。

5.2.8　以太网错误

为什么要学习以太网的错误呢？因为以太网是当前主流的局域网技术，更多地了解一些典型的错误对理解以太网的工作原理和排除故障都是很有帮助的。

本地冲突和远程冲突是以太网正常工作的一个组成部分，后期冲突则被认为是一种错误。以太网上错误总是需要更深入地分析判断。错误的严重性一般表示着排除故障的紧迫性。在几分钟或者几小时里出现的少量错误可以低优先级处理。几分钟之内上千错误的出现是需要引起高度重视的。以太网需要考虑的错误包括：

- 在时隙消失之前出现的同时传输（冲突或小帧）。
- 在时隙消失之后出现的同时传输（后期冲突）。
- 过量的或者非法的长传输（jabber、长帧和范围错误）。
- 非法的短传输（短帧、冲突碎片或者小帧）。
- 被破坏的传输（FCS校验错误）。
- 过多或者过少的位传输（调节错误）。
- 实际和报告的帧长度不一致（范围错误）。
- 非常长的前导码或堵塞事件（ghost或者Jabber）。

每一种情况都被分别定义。在错误情况下产生错误的帧是经常出现的，但是错误帧并不一定总是被丢弃掉。为了有一个比较完整的列表，正常的冲突也被包括在其中，但是我们不认为这是错误帧。下面的小节简单地描述了以太网的一些错误。

逾限（Jabber）

*逾限*在802.3标准中好几个地方都有定义，它在期间内传输至少20,000到50,000比特时间。然而，大多数的诊断工具只要检测到传输超过了最大合法帧尺寸就会报逾限错误——这个尺寸比起20,000到50,000比特时间来说相当小。这会导致一个模糊的定义，因为报告设备既可能认为也可能不认为1518个8bit字节带有VLAN标记的帧超过了合法的限制。同时，逾限也没有帧检验序列（FCS）是好或坏的指示存在。多数说到逾限的情况被称为长帧会更合适些。

长帧（long frame）

*长帧*是比最大合法尺寸大的帧，并考虑到帧是否进行了标记。它不管帧有没有合法的FCS检验和。这种错误通常表示有人在网络中检测到了逾限错误。图5-18所示为一个比1518个8bit字节长的长帧。

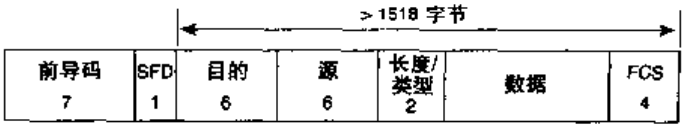


图5-18　长帧

逾限和长帧都超过了最大帧尺寸。然而，逾限要大得多。如果帧是用802.1q标记的话，通常对非法的大帧不予计算。IEEE的802.1Q标准定义了虚拟局域网（VLAN）桥接的操作，该操作允许在桥接的局域网基础设施中定义、操作和管理虚拟局域网拓扑。IEEE的802.1Q标准是开发出来用于解决如何将一个大的网络划分成小的部分的问题，从而使得广播和组播通信量不占用比必要的更多的带宽。

短帧（Short Frame）

*短帧*是比最小合法尺寸64个8bit字节还要小的帧，它有合法的FCS校验和。有些协议分析器或者网络监视器把这些帧称为残帧，不过这个术语是不精确的。通常，你不必留意短帧，尽管它们的存在并不保证网络失效。

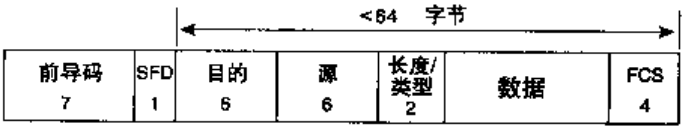


图5-19 短帧

短帧除了某一方面外其他都是适当成形的，并且具有合法的FCS校验和；然而，它们比最小帧尺寸（64个8bit字节）要小。图5-19所示为一个比64个8bit字节要小的短帧。

残帧（Runt）

术语*残帧*一般是一个不精确的俚语术语，表示比合法帧尺寸要小的帧。是指具有合法的FCS校验和的短帧。残帧通常是冲突分片引起的。以太网标准中描述了这样一个叫做runt的SNMP管理属性，它大约比74比特时间大，但是又比最小帧尺寸（在10/100M bit/s是64个8bit字节，或者在1000Mbit/s的最小半双工传输事件时是517个8bit字节）要小；它不是局部冲突。

FCS错误

收到的帧的FCS是坏的（也被称为校验和错误或者CRC错误），它与传输的帧相比至少有1bit的差异。在有FCS错误的帧里，其头信息可能是正确的（寻址等），但是由接收站计算出来的校验和与发送站附在帧后面的校验和不一致。信任单个帧中的寻址信息的精确性可能是一个差劲的主意，但是如果很多帧都是同一个源地址，那么则可以认为源地址是正确的。

从一个工作站发出大量的FCS错误通常表示在网络接口卡上有故障或者软件驱动程序有故障或者被破坏了，或者是工作站到网络的电缆连接坏了。如果FCS错误与许多工作站相关，通常源于劣质的布线、有故障的网络接口卡驱动程序版本、有故障的集线器端口，或者是线缆系统中引发的噪声。

当在传输中至少有1bit的改变就会报告FCS错误。当接收站计算出一个新的校验和并与FCS字段中的校验和相比，两者不同的时候，帧就被丢弃。

调节错误（Alignment Error）

不以8bit字节边界结尾的消息被称为***调节错误***。即不是用正确数量的二进制bit来形成完整的8bit字节分组（grouping），而是剩余了一些额外的字节（不足8）。于是帧被截断到最接近的8bit字节边界；如果FCS校验和失败，就会报告调节错误。这常常是由于不好的软件驱动程序或者冲突引起的，经常伴随着FCS校验和失败。其他引发因素表现出由软件bug导致的读写错误的特点。如果调节错误没有被纠正，可以导致崩溃。通常，软件会自己纠正，但是对路由器的CPU资源来说会引起突然的毛刺（spike）。

范围错误（Range Error）

在长度字段具有合法尺寸值的帧，其数据字段中的8bit字节的实际数量却与该尺寸不一致，这种收到的帧被称为范围错误。这种错误也出现在长度字段的值小于数据字段的最小合法非填充尺寸

时。类似的错误是当长度字段的值指出数据的尺寸太大而不合法的时候所报告的超出范围（Out of Range）错误。

幽灵（Ghost）

Fluke网络发明的术语*幽灵*是指在线缆中检测到的能量（噪声）看起来像是一个帧却没有合法的起始帧定界符（SFD）。要鉴定为幽灵，该“帧”必须要有至少72个8bit字节长（包括前导码）；否则，它被分类为远程冲突。由于幽灵的奇特性质，注意到测试结果很大程度上依赖于在分段的什么地方进行的测量这一点很重要。

一些类型的噪声让网络分段上的节点误认为它们收到了一个帧。然而，感觉到的帧却永不会来，于是也没有数据传到网络接口卡上处理。不久，感觉到的传输终止了，网络接口卡恢复传送它自己的消息。不同的网络接口表现不一样，没有标准定义网络接口卡应该如何或者什么时候对噪声分段反应。中继器常常会将这些噪声信号传播到冲突域中的其他分段。

幽灵的显示症状是网络没有明显原因地变慢。文件服务器几近空闲，网络监视设备显示非常低的网络利用，但是用户却抱怨网络非常的慢或者完全断掉了（down）。这种现象可能是地域限制，即在大的长的分段的一端看起来可以操作而在另一端则很慢或者完全断掉。

接地环路和其他布线问题通常会导致幽灵。幽灵导致一些中继器好像收到了帧一样反应。由于中继器只对线缆上的交流电压响应，因此就不会让有效的帧传到其他端口上了。然而中继器将这个能量传送到其他端口上。传送的幽灵看起来可能像拥塞模式（jam pattern）或者非常长的前导码。

大多数网络监视工具不会识别幽灵的存在，同理，它们也不能识别前导码冲突——它们完全依据芯片来判断。纯软件协议分析器、许多基于硬件的协议分析器和手持测试工具，以及大多数的RMON探测器都不会报告这些事件。

5.2.9　以太网自动协商

随着以太网从10Mbit/s发展到100Mbit/s，再到1000Mbit/s，一个目标是使各种技术能互操作，甚至是使得10、100和1000的接口能直接互联。因此开发了一个称为自动协商（autonegotiation，协商速度以及使用半双工还是全双工）的过程。具体说，再快速以太网引入时，该标准就包括了一种能自动配置特定接口方法，能实现速度和能力与链路对端接口相匹配。特别地，在快速以太网被提出时，标准包含有自动配置指定接口的方法以匹配链路伙伴的速度和能力。该过程定义了两个链路伙伴如何能自动协商配置来提供最好的共用性能等级。这是仅仅涉及物理层最低部分的附加好处。

10BASE-T要求每个工作站在不发送消息时每隔约16 ms发送一个链路脉冲。自动协商采用该信号并将之重命名为正常链路脉冲（NLP）。当一串NLP按组发送进行自动协商时，该组称为快速链路脉冲（FLP）突发。每个FLP突发在与NLP相同的定时间隔被发出，这可允许较老的10BASE-T设备能正常操作，如果它们接收FLP突发的话。图5-20解释了NLP和FLP定时。

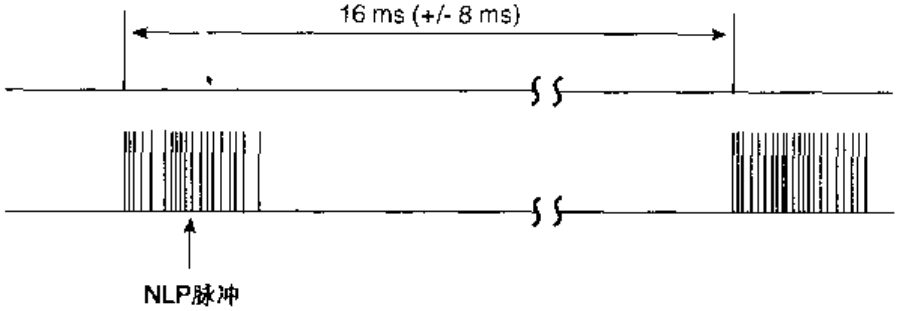


图5-20　NLP定时与FLP定时

10BASE-T采用+1和-1伏特间的信令来发送，达到2伏的峰间差值信号。NLP信令仅采用0到+1伏特的范围。单个NLP脉冲的时长为100ns。图5-21解释了两个样本NLP脉冲。左边的脉冲很陡和清晰，它来自能进行1000Mbit/s操作的接口。右边的脉冲来自较老的仅能进行10/100Mbit/s操作的设备，它不要求信号的精确。

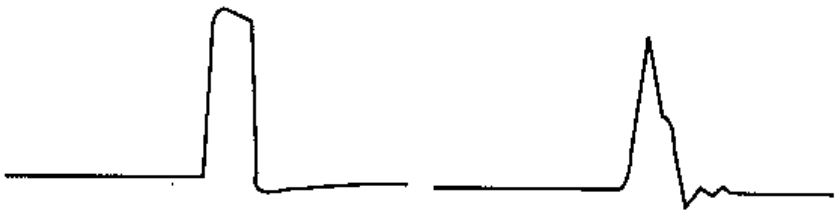


图5-21 NLP脉冲

自动协商通过传输来自两个链路伙伴的10BASE-T链路脉冲的突发来实现。突发将发送站的能力传送到其链路伙伴。在两个工作站都理解了另一伙伴所提供的消息之后，两者都切换到最高性能的共用配置，并在该速度建立链路。如果有任何情况中断了通信且链路丢失，则这两个链路伙伴首先试图以上次所协商的速度进行连接。如果这也失败了，或链路丢失已经很长时间了，则自动协商过程重新来过。链路的丢失可能是因为外部的影响，诸如电缆故障，或因为一个伙伴发出重置。

图5-22所示是实际的FLP自动协商突发。FLP突发由多个NLP链路脉冲组成。



图5-22 NLP自动协商突发

FLP突发包含33个脉冲位置，它们表示出17个时钟脉冲所构造的一个16比特链路码字。在突发中脉冲间隔为62.5ms（±7ms）。在每个时钟脉冲间有数据脉冲位置。如果数据脉冲出现，则表示为二进制1。在两个时钟脉冲间数据脉冲在窗口中不出现，则表示为二进制0。如图5-23所示，17个时钟脉冲总是存在的。16个数据脉冲仅在表示二进制1时才出现；如果它们在编码的16比特数据码字中表示二进制0，则不出现。数据中表示二进制1的脉冲以灰色来突出显示。

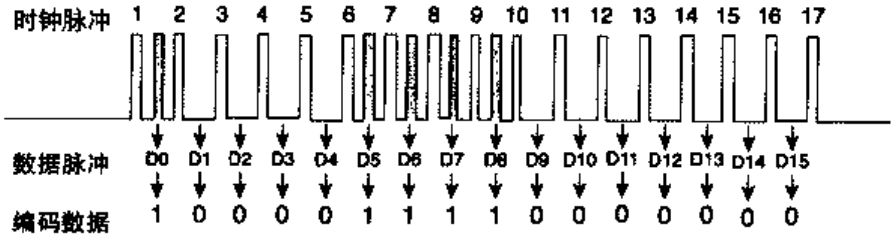


图5-23 自动协商脉冲的说明

当自动协商实现后，附加的信息可采用页的概念来补充。页是表示更为复杂的协商和链路参数的附加比特。

在设备将由链路伙伴所提供的链路码字解码后，它通过发送至少有三个确认比特置位的FLP突发来确认当前码字的接收。在两个链路伙伴都确认了当前以该种方式所交换的FLP链路码字，则链路伙伴或是进行到下一页的发送，或是使已协商的配置运作并试图据此连接起来。链路伙伴在初始的配置基础页之后可发送任意数量的下一页，以及与基础页有联系的任意数量的下一页。

5.2.10 链路建立和全/半双工

链路伙伴允许略过它们所能提供的配置，但不允许包括它们所不能提供的配置。这使得网络管理员能强制端口为所选择的速度和双工设定，而无需禁用自动协商。

自动协商对于大多数以太网实现是可选项。吉比特以太网要求实现自动协商，尽管用户能禁用它。自动协商最初是为以太网的UTP实现所定义的，通过在FLP突发中使用/C/有序集，它被扩展到在其他光纤实现的以太网中进行工作。

当一个准备自动协商的工作站开始试图连接时，可推测到的就是前端芯片集的10BASE-T部分试图立即建立一条链路。如果10BASE-T信令出现且工作站支持10BASE-T，则无需协商就试图建立一条链路。如果信令产生一条链路，或是接收到FLP突发，工作站将继续进行该技术的操作。如果链路伙伴不提供FLP突发而用NLP代替，则该设备自动被认为是一个10BASE-T工作站。在测试其他技术的初始间隙，发送路径上传送FLP突发。该标准不允许对任何其他技术的并行检测。

如果一条链路是通过并行检测而建立，则它必须是半双工。仅仅存在两种实现全双工链路的方法：

- 经过完整的自动协商过程。
- 在管理上强制使两个链路伙伴为全双工。

如果一个链路伙伴被强制为全双工，而另一个链路伙伴在试图自动协商时进行并行检测，则无疑会产生双工的不匹配，结果导致链路上的冲突和错误。如果你强制一端，那么也必须强制另一端。对此的例外是10吉比特以太网不支持半双工。

很多厂商以这种循环经过各种可能状态的方式实现了硬件产品。它发送FLP突发进行一会儿自动协商，然后它把自己配置为快速以太网并试图连接一会儿，最后它简单地进行一会儿监听。一些厂商的产品不提供任何连接的发送企图，直到第一次收到FLP突发或某个其他的信令机制。在沉默的监听状态，便携式计算机能节约足够的电池能量，这是很值得做的，虽然该模式不被标准所支持。

以太网双工操作

存在两种双工模式：半双工和全双工。对于共享介质，半双工模式是强制性的。所有同轴的实现在本质上都是半双工的，不能进行全双工操作。UTP和光纤的实现可在半双工模式下工作，但该模式是管理上的强制。所有的10 Gbit/s实现仅为全双工而指定。

在半双工模式，一次仅一个工作站能发送。对于同轴实现，第二个工作站的发送会导致信号重叠和冲突，结果信号破坏。因为UTP和光纤一般地在不同线对上发送，所以信号不会重叠和破坏。以太网建立了仲裁规则以解决当多于一个工作站试图同时发送时所产生的冲突。在点到点的全双工链路中两个工作站能够在任何时间发送，而不管另一个工作站是否同时在发送。

自动协商避免了大多数情况发生，即在点到点链路中一个工作站按半双工规则发送，而另一个在全双工规则下操作。在低于10吉比特以太网的速度下实现全双工连接仅有两个方法：

- 通过使用自动协商。
- 通过管理上强制接口模式。

如果在点到点链路上一个工作站准备自动协商而另一个没有，则进行自动协商的工作站需选择半双工。这样，如果链路的一端是被强制了的，则网络支持人员有责任把另一端也作强制处理。对两端强制处理的失效导致人为提高的错误等级和链路上差的性能。双工不匹配可能是交换网络中所发现的最普遍问题。

优先级判定

在预先情况下，链路伙伴共享多种的共同技术，下面的列表用于决定自所提供的配置中选择何

种技术。换句话说，对于10/100/1000 Mbit/s基于铜的以太网版本

换句话说，需要的是基于铜线以太网的10-/100-/1000-Mbit/s接口能就连接的最佳方式自动取得一致。

下面的列表是按优先级排序的，最希望使用的链路配置排在最上面：

- 1000Mbit/s、全双工
- 1000Mbit/s、半双工
- 100Mbit/s、全双工
- 100Mbit/s、半双工
- 10Mbit/s、全双工
- 10Mbit/s、半双工

光纤以太网的实现方式没有保护在这个优先级确定列表中，因为接口的电子和光器件不支持很容易地在不同实现方式之间进行重新配置。假设接口配置是固定的。如果两个接口能自动协商，它们必定已经使用了相同的以太网实现方式，尽管还有很多的配置选项需要确定，比如双工设定或者谁作为定时的主导方。

5.3 冲突域和广播域

本节介绍冲突域和广播域相关的内容。过多的广播和冲突会影响网络的性能。本节将讨论如何减少网络中广播和冲突的影响。本节定义了术语*分段*（*segment*），并将讨论不同类型的分段。

5.3.1 直连网络

要理解冲突域，首先要知道什么是冲突域以及它是怎么产生的。回顾一下第1层的介质和拓扑将有助于解释冲突域。

图5-24表示了如下不同类型的直连网络：

- **共享介质环境**——共享介质环境发生在多台主机连接到同一介质时。例如，如果几台PC连接到同一物理电缆或者光纤上，或者共享同一物理空间，它们就是共享相同的介质环境。在这种情况下，称他们共享同一冲突域。传统的总线型以太网（同轴电缆）和集线器连接的以太网（UTP连接）都是共享介质环境。
- **扩展的共享介质环境**——这是一种特殊类型的共享介质环境，其中网络设备可以扩充环境以便它能适应多样的通路访问或比较长的电缆距离。使用以太网中继器或者多个集线器能够产生扩展的共享介质环境。这将产生一个扩展的冲突域。
- **点到点网络环境**——它广泛应用于拨号连接，对家庭用户最为熟悉。它是一种共享网络环境，像个人电脑用调制解调器和电话线连接到互联网业务提供商（ISP）那样，其中一台设备只连接到另一

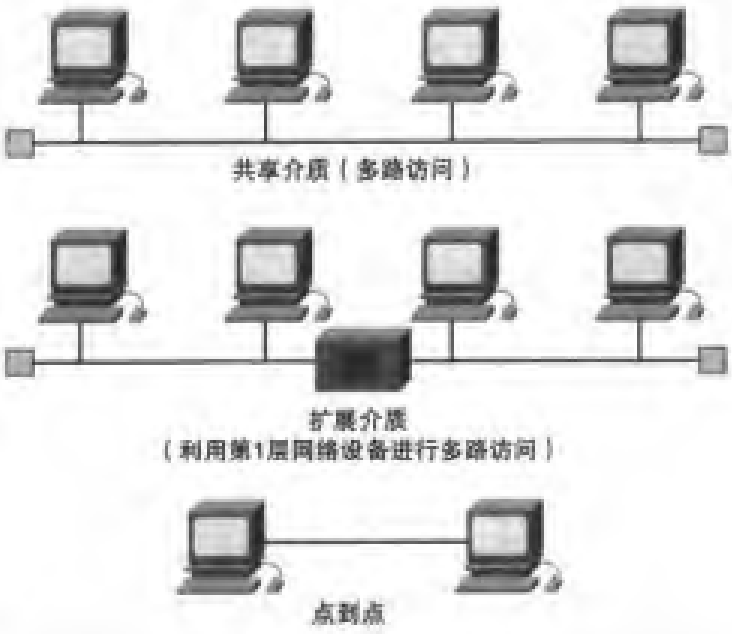


图5-24 直连网络

台设备上。因为这是一个点到点专用连接，所以没有潜在的冲突发生。没有其他设备共享链路。

5.3.2　非直连网络

有些网络是间接连在一起的，意味着在两个通信主机之间有一些高层网络设备或者一些地理距离存在。图5-25显示了如下两种类型的非直连网络：



图5-25　非直连网络

- **电路交换型**——一种非直接相连的网络，在这种网络环境下，在通信过程中维持着实际的电路。电路交换在端点间建立其物理的、端到端的连接。带宽全部分配给了这个点到点连接。现在的电话系统仍然部分地是电路交换的，尽管许多国家的电话系统现在对于电路交换技术已经不像以前那样热衷了。因为这不是共享环境，所以没有突冲。
- **分组交换型**——不是在两台通信主机之间分配一条链路作为惟一的电路连接，而是源主机以分组的形式发送信息。每个分组都包括了足够的信息，使它能够被路由选择到正确的目标主机上。分组交换网络常常共享物理介质，但是由于建立了逻辑上的点到点连接，所以没有冲突发生。

5.3.3　冲突和冲突域

确认介质是否共享环境很重要，这是因为共享环境会引起冲突。类似的情形是在高速公路上的汽车。如果公路上只有一辆汽车，不会有任何碰撞发生。然而，像图5-26所示那样，如果同时有多辆汽车试图使用同一路段，就会发生冲突。对网络情况亦是如此：如果同时有超过一台计算机试图在同一网段内传输数据，就会导致冲突。

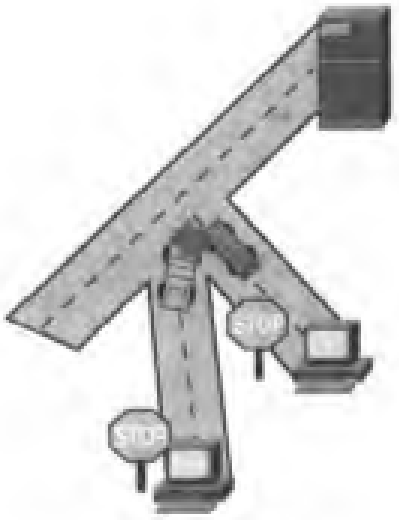


图5-26　冲突

冲突是这样一种情形，当2bit同时在同一网络上传播时就有可能发生。小型低速网络可以在这种系统下良好地工作，即只有两台计算机被允许按照顺序发送消息。问题是大型网络中有许多计算机连接在一起，每个区段每台计算机都有数百万计bit要通信。

冲突域是物理上连在一起可能发生冲突的网络分段（segment）。冲突导致网络低效。每次网络上有了冲突，所有的传输都要停止一段时间。这个停止时间长度是可变的，它由每个网络设备的后退算法（backoff algorithm）决定，对于允许恢复广播传输这是必需的。

除了单个独立的以太网局域网（LAN）环境外，使介质片断连接在一起的设备类型定义了冲突域。这些设备分别归类于OSI的第1、2和3层设备。第1层设备不会隔离冲突域；第2和第3层设备像图5-27描述的那样确实隔离了冲突域。用第2层和第3层设备隔离冲突域或者增加冲突域的数量称为*分段*（*segmentation*）。

应用层	
表示层	
会话层	
传输层	
网络层	隔离冲突域
数据链路层	隔离冲突域
物理层	一个冲突域

图5-27　冲突域分段

像中继器和Hub等第1层设备，对延伸以太网电缆分段起到主要作用。延伸网络后，可以有更多的主机加入进来。然而，主机的增加增大了网络中潜在的通信量。由于第1层设备传递所有发送到介质的东西，所以同一冲突域中要传输的通信量越大，发生冲突的可能性就越大。最后结果降低了的网络性能，而且如果网络上的所有计算机对带宽有更大的需求的话，这种性能降低越明显。如图5-28那样是简单地用第1层设备来扩充冲突域的范围，不过这样可能会把局域网的长度过分扩张并可能导致其他冲突问题。

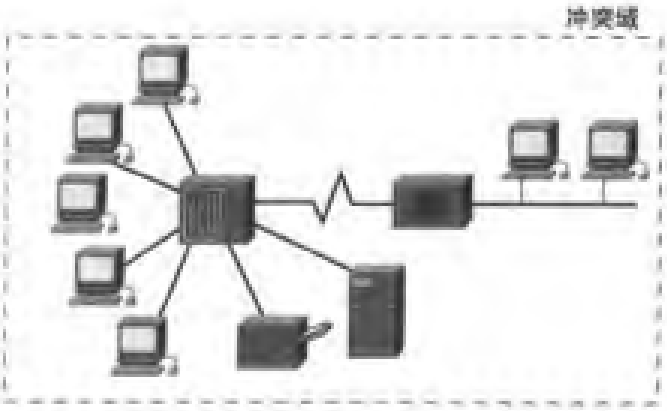


图5-28 中继器增加冲突域

以太网中的四中继器原则是指，在网络上的任何两台计算机之间不能安装超过4台中继器或者中继集线器，如图5-29所示。为了保证使用中继的10BASE-T网络的正常功能，往返一次的延迟计算结果必须在一定的范围内。否则，将不是所有的工作站都能接收到网络上所有的冲突信息。

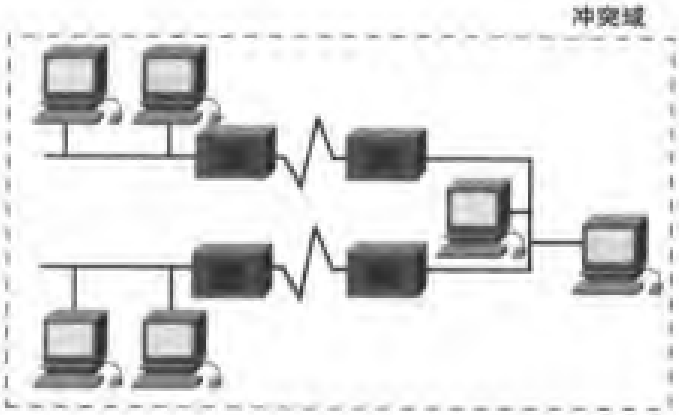


图5-29 四中继器原则

四中继器原则考虑了中继器等待时间、电路传播延迟和网卡等待时间等因素的作用。超过四中继器原则会违反最大延迟的限制，一旦越限，后期冲突数量会大大增加。后期冲突是指已经传输了帧的前64字节后发生的冲突现象。后期冲突发生时网卡的芯片组不会自动重新传输数据。这些后期冲突帧增加了一种被称之为消耗延迟（consumption delay）的延迟现象。随着消耗延迟和等待时间增加，网络性能随之下降。这个以太网定律被称之为5-4-3-2-1规则。这意味着不能超过如下的指导方针：

- 主机段包含
  —5段网络介质。
  —4个中继器或者集线器。
  —3段网络。
- 2段链路段（没有主机）。
- 1个大的冲突域。

5.3.4 分段

作为一名专业的网络工作人员，具有识别冲突域的能力是所需的一项重要技能。将几台计算机连接到一个单独的，没有其他的网络设备相连的共享访问介质上就构成了一个冲突域。这种情形限制了可以使用介质的计算机数量，被称之为*分段（segment）*。如同图5-30所示，第1层设备扩大了冲突域但是并不控制冲突域。

第2层设备形成分段，亦即隔断了冲突域。它通过用分配到每个以太网设备的MAC地址来控制帧传播实现了这个功能。第2层设备（像网桥和交换机）记录下设备MAC地址和它们所属的分段。使用这个方式，这些设备就能在第2层上控制通信流量。这个功能同时让数据在局域网内的不同分段

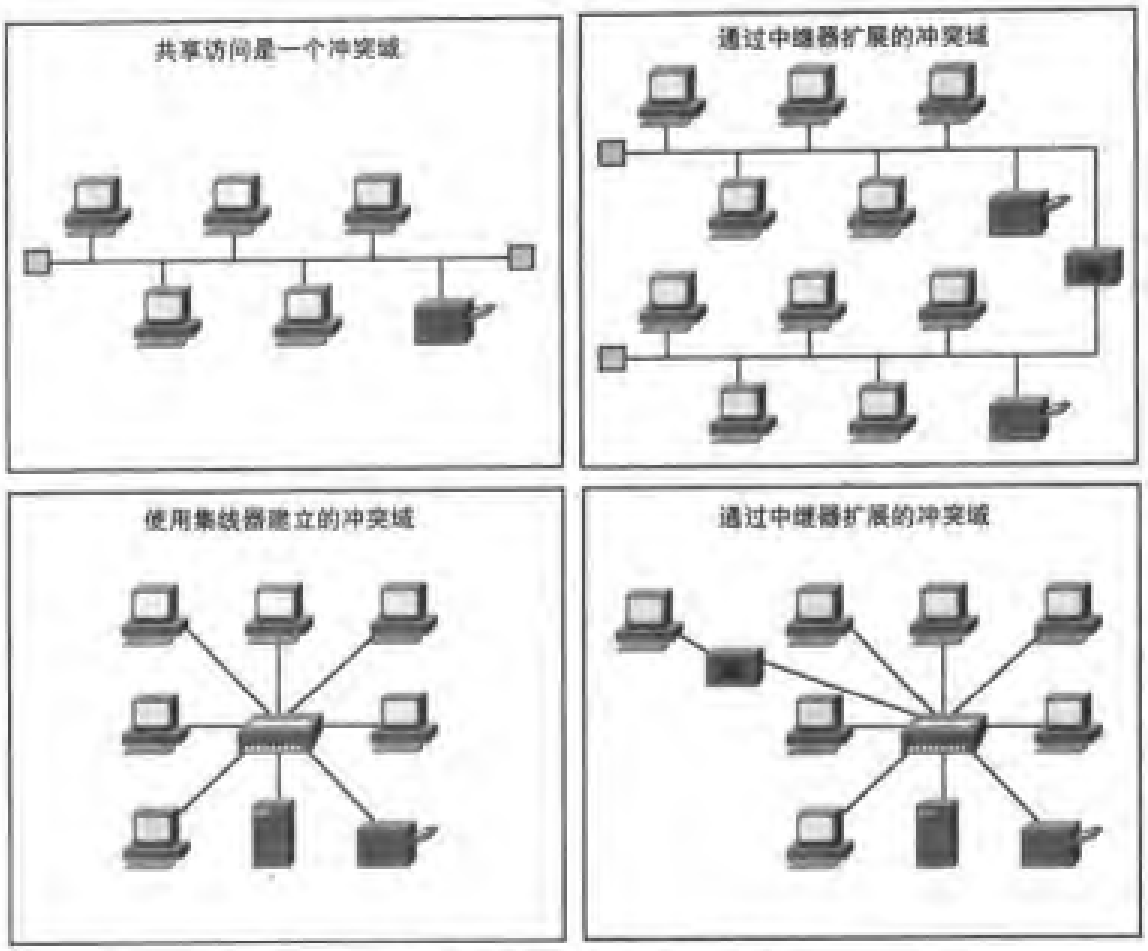


图5-30　扩展冲突域的第1层设备

中传输而不引起帧的碰撞（colliding），使网络变得更有效率。通过使用网桥和交换机，冲突域被有效地分割为小的部分，每个部分又形成自己的冲突域。

这些小的冲突域比原来的冲突域有更少的主机和更小的通信量，于是就增加了该域中每个主机的可用带宽数量。冲突域中的通信量越少，当主机希望传输数据时介质可用的机会就越大。当网络分段之间的通信量不太大时上述情况有效，否则，第2层设备实际上可能会减慢通信并形成瓶颈。

同第2层设备一样，第3层设备并不传递冲突。因为这个原因，在网络中使用第3层设备可以起到将冲突域划分成更小的域的作用。第3层设备起到的作用不仅仅是划分冲突域。第3层设备和它们的功能将在“广播域”一节有更深入的介绍。如图5-31所示，第2层和第3层设备可以隔离冲突域。

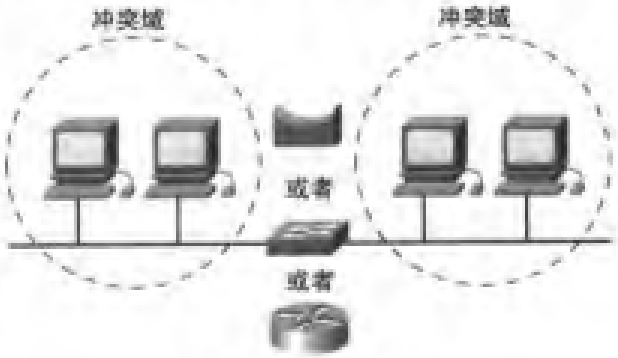


图5-31　限制冲突域

5.3.5　第2层广播

为了在所有的冲突域之间进行通信，协议在OSI模型的第2层使用广播（broadcast）和组播（multicast）帧。当一个节点希望同网络上的所有主机进行通信时，它就发送一个目标MAC地址是0xFFFF FFFF FFFF的帧。这个地址能够被每个主机上的网卡（NIC）所识别。

第2层设备必须泛洪所有的广播和组播通信量。网络中每个设备传来的广播和组播通信累积起来被称之为广播辐射（broadcast radiation）。图5-32所示为网桥转发到网络上所有主机的广播。

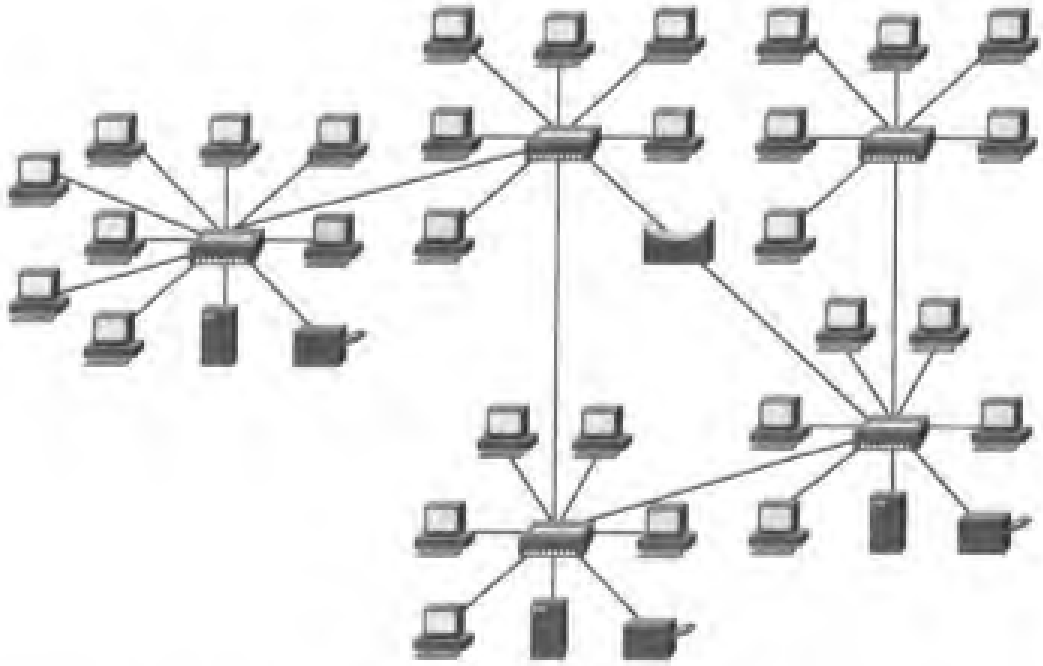


图5-32 第2层广播

因为网卡必须中断CPU来处理每个它所属于的广播和组播组，所以广播辐射会影响网络上主机的性能。大多数情况下，由于某主机不是要找寻的目标，所以该主机并不能从处理广播中获益。要么这个主机并不关注广播的服务，要么这个主机已经获知这个服务。有如图5-33所示，大规模的广播辐射会明显地降低主机性能。IP网络中的三个广播和组播的源头分别是：工作站、路由器和组播应用程序。

每当需要定位一个不在ARP表中的MAC地址时，工作站就会广播一个地址解析协议（ARP）请求。比如，“telnet mumble.com”命令通过域名系统（DNS）解析出IP地址，然后就会广播ARP请求来寻找实际的工作站。通常，IP工作站会缓存大约2小时10至100个地址。一个典型的工作站的ARP速率可能在每2小时50个地址左右，折合每秒0.007个ARP请求。换言之，如果有2000个IP端点，每秒钟将会产生约14个ARP请求。

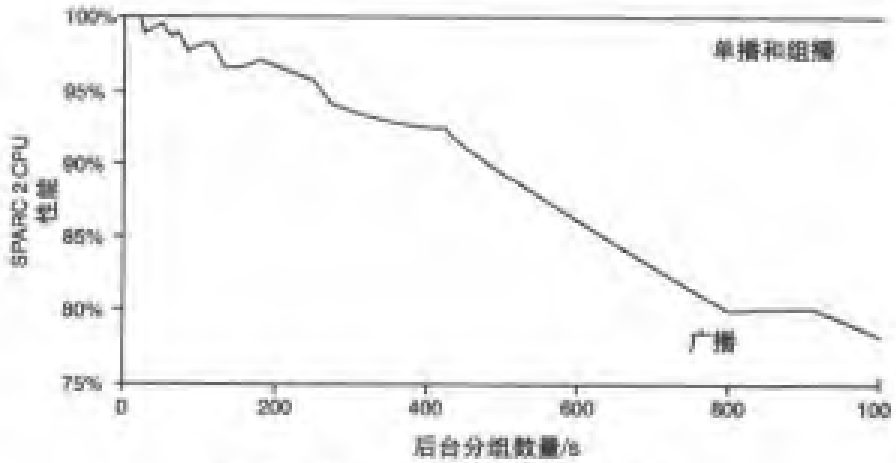


图5-33 IP网络中广播辐射对主机的影响

表5-7列出了在IP网络中广播和组播的平均数量。

表5-7 IP网络中广播和组播的平均数量

主机数量	平均每台主机的CPU耗费率
100	0.14
1000	0.96
10,000	9.15

尽管表5-7中的数据看起来可能挺小的，它们所表示的是一个设计良好的IP网络的平均情况，并且该网络上没有运行路由选择信息协议（RIP）。由于广播风暴的原因，广播和组播通信达到峰值时，CPU的耗费峰值可能比平均耗费值大几个数量级。广播风暴可能会由来自某个变得非常巨大的

网络的设备请求信息而引起。大量的应答被送回到原始的请求处而设备却不能处理它们，或者由于第一个请求引发其他设备的相似请求从而显著阻隔网络中正常的通信流。

IP路由器是指运行任何距离矢量路由选择协议的路由器或工作站。一些管理员配置所有的工作站运行RIP协议（一种路由选择协议）作为冗余可达策略。RIP协议每30秒就会使用广播将整个RIP路由选择表重新传递到其他RIP路由器上。如果有大量的路由器都配置运行RIP协议，而平均每个路由选择表有50个分组需要传送，那么路由器将会每秒钟产生3333个广播。大部分的网络管理员只配置少量的（一般是5到10个）路由器运行RIP协议。假定每个路由选择表有50个分组大小，10个运行RIP协议的路由器每秒钟将产生大约16个广播。路由选择协议和路由选择表将在第8章"路由基础和子网"中讨论。

IP组播应用对大型、可扩展、交换网络的性能有负向作用。虽然组播是向同一共享介质Hub内的大量用户发送多媒体数据流的有效方案，但它对平面交换（flat-switched）网络的每一用户都有影响。平面交换网络是指用交换机互联起来的，未采用第3层的路由或者类似手段的网络。在交换网络中，一个特定的分组视频应用可以产生约7MB的组播数据流，这些数据流将会被传送到每个分段，导致严重的拥塞现象。

5.3.6　广播域

*广播域（broadcast domain）*是指由第2层设备所连接的一组冲突域。将局域网分成多个冲突域，允许在分开的冲突域上同时进行多重数据传播提高了网络的性能。不过如果广播在通过第2层设备的时候超过了设备的负荷就会降低整个局域网的性能。必须在第3层上进行广播的控制，因为第1层和第2层设备对广播都没有办法控制。整个广播域的大小可以通过辨别所有那些传递相同广播帧的冲突域来得到。换言之，所有的节点都是由第3层设备作为分界的网络分段的一部分。广播域能被第3层设备所控制，因为路由器不转发广播。如图5-34所示，从左边蓝色突出显示的工作站发出的广播不会被路由器转发到右边的主机去。

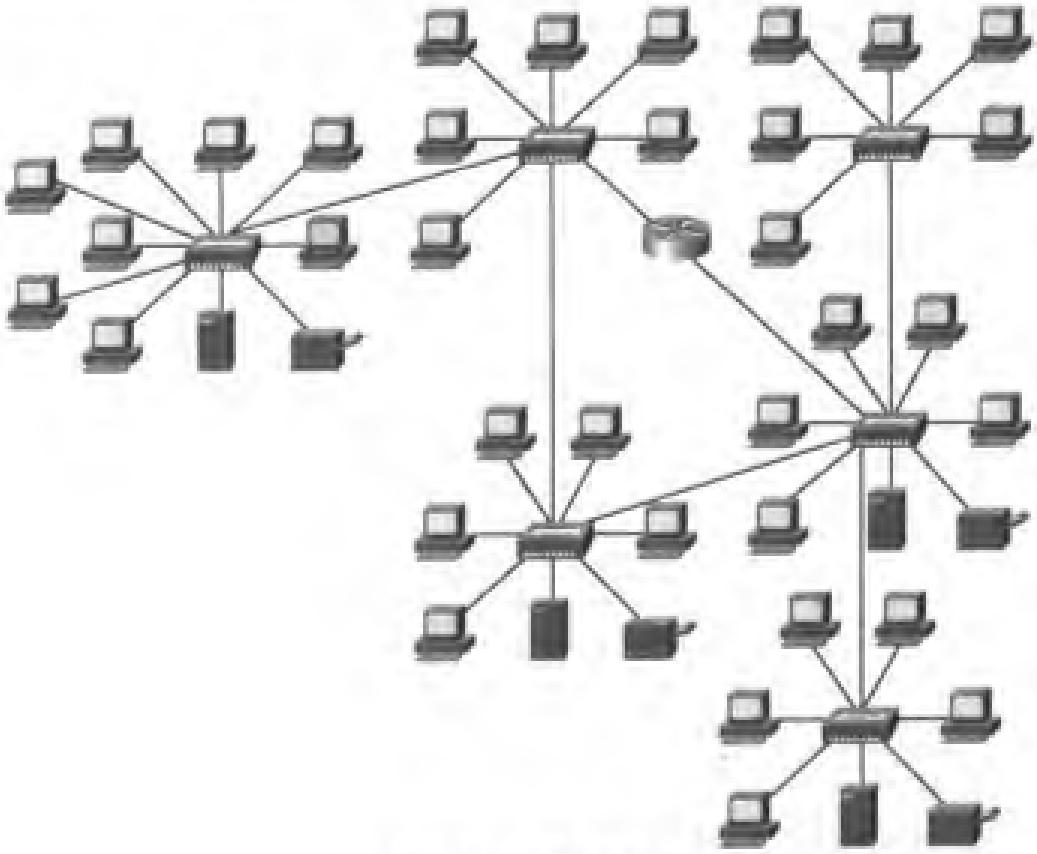


图5-34　广播域分段

路由器事实上工作在第1、2和3层。同所有的第1层设备一样，路由器具有到介质的物理连接并能在介质上传输数据。它们在所有的接口上具有第2层的封装，并与任何的第2层设备一样执行工作。第3层的技术允许路由器把广播域分段。

对于要通过路由器转发的分组，一定已经由第2层设备处理过了，其帧信息必然已经被剥离了。第3层的转发是基于目标IP地址而不是MAC地址。对一个要转发的分组信息，必须包含处于局域网分段地址范围外的IP地址，同时路由器上的路由选择表中有该分组应送达的目标位置。

5.3.7 数据流介绍

冲突域和广播域范围内的数据流关注的是数据帧怎样通过网络传播。它涉及到数据在第1层、第2层和第3层设备中的移动，以及要有效地完成数据传播必须如何对数据进行封装。记住数据都是封装了的，在网络层封装了IP源地址和目的地址，在数据链路层封装了MAC源地址和目的地址。

这里要遵从的基本规则是，第1层设备总是转发帧，第2层设备想要转发帧（换言之，它总是转发帧，除非有什么东西不让它转发），第3层设备一般不转发帧除非要求它转发。使用这个规则可以帮助识别数据流是如何通过网络的。

第1层设备（像中继器和集线器）不对数据过滤，它们将收到的所有东西都转发到下一分段。帧只是简单地重新产生和重新定时，并回到原始的传输质量。

第2层设备（像网桥和交换机）根据目标MAC地址对数据帧进行过滤。如果一个帧的目标地址未知（即在冲突域之外），那么它就会被转发。如果帧是一个要到本冲突域外的广播、组播或者单播，它也会被转发。仅当第2层设备发现发送主机和接收主机在同一冲突域时帧不会被转发。桥接设备（第2层设备）形成多个冲突域但只有一个广播域。

第3层设备（路由器和一些高端交换机）根据目标IP地址对数据帧过滤。惟一要转发分组的情况是目标IP地址位于广播域之外且路由器能辨别出要发送的分组的目标位置。第3层设备形成多个冲突域和多个广播域。

数据流通过基于被路由IP的网络涉及到数据在位于OSI模型中的第1层、第2层和第3层设备的通信管理设备之间的移动问题。通信管理设备包括：第1层设备用来实现在物理介质上传输，第2层设备用来管理冲突域，第3层设备对广播域进行管理。图5-35所示为数据流从工作站X经过路由器A、

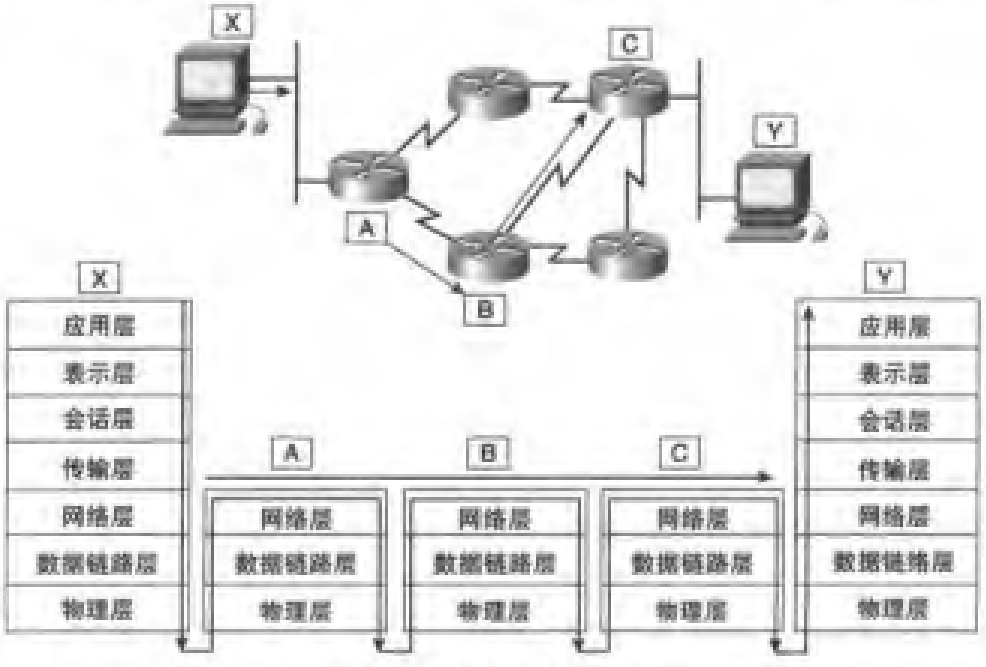


图5-35 数据流通过网络

B和C到达工作站Y的过程。

5.3.8　网络分段

像许多的术语和缩略词一样，*分段*（*segment*）有多重的含意。字典上对这个术语的定义如下：

- 某种东西被分割后的片断。
- 某个被自然边界或类似的东西分开或者划分的实体或者数量的一部分。

在数据通信范围内，使用的是如下的定义：

- 由网桥、路由器或者交换机作界限划分的网络段。
- 使用总线拓朴的局域网中的一段连续的电子电路，它往往是使用中继器来与其他这样的分段连接的。
- TCP规范中使用的术语，用来描述信息的单个传输层单元。其他的术语像数据报（datagram）、帧（frame）、消息（message）和分组（packet）也用于描述位于OSI参考模型中不同层次和不同技术派系中的逻辑信息分组。

图5-36表示了在数据通信领域内关于术语*分段*（*segment*）的3种定义。

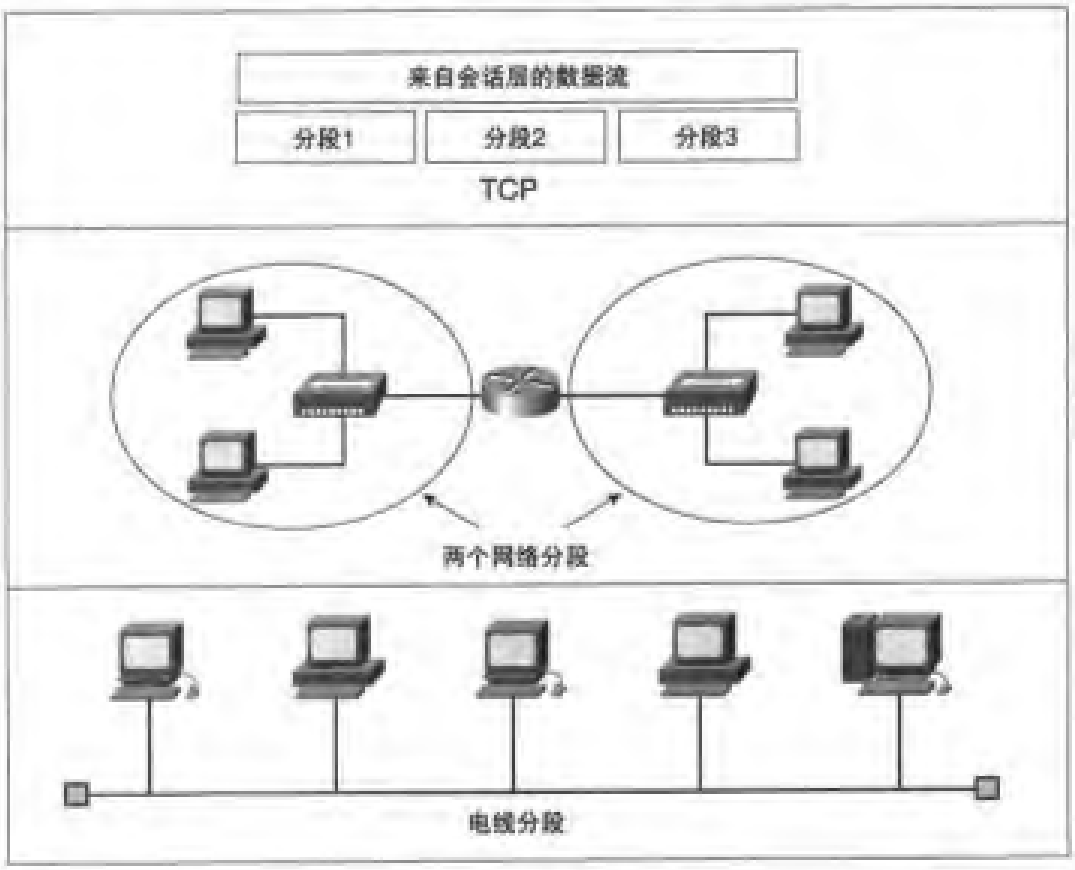


图5-36　分段

要给*分段*这个术语一个恰当的定义，需要给出这个单词使用的范围。如果分段是在TCP范围使用的话，它被定义为分开的数据片断。如果*分段*是在被路由网络中的物理网络介质相关内容中使用的话，它被看做整个网络的一部分或者一段。

5.4　总结

本章学习了以下知识点：

• 电气与电子工程师协会（IEEE）是定义网络标准的专业组织。IEEE的局域网标准是广为人知的IEEE通信标准，也是当今世界主要的局域网标准。

• IEEE将OSI的数据链路层划为两个独立的子层：介质访问控制层（MAC）和逻辑链路控制层（LLC）。

• 以太网用到MAC地址，即网络接口卡上的物理地址。

• 使用帧可以帮助获得那些关键的信息，这些关键信息不能通过单独使用比特编码流获得。

• 关于介质访问控制的两个广义分类：确定性（依次进行）和非确定性（先到先服务）。

• 以太网使用载波侦听多址/冲突检测（CSMA/CD）。

• 半双工传输允许信号双向传输，但不能同时在两个方向进行。全双工传输允许同时发送和接收数据。

• 共享介质环境可能导致通信拥塞而使网络效率变低。

• 以太网中最常见的（常常是良性的）错误情况是冲突。

• 能够通过协议分析会话获取的主要的以太网帧错误类型是局部冲突、远程冲突和后期冲突。

• 被认为是以太网错误的情形是逾限（jabber）、长帧（long frame）、短帧（short frame）、残帧（runts）、帧检验序列错误（FCS error）、调节错误（alignment error）和范围错误（range error）。

• 共享介质环境中的设备基本集合是冲突域。

• 冲突域可以被分段以减小拥塞和增加网络效能。

• 冲突域能够被第2层和第3层设备分段。

• 广播被设计得可以通过冲突域，它能够提高网络性能。

• 广播域可以被第3层设备分段。

• 联合使用第2层和第3层设备进行数据封装能控制数据流。

• 网络术语和缩略词必须在一定的上下文中定义，而不是在独立的环境下定义。

作为对本章所学内容的补充，请参考随书附送的CD-ROM上与本章相关的视频、插图和e-Lab实验活动。

5.5　关键术语

10吉比特以太网（*10-Gb Ethernet*）　建立在以太网技术上，在今天大多数的局域网当中都有应用。10吉比特以太网被描述为这样一种技术，它提供了更高效、更经济的手段在网络间的骨干连接间传输数据，同时也提供了一种端到端的一致技术。现在可以建设提供数据传输速率在10G bit/s的以太网。

调节错误（*alignment error*）　不是以8bit字节边界（octet boundary）结尾的消息。

后退（*back off*）　冲突发生后强制重发延迟。

广播（*broadcast*）　被发送到网络中的所有节点的数据分组。广播通过广播地址来识别。

广播域（*broadcast domain*）　设备集合，其中的所有设备都可以收到从该设备集合中某个设备发出的广播帧。广播域的边界通常是路由器（或者在交换网络中是VLAN）。因为路由器并不转发广播帧。

冲突（*collision*）　以太网中两个节点同时传输导致的结果。从各自设备发出的帧在物理介质上相遇的时候，就会发生冲突和被损坏。参见冲突域。

冲突域（*collision domain*）　以太网中冲突的帧得以传播的网络区域。中继器和集线器都会传播冲突，而局域网交换机、网桥和路由器则不会。

无连接（*connectionless*）　不需要虚电路存在的数据传输。

载波侦听多址/冲突检测（*Carrier Sense multiple access collision detect, CSMA/CD*）　一种介质访问机制，其中的设备在传输数据之前首先检查载波通道。如果在特定的时间段内没有探测到载波，该设备就进行传输。如果同时有两个设备进行传输，就会发生冲突并且将被所有发生冲突的设备检测到。然后这种冲突使得这些设备延迟随机长度的时间段来重发数据。CSMA/CD访问用于以太网和IEEE 802.3。

封装（*encapsulation*）　将数据用特定的协议头包装起来。例如，上一层的数据在被网络传输之前会被包装上特定的以太网协议头。同样，当桥接相异的网络时，源自一个网络中的整个帧可以简单地放置于另一个网络的数据链路层协议头后面。

以太网（*Ethernet*）　一种基带局域网规范，由施乐（Xerox）公司发明，并由施乐、英特尔（Intel）和DEC公司所发展。以太网使用CSMA/CD技术，可以10、100或1000Mbit/s运行各种电缆。以太网类似于IEEE 802.3系列标准。

快速以太网（*Fast Ethernet*）　许多100Mbit/s以太网规范中的任何一种，快速以太网提供比10BASE-T以太网规范快10倍的速度，同时保留了帧格式、MAC机制和MTU这样的性质。这些相似之处允许已有的10BASE-T应用和网络管理工具也能在快速以太网中使用。快速以太网是在IEEE 802.3规范的基础上扩展形成的。

光纤分布数据接口（*Fiber Distributed Date Interface, FDDI*）　一种局域网标准，由美国国家标准协会（ANSI）3T9.5制订。它要求是使用光缆，传输距离能达到2km的100Mbit/s的令牌环网。FDDI采用双环结构提供冗余。

全双工（*full duplex*）　指发送方和接收方可以同时传输数据的性能。

幽灵（*ghost*）　由Fluke网络公司创造的新术语，该术语指的是在电缆中探测到的能量（噪声），该噪声看起来像一个帧但是缺乏正确的SFD。要鉴别是否幽灵，该“帧”必须至少要有72个8bit字节长（包含前导符在内）。否则，将被当作是远程冲突。

吉比特以太网（*Gigabit Ethernet*）　高速以太网标准，1996年由IEEE 802.3z标准委员会核准。

半双工（*half duplex*） 指发送方和接收方之间同时只能有一个方向的数据传输的性能。

报头（*header*） 在对需要进行网络传输的数据进行封装时，放置在数据前面的控制信息。

IEEE 802.2 IEEE的局域网协议，其中对数据链路层的LLC子层进行了详细说明。IEEE 802.2负责处理错误、帧、流控制和网络层（第3层）服务接口。

电气与电子工程师协会（*IEEE*） 专业组织，其活动包括制订通信发展和网络标准。IEEE的局域网标准是现在主要的局域网标准。

IEEE 802.3 IEEE的局域网协议，其中定义了物理层和数据链路层的MAC子层。IEEE 802.3对不同物理介质上的不同速率的访问采用CSMA/CD技术。IEEE 802.3的扩展标准定义了快速以太网。最初根据物理介质不同，IEEE 802.3制订了包括如下的规范：10BASE2，10BASE5，10BASE-F，10BASE-T和10BROAD36。快速以太网不同物理介质下的规范包括100BASE-TX和100BASE-FX。

逾限（*jabber*） 在802.3标准中有几处进行了定义，指在短时间内传输至少20,000到50,000 bit-time。不过，许多诊断工具只要检测到传输超过了最大合法的帧尺寸就会报逾限错误，这个尺寸可能比20,000到50,000 bit-times小得多。

逻辑链路控制（*Logical Link Control, LLC*） 由IEEE定义的两个数据链路层子层的较高一层。LLC子层处理错误控制、流控制、帧和MAC子层寻址。最流行的LLC协议是IEEE 802.2，它包括无连接和面向连接两种。

长帧（*Long frame*） 指帧的长度超过了最大合法的尺寸，无论该帧是否已被标记都将被考虑为长帧。

介质访问控制（*Media Access Control, MAC*） 由IEEE定义的两个数据链路层子层的较低一层。MAC子层处理共享介质访问，比如是进行令牌竞争还是进行传递。参见LLC。

MAC地址（*MAC address*） 连接到局域网的每个设备都需要的标准数据链路层地址。网络中的其他设备通过这个地址来定位该网络中的设备和建立及更新路由选择表和数据结构。MAC地址有6 字节长，由IEEE进行控制。它也被称为硬件地址、MAC层地址或者物理地址。

最大传输单元（*Maximum Transmission Unit, MTU*） 特定接口可以处理的以字节为单位的最大分组尺寸。

组织惟一标识符（*Orgnizationally Unique identifier, OUI*） 一批48 bit的局域网地址中由IEEE分配的三个8 bit字节。

传播延迟（*Propagation delay*） 数据从源传输到最终目标位置所需要的时间。

范围错误（*range error*） 其长度域包含的值是合法的尺寸，但是在接收到的帧的数据域中所包含的实际8bit字节数却与该长度值不相符。

分段（*segment*） 以网桥、路由器或者交换机作为边界的一段网络。

单工（*simplex*） 在发送点和接收点之间只能有一个方向进行传输。广播电视就是单工技术的一个实例。

简单网络管理协议（*Simple Network Management Protocol, SNMP*） 几乎是TCP/IP网络专用的网络管理协议。简单网络管理协议提供方法监测和控制网络中的设备，以及管理配置信息，并提供统计数据的收集、性能和安全性。

令牌环（*Token Ring*） IBM开发维护的一种令牌传递局域网。令牌环网是环状拓扑，速率是4M bit/s或者16M bit/s。

尾（*trailer*） 对进行网络传输的数据进行封装，加在数据尾部的控制信息。

5.6 复习题

请通过完成下面所有的复习题来检查你对本章主题和概念的理解程度。答案列在附录C “复习题答案”中。

1. 下面哪个不是被当成IEEE的子层之一？
   A. 介质访问控制层
   B. 数据链路层
   C. 逻辑链路层
   D. 以上都不是
2. IEEE子层与OSI参考模型中的哪层相关？
   A. 2和3
   B. 1和2
   C. 3和4
   D. 1和3
3. 子层中的LLC，执行 _____ 进程。
   A. 加密
   B. 封装
   C. 分组
   D. 以上全部
4. MAC地址的前6个16进制数代表 _____ 。
   A. 接口序列号
   B. 组织惟一标识符
   C. 接口惟一标识符
   D. 以上都不是
5. MAC地址有 _____ 位长。
   A. 12
   B. 24
   C. 48
   D. 64
6. 解释以太网工作的访问方法的名称是？
   A. TCP/IP
   B. CSMA/CD
   C. CMDA/CS
   D. CSMA/CA
7. MAC地址位于？
   A. 收发器
   B. 计算机BIOS
   C. NIC
   D. CMOS
8. 下列哪个叙述将局域网中两台设备之间的通信描述得最好？
   A. 源设备将数据封装在帧中并传送出去，该帧包含有目标设备的MAC地址。局域网中的每个人都可以看到，但那些地址不匹配的设备将忽略该帧。
   B. 源设备封装数据并将目标MAC地址放到帧里。源设备将帧放于局域网中，只有地址匹配

的设备可以检查其地址域。

C. 目标设备将数据封装在帧中并将帧放到局域网中，该帧含有源设备的MAC地址。地址匹配的设备取走该帧。

D. 局域网中的每个设备都收到帧并将该帧传递下去，由软件决定是保留还是丢弃该帧。

9. 哪些功能与帧有关？

A. 确定哪些计算机在相互通信

B. 不同计算机之间的通信信号的开始时间和结束时间

C. 出错帧的标志

D. 以上全部

10. 局域网上的计算机如何判断帧中的错误？

A. 它复制一份帧送回到发送者来验证。

B. 它检查目标地址来验证该帧确实是有意给它的。

C. 它检查帧中的FCS与计算机从帧内容计算出来的是否一致。

D. 它计算出帧中数据的校验和然后送回到源进行验证。

11. 介质访问控制是指什么？

A. 网络接口卡获取了网络介质，可以进行传输的状态。

B. 支配介质抓取和释放的原则。

C. 决定在共享介质环境中的计算机是否被准许传输数据的协议。

D. 已被传输的正式的字节序列。

12. 下面哪个描述最符合CSMA/CD网络？

A. 一个节点的传输内容在整个网络中传送，网络上每个节点都接收和检查该内容。

B. 如果发送源知道目标的MAC地址和IP地址，信号会被直接传到目标位置。

C. 一个节点的传输内容到最近的路由器，由路由器将其直接发给目标。

D. 信号总以广播模式发送。

13. 在以太网或者IEEE 802.3局域网中，什么情况下会发生冲突？

A. 当一个节点在没有通知其他节点的情况下就放置一个分组在网络中时。

B. 当两台主机侦听流量信息，都侦听到没有流量，于是同时传输数据时。

C. 当网络中两个节点向一个不再广播的节点发送分组时。

D. 当检测到抖动，正常传输过程的通信被中断时。

14. 下列哪一个是第2层数据链路层的重要功能？

A. 逻辑链路控制

B. 寻址

C. 介质访问控制

D. 以上全部

15. 下列哪个是以太网帧错误类型？

A. 本地冲突

B. 远程冲突

C. 后期冲突

D. 以上全部

16. 那个协议是非确定性协议？

A. 令牌环

B. CSMA/CD

C. IPX
D. RIP

17. 关于确定性MAC协议哪个说法是正确的?
A. 它定义了冲突并说明冲突发生时需要怎么做。
B. 它允许集线器在任何一个时间检查活动用户的数量。
C. 在传输数据时它允许主机“排队”发送数据。
D. 它使用网络管理员提供的“发言棒”来控制任何被认作是“麻烦制造者”的用户的介质访问。

18. 数据分组产生和冲突的网络区域被称为 _____ ?
A. 冲突域
B. 网络域
C. 广播域
D. 网络分段

19. 下列哪个描述广播最准确?
A. 同时传送一个帧到多个主机。
B. 同时传送一个帧到所有的路由器来更新它们的路由选择表。
C. 同时传送一个帧到所有的路由器。
D. 同时传送一个帧到所有的集线器和网桥。

20. 使用中继器会 _____ 冲突域。
A. 减少
B. 不影响
C. 扩展
D. 以上都不是

21. 使用复杂的网络设备，像网桥、交换机和路由器来划分冲突域的过程被称为:
A. 分节
B. 分段
C. 减小冲突域
D. 以上都不是



第6章　以太网技术和以太网交换

目标

学习完本章之后，你应该能够：

- 了解以太网技术的发展。
- 了解以太网技术的介质访问控制方法、帧结构和传输过程。
- 了解在每种以太网技术中使用的特定介质和编码。
- 了解每种以太网技术的插脚引线和线缆类型。
- 了解每种以太网技术基本的架构考虑。
- 定义微分段。
- 描述第2层桥接。
- 描述局域网交换操作是怎样进行的。
- 描述全双工传输。
- 分辨普通的交换方法：直穿式交换（cut-though switching），存储和转发交换（store-and-forward switching）和分片隔离交换（fragment-free switching）。
- 描述生成树协议的功能和特征。
- 描述生成树协议是怎样工作的。
- 描述不同的生成树端口状态。

以太网及其相关的IEEE 802.3协议，是世界上最重要的网络标准之一。因为早期以太网取得了巨大成功并且其设计完整健全，所以随着时间的推移它逐步发展成型，这个发展是由现代局域网发展的需要引起的。并且以太网很可能会继续发展来满足网络性能将来的需求。

前一章介绍了以太网的历史和以太网相关的标准。同时还学习了术语*以太网*及其所涉及的一系列以太网技术。本章将进一步讨论以太网技术细节。

另外，本章介绍了第2层桥接和交换技术。交换和桥接技术通过减少通信量和增加带宽的方式，减少了局域网中发生拥塞的现象。

最后，本章介绍了生成树协议（STP），讲述了STP是怎样工作的以及STP交换端口状态。

请务必在本书配套的光盘中查看与本章相关的e-Lab实验活动、视频和插图。这些光盘资料提供

了补充材料，能够强化本章中涉及的概念。

6.1　10Mbit/s和100Mbit/s以太网

本节介绍几种最重要的以太网细节。本节的目的不是要求去记住各种以太网的方方面面，而是培养一种感觉，这种感觉要求对各种类型的以太网的共同点是什么以及对商业上重要的各种形式的以太网的优缺点分别是什么要清楚。

随着粗同轴电缆10BASE5的出现，以太网开始普及。然而，粗缆的安装性能并不令人满意。10BASE2使用的是细缆——细一点的电缆，从而更容易安装和折断；安装距离则由500m降到185m。便捷的安装和廉价的投入是一种趋势，以非屏蔽双绞线（UTP）为基础的10BASE-T的引入，使得这种趋势带来了以太网发展的大飞跃。然而，非中继信号使传输的长度降到了100m，迫使中继器出现，然后是多端口中继器即集线器（hub）的出现。中继器的概念使得10BASE-T网络能够长达500m。随着工作组大小的增加和应用复杂程度的增长，共享带宽的集线器成为了限制因素。在10BASE-T以太网中引入交换，既解决了长度问题又解决了带宽限制——工作站与交换机的连接现在成了点到点连接。

10BASE-T强大功能多而又经济划算，带来了局域网用户数量和Internet用户数量爆炸式的增长（同时也增加了局域网的通信量）以及应用复杂度的增加。要求更大带宽的需求增长了，导致快速以太网的产生。使用铜缆的快速以太网被称为100BASE-TX，它在商业应用上很成功，并且其上开发有许多精巧的、与10BASE-T系统互相通用的功能（比如10/100自适应端口的出现）。为了与光纤分布数据接口（FDDI）的主干/局域网技术竞争，引入了使用光纤的100BASE-FX。在以上所有以太网技术中，MAC寻址概念、帧结构和CDMA/CD方法仍然适用。

6.1.1　10Mbit/s 版本以太网

图6-1表示的是以太网物理层实现方式的子集。在后面章节中，以太网形式10BASE5、10BASE2和10BASE-T被称作是传统的实现方式。



图6-1　以太网的类型

这些传统的以太网有四个共同点：

- 计时参数。
- 帧结构。
- 传输过程。
- 基本设计准则。

了解这三个重要的历史性版本的共性之后，就可以对它们分别做更详细的调查。

10BASE5、10BASE2和10BASE-T都具有相同的计时参数，如表6-1所示。注意10Mbit/s 的1bit时间 = 100ns = 0.1μs = 千万分之一秒。

表6-1　10Mbit/s以太网运行的参数

参数	值
bit时间	100ns
时隙	512个bit时间
帧间距	96bits*
冲突重试限制	16

续表

参数	值
冲突回退限制	10
冲突堵塞尺寸	32bits
最大未标记帧尺寸	1518个8bit字节
最小帧尺寸	512bits（64个8bit字节）

*列出来的值是官方的帧间距数值

帧结构对10BASE5，10BASE2和10BASE-T是共通的。图6-2所示为在MAC子层观察到的以太网帧结构。

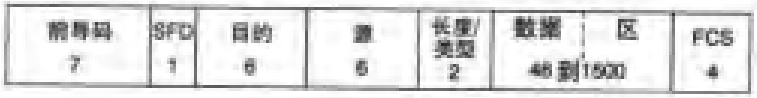


图6-2 以太网帧

传统以太网的传输过程在OSI物理层的低端部分是一致的。随着帧从MAC子层传到物理层，把bit从物理层送到介质上之前会被进一步处理。这个阶段的一个特别重要的过程是信号质量错误（SQE）信号。这种信号是在许多网络技术中都可以看到的典型信号。在物理层，为了保证网络功能正常，与用户数据不一样，网络通信是“时时进行”的。SQE总是用于半双工；在全双工操作中SQE不是必需的但是允许使用。SQE在下列情况下存在：

- 在正常传输后面的4ms到8ms时间里，用来指示边界帧已经将被成功传输。
- 介质中发生冲突的时候。
- 介质中有不正确信号的时候。不正确的信号可能包括监测到的逾限（jabber），或者由于线缆失效导致的反射，比如短路的时候（根据使用的介质不同会有不同的情况）。
- 任何传输被当作逾限（jabber）而中断的时候——就是说，它比允许的传输内容传得更长。

所有形式的10 Mbit/s以太网从MAC子层取得8bit字节并执行一个被称为是*线路编码*（*line encoding*）的过程。线路编码描述了bit在线路中实际是怎样用信号来表示的。最简单的*编码*（例如*不归零码*，即NRZ，它的1对应5伏特，0对应0伏特）往往都有不太理想的计时和电学特性。因此，线路编码被设计得具有良好的传输特性并适合每种介质。在10Mbit/s系统中使用的线路编码形式被称为*曼切斯特编码*（*Manchester encoding*）。图6-3显示的是一个曼切斯特编码的例子。其y轴表示电压；x轴表示时间。

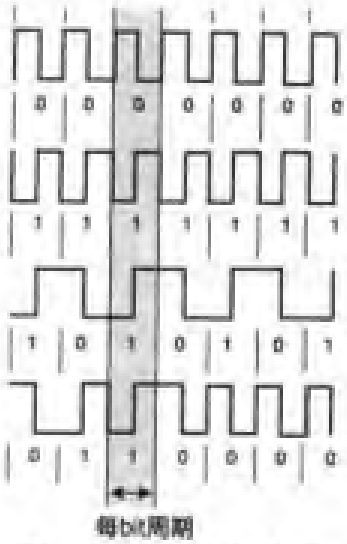


图6-3 曼切斯特编码例子

注释：在不归零码（NRZ）编码中，如果在bit间隔之间没有信号传输，信号将维持在恒定的电压上（不恢复到0V）。

*曼切斯特编码*根据时间窗口中部的沿转换方向来确定该bit间隔的二进制值。在图6-3所示的编码例子中，有一个时间窗口被突出地垂直标示在所有这4个波形示例上。最上面的波形在时间窗口的中部是一个下降沿（falling edge），所以它被标记为0。

第二个波形的结果是在时间窗口的中部有一个上升沿（rising edge），所以它被记作1。

在第三个波形例子中不是使用同样二进制数值的重复序列，而是使用交错二进制序列。在前两个例子中，信号必须回到bit周期（bit period）之间以便于每次在时间窗口中部都是同一方向的变换。对于交错二进制数据，没有必要转变回到原来的电压水平来为下一次时间窗口中部的变换做准备。因此，只要一个沿和下一个沿之间有一个长的间隔，就可以认为这两个沿代表的都是时间窗口中部的情况。第四个波形的例子是一组随机数据，用来验证在两次变换之间随时会有一个宽的间隔，这

两个沿在时间窗口的中部，都代表了时间窗口的二进制值。

传统以太网（10Mbit/s）有一些共同的结构特性。所有的这些传统版本都被当作共享介质以太网，因为它们都共享同一个冲突域。它不仅仅允许，还预期一个以太网有多种类型的介质（例如，10BASE5，10BASE2，10BASE-T，等等）。它的标准制订就是要保证互用性的维持。然而，在实施一个混合介质网络时，特别注意整体结构的设计非常重要。当网络膨胀并且变得越来越复杂，很容易就会超过最大延迟限制。计时限制根据以下几个参数来确定：

- 线缆长度和传输延迟。
- 中继器延迟。
- 收发器延迟（包括网络接口卡、集线器和交换机）。
- 帧间间隙收缩。
- 站间延迟。



实验活动　波形解码

这个实验的目的是通过解码一个以太网帧的数字波形，将以下方面的知识结合起来：网络介质、OSI模型的第1、2和3层以及以太网的知识。

5-4-3原则

10Mbit/s以太网由于计时限制，不能连续使用超过4个中继器，不能超过五个分段。也就是说，这个系列的任意两台远程站点之间连接不能超过4个中继器。同轴实现还有更严格的要求，在任意两台远程站点之间不能超过3个组装分段（populated segment）。另外两个分段是允许同轴分段用来扩展冲突域直径的，被称为是连接分段（link segment）。连接分段的主要特点是它严格地只与两个设备相连。所有的双绞线连接，比如10BASE-T，都符合连接分段的定义。

6.1.2　10BASE5

早期的（1980年）以太网产品（10BASE5）在单根粗同轴电缆总线上传输10Mbit/s，被称之为*粗电缆网（Thicknet）*。10BASE5的重要性有其历史原因：它是第一种被以太网使用的介质。10BASE5是原始802.3标准的一部分。现在还能看到它作为传统安装（legacy installation）的一部分存在。它不是新建网络的首选，因为它的主要优点即长度可以通过其他方式获得。虽然10BASE5系统并不昂贵也不需要进行配置（它不需要使用集线器来扩展系统的长度），但是其基本的部件像网络接口卡很难找到，并且该技术对线缆中的信号反射非常敏感。另外，10BASE5系统非常依赖整个冲突域上的线缆，因此呈现一大的单点故障。

计时、帧结构和传输过程在前面第5章“以太网基础”中已经讲述，它们对所有10Mbit/s传统以太网都是相同的。10BASE5在粗同轴电缆上使用曼切斯特编码信号。图6-4是一个10BASE5信号的

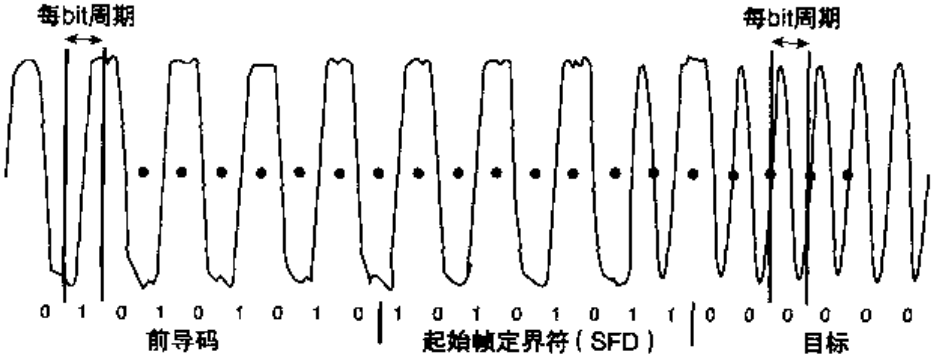


图6-4　10BASE5信号解码

例子。它通过大约0V到-1V的电平来传输。如果没有站点要传输数据，10BASE5的电压可能数天中都为零（0V）。10BASE5是异步的。

在图6-4中，为了帮助辨别计时窗口，加入了计时标记，二进制数据从该窗口开始被解码。图中的y轴表示电压；x轴表示时间。电压是同轴电缆从中心导体到外部覆盖层开始测量的。

如图6-5所示的10BASE5粗同轴电缆，有一个固体的中心导体，其最小名义传输速率（NVP）是0.77c，其最小阻抗（impedance/termination resistance）是50Ω；它使用N型旋接接口。五个分段的粗同轴电缆每个都取最长，可以到500m（合1640英尺）长，站点通过同轴电缆连接到收发器，同轴电缆的附加单元接口（AUI）线缆长度可以到50m（合164英尺）。虽然线缆又粗又沉，安装起来很困难，但是它的长度限制令人满意，这使得它还能在某些应用上使用。



图6-5 10BASE5粗电缆网线缆

10BASE5线缆的其他规范或限制如下：

- 同时只有一台站点可以传输数据（否则会发生冲突）。
- 在CSMA/CD规则下，10BASE5只能在半双工模式下工作。
- 包括中继器在内，在任何单独的10BASE5分段上总共可以有100台站点存在。

6.1.3 10BASE2

10BASE2（原来的802.3a-1985）在1985年被引入。因为同10BASE5相比，它的线缆有较小的尺寸，较轻的重量和更大的灵活性，使得它在安装时更加容易。因为它使用的是细一点的线缆，所以10BASE2常常被称为是细电缆网。10BASE2仍然在传统网络中使用。虽然现在没有什么理由还去安装10BASE2网络，其低廉的花费和不需要集线器仍然富有吸引力。虽然获得网络接口卡变得越来越困难，不过本质上10BASE2不需要什么配置。就像10BASE5系统一样，10BASE2系统在整个冲突域上对线缆非常依赖，并呈现一个大的单点故障。

计时、帧结构和传输过程在前面第5章已经描述，并且这些对所有的10Mbit/s的传统以太网都是一样的。

10BASE2在细线缆上使用的是曼切斯特编码信号。一个10BASE2信号传输电平从大约0V到-1V（其中y轴是电压；x轴是时间。电压是从中心导体到外部屏蔽导体来测量的）。如果没有站点要传输数据，10BASE2的电压可能数天中都为零（0V）。10BASE2是异步的。

就像项链上的珠子一样，局域网中的计算机被一段段连续的同轴线缆连起来。这些一段一段的同轴线缆被同轴电缆连接件（British Naval Connector, BNC）连接到网络接口卡上的T型接头上，如图6-6所示。这个单根同轴缆线是网络的共享总线。工作站可以很容易地移去和重新连接，新的工作站也可以很容易地加入进来。另外，10BASE2同样使用最初的以太网半双工协议。

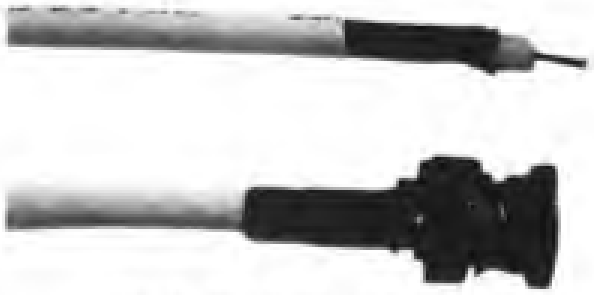


图6-6 细缆线网和BNC连接头

如图6-6所示的10BASE2的细同轴缆线，有一个被包住的中心导体（当订购新线缆时，请确保列出这种包心导体。一些安装者发现这种导体很难操作，可能的时候就会换成固体心的线缆）。它的最小名义传输速率（NVP）是0.65c，有50欧姆的阻抗（impedance/termination resistance），使用的是BNC的T型接头。五个分段的细同轴电缆每个都取最大，可以到185m（合600英尺）长，每一个站点由BNC的T型接头直接连接到线缆上。

6.1.4　10BASE-T

10BASE-T（原来的802.3i-1990）使用又便宜又便于安装的UTP铜线缆替代同轴电缆。这种线缆插到一个中心连接设备（集线器或者交换机）上，该设备再连接到共享总线上。在10BASE-T中使用的线缆的类型，从集线器能够延伸出来的线缆距离，UTP安装、互连以及测试的方法，在“结构化布线系统”中做了规范，该规范中逐步定义了星型或扩展星型拓扑。10BASE-T原来使用半双工协议，不过后来加上了全双工特性。在90年代，以太网呈爆炸式的流行就是使用5类UTP线的10BASE-T，这个时候也正是以太网成为局域网的主流技术的时候。要重新认识网络拓扑和网络介质，请参考第2章“网络基础”和第3章“网络介质”。

计时、帧结构和传输过程在前面已经描述，并与所有的10Mbit/s传统以太网是一致的。

10BASE-T在3类线（现在是5类线，超5类线，或者更好的线）上使用的曼切斯特线路编码信号。

10Mbit/s以太网是异步的，在传输间歇，线缆上常常很长时间都是完全空闲的（0V）。10BASE-T连接大约每125ms产生一个*链路脉冲（link pulse）*（8次/s），其他时候都是空闲的。10BASE-T网络由于连接脉冲变“活”了。

10BASE-T使用的非屏蔽双绞线（UTP）每根电线中有一个固态的导体，这些电线放在一个最大90m粗的水平线缆中，电线直径的尺寸应该是0.4mm到0.6mm（合26到22美国电线标准尺[AWG]）。其中10m长的补缀线缆（patch cable）使用相似尺寸的包心线缆来保证耐久性，因为它们会经历反复的弯折。合适的UTP线缆最小名义传输速率（NVP）是0.585c，10欧姆的阻抗，使用在ISO/IEC 8877中定义的8插脚RJ-45标准接头。虽然精确的最大允许线缆长度由连接分段的传输延迟来确定（延迟不要超过1000ns的任何长度都可以接受），不过在站点和集线器之间的线缆通常是0m到100m（合0英尺到328英尺）长。一般情况下，多股线缆中UTP细线直径0.5mm（24AWG）就能满足100m传输长度的要求。

虽然3类线缆对10BASE-T网络来说足够用了，仍要强烈推荐在安装新的线缆时采用超5类线（CAT5e）或者更好的材料和线路实现。要使用所有的4对线，并用T568A或者T568B线缆插脚引线（pinout）排列。使用这种线缆安装方式，可以在同一线缆布局中使用很多不同的介质访问协议（包括1000BASE-T）无须重新布线。

表6-2列出了10BASE-T连接的插脚引线。注意存在两个分开的传输/接收路径（同轴电缆只有一个）。

表6-2　10BASE-T 线缆插脚引线

插脚编号	信号
1	TD+（传送数据，正向微分信号）
2	TD-（传送数据，负向微分信号）
3	RD+（接收数据，正向微分信号）
4	未用
5	未用
6	RD-（接收数据，负向微分信号）
7	未用
8	未用

图6-7所示为两个站点之间概念上和物理上的连接。需要一条交叉线（crossover cable），设备A上的Tx发送信号到设备B上的Rx。注意存在两个点到点的连接（TxA到RxB和TxB到RxA）。

图6-8显示的是主机和中继器、多端口中继器（集线器）或者交换机之间的连接，在路由器和集线器或者交换机之间是同样的连接。采用的是直连线（straight-though cable）。注意在集线器内部是一个总线拓扑，即一个冲突域。当一台工作站用直连线与交换机相连时，所有的连接都是点到点的。交换机的线路构造允许多对端口同时全带宽工作而不发生冲突。

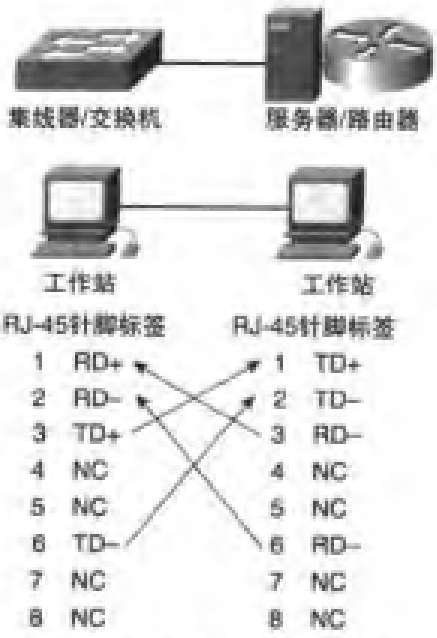


图6-7 10BASE-T站点到站点

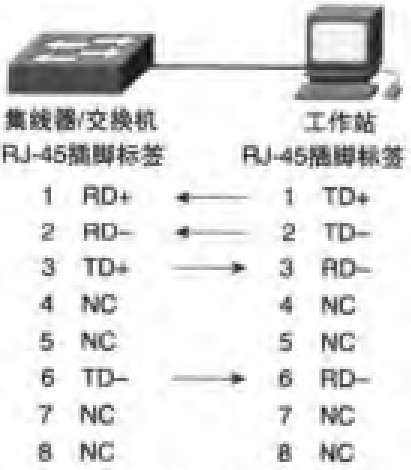


图6-8 10BASE-T直连线

因为站点到站点，交换机到交换机，工作站到交换机的连接都是点到点的连接，它们在两个分开的UTP线对上是物理上分开的两个通信路径/通道。这样的话，冲突就不是物理事件而是决定不允许同时进行发送和接收的结果。因此，不论半双工（遵从CSMA/CD原则）还是全双工（没有物理的冲突发生），只是一个配置选择。大多数时间，你是在全双工下使用这些连接，这样不仅消除了冲突，还将连接的吞吐量（throughput）加倍了。第一次出现的时候，有关的IEEE标准被命名为802.3-1997全双工。然而，工作站到集线器的连接包括集线器内部的总线拓扑，该拓扑是一个实际物理冲突域。因此，由于其自然结构的物理特性，这个连接*只能*使用半双工，并遵从CSMA/CD。

10BASE-T在半双工模式下传输10Mbit/s；然而，在全双工模式下10BASE-T实际上可以20Mbit/s交换数据（虽然这些数据有一部分是开销（overhead），不是用户数据）。当想要增加以太网连接的速度的时候，这个概念会变得越来越重要。

6.1.5 10BASE-T体系结构

10BASE-T连接通常包含站点与集线器或者交换机的连接。集线器可以认为是多端口的中继器，受到远程主机之间连接中继器个数限制的约束。交换机可以看作是多端口的网桥，存在100m长度的限制但是远程主机之间的交换机的数量不受限制。

虽然集线器可以连成一个序列（有时称为菊花链，或者层叠），在可能的时候尽量避免这样安排，以免违反远程主机之间最大延迟的限制。10BASE-T网络的物理尺寸遵从相同的原则，该原则是10BASE5和10BASE2考虑中继器数量时采用的原则。当需要多个集线器的时候，最好是把它们分等级层次安排，采用树状结构而不是链式结构。而且，使用较少的中继器来分开站点能够提高性能。"可堆叠"集线器，或者是可以支持几个多端口适配卡的、有共同背板的集中器，允许有大量的站点连接到设备上，而它在整体上则扮演单个集线器（或中继器）的脚色。菊花链接（daisy-chaining）的交换机很好用，并且不受此限制。

虽然在一个方向上，站点之间的距离被体系结构所限制，但是在站点之间任何距离都是可以的。要考虑的最重要方面的是怎样保持远程主机之间的延迟最小——而不管有关的体系结构和介质类型。较小的最大延迟能提供更好的全局性能。考虑以下的体系结构：

- 在图6-9中，这些路径中从站点1到其他任何站点要经过5个分段和4个中继器。对于10BASE-T

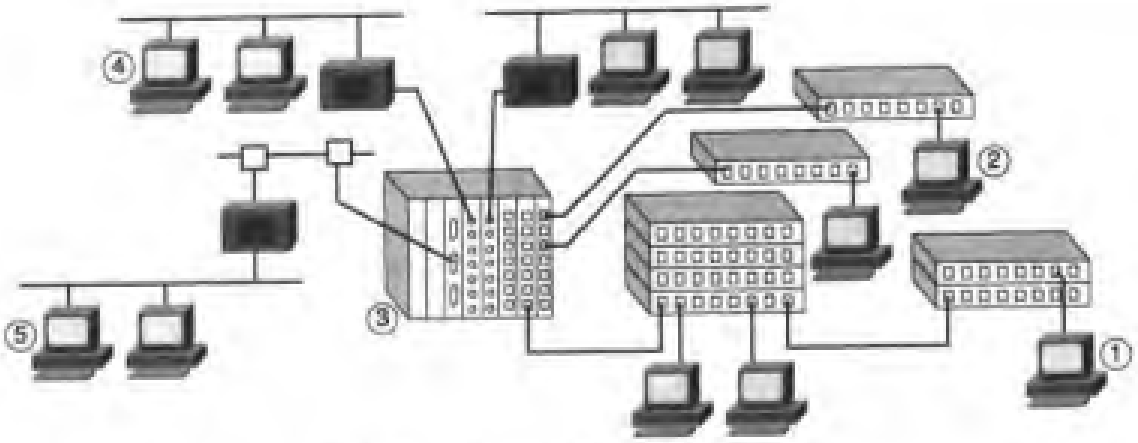


图6-9　10Mbit/s混合体系结构的例子1

连接来说，站点间最大只能有3个分段的限制不适用，因为在同一条线缆上没有其他的站点。所有的链接都记作连接分段（link segment）。

• 在图6-10中，从任何站点（除了站点1以外）到其他任何站点，要经过的路径中只有3个中继器。由于这些替代路径既有10BASE5的又有10BASE2的连接，所以仍要满足其他的要求（比如站点之间只能有三个分段）。

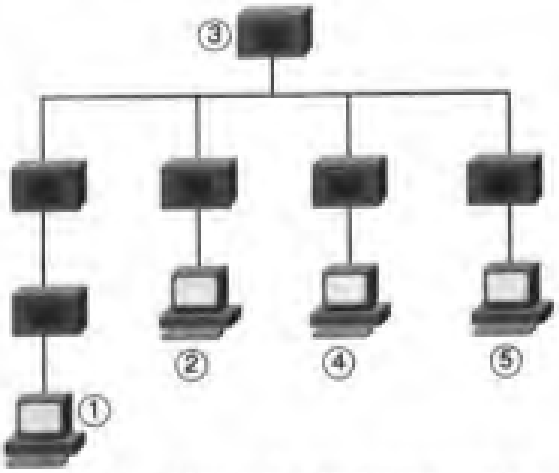


图6-10　10Mbit/s混合体系结构的例子2

10BASE-T连接的非中继距离可以达100m。这个距离看起来很长，但在实际建筑中布线的时候，这个距离往往很快就用光了。使用集线器可以解决这个问题，尽管由于计时的考虑，最大能有4个中继器被连接在一起。广泛使用的交换机使得这个距离限制变得不那么重要了。只要工作站距离交换机在100m以内，这100m的距离是到这个交换机结束的，这个交换机又可以通过另外的100m连接到其他的交换机上，以此类推。由于现在大多数的10BASE-T以太网都是交换的，所以在设备之间有一些实际的限制。环型、星型和扩展星型拓扑都允许使用。问题就变到逻辑拓扑和数据流上而不是计时和距离限制上了。

表6-3显示了10BASE-T连接特性图表。

表6-3　10BASE-T连接特性图表

连接	最大分段
站点到站点、站点到交换机、交换机到交换机	100m，对菊花链没有限制
站点到集线器	100m，受到4中继器原则限制

100Mbit/s版本的以太网

100Mbit/s的以太网，又被称为快速以太网（相比原来的10Mbit/s以太网来说的），是一个系列的技术。在商业上很重要的两种技术是*100BASE-TX*（基于铜质非屏蔽双绞线）和*100BASE-FX*（基于多模光纤）。本小节将考查这两种技术的共同点和各自的特性。

100BASE-TX和100BASE-FX以下3点是相同的：

• 计时参数。

• 帧结构。

• 部分传输过程。

表6-4所示为100Mbit/s以太网操作的参数。

表6-4 100Mbit/s以太网操作参数

参数	值
bit时间	10ns
时隙	512bit时间
帧间距	96bits
冲突重试限制	16
冲突回退限制	10
冲突堵塞尺寸	32bits
最大未标记帧尺寸	1518个8bit字节
最小帧尺寸	512bits（64个8bit字节）

100BASE-TX和100BASE-FX都是一样的参数。注意在100Mbit/s以太网中每bit传输时间是10ns = 0.01ms = 万分之一秒。

100Mbit/s的帧结构与10Mbit/s的帧是一样的。它不像10Mbit/s以太网，10Mbit/s以太网在信号被放到介质上之前所有技术的进程都是一样的。

快速以太网速度上增长了10倍。随着速度的增加产生了额外的需求。比特流传输持续时间变短了并且更频繁了。它们需要更仔细的计时，而且它们的传输频率接近介质带宽限制从而变得更容易受到噪声影响。作为对同步问题、带宽和***信噪比（SNR）***的反应，在100Mbit/s以太网中使用两个分离的编码步骤。使用编码（它被设计得具有良好的特性）的基本思想是为了能更有效地传输用户数据，包括同步，高效的带宽和改良的信噪比特性。编码的第一部分是使用一个被称为是4-bit/5-bit（4B/5B）的技术；第二部分是针对铜缆或者光纤的实际线路编码。

在本课程所考虑的两种100Mbit/s以太网中，即100BASE-TX和100BASE-FX，对MAC子层的上面部分取得的半位元组（nibble，每4bit为一个分组）进行编码。这个4-bit的模式被转换成5-bit的符号；有时这些符号包含控制信息（像开始帧、结束帧和介质空闲条件）。要被传输的整个帧由控制符号和数据符号（数据编码组）组成。此外，所有额外的复杂性对于实现网络速度10倍的增加都是必要的。

在4B/5B编码后，bit（以编码组的形式存在）仍然需要被放到介质上（就是说，它们必须进行线路编码）。进行4bit到5bit的转换同时意味着在同样的时间间隔内现在要传输的是125Mbit/s而不是100Mbit/s。这对介质、发送器和接收器都有更严格的要求。例如，为了保证良好的传输特性，线缆必须在更高频率下进行测试。在没有数据传输的时候，在空闲周期仍要发送“空闲码”组来填充并维持同步。在这个点上，根据所使用的是铜缆（100BASE-TX）还是光纤（100BASE-FX）介质，数据路径分支了。

6.1.6 100BASE-TX

1995年由于对更快速网络的需求导致了100BASE-T快速以太网和自动协商（autonegotiation）标准（原始的802.3u-1995）的发布。100BASE-T使以太网的bit速率增长到100Mbit/s。100BASE-TX是取得商业成功的100BASE-T的5类非屏蔽双绞线版本。很快，10/100自适应集线器和交换机使原来传输速率10Mbit/s的以太网能够共享帧传输达100Mbit/s的网络。

原来的同轴以太网使用半双工传输；因此，同时只能有一个设备进行传输。1997年，以太网扩展到包含全双工特性（原来的802.3x），全双工允许同一时间网络上超过一台PC进行传输。被称为以太网交换机的设备被开发出来，该设备允许全双工通信并且比集线器更有效地处理网络通信。

因为这些交换机的全双工性能和快速处理以太网帧的能力，它们逐渐取代了高速网络中的集线器。

在第5章中讲述的计时、帧结构和传输对本章涉及的两种版本的100Mbit/s快速以太网是一样的。

100BASE-TX使用4B/5B编码数据，然后这些数据被拼在一起进行多层传输——3层，即MLT-3，在5类线（或者更好的）上进行线路编码。MLT-3编码使用连续信号系统把二进制数据流转换成电波信号。MLT-3与*反转不归零码（NRZI）*不同，它的信号水平在零上和零下变化而不是只有两种水平。

注释：在反转不归零码（NRZI）编码中，如果没有信号传输，信号将维持在恒定的电压上（不恢复到0V）。仅在信号传输的bit间隙开始时认为有数据传输，没有变化的时候就解释为没有数据。

图6-11所示为一些MLT-3编码的例子。MLT-3的基本原则是，二进制1引起电平下一周期下降然后再回升，二进制0不会引起电平转换。

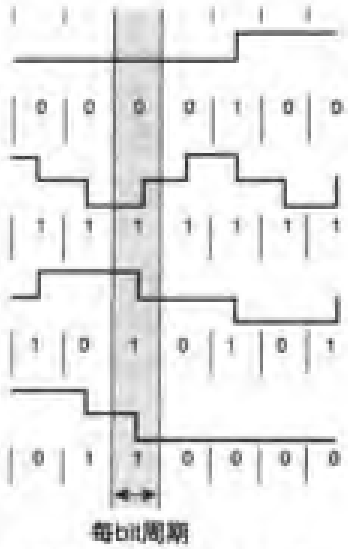


图6-11　MLT-3编码例子

在图6-11所示的编码例子中，垂直地突出显示在四个波形示例上的是一个时间窗口。最上的波形在时间窗口的中部没有变化。没有变化意味着它表示的是二进制0。如果例子中的波形在线路上是全0，波形上的信号电平表示可能总是高（为0）或者总是低。单个的1会使后面的0变化到一个不同的电平上，说明0可以用多个电平来表示。转换到的电平是依据前一个电平（高或低）将自己换到相反的方向。在第一个波形中，显然前一电平（图中未标示）是低电平。

图6-11的第2个波形在时间窗口的中部有一个变换，变换表示的是二进制1。至于到底变换是升或降并不重要，或者说新的电平是到高电平（0）还是到低电平并不重要。在第3个波形例子中，不是同样二进制的重复序列，采用的是交错二进制序列。同样，这种模式下没有变换表示的是二进制的0，有变换表示的是1。上升或者下降沿表示的是1。从一个极端到另一个极端的非常陡峭的信号变换表示连续为1，并且这个变换在0附近的梯度只有轻微的减小。信号中任何明显的水平线表示0或者连续为0。

图6-12是从示波器上取得的100BASE-TX的信号例子。（图6-12中，y轴代表电压；x轴代表时间。测得电压是在2之间的微分信号。）


图6-12　100BASE-TX信号例子

在同连接对象建立连接的初始化同步信息过程中，接收器电路只接收4B/5B空闲编码组。

100BASE-TX的连接线缆插脚引线排列与10BASE-T的是一样的。有两对分开的发送/接收路径。对两个站点或者两个交换机之间的连接来说，需要使用交叉线。对站点与中继器或者多端口中继器（集线器）之间的连接，使用直连线。注意在专用的100Mbit/s集线器内部是总线拓扑，即一个冲突域。然而，如果这个集线器是一个10/100自适应的集线器，那么其内部拓扑更加复杂，来解决10BASE-T和100BASE-TX之间的速度差异问题，现在这种自适应的集线器使用得更加广泛普遍。需要注意的是，即使100Mbit/s的以太网集线器比10Mbit/s的集线器明显快不少，冲突仍然是个问题，因为它们都是共享总线体系结构。只有通过使用交换机和全双工才能避免冲突。

对于主机和交换机之间的连接，使用的是直连线。交换机的线路构造允许在多个端口同时全带宽传输而不发生冲突。

在快速以太网中，站点到站点，交换机到交换机，站点到交换机的连接都是点到点的连接：它们有两个物理上分开的通信路径/通道。这样的话，冲突就不是物理事件而是不允许同时进行发送和接收的决定结果。因此，不论半双工（遵从CSMA/CD原则）还是全双工（没有物理的冲突发生），只是一个配置选择。大多数时间，你是在全双工下使用这些连接。

然而，站点到集线器的连接必须考虑到集线器内部的总线拓扑，那是一个冲突域。因此，这种

连接只能在半双工下运行并遵从CSMA/CD，这是由其物理上的自然结构决定的。

100Mbit/s的技术可以允许传输200Mbit/s的通信吗？100BASE-TX在半双工模式下以100Mbit/s传输数据（虽然这些数据有一部分是开销（overhead），不是用户数据）。但是100BASE-TX在全双工模式下可以200Mbit/s交换数据（同样，虽然有一部分是开销而非用户数据）。当想要增加以太网连接的速度的时候，这个概念会变得越来越重要。本章后面部分将讲到100BASE-TX的体系结构原则。

6.1.7 100BASE-FX

为什么要使用100BASE-FX（作为802.3u-1995标准的一部分引入的）呢？在铜质的快速以太网引入的时候，就希望有一种基于光纤的版本用于主干应用上，用在那些不希望使用铜线的地板和建筑以及那些较大环境噪声的地方的连接。100BASE-FX也被作为后来流行的FDDI（100Mbit/s双光纤令牌环网）的可选替代品。然而，现在安装最广泛的快速以太网是100BASE-TX。100BASE-FX相对不被接受的一个原因是，很快就引入了吉比特以太网的铜质和光纤标准。这些标准成了主干安装、高速互联和常规基础设施的主流技术。

在前面第5章描述的计时、帧结构和传输，对本章要考虑的两种100Mbit/s的快速以太网都是一样的。

100BASE-FX使用4B/5B编码数据和反转不归零码（NRZI）线路编码。信号是在多模光纤上传输的LED脉冲。在每bit周期中，反转不归零码根据时间窗口中部有还是没有变换来确定二进制数据的值。100BASE-FX是同步的。

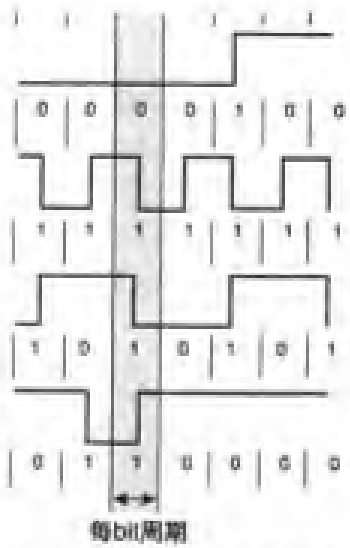


图6-13 反转不归零码编码例子

图6-13所示为一个反转不归零码的例子（其y轴是光能，x轴是时间）。

在图6-13的编码例子中，垂直地突出显示在四个波形示例上的是一个时间窗口。最上的波形在时间窗口的中部没有变化。所以它意味着是二进制0。没有变换表示这是一个二进制0。如果在该波形例子中线路全是零，波形上的信号电平表示可能为低也可能为高。信号1的引入会导致0在两个电平的任何一个上。

在第2个波形图的时间窗口中部，由一个变换表明它是二进制1。至于是上升变换还是下降并不重要。第三个波形不再采用同样二进制值的重复序列，而是采用交错二进制序列。在这个例子中，这种现象更加明显：没有变换是二进制0，有变换是1。

使用反转不归零码进行编码，连续bit流就可以通过光脉冲来传输。因为让接收器每次都完全打开和关闭的时间周期问题，光脉冲使用低能量和高能量来实现。其中用低能量代表逻辑0，高能量代表逻辑1。

表6-5概括了100BASE-FX的连接和插脚引线。最经常使用的是带有（ST）或者（SC）接头的光纤对。

表6-5 100BASE-FX针脚顺序

光纤	信号
1	Tx（LED和激光传输）
2	Rx（高速光敏二极管检测器）

图6-14是一个接口到接口的光纤连接。两束分开的多模光纤通常是在同一线缆结构里，每个末端都是双接头。

介质访问控制方法把这个连接当作点到点的连接，由于是分离的发送和接收光纤，所以光纤本

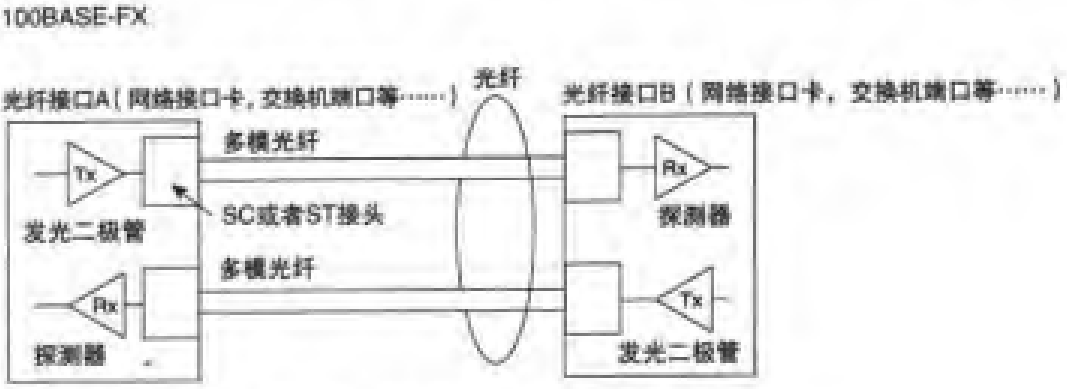


图6-14　光纤接口到接口连接

质上是全双工工作的。100BASE-TX能够在半双工模式下运行，但是受到长度限制（计时是主要的限制因素，同时还有衰减/散射/光纤的长度限制和分段的数量限制）。同样，电压间的物理冲突不是问题——在光纤上有光脉冲连续流——不过可以基于不允许同时进行Tx和Rx来管理利用CSMA/CD。

100Mbit/s的光纤技术可以运行200Mbit/s的通信量吗？有点类似于在UTP上的分开的发送和接收的路径，在100BASE-FX光纤上有这样的两个路径，所以200Mbit/s是可能的。

6.1.8　快速以太网体系结构

快速以太网连接一般包含站点与集线器或者交换机之间的连接。集线器应该被看作是多端口中继器，能解决远程站点间中继器数量限制的问题。交换机可以看作是多端口网桥。它们受到UTP介质100m长度的距离限制，但是没有菊花链的限制。

中继器必须用单词*Class*（*类*）跟罗马数字I或者II来标记，指明是I类还是II类。I类中继器会带来140 个bit时间（bit-time）的等待时间（延迟）。任何从一种以太网实现到另一种以太网（比如，100BASE-TX和100BASE-FX）的是I类中继器。同时假设所有没有标记的中继器都是I类设备。图6-15所示为100BASE-TX使用的I类中继器的最大冲突域直径。使用交换机没有这些限制，其限制因素变为两个端口间由介质确定的最大长度。

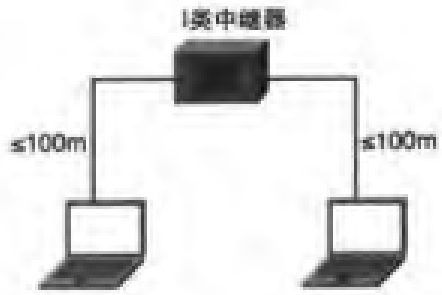


图6-15　I类中继器的最大冲突域直径

II类中继器只带来最大92个bit时间（bit-time）的等待时间，在一个连续段里可以有两个II类中继器，不过这两者之间的线缆长度要很短，图6-16所示为在100BASE-TX中使用的II类中继器的最大冲突域半径。使用交换机没有这些限制，其限制因素变为两个端口间由介质确定的最大长度。

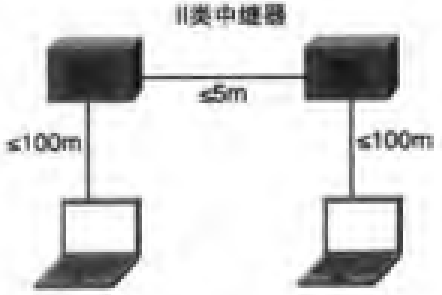


图6-16　II类中继器的最大冲突域直径

就10Mbit/s版本而言，修改它的一些体系结构原则去适用于100Mbit/s版本是可能的；然而，不允许带来事实上额外的延迟。如果网络实现采用的是高性能的硬件，部分超过这些限制是可以的。例如，如果在中继器之间使用较长的线缆，在每个站点间就应该使用较短的线缆。对100BASE-TX改变体系结构原则是*很不鼓励的*。试图修改之前请参考当前的802.3标准中的第29条有关计时技术的详细描述和所采用的硬件性能的技术信息。任何能适应不同以太网速率的设备，比如能够在10Mbit/s和100Mbit/s之间适应的设备，都是OSI第2层网桥。不可能适应不同的速率却还是中继器。不过，只是中继器的设备是可

以在相同速率连在一起的端口间进行中继的。

100BASE-TX的非屏蔽双绞线与在10BASE-T中使用的线缆是一样的，除了连接性能必须满足高品质5类线或者国际标准化组织（ISO）的D类要求外。

全双工运行时的连接可以比表6-6所示的要长很多，因为它们所受的限制只是介质的性能要能够传送适合解码的足够稳定的信号，而不是对来回一次延迟的限制。快速以太网运行在半双工下也并非罕见。不过，半双工并不合适，因为信号模式是全双工的，所以强制把半双工的通信原则加在全双工的信号系统上对资源利用来说并不是明智之举。

推荐所有站点和集线器或交换机之间的连接设置成为自动协商的，这样可以不用冒着错误配置线路的风险建起共同的最高性能配置。仅在自动协商失败或者在某些选择的连接中禁用自动协商并采用强制连接配置。一般的站点连接应该使用自动协商来建立。

表6-6 体系结构配置的线缆长度

体系结构	100BASE-TX	100BASE-FX	100BASE-FX和100BASE-FX
站点到站点，站点到交换机，交换机到交换机（半双工或者全双工）	100m	412m	-
一个I类中继器（半双工）	200m	272m	100mTx 160.8mFX
一个II类中继器（半双工）	200m	320m	100mTx 208mFX
两个II类中继器（半双工）	205m	228m	105mTx 211.2mFX

100BASE-TX连接的非中继距离可以达到100m。这个距离看起来很长，在实际建筑中布线的时候通常很快就用光了。使用集线器可以解决这个距离问题，但是因为计时的考虑要受到表6-6中所示的限制。广泛使用的交换机使得这个距离限制变得不那么重要了。只要工作站距离交换机在100m以内，这100m的距离是到这个交换机结束的，这个交换机又可以通过另外的100m连接到其他的交换机上，以此类推。由于现在大多数的快速以太网都是交换的，所以在设备之间是有一些实际的限制。环型、星型和扩展星型拓扑都允许使用。问题就变到逻辑拓扑和数据流上而不是计时和距离限制上了。

6.2 吉比特、10Gbit和未来的以太网

快速以太网（100Mbit/s）代表了对传统以太网（10 Mbit/s）的一次重大改进。然而从快速以太网到吉比特以太网更为迅速的发展见证了IEEE标准、工程上的进步和市场力的强大动力。吉比特以太网、1000Mbit/s在网络速度上比广泛普及的10BASE-T提高了一百倍。尽管MAC寻址、CSMA/CD，以及更为重要的以太网早期版本以来的帧格式得到了保留，但MAC子层、物理层和介质等很多其他方面均已改变了。

能进行10/100/1000操作的铜接口现在很普遍。吉比特交换机、路由器端口和刀片服务器在布线间正变得普通。更多的单模和多模光纤在安装。吉比特以太网的一个重点是光纤技术，但对铜版本的需要——利用已存的电缆设施，且利用铜缆在用户环境的耐久性——导致一种很聪明的方案，即让1000 Mbit/s运行在10 Mbit/s和100 Mbit/s以太网如此成功使用的5类UTP上。所有的吉比特技术本质上是全双工的。当前，伴随着40 Gbit/s、100 Gbit/s及160 Gbit/s标准和技术的应用，技术那势不可挡的步伐仍在向前迈进。最具戏剧性的是以太网的演变，从单单的LAN应用到端到端的LAN、MAN和WAN技术。

6.2.1 1000Mbit/s版本的以太网（吉比特）

1998年IEEE 802.3z委员会通过了1000BASE-X标准。该标准将光纤上的数据传输率提升到全双

工1Gbit/s，在速度上比10BASE-T有一百倍增长。指定在5类或更高类UTP上的全双工1Gbit/s的1000BASE-T标准在1999年通过。

表6-7所示为1000Mbit/s以太网的运行参数。

表6-7　吉比特以太网的运行参数

参数	值
比特时间	1ns
时隙	4096比特时间
帧间间隔	96bit*
冲突企图限制	16
冲突后退限制	10
冲突阻塞大小	32bit
最大无标记帧大小	1518octet
最小帧大小	512bit（64 octet）
突发限制	65 536bit

* 所列值为官方规定的帧间间隔。

1000BASE-T、*1000BASE-SX*和*1000BASE-LX*都有相同的计时参数。应当注意，1000Mbit/s的比特时间 = 1ns = 0.001ms = 十亿分之一秒。你同样需注意到相对于传统和快速以太网在计时上的差异正表现出来，这是由如此短的比特和时隙所产生的特定问题。

1000Mbit/s（吉比特）以太网帧与用在10Mbit/s和100Mbit/s以太网上的帧有相同的格式。1000Mbit/s以太网对于将帧转换为电缆上比特的处理有不同方式，这取决于采用何种实现方式。

吉比特以太网在速度上比快速以太网提高了十倍。正如同快速以太网一样，随着速度上的提高，出现了额外的需求——发送的比特在时长上（1ns）变得更短，出现得更加频繁，从而需要更精确的计时。它们传输所需的频率也更接近于介质带宽限制，且它们更易受到噪声干扰。作为对同步、带宽和SNR等问题的回答，吉比特以太网采用两种不同的编码措施。基本的思想是使用这种码——经过设计，它可具备满意的特性——以高效传输的方式表示用户数据，包括同步、带宽的有效使用，以及增强的SNR特性。

MAC子层的比特模式被转换为符号，符号有时控制着信息（诸如起始帧、结束帧和介质空闲状态）。整个帧分为控制符号和数据符号（数据码组）。所有这些额外的复杂性对于实现在网络速度上比快速以太网提高十倍而言是必需的。对于1000BASE-T，编码第一部分所采用的技术称为***8比特五进制四等分（8B1Q4）***；编码第二部分是特定于铜缆的实际线性编码，称为***4维5电平脉冲幅值调制（4D-PAM5）***。在4D-PAM5线性编码之前的8B1Q4编码提供了使得四个线对（并行工作）同时在每个线对上全双工运行成为可能所需的同步、带宽和信噪比特性。对于1000BASE-X，采用的是8比特/10比特（8B/10B）编码（类似于4B/5B概念），接着是在光纤上对光进行简单的NRZ线性编码。

6.2.2　1000BASE-T

1000BASE-T（作为802.3ab-1999——双绞线上1000BASE-T吉比特以太网而提出）的目标包括这些：

- 具备运行在已存的5类铜缆设施上的能力。
- 保证通过5e类测试的电缆能够工作，大多数电缆经过仔细的再次端接后能够通过该类测试。
- 具备与10BASE-T以及100BASE-TX的互操作性。
- 支持应用诸如建筑物主干、交换机间链路、配线室应用、服务器群，和高端台式工作站。
- 具备快速以太网10倍带宽，终端用户所广泛安装的快速以太网使得网络中更高速的上行成为必需。

为了实现在5e类铜缆上达到该速度，1000BASE-T需利用所有四对线。5e类电缆能可靠地承载达到125Mbit/s的流量。通过使用尖端的电路，同一线对上全双工传输允许每个线对达到250Mbit/s；乘以四个线对，则达到总量1000Mbit/s（1Gbit/s）。对于某些用途，可认为这四个线对作为“分路”，在其上数据同时传输（接收端需仔细地进行再重组）。

计时、帧格式和传输在前面第5章已做了叙述，它们与这里所考虑的1000Mbit/s以太网的所有版本都是共同的。

1000BASE-T在5e类或更好的UTP上采用8B1Q4编码和4D-PAM5线性编码。实现1 Gbit/s速率需利用所有四对线同时全双工工作。这导致线对上永久的冲突，这与最初的同轴以太网系统完全不同。这个“永久”冲突——数据的传输和接收发生在同一条线同一时间的两个方向上——导致非常复杂的电压模式。但通过使用尖端的集成电路，其中采用一种称为*回应取消*的技术，它工作地很好。

尽管有信号的持续冲突，但通过仔细选择电压电平和使用第1层前向纠错，系统能运行起来。

图6-17所示是1000BASE-T的输出（发送[Tx]）信号（y轴是电压；x轴是取自示波器的时间——电压是“差值信号”，其测量取自UTP电缆中四个线对中一对的两根线之间）。

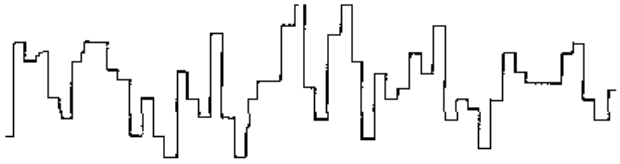


图6-17　1000BASE-T输出（Tx）信号

图6-18所示是实际的1000BASE-T信号，通过数字存储示波器在电缆的几米处所捕获（y轴是电压；x轴是时间——电压是“差值信号”，其测量取自UTP电缆中四个线对中一对的两根线之间）。



图6-18　1000BASE-T实际信号

最不不可思义的是，当人们发现在空闲期间电缆上存在9个电压电平、而在数据传输期间电缆上有17个电压电平时，信号竟然可以完全恢复。应当注意复杂线性编码的开始。而且，在图6-18中可观察到电线上实际信号有持续的冲突，以及衰减影响和噪声。信号看上去像模拟信号。这里的关键是尖端的电路对所有这些进行解码。然而，除非有后继的标准，否则系统易受到电缆问题、端接问题和噪声的影响。如果遵循布线、端接和噪声规则，则吉比特以太网将顺利工作。

表6-8总结了UTP电缆中所有四个线对的使用。A、B、C和D被认为是数据的“分路”。来自发送站的数据被仔细地分成四条并行流，并行地编码、传输和检测，然后被重组为一接收比特流。

表6-8　1000BASE-T插脚

插脚号	信号
1	BI_DA+（双向数据，正）
2	BI_DA-（双向数据，负）
3	BI_DB+（双向数据，正）
4	BI_DC+（双向数据，正）
5	BI_DC-（双向数据，负）
6	BI_DB-（双向数据，负）
7	BI_DD+（双向数据，正）
8	BI_DD-（双向数据，负）

图6-19是四个线对同时全双工的图表示意。站到站、交换机到交换机和站到交换机布线连接与快速以太网中相同。

对于桌面、办公室和配线室应用尤其重要的是存在吉比特、快速和10BASE-T以太网之间的互操作。这像是没有希望的事情。但经过严格的检验，注意到如果安装在墙上的布线通过5e类考验（这经常或容易通过再端接来实现），且如果在RJ-45连接器和插座中所有八根线都是连接的，则存在

为吉比特、快速和10BASE-T以太网进行互操作的信号路径。正像10/100设备融合在快速以太网中，10/100/1000接口正被开发用于互操作。通过使用相同的帧格式、兼容的配线路径和智能的接口设计，互操作会顺利工作。

由于历史的原因，CSMA/CD和半双工是1000BASE-T的可选项。但绝大多数1000BASE-T的使用是全双工。这是通过尖端的混合电路来实现，它可以同时让相同的线来承担Tx和Rx工作。

在通信开始之前，两个链路伙伴必须决定哪一端作为主时钟的源和哪一端使用数据流来恢复从时钟。主时钟和从时钟都被用做信号传输的时间标记。这个过程通常在自动协商阶段被确定下来，尽管也可手工配置。许多其他参数也以相同的方式被确定下来，包括双工类型。自动协商通常规定多端口设备（交换机或集线器）应作为主时钟。这里概括性地说来在1ns比特时间、10亿bit/s数据传输率和四个线对同时发送及接收的情况下，同步就显得极其重要。

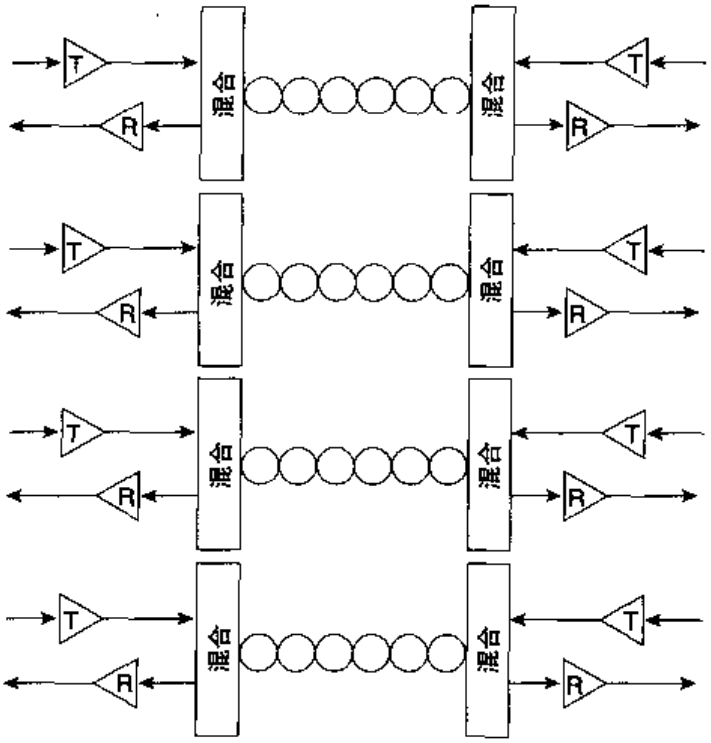


图6-19　1000BASE-T信号传输

以下将概括介绍1000BASE-X（1000BASE-SX和1000BASE-LX），也包括与1000BASE-T体系的比较。

6.2.3　1000BASE-SX和1000BASE-LX

光纤上吉比特以太网是最受推荐的主干技术之一。它有非常大的好处：

- 1000Mbit/s数据传输，它可以汇聚广泛部署的快速以太网设备群组。
- 噪声抗扰性。
- 在地板或建筑物间没有任何接地的潜在问题。
- 1000BASE-X设备选择上的极大丰富。
- 极好的距离特性。

光纤上吉比特以太网最开始是作为IEEE 802.3标准的补充而提出的，称为“802.3z-1998 1000BASE-X吉比特以太网”。1000BASE-SX和1000BASE-LX没有迅速抓住的惟一应用是办公室桌面——就日常的磨损而言1000BASE-TX被认为是更为“经受用户考验”，且10/100/1000Mbit/s铜接口很普遍。

计时、帧格式和传输在前面第5章已做了叙述，它们与这里所考虑的1000Mbit/s以太网的所有版本都是共同的。

1000BASE-X采用8B/10B编码，再转换为NRZ线性编码，采用较低成本的短波长850nm激光（或有时是LED）源和多模光纤（1000BASE-SX，S代表短波），或长波长1310nm激光源和单模光纤（1000BASE-LX，L代表长波）。

NRZ编码根据在计时窗口所发现的信号电平来确定那个比特周期的二进制值。和大多数其他编码机制不同，该编码系统是电平驱动，而不是边沿驱动。

在图6-20的编码例子中，计时窗口在所有四个波形示例中做了垂直加亮处理。最上面的波形通过计时窗口时是低电平。低信号电平代表二进制0。信号1在该波形的末端出现表示的是另一个信号电平。

第二个波形通过计时窗口时是高电平。高电平代表二进制1。此外，信号0在该波形的末端出现表示的是另一个信号电平。第三个波形不再是重复相同的二进制值序列，而是一个交替的二进制序列。在该例子中，低信号电平表示二进制0和高信号电平表示二进制1就表现得更加明显。

第四个例子是随机数据的波形。这些例子中的三个很好地说明了为什么该编码机制可能会使直流电压偏移铜介质。第二个例子改变每个比特周期的电平，就不会受到直流电压偏移的影响。对于一串相同的二进制信号，很容易会在电缆上产生直流电压的偏离，这会潜在地产生时钟错误。而在光纤介质上，这不成为问题。

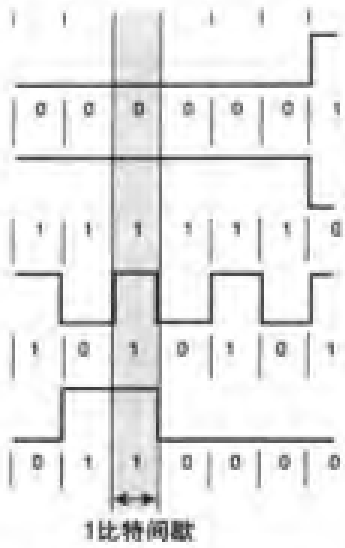


图6-20 NRZ编码例子

NRZ编码的串行比特流采用1000BASE-SX或1000BASE-LX所指定的脉冲光进行传输。由于涉及到每次完全打开和关闭发送器的周期时间问题，光被用低和高功率脉冲化。低功率表示逻辑0，高功率表示逻辑1。

表6-9所示是光纤上吉比特以太网极其简单的接口到接口互连。SC光纤连接器是最普遍使用的。

表6-9 吉比特以太网接口到接口互连

光纤	信号
1	Tx（激光发送器）
2	Rx（高速光电二极管检波器）

图6-21所示是1000BASE-SX接口到接口连接。短波长激光源（或有时是LED）典型地是和多模光纤一起使用。

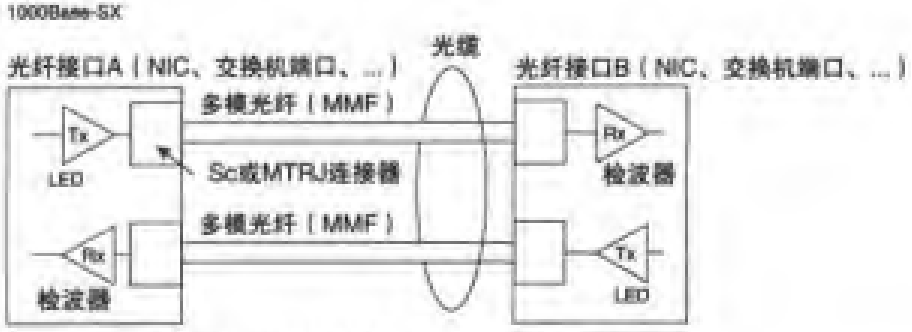


图6-21 1000BASE-SX光纤接口到接口连接

图6-22所示是1000BASE-LX接口到接口连接。激光源典型地是和单模光纤一起使用，以达到长

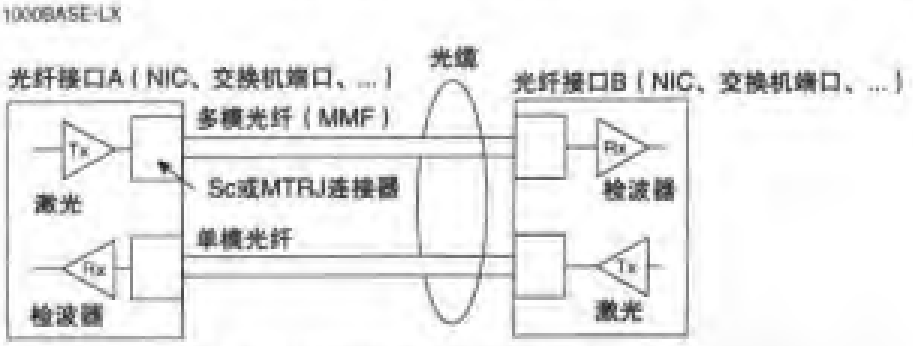


图6-22 1000BASE-LX接口到接口连接

达5000m的距离。

MAC机制是把链路看成是点到点的，而光纤本质上是全双工的，这是因为有不同的Tx和Rx光纤。吉比特以太网允许两个站间有一个中继器。

6.2.4　吉比特以太网体系结构

任何在不同以太网速度间适应的设备，比如在100Mbit/s和1000Mbit/s间，都是OSI第2层网桥。中继器不可能在不同速度间适应。

全双工链路要比表6-9和6-10中所示长很多，因为它们仅仅受到介质，而不是往返延迟的限制。吉比特以太网体系结构的绝大部分是在站到站、站到交换机、交换机到交换机和交换机到路由器连接上全双工运行。1000BASE-SX是针对多模光纤而制定。1000BASE-LX则是针对多模和单模光纤而制定。

表6-10和6-11所示是1000BASE-SX和1000BASE-LX的距离限制。因为大多数吉比特以太网是交换的，这些是设备间的实际限制。菊花链、星型和扩展的星型拓扑都是允许的。于是，这就变成了一个逻辑拓扑和数据流的问题，而不是计时或距离的限制了。

表6-10　1000BASE-SX最大电缆距离

介质	模态带宽	最大距离
62.5μm MMF	160	220m
62.5μm MMF	200	275m
50μm MMF	400	500m
50μm MMF	500	550m

在805nm处最大的1000BASE-SX电缆距离（最小过填充发射）。

表6-11　1000BASE-LX最大电缆距离

介质	模态带宽	最大距离
62.5μm MMF	500	550m
50μm MMF	400	550m
50μm MMF	500	550m
10μm SMF	—	5000m

在805nm处最大的1000BASE-LX电缆距离（最小过填充发射）。

除链路性能必须满足更高质量的5e类或ISO D类（2000年）要求以外，1000BASE-T UTP电缆与10BASE-T和100BASE-TX电缆大致相同。

对于10Mbit/s和100Mbit/s版本，轻微修改一些体系结构规则是可能的；然而，在半双工情况下事实上不允许有附加的延迟。而对于1000BASE-T体系结构规则的修改是完全不予鼓励的。在100m距离上，1000BASE-T工作在接近于硬件性能的边界以恢复传输信号。任何布线问题或环境噪声可能导致在其他方面符合的电缆，甚至在符合规范的距离内不能工作。在试图对体系结构规则有任何调整之前，请参考当前的802.3标准中技术上的计时描述和关于硬件性能的技术信息。

全双工链路上的链路操作可能比表6-12所示要长，这是因为它们仅受介质能力限制，即发出足够强的信号来对信令解码；它们不受往返延迟的限制。吉比特以太网在半双工下工作是十分少见的。半双工不合乎要求，这是因为信令机制本质上是全双工的，且在全双工信令系统上强制进行半双工的通信规则不是对资源聪明的使用。在半双工规则下工作要求遵守时隙往返延迟限制，这就减少了有效的电缆长度，且也存在由载波扩展所带来开销的大量增长。此外，很少使用吉比特中继器，这意味着链路可能是在站和OSI第2层网桥之间，或在两个网桥之间，因此无论如何冲突域将在网桥处终止。

建议将站和交换机间所有链路配置成自动协商，这样便可不冒链路错误配置的风险就建立起最高的通用性能配置，并且避免了其他用于正常吉比特以太网工作的参数出现意外的错误配置。

表6-12所示是用于半双工工作的速度示例。但因为大多数吉比特以太网是交换的，它受到前面表6-10和6-11所示逐链规则的影响。

表6-12 半双工工作的体系结构配置和电缆距离

体系结构	1000BASE-T	1000BASE-SX/LX	1000BASE-SX/LX和1000BASE-T
站到站	100m	316m	—
1个中继器	200m	220m	100m 1000BASE-T（+） 110m 1000BASE-SX/LX

6.2.5 10Gbit/s版本的以太网

最近在2002年IEEE 802.3ae标准得到了通过。该标准制定了光缆上10Gbit/s全双工传输。总的看来，802.3ae和802.3（最初的以太网）之间的相似处和以太网所有其他的种类都是值得注意的。梅特卡夫最初的设计已经进化了，但在现代以太网中它仍很明显。近来，10Gbit以太网（10GbE）已作为以太网系统可扩展性的一个最新例子而出现。10GbE提供了令人激动的、新的联网可能，可用于LAN、存储区域网络（SAN）、城域网（MAN）和WAN。那么，什么是10GbE？为什么应采用它？

传统以太网、快速以太网和吉比特以太网目前在LAN市场占支配地位。以太网的下一步演变是向10Gbit以太网发展（10GbE，工作在10,000,000,000bit/s）。通过维持帧格式和其他第2层的以太网规范不变，提高带宽的需求可由低成本、易实现和易互操作的10GbE来满足。10GbE仅运行在光纤介质上。端到端以太网络成为可能。

因为互联网和内联网上流量的大量增多，以及吉比特以太网迅速增加的使用，甚至需要更高带宽的互连。互联网服务供应商（ISP）和网络服务供应商（NSP）可以采用10GbE在集中放置的交换机和路由器之间创造高速、低成本、易互操作的连接。接入服务提供点（POP）、由吉比特以太网服务器所组成的内联网服务器群、数字视频工作室、SAN和主干已成为设想中的应用。

可能最值得注目的是，10GbE带来了一个主要的概念性改变。以太网传统上被认为是LAN技术。但10GbE物理层标准允许距离上的延伸（单模光纤达到40km）和与同步光纤网（SONET）/同步数字体系（SDH）的兼容。在40km距离上运行使得10GbE成为可行的MAN技术。与SONET/SDH网络的兼容，运行达到OC-192速度（9.584640Gbit/s）使得10GbE成为可行的WAN技术。对于某些应用，10GbE也能与异步传输模式（ATM）进行竞争。

以下总结了10GbE与其他种类以太网的比较：

- 帧格式相同，容许在传统、快速、吉比特和10Gbit以太网等种类间互操作，无帧重组或协议转换。
- 比特时间现在是0.1ns。所有其他时间变量是相应的尺度。
- 无需CSMA/CD，因为仅采用全双工光纤连接。
- OSI第1层和第2层中的IEEE 802.3子层绝大多数被保留下来，有一些补充以满足40km光纤链路和与SONET/SDH技术的互操作。
- 创造灵活、有效、可靠、相对低成本的端到端以太网络成为可能。
- 能在LAN、MAN、WAN上运行TCP/IP，具有第2层传输方法。

规定CSMA/CD的基本标准是IEEE 802.3。IEEE 802.3标准的一个补充，标题为802.3ae，规定了10GBASE标准族。典型地，对于新技术需考虑多种实现方式，包括如下这些：

- 10GBASE-SR——计划在已安装的多模光纤实现短距离传输，支持范围在26m和82m之间。
- 10GBASE-LX4——采用*波分复用（WDM）*。在已安装的多模光纤上支持240m到300m，在单

模光纤上支持10km。

• 10GBASE-LR和10GBASE-ER——在单模光纤上支持10 km和40 km。

• 10GBASE-SW、10GBASE-LW和10GBASE-EW——计划和OC-192/STM SONET/SDH WAN设备共同工作。

IEEE 802.3ae任务组和10Gb以太网联盟（10GEA）正在对这些新兴的技术进行标准化工作。

10Gbit以太网（IEEE 802.3ae）在2002年6月成为标准。它是全双工协议，仅采用光纤作为传输介质。最大传输距离取决于所使用的光纤类型。当使用单模光纤作为传输介质时，最大传输距离为40km（25英里）。IEEE 成员间的讨论暗示了40Gbit/s、80Gbit/s、甚至100Gbit/s以太网成为标准的可能性。看看以太网的历史，没有理由会想到它的发展会停止。更高速度和更大的传输距离使得以太网成为LAN和MAN技术，它不再仅是我们可能看到的以太网标准的补充。因为光纤被用作传输介质，所以在以太网分组通过网络的过程中，数据中错误发生的可能性是很低的，要比最初的以太网低很多。在有很低错误率的网络上传输更大的数据分组就变得有意义。

一个以太网分组（1帧）中所承载数据量的上限是1500字节。在1帧中发送的数据超过该限制将使得该帧成为无效的以太网帧，会促使网络丢弃该帧。自以太网创造以来这已是标准。假设在一个出错可能性低的网络，如果每个帧能承载更大量的数据，则大文件能通过网络更有效地移动。其理由是计算机产生和处理以太网帧头和帧尾需花费时间。每个以太网帧必须具有1个帧头和1个帧尾。例如，如果每帧可以发送6倍的数据，则需要更少的帧（仅六分之一）来承载一个文件中的所有数据。这意味着有更少的帧头和帧尾需要由发送器产生和接收器来处理。结果是通过网络在两台计算机之间移动一个大文件需更少的时间。WAN采用光纤作为其传输介质，一般用于传输大数据分组。

由于这个原因，特别是当多吉比特LAN连接到WAN时，很可能我们会看到特大以太网帧的使用。特大以太网帧是承载超过1500字节数据的以太网帧。对于特大帧所承载的数据量，所建议的上限值大约为9,000字节。特大帧目前不是新的IEEE 802.3ae标准的一部分。然而，很可能一些以太网网络设备厂商容许特大帧出现在仅由他们设备所组建的以太网网络上。这可能迫使IEEE 802.3委员会在新的多吉比特标准中将支持更大帧作为可选项。

表6-13所示是10Gbit以太网的工作参数。

表6-13　10Gbit/s以太网的工作参数

参数	值
比特时间	0.1ns
时隙	—*
帧间间隔	96bits**
冲突企图限制	—*
冲突后退限制	—*
冲突阻塞大小	—*
最大无标记帧大小	1518octets
最小帧大小	512bits（64 octets）
突发限制	—*
帧间间隔伸长率	104bits***

* 10Gbit/s以太网不容许半双工操作，因此与时隙计时和冲突处理有联系的参数不适用；

** 所列值为*官方规定的*帧间间隔；

*** 帧间间隔伸长率仅适用于10GBASE-W定义。

令人惊异的是，10GbE采用与10、100和1000Mbit/s以太网相同的帧格式（一些特殊情况除外）。

6.2.6　10GbE介质、连接和体系结构

10Gbit以太网在速度上比吉比特以太网有10倍的提升。正像吉比特以太网一样，随着速度上的

提高，出现了额外的需求——发送的比特在时长上变得更短（0.1ns），出现得更加频繁，从而需要更为精确的计时。此外，它们传输所需频率更接近于介质带宽限制，且它们更易受到噪声影响。作为对同步、带宽和SNR等问题的回答，10Gbit以太网采用了两种不同的编码措施。基本的思想是使用这种码——经过设计，它可具备满意的特性——以高效传输的方式表示用户数据，包括同步、带宽的有效使用和增强的SNR特性。

MAC子层的比特模式被转换为符号，符号有时控制着信息（诸如起始帧、结束帧和介质空闲状态）。整个帧分为控制符号和数据符号（数据码组）。所有这些额外的复杂性对于实现在网络速度上比吉比特以太网提高十倍而言是必需的。8B/10B编码（类似于4B/5B概念）被采用，接着是光纤上几种不同类型的线性编码。

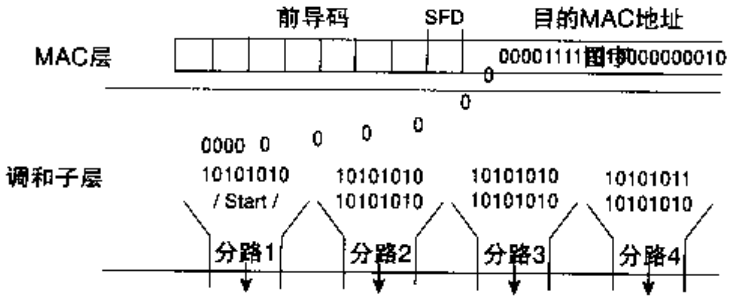


图6-23 10GbE如何将MAC帧转换为四个比特分路

图6-23所示是8B-10B被线性编码前所在状况。10Gbit以太网在进行线性编码前采用多种复杂编码，包括8B/10B和64B/66B。然后来自这些码的比特被转换成线性信号：低功率光表示二进制0，较高功率的光表示二进制1。复杂的连续比特流被所有版本的10GbE所采用，不包括10GBASE-LX4，其采用宽波分复用（WWDM）来复用4比特的同步比特流，即一次把四个波长的光发射入光纤。

图6-23所示是10GbE如何将MAC帧转换为四个比特分路用于在UTP四个线对上的并行传输或作为一个串后被序列化用于单模光纤上激光传输的比特流。

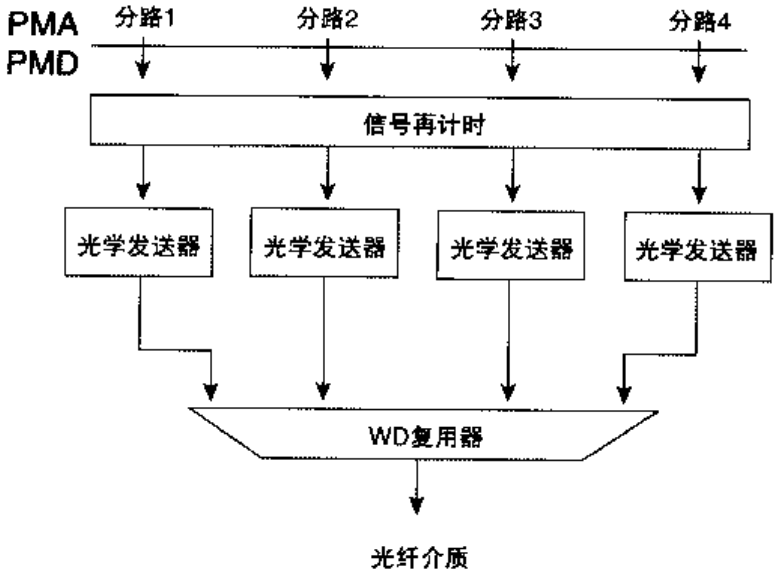


图6-24 10GBASE-LX4信号复用

图6-24表示四个有轻微颜色不同的激光源的特别情况。光信号流从介质接收到，并被分路为四个不同的光信号流。然后，四个光信号流被反向转换为四个电比特流，这大约在它们按相反的处理过程自一些子层倒退到MAC子层的过程中。

当前，大多数10GbE产品以模块（线卡）的方式作为高端交换机和路由器的补充。随着10GbE技术的发展，可以期望有更加多样的信令组件。并随着光学技术的涉及，增强的发送器和接收器，以及模块化的进一步使用将被结合到这些产品中。所有种类的10GbE都使用光纤介质。光纤类型包括10mm单模光纤、50mm和62.5mm多模光纤。光纤衰减的范围和散射特性得到支持，但它们限制了工作距离。

SC光纤连接器是最普遍使用的。因为10GbE采用光纤介质，所以光纤对一般是把设备1的Tx连接到设备2的Rx，反之亦然。当前10GbE连接的主要设备是高端模块化的交换机和路由器。表6-14列举了10GbE的插脚选项。

表6-14　10GbE的插脚

光纤	信号
1	Tx（激光发送器）
2	Rx（高速光电二极管检波器）

10Gbit以太网只可用全双工模式，且只能在光纤上工作。因此不存在冲突，也不需要CSMA/CD。

随着10GbE标准和产品的发展，更宽范围的体系结构和应用准则正成为可能。最需考虑的是，10GbE的加入以及其具有的LAN、SAN、MAN和WAN能力，使得网络工程师要思考很复杂的端到端以太网络。采用吉比特以太网的LAN、SAN、MAN和WAN拓扑正在实现中。

10Gbit以太网的运行仅被光纤介质所支持。62.5μm和50μm多模光纤，以及10μm单模光纤是得到支持的。即使这种支持仅限于光纤介质，但一些最大电缆长度也是惊人地短。10 Gbit以太网中没有定义中继器，因为半双工明显是不被支持的。

对于10Mbit/s、100Mbit/s和1000Mbit/s版本，轻微修改一些体系结构规则是可能的。可能的体系结构调整与介质上的信号丢失和失真有联系。因为信号散射和其他问题，光脉冲在超过一定距离后变得难以辨认。在试图对体系结构规则有任何调整之前，请参考当前的802.3标准中技术上的计时描述和光谱需求，以及关于硬件性能的技术信息。

表6-15所示是10Gbit以太网的实现情况。R和W规范都被每个适当的项目所包括（例如，10GBASE-E包括10GBASE-ER和10GBASE-EW）。

表6-15　10Gbit以太网的实现

实现	波长	介质	最小模态带宽	工作距离
10GBASE-LX4	1310nm	62.5μm MMF	500MHz/km	2m到300m
10GBASE-LX4	1310nm	50μm MMF	400MHz/km	2m到240m
10GBASE-LX4	1310nm	50μm MMF	500MHz/km	2m到300m
10GBASE-LX4	1310nm	10μm SMF	—	2km到10km
10GBASE-S	850nm	62.5μm MMF	160MHz/km	2m到26m
10GBASE-S	850nm	62.5μm MMF	200MHz/km	2m到33m
10GBASE-S	850nm	50μm MMF	400MHz/km	2m到66m
10GBASE-S	850nm	50μm MMF	500MHz/km	2m到82m
10GBASE-S	850nm	50μm MMF	2000MHz/km	2m到300m
10GBASE-L	1310nm	10μm SMF	—	2m到10km
10GBASE-E	1550nm	10μm SMF	—	2m到30km*

* 如果链路衰减足够低的话，该标准容许40km长度。

应当注意10GbE的多功能性。光纤种类和激光源的多样性集合可被用于达到LAN、MAN和WAN距离。

6.2.7　以太网的未来

正如前几个章节所记录的，以太网经历了从传统到快速、到吉比特、到多吉比特技术的发展。虽然其他LAN技术仍旧在起作用（传统的安装设施），以太网统治了新的LAN安装——如此之多以致一些人将以太网称为LAN“拨号音”。以太网现在是水平、垂直和建筑物间连接的标准。事实上，最近正在开发的以太网版本正将LAN、MAN和WAN在覆盖网络的地理距离方面的差别变得模糊。

图6-25阐明了以太网的扩展范围。

虽然吉比特以太网现在广泛采用，且10Gbit产品也更易得到，但是IEEE和10Gbit以太网联盟当前又发布了40Gbit/s、100Gbit/s，甚至160Gbit/s标准。事实上，何种技术被采纳取决于多种因素，

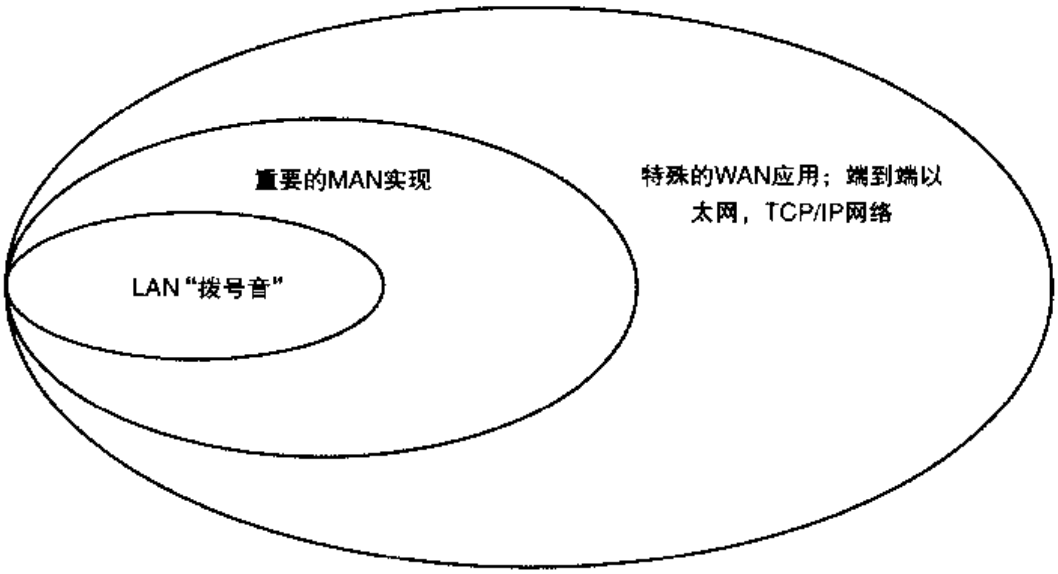


图6-25 以太网的扩展范围

包括技术和标准的成熟比率、被市场吸纳的比率，以及成本。

不同于CSMA/CD的以太网仲裁机制的方案已经提出。但对于10BASE5、10BASE2、10BASE-T和100BASE-TX集线器的物理总线拓扑如此基础的冲突问题，不再是那样普遍。光纤和UTP两者都有不同的Tx和Rx通路，它们的使用以及替代了集线连接的交换成本的缩减使得单条共享介质、半双工介质连接不再重要。

网络介质的未来是三个层次：

- 铜（达到1000Mbit/s，可能更高）。
- 无线（接近100Mbit/s，可能更高）。
- 光纤（当前是10,000Mbit/s，不久会更高）。

在铜和无线介质中最高频率信号的传输正接近于某些物理和实际限制，与它们不同，光纤上带宽限制特别地宽，且在可预见的未来这不是一个限制因素。在光纤系统中电子技术（例如，发射体和探测器）和光纤制造过程最大地限制了速度。因此，对于以太网即将到来的开发很可能重点是朝向激光源和单模光纤。

当以太网还较慢时，半双工（易受到冲突和对优先级“民主”处理的影响）被认为不具有处理某些类型流量所需的服务质量（QoS）能力。这包括诸如IP电话和视频组播等应用。

然而，目前在市场占显著地位的全双工、高速的以太网技术证明有足够能力支持甚至对QoS敏感的应用。这使得以太网的潜在应用甚至更加广泛。具有讽刺意味的是，在20世纪90年代中期端到端QoS能力把ATM推到桌面和WAN，但现在是以太网，而不是ATM，接近了这个目标。

以太网已有30个年头，它将继续发展，并拥有一个非常光明的未来。

6.3 以太网交换

随着更多的节点加入到以太网的物理分段，对介质的竞争在增加。更多节点的加入增加了对可用带宽的需求，且在介质上增加了更多的负载。随着流量的增加，冲突的概率增多，导致更多的重传发生。对该问题的解决方法是将大的分段分成多个部分，并用Catalyst交换机将其隔开。将这些新分割的部分隔绝为单独的冲突域。这就减少了冲突的数量，且增加了网络的可靠性。

桥接和交换是通过减少流量和增加带宽来降低LAN中拥塞的技术。LAN交换机和网桥工作在OSI参考模型的第2层，它们根据MAC地址转发帧来执行交换功能。如果第2层MAC地址未知，则设

备通过泛洪该帧以试图到达所希望的目的地。LAN交换机和网桥也转发所有的广播帧。结果可能是无穷循环的流量风暴流过网络。*生成树协议（STP）*是防止环路的协议；它是一种使得交换机间相互通信以发现网络中物理环路的技术。

以下几节将介绍第2层桥接、第2层交换、交换模式和生成树（STP）。

6.3.1　第2层桥接

*网桥*是设计用于创造两个或多个LAN分段的第2层设备，每个分段是一单独的冲突域。换句话说，网桥被设计以创造更多可用的带宽。网桥的目的是过滤LAN上的流量以保持本地流量的本地化，但容许和LAN其他部分（分段）的连接性，这是针对流向那里的流量而言的。为了过滤或选择性地发送网络流量，网桥为位于网络分段上的所有MAC地址和其他网络建立一对应表。其处理过程如下：

- 如果数据沿网络介质到达，网桥将数据所带的目的MAC地址和它表中所包含的MAC地址进行比较。
- 如果网桥确定数据的MAC目的地址和源地址出自同一网络分段，则它不把该数据转发到其他网络分段。该处理过程称为过滤。该过程的执行去除了不必要的流量，网桥能有效地减少网络分段间的流量。
- 如果网桥确定数据的目的MAC地址和源地址不是出自同一网络分段，则它把该数据转发到适当的分段。
- 如果目的MAC地址对于网桥是未知的，则网桥向网络上的所有设备广播该数据，不包括接收到数据的那个网络。该处理过程称为*泛洪*。

一般地，网桥仅有两个端口，把一个冲突域分为两个部分。网桥的所有决定都根据MAC地址或第2层寻址做出，不会影响到逻辑的或第3层寻址。因此，网桥划分冲突域而不是逻辑的或广播域。不管有多少网桥在网络上，除非有一个类似路由器的设备工作在第3层寻址，否则所有网络将共享同一个逻辑（广播）地址空间。网桥会创造更多（且更小）的冲突域，但不会增加广播域。因为网络上每个设备必须关注广播，网桥始终要转发它们。所以，桥接环境中的所有分段被认为是处于相同的广播域。

6.3.2　第2层交换

LAN交换机基本上是一多端口的网桥，其采用*微分段*来减少LAN中冲突的数量，增加了带宽。LAN交换机也支持诸如全双工通信和多个同时发生的会话等特征。图6-26所示是一个有三个工作站和一个LAN交换机的LAN，以及LAN交换机的地址表。LAN交换机有四个*接口*（或网络连接）。站A和C连接到交换机的接口3，站B在接口4。如图6-26所示，站A需传送数据到站B。

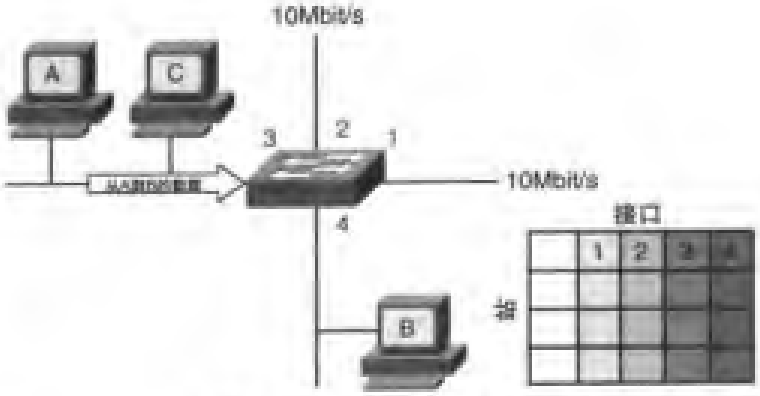


图6-26　LAN交换机的操作

记住，随流量流过网络，交换机在第2层工作，这意味着交换机能查看到MAC层地址。当站A发送且交换机接收到帧，则交换机在流量通过时进行评估以发现源MAC地址并将其存储在地址表中，如图6-27所示。

随着流量流过交换机，地址表中一条项目建立起来以识别源站和其所连接的交换机接口。交换机现在知道站A连接在何处。当数据帧在交换机中，由于目的站未知它泛洪到所有端口，如图6-28

所示。

当表中建立起地址项目之后，在另一方面，一个响应自站B返回到站A。交换机现在知道站B连接到接口4，如图6-29所示。

数据发送到交换机，但注意到这次交换机没有泛洪流量。交换机仅从接口3送出数据，因为它知道站A在网络的什么位置，如图6-30所示。

最初的传输指示了MAC地址来自哪里，使得交换机更有效地在网络上发送数据。

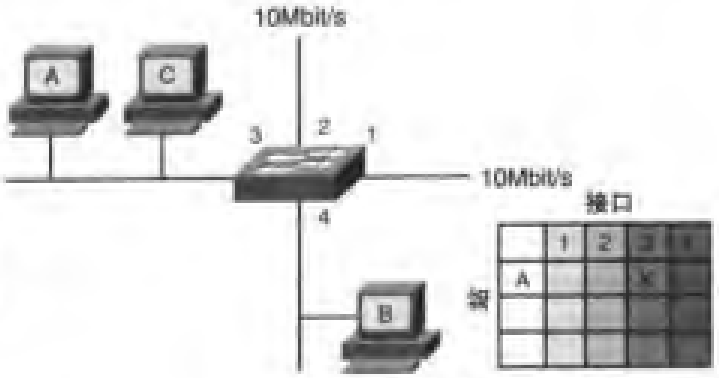


图6-27 建立一地址表

6.3.3 微分段

随着技术进步，建造具有更高性能的网桥成为可能。自然，基本目标是在网桥的每个端口仅有一个节点。这将减少冲突域，以致几乎不存在冲突。交换机确实做到这一点，简单地说是有多个端口的网桥。这些小的物理分段称为*微分段*。

微分段使得专用分段的创建变得容易，且给网络上每个用户提供了专用带宽。每个用户即刻接入到全部带宽，且不必和其他用户竞争可用带宽。这意味着同一交换机上的每对设备能以最少量的冲突并行通信。微分段减少了网络中的冲突，且有效地增加了连接到网络上每个站的性能。

除了更快的微处理器和内存之外，另外两项技术进步使交换机成为可能。内容可寻址存储器（CAM）对比于传统内存基本上工作相反。数据进入内存会返回所关联的地址。采用CAM容许交换机无需搜索算法就可直接发现与MAC地址相关联的端口。专用集成电路（ASIC）是由非专用的逻辑门所组成的设备，逻辑门可被编程以逻辑速度执行操作。以软件所完成的操作现在可采用ASIC在硬件中完成。这些技术的使用极大地减少了由软件处理所带来的延迟，且使得交换机满足很多微分段和高比特率的数据需求。

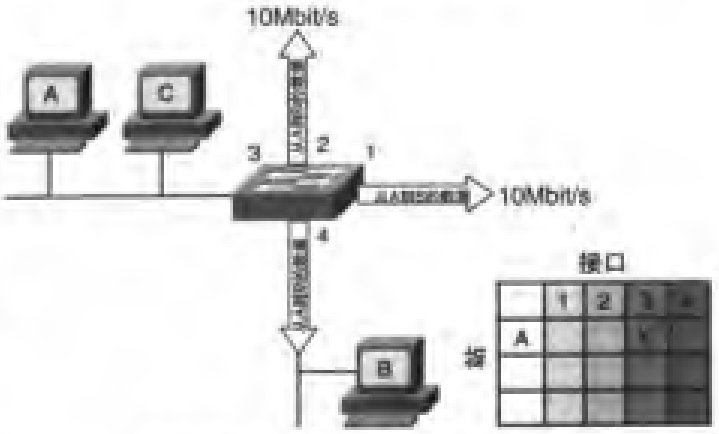


图6-28 泛洪数据到所有交换机端口

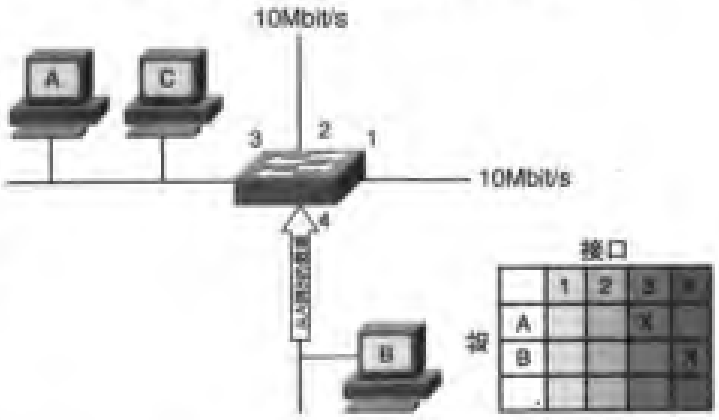


图6-29 泛洪消息的响应

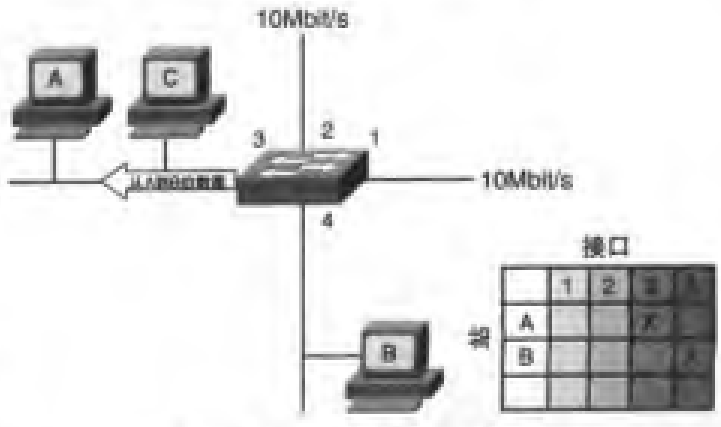


图6-30 发送数据到一已知站

6.3.4 全双工传输

LAN交换的另一项极大地提高带宽的功能是全双工传输，其将节点间的带宽数量有效地加倍。站间的全双工传输通过点到点的

以太网连接来实现。该特性是重要的，例如，在高带宽的设备间，诸如交换机和服务器之间的连接。全双工传输提供了无冲突的传输环境。因为两个节点可以同时发送和接收，没有对带宽的协商。



图6-31　交换技术：全双工

例如，在10Mbit/s连接中，全双工提供了10Mbit的发送能力和10Mbit的接收能力，则一个连接实际上有20Mbit的能力。同样，100Mbit/s连接实际上提供了200Mbit/s的吞吐量，如图6-31所示。全双工通信也支持两条速度达到1Gbit/s的数据传输路径。

6.3.5　等待时间

等待时间，有时称为*传播延迟*，它是数据帧（或分组）自源站或节点到达网络上最终目的所需的时间。当帧自源向目的传播，有很多种的情况会导致延时。

- 介质延迟，信号通过物理介质以有限的速度传播所引起。
- 电路延迟，由电子器件处理路径上信号引起。
- 软件延迟，软件为实现交换和协议必须所作的决定引起。
- 由帧的内容以及在何处完成帧交换所引起的延迟。例如，设备不能将帧发送到目的地，除非已读到目的MAC地址。

等待时间是当帧开始离开源设备到帧的第一部分到达目的之间的时间延迟。

6.3.6　交换模式

帧的内容如何被交换到目的端口是在等待时间和可靠性间的一种权衡。三种交换模式——存储转发、贯穿和无分片交换——提供了不同的性能和等待时间。

存储转发交换

在***存储转发交换***中，交换机读取整个数据帧，对帧进行查错，决定该帧去向何处，然后把它发送上路。图6-32解释了存储转发交换的操作。这里明显的权衡是需交换机花费更多的时间读取整个帧。然而，是在读完整个帧之后，交换机才检测帧上的错误。如果帧存在错误，则帧不被转发而被丢掉。虽然贯穿交换会更快，但它没有错误检测。由存储转发交换所引起的等待时间通常不是太大的问题。



图6-32　存储转发交换

贯穿交换

在***贯穿交换***中，随流量流经交换机，交换机自帧的开始部分一直读到目的MAC地址，然后“贯穿”到目的地而不再继续读帧的其他部分，如图6-33所示。

贯穿交换减少了传输的等待时间。然而，贯穿交换无错误检测。

无分片交换

*无分片交换*是贯穿交换的一种修订形式。在转发开始之前，无分片交换滤掉占分组错误多数的冲突分片。无分片交换在转发分组前一直等待，直到所接收到的分组已确定不是冲突分片。



图6-33 贯穿交换

何时采用何种交换模式

当采用贯穿和无分片模式，源端口和目的端口都必须工作在相同的比特率以保持帧的完整。这称为*同步交换*。如果比特率不相同，帧必须以一比特率先存储起来，然后再以另一比特率发出。这称为异步交换。存储转发模式必须用于异步交换。非对称交换提供了在不同的带宽端口间的交换连接，比如，100Mbit/s和1000Mbit/s的一种组合。非对称交换用于优化客户/服务器流量，其中多个客户同时与一个服务器通信，则需要给服务器端口有更多专用的带宽以防止该端口处的瓶颈。

6.3.7 生成树协议的介绍

当多个交换机连接起来，存在产生环路的可能性，即从源到目的没有明显的路径。如果交换机按简单的等级来安排，则无环路产生，如图6-34所示。

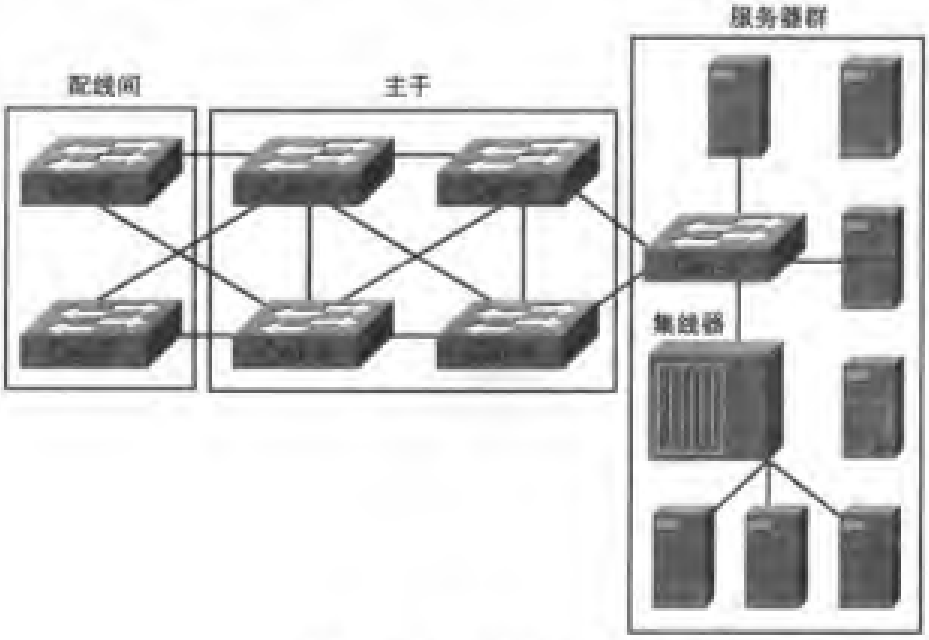


图6-34 STP减少路由环路

然而，当有额外的交换机和网桥加入为实现可靠性和容错提供冗余路径时，则环路可能发生，如图6-35所示。

在图6-35中，发生下列步骤：

- 主机1广播。
- SWA和SWB收到帧。
- SWA转发到SWB。
- SWB转发到SWA。
- 现在每个交换机开始看到同一广播的多个帧，因此导致路由环路。

为了减少环路产生的可能性，交换机所具有的一种协议可用于它们相互交流以避免该情况。交换机从其所有端口发送出称为***网桥协议数据单元（BPDU）***的特殊消息，让其他交换机知道它的存在，如图6-36和图6-37所示。交换机采用生成树算法（STA）来消除和关闭冗余路径。关闭端口的处理称为阻塞。解决和消除环路的结果是创造了一个没有环路的、逻辑上有等级的树。然而，预备路径在万一需要时仍然可用。用于解决和消除环路的协议称为生成树协议（STP）。这就创造了另一个交换和网桥的操作模式，称为环路避免模式。

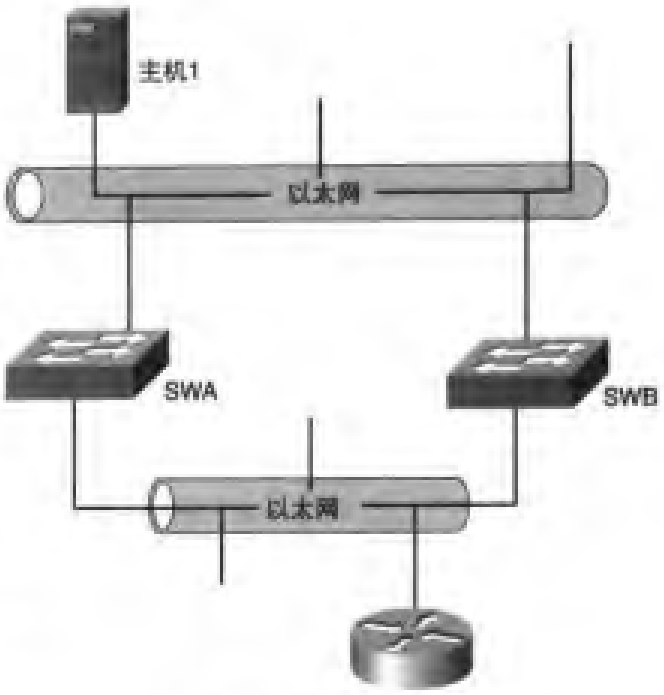


图6-35　广播风暴

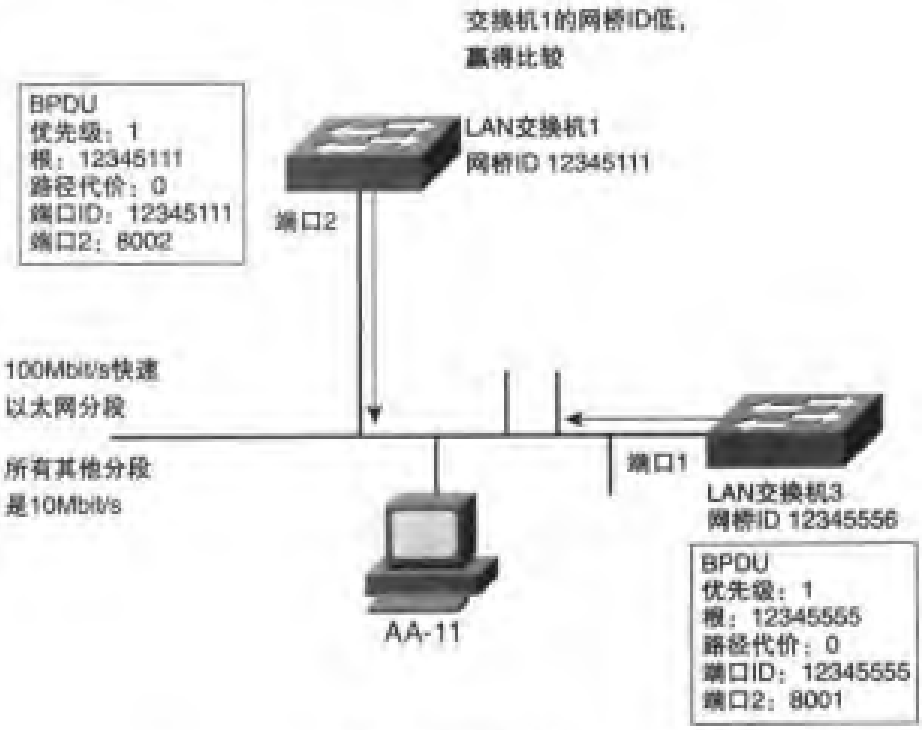


图6-36　BPDU通信

因此，交换机有五种工作模式：

- **阻塞**——处于阻塞状态的端口发送和监听BPDU，但不转发帧。默认地，当交换机打开时所有端口都处在阻塞状态。
- **监听**——在监听状态，端口监听BPDU以确认网络中无环路。该状态下不转发帧。
- **学习**——在该状态，端口学习MAC地址，建立地址表，但不转发帧。

• **转发**——处于转发状态的端口转发帧。发送和监听BPDU。

• **禁用**——处于禁用状态的端口不参与STP的工作。因此，它不监听BPDU或转发帧。

图6-38解释了使用STP的交换网络中的一些端口状态和操作模式。

实验活动 介绍Fluke网络测试仪

这个实验是针对如何使用Fluke网络测试仪（NI）来发现和分析广播域中网络设备的一个示范教程。这个实验示范了该工具的关键特性，可被合并入剩下实验中不同种的故障检修手段中。



图6-37 BPDU协议设计

6.4 总结

本章学习了以下知识点：

• 存在几种类型的以太网：以太网、快速以太网、吉比特以太网和10Gbit以太网。每种类型都与不同的传输率相关联。

• 以太网采用载波侦听多址/冲突检测（CSMA/CD）。

• 10 Mbit/s以太网的操作受到计时限制，这是由不超过四个中继器所划分的一系列不超过五个分段所提供的。

• 交换机可提供专用的访问以提高共享的LAN技术。

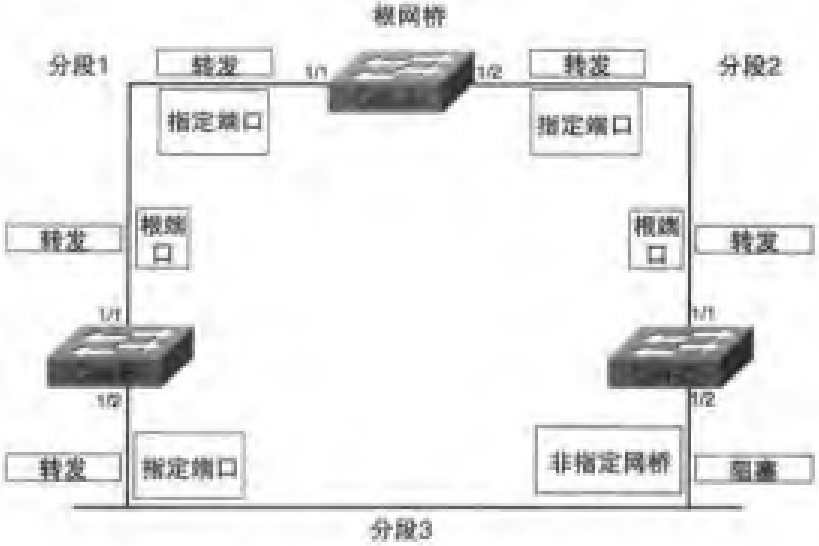


图6-38 端口状态

• 交换机把LAN划分为微分段。微分段将冲突的数量减到最小并增加了有效带宽。

• 交换机通过读取帧分组的第2层目的MAC地址实现了高速传输。

• 全双工通信容许两个设备互相同时通信，有效地将LAN交换机所传输的吞吐量加倍。

• 交换机能支持网络中多个同时发生的会话。

• 三种交换模式用于转发通过交换机的帧：存储转发交换、贯穿交换和无分片交换。

• 生成树协议（STP）的主要任务是防止在网络的第2层发生网络环路。

• 使用STP的网桥或交换机的端口处于下面五种状态之一：阻塞、监听、学习、转发或禁用。

为了补充你在本章所学到的知识，请参考本书所附带CD-ROM中特定章的视频、插图和e-Lab实验活动。

6.5　关键术语

10BASE2　使用10欧姆细同轴电缆的10Mbit/s基带以太网规范。10BASE2是IEEE802.3规范的一部分，其对每个分段有185m（606英尺）的距离限制。

10BASE5　使用标准（粗）50欧姆基带同轴电缆的10Mbit/s基带以太网规范。10BASE5是IEEE802.3基带物理层规范的一部分，其对每个分段有500m（1640英尺）的距离限制。

10BASE-T　10Mbit/s基带以太网规范，使用两对双绞线电缆连接（3、4或5类）：一对用于传输数据，另一对用于接收数据。10BASE-T是IEEE802.3规范的一部分，其对每个分段有大约100 m（328英尺）的距离限制。

100BASE-FX　100Mbit/s基带快速以太网规范，每个链路使用两股多模光纤电缆。为了保证正确的信号计时，100BASE-FX链路在长度上不能超过400m（1312英尺）。它是基于IEEE802.3标准的。

100BASE-TX　100Mbit/s基带快速以太网规范，使用两对UTP或STP连接。第一对用来接收数据；第二对用来发送。为了保证正确的信号计时，100BASE-TX分段在长度上不能超过100m（328英尺）。它是基于IEEE802.3标准的。

1000BASE-T　1000Mbit/s基带吉比特以太网规范，使用四对5类UTP电缆，最大100m（328英尺）的长度。

1000BASE-SX　1000Mbit/s基带吉比特以太网规范，在多模光纤电缆上使用短激光波长，最大550m（1804.5英尺）的长度。

1000BASE-LX　1000Mbit/s基带吉比特以太网规范，在长途光缆上使用长波长，最大10,000m（32808.4英尺）的长度。

4D-PAM5　用于1000BASE-T的符号编码方法。从8B1Q4数据编码接收到的四维五进制符号（4D）采用五个电压电平（PAM5）发送出去。每个符号周期并行发送四个符号。

8B1Q4　对于IEEE802.3标准，它是1000BASE-T所用的数据编码技术，即把GMII数据（8B—8比特）转换为四个五进制符号（Q4），并在一个时钟期间发出。

网桥协议数据单元（*bridge protocol data unit, BPDU*）　生成树协议hello分组，在可配置的间歇发送，以在网络中网桥间交换信息。

贯穿交换（*cut-through switching*）　一种分组交换方法，其将通过交换机的数据连续发出，使得分组在完成进入输入端口之前，其分组的前面部分就已在输出端口离开交换机。使用贯穿分组交换的设备读、处理分组，一旦找到其目的地址且确定输出端口就转发分组。也可*参阅存储转发交换*。

编码（*encoding*）　通过它的处理，比特由电压来表示。

无分片交换（*fragment-free switching*）　在转发开始前，滤掉占分组错误多数的冲突分片的交换方法。

延迟（*latency*）　在设备接收到帧和帧被转发出目的端口之间的延迟。

曼切斯特编码（*Manchester encoding*）　IEEE802.3和以太网所采用的数字编码机制，其中比特时间中的跳变作为时钟；比特时间的前半部为高电平表示1。

微分段（*microsegmentation*）　将网络分为更小的分段，通常是为了增加网络设备的堆叠带宽。

不归零码（*nonreturn to zero, NRZ*） 在比特间歇没有信号跳变（不返回到0 V电平），维持不变电压电平的信号。

反转不归零码（*nonreturn to zero inverted, NRZI*） 没有信号跳变（不返回到0V电平），维持不变电压电平的信号。它把在比特间歇的开始出现数据认为是信号跳变，把没有数据出现认为是无跳变。

信噪比（*signal-to-noise ratio, SNR*） 可用的传输信号与不需要的信号（噪声）的比率。它是传输质量的量度。线路上好的数据（信号）与坏数据（噪声）的比率以分贝来表示（dB）。

存储转发交换（*store-and-forward switching*） 一种分组交换技术，帧在被转发出正确的端口之前经过了完全的处理。该处理过程包括计算CRC和检验目的地址。另外，帧必须被暂时存储起来直到网络资源（例如，未使用的链路）可以用于转发消息。

生成树协议（*Spanning Tree Protocol, STP*） 网桥协议，其采用生成树算法，使得学习网桥通过创建生成树能动态地避免网络拓扑中的环路。网桥和其他网桥交换BPDU消息以探测环路，然后通过关闭所选择的网桥接口来消除环路。

细线缆网（*Thinnet*） 用于定义细缆的单词，其是IEEE 802.3 10BASE-2标准所制定的较廉价的电缆版本。

波分复用（*wavelength-division multiplexing, WDM*） 多个光纤波长能共享相同的传输光纤。每个信道所占的光谱必须相互适当地隔开。

6.6　复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 以太网中采用何种方法来阐明以太网的工作？

A. TCP/IP

B. CSMA/CD

C. CMDA/CS

D. CSMA/CA

2. 不使用中继器的粗以太网的最大距离是多少？

A. 185m（606.95英尺）

B. 250m（820.2英尺）

C. 500m（1640.4英尺）

D. 800m（2624.64英尺）

3. 10Mbit/s以太网的工作受到计时限制，这是由不超过 _____ 个中继器所划分的一系列不超过 _____ 个分段所提供的。

A. 2，3

B. 3，4

C. 4，5

D. 5，6

4. 快速以太网所支持的传输速率达到多少？

A. 5Mbit/s

B. 10Mbit/s

C. 100Mbit/s

D. 1000Mbit/s

5. 识别出两个吉比特以太网电缆规范。

A. 1000BASE-TX

B. 1000BASE-FX

C. 1000BASE-SX

D. 1000BASE-LX

E. 1000BASE-X

6. 1000BASE-SX的传输介质是什么？

A. 单模和多模光纤上的长波激光

B. 5类UTP铜缆

C. 平衡的、屏蔽的、150欧姆、两对STP铜缆

D. 多模光纤上短波激光

7. 4D-PAM5编码方法用于下列何种吉比特以太网？

A. 1000BASE-LX

B. 1000BASE-SX

C. 1000BASE-T

D. 1000BASE-CX

8. 10 Gbit以太网的IEEE标准是什么？

A. 802.3z

B. 802.3u

C. 802.3ae

D. 802.3

9. 下列哪一个不是微分段的特点?

A. 它实现专用访问

B. 它支持在任何指定时间的多个会话

C. 它增加了每个连接到网络的工作站的性能

D. 它增加了冲突

10. 下列哪一个被LAN交换机用于转发决定?

A. IP地址

B. MAC地址

C. 网络地址

D. 主机地址

11. 下列哪一个是全双工传输的特点?

A. 它提供两个10到1 Gbit/s数据传输路径

B. 它将节点间带宽加倍

C. 它提供了无冲突传输

D. 以上全部

12. 三种常见类型的交换方法是 _____ 、 _____ 和 _____ 。

13. 生成树协议容许下列哪一种情况?

A. 网桥传送第3层信息

B. 一条冗余的网络路径，不受网络中环路的影响

C. 防止环路的静态网络路径

D. 以上都不是

14. 下列哪一个不是STP端口状态?

A. 阻塞

B. 学习

C. 监听

D. 传输

15. 下面哪一个关于网桥和其转发决定是正确的?

A. 网桥工作在OSI第2层，用IP地址来作决定

B. 网桥工作在OSI第3层，用IP地址来作决定

C. 网桥工作在OSI第2层，用MAC地址来作决定

D. 网桥工作在OSI第3层，用MAC地址来作决定

16. 下列哪一个不是网桥的特点?

A. 它们工作在OSI模型的第2层

B. 它们比集线器更加智能

C. 它们不作任何转发决定

D. 它们建立和维持地址表

17. 下列哪一个是微分段的正确陈述?

A. 每个工作站得到自己专用的分段通过网络

B. 所有的工作站组成一个分段

C. 微分段增加了网络中的冲突数量

D. 以上都不是

18. 下列哪一个关于LAN交换机是正确的?

A. 它们修补称为是微分段的网络分片

B. 它们是很高速的多端口网桥

C. 更低的带宽补偿了更高的等待时间

D. 它们要求在所连接的主机上有新的网络接口卡



第7章 TCP/IP协议集和IP寻址

目标

学习完本章之后，你应该能够：

- 识别TCP/IP模型的组件。
- 描述未来的IP版本。
- 讨论TCP/IP模型和OSI模型的关系。
- 识别TCP/IP模型中每一层特有的应用服务和协议。
- 识别TCP/IP模型中每一层之间的关系和排序。
- 阐述IP网络各个相关部分的形式及意义，它们是：IP地址，IP地址分类，保留IP地址空间，私有IP地址空间和IP子网划分。
- 按照IP寻址方案为用户的网络需求计算正确的IP子网及子网掩码数值。
- 阐述IP寻址的演变发展，包括不断增加的IP地址空间需求等。

本章概括介绍*传输控制协议/Internet协议（TCP/IP）*协议集。以TCP/IP的历史和将来作为开始。然后比较TCP/IP协议模型和OSI模型，识别和描述TCP/IP协议集的每一层以及它怎样对应Internet的体系结构。第9章“TCP/IP传输层和应用层”中更详细地介绍了TCP/IP。

本章还深入讨论了IP寻址问题。包括怎样转换十进制和二进制的地址以及怎样识别不同类别的IP地址——A类、B类、C类、D类和E类。IPv4（IP协议第4版），自颁布多年来，一直作为IP地址寻址的标准，但即将被更先进的IP地址寻址方案IPv6所代替。本章将描述并比较IPv4和IPv6。

7.1 TCP/IP介绍

TCP/IP参考模型由美国国防部（DoD）创建，如图7-1所示，因为美国国防部需要一个能经受得住任何情况的网络。进一步说，假设一个处于战争的世界，交叉着各种不同的连接方式——线缆、微波、光纤和卫星链路。再设想一下数据传输的需求，而不管互连网络中任何特定节点、网络的情况如何。美国国防部想让分组在任何时间，任何情况下，从任何位置顺利到达其他的位置。正是这

种苛刻的要求促使了TCP/IP模型的产生。从那时起，TCP/IP就逐渐成为Internet的标准。



图7-1　TCP/IP协议集层次

在阅读TCP/IP模型各层的时候，一定要记住Internet最初的设计目的，这对解释为什么某些事情是现在这个样子会很有帮助。TCP/IP模型有4层：应用层、传输层、Internet层和网络访问层。特别需要注意的是，TCP/IP模型中的有些层的名称和OSI参考模型中的层名称相同，但是不要混淆这两个模型中的对应层次，它们有不同的功能。层的编号是不一致的，所以在OSI模型中第2层所执行的功能与TCP/IP模型中的第2层可能是不同的。例如，在OSI模型中，第3层是IP所处的层，而TCP/IP模型的第2层是IP所处的层。另一个例子，TCP/UDP功能位于OSI模型的第4层（传输层），而在TCP/IP模型中却位于第3层（传输层）。

当前的TCP/IP是老版本。IP协议第4版（IPv4）在1981年9月标准化。1992年，在Internet工程任务组（IETF）的推动下，制定了新一代的Internet协议（IP）标准，通常称为IPng。IPng现在被称为*IP协议第6版（IPv6）*。IPv6，如图7-2所示，还没有得到广泛的应用，但已经被大部分设备厂商采用并发布了产品，它将会成为未来的主流标准。

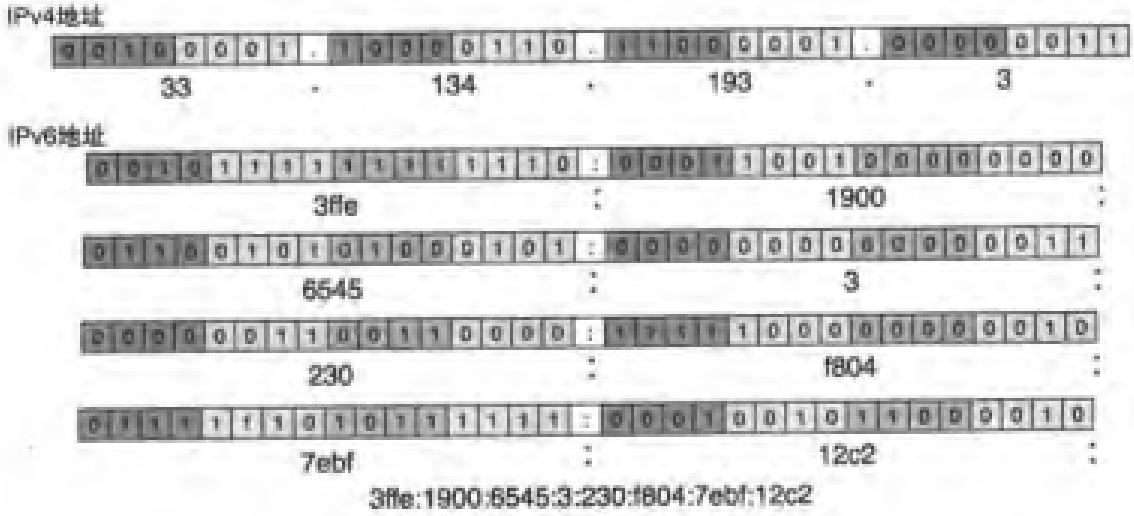


图7-2　IPv4与IPv6的对比

7.1.1　应用层

TCP/IP的高层协议设计成包含OSI模型中的会话层、表示层和应用层的功能。它的*应用层*，如图7-3所示，处理高层协议和有关表示、编码及会话控制的问题。

TCP/IP协议集把所有与应用层相关的功能整合为一层，并且保证这一层的数据能够被下一层正确封装。TCP/IP协议集不仅仅描述了Internet层和传输层的技术规范（比如IP协议和TCP协议），还详细叙述了一些常用的应用层协议。TCP/IP包含很多协议，支持文件传输、电子邮件和远程登录等功能，这些应用包括：

- **超文本传输协议（HTTP）**——这是“万维

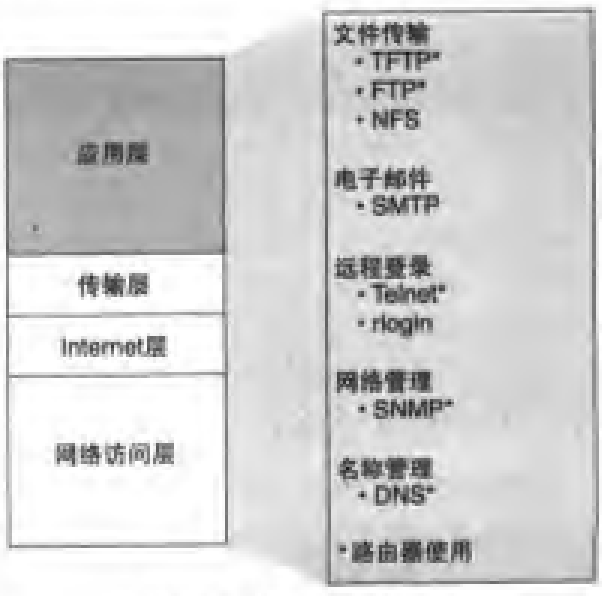


图7-3　TCP/IP应用层协议

网”的基本协议。HTTP协议定义了信息的格式以及传输。它还定义了Web服务器和浏览器针对不同的命令应如何响应。

- **简易文件传输协议（TFTP）**——这是基于用户数据报协议（UDP）的无连接服务。TFTP用于在路由器上传输配置文件和Cisco IOS映像文件，或者在两个支持TFTP协议的系统之间传输文件。它在一些局域网中十分有用，因为在稳定的网络环境中TFTP协议比FTP协议运行更快。
- **文件传输协议（FTP）**——FTP是可靠的、面向连接的服务，使用TCP协议在两个支持FTP的系统之间传输文件。它支持双向二进制文件和ASCII文件的传输。
- **网络文件系统（NFS）**——由SUN公司开发的分布式文件系统协议集。NFS允许通过网络远程访问文件。
- **简单邮件传输协议（SMTP）**——负责管理在计算机网络中电子邮件的传输。除了普通文本，SMTP不支持其他数据的传输。
- **终端仿真（Telnet）**——提供远程访问其他主机的功能。它允许用户登录Internet主机，并在这台主机上执行命令。Telnet的客户端被称为本地主机；Telnet的服务器端称为远端主机。
- **简单网络管理协议（SNMP）**——该协议提供了监控网络设备的方法，以及配置管理，统计信息收集，性能管理及安全管理等。
- **域名系统（DNS）**——该系统用于在Internet中将域名及其公共广播的网络节点转换成IP地址。

7.1.2 传输层

*传输层*提供从源主机到目的主机的传输服务。在端点（源设备和目的设备）之间建立逻辑连接。传输层协议，如图7-4所示，分段和重组上层应用程序发送的数据，并在端点之间重组成同一数据流。传输层数据流提供端到端的传输服务，也称为端到端的服务。

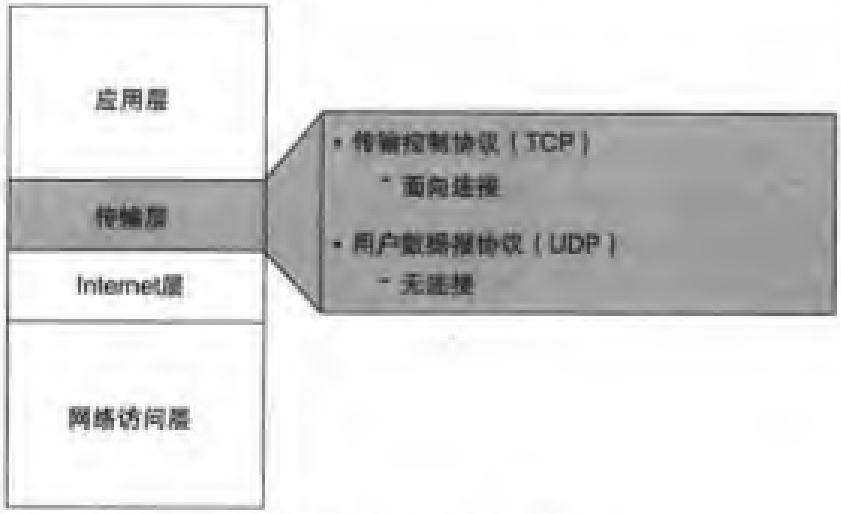


图7-4 TCP/IP传输层协议

传输层数据流要在网络端点之间建立逻辑连接。如果使用UDP，传输层的首要任务是将数据从源设备传送到目的设备。如果使用TCP，传输层主要通过滑动窗口来提供端到端控制，以及利用序列号和确认信息提供可靠性。传输层定义主机应用程序之间端到端的连接。使用TCP，传输层可以提供以下服务，但如果使用UDP，则只能提供前两个服务：

- 分段上层应用程序的数据。
- 把数据段从终端设备发送到其他终端设备。
- 建立端到端的操作。
- 通过滑动窗口提供流量控制。
- 通过序列号和确认信息提供可靠性。

传输层假定能利用网络（看作网云）把数据分组从源设备传送到目的设备，如图7-5所示。在网云中，到达目的设备可能会有多条路径，需要从中选出最佳路径，如图7-6。



图7-5　Internet网云

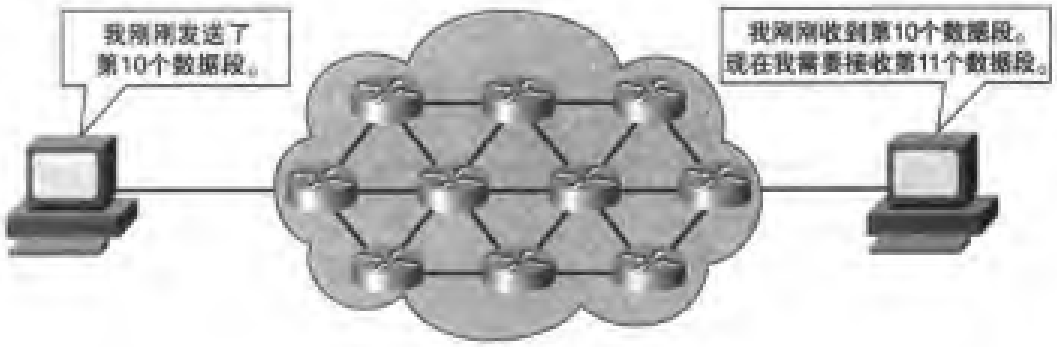


图7-6　Internet路径

7.1.3　Internet层

在OSI参考模型中，网络层使得上层协议不用关心网络中的具体情况，网络层管理跨网络的连接。IP正式来说是作为TCP/IP网络层，因为其在TCP/IP互联网中的重要性，所以一般称为TCP/IP模型中的*Internet层*（见图7-7）。通过TCP/IP协议集传输数据，所有的上层和底层通信都需要通过IP协议。Internet层的目的是利用相应的本层协议发送分组。决定最佳路径和分组交换都在这层完成。对比邮政系统来看，信件投递时，不用太关心信件如何到达目的地（可能有很多条路），最重要的是信件能到达。

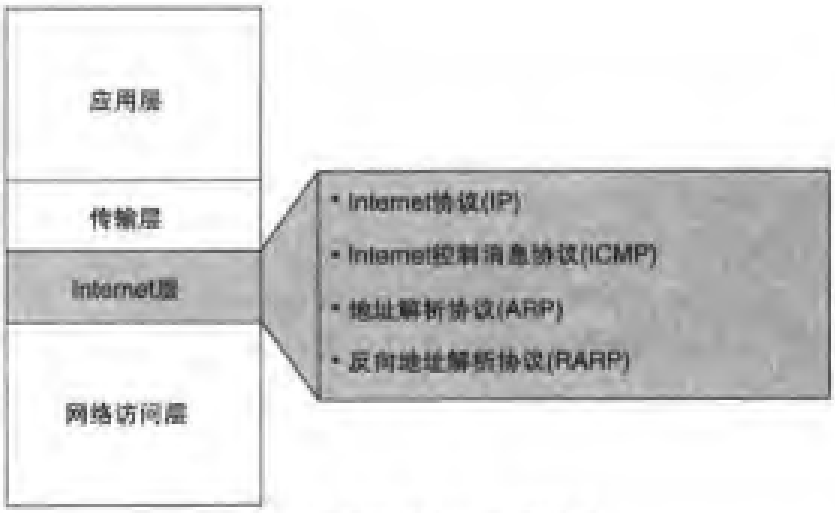


图7-7　TCP/IP Interne层协议

有如下几个协议工作在TCP/IP的Internet层：

• IP——提供无连接，尽力而为的分组传送路由。它不关心分组的具体内容，只查找把分组发送到目的地的路径。

• Internet控制消息协议（ICMP）——提供控制和消息传递能力。

• 地址解析协议（ARP）——已知IP地址，获取相应的数据链路层地址（介质访问控制[MAC]地址）。

• 反向地址解析协议（RARP）——已知数据链路层地址（MAC地址），获取相应的IP地址。

IP实现如下操作：

- 定义分组和寻址方案。
- 在Internet层和网络访问层之间传送数据。
- 路由转发分组到远程主机。

最后，为了阐明这个术语，有时把IP看作不可靠的协议。这并不意味着IP不能在网络中准确地传送数据，只是表明IP不负责错误检测和纠正工作。这些功能一般都由传输层或应用层等上层协议来完成。

7.1.4 网络访问层

如图7-8所示，***网络访问层***又称作主机至网络层（host-to-network）。这一层主要参与在传输IP分组时建立和网络介质的物理连接。本层包括局域网和广域网技术，以及OSI参考模型中的物理层和数据链路层的内容。

应用软件和驱动程序设计成独立于硬件系统，比如以太网卡（NIC）、令牌环网卡、ISDN网卡或调制解调器。这些设备都支持网络访问层功能。这使得用户有些迷惑，因为很多协议是由其他标准定义的，这些标准都支持网络访问层功能。Internet层和传输层协议（IP、TCP和 UDP）以及应用层协议（SMTP、HTTP和FTP）都属于TCP/IP协议集的协议。

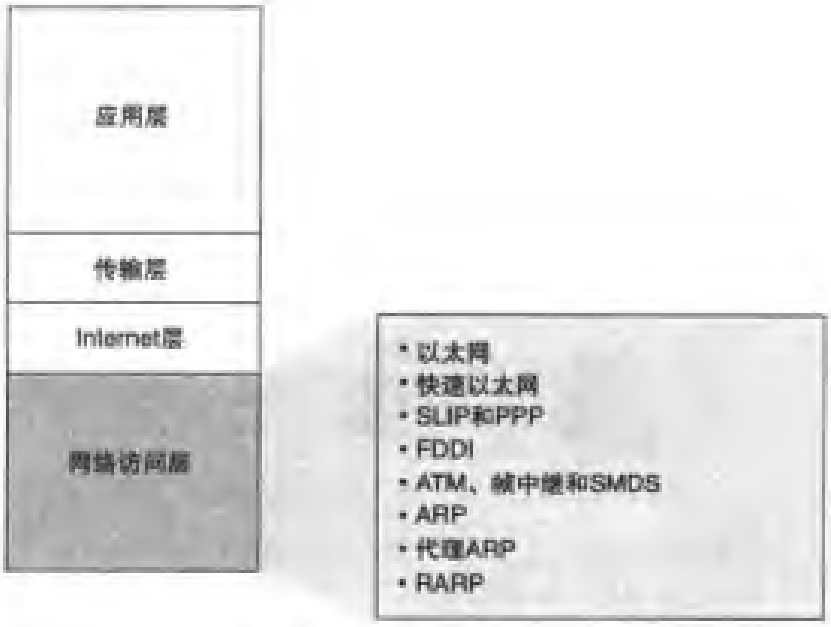


图7-8 TCP/IP网络访问层协议

网络访问层的功能包括IP地址与物理硬件地址的映射，以及将IP分组封装成帧。基于不同硬件类型的网络接口，网络访问层定义了和物理介质的连接。

网络访问层配置的一个典型例子是Windows系统采用第三方的网络接口卡（NIC）。根据不同的Windows版本，操作系统会自动检测NIC，安装相应的驱动程序。如果使用一个版本较老的Windows系统，用户必须使用指定的网卡驱动程序。网卡厂商一般在软盘或光盘中提供相应的驱动程序。

7.1.5 OSI参考模型与TCP/IP参考模型的比较

图7-9将OSI模型和TCP/IP模型做了比较。

注意上述两个模型既有相同点又有不同点：

- 相同点

— 都是分层的模型。

— 都有应用层，尽管所包含的应用服务不同。

— 都有类似的传输层和网络层。



图7-9 OSI模型与TCP/IP模型的比较

— 都使用分组交换（而不是电路交换）技术。

— 网络专业人员对两者都要熟悉。

• 不同点

— TCP/IP模型将表示层和会话层合并到应用层之中。

— TCP/IP模型将OSI模型的数据链路层和物理层合并成为网络访问层。

— 由于具有较少的层数，TCP/IP模型看上去较为简单。

— OSI模型的传输层能够保证分组的可靠传输，而TCP/IP模型的传输层如果采用UDP则不能保证分组的可靠传输。

TCP/IP协议是围绕Internet开发的标准，它也由此赢得信任。相反，OSI参考模型一般不用来构建网络，它常被用来帮助理解通信过程。

7.1.6　Internet体系结构

尽管Internet非常复杂，但也遵循一些基本的理论。本节将研究Internet基本的体系结构，即一些看上去很复杂的简单理论。通过大规模地重复应用这些理论，不论何时、何地，任何人之间都可以进行几乎实时的全球性数据通信。如图7-10所示，X和Y是两台连网的计算机，他们可以跨越全球进行通信。



图7-10　通过路由器相连的两个网络

局域网的局限性在于它的可扩展性较差：

• 可以连接的主机数有限。

• 可跨越的地理范围有限。

通过对局域网进行有效的分层设计，现在局域网上可连接的主机数量已经取得了相当大的增长，并且也发展了很多新技术，如城域光缆、吉比特以太网、万兆以太网。然而，主机最终还是要依靠长距离，类似于广域网的分组交接网络获得资源。

Internet体系结构的一种假定就是主机以及所在的局域网与网络间如何获得消息无关。

要掌握Internet体系结构的概况，一种途径就是观察源主机与目的主机以及中间所经过的任何主机之间应用层的交互。将相同的应用程序安装到所有连接到网络上的计算机上，就可以很轻松地在大型网络上传递信息。但这样做不利于升级。要使新软件的功能生效，需要网络中所有主机都安装新软件；而且硬件的升级也需要重新修改软件。任何一台中间主机或它的应用程序出错就会将消息传递链打断。

相反，Internet利用网络层互联的规则。OSI模型就是一个很好的例子，目的是将网络功能封装到独立的模块中。第1层和第2层允许有多种局域网技术存在。第5、6、7层允许有不同的应用功能。然而你需要的是一个能隐藏底层和上层细节的系统，这个系统可以让中间网络设备中继数据流量，而不用理会局域网的细节（用户只需管理好本地，从全局来看网络是透明的）或应用程序产生网络流量的细节。

这就引出了另一个概念：***网络互联（internetworking）***——构建网络的网络。网络的网络是指互联网络（internet，注意是小写的i）。（大写的I通常指由美国国防部创建的网络发展起来的Internet，也就是人们平时访问WWW服务所用的网络，称为Internet）。网络互联（internetworking）必须具有以下特征：

• 所连接的网络和计算机的数量可扩展。

- 能处理长距离的数据传输，包括跨越全球或近地空间。
- 具有灵活性以适应不断的技术更新。
- 能适应网络中的各种动态环境。
- 具有成本效益。
- 是一个可以在任何时间、任何地点可以与任何人通信的系统。

图7-10是物理网络之间通过专用的计算机（路由器）相连的例子。此图与导致思科公司于1984年在斯坦福大学创立以及路由器的发明的问题不同。这些网络可以说是与路由器“直连”。在这里，路由器对于处理两个网络通信时所需要的“转换”是很有效的。由于用户需要在任何时间、任何地点与任何人建立连接，而这个方案只连接了两个网络，所以它很快就不能满足要求了。

图7-11显示了两台路由器连接三个物理网络。现在路由器需要完成更为复杂的决策。因为不论是否直连在一起，所有网络上的所有用户都需要相互通信，路由器必须通过某种途径处理这个问题。

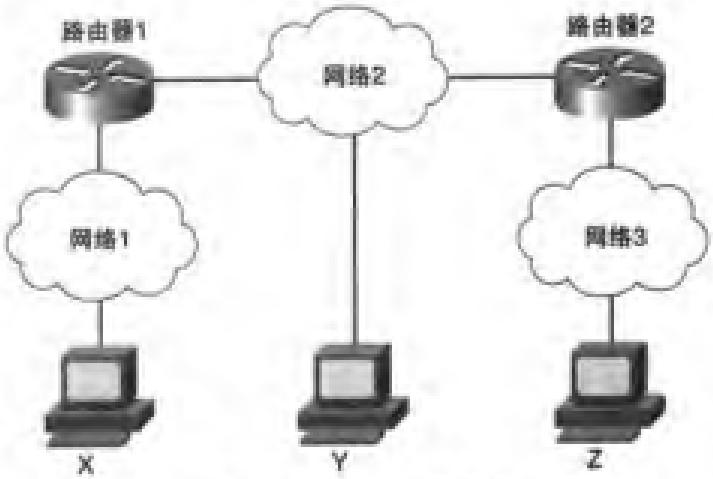


图7-11 本地与远程网络

一种方法是让路由器维护所有的用户计算机及到达他们的路径列表。路由器可以根据目的主机和所知用户列表来决定是否需要转发数据分组以及向哪里转发数据分组。然而，随着用户数量的不断增长，这种方法将会很快出现扩展性不强的问题。如果只让路由器保留网络的列表，细节情况留给本地物理网络，情况会怎样呢？相比之下，这种方法要更好一些，而且扩展性更强（根据目的网络来转发数据）。这样，路由器就可以转发数据。理论上，路由器可以将所连接的网络信息共享给其他路由器，这样就可以把这一思想扩展到许多路由器。

图7-12就是网络扩充的结果，也是用户希望看到的结果：全球互联网络，最终用户穿过网云获取分组只需要关系很少的细节问题。但是要达到这样的目标，网络的物理和逻辑拓扑都将极为复杂。实际上，Internet是指数增长的，设备和协议也在不断地改善以容纳更多的用户。Internet已经如此之庞大，有超过9万台核心路由器和3亿多终端用户，这也证明了它的基本体系结构的合理性。

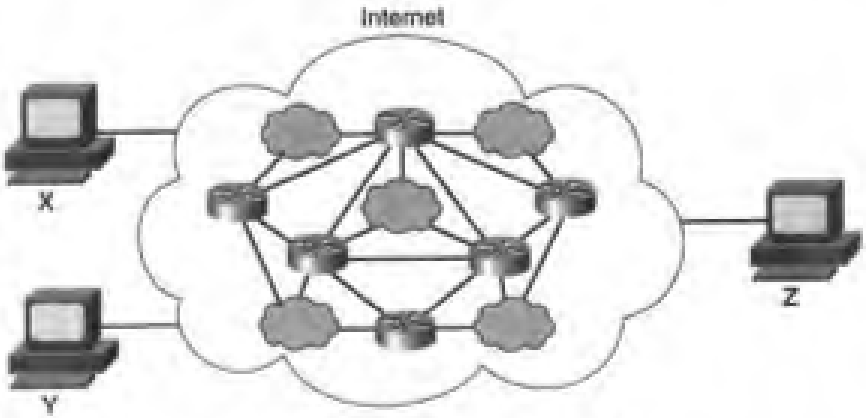


图7-12 对用户隐藏物理网络细节

这样，利用特定的硬件、软件和网络协议，位于世界上任何地方的两台计算机就可以进行可靠的通信（“任何地方/任何时间/任何人”）。即使它们并非直连的（甚至没有接近于直连的网络），通过相互协作以及在网络的网络上移动数据的程序，也可以使Internet成为可能。

7.2 IP地址

网络层负责在网络中传输数据。该层的功能是发现网络中的最佳路径。网络设备使用网络层地

址来决定数据的流向。本节主要讲述5类IP地址、子网划分、子网掩码以及它们在IP地址方案中的角色。此外，本节还将讨论公有地址与私有地址、IPv4寻址与IPv6寻址、单播通信与广播通信之间的区别。

7.2.1　32位点分十进制IP地址

对于任何两个通信的系统，它们必须能够识别和定位对方。如图7-13所示，尽管这些地址不是实际的网络地址，但它们可以代表地址概念。图中，A和B标识网络，数字标识主机。字母（网络地址）和数字（主机地址）结合起来，为网络中的每台设备分配惟一的地址。在日常生活中，常使用名字或数字（例如电话号码）作为惟一的标识符。同样地，TCP/IP中的每台计算机至少要有一个惟一的标识符或地址。这个地址允许一台主机定位网络中的其他主机。

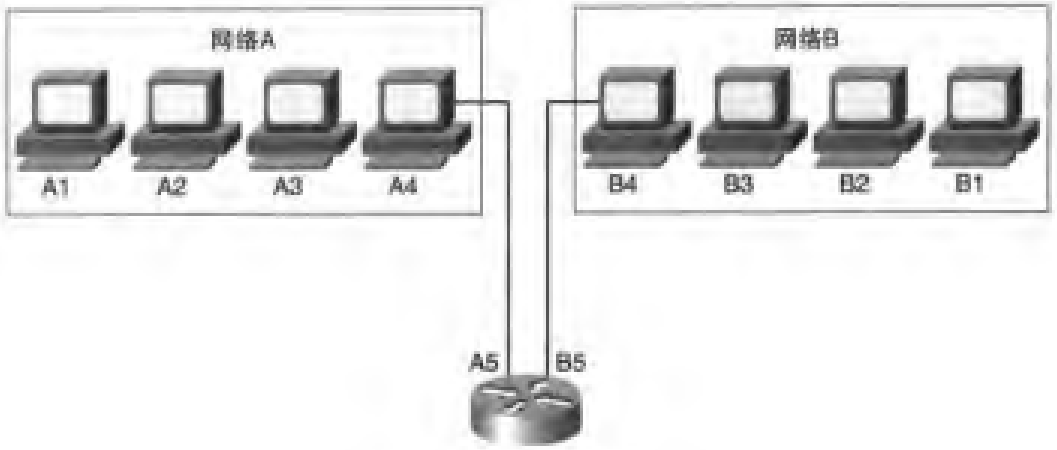


图7-13　主机地址

一台主机可以连接到一个以上的网络，如图7-14所示。该例显示了一台主机连接到两个不同的网络中。这是由于该计算机中装有两块网卡，称为双宿主设备（dual-homed）。值得注意的是，这台主机的两个接口处于不同的网络中，因此在地址结构中它们有不同的网络标识。另一点重要的是，不能通过这台主机传递数据，除非指定让它这样做，它仅仅可以访问两个网络。在这种情况下，必须为系统分配多于一个地址，每个地址标识它到不同网络的连接。严格地讲，不能说一台设备有一个地址，而是到网络的每一个连接点（或接口）有一个地址，这使得网络中的其他主机可以定位它。

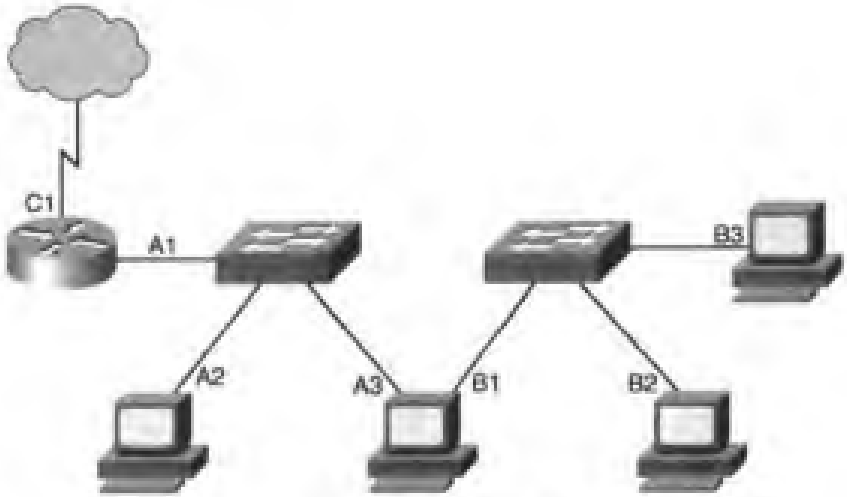


图7-14　双宿主设备

如图7-15所示，IP地址以32位二进制位的形式存储于计算机中。为方便使用，通常写成4个由点分隔的十进制数。例如，一台主机的IP地址为192.168.1.2，另一台主机的IP地址为128.10.2.1。这种书写地址的方法称为*点分十进制格式*。在这种格式中，每个IP地址被写成由点分隔的四部分。因

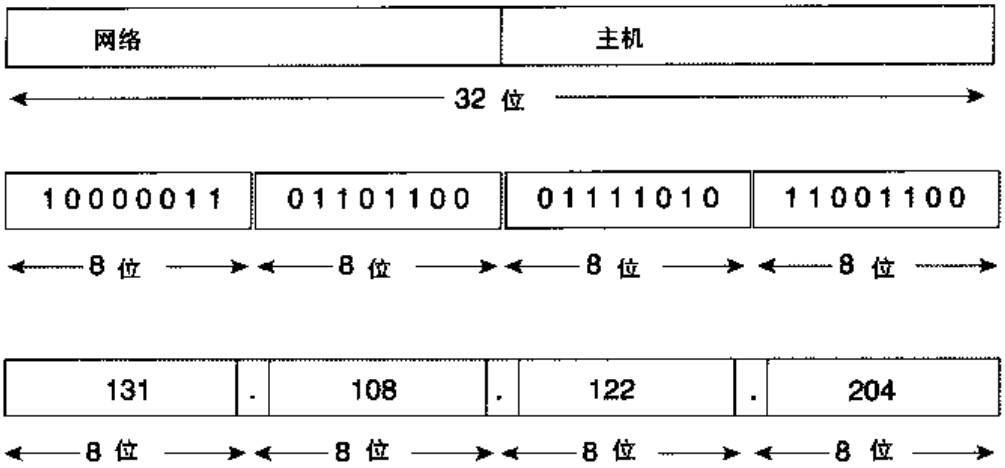


图7-15 IP地址格式

为每部分是由8位二进制组成，因此称为一个八位组（octet）。例如，192.168.1.8使用二进制表示为11000000.10101000.00000001.00001000。人们显然更容易理解点分十进制的格式而不是用0和1表示的二进制。这避免了使用二进制数造成的转换错误。

如图7-15所示，使用点分十进制格式更容易理解。图中的二进制数和十进制数代表相同的值，但是我们更容易理解点分十进制的数值。而长长的0、1的二进制字串容易出现转换和遗漏错误。换句话说，比起点分二进制数值，更容易看出以下两个数值之间的关系：

192.168.1.8

192.168.1.9

我们来看一下二进制数的表示方法，很难看出它们是连续的编号：

11000000.10101000.00000001.00001000

11000000.10101000.00000001.00001001

7.2.2 十进制和二进制转换

解决数学问题通常可以使用很多方法，二进制到十进制之间的转换也不例外。本节给出了一种转换方法，如果有其他更容易的方法，也可以使用。

为了将十进制数转换成二进制数，首先要找到对应于该十进制数的2的最高次幂，如表7-1所示。如果是由计算机来完成这项工作，起始的逻辑位应从一个字节或两个字节中的最高位开始。

表7-1 计算可用主机地址

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

正如前面所提到的，一个字节通常是由8个二进制位组成。一个字节的最大数值为255，但有时实际数值要大于255。针对这种情况，须将字节组合起来。如果是一个16位的数，可以使用两个8bit字节；如果是一个24位的数，可以使用3个8bit字节。应用8 bit数字的规则为：当前纵列的数值等于前一列数值的2倍。表7-1显示了这些值（以两个字节/16位开始），这对于学习子网划分非常重要。

因为计算机通常使用字节，很容易从字节的边界处开始计算，如表7-2所示。为了更好地说明这一点，我们举个例子，十进制数6783。因为该数大于255，而255是一个字节中的最大数值，所以应该使用两个字节，从2^{15}开始计算。计算结果是：00011010 01111111。

表7-2　十进制－二进制转换表

该位的幂	十进制数	该位的值	二进制数	余数
2^{15}	6783	32678	0	6783
2^{14}	6783	16384	0	6783
2^{13}	6783	8192	0	6783
2^{12}	6783	4096	1	2687
2^{11}	2687	2048	1	639
2^{10}	639	1024	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

再举一个104的例子。因为该数小于255，所以转换可以在一个字节内完成，如表7-3所示。

表7-3　8位内的转换

该位的幂	十进制数	该位的值	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

104转换成二进制的结果为01101000。

这种方法适用于任何十进制的数。我们来考虑一下十进制数1,000,000。因为1,000,000大于两个字节内支持的最大数（65,535），所以至少需用3个字节。一直乘以2到第24位（3个字节），得出8,388,608，意味着24位支持的最大数为16,777,215。所以从第24位开始计算，直到第0位。最后得出十进制1,000,000转换成二进制为00001111 01000010 01000000。

二进制到十进制的转换正好相反。首先将二进制位填入表中。如果该位为1，则加上相应的值，直到得出最后的结果，如表7-4所示。该表显示了将二进制数00000100 00011101转换成十进制数，结果为1053。

表7-4　基于16位的二进制到十进制的转换

该位的幂	十进制数	该位的值	二进制数	取值
2^{15}	0	32768	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

续表

该位的幂	十进制数	该位的值	二进制数	取值
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

7.2.3 IPv4寻址

如图7-16所示，IP在发送网络和目的网络之间转发分组。因此，在这种寻址方案中必须包括源网络和目的网络的标识符。通过使用目的网络标识符，IP协议可以向目的网络发送数据分组。当数据分组到达与目的网络相连接的路由器时，IP协议必须定位与目的网络相连的主机。这种工作方式和邮政系统类似。当发送一封信件时，首先要根据邮政编码把信发送到收件人所在城市的邮局；然后，邮局根据街区地址找到最终的收件人。这是一个两步的过程。

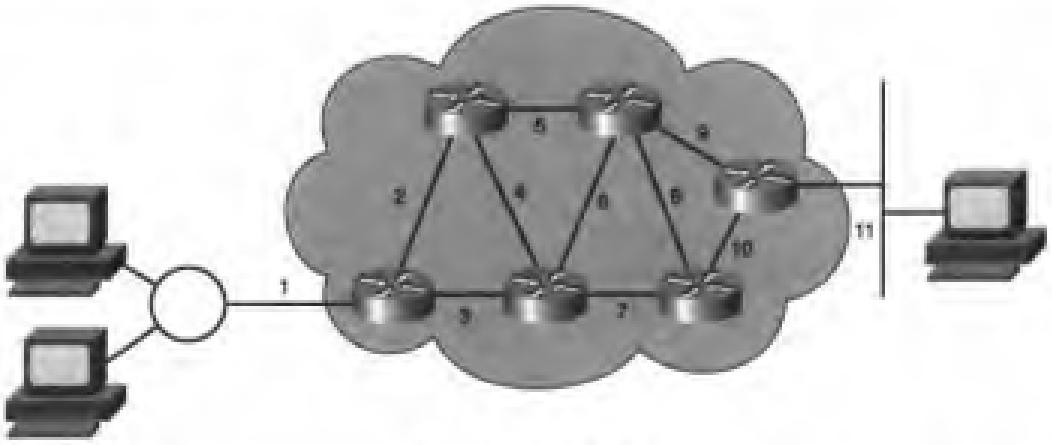


图7-16 通信路径

如图7-17所示，每个IP地址由两部分组成。一部分标识系统所连接的网络，另一部分标识该网络中的特定系统。因为这种地址结构包含不同的级别，所以该类型的地址称为分层次的地址结构（hierarchical address），如图7-18所示。图中，每个八位组的范围从0到255。每个八位组分成256个小组，这些小组中的每一个又可分成256个小组，其中每个小组包含256个地址。地址结构中的每个小组可以逐层地组成地址，地址结构中一条分支下的所有组看作同一整体。一个IP地址将这两个标识符结合成一个编号。这个号是惟一的，不允许重复寻址。这个编号的第一部分是网络地址。

网络	主机
1	1
	2
	3
2	1
3	1

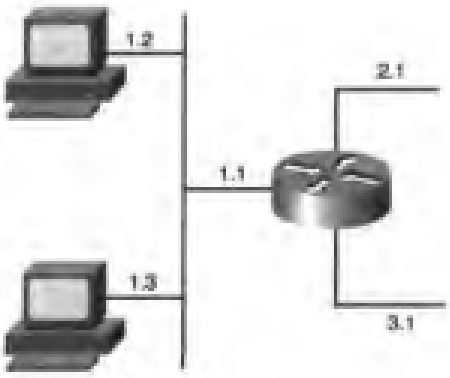


图7-17 IP地址中的网络和主机部分

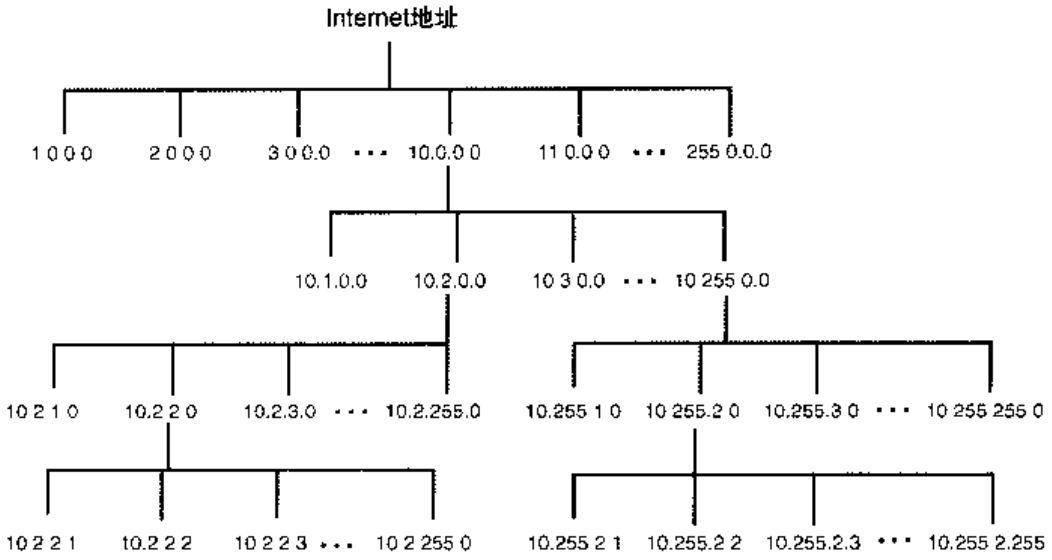


图7-18　分层次的IP地址结构

第二部分，即主机部分，标识位于该网络的特定主机。

用户如何确定地址中的哪部分标识网络，哪部分标识主机？答案由Internet的设计人员决定，他们认为网络规模的大小取决于网络所容纳的主机数量，如表7-5所示。

表7-5　IP地址类别

地址类别	网络数量	每个网络下的主机数量
A	126*	16,777,216
B	16,384	65,535
C	2,097,152	254
D（组播）	-	-

* 127.x.x.x地址段作为回环地址保留，用于测试和诊断。

假设有三种情况。第一种需要少数大型网络，每个网络下有数百万台主机；第二种需要中等规模的网络，每个网络下有数千台主机；最后一种需要有大量的小型网络，每个网络下仅需几百台主机。这样，设计人员就需要将可用的IP地址进行分类，以定义大型网络（A类）、中型网络（B类）和小型网络（C类），如表7-6所示。如何决定IP地址中哪部分标识网络，哪部分标识主机的首要步骤是了解IP地址的分类。

表7-6　识别地址类别

地址类别	高位值	第一个八位组地址范围	网络地址所用位数
A	0	0到127*	8
B	10	128到191	16
C	110	192到223	24
D（组播）	1110	224到239	28

*127（01111111）用作回环（loopback）测试，不能分配给网络。

7.2.4　IP地址分类

为适应不同规模的网络，可将IP地址分类，如图7-19所示，这称为有类寻址。每个32位的IP地址可以分成网络部分和主机部分。每个地址的最高位或起始几位标识地址的类别，如图7-20所示。共有5类IP地址。

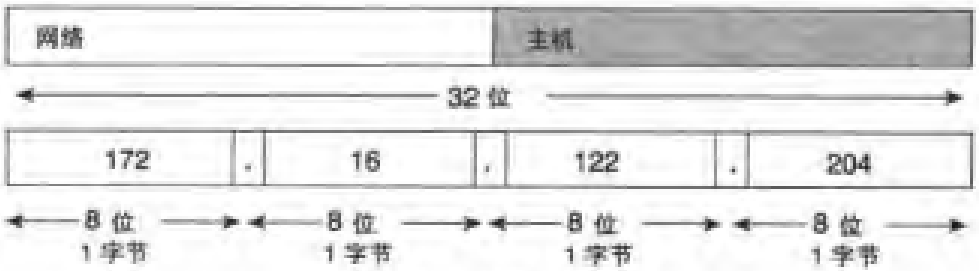


图7-19 区分网络和主机

A类地址

如图7-21所示，*A类地址*用来支持超大型网络。A类IP地址仅使用第一个八位组来标识地址的网络部分。其余的3个八位组用来标识地址的主机部分。

用二进制表示时，A类地址的第1位（最左边）总是0。因此，第一个八位组的最小值为00000000（十进制数为0），最大值为01111111（十进制数为127）。但是0和127两个数保留使用，不能用作网络地址。任何IP地址第一个八位组的取值范围在1到126之间都是A类地址。

B类地址

如图7-22所示，*B类地址*用来支持中大型网络的需求。B类IP地址使用4个八位组的前两个来标识地址的网络部分。其余的两个八位组用来标识地址的主机部分。

B类地址的前两位总是10（1和0）。其余的6位是1或0。因此，第一个八位组的最小值为10000000（十进制数为128），最大值为10111111（十进制数为191）。任何IP地址第一个八位组的取值范围在128到191之间都是B类地址。

C类地址

如图7-23所示，*C类地址*空间是最初地址类型中最为常用的。C类地址用来支持小型网络的需求。

C类地址的前3位总是二进制数110。因此，第一个八位组的最小值为11000000（十进制数为192），最大值为11011111（十进制数为223）。任何IP地址第一个八位组的取值范围在192到223之间都是C类地址。

前缀位数编号	1	7	24
A类：前缀值	0	网络位	主机位
前缀位数编号	2	14	16
B类：前缀值	10	网络位	主机位
前缀位数编号	3	21	8
C类：前缀值	110	网络位	主机位
前缀位数编号	4	28	
D类：前缀值	1110	地址	
前缀位数编号	4	28	
E类：前缀值	1111	地址	

D类地址用于组播。不需要用八位组或位来区分网络地址和主机地址。

E类地址保留，仅用于研究。

图7-20 地址类别前缀



图7-21 A类地址



图7-22 B类地址



图7-23 C类地址

D类地址

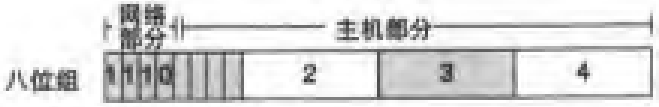


图7-24　D类地址

如图7-24所示，*D类地址*用来支持组播。*组播地址*是惟一的网络地址，用来转发目的地址为预先定义的一组IP地址的分组。因此，一台工作站可以将单一的数据流传送给多个接收者。

正如其他类别的地址空间一样，D类地址空间也有自己的范围。D类IP地址的前4位总是1110。D类地址第一个八位组的范围是从11100000到11101111，即224到239。任何IP地址第一个八位组的取值范围在224到239之间都是D类地址。

E类地址

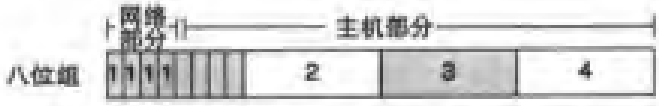


图7-25　E类地址

*E类地址*如图7-25所示。Internet工程任务组（Internet Engineering Task Force，IETF）保留E类地址作为研究使用。因此，Internet上没有发布E类地址使用。E类IP地址的前4位总是1111。E类地址第一个八位组的范围是从11110000到11111111，即240到255。

表7-7显示了每个IP地址类别中第一个八位组的范围。

表7-7　IP地址分类：第一个八位组的范围

IP地址类别	IP地址范围（第一个八位组的十进制数值）
A类	1到126（00000001到01111110）*
B类	128到191（10000000到10111111）
C类	192到223（11000000到11011111）
D类	224到239（11100000到11101111）
E类	240到255（11110000到11111111）

根据IP地址第一个八位组的值来确定地址的类别。

*127（01111111）用作回环（loopback）测试，不能分配给网络。

7.2.5　保留IP地址

有一些地址保留使用，不能分配给网络中的设备。这些保留地址空间如下所示：

- **网络地址**：用于标识网络本身（如图7-26）。上部的图框表示网络198.150.11.0。从局域网外

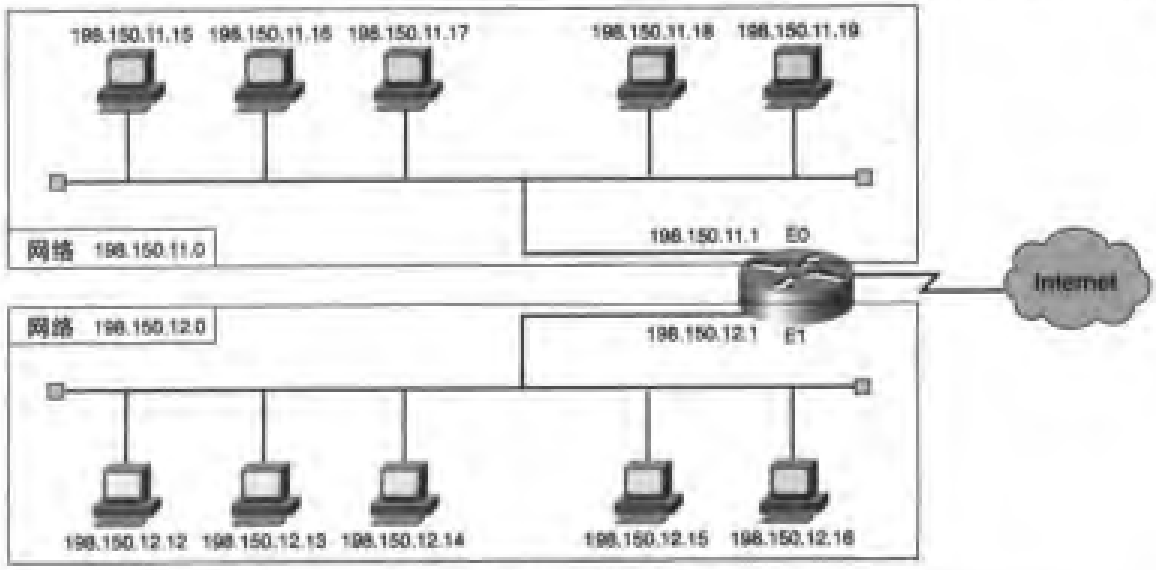


图7-26　网络地址

看，任何发往该网络主机（198.150.11.1到198.150.11.254）的数据，目的网络都是198.150.11.0。只有数据到达局域网时，才进行主机位的匹配。下面图框的情况如上所述，只是网络编号为198.150.12.0。

• **广播地址**：用于向网络中的所有设备广播分组（如图7-27）。上部的图框表示广播地址198.150.11.255。网络中的每台主机（198.150.11.1到198.150.11.254）都要读取发往广播地址的数据。下部图框的情况如上所述，只是广播地址为198.150.12.255。

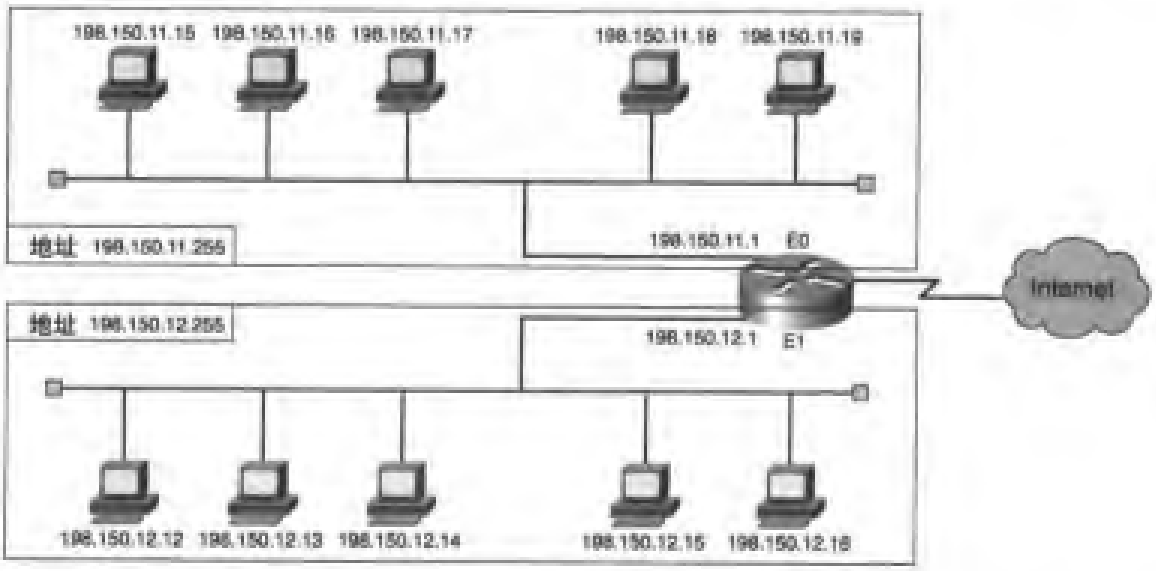


图7-27 广播地址

IP地址中主机位全为0代表网络地址，如图7-28所示。这个B类地址的主机位全为0，这就是它用作网络地址的原因。举一个A类网络的例子，网络地址113.0.0.0包含主机113.1.2.3。当路由器在Internet上转发数据时，它使用该网络地址。如图7-28所示，IP地址176.10.0.0是一个B类网络地址。

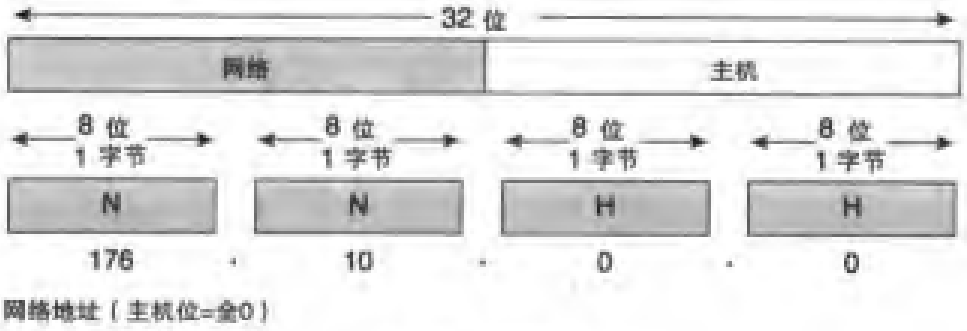


图7-28 网络地址

B类的网络地址，前两个八位组是默认分配的，写作点分十进制数。后两个八位组都是0，因为B类地址的后16位是主机位，它标识网络所连接的设备。这称为单播地址（uni意味着1个）。单播地址仅表明网络中的一台设备。本例中，IP 地址176.10.0.0为网络地址，任何连接在此网络中的设备都不能使用。176.10.16.1为176.10.0.0网络中设备的IP地址。176.10是网络部分，16.1是主机部分。

为了向网络中的所有设备发送数据，需要用到广播地址。当源设备向网络中的所有设备发送数据时，就会发生广播，如图7-29所示。176.10.255.255这个B类地址就是该网络的广播地址。当接收到的分组的目的地址是这个地址时，网络中的所有主机都要对这个数据进行处理。为使网络中的其他主机能处理该广播，源设备必须使用一个他们可以识别和处理的目的IP地址。广播IP地址是主机

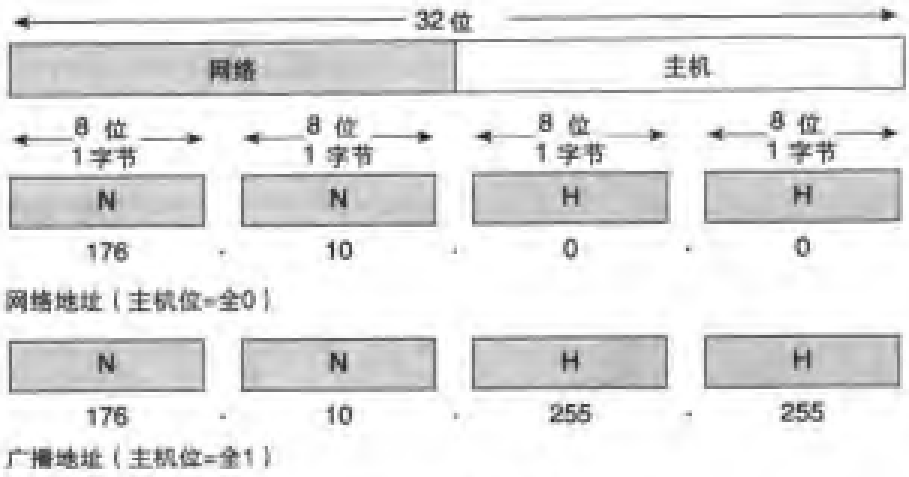


图7-29　广播地址

部分（主机域）全为二进制1的地址。

对于网络176.10.0.0，最后16位组成了主机字段（或称主机部分），发送给网络中所有设备的广播包含了目的地址176.10.255.255（因为十进制255相当于二进制11111111）。

7.2.6　公有地址和私有地址

Internet的稳定直接取决于网络地址公布的惟一性。如图7-30所示是一个有关网络地址方案的问题。两个网络使用同一个网络地址198.150.11.0。当数据传输到路由器时，路由器不知该将数据转发到哪个网络。这种问题会大大增加网络的流量，而且会影响路由器的基本功能。因此，需要建立一些机制以确保地址的惟一性。这个工作最初是由InterNIC（Internet网络信息中心）完成的。这个组织现在已被Internet地址分配中心（IANA）取代了。IANA谨慎地管理着剩余IP地址的分配，以确保不会发生公有地址重复使用的问题。这种重复问题将导致Internet的不稳定，而且使用重复地址在网络中传递数据报会危及Internet的性能。

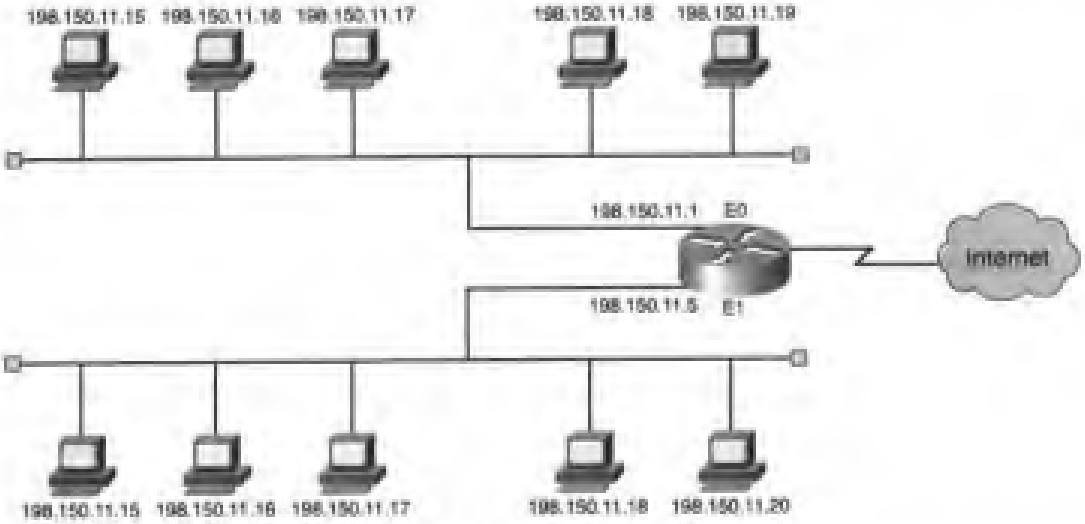


图7-30　需要惟一地址

公有IP地址是惟一的。因为公有IP地址是全局的和标准的，所以没有任何两台连到公共网络的主机拥有相同的IP地址。所有连接Internet的主机都遵循此规则。花费一些费用，便可以从Internet服务供应商（ISP）或地址注册处获得公有IP地址。

随着Internet的快速增长，公有IP地址已几近枯竭。为解决这个问题，开发出了像无类域间路由（CIDR）和IPv6等机制。CIDR和IPv6在以后的章节中讨论。

另一种解决方法是使用私有IP地址，如表7-8所示。如前所述，Internet主机需要一个全局惟一的IP地址。然而，私有网络不连到Internet上，它可以使用任何有效的地址，只要这个地址在该专用网络内是惟一的。许多私有网络的存在依靠公有网络。当然仅抓住“只是任何地址”这句话是不现实的，因为网络最终要连到Internet上。

REC 1918留出3块IP地址空间（1个A类地址段，16个B类地址段，256个C类地址段）作为私有的内部使用的地址。在这个范围内的IP地址不能被路由到Internet骨干网上；Internet路由器将丢弃该私有地址。

表7-8 私有IP地址

IP地址类别	RFC 1918内部地址范围
A类	10.0.0.0到10.255.255.255
B类	172.16.0.0到172.31.255.255
C类	192.168.0.0到192.168.255.255

如果你在非公有的Intranet（内部网）、一个测试实网或家庭网络中寻址，可以使用私有地址取代全局惟一地址。私有IP地址可以与公有IP地址混合使用，如图7-31所示，这可以保留一部分地址用于内部连接。

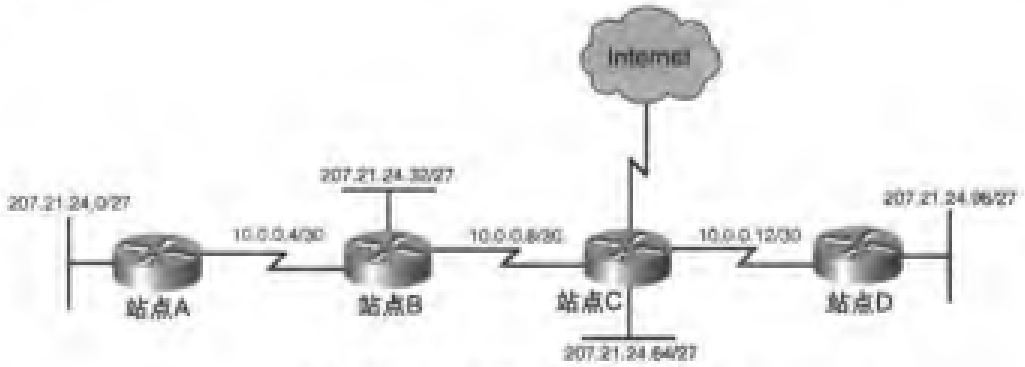


图7-31 在广域网内使用私有IP地址

使用私有地址将网络连至Internet，需要将私有地址转换为公有地址。这个转换过程称为网络地址转换（Network Address Translation，NAT）。通常使用路由器来执行NAT转换。

7.2.7 子网划分介绍

正如CIDR、IPv6和私有地址一样，另一种保留IP地址的方法是***子网划分***（*subnetting*）。这种方法可以将整个网络地址划分成小的部分，以避免IP地址用尽。图7-32显示了将一个B类网络（131.108.0.0）划分成3个子网的例子。讲述TCP/IP的内容不可能不提及子网划分。作为一名系统管理员，必须了解子网划分是划分和标识网络的方法。将网络划分为小的网络不是必要的，但对于大型网络来说，就需要进行子网划分。

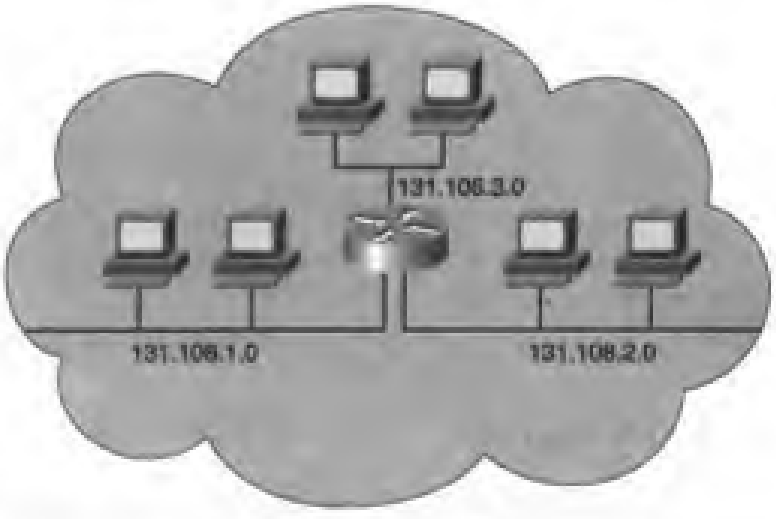


图7-32 子网寻址

简单地说，划分子网，使用子网掩码（subnet mask）将大型网络划分为小部分，或称子网（subnet），如图7-33所示。这好像美国的电话系统，将电话系统分成区号、交换台号码和本地号码。这些电话系统中的号码就好像IP网络中的网络号、子网地址和主机地址一样。

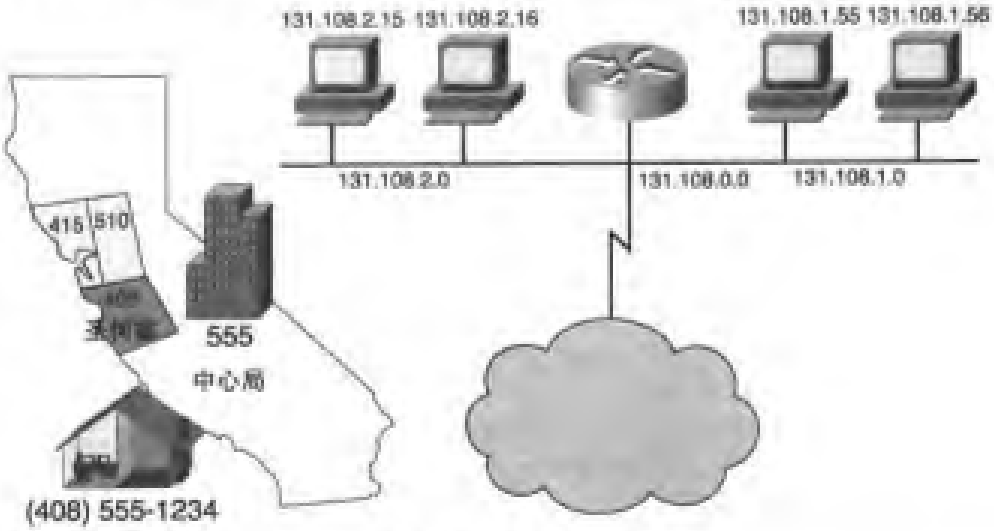


图7-33　子网地址

当需要增加和扩充网络时，系统管理员必须解决这些问题。了解需要多少子网和网络，每个子网下需要多少台主机很重要。使用子网划分，网络可以不再局限于标准的A、B、C类网络掩码，这使得网络设计变得灵活。

子网地址包括A类、B类、C类的网络部分，加上子网字段和主机字段。整个网络的这些字段是从最初的主机部分创建的。网络管理员灵活掌握和决定如何将主机部分划分成新的子网字段和主机字段。

为了创建子网地址，网络管理员从主机字段借位作为子网字段，如表7-9所示。最少借位的位数是2位。如果你只借1位来创建子网，你就只有一个网络号（.0网络）和一个广播号（.255网络）。最多借位的位数是至少要给主机位留2位。表7-9的例子中显示了一个C类IP地址，从主机字段中借位作子网字段。

表7-9　子网地址

第一个主机八位组的十进制表示	子网数	A类地址每个子网下的主机数	B类地址每个子网下的主机数	C类地址每个子网下的主机数
.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	–

实验活动　IP寻址基础

本练习将有助于理解IP地址和TCP/IP网络的操作过程。

7.2.8　IPv4与IPv6

TCP/IP是在20世纪80年代被采用的，它使用两层地址结构，这在当时可以提供充分的可扩展性。不幸的是，这种体系结构不能预见TCP/IP协议最终成为支持信息、商业、娱乐业的网络。20多年前，

IPv4提供了一种地址策略，尽管一度可以提供扩展性，但最终导致了低效率的地址分配。

A类和B类地址占用了IPv4地址空间的75%，如图7-34所示，但只有很少的机构（少于17,000家）可以申请到A类和B类地址。C类地址远远多于A类和B类地址，但是它们仅占40亿IP地址中的12.5%。

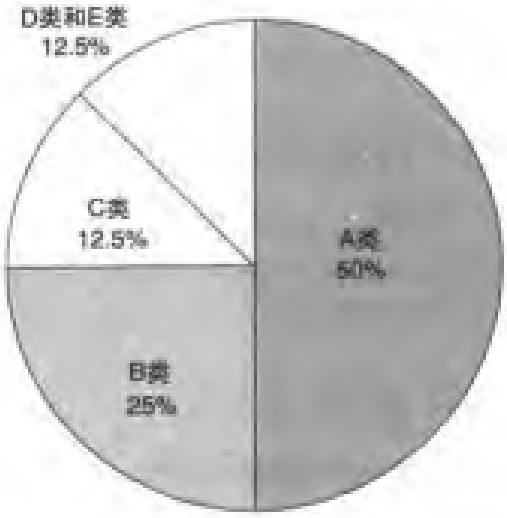


图7-34 IPv4地址分配

不幸的是，每个C类地址仅局限于254台主机，不能满足申请不到A类或B类地址的大型机构的需求。即使有很多的A、B、C类地址，太多的网络地址也会导致路由器负担过重，因为路由器中需要存储庞大的路由表。

早在1992年，IETF明确了两方面内容：

- **剩余IPv4网络地址分配几近枯竭**——那时，B类地址空间已濒临用尽。
- **因为Internet的发展，导致路由表快速增长**——随着越来越多的C类地址的使用，逐渐增加的新的网络信息威胁到Internet路由器的处理效率。

在过去的20年中，已经开发出基于使用32位地址空间而改善IPv4性能的方法。其中两种重要的方法是子网掩码和CIDR。

其间，又定义和开发出了另一种可扩展、可升级的IP版本，即IPv6。IPv6取代IPv4现用的32位地址而使用128位地址空间，如图7-35所示。IPv6使用16进制数来表示这128位。它可以提供160亿IP地址（3.4×10^{38}个地址）。此版本的IP为今后的通信需求提供了充足的地址。

IPv6使用8个16位数来表示128位，4个16进制数一组，如图7-36所示。每4个一组的16进制数间用冒号分隔。

IP协议第4版（IPv4）	4个八位组
11010001.11011100.11001001.01110001	
209.156.201.113	
4,294,467,295 IP Addresses	

IP协议第6版（IPv6）	16个八位组
11010001.11011100.11001001.01110001.11010001.11011100. 110011001.01110001.11010001.11011100.11001001. 01110001.11010001.11011100.11001001.01110001	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	
3.4×10^{38} IP地址	

图7-35 IPv4和IPv6

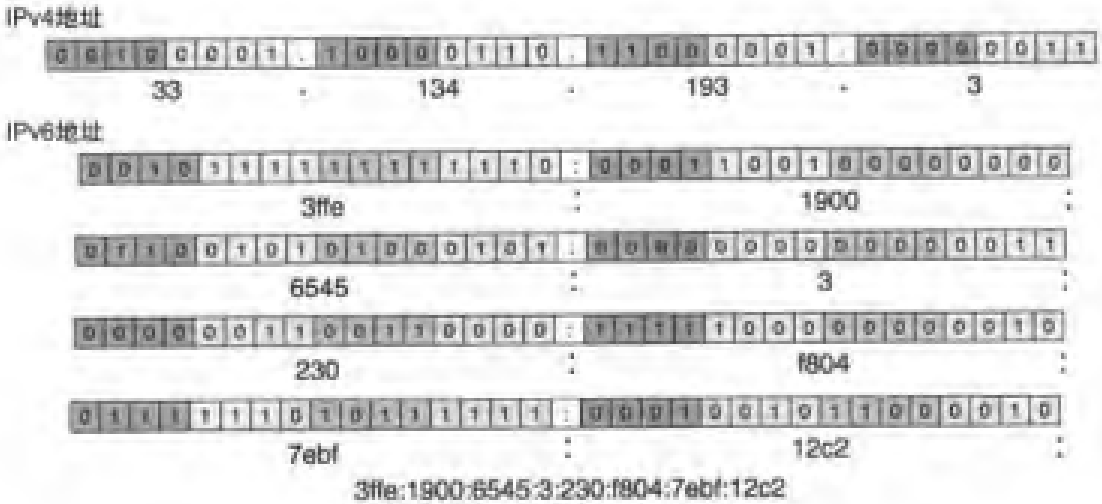


图7-36 IPv6

通过多年的规划和开发，IPv6逐渐在一些选定的网络中实施。最终，IPv6将取代IPv4成为Internet的主要协议。

7.3　IP地址的分配、获取和分层

本节将论述网络设备如何获得IP地址。为实现网络功能，必须依据指定的层次分配IP地址。如何分配以及为什么这样分配将在下面的内容中介绍。IP地址可以静态分配或动态分配。这两种方法本节内容中都会介绍。

7.3.1　获取IP地址

为使一台主机能够获得Internet的网络功能，需要为它分配一个全局惟一的地址。主机的物理地址或称MAC地址仅仅在本地有意义。这意味着MAC地址仅仅能在自己所在的局域网内标识主机。对于其他局域网内的设备该地址没有任何意义。

IP地址是全局地址结构中最常用的地址。它是层次的地址结构，可将单独的地址联合起来作为地址组，如图7-37。这些地址组可以在Internet中有效地传输数据。

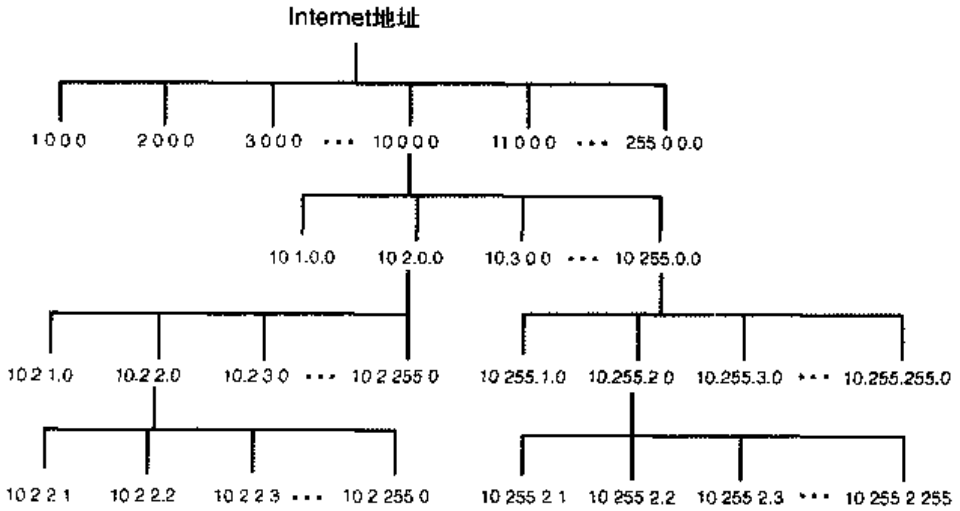


图7-37　Internet地址层次

两种有效的分配IP地址的方法是——*静态分配地址*和*动态分配地址*。后面将讲述静态和动态分配地址的方法。无论选择何种地址分配方法，都不允许任何两个接口拥有相同的IP地址。否则将导致冲突，使得两台主机都不能正常运行。

7.3.2　静态分配IP地址

静态分配IP地址时，需要为每台设备配置一个IP地址。每个操作系统有自己配置TCP/IP的方法。这种方法需要保存地址分配记录，因为如果使用重复的IP地址，会导致网络故障。有些操作系统，像Windows 95和Windows NT在初始化TCP/IP时会发送ARP（地址解析协议）请求来检测是否有重复的IP地址。如果发现重复的地址，操作系统不会初始化TCP/IP，并发送错误消息。不是所有的操作系统能识别重复的IP地址。这里再次强调保存地址分配记录的重要。

如果其他设备需要引用某台设备，就需要为这台设备分配静态的IP地址。Web服务器就是一个很好的例子。如果每次启动Web服务器都要获得一个新的IP地址，将很难找到这台Web服务器。举一个地址改变的例子，如果一个城市总是改变其街道名称和楼宇名称，就不能使用地图来定位特定

的建筑物。如果地址改变，将很难恢复其定位。如果某个建筑物很难到达，人们将不再尝试找到它。

某些类型的设备需要维护静态的IP地址。像Web服务器、网络打印机、应用服务器和路由器都需要永久的IP地址。

7.3.3 地址解析协议

为使设备之间能够互相通信，源设备需要目的设备的IP地址和MAC地址。当一台设备试图与另一台已知IP地址的设备通信时，它必须确定对方的MAC地址。使用TCP/IP协议集中的地址解析协议（Address Resolution Protocol，ARP）可以自动获得MAC地址。ARP协议允许主机根据IP地址查找MAC地址，如图7-38所示。

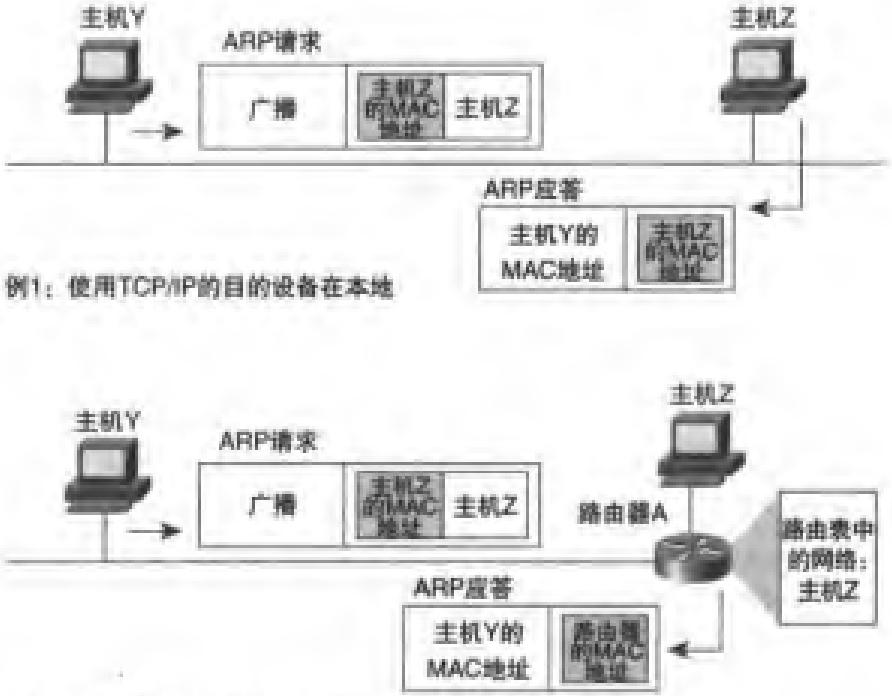


图7-38 ARP通过IP地址获得MAC地址

某些设备维护有ARP表，表中包含同一个局域网内其他设备的MAC地址和IP地址。ARP表将IP地址匹配到相应的MAC地址。ARP表存储在RAM中，每台设备自动维护，如表7-10和表7-11。很少需要手动修改ARP表中的条目。网络中的每台主机维护着自己的ARP表。

表7-10 ARP表条目

Internet地址	物理地址	类型
68.2.168.1	00-50-57-00-76-84	动态

表7-11 198.150.11.36的ARP表

MAC地址	IP地址
FE：ED：F9：44：45：66	198.150.11.34
DD：EC：BC：AB：04：AC	198.150.11.33
DD：EC：BC：00：94：D4	198.150.11.35
FE：ED：F9：23：44：EF	198.150.11.36

只要网络设备想要发送数据，它就要使用ARP表中提供的信息。在图7-39中，源设备想要向其他设备发送数据。

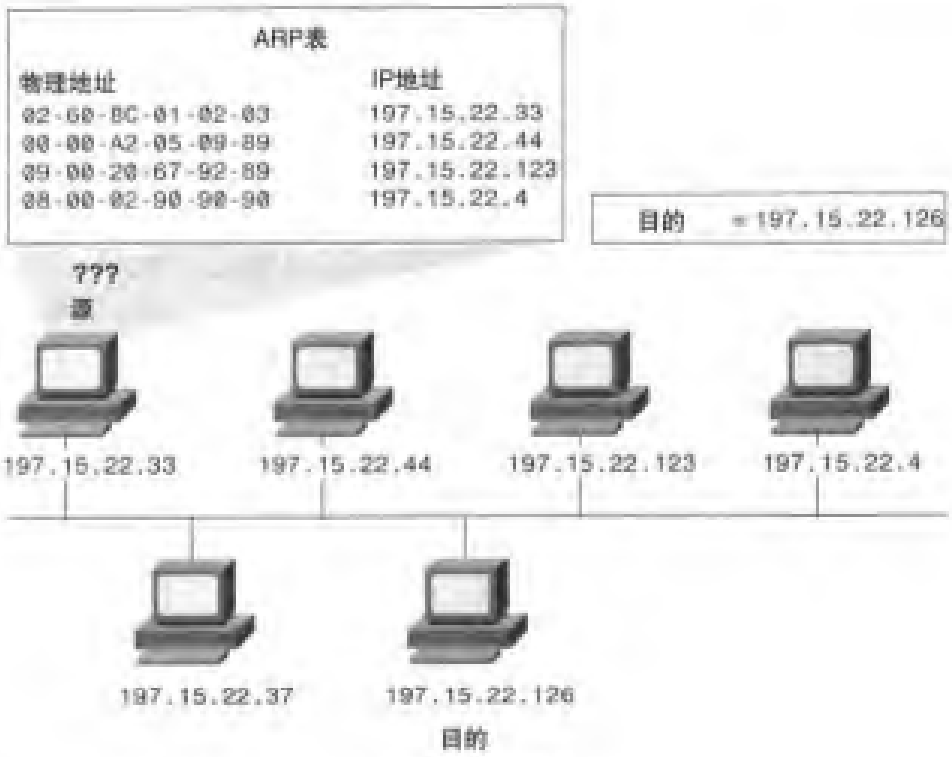


图7-39　ARP表

子网中实施ARP

如果一台主机想要向其他主机发送数据，它必须了解目的主机的IP地址和MAC地址。

如果它不能在自己的ARP表中定位目的主机的MAC地址，它将启动发起ARP请求的过程，如图7-39所示。

ARP请求可以使主机发现目的主机的MAC地址。主机创建ARP请求分组，并将它发送到网络中的所有设备。ARP请求分组分成两部分：

- 帧头。
- ARP消息。

为确保网络中的所有设备都能收到ARP请求分组，源设备使用广播MAC地址。广播MAC地址是将MAC中的所有位设为16进制数的F。因此，MAC地址的广播地址形式为FF-FF-FF-FF-FF-FF。因为ARP请求分组是以广播形式传输的，所以本地网络中的所有设备都要接收该分组，并将它们发送到上一层网络层做进一步的检查。如果一台设备的IP地址与ARP请求中目标主机的IP地址相匹配，那么就由这台设备应答源设备的ARP请求，并告之其MAC地址。这称为ARP应答。

当源设备接收到ARP应答后，它从源设备的硬件地址字段中提取其硬件地址并更新自己的ARP表。这时源设备就可以给要发送的数据适当的地址，包括目的MAC地址和目的IP地址。在把数据发送出网络之前，源设备使用这些新信息用于数据的第2层和第3层封装。当数据到达目的地时，数据链路层作匹配检查，剥去MAC报头，把其中的数据向上送到网络层。网络层检查数据，并找出它的IP地址，这个地址是数据IP报头中所携带的目的地址。网络层剥去IP报头，把封装数据传送到OSI模型的上一层，即传输层（第4层）。这个过程将被重复执行直到分组中的解封装数据到达应用层，在应用层可以读取用户数据。



实验活动　地址解析协议（ARP）

在本实验中使用工作站的ARP表和命令arp -a来确定计算机正确地把网络（第3层）地址解析为MAC（第2层）地址。

缺省网关

缺省网关是与源主机所处网段相连接的路由器接口的IP地址。缺省网关的IP地址必须处在和源主机相同的网段中，如图7-40所示。

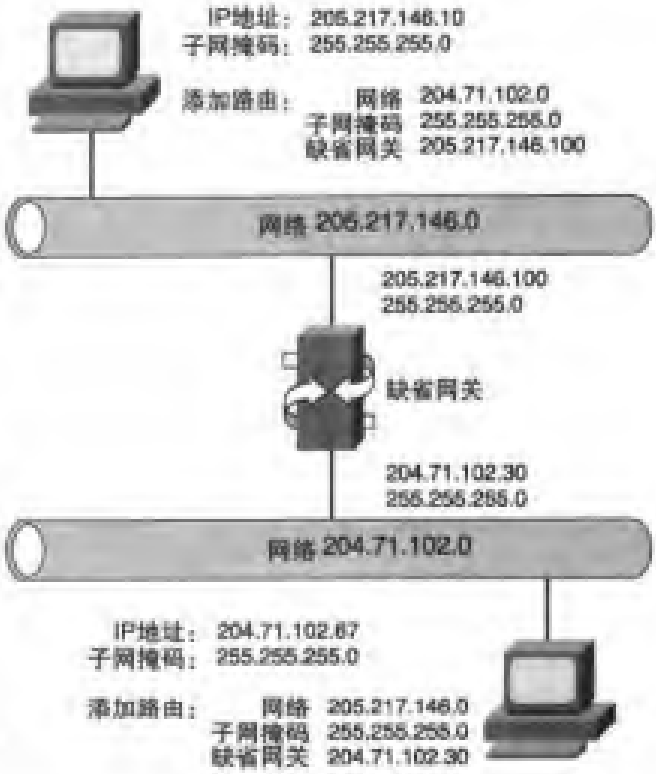


图7-40 缺省网关

7.3.4 反向地址解析协议IP地址分配

反向地址解析协议（RARP）把MAC地址绑定到IP地址。此种绑定允许一些网络设备在把数据发送到网络之前对数据进行封装。一个网络设备或工作站可能知道自己的MAC地址，但是不知道自己的IP地址。设备发出RARP请求，网络中的一个RARP服务器出面来应答RARP请求，如图7-41所示。

让我们设想一个例子，一个源设备想发送数据到另一个设备，源设备知道目的设备的MAC地址，但在ARP表中却不能定位自己的IP地址。为了能让目的设备接收数据，把数据送往OSI模型中的更高层，对源设备进行回应，源设备必须具有自己的MAC地址和IP地址。因此源设备必须初始化一个称为RARP请求的过程，这个请求可以帮助源设备发现自己的IP地址。设备建立一个RARP请求分组，如图7-42所示，并且在网络上发送该请求分组。为了确保网络上的所有设备都能看到该RARP请求，设备使用的是广播MAC地址。

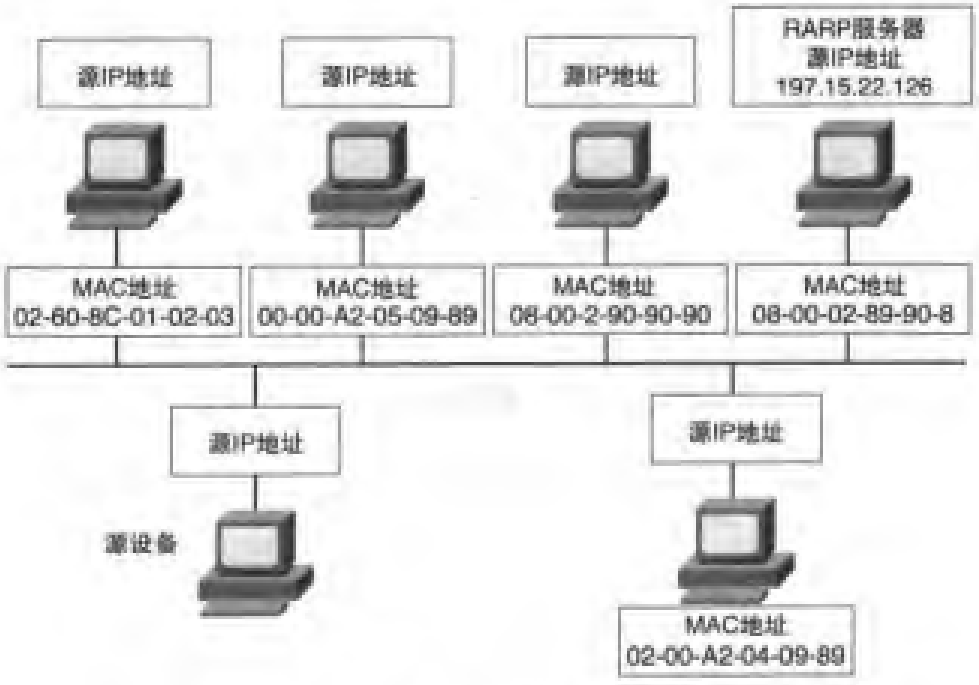


图7-41 RARP协议的IP地址分配

以下是RARP头结构中各组成部分的说明：

- **硬件类型**——指定发送者需要为之取得回复的硬件接口类型。

• **协议类型**——指定发送者所应用的上层协议地址类型。

• HLen——硬件地址长度。

• PLen——协议地址长度。

• **操作类型**——其值含义如下：

— 1：ARP请求。

— 2：ARP响应。

— 3：RARP请求。

— 4：RARP响应。

— 5：动态RARP请求。

— 6：动态RARP应答。

— 7：动态RARP错误。

— 8：InARP请求。

— 9：InARP应答。

图0-16位		16-31位
硬件类型		协议类型
HLen(1字节)	Plen(1字节)	操作
发送者硬件地址（HA）（字节1-4）		
发送者硬件地址（HA）（字节5-6）		发送者协议地址（HA）（字节1-2）
发送者协议地址（HA）（字节3-4）		目标硬件地址（HA）（字节1-2）
目标硬件地址（HA）（字节3-6）		
目标协议地址（HA）（字节1-4）		
RARP报头结构		

图7-42　ARP/RARP消息结构

• **发送者（HA）硬件地址**——以字节数为长度的HLen。

• **发送者（PA）协议地址**——以字节数为长度的PLen。

• **目标（HA）硬件地址**——以字节数为长度的HLen。

• **目标（PA）协议地址**——以字节数为长度的PLen。

RARP与ARP所用的分组格式相同。但在RARP请求中，MAC头和操作码与ARP请求中的不同。RARP分组格式中同时包含源和目的MAC地址的位置。源IP地址字段是空的。因为要广播到网络上的所有设备，所以目的MAC地址设置全部为1（广播地址）。运行RARP的工作站在ROM中有代码来指示他们开始RARP进程。如图7-43所示RARP进程。

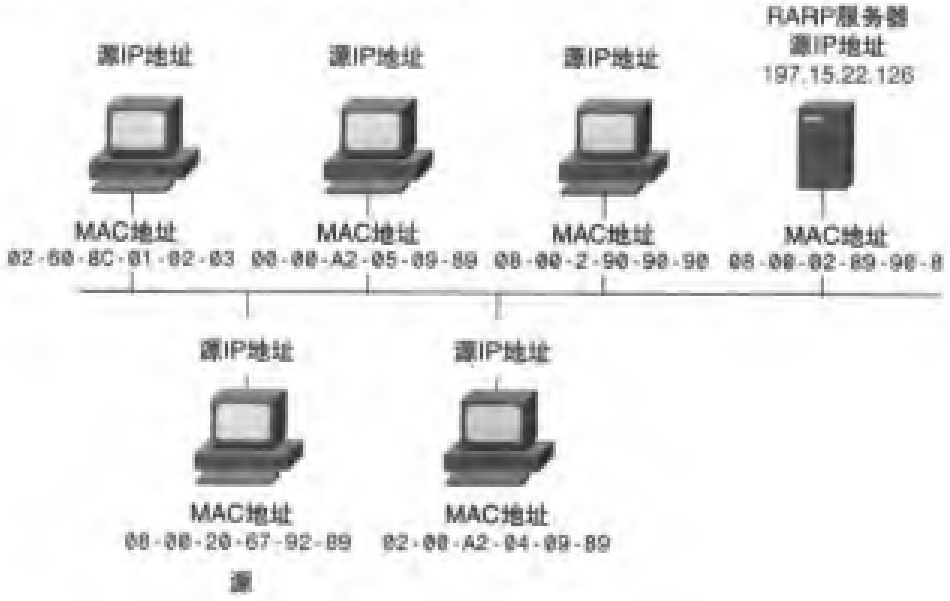


图7-43　RARP进程

7.3.5　自举协议IP地址分配方法

如同RARP一样，BOOTP也运行于客户端/服务器环境中，并且只需要一次分组交换来获得IP信息。但与RARP不同的是，RARP只返回一个四字节的IP地址，而BOOTP数据包中不仅包含了IP地址，还包含了一个路由器地址（缺省网关）、一个服务器地址以及供应商特定的信息，如图7-44所示。

BOOTP的问题之一是：设计并不支持动态地址分配。若用BOOTP，那么管理员就要创建一个配置文件来指定每一个设备的参数。管理员必须添加主机并且维护BOOTP数据库。即使地址可以动态分配，IP地址的数量和主机的数量也是一一对应的关系。这就意味着网络上的每一台主机，都需要有一个分配了IP地址的BOOTP配置文件与之对应。两个配置文件不能使用相同的IP地址，因为这些配置文件可能会同时使用，这样就会有两台主机使用同一个IP地址了。

0-7位	8-15位	16-24位	25-31位
操作信息代码	报头类型（1）	报头长度（1）	跳数（1）
Xid（4字节）			
秒数（2字节）		未使用	
客户机请求IP地址（4字节）			
DHCP客户IP地址（4字节）			
服务器主机地址（4字节）			
中继代理IP地址（4字节）			
DHCP客户硬件地址（16字节）			
服务器主机名（32字节）			
启动文件名（64字节）			
厂商指定部分（32字节）			
BOOTP消息结构			

图7-44 BOOTP消息结构

设备会在启动时使用BOOTP来取得IP地址。BOOTP利用UDP来传送消息；UDP消息是封装在IP分组里的。计算机利用BOOTP发送一个广播的IP分组（利用一个所有位都为1的目的IP地址，点分十进制表示法是255.255.255.255）。BOOTP服务器收到这个广播后发回一个广播。客户端收到数据帧后检查MAC地址。如果发现目的地址字段为自己的MAC地址，并且目的IP地址字段为广播地址，就会采用并且存储这个BOOTP回应消息提供的IP地址和其他信息。

7.3.6 动态主机配置协议IP地址分配方法

动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）是BOOTP的替代者。与BOOTP不同，DHCP允许主机动态取得IP地址，而不用网络管理员为每台机器设置独立配置文件。使用DHCP时需要作的所有工作就是在DHCP服务器上指定一个IP地址范围。主机启动时会与DHCP服务器联系并请求一个IP地址。DHCP服务器选择一个IP地址，租给发出请求的主机。使用DHCP时，计算机TCP/IP配置所需的所有信息都包含在一条消息中。这包括BOOTP消息提供的所有信息以及租用的IP地址和子网掩码。

0-7位	8-15位	16-24位	25-31位
操作信息代码	报头类型（1）	报头长度（1）	跳数（1）
Xid（4字节）			
秒数（2字节）		标志（2字节）	
客户机请求IP地址（4字节）			
DHCP客户IP地址（4字节）			
服务器主机地址（4字节）			
中继代理IP地址（4字节）			
DHCP客户硬件地址（16字节）			
服务器主机名（32字节）			
启动文件名（64字节）			
厂商指定区域（32字节）			
DHCP消息结构			

图7-45 DHCP消息结构

DHCP对于BOOTP主要的改进就是允许用户移动。这就允许用户自由地将网络连接从一个地方换改变到另一个地方。不再需要为网络上的每一个设备都设置一个配置文件，而这在BOOTP系统中是必需的。DHCP先进的关键是可以将一个IP地址租用给一个设备，而在第一个用户释放这个地址之后再重新租用给另一个用户。这就意味着IP地址与网络上的设备的比率是一对多的，并且每一个IP地址都可以被连接到网络上的任意一台设备使用。

除了以下不同之外，DHCP使用的消息格式与BOOTP相同，如图7-45所示。在BOOTP格式中未使用的字段现在用作标志

字段，当前只定义了最高位用作标志字段。这表示一个广播消息。DHCP和BOOTP也定义了如下供应商指定区域：

- 一个字节的可选（Option）字段。
- 一个字节的长度（Length）字段。
- 可变长（由长度字段指定）可选数据（Option Data）字段。

对于DHCP消息类型，其字段的值如下：

- 可选（Option）字段为53，表示为DHCP消息。
- 长度（Length）字段为1，表示数据（Data）字段的长度为一个字节。

当DHCP客户端启动时，进入初始化状态。发送一个DHCPDISCOVER广播消息，这是一个端口号为BOOTP端口的UDP分组。在发送完DHCPDISCOVER消息后，客户端进入选择状态，并且收集DHCP服务器响应的DHCPOFFER。客户端选择所收到的第一个响应消息，然后向DHCP服务器发送DHCPREQUEST分组来协商租期（在需要重新更新之前能保留此地址的时间）。然后，客户端就进入绑定状态，并且开始使用这个地址。图7-46概述了DHCP的状态。



图7-46　DHCP启动状态


实验活动　DHCP客户端设置

在此实验中，你需要将一台联网的计算机设置成DHCP客户端来使用DHCP服务。

7.3.7　地址解析时的问题

网络中的主要问题之一是如何同其他的网络设备进行通信。在TCP/IP通信中，局域网中的数据报必须同时有目的MAC地址和目的IP地址。如图7-47所示，计算机176.10.16.1想要向176.10.16.4发送数据。已经知道对方的IP地址，但数据传输需要176.10.16.4的IP地址和MAC地址。他怎样来得到对方的MAC地址以完成数据传输呢？

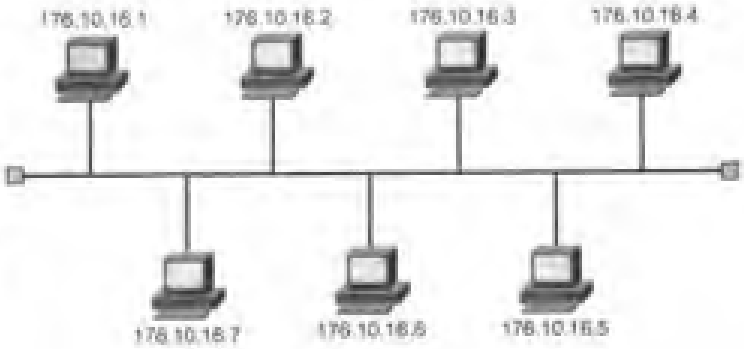


图7-47　地址解析问题

这些地址必须是正确的，并且与目的主机的MAC地址和IP地址相匹配，否则目的主机就会丢弃这些数据报。所以在局域网上必须有办法能够自动地将IP地址解析（或转换）成MAC地址。让用户手工进行解析既苛刻又耗时。这种解决方法也只能解决局域网的问题，当向局域网以外发送数据时又会出现其他的问题。

与非同一物理网段上的主机通信的问题有两方面：

- 取得中间设备的MAC地址。
- 从一个网段向另一个网段传递数据分组以到达目的主机。

图7-48举例说明了这个问题。计算机192.168.10.34需要与计算机192.168.1.1通信。怎样来得到192.168.1.1的MAC地址，并且得到MAC地址又有什么用呢？记不记得MAC地址只在局域网内有用？对于192.168.10.0以外的网络，没有任何作用。所以需要路由器的MAC地址，以便能将数据发出局域网，发送到广域网系统中。

运行代理ARP的路由器会捕获ARP分组。对于请求的IP地址不在本地网络地址范围内的情况，他们会回应自己的MAC地址给请求者。例如，如图7-49所示，如果机器A向机器F发送一个ARP请

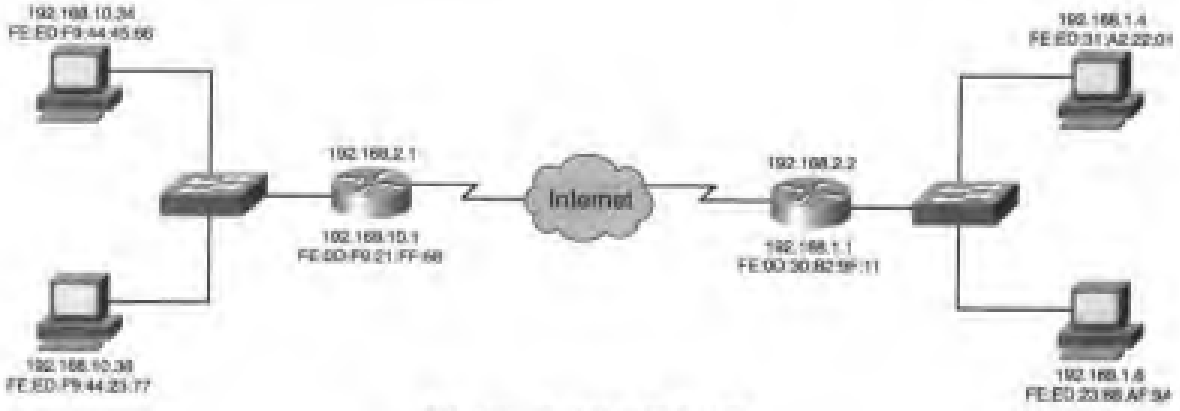


图7-48 远端地址解析问题

求，路由器就会处理这个请求并将它自己的MAC地址回应给机器A，以映射到机器F的IP地址。前面讲过了在设置了缺省网关的情况下数据是怎样发送到其他网段上的。如果源主机没有设置缺省网关，也会发送一个ARP请求。路由器比较目的IP地址与本子网地址，判断目的IP地址是不是与源主机在同一个子网内。如果子网地址相同，路由器就丢弃这个分组。之所以丢弃这个分组是因为目的IP地址与源IP地址处于同一网段。这就意味着处于这个网段上的目的设备就会响应这个ARP请求。例外情况就是当前目的IP地址尚未分配时，在源主机上将会产生一个错误响应信息。

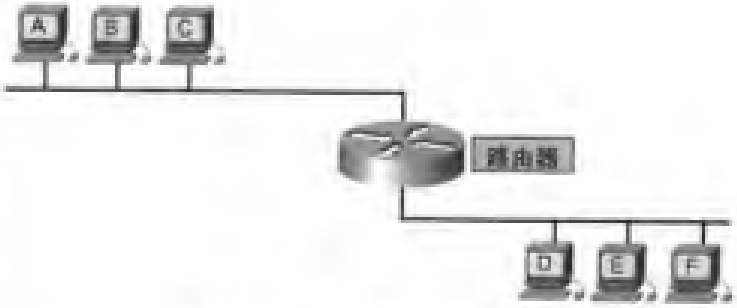


图7-49 代理ARP网络实例

7.4 总结

本章学习了以下知识点：

• 为了给网络管理员提供更大的弹性，网络——尤其是大型网络——常被分割成小网络，称之为子网络或子网。划分子网允许网络管理员可以将一个网络地址分割成多个子网的形式来打破IPv4的限制。这些子网只在这个网络内可见。

• 子网掩码的作用就是告诉设备一个地址的哪部分是子网的网络部分，哪部分是主机部分。

• 网络层的网络互联功能包括数据通信的网络寻址和最优路径选择。

• 怎样解释IP寻址、IP地址分类、保留的IP地址空间、私有IP地址空间和IP子网化。

• 怎样解释IP寻址的发展，包括地址空间增大的需求。

• 计算机需要一个IP地址（分层的地址）以在Internet上进行通信。

• 有两种IP地址配置方法：静态配置和动态配置。

• 当一台设备不知道自己的IP地址时，可以使用RARP、BOOTP或DHCP协议。

• 当发出RARP请求的设备收到RARP回应之后，将相应的IP地址复制到内存缓存中，并且至少在会话结束之前一直驻留在那里。

• BOOTP可以给客户端提供包括IP地址的更多信息。

• DHCP允许计算机移动，根据需要连接到许多不同网络上。

为了补充你在本章所学的知识，请参考本书配套光盘中对应章节的视频、插图和e-Lab实验活动。

7.5　关键术语

应用层（*application layer*）　处理高层协议，以及表示、编码和对话控制等事宜。TCP/IP协议集将应用相关事宜合并到一层，并且确保数据能正确地为下一层打包。

广播地址（*broadcast address*）　用于将分组广播到网络上的所有设备。

A类地址（*Class A address*）　设计用于支持超大型的网络，A类地址只使用一个字节来表示网络地址，其他三个字节列举主机地址。

B类地址（*Class B address*）　设计用于支持中等或大型网络的需求。B类IP地址使用四个字节中的两个字节来表示网络地址，其他两个字节表示主机地址。

C类地址（*Class C address*）　原始分类地址中最常用的一类，此类地址空间用于支持许多小网络。

D类地址（*Class D address*）　用于支持组播的IP地址

E类地址（*Class E address*）　IETF保留此类地址用于内部研究，因此没有E类地址用于Internet。

点分十进制格式（*dotted-decimal format*）　此表示法中，每个IP地址写成4个部分以圆点分隔。

IP地址类别（*IP address class*）　将32位的IP地址分为网络部分和主机部分，由开始部分的比特或比特序列来决定地址所属的类别。

IP协议第6版（*IPv6*）　IP协议第6版是当前版本的IP协议（第4版）的替代协议。IPv6包括了对分组头中的流标识符的支持，该标识符可以用来识别流。IPV6以前称为IPng（下一代IP协议）。

组播地址（*multicast address*）　组播地址是将分组定向到一个预定义的IP地址组的惟一网络地址。

网络访问层（*network access layer*）　网络访问层处理IP分组需要在网络介质上传送时建立物理链路相关的事宜。

划分子网（*Subnetting*）　将一个完整的网络地址类分成多个小网络的方法。此方法用于防止IP地址枯竭。

传输控制协议/Internet协议（*Transmission Control Protocol/Internet Protocol（TCP/IP）*）　传输控制协议/Internet协议是由美国国防部在20世纪70年代开发的、用来支持全球互联网络建设的协议集的常用名称。TCP和IP是该协议集中最著名的两个。

传输层（*transport layer*）　传输层提供从源主机到目的主机的传输服务。在网络端点（发送主机和接收主机）之间建立逻辑连接。

7.6 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. TFTP使用传输层的哪种协议？
   A. TCP
   B. IP
   C. UDP
   D. CFTP
2. 下面哪个是传输层的基本服务？
   A. 通过序号和确认来提供可靠性
   B. 将上层应用的数据进行分段
   C. 建立端到端的操作
   D. 以上全部
3. 下面哪种协议工作于TCP/IP Internet层？
   A. IP
   B. ICMP
   C. ARP
   D. 以上全部
4. DHCP客户端启动时发生的第一件事情是什么？
   A. DHCPREQUEST
   B. DHCPBOOT
   C. DHCPDISCOVER
   D. 以上都不是
5. 网络层是怎样从源向目的转发分组的？
   A. 通过使用路由表
   B. 通过使用ARP响应
   C. 通过域名服务器
   D. 通过网络
6. 如果一台设备不知道相邻网段上的另一台设备的MAC地址，那么它将向谁发送ARP请求？
   A. 缺省网关
   B. 最近的路由器
   C. 路由器接口
   D. 以上全部
7. RARP请求中有什么？
   A. 一个MAC头和RARP请求消息
   B. 一个MAC头、一个RARP头和一个数据分组
   C. 一个RARP头、MAC地址和IP地址
   D. 一个RARP头和一个ARP尾
8. IP地址的两个部分各是什么？
   A. 网络地址和主机地址
   B. 网络地址和MAC地址
   C. 主机地址和MAC地址
   D. MAC地址和子网掩码

9. 哪种Internet协议将一个已知的IP地址映射到一个未知的MAC地址?
   A. UDP
   B. ICMP
   C. ARP
   D. RARP
10. 下面哪个会发起ARP请求?
   A.可以在ARP表中定位目的IP地址的设备
   B. RARP服务器响应出故障的设备
   C. 缓存为空的无盘工作站
   D.在ARP表中无法定位目的MAC地址的设备
11. 下面对ARP表的描述哪个是最佳的?
   A. 一种通过提供常用目的地址的快捷方式和路由列表来减少网络流量的方法
   B. 一种在划分了子网的网络中路由数据的方法
   C. 一种进行从一个堆栈到另一个堆栈应用层信息转化的协议
   D. 每个设备上都有的一段映射IP地址和MAC地址的内存
12. 下面对ARP回应的描述哪个是最佳的?
   A. 设备将自己的MAC地址发送回源主机以响应其ARP请求
   B. 源与目的之间的最短路径
   C. 通过截获和读取网络上的消息来更新ARP表
   D. 一种基于MAC地址找IP地址的方法，主要用于RARP服务器
13. 为什么保持当前更新ARP表非常重要?
   A. 可以测试网络链路
   B. 可以限制广播的数量
   C. 可以减少网络管理员的维护时间
   D. 可以解决地址冲突
14. 为什么要产生RARP请求?
   A. 源主机知道自己的MAC地址，但不知道自己的IP地址
   B. 数据分组需要找到目的与源之间的最短路由
   C. 管理员需要手工配置系统
   D. 一条网络链路出现故障，需要启用冗余系统
15. 下列对TCP/IP的描述哪个是最佳的?
   A. 一套可以用来穿越许多相互连接的网络进行通信的协议
   B. 一套允许将局域网连接到广域网上的协议
   C. 一套允许穿过多个网络进行数据传输的协议
   D. 一套允许通过相互连接的网络来共享不同的设备的协议
16. 下列哪个不是描述TCP/IP协议栈的?
   A. 非常接近的对应OSI参考模型的上层
   B. 支持所有的物理和数据链路协议
   C. 以序列的数据报的形式来传递信息
   D. 在接收端将数据报重组成完整信息
17. TCP/IP协议集指定了OSI模型的哪一层?
   A. 1到3层

B. 1到4层和第7层

C. 3、4层以及5到7层

D. 1、3、4层

18. 下列哪个不是网络层的功能?

A. 数据链路层地址已知的情况下，RARP确定网络层地址

B. ICMP提供控制和消息能力

C. ARP在已知IP地址的情况下确定数据链路层地址

D. UDP提供无连接的数据报交换，并无确认机制

19. 下列哪个协议可以在传输层中找到?

A. UCP

B. UDP

C. TDP

D. TDC



第8章　路由选择基础与子网

目标

学习完本章之后，你应该能够：

- 描述可路由/被路由协议的用途，例如IP协议。
- 了解IP协议作为一种无连接的和面向连接的网络服务的功能。
- 说明在网络层路由器是如何运行的。
- 描述被路由协议如何定义分组的格式和其中使用的各个字段。
- 比较OSI模型第2层LAN交换和第3层路由选择之间的功能。
- 解释在路由器之间路由选择协议是如何用于确定路径和维护路由选择表的。
- 解释分组在互联网络中传输时，路由器是如何实现路径选择和交换功能的。
- 描述静态和动态路由选择之间的区别。
- 描述距离矢量路由选择协议和链路状态路由选择协议的区别，包括它们在收敛过程中的差别。
- 描述内部和外部路由选择协议的区别，并能够分别列举这两种协议的例子。
- 了解子网划分的目的和益处。
- 能够按照需求使用子网掩码创建子网。
- 通过与运算得出网络号。

本章介绍了有关Internet协议（IP）的主题。IP是用于Internet中的基本协议。本章讨论的主题包括IP怎样被传输、数据报头怎样在第3层设备被更改以及IP分组的实际结构。本章也包括了无连接网络服务和面向连接网络服务之间的关系。你将会学到路由选择协议和被路由协议的区别，以及路由器怎样计算不同位置之间的距离。本章介绍了距离矢量、链路状态、混合路由选择方法以及它们是

怎样解决一般的路由选择问题的。

请务必结合相关的e-Lab实验活动、视频和插图来学习本章内容。你将会在随书附赠的CD-ROM中找到这些内容。这些CD提供补充资料和强化本章中介绍的概念。

8.1　被路由/可路由协议与路由选择协议

协议是定义计算机之间如何通过网络互相通信的规则标准的集合。协议也作为一般标准或介质在不同的应用程序、主机或系统的通信中提供服务。当一台计算机与另一台计算机通信的时候，它们彼此交换数据信息。为接收和处理这些信息，计算机必须有预先的定义，这个定义应包含信息如何被解释以及信息所表达的含义。信息的例子包括与一台远程计算机建立连接，发送和接受电子邮件，以及传送文件和数据。

一个协议描述了：

- 信息必须采取的格式。
- 计算机在一个特定环境中交换信息所使用的方式，比如从网络上发送信息。

因为被路由／可路由协议与路由选择协议有些相似，所以经常发生把它们混淆的情况。下面提供几点识别的方法：

- ***被路由协议***——以寻址方案为基础，为分组从一个主机发送到另一个主机提供充分的第3层地址信息的任何网络协议。被路由协议定义了分组所包含的字段格式。分组一般在终端系统之间传送。被路由协议使用路由选择表来转发分组。如图8-1所示的路由选择表中显示了被路由／可路由协议的例子：

— Internet协议（IP）。
— 网间分组交换（IPX）。
— AppleTalk。

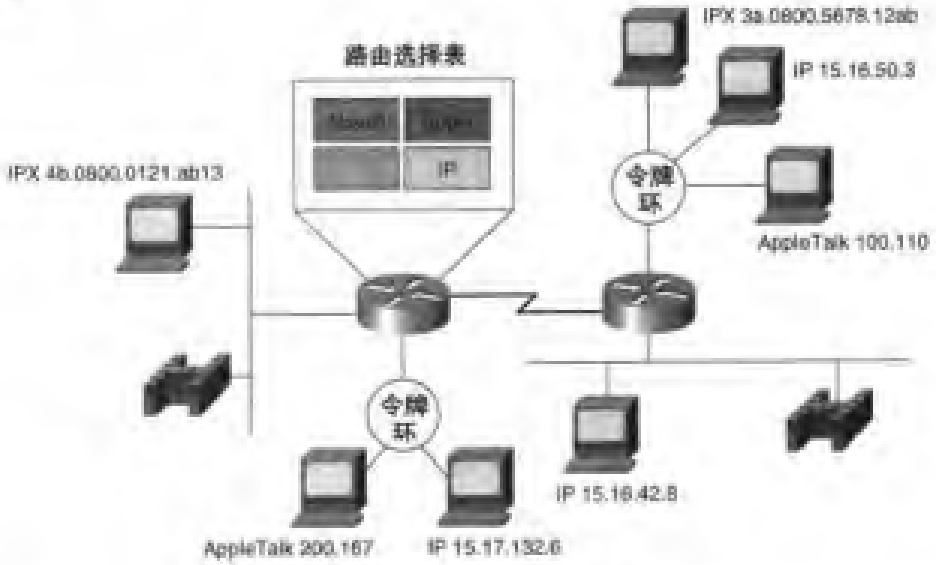


图8-1　被路由／可路由协议

- **路由选择协议**——通过在设备之间提供路由选择信息共享机制，为被路由协议提供支持。路由选择协议消息在路由器之间移动。路由选择协议使路由器之间可以传达路由更新和维护路由选择表。这里有一些TCP／IP路由选择协议的例子：

— 路由信息协议（RIP）。
— 内部网关路由协议（IGRP）。
— 增强型内部网关路由协议（EIGRP）。

— 开放式最短路径优先（OSPF）。

对于可路由协议来说，它必须有为每一个设备分配网络号、主机号的能力。有一些协议，比如网间分组交换（IPX），只要求管理员分配一个网络号，因为这些协议把主机的介质访问控制（MAC）地址作为主机号。其他的协议，比如IP协议，需要提供完整的地址信息，包括网络掩码信息也需要提供。

在一个被路由网络中，*IP地址*和网络掩码都是必需的。网络掩码负责分隔32位IP地址中的网络域和主机域。IPX利用MAC地址和管理员赋予的网络号结合起来创建完整的地址，而且不需要网络掩码。对IP地址来说，只有通过地址和网络掩码的对照才能得知网络地址。

网络掩码可以将连续的IP地址组当作单一的单元来看待。如果不允许分组的话，就要在路由选择表里为每个单个主机映射一个路由条目。对于Internet上数以百万计的主机数目来说这几乎是不可能的。如图8-2所示，从192.168.10.1到192.168.10.254顺序排列的254个地址可以用一个网络地址192.168.10.0来表示。这样一来允许只依靠网络地址就可以把数据发送到这些主机中的任何主机。也就是说路由选择表中只需要用一条192.168.10.0的路由条目就可以代替所有254个单独的条目。这是由Internet软件联盟（www.isc.org）所制定的。为了路由选择能够正常操作，就一定要使用地址分组的方法。

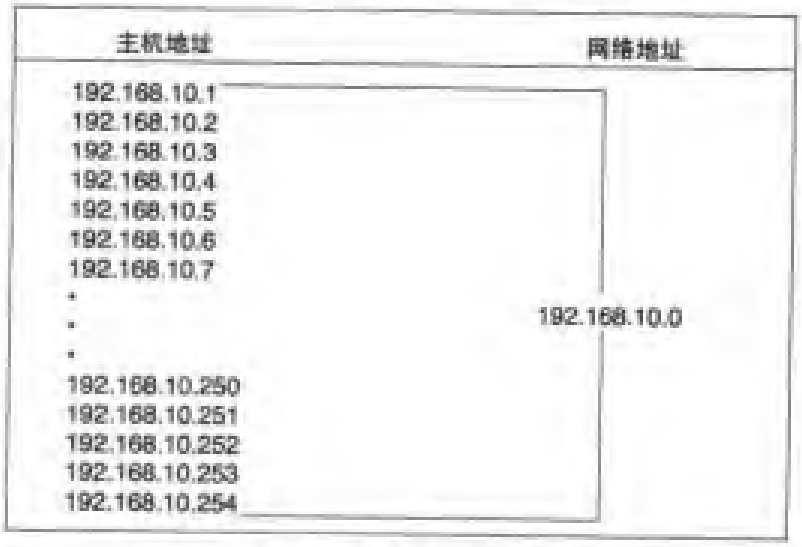


图8-2 网络和主机地址

下面几小节描述了路由器在开放系统互联（OSI）参考模型的网络层（第3层）中执行关键性网络互联功能的用法和操作。另外，你将会学到关于路由选择协议和被路由协议的区别，以及路由器是怎样计算不同位置之间的距离的。最后，你将会学到关于距离矢量、链路状态和混合路由选择途径以及它们怎样解决一般的路由选择问题。

8.1.1 路由选择概述

路由选择是OSI模型第3层的功能。它就像一个分层的组织方案，允许单个的地址结合成组并被视为一个整体单元，直到需要用单个的地址来做最后的数据传送。路由选择是寻找从一个设备到另一个设备的最有效路径的过程，如图8-3所示。执行这个过程的主要设备就是*路由器*。

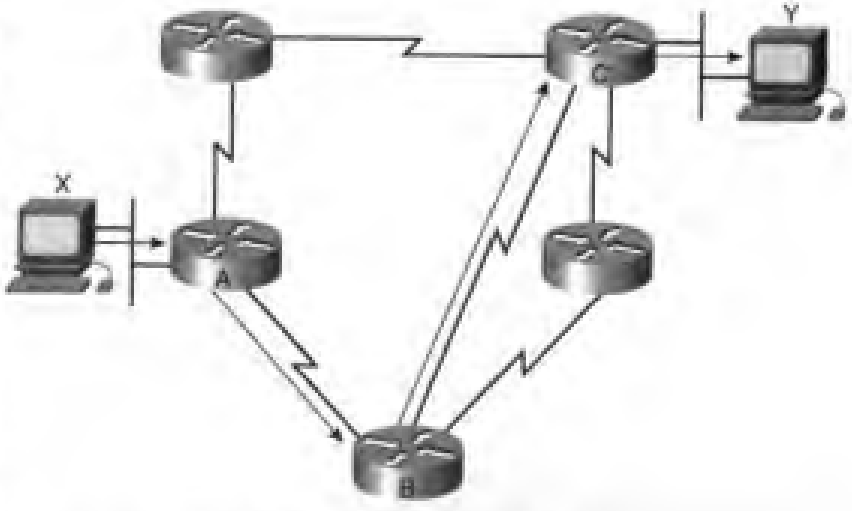


图8-3 网络层协议操作

路由器有两个关键的功能：

- 维护路由选择表并确保其他路由器知道网络拓扑中的变化。这个功能在使用路由选择协议传达网络信息到其他路由器时完成。

• 当分组到达一个接口时，路由器用路由选择表来决定把分组发送到哪里。把这些数据交换到相应的接口，依照接口类型进行必要的成帧，然后发送帧。

路由器是一个网络层设备，它使用一个或多个*路由选择度量标准*来决定网络流量发送的最佳路径。路由选择度量标准起着决定路由可取性的作用。路由选择协议使用多种多样的标准组合来决定路由选择度量标准，如图8-4所示。

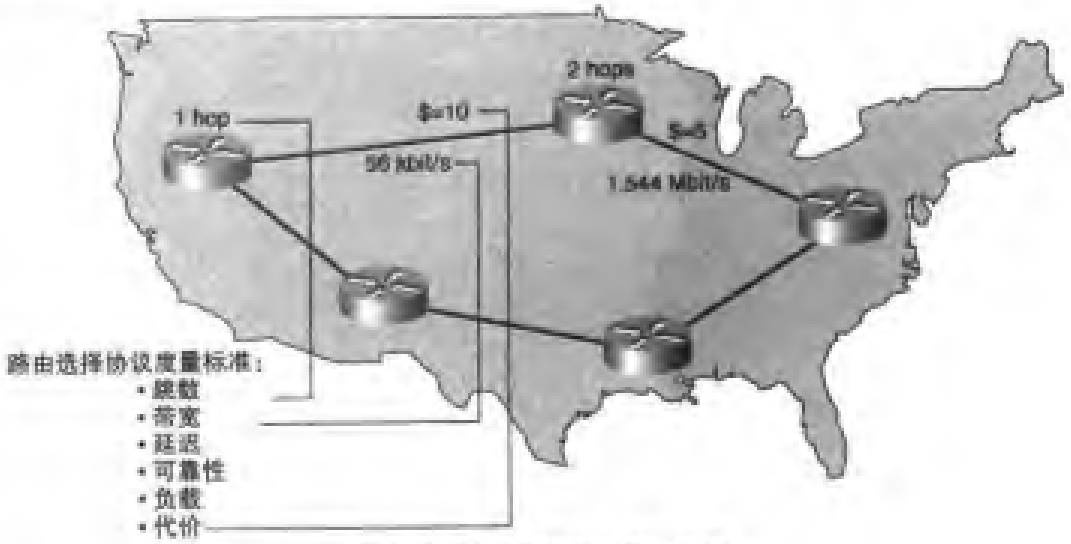


图8-4　路由选择协议度量标准

利用跳数、带宽、延迟、可靠性、负载与代价这些度量标准，进行多样的组合计算用于决定通过互联网络的最佳路径。路由器互连网段或整个网络。它们在网络之间以第3层信息为基础传递数据帧。路由器作出在互联网络中传送数据最佳路径的合理决定，然后直接将分组送到相应的出站端口去封装，然后发送。每次封装和解封装的过程都在分组穿过路由器或者说数据从一个设备发送到另一个设备时发生，如图8-5所示。封装使数据流分成段，加上适当的头和尾，并传输数据。解封装的过程正好相反，它去掉头和尾并且重新合并数据成为一个连贯的数据流。路由器从LAN设备获得帧，并以第3层信息为基础，通过网络转发它们。

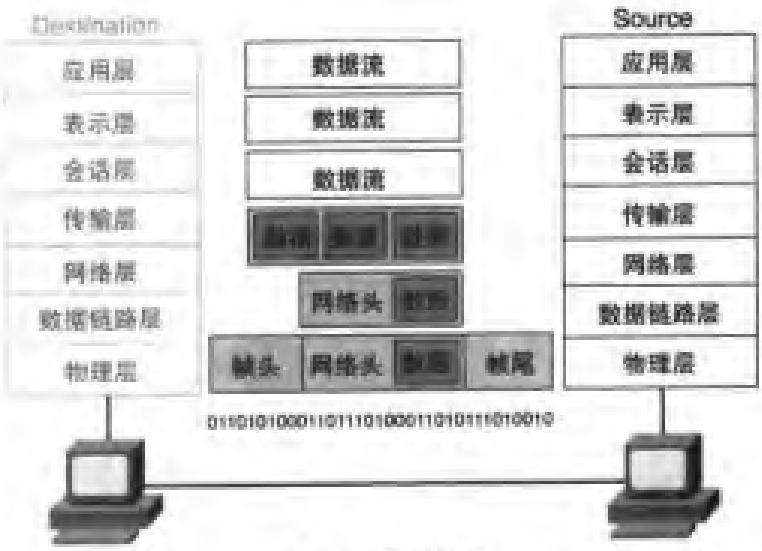


图8-5　数据封装

本章以及本书其余部分的重点大都放在可路由协议（或被路由协议）——IP上，尽管重点是IP协议，但还有另一些重要的可路由协议，例如IPX / SPX和AppleTalk。

像IP，IPX / SPX和AppleTalk这样的协议都提供了对第3层的支持并且是可路由的。不支持第3层功能的协议被称为不可路由协议。这种协议最常见的就是*NetBIOS扩展用户接口（NetBEUI）*，即一个小的、快速的、高效率的协议，但是限制在一个网段内运行。

8.1.2　路由选择与交换的比较

路由选择协议经常被拿来和第2层的交换作比较，他们的功能不经意看来好像是一样的。这两

者之间最主要的不同是交换是工作在OSI模型的第2层（数据链路层），路由选择协议工作在第3层。这个区别说明：在把数据从源发送到目的地的过程中路由选择和交换利用的信息是不同的。

交换和路由选择的关系就好比本地电话呼叫和长途电话呼叫之间的关系。当一台电话机呼叫另一个本地号码时（在同一区号下的号码），是由本地交换机处理呼叫。但是本地交换机不可能知道世界上所有的电话号码——只能知道它所处的本地的号码。当本地交换机收到发送出本区域的呼叫请求时，交换机会呼叫高一层识别不同区号的交换机。高一层交换机把这个呼叫请求交换到目的区域中的本地交换机。

路由器所执行的功能和电话网络中的较高层次的交换机类似，如图8-6所示。第2层交换机被放置在局域网中，这个范围也被称作*广播域*。第3层路由选择负责在广播域之间搬移通信。这需要3层的寻址机制，如IP，提供一个分级的寻址方案。第2层交换机不能识别第3层地址——只能识别本地MAC地址。当一个主机向一个非本地IP地址发送数据时，它将使用路由器的MAC地址把数据封装后发往缺省网关（也就是路由器）。

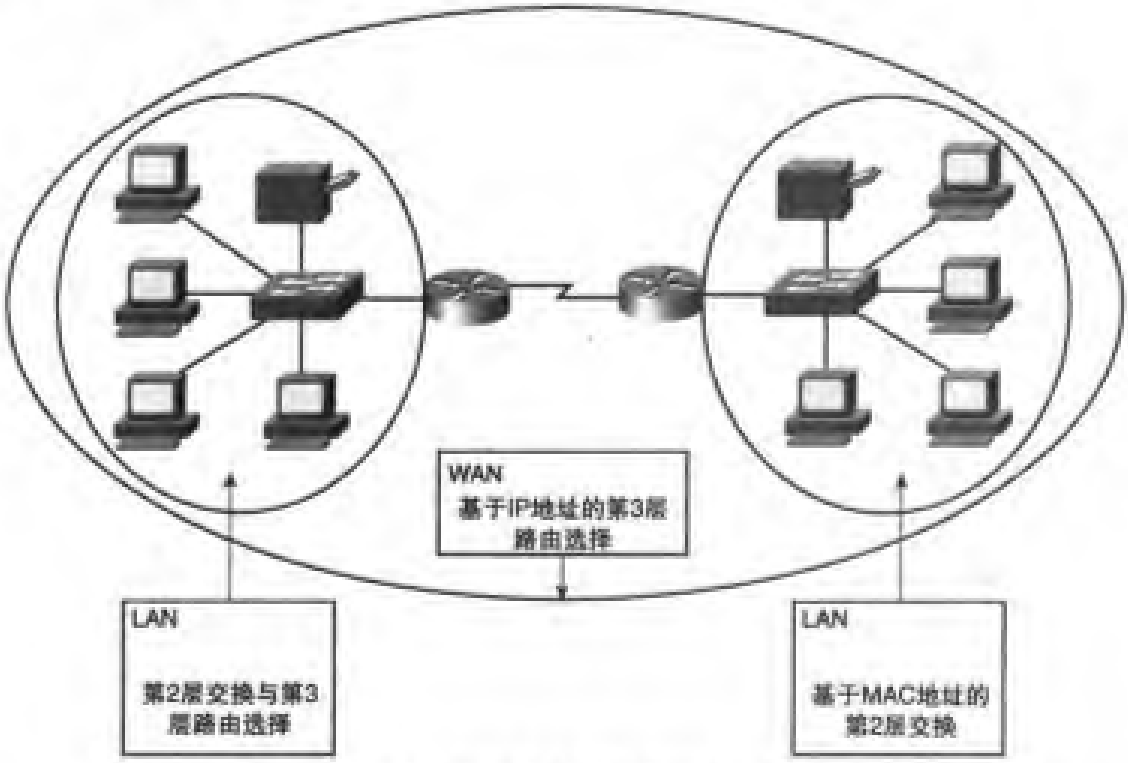


图8-6 第2层交换和第3层路由选择

一台第2层交换机所连接的网段都属于同一逻辑网络或*子网络*。如果主机X要发送一个帧到另一个网络或子网络上的另一个主机，主机X会把帧发送到同样连接在交换机上的路由器。因为主机X的IP配置里包括了缺省网关的IP地址信息，所以主机X知道路由器的IP地址，但是不知道路由器的MAC地址。主机X通过发送地址解析协议（ARP）请求来学习路由器的MAC地址，这个协议可以把IP地址转换成MAC地址。交换机依照路由器的目的MAC地址把帧转发到路由器。路由器检查分组中的第3层目的地址来做出转发决定。缺省网关就是和主机X在同一个网络或子网络中的路由器。

正如交换机为它知道的所有MAC地址维护一个表一样，路由器也为IP网络地址维护着一个表，这个表被称为*路由选择表*，如图8-7所示。每一台计算机和路由器的以太网接口都维护着一个ARP表，这个表用于第2层通信。ARP表只在设备所直连的广播域范围中起作用。路由器维护着路由选择表，这个表可以使数据发送到其他广播域。每个ARP表都包含IP-MAC地址对（图8-7中所示MAC地址都被缩写了，因为实际的MAC地址对这个图来说实在是太长了）。路由选择表中显示了路由从什

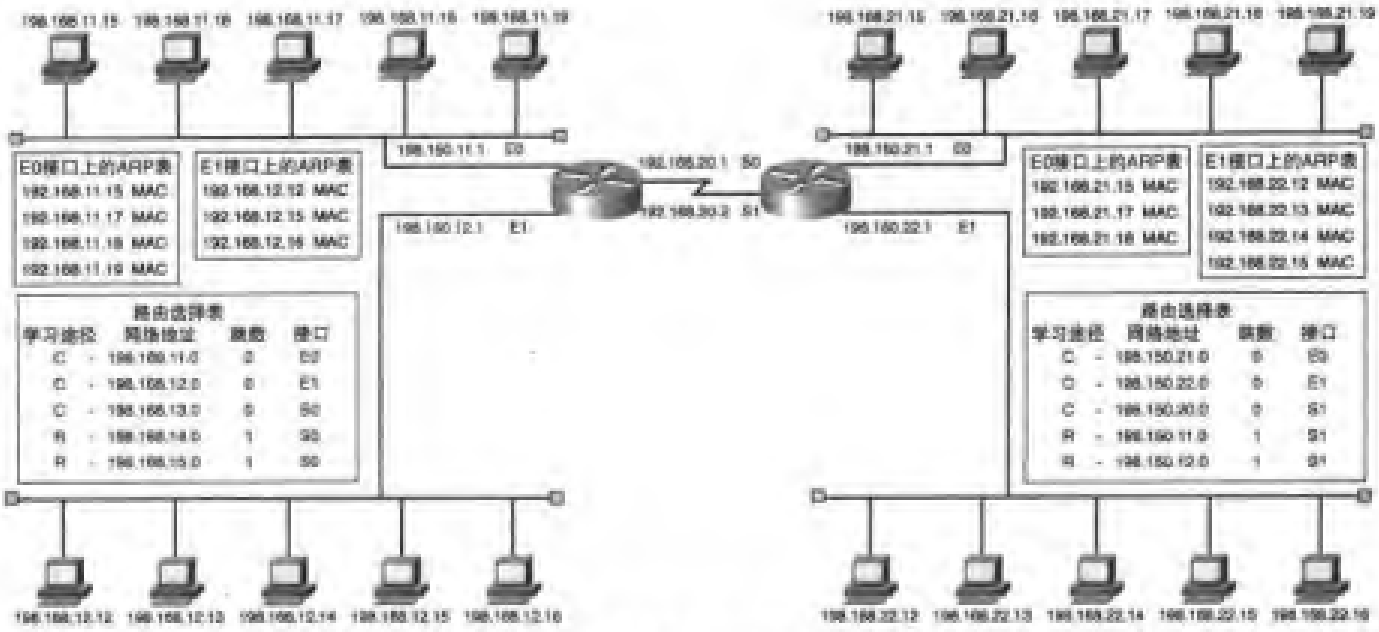


图8-7　路由器ARP表

么途径学习而来的（在这个例子中是直连（C）和RIP（R）——可达网络的IP地址）、到达这些网络的跳数和到达目的网络经由转发数据的端口。这两种地址之间的不同之处在于：MAC地址没有用什么特殊的方法来组织。在MAC表中因为每个单独的网络分段中所含的主机数目不是很大，所以这种情况是可管理的。在路由选择表中如果IP网络地址也按这种方法处理，那么Internet很容易就会崩溃。根本没有办法组织所有的地址和确定到达它们的方向（正确的办法是分层）。分层组织IP地址可以让你把地址分组，每个组被看作是一个整体的单元，直到你需要定位一个单独的主机为止。有个方法可以理解这一点，就是想像一个图书馆，它容纳了百万张单独的书页，都堆成一大堆。这些材料是没有用的，因为定位一个单独的书页是不可能的。如果这些书页被组织装订成书本，每一页都被单独标记，而且这些书可以被列入一个索引文件，那么寻找和使用数据将会方便很多。

交换网络和路由网络的另一个不同是第2层交换网络不会阻挡第3层广播。因此，会造成大量的广播风暴。路由器一般可以阻挡广播的，所以广播的影响只会限制在广播发起源所处的广播域中。因为可以阻挡广播，路由器可以比第2层交换机提供更高的安全性和带宽控制。

表8-1　路由器和交换机的特性比较

特性	路由器	交换机
速度	慢速	快速
OSI层次	第3层	第2层
使用的寻址方式	IP	MAC
广播处理	阻止	转发
安全性	较高	较低
网络分段	划分广播域	划分冲突域

8.1.3　被路由与路由选择的比较

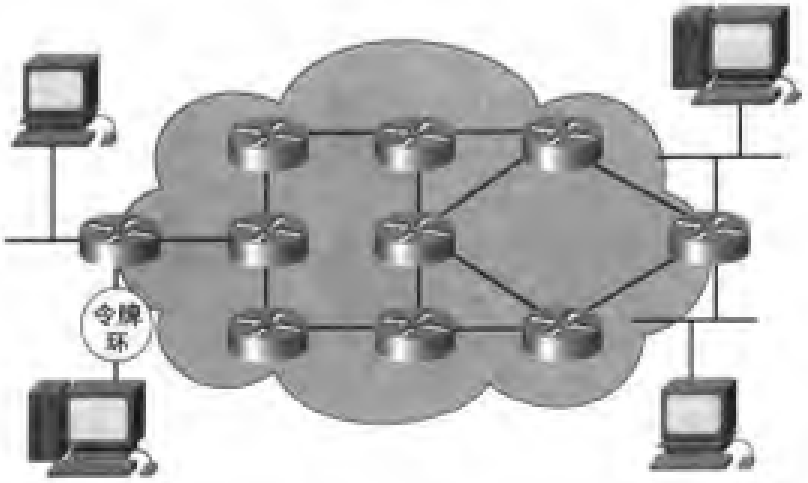
在网络层中有两个协议范畴——被路由和路由选择（见图8-8）。被路由协议通过网络传输数据，路由选择协议允许路由器适当地将数据从一个特定区域定向到另一个特定区域。

通过路由器把数据从一个主机传输到另一个主机的协议是被路由或可路由协议。

被路由协议的操作如图8-9所示：

- 它包括任何网络协议集，以提供足够网络层地址信息，使路由器能够转发到下一个设备并最

被路由协议用在路由器之间引导用户流量。例子包括IP和IPX。



路由选择协议用在路由器之间维护路由选择表。例子包括RIP、IGRP和OSPF。

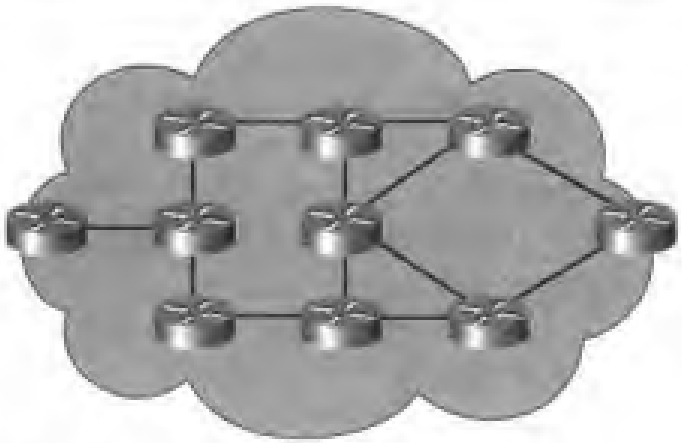


图8-8 被路由协议和路由选择协议

终到达目的地。

• 它定义了分组的格式和其中所用的字段。分组通常在终端系统之间传送。

IP和IPX是被路由协议的两个例子。其他例子包括DECnet、AppleTalk、Banyan VINES（虚拟集成网络服务）和Xerox网络系统（XNS）。

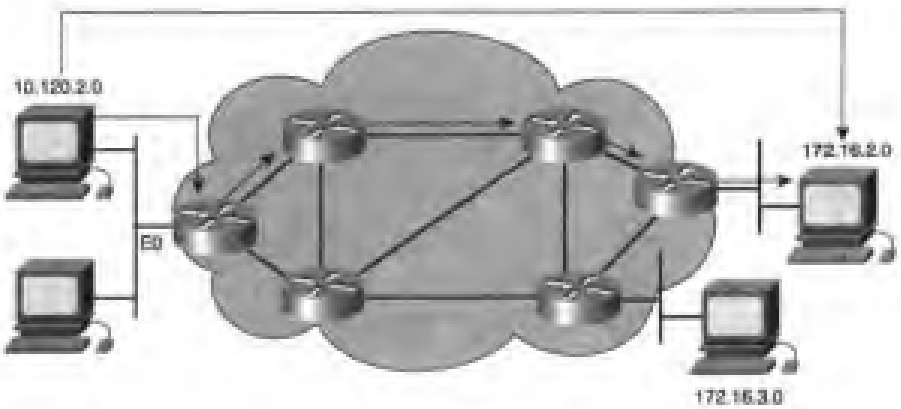


图8-9 被路由协议

路由器使用路由选择协议来交换路由选择表和共享路由选择信息。换句话说，*路由选择*协议使得路由器在确定路径之后发送*被路由*协议数据。

路由选择协议操作如图8-10所示：

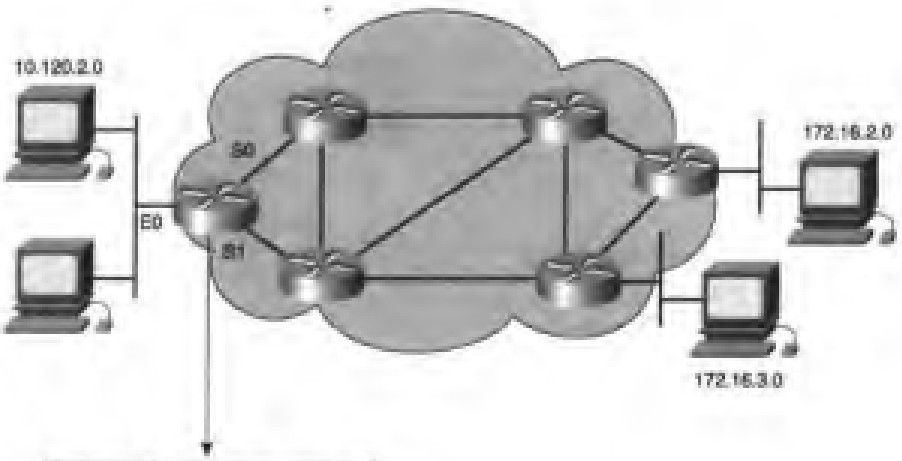
• 它提供共享路由选择信息的方法。

• 它允许路由器与其他路由器通信来更新与维护路由选择表。

支持IP被路由协议的路由选择协议的例子包括RIP、IGIP、OSPF、边界网关协议（BGP）和EIGRP（增强内部网关路由选择协议）。

8.1.4　路径确定

路径确定发生在第3层（网络层）。它允许路由器评估到达目的地的有效路径，以及确定分组的首选处理方法。路由选择服务在估算网络路径时使用网络拓扑信息，如图8-11所示。路径确定是路由器在通往分组最终目的地的路径中选择下一跳的过程。这个过程也叫做*路由选择*分组。



网络协议	目的网络	出口
Connected	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

图8-10　路由选择协议

分组的路径确定就好比一个人开车从城市的一端到另一端。司机有一份地图显示了所有可以通向目的地的街道。从一个十字路口行驶到另一个十字路口之间的过程叫做一*跳*。同样地，路由器使用一份显示所有通向目的地的有效路径的地图。路由器能够根据流量密度和连接速度（带宽）来作出决定，正如司机可以选择一条最快的路（高速公路）或者一条人群最少的后街。在本节中，你可以看见路由器是怎样确定分组从一个网络传递到另一个网络的最佳路径的。

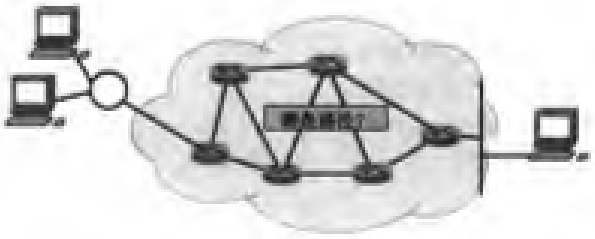


图8-11　路径选择

网络层寻址

网络地址帮助路由器识别网络云中的路径，而且也提供分层或子网信息。路由器用网络地址来标示互联网络中分组的目的网络。除了网络地址之外，网络协议也采用一些特定格式的主机或节点地址。对于一些网络层协议，网络管理员要根据一些预先决定的网络地址分配计划来分配主机地址。对于其他一些网络层协议，分配主机地址是部分或全部动态或自动的。图8-12显示了网络1中的3个设备（两个工作站和一个路由器），每个都有自己惟一的主机地址。（图中也显示了路由器被连接到另外两个网络上——网络2和3）。

网络	主机
1	1 2 3
2	1
3	1

逻辑寻址发生于网络层，回想一下网络地址和电话号码的类比。电话号码的前三个数字是区号，电话号码的后四个数字是告知电话公司的设备应该拨通哪一部电话机。这与网络地址中主机部分的功能很相似。主机部分是用来告诉路由器它应该向哪一个特定的设备发送分组。

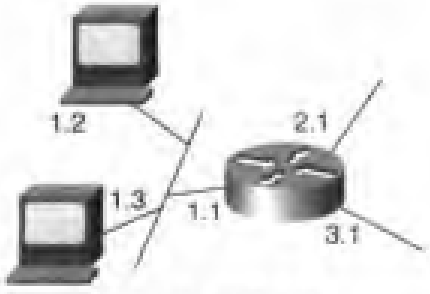


图8-12　网络地址

没有网络层寻址，路由选择就不会发生。路由器需要网络地址来保证分组的正确发送。没有分层编址结构，分组也不会在互联网络中传送。同样地，如果没有分层结构的电话号码、

邮政编码和运输体系的话，将不能顺利地发送货物或者提供良好的服务。

*MAC地址*就好比你的名字，网络层地址（网络地址和主机地址）好比是你的通讯地址。举一个例子，如果你去了另一个城市，你的名字不会改变，但你的通讯地址指明了你所在的新地方。网络设备（路由器以及单个的计算机）同时具有MAC地址和协议（网络层）地址。当你把一台计算机移往其他网络，计算机仍维护着原来的MAC地址，但是你必须给它分配一个新的网络层地址。

通信路径

网络层的功能就是找出穿越网络的最佳路径。在实际中，一个网络一直被用来表示两个路由器之间的可用路径。如图8-13所示，每条路由器之间的线路都有一个编号，这代表一个网络地址，这些地址可以提供路由选择过程中所需要的信息。这就意味着这些地址必须包含有关介质连接的路径信息，这些介质连接被路由选择过程用来把分组从源发送到目的地。

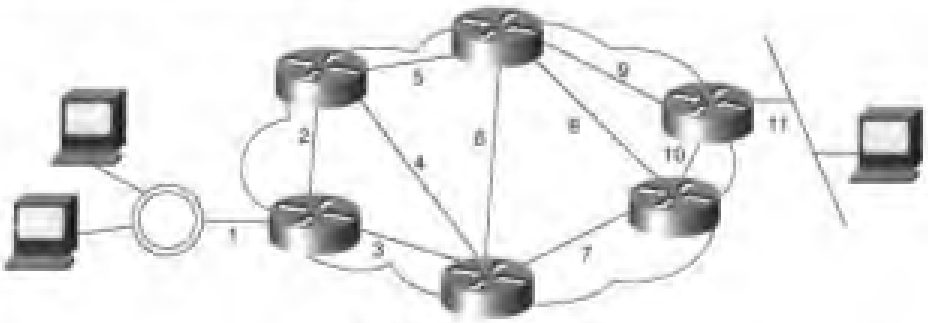


图8-13 网络介质连接

使用这些地址，网络层能够在独立的网络之间提供中继使他们互相连接。通过抑制不必要的广播，遍布整个互联网络的第3层地址的一致性也改善了带宽的使用。*广播*导致了不必要的处理开销，并且浪费了不需要接收广播的设备或链路的容量。通过使用一致的终端到终端的编址方法来表示介质连接的路径，网络层就可以找到通向目的地的路径，而避免设备或者链路因广播导致的负载。

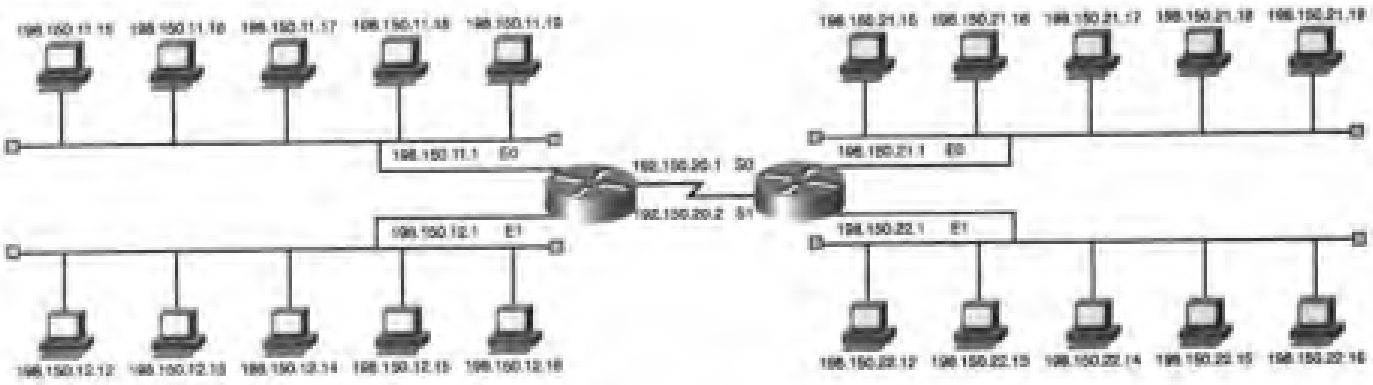
8.1.5 路由选择表

为了对路径确定的过程有所帮助，路由选择协议建立和维护路由选择表来容纳路由信息，如图8-4所示。根据所使用的路由选择协议不同，路由信息也会有所不同。路由选择协议以多种信息来填充路由选择表。

路由器在它们的路由选择表中保存着重要的信息：

- **协议类型**——创建路由选择表条目的路由选择协议的类型。
- **目的地／下一跳**——告诉路由器特定的目的地是直接连接在路由器上还是通过另一个路由器到达，这个位于到达最终目的地途中的路由器叫做下一跳。当路由器接收到一个入站分组，它就会查找目的地地址并试图将这个地址与路由选择表条目匹配。
- **路由选择度量标准**——不同的路由选择协议使用不同的路由选择度量标准。路由选择度量标准用来判别路由的好坏。例如，RIP使用跳数作为自己的路由选择度量标准。IGRP使用带宽、负载、延迟和可靠性来创建合成的度量标准值。这些内容将会在CCNA 2中更深入地阐述。
- **出站接口**—— 数据必须从这个接口被发送出去以到达最终目的地。

路由器与另一个路由器之间通信，通过传送路由选择更新消息来维护它们的路由选择表。根据特定的路由选择协议，更新消息可以周期性地发送或者仅仅当网络拓扑中有变化的时候才发送。路由选择协议也决定在路由更新的时候是仅仅发送有变化的路由还是整个的路由表。通过分析来自邻近路由器的路由选择更新，路由器能够建立和维护它自己的路由选择表。



路由选择表

学习途径	网络地址	跳数	接口
C	198.150.11.0	0	E0
C	198.150.12.0	0	E1
C	198.150.13.0	0	S0
R	198.150.14.0	1	S0
R	198.150.15.0	1	S0

路由选择表

学习途径	网络地址	跳数	接口
C	198.150.21.0	0	E0
C	198.150.22.0	0	E1
C	198.150.23.0	0	S1
R	198.150.24.0	1	S1
R	198.150.25.0	1	S1

图8-14　路由选择表

8.1.6　路由选择算法和度量标准

路由选择协议通常有以下一个或多个设计目标：

• **最优化**——根据计算机使用的度量标准和度量标准权值，最优化描述了路由选择协议/算法的选择最佳路由的能力。例如，一个算法可以用跳数和延迟作为度量标准，但也许延迟占的比重要大一些。

• **简单性与低开销**——如果路由器运行路由选择协议占用的CPU和存储器开销很小，那么就达到了理想有效的路由选择算法功能的目标。这对网络能够最大比例地扩展非常重要，比如Internet。

• **强壮性与稳定性**——路由选择算法应该在面临非正常或不可预见的情况时还能够正常运行，比如硬件故障、高负载状况和执行错误等情况下。

• **快速收敛**——收敛是指所有路由器都有统一的路由认知的过程。当一个网络事件引起路由有效性的变化时，就需要重新计算来重建网络连接性。收敛缓慢的路由选择算法可能导致数据不能被传送。

• **灵活性**——路由选择算法应该很快适应各种各样的网络变化。这些变化包括路由器有效性、带宽的变化、队列长度和网络延迟。

• **可扩展性**——一些路由选择协议的可扩展性被设计得比较好。重要的是，要记住如果网络要被扩展（或即使以后再扩展），使用EIGRP这样的路由选择协议要胜于使用RIP。

当路由选择算法更新路由选择表的时候，它首要的目标是选择最好的信息放到路由选择表中。路由选择算法用不同的度量标准来确定最佳路由。每个路由选择算法用它自己的方式来解释什么样的路由是最佳路由。路由选择算法为每一条通过网络的路径生成一个数值，叫做度量标准值。复杂的路由选择算法能够把路由选择建立在多种度量标准基础上，使它们合并为单一的复合度量标准，如图8-15所示。通常，度量标准越小，路径就越佳。

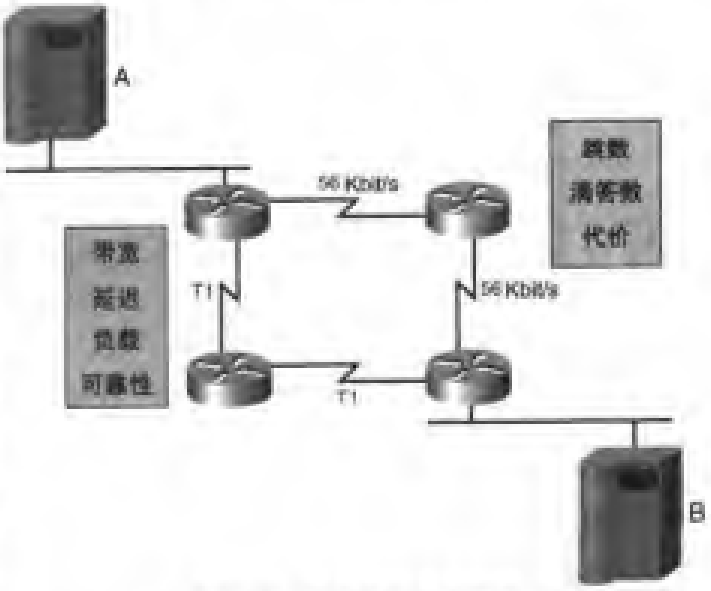


图8-15　路由选择度量标准

度量标准可以以单一的路径特征为基础，或者以几种不同特征来计算。路由选择协议使用得最为普遍的度量标准如下所示：

- **带宽**——链路的数据容量（一般来讲，10Mbit/s以太网链路比64kbit/s专用线要更好）。
- **延迟**——从信号源到目的地沿每条链路移动分组所需要的时间长度。延迟取决于中间链路的带宽、每个路由器的端口队列、网络拥塞情况以及物理距离等因素。
- **负载**——网络资源（如路由器或链路）上的活动量。
- **可靠性**——通常指的是每个网络链路的出错率。
- **跳数**——分组在到达目的地前所必须经过的路由器的数量。只要分组通过一个路由器，就是一跳。一条路径中有4个跳数就代表到达目的地前数据沿着这条路径传送时经过了4个路由器。如果到达一个目的地有很多条路径，路由器就会选择跳数最少的路径。
- **代价**——一个任意的值，通常以带宽、金钱的花销或其他的衡量标准为基础，可以由网络管理员指定。

8.1.7 内部路由选择协议与外部路由选择协议

路由器使用路由选择协议来交换路由选择信息。换句话说，路由选择协议决定被路由协议怎样被路由。路由选择协议有两个系列：***内部网关协议（Interior Gateway Protocol, IGP）***和外部网关协议（Exterier Gateway Protocal, EGP），如图8-16所示。这些系列的分类是基于它们运作时与自治域系统的关系而言。

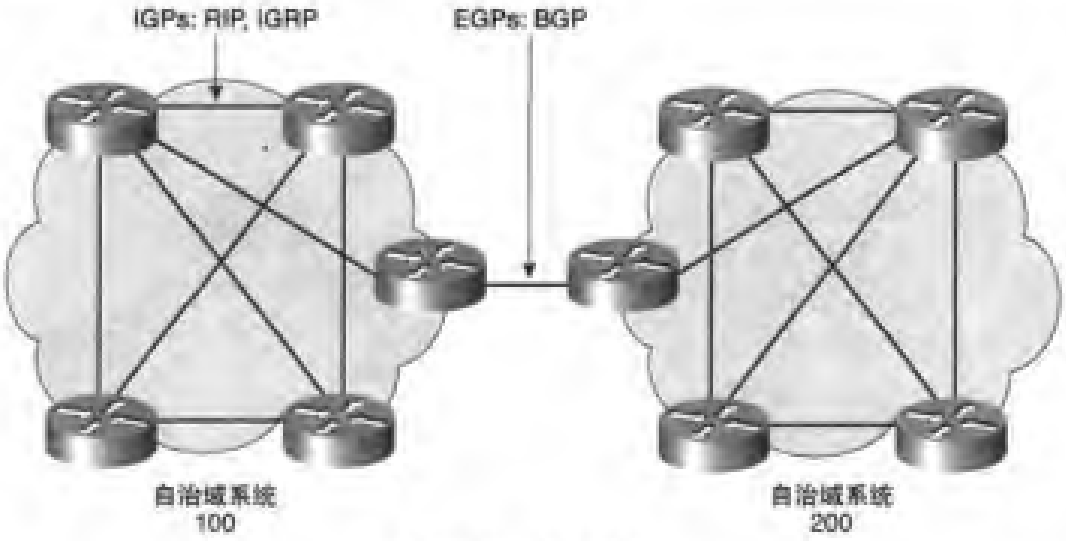


图8-16 IGP与EGP

自治域系统是在单一实体管理控制下的一个或者多个网络的集合，比如cisco.com域。一个自治域系统由在外部世界看来享有一致路由选择的路由器组成。因特网地址授权委员会（IANA）将自主系统编号分派给区域性的注册处。这些注册处在美国、加勒比地区和非洲的是ARIN（hostmaster@arin.net）；在欧洲是RIPE-NCC（ncc@ripe.net）；在亚洲太平洋地区的是AP-NIC（admin@apnic.net）。自主系统是一个16位编号。一些路由协议如BPG要求你在配置中指明惟一的已分配的自主系统编号。

IGP在一个自主系统内部路由数据。下面是IGP的几个例子：

- RIP和RIP V2。
- IGRP。
- EIGRP。

• OSPF。
• 中间系统到中间系统（IS-IS）协议。
EGP在不同自治域系统之间路由数据。BGP是应用最普遍的EGP例子。

8.1.8　路由选择协议

路由选择协议能够用不同的方法来分类，例如IPG或EGP。其他描述路由选择协议的分类有距离矢量或链路状态。IGP和EGP描述路由器之间的物理关系，而距离矢量和链路状态则是描述在路由选择更新方面路由器之间是怎样相互作用的。

距离矢量路由选择协议

距离矢量路由选择方法确定到互联网络中任意链路的方向（矢量）和距离（跳数）。距离矢量算法周期性（例如每30秒）发送它们路由选择表的全部或某些部分给邻近设备。即使网络没有发生变化，运行距离矢量路由选择协议的路由器也会发送周期性的更新。通过接收邻近设备的路由选择表，路由器能够检验所有已知的路由，并且能根据邻近设备发来的更新信息来改变本地路由选择表。这个过程叫做“根据传闻进行路由选择”，这是因为网络中路由器的理解是以网络拓扑中邻近设备的观点为基础的。距离矢量协议采用贝尔曼-福特路由选择算法来计算最佳路径。

距离矢量协议的例子包括以下几个：

• **路由选择信息协议（RIP）**——Internet中最普遍的IGP，RIP用跳数作为它的路由选择度量标准。
• **内部网关路由选择协议（IGRP）**——思科开发这个IGP来解决在庞大而多种类的网络中与路由选择相关的那些问题。

链路状态协议

链路状态路由选择协议的设计意图是为了克服距离矢量路由选择协议的局限性。链路状态路由选择协议对网络的变化能很快地作出反应，仅当网络变化发生的时候发送触发器更新，以较长时间的间隔时间（比如每30分钟）发送周期性更新（叫做链路状态刷新）。

当链路状态发生变化，检测到这个变化的设备就创建一个与此链路（路由）有关的链路状态通告（LSA），而且这个LSA被传播到所有邻近的设备上。每个路由设备都复制一份这个LSA，更新自己的链路（拓扑）数据库，再把这个LSA转发给所有邻近的设备。LSA的泛洪保证所有的路由选择设备先更新它们的数据库，然后创建或者更新反映新拓扑的路由选择表内容，如图8-17所示。

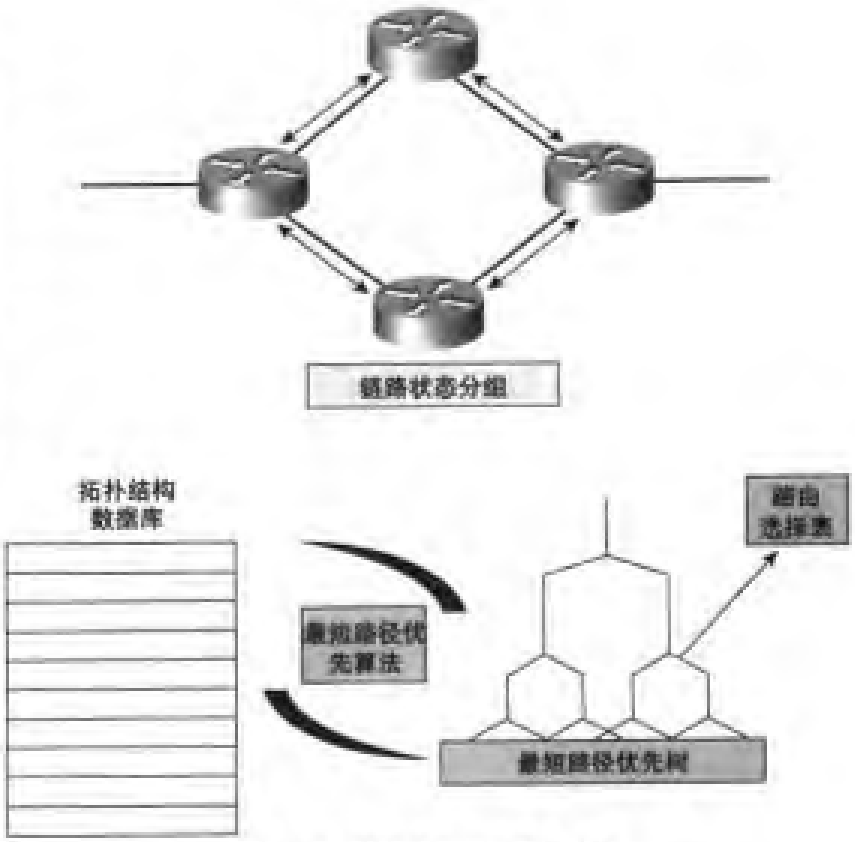


图8-17　链路状态路由选择协议

链路状态数据库用来计算通过网络的最佳路径。链路状态路由器通过对链路状态数据库执行Djikstra最短路径优先算法（SPF），找到通往目的地的最佳路径，并建立SPF树型结构。最佳（最短）路径从最短路径优先的树型结构中被挑选出来放入路由选择表。

链路状态协议的例子包括OSPF和IS-IS，如图8-18所示。

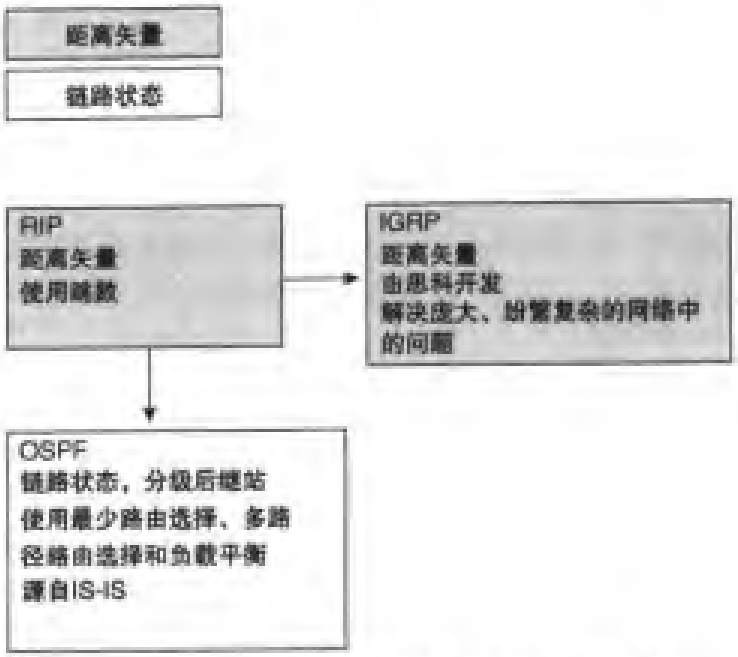


图8-18 链路状态路由选择协议：OSPF和IS-IS

路由选择协议的特征

下面几小节描述了度量标准、网络可用性和其他普遍使用的路由选择协议的显著特征。

RIP

RIP以跳数来决定到互联网络中任一链路的方向和距离，如图8-19所示。如果到目的地有多条路径，RIP就选择跳数最少的路径。然而，因为跳数是RIP惟一使用的路由选择度量标准，它不必选择到达目的地的最快路径。RIP-1只使用有类路由选择。这就意味着网络中的所有设备必须要使用相同的子网掩码，因为RIP-1路由选择更新中不包含子网信息。

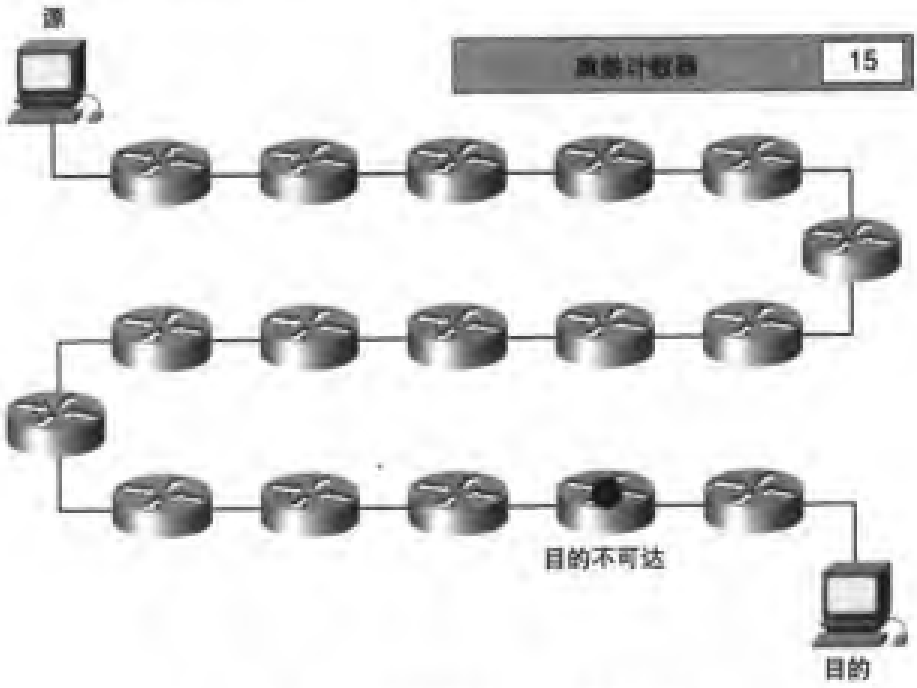


图8-19 RIP用跳数作为它的度量标准

RIP-2提供“前缀路由选择”并且发送含有子网掩码信息的路由更新。它支持无类路由选择。使用无类路由选择协议，同一个网络中不同的子网能够有不同的子网掩码。在相同网络中使用不同子网掩码的方法叫做可变长度子网掩码（VLSM）。

IGRP

IGRP是一个由思科开发的距离矢量路由选择协议，专门针对解决超出协议范围（如RIP）的庞

大的网络中与路由选择相关的问题。IRGP能够以延迟、带宽、负载和可靠性为基础来选择最快的路径。默认情况下，IGRP仅仅使用带宽和延迟度量标准，并且用24位度量标准。IGRP也有比RIP更高的最大跳数限制来允许网络更大延伸。IGRP只使用有类路由选择。

EIGRP

跟IGRP一样，EIGRP也是一个思科的专利协议。EIGRP是一个IGRP的高级版本，使用32位度量标准。特别的是，EIGRP提供优良的操作效率，如更快的收敛和低带宽开销。它是一个高级的距离矢量协议。EIGRP也使用一些链路状态协议功能。因此，术语*混合*也用来形容EIGRP。

OSPF

OSPF是一个链路状态路由选择协议。Internet工程任务组（IETF）在1988年开发了OSPF。现在最新的版本，OSPF版本2，在RFC 2328中有描述。OSPF是一个IGP，意味着它在属于同一自治域系统中的路由器之间分发布路由选择信息。OSPF可以满足RIP所不能满足的庞大、可升级的网络的需求。

IS-IS

中间系统到中间系统（IS-IS）是适合于OSI***协议栈***的动态链路状态路由选择协议。因此，它在ISO无连接网络服务（CLNS）环境中为路由无连接网络协议（CLNP）的数据发布路由信息。集成的IS-IS作为IS-IS协议的实现，可以为多种网络协议提供路由选择服务。集成的IS-IS以关于IP网络和子网的信息来标记CLNP路由。在IP的网络环境中，可以作为OSPF的替代选择，将ISO CLNS和IP路由选择混合到一个协议中。它能够纯粹地用于IP路由选择，纯粹地用于ISO路由选择，或用于两者的结合。

注意：CLNP指的是在数据被传输以前不需要建立线路的OSI网络层协议。

BGP

边界网关协议（BGP）是一个EGP的例子。BGP在自治系统之间交换路由选择信息并且同时保证无环路的选择。它是Internet上多数公司和ISP们所使用的主要的路由通告协议。BGP-4是支持***无类域间路由选择（CIDR）***和路由聚合的第一个BGP版本。不像一般的IGP（如RIP、OSPF和EIGRP）那样，BGP不使用跳数、带宽或延迟这样的度量标准。BGP以网络策略或规则为基础，使用多样的BGP路径属性来作出路由选择决定。



实验活动　购买小型的路由器（Cable / DSL 路由器）

这个实验的目的是为了介绍市场中网络组件的价格和多样性。这个实验特别着眼于在家里工作时远程交换所用到的小型路由器。

8.1.9　IP是被路由协议

IP是分层网络寻址方案中应用最广泛的协议。IP是一个在Internet中使用的无连接、不可靠、尽力传送的系统协议。术语***无连接***的意思是不需要专用的电路连接，就像打电话一样，在电话接通前是没有数据在主机之间传输的。IP协议无论采用哪一个路由作为最佳路由，都是以路由选择协议的决定为基础的。不可靠和尽力并不是说系统是不可靠的或不正常工作的，而是说IP协议尽最大努力传送分组但并不保证传送结果。这个功能由上层协议来完成。

当信息沿着OSI模型层下行的时候，数据在每一层都会被加工。在网络层中，数据被封装到分组里，叫做***数据报***，如图8-20。

IP定义了IP分组头（包括寻址方法和其他控制信息）的格式，但是它并不考虑实际的数据。它接受一切从更高的层传送下来的信息，如图8-21所示。

8.1.10 分组在路由器中的传播和交换

当一个分组为了到达它最终的目的地而通过互联网络传播时，帧头和帧尾在每个路由器（第3层）设备中被剥离和替换，如图8-22所示。这样做的原因是第2层数据单元（帧）只适合于本地寻址方法，而第3层数据单元（分组）适合于端到端寻址。

第2层以太网帧是在广播域中工作且与分配到物理设备上的MAC地址关联。其他的第2层帧包括使用自己的第2层寻址方案的点到点串行链路和帧中继广域网连接。重要的一点是不管第2层使用什么类型的寻址方案，它都要留在第2层广播域中。当数据穿过第3层设备的时候，第2层的信息会发生变化。

关于第3层设备运行的确切过程在下面一段的图8-23中描述。

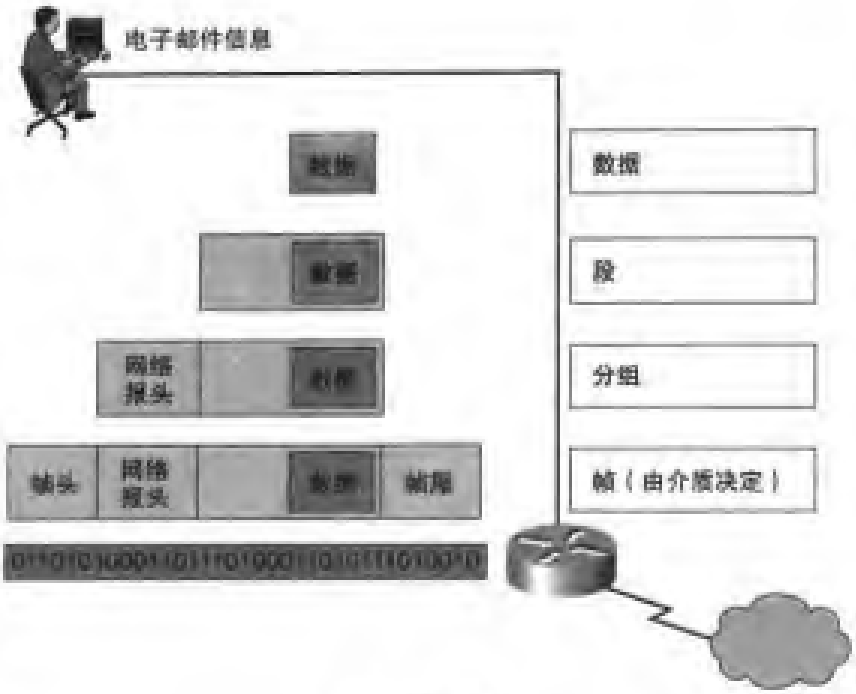
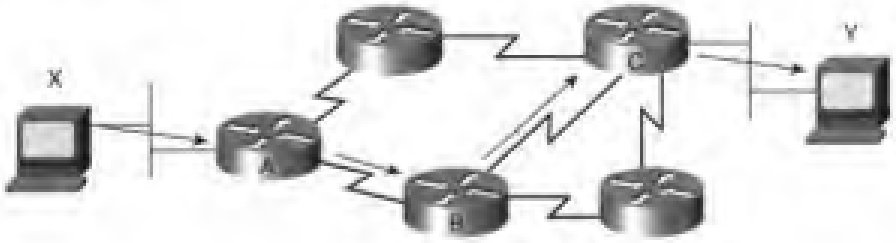


图8-20 封装



图8-21 IP头



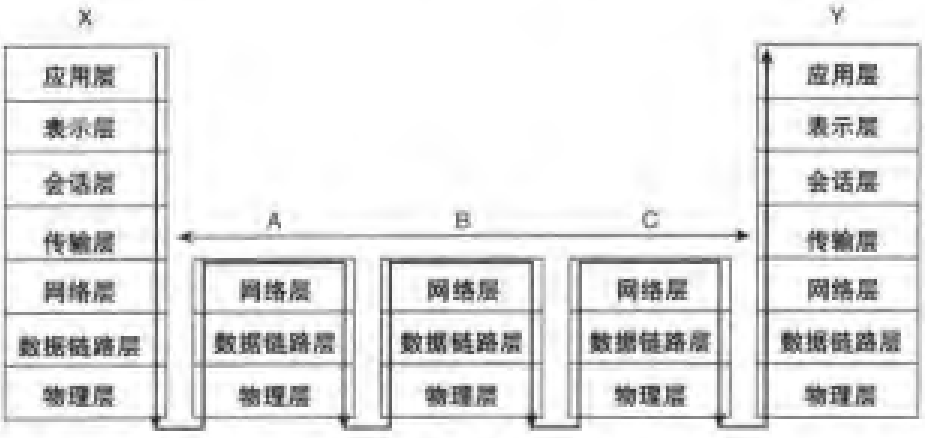


图8-22 网络层设备数据流

当一个帧被路由器接口接收后，帧中的MAC地址被提取出来并进行检查，*冲突域*里的所有设备都会执行这样的过程，这是为了确定这个数据帧的目的地址是否在本端口，或者这个帧是否是一个广

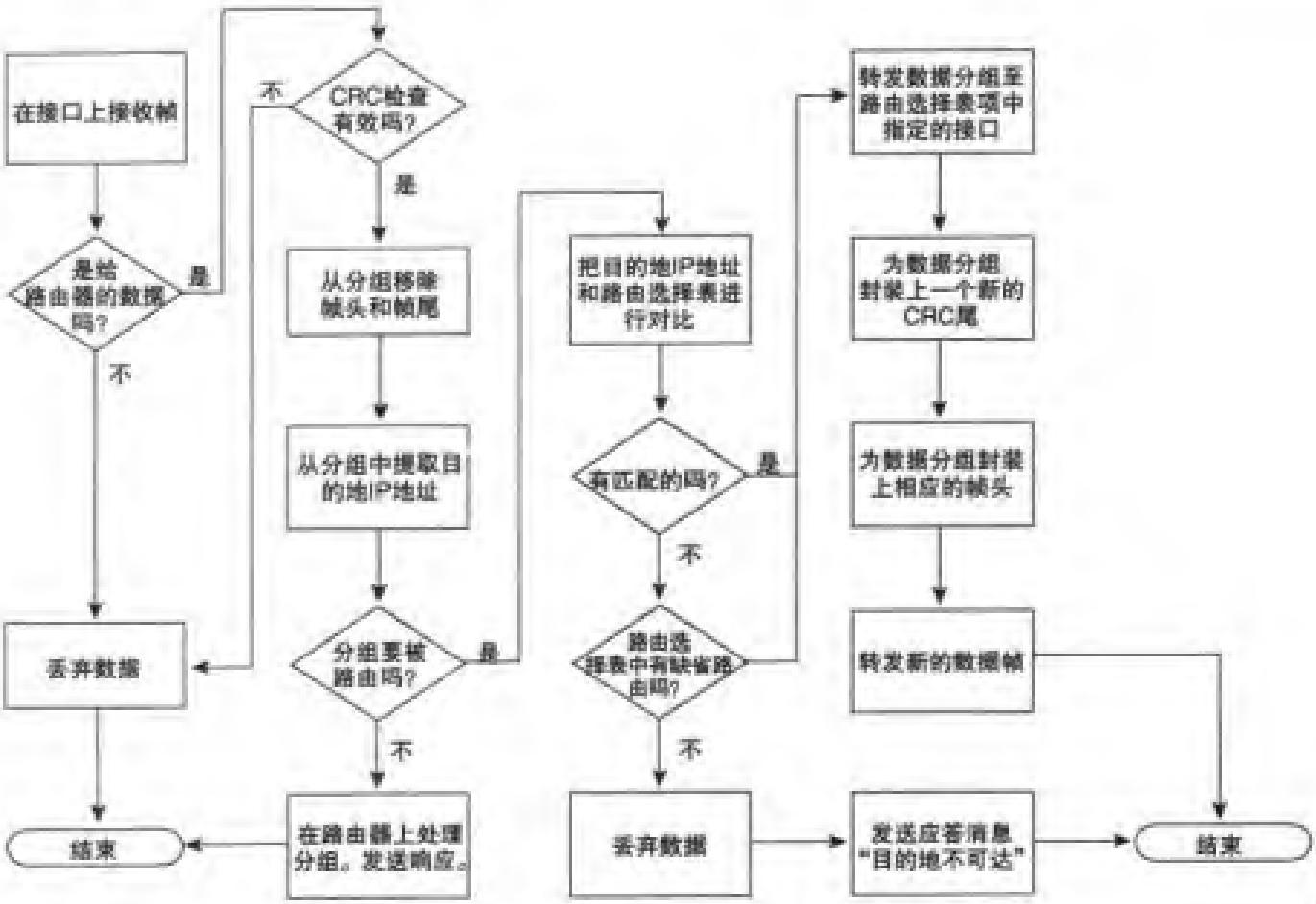


图8-23　路由器中数据封装的变化

播信号。这两种情况的结果是，数据要么被接收，要么被丢弃（因为这些数据是去往冲突域中的另一个设备）。被接收的帧要从帧尾提取信息用以进行循环冗余校验（CRC），计算的结果用来验证在接口接收的帧是否有错误。如果检查失败，帧就会被丢弃。如果检查有效，数据帧将会被剥去帧头、帧尾，其中的分组被送到第3层，路由器将会检查这个分组，看看这个分组是发给自己的还是被路由到互联网络中的其他设备。如果分组中的目的地址为路由器接口IP地址，这种类型的分组的报头将会被剥离并将数据送往第4层。如果分组需要被路由，那么分组中的目的地IP地址和路由表进行比对。如果匹配了路由选择表中的一个条目或者一条缺省路由，分组将会发往路由条目中所指向的接口。

当分组被交换到出站接口时，新的CRC值加入到帧尾，并且依照不同的接口类型（以太网、串行口、帧中继），为分组加上适当的帧头，然后数据帧被发送到去往目的地的下一个广播域。

8.1.11　无连接与面向连接网络服务的比较

OSI参考模型中大多数网络服务使用的是无连接传送系统，如图8-24所示，它们对每个分组分开对待，并且按自己的方式使分组穿越网络。也许分组经由不同的路径穿越网络，但是在到达目的地之后这些分组能够被重新组合起来。在无连接系统中，在数据发送之前，源和目的并不发生联系。与无连接系统最好的最相似的例子就是邮政系统，在信发往某地之前，接收者并不知情。信按照邮政系统的方式进行

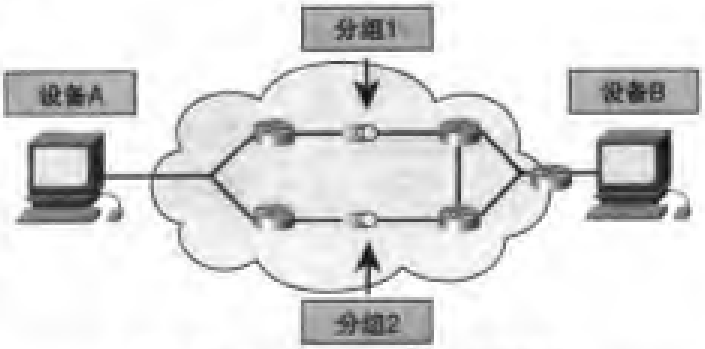


图8-24　网络服务的无连接传递系统

发送，接收者直到信到达了才了解情况。

无连接网络处理过程经常被称为*分组交换*。在这些处理过程中，在分组从源到目的地的过程中，它们可以被交换到不同路径，也会（可能）不按照顺序抵达。设备在为每个分组进行路径选择时依靠多种标准。有些标准（例如可用带宽）在转发两个分组的过程之间就有可能发生变化。

Internet是一个巨大的无连接网络，网络之中所有分组的传送都依靠IP协议。TCP（第4层）把面向连接的、可靠的服务信息附加于IP（第3层）数据之上，TCP分段信息被封装在IP分组之内，用于在Internet中传送。

IP就是一个无连接的系统；它单独处理每个分组。举一个例子，如果你使用FTP程序下载一个文件，IP协议不会把文件以整个数据流的形式进行传递；它会单独地处理每个分组。每个分组都可以通过不同的路径传送。也许其中的一些分组会丢失，IP协议依靠传输层协议来判断数据是否丢失并且请求重新传输。传输层也负责重新组合分组。

*在面向连接*系统中，数据传送之前，发送方和接收方之间就已经建立了连接，如图8-25所示。面向连接网络的一个例子是电话系统。当你打电话时，连接就建立了，然后开始通信。在面向连接网络处理过程中，首先与接收者建立连接，然后发送数据。所有的分组都沿着同一物理电路持续传输——或者，更一般情况下，是沿同一虚电路进行传输。

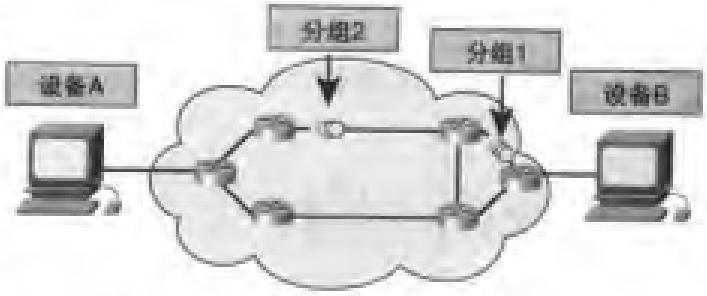


图8-25 网络服务的面向连接传递系统

8.1.12 IP分组的剖析

正如先前所讨论的，第3层分组/数据报成为第2层数据，第2层数据又被封装成为帧。类似的，IP分组，如图8-26所示，是由来自上层的数据加上IP头构成的：



图8-26 IP分组的内容

- **版本信息**——一个4比特的字段，它含有当前正在运行的IP版本信息。所有的设备必须运行相同的版本的IP协议，否则运行版本不同的设备将会拒绝接收分组。
- **IP头长度（HLEN）**——一个4比特的字段，它标明了以32比特为单位的消息中数据报报头的长度。这是所有报头信息的总长度，其中有两个可变长度报头字段。
- **服务类型（TOS）**——一个8比特的字段，它标明了一个特定的上层协议所分配的重要等级。
- **总长度**——一个16比特的字段，它表明了整个分组的长度，包括数据和报头。从总长度中减去HLEN，得到的就是数据有效载荷的长度。
- **标识符**——一个16比特的字段，它包含一个整数，用来标示当前数据报。这是一个序列号。
- **标记**——一个3比特的字段，其中后两位控制分段。第一位用来表示分组是否允许分段，第二位用来表示在连续的数据分段中，本数据分段是否是最后一个。
- **分段偏移量**——一个13比特的字段，它帮助重组数据分段。这个字段允许标记字段终止在16比特边界。

• **存活时间（TTL）**——一个8比特的字段，它维护着一个计数器，这个计数器按一定增量逐渐地减少到0。当到0这一点时，数据报将被丢弃，使分组不会无限制地循环。一个典型的例子是跳数。

• **协议**——一个8比特的字段，它指明了在IP处理过程结束后，哪一个上层协议将接收入站的数据。例如TCP和UDP。

• **报头校验和**——一个16比特的字段，它帮助确保IP头的完整性。

• **源IP地址**——一个32比特的字段，它指明了发送节点的IP地址。

• **目的地IP地址**——一个32比特的字段，它指明了接收节点的IP地址。

• **选项**——一个可变长度的字段，它使IP可以支持不同的功能选项，比如安全性。

• **填充**——这个字段填充了额外的0以确保IP头总是32比特长度的倍数。

• **数据**——可变长度字段（最大为64Kb），它包含来自上层协议的信息。

IP分组由上层数据和刚才描述的报头信息组成。迄今为止，尽管本书的焦点在IP源地址和目的地址上，但其他的报头字段使IP具有灵活性和富有弹性。报头字段是一些提供给上层协议的信息，上层协议定义分组中的数据。在前面几章中讨论了层的独立性；在前面列表中的报头信息允许了这种独立性的存在。

8.2　子网划分的机制

Internet最初的两层分层结构假想每个站点都仅仅有一个网络。这样，从每个站点到Internet就只需要一个单一的连接。一开始，这个假想是可行的。然而随着时间的推移，网络计算技术不断成熟并扩充。到1985年，一个组织只有一个单一的网络或满足于与Internet只有一个单一的连接的假想就已经不再可行了。

当站点开始开发多个网络时，对Internet工程任务组来说面临着一个很突出的问题就是：他们非常需要一种机制来区分已经形成的多重逻辑网络，如Internet第二级子网。

8.2.1　子网划分介绍及原因

为创建子网结构，主机8比特字节位必须划分为网络位来使用。这通常被叫做*借位*，更精确的术语应该叫做*租位*。这个过程通常都是从最左边的主机位为起点，起点取决于IP网络的类别。

除了易管理的需求之外，子网连接让网络管理员为LAN提供了广播限制和基本的安全性。提供安全性是因为，经由LAN上的子网划分，到其他子网的访问是由路由器来提供的。路由器，正如将在第20章“访问控制列表”中学到的，能够基于各式各样的标准来配置，由它决定是允许还是拒绝对一个子网的访问，从而提供了安全性。一些A类和B类的网络拥有者发现通过子网配置，还能把闲置的IP地址租借或售卖，为组织创造新的收入来源。

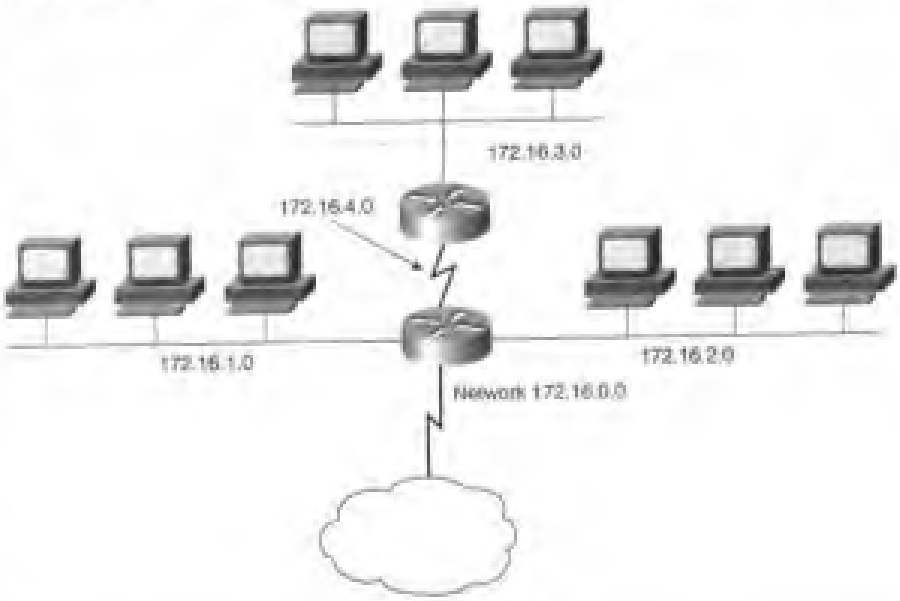


图8-27　子网

在多网络的环境里，每个子网连接到Internet上都要通过一个共同的节点——路由器，如图8-27所示。内部网络环境的详

细情况对Internet来说是无意义的，它们由一个能够（或应该能够）传送自己的数据报的专用网络组成。因此，Internet只用关心怎样使数据发送到专用网络的网关路由器就可以了。在专用网络中，主机部分的IP地址能够被再分，以此来创建子网。

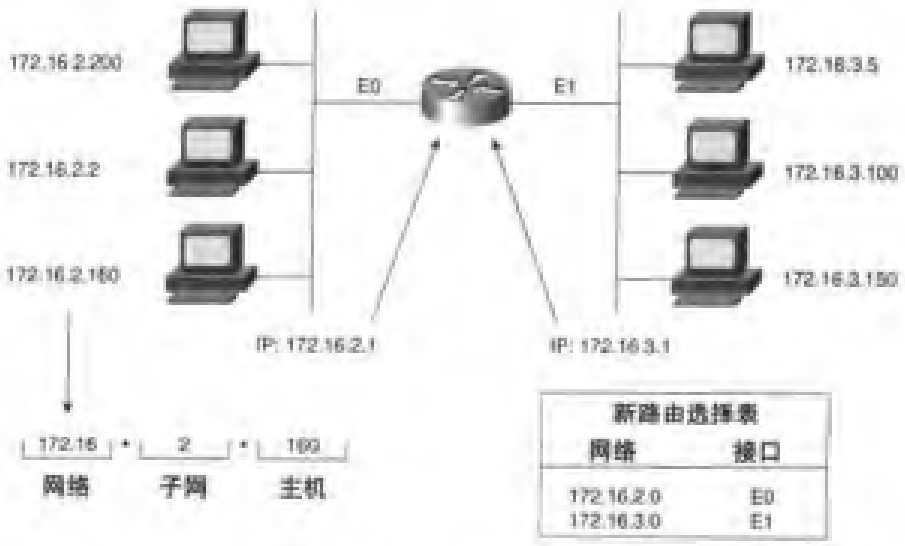


图8-28 子网地址

因为子网地址是取自A类、B类或C类的主机部分，它是本地分配的，通常由管理员来分配。而且，像其他IP地址部分一样，每个子网地址在它的域里必须是惟一的，如图8-28所示。

在局域网被互相连接形成广域网的时候，子网划分通常是很必要的。例如，如果你想要连接两个在不同地理位置的局域网，你可以给每一个局域网和它们之间的广域网链路指定一个单一的子网。然后两个路由器（每个局域网上一个）就能够在局域网（子网）之间路由分组了。

另一个使用子网的最初原因就是为了减少广播域的大小。广播被发送到在网络或子网网络上的所有主机。当广播流量开始消耗太多可用带宽的时候，网络管理员也许就会选择减少广播域的大小。

外部世界把局域网看作是一个整体的网络，并不知道其内部的网络结构。这样的网络概念保持着路由选择表的小容量和有效性。给定一个本地节点地址192.168.10.14，局域网外的领域看到的只有被通告的主要网络号192.168.10.0。这样的原因是本地地址192.168.10.14只在局域网192.168.10.0中有效。它在其他任何地方都是不起作用的。

子网地址包括A类、B类和C类网络部分，加上子网字段和主机字段。这些是从主IP地址最初的主机部分中创建的，具体的方法是将主机部分的比特分配给地址中最初的网络部分。把地址的初始主机部分分成新的子网和主机字段，能够为网络管理员提供分配地址的灵活性，如图8-29，8-30和8-31所示。这就

C类网络地址 192.168.10.0

11000000.10101000.00001010.00000000
N . N . N . H

11000000.10101000.00001010.00000000
N . N . N -sN H

在这个例子中，有3位被指派给子网

图8-29 C类地址的主机八位字节的再划分

B类网络地址 147.10.0.0

10010011.00001010.00000000.00000000
N . N . N . H

10010011.00001010.00000000.00000000
N . N . sN H . H

在这个例子中，有5位被指派给子网

图8-30 B类地址的主机八位字节的再划分

A类网络地址 28.0.0.0

00011100.00000000.00000000.00000000
N . H . H . H

00011100.00000000.00000000.00000000
N . sN . sN H . H

在这个例子中，有12位被指派给子网

图8-31 A类地址的主机八位字节的再划分

意味着在分配一个IP寻址方案和扩展网络的时候，网络管理员有更多的选择。

8.2.2　建立子网掩码地址

选择子网中所用的位数取决于每个子网所要求的最大主机数。创建子网网络时，为了计算所使用的主机位的结果，你必须了解一些基础的二进制算术和每8位字节中每个位置的值，如表8-2中所示。

表8-2　子网划分图表：比特位和值

比特	1	2	3	4	5	6	7	8
值	128	64	32	16	8	4	2	1

无论IP地址类别，其最后的八位字节的最后两位不允许分配给子网。它们叫做最后两位有效比特位。除了这两个比特，如果使用所有剩下的比特位，那么每个子网中只有两个可用主机地址。这是在串行路由器链路上节省地址的方法。然而，对一个工作着的局域网来说，这么做的后果是高昂的设备开销。

通过计算特定主机所属的子网，来给出路由器所必需的子***网掩码***，找到上表中相对应所需的位数的列，并记下掩码值，如后面的图8-35所示。这个值是由累加所使用比特位的位置值计算出来的。如果借用了3比特，C类网络地址的子网掩码就应该是255.255.255.224，如表8-3所示。这个掩码也可以用斜杠格式来表示，如/27。斜杠后的数字是网络部分和子网掩码中比特的总个数。

表8-3　子网划分图表：子网掩码标识符（两种格式）

斜杠格式	/25	/26	/27	/28	/29	/30	—	—
掩　码	128	192	224	240	248	252	254	255
比　特	1	2	3	4	5	6	7	8
数　值	128	64	32	16	8	4	2	1

为了决定所要用到的比特位，网络设计者需要计算出最大的子网络需要多少台主机，以及子网络的数量。例如，假设需要30台主机和5个子网络。要计算再分配所用到的比特位，请参考表8-4中的“可用主机”一行。例如，有30台可用主机，就需要3比特位。这样也能创建6个可用子网网络，可以满足这个方案的要求。此外，可用主机数和主机总数的区别在于：每个子网络使用第一个可用的地址作为网络ID，最后一个可用地址作为广播地址。有类路由选择不能提供使用这些子网的功能，而无类路由选择挽救了很多这样的“丢失”的地址，如表8-4所示。这个表解释了当你不是使用无类路由选择协议时子网和主机的损耗。

表8-4　子网划分图表：子网与主机

斜杠格式	/25	/26	/27	/28	/29	/30	—	—
掩　码	128	192	224	240	248	252	254	255
比　特	1	2	3	4	5	6	7	8
数　值	128	64	32	16	8	4	2	1
子网总和		4	8	16	32	64		
可用子网		2	6	14	30	62		
主机总和		64	32	16	8	4		
可用主机		62	30	14	6	2		

另一种用以计算子网掩码和网络数量的公式是：

可用子网数等于2的借用子网位数次幂减去2：

（$2^{\text{子网借用位数次幂}}$）-2 = 可用子网数

例$2^3-2=6$

可用主机数等于2的剩余部分位数次幂减去2：

（$2^{\text{剩余位数次幂}}$）-2 = 可用主机数

例$2^5-2=30$

8.2.3 创建子网

要创建子网，你必须要扩展地址的路由选择部分。Internet把你的网络当成完整的网络来“了解”，识别成拥有8、16、24个路由选择位（网络号）的A、B、C类地址。子网字段表示的是附加的路由选择位，所以在你组织内的路由器可以在整个网络的内部辨认出不同的区域或子网。

子网掩码与IP地址使用一样的地址结构。换句话说，每个子网掩码是32位长，并且被分成了4个8比特字节。子网掩码的网络和子网络部分全为1，主机部分全为0。缺省情况下，如果在没有借位的情况下，B类网络的子网掩码是255.255.0.0。如果借了8位，那么这个B类网络的子网掩码为255.255.255.0，如图8-32、8-33所示。因为一个B类网络地址的主机字段中含有两个8比特字节，所以总共有14位可以被借来创建子网。一个C类地址的主机部分只含有一个8比特字节，所以在C类网络中只有6位可以被借来创建子网。

子网字段总是直接跟在网络号后面。也就是说，被借的位必须是缺省主机字段的前n位。这个n是新子网字段的长度，如图8-34所示。对路由器来说，子网掩码是判断哪些位是路由选择位，哪些位是主机位时的依据。

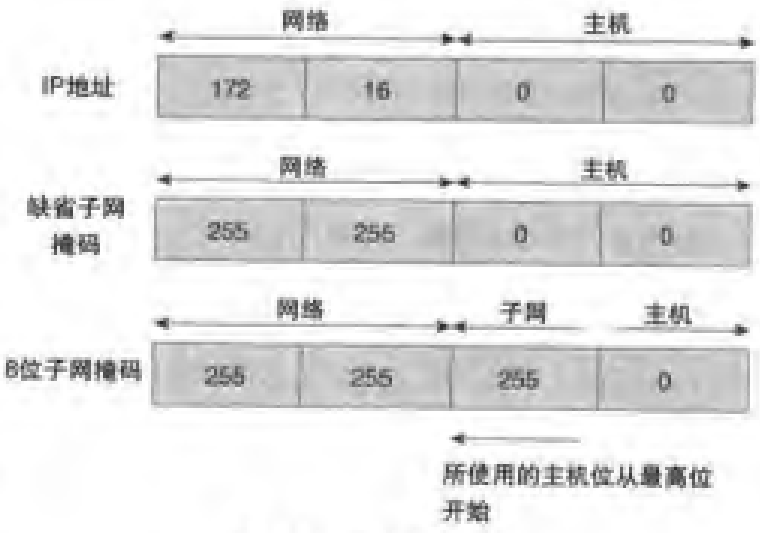


图8-32 网络与主机地址

128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

图8-33 二进制转换图表



图8-34 B类地址子网划分

决定子网掩码的大小

子网掩码使地址网络位（由地址类别决定）和子网位全为1，剩下的位都为0，这些位作为地址的主机部分。

缺省情况下，如果你没有借位，一个B类网络的子网掩码是255.255.0.0，这是点分十进制表示形式，它等同于B类网络的网络号部分全为1，其余16比特全为0。

如果为建立子网借用8比特的话，子网掩码因为包括8个额外的1比特而变成255.255.255.0。结合B类地址130.5.2.144（子网划分借走8位），路由器知道要把分组发送到网络130.5.2.0而不是网络130.5.0.0，如图8-35所示。

另一个例子，C类地址197.15.22.131，子网掩码是255.255.255.224。最后一个8比特字节的值是224（二进制表示为11100000），从24比特的C类网络部分借用3比特，一共是27比特。最后一个8比特字节131表示它是子网197.15.22.128中的第三个可用主机地址，如图8-36所示。Internet中的路由器（因为不知道主机的子网掩码）只需要考虑到C类网络197.15.22.0的路由选择，而这个网络中的路由器，因为知道子网掩码，依据27比特做出路由选择决定。



图8-35　子网掩码：B类地址



图8-36　子网掩码：C类地址

计算子网掩码和IP地址

当你从主机字段借位，应当注意到每次当你借用1位时，所创建出来的附加子网数量。我们已经了解到，在借位时不能只借1比特，至少要借2比特。借2比特可以创建4（2×2）个子网（但是你必须知道这其中包括两个保留子网和两个可用子网）。当每次从主机字段借位时，所创建的子网数量就增加2的乘方，当你借3位时就可以创建8个子网（2×2×2）。借4位就可以创建16个子网（2×2×2×2）。从这些例子和如图8-33所示的二进制转换表，很容易就可以看到，每从主机字段借一位，子网数量就增加一倍。

计算每个子网中的主机数

当每次从主机字段借走一位时，用于主机数量的位就少了一位。相应地，当每次从主机字段借一位时，可用主机的数量就减少2的乘方（减少一半）。

为了了解这是如何工作的，考虑一个C类网络地址。如果没有标明子网掩码的话，最后一个8比特字节中的所有8比特全都用于主机字段，因此，一共有256（2^8）个地址可以分配给主机（减去两个不可用地址后，一共有254个可用地址）。现在，设想一下把这个C类网络划分成子网。如果从8比特的主机字段借2位时，主机字段减少到6比特。如果你把剩下6比特位中0和1的所有可能的排列组合写出来，你就会发现每个子网中主机总数减少到了64（2^6）个，可用主机数减少到62个。

还是同一个C类网络，如果你借3位，主机字段减少到5位，每个子网中主机总数减少到了32（2^5）个，可用主机数减少到30个。

每个子网中的主机地址数量与所创建的子网数量有关。举一个例子，在一个C类网络中，如果所应用的子网掩码是255.255.255.224，从主机字段借用了3比特（十进制数224等于二进制数11100000），创建了6个可用子网（8-2），每个子网中有30（32-2）可用主机地址。

8.2.4　通过与运算计算驻留子网络

就像先前提到的，网络地址或子网地址的主机部分全为0。要路由一个分组，路由器首先要测定目的地的网络/子网地址。为了实现这个目的，路由器要对目的主机IP地址和它的子网掩码做一次逻辑与运算。

设想一下，你有一个网络号为172.16.0.0的B类网络，在评估了网络需求后，你决定借8位用来创建子网。正如先前所学习的，在一个B类网络中借8位的话，子网掩码为255.255.255.0，如图8-37所示。



图8-37　8比特子网

当一些外部网络向IP地址为172.16.2.120的主机发送数

据时，为了决定向哪发送数据，路由器会把这个地址和子网掩码作与运算。将这两个数进行与运算之后，主机部分的运算结果始终是0。主机部分左面的就是网络号和子网。因而，数据都被发往子网172.16.2.0，只有最终的路由器注意到这些分组是发送给子网中的主机地址为120这个主机的。

现在，设想你有一个同样的网络172.16.0.0。可是这次你决定只借7位用来创建子网，那么这里子网掩码的二进制表示为11111111.11111111.11111110.00000000。它的十进制数表示结果是多少？当一些外部网络再次向IP地址为172.16.2.120的主机发送数据时，为了决定向哪里发送数据，路由器会把这个地址和子网掩码作与运算。和上面一样，将这两个数进行与运算之后，主机部分的运算结果始终是0。在第二个例子当中有什么不同吗？在十进制数表示下，所有数字看起来都是一样的。不同的是可用子网数和每个子网中的可用主机数，你只能通过比较两个不同的子网掩码了解这些，如图8-38所示。



图8-38 网络号增长7比特

子网字段有7比特，这样只会产生126个子网络，那么每个子网中会有多少个主机呢？主机字段占多少位？主机号占9比特，那么在126个子网中，每个子网都具有510个主机。

实验活动 子网划分基础

这个练习概括论述了子网划分和与运算。通过给出的网络地址和使用要求，由你来计算出子网掩码、每个子网的网络号和子网中的主机号及可用子网和主机数。你也需要通过与运算来判断一个IP地址是本地的还是远程的。最后，通过给定的网络号和子网掩码，由你判断出有效和无效的IP地址。

实验活动 A类网络的子网划分

在这个练习中，你将通过指定的网络部分位数来分析一个A类网络地址，由此得出子网掩码、子网号、每个子网的主机数和子网的详细信息。

实验活动 B类网络的子网划分

在这个练习中，你将通过指定的网络部分位数来分析一个B类网络地址，由此得出子网掩码、子网号、每个子网的主机数和子网的详细信息。

实验活动 C类网络的子网划分

在这个练习中，你将通过指定的网络部分位数来分析一个C类网络地址，由此得出子网掩码、子网号、每个子网的主机数和子网的详细信息。

8.3 总结

本章学习了以下知识点：

- 路由选择协议和被路由协议的差别，包括机制和特征上的不同。
- 为了给网络管理员分派地址提供更大的弹性，网络——特别是庞大的网络——经常被划分为几个更小的网络，叫做子网网络或者子网。子网划分通过把一个单一的网络划分为仅在这个网络内可见的许多个子网，使网络管理员能避免可用IP地址的局限性。
- 子网掩码的作用是告诉设备，地址的哪个部分为网络号、子网号，哪部分是主机号。
- 网络层的网络互联功能包括网络寻址和数据流的最佳路径选择。
- 如何解释IP寻址、IP地址分类、保留地址空间、私有地址空间和IP子网划分。

请务必结合相关的e-Lab实验活动、视频和插图来补充学习本章内容。你将会在随书附赠的CD-ROM中找到这些内容。这些CD是用来补充资料以及强化本章中介绍的概念。

8.4　关键术语

算法（*algorithm*）　算法是已经定义好的解决某种问题的规则或处理过程。在网络环境中，算法通常用来决定数据从某个源到某个目的地的最佳路由。

自治域系统（*autonomous system*）　在单一管理控制之下的一个或一组网络，例如Cisco.com域。

广播（*broadcast*）　广播是指发送给网络上所有节点的数据分组，它通过广播地址进行识别。

广播域（*broadcast domain*）　广播域是一个设备集，其中的设备能接收来自该设备集中任何设备的广播帧。因为路由器不会转发广播帧，所以广播域通常以路由器为边界。

无类域间路由（*classless interdomain routing, CIDR*）　由BGP支持的基于路由聚合的技术。CIDR可以聚合路由条目以削减核心路由器上的路由信息的数量。使用CIDR技术，多个IP网络对于外界网络看起来好像是一个单独的大型实体。

冲突域（*collision domain*）　在以太网环境中，冲突的帧传播的网络区域。中继器和集线器传播冲突，交换机、网桥和路由器则不会传播冲突。

无连接（*connectionless*）　数据传输时不需建立虚电路。

面向连接（*connection-oriented*）　数据传输时需要建立虚电路。

数据报（*datagram*）　数据报是指信息的逻辑组，作为一个网络层单元而通过传输介质传送，发送时不需要预先建立虚电路。IP数据报是Internet中主要的信息单元。“信元”、“帧”、“消息”、“分组”和“段”等术语也在OSI模型的各层和各种技术领域被用来描述逻辑信息组。

距离矢量路由选择（*Distance-vector routing*）　距离矢量路由选择算法是一种计算路由的跳数以找到最短路径生成树的路由选择算法。该算法要求每个路由器每次路由更新时发送整个路由选择表，但仅发送给其相邻路由器。这种算法易于产生路由环路，但算法要比链路状态路由选择算法简单。也称为Bellman-Ford路由选择算法。

外部网关协议（*Exterior Gateway Protocol, EGP*）　在自治系统之间交换路由选择信息的Internet协议。边界网关协议（BGP）就是一个EGP。

跳（*hop*）　数据分组从一个网络节点（通常为路由器）传送到另一个网络节点的一段通路。

跳数（*hop count*）　跳数是一种用来度量源和目的地之间距离的路由选择度量标准。RIP把跳数作为它的惟一度量标准。

内部网关协议（*Interior Gateway Protocol, IGP*）　用于自治系统内部交换路由选择信息的Internet协议。常见的Internet内部网关协议的例子有IGRP、OSPF和RIP。

内部网关路由协议（*Interior Gateway Routing Protocol, IGRP*）　Cisco开发的用于处理大型多种类网络中与路由选择相关的问题的IGP。

IP地址（*IP address*）　IP地址是分配给TCP / IP主机的32位地址。IP地址分成五类（A、B、C、D、E），表示为以句点分开的4个八位字节（点分十进制格式）。每个地址包含网络号、子网号码（可选）和主机号码。网络和子网号码一起用于路由选择，主机号码用于寻址网络中的单个主机。子网掩码用于从IP地址中抽取网络和子网信息。CIDR提供了一种新方式来表示IP地址和子网掩码。也称为Internet地址。

MAC地址（*MAC address*）　MAC地址是每一个连接到局域网的端口或设备所必需的标准化数据链路层地址。网络中的其他设备使用这些地址来寻找网络中的特定端口，创建并更新路由选择表和数据结构。

MAC地址由IEEE控制，其长度为6个字节。也称为硬件地址、MAC层地址和物理地址。

NetBios扩展用户接口（*NetBIOS Extended User Interface, NetBEUI*） NetBIOS的增强版本，诸如LAN Manager、LAN Server、Windows for Workgroups和Windows NT这些网络操作系统采用此协议。NetBEUI标准化了传输帧并添加了附加的功能。NetBEUI实施了OSI LLC2协议。

8比特字节（*octet*） 由8比特构成的字节。在网络互连中经常使用的一个术语，而不用术语“字节（byte）”，这是因为某些计算机体系使用的不是8比特长的字节。

分组（*packet*） 包括含有控制信息的头和用户数据（通常情况下）信息的逻辑组。分组最常用来指网络层数据单元。“数据报”、“帧”、“消息”和“段”等术语也在OSI模型的各层和各种技术领域中被用来描述逻辑信息组。

协议栈（*Protocol stack*） 协议栈是指一套作为一组同时运行的相关通信协议，它们在OSI模型7层的几层或所有层上进行通信。并不是所有协议栈都覆盖模型的每一层，通常协议栈中的一个协议一次处理多个层。TCP／IP就是一个典型的协议栈。

被路由协议（*Routed protocol*） 能够为信息分组按照寻址方案从一个主机发往另一个主机提供足够的网络层地址信息的任何网络协议。

路由器（*Router*） 路由器是网络层设备，它采用一种或多种度量标准来确定转发网络数据的最佳路径。路由器根据网络层信息将分组从一个网络转发到另一个网络。有时也称为网关（尽管网关的定义已经渐渐过时）。

路由选择信息协议（*Routing Information Protocol, RIP*） 是随UNIX BSD系统提供的IGP（内部网关协议），使用跳数作为路由选择度量标准。

路由选择度量标准（*Routing metric*） 它是路由选择算法用来确定一个路由是否优于另一个路由的依据。该信息存储在路由选择表中。度量标准包括带宽、通信代价、延迟、跳数、负载、MTU、路径代价和可靠性。有时简称为度量标准。

路由选择协议（*Routing protocol*） 路由选择协议是通过特定路由选择算法来完成路由选择的协议。路由选择协议的实例包括IGRP、OSPF和RIP。

路由选择表（*Routing table*） 路由选择表是存储在路由器或其他网络互连设备中的表，该表记录到特定网络目的地的路由，可能也会包含与这些路由相关的度量标准。

子网地址（*Subnet address*） 子网地址是通过子网掩码指定作为子网的IP地址部分。

子网掩码（*Subnet mask*） 子网掩码是32位的地址掩码，在IP中用来指示子网地址所使用的比特。有时也简称为掩码。

子网络（*Subnetwork*） 1. 在IP网络中，是指共享某一特定子网地址的网络。子网络是由管理员进行任意分段的网络，其目的是提供多层次、分层的路由选择结构，而屏蔽连接网络的寻址复杂性。有时也称为子网（subnet）。2. 在OSI网络中，子网络是指在一个管理域的控制下使用一个网络访问协议的ES和IS的集合。

8.5 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 一个IP地址由多少比特构成?
   A. 16
   B. 32
   C. 64
   D. 以上都不是
2. IP地址中每个8比特字节的最大值是多少?
   A. 28
   B. 255
   C. 256
   D. 以上都不是
3. 在IP地址中网络号扮演什么角色?
   A. 它确定了主机所属的网络
   B. 它标识了网络中主机的身份
   C. 它确定了子网络中哪一个节点存在编址
   D. 它确定了网络中哪一些设备可以相互通信
4. 在IP地址中主机号扮演什么角色?
   A. 它标识了网络中主机的身份
   B. 它确定了子网络中哪一个节点存在编址
   C. 它确定了主机所属的网络
   D. 它确定了网络中哪一些设备可以相互通信
5. 二进制数101101转换为十进制数是多少?
   A. 32
   B. 35
   C. 45
   D. 44
6. 将十进制数192.5.34.11转换为二进制数是
   A. 11000000.00000101.00100010.00001011
   B. 11000101.01010111.00011000.10111000
   C. 01001011.10010011.00111001.00110111
   D. 11000000.00001010.01000010.00001011
7. 将二进制数IP地址 11000000.00000101.00100010.00001011转换为十进制是
   A. 190.4.34.11
   B. 192.4.34.10
   C. 192.4.32.11
   D. 以上都不是
8. 下面哪一部分是B类地址154.19.2.7的网络地址?
   A. 154
   B. 154.19
   C. 154.19.2
   D. 154.19.2.7

9. 下面哪一部分是IP地址129.219.51.18的网络地址?

A. 129.219

B. 129

C. 14.1

D. 1

10. 下面哪一个地址是带有子网掩码255.255.0.0 的网络123.10.0.0的广播地址?

A. 123.255.255.255

B. 123.10.255.255

C. 123.13.0.0

D. 123.1.1.1

11. 一个C类网络中有多少个可用主机地址?

A. 253

B. 254

C. 255

D. 256

12. 一个B类网络中最多可以有多少个子网?

A. 16

B. 256

C. 128

D. 以上都不是

13. 在划分子网时至少可以借几位?

A. 1

B. 2

C. 4

D. 以上都不是

14. 使用子网的主要原因是什么?

A. 减少冲突域的尺寸

B. 增加主机的数量

C. 减少广播域的尺寸

D. 以上都不是

15. 子网掩码由多少比特构成?

A. 16

B. 32

C. 64

D. 以上都不是

16. 对IP地址131.8.2.5和255.0.0.0执行与运算，得到的网络地址是多少?

A. 131.8.1.0

B. 131.8.0.0

C. 131.8.2.0

D. 以上都不是

17. 在C类网络中划分子网最多可借多少位?

A. 2

B. 4
C. 6
D. 以上都不是

18. 对于C类网络地址197.15.22.31和子网掩码255.255.255.224，在划分子网时最多可借多少位？
A. 1
B. 2
C. 3
D. 以上都不是

19. 对IP地址172.16.2.120和255.255.255.0执行与运算，得到的子网地址是多少？
A. 72.0.0.0
B. 172.16.0.0
C. 172.16.2.0
D. 以上都不是

20. 下面哪一条是对OSI模型第3层——网络层的最佳描述？
A. 它保证节点之间的可靠通信
B. 网络层与物理地址和网络拓扑有关
C. 它决定数据在网络中传输时的最佳路径
D. 它管理在两个表示层之间的数据交换

21. 路由器的哪个功能是用来评估路径并确定转发数据报的首选路径？
A. 数据联系
B. 路径选择
C. 同步数据链路控制接口协议
D. 帧中继

22. 网络层是如何将分组从源发送到目的地的？
A. 通过使用IP路由选择表
B. 通过使用ARP响应
C. 通过向名称服务器咨询
D. 通过向网桥咨询

23. 网络层地址的哪两个部分被路由器用来在网络中传送数据？
A. 网络地址和主机地址
B. 网络地址和MAC地址
C. 主机地址和MAC地址
D. MAC地址和子网掩码



第9章 TCP/IP传输层与应用层

目标

学习完本章之后，你应该能够：

- 描述TCP / IP传输层的功能。
- 描述流控制。
- 描述对等系统之间建立连接的过程。
- 描述窗口机制。
- 描述确认机制。
- 鉴别和描述传输层协议。
- 描述传输控制协议（TCP）的报头格式及端口号。
- 描述用户数据报协议（UDP）的报头格式及端口号。

传输层使用网络层为其提供的服务，例如最优路径选择和逻辑寻址，以提供源主机与目的主机之间端到端的通信。本章讲述了传输层如何可靠而又准确地控制源主机与目的主机之间的信息流。传输层的主要特征包含以下几方面：

- 传输层数据流是网络端点之间的逻辑连接。
- 通过滑动窗口、序号和确认机制来提供端到端的控制及可靠性。
- 第4层协议TCP和UDP使用*端口号*来区分网络上同一时间的不同会话，并向上层传递信息。

TCP / IP应用层的主要特征包含以下几方面：

- 终端用户的应用位于此层。
- 常用的应用包括NFS，DNS，ARP，rlogin，talk，FTP，NTP和traceroute。

请注意查看随书的CD-ROM中与本章相关的e-Lab实验活动、视频和插图。这些CD中的内容提供补充材料，并可强化本章中介绍的概念。

9.1 理解TCP / IP传输层

服务质量（quality of service）常用于描述第4层——传输层的作用。稍后讲到的UDP协议也工作在第4层，并且可以提供无连接的网络服务。但是，工作在本层的主要协议是面向连接的TCP协议，它的主要功能是可靠而又准确地传输并控制源主机与目的主机之间的信息流。传输层的主要职责是

提供端到端的控制，通过滑动窗口机制提供流控制，通过序号和确认机制来保证可靠性。

为了理解可靠性和流控制，可以想像一个说话非常快的人。在对话过程中，听者如果没有听明白，可能会要求他重复一遍刚才说过的话（可靠性），并且要求对方说得慢一点以便他能跟上（流控制），如图9-1所示。

传输层提供从源主机到目的主机的传输服务。它在网络端点之间建立逻辑连接。传输服务可以将数据进行数据分段并可将多种上层*应用*发送的数据重组到同一个传输层数据流中。传输层的数据流可以提供端到端的传输服务。

传输层数据流是网络端点之间的逻辑连接。传输层定义了主机应用之间端到端的连通性。图9-2举例说明了传输层。

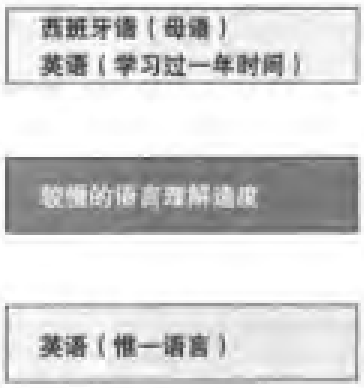


图9-1　传输层类比

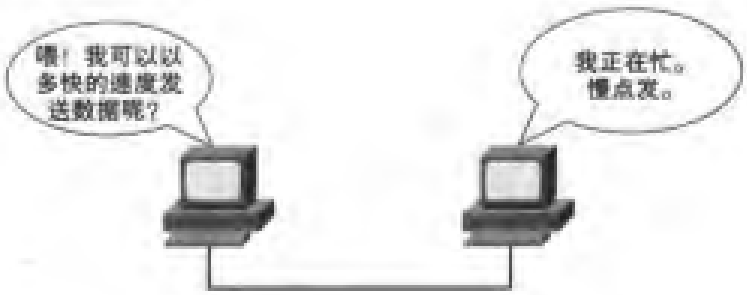


图9-2　传输层在网络设备通信中的角色

传输层提供了下列基本服务：

- 将上层的应用数据进行分段。
- 建立端到端的操作。
- 从一个终端主机向另一个终端主机发送数据分段。
- 确保通过滑动窗口提供流控制。
- 确保通过序号和确认机制提供可靠性。

传输层把网络看作“网云”，它可以通过网云从源设备向目的设备发送数据分组。网云可以从多条路径中选择到目的地的最优路径。这说明了路由器在此过程中所扮演的角色。

TCP／IP由两个独立的协议TCP和IP组成。IP是第3层的协议，它在网络中提供最有效率的网络传递服务，这是一种无连接服务。TCP是第4层的协议，提供流控制以及可靠的面向连接的服务。两个协议组合起来可以提供广泛的网络服务。TCP／IP协议集由很多协议组成，但TCP和IP是其中最关键的两个。Internet就是基于TCP／IP协议集的。

9.1.1　流控制

TCP传输控制协议发送数据分段时，可以保证数据的完整性。确保数据完整性的一种方法就是*流控制*。流控制可以避免发送数据的主机使接收主机缓存溢出的问题。缓存溢出是非常严重的问题，它会导致数据丢失。

传输层服务可使数据在主机之间可靠地传输。为了获得可靠的数据传输，正在通信的终端系统之间必须维护一个面向连接的关系。可靠的传输可以通过下列方法实现：

- 确保传送的数据分段要向发送方确认。
- 重传所有未确认的数据分段。
- 在目的端将数据分段按正确的顺序重组。

• 提供避免和控制拥塞的机制。

9.1.2 会话的建立、维持和终止的概述

在OSI参考模型和TCP / IP参考模型中，多个应用可以共享一个传输层连接。传输层的功能性是一个数据分段一个数据分段实现的。这就意味着不同的应用可以按照先来先服务（first-come，first-serverd）的原则来发送数据分段。数据分段的目的地可以是相同的，也可以是不同的，如图9-3所示。

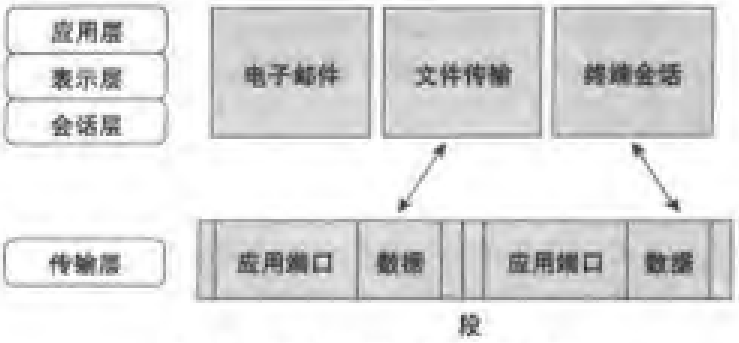


图9-3 多种应用层数据共享传输层

传输层的其中一个功能就是与其对等系统建立面向连接的会话。在数据传送开始时，发送方和接收方的应用都要通知各自的操作系统初始化一个连接。一台主机发起的连接必须被另一台台主机接受才行。操作系统中的协议软件模块会在网络上发送消息进行通信，以验证传输是经过授权的，并且双方都已经准备完毕。





图9-4 与对等系统建立连接

当所有的同步操作完成之后，一个连接就建立了，数据传输也就开始了。在传输的过程中，两台主机还需要继续通过协议软件来通信以验证数据是否被正确接收。

图9-4是一个典型的发送系统和接收系统之间的连接。第1次握手用来请求同步。第2次和第3次握手确认刚才的同步请求并且同步反方向上的连接参数。最后一个握手数据分段是一个确认，用来通知目的主机双方都同意已建立的连接。当连接建立之后，就开始进行数据传输。

在数据传输过程中，有两种原因会导致拥塞发生。第一种，一台高速主机发送的数据流量大于网络所能传输的流量。第二种，如果多台主机需要同时向同一个目的主机发送数据，目的主机就会发生拥塞，这种问题不是由单一的源主机导致的。

当数据报到达得太快而主机或网关不能处理时，它会将数据报临时存放在内存中。如果仍有持续流量，主机或网关的内存就会耗尽，此时必须丢弃再到达的数据报。

为避免数据丢失，传输层可以向发送方发送一个标识“未准备好”的指示器。该指示器像停止标志一样，指示发送方停止发送数据。当接收方有能力处理额外的数据时，接收方就会发送一个标识“准备接收”的指示器，这就像一个继续信号。当发送方收到此信号时，就会恢复数据传输。

数据传输完成后，发送端主机发送一个标识数据传输结束的指示器。接收端主机在数据传输完成后确认数据传输结束，连接终止。

9.1.3 三次握手

TCP协议是面向连接的，所以它在开始传输数据之前需要先建立连接。要建立或初始化一个连接，两端主机必须同步双方的初始序号（ISN）。同步是通过交换连接建立数据分段和ISN（初始序

号）来完成的，在连接建立数据分段中包含一个称为SYN（同步）的控制位。包含SYN位的数据分段也称作SYN。因此，此方案需要一种相应的机制来选择一个初始序号，以及稍微复杂一点的握手机制来交换ISN。

同步需要双方都发送自己的初始序号，并且接收对方的确认（ACK）信息。双方都需要接收对方的INS（初始序号），并且发送确认的ACK。具体顺序如下：

1. A->B SYN——我的初始序号是X，ACK（确认）号是0，设置SYN位，未设置ACK位。

2. B->A ACK——你的序号是X+1，我的初始序号是Y，设置SYN位和ACK位。

3. A->B ACK——你的序号是Y+1，我的序号是X+1，设置ACK位，未设置SYN位。

如图9-5所示，此交换过程就是所谓的*三次握手*。

三次握手是一种异步连接的机制，之所以需要进行三次握手是因为序号与网络上的全局时钟没有绑定在一起；由此，TCP协议可以有其他获取ISN的机制。三次握手解决的不仅仅只有序号的问题，还解决了包括窗口大小、MTU以及所期望的网络延时等其他问题。第1个SYN的接收方无法知道该数据分段是否过期，除非它能记住该连接中所用的最后一个序号（这几乎是不可能的），因此必须请求发送方验证此SYN。

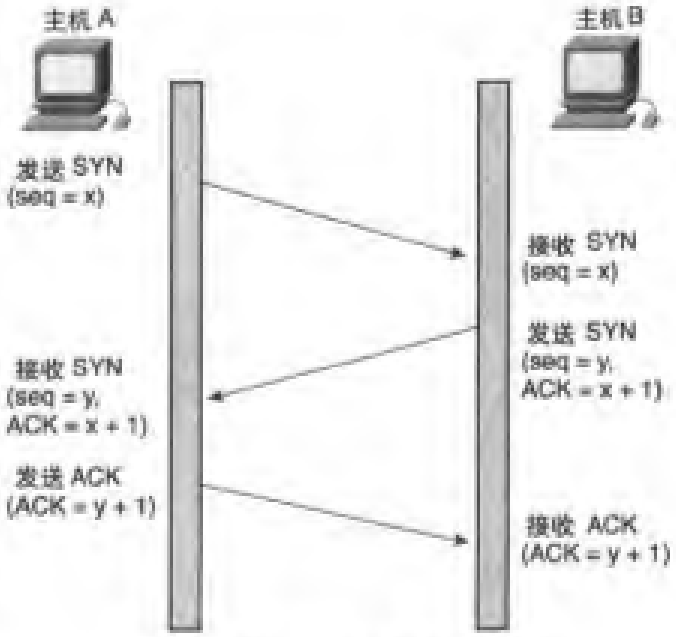


图9-5　三次握手

9.2　滑动窗口

在大多数可靠的、面向连接的数据传输的基本形式中，数据分组必须以与发送时相同的顺序传输到接收端。任何数据分组丢失、损坏、重复或接收时乱序都将导致协议出错。最基本的解决方法就是让接收方在接收每一个数据分段后都进行确认。

如图9-6所示，如果发送方在发送每一个数据分段后都要等候确认，吞吐量是很低的。因此大多数面向连接的、可靠的协议都允许一次发送多个数据帧或数据分段。因为发送方在发送完数据分组之后和处理完接收到的确认之前是有一段时间间隔的，这段间隔可以用来传输更多的数据。在没有收到确认的情况下，窗口是允许发送方发送的数据分组的个数。

TCP使用期待确认，即确认号就是所期待接收的下一个字节。滑动窗口是指在TCP会话过程中窗口大小是动态协商的。滑动窗口是一个流控制机制，要求源设备在向目的设备发送一定数量的数据之后接收一个确认。

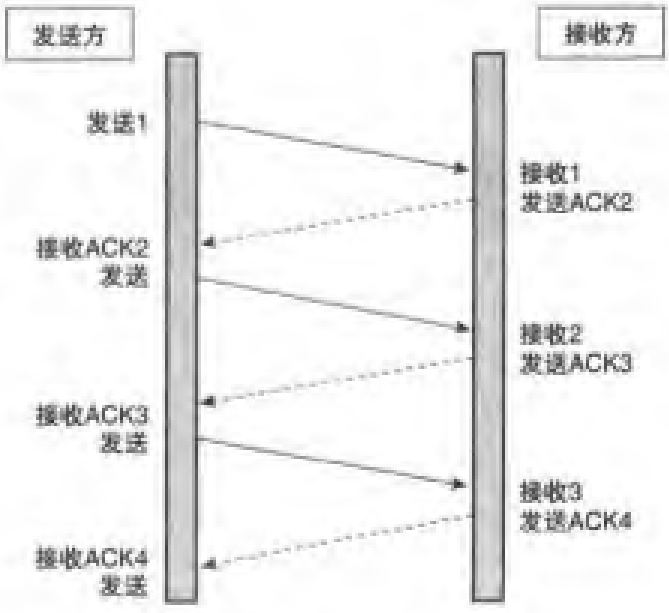


图9-6　窗口大小为1

为了控制设备之间的数据流，TCP使用了流控制的机制。接收设备向发送设备报告一个“窗口”。该窗口指定了以确认号开始、接收设备当前能够接收的比特字节数。

例如窗口大小为3，源设备可以发送3个字节到目的设备，然后需要等待一个确认。目的设备接收到这3个字节之后，向源设备返回一个确认，这时候源设备就可以继续传输下面3个字节了。如果目的设备没有接收到这3个字节——例如，因为缓存溢出——它就不会返回确认。因为源设备没有接收到确认，它知道这些字节需要重传，并且传输的速率应该降低。

在连接的生存时间中，TCP窗口的大小是可变的。每一个确认都包含着一个表示接收方能够接收多少字节的窗口信息。TCP还维持着一个拥塞控制窗口，通常，窗口大小和接收方窗口的大小一样，但是当有数据分段丢失时（例如，拥塞发生时），窗口大小就会减半。这种方法可以通过扩大或减小窗口的大小来管理缓存空间和处理进程。更大的窗口允许在收到确认前传输更多的字节。

如果发送方发送了3个字节，那么它期待的ACK就是4。如果接收方所能处理的窗口大小仅为两个字节，它就会丢弃分组3，指明3为下一个字节，并且指明新的窗口大小为2。发送方会发送下两个字节，但仍然指定自己的窗口大小为3（例如，它仍然可以接收从接收方那里来的3个字节）。接收方对它进行回复并请求字节5，它指明的窗口大小还是2。

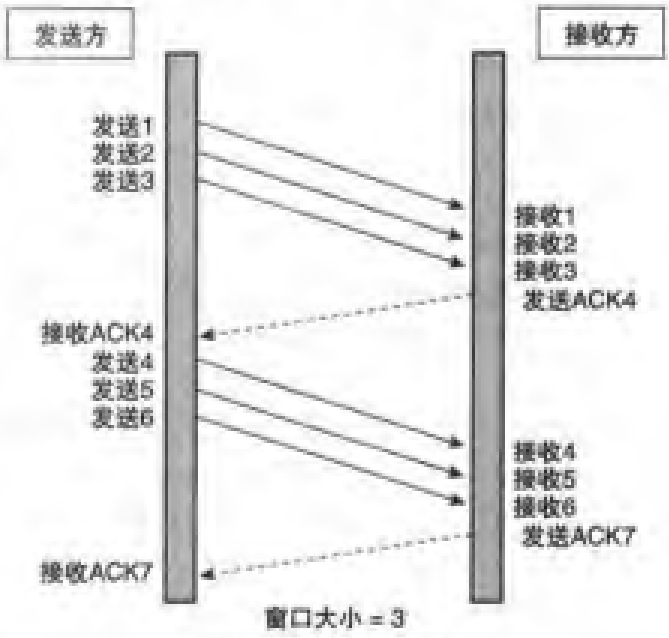


图9-7 窗口大小为3

9.2.1 确认

可靠的传输保证数据流能从一台主机通过数据链路传递到另一台主机而没有数据重复或丢失。主动确认及重传是一种保证数据可靠传输的技术。主动确认要求接收方与发送方通信，当它收到数据后，发回确认信息。发送方保持所发送的每一个数据分组（TCP数据分段）的记录并等待确认。发送方还会在发送一个数据分段时启动一个定时器，如果在定时器到期时确认还没有收到，就会重传该数据分段。

如图9-7所示，发送方发送数据分组1，2和3。接收方通过请求数据分组4来确认收到分组。发送方在收到确认之后就会发送分组4，5和6。如果分组5没有到达目的地，接收方就会通过请求重新发送分组5来进行确认。发送方在重新发送分组5且收到确认后再继续发送分组7。

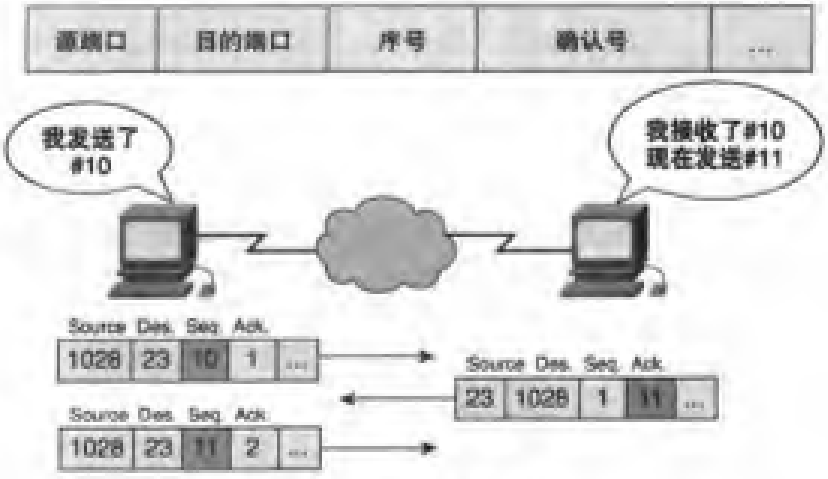


图9-8 TCP序号及确认

TCP通过前向参考确认来确定数据分段的先后顺序。如图9-8所示，在传输前，需要为每个数据报进行编号。TCP会在接收端主机将数据分段重组成完整信息。TCP必须恢复由Internet通信系统导致的数据损坏、丢失、重复和乱序。这通过为传输的每个字节指定序号，并且要求接收端TCP的主动确认（ACK）来实现。如果在一个超时

间隔内没有接收到ACK，数据就重新传输。在接收端，序号可以用来将在传输过程中可能出现乱序的数据分段正确地排列，并且排除重复的数据段。数据损坏问题可以通过在传输的每个数据分段后加上校验和来解决，接收方检查校验和，丢弃损坏的数据分段。

9.2.2 TCP

*传输控制协议（TCP）*是一种面向连接的传输层协议，能提供可靠的全双工的数据传输。TCP是TCP/IP协议栈的一部分。在面向连接的环境中，开始传输数据之前，端点之间先要建立连接。TCP负责将消息拆分成数据分段，重传丢失的数据分段并将数据分段在目的主机重组成消息。TCP在端用户应用之间提供了一条虚电路。

以下协议使用TCP：

- 文件传输协议（FTP）。
- 超文本传输协议（HTTP）。
- 简单邮件传输协议（SMTP）。
- 域名系统（DNS）。

图9-9显示了TCP数据分段格式。

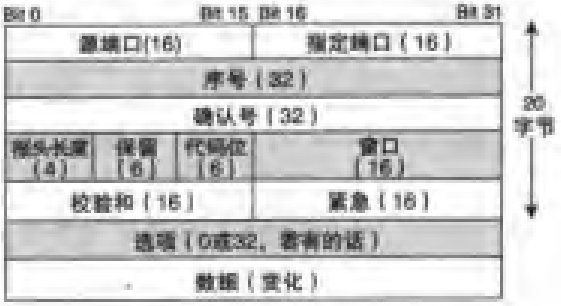


图9-9　TCP数据分段格式

下面列出图9-9中TCP数据分段中各字段的定义：

- **源端口**——呼叫方的端口号。
- **目的端口**——被叫方的端口号。
- **序号**——用于保证到达数据正确顺序的数字。
- **确认号**——期待传输的下一个TCP字节的编号。
- **HLEN**——报头字数，字长为32位。
- **保留**——设置为0。
- **代码位**——控制功能（例如建立和终止一个会话）。
- **窗口**——发送方希望接收的字节数。
- **校验和**——根据报头与数据字段计算出的校验和。
- **紧急指针**——指示紧急数据的结束。
- **可选项**——当前定义的一个选项——TCP数据分段的最大长度。
- **数据**——上层协议数据。

9.2.3 UDP

*用户数据报协议（UDP）*是TCP/IP协议栈中无连接的传输协议，其数据分段格式如图9-10所示。UDP是一种简单协议，它交换数据报而没有确认机制或传输保证。在比较UDP和TCP数据分段格式时，UDP的简单性就非常明显了。错误处理和重传机制必须由上层协议来完成。例如，如果一个TFTP下载进程因某种原因中断，操作员只能重试直到成功为止。

下面列出了图9-10中UDP数据分段中各字段的定义：

- **源端口**——呼叫方的端口号。
- **目的端口**——被叫方的端口号。
- **长度**——报头与数据的字节数。
- **校验和**——根据报头与数据字段计算出的校验和。
- **数据**——上层协议数据。



图9-10　UDP数据分段格式

UDP没有窗口机制或确认机制；所以要由*应用层*协议来提供可靠性。UDP是为那些无需将数据段排序的应用而设计的。

以下协议使用UDP：

- 简易文件传输协议（TFTP）。
- 简单网络管理协议（SNMP）。
- 动态主机配置协议（DHCP）。
- 域名系统（DNS）。

9.2.4 TCP与UDP端口号

TCP和UDP都使用端口号向上层传递信息。一个IP地址和一个端口号组合在一起称为套接字。端口号用来跟踪网络上同一时间的不同会话。

应用软件开发者一致使用由Internet地址授权委员会（IANA）控制管理的知名端口号。例如，任何FTP应用的会话使用标准端口20（对于数据）和21（对于控制），如图9-11所示。如果会话不在知名端口应用的范围内，可以从指定的1023以上的范围内随机分配。TCP和UDP都保留了一些端口，可能还没有应用支持它们，如表9-1所示。表中显示了端口号的指定范围。

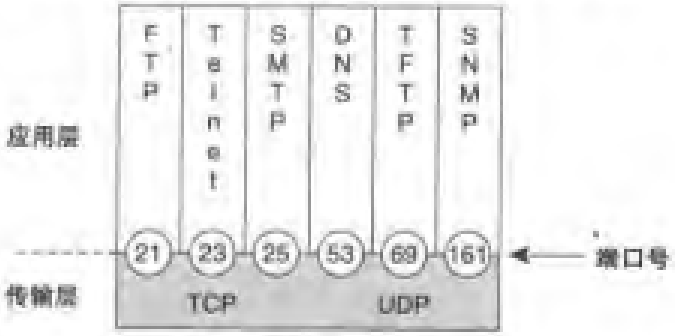


图9-11 端口号

表9-1 保留的TCP和UDP端口号

十进制端口号	关键字	描述
0	-	保留
1到4	-	未分配
5	Rje	远程作业项目
7	Echo	回应
9	Discard	丢弃
11	Users	活动用户
13	Daytime	白天
15	Netstat	谁在线或netstat
17	Quote	日期引用
19	Chargen	字符生成器
20	ftp-data	文件传输协议（数据）
21	ftp	文件传输协议
23	telnet	远程登录
25	Smtp	简单邮件传输协议
37	Time	时间
39	Rlp	资源定位协议
42	Nameserver	主机名称服务器
43	Nickname	别名
53	Domain	域名服务器
67	Bootps	自举协议服务器
68	Bootpc	自举协议客户端
69	Tftp	简易文件传输协议
75	-	任何专用拨出服务
77	-	任何专用RJE服务
79	Finger	查找器
80	HTTP	超文本传输协议
123	Ntp	网络时间协议
133到159	-	未分配

续表

十进制端口号	关键字	描述
160到223	-	保留
224到241	-	未分配
242到255	-	未分配

1024以下称为知名端口号。
1024以上为动态分配端口号。
已注册端口号是那些特定于的厂商应用已注册的端口号，多数在1024以上。

如图9-12所示，终端系统使用端口号来选择适合的应用程序。初始源端口号由源主机动态分配，通常是高于1023以上的端口号。例如，一台主机使用FTP发送分组，该分组中目的TCP端口号为21（FTP），动态生成的源端口号为1028。这对端口号（目的端口号与源端口号）定义了这些主机之间惟一的“会话”。如果同一台主机与另一台主机又发起另一个FTP会话，目的端口号仍是21，但生成的源端口号就不同了（例如1030），这样可以区分两个会话。

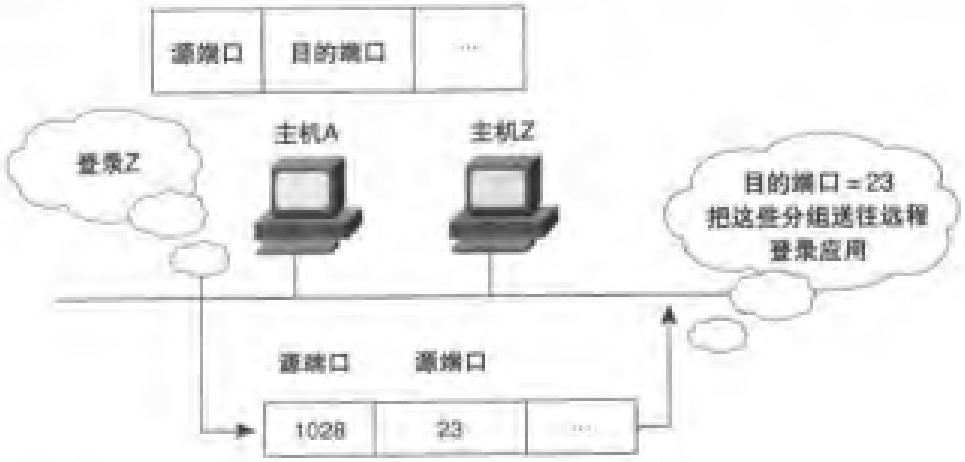


图9-12　端口号指定应用类型

9.3　TCP/IP应用层

OSI和TCP/IP模型的最后一层都是应用层。当最终用户使用应用软件与网络进行交互时，例如收发电子邮件，应用层是最接近最终用户的。通过检查以下内容你就可以看到应用层是如何处理来自客户/服务器应用、域名服务和网络应用的分组：

- Client/Server（客户/服务器）。
- Redirectors（重定向器）。
- Domain Name System（域名系统）。
- E-mail（电子邮件）。
- Telnet（远程登录）。
- FTP（文件传输协议）。
- HTTP（超文本传输协议）。

9.3.1　应用层介绍

在OSI参考模型中，应用层（第7层）为应用的通信组件提供了支持，如图9-13所示。应用层负责以下工作：

- 为预定的通信双方确认和建立通信。
- 同步协同工作的应用程序。

- 为错误恢复过程建立协商。
- 控制数据的完整性。

应用层是最靠近终端用户的一层。它决定系统之间是否具有进行通信的足够资源。如果没有应用层，就不会有网络通信的支持。应用层不能为其他层提供服务，但它为处于TCP / IP模型之外的应用程序（比如电子制表软件程序、文字处理程序和银行终端程序等）提供服务。此外，应用层为模型中其他层的网络应用程序（比如浏览器或电子邮件程序）提供直接接口，或者使用网络重定向器（redirector）为独立的应用程序（比如文字处理、电子制表以及演示管理器）提供间接接口。



图9-13 应用层

直接网络应用

大多数工作在网络环境中的应用都属于客户端 / 服务器应用。这些应用，比如FTP客户端（不是协议）、Web浏览器和电子邮件程序，都包含两部分，可分别完成客户端和服务器端的功能。客户端位于本地计算机，是服务的请求方。服务器端位于远程计算机，为客户端的请求提供响应服务。

客户端 / 服务器应用不断重复下面的循环：客户端请求，服务器响应；客户端请求，服务器响应……举例来说，Web浏览器通过请求一个统一资源定位符（URL）来访问网页，该URL解析为位于远程Web服务器的IP地址。定位URL之后，URL标识的Web服务器应答请求。然后，根据从Web服务器上接收的信息，客户端能够从同一台Web服务器上请求更多的信息，或者从另一台Web服务器中获取其他页面。

Netscape的Navigator浏览器和微软的IE浏览器几乎是最常用的网络应用。理解Web浏览器的一种简单比喻是电视遥控器。遥控器可以直接控制电视机：包括音量、频道和亮度等等。要实现正确的远程控制，无需了解远程电子控制功能是如何工作的。Web浏览器也类似，通过点击超链接来浏览网页。要使浏览器正确工作，无需关心底层的OSI协议如何完成交互工作。

间接网络支持

在局域网环境中，间接应用网络支持也是一种客户端 / 服务器功能。如果客户端要将一个文件从字处理程序存储到网络服务器中，重定向器就会使得字处理程序能够透明地完成此操作。需要记住透明性是由会话层的远程过程调用（RPC）功能提供的。

重定向器是OSI模型会话层的一个功能，它工作在计算机的操作系统和网络客户端上，而不是特定的应用程序上。

下面列出了使用重定向器的一些协议：

- AppleTalk文件归档协议。
- NetBIOS扩展用户接口（NetBEUI）。
- Novell IPX / SPX协议。
- TCP / IP协议集的网络文件系统（NFS）。

重定向器使网络管理员能够将远程资源指定给位于本地客户端的逻辑名称。当选择这样的逻辑名进行操作时，如保存文件或打印文件，网络重定向器将指定的文件发到正确的远程服务器上去处理。如果资源在本地计算机上，重定向器就会忽略该请求，让本地操作系统来处理。

在本地客户端使用网络重定向器的优点是客户端应用程序不用寻找网络。此外，应用程序在本地

请求资源服务之后，重定向器把请求重定向到相应的网络资源，而应用程序则把它看作是本地的请求。

重定向器扩展了非网络软件的能力。这使得用户在不需要特殊应用软件的情况下，可以共享文档、模板、数据库、打印机以及许多其他资源。

网络对一些应用程序的开发有很大影响，比如字处理程序、电子制表程序、演示管理器、数据库软件、图形软件以及产品软件，等等。现在很多这样的软件包都是集成了网络功能的。它们能够集成Web浏览器或Internet工具，并可以通过*超文本标记语言（HTML）*在Web上发布。

建立和中断连接

值得注意的一点是：在以前提到的例子中，与服务器的连接时间仅仅维持到一次任务的完成。在Web的例子中，连接只需维持到Web下载完成时为止。在打印机的例子中，连接仅仅维持到把文件发送到打印服务器。一个操作完成之后，连接就被拆除了。下次处理请求需要重新建立连接。这是两种通信会话方式中的一种。

在本章的后面，将学到第二种方式。通过一些例子来说明，比如Telnet、FTP，在这种方式中要建立一个服务器的连接，并一直维持到所有的操作完成为止。当用户完成操作之后，客户端计算机才终止连接。所有的通信活动都可归为上述两类。下一节，将学习应用层所支持的***域名系统（DNS）***。

9.3.2　域名系统（DNS）

Internet是建立在层次化的地址结构上的。这样可以按照地址分类来路由，而不用按单个地址进行路由选择。但是，问题在于用户如何将正确的地址和Internet站点地址对应起来。有些地址容易混淆，比如198.151.11.12和198.151.11.21，只有一个数字不同。这样，用户很容易忘记这些站点的地址，因为这些地址和站点的内容没有对应关系。

为了将站点的内容和地址对应起来，人们开发了域名系统。DNS用于Internet中，可将域名以及网络节点通告的名称转换为IP地址。域是一组通过地理位置或者商业类型相互关联的计算机。域名是一串字符和／或数字，通常是一个名称或缩写，它用来表示数字的地址。Internet中大约有超过200个顶级域名。例如：

- .us——美国。
- .uk——英国。

还有一些一般性的顶级域名，例如：

- .edu——教育站点。
- .com——商业站点。
- .gov——政府站点。
- .org——非赢利站点。
- .net——网络服务。
- .mil——美国军方站点。
- .int——国际数据库／条约组织站点。

注意：要了解关于域名的更多信息，请访问IANA站点（www.iana.org/domain-names.htm）查看域名。

域名服务器

域名系统（DNS）服务器是一种网络设备，其功能是响应客户端的请求，把域名转换为相应的IP地址。DNS系统以分级结构建立，创建不同级别的DNS服务器。

如果本地DNS服务器能将某个域名转换成为相应的IP地址，就可以在本地完成，并把结果返回

给客户端。如果它不能转换这个域名，就会将请求转发给上一级域名服务器，然后，高级服务器试图去转换这个域名。如果这一级别的服务器能转换这个域名，那么它把对应的IP地址信息发送给客户端；如果这一级别的服务器不能转换该域名，那么它把请求转发到更高级别的服务器。这个过程持续到该域名被转换或者到达最高级别的域名服务器。如果顶级域名服务器也无法找到这个域名信息，那么该域名被认为是错误的，并返回相应的错误信息。任何类型的应用，只要使用域名表示IP地址，那么都需要DNS服务器把域名转换成相应的IP地址。

9.3.3 FTP和TFTP

文件传输协议（FTP）为了下载文件（从Internet接收或者获取文件）或者上载文件（从Internet发送或者放置文件）。上载和下载文件是Internet提供的一个非常有用的功能。该功能对于那些经常使用计算机的人以及那些需要从Internet下载驱动程序并及时升级的人特别有帮助。网络管理员无需等待太久就可获得必要的驱动程序，从而使他们的网络服务器能够重新正常运行。Internet可以通过FTP及时提供这些文件。与E-mail和Telnet类似，FTP也是客户端/服务器应用。它需要在主机上运行一个服务器软件，并能够通过客户端软件来访问该主机。

FTP的会话建立和Telnet的会话建立过程一样。与Telnet类似，FTP的会话维持到客户端终止会话或者有某种通信错误发生时终止。当需要和FTP进程或者守护进程建立连接时，需要提供登录ID和密码。一般来说，可以使用Anonymous作为登录ID，用E-mail地址作为密码，这种FTP连接一般称为***匿名FTP***。建立身份标识之后，在客户端和服务器之间开启了一条命令链路。与Telnet会话类似，命令被发送到服务器并执行，结果返回给客户端。FTP能提供创建和改动文件夹、删除和重命名文件、执行等和文件管理相关联的很多其他功能。

FTP的主要功能是在计算机之间传送文件，该功能通过从服务器复制和移动文件到客户端或者从客户端复制和移动文件到服务器来完成。从服务器复制文件时，FTP建立第二条连接，也就是计算机之间的数据链路，通过这条链路传送数据。数据传输可以以美国信息交换标准码（ASCII）方式或二进制方式进行。这两种方式决定了数据文件如何在计算机之间进行传输。ACSII格式返回的是以7个ACSII字符编码表示的可读信息。第一个字符是空格或者负号，接下来是三个数字，一个小数点，最后是两个数字。如果ACSII编码小数点左边的数字少于3个数字字符，那么可选符号和数字靠右边放置，在左边填充空格。因为二进制方式每次传送4个字节，相对于ACSII格式的7个字节来说，二进制方式通过串行链路传送，花费的时间较少。但是，使用ASCII表示方式也有明显的优点。在文件传输结束以后，数据连接自动终止。当完成所有的文件复制和移动操作之后，可以退出系统，从而关闭命令链路并结束本次会话。

简易文件传输协议（TFTP）是基于UDP的无连接服务。TFTP用于路由器和交换机中传送配置文件和Cisco IOS映像文件，它在支持TFTP的系统之间传送文件。TFTP设计成很小且实施简单。因此，它丢掉了常规FTP拥有的很多特性。TFTP仅仅支持从远程服务器上读写文件（或者发送邮件）。TFTP不能列目录，到目前为止不能提供用户认证功能。TFTP在局域网内非常有用，因为它在稳定的环境中工作更快。

另一个支持文件下载的协议是超文本传输协议（HTTP），在下一节中进行讨论。HTTP的局限性在于只能下载文件，不能上载文件。

9.3.4 HTTP

超文本传输协议（HTTP）通过万维网（World Wide Web）工作，是Internet上增长最快、应用最为广泛的协议。Web迅速增长的一个主要原因是它可以很容易地实现信息的访问。Web浏览器是客户端/服务器应用，这意味着它需要服务器和客户端组件协同工作。Web浏览器在网页上以多媒

体格式表示数据，如文本、图像、声音和视频。Web页面通过一种称为超文本标记语言（HTML）的格式语言来创建。HTML使得网页浏览器把指定的网页以某种特定的方式显示出来。此外，HTML对从Web服务器上传送到Web浏览器的文本、文件和其他对象的存放地点进行了规定。

超链接使得在万维网上可以很容易进行导航。超链接是Web页面上的一个对象（单词、短语或者图片）。当点击超链接时，将会进入新的Web网页。Web页面包含（通常隐藏在HTML的内部描述中）地址定位，称它为统一资源定位符（URL）。

表9-2显示了标准URL地址的组成部分（本例中，URL为http://www.cisco.com/edu/）。

表9-2　URL的组成

http://	www.	Cisco.com	/edu/
确定浏览器所使用的协议	确定浏览器相连接的站点类型	表示Web站点的域名	确定服务器中Web页面所在的文件夹。因为没有指定文件名，所以调用该服务器中的缺省页面

当打开Web浏览器时，通常会看到起始页面（或者称为主页）。这是因为起始页面的URL已经存储在Web浏览器的配置中了。可以随时修改此设置。在起始页面上，可以点击其中的超级链接或者在浏览器的地址栏中键入新的URL。Web浏览器将会检查协议以决定是否需要打开新的窗口，并且检查Web服务器的IP地址。随后，传输层、网络层、数据链路层和物理层会发起和Web服务器的会话。发往HTTP服务器的数据包含了Web页面所处的文件夹名称（该数据也会包含HTML页面的特定文件名）。如果没有给出文件名，服务器使用缺省名称（一般在服务器配置中指定）。

服务器响应请求，并按照HTML中的指令，把所有的文本、音频、视频和图像文件发送到客户端。客户端浏览器重组所有的文件以建立一个Web页面，并终止会话过程。如果点击位于同一台服务器上或者其他服务器上的不同页面，整个过程将重新开始。

9.3.5　SMTP

E-mail服务器之间通过简单邮件传输协议（SMTP）进行通信来收发电子邮件。SMTP协议把e-mail信息转换成ASCII格式，通过TCP传送。你可以通过ping SMTP端口（25）连接SMTP服务器。这也是一种测试邮件服务器是否可达的方法。

当邮件服务器接收到发往本地客户端的消息，就把这些消息存储下来，等待客户端取走邮件。邮件客户端可以通过几种方式取走邮件：通过程序直接访问邮件服务器上的文件或者通过一些网络协议。最流行的邮件客户端协议是：邮局协议版本3（POP3）和消息访问协议版本4（IMAP4），这两个协议都通过TCP传送数据。即使邮件客户端通过这些特殊的协议获取邮件，也必须通过SMTP发送邮件。因为发送和接收邮件要涉及到两个不同的协议，或者是两台不同的服务器，所以邮件客户端有可能只能完成一个任务。因此，应该分别去调试解决发送和接收邮件的问题。

当检查邮件客户端的配置时，邮件转发服务器（SMTP）和邮件服务器（POP3或者IMAP）都需要进行验证。SMTP不能提供多少安全方面的功能，并且不需要进行认证。为了防止未授权用户探测邮件服务器，网络管理员一般不允许本网络之外的主机通过SMTP服务器发送（或中继）邮件。

9.3.6　SNMP

*简单网络管理协议（SNMP）*是应用层协议，在网络设备之间实施管理信息的交换。SNMP使得网络管理员可以管理网络的性能，查找和解决网络问题，以及规划网络的增长。

SNMP管理的网络包含以下三个组件：

• **被管理设备**——包含SNMP代理的网络节点，位于被管理网络。被管理设备收集和存储管理信息，通过SNMP使这些协议能够访问网络管理系统（NMS）。被管理设备，有时称为网络基本设备，

它们可能是路由器和访问服务器，交换机和网桥，集线器，计算机主机，或者打印机。

• **代理**（Agent）——存在于被管理设备上的网络管理软件模块。代理有本地管理信息的认知，能把这些信息转换成兼容于SNMP的格式。

• **网络管理系统**（NMS）——监测和控制被管理设备的执行应用软件。NMS提供网络管理所需要的处理和内存资源。在管理网络中，至少有一个或一个以上的NMS。

9.3.7 Telnet

终端仿真（*Telnet*）软件提供远程访问其他计算机的能力。这个功能允许登录到Internet主机并执行命令。Telnet一般用于远程地管理服务器或者网络设备（比如路由器和交换机）。Telnet客户端一般称为本地主机，而Telnet服务器（运行特定的软件，称为后台程序）一般称为远程主机，如图9-14所示。

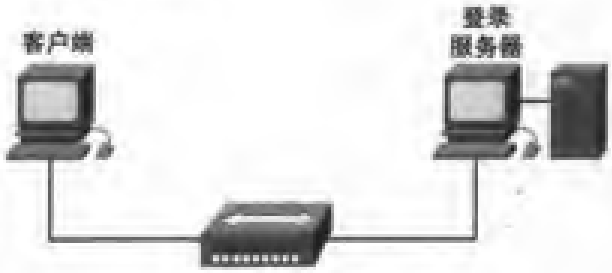


图9-14 telnet

从Telnet客户端发起连接，必须选择连接参数。需要在命令行提示符下输入主机名和终端类型。主机名是指希望连接的远程计算机的IP地址（DNS）。终端类型是指希望计算机执行的终端模拟类型。使用Telnet不需要占用计算机的处理资源，仅仅传送按键信息到远程主机，并把输出结果发送到本地监视器。所有的处理和存储过程都在远程计算机上进行。

如果输入DNS名称来定位Telnet，那么在建立连接以前，域名必需转换成为相应的IP地址。Telnet应用主要工作在OSI模型的顶3层，分别为应用层（命令）、表示层（格式，通常为ASCII）和会话层（传输）。然后，将数据发送给传输层，在传输层分段，加入端口地址和错误校验信息。数据随后传送到网络层，添加IP头（包含源和目的地址）。接下来，分组穿过数据链路层，将分组封装成数据帧，加上源和目的MAC地址，再加上一个帧尾。如果源主机没有目标主机的MAC地址，则执行ARP请求。确定了目的MAC地址之后，数据帧通过物理介质（以二进制格式）传送到下一台设备。Telnet是很好的网络调试工具，因为它能测试全部7层，而且允许实现远程故障诊断。

当数据到达远程主机，经过数据链路层、网络层，在传输层将数据分段重组为原始数据命令。远程主机执行这些命令，并使用同样的封装过程将结果传回到本地客户机。整个过程不断地重复，发送命令和接收执行结果，直到本地客户端完成所有的工作。当工作完成后，客户端终止会话。

9.4 总结

本章中，我们学习了关于TCP/IP应用层和传输层的功能。也学习了当数据分组传送到这两层时发生的不同过程。更具体地说，了解到应用层负责如下功能：

- 为预定的通信双方确认和建立通信。
- 同步协同工作的应用程序。
- 为错误恢复过程建立协商。
- 控制数据的完整性。

此外，了解了应用层支持如下应用：

- 直接和间接的网络应用。
- 域名系统。
- Telnet、FTP和HTTP。
- TCP、UDP、SMTP和SNMP。

为了补充本章所学的内容，可参考本章的视频、缩略图和e-Lab实验活动，这些都可以在随书的CD-ROM中找到。

9.5　关键术语

确认（*acknowledgment*）　确认是从一台网络设备发往另一台网络设备的通知，用来确认某个事件的发生（比如，一条消息的接收）。有时缩写为ACK。

应用（*Application*）　应用是直接为用户实现某些功能的程序。FTP和Telnet客户端就是应用的实例。

应用层（*application layer*）　应用层是OSI参考模型的第7层。该层向应用进程（比如电子邮件、文件传输以及终端仿真）提供超出OSI模型范畴的服务。应用层识别和建立预定通信方（以及它们所需要的资源）的可用性，同步协同工作的应用以及建立错误恢复过程的协商定和控制数据完整性。

美国信息交换标准码（*ASCII*）　美国信息交换标准码是用于表示字符的8bit编码（7bit再加上校验比特）。

域名系统（*DNS*）　域名系统是在Internet中把网络节点的名称转换成地址的系统。

流控制（*flow control*）　流控制用于确保传输设备（如调制解调器）发送数据的速率不超过接收设备的处理能力的技术。当接收设备的缓存用尽时，接收设备会向发送设备发出要求暂缓发送数据的消息，直到缓存中的数据处理完之后再继续发送。在IBM的网络中，这种技术称为调速。

文件传输协议（*FTP*）　文件传输协议是用于在网络节点之间传输文件的应用协议，是TCP／IP协议栈的一部分。FTP在RFC 959中进行了定义。

超文本标记语言（*HTML*）　超文本Web标记语言是一种简单的超文本文档格式化的语言，它使用标记来告诉浏览应用程序（如Web浏览器）如何解释文档中的特定部分。

超文本传输协议（*HTTP*）　超文本传输协议是Web浏览器和Web服务器之间用来传输文件（比如文本和图形文件）的协议。

端口（*Port*）　在IP术语中，从低层接收信息的的上层进程。端口进行了编号，每个端口号都与特定的进程相关联。例如，SMTP与端口25关联。这种类型的端口号也称为知名端口或地址。

传输控制协议（*TCP*）　传输控制协议是面向连接的传输层协议，能提供可靠的全双工数据传输。TCP是TCP／IP协议栈的一部分。

远程登录（*Telnet*）　远程登录是TCP／IP协议栈中的标准终端仿真协议。Telnet用于远程终端连接，使用户能登录到远程系统并使用远程资源（就像这些资源连接到本地一样）。Telnet在RFC 854中定义。

简易文件传输协议（*TFTP*）　TFTP是FTP的简化版，允许文件从一台计算机通过网络传送到另一台计算机。

三次握手（*Three-way handshake*）　三次握手是指在连接建立过程中两个协议实体进行同步的过程。

用户数据报协议（*UDP*）　UDP是TCP／IP协议栈中的无连接传输层协议。UDP是一种无需确认或者传输保证的简单协议，需要由其他协议来完成错误处理和重传。UDP在RFC 768中定义。

窗口（*Windowing*）　一种流控机制，源设备发送一定的数据量之后，要求目的设备给予确认。

9.5 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 当你和母语不同的人交谈时，也许需要重复你所说的话并且放慢讲话速度。重复谈话可以比喻成传输层 _____ 功能，放慢说话的速度可以比喻成传输层 _____ 功能。

A. 可靠性；流控

B. 流控；可靠性

C. 传输；确认

D. 流控；传输

2. 以下特点描述了哪种TCP／IP协议：面向连接；重传任何没有接收到的数据；将向外发送的消息分成数据分段。

A. IPX

B. TCP

C. UDP

D. SPS

3. TCP数据分段中的窗口字段表示什么含义？

A. 报头中32bit字的数量

B. 被叫方的端口号

C. 确保数据能按正确顺序接收的序号

D. 接收设备期望接收的8位字节的数量

4. 哪种传输协议交换数据报，不需要确认和传送保证机制？

A. UDP

B. TCP

C. IRQ

D. LLC

5. TCP和UDP使用什么在同一时间对网络的不同会话进行跟踪？

A. 端口号

B. IP地址

C. MAC地址

D. 路由号

6. 开始传输数据前，TCP如何对源设备和目的设备之间的连接进行同步？

A. 两方握手

B. 三次握手

C. 四方握手

D. Holton功能

7. 哪个范围的端口号没有进行规定？

A. 255以下

B. 256到512之间

C. 256到1023之间

D. 1023以上

8. 在TCP传输过程中，如果某个数据分段发送之后在一定时间内没有接收到确认信息，会发生什么情况？

A. 由UDP取代这次传输

B. 终止虚电路的连接
C. 什么都没有发生
D. 开始重传

9. 下面哪个选项最佳描述了流控?
A. 管理有限带宽的方法
B. 同步连接两台计算机的方法
C. 防止缓冲溢出的方法
D. 在传输之前对数据进行病毒检查的方法

10. 下面哪个选项最佳描述了TCP / IP协议栈的功能?
A. 与OSI模型的高层紧密对应
B. 支持所有标准的物理层和数据链路层协议
C. 按照数据报的序号把消息从一台主机传送到另一台主机
D. 在接收方把数据报重组为完整的消息

11. 下面哪个协议是传输层协议?
A. UCP
B. UDP
C. TDP
D. TDC

12. 端口号的作用是什么?
A. 跟踪在同一时间通过网络的不同上层会话
B. 源系统使用它们来使会话具有组织性
C. 根据应用层的用途，为终端用户动态分配一个特定的会话过程
D. 源系统生成端口号对目的地址进行预测

13. 为什么要使用TCP三次握手 / 开放连接? 选择所有可能的选项。
A. 如果以后传输中有错误出现，可以恢复丢失的数据
B. 决定接收设备每次能够接收多少数据
C. 为用户提供有效的利用带宽
D. 把二进制的ping响应转化为上层信息

14. 动态TCP窗口字段的功能是什么?
A. 可使窗口变得更大，每次传送的数据更多，从面更有效地利用带宽
B. 窗口随着数据报的每个部分面滑动，以接收数据，从而更有效的利用带宽
C. 在TCP会话中允许动态协商窗口大小，从而更有效地利用带宽
D. 限制入站数据，使得数据分段一个一个发送，使得带宽的利用效率较低

15. UDP数据分段利用什么协议提供可靠性?
A. 网络层协议
B. 应用层协议
C. Internet层协议
D. 传送控制协议

16. 网络重定向器使得数据传送到 _____ ?
A. 只能传送到一台网络打印服务器
B. 只能传送到一台网络文件服务器
C. 只能以单方向传送
D. 以上都不是

17. 客户端/服务器应用程序的实例是?
A. 电子邮件
B. 电子制表软件
C. NIC
D. 硬件驱动工具
18. 在客户端/服务器应用中，客户端的角色是?
A. 位于远程计算机上
B. 服务请求者
C. 最重要
D. 总是位于服务器上
19. 以下哪个选项最佳描述了域名?
A. 代表Internet站点的数字地址
B. 和主服务器的名称相同
C. 代表你所在局域网中的特定地点
D. 代表一台打印服务器的IP地址
20. .COM域名通常分配给 _____ ?
A. 客户端主机
B. 客户
C. 网络服务提供商
D. 公司
21. 在一个Telnet连接过程中，远程主机负责什么?
A. 不负责任何事
B. 处理工作
C. 客户端Telnet应用
D. 客户端打印工作
22. Telnet主要工作在OSI参考模型的哪3层?
A. 应用层、会话层、传输层
B. 表示层、会话层、传输层
C. 数据链路层、传输层、表示层
D. 应用层、表示层、会话层
23. 一般来说，匿名FTP会话使用 _____ 作为登录ID，使用 _____ 作为密码?
A. Anonymous；用户E-mail地址
B. 用户E-mail地址；FTP
C. FTP；FTP
D. Guest（客人）；Anonymous
24. 重定向器不和特定应用程序协同工作，那它和什么协同工作?
A. 计算机操作系统
B. 电子制表软件
C. 电子邮件
D. Web浏览器

第二部分　路由器和路由选择基础

第10章　广域网和路由器
第11章　路由器基础
第12章　路由器配置
第13章　邻居和远程设备的学习
第14章　管理Cisco IOS软件
第15章　路由选择和路由选择协议
第16章　距离矢量路由选择协议
第17章　TCP/IP差错消息和控制消息
第18章　基本路由器故障处理
第19章　深入理解TCP
第20章　访问控制列表



第10章 广域网和路由器

目标

学完本章之后，你应该能够：

- 识别广域网连接的类型，封装和协议。
- 了解广域网和局域网的差别以及各自使用的地址类型。

本章中，你将了解各种广域网设备、技术和标准。此外，你还将学习路由器在广域网中的功能。

请务必看看关于本章的e-Lab实验、视频和插图，这些内容可以在本书所附的光盘中找到。光盘中的这些内容用作补充材料，能强化本章中所介绍的概念。

10.1 广域网的特征

*广域网（wide-area network, WAN）*是跨越一个很大地理区域的数据通信网络。广域网通常使用电信公司，例如电话公司，所提供的传输设施。

广域网（WAN）与局域网（LAN）在很多方面存在差别。例如，与局域网连接一座楼内或其他小区域内的多台工作站、外设、终端和其他设备不同，广域网提供跨越广大地理区域的数据连接。公司通常用广域网来连接各个办公地点，以便信息能在各个远程办公室之间进行交换。

广域网运行在OSI参考模型的物理层（第1层）和数据链路层（第2层）。它负责将地理上相隔很远的多个局域网连接起来。广域网能提供*路由器/交换机*以及它们所支持的局域网之间的分组/帧交换。

表10-1列出了一些表示多个数据网络实例特征的关键信息。

表10-1 各种数据网络

名称	主机的位置	设备间的距离
教室内的局域网	屋内	10m
学院内的局域网	楼内	100m
大学内的局域网	校园内	1000m = 1km
思科系统公司的广域网	国内	100,000m = 100km
非洲的广域网	洲内	1,000,000m = 1000km
Internet的广域网	地球内	10,000,000m = 10,000km
地球和人造卫星之间的广域网	地-月系统内	100,000,000m = 100,000km

如图10-1所示，广域网的主要特征如下：

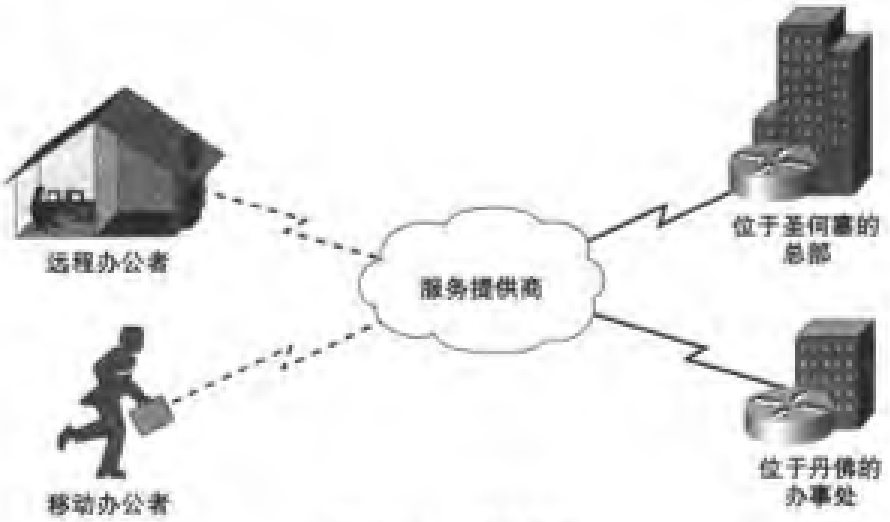


图10-1　广域网连接

- 连接地理上相隔很远的设备。
- 使用电信公司的服务，例如各个地区性贝尔运营公司（RBOC）、Sprint 和MCI。
- 使用各种类型的串行连接来接入广泛地理领域内的带宽。
- 连接分布在广泛地理领域内的设备。

更多信息：广域网的性能指标

部件的正常运行时间（Component Uptime）

广域网所有部件的可用性都可以用“正常运行时间（uptime）”来监视和测量。“正常运行时间”与“故障时间（downtime）”相对，指的是根据用户对可用性的需要，设备正常工作或提供服务的时间。通常对于“正常运行时间”会被夸大到7×24级，即使用户的需求可能只是5×12。正确的做法是把这一参数和其他的参数调整到与用户对网络性能的要求尽可能接近的程度。

尽管电子设备的可靠性很高，最后还是会出现故障。大多数制造商提供设备的平均无故障时间（MTBF）等级来作为其产品实际可靠性的保证。通常MTBF等级是以数万小时计的。也就是说可以很多年无故障地提供服务。不幸的是，这些等级都是通过统计获得的。实际上，无故障时间取决于很多因素，包括：

- 设备运行环境的温度变化范围。
- 商用电能的洁净程度。
- 这些设备在运转前和运转中的操作情况。

检测和记录单个组件的正常运行时间使得你能向你的客户表明，你充分地满足了他们对于网络可用性的需求。关于组件可用性的数据可以制成图表，以便确定网络基础设施中潜在的值得怀疑的组件。这些趋势可以提供关于某个特定的类型和品牌硬件可靠性的一般情况，以后就可以用来识别容易产生故障的单个组件。

注意术语“可用性”有时用来描述网络合计的正常运行时间。不幸的是，这并不是一个好的度量值。理论上，网络的“可用性”提供了关于网络状态良好程度的量化的总体指标。实际上，“可用性”的概念是十分模糊的，以至于基本上没有意义。

举例说明，如果用户端的路由器出现故障，对于这个位置的用户而言，整个网络都是不可用的。然而，网络对于其他位置的用户而言是可用的。其他位置的用户虽然不能访问受影响位置的主机，但对网络上其他主机的访问却不受影响。网络可用的程度随着位置的不同和用户需

求的不同而有很大的变化。因此，量化网络可用性所付出的代价可能超出这个指标的价值。

通信量（Traffic Volumes）

所希望支持的通信量对任何广域网来讲都是重要的指标。通信量总是不断变化的，随时间、商业周期、季节等因素变化。换句话说，你不可能奢希望于通信量保持不变。考虑到通信量的易变性，需要用两种方式衡量通信容量，最大通信量和平均通信量：

- 你希望网络传输支持的*最大通信量（maximum volume）*被称为*峰值通信量（peak volume）*。顾名思义，这是你希望网络支持通信量的上限。
- *平均通信量（average volume）*是你所预计的任何工作地点在工作日的正常通信量。

这两个通信量的概念对于选择广域网传输设施和路由器是至关重要的。如果你预计任何工作地点在工作日的正常通信量是100kbit/s，很显然56kbit/s的传输设施是不够的。

延迟（Delay）

延迟是用来衡量网络性能的一个常见的指标。延迟是两件事情之间所经过的时间。在数据通信中，这两件事情通常是数据的发送和接收。因此，延迟是网络将一个分组从源送到目的总共所需要的时间。根据这个定义，延迟是由很多可能因素产生的一个聚集现象。下列是三个常见的原因：

- **传播延迟**——传播延迟（propagation delay）是数据经过一条端到端的传输路径时所需的总的传输时间。数据所经过路径上的网络基础设施会对传输延迟产生直接的影响。另一个影响传播延迟的因素是通信量。当前经过某一设施的通信量越大，供新的传输使用的带宽就越少。无论是通过玻璃介质、铜介质还是使用微波以空气为介质，传播延迟都是不可避免的。
- **人造卫星上行/下行延迟**——某些传输设施是基于人造卫星的。这需要先将信号向上传递给人造卫星，然后由它向下传递。由于发送接收设备距离卫星的距离很远，产生的延迟可能很大。
- **转发延迟**——转发延迟（forwarding delay）是物理设备接收、缓存、处理和转发数据所需的时间。某个物理设备的转发延迟可能会随时间变化。接近处理能力上限的设备的转发延迟会比轻负载设备的转发延迟大得多。此外，网络中较高的通信量和出错的情况也会使转发延迟进一步恶化。对于单个邮件，转发延迟也可以称作等待时间（latency）。

10.1.1 广域网设备

下列设备用在广域网中，如图10-2所示：

- **路由器（Routers）**——提供多种服务，包括局域网互连和各种广域网接口。
- **交换机（Switches）**——连接到广域网带宽上，进行语音、数据、视频通信。
- ***调制解调器（Modems）***——包括针对各种话音级业务（模拟拨号调制解调器）的不同接口；信道服务单元/数字服务单元（CSU/DSU）是T1/E1业务的接口，终端适配器/网络终结器1（TA/NT1）是综合业务数字网（ISDN）业务的接口。
- **通信服务器（Communication server）**——汇集拨入和拨出的用户通信。

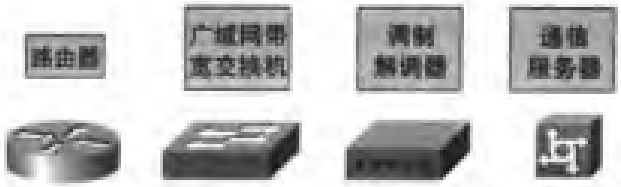


图10-2 常见的广域网设备

10.1.2 广域网标准

广域网的数据链路层协议描述了在系统之间的单一链路上，数据帧是如何传送的。包括针对点到点、多点和多路访问交换服务（比如帧中继）所设计的协议。广域网的标准由下列的权威机构制

定和管理：

- 国际电信联盟-电信标准部门（ITU-T），即以前的国际电话与电报委员会（CCITT）。
- 国际标准化组织（ISO）。
- Internet工程任务组（IETF）。
- 电子工业联合会（EIA）。
- 电子电气工程师协会（IEEE）。

广域网物理层描述了*数据终端设备*（DTE）和*数据通信设备*（DCE）之间的接口。通常，DCE是服务提供商的设备，在网络中用于提供时钟和交换服务；DTE是所连接的用户设备。在这个模型中，各种服务通过调制解调器、信道服务单元/数据服务单元（CSU/DSU）提供给DTE（见图10-3）。

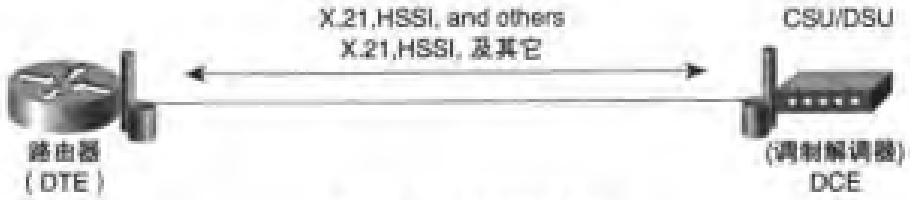


图10-3　广域网服务

为了确保使用恰当的协议，你必须在路由器上配置适当的第2层封装。协议的选择需要根据所采用的广域网技术和通信设备确定。

广域网的物理层协议描述了如何为广域网服务提供电子的、机械的、操作上的以及功能上的连接。这些服务通常由广域网服务提供商提供，比如RBOC，或者同类的电信公司，以及邮电管理局（PTT）等机构。

规定了下列的物理层标准：

- EIA/TIA-232——常用的物理层接口标准，用于支持信号速率小于64kbit/s非平衡的电路。非常接近V.24规范。
- EIA/TIA-449——速度更高（最高可达2Mbit/s）版本的EIA/TIA-232，支持更长的线缆距离。
- V.24——DTE和DCE之间的物理层接口。在本质上，V.24与EIA/TIA-232是相同的。
- V.35——同步的物理层协议，用于网络接入设备和分组网络之间的通信。V.35在美国和欧洲最为常见，推荐的速率最高可达48kbit/s。
- X.21——针对同步数字线路上串行通信的协议。X.21协议主要用于欧洲和日本。
- G.703——针对电话公司设备和DTE之间连接的ITU-T的电子和机械规范。这些PTE采用BNC接头，工作在E1速率。
- EIA-530——涉及EIA/TIA-449的两个电子实现：RS-422（针对平衡的传输）和RS-423（针对非平衡的传输）。

同步串行线路中封装了多条数据链路，这些数据链路的特征如表10-2所列。

表10-2　同步串行数据链路的各种封装

封装	特征
高级数据链路控制（HDLC）	IEEE的一项标准。 点到点专用链路和电路交换连接的缺省封装。 Cisco HDLC是一个专用版本的、面向比特的、同步的数据链路层协议，通常用于两台Cisco设备之间的通信。 由于不同厂商选择的实现方式不同，Cisco HDLC可能与其他厂商版的不兼容。 既支持点到点配置，也支持多点配置，开销最小

续表

封装	特征
帧中继（Frame Relay）	使用高质量的数字设备。 采用简化的成帧技术，没有纠错机制。这意味着它能比其他广域网协议更快地传送第2层的信息。 能处理多条虚电路的业界标准交互型数据链路层协议。 作为X.25的下一代，帧中继通过精简去除了X.25中实现的一些耗时的处理过程，比如错误纠正和流控制
点到点协议（PPP）	在RFC 1661中描述。 IETF开发的两项标准。 包含一个“协议”字段，用于标识网络层协议。 提供同步或异步电路上的路由器到路由器和主机到网络的连接。 设计用于与多种网络协议一同工作，比如Internet协议（Internet Protocol, IP）和网间分组交换（Internetwork Packet Exchange, IPX）。 内置安全机制，例如口令验证协议（Password Authentication Protocol, PAP）和挑战握手验证协议（Challenge Handshake Authentication Protocol, CHAP）
同步数据链路控制（SDLC）协议	由IBM设计的广域网数据链路层协议，用于系统网络结构（SNA）环境。 大多已经被用途更多的HDLC协议所替代
串行线路Internet协议（SLIP）	曾经很流行的传送IP分组的广域网数据链路协议。 在很多应用中已经被用途更多的PPP所取代。 针对使用TCP/IP的点到点串行连接的标准协议
平衡型链路访问规程（LAPB）	供X.25使用。 有广泛的错误检查能力
D信道链路访问规程（LAPD）	用于ISDN D信道上的信令和呼叫建立的协议
帧方式链路访问规程（LAPF）	用于各种帧模式的承载业务。 类似于LAPD，与帧中继技术一起使用
X.25/平衡型链路访问规程（LAPB）	ITU-T的一项标准，定义了在公众数据网络中，DTE与DCE之间用于远程终端接入和计算机通信的连接是如何维持的。 规定了LAPB，一种数据链路层协议。 帧中继的前辈

图10-4图解了与同步串行线路相关的一些常用的数据链路封装。

图10-5图解了同步串行通信的模型，其中提供给路由器的服务是通过一个调制解调器或者CSU/DSU实现的。

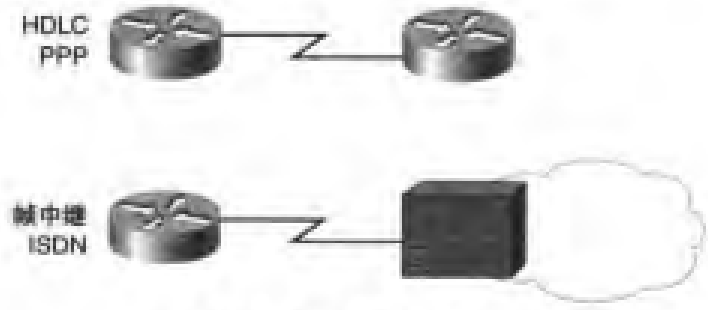


图10-4 数据链路封装

10.1.3 广域网连接的各种选择

你可以使用各种不同的广域网连接选择来互联局域网。下列几小节简要描述了最常用的广域网连接服务：

- 电路交换服务。
- 分组交换服务。
- 信源交换服务。
- 专用数字服务。
- 拨号、电缆和无线服务。

图10-6描述了各种WAN连接服务

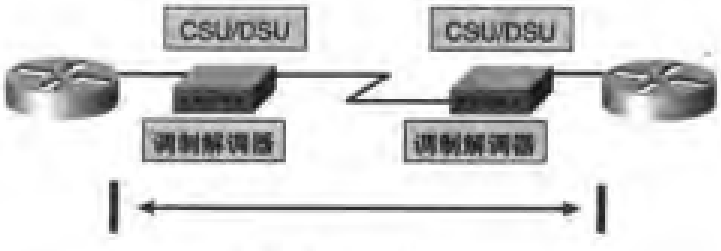


图10-5 CSU/DSU

电路交换服务

*电路交换服务（Circuit-switched services）*是一种广域网交换方式，在电信公司的网络中为每个通信会话建立、保持和终止一条专用物理电路。ISDN是电路交换广域网技术的一个例子。图10-7图解了支持电路交换的网络拓扑结构。

表10-3描述了两种最常用的电路交换服务各自的特征——旧式电话服务（plain old telephone service, POTS）和窄带综合业务数字网（narrowband ISDN）

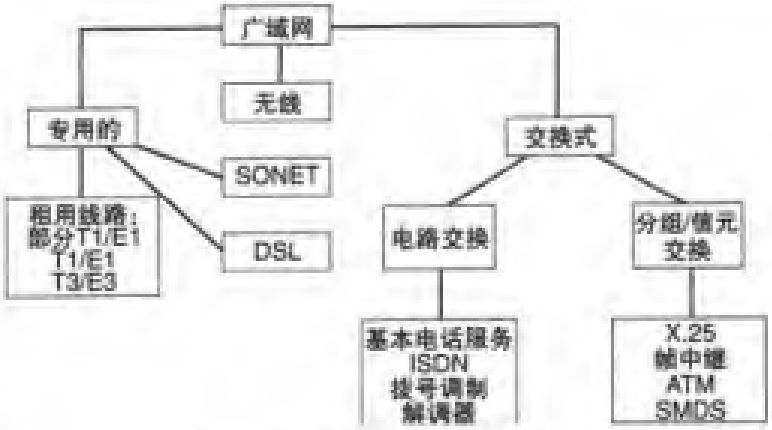


图10-6　各种广域网连接服务

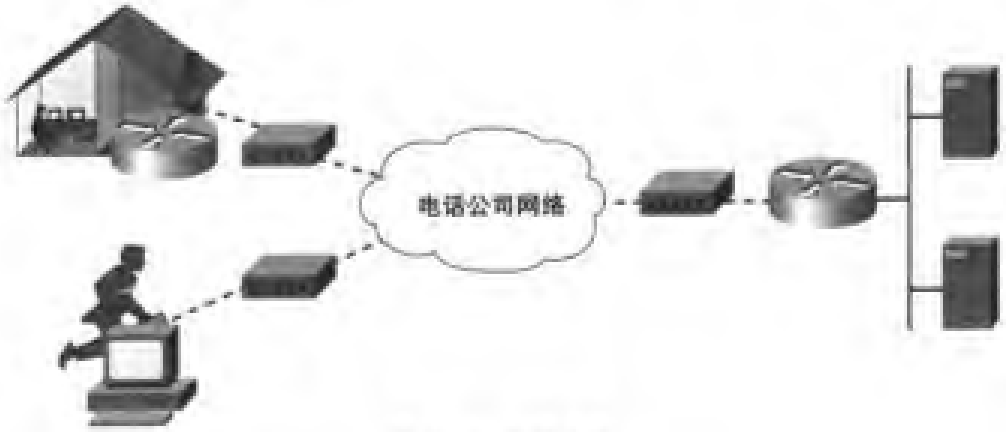


图10-7　电路交换

表10-3　电路交换服务

电路交换服务	特征
POTS	不是计算机数据业务，将它包括在此是因为：它的许多技术是不断发展的数据基础设施的一部分；它是一种可靠、易用的广域通信网络。 典型介质是双绞铜线
窄带 ISDN	一种通用的、普通的、曾经十分重要的技术。 是第一个全数字化的拨号服务。 费用中等。 对于费用较低的基本速率接口（BRI）带宽是128kbit/s，对基群速率接口（PRI）带宽是3 Mbit/s。 应用十分广泛，尽管这项技术在不同国家之间的差别很大。 典型介质为双绞铜线

POTS和ISDN都是拨号服务，这意味着在进行呼叫时，建立了端到端的物理路径并预留了带宽。POTS和ISDN都使用直接的时分多路复用（TDM），有时也称作同步传输模式（STM）。

分组交换服务

*分组交换服务（Packet-switched services）*在网络中对被称为分组（packet）的小数据单元进行路由，所依据的是每个分组内所包含的目的地址。图10-8显示了一个支持分组交换服务的网络拓扑结构示例。

表10-4描述了两种最常用的分组交换服务各自的特征——X.25和帧中继。

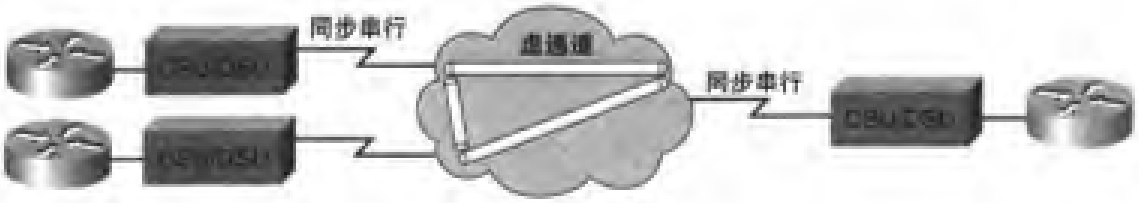


图10-8 分组交换

表10-4 分组交换服务

分组交换服务	特征
X.25	比较旧的一项技术，仍然广泛使用。 因为当时的广域网链路很容易产生错误，所以X.25具有广泛的检错能力，这使得它很可靠，但是却限制了带宽。 带宽最高可达2 Mbit/s。 应用相当广泛。 费用中等。 典型介质为双绞铜线
帧中继	一种分组交换版的窄带ISDN。 已经成为一项非常流行的广域网技术。 效率比X.25高，但提供的服务类似。 其最大带宽为44.736Mbit/s。 在美国，56kbit/s 和 384kbit/s 非常流行。 应用广泛。 费用中等偏低。 典型介质包括双绞铜线和光纤

X.25在第2层和第3层都是面向连接和可靠的，这是其速率远低于帧中继的原因。

通常认为帧中继作为X.25 的改进版本，速度快得多。帧中继没有规定第3层协议，也是不可靠的。但是，帧中继是面向连接的。

电路交换业务使用时分复用（TDM），并且被称为同步的（使用同步传输模式（STM）），分组交换使用统计时分复用（statistical TDM ）并且有时被称为异步的（类似于ATM）。

信元交换服务

信元交换服务（Cell-switched services）提供了一种专用连接交换技术，将数字化的数据组织成信元单元，然后用数字信号技术将其在物理介质上传输。

表10-5描述了两种最常用的分组交换服务各自的特征——异步传输模式（Asychronous Transfer Mode, ATM）和交换式多兆比特数据服务（Switched Multimegabit Data Service, SMDS）。

表10-5 信元交换服务

信元交换服务	特征
ATM	与宽带ISDN密切相关。 正在成为一项日益重要的广域网技术。 使用长度很短的定长信元（53字节）来传送数据。 最大带宽是622Mbit/s，支持更高速率的技术正在开发当中。 典型的传输介质包括双绞铜线和光纤。 应用广泛并在不断增长。 费用高
SMDS	与ATM密切相关，通常用在城域网（MAN）中。 最大带宽为44.736Mbit/s。

续表

信元交换服务	特征
	典型介质为双绞铜线和光纤。 应用不很广。 费用相对较高

专用数字化服务

*专用数字化服务（Dedicated digital services）*也提供了一种电路交换服务，不过连接是“始终保持的（always-up）”。

表10-6描述了最常用的专用数字化服务各自的特征——T1、T3、E1、E3；数字用户线（digital subscriber line, xDSL）；以及同步光纤网（Synchronous Optical Network, SONET）

表10-6　专用数字化服务

专用数字化服务	特征
T1、T3、E1、E3	美国采用的T系列和欧洲采用的E系列都是非常重要的广域网技术。 它们使用TDM技术为数据传输切片和分配时隙。 T系列和E系列线路的带宽为： T1 —— 1.544 Mbit/s T3 —— 44.736 Mbit/s E1 —— 2.048 Mbit/s E3 —— 34.368 Mbit/s 也有其他的带宽。 采用介质是双绞铜线和光纤 使用非常广泛。 价格中等
xDSL	一项新兴的、正在不断发展的针对家庭使用的广域网技术。 xDSL代表整个DSL技术家族，包括： 高数据速率DSL（high-bit-rate DSL, HDSL） 单线DSL（single-line DSL, SDSL） 非对称的DSL（asymmetric DSL, ADSL） 甚高速DSL（very-high-date-rate DSL, VDSL） 带宽随着与电信公司设备之间距离的增加而减少。 在离电信公司设备近的地方，可达到最高速率51.84 Mbit/s，大多数情况下带宽低得多（从几百kbit/s到几Mbit/s）。 费用中等而且正在下降
SONET	一系列高速的物理层技术。 设计是针对光纤的，但也可以运行在铜质电缆上。 有一系列的数据速率，每种速率都有专用的名称。 可以实现在不同等级的光纤载波（OC）上，从51.84Mbit/s（OC-1）到9952Mbit/s（OC-192）。 通过波分复用（wavelength division multiplexing, WDM）可以实现高数据速率。WDM就是通过将激光调节为稍微不同的颜色，或者说波长，从而实现用光传送非常大量数据的技术。 在互联网骨干上的使用非常广泛。 费用昂贵，这不是连接家庭的技术

拨号、电缆和无线服务

表10-7描述了不属于前面所讲的任何一类广域网技术的其他服务的特征。这些五花八门的技术包括拨号调制解调器（dialup modems），电缆调制解调器（cable modems），以及地面和人造卫星的

无线服务（terrestrial and satellite wireless）。

表10-7 拨号、电缆和无线服务

广域网服务	特征
拨号调制解调器 （交换式模拟技术）	速度有限但是很通用。 工作在现有的电话网上。 最大带宽约为56kbit/s。 费用低。 应用仍然很广泛。 典型介质为双绞电话线
电缆调制解调器 （共享式模拟技术）	将数据信号和电视信号放在同一条电缆上。 在那些已经布有大量有线电视同轴电缆的地区越来越流行。美国90%的家庭都使用有线电视。 最大带宽能达到10Mbit/s，但是带宽会随网段上用户的增加而减少。 与非交换式（共享式）局域网类似。 费用较低。 介质为同轴电缆
无线	不需要使用介质，因为所使用的信号是通过空气传播的电磁波。存在多种无线的广域网链路，包括： 地面无线的带宽通常在11Mbit/s左右（比如，微波）。费用较低、通常要求视距，使用程度适中。 人造卫星可以为处于蜂窝电话网络中的用户和位置偏远、距离任何线缆都很远的用户提供服务。 使用广泛。 费用高

图10-9图解了通过路由器连接的各种广域网技术。



图10-9 通过路由器连接的各种广域网技术

各种广域网技术的对比

表10-8列出了前面讨论过的各种广域网技术。

表10-8 各种广域网技术

广域网技术缩写	广域网技术名称	最大带宽	注解
POTS	旧式电话服务（plain old telephone service）	4 kHz 模拟带宽	一流的可靠性

续表

广域网技术缩写	广域网技术名称	最大带宽	注解
ISDN	综合业务数字网（Integrated Services Digital Network）	128Kbit/s	数据和语音一起
X.25	X.25	2Mbit/s	旧式的、可靠的、广泛应用的技术
Frame Relay	帧中继（Frame Relay）	最高可达44.736Mbit/s	新型的广泛应用技术
ATM	异步传输模式（Asynchronous Transfer Mode）	622Mbit/s	强力网络
SMDS	交换式多兆比特数据业务（Switched Multimegabit Data Service）	1.544Mbit/s 和 44.736Mbit/s	ATM的城域网变种
T1、T3	T1、T3	1.544Mbit/s 和 44.736Mbit/s	在电信中广泛使用
xDSL	数字用户线（digital subscriber line）	384kbit/s	电话线上的技术
SONET	同步光纤网（Synchronous Optical Network）	9,992Mbit/s	快速的光纤传输
拨号调制解调器（Dialup modem）	调制解调器（modem）	56kbit/s	使用电话线的成熟技术
电缆调制解调器（Cable modem）	电缆调制解调器（cable modem）	10Mbit/s	使用有线电视的技术
地面无线（Terrestrial wireless）	无线（wireless）	11Mbit/s	微波和激光链路
人造卫星无线（Satellite wireless）	无线（wireless）	2Mbit/s	微波和激光链路

更多信息：广域网的费用

制约性能的一个因素是费用。拥有和运行广域网的费用包括最初的启动费用和每个月的费用，自然，网络的规模越大，费用越昂贵。因此，广域网设计变成了一项经济上的行为，需要达到性能和费用之间的平衡。

但要达到这样的平衡是十分痛苦的。谁都不想设计一个性能上让用户失望的广域网，但谁也不想设计一个超出预算的广域网。下面这些原则能指导广域网的设计，使得所设计的网络既能满足用户的当前需求，又具备针对未来发展的灵活性，同时还不会超出预算：

- 在路由器和其他网络硬件上的投资是网络的固定费用。一旦硬件设备开始运行，要进行更换是非常麻烦的。同时，根据单位的固定资产折旧时间，你会发现这些设备不得不使用五年甚至更长的时间。随着对硬件性能需求的提升，将来你可以添加一些硬件，比如内存、CPU和接口，这使得将来扩展所新增的成本较低，而且停机时间很短，甚至可能没有。
- 更换传输设施相对容易，它们是耗材，不是固定资产，因此不存在折旧期的问题。只要你和电信公司之间达成了协议，就能更换传输设施。因此，为了使用视频会议，你可以有多种采用不同传输设施和技术的选择

更多信息：资源利用率

广域网各种物理资源的利用程度是衡量广域网运行好坏的重要指标。需要监测的两类资源利用率是：

- 路由器CPU和内存的利用率。
- 传输设施的利用率

路由器物理资源利用率

路由器是任何广域网的核心部件之一。和传输设施不同，路由器不归电信公司所有。因此，对路由器进行管理是完全用户的责任。幸运的是，路由器是非常智能的设备，配有CPU和内存。这些物理资源是广域网路由计算和转发分组所必备的，它们也可以用来监测路由器的性能。

如果CPU或内存的利用率接近百分之百，性能就会下降。很多情况都可能造成CPU或内存利用率短暂的急速上升，从而引起性能的下降。比如，从局域网到广域网传输数据量的突然增加。局域网的速度可以达到1Gbit/s，但通常工作在10、16、或100Mbit/s。但任何一种速率与广域网设施都是不匹配的，广域网的带宽通常只有1.544Mbit/s。这种不匹配必须通过路由器缓存来解决。但是，如果局域网持续传输大量的数据，路由器的资源很快就会不够用。

仅仅通过升级内存，是不能解决高CPU占用率的问题的。要解决这个问题，可行的方法只有三种：

- 如果可能，给路由器添加另一块CPU。
- 升级到处理能力更强的路由器。
- 对广域网通信模型进行分析，看看能否减轻路由器的负载。

改变通信模型实际上只适用于使用复杂技术并且能提供路由冗余的大型的广域网。

传输设施利用率

传输设施的利用率也可以检测，通常，传输设施的利用率都是用带宽占用百分比来表示的。如果你使用T1线路，当前的采样可能显示当前使用的带宽是可用带宽1.544Mbit/s的30%。

对利用率进行分析是很复杂的，甚至可能产生误导。比如，使用网管软件定期采集利用率是常见的做法。所选择的时间间隔可能是1小时，5分钟，或者其他。如果时间间隔太大，就不能反映带宽占用的短期波动。如果采样过于频繁，可能会获得大量无用的数据点。技巧就在于根据用户对网络性能了解的需要，选择适当的采样频率。

除了采样速率，还有采样窗口的问题。采样窗口应该根据用户对广域网可用性的要求确定。如果采样是每天24小时，每周7天进行，但用户每天只工作10小时，每周5天，统计数据就不能显示用户的需求是否得到了满足。

利用率是监控和测量传输设施状态的极好的统计工具，但并不是评价网络性能的惟一指标。只有满足用户需求的网络才是成功的。因此，采用多项性能指标的组合，从多方面综合地进行观察，才能对网络性能进行更好的评价。

10.2 广域网路由器

就像计算机需要操作系统来运行应用软件一样，路由器需要Cisco IOS 软件来运行配置文件。这些配置文件中包含控制进出路由器通信流的指令和参数。具体说来，利用路由选择协议来指引被路由协议和路由选择表，路由器会为分组选择最佳路径。配置文件中规定了路由器作出这些选择所需的全部信息。

10.2.1　路由器的内部配置部件

表10-9列出了路由器主要的内部配置部件。

表10-9　路由器主要的内部配置部件

内部部件	特征
随机访问存储器（RAM/DRAM）	存储路由选择表。 地址解析协议（ARP）高速缓存。 快速交换（fast-switching）高速缓存。 分组缓冲（共享RAM）。 分组保持（Packet-hold）队列。 在路由器通电后，负责提供临时的和运行的内存给路由器的配置文件。 重启或关闭路由器后，RAM中内容丢失
非易失性随机存取存储器（NVRAM）	存储路由器的备份/启动配置文件。 重启或关闭路由器后，内容仍旧保持
闪速存储器	可擦除，可编程的只读存储器（EPROM）。 存有操作系统映像和微代码。 允许对软件进行升级而不需替换处理器的芯片。 重启或关闭路由器后，内容仍旧保持。 在闪速存储器中存放多个版本的Cisco IOS软件
只读存储器（ROM）	存放加电自测试（POST）诊断所需的指令。 存放自举程序和操作系统软件。 ROM中的软件升级需要替换CPU中的可插拔芯片
接口	用于网络连接，分组通过接口进入和离开路由器。 可以位于主板上，也可以在一个单独的接口模块中

更多信息：路由器详解

路由器设计用于互联多个网络。这种互联使得不同网络上的机器能相互通信。所互联的网络在地理上可以是集中的也可以是分散的。地理上分散的网络通过广域网互联。广域网由许多不同的技术构成，包括路由器、传输设施和线路驱动。连接广域网中不同网络的功能使得路由器是不可或缺的。

路由器是智能的网络设备，主要工作在OSI参考模型的下三层。和主机一样，路由器实际上也可以运行在OSI参考模型的所有七层。根据特定配置，你可以使用七层所有的功能，也可以不使用。然而，下三层的功能几乎总是需要的。下两层的通信功能使得路由器能直接与局域网（数据链路层的概念）通信。更重要的是，路由器能通过第三层地址识别路由。这使得路由器能通过网络层寻址互联不同多个网络，无论它们之间的距离多近还是多远。

理解路由器和路由选择需要从两个不同的角度考察路由器：物理上和逻辑上。从物理角度看，路由器包含无数的组成部分，每一部分都有特定的功能。从逻辑角度看，路由器完成许多功能，包括发现网络中其他的路由器，学习关于潜在的目的网络和主机的信息，发现并记录潜在的路由，并将数据报转发到其特定的目的地。总之，这些物理部件和逻辑功能使得你能构建并使用互联网络，包括广域网。

路由器的物理部件

路由器是一种十分复杂的设备。其复杂性在于其路由选择引擎逻辑，它使得物理设备能完成各种不同的路由选择功能。路由器物理上的相对简单隐藏了路由选择逻辑的复杂性。最为常见的路由器实际上就是非常专用的计算机；它也包含与其他计算机相同的基本部件。这些部件包括：

- 中央处理单元（CPU）。
- 随机访问存储器（RAM）。
- 基本输入/输出系统（BIOS）。
- 操作系统（OS）。
- 主板。
- 物理输入/输出（I/O）端口。
- 电源、底板和金属机壳。

路由器的金属机壳隐藏了路由器的主要部件，使得网络管理员永远也看不见。这些部件极为可靠，在正常运行的情况下，是不需要见天日的，明显的例外是升级扩展。当你需要给路由器添加更多的资源时，你可能需要打开机箱。这些资源通常包括内存或I/O端口。

网络管理员经常打交道的部件是操作系统和I/O端口。路由器的操作系统（Cisco路由器的操作系统称为互联网络操作系统（IOS））是控制不同硬件并使之正常工作的软件。网路管理员通常使用命令行界面来生成路由器的逻辑配置。该配置是系统的简介：设备编号，位置，每个I/O端口的类型，有关地址和带宽的详细信息。路由器的配置也可以包括安全信息，比如哪些用户能访问特定端口和所能进入的配置模式

在日常管理中，网络管理员所看到的路由器物理组件是I/O端口。这些端口证实了路由器连接各种看起来无穷无尽的局域网和广域网传输技术组合的独特能力。每一个端口，不论是局域网还是广域网，在路由器上都必须有自己的I/O端口。这些端口的功能与连接局域网计算机的网卡（NIC）所起的作用一样；他们与所需的机制和成帧方式相关，并且提供适当的物理接口。许多物理接口看起来很相似。这种物理上的相似性掩饰了不同技术在上层功能上的差别。因此，分析传输技术比分析特定的物理接口更有用。

路由器的功能

路由器的逻辑功能与为多个网络提供物理上的连接同样重要。这些功能使得物理连接可用。比如，互联网通信要求至少存在一条连接源和目的机器的物理路径。然而，存在路径和使用路径是两件差别很大的事情。具体来说，源和目标机器必需使用一种共同的语言（一种*被路由协议*）。还需要途中的路由器也使用一种共同的语言（一种*路由选择协议*）并且都选择同一条物理路径作为最佳路由。

因此，路由器所提供的显著功能如下所示：

- 物理互连。
- 逻辑互连。
- 路由的计算和维护。
- 安全性。

物理互连

一台路由器至少（通常会多得多）有两个物理I/O端口。I/O端口，或者叫接口（interface），用于物理地连接网络传输设施。每个端口都连接到与路由器主板相连的电路板上。因此，实际上是主板提供了不同网络之间的相互连接。

网络管理员必须通过路由器的控制台对每个端口进行配置。配置包括定义路由器接口的编号，确定接口所连接网络中可用的传输技术和可用带宽，以及接口使用的协议类型。实际需要定义的参数随网络接口类型而变化。

注意，在高端平台上（7500和12000），接口（VIP2或线路卡）自身就能完成分组的转发功能而不需要中断主CPU。

逻辑互连

一旦对路由器接口进行了配置，就可以将其激活。接口的配置指明了它所连接的传输设施的类型、接口的IP地址和所连接网络的地址。接口一旦激活，路由器立刻开始监视与之相连的网络中传输的所有分组，这使得路由器能学习到通过该接口所能到达的网络和主机IP地址。这些地址存储在*路由选择表*（*routing tables*）中。路由选择表将路由器中每个接口的端口编号与通过该端口所能到达（直接或间接）的网络层地址相关联。

路由器上也可以配置*缺省路由*（*default route*）。缺省路由将某个路由器接口与所有未知的目的地址相关联。这种关联使得路由器能将目的地址未知的数据报转发到目的地。缺省路由在很多方面都是很有用的。比如，缺省路由可以用来将路由选择表的增长速度降到最低。它还能减少路由器之间为了交互路由选择信息所产生的通信量。

然而，在使用缺省路由时需要进行仔细的考虑，因为如果不全面地考虑通信流，缺省路由可能带来问题。

路由的计算和维护

路由器之间通过预先确定的协议进行相互通信，这种协议称为路由选择协议（routing protocol）。路由选择协议使得路由器能完成下列功能：

- 识别到达某个目的网络的可能路由。
- 根据路由选择协议的算法，进行数学计算，以确定到达每个目的地的最佳路径。
- 不断地对网络进行检测以发现可能造成已知路由不可用的拓扑结构改变。

存在许多不同类型的路由选择协议。有的十分简单，比如路由选择信息协议（RIP）。有的功能非常强大并且有很多特性，但很复杂。通常，路由选择协议可以使用两种方法进行路由选择：距离矢量和链路状态。距离矢量路由选择协议根据对源和目的之间路由的某种测量进行路由选择。链路状态路由选择协议根据链路，即连接源主机和目的主机的传输设施，的不同状态进行路由选择。这两种方法不存在对与错：他们只是不同的路由选择方式。然而，他们的性能是不同的，包括不同的收敛时间。

除了所使用的路由选择方式，你还可以用很多更加具体的标准来衡量路由选择协议。下列是一些有意义的标准：

- **最优性**（*Optimality*）——最优性描述了路由选择协议从所有可能的路由中选择最优的能力。不幸的是，“最优（best）”这个词的含义很含糊。有多种方法可以用来评估到达特定目的地的不同路由。每种方法都可能根据所使用的标准选择一条不同的“最优”路由。路由选择协议用于计算和评估路由的标准称为*路由选择度量标准*（*routing metrics*）。有多种度量标准，不同路由选择协议所采用的度量标准差别很大。最为简单的度量标准是*跳数*（*hop count*），即源主机和目的主机之间所经过的跳或路由器的数目

- **效率**（*Efficiency*）——评价路由选择协议时需要考虑的另一个标准是运行效率。运行效率可以通过考察路由选择协议所需的物理资源（包括路由器的RAM和CPU时间）和网络带宽来衡量。你可能需要咨询路由器制造商或销售商，以确定各种路由选择协议的相对效率。

- **健壮性**（*Robustness*）——路由选择协议应该总是处于可靠工作状态，而不仅仅是当网络处于稳定状态时。出错的情况，包括硬件和传输设施故障，路由器配置错误，甚至是通信负载过重，都会对网络产生影响。因此，路由选择协议在网络出现故障或不稳定的情况下仍然正常工作是十分关键的。

- **收敛**（*Convergence*）——因为路由器是智能设备，所以能自动地检测到互联网络中发生的变化。当检测到变化时，变化涉及的所有路由器都必须收敛在一个新的对于网络拓扑结构的

一致认识上，并相应地重新计算到已知目的地的路由。这个达到相互一致的过程称为收敛（*convergence*）。每种路由选择协议都用不同的机制检测和传递有关网络变化的信息。因此，每种路由协议收敛的速度都是不同的。通常，路由选择协议的收敛速度越慢，造成整个网络服务中断的可能性就越大。

- **可扩展性**（*Scalability*）——网络的可扩展性就是其增长的能力。尽管增长不是每个组织都需要，但路由协议的选择应该能向上兼容以适应网络的增长计划。

10.2.2 路由器的外部连接

路由器上的三种基本的连接类型为局域网接口、广域网接口和管理端口，如图10-10所示。局域网端口使得路由器能连接局域网介质，通常是某种类型的以太网。然而，也可以是某些其他的局域网技术，例如令牌环或ATM。

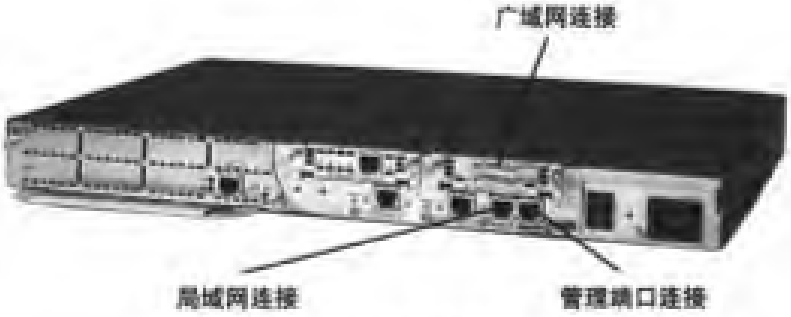


图10-10 路由器的外部连接

广域网连接提供了通过某个服务提供商到达一个远端地点或接入Internet的连接。这些连接可以是串行连接或者任何其他的广域网接口。对某些类型的广域网接口，需要一个外部设备，比如CSU，来将路由器连到服务提供商的本地连接上。对某些其他类型的广域网连接，路由器可能直接连接到服务提供商。

管理端口的功能与其他的各种连接不同。局域网和广域网连接所提供的是帧分组传递所需经过的网络连接。管理端口提供了一个基于文本的连接，用于完成路由器的配置和故障排除。常用的管理接口是控制台端口（console port）和辅助端口（auxiliary port）。这些都是EIA-232异步串行端口。它们都连接到计算机的通信端口上。计算机需要运行一个终端模拟程序来提供与路由器之间基于文本的会话。通过这个会话，网络管理员就可以管理该设备。

10.2.3 管理端口连接

控制台端口和辅助（AUX）端口都是管理端口。这些异步串行端口不是设计用作网络连接端口的。完成路由器的初始配置时，需要这两个端口之一。进行初始配置时，推荐使用控制台端口。不是所有的路由器都有辅助端口。

当路由器首次投入使用时，没有配置任何的网络连接参数。因此，路由器不能与任何的网络进行通信。为了准备初始的启动和配置，需要连接一个RS-232 ASCII终端或者一个计算机模拟的ASCII终端到系统控制台端口。然后，你就可以输入配置命令来配置路由器。

一旦通过控制台端口或者辅助端口为路由器输入了初始配置，接下来你就可以将路由器连接到网络中进行故障排除或者监测。

通过拨号到连接在路由器控制台端口或者辅助端口上的调制解调器，你也可以在远端对路由器进行配置。

在进行故障排除时，相比辅助端口，控制台端口也是首选的。之所以首选控制台端口是因为它缺省就能显示路由器的启动、调试和错误消息。当网络服务未启动或者失效时，你仍可以使用控制台端口。因此，你可以使用控制台端口完成灾难和口令恢复过程。

10.2.4　广域网中路由器的功能

虽然路由器可以用来对局域网进行分段，但路由器的主要用途是作为广域网设备。路由器既有局域网接口又有广域网接口。事实上，常常用广域网技术来连接多台路由器。路由器之间通过广域网连接进行通信。路由器是大型内联网和Internet的骨干设备。路由器工作在OSI模型的第3层，根据网络层地址进行路由选择（在Internet中使用IP）

路由器的两项主要功能如下：

- 为进入的数据分组选择最佳路径。
- 将分组交换到适当的出站端口。

路由器通过建立路由选择表并与其他路由器交换路由选择表中的网络信息来完成这些功能。

管理员可以通过配置静态路由来手工维护路由选择表。然而，路由选择表通常是通过路由选择协议动态维护的，路由选择协议负责与其他路由器交换网络拓扑（路径）信息。

比如，如果一台计算机x需要与计算机y和计算机z通信。计算机y和计算机z位于世界上间隔很远的不同部分。计算机x为了实现与其他计算机的通信，必须有针对信息流的路由选择功能，此外为了实现可靠性，还需要冗余路径。许多网络设计方案和技术，归根结底都是为了使得计算机x、y和z能相互通信，或者叫互连。

然而，需要注意的是，一个互联网络必须包含下列功能：

- 一致的端到端寻址方式。
- 能反映网络拓扑结构的地址。
- 最佳路径选择。
- 动态路由选择和/或静态路由选择。
- 交换。



实验活动　连接控制台接口

在本实验中，你需要识别出路由器上的控制台接口。然后找到适当的电缆来将PC连接到路由器上，用作路由器的控制台



实验活动　连接局域网接口

在本实验中，你需要识别出路由器上的快速以太网接口。然后找到适当的电缆来连接路由器。最后，你用该电缆将路由器和计算机连接到集线器上。



实验活动　连接广域网接口

在本实验中，你需要识别出路由器上的串行接口。然后找到适当的电缆来连接路由器。最后，你用该电缆来连接多台路由器。

更多信息：路由器在广域网中的角色

通常，互联网络会包含大量的路由器、传输设施和接入的终端系统。在一个很大的互联网络中，比如Internet或者甚至是大型专用网络，要让任何一台计算机知道其他所有的计算机几乎是不可能的。因此，需要某种形式的层次、对互连的计算机进行分层组织就需要有专用的路由选择功能。

路由器可以专门用于学习和传播域内的路由信息。这些路由器称为内部网关（*interior gateways*）。另外，路由器也可以专门用于学习和传播域外网络的路由信息。这些路由器称为外部网关（*exterior gateways*）。

连网（networking）这个词是一个一般的或者通用的术语。然而，连网机器的通信方式在很多方面差别很大。路由器可以在一个互联网络中发挥不同的作用——比如，内部路由器、外部

路由器或边界路由器。

你可能已经注意到了，在前面的段落里多次将内部路由器、外部路由器和边界路由器分别称为内部网关、外部网关和边界网关。术语“网关（*gateway*）”本身就和“路由选择（routing）”一样老。但渐渐地，“网关”这个术语已经失去了某些字面上的意思。因此，除了在用词要求极为严格的地方，这两个词都是正确的。如果要求非常严格，你就得选择他们认为正确的词。

这些有关功能的专门描述不是纯理论性的。要理解它们之间的差别必须放在广域网环境中考察。因此，一个逻辑上的起点就是从上下文环境入手。“*广域网（WAN）*”、“*网络（network）*”、“*互联网络（internetwork）*”和“*自治系统（autonomous）*”这几个词可以互换，但仍然有细微的差别：

- **广域网**（*WAN*）——广域网是由相关的局域网通过路由器和租用线或帧中继电路等传输设施相互连接形成的聚集体。这个定义暗示了广域网中的局域网可能在地理上是分散的，但都由同一个组织支持，比如一个公司或者一个学校。
- **网络**（*Network*）——这个词的含义更为模糊，不是特指。从局域网到广域网，所有的都可以归入网络。因此，在本书中，“网络”这个词泛指许多构成网络的机制。因此，网络可以是局域网，也可以是广域网，但必须属于单一的组织并使用一致寻址体系结构。这个词有时用来指互联网络，甚至是Internet。
- **互联网络**（*Internetwork*）——“互联网络”这个词只比“网络”稍微具体一些。互联网络就是相互连接的关系松散的网络的聚集体。这些相互连接的网络可以属于不同的组织。比如，两个公司可以通过Internet互联各自专用的广域网。所形成的互联网络包括相互连接的一个公用网和两个专用网。互联网络最常见的定义是通过路由器连接的一组网络。这个定义并不要求这些网络之间有松散的联系，尽管这个词既可以指只有单个域或者单个自治系统的互联网络，也可以指由多个不同的自治系统组成的互联网络。
- **自治系统**（*Autonomous system*）——一个自治域系统（AS）是一个相对独立的网络或互联网络（既可以是局域网，也可以是广域网）。一个自治域系统由一个人（或者一个组织）管理，运行单一的被路由协议，使用一种地址结构。自治域系统可以支持与属于同一个组织或者由同一个组织运行的其他自治域系统的连接。另外，自治域也可以连接到其他的网络，比如Internet，但在运转上仍然是自治的。这个词通常跟特定的路由选择协议（比如OSPF或BGP）一起使用。这些路由选择协议支持把一个网络分成多个带编号的分段。

有了这些定义，就能更好地定义不同功能的路由器。内部路由器（interior router）是一种可以被网络中的一个端系统用来访问相同网络中的另一个端系统的路由器。内部路由器不支持到任何其他网络的连接。图10-11图示了一个小型网络并标识出了用作内部路由器的设备。

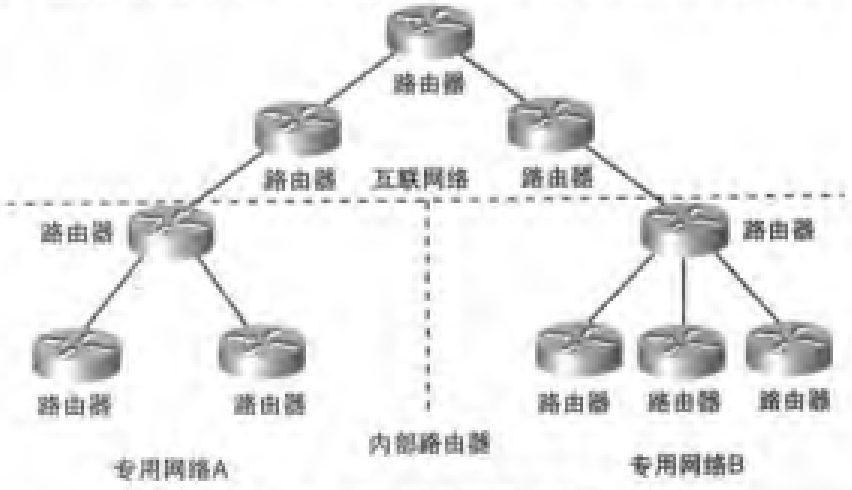


图10-11 网络中的内部路由器

外部路由器（exterior router）是处于任何一个网络边界以外的路由器。图10-12描述了一个高度简化的Internet拓扑结构，这只是为了解释什么是外部路由器，而不是要描述Internet真正的拓扑结构。

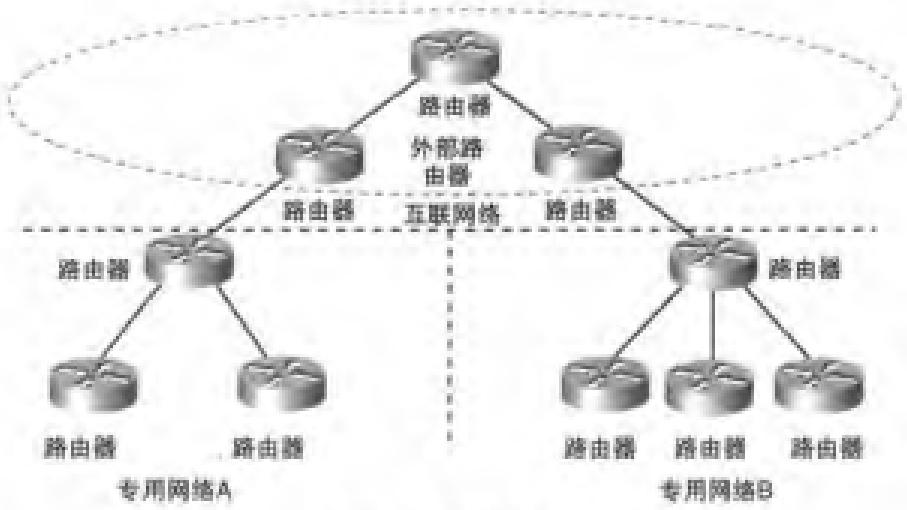


图10-12　外部路由器

最后一个功能分类是边界路由器（border router）。顾名思义，边界路由器是将一个网络与其余网络进行连接的路由器。需要注意的是，一个组织可能拥有并运行多个自治域系统。因此，一个边界路由器可能表明了两个自治域系统的边界，而不是某个专用网络和其他网络的边界。图10-13中标明了图10-11和图10-12的示例网络中的边界路由器。

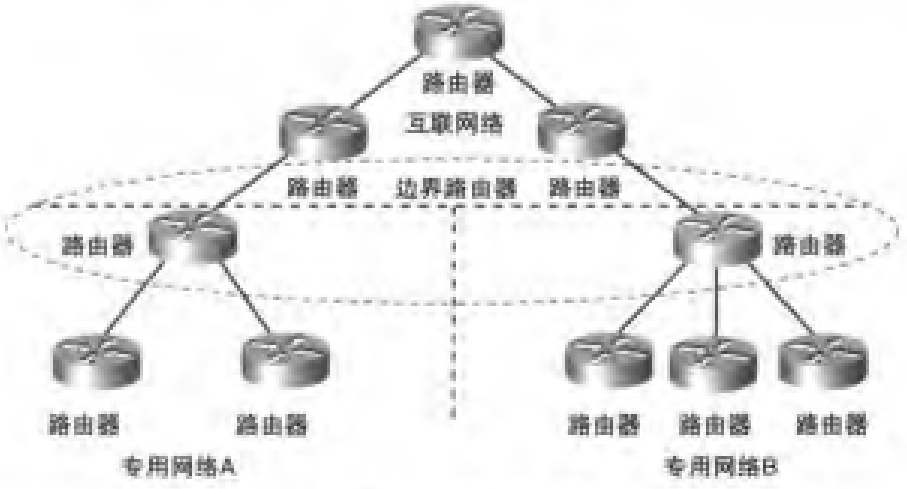


图10-13　边界路由器

10.2.5　实验室广域网模拟

一条可用的广域网线路能连接全球范围内的多台路由器。在学院的实验室中，所有的网络都是通过串行线缆或者以太网线缆相连的，以便学生能看到并亲自接触到设备。在现实环境中，一台路由器可能在纽约，另一台路由器可能在澳大利亚的悉尼。悉尼的管理员只能通过广域网网云连接到位于纽约的路由器，以便对其进行故障排除。

在学院的实验室中，整个专用电路网云已经被做得非常小，放在多条背靠背（back-to-back）DTE-DCE电缆之间的“裂缝（crack）”中。从一台路由器的接口s0/0到另一台路由器接口s0/1之间

的连接模拟了整个电路网云。

注意，必须配置时钟，否则CSU/DSU就无法正常工作。

更多信息：网络互联案例

通过对路由选择和网络互联背后的基本概念，以及这些主题所涉及的内在术语的分析，现在你可以通过分析三个网络互联案例，看看它们是如何使用的。每个场景都示范了一些在任何网络或互联网络中所必须回答的问题：

- 单个网络内的路由选择。
- 相邻网络之间的路由选择。
- 非相邻网络之间的路由选择。

这三个基本的方面几乎包含了你可能遇到的每一种形式的网络互联。每个方面对网络管理员都有不同的含义，包括路由计算和传播、收敛以及安全性等路由选择方面。下面的几小节对每个网络互联案例都进行了概述，并且着重强调了网络管理员需要关心的范围。对这些关于路由选择的问题的各种可能的解决方案贯穿了本书。

网络内的路由选择

路由选择最简单的形式是单个网络内的路由。这样的网络只包含内部路由器。理论上，这种网络只会使用一种路由协议、一种地址结构和最少数量的目的地。这种结构将大大减少每台路由器的负载，并使得网络的潜在性能发挥到最大。因此，内联网中的路由选择问题与网络规模和拓扑结构的关系比这一问题与地址结构和路由选择协议的关系更为紧密。所以必须认真选择拓扑结构以符合用户团体的需求。

如果网络足够小，管理员可以预先静态配置所有的路由而不需要引入复杂的动态路由选择协议。然而，静态配置的路由在不断增长和变化的网络中可能会成为一个繁重的负担。每当网络中发生变化时，你都必须到每一台路由器去手工更新，而不能由路由器自动更新。

相邻网络之间的路由

相邻网络之间的互联网络路由选择，比内部网路由选择稍微复杂一些。物理上邻接意味着两个网络直接相连。设计成相邻，可能是为了加快收敛速度，增加安全性，或者满足其他的一些性能指标。

在逻辑上划分多个网络意味着边界路由器必须在不同网络之间汇总和重新分发路由信息。这样，一个网络的端系统就能直接与另一个网络的端系统进行通信。图10-14解释了这种形式的

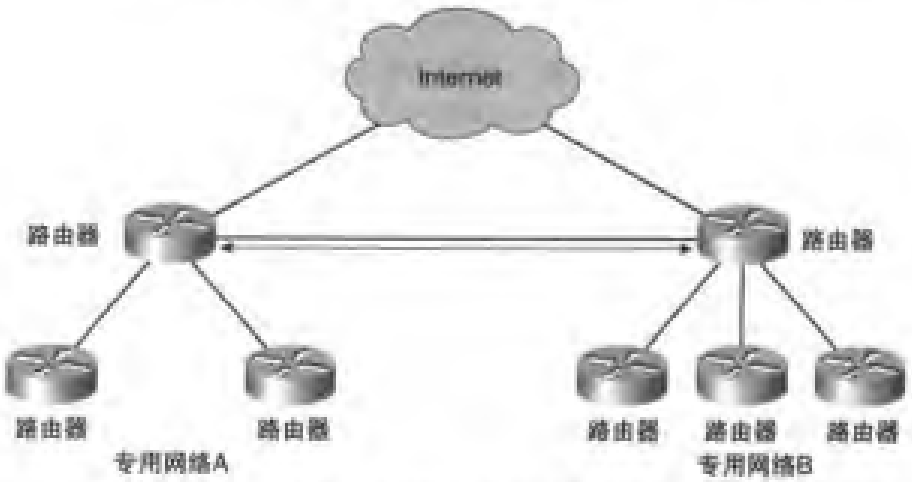


图10-14 相邻网络之间的路由选择

路由选择。

这类互联网络中需要解决的路由选择问题源自于两个网络的差别。下列是一些必须明确的可能存在的差别：

- 两个网络是否属于同一个组织？如果不是，边界路由器需要保证边界内网络的安全。
- 两个网络是否使用相同的路由选择协议？如果不是，你必须使用某种可以相互接受的度量标准。
- 两个网络是否使用同样的路由协议？如果不是，为了便于网络互联，你的网络可能必须支持另一种路由协议。

此外，拓扑结构也会影响相邻网络之间的路由选择。例如，在两个网络之间只设一个单独的互联点会使得路由信息的计算和网络间路由信息的传播更为容易。然而，这种方便性会引入单点故障，这可能是你的用户所不能接受的。引入另一个（甚至是多个）互联点能解决单点故障的问题，但可能产生无限路由选择环路的问题。要解决这个两难问题，必须了解你的用户对于风险和故障时间的承受能力。理解了用户需求，你就能考察特定路由选择协议的收敛速度的快慢和补偿潜在路由选择问题的能力。

非相邻网络之间的路由选择

非相邻网络之间的路由选择是最有用的同时也是最复杂的一种路由选择类型。两个网络可以使用第三个网络作为中介。这三个不同的网络很可能使用不同的路由选择协议、被路由协议和地址结构。因此，边界路由器的工作就是跨越这些障碍进行通信，并保护边界内网络的安全。图10-15图示了多个小规模的非相邻网络之间的路由选择。

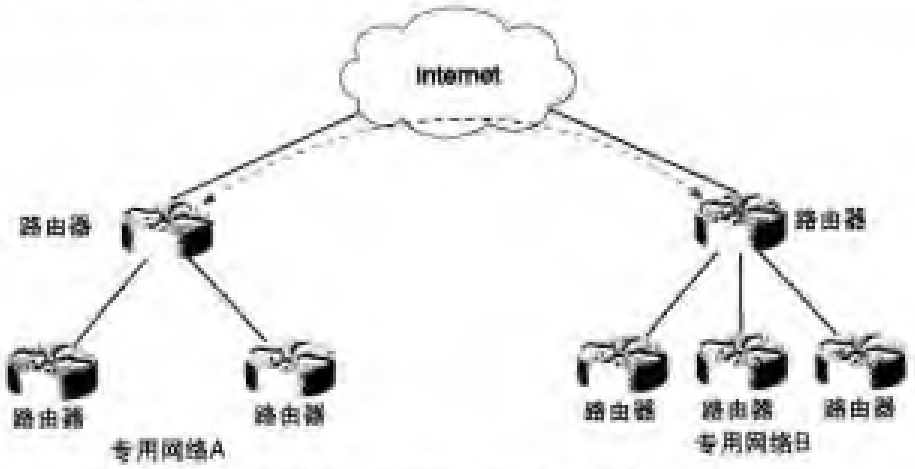


图10-15　非相邻网络间的路由选择

在这个图示中，每个专用网的边界路由器需要保护边界内的网络不受到非法入侵。由于需要通信的两个网络不相邻，并且中介网络不归它们控制，出现非法入侵的风险比两个网络直接相连要大得多。因此，网络管理员必须制定一套准则，只允许特定的外部用户进入他们的网络，除此之外不允许任何人访问。边界路由器可以通过访问控制列表来实现这些准则。

边界路由器的另一项责任就是对内部路由进行汇总，然后重新分发到区域以外的网络。这个过程使得专用网边界以外的用户能访问网内的终端系统。如果不分发路由选择信息，专用网以外的用户都无法访问网内的终端系统。

最后，在边界路由器上通常要配置多种路由选择协议。可能选择一种内部网关协议用于网内路由选择。但计算跨越互联网络的路由可能需要另一个协议——该协议需要有更强的路由汇总功能。通过将到不同网络的多个路由聚集成一条或者两条路由选择项，路由汇总能减小路由选择表的大小。

10.3 总结

本章学习了以下知识点：

- Internet是全球数以千计大小网络的相互连接。
- 广域网用于互联地理上间隔很远的局域网。
- 专线、电路交换、分组交换和信元交换是一些常见的广域网连接类型。
- 广域网用户有多种类型的广域网服务可以选择，但必须知道与广域网服务提供商之间的接口。
- 广域网设备包括路由器、广域网交换机、调制解调器、CSU/DSU和接入服务器。
- 广域网的物理层协议描述了如何为广域网服务提供电子的、机械的、操作的和功能的连接。
- 广域网数据链路层协议描述了帧如何在系统之间的单条数据链路上传递。

作为对你在本章中所学内容的补充，请参考本书所附光盘中与本章配套的视频、插图和e-Lab实验。

10.4　关键术语

信元交换服务（*cell-switched services*）　提供专用连接的交换技术，能将数字化的数据组织为信元单元并将信元在使用数字信号技术的物理介质上传输。

电路交换（*circuit switching*）　一种广域网交换方式，对于每个通信会话，需要建立穿越电信公司网络的专用物理电路。ISDN是电路交换式广域网技术的一个例子。

DCE（数据电路端接设备）（*data circuit-terminating equipment*）（ITU-T 术语）　组成用户-网络接口的网络端通信网络设备和连接。DCE提供到网络的物理连接，转发流量，并提供用于同步DCE和DTE设备之间数据传输的时钟信号。调制解调器和接口卡都是DCE的例子。

DTE（数据终端设备）（*data terminal equipment*）　用户-网络接口的用户端设备，可用作数据源、目的地或同时作为这两者。DTE设备通过DCE设备（如调制解调器）连接到数据网络，并且通常使用DCE产生的时钟信号。DTE包括诸如计算机、协议转换器和多路复用器之类的设备。

调制解调器（*modem*）　将数字信号与模拟信号进行转换的设备。在源端，调制解调器将数字信号转换为适于通过模拟通信设备进行传输的形式。在目的端，模拟信号被还原为数字形式。调制解调器使得数据能通过语音级电话线进行传输。术语“调制解调器”也可以用于描述各种类型的数字设备，比如CSU/DSU和ISDN终端适配器。

分组交换服务（*packet-switched services*）　根据每个分组中所包含的目的地址，在网络内对被称为分组的小数据单元进行路由。

传播延迟（*propagation delay*）　数据在网络中从源到最终目的传播所需要的时间。

路由器（*router*）　使用一种或多种度量标准来确定转发网络流量最佳路径的网络设备。路由器根据网络层信息将分组从一个网络转发到另一个网络。

交换机（*switch*）　根据每个帧的目的地址过滤、转发和泛洪帧的网络设备。交换机运行在OSI模型的数据链路层。

正常运行时间（*uptime*）　以用户对可用性的需求为标准，设备的工作和服务时间。

广域网（*WAN*）　诸如州、省或者国家等较大地理范围内的数据通信网络。广域网服务通常使用电信公司，比如电话公司，所提供的传输基础设施。

10.5 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 下面哪一项最准确地描述了广域网？
   A. 连接地理上相隔很远的局域网
   B. 连接一个大城市内的多个工作站、终端和其他设备
   C. 连接一座楼内的多个局域网
   D. 连接一座楼内的工作站、终端和其他设备
2. 广域网和局域网的区别是什么？
   A. 广域网主要是通过低速的串行接口访问
   B. 广域网提供高速的多种接入服务
   C. 广域网通常存在于一个小的地理区域内
   D. 广域网使用令牌来控制网络通信
3. 下列哪些是广域网技术的例子？
   A. 令牌环，ARCNet
   B. 帧中继，ISDN
   C. 星形，Banyan VINES
   D. CSU/DSU，ARCView
4. 广域网标准描述了OSI模型的哪些层？
   A. 数据链路层和网络层
   B. 数据链路层和表示层
   C. 物理层和应用层
   D. 物理层和数据链路层
5. 下列哪项最准确地描述了数据电路终结设备（DCE）？
   A. 由位于网络末端的用户设备组成
   B. 作为数据源或目的
   C. 由类似协议转换器和复用器的物理设备组成
   D. 由位于广域网连接末端的物理设备组成
6. 下列哪些部件提供了与语音级服务的接口，与T1/E1接口的信道服务单元/数字服务单元（CSU/DSU），与综合业务数字网（ISDN）接口的终端适配器/网络终端器（TA/NT1）？
   A. 交换机
   B. 路由器
   C. 调制解调器
   D. 通信服务器
7. 下列哪种设备主要用于提供拨入和拨出的用户连接？
   A. 交换机
   B. 路由器
   C. 调制解调器
   D. 通信服务器
8. 广域网物理层和数据链路层的标准包括：
   A. EIA/TIA-232
   B. PPP
   C. 帧中继

D. 以上全部

9. 将下面的部件与功能进行匹配

1）RAM/DRAM

2）NVRAM

3）ROM

4）闪速存储器

5）接口

选项：

a. 当一个单元断电后仍能保持其内容的RAM

b. 可以被微处理器读写的易失性内存

c. 可以被微处理器读但不可写的易失性内存

d. 可以电擦除和重新编程的非易失性存储器，可以根据需要存储、启动和重写软件映像

e. 两个系统或设备之间的连接

选择你的答案：

A. 1-b, 2-a, 3-c, 4-e, 5-d

B. 1-a, 2-b, 3-c, 4-e, 5-d

C. 1-b, 2-a, 3-e, 4-c, 5-d

D. 1-b, 2-a, 3-c, 4-d, 5-e

10. 互联网络可能提供：

A. 一致的端到端寻址和区分优先级的带宽分配能力

B. 能体现网络拓扑的地址和服务质量保证

C. 最优的路径选择和动态路由选择

D. 以上全部

11. 下列哪些是广域网的数据链路层的封装：

A. 高级数据链路控制（HDLC）

B. 帧中继

C. 点到点协议（PPP）

D. 以上全部

12. 路由器的主要功能有哪些？

A. 为入站的数据分组确定最佳路径，并将分组交换到适当的出站接口

B. 当两个节点位于不同的局域网上时，回复ARP请求

C. 构建路由选择表并与其他的路由器交换路由选择表内的信息

D. A与B

13. 哪一项是IBM设计的，针对系统网络结构（SNA）环境设计的，现在已大多被更通用的HDLC替代的广域网数据链路？

A. 串行链路接口协议

B. 点到点协议

C. 同步数据链路控制协议

D. 简单数据层控制协议

14. 那种广域网数据链路协议用于ISDN D信道的信令和呼叫建立？

A. LAPD

B. LAPF

C. LAPB

D. LAPR

15. 哪些属于广域网电路交换服务：

A. 旧式电话服务（POTS）

B. 最大带宽为1.544Mbit/s的窄带ISDN

C. 最大带宽为128kbit/s的的窄带ISDN

D. A和C

16. 哪一种服务已经成为非常流行的广域网技术？它比X.25的效率更高但提供的服务类似，最大带宽为44.736Mbit/s，并能提供非常受欢迎的56-Kbit/s和384-Kbit/s。

A.帧中继

B. X.25

C. POTS

D. ATM

17. 哪些属于信元交换技术：

A. ATM

B. 交换式多吉比特数据服务

C. T1

D. A和B

18. 哪些属于常见的DSL技术？

A. 高比特率DSL（HDSL）

B. 单线DSL（SDSL）

C. 非对称DSL（ADSL）

D. 以上全部

19. 下列哪项是一个甚高速物理层技术家族，它能提供一系列的数据速率并且都有专用的标识，它可以实现在从51.84Mbit/s（OC-1）到9952Mbit/s（OC-192）的不同光载波（OC）上，能通过波分复用（WDM）实现这些令人惊奇的数据速率？

A. SONNET

B. HDSL

C. ATM

D. SMDS

20. 下列哪种类型的路由器构成了用于源自其他网络或发往其他网络的流量的主要路径？

A. 内部路由器

B. 区域边界路由器

C. 骨干路由器

D. 自治系统（AS）边界路由器



第11章　路由器基础

目标：

学习完本章之后，你应该能够：

- 建立一个超级终端会话。
- 登录到路由器。
- 在命令行界面下使用帮助功能。
- 对命令的错误进行故障排除。
- 理解Cisco IOS软件及其功能的基本运行方式。
- 对Cisco IOS软件进行故障排除。
- 使用show version命令。
- 理解路由器用户界面和各种模式。

本章中，你将学习如何用正确的命令和启动顺序来完成路由器的首次启动和初始化配置。本章也解释了路由器的启动顺序和路由器使用当前的Cisco Internet操作系统软件来创建初始化配置文件时所使用的配置对话。

请务必看看关于本章的e-Lab实验、视频和插图，这些内容可以在本书所附的光盘中找到。光盘中的这些内容用作补充材料，能强化本章中所介绍的概念。

11.1　路由器启动顺序和Setup模式

路由器通过加载*自举程序（bootstrap）*、操作系统和配置文件来完成初始化。如果路由器找不到配置文件，就将进入setup模式。路由器会将通过setup模式创建的新配置的备份保存在***非易失性随机存取存储器（NVRAM）***中。

路由器加电后，会进行***加电自检（POST）***。在自检过程中，路由器执行ROM内的诊断程序，对所有的硬件模块进行检查。这些诊断程序会检查CPU、内存和网络接口的情况。确定了硬件都能正常工作，接下来路由器便进行软件初始化过程，以下列两个过程为特征：

- 系统启动例程对路由器软件进行初始化。
- 回退例程（fallback routines）在需要时提供其他的启动方式供选择。

Cisco IOS软件启动例程的目标是使路由器开始运转。路由器在运转过程中必须根据配置，为所

连接的用户网络提供可靠的服务。为了达到这一点，启动例程必须完成如下的工作：

1. 确认路由器启动时对所有的硬件进行了测试。
2. 找到并装载路由器用作操作系统的Cisco IOS软件。
3. 找到配置文件并应用各条配置语句，或者进入setup模式。

11.1.1　路由器启动顺序

完成加电自检 后，接着进行路由器初始化，步骤如下：

1. 执行ROM中的普通自举程序加载器（generic bootstrap loader）。自举程序（Bootstrap）是一个简单的预制操作，用于加载一些指令，这些指令又将其他的指令装入内存，或是使得路由器进入其他的配置模式。

2. Cisco IOS软件映像可以存放在很多地方。装载Cisco IOS软件映像 时所使用的位置由配置寄存器（configuration register）的启动字段（boot field）决定。如果启动字段指明是从*Flash*存储器或是网络加载，那么在配置文件中的boot system命令就指明了映像的确切名称和位置。

3. Cisco IOS软件映像 加载完成。当Cisco IOS软件加载完成并开始运行后，操作系统就定位硬件及软件部件并在控制台终端（console terminal）上列出结果。

4. 将保存在NVRAM中的配置文件加载入主存中，然后逐行执行。这些配置命令将完成启动路由选择进程，为每个接口分配地址，设置介质特性等任务。

5. 如果NVRAM中没有有效的配置文件，或者是NVRAM的内容被擦除了，操作系统将执行问题驱动（question-driven）的初始化配置历程，称为系统配置对话（system configuration dialog），当路由器重新启动时，也叫setup模式。

图11-1显示了这一启动顺序。

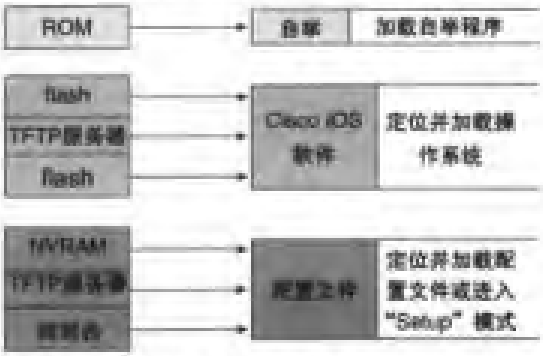


图11-1　启动顺序

11.1.2　系统配置对话

Setup模式不是用于在路由器上输入复杂的协议功能的。setup模式的主要用途为无法从其他途径找到配置文件的路由器快速地建立一个最小配置。

在setup模式下，对于许多系统配置对话的提示问题，缺省的回答都显示在问题后面的方括号内（[]）。按回车键就能使用这些缺省回答。

如果系统此前已经进行了配置，则缺省值为当前的配置值。如果希望完全重新配置，可以用erase startup-config命令来去除NVRAM中的当前配置文件。Reload命令会将路由器重启，并再次启动setup。如果是首次对系统进行配置，则采用厂商的缺省值。如果没有厂商的缺省值，如密码，则在问号（?）后什么也不显示。在Setup过程中，可随时按Ctrl+C终止这一过程并重新开始。一旦setup被中断，所以接口都会被强行关闭。例11-1显示了setup命令

例11-1　setup命令。

```
r setup

-- System Configuration Dialog --
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

```
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: no

First, would you like to see the current interface summary? [yes]: yes

Interface    IP-Address     OK?  Method   Status                  Protocol
Ethernet0    198.133.219.1  YES   NVRAM  up                     down
Serial0      unassigned     YES   NVRAM  administratively down   down
Serial1      unassigned     YES   NVRAM  administratively down   down
```

在setup模式下完成配置过程后，屏幕将会显示你所创建的配置。当询问你是否使用这些配置时，如果回答“yes”，就会执行该配置并将其保存到NVRAM。如果回答“no”，配置不会被保存，setup过程重新开始。如果出现提示符--More--，按空格键继续显示下一屏信息。

你可以从全局配置模式的提示符进入setup 模式：Router # setup。路由器会显示路由器端口的当前配置。

11.1.3 设置全局参数

查看了当前接口的概要信息之后，显示器上会出现一个提示符，如例11-2所示，指明你必须为路由器配置全局参数。这些参数是你所选择的配置值。

第一句指出你正在配置路由器的全局参数。第一个全局参数是路由器的主机名(host name)。该主机名将成为Cisco IOS软件所有EXEC模式下提示符的一部分。在初始配置时，方括号中显示的缺省值为[Router]。设置了路由器名称后，你需要设置路由器上使用的各种口令。

例11-2 全局参数

```
Configuring global parameters:

Enter host name [Router]: Cisco

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: cougars

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: lumberjacks

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: matadors
Configure SNMP Network Management? [yes]: no
```

你必须输入enable口令。在提示符“Enter enable secret”下输入的字符串会通过Cisco专用的加密算法进行加密。这增强了口令字符串的安全性。任何人列出路由器配置文件的内容时，enable口令都会显示为一个无意义的字符串。

在setup模式中，系统建议使用不同的“*enable*口令”和“*enable secret*口令”，但不要求必须这样做。Enable secret口令是单向的加密字。当enable secret口令存在时，则替代enable口令。当enable secret口令不存在时才使用enable口令。由于是单向的加密，如果遗忘了，enable secret口令是无法恢复的，但enable口令是明文，可以从配置文件中得到。

其他一些版本的CiscoIOS软件中也使用enable口令。所有的口令都是区分大小写的，可以包含字母和数字。

可以通过用口令限制到路由器各个线路的访问来保护路由器。例11-3使用了line-console 0命令和后续的login与password来为控制台终端设定登录口令。这样做的目的是要求用户在获得对路由器的访问权之前，必须登录进入控制台。console 0指明了是路由器的控制台连接，login提示用户在进入控制台连接之前需要输入口令。

例11-3 配置路由器的控制台口令

```
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password cisco
```

如例11-4所示，line vty 0 4命令和后续的password子命令设定了针对入站Telnet会话的登录口令。

例11-4 配置路由器的虚拟终端口令

```
Router(config)# line vty 0 4
Router(config-line)# password sanjose
```

为各种端口设置了口令后，路由器会提示你输入要使用的路由选择协议，如例11-5所示。当系统提示你为每个协议设定参数时，你可以使用已经为你的路由器选择的配置值。如果你回答“yes”，可能会出现关于该协议的附加问题。

例11-5 控制台显示的全局参数提示符

```
Configure IP? [yes]:
Configure IGRP routing? [yes]: 200
% Please answer 'yes' or 'no'.
Configure IGRP routing? [yes]: yes
Your IGRP autonomous system number [1]: 200
Configuring interface parameters:

Do you want to configure Ethernet0 interface? [yes]: yes
Configure IP on this interface? [yes]: yes
IP address for this interface: 10.10.10.1
Subnet mask for this interface [255.0.0.0] :
Class A network is 10.0.0.0, 8 subnet bits; mask is /8

Do you want to configure Serial0 interface? [yes]: n
```

```
Do you want to configure Serial1 interface? [yes]: n
The following configuration command script was created:
hostname Cisco
enable secret 5 $1$37Kq$vA6UckClKEBzOIWGIF54U/
enable password lumberjacks
line vty 0 4
password wildcats
no snmp-server
!
no bridge 1
ip routing
!
interface Ethernet0
ip address 10.10.10.1 255.0.0.0
!
--- output omitted ---
```

实验活动 用sctup进行路由器配置

在本试验中，你将使用系统配置对话（setup）来设定基本的路由器配置参数。

11.1.4 路由器的LED指示器

Cisco路由器使用*发光二极管（LED）*指示器来提供状态信息。根据Cisco路由器型号的不同，LED指示器也有差别。

子卡（daughter card）上端的LED指示了该子卡上串口1的活动情况。子卡下端的LED指示了广域网端口或BRI端口的活动情况。图11-2和11-3图示了路由器的LED指示器。

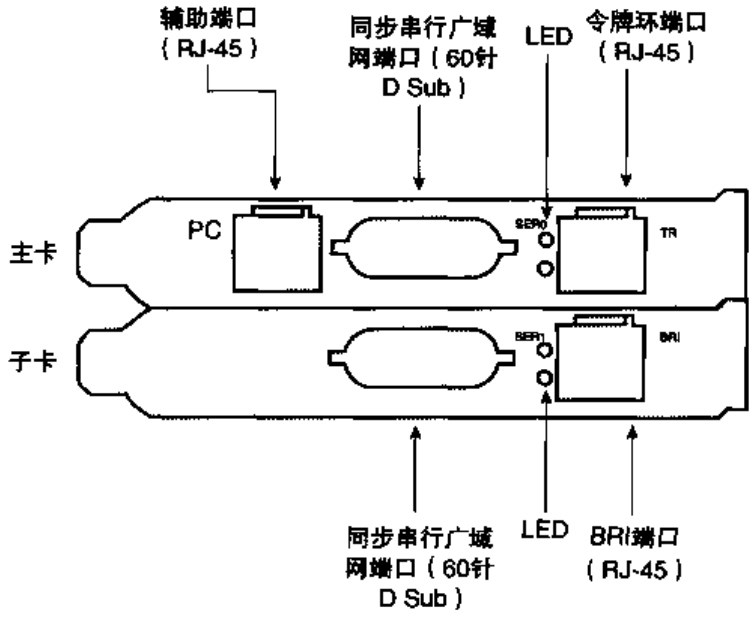


图11-2 2500系列路由器的LED指示器

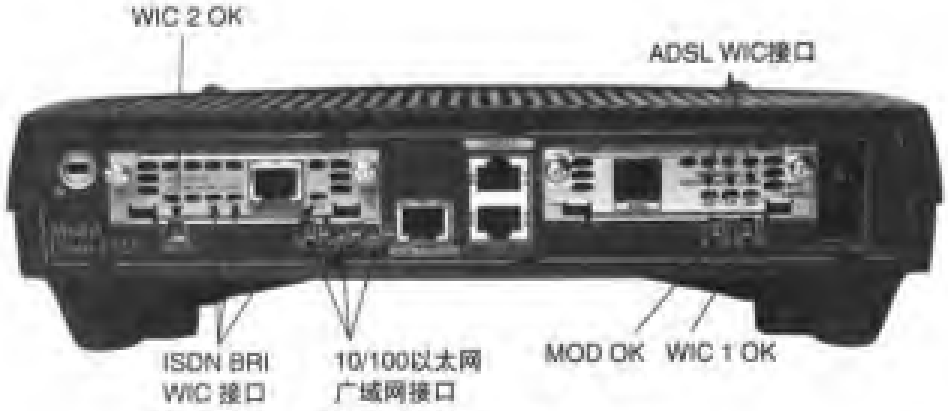


图11-3　1721系列路由器的LED指示器

接口上的LED指示了相应接口的活动情况。如果当接口活动时LED未亮，并且接口连接是正确的，这可能就表明存在问题。如果某个接口极忙，则其LED总是亮的。当系统正确初始化后，两个广域网接口卡底部的绿色OK LED变亮。

11.1.5　路由器初始启动时的输出

每次加电，路由器都会经过下列的启动序列：

1. 路由器经过POST诊断程序来检查CPU、内存和各个接口的基本运行情况。
2. 要确认系统的自举软件加载正确，启动映像执行并寻找一个有效的Cisco IOS软件映像（路由器操作系统软件）。Cisco IOS软件映像的来源，无论是Flash存储器还是TFTP服务器，都是由配置寄存器的设置确定的。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存储器中加载Cisco IOS软件映像。
3. 如果经过五次尝试，都没有在Flash存储器中找到有效的Cisco IOS软件映像，路由器就回到启动ROM模式（boot ROM mode）。该模式用于安装或者升级Cisco IOS 软件映像。
4. 如果找到了有效的Cisco IOS软件映像，路由器会搜索有效的配置文件。
5. 如果没有在NVRAM中找到有效的配置文件，路由器会通过所有接口搜索TFTP服务器。如果没有找到配置文件，路由器就运行系统配置对话，以便手工生成配置。

在例11-6和11-7中，根据路由器上接口和Cisco IOS版本的不同，所显示的消息也不同。本图中的屏幕显示只是作为参考，可能没有完全准确地反映控制台的屏幕显示。

例11-6　NVRAM 无效

```
System Bootstrap, Version X.X(XXXX) [XXXXX XX], RELEASE SOFTWARE
Copyright (c) 1986-199X by Cisco Systems
1721 processor with 4096 Kbytes of main memory

Notice: NVRAM invalid, possibly due to write erase.

--- output omitted ---
```

例11-7　自举程序和Cisco IOS 软件版本

```
--- output omitted ---
IOS (tm) 1721 Software (XXX-X-X), Version (XXXXX XXX)
Copyright (c) 1986-199X by Cisco Systems, Inc.
```

注意：在例11-6中NVRAM是无效的；这可能是由于写擦除。这就告诉了用户路由器尚未进行初次配置或者NVRAM被擦除了。路由器只有经过了配置才能使用。

在例11-7，用户可以确定路由器使用的自举程序的版本和Cisco IOS软件的版本。用户可以确定路由器型号、处理器和路由器所包含的内存大小。输出中还包括了下列信息，如例11-8所示：

- 路由器有多少个接口。
- 路由器有哪些类型的接口。
- NVRAM的容量。
- Flash存储器的容量。

例11-8 自举程序和Cisco IOS 软件版本

```
Processor board ID 10226279
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
MICA-6DM Firmware: CP ver 2730 - 5/23/2001, SP ver 2730 - 5/23/2001.
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
Primary Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
24 Serial network interface(s)
4 low speed serial(sync/async) network interface(s)
6 terminal line(s)
1 Channelized T1/PRI port(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

11.2 建立一个超级终端会话

所有的路由器都包含EIA/TIA-232异步串行控制台端口（RJ-45）。将控制台终端（一台ASCII终端或者运行终端模拟软件的PC）连接到控制台端口需要线缆和适配器。要将运行终端模拟软件的PC连接到控制台端口，需要使用带有母式接头RJ-45到DB-9或者RJ-45到DB-25适配器的RJ-45到RJ-45反转电缆。

控制台端口缺省的参数是9600波特、8个数据位、无奇偶校验、1个停止位并且无流控制。控制台端口不支持硬件流控制。

按照下面的步骤将一台终端连接到路由器的控制台端口上：

步骤1 用RJ-45到RJ-45反转电缆和RJ-45到DB-9或者RJ-45到DB-25适配器连接终端或PC

注意：如果你在这一端使用交叉电缆，则另一端必须是直通的或类似的电缆。

步骤2 将终端或者PC终端模拟软件配置为9600波特、8个数据位、无奇偶校验、1个停止位并且无流控制。

图11-4　示例了一个到PC的控制台连接，可以与PC建立一个超级终端连接。

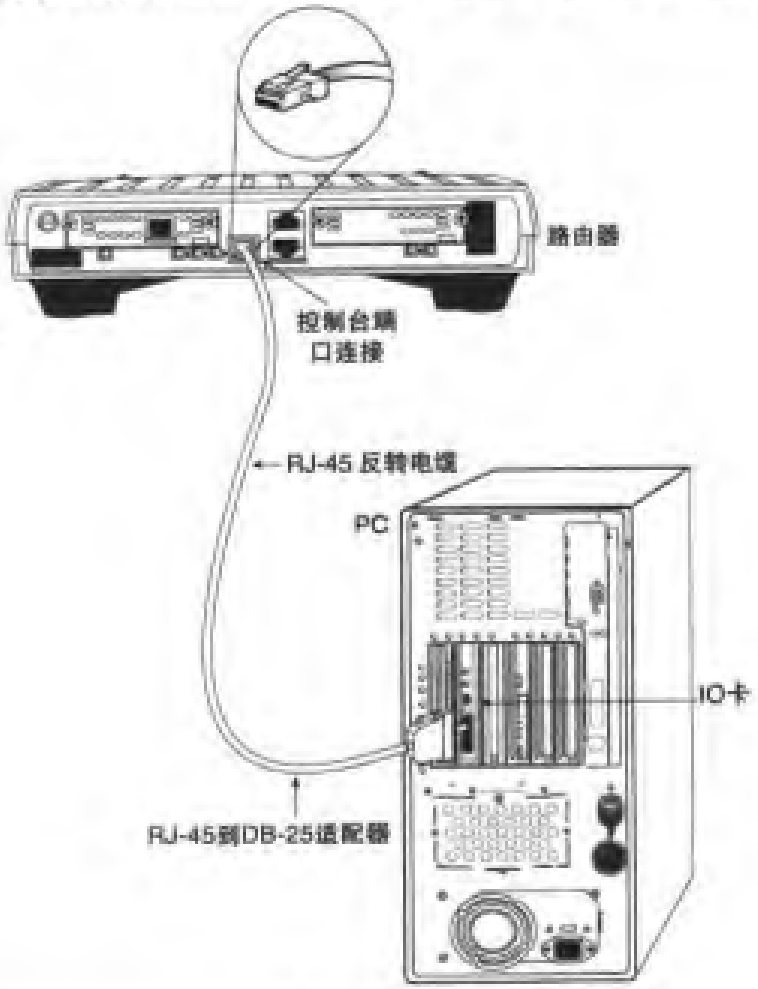


图11-4　终端控制台电缆

表11-1列出了多个操作系统和相应的终端模拟软件。

表11-1　可用的终端模拟软件

PC操作系统	软件
Windows 9x NT, 2000和XP	HyperTerminal（包含在Windows自带的软件中）, ProComm Plus
Windows 3.1	Terminal（包含在Windows自带的软件中）
Macintosh	ProComm, VersaTerm, ZTerm（单独提供）

实验活动　用超级终端建立一个控制台连接

在本实验中，将用控制台电缆将一台工作站连接到路由器，并通过配置超级终端来建立一个与路由器的控制台会话。

11.3　登录进入路由器

要配置Cisco路由器，必须首先通过终端或远程接入访问用户界面。访问路由器时，你在输入任何其他的命令之前必须首先登录。

出于安全的考虑，路由器有两级的命令访问控制，如例11-9所示：

- 用户EXEC模式——典型的任务包括路由器状态的查看。在此模式下，无法更改路由器配置。
- 特权EXEC模式——典型的任务包括改变路由器的配

登录到路由器后，会显示用户EXEC模式提示符。这种模式下可用的命令是特权模式下可用命

令的一个子集。这些命令大多数都是用于显示信息的，不能改变路由器的配置。

例11-9 路由器的各种模式

```
Router> ---------------- User Mode
Router>enable
Password:
Router# ---------------- Privileged-Mode
Router>disable
Router>
```

要使用整个命令集，你必须首先进入特权模式。在 > 提示符下键入enable。在password提示符处键入由enable secret设置的口令。当你完成了这些登录步骤，提示符就会变成井号（ # ），显示你现在已经处于特权模式下了。从特权EXEC模式，你可以进入全局配置模式和其他的特定配置模式，包括：

- **接口模式**（*Interface*）（central_2(config-if)# ）。
- **子接口模式**（*Subinterface*）(central_2(config-subif)#)。
- **Line模式**（*Line*）(central_2(config-line)#)。
- **路由器模式**（*Router*）(central_2(config-router)#)。
- **路由映射模式**（*Route-map*）(central_2(config-map-class)#)。

要退回用户EXEC模式，可输入disable。要从路由器注销，输入exit 。屏幕的输出随特定的Cisco IOS 软件级别和路由器配置的不同而有所差别。

更多信息：Cisco IOS软件的基本运行方式

Cisco互联网操作系统（IOS）软件平台实现在各种不同的硬件之上。它是所有Cisco路由器上内嵌的软件体系结构。

Cisco IOS软件使得这些产品能提供下列的网络服务：

- 用于传送特定的网络协议和功能的特性。
- 设备之间的高速通信连接。
- 控制访问并拒绝非授权者使用网络的安全性。
- 为了适应网络的发展所必需的增加接口和处理能力的可扩展性。
- 保证对网络资源可靠访问的可靠性。

可以通过控制台、调制解调器或Telnet会话等多种方式进入Cisco IOS软件的命令行界面。无论采取那种方式，进入IOS命令行界面通常称为一个EXEC会话。

11.3.1 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（？），会显示常用命令的列表，如例11-7所示。

注意示例输出底部的“--More--”。屏幕一次显示22行，底部的“--More--”提示符表明输出有多屏。只要出现了--More--，你就可以按空格键查看下一屏。如果只要显示下一行，可以按回车键（Enter）。按其他任意键，则回到提示符。

例11-10 键盘帮助

```
?
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
```

注意：此处显示的命令列表是与所处的配置模式有关的。你在用户模式下看到的命令列表和特权模式下看到的就不同，在全局配置模式下看到的和在接口配置模式下看到的也不一样。

要访问特权EXEC模式，需要输入enable或者缩写ena。输入enable后路由器会提示输入口令。在特权EXEC模式下输入问号（参见例11-11），会显示比用户EXEC模式提示符下更长的命令列表。

例11-11 特权EXEC模式下的命令

```
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
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--
```

根据Cisco IOS软件级别和路由器配置的不同，屏幕输出也会有差别。

11.3.2 路由器的帮助功能

假设一个用户希望设定路由器的时钟。如果不知道所需要的命令，这个用户可以用帮助功能来查看关于时钟设定的语法。下面的练习演示了帮助功能诸多用途的一种。你的任务是设置路由器的时钟。假设你不知道需要使用的命令，请执行以下七个步骤：

步骤1 使用? 查找设定时钟所需的命令。帮助输出显示了需要使用clock命令。

步骤2 检查更改时间的语法。

步骤3 按所示格式输入当前时间，即小时、分钟和秒。系统提示需要其他的信息以完成该命令。例11-12中的帮助输出显示了需要使用关键字set。

例11-12 时钟set关键字

```
Cisco# clok
Translating "clok" ...domain server (255.255.255.255)

% Unknown command or computer name, or unable to find computer address
Cisco# cl?
clear# clock

Cisco# clock
% Incomplete command.

Cisco# clock ?
set  #Set the time and date

Cisco# clock set
% Incomplete command.

Cisco# clock set?
hh:mm:ss# Current Time
```

步骤4 检查输入时间的语法，并用小时、分钟和秒输入当前时间。如例11-13所示，系统再次提示需要其他的信息以完成该命令。

例11-13 时钟时间和日期设定格式

```
Cisco# clock set 19:50:00
% Incomplete command.

Cisco# clock set 19:50:00 ?
<1-31># Day of the month
MONTH  #Month of the year

Cisco# clock set 19:50:00 14 7
                             ^
% Invalid input detected at  '^'  marker.

Cisco# clock set 19:50:00 14 July
% Incomplete command.

Cisco# clock set 19:50:00 14 July ?
<1993-2035>  #Year

Cisco# clock set 19:50:00 14 July 2003

Cisco#
```

步骤5 按下 Ctrl + P（或向上箭头）来自动重复前一个命令。然后输入空格和问号（？）来获得还需要输入的参数。现在你可以完成整个命令了。

步骤6 脱字符(^)和帮助响应表明存在错误。脱字符的位置显示了可能存在问题的地方。要输入正确的语法，重新输入命令到脱字符所在的位置，然后纠正错误，在这之后输入问号（？）。

步骤7 用正确的语法输入年份，按回车键执行这条命令。

用户界面通过在出错的地方标上“^”来进行语法检查。“^”出现在输入了错误的命令、关键字或者参数的地方。出错位置提示和交互式的帮助系统能帮助你很容易地找出并更正语法错误。

11.4 Cisco IOS软件的编辑命令

用户界面包括一种增强的编辑模式，用来对键入的命令行提供一系列的编辑功能。使用表11-2中的按键组合来移动光标在命令行中的位置，以便改错或变更。尽管在当前的软件版本中，增强编辑功能是自动启用的，但如果你编写的脚本在增强编辑功能启动时不能很好地与系统交互，你也可以禁用这一功能。要禁用增强编辑功能，可在特权模式提示符下输入terminal no editing 。

表11-2 编辑命令

命令	说明
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

对于长度超过屏幕上单行长度的命令，编辑命令提供了自动滚行的功能。当光标移动到右边界时，命令行向左移出10个空格。行首的10个字符不可见，但用户可以回滚到行首进行语法检查。会滚的方法是不断按下Ctrl+b或者向左的箭头直到回到命令行的首部，也可以按Ctrl+a直接回到命令行的首部。

在例11.14中，命令输入超过了一行。当光标首次到达行尾时，该行左移10个字符，然后重新显示。美元符号（$）表明命令行进行了左移。每次光标移动到达行尾时，命令行就会向左移出10个空格。

例11-14　命令项的扩展

```
Cisco>$ value for our customers, employees, investors, and partners
```

根据Cisco IOS 软件级别和路由器配置的不同，屏幕的输出也不同。

Ctrl+z命令可以退出配置模式。使用该命令会返回到特权EXEC模式提示符。

11.5　路由器命令历史

用户界面提供你所输入命令的历史或者说是记录。这一功能对于再次使用很长或者很复杂的命令是很有用的。利用命令历史功能，你可以完成以下的任务：

- 设置命令历史缓存的大小。
- 重用命令。
- 禁止命令历史功能。

缺省情况下，命令历史功能是启动的，系统会在历史缓冲区中记录10条命令。要改变系统在一个终端会话中记录的命令行数，可以使用terminal history size 或 history size 命令。可以设定的最大命令数是256。表11-3显示了关于命令历史的命令。

表11-3　有关命令历史的命令

命令	说明
Ctrl + p	这个组合键或者向上箭头可以重用最近一条（前一条）命令
Ctrl + n	这个组合键或者向下箭头可以重用下一条命令
show history	显示命令缓冲区的内容
terminal history [size *number-of lines*]	设置命令缓冲区的大小
no terminal 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

要重用历史缓冲区中的命令，可以按Ctrl+p，最近使用的命令出现在最前面。继续按下Ctrl+p或者向上箭头可以重用更早的命令。按下Ctrl+p或者向上箭头后，要回退到历史缓冲区中更新的命令，可以按Ctrl+n或者向下箭头。

作为快捷方式，在输入命令时，你可以输入能表示该命令的惟一字符串。然后按下Tab键，用户界面会替你完成命令行。当已经输入的字母能惟一标识该命令时，按下Tab键是让你能更清楚地看到路由器已经理解了你所要使用的命令。

在大多数计算机上，还可以使用额外的选择和复制功能。以前的一个命令串可以被复制，然后粘贴或者插入到当前的命令输入中。



实验活动　命令行基础

在本实验中，你将登录到路由器的用户模式和特权模式。你会使用一些基本的路由器命令来确定路由器的配置。你还会了解路由器的帮助功能，并使用命令历史和命令编辑功能。

11.6 Cisco IOS软件基础

与任何计算机一样，路由器或交换机离开操作系统就无法工作。Cisco将自己的操作系统称为Cisco 互联网络操作系统，或者Cisco IOS软件。它是内置在几乎所有的Cisco路由器和Catalyst交换机上的软件体系结构。某些Catalyst交换机使用Cisco命令行界面(CLI)。路由器只有在加载了Cisco IOS软件后才能工作。没有操作系统，硬件就无法发挥作用。Cisco IOS软件提供了下列的网络服务：

- 基本的路由选择和交换功能。
- 对联网资源可靠和安全的访问。
- 网络的可扩展性。

11.6.1 Cisco IOS 软件的运行

Cisco IOS 软件设备有三种不同的运行环境或者叫模式：

- ROM monitor
- Boot ROM
- Cisco IOS

路由器的启动程序通常会被加载到RAM中，并在上述三种运行环境之一中工作。系统管理员可以用配置寄存器来控制路由器使用哪种模式进行装载。

ROM monitor完成自举过程，并提供低级别的功能和诊断。ROM monitor用于恢复系统故障或口令恢复。只能通过控制台端口会话访问，不能通过其他的任何网络接口访问ROM monitor。

当路由器运行在boot ROM模式时，只能使用Cisco IOS软件功能的一个有限子集。Boot ROM允许对Flash存储器执行写操作，主要用于替换Flash中存储的Cisco IOS软件映像。在boot ROM模式下，可以用copy tftp flash命令修改Cisco IOS软件映像，该命令能将存储在TFTP服务器上的IOS映像复制到路由器的Flash存储器中。

路由器的正常运行，需要使用Flash存储器中完整的Cisco IOS软件映像。在某些设备中，IOS直接在Flash中工作。但大多数的Cisco路由器要求将Cisco软件映像的一个拷贝加载到RAM中，从RAM中执行。某些Cisco IOS软件在Flash中以压缩格式存放，在复制到RAM时必须解压。

要查看正在运行的Cisco IOS软件映像及其版本，需要使用show version命令，该命令还能显示配置寄存器的设置。例11-15中的show flash命令检验了系统有足够的存储容量来装载一个新的Cisco IOS 软件映像。

例11-15 检验Cisco IOS 软件映像

```
Cisco> show flash

System flash directory:
File Length Name/status
1 8022152 /c2500-i-l.121-26.bin
[8022216 bytes used, 366392 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

11.6.2 Cisco IOS软件的功能

Cisco为很大范围网络产品平台的设备提供了Cisco IOS软件映像。为了优化各种产品平台所需要的Cisco IOS软件映像，Cisco正在开发多个不同的Cisco IOS软件映像。每个映像都代表了一个，

服务各种的设备平台的不同的功能集合，不同的存储器资源以及不同的客户需求。

针对不同的Cisco设备和功能集，存在许多的Cisco IOS软件映像。然而，基本配置命令的结构是一样的。在任何一种设备上获得的配置和故障排除的经验都可以应用到很大范围的多个产品上。

针对各个Cisco IOS软件版本的命名约定包含三个部分：

- 该映像所运行的平台。
- 该映像所支持的特定功能。
- 该映像在哪里运行，以及它是否是压缩的。

这些内容将在第14章“管理Cisco IOS软件”中进行更详细的介绍。

Cisco IOS软件的命名约定、映像的内容和其他的细节都是易改变的。

确定了符合网络需求的功能项后，就可以选择硬件所支持的Cisco IOS软件版本。各个设备的软件需求列在了文档CD的“Cisco产品文档”部分。Cisco软件顾问（Cisco Software Advisor）是一个交互式的工具，能提供最新的信息。

在选择一个新的IOS映像时，需要考虑的一个主要问题就是与路由器的Flash和RAM存储器兼容。通常，版本越新，提供的功能就越多，所需要的内存也越多。如例11-13所示，在Cisco设备上使用show version命令检查当前的映像和可用的Flash存储器空间。Cisco的支持站点上有工具能帮助确定每个映像所需要的Flash存储器和RAM的大小。

在安装一个新的Cisco IOS软件映像到路由器之前，检查一下路由器是否达到该映像对于内存容量的要求。要查看RAM的容量，可以使用show version 命令，并查看例11-16中的下列输出。

例11-16　show version命令输出

```
Cisco> show version
Cisco Internetwork Operating System Software
--- output omitted ---
image file is "flash:/c2500-i-l.121-16.bin"

cisco 2600 (680301) processor (revision N) with 61440K/2048K bytes of memory.
```

高亮的一行显示了路由器上安装了多少主内存和共享内存。某些平台使用“动态RAM(DRAM)”的一部分作为共享内存。内存的需求也要考虑这一点，因此需要将两个数字相加来确定安装在路由器上的DRAM的容量。

要确定空闲的Flash存储器的容量，可以使用show flash命令，如例11-17所示。

例11-17　show flash 命令输出

```
Cisco> show flash

System flash directo ry:
File   Length    Name/status
1      8022152   /c2500-i-l.121-16.bin
[8022216 bytes used, 366392 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

11.6.3　show version命令

show version 命令显示关于当前在路由器上运行的Cisco IOS 软件版本的信息。这包括配置寄存器和启动字段的设置。

- Cisco IOS软件版本和描述信息。
- 自举ROM版本。
- 启动ROM 版本。
- 路由器启动后持续的时间。
- 最近一次启动的方式。
- 系统映像文件及其位置。
- 路由器平台。
- 配置寄存器的设置。

11.6.4 路由器用户界面

回忆一下，Cisco IOS软件使用*命令行界面（CLI）*作为自己传统的控制台环境。Cisco IOS软件是一项核心技术，它跨越大多数Cisco产品线。根据使用它的联网设备的不同，Cisco IOS软件的运行细节也有所差别。

CLI环境可以通过几种方式访问：

- 通过控制台会话。控制台端口使用低速串行连接，从计 算机或终端直接到路由器的控制台端口。这种方式不要求配置路由器的网络服务。这种方式不要求配置路由器上的网络服务。
- 通过连接到路由器AUX端口的调制解调器或者零调制解调器（null modem）。这种方式同样不要求配置路由器上的网络服务。
- 通过Telnet作为虚拟终端连接到路由器。要建立一个到路由器的Telnet会话，至少需要给一个接口配置IP。必须为各个虚拟终端会话配置登录并设定口令。

11.6.5 路由器用户界面和各种模式

Cisco CLI使用了一种分级的结构。这种结构要求进行不同的模式以完成各种特定的任务。例如，必须进入接口配置模式以完成对路由器接口的配置。在接口配置模式下，输入的所有配置都只应用到该接口。每种命令模式都用独特的提示符显示，并且只许可适合该模式的命令。

Cisco IOS 软件提供了一种称为命令执行者（command executive，EXEC）的命令解释器服务。每个命令输入后，EXEC都会验证并执行该命令。

作为一项安全功能，Cisco IOS软件将EXEC会话分成了两个访问级别。这两个级别分别是“用户EXEC模式”和“特权EXEC模式”，后者也称为“enable 模式。”

用户EXEC模式只允许有限数量的基本监视命令。这通常被称为“只查看view-only模式”。用户EXEC级别不允许任何会改变路由器配置的命令。用户EXEC模式通过提示符“>”标识。

特权EXEC模式提供了对路由器所有命令的访问。特权EXEC模式可以通过要求输入用户ID和口令来保护。这种模式只允许经过授权的用户访问路由器。配置和管理命令要求网络管理员能进入特权EXEC级别。全局配置模式和所有其他的特定配置模式都只可以从特权模式到达。特权模式通过提示符“#”标识。

要从用户EXEC级别进入特权EXEC级别，需要在提示符“>”下输入enable命令。如果配置了口令，路由器会在此时询问口令。出于安全性的原因，Cisco网络设备不会显示所输入的口令。当输入了正确的口令时，路由器的提示符会改变为#，表明路由器现在已经处于特权EXEC级别在特权EXEC级别下输入问号（？）比在用户EXEC级别下输入问号所得到的命令选项要多得多。

11.7 对Cisco IOS软件进行故障排除

一些情况会阻止路由器正确地启动：

- 缺少配置文件或者boot system语句不正确。
- 不正确的配置寄存器值。
- 受损的Flash映像。
- 硬件故障。

当路由器启动时，会在配置文件中查找boot system语句。这一语句能迫使路由器从另一个映像启动，而不是从Flash中的Cisco IOS软件映像启动。要明确启动映像的来源，可以输入show version命令，并查找标明映像启动来源的行，如例11-18所示。

例11-18 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
SOFTWARE (fc1)
```

错误的配置寄存器设定会组织Cisco IOS软件从Flash存储器正确地加载Cisco IOS软件。配置寄存器中的值告诉了路由器从何处获得Cisco IOS软件映像。这可以通过使用show version并查看针对配置寄存器的最后一行进行确认，如例11-19所示。

例11-19 配置寄存器

```
Cisco> show version
---- output omitted ----

Configuration register is 0x2102
```

在不同的硬件平台上，正确的值有所差别。Cisco IOS软件文档应该包括一份打印的show version命令的输出。如果没有文档，Cisco文档CD或者Cisco.com上也有资源能确定正确的配置寄存器值。可以通过在配置中改变配置寄存器的值，并将该值保存为启动配置来纠正配置寄存器的值。

如果仍存在问题，路由器的Flash映像文件可能受损。如果是这样，在启动过程中会显示一条错误消息。错误消息可能如下所示：

```
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:"d
```

如果Flash映像受损，需要上载一个新的Cisco IOS软件映像到路由器上。如果不是这部分的问题，则路由器可能存在硬件故障。如果是硬件故障，你需要联系Cisco技术援助中心（TAC）。尽管硬件故障很少见，但也是的确会出现的。

表11-4列出并描述了其他有用的路由器状态命令。你可以通过输入show命令，后跟一个空格和一个问号来列出所有的show命令。

表11-4 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、配置文件的名称和来源、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对堆栈的使用情况
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	显示所配置的所有接口的统计信息

11.8 总结

本章学习了以下知识点：

- 建立一个超级终端会话。
- 登录进入路由器。
- 使用命令行界面的帮助功能。
- 使用增强的编辑功能。
- 使用命令历史功能。
- 对命令的错误进行故障排除。
- 路由器可以启动进入ROM monitor模式、boot ROM模式或Cisco IOS模式。
- show version 和show flash 命令提供了关于当前路由器上Cisco IOS软件和配置寄存器设定的信息。
- 路由器命令需要在命令行界面（CLI）下的用户EXEC模式、特权EXEC模式、全局配置模式或者特定配置模式中输入。

作为对本章你所学内容的补充，请参考本书配套光盘中针对本章的视频、插图和e-Lab实验。

11.9 关键术语

Cisco互联网络操作系统软件（*Cisco Internetwork Operating System(IOS)软件*） 该软件作为映像文件存储在路由器上的Flash存储器中，当被加载到RAM中时，它提供运行在路由器上的操作系统。

命令行界面（*command-line interfaceCLI*） 使得用户能通过输入命令和可选的参数与操作系统交互的界面。

子卡（*daughter card*） 类似一个扩展卡，但能直接访问主板部件（内存和CPU），而不需要通过速度较慢的扩展总线发送数据。

Flash存储器（*Flash memory*） 一种特殊类型的EEPROM，可以按块而非字节为单位进行擦除和重新编程。许多现代的PC都将其BIOS保存在一个Flash存储器芯片上，以便能在需要时很容易地更新。Flash存储器在调制解调器上也很常见，因为它使得调制解调器生产厂商能在新协议标准化后就对其提供支持。

发光二极管（*light-emitting diode，LED*） 通过转换电能发光的半导体设备。硬件设备上的状态灯通常都是发光二极管。

非易失性RAM（*nonvolatile RAM，NVRAM*） 断电后仍能保持其内容的RAM。

加电自检（*power-on self-test，POST*） 当硬件设备加电后运行的一组硬件诊断程序。

11.10 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C “复习题答案。”

1. 路由器初始化时会完成下列那项？
   A. 加载NVRAM、setup程序和操作系统
   B. 加载自举程序、操作系统和配置文件
   C. 加载自举程序、setup程序和操作系统
2. 在路由器的setup过程中，哪个组合键可以用于退出该过程？
   A. Ctrl-A
   B. Ctrl-E
   C. Ctrl-C
3. 将右边的配置参数设定与左边这些建立一个超级终端会话所需的项进行匹配。
   A. 波特率　无[w1]
   B. 数据位　1
   C. 奇偶校验　8
   D. 停止位　无
   E..流控制　9600
4. 针对初始启动的输出，下列哪一项是正确的？
   A. 能看到路由器使用的Cisco IOS软件版本
   B. 不能看到路由器使用的Cisco IOS软件版本
5. 针对初始启动的输出，下列哪一项是正确的？
   A. 能看到Flash存储器的容量
   B. 不能看到Flash存储器的容量
6. 将左侧的命令与右侧的描述进行匹配。

Ctrl + a	退出配置模式
Ctrl + b	移动到命令行的末尾
Ctrl + e	向后移动一个词
Ctrl + f	移动到命令行的起始位置
Esc + b	向前移动一个字符
Esc + f	向前移动一个词
Ctrl + a	向后移动一个字符

7. 将左侧的命令与右侧正确的描述进行匹配。

Tab	启动高级编辑功能
Ctrl + p	设定命令缓冲区的大小
Ctrl + n	重用最近的命令
show history	显示命令缓冲区
terminal history size #	重用上一条命令
terminal editing	完成输入
no Terminal editing	禁用高级编辑功能

8. 典型路由器配置的主要元素包括：
   A. 口令、接口、路由选择协议、DNS
   B. 启动序列、接口、TFTP服务器、NVRAM

C. NVRAM、ROM、DRAM、接口

D. 接口、路由选择协议、配置寄存器、Flash存储器

9. 下列哪项正确地描述了一种用于指定路由器如何装载Cisco IOS软件的方法?

A. 在NVRAM中指定路由器可以使用的回退软件来源序列

B. 配置Cisco IOS软件映像，指定它启动的位置

C. 在虚拟终端上手工启动一个缺省的系统映像

D. 在网络服务器上手工启动一个缺省的系统映像

10. 下列哪项不是一个可以通过配置寄存器的启动字段设定的启动选项:

A. Cisco IOS软件在ROM monitor模式下启动

B. Cisco IOS 软件自动从ROM中启动

C. Cisco IOS软件自动从TFTP服务器上启动

D. 检查NVRAM中的boot system命令

11. 下列哪一项是通过Cisco IOS软件show version 命令显示的信息?

A. 关于路由器内存每个页面的详细统计信息

B. 系统映像的名称

C. Flash存储器中所有文件的名称和大小

D. 所配置的各种网络协议的状态

12. 下列哪一项中包含一个受限版本的路由器Cisco IOS 软件?

A. ROM

B. Flash 存储器

C. TFTP服务器

D. 自举程序

13. 如果你想彻底退出配置模式，需要输入下列哪一项?

A. Exit

B. no config-mode

C. Ctrl + e

D. Ctrl + z

14. 如果你计划配置一个接口，路由器应该处于哪个提示符?

A. router(config)#

B. router(config-in)#

C. router(config-intf)#

D. router(config-if)#

15. 下面哪个缩写用于描述Cisco路由器的基于文本的用户界面?

A. CLI

B. TCP/IP

C. OSPF

D. OSI

16. 对于Cisco路由器，存在哪两种访问路由器命令的模式?

A. 用户与特权

B. 用户与客户

C. 特权与客户

D. 客户与匿名

17. 在Cisco路由器上，你用哪种模式改变路由器的配置

A. 用户

B. 特权

C. 管理员

D. Root目标



第12章　路由器配置

目标

学习完本章之后，你应该能够：

- 为路由器命名。
- 设置口令。
- 研究show 命令。
- 配置一个串行接口。
- 配置一个以太网接口。
- 执行路由器变更。
- 保存路由器变更。
- 配置接口描述。
- 配置当日消息横幅。
- 配置主机表。
- 描述备份和文档。
- 口令恢复。

本章涉及各种路由器模式和更新路由器的配置文件时所使用的各种配置方法。深入理解Cisco IOS软件并了解路由器的启动过程是非常重要的。此外，本章还描述了进行口令恢复时所需要完成的任务。

请务必在本书配套的光盘中查看与本章相关的e-Lab实验、视频和插图。这些光盘资料提供了补充材料，能够强化本章中涉及的概念。

12.1　命令行用户界面的命令模式

要访问路由器，必须首先登录。登录后，需要进行模式选择。模式负责解释所输入的命令并执行相应的操作。有两种EXEC模式：

- 用户模式。
- 特权模式（或者enable模式）。

12.1.1 用户模式命令列表

用户首次登录到路由器时，自动进入用户EXEC模式。用户模式下可以对路由器进行有限的检查。表12-1提供了用户模式的命令和相应的描述。

表12-1 用户模式命令

命令	说明
access-enable	创建一条临时的访问列表条目
atmsig	执行有关ATM信令的命令
cd	改变当前的设备
clear	将函数复位
connect	新建一个终端连接
dir	列出给定设备上的文件
disable	退出特权模式
disconnect	关闭一个已经存在的网络连接
enable	进入特权模式
exit	退出EXEC
help	获得关于交互式帮助系统的描述
lat	新建一个LAT连接
lock	锁定终端
login	以特定用户登录
logout	退出EXEC模式
mrinfo	向组播路由器询问邻居和版本信息
mstat	显示多次组播路由跟踪后的统计信息
mtrace	跟踪从目的到源的反向组播路径
name-connection	为已经存在的网络连接命名
pad	新建一个X.29 PAD 连接
ping	发送echo 消息
ppp	启动IETF点到点协议（PPP）
pwd	显示当前设备
resume	继续一个活动的网络连接
rlogin	新建一个rlogin连接
show	显示运行系统的信息
slip	启动串行线路IP协议（SLIP）
systat	显示有关终端连接的信息
telnet	新建一个Telnet连接
terminal	设置终端连接的参数
tn3270	新建一个TN3270连接
traceroute	启动到目的地的路由跟踪
tunnel	新建一个隧道（tunnel）连接
where	显示所有地活动连接
X3在PAD	在PAD上设置X.3参数
Xremote	进入Xremote 模式

注释：此处所显示的命令列表是与上下文相关的。用户模式下的列表与enable模式下的不同；*全局配置模式*下的与*接口模式*下的也不同。

12.1.2 特权模式命令列表

特权EXEC模式下可以对路由器进行更为详细的检查，并允许对路由器的配置进行变更。根据所需要进行的配置变更，需要进入特定的模式。从特权EXEC模式可以进入其他模式；在进入其他

模式之前必须首先进入特权EXEC模式（见下一节，“路由器的配置模式”）。

要从用户EXEC模式进入**特权模式**，需要输入enable（或者缩写en）：

```
Router>enable
Password:

Router>en
Password:
```

该命令会提示你输入口令；如果你在特权模式提示符Router#下输入问号（?），屏幕会显示一个比用户模式下更长的命令列表。表12-2提供了一个特权模式命令的完整列表，其中包括对每个命令的描述。

注意，根据所配置的路由器平台的不同，该命令列表也有所差别。

表12-2 特权模式命令

命令	说明
access-enable	创建一条临时的访问列表条目
access-template	创建一条临时的访问列表条目
appn	向APPN子系统发送一条命令
atmsig	执行有关ATM信令的命令
bfe	设置手工紧急模式
calendar	管理硬件日历
cd	改变当前的设备
clear	将函数复位
clock	管理系统的时钟
cmt	启动或停止FDDI连接管理功能
configure	进入配置模式
connect	新建一个终端连接
copy	拷贝配置或映像数据
debug	使用调试功能（也见 undebug）
delete	删除一个文件
dir	列出给定设备上的文件
disable	关闭特权模式
disconnect	关闭一条已经存在的网络连接
enable	进入特权模式
erase	擦除闪存（Flash）或配置存储器
exit	退出EXEC模式
format	格式化某个设备
help	获得关于交互式帮助系统的描述
lat	打开一个LAT连接
lock	锁定终端
login	以特定用户登录
logout	退出EXEC
mbranch	沿树枝向下跟踪组播路由
mrbranch	沿树枝向上跟踪反向的组播路由
mrinfo	向组播路由器询问邻居和版本信息
mstat	显示多次组播路由跟踪后的统计信息
mtrace	跟踪从目的到源的反向组播路径
name-connection	为已经存在的连接命名
nica	启动/停止 NCIA 服务器
pad	新建一个X.29 PAD 连接
ping	发送echo 消息
PPP	启动IETF点到点协议（PPP）
pwd	显示当前设备

续表

命令	说明
reload	停止并执行冷启动
resume	继续一个活动连接
rlogin	打开一个rlogin连接
rsh	执行一个远程命令
sdlc	发送SDLC测试帧
send	在tty连接上发送消息
setup	启用setup命令配置工具
show	显示运行系统的信息
slip	启动串行线路IP协议（SLIP）
squeeze	挤压某个设备
start-chat	在一个连接上启动一个聊天脚本
Systat	显示有关终端连接的信息
tarp	目标ID解析过程（TRAP）命令
telnet	新建一个Telnet连接
terminal	设置终端连接的参数
test	测试子系统、内存和接口
tn3270	新建一个TN3270连接
traceroute	启动到目的地的路由跟踪
tunnel	新建一个隧道（tunnel）连接
undebug	停止调试功能（也见 debug）
verify	检查某个闪存文件的校验和
where	显示所有的活动连接
which-route	执行OSI路由表查找并显示结果
write	将当前运行的配置文件写入存储器、网络或终端
x3	在PAD上设置X.3参数
xremote	进入Xremote 模式

12.1.3　路由器的配置模式

路由器上的全局配置模式命令用于施加会影响整个系统的配置语句。使用特权EXEC命令configure 来进入全局配置模式。输入该命令后，会出现询问配置命令来源的提示符，你可以选择终端、nvram或者网络。缺省的选择是从终端控制台输入命令。按下回车键开始这种配置方式。

第一种配置模式被称为全局配置模式，或者简称为全局模式。表12-3描述了你能从全局配置模式访问的一些配置模式。

表12-3　路由器的配置模式

配置模式	提示符
接口（Interface）	Router(config-if)#
子接口（Subinterface）	Router(config-subif)#
控制器（Controller）	Router(config-controller)#
映射列表（Map-list）	Router(config-map-list)#
映射类（Map-class）	Router(config-map-class)#
连接（Line）	Router(config-line)#
路由器（Router）	Router(config-router)#
IPX-路由器（IPX-router）	Router(config-ipx-router)#
路由映射（Route-map）	Router(config-route-map)#

在这些特定的配置模式下输入exit能退回全局配置模式。按下Ctrl-Z彻底离开某个配置模式，返回路由器的特权EXEC模式。

例12-1演示了各种配置模式之间的切换。

例12-1 在特权EXEC模式、全局配置模式和特定配置模式之间切换

```
Router# configure terminal
Router(config)#(commands)
Router(config)# exit
Router#

Router#configure terminal
Router(config)# router protocol
Router(config-router)#(commands)
Router(config-router)# exit
Router(config)#interface type port
Router(config-if)#(commands)
Router(config-if)# exit
Router(config)# exit
Router#
```

12.1.4 路由器的启动模式

无论是从控制台访问，还是是通过虚拟类型终端（vty）端口的Telnet会话访问，路由器都可以被置为多种模式。每种模式都提供不同的功能。

• ROM monitor模式通常是一个恢复模式。它允许完成某些配置任务，比如恢复丢失的口令或者下载软件（IOS）。如果路由器没有找到有效的系统映像，或者在启动过程中启动序列被中断，路由器都会启动进入ROM monitor模式。在很多路由器上，Rommon>是ROM monitor模式的缺省提示符。

• Setup模式是一个帮助用户创建首次基本配置的会话。Setup模式由一系列的问题构成，每个问题后面的方括号内都有缺省的答案。Setup模式没有定义缺省提示符。如果没有找到有效的配置文件，路由器就会提示用户进入setup模式。也可以在特权模式下输入setup 进入Setup模式。注意，如果用户擦除了NVRAM并且重新启动了路由器，也可以手工进入setup模式。

• RXBoot模式是一个特殊的模式，使路由器进入该模式需要改变配置寄存器的设置并重启路由器。RXBoot模式为路由器提供了一个Cisco IOS 软件的子集，并进入一个简化的setup模式。简化的setup模式与标准的setup模式是有差别的，因为简化的setup模式不涉及全局路由器参数的配置，只提示配置接口参数，以便路由器能启动。这使得路由器无法在闪存中找到有效的Cisco IOS软件映像时也能启动。缺省的提示符是主机名后跟<boot>。

表12-4简要地描述了一些常用的配置命令。

表12-4 选择路由器的配置命令

命令	说明
configure terminal	从控制台终端手工配置路由器
configure memory	从NVRAM加载配置文件
copy tftp running-config	从网络中的TFTP服务器上加载配置文件
show running-config	显示RAM中的当前配置
copy running-config startup-config	将RAM中的当前配置保存到NVRAM中
copy running-config tftp	将RAM中的当前配置保存到网络中的TFTP服务器上
show startup-config	显示NVRAM中保存的配置的内容
erase startup-config	擦除NVRAM的内容

图12-1中显示的命令适用于运行11.0或更高版本Cisco IOS软件的路由器。

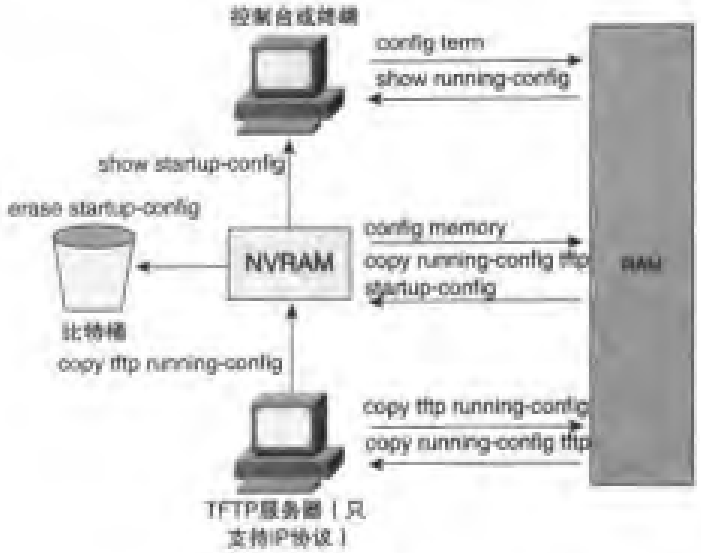


图12-1　关于配置文件的命令

12.2　配置路由器的名称

为路由器命名是最初的基本配置之一，如例12-2所示。通过为路由器命名，能惟一地标识网络中的每台路由器，以实现对网络更好的管理。在全局配置模式下完成对路由器的命名。路由器的名称被称为主机名，显示作为系统提示符。如果路由器尚未命名，系统提示符缺省为Router。

例12-2 为路由器命名

```
Router(config)#hostname Cougars
Cougars(config)#
```



实验活动　CLI模式和路由器标识

在本实验中，你将识别用户模式和特权模式这两种基本的路由器模式。你还会使用一些命令进入特定的模式，并输入各个模式的路由器提示符。此外，你还将为路由器命名。

12.3　配置并保护路由器的口令

用口令限制访问，可以保证路由器的安全。可以为虚拟终端连接和控制台连接设定口令。特权模式EXEC也有口令。

在全局配置模式下，用enable password命令可以限制对特权模式的访问。然而，这个口令是可以从路由器的配置文件中看到的。要在特权模式下输入加密的口令，需要使用enable secret命令。如果配置了enable secret口令，它就会替代enable口令。从配置文件中只能看到密文，不能看到实际的口令。

Enable secret口令是不可读的；另一个用户也许能非法获得配置文件，但所能做的事只是覆盖原有的口令，因为这是一种单向的加密，不能反向转换为明文。

通过service password-encryption 命令可以对口令的显示做进一步的保护。该命令是在全局配置模式下使用的。

line console 0 配置模式可以用于设定一个针对控制台终端的登录口令。这对于网络中有多人拥有对路由器访问权的情况是有用的。它能防止未经授权的用户访问路由器。

Telnet要求口令检查。不同硬件平台所定义的vty连接数是不同的。0到4用于标识5个vty连接。

这5个入向的Telnet会话可以是同时发生的。可以为所有的连接配置相同的口令，也可以为每个连接设定单独的口令。后者用于大型网络中有多个网络管理员的情况。如果网络中发生了灾难性的问题，并且所有公共的vty连接都被占用，那么一个独特的连接可以保留用于恢复。

用命令line vty 0 4 为各个入向的Telnet会话建立一个登录口令。例12-3演示了配置和保护口令的各种方式。

例12-3 配置/保护口令

```
! Console Password
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password cisco
! Virtual Terminal Password
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password cisco
! Enable Password
Router(config)# enable password san-fran
!Perform Password Encryption
Router(config)# service password encryption set password here
Router(config)# no service password encryption
```



实验活动 配置路由器的口令

本实验中，你会配置控制台口令、虚拟终端的口令和一个加密口令。

12.4 研究show命令

存在很多种的show命令，它们能帮助检查路由器中文件的内容，对故障排除也很有用。在路由器的各种模式下，show ?命令都可以用于显示所有可用的选项。表12-5列出了show命令的一些选项。

表12-5 show 命令

命令	说明
show interfaces	显示路由器上所有接口的统计信息。如果路由器管理员想查看某个特定接口的统计信息，则可以输入show interfaces 命令，后跟特定的接口或端口编号。例如：Router# show interfaces serial 1
show controllers serial	显示专门针对接口硬件的信息
show clock	显示路由器上的时间设定
show hosts	显示一个缓存的主机名和地址的列表
show users	显示连接到路由器的所有用户
show history	显示已经输入命令的历史
show flash	显示关于闪存的信息和其中所保存的Cisco IOS 软件文件的信息
show version	显示有关运行在RAM中的Cisco IOS 软件映像的信息
show arp	显示路由器的地址解析（ARP）表
show protocol	显示配置的所有3层协议的全局和特定接口的状态
show startup-configwration	显示NVRAM中包括的配置文件
show running-configwration	显示当前在RAM中运行的配置

例12-4、12-5和12-6分别显示了show protocols、show version以及show interfaces命令的示例输出。

例12-4 show protocols命令的输出

```
Router# show protocols
Global values:
Internet Protocol routing is enabled
DECnet routing is enabled
XNS routing is enabled
Vines routing is enabled
AppleTalk routing is enabled
Novell routing is enabled
--More--
Ethernet0 is up, line protocol is up
Internet address is 183.8.126.2, subnet mask is 255.255.255.128
DECnet cost is 5
XNS address is 3010.aa00.0400.0284
CLNS enabled
Vines metric is 32
AppleTalk address is 3012.93, zone ld-e0
Novell address is 3010.aa00.0400.0284
--More--
```

例12-5 show version 命令的输出

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M), Version 12.1.5
Copyright (c) 1986-1996 by Cisco Systems, Inc.
Compiled Fri 28-Jun-96 16:32 by rbeach
Image text-base: 0x600088A0, data-base: 0x6076E000
ROM: System Bootstrap, Version 5.1(1) RELEASE SOFTWARE (fc1)
ROM: 4500-XBOOT Bootstrap Software, Version 10.1(1) RELEASE SOFTWARE (fc1)
router uptime is 1 week, 3 days, 32 minutes
System restarted by reload
System image file is c4500-j-mz, booted via tftp from 171.69.1.129
--More-
```

例12-6 show interfaces 命令的输出

```
Router# show interfaces
Serial0 is up, line protocol is up
Hardware is MK5025
Internet address is 183.8.64.129, subnet mask is 255.255.255.128
MTU 1500 bytes, BW 56 kbit, DLY 20000 usec, rely 255/255, load 9/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

```
Last input 0:00:00, output 0:00:01, output hang never
Last clearing of show interfaces counters never
Output queue 0/40, 0 drops, input queue 0/75, 0 drops
Five minute input rate 1000 bits/sec, 0 packets/sec
331885 packets input, 62400237 bytes, no buffer
Received 230457 broadcasts, 0 runts, 0 giants
3 input errors, 3 CRC, 0 frame, 0 overrun, 0ignored, 0 abort
403591 packets output, 66717279 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets, 0 restarts
45 carrier transitions
```



实验活动 使用show 命令

本实验会帮助你熟悉路由器的show命令。show 命令是路由器上最重要的信息收集命令。

12.5 配置串行接口

通过控制台或者虚拟终端连接可以对串行接口进行配置。串行接口需要时钟信号来控制通信同步。在多数环境中，数据通信设备（DCE），比如信道服务单元/数据服务单元（CSU/DSU）提供该时钟。缺省时，Cisco路由器是数据终端设备（DTE），但可以被配置为DCE设备。

在直接相互连接的串行链路上，一侧必须作为DCE并提供时钟信号。通过clockrate命令激活时钟并设定其速率。可用的以“比特每秒”为单位的时钟速率为1200、2400、9600、19,200、38,400、56,000、64,000、72,000、125,000、148,000、500,000、800,000、1,000,000、1,300,000、2,000,000和4,000,000。然而，根据功能的不同，某些速率在某些串口上是不可用的。

要配置一个串口，需要完成下列的步骤，见例12-7：

步骤1 进入全局配置模式。

步骤2 进入接口模式。

步骤3 指定带宽。

步骤4 设定DCE时钟速率（在DTE上跳过此步）。

步骤5 开启该接口。

例12-7 配置一个串行接口

```
Router(config)# interface serial 1/0
Router(config-if)# bandwidth 56
Router(config-if)# clockrate 56000
Router(config-if)# no shutdown
```

缺省时，接口都是关闭的。要开启一个接口，必须输入命令no shutdown。在进行硬件维护、改变接口配置，进行故障排除或者其他维护时可能需要强制关闭某个接口。关闭一个接口的命令是shutdown。

下面这个命令强制关闭了一个接口：

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

下面这个命令启动了一个被关闭的接口：

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

下面这个命令推出了接口配置模式：

```
Router(config-if)# exit
```



实验活动 配置一个串行接口

本实验中，你将配置两个路由器上的串行接口，使得它们能相互通信。

12.6 配置以太网接口

可以从控制台端口或者虚拟终端连接配置以太网接口。每个以太网接口必须有一个IP地址和子网掩码。

要配置一个以太网接口，必须完成下列的步骤，见例12-8：

步骤1 进入全局配置模式。

步骤2 进入接口配置模式。

步骤3 指定接口地址和子网掩码。

步骤4 开启该接口。

例12-8 配置一个以太网接口

```
Router(config)# interface e0
Router(config-if)# 183.8.126.2 255.255.255.128
Router(config-if)# no shutdown
```

缺省时，接口都是关闭的。要开启一个接口，必须输入命令no shutdown。在进行硬件维护、改变接口配置、进行故障排除或者其他维护时可能需要强制关闭某个接口。关闭一个接口的命令是shutdown。



实验活动 配置一个以太网接口

在本实验中，你将配置一台路由器上连接到局域网的一个以太网接口和一个快速以太网接口。

12.7 执行路由器变更

如果需要对配置进行变更，需要进入适当的模式并完成变更。例如，如果一个接口没有开启，需要进入全局配置模式，然后进入接口模式，并执行no shutdown命令。

要验证所做的变更，可以使用命令show running-config。该命令能显示当前的配置。如果所显示的变量与设想的不一样，可以通过下面的方法进行纠正：

- 指定某个命令的no形式。
- 重启系统并从NVRAM加载原始的配置文件。
- 用erase startup-configuration 命令去除启动配置文件，重启路由器，然后进入setup模式。

要将所配置的变量保存到NVRAM的启动配置文件中。需要在特权EXEC提示符下输入下列命令：

```
Router# copy running-configuration startup-configuration
```

表12-6 显示了Cisco IOS 软件11.x或更高版本中用于管理NVRAM内容的命令。

表12-6 在Cisco IOS 软件11.x或更高版本中用于管理NVRAM内容的命令

命令	说明
configure memory	加载来自NVRAM的配置信息
erase startup-config	擦除NVRAM的内容
copy running-config startup-config	将RAM中的当前配置（即运行中的配置）保存到NVRAM中（作为启动配置）
show startup-config	显示所保存的配置，即NVRAM的内容



实验活动 改变配置

本实验中，你将改变某个路由器上的当前配置。你通过将某个接口关闭，然后备份来查看其状态。

12.8 结束配置

下面列出了用于结束配置的推荐任务（某些组织不具有某些推荐的配置任务，比如当 日消息）。

- 建立配置标准。
- 提供并配置接口描述。
- 配置登录横幅。
- 配置当日消息（MOTD）横幅。
- 进行主机名解析。
- 进行配置备份和文档说明。

12.8.1 配置标准的重要性

在一个组织内制定关于配置文件的标准是非常重要的。这能方便控制需要维护的配置文件的数量，这些文件是如何存储的，以及它们存放在什么地方。

标准是广泛使用或官方制定的一组规则或过程。如果一个组织内没有标准，当服务出现中断时网络就会陷入混乱。

要管理网络，就必须有集中的支持标准。为了使网络能平稳地运行，配置、安全性、性能和其他问题都必须充分地考虑。为网络的一致性建立标准有助于减少网络的复杂性，减少计划外的停工时间，减少可能影响网络性能事件的发生。

12.8.2 提供接口描述

接口描述信息应该用于标识重要的信息，比如远程的路由器、电路编号或者特定的网络分段。对于接口的描述有助于网络用户记住关于该接口的特殊信息，比如接口所服务的网络。下一节“配置接口描述信息”中提供了一个具体的例子。

描述信息只是作为对接口的注释。尽管描述信息出现在路由器内存的配置文件中，但并不影响路由器的运行。描述信息的创建需要遵循适用于每个接口的标准格式。描述信息可以包括接口的用途和位置，连接到接口的其他设备或其他位置，电路标识。描述信息使得支持人员能更好地了解与某个接口相关的问题范围，从而能更好地解决问题。

12.8.3 配置接口描述信息

进入全局配置模式配置接口描述信息。完成下列步骤，参见例12-9：

步骤1 输入命令configure terminal，进入全局配置模式。

步骤2　输入命令interface ethernet 0，进入特定的接口模式（例如，接口Ethernet 0）。

步骤3　输入命令description，后跟需要显示的信息（例如，XYZ Network,Building10）。

步骤4　按下Ctrl-z，从接口模式退回特权EXEC模式。

步骤5　用命令copy running-config startup-config，将配置变更保存到NVRAM。

例12-9　配置接口描述信息

```
Router(config)# interface ethernet 0
Router(config-if)# description SkyDome LAN Communication Building
Router(config-if)# exit
! Results of issuing the show running config command
interface Ethernet0
description SkyDome LAN Communication Building
ip address 198.133.215.1 255.255.255.0
```



实验活动　配置接口描述信息

本实验中，你将为接口选定描述信息，并使用接口配置模式来输入该描述信息。

12.8.4　登录横幅

登录横幅（login banner）是显示在登录时的消息。登录横幅对于传递影响所有网络用户的消息是很有用的，比如关于系统即将关闭的通知。

任何人都可以看到登录横幅。因此，对于其中的用词应该特别注意。“欢迎”表示邀请任何人进入路由器，这可能不是一个适合的消息。

登录横幅应该是对非授权登录尝试的警告。类似“这是一个安全系统，只允许授权访问”这样的消息，通知访问者，任何进一步的入侵或尝试都是不希望发生和违法的。例12-10显示了一个关于登录横幅的例子。

例12-10　登录横幅

```
Tokyo con0 is now available
Press RETURN to get started.

This is a secure system. Authorized Access ONLY!!!
User Access Verification

Password:
Tokyo>enable
Password:
Tokyo#
```

12.8.5　配置当日消息

当日消息（message-of-the-day，MOTD）或者登录横幅都能在连接的所有终端上显示。

进入全局配置模式，配置MOTD横幅。使用banner motd 命令，后跟一个空格和一个定界字符，比如井号（#）。添加当日消息，后跟一个空格和一个定界符。

完成下列步骤，创建并显示当日消息。参见例12-11：

步骤1 用命令configure terminal 进入全局配置模式。

步骤2 输入命令banner motd # The message of the day goes here #。

步骤3 用命令copy running-configuration startup-configuration，或简写为copy run start来保存所做的变更。

例12-11 MOTD显示

```
Tokyo(config)# banner motd #
You have entered a secure system, authorized access ONLY!#
```



实验活动 配置当日消息

在本实验中，你将用全局配置模式为路由器输入当日消息。这个过程使得所有的用户在进入路由器时都能看到该消息。

12.8.6 主机名解析

主机名解释是一个计算机系统用于关联主机名和网络地址的过程。

各种协议，比如Telnet，都能用主机名来识别网络设备。要用主机名与其他的IP设备通信，网络设备（比如路由器）必须能将主机名与IP地址关联。主机名和与之关联的IP地址的列表称为*主机表（host table）*。表12-7显示了一个示例的主机表。

表12-7 主机表

路由器名称	路由器类型	E0	E1	S0
Tokyo	2601	205.7.5.1	192.5.5.1	201.100.11.1
Paris	2621	205.7.5.2		204.204.7.2

主机表可能包括网络中所有的设备。每个惟一的IP地址都可以与一个主机名相关联。Cisco IOS软件维护了一个供EXEC命令使用的“主机名-地址”映射缓存。这个缓存加速了将名称转换为地址的过程。

与域名系统（DNS）的名称不同，主机名只在所配置的路由器上有效。例12-12显示了一台路由器上主机表的配置。

例12-12 主机表配置

```
Router(config)# ip host Auckland 172.16.32.1
Router(config)# ip host Beirut 192.168.53.1
Router(config)# ip host Capetown 192.168.89.1
Router(config)# ip host Denver 10.202.8.1
```

这个主机表使得网络管理员能输入主机名或者IP地址来Telnet到远端的主机。Auckland或IP地址172.16.32.1就是使用主机名的一个例子。要显示某台路由器上定义的关于主机和与之相关的IP地址的列表，需要使用命令show hosts。



实验活动 配置主机表

本实验中，你将使用全局配置模式来创建IP主机表，以使得路由器能将路由器名称转换为所连接的接口。

12.8.7　配置信息的备份和文档说明

网络设备的配置决定了网络工作的方式。管理设备的配置包括下列任务：

- 列出并比较运行设备的配置文件。
- 在网络服务器上存放配置文件。
- 进行软件安装和升级。

配置文件应该保存作备份文件，以备出现问题时使用。配置文件可以存储在网络服务器，比如TFTP服务器，或者存放在安全地点的磁盘上。对于这些离线信息应该包含文档说明。

路由器上的配置也可以通过捕捉文字的方式存放到磁盘，可以存放在软盘或硬盘上。如果需要将文件复制到别的路由器上，可以直接粘贴到别的路由器上。第14章“管理Cisco IOS 软件”中详细介绍了这些保存和存储路由器配置的方法。

图12-2显示了路由器配置过程的概况。

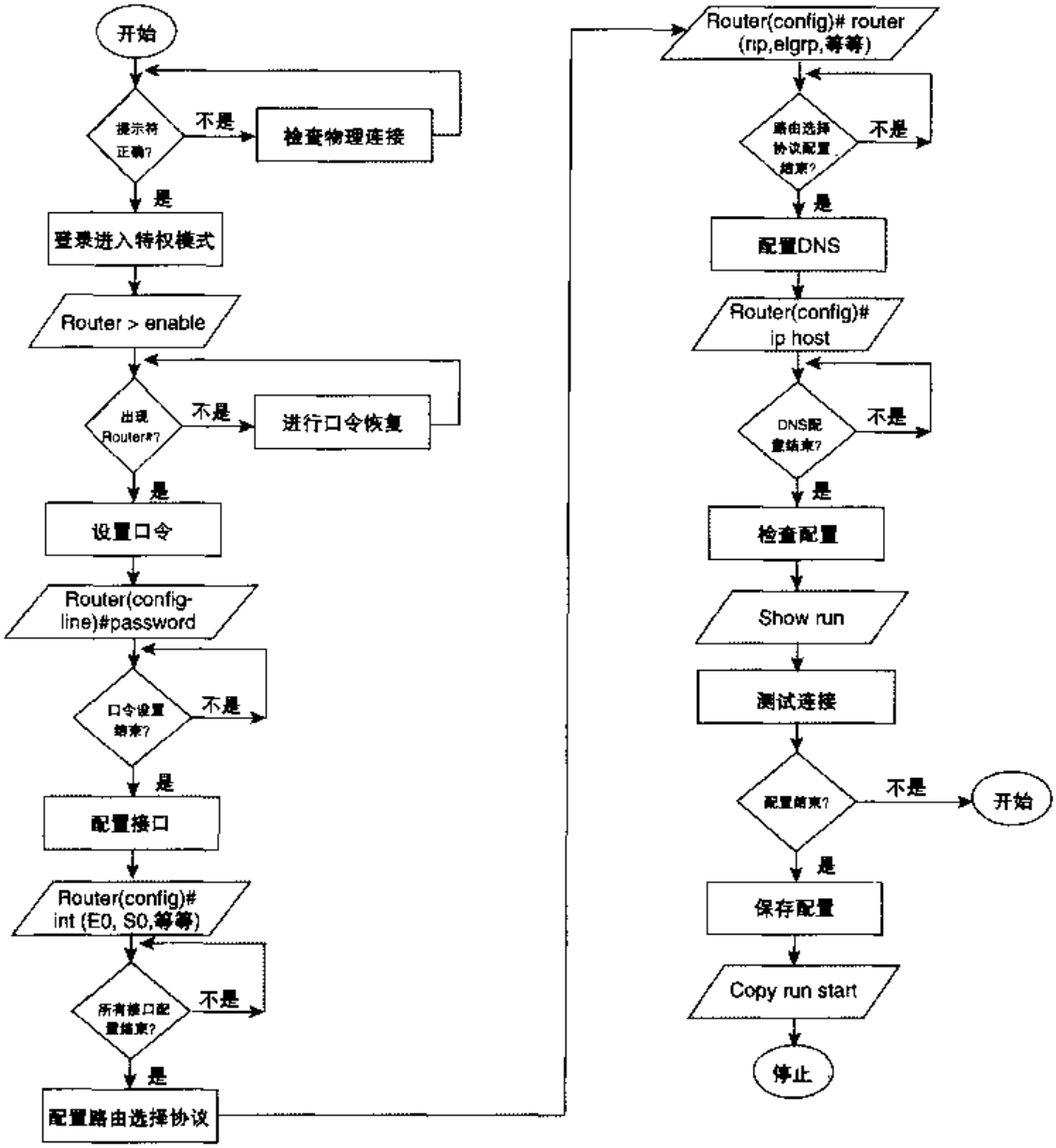


图12-2　路由器配置过程流程图

12.9　口令恢复

本节解释用于Cisco 路由器和Catalyst交换机的一些口令恢复技术。你可以在不改变硬件跳线的

情况下对绝大多数的设备进行口令恢复，但无一例外都需要将路由器重启。口令恢复只能从控制台端口进行（物理上连接到路由器）。

12.9.1 口令恢复概述

当口令丢失时，要访问路由器有三种方法。你可以查看口令，改变口令，或者清除配置然后完全重新开始。

每个过程都包含下面一些基本步骤：

步骤1 通过配置使得路由器启动时不读取配置存储器(NVRAM)。完成这项任务的模式被称为测试系统模式（test system mode）、ROM模式或boot模式。

步骤2 重新启动系统。

步骤3 进入enable模式（如果你在步骤1时正确地设定了配置寄存器的值，这将不需要口令）。

步骤4 查看或改变口令，或者清除配置。

步骤5 重新配置路由器，使之像正常情况一样在启动时读取NVARM中的配置。

步骤6 重新启动系统。

某些口令恢复过程需要终端发出BREAK信号；你必须熟悉如何用你的终端或者PC终端仿真程序发出这一信号。比如，在ProComm中，按下Break或者Ctrl-Break。Windows Terminal也允许你定义用于产生BREAK的功能键。在终端窗口中，选择“功能键”，通过输入字符串^$B（Shift+6、Shift+4和大写的B）定义功能键。从Internet上可以下载很多免费的终端仿真程序包，你可以从中选择喜欢的。

下面的几小节包含针对特定型号的Cisco 路由器的详细指令。在每节开始处查找你的设备，以确定使用哪种技术。

12.9.2 口令恢复技术1

该技术所针对的设备包括：

- Cisco 2500 系列。
- Cisco 3000 系列。
- ROM中运行Cisco IOS 10.0或更高版本的Cisco 7000 系列。

对于Cisco 7000和Cisco 7010系列，只有路由处理器（Route Processer，RP）卡上安装了Cisco IOS 10.0的ROM时，才能使用这一技术。可以是启动闪存中的Cisco IOS 10.0软件，但处理器卡上必须确实配有ROM。下列是口令恢复技术1的步骤：

步骤1 将终端或者配有终端仿真程序的PC连接到路由器的控制台端口。为了将PC机连接到控制台端口，需要在控制台端口上连接一个Null调制解调器适配器(Tandy 牌的Null调制解调器No.26-1496已经测试过)，然后用直连的调制解调器线缆连接到Null调制解调器适配器。

步骤2 输入show version命令，记录配置寄存器的设置。通常是0x2102或0x102。如果没有使用show version的提示符，可以从一台相似的路由器上获得配置寄存器的值，或者尝试使用0x2102。

步骤3 开关路由器。

步骤4 在上电后的60秒内，按下终端上的Break键。你将看到>提示符，没有路由器的名字。如果你无法看到这一提示符，终端就没有发送正确的BREAK信号，需要检查终端或者终端模拟程序的设置。

步骤5 在>提示符下输入o/r 0x42，使路由器从闪存中启动，或者输入o/r 0x41，使路由器从ROM中启动。如果系统配有闪存，并且没有受到损坏，0x42是最好的设置，因为这是默

认值。只有在闪存中的内容被擦除或者没有闪存的情况下，才使用0x41。如果你使用0x41，你可以查看口令或者清除配置文件，但不能改变口令。

步骤6　在>提示符下输入i。路由器会重新启动，并忽略自身保存的配置。

步骤7　对所有setup模式下的问题回答no，或者按下Ctrl + C。

步骤8　在Router>提示符下输入enable。你将处于enable模式，能看到提示符Router#。

步骤9　从下列三种选择中选出一项：

- 输入show start查看口令。
- 要改变口令（例如在口令加密时使用），步骤如下：

  a 输入copy start run 将NVRAM中的内容复制到内存中。

  b 输入show run。

  c 如果你已经设置了enable secret Password，执行以下步骤：

  输入 config term，进行变更。

  输入 enable secret *new_password*。

  按下 Ctrl-Z。

  d 如果没有设置enable secret xxxx，输入*enable password new_password*，按下Ctrl-Z。

  e 输入copy run start来保存更改

- 要删除配置文件，输入erase start。

步骤10　在提示符下输入config term。

步骤11　输入config-register 0x2102，或在步骤2中记录的其他值。

步骤12　按下Ctrl-Z，返回特许EXEC模式。

步骤13　在提示符下输入reload。不必写存储器。

12.9.3　口令恢复技术2

该过程能为下列的路由器恢复口令：

- Cisco 1003。
- Cisco 1600 系列
- Cisco 2600 系列。
- Cisco 3600 系列。
- Cisco 4500 系列。
- Cisco 7100 系列。
- Cisco 7200 系列。
- Cisco 7500 系列。
- IDT 基于Orion的路由器
- AS5200和AS5300 平台

用过程2进行口令恢复的步骤如下：

步骤1　将终端或者配有终端仿真程序的PC连接到路由器的控制台端口。

步骤2　输入show version命令，记录配置寄存器的设置。通常是0x2102或0x102。

配置寄存器的值显示在最后一行。注意查看配置寄存器是被设为“enableBreak”还是“disableBreak”。

步骤3　关闭路由器然后再次开启。

步骤4　在上电后的60秒内，按下终端上的Break键。你将看到rommon>提示符。如果你无法看到这一提示符，那么终端就没有发送正确的BREAK信号。

如果没有出现该提示符，需要检查终端或者终端模拟程序的设置。

步骤5 在rommon>提示符下输入confreg。

出现下面的提示：

```
Do you wish to change configuration?y/n]?
```

步骤6 回答yes并按回车。

步骤7 对后续的问题都回答no，直到出现下面的 提示：

```
Ignore system config info?y/n]?
```

步骤8 输入yes

步骤9 对后续的问题都回答no，直到出现下面的提示：

```
Change boot characteristics?y/n]?
```

步骤10 输入yes。

会出现下面的提示：

```
enter to boot
```

步骤11 在此提示符下，如果从闪存启动则输入2并按回车，如果闪存被擦除则输入1。

如果闪存的内容被擦除，Cisco 4500必须送到Cisco公司完成口令恢复。如果你输入1，你只能查看或者删除配置，不能改变口令。

将显示配置总结，并出现下面 的提示信息：

```
Do you wish to change configuration? y/n]?
```

步骤12 输入no 并按回车。

出现下面的提示符：

```
rommon>
```

步骤13 在特权EXEC模式下输入reset，或者对于Cisco 4500系列和Cisco 7500系列，关闭路由器并重新开启。

步骤14 在路由器启动过程中，对所有的setup问题都回答no，直到出现下面的提示符：

```
Router>
```

步骤15 输入enable进入enable模式。

出现提示符Router#。

步骤16 选择下列的选项之一：

- 要查看口令，如果没有加密，输入more nvram:startup-config。
- 要改变口令（例如，如果口令是加密的），输入下列命令：

```
Router# configure memory
Router# configure terminal
Router(config)# enable secret 1234abcd
Router(config)# ctrl-z
Router# write memory
```

enable secret命令通过用不可逆的加密函数存放enable secret口令，提供了更强的安全性；然而，如果一丢失的口令被加密，你将不能恢复该口令。

步骤17 在提示符下输入configure terminal。

步骤18 输入config-register，和你在步骤2中记录的值。

步骤19 按下Ctrl-Z 退出配置编辑器。

步骤20 在提示符下输入reload，并输入write memory来保存配置。



实验活动　口令恢复过程

本实验中，你将在路由器口令未知的情况下获得对路由器的访问权。

12.10　总结

本章学习了配置路由器的一些知识点：

- 路由器有多种模式：
  - ——用户模式
  - ——特权模式
  - ——全局配置模式
  - ——其他配置模式
- 命令行界面（CLI）用于改变配置，包括下列功能：
  - ——设定主机名
  - ——设定口令
  - ——配置接口
  - ——修改配置
  - ——显示配置
- 接口描述信息包括用于帮助网络管理员理解网络并对网络进行故障排除的重要信息。
- 登录横幅和当日消息在用户登录到路由器时为其提供了信息。
- 主机名解析将名字转换为IP地址，使得路由器能快速地将名称转换为地址。
- 口令丢失时，有三种方式可以重新获得对路由器的访问：
  - ——可以查看口令。
  - ——可以修改口令。
  - ——可以清除配置，然后重新开始，就好像设备是新的一样。
- 任何组织要实现维护高效网络的目标，配置标准都是十分关键的要素。配置的备份和文档说明对于保证网络平稳运行是极其重要的。

为了补充你在本章所学的知识，请参考本书配套光盘中对应章节的视频、插图和e-Lab实验活动。

12.11 关键术语

命令行界面（*command-line interface，CLI*） 使得用户能通过输入命令和可选参数与操作系统交互的界面。

全局配置模式（*global configuration mode*） 用于单行命令和完成对路由器配置进行全局变更的命令。

接口（*inerface*） 两个系统或设备之间的连接。按路由选择的术语，就是一个网络连接。

非易失性RAM（*Nonvolatile RAM，NVRAM*） 断电后仍能保持其内容的RAM。

特权模式（*privileged mode*） 用于复制和管理整个配置文件。

小文件传输协议（*Trivial File Transfer Protocol，TFTP*） 简单版本的FTP，使得文件能通过网络从一台计算机传送到另一台计算机，通常不使用客户身份验证（比如，用户名和口令）。

12.12 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 什么是标准？
   A. 管理网络设备如何交换信息的一套规则和惯例的正式描述
   B. 广泛使用或者官方规定的一套规则或规程
   C. 网络设备访问网络介质的一种方式
2. 接口上描述信息的用途？
   A. 欢迎用户访问路由器
   B. 警告用户不要进入路由器
   C. 显示关于接口的注释信息
3. 哪一项是一个好的登录横幅？
   A. 欢迎每个人
   B. 任何人请登录
   C. 只允许授权的访问
4. 什么是主机名解析？
   A. 将名称与网络位置相关联的过程
   B. 显示登录消息的过程
   C. 显示关于路由器的描述信息的过程
5. 配置备份和文档说明对组织维护一个高效网络是必需的。正确还是错误？
   A. 正确
   B. 错误
6. 配置文件的备份不是必需的。正确还是错误？
   A. 正确
   B. 错误
7. TFTP服务器是备份文件惟一能存放的位置。正确还是错误？
   A. 正确
   B. 错误
8. 如果你计划配置一个接口，应该在哪种提示符下进行？
   A. router(config)#
   B. router(config-in)#
   C. router(config-intf)#
   D. router(config-if)#
9. 下列哪一项是配置路由器过程的正确顺序？（假设你已经在配置模式下对路由器进行了变更。）
   A. 保存变更到备份，决定变更是否是想要的结果，检查结果，检查备份文件
   B. 检查结果，决定变更是否是想要的结果，保存变更到备份，检查备份文件
   C. 决定变更是否是想要的结果，检查备份文件，保存变更到备份，检查结果
   D. 检查结果，保存变更到备份，决定变更是否是想要的结果，检查备份文件
10. 下列哪项命令能用于将路由器配置保存到备份？
    A. Router# **copy running-config tftp**
    B. Router# **show running-config**
    C. Router# **config mem**
    D. Router# copy tftp running-config

11. 下列哪项正确地描述了路由器上口令的配置?
A. 所有口令都是在用户EXEC模式下设定的
B. 所有口令都会修改实际的口令字符串
C. 可以为所有的入向Telnet会话设定相同的口令
D. enable口令限制了对用户EXEC模式的访问
12. 下列哪一项没有正确描述[w6]路由器上的口令配置?
A. 每个配置模式下都可以设定口令
B. 可以在任何的控制台连接上设定口令
C. enable secret口令使用一个加密过程来修改口令字符串
D. 所有口令的设定都是在全局配置模式下开始的
13. 哪种模式用于改变整个路由器的单行命令?
A. 全局配置模式
B. 特权模式
C. 用户EXEC模式
D. 接口模式
14. 在提示符为Router(config-if)#的配置模式下，exit命令的作用是什么?
A. 退出当前的接口配置模式
B. 到达特权EXEC提示符
C. 退出路由器
D. 切换到用户EXEC提示符
15. 哪些是典型路由器配置的要素?
A. 口令、接口、路由选择协议、DNS
B. 启动序列、接口、TFTP服务器、NVRAM
C. NVRAM、ROM、DRAM、接口
D. 接口、路由选择协议、配置寄存器、闪存
16. 口令恢复过程中，在路由器启动时执行Ctrl-Break后，紧接着配置寄存器的设置应该为多少?
A. 0x2102
B. 0x2142
C. 0x0000
D. 0x10F
17. 在口令恢复过程中，在保存运行配置之前，在启用新的加密口令之后，配置寄存器的值应该是多少?
A. 0x2102
B. 0x2142
C. 0x0000
D. 0x10F



第13章　邻居和远程设备的学习

目标

学习完本章之后，你应该能够：

- 描述如何执行、监控和维护CDP（Cisco发现协议）。
- 理解如何创建环境的网络映像。
- 禁用CDP和对CDP的故障排除。
- 远程登录（Telnet）到其他路由器。
- 检验、断开和挂起远程登录（Telnet）连接。
- 操作其他的连接测试。

在本章中，将学习到如何通过使用正确的路由器命令执行、监控和维护Cisco发现协议（Cisco Discovery Protocol，CDP）。除此之外，本章还将讲解常用于排除与地址相关故障的命令。

请务必在本书配套的光盘中查看与本章相关的e-Lab实验活动、视频和插图。这些光盘资料提供了补充材料，能够强化本章中涉及的概念。

13.1　CDP介绍

Cisco发现协议（*CDP*）是第2层协议，该层连接底层的物理介质和上层的网络层协议，如图13-1所示。CDP用来获得邻居设备信息。这些信息包括被连接设备的类型、连接到的路由器的接口、本地的连接接口和设备的模块数量。CDP运行在所有Cisco设备上，独立于介质和协议，位于**子网访问协议**（*SNAP*）之上。CDP是Cisco网络设备的专有协议，也只能运行在Cisco的网络设备上。

CDP版本2（CDPv2）是这个协议的最新版本。Cisco的IOS 12.0(3)T版本及以后的版本都支持CDPv2。Cisco IOS 10.3版本及以后的版本缺省支持CDP版本1（CDPv1）。



图13-1　CDP的适用位置

当Cisco设备启动后，CDP自动开始运行，检测已运行CDP的邻居设备。CDP运行在数据链路层上，它允许采用不同网络层协议的两个系统也可以彼此学习。

配置了CDP的设备周期性发送消息（即通告）给多个路由器。每个设备至少通告一个地址，在这个地址上它能够接收**简单网络管理协议**（*SNMP*）消息。这个通告中当然也包括生存时间（TTL）和保持时间（holdtime）的信息。这个保持时间信息是表示接收通告的设备在丢弃CDP信息之前持有该信息的时间。除此之外，每个设备都会侦听由其他路由器周期发送的CDP消息，来学习邻居设备。

13.1.1　通过CDP获得信息

CDP的主要作用就是来发现所有与本地设备直接连接的Cisco设备。CDP帧虽然小，但从中可以获得很多关于邻居路由器和交换机的有用信息。可以使用show cdp entry [*device name*]命令显示缓存的单条CDP信息，如例子13-1所示。

例13-1　show cdp entry命令输出

```
routerA# show cdp entry routerB
-------------------------
Device ID: routerB
Entry address (es):
IP address: 198.92.68.18
Platform: 2501, Capabilities: Router
Interface: Ethernet1, Port ID (outgoing port): Ethernet0
Holdtime: 155 sec
--- output omitted ---
```

注意，这条命令的输出包含了在邻居路由器（Router B）中出现的所有第3层地址。管理员在Router A上使用这条命令，就能看见目标CDP邻居（Router B）的IP地址。保持时间值指示包含此信息的CDP帧从到达至今的时间。show cdp entry [*device name*]命令包含了Router B的简短版本信息。知道了邻居设备的版本信息，就可以从中获得准确的物理拓扑结构，进而正确地配置设备。

13.1.2　显示CDP的邻居

图示13-2显示一个CDP如何把自己收集的信息发送给网络管理员的例子。每个运行CDP的路由器与自己的邻居交换协议信息。网络管理员可以将CDP信息交换的结果显示在连接到本地路由器的控制台上。

使用show cdp neighbors命令可以显示与路由器直接相连接的网络的信息。CDP通过传送*类型长度值*（*TLV*）的方式，提供每个CDP邻居的信息。TLV是内含在CDP通告中的一组信息。

使用show cdp neighbors命令可以显示设备的TLV，如例13-2所示，详细信息如下：

- 设备标识（ID）。

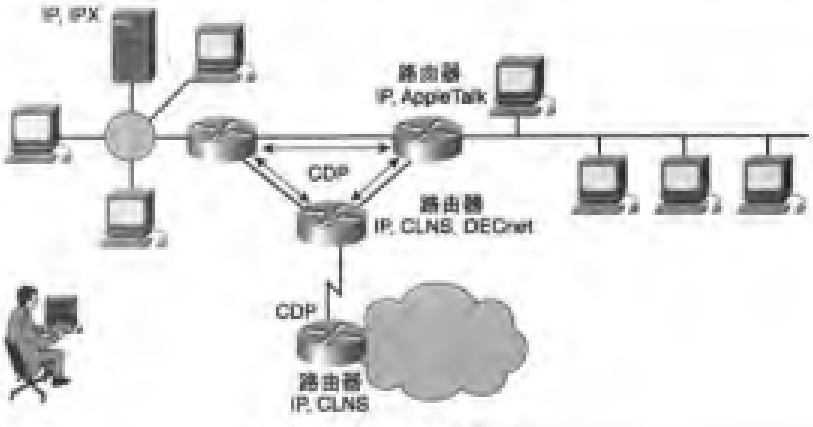


图13-2　CDP邻居

- 本地接口。
- 保持时间。
- 功能。
- 平台。
- 端口标识（ID）。
- VTP管理域名（只适用于CDPv2）。
- 本地VLAN（只适用于CDPv2）。
- 全双工/半双工（只适用于CDPv2）。

例13-2 show cdp neighbors命令输出

```
routerA# show cdp neighbors
Capability Codes:
R ®C Router, T ®C Trans Bridge,
B ®C Source Route Bridge,
S ®C Switch, H ®C Host, I ®C IGMP

Device ID    Local Interface    Holdtime    Capability    Platform    Port    ID
routerB      Eth 0              151         R             2501        Eth     0
routerB      Ser 0              165         R             2501        Ser     0
```

为了在show cdp neighbors的输出中显示与show cdp entry命令类似的所有信息，可以选用show cdp neighbors detail命令，如例13-3所示。

例13-3 show cdp neighbors detail命令输出

```
routerA# show cdp neighbors detail
Device ID: routerB
Entry address(es):
IP address: 198.92.68.18
Platform: 2501, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): Ethernet0
Holdtime: 143 sec
```

注意，在图13-2中，最下方的路由器并没有与管理员的控制台路由器直接连接。为了获得关于这台设备的CDP信息，管理员需要远程登录到与之直接连接的路由器上。正如前面所说的一样，所得到的信息将会有助于获得网络上设备的所有概况，更好地帮助理解物理拓扑结构。

13.1.3 执行、监控和维护CDP信息

表13-1中的命令是用来执行、监控和维护CDP信息的命令。

使用cdp run命令是在路由器上全局启用CDP。缺省方式下CDP是全局启用的。使用cdp enable命令是在特定接口上启用CDP。在Cisco IOS 10.3版本或之后的版本中，可以在设备的每个接口上使用cdp enable命令启用CDP。尽管在大多数Cisco设备中CDP是缺省启用的，仍然可能遇到某些需要基于接口的手工启用CDP的情况。这种手工启用的例子会发生在不支持cdp run命令的1900系列交换机上。1900系列的交换机需要基于接口的启用的或禁用 CDP。另一些例子是某些特定接口出于安全目的而不启用CDP。

表13-1　CDP命令

命令	模式	说明
cdp run	全局配置模式	在路由器上全局启用CDP
cdp enable	接口配置模式	在接口上启用CDP
clear cdp counters	特权EXEC模式	将CDP流量计数器值复位为0
show cdp	特权EXEC模式	显示CDP通告的发送间隔、特定端口上CDP通告的有效秒数和通告版本
show cdp entry {*entry-name* [protocol | version]}	特权EXEC模式	显示指定邻居的信息，可以将显示限制为协议或版本信息
show cdp interface [*type number*]	特权EXEC模式	显示启用了CDP的接口的信息
show cdp neighbors [*type number*] [detail]	特权EXEC模式	显示被发现的设备类型、设备名称、本地接口（端口）的数量和类型、该端口CDP通告的有效秒数、设备型号、设备产品编号和端口ID。使用关键字detail可以显示本地VLAN ID信息、双工模式和与邻居设备相关联的VLAN中继协议（VTP）域名

使用show cdp interface命令可以获取CDP用于其通告和发现帧传输的信息。例13-4显示了该命令的一些输出示例。这些信息能够帮助提供详细的信息，比如保持时间、CDP分组发送频率、接口封装时间以及接口的管理和协议情况。

例13-4　show cdp interface命令输出

```
routerA# show cdp interface
Serial 0 is up, line protocol is up, encapsulation is Frame Relay
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Ethernet0 is up, line protocol is up, encapsulation is ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
```

13.1.4　创建环境的网络映像

CDP被设计、实现成一个简单的低开销协议。通过非常小的CDP帧，CDP能够获得关于相连邻居路由器的大量有用信息。

show cdp neighbors命令可以用来获得以下信息：

- 设备ID。
- 地址。
- 端口ID。
- 功能。
- 版本。
- 硬件平台。
- IP网络前缀。
- VTP管理域名（只适用于CDPv2）。
- 本地VLAN（只适用于CDPv2）。
- 全双工/半双工（只适用于CDPv2）。

这些信息可以用来创建相连设备的网络映像。可以通过Telnet登录到邻居设备上来发现与邻居相连接的设备。使用show cdp neighbors detail命令可以发现与邻居相连的设备。

13.1.5 禁用CDP和CDP故障排除

如前所述，缺省方式下CDP是全局启用 的。要在全局级别下禁用CDP，应在全局配置模式下使用no cdp run命令。如果CDP被全局禁用，那么接口上也不能启用CDP。例如，出于安全目的而不希望使用某个设备的信息时，就可以禁用该设备的CDP。

在Cisco IOS 10.3版本和之后的版本中，每个接口上的CDP缺省被禁用。必须使用cdp enable命令启用CDP，来发送和接收CDP消息。在接口配置模式下使用no cdp enable命令禁用指定接口上已启用的CDP。表13-2列举并描述了可以用来显示版本、更新信息、表格和流量的故障排除命令。

表13-2 CDP故障排除命令

命令	说明
clear cdp table	删除CDP表中的邻居信息
clear cdp counters	将CDP流量计数器值复位为0
show cdp traffic	显示CDP计数器值，包括发送、接收和校验和错误的分组个数
show debugging	显示路由器上启用的调试类型信息
debug cdp adjacency	显示CDP邻居信息
debug cdp events	显示CDP事件信息
debug cdp ip	显示CDP IP信息
debug cdp packets	显示CDP与分组相关的信息
cdp timers	指定Cisco IOS软件发送CDP更新的时间
cdp holdtime	指定接收设备在丢弃CDP分组前，保持这个信息的时间
show cdp	显示CDP更新分组的信息

实验活动 使用CDP创建网络映像

在本活动中，使用CDP命令获取邻接网络和路由器的信息。

实验活动 CDP邻居

在本活动中，使用CDP命令获取邻接网络和路由器的信息，显示如何配置CDP来传输其通告和发现帧。

13.2 获取远程设备的信息

本节描述用来获取远程设备信息的远程登录（Telnet）、*ping*和*traceroute*，如图13-3所示。

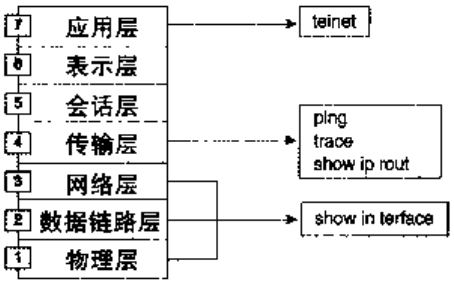


图13-3 测试流程概况

13.2.1 远程登录（Telnet）

Telnet是TCP/IP协议集中的一个虚拟终端协议。Telnet允许连接远程主机，并允许一个网络终端远程登录该主机。telnet是Cisco IOS软件的EXEC命令，用来检测源和目的间的应用层软件。这个命令是最全面的可用测试机制。

Telnet运行在OSI模型的应用层，在客户机和服务器之间依靠TCP来保证数据的正确和按序交付。

一个路由器可以有多个同步的入向Telnet会话，值0到4定义了5条vty或Telnet连接。这5条入向的Telnet会话可以在同一时刻发生。

检测应用层的连通性是Telnet的一个附带功能。Telnet的主要作用是连接远程网络设备，例如路由器、交换机和服务器，来收集信息或进行维护。它是一个简单而通用的应用程序。

建立和检测Telnet连接

Cisco IOS软件的EXEC命令telnet允许用户从一个Cisco设备Telnet到另一个设备。在Cisco实现

的TCP/IP中，不需要输入命令connect或telnet来建立Telnet连接，只需要输入远程路由器的主机名或IP地址即可。要终止一个Telnet会话，则使用EXEC命令exit或logout。图13-4显示了一条Telnet连接的开始和终止。

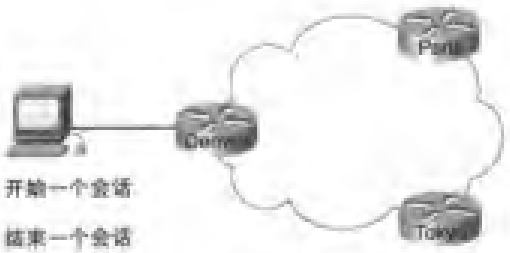


图13-4　Telnet操作

在Telnet会话中使用名字时必须为Telnet提供一张主机名表或访问DNS，否则只能使用主机的IP地址。开始一个Telnet会话，可以使用以下方法之一：

```
Denver>connect paris
Denver>paris
Denver>131.108.100.152
Denver>telnet paris
```

Telnet可以用来检测确定能否访问远程路由器。如图13-5所示，如果Telnet成功地将York路由器连接到Paris路由器，那么该网络连接的基本测试即为成功。这个操作可以在用户或特权EXEC模式下执行。

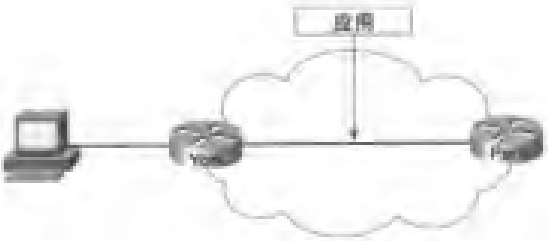


图13-5　测试应用层

如果能够远程访问另一个路由器，那么至少有一个TCP/IP应用可以到达远程路由器。一个成功的Telnet连接显示了高层应用运行正确。

如果能够成功Telnet到一台路由器，却不能Telnet到另一台路由器上，那么失败的原因可能是特殊地址、名字或访问权限的问题。而且，这些问题可能存在于源路由器或Telnet的目的路由器上。因此，下一步就是尝试本章稍后介绍的ping。ping允许在网络层上测试端到端的连接。

一旦完成Telnet，就要退出主机。缺省方式下如果连接空闲10分钟，EXEC会自动终止该连接；或者还可以在EXEC提示符下输入exit命令来终止连接。

实验活动　建立并检测一条Telnet连接

在本活动中，建立与远程路由器之间的Telnet连接，并收集该路由器的信息。

高级Telnet操作

如果同时打开了多个Telnet会话，可以在这些会话之间进行切换。session limit命令定义了允许同时打开的会话个数。

从一个会话切换到另一个会话的命令如下：

- Ctrl + Shift + 6，然后键入字母x——离开当前连接，返回到EXEC提示符。
- resume——获得该连接。

在EXEC提示符下可以获得一个新的连接。大多数路由器限制同时发生的会话数为5个。

使用Ctrl + Shift + 6，然后键入字母x，可以使用和挂起多条Telnet会话。会话的恢复可以使用回车键。如果使用回车键，Cisco IOS软件将恢复最近被挂起的那条Telnet连接。resume命令的使用需要一个连接ID，使用Show session（TNR）命令可以显示所有已被打开的会话的连接ID。

实验活动　结束和挂起一个Telnet会话

在本活动中，建立与远程路由器之间的Telnet连接，临时挂起然后恢复该会话。

实验活动　高级Telnet操作

在本活动中，使用telnet命令远程访问其他路由器，检测源和目的之间应用层的正常运行。挂起一个Telnet会话，并执行其他多个Telnet会话；然后返回被挂起的会话并结束该会话。

13.2.2 其他的连通性测试

以下几小节包含一些用来测试并检查设备之间连通性的命令。本节描述的工具和命令如下：

- ping
- traceroute
- show ip route
- show interfaces serial
- show interfaces/clear counter
- debug

ping命令

许多网络协议都支持一种用来诊断基本网络连通性的echo协议。echo协议用来测试协议分组是否被路由。

ping命令向目的主机发送一个分组，然后等待一个来自该主机的应答分组。echo协议的结果可以有助于评估到目的主机的路径的可靠性、路径延迟以及该主机是否能够到达或是否正在运行。这个命令是一个基本测试机制，其操作可以在用户或特权EXEC模式下执行。

用户EXEC模式下的ping命令可以用来诊断基本的网络连通性。ping命令的使用如下：

1.ping目的主机的IP地址或名字。

2.按回车键。

表13-3显示了Cisco **ping**命令的返回代码。ping使用的是Internet控制消息协议（ICMP）。

表13-3 Cisco ping命令的返回代码

代码	含义	可能的原因
!	每个惊叹号代表接收到一个ICMP回应应答	ping成功完成
.	每个句号表示等待一个应答时网络服务超时	这个消息可能表示以下问题：ping被访问列表或防火墙阻隔；路径上的一台路由器没有到达目的主机的路由，也没有发送ICMP目的不可达消息；路径上的某处发生了物理连接问题
U	收到一条ICMP不可达消息	路径上的一台路由器没有到达目的主机的路由
C	收到一条ICMP源抑制消息	路径上的一台设备——可能是目的主机——收到过多的流量；检查输入队列
&	收到一条ICMP超时消息	可能发生路由环路

图13-6是ping工作的一个简单示意图。

图13-6中ping的目标172.16.1.5对5个发送的数据报进行了成功的响应，显示如下：

```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

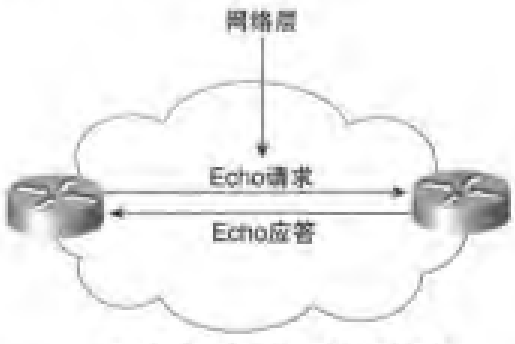


图13-6 使用ping命令的测试

惊叹号（！）表示每个成功的回应。如果显示中收到的惊叹号被一个或多个句号（.）代替，则表示该路由器上的应用等待来自ping目标的特定分组回应时已经超时。

实验活动　其他的连通性测试（ping）

在本活动中，使用ping命令向目标的主机发送ICMP数据报，检测源和目的之间网络层的正常运行。根据返回的信息评估到目标主机的路径的可靠性，确定路径延迟，并确定该主机是否能够到达或是否正在运行。

traceroute命令

traceroute命令（简写为trace）是一个用来查找数据正从网络中的什么地方发送出去的理想工具。traceroute命令与ping命令类似，只是traceroute测试路径中的每一步，而不是测试端到端的连通性。这个操作可以在用户或特权EXEC模式下执行。

traceroute命令的使用如下：

1. traceroute目的IP地址或名字。
2. 按回车键。

表13-4显示了Cisco traceroute命令的返回代码。

表13-4　Cisco traceroute命令的返回代码

代码	含义	可能原因
nn msec	提供了特定数量探测包到达各个节点间的往返时间（毫秒为单位）	正常
*	探测包超时	路径中的一台设备没有收到探测或者没有用ICMP“包生命周期超时包（packet life exceeded）”消息进行响应
A	强制进制	路径中的一台设备，比如一台防火墙或路由器，可能阻塞了探测包和其它的或所有的通信；检查访问列表。
Q	源端抑止	路径中的一台设备可能收到了太多的通信；检查输入队列。
H	收到了一条ICMP不可达消息	可能出现了路由选择环路

图13-7　是traceroute工作的一个简单示意图。

在这个例子中，从约克（York）到罗马（Rome）的路径跟踪结果如下：

```
York# trace Rome
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
1 LONDON (172.16.12.3) 1000 msec 8 msec 4 msec
2 PARIS (172.16.16.2) 8 msec 8 msec 8 msec
3 ROME (172.16.35.5) 8 msec 8 msec 4 msec

York#
```

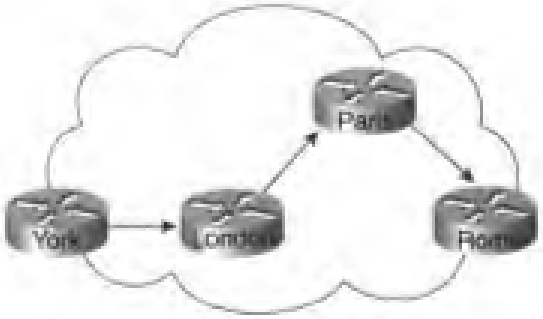


图13-7　traceroute命令

该路径必须经过伦敦（London）和巴黎（Paris）。如果其中任何一台路由器无法到达，将返回3个星号（*）来取代该路由器的名字。traceroute命令会继续尝试到达下一步直至使用Ctrl-Shift-6。

traceroute命令利用了分组的TTL或跳数值溢出时路由器所产生的出错消息。traceroute命令使用递增TTL值的方式发送多个ping分组，并显示每个分组的往返时间。由于TTL值在发送每个ping分组时递增，因此每次成功的ping都更接近目的。traceroute命令的好处是可以告之路径中最后一个可达路由器是谁，这样即可进行故障隔离。

用show ip route命令测试网络层

路由器为网络层的测试提供了一些强大的工具：查看路由表，并结合使用其他针对网络层的基本测试。路由表是路由器用来决定如何指引流量穿越网络的指示信息。例13-5显示的例子是用show ip route命令来确定是否存在一条有关目标网络的路由表项，其输出显示Rome（131.108.33.0）可以通过Paris（131.108.16.2）的Ethernet 1接口到达。

例13-5 show ip route命令输出

```
Paris# show ip route
Codes: I - IGRP derived, R - RIP derived, O - OSPF derived
C - connected, S - static, E - EGP derived, B - BGP derived
i - IS-IS derived, D - EIGRP derived
* - candidate default route, IA - OSPF inter area route
E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
L1 - IS-IS level-1 route, L2 - IS-IS level-2 route
EX - EIGRP external route

Gateway of last resort is not set
I    144.253.0.0 [100/1300] via 133.3.32.2 0:00:22 Ethernet1
131.108.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
I          131.108.33.0 [100/180771] via 131.108.16.2, 0:01:29, Ethernet1
C          131.108.12.0 is directly connected, Ethernet1
C          101.108.16.0 is directly connected, Ethernet0
I          219.100.103.0 [100/1200] via 133.3.32.2, 0:00:22, Ethernet1
```



实验活动 其他的连通性测试（traceroute和show ip route）

在本活动中，使用Cisco IOS软件的traceroute命令检测源、目的和其间每个路由器的网络层的正常运行。Windows OS的tracert命令用来检测从源工作站点到目的路由器。还可以使用show ip route命令显示路由器上的路由表。

用show interface serial命令测试物理层和数据链路层

图13-8显示了两个路由器接口之间的一条串行连接。该接口有物理（硬件）和逻辑（软件）两部分：

- 硬件（包括线缆、连接器和接口）必须在设备之间建立实际的连接。
- 软件负责在相邻设备间传递消息，例如keepalive消息、控制信息和用户信息。数据在两个直接相连的路由器的接口间传输。

在测试物理层和数据链路层时，需要提出以下问题：

- 是否有载波探测信息？
- 设备间的物理连接是否良好？
- 能否收到keepalive消息？
- 数据分组能否通过物理链路来发送？

show interface serial命令输出中最重要的一个内容是线路和数据链路协议状态的显示。图13-9显示了用来检测线路和数据链路协议的关键状态值及其含义。

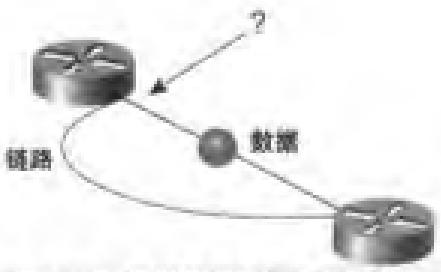


图13-8 测试物理层和数据链路层

这个例子中的线路状态由一个载波探测信号触发，是指物理层状态。但是链路协议由keepalive帧触发，是指数据链路的成帧（第2层的一个功能）。

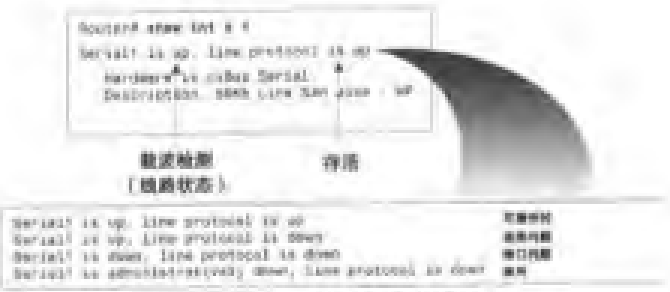


图13-9　鉴别线路和协议问题

使用show interface命令和clear counters命令

路由器能够跟踪其接口的统计信息。使用show interface命令可以显示如例13-6所示的统计值。

例13-6　show interfaces命令输出

```
Router# show interfaces serial 1
Serial1 is up, line protocol is up
Hardware is cxBus Serial
Description: 56Kb Line San Jose - MP
Internet address is 150.136.190.203, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:07, output 0:00:11, output hang never
Last clearing of show interfaces counters 2w4d
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
   16263 packets input, 1347238 bytes, no buffer
   Received 13983 broadcasts, 0 runts, 0 giants
   2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
   0 input packets with dribble condition detected
   22146 packets output, 2383680 bytes, 0 underruns
   0 output errors, 0 collisions, 2 interface resets, 0 restarts
   1 carrier transitions
```

这些统计反映了路由器自上一次清除计数器值以来的运行情况。使用clear counters命令可以将计数器值复位为0。这样就可以从0开始获得网络当前状态的概貌。show interface命令还可以用来检查其他接口类型的状态，例如以太网（E0）、快速以太网（Fa0）和综合业务数字网（ISDN）（BRI0）。

使用debug命令检查实时流量

路由器的硬件和软件能够帮助该路由器追踪自己或网络上其他主机的问题。特权EXEC模式下的debug命令将该命令参数所指定的网络事件显示在控制台上。使用terminal monitor命令可以将debug的输出重定向到Telnet会话终端上。

警告：在一个正在运行的网络中要非常小心使用debug命令。在一个繁忙网络中的实时调试将严重减慢网络。不要一直打开调试，在诊断出问题后应立即关闭调试。在RAM较小的路由器上过多的调试会造成该路由器的重新启动。

图13-10显示了使用debug broadcasts命令后路由器所收到的数据链路广播。不再需要调试时可以使用undebug all（或no debug all）命令关闭调试。调试主要是为了解决问题。

缺省方式下，路由器将系统错误消息和debug EXEC命令的输出发送到控制台终端，但是可以将这些消息重定向到UNIX主机或一个内部缓冲区中。terminal monitor命令能够将这些消息重定向到终端，这在使用UNIX或Linux主机而不是用控制台终端管理设备时非常有用。

实验活动 IP地址问题的故障排除

在本活动中，将配置工作站的IP地址，并测试端到端的网络连通性。

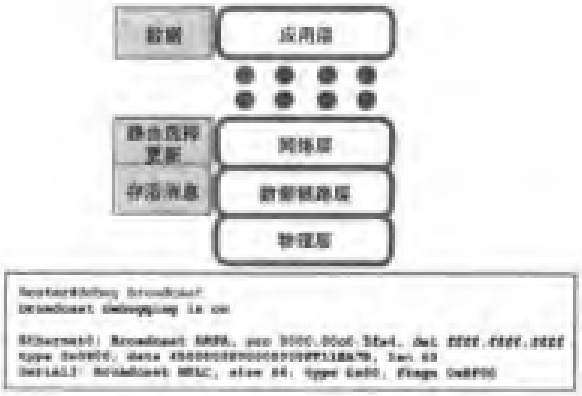


图13-10 使用debug命令检查实时流量

13.3 总结

本章学习了以下知识点：

- CDP是一个独立于介质和协议的、用于邻居发现的Cisco专有协议。
- CDP只显示直连邻居的信息。
- 使用CDP可以显示邻居的第2层和第3层信息。
- 应该一层一层地测试网络的连通性。
- 处理连通性问题时，最常见的问题发生在IP网络中。以下3个命令用来执行与地址相关的故障排除：
  - ping使用ICMP协议检测硬件连接和网络层的IP地址。这个命令是一个非常基础的测试机制。
  - telnet检测源和目的之间的应用层软件。这个命令是一个最全面的可用测试机制。
  - traceroute允许定位源和目的之间的路径故障。traceroute或trace利用TTL值让沿途的每个路由器产生消息。

为了补充你在本章所学的知识，请参考本书配套光盘中对应章节的视频、插图和e-Lab实验活动。

13.4 关键术语

Cisco发现协议（*Cisco Discovery ProtocolCDP*） 用来获得邻居设备的信息，比如所连接设备的类型、所连接的路由器接口、用于连接的本地接口，以及设备上的模块数量。

调试（*debugging*） 发现并删除程序或者设计上的错误（bug）。

ping 分组互连测试，使用ICMP回应消息及其应答。经常用在IP网络中测试网络设备的可达性。

子网访问协议（*Subnetwork Access ProtocolSNAP*） 操作在子网网络实体和端系统网络实体间的Internet协议。SNAP定义了在IEEE网络上封装IP数据报和ARP消息的标准方法。端系统上的SNAP实体使用子网的服务，并且执行3个关键功能：数据传输、连接管理和QoS选择。

简单网络管理协议（*Simple Network Management ProtocolSNMP*） 专门用于TCP/IP网络的网络管理协议。SNMP提供一种监测和控制网络设备的手段，并且能够管理配置、记帐、性能和安全。

Telnet TCP/IP协议栈中的标准终端仿真协议。Telnet用于远程终端连接，能够让用户登录到远程系统，并且像连接在本地系统一样使用资源。

类型长度值（*Type Length ValuesTLV*） 内含在CDP通告中的一组信息。

traceroute 在许多系统中用来跟踪分组到达目的的路径的程序，通常用于调试主机间的路由问题。

13.5 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 什么是telnet的定义？
   A. 一个用来判断指定IP地址是否可以到达的命令，其工作方式是发送一个分组到指定地址并等待应答
   B. 一个利用TTL值让路径上的每个路由器产生消息的命令
   C. 一个用来检查源和目的站点间应用层软件的命令，是最全面的可用测试机制
2. 使用show interfaces serial命令测试网络时，会提供什么信息？
   A. 显示线路和数据链路协议的状态
   B. 显示路由器是如何引导流量穿越网络
   C. 显示分组穿越网络的路径
   D. 显示网络中路由器的名称
3. show cdp neighbors命令为每个CDP邻居提供了什么信息？
   A. 设备标识
   B. 地址列表
   C. 端口标识
   D. 以上全部
4. show cdp interface 命令显示以下哪项？
   A. CDP计时器的值和接口状态
   B. CDP通告和发现帧传输时所使用的封装
   C. 邻居路由器的接口配置
   D. A和B
5. 关于show cdp entry [*device name*]命令的输出，以下哪项是正确的？
   A. 显示邻居路由器的所有第3层地址
   B. 显示路由器的邻居个数
   C. 显示所有邻居路由器的设备编号清单
   D. 显示邻居路由器接口上的所有第2层地址
6. 为了显示show cdp neighbors和show cdp entry [*device name*]命令的共同信息，使用以下哪个命令？
   A. show cdp neighbors detail
   B. show cdp interface entry
   C. show cdp neighbors entry
   D. show cdp details
7. show cdp neighbors命令显示什么信息？
   A. 邻居设备的标识
   B. 本地端口类型和数量
   C. 以秒为单位的递减保存时间（holdtime）值
   D. 以上全部
8. 使用ping命令后获得的4项重要信息是什么？
   A. ICMP分组的数量和大小；超时时限；成功率；往返时间的最小值、平均值和最大值
   B. ICMP分组的数量和大小；MAC地址；成功率；往返时间的最小值、平均值和最大值
   C. 以上全部
   D. 以上都不是

9. 使用traceroute命令测试网络时，将提供哪些信息？
   A. 检验链路协议是否运行正常
   B. 检验目的网络是否在路由表中存在
   C. 映射分组传输到目的网络过程中经过的每个路由器
   D. 检验上层应用是否工作正常
10. 在应答ping 命令时，惊叹号（!）表示什么含义？
   A. 成功回应的数量
   B. 不成功回应的数量
   C. 达到目的前所经过的跳数
   D. 以上全部
11. 关于路由器debug命令，下面哪个描述是正确的？
   A. debug特权EXEC命令根据指定的命令参数，在控制台上显示相应的网络事件
   B. undebug all命令（或no debug all）关闭调试
   C. buffer debug命令用来缓冲登录
   D. A和B



第14章　管理Cisco IOS软件

目标

学习完本章之后，你应该能够：

- 识别路由器启动顺序的各个阶段。
- 确定一个Cisco设备如何定位和加载Cisco IOS软件。
- 使用boot system命令。
- 识别配置寄存器的值。
- 描述用来定位Cisco IOS软件的过程。
- 描述用来创建、加载软件映像和配置文件备份的过程和命令。
- 描述Cisco IOS软件的命名规则。

本章介绍路由器启动顺序的各个阶段，包括Cisco路由器如何定位和加载Cisco IOS软件。本章还介绍boot system命令，并解释boot system命令如何告知路由器进行启动。你还将学习如何使用多种Cisco IOS软件来源的选项，通过执行命令将Cisco IOS软件加载到路由器上，维护备份文件，以及升级Cisco IOS软件。此外，你将了解到配置寄存器（configuration register）的功能以及如何确定所拥有的Cisco IOS软件映像文件的版本。最后，本章描述了如何将一个TFTP服务器作为Cisco IOS软件映像和配置文件的软件来源来使用。

请认真查看随书的光盘，这里面有关于这章内容的e-Lab实验、视频和插图。光盘中提供了一些与本章内容相关的素材，帮助读者加深理解和巩固所学知识。

14.1　路由器加电/启动顺序的阶段

路由器的初始化是通过加载*引导程序*（*bootstrap*）、操作系统和一个配置文件来进行的。如果路由器找不到任何一个配置文件，它将进入设置模式。路由器将设置模式下的新配置的备份拷贝保存在*非易失性随机存取存储器*（*NVRAM*）中。图14-1显示了在路由器初始化过程中发生的事件。



图14-1　路由器启动顺序

Cisco IOS软件启动例程的目的是为了启动路由器的所有操作。路由器根据配置连接用户网络时，必须提供可靠的性能。为了达到这个目的，启动例程必须完成以下几个内容：

1. 确定路由器加载了ROM。
2. 找到并加载用于路由器操作系统的Cisco IOS软件映像。
3. 找到并应用包括协议功能和接口地址的配置语句。

一个Cisco路由器加电时，执行加电自检（POST）。在自检过程中，路由器执行ROM中的诊断程序，检查所有的硬件模块。这些诊断程序检查CPU、内存和网络接口的基本操作。检验硬件功能后，路由器进行软件初始化。

14.2　定位和加载Cisco IOS软件

Cisco IOS软件启动的默认来源取决于硬件平台。但是，路由器通常会去查看存放在NVRAM中的boot system命令。Cisco IOS软件确实允许使用几个备选方案。可以指定路由器查看其他 的软件来源。当然，如果需要的话，路由器也可以使用自己的后退顺序（Fallback sequence）来加载软件。图14-2举例说明了如何定位Cisco IOS软件映像。

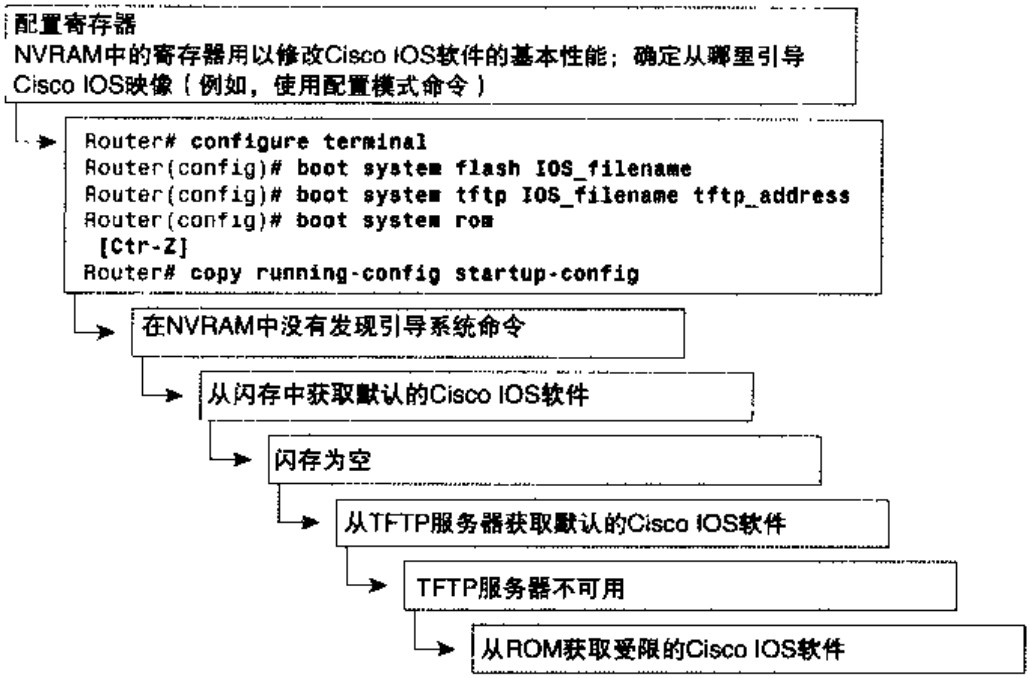


图14-2　定位Cisco IOS软件

配置寄存器中的设置允许以下这些选择：

- 可以通过指定全局配置模式下的boot system命令，按后退顺序输入路由器所使用的来源。当路由器重新启动后，它会在必要时按顺序使用这些命令。
- 如果NVRAM中没有设置路由器可用的boot system命令，系统将缺省使用*闪存*（*Flash memory*）中保存的Cisco IOS软件。
- 如果闪存为空，路由器接下来尝试使用*简单文件传输协议*（*TFTP*）从网络上加载Cisco IOS软件映像。此时，路由器使用配置寄存器的值构建一个文件名，该文件名可以用来引导一个存储在网络服务器上的缺省系统映像。
- 如果TFTP服务器无效，路由器将装载存储在ROM中的受限版本的Cisco IOS软件映像。

14.2.1　使用boot system命令

可以输入多个boot system命令来指定引导Cisco IOS软件的后退顺序。例14-1、14-2和14-3显

示的boot system命令指定Cisco IOS软件映像首先从闪存中加载，其次是从网络服务器加载，最后是从ROM加载。

命令copy running-config startup-config将那些命令保存在NVRAM中。路由器在需要时执行这些boot system命令，并按照它们在配置模式下的输入顺序来执行。如果要查看是否已经输入了boot system命令，可以使用show startup-config命令。

从闪存引导

从闪存引导包括从可电擦除可编程只读存储器（EEPROM）中加载一个系统映像。优点是存储在闪存中的信息不易受到网络故障的攻击，而这些网络故障会在从TFTP服务器加载系统映像时发生。例14-1指定从闪存加载Cisco IOS软件文件gsnew-image。

例14-1 从闪存引导

```
Router# configure terminal
Router(config)# boot system flash gsnew-image
[Ctrl-Z]
Router# copy running-config startup-config
```

从网络服务器引导

在闪存损坏的情况下，系统映像可以通过指定从TFTP服务器加载的方式提供一个备份。例14-2指定从IP地址为172.16.13.111的TFTP服务器加载映像文件IOS_image。

例14-2 从网络服务器引导

```
Router# configure terminal
Router(config)# boot system tftp IOS_image 172.16.13.111
[Ctrl-Z]
Router# copy running-config startup-config
```

从ROM引导

如果闪存损坏，而且从网络服务器加载映像失败，那么从ROM引导是软件中最后一个引导程序选项。但是，ROM中的系统映像很可能是Cisco IOS软件的一个子集。这个子集缺少完整Cisco IOS软件所拥有的协议、特性和配置。而且，如果在购买了路由器后，软件已经升级，ROM中也许是一个旧版的Cisco IOS软件\。例14-3展示了这个最后的引导程序选项。

例14-3 从ROM引导

```
Router# configure terminal
Router(config)# boot system rom
[Ctrl-Z]
Router# copy running-config startup-config
```



实验活动 使用boot system命令

在本活动中，收集关于Cisco IOS映像的信息，确定它的引导源。检查配置寄存器的设置，记录一个后退引导顺序。

14.2.2 配置寄存器的值

路由器加载Cisco IOS软件时，寻找Cisco IOS软件映像的顺序取决于配置寄存器中设置的引导字段。你可以使用全局配置命令config-register来更改默认的配置寄存器设置。该命令的参数是一个十六进制数，如例14-4所示。

例14-4 更改配置寄存器的引导字段

```
Router# configure terminal
Router(config)# config-register 0x10F
[Ctrl@C2]
```

配置寄存器的设置是让路由器为引导系统选项检查保存在NVRAM中的启动文件。配置寄存器是NVRAM中的一个16位寄存器。配置寄存器的低4位（比特3、2、1和0）是引导字段。如果要更改引导字段而保持其他位的值不变，应遵循以下指导方案：

- 如果要进入ROM监视器，则设置配置寄存器为0x100。该设置主要是程序员环境。操作系统将从ROM监视器中手动引导。在ROM监视器提示符下使用b命令引导系统。这个值设置引导字段的比特为0-0-0-0。
- 设置配置寄存器为0x101，将系统配置为自动使用ROM中的受限Cisco IOS软件映像引导。这个值设置引导字段的比特0-0-0-1。
- 设置配置寄存器为0x102到0x10F间的任意值，将系统配置为使用NVRAM中的boot system命令。该设置是默认设置。这些值设置引导字段的比特为0-0-1-0到1-1-1-1。

如果NVRAM中没有boot system命令，系统将在闪存中寻找Cisco IOS软件映像。

表14-1显示了配置寄存器中引导字段的值。

表14-1 配置寄存器中引导字段的值

值	说明
0x100	使用ROM监视器模式（使用b命令手动引导）
0x101	自动从ROM引导（路由器没有闪存时的缺省设置）
0x102 到 0x10F	检查NVRAM中的boot system命令（0x102是路由器有闪存时的缺省设置）

要检查启动字段的设置并检验config-register命令，可使用show version命令。



实验活动 配置寄存器引导问题的故障排除

在本活动中，检查并记录与引导方法有关的配置寄存器设置，配置路由器从闪存启动。

14.2.3 显示当前运行的Cisco IOS软件版本

show version命令，如例14-5所示，显示了当前运行在路由器上的Cisco IOS软件版本的信息。这个版本信息包括配置寄存器和引导字段的设置。

例14-5 配置寄存器

```
Router# show version
Cisco Internetwork Operating System Software IOS (tm) 2500 Software (C2500-JS-L),
 Version 12.1[5], RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by
  Cisco Systems, Inc. Compiled Wed 25-Oct-00 05:18 by cmong Image text-base:
```

```
  0x03071DB0, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE BOOTFLASH:
  3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)
Router uptime is 7 minutes System returned to ROM by reload System image file
  is "flash:c2500-js-l_121-5.bin"
Cisco 2500 (68030) processor (revision D) with 16384K/2048K bytes of memory.
  Processor board ID 03867477, with hardware revision 00000000 Bridging software.
  X.25 software, Version 3.0.0. SuperLAT software (copyright 1990 by
  Meridian Technology Corp). TN3270 Emulation software. 1 Token Ring/IEEE 802.5
  interface(s) 2 Serial network interface(s) 32K bytes of non-volatile
  configuration memory, 16384K bytes of processor board System flash (Read ONLY)
Configuration register is 0x2142
```

在本例中，Cisco IOS软件版本和描述信息在输出的第二行中高亮标识。捕获的屏幕显示软件版本是12.1（5）。

输出的下一个高亮部分指出系统映像文件是c2500-js-l，使用闪存引导。请注意文件名称部分，它表明该映像是为Cisco 2500平台提供的。

show version命令的后续输出中，还显示了Cisco IOS软件版本当前正在运行的平台类型信息。最后一个高亮输出提供了命令——config-register 0x2142的最终结果。该命令用来输入配置寄存器的值。

注释：在show running-config或show startup-config命令输出中没有任何配置寄存器设置的迹象。

14.3 管理Cisco IOS软件映像

路由器和交换机依赖相应的软件来执行它们的操作。所需的两类软件分别是操作系统和配置文件。

在几乎所有的Cisco设备上所使用的操作系统都是Cisco InternetWork Operating System（IOS）。Cisco IOS软件允许硬件作为一个路由器或交换机运行。Cisco IOS软件文件有几兆字节的大小。Cisco IOS软件是一个确保网络提供连通性、可靠性、安全性、服务质量、可伸缩性以及应用所需管理功能的平台。

路由器或交换机使用的一种软件被称为*配置文件*（*configuration file*）或者*配置*（*config*）。配置文件包含一些规定设备如何路由或交换的指令。网络管理员创建一份定义Cisco设备所需功能的配置文件。可以由配置文件指定的功能的例子有接口的IP地址、路由选择协议和被通告的网络。配置文件一般有几百到几千字节的大小。

每一个软件组件都是作为一个独立的文件存放在存储器中。这些文件同样也可以存放在不同类型的存储器中。

Cisco IOS软件映像存储在被称为闪存（Flash）的存储区域中，闪存为启动时用作操作系统的Cisco IOS软件提供非易失性的存储。闪存允许升级Cisco IOS软件或存储多个Cisco IOS软件文件。在许多路由器系统结构中，Cisco IOS软件映像从闪存中复制，在**随机访问存储器**（*RAM*）中运行。

配置文件的一个拷贝被存放在NVRAM中，用作启动时的配置。该NVRAM配置文件被称为**启动配置**（*startup config*）。启动配置在启动时被复制到RAM中。RAM中的配置用来操作路由器。RAM配置文件被称为*运行配置*（*running config*）。

Cisco IOS软件版本12为路由器使用的所有文件系统提供一个单一接口。该版本被称为Cisco IOS文件系统（IFS）。IFS提供了一个单一方法来实现路由器使用的所有文件系统管理。IFS包括闪

存文件系统、网络文件系统以及读写数据（reading or writing data）。网络文件系统包括TFTP、远程复制协议（*RCP*）和文件传输协议（FTP）。读写数据包括NVRAM、运行配置和ROM。IFS使用一组通用的前缀来指定文件系统设备。表14-2提供了IFS的综述。

表14-2 IOS文件系统

前缀	说明
bootflash:	引导闪存
flash:	闪存。该前缀可用于所有平台。在没有闪存设备的平台上，前缀flash：化名为slot0：。因此，前缀flash：可以用来表示所有平台上的主要闪存
flh:	闪存加载帮助日志文件
nvram:	NVRAM
rcp:	远程复制协议（RCP）网络服务器
Slot0:	第一块个人计算机存储卡工业协会（PCMCIA）闪存卡
Slot1:	第二块PCMCIA闪存卡
system:	系统内存，包含运行配置
Tftp:	TFTP网络服务器

IFS使用统一资源定位符（URL）协定来指定网络设备和网络上的文件。统一资源定位符协定使用跟随在冒号后的诸如[[[*//位置*]/*目录*]/*文件名*]的格式来识别配置文件的位置。IFS也支持FTP文件传输。表14-3列举了用来管理软件版本12.0的Cisco IOS软件的命令，并将它们同Cisco IOS软件版本12.0以前版本的命令逐一进行了比较。

表14-3 管理Cisco IOS软件版本12.0及先前版本的命令

Cisco IOS 软件版本12.0之前的命令	Cisco IOS 软件版本12.x 的命令
configure network（Cisco IOS软件版本10.3之前） copy rcp running-config copy tftp running-config	copy ftp: system:running-config copy rcp: system:running-config copy tftp: system:running-config
configure overwrite-network（Cisco IOS软件版本10.3之前） copy rcp startup-config copy tftp startup-config	copy ftp: nvram:startup-config copy rcp: nvram:startup-config copy tftp: nvram:startup-config morenvram:startup-config
show configuration（Cisco IOS软件版本10.3之前） show startup-config	: :
write erase（Cisco IOS软件版本10.3之前） erase startup-config	erase nvram copysystem:running-config
write memory（Cisco IOS软件版本10.3之前） copy running-config startup-config	nvram:startup-config copy system:running-config ftp:
write network（Cisco IOS软件版本10.3之前） copy running-config rcp copy running-config tftp	copy system:running-config rcp: copy system:running-config tftp more system:running-config
write terminal（Cisco IOS软件版本10.3之前） show running-config	

14.3.1 Cisco IOS软件命名规则

Cisco开发了许多不同版本的Cisco IOS软件。Cisco IOS软件支持多种硬件平台和特性。Cisco还在继续开发和发布新版本的Cisco IOS软件。

Cisco有一个针对Cisco IOS软件文件的命名规则，用来识别不同版本的Cisco IOS软件文件，如图14-3所示。

如图14-3所示，Cisco IOS软件命名规则在名字中使用不同的字段：

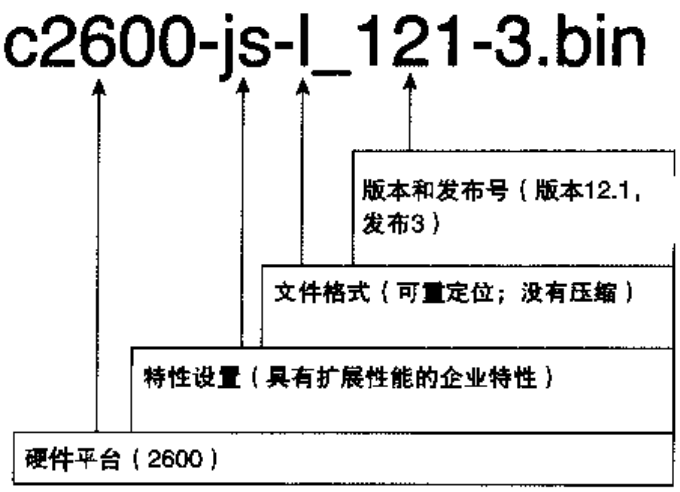


图14-3 Cisco IOS软件命名规则

- **硬件平台**——文件名的第一部分确定硬件平台。该映像专为硬件平台设计。
- **特性设置**——文件名的第二部分确定Cisco IOS软件文件拥有的各种特性。你可以在多种特性中进行选择，这些特性被封装在“软件映像”中。每一个特性设置包含一个Cisco IOS软件特性的特定子集。特性设置种类示例如下：
  - Basic——Basic是硬件平台所需的基本特性设置。Basic的例子有IP和IP/FW。
  - Plus——Plus是Basic基本特性设置加上其他的特性，例如IP Plus、IP/FW Plus和Enterprise Plus。
  - Encryption——Encryption是在Basic或者Plus的基础上加上56位数据加密特性设置。例子包括IP/ATM PLUS IPSEC 56或Enterprise Plus 56。加密指示符是以Cisco IOS软件版本12.2开始的k8/k9。k8小于或等于版本12.2及其后版本的64位加密。k9大于版本12.2及其后版本的64位加密。
- **文件格式**——IOS文件名的第三部分确定了文件格式。第三部分指定Cisco IOS软件是否以压缩格式存放在闪存中，以及Cisco IOS软件映像是否可重定位。如果闪存映像被压缩，那么Cisco IOS软件在引导过程中必须被解压为映像后复制到RAM中。可重定位的映像将从闪存中复制到RAM中运行。不可重定位的映像直接从闪存中运行。
- **版本和发布**——IOS文件名的第四部分确定了Cisco IOS软件的版本号和发布版本。当Cisco开发一个新版本的Cisco IOS软件时，版本号将会增加。

14.3.2 使用TFTP管理配置文件

在一个Cisco路由器或交换机中，活动配置存放在RAM中。路由器或交换机中启动配置的默认位置是NVRAM。因为配置会丢失，所以应当备份启动配置。你可以在TFTP服务器上存放配置的一份备份拷贝。可以使用copy startup-config tftp命令来备份配置。执行这个备份过程的步骤如下：

步骤1 输入copy startup-config tftp。

步骤2 在提示符下输入用来保存配置文件的TFTP服务器的IP地址。

步骤3 输入指派给配置文件的名称或者接受默认名称。

步骤4 每次都键入yes来确认选择。

例14-6显示了实际过程。

例14-6 在TFTP服务器上备份启动配置

```
Cougar# copy startup-config tftp
Address or name of remote host [] 192.168.119.20
Destination file name [Cougar config]?
!!!!!!!!!!!!!!!!!!!!!!!!
624 bytes copied in 7.05 secs
Cougar#
```

注释：如果路由器配置文件丢失，或使用了erase startup-config和reload命令，那么该路由器将没有任何已配置的接口。TFTP需要IP来进行连接，所以你需要使用控制台端口配置接口的IP地址，从而提供对TFTP服务器的访问。

你可以从TFTP服务器加载备份的配置文件来恢复路由器配置。恢复配置的步骤如下：

步骤1 输入copy tftp startup-config。

步骤2 在提示符下选择一个主机或者网络配置文件。

步骤3 在系统提示符下，输入配置文件所在的TFTP服务器的IP地址。

步骤4 在系统提示符下，输入配置文件的名称或者接受默认名称。

步骤5 确认系统提供的配置文件名称和服务器地址。

例14-7显示了从TFTP服务器恢复配置的过程。

例14-7 从TFTP服务器上恢复启动配置

```
Cougar# copy tftp startup-config
Address or name of remote host [] 192.168.119.20
Source filename []? Cougar-confg

Destination filename [running-config]?

Accessing tftp://192.168.119.20/GAD-confg…
Loading GAD-confg from 192.168.119.20
   (via FastEthernet 0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK-624 bytes]
624 bytes copied in 9.45 secs
Cougar#
```

要将配置文件从TFTP服务器复制回路由器，执行以下步骤：

步骤1 输入命令copy tftp running-config进入配置模式。

步骤2 在系统提示符下，选择主机配置文件或网络配置文件。网络配置文件包括应用在网络上所有路由器和终端服务器的命令。主机配置文件包括专门应用在一台路由器的命令。在系统提示符下，输入配置文件所在的远程主机的可选IP地址。例14-8中，路由器从IP地址为131.108.2.155的TFTP服务器上进行配置。

步骤3 在系统提示符下，输入配置文件的名称或者接受的默认名称。文件名规则是基于UNIX的。主机配置文件的默认名为hostnam-econfig，网络配置文件的默认名为network-config。在DOS环境下，服务器文件名称被限制为8个字符加上一个3字符的扩展名。例如router.cfg。确定系统提供的配置文件名和服务器地址。注意例14-8中路由器的提示符立刻更改为tokyo。这一改变证明新文件被下载后立即开始重新配置。

例14-8展示了从TFTP服务器复制配置文件的过程。

例14-8 从TFTP服务器复制配置文件

```
tokyo# copy tftp running-config
Host or network configuration file [host]?
IP address of remote host [255.255.255.255]? 131.108.2.155
```

```
Name of configuration file [Router-config]? tokyo.2
Configure using tokyo.2 from 131.108.2.155? [confirm] y
Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]
tokyo#
```

实验活动 使用TFTP管理配置文件

在本活动中，将一个路由器配置文件复制到TFTP服务器。然后，将该配置文件从TFTP服务器复制回路由器，用它来配置路由器。

14.3.3 使用超级终端管理配置文件

捕获show running-config命令的输出是另一种创建配置文件备份拷贝的途径。你可以在终端会话中执行该备份操作，首先复制输出，将其粘贴到一个文本文件中，然后保存该文本文件。尽管如此，在你使用该文件恢复路由器的配置之前，需要对该文件进行一些编辑。图14-4展示了一个剪切和粘贴配置的实例。

要将显示在屏幕上的超级终端（HyperTerminal）中的配置捕获到一个文本文件中，需要使用以下步骤：

步骤1 选择Transfer。

步骤2 选择Capture Text。

步骤3 指定用来捕获配置的文本文件名称。

步骤4 选择Start，开始捕获文字。

步骤5 输入show running-config，将配置内容显示到屏幕上。

步骤6 在每出现“-More-”提示符时，按下空格键，直到配置文件结束。

步骤7 当配置内容显示完毕之后，执行下面的步骤停止捕获：

a. 选择Transfer。

b. 选择Capture Text。

c. 选择Stop。



图14-4 捕获配置文件

捕获结束后，你需要编辑该配置文件，去除额外的文本。要创建一个能够复制粘贴回路由器的文件，就必须从捕获的配置中删除不必要的信息。你可以在该文本中加入注释来解释配置的不同部分。添加注释的时候，需要另起一行，并在行首使用感叹号（！）。

你可以在一个诸如记事本这样的文本编辑器中编辑配置文件。要在记事本中编辑文件，请执行以下步骤：

步骤1 点击File>Open。

步骤2 找到捕获的文件，选定它。

步骤3 点击Open。

需要删除的文本行包括以下内容：

- show running-config
- Building configuration...
- Current configuration:
- - More -
- 出现在单词*End*之后的任何行

在每一个接口部分的末尾，加上no shutdown命令。点击File>Save，保存配置文件的清理版本。

然后，你就可以从一个超级终端会话中恢复备份的配置。不过，在恢复配置之前，请删除路由器上存在的其他 任何配置，这可以通过在特权模式提示符下使用erase startup-config命令，然后输入reload命令重启路由器来完成。

在删除了所有残余配置后，可以使用超级终端来恢复配置。将清理的备份配置复制到路由器的步骤如下：

步骤1　进入路由器的全局配置模式。

步骤2　在超级终端中，选择Transfer>Send Text File。

步骤3　选择所保存的备份配置的文件名。

步骤4　文本行被输入到路由器，就像手工输入一样。

步骤5　寻找任何可能的错误。

步骤6　在配置文件全部输入之后，按Ctrl+z退出全局配置模式。

步骤7　使用命令copy running-config startup-config恢复启动配置。



实验活动　复制、编辑和粘贴配置

在本活动中，使用超级终端捕获一个路由器的运行配置，保存为ASCII文本文件。使用诸如记事本这样的文本编辑器编辑和修改捕获的文本文件，来清理配置。然后，使用超级终端上载清理后的文本文件来配置其他 的路由器。

14.3.4　使用TFTP管理Cisco IOS软件映像

有时候，路由器需要升级或者恢复Cisco IOS软件映像。第一次使用路由器时，应该使用命令copy tftp flash将Cisco IOS软件备份到一台TFTP服务器上。Cisco IOS软件映像可以和其他 版本的Cisco IOS软件映像一起存放在一台中心服务器上，以便升级和恢复互联网中路由器和交换机的Cisco IOS软件映像。

该服务器应该运行一个TFTP服务。你可以在特权模式下面用命令copy tftp flash来开始Cisco IOS软件的升级，如例14-9所示。

例14-9　从TFTP服务器升级Cisco IOS软件

```
Cougar# copy tftp flash
Address or name of remote host []? 192.168.119.20
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服务器的地址。在被提示输入服务器上的Cisco IOS软件映像文件名时，路由器也许还会接着提示清除闪存。清除闪存的提示通常发生在没有足够的闪存来存放新映像时。从闪存中删除映像时，会出现一连串的字母“e”来显示删除的进度。

每下载一个Cisco IOS软件映像文件的数据报，都会显示一个“!”。Cisco IOS软件映像有几兆字节的大小，需要一些的时间来下载。

注释：符号“!”表示闪存文件装载成功，符号“.”表示没有找到闪存文件。如果出现符号“.”，请确定输入了正确的命令语法。

新的闪存映像下载之后将进行检验。路由器此时准备重新启动，以使用新的Cisco IOS软件映像。

例14-10使用一个不同的路由器和TFTP服务器，并且提供了一些额外的信息，这些信息介绍了从TFTP服务器复制Cisco IOS软件映像到路由器的步骤。

在输入copy tftp flash命令之后，如例14-10所示，系统提示输入TFTP服务器的IP地址或名字，这个地址或名字也可以是另一个提供ROM或闪存软件映像的路由器。随后系统提示输入该软件映像的文件名。例14-10显示了复制一个名为C4500-I的系统映像到闪存中的输出示例。

例14-10 从TFTP服务器复制 Cisco IOS软件映像到路由器

```
Router# copy tftp flash
IP address or name of remote host [255.255.255.255]? 172.16.13.111
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]
xxxxxxxx bytes available for writing without erasure.
erase flash before writing? [confirm]
Clearing and initializing flash memory [please wait] ####...##
Loading from 172.16.13.111: !!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! (text omitted) [OK - 324572/524212 bytes]
Verifying checksum...
VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
VVVVVVVV (text omitted)
Flash verification successful. Length = 1204637, checksum = 0x95D9
```

如果你试图复制到闪存中的文件已经存在，一个提示会告知具有相同名字的文件已经存在。在将新文件复制到闪存中时，原有文件将被删除。如果闪存中还有空间来容纳两份拷贝，那么该文件第一份拷贝仍留在闪存中，但是将不再作为最新版本来使用；使用show flash命令时该文件的显示将带有[deleted]标记。

如果中止复制过程，新文件将被标记为[deleted]，因为并没有复制整个文件，所以无效。在这种情况下，原始文件仍然保留在闪存中并可用于系统中。



实验活动 使用TFTP管理IOS映像

在本活动中，将路由器的一份Cisco IOS映像拷贝备份到TFTP服务器上。然后从TFTP服务器重载该备份拷贝到路由器的闪存中。

14.3.5 使用ROMmon管理Cisco IOS软件映像

如果闪存中的Cisco IOS软件映像已经被删除或者损坏，你也许需要从ROM监视器模式（ROMmon）

下恢复Cisco IOS软件映像。在很多的Cisco硬件系统结构中，ROMmon模式通过提示符rommon# > 来辨认。

这个过程的第一步是确认为什么Cisco IOS软件映像没有从闪存中加载。这个问题可能是由于映像文件的丢失或损坏，或者是闪存损坏造成的。可以用命令dir flash:检查闪存。

如果找到了一个看起来有效的映像，那么尝试从该映像进行引导。可以使用命令boot flash:来执行这个引导尝试。例如，如果映像文件名为c2600-is-mz.121-5，命令如下：

```
rommon > boot flash:c2600-is-mz.121-5
```

如果路由器完全启动了，你需要检查几个条款，因为需要确定为什么路由器启动进入了ROMmon模式，而不是直接使用闪存中的Cisco IOS软件。首先，使用show version命令检查配置寄存器，确保其配置为默认启动顺序。如果配置寄存器值正确，使用show startup-config命令。该命令可以显示是否有一个boot system命令指示路由器使用Cisco IOS软件进入ROMmon。

如果路由器不能很好地从该映像引导，或者根本没有Cisco IOS软件映像，你需要下载一个新的Cisco IOS软件映像。要恢复Cisco IOS软件文件，既可以通过控制台使用Xmodem恢复映像，也可以在ROMmon模式下使用TFTP下载映像。

在ROMmon下使用Xmodem下载Cisco IOS软件

要通过控制台来恢复Cisco IOS软件映像，本地PC需要有一份用来恢复的Cisco IOS软件文件拷贝和一个诸如超级终端这样的终端仿真程序。恢复Cisco IOS软件映像时，可以使用9600 bit/s的缺省控制台速率，你可以将波特率更改到115200 bit/s来加速下载。可以在ROMmon模式下使用confreg命令更改控制台速率。在输入confreg命令之后，路由器将提示一系列可以修改的参数，如例14-11所示。

例 14-11 更改控制台速率

```
rommon 1 > confreg

Configuration Summary
…<output omitted>…
…console baud: 9600
boot: the ROM Monitor
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode" ? y/n [n]:
…<output omitted>…
enable "ignore system config info" ? y/n [n]:
change console baud rate? y/n [n]: y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: 7
change the boot characteristics? y/n [n]:

Configuration Summary
enabled are:
break abort has effect
console baud: 115200
boot: the ROM Monitor

do you wish to change the configuration? y/n [n]:
```

必须重新启动或者重新加电，以便新的配置发挥效用。

当提示“change console baud rate? y/n [n]:”时，选择y将提示选择新的速率。在更改了控制台速率之后，重新启动路由器进入ROMmon模式。9600 bit/s的终端会话被终止，一个新的会话以115200 bit/s开始来匹配控制台速率。

你可以在ROMmon模式下使用xmodem命令从PC恢复Cisco IOS软件映像。xmodem命令的格式如下：

```
xmodem -c image_file_name
```

例如，要恢复一个名为c2600-ismz.122-10a.bin的Cisco IOS软件映像文件，可输入如例14-12所示的命令

例14-12 使用xmodem命令恢复Cisco IOS软件映像文件

```
rommon 1 >
        rommon 1 > xmodem -?
        xmodem: illegal option    ?
        usage: xmodem [-cyrx] <destination filename>
        -c  CRC-16
                -y  ymodem-batch protocol
                 r  copy image to dram for launch
                -x  do not launch on download completion
rommon 2 > xmodem -c c2600-is-mz.122-10a.bin

Do not start the sending prograr vet...

        Warning: All existing data in bootflash will be lost!

Invoke this application only for disaster recovery.
Do you wish to continue? y'n [n]: y
Ready to receive file c2600-is-mz.122 10a.bin ...
```

命令格式中的参数-c指示Xmodem进程使用循环冗余校验（CRC）检查下载过程中的错误。

你将收到一个来自路由器的提示，提示不要开始传输，同时还将显示一个警告消息。该警告消息显示bootflash将要被删除，同时路由器要求确认是否继续该进程。当你继续该进程的时候，路由器随后会提示开始传输。

现在需要从终端仿真器上开始Xmodem传输。在超级终端中，选择Transfer>Send。然后，在“发送文件”弹出窗口中，指定映像文件的名称/位置，选择Xmodem协议，开始传输。在传输过程中，“发送文件”弹出窗口会显示传输的状态。

传输结束后，将显示一个消息表示闪存已经被清除。该消息后紧跟着“Download Complete!”消息。在重新启动路由器之前，需要将控制台速率重新设置回9600 bit/s，将配置寄存器重新设置回0x2102。在特权EXEC模式下使用confreg 0x2102命令设置回配置寄存器。

当路由器重新启动的时候，你需要结束115200 bit/s的终端会话，并开始一个9600 bit/s的会话。

使用环境变量来恢复Cisco IOS软件映像

也可以从一个TFTP会话恢复Cisco IOS软件。在ROMmon模式下使用TFTP下载映像是将Cisco IOS软件映像恢复到路由器的一个最快捷的方法。可以通过设置环境变量和使用tftpdnld命令来执行该进程。

因为ROMmon模式的功能有限，在引导过程中没有加载配置文件。因此，路由器没有IP或接口配置。环境变量提供了一个最小化的配置来允许从TFTP下载Cisco IOS软件映像。ROMmon模式下

的TFTP传输仅仅工作在第一个LAN端口上，所以为该接口设置了一组简单的IP参数。设置一个ROMmon环境变量，你要输入变量名称，然后是等号（=），接着是该*变量的值*（*变量名=值*）。例如，要设置IP地址为10.0.0.1，可在ROMmon提示符下输入IP_ADDRESS=10.0.0.1。

注释：*所有的环境变量名都是大小写敏感的。*

使用tftpdnld所需的最少变量如下：

- IP_ADDRESS——LAN接口的IP地址。
- IP_SUBNET_MASK——LAN接口的子网掩码。
- DEFAULT_GATEWAY——LAN接口的缺省网关。
- TFTP_SERVER——TFTP服务器的IP地址。
- TFTP_FILE——服务器上的Cisco IOS软件文件名。

要检查ROMmon环境变量，可以使用set命令，如例14-13所示。

例 14-13　检查ROMmon环境变量

```
rommon 10> set
    IP_ADDRESS=10.0.0.1
    IP_SUBNET_MASK=255.255.255.0
    DEFAULT_GATEWAY=10.0.0.254
    TFTP_SERVER=192.168.1.1
    TFTP_FILE=GAD/original_2003_Jan_22/c2600-i-mz.121-5
```

一旦为Cisco IOS软件的下载设定了变量，就可以输入tftpdnld命令，如例14-14所示，不带任何参数。ROMmon回显这些变量，随后显示一个确认提示和警告该进程将清除闪存。

例14-14　tftpdnld

```
rommon 12 > tftpdnld
IP_ADDRESS: 10.0.0.1
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 10.0.0.254
TFTP_SERVER: 192.168.1.1
TFTP_FILE: GAD/original_2003_Jan_22/c2600-i-mz.121-5
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]: y
Receiving GAD/original_2003_Jan_22/c2600-i-mz.121 5 from
192.168.1.1!!!!.!!!!!!!!!!!!!!!!!!!!.!!
File reception completed.
Copying file GAD/original_2003_Jan_22/c2600-i-mz.121-5 to flash.
Erasing flash at 0x607c0000
program flash location 0x60440000
rommon 13>
```

每收到一个Cisco IOS软件文件的数据报，就会显示一个“！”。当完整的Cisco IOS软件文件接收完毕之后，闪存被清除并写入新的IOS映像文件。该进程结束的时候显示会适当的消息。

当新的映像被写入闪存并且出现了ROMmon提示符后，你可以输入i来重新启动路由器。此时，路由器将从闪存中的Cisco IOS软件映像引导。



实验活动 使用ROMmon和Xmodem管理IOS映像

在本活动中，从ROM监视器模式下恢复一台丢失或者损坏了IOS/boot flash映像的Cisco 1700系列路由器。

14.3.6 检验文件系统

可以使用几个命令来检验文件系统。其中一个命令是show version命令，可以用来检查当前的映像以及闪存的总量。该命令也检验与加载Cisco IOS软件映像相关的另外两个条款。show version命令确定路由器引导时使用的Cisco IOS软件映像的来源，并且显示了配置寄存器值。可以检查配置寄存器引导字段的设置来确定路由器究竟是从什么地方加载Cisco IOS软件映像的。如果当前映像和配置寄存器引导字段的设置不一致，那么闪存中的 Cisco IOS软件映像可能已经损坏或丢失，或者在启动配置中有boot system命令。

例14-15显示了show version命令的使用。

例14-15 检验路由器文件系统

```
HMH# show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-BNSY-L), Version 12.2(11)P, RELEASE SOFTWARE (fc1)
… <output omitted>…
System image file is "flash:c1700-bnsy-l.122-11.p", booted via flash
cisco 171 (68360) processor (revision C) with 3584K/512K bytes of memory.
Processor board ID 12014633, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
2 serial(sync/async) network interface(s)
System/IO memory with parity disabled
2048K bytes of DRAM onboard 2048K bytes of DRAM on SIMM
System running from FLASH
8K bytes of non-volatile configuration memory.
6144K bytes of processor board PCMCIA flash (Read ONLY)
Configuration register is 0x2102
HMH#
```

还可以使用show flash命令来检验文件系统，确定闪存中的一个或者多个Cisco IOS软件映像以及闪存的可用总量。show flash命令通常用来确定是否有足够的空间存放新的Cisco IOS软件映像。例14-16显示了show flash命令的输出示例。

例14-16 show flash命令输出

```
Router# show flash
4096 bytes of flash memory on embedded flash (in XX).
file offset length name
0 0x40 1204637 xk09140z
[903848/2097152 bytes free]
```

正如前面所提及的一样，配置文件可能包含boot system命令。可以使用这些命令来确定启动时需要的Cisco IOS软件映像的来源。可以使用多个boot system命令来创建一个发现和加载Cisco IOS软件映像的后退顺序。这些boot system命令将按照它们在配置文件中的出现顺序来执行。

14.4　总结

本章学习了以下知识点：

- Cisco IOS软件的默认来源取决于硬件平台。但是，路由器通常寻找保存在NVRAM中的配置命令。
- 使用show version命令显示当前运行在路由器上的Cisco IOS软件版本信息。
- 输入多个boot system命令来指定引导Cisco IOS软件的后退顺序。路由器可以从闪存、TFTP服务器以及ROM中引导Cisco IOS软件。
- 使用show flash命令检验系统是否有足够的存储空间来存放需要加载的Cisco IOS软件。
- 在Cisco IOS软件版本11.2及以后的版本中，Cisco IOS的命名规则包括以下三部分：
  — 映像所在的平台。
  — 映像的特殊性能。
  — 映像将在哪里运行以及是否被打包或压缩。
- 可以将一份系统映像复制到网络服务器上。这份系统映像的拷贝可以作为一个备份拷贝，并且用来检验闪存中的拷贝是否和原始文件一致。
- 如果需要加载备份的Cisco IOS软件版本，可以使用copy命令的一个变换形式，copy tftp flash，来下载先前上传到TFTP服务器上的映像。

关于本章学习的补充内容，请参阅本书附赠光碟中与本章相关的视频、插图和e-Lab实验。

14.5 关键术语

引导程序（*bootstrap*） 网络节点使用的一种协议，用来确定其以太网接口的IP地址继而影响网络引导。

闪存（*Flash memory*） 一种特殊类型的EEPROM，可以一次整块而不是一字节地被清除和再编程。许多现代PC都将它们的BIOS存放在闪存芯片中，便于需要时容易升级。这样的BIOS有时候又被称作Flash BIOS。闪存在调制解调器中也非常流行，因为它允许调制解调器制造商支持成为标准的新协议。

非易失性随机存储器（*nonvolatile random-access memoryNVRAM*） 当单元掉电时依然保有其内容的RAM。

随机存储器（*random-access memory，RAM*） 可以由一个微处理器读写的易失性存储器。

远程复制协议（*remote copy protocol，RCP*） 允许用户将文件复制到网络上一个远程主机或服务器的文件系统中，并从该文件系统中复制文件。

简单文件传输协议（*Trivial File Transfer Protocol，TFTP*） FTP的简化版本，允许文件从一台电脑通过网络传输到另一台电脑上，通常没有使用客户端认证（例如，用户名和密码）。

14.6　复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 下面哪一项正确描述了指定一个路由器如何加载Cisco IOS软件的方法？
   A. 从NVRAM中按顺序指定路由器可以使用的后退源。
   B. 配置Cisco IOS软件映像所引导的位置。
   C. 从虚拟终端手动引导一个默认的系统映像。
   D. 从网络服务器手动引导一个默认的系统映像。
2. 下面哪一项不是可以配置寄存器引导字段所设置的引导选项？
   A. 从ROM监视器模式引导Cisco IOS软件。
   B. 从ROM自动引导Cisco IOS软件。
   C. 从TFTP服务器自动引导Cisco IOS软件。
   D. 检查NVRAM中是否有boot system命令。
3. 下面哪一项是show version命令显示的信息？
   A. 路由器内存每一页的详细统计信息。
   B. 系统映像的名称。
   C. 闪存中所有文件的名称和大小。
   D. 配置的网络协议状态
4. 哪一个命令用来发现配置寄存器的设置？
   A. show register
   B. show running-config
   C. show version
   D. show startup-config
5. 哪一个信息不是在Cisco映像文件名系统中提供的？
   A. 映像的特性
   B. 映像所在的平台
   C. 映像在哪里运行
   D. 映像的大小
6. 从TFTP服务器加载新的Cisco IOS软件映像到闪存中时，下面的哪一项不是该推荐进程的一部分？（该进程按照正确的顺序列举）
   A. 将当前软件映像的一份拷贝备份到TFTP服务器。
   B. 输入copy flash tftp命令，开始从服务器下载新的映像。
   C. 该进程询问是否愿意清除闪存
   D. 显示一系列的V，表示成功进行了校验和验证。
7. 如果配置寄存器设置为0x101，哪一项是路由器的初始引导尝试？
   A. 设置模式
   B. TFTP服务器
   C. ROM
   D. 闪存
8. 下面的哪一项拥有一个受限版本的路由器Cisco IOS软件？
   A. ROM
   B. 闪存
   C. TFTP服务器

D. 引导程序

9. 如果配置寄存器设置为0x102，哪一项是路由器的初始引导尝试？

A. 闪存

B. TFTP服务器

C. ROM

D. 检查boot system命令

10. 下面的哪一项是路由器用来自动后退定位Cisco IOS软件的顺序？

A. （1）闪存，（2）NVRAM，（3）TFTP服务器

B. （1）NVRAM，（2）TFTP服务器，（3）闪存

C. （1）NVRAM，（2）闪存，（3）TFTP服务器

D. （1）TFTP服务器，（2）闪存，（3）NVRAM

11. 下面哪一项不是show version命令显示的信息？

A. 配置接口的统计信息

B. Cisco IOS软件运行的平台类型

C. 配置寄存器的设置

D. Cisco IOS软件版本

12. 下面哪一项正确描述了使用TFTP服务器将软件复制到闪存的准备工作？

A. TFTP服务器必须是一个可连接的路由器或主机系统，例如一个UNIX工作站或一个膝上型电脑。

B. TFTP服务器必须是一个连接到以太网的系统。

C. 必须确定包含闪存的路由器的名称。

D. 闪存必须是可用的。

13. 为什么要创建一个Cisco IOS软件映像备份？

A. 为了检验闪存中的拷贝与ROM中的拷贝一致。

B. 为了在复制该映像到新的路由器之前，提供当前版本的一个后退拷贝。

C. 为了创建当前映像的一个后退拷贝作为恢复系统故障程序的一个部分。

D. 为了在更新新版本之前创建当前映像的一个后退拷贝。

14. 如果想要从TFTP服务器下载一个新映像来升级一个旧版本Cisco IOS软件，应该使用下面哪个命令？

A. boot system tftp 131.21.11.3

B. copy tftp flash

C. show flash

D. tftp ios.exe



第15章　路由选择和路由选择协议

目标

学习完本章之后，你应该能够：

- 理解路由选择基础。
- 描述被路由协议和路由选择协议。
- 描述内部和外部协议。
- 描述静态及动态路由。
- 配置静态路由。
- 配置默认路由。
- 静态路由配置的故障排除。
- 描述为什么需要动态路由选择协议。
- 描述距离矢量路由选择。
- 描述链路状态路由选择。
- 理解如何使用不同的路由选择协议适应各种情况。

在本章中，你可以进一步学习开放式系统互连（OSI）参考模型网络层（即第三层）的重要互联功能中路由器的使用和操作。另外，将回顾路由选择协议和被路由协议的区别，以及路由器如何追踪位置间的距离。最后，将学习关于距离矢量、链路状态和混合路由选择方法，以及它们怎样解决普通的路由选择问题。

请认真查看随书的光盘，这里面有关于这章内容的e-Lab实验、视频和插图。光盘中提供了一些与本章内容相关的素材，帮助读者加深理解和巩固所学信息。

15.1　路由选择基础

穿越网络云的流量的路径确定发生在网络层（第3层）。路径确定功能允许路由器评估指向目的的可用路径，并建立分组的首选处理操作。路由选择服务在评估网络路径时使用网络的拓扑信息。该信息由网络管理员配置或通过网络中的动态进程来收集。

网络层提供跨越互联网络的、尽力而为的、端到端的分组发送。网络层使用IP路由选择表将分组从源网络发送给目的网络。路由器决定使用哪条路径后，就进行转发分组的处理。路由器将一个

接口上所接受的分组转发到反映到达该分组目的的最佳路径的另一个接口或端口上。

路由选择是路由器用来将分组转发到目的地网络的过程。路由器根据分组的目的IP地址做出决定。沿途所有设备使用目的IP地址指向分组的正确方向。目的IP地址使分组最终可以到达目的地。为了做出正确的决定，路由器必须获知远程网络的方向。当路由器使用动态路由选择协议时，可以从其他 路由器学习到达远程网络的方向。当使用静态路由选择时，网络管理员手工配置远程网络的信息。

因为静态路由必须是手工配置，任何网络拓扑改变都需要网络管理员增加或删除静态路由以适应该变动。在一个大型网络中，这种手工维护的路由选择表可能需要很多管理时间。几乎没有可能改变的小型网络中，静态路由就只需要极少的维护。因为没有额外的管理需求，静态路由选择没有动态路由选择那样的可伸缩性。但是，即便在大型网络中，实现特殊意图的静态路由也经常与动态选择路由协议一起配置。尽管动态路由选择协议可以自动确定路由，但它们依然必须要由网络管理员来完成初始的启动和配置。

以下小节包括几个路由选择概念：

- 分组从源到目的的路由选择过程。
- 寻址。
- 路径选择和分组交换。
- 被路由协议和路由选择协议。

15.1.1　路由器如何为分组从源端到目的端选择路由

为了确保实用，网络必须一致地表示路由器之间的可用路径。如图15-1所示，路由器间的每条链路都有一个号码让路由器用来作为网络地址。这些地址必须携带能被路由选择进程用来将分组从源端送往目的端的信息。使用这些地址，网络层可以提供互连独立网络的中继连接。

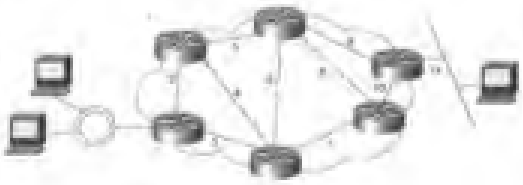


图15-1　网络地址

穿越整个互联网的第3层地址的一致性还通过阻止不必要的广播来提高带宽的使用。广播会造成不必要的处理开销，浪费所有不需要接收广播的设备或链路的容量。通过使用一致的端到端寻址来表示介质连接的路径，网络层可以找到一条通往目的的路径，不必采用广播而给互联网上的设备或链路增加不必要的负担。

15.1.2　网络和主机寻址

路由器使用网络地址识别互联网中分组的目的网络。图15-2中显示了识别路由器所连网段的三个网络号码。

大多数的网络协议寻址方案使用某种形式的主机或节点地址。对于一些网络层协议，网络管理员根据预先设计好的互联网络寻址计划分配网络主机地址。对其他 一些网络层协议来说，主机地址的分配是部分或全部动态的。在图15-2中，三个主机共享网络号码1。

网络	主机
1	1 2 3
2	1
3	1

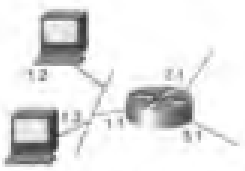


图15-2　网络地址和主机部分

15.1.3　路径选择和分组交换

路由器通常使用以下两个基本功能将分组从一条数据链路中继到另一条数据链路上：

• 路径确定功能。

• 交换功能。

图15-3举例说明了路由器如何使用寻址来实现路由选择和交换功能。路由器使用地址的网络部分进行路径选择，将分组沿路径发送给下一个路由器。

交换功能允许路由器从一个接口上接受分组，并将其转发到另一个接口。路径确定功能允许路由器选择最适当的接口来转发这个分组。最终的路由器（即连接目的网络的路由器）使用地址的节点部分将分组发送给正确的主机。

目的网络	方向和路由器端口
1.0	1.1
2.0	2.1
3.0	3.1



图15-3 路由器如何使用寻址来实现路由选择和交换功能

15.1.4 被路由协议与路由选择协议

被路由协议与路由选择协议这两个术语很类似，经常容易混淆（如图15-4所示）。以下进行一些澄清：

• ***被路由协议（routed protocol）***——任何在网络层地址中提供足够信息的网络协议，允许基于寻址方案将分组从一个主机转发到另一个主机上。被路由协议定义了分组中各字段的格式。分组一般在端系统之间传送。被路由协议使用路由选择表转发分组。Internet协议（IP）就是被路由协议的一个例子。

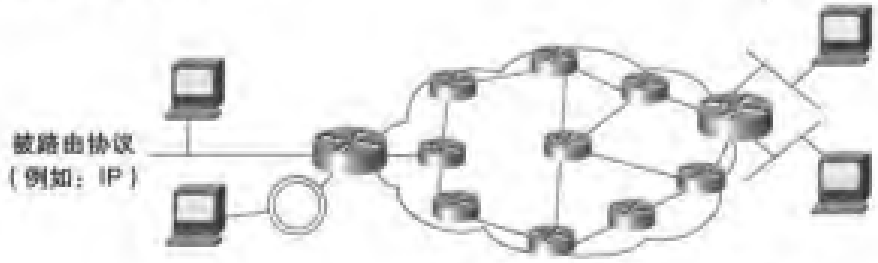
• ***路由选择协议（routing protocol）***——通过提供共享路由选择信息机制来支持被路由协议。路由选择协议的消息在路由器之间传递。路由选择协议允许路由器与其他 路由器通信来更新和维护路由选择表。TCP/IP中的路由选择协议例子如下：

— 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（EIGRP）。

— 开放式最短路径优先（OSPF）。



网络协议	目的网络	使用的输出端口
协议名字	1.0	1.1
	2.0	2.1
	3.0	3.1

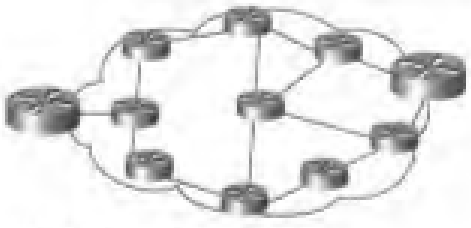


图15-4 被路由协议和路由选择协议

15.1.5　网络层协议操作

假设一个主机的应用程序需要向另一个网络中的目的主机发送分组。主机使用路由器的一个接口地址将数据链路帧发送给路由器。路由器的网络层进程检查入站分组的第3层报头来确定目的网络，然后参考将网络与出站接口相关联的路由选择表（如图15-5所示）。分组再次被封装在所选接口的数据链路帧中，排队等待发送到路径上的下一跳。

在每次将分组转发给另一个路由器时都要发生这个过程。当分组到达连接目的主机网络的路由器时，它被封装成目的局域网的数据链路帧类型并被发送到目的主机。

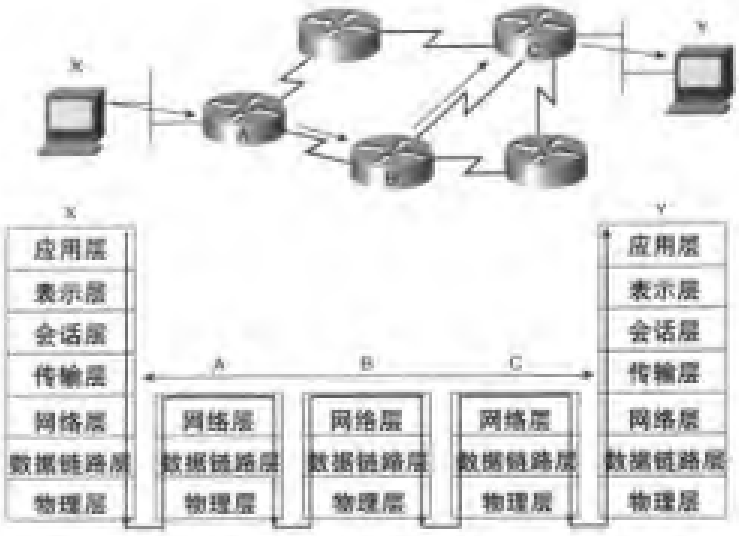


图15-5　路由器的服务

15.1.6　多协议路由选择

路由器能够支持多个独立的路由选择协议，并同时为几个被路由协议维护路由选择表。这种能力允许路由器从多个被路由协议上将分组发送在同一条数据链路上（如图15-6所示）。

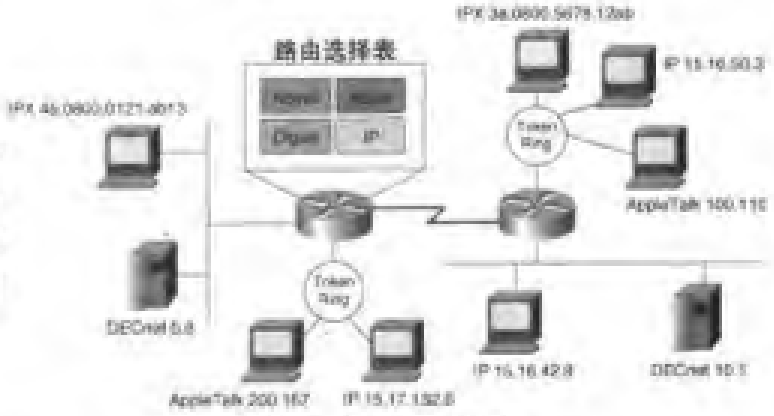


图15-6　路由器流量

15.2　静态路由选择

路由选择只是获得从一个网络到另一个网络的方向。这些方向也被称为路由，可以由另一个路由器动态交给一个路由器。管理员也可以静态地将这些方向分配给路由器。本节介绍管理员所指派的路由。

15.2.1　静态路由与动态路由

静态路由信息是通过网络管理员将其输入路由器配置来手工管理的。只要互联网络拓扑的改变要求更新，管理员就必须手工更新这些静态路由条目。

动态路由信息的操作不同。网络管理员输入配置命令启动动态路由选择后，只要从互连网络中收到新的信息，路由选择进程就自动更新路由信息。路由器之间交换动态信息的变化是更新进程的一部分。

15.2.2　静态路由的目的

静态路由选择有几个有用的应用。动态路由选择往往展示了关于一个互联网络的所有知道的信息；但是由于安全的原因，你也许想隐藏互联网络的一部分。***静态路由选择***允许指定希望展示的有限的网络信息。

当一个网络只有一条路径可以到达时，到该网络的静态路由就足够了。这种类型的网络被称为***stub网络***。一个stub网络就是一个OSPF区域，这个区域可以具有默认路由、区域内路由（intra-area routes）和区域间路由（interarea routes），但是不具有外部路由（external routes）。如图15-7所示，配置到stub网络的静态路由选择可以避免动态路由选择的开销。

15.2.3 静态路由的操作

静态路由的操作可以总结为三个步骤：

1. 网络管理员配置路由。
2. 路由器将路由装入路由选择表。
3. 使用静态路由来路由分组。

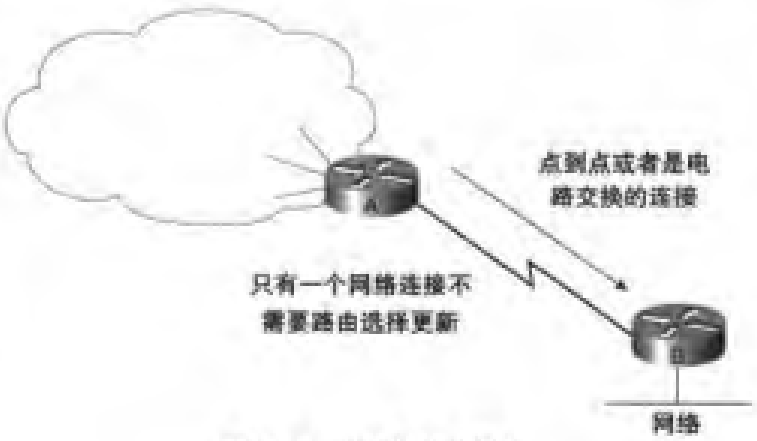


图15-7 静态路由的操作

因为静态路由是手工配置的，管理员必须在路由器上使用ip route命令配置静态路由。正确的ip route 命令语法如下：

```
Router(config)# ip route prefix mask {address|interface}[distance]
```

在图15-8中，Hoboken路由器的网络管理员需要配置一条静态路由指向在另一台路由器上的172.16.1.0/24和172.16.5.0/24网络。



图15-8 静态路由

管理员应该输入下面两个命令中的任何一个来完成该目标。例15-1中的方法是指定出站 接口（Serial 0）。例15-2中的方法是指定邻近路由器下一跳IP地址(172.16.2.2)。这两个命令中任何一个都将静态路由安装在Hoboken的路由选择表中。这两个命令惟一的区别是放入路由选择表中时路由器为该路由所指派的***管理距离***（*administrative distance*）不同。

例15-1 使用接口的ip route命令

```
Sterling(config)# ip route 172.16.3.0 255.255.255.0 s0
```

例15-2 使用下一跳路由器IP的ip route命令

```
Sterling(config)# ip route 172.16.3.0 255.255.255.0 172.16.2.2
```

管理距离是提供路由可靠性测量的一个可选参数。管理距离值越小表示路由越可靠。这意味着具有较小管理距离的路由将在具有较大管理距离的相同路由之前被安装。使用下一跳地址方式的默认管理距离是1。使用出站接口的默认管理距离是0。表15-1显示Cisco所支持协议的管理距离值。具有较小管理距离的路由比具有较大管理距离的路由更可信。如果管理距离不是所希望的默认值，那么一个介于0-255之间的数值可以在下一跳或出站接口后输入，如下所示：

```
ip route 172.16.3.0 255.255.255.0 192.168.2.1 255
```

表15-1 Cisco 管理距离

路由源	默认距离值
直连接口	0
静态路由	1
增强内部网关路由选择协议（EIGRP）汇总路由	5
外部边界网关协议（BGP）	20
内部EIGRP	90
IGRP	100
OSPF	110
中间系统到中间系统（IS-IS）	115

续表

路由源	默认距离值
路由选择信息协议（RIP）	120
外部网关协议（EGP）	140
外部EIGRP	170
内部BGP	200
未知	255

如果路由器不能到达路由所指向的出站接口，该路由将不会被安装在路由选择表内。这意味着如果一个接口关闭了，那么该路由将不会出现在路由选择表里。

有时会出于备份目的使用静态路由。路由器上配置的静态路由仅在动态学习的路由失效时才会被使用。为了以这种方式使用静态路由，就要将静态路由的管理距离设置得高于正在使用的动态路由选择协议的管理距离。

15.2.4　配置静态路由

本节将列出配置静态路由的步骤，并给出一个简单网络的静态路由配置的例子。

使用以下步骤配置静态路由：

步骤1　确认所有想要到达的目的网络、它们的子网掩码和它们的网关。网关可以是本地接口或者是指向所要到达目的地的下一跳地址。

步骤2　进入全局配置模式。

步骤3　输入ip route命令和目的网络地址、子网掩码，以及步骤1中的相应网关。包括可选的管理距离。

步骤4　重复步骤3以完成步骤1中定义的许多目的网络。

步骤5　退出全局配置模式。

步骤6　使用copy running-config startup-config或write memory命令将活动配置保存到NVRAM中。

图15-9中的网络示例是一个由3个路由器组成的简单配置。必须配置Hoboken使其可以到达172.16.1.0网络和172.16.5.0网络。这两个网络的子网掩码都为255.255.255.0。

目的网络是172.16.1.0的分组需要被路由到Sterling。目的地址是172.15.5.0的分组需要被路由到Waycros。可以使用路由器的出站接口(S0和S1)来配置静态路由从而实现以上过程，如例15-3所示。

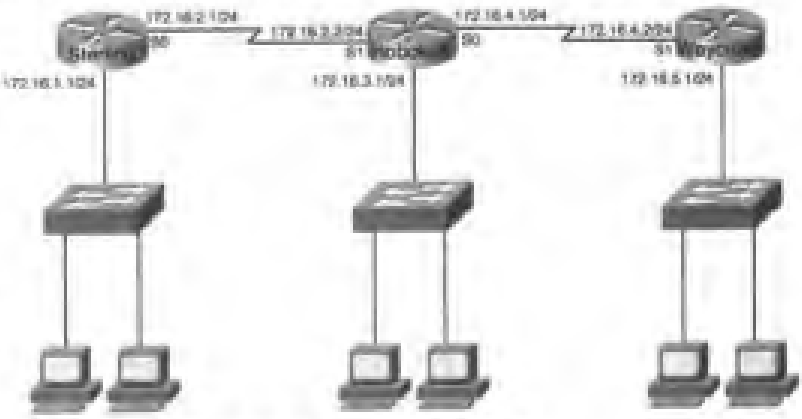


图15-9　静态路由操作

例15-3　使用出站接口的ip route命令

```
Hoboken(config)# ip route 172.16.1.0 255.255.255.0 s1
Hoboken(config)# ip route 172.16.5.0 255.255.255.0 s0
```

两个静态路由首先被配置使用本地接口作为到目的网络的网关，如图15-10所示。因为没有指定管理距离，所以在路由被装入路由选择表时缺省为0。记住管理距离为0与直连网络一样。

两条静态路由也可以使用下一跳地址作为网关进行配置。第一条路由到172.16.1.0网络的网关是172.16.2.1。第二条路由到172.16.5.0网络的网关是172.16.4.2。例15-4显示了使用下一跳接口地址的静态路由配置，并且包括将会显示在配置文件上的注释（以!开始）。因为没有指定管理距离，所以缺省为1。

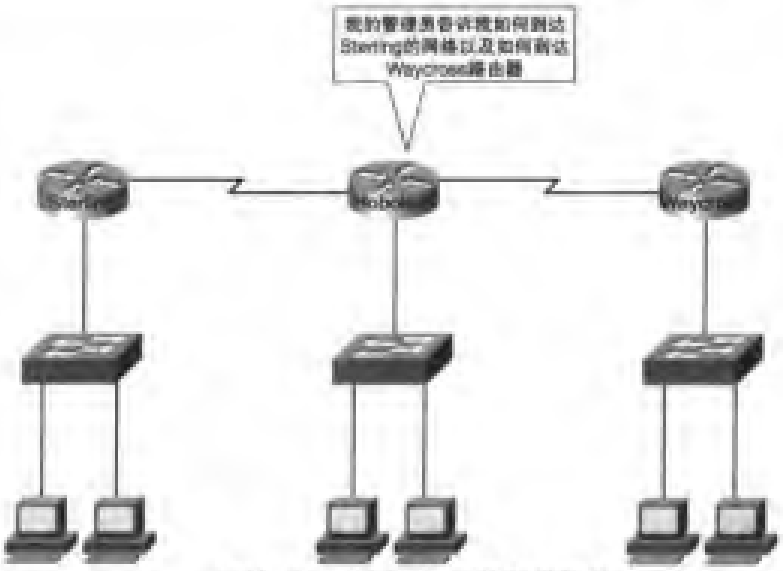


图15-10 管理员配置的静态路由

例15-4使用下一跳和注释的ip route命令

```
Hoboken(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1
!This command points to Sterling's LAN
Hoboken(config)# ip route 172.16.1.0 255.255.255.0 172.16.4.2
!This command points to Waycross LAN
```

实验活动 使用静态路由

在本实验中，要在路由器之间配置静态路由，使得数据可以在它们之间传送而不必使用动态路由选择协议。

15.2.5 如何使用默认路由

图15-11显示了默认路由的使用，默认路由是一条把目的网络没有明确列在路由选择表中的分组直接指向下一跳的路由选择表项。可以将默认路由设置为静态配置的一部分。

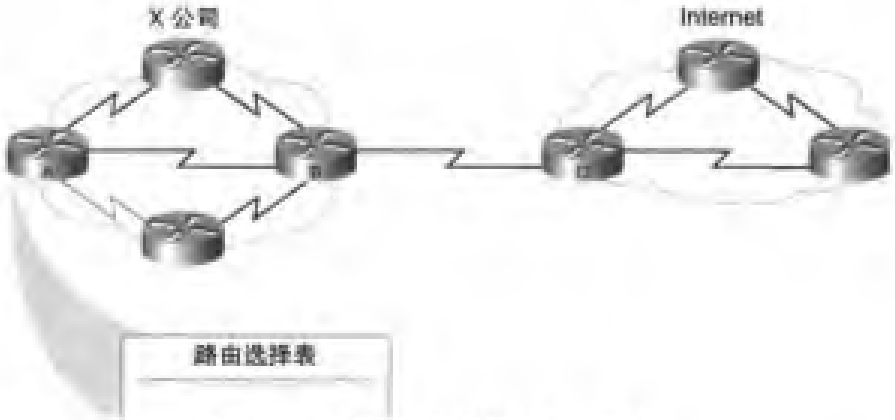


图15-11 使用下一跳的静态默认路由

在这个例子中，X公司路由器对X公司的网络拓扑有明确的认识，但对其他网络则没有。维护每一个经Internet网络云到达的其他网络的信息是不必要和不切实际的。

X公司中的每个路由器可以使用默认路由将分组指向Internet，从而到达任何一个未知的目的，而不是维护特定网络的信息。

15.2.6 配置默认路由转发

默认路由用来路由那些目的不匹配路由选择表中的任何一条其他路由的分组。路由器典型地为Internet边界流量配置一条默认路由，因为维护Internet上所有网络的路由是不切实际和不必要的。事

实上默认路由是使用以下格式的一条特殊的静态路由：

```
ip route 0.0.0.0 0.0.0.0 {next-hop-address | outgoing interface}
```

注释：0.0.0.0的掩码与转发分组的目的IP地址进行逻辑与（AND）后，总是得到网络0.0.0.0。如果分组不匹配路由选择表中的其他特定路由，那么它将被路由到0.0.0.0网络上。

使用以下步骤配置默认路由：

步骤1　进入全局配置模式。

步骤2　输入目的网络地址为0.0.0.0、子网掩码为0.0.0.0的ip route命令。默认路由的网关可以是连接外部网络的本地路由器接口，也可以是下一跳路由器的IP地址。在大多数情况下，最好指定下一跳路由器的IP地址。

步骤3　退出全局配置模式。

步骤4　使用copy running-config startup-config将活动配置保存到NVRAM中。

根据本章前面提到的内容，在图15-8中，路由器Hoboken上的静态路由配置表明Sterling上的网络172.16.1.0和Waycross上的网络172.16.5.0可以到达。这样可以从Hoboken上将分组路由到这两个网络中。但是，正如配置所示，Sterling或Waycross都不知道如何将分组送回到没有与它们直连的网络。在Sterling和Waycross上可以为这些没有直连的目的网络配置静态路由，但是在大型网络中这种方法不是一个可扩展的解决方案。

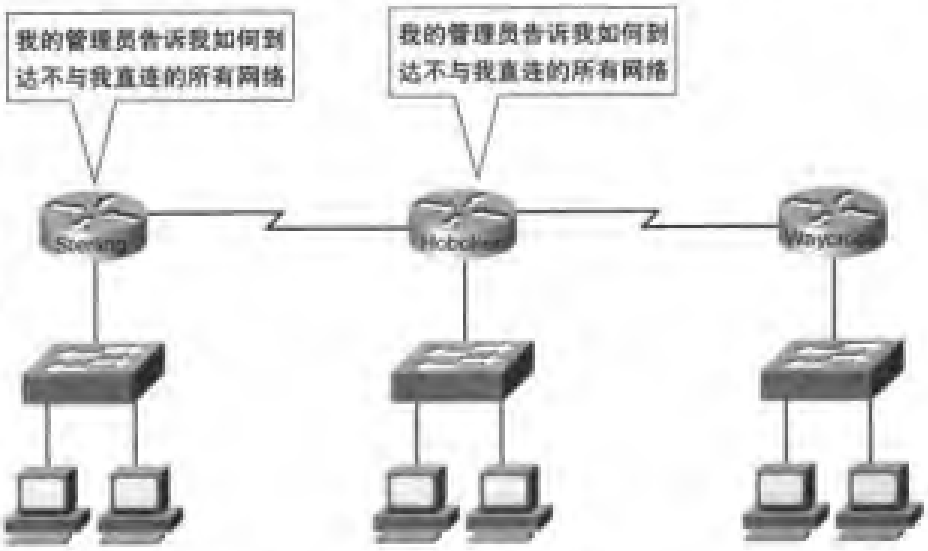


图15-12　Waycross的静态路由

Sterling通过接口S0连接所有非直连网络。Waycross也只有一条连接到达所有非直连网络，即通过接口S1。Sterling和Waycross上的默认路由为所有去往非直连网络的分组提供路由，如图15-12所示。例15-5和15-6分别显示在Waycross和Sterling上定义默认静态路由所需的命令。

例15-5　Waycross的默认路由

```
Waycross(config)# ip route 0.0.0.0 0.0.0.0 s1
```

例15-6　Sterling的默认路由

```
Sterling(config)# ip route 0.0.0.0 0.0.0.0 s0
```

15.2.7　检验静态路由的配置

检验路由选择表中的静态路由以及配置完静态路由后路由选择是否像期望的那样工作是很重要的。show running-config命令用来查看NVRAM中的活动配置，从而检验静态路由的输入是否正确。使用show ip route命令确保静态路由在路由选择表中存在。

使用以下步骤检验静态路由的配置：

步骤1 在特权模式下，输入命令show running-config查看活动配置。

步骤2 检验静态路由已经正确输入。如果路由不正确，需要退回到全局模式下删除不正确的静态路由，并输入正确的路由。

步骤3 输入命令show ip route。

步骤4 检验配置的路由在路由选择表中。

15.2.8 静态路由配置的故障排除

拥有静态路由选择方面的故障排除工具和操作过程的信息与拥有网络任何其他 方面的信息一样重要。你可以使用show interfaces命令来查看作为路由网关的接口的状态和配置情况。使用ping命令可以帮助确定端到端连接是否存在。如果在一个ping之后没有收到一个回应（echo）应答，可以使用traceroute命令来确定路由路径上的哪个路由器丢弃了分组。路由选择过程必须发生在分组传输所经过的每一台路由器上，否则分组就会被丢弃。在大多数情况下，分组确实到达了它们的目的，但是远程网络路由器不具有回应发送者的路由信息。

使用以下步骤对静态路由配置进行故障排除：

步骤1 确定该路由作为网关的链路是可用的。

步骤2 输入命令show interfaces，检验这个接口状态是up，链路协议状态是up。

步骤3 检验接口所使用的IP地址是正确的。

步骤4 ping直接连接到路由网关上的远程路由器接口的IP地址。如果ping不成功，问题与路由选择无关。直接相连的路由器的一个或两个接口也许配置不正确，或者链路存在物理故障。返回步骤1进行故障排除。

步骤5 如果ping远端路由器失败，使用traceroute命令来确认路由路径上的哪个路由器正在丢弃分组。

步骤6 登录到traceroute失败的路由器上。返回步骤1重新开始故障排除。

步骤7 如果ping成功了，尝试去ping远端路由器。如果这次ping也成功了，端到端的连通性已经达到。静态路由的测试完成。

15.3 动态路由选择概述

*动态路由选择*可以允许网络快速地更新和适应于变化。图15-13中显示的网络可以根据它所使用的是静态还是动态配置的路由选择信息，来不同地适应拓扑结构的变化。

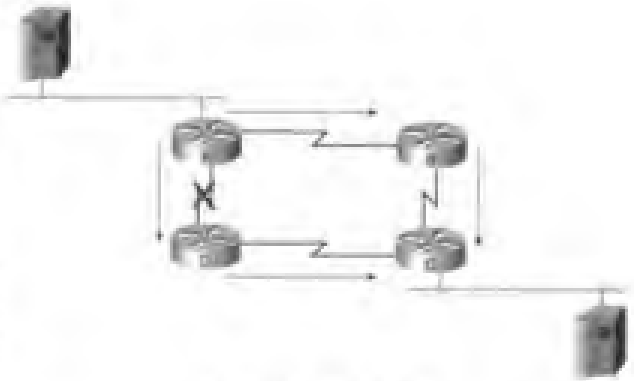


图15-13 动态路由

静态路由选择允许路由器根据人工配置的信息正确地将分组从一个网络路由到另一个网络。例如，路由器A总是将去往路由器C的流量发送给路由器D。路由器引用它的路由选择表并根据表中的静态信息将分组中继给路由器D。路由器D用同样的方法将分组中继给路由器C。路由器C将分组递交给目的主机。

如果路由器A和路由器D间的路径断开了，路由器A将不能使用静态路由将分组中继给路由器D。在路由器A被人工重新配置为经由路由器B中继分组之前，与目的网络的通信是不可能的。动态路由选择提供更多的适应性。根据路由器A产生的路由选择表，分组可以通过经由路由器D的优先路由到达其目的地。

但是，通过路由器B到达目的的第二条路径也是可用的。当路由器A意识到通向路由器D的链路断开时，它会调整自己的路由选择表，使得经由路由器B的路径成为到达目的的首选路径。路由器可以通过这条链路继续发送分组。

当路由器A和D之间的路径恢复工作后，路由器A可以再次改变它的路由选择表，来指示通过路由器D和路由器C的逆时针方向的路径是到达目的网络的优先选择。动态路由选择协议还可以为获取更好的性能指引同一会话的流量经由网络中的不同路径。这就是所谓的***负载均衡（load sharing）***。

15.3.1　路由选择协议例子

本节将提供一些最常见的路由选择协议的概要和它们的关键特性。

RIP最初定义在RFC 1058中。它的关键特点包括以下内容：

- 它是距离矢量路由选择协议。
- 它使用跳数（hop count）作为路径选择的度量标准。如果跳数大于15，则丢弃分组。
- 默认情况下，路由选择更新每30秒广播一次。

IGRP是Cisco开发的距离矢量路由选择协议。IGRP间隔90秒发送路由选择更新，通告特定自治系统[6]中的网络。IGRP提供以下设计特征和特点：

- 可处理自动处理不确定的或复杂的拓扑的多功能性。
- 可处理不同带宽和延迟的网段这种灵活性。
- 大型网络中功能的可伸缩性。

默认情况下，IGRP路由选择协议使用两个度量标准：带宽和延迟。此外，IGRP可以配置使用多个变量的组合来确定一个复合度量标准。这些变量包括：

- 带宽（Bandwidth）。
- 延迟（Delay）。
- 负载（Load）。
- 可靠性（Reliability）。

OSPF是针对IP使用的链路状态路由选择协议。链路状态协议维持一个详细的拓扑，允许协议进行计算来防止环路。在OSPF中，子网掩码同样被传送，允许诸如可变长度子网掩码（VLSM）和路由汇总（route summarization）等特征。

EIGRP是Cisco开发的平衡式混合路由选择协议。EIGRP具有距离矢量协议和链路状态协议的共同特征。EIGRP计算到网络或子网的最佳路由，并在当前路由失效时提供备选路由。EIGRP也为每个路由选择表项发送子网掩码。因此，容易支持诸如VLSM和路由汇总等特征。

BGP是外部路由选择协议。BGP被设计运行在自治系统之间。BGP可以用于两个ISP之间或者用于公司和ISP之间。

15.3.2　路由选择协议和自治系统的目的

路由选择协议的目的是建立和维护路由选择表。这个表包括所学习到的网络和与这些网络相关的端口。路由器使用路由选择协议管理从其他路由器接收到的信息以及自身接口配置中产生的信息。

路由选择协议识别所有有效的路由，将最佳路由放在路由选择表中，同时删除不再有效的路由。路由器使用路由选择表中的信息转发被路由协议分组。

路由选择算法是动态路由选择的基础。无论何时，因为网络扩大、重新配置或者故障而导致网络拓扑结构的改变，所掌握的网络信息也必须改变。网络信息需要反映新拓扑结构的准确和一致的视图。

当互联网络中的所有路由器使用相同的信息运行时，互联网络被称为已经收敛。因为快速收敛可以减少错误路由选择的决策时间，所以快速收敛是值得的。

*自治系统*将全球的互联网络划分为一些小的、更易于管理的网络。每个AS有自己的一组规则和策略，以及区分于世界其他自治系统的AS号。

15.3.3 动态路由选择操作

动态路由选择的成功基于两个基本的路由器功能：

- 路由选择表的维护。
- 以路由选择更新的形式，将信息适时地发布给其他路由器（如图15-14所示）。

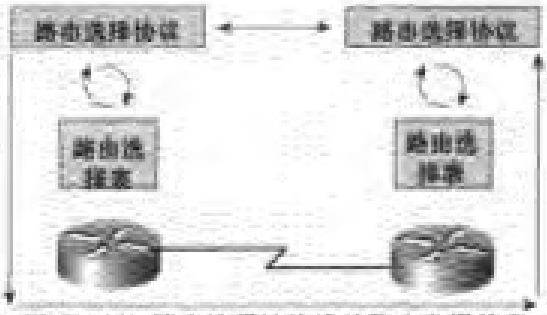


图15-14 路由选择协议维护路由选择信息

动态路由选择依赖于一个路由选择协议在路由器之间共享信息。在与相邻路由器通信时，路由选择协议定义一组规则供路由器使用。例如，一个路由选择协议描述如下：

- 如何发送更新。
- 更新中包含什么信息。
- 什么时候发送这些信息。
- 如何定位更新的接收者。

15.3.4 如何用多种度量标准来确定网络路径的距离

当路由选择算法更新路由选择表时，它的主要目标是确定路由选择表中包含的最佳信息。每个路由选择算法都以自己的方式诠释何为最佳。算法为穿越网络的每条路径产生一个数字，称为*度量标准（metric）*。通常，度量标准值越小，路径就越好，如图15-15所示。

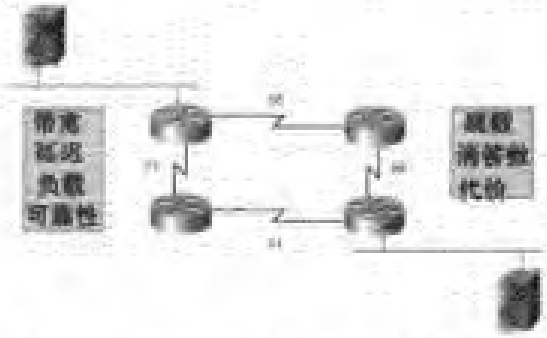


图15-15 用于定义最佳路径的度量标准

你可以基于单个特征（比如路径）来计算简单的度量标准，或者可以将几个特征复合在一起计算更为复杂的度量标准。路由器最常用的度量标准特征如下：

- **带宽**（bandwidth）——链路的数据容量（一般来说，一个10Mbit/s的以太网链路比64kbit/s专用线路更好）。
- **延迟**（delay）——将分组沿着从源到目的每条链路移动所需的时间。
- **负载**（load）——网络资源（比如路由器或链路）的活动量。
- **可靠性**（reliability）——通常参考每个网络链路的错误率。
- **跳数**（hop count）——分组到达目的之前必须经过的路由器个数。
- **滴答数**（ticks）——使用IBM PC时钟滴答计数（大约55ms，或者1/18s）的数据链路延迟。
- **代价**（cost）——一个任意值，通常基于带宽、花费或其他度量，由管理员配置指派。

15.4 识别路由选择协议的种类

大多数路由选择算法可以被分为以下3类：

- 距离矢量（Distance vector）。
- 链路状态（Link-state）。
- 平衡混合（Balanced hybrid）。

*距离矢量路由选择协议*方法确定互联网络中任何一条链路的方向（或矢量）和距离。*链路状态*

*路由选择协议*方法也被称为最短路径优先（SPF），它重建整个互联网络的精确拓扑结构。*平衡混合路由选择协议*方法结合了链路状态和距离矢量算法的特点。

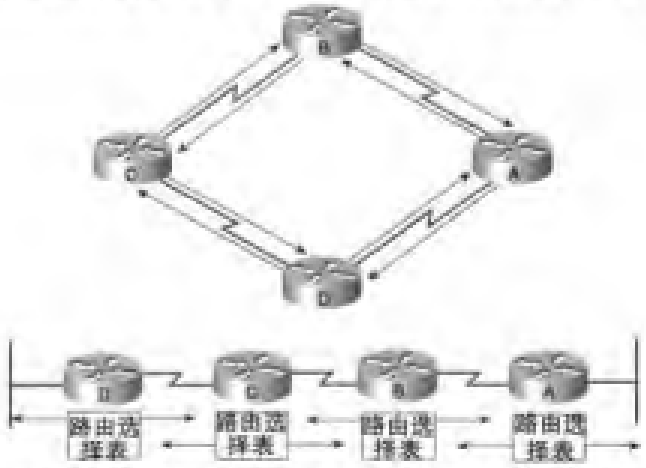
15.4.1　距离矢量路由选择协议特性

距离矢量路由选择算法定期地将路由选择表的拷贝从一个路由器发往另一个路由器。这些在路由器间的定期更新交流了拓扑的变化。基于距离矢量的路由选择算法也称为贝尔曼－福特（Bellman-Ford）算法。

在图15-16中，每个路由器收到来自相邻路由器的路由选择表。路由器B收到来自路由器A的信息。路由器B就加一个距离矢量数，例如跳数，来增加距离矢量。然后，路由器B将新的路由选择表发送给它的其他 邻居，路由器C。这种一步一步的处理发生在所有相邻路由器之间的所有方向上。

算法累积网络距离信息，以便可以维护一个网络拓扑信息的数据库。但是，距离矢量算法不向路由器提供互联网络的确切拓扑结构，因为路由器仅知道自己的邻居路由器。

每个使用距离矢量路由选择的路由器从标识自己的邻居路由器开始。图15-17显示距离矢量发现过程。每个直连网络的接口都显示距离为0。当距离矢量网络发现进程启动后，路由器根据接收自每个邻居的信息发现到目的网络的最佳路径。例如，路由器A根据接收自路由器B的信息获知其他 的网络。路由选择表中的每一条其他 网络条目通过累积的距离矢量值表示该网络在给定方向上的距离是多少。



将路由选择表拷贝定期地发送到相邻路由器并且累积距离矢量

图15-16　距离矢量原理

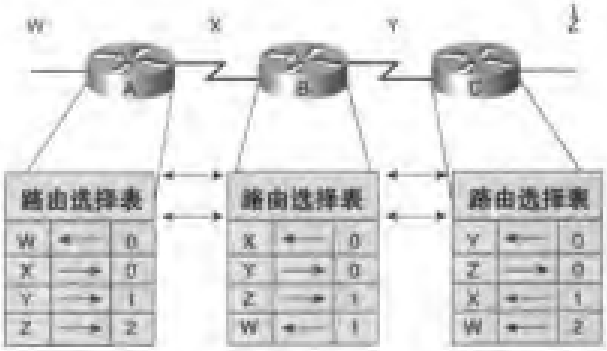


图15-17　距离矢量的网络发现

一旦网络拓扑发生变化，就会引起路由选择表更新。与网络发现过程一样，拓扑变化的更新也是路由器到路由器一步一步地进行，如图15-18所示。距离矢量算法要求每个路由器将自己的完整路由选择表发送给它的邻居。路由选择表包括以度量标准定义的总路径代价，以及到表中每个网络的第一个路由器的逻辑地址。度量标准由几个成分组成，如图15-19所示。

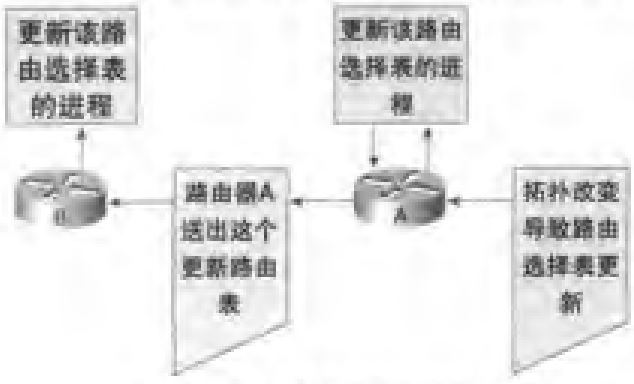


图15-18　距离矢量的拓扑改变

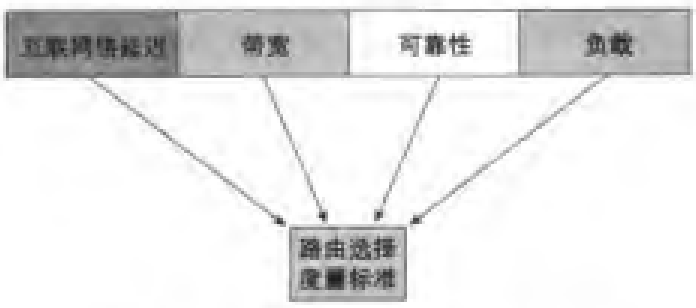


图15-19　距离矢量路由选择度量标准的组成

路由选择更新解释

每个路由器接收来自它的直连邻居路由器的路由选择表。例如，图15-18中，路由器B接收来自路由器A的信息。路由器B就加一个距离矢量数（例如跳数）来增加距离矢量，并将新的路由选择表发送给它的其他 邻居。这种一步一步的处理发生在所有相邻路由器之间的所有方向上。

距离矢量可以类比于高速公路上的标记。高速公路标记指示司机到达目的地的方向并指出到达目的地的距离。沿着高速公路走下去，还有另外的标记指向同一个目的，但是距离会越来越短。只要标示的距离越来越短，车流就可以确定在正确的方向上。

15.4.2 链路状态路由选择基础

第二种用于路由选择的基本算法是链路状态算法。链路状态算法也称为Dijkstras算法或者最短路径优先（SPF）算法。它们维护一个复杂的拓扑信息数据库。尽管距离矢量算法没有关于远端网络的确切信息以及对远端路由器的认识，链路状态算法却维护着远端路由器及其互连情况的全部信息。链路状态路由选择使用以下内容：

- ***链路状态通告（LSA）***——路由器之间发送的路由选择信息的小分组。
- ***拓扑数据库***——通过LSA收集到的信息集合。
- ***最短路径优先（SPF）算法***——基于数据库的计算，结果是SPF树。
- ***路由选择表***——已知路径和接口的列表。

工程师已经在开放式最短路径优先（OSPF）路由选择中实现了这种链路状态的原理。RFC 1583描述了OSPF链路状态的原理和操作。

图15-20举例说明了这些链路状态原理。

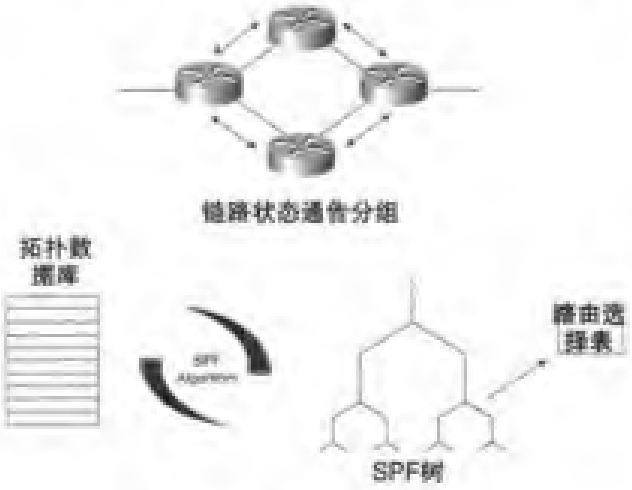


图15-20 链路状态原理

链路状态路由选择的网络发现过程

路由器之间交换LSA，首先从直连网络开始。每个路由器，并行于其他 路由器，构造一个由所有交换过来的LSA组成的拓扑数据库。

SPF算法计算网络的可到达性。路由器将这个逻辑拓扑构造成一棵树，自己作为树根，这棵树由到达这个链路状态协议互联网络中的每个网络的所有可能路径组成。然后使用SPF挑选路径。路由器在路由选择表上列出最佳路径和到这些目的网络的接口。路由器还维护其他 与拓扑和状态细节相关的数据库。

链路状态协议如何交换路由选择信息

使用链路状态网络的发现机制来创建整个网络的一张公共视图。所有的链路状态路由器共享这个网络视图。这与一个城镇拥有几张同样的地图类似。在图15-21中，3个链路状态路由器连接了4个网络（W、X、Y和Z）。链路状态路由选择的网络发现使用以下过程：

1. 路由器之间相互交换LSA，每个路由器都从与之直接相连的网络开始，因为它拥有直接的第一手信息。
2. 每个路由器，并行于其他 路由器，构造一个由来自互联网络的所有LSA组成的拓扑数据库。
3. SPF算法计算网络的可达性。路由器将这个逻辑拓扑构造成一棵树，自己作为树根，这棵树由

到达这个链路状态协议互联网络中的每个网络的所有可能路径组成。然后使用SPF挑选路径。

4. 路由器在路由选择表上列出最佳路径和到这些目的网络的接口。路由器还维护其他与拓扑和状态细节相关的数据库。

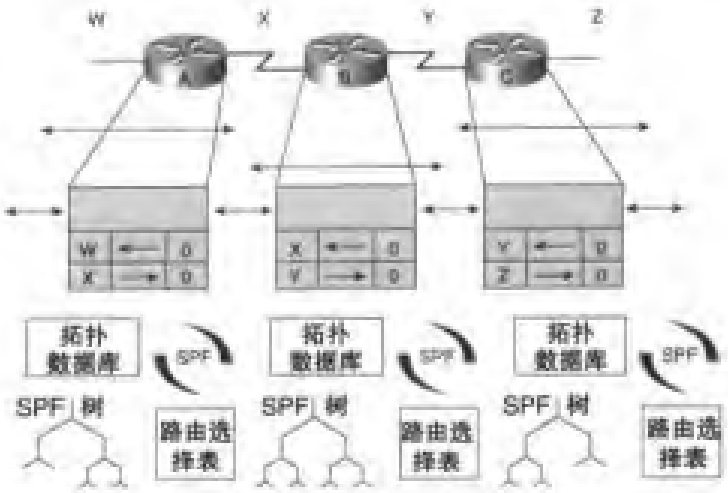


图15-21　链路状态算法最短路径计算

当路由器知道链路状态拓扑改变时，它将发送信息，以便其他 路由器可以根据该信息进行更新。这包括发送公共路由选择信息给互联网络上的所有路由器。为了达到收敛，每个路由器需要明了它的邻居路由器、路由器的名字、接口状态和到邻居的链路代价。路由器构造一个LSA分组，该分组列出了这些信息以及新邻居、链路代价的改变和链路不再有效等。然后这个LSA分组被发送出去，以便所有其他路由器接收该分组。图15-22显示一个链路状态拓扑改变的例子。



图 15-22　链路状态拓扑改变

当路由器接收到一个LSA分组后，数据库根据最新的信息更新。累积的数据用来计算出互联网络的结构图，并且使用SPF算法计算出到达其他 网络的最短路径。每当一个LSA分组改变了链路状态数据库，SPF都要重新计算最佳路径并更新路由选择表。每个路由器都会考虑拓扑变化以确定最短的路径用以进行分组的路由选择。

链路状态需要考虑的问题

运行链路状态协议要注意3个问题：

- 处理器的开销。
- 内存的需求。
- 带宽的消耗。

与距离矢量路由选择协议相比，运行链路状态协议的路由器需要更多的存储容量并执行更多的进程。路由器必须有足够的内存来存放各种数据库、拓扑树和路由选择表的所有信息，如图15-23所示。初始链路状态分组的泛洪消耗带宽。在初始化的发现过程中，所有使用链路状态路由选择协议的路由器向其他 所有的路由器发送LSA分组。这种行为充满了互联网络并临时减少了用于传输用户数据流量的带宽。在初始的泛洪后，链路状态路由选择协议一般只需要很小的带宽发送反映拓扑变化的很少的或事

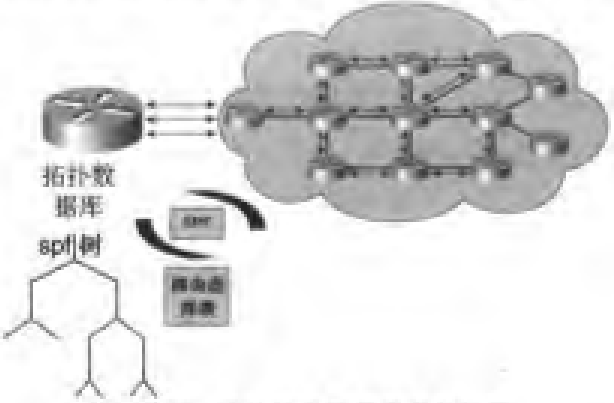


图15-23　链路状态需要考虑的问题

件触发的LSA分组。

15.4.3 混合路由选择协议特性

第三种路由选择协议是平衡混合路由选择，它具有距离矢量和链路状态两种路由选择协议的特点。平衡混合路由选择协议使用具有更精确度量标准的距离矢量来确定到目的网络的最佳路径。但是，它们与大多数距离矢量协议不一样的地方是它们使用拓扑改变来触发路由选择数据库的更新，而不是周期性的更新。

类似链路状态协议，平衡混合路由选择协议收敛很快。但是它与距离矢量和链路状态协议不同的是使用更少的带宽、内存和处理器开销。混合协议的例子有中间系统到中间系统（IS-IS）和增强内部网关路由选择协议（EIGRP）。

15.5 配置路由器使用路由选择协议

在路由器上启动IP路由选择协议，必须设置全局和接口参数。全局任务包括选择一个路由选择协议，如RIP、IGRP、EIGRP或OSPF。路由选择配置模式中的主要任务是指明IP网络号。动态路由选择使用广播和组播与其他路由器通信。路由选择的度量标准帮助路由器找到到达每个网络或子网的最佳路径。

router命令启动一个路由选择进程。router命令的语法如下：

```
Router(config)# router protocol[options]
```

其中：

- *protocol*可以是RIP、IGRP或者EIGRP。
- *options*表示自治系统号码，例如IGRP和EIGRP协议中所使用的。

network命令是必需的，因为它允许路由选择进程识别参与发送和接收路由选择更新的接口。network命令的语法如下：

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

这里的network number是直连网络的IP网络地址。

对于RIP和IGRP，网络地址必须是基于网络分类的地址，而不是子网地址或者是单独的主机地址。主要的网络地址被限制为A类、B类和C类网络号。

在TCP/IP协议集的Internet层上，路由器可以通过加入确切的路由选择算法使用IP路由选择协议完成路由选择。IP路由选择协议的例子包括以下协议，如图15-24所示：

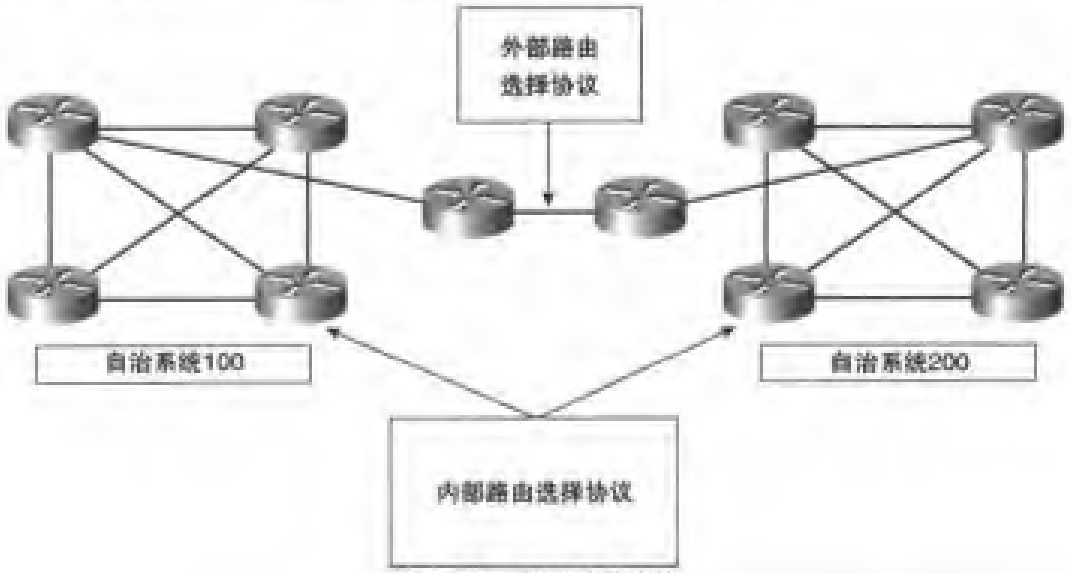


图15-24 路由选择协议

- **路由选择信息协议**（*RIP*）——一个距离矢量内部路由选择协议。
- **内部网关路由选择协议**（*IGRP*）——Cisco公司开发的一个距离矢量内部路由选择协议。
- **开放式最短路径优先**（*OSPF*）——一个链路状态内部路由选择协议。
- **增强内部网关路由选择协议**（*EIGRP*）——Cisco公司开发的一个平衡混合内部路由选择协议。
- **边界网关协议**（*BGP*）——一个外部路由选择协议。

15.6　自治系统和IGP与EGP

内部网关协议（*IGP*）被设计用于由一个组织控制或者管理的网络中。IGP被设计用来发现穿越网络的最佳路径。换言之，度量标准和如何使用度量标准在IGP中是非常重要。

外部网关协议（*EGP*）被设计用于两个不同组织所控制的网络之间。EGP一般用在Internet服务提供商（ISP）之间或公司与ISP之间。例如，一个公司在它的路由器和ISP内的路由器之间使用BGP，即EGP。IP EGP在路由选择前需要以下3组信息：

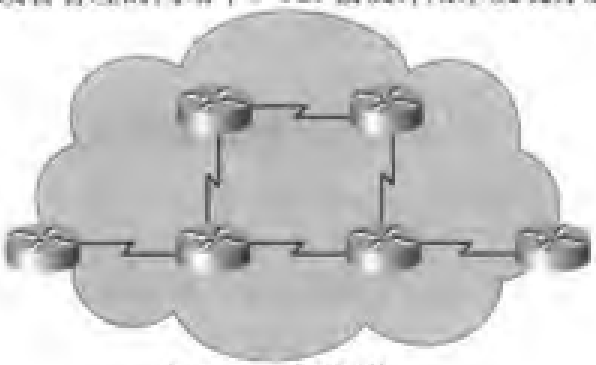


图15-25　自治系统

- 用于交换路由选择信息的一组邻居路由器。
- 通告为可以直接到达的一组网络。
- 本地路由器的自治系统号。

EGP必须隔离自治系统。因为自治系统被不同的管理机构管理，而网络必须有一个协议用于不同系统之间的通信。图15-25显示了一个自治系统。

美国Internet编号注册局（ARIN）或ARIN提供者为每个自治系统分配一个16-bit的标识号码。诸如Cisco IGRP和EIGRP的路由选择协议需要指派一个惟一的自治系统号。

15.7　总结

本章学习了以下知识点：

- 路由器不会在没有一条到达目的网络的路由情况下发送分组。
- 网络管理员手工配置静态路由。
- 默认路由是一种特殊的静态路由，为路由器提供最后可用的网关。
- 静态和默认路由使用ip route命令配置。
- 静态和默认路由配置可以通过show ip route、ping和traceroute命令检验。
- 存在3种路由选择协议：
  - 距离矢量。
  - 链路状态。
  - 平衡混合。
- 自治系统（AS）是在同一管理下共享相同路由策略的网络集合。

关于本章学习的补充内容，请参阅本书附赠光碟中与本章相关的视频、插图和e-Lab实验。

15.8 关键术语

管理距离（*administrative distance*） 表示路由选择信息源的可信程度等级。值是0和255之间的数字。值越高，可信度越低。

自治系统（*autonomous system*） 在同一管理域下的网络集合。

平衡混合路由选择协议（*balanced hybrid routing protocol*） 利用距离矢量和链路状态协议要素的路由选择协议。

距离矢量路由选择协议（*distance vector routing protocol*） 该类路由选择算法在路由的跳数上迭代来寻找最佳路径。距离矢量路由选择算法要求每个路由器在每个更新中发送自己的整张路由选择表，但只发送给自己的邻居。距离矢量路由选择算法可能造成路由选择环路，但是比链路状态路由选择算法计算简单。也被称为Bellman-Ford路由选择算法。

动态路由选择（*dynamic routing*） 可以自动适应网络拓扑或流量改变的路由选择协议。也称为适应性路由选择。需要在路由器之间运行路由选择协议。

外部网关协议（*EGP*） 被设计用于由两个不同组织控制的网络间的路由选择协议。

内部网关协议（*IGP*） 被设计用于由单一组织控制或管理的网络内的路由选择协议。

链路状态通告（*LSA*） 在路由器之间发送路由选择信息的小分组。

链路状态路由选择协议（*link-state routing protocol*） 一个路由选择算法，即每个路由器将关于到达其邻居的代价信息广播或组播给互联网络中的所有节点。链路状态算法创建一个一致的网络视图，因此将不会形成路由选择环路。但是完成这个目的的代价是比距离矢量算法更大的计算难度和更多分布广泛的流量。

负载共享（*load sharing*） 动态路由选择协议为得到更好的性能，将同一会话的流量定向到网络中的不同路径。

度量标准（*metric*） 在网络中为每个路径产生一个数值的算法。典型的是度量标准值越小，路径就越好。

被路由协议（*routed protocol*） 一个可以被路由器路由的协议。路由器必须有能力根据该被路由协议确定的内容说明逻辑互联网络。被路由协议的例子有AppleTalk、IPX和IP。

路由选择协议（*routing protocol*） 通过执行一个特定路由选择算法完成路由选择的协议。路由选择协议的例子有IGRP、OSPF和RIP。

路由选择表（*routing table*） 已知路径和接口构成的列表。

路由选择（*routing*） 寻找到达目的主机的路径的过程。因为在分组到达目的主机前可能经过很多的中间节点，所以路由选择在大型网络中会很复杂。

最短路径优先（*SPF*） 算法 基于数据库的计算，结果是SPF树。

静态路由选择（*static routing*） 手工定义和配置路由的过程。

拓扑数据库（*topological database*） 从LSA中收集的信息总和。

15.9 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 下面哪一项正确描述了OSI模型中第3层（网络层）的功能？
   A. 负责节点间可靠的网络通信
   B. 关注的物理寻址和网络拓扑
   C. 为通过网络的通信流量确定最佳路径
   D. 管理表示层实体间的数据交换
2. 下面哪一功能允许路由器估计到达目的地的可用路由，并建立分组的优先处理操作？
   A. 数据连接
   B. 路径确定
   C. SDLC接口协议
   D. 帧中继
3. 网络层如何从源向目的转发分组？
   A. 使用一个IP路由选择表
   B. 使用ARP响应
   C. 查询名字服务器
   D. 查询网桥
4. 路由器使用网络层地址的哪两个部分转发穿越网络的流量？
   A. 网络地址和主机地址
   B. 网络地址和MAC地址
   C. 主机地址和MAC地址
   D. MAC地址和子网掩码
5. 下面哪一项正确描述了被路由协议？
   A. 为主机间的分组传送提供足够的信息
   B. 为将分组送至更高的网络层提供必需的信息
   C. 允许路由器之间进行通信以维护及更新地址表
   D. 允许路由器绑定MAC地址和IP地址
6. 下面哪一项正确描述了路由选择协议？
   A. 一种通过执行一个算法来完成路由选择的协议
   B. 一种指定如何以及何时绑定MAC地址和IP地址捆绑的协议
   C. 一种定义数据分组中各字段格式和用法的协议
   D. 一种允许分组在主机间传送的协议
7. 距离矢量路由选择算法的优点之一是：
   A. 不可能计数到无穷大
   B. 易于在大型网络中执行
   C. 不会产生路由环路
   D. 计算简单
8. 下面哪一项最好地描述了链路状态算法？
   A. 重建整个互联网络的精确拓扑
   B. 需要大量的计算
   C. 确定互联网络中任一连接的距离和方向
   D. 几乎没有网络开销，并且减少过载流量

9. 路由环路为何会发生?

A. 互联网络发生变化后缓慢收敛的发生

B. 水平分割是人工建立的

C. 网络突然失败或者是层叠作用下拆卸另一网段

D. 网络管理员未建立和初始化默认路由

10. 下面哪一项正确描述了平衡混合路由选择?

A. 确定最佳路径，但是拓扑变化会触发路由选择表更新

B. 大量业务时使用距离矢量路由选择来确定拓扑间的最佳路径

C. 使用拓扑确定最佳路径，但是不是频繁更新路由选择表

D. 使用拓扑确定最佳路径，但是使用距离矢量绕过非活动的网络连接

11. 只有一条路径到路由器的网络称作什么?

A. 静态网络

B. 动态网络

C. 实体网络

D. stub网络

12. 哪一项最好地描述了默认路由?

A. 网络管理员手工输入的紧急数据路由

B. 当网络一部分故障时使用的路由

C. 当目的网络没有明确列在路由选择表中时使用

D. 预先设置的最短路径



第16章　距离矢量路由选择协议

目标

学习完本章之后，你应该能够：

- 描述初始路由器配置。
- 描述路由选择信息协议（RIP）特点。
- 配置RIP路由选择。
- 描述内部网关路由协议（IGRP）特点。
- 配置IGRP路由选择。
- 描述并测试在多路径上的负载均衡。

已经学习了路由选择协议后，现在将学习配置IP路由选择协议。正如你所知的一样，路由器上可以配置一种或多种路由选择协议。在本章中，将学习路由器的初始配置来启动路由选择信息协议（RIP）和内部网关路由协议（IGRP）。除此之外，还将学习如何监控IP路由选择协议。

请认真查看随书的光盘，这里面有关于这章内容的e-Lab实验，动画演示和图片库。光盘中的内容是提供一些相关这章内容的素材，帮助读者用于加深理解和巩固所学知识。

16.1　初始路由器配置

路由器在检测硬件和加载Cisco IOS软件映像后，就开始寻找并应用配置语句。这些配置语句为路由器提供了详细的路由器特定属性、协议功能和接口地址。要记住，如果路由器无法找到有效的启动配置文件，就会进入被称为设置模式（setup mode）或系统配置对话（system configuration dialog）的初始路由器配置模式。

利用设置模式命令工具，只需要回答系统配置对话中的提问。该工具会提示基本的配置信息。输入的答复使得路由器生成一个充分而最小的配置。设置工具提供以下内容：

- 接口列表。
- 选择输入全局参数。
- 选择输入接口参数。
- 设置脚本浏览。
- 选择是否希望路由器使用该配置。

当确认设置模式的输入以后，路由器就会将这些条目作为一份运行配置。路由器也会把这个配置保存在非易失性随机存取存储器（NVRAM）中，作为新的启动配置，然后就可以开始使用路由器了。要改变更多的协议和接口，可以在特权（enable）模式下输入configure命令来实现。

16.2　距离矢量路由选择

本节讲述距离矢量路由选择协议和它们的缺点，以及确定距离矢量路由选择所呈现的问题的解决方法。基于距离矢量的路由选择算法定期在路由器之间传送路由选择表的拷贝。这种路由器间的定期更新交流了拓扑的变化。

16.2.1　通过距离矢量协议维护路由选择信息

当距离矢量协议的网络发生变化的时候，一定会引起*路由选择表*的周期更新。路由选择表更新的效率对路由选择协议非常重要。类似于网络的发现过程，拓扑改变的更新系统地从一个路由器到另一个路由器逐步进行。图16-1说明了距离矢量协议如何处理拓扑变化。

距离矢量算法指示每个路由器将自己的整张路由选择表发送给它的每个*邻近的邻居*（*adjiacent neighbors*）。路由选择表包括整条路径的代价，这个被定义为度量标准，以及到每个网络的路径上发布路由器的逻辑地址。

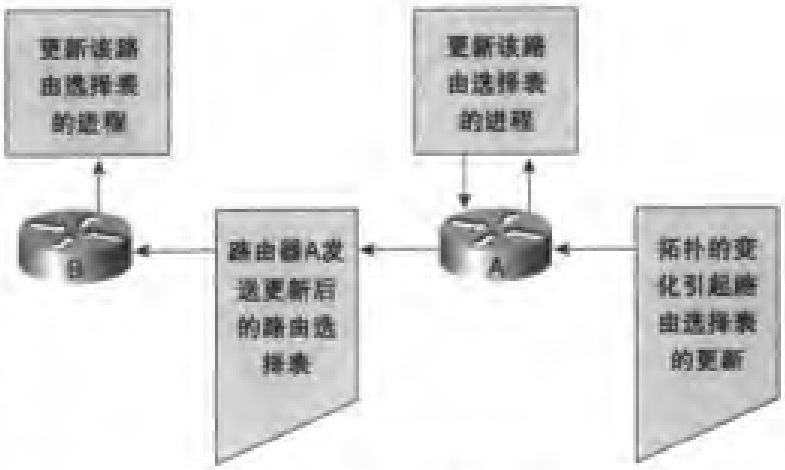


图16-1　距离矢量拓扑变化

16.2.2　多路径上的负载均衡

负载均衡是描述路由器在多条路径上将分组传输到一个目的IP地址的能力。负载均衡的概念是允许路由器利用到一个给定目的的多条路径。这些路径的获得可以通过静态方式或通过动态协议，比如RIP、EIGRP、开放式最短路经优先（OSPF）和IGRP。图16-2显示了负载均衡的一个例子。

当路由器通过多个路由选择进程或路由选择协议获得到指定网络的多条路由后，它将具有最小管理距离的路由安装在路由选择表中。有时，路由器还必须在具有相同管理距离的同一路由选择进程提供的多条路由中选择。在这种情况下，路由器选择到目的具有最小代价或度量标准的路径。每个路由选择进程计算代价的方法是不同的，而且代价可能需要手工配置才能满足负载均衡。

如果路由器收到并安装了到一个目的具有相同管理距离和代价的多条路径，就会发生负载均衡。Cisco IOS软件强制在路由选择表中只能有6条等价路由，但是有些内部网关协议（IGP）有自己的限制。比如，EIGRP允许最多有4条等价路由。

默认情况下，大多数IP路由选择协议在路由选择表中安装了最多4条并行路由。静态路由一直都安装6条路由。作为外部路由选择协议的边界网关协议（BGP）是一个例外，默认情况只允许一条路径到达目的。

最大路径数的范围从1到6条路径。要改变路由选择表中所允许的最大路径数，可以在路由器配置模式下使用以下命令：

maximum-paths *maximum*

IGRP可以最多在6条非等价链路上进行负载均衡。RIP网络必须在具有相同跳数值的路径上进行负载均衡，而IGRP使用带宽来确定如何进行负载均衡。

在图16-2中，有3条路径可以访问X网络：

- 从E经B到A，度量标准值是30。
- 从E经C到A，度量标准值是20。
- 从E经D到A，度量标准值是45。

路由器E选择第2条路径，从E经C到A的度量标准值是20，这比另外两条路径的度量标准值30和45都要小。如果有两条或者更多的路径具有相同的度量标准值，就可以发生负载均衡。

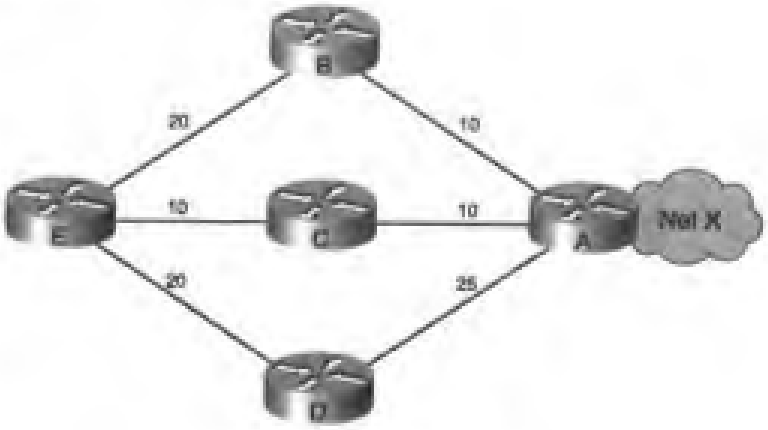


图16-2 负载均衡

当进行IP路由选择时，Cisco IOS软件提供两种负载均衡的方法：

- 基于每个分组的负载均衡。
- 基于每个目的的负载均衡。

如果启用进程交换，路由器将基于每个分组交替路径。如果启用快速交换，那么只有一条到达目的地址的替换路径会被缓存，因此到达指定主机的分组流的所有分组都使用相同的路径。到达同一网络中不同主机的分组才会使用替换路径，这个时候的流量是基于目的地址进行负载均衡的。

16.2.3 如何在距离矢量中产生路由选择环路

如果网络或路由选择拓扑变化造成路由选择条目不一致，结果使网络经历了缓慢的***收敛***（*convergence*），那么就会产生路由选择环路。图16-3显示了路由选择环路。

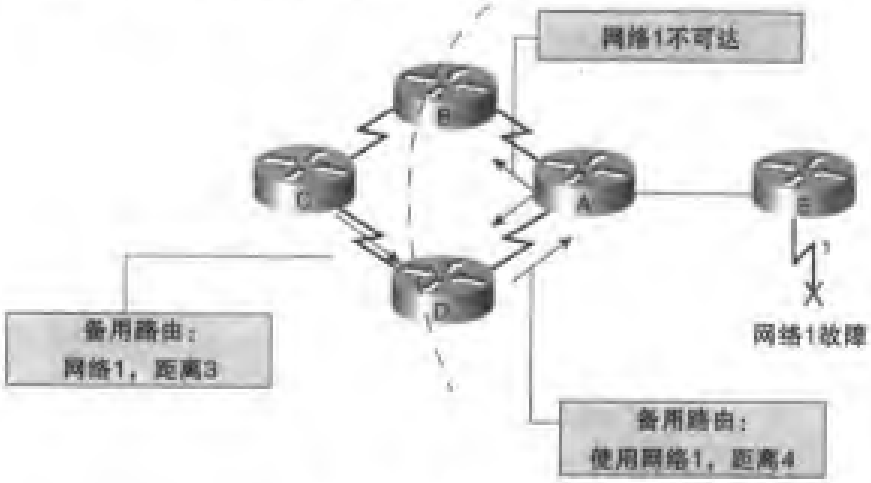


图16-3 路由选择环路

路由选择环路产生的过程（基于图16-3）如下：

1. 在网络1出现故障以前，所有的路由器都拥有一致的认识和正确的路由选择表。这时网络被称为已经收敛。假设该例中路由器C的其他部分，到达网络1的最佳路径通过路由器B，并且从路由器C到网络1的距离是3。

2. 当网络1出现故障时，路由器E发送一条更新给路由器A。路由器A停止向网络1路由分组，但是路由器B、C和D继续向网络1路由分组，因为该故障没有通知给它们。当路由器A发出自己的更新

后，路由器B和D停止向网络1路由分组。但是路由器C仍然没有收到更新。对于路由器C而言，网络1仍然可以通过路由器B到达。

3. 现在路由器C向路由器D发送定期更新，指示有一条路径经路由器B可以到达网络1。路由器D修改自己的路由选择表以反映这条不正确的信息，并把这个信息发送给路由器A。路由器A将这个信息发送到路由器B和E，以此类推。任何到达网络1的分组现在都会沿着路由器C到B到A到D然后回到C如此循环地传输。

16.2.4　定义一个最大值来防止计数到无穷大

网络1的无效更新会不断地循环下去，直到其他进程停止该循环。这种情况被称为***计数到无穷大（count to infinity）***。尽管目的网络（网络1）已经出现了故障，分组仍然在网络中循环。当路由器计数到无穷大时，无效信息使得路由环路存在，如16-4图所示。

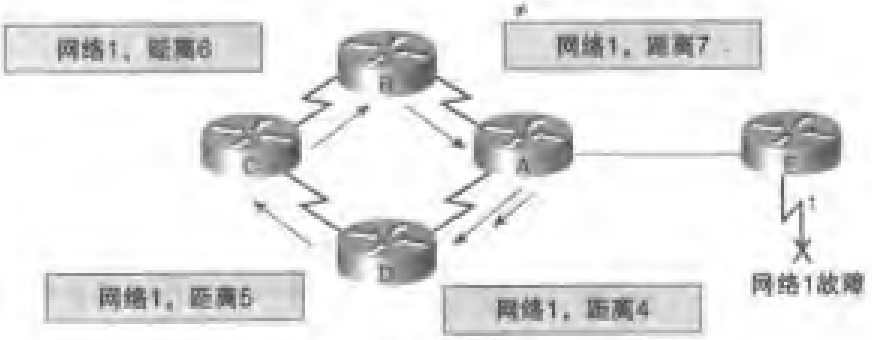


图16-4　计数到无穷大

如果没有对策来停止这个过程，那么分组被路由器转发一次，距离矢量或者度量标准跳数就会加1。度量标准在第15章“路由选择和路由选择协议”中有讲解。由于路由选择表中的不正确信息，这些分组就会在网络中循环传输。

距离矢量路由选择算法具有自我纠正能力，但是路由选择环路的问题需要计数到无穷大来解决。为了避免这种拖延问题，距离矢量协议将无穷大定义为一个特定的最大值。这个值就是路由选择度量标准，可以简化为跳数。图示16-5解释了这个概念。



图16-5　定义最大度量标准

通过为无穷大指派一个最大值，路由选择协议允许路由选择环路度量标准值超过其最大允许值之前继续存在。图16-5显示度量标准是16跳，超过了距离矢量的默认最大值15跳，路由器丢弃这个

分组。在任何情况下，当度量标准值超过最大值时，网络1被认为不可达。

16.2.5 通过水平分割消除路由选择环路

路由选择环路产生的另一种可能原因是返回给路由器的不正确信息与该路由器最初发送的正确信息矛盾。图16-6所示的以下过程解释了这个问题的产生：

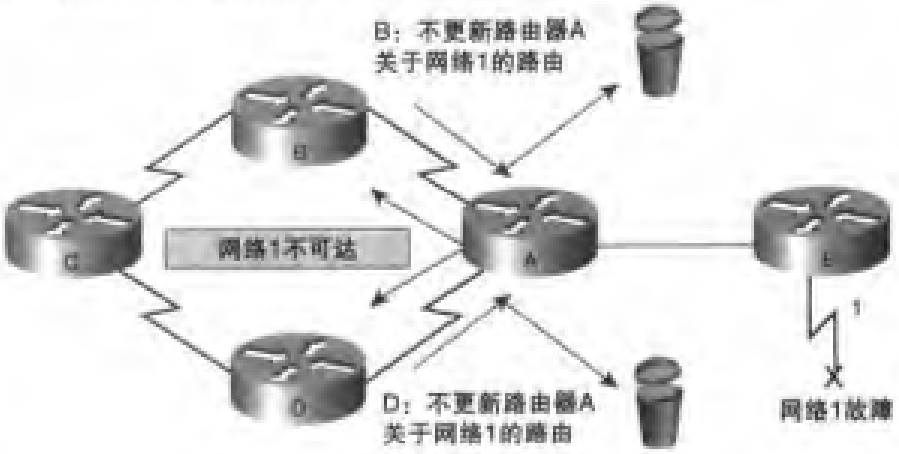


图16-6 水平分割

1. 路由器A向路由器B和D发送更新，指示网络1出现故障。然而路由器C向路由器B传输的更新指示网络1可以通过路由器D以4跳的距离到达。这个行为没有违反水平分割原则。

2. 路由器B错误地推断路由器C仍然有一条有效路径到达网络1，尽管它的度量标准差一些。路由器B向路由器A发送一个更新，通告路由器A有一条新路由到达网络1。

3. 路由器A现在确定它可以通过路由器B向网络1发送信息。路由器B又确定它可以通过路由器C向网络1发送信息，而路由器C又确定它可以通过路由器D向网络1发送信息。所有进入这个环境的分组都将在路由器之间进行循环。

4. 水平分割尝试避免这种情况。如果关于网络1的路由选择更新从路由器A到达，那么路由器B和D就不能把关于网络1的信息返回给路由器A，如图16-6所示。*水平分割（split horizon）*就减少了错误的路由选择信息，也减少了路由选择开销。

16.2.6 路由中毒

*路由中毒（route poisoning）*由各种距离矢量协议使用，用来克服大型路由选择环路，并在一个子网或网络不能被访问时提供直接的信息。路由中毒一般通过将跳数设置成为最大跳数加1来实现。

毒性反转（poison reverse）是避免路由环路的另一种方法。它的规则是：

一旦从一个接口学习到了一个路由，那么这个路由作为不可达路由从同一个接口回送。

假设图16-7中的路由器都启用了毒性反转。当路由器1从路由器2学习到了网络A后，它通过它的链路向路由器2和3通告网络A不可到达。路由器2如果收到通过路由器1到达网络A的路径，因为不可达的通告就要删除这条路径。EIGRP就结合两种规则来防止路由环路的存在。

EIGRP在以下情况中使用水平分割或通告一个路由不可达：

- 两个路由器在启动模式（第一次交换拓扑表）。
- 通告拓扑表的变化。
- 发送一个请求。

路由中毒与触发更新一起使用时，由于邻接路由器在通告中毒路由前不需要等30秒，这样就加快了收敛时间。路由中毒使得路由选择协议将失效路由通告为具有无穷度量标准值的路由。路由中

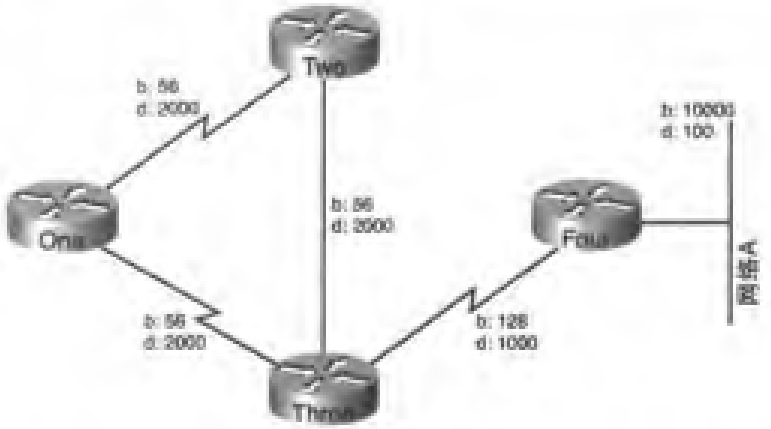


图16-7　路由中毒

毒不会破坏水平分割原则。带有毒性反转的水平分隔主要是让路由中毒，但特定用于水平分隔通常不允许路由选择信息流过的链路上。在其他情况下，失效路由被通告为无穷的度量标准值。

16.2.7　用触发更新避免路由选择环路

新的路由选择表一般是定期发送给邻接路由器的。RIP更新每30秒一次。然而***触发更新***（*triggered update*）则是立即发送以响应路由选择表的变化。路由器一旦检测到拓扑发生变化就向邻近的路由器发送一条更新消息。然后这些路由器又产生触发更新，将变化通知给它们的邻近邻居。当一条路由失效时，直接发送更新，而不是等待更新定时器期满。触发更新的使用，并结合路由中毒，能确保所有路由器在抑制（hold-down）定时器期满之前就知道失效的路由。

触发更新是无需等待更新定时器期满就发送更新。路由器立即在它的其他接口上发送路由选择信息，而不是等待路由选择更新定时器期满。这个行为使得邻接路由器上关于该路由状态的更新信息的转发和抑制（hold-down）定时器的启动更加迅速。这些更新会很快传遍整个网络。图示16-8说明了这个原理。



图16-8　触发更新

路由器C产生一条触发更新，宣布网络10.4.0.0不可到达。路由器B接收这个信息后，通过接口S0/1发布网络10.4.0.0出现故障。依次地，路由器A通过接口Fa0/0发送一条更新。

16.2.8　用抑制定时器防止路由选择环路

可以用抑制（hold-down）定时器来避免计数到无穷大的问题。这个过程的正确顺序如下：

1. 当一个路由器从邻居处接收到一条更新，指示以前可到达的网络目前不可达了，这个路由器标记该路由为不可达，同时启动一个抑制定时器。如果在抑制定时器期满以前，从同一个邻居处收到指示该网络又可到达的更新，那么该路由器就标识这个网络可以到达，并且删除抑制定时器。

2. 如果这个更新来自其他的邻接路由器，而且具有比以前记录更好的度量标准，那么该路由器就标识这个网络可以到达，并删除抑制定时器。

3. 如果在抑制定时器期满以前收到来自其他邻接路由器的更新，而且度量标准更差，则忽略这个更新。这种情况下忽略更新会允许有更多的时间将分裂性的变化传播到整个网络，如图16-9所示。

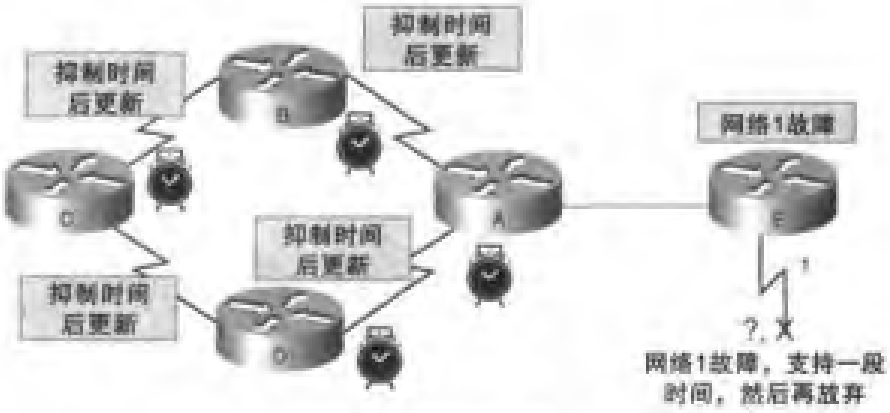


图16-9 抑制定时器

16.2.9 防止通过接口发布路由选择更新

路由过滤是通过调节那些进入或通告出路由表的路由来工作的。链路状态路由选择协议的路由过滤效果和距离矢量协议的效果不同。运行距离矢量协议的路由器通告的路由基于其路由表中的信息。由于这个原因，路由过滤会影响路由器通告给邻居的路由。

相反，运行链路状态协议的路由器基于链路状态数据库中的信息来确定路由，而不是基于邻接路由器所通告的路由条目。路由过滤对于链路状态通告或链路状态数据库没有影响。由于这个原因，这里所介绍的信息只适用于距离矢量IP路由选择协议，比如RIP和IGRP。

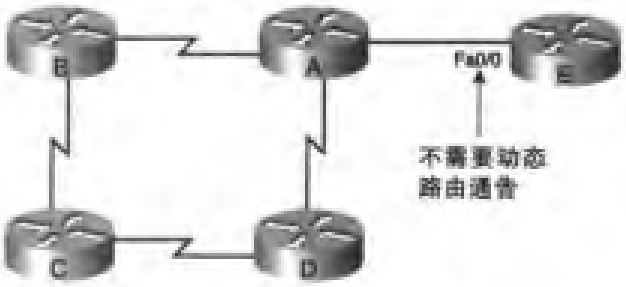


图16-10 定义一个被动接口

使用passive-interface命令能够防止路由器通过路由器接口发送路由选择更新。阻止从该路由器接口发送路由选择更新消息，可以防止网络中的其他系统动态学习这些路由。如图16-10所示，路由器E使用passive-interface命令阻止了路由选择更新的发送：

```
RouterE(config-router)# passive-interface Fa0/0
```

对于RIP和IGRP，passive-interface命令禁止路由器发送更新信息到指定的邻居，但是路由器仍然可以接收并且可以使用从邻居来的路由选择更新。禁止路由选择更新信息从这个路由器接口发送出去就是禁止在这个接口上的其他设备动态地从它那里学习路由。

16.3 检查路由选择表

路由器可以使用动态路由选择协议来获悉到达目的网络的路由，也可以经由网络管理员所配置的静态路由来获悉。路由器通常结合动态和静态路由选择来发现路由选择信息。无论使用哪一种路由发现方法，当路由器确定一条路由是到达目的的最佳路径时，就将该路由安装在自己的路由选择表中。本节描述检查并解释路由选择表的内容的方法，主要包括以下专题：

- show ip route命令。
- 确定最后的可用网关（the gateway of last resort）。
- 确定路由的源和目的地址。
- 确定路由的管理距离（administrative distance）。
- 确定路由的度量标准（metric）。
- 确定路由的下一跳（next hop）。

- 确定最近的路由更新。
- 注意到达目的的多条路径。

16.3.1　show ip route命令

路由器的一个主要功能是确定到达特定目的的最佳路径。路由器从管理员的配置或通过路由协议从其他路由器那里学习到路径，也称为路由。路由器将这些路由选择信息存储在内存（RAM）中的“路由选择表”里。路由选择表包含了路由器用来决定分组转发的一组最佳可用路由。

show ip route命令显示了IP路由选择表的内容。这张表包含了所有已知网络或子网条目，以及指示如何获得该信息的代码。show ip route命令中使用的其他关键字如下：

- connected——显示IP路由选择表中的直连路由信息。
- network——显示指定网络的路由选择信息。
- rip——显示IP路由选择表中的RIP路由选择信息。
- igrp——显示IP路由选择表中的IGRP路由选择信息。
- static——显示IP路由选择表中的静态路由选择信息。

路由选择表将网络前缀映射到一个出站接口。当路由器RTA收到一个去往192.168.4.46的分组时，它将在自己的路由选择表中查找前缀192.168.4.0/24，然后将该分组从路由选择表项所指定的接口（Ethernet 0）转发出去。如果RTA收到一个去往10.3.21.5的分组，则将该分组从接口Serial 0/0发送出去。

此外，RTA将丢弃任何去往自己路由选择表中未列出网络的分组。为了转发去往其他目的的分组，RTA的路由选择表中应该包括更多的路由。可以用两种方法来添加新的路由：

- **静态路由选择**（Static routing）——管理员手工定义到一个或多个目的网络的路由。
- **动态路由选择**（Dynamic routing）——路由器遵循路由选择协议所定义的规则交换路由选择信息，并独立选择最佳路径。

管理性定义的路由称为静态路由，因为它们在管理员手工干预之前保持不变。从其他路由器那里学习到的路由称为动态路由，因为它们在邻近路由器用新路由信息相互更新时会自动改变。每种方法都有基本的优点和缺点。

16.3.2　确定最后的可用网关

要求一台路由器维护到每个可能目的的路由是不可行的，更是不必要的。相反，路由器应该保存一条默认路由（default route），或称为最后的可用网关（gateway of last resort）。当路由器不能用路由选择表中的一条特定条目匹配一个目的网络时，就使用默认路由。路由器使用默认路由——最后的可用网关，将分组转发给另一台路由器。

默认路由的一个关键的可扩展特性是将路由选择表的大小保持得尽可能小。使得路由器能够转发去往任何Internet主机的分组而不必为每个Internet网络维护一条路由表项。在大多数情况下，默认路由都指向Internet服务提供商（ISP）的网络。默认路由可以由管理员静态输入或通过路由选择协议动态学习到。

默认路由选择过程从管理员的配置开始。在路由器动态交换信息之前，管理员必须至少为一台路由器配置了一条默认路由。管理员可以使用两条不同的命令来静态配置默认路由：

```
ip route 0.0.0.0 0.0.0.0
ip default-network
```

ip default-network命令使用动态路由选择协议在网络中建立一条默认路由。

全局命令ip default-network 195.16.11.0指定C类网195.16.11.0作为那些没有匹配路由选择表项

的分组的目的路径。对每一个配置在ip default-network命令中的网络而言，如果路由器有一条到达该网络的路由，那么该路由即被标记为候选默认路由。

创建一条到0.0.0.0/0的ip route是配置默认路由的另一种方法：

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

在配置完一条默认路由或默认网络后，show ip route命令将显示如下信息：

```
Gateway of last resort is 172.16.1.2 to network 0.0.0.0
```

路由器RTY将去往其路由选择表中未知网络的分组送交给172.16.1.2。

16.3.3 确定路由的源和目的

当流量通过一个网络云时，路径决定发生在网络层。路径决定功能使路由器能够评估到目的的可用路径，制定分组的首选处理操作。在评估网络路径时，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配置，或者通过网络中运行的动态进程收集。

网络层提供穿越互联网络的尽力而为的端到端分组传送。网络层使用IP路由选择表将分组从源网络发送至目的网络。在路由器确定所使用的路径后，就将从一个接口收到的分组转发至另一个接口或端口，这个接口反映到该分组目的的最佳路径。

16.3.4 确定从源到目的的第2层和第3层地址

将分组从源送往目的时使用的是网络层（第3层）地址，如IP地址，但是分组从一个路由器送至下一个路由器时所使用的则是不同类型的地址。在将分组从源送往目的时，第2层地址和第3层地址都要用到。

第3层地址用来将分组从源网络路由到目的网络。在这个过程中源和目的IP地址保持不变，MAC地址（第2层）则是逐跳改变。由于源主机必须要寻址转发其分组的下一跳路由器，因此数据链路层地址是必要的。而且，当分组被交付给LAN中的指定主机时，路由器使用该主机的MAC地址直接发送分组。

16.3.5 确定路由的管理距离

Cisco路由器，特别是对路由选择来说，有一个有趣的问题：路由器如何从经由路由选择协议、手工配置或其他方式获得的路由中选择一条最佳路径？

每个路由选择进程在收到更新或其他信息时，要选择到达特定目的的最佳路径，并将该路径添加到路由选择表中。

路由器根据路由的管理距离来决定是否添加路由进程所提供的路由。如果到达特定目的的一条路径具有最小的管理距离，则将该路径添加到路由选择表中；反之，则拒绝该路由。表16-1列出了Cisco IOS软件所支持的各协议的默认管理距离值。

表16-1 默认管理距离

路由类型	管理距离
直连路由	0
静态路由	1
EIGRP汇总路由	5
外部边界网关协议（eBGP）	20
EIGRP（内部）	90
IGRP	100
OSPF	110

续表

路由类型	管理距离
IS-IS	115
RIP	120
EIGRP（外部）	170
内部边界网关协议（iBGP）	200

16.3.6 确定路由的度量标准

路由选择协议使用*度量标准（metrics）*来确定到达目的的最佳路径。度量标准是量度路由好坏的一个值。有些路由选择协议只使用一个因子来计算度量标准，例如RIP-1只使用跳数这一个因子来决定路由的度量标准。另一些协议的度量标准则基于跳数、带宽、延迟、负载、可靠性、滴答延迟（ticks delay）、最大传输单元（MTU）和代价。表16-2列出了每种度量标准及其含义。

表16-2　路由度量标准

度量标准	说明
跳数（Hop count）	到达目的所经过的路由器个数。首选跳数值最小的路径
带宽（Bandwidth）	链路速度。首选带宽值最大的路径
延迟（Delay）	分组在链路上传输的时间。首选延迟值最小的路径
负载（Load）	链路的有效负荷。Cisco路由器中的取值范围是1~255；1表示负载最小，255表示负载最大。首选负载值最小的路径
可靠性（Reliability）	链路的差错率。Cisco路由器中的取值范围是1~255；255表示链路的可靠性最高。首选可靠性值最大的路径
滴答延迟（Ticks delay）	用在IPX RIP中，表示以1/18s为单位计数的链路延迟。首选滴答延迟值最小的路径
最大传输单元（MTU）	链路上所允许传输的最大分组长度（单位：字节）。首选MTU值最大的路径
代价（Cost）	管理定义的度量标准。首选代价值最小的路径

每种路由选择算法都以自己的方式来解释何谓最佳。路由选择算法为每条穿越网络的路径产生一个数值，即度量标准值。度量标准值越小，该路径越好。

有些因子是静态的，例如带宽和延迟，它们在每个接口上保持不变直到重新配置路由器或重新设计网络。有些因子是动态的，例如负载和可靠性，路由器实时计算每个接口的动态因子。

构成度量标准的因子越多，调节网络运行以满足特定需要的灵活性越强。IGRP默认使用两个静态因子来计算度量标准值：带宽和延迟。可以手工配置这两个因子来精确控制路由器所选择的路由。IGRP也可以配置使用负载和可靠性这两个动态因子来计算度量标准。通过使用动态因子，IGRP路由器可以根据当前的情形作出路由决定。因此，如果一条链路的负载很重或不可靠，IGRP将增加该链路的路由度量标准，并使用具有比该降级路由更低的度量标准的其他路由。

IGRP在计算度量标准时，为链路的每个特征因子分配不同的权值。其中，参数值（带宽，带宽/负载，延迟）经由常数K1、K2和K3加权。

度量标准 = K1 × 带宽 +（K2 × 带宽）/（256 - 负载）+ K3 × 延迟

加权常数的默认值是：K1 = K3 = 1，K2 = K4 = K5 = 0，因此

度量标准 = 带宽+延迟

16.3.7 确定路由的下一跳

路由选择算法在路由选择表中填入多种信息，其中的目的/下一跳关联信息告诉路由器将分组送给“下一跳”所指示的特定路由器，从而到达特定的目的。

当路由器收到一个送来的分组时，它要检查目的地址，并找到与该地址关联的下一跳。

16.3.8 确定最近的路由更新

网络管理员可以使用以下命令查询最近的路由更新：

- **show ip route**——用来显示路由器的IP路由选择表。
- **show ip route *network***——提供指定网络的详细路由选择信息。
- **show ip protocols**——用来显示IP路由选择协议信息。
- **show ip rip database**——显示启动触发扩展RIP时的RIP专有数据库内容。

RIP的默认更新时间是30s，IGRP的默认更新时间是90s。例16-1显示了show ip route命令的输出。

例16-1 show ip route命令输出

```
rt1# 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

R  200.200.200.0/24 [120/1] via 192.168.10.2, 00:00:14, Serial0/0
C  192.168.10.0/24 is directly connected, Serial0/0
C  192.168.0.0/24 is directly connected, Loopback0
```

路由器rt1收到来自192.168.10.2的关于网络200.200.200.0的RIP更新。RIP每30秒更新一次，例16-1中的阴影区域是该RIP路由最近一次更新至今的时间。

例16-2显示了show ip route 200.200.200.0命令的输出。

例16-2 show ip route 200.200.200.0命令输出

```
rt1# show ip route 200.200.200.0
Routing entry for 200.200.200.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 192.168.10.2 on Serial0/0, 00:00:11 ago
  Routing Descriptor Blocks:
  * 192.168.10.2, from 192.168.10.2, 00:00:11 ago, via Serial0/0
      Route metric is 1, traffic share count is 1
Rt1 has received a RIP update for the network 200.200.200.0 from 192.168.10.2.
RIP updates every 30 seconds and the last update was 11 seconds ago.
```

例16-3显示了show ip protocols命令的输出。

例16-3 show ip protocols命令输出

```
rt1# show ip protocols
```

```
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 9 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Redistributing: rip
Default version control: send version 1, receive any version
  Interface    Send  Recv    Triggered RIP    Key-chain
  Serial0/0    1     1 2
  Loopback0    1     1 2
Routing for Networks:
  192.168.0.0
  192.168.10.0
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.10.2         120      00:00:03
Distance: (default is 120)
```

例16-4显示了show ip rip database命令的输出。

例16-4 show ip rip database命令输出

```
rtl# show ip rip database
192.168.0.0/24    auto-summary
192.168.0.0/24    directly connected, Loopback0
192.168.10.0/24   auto-summary
192.168.10.0/24   directly connected, Serial0/0
200.200.200.0/24  auto-summary
200.200.200.0/24
    [1] via 192.168.10.2, 00:00:20, Serial0/0,
```

这个命令输出显示了最近一次的更新是在20s之前。

16.3.9 注意到达目的的多条路径

有些路由选择协议支持多条路径至同一目的。与单路径算法不同的是，多路径算法允许流量经由多条链路，从而提供更好的吞吐量和可靠性。

16.4 RIP的特性

*路由选择信息协议（RIP）*最初定义于1988年的RFC 1058，其关键特点如下：

- 它是一个距离矢量路由选择协议。
- 使用跳数作为路径选择的度量标准（见图16-11）。
- 路由跳数值大于15时，丢弃使用该路由的转发分组。
- 默认情况下，*路由选择的更新*每30s广播一次。

注意图16-11中，两端主机间的19.2kbit/s路径有2跳，使用3条T1链路的另一条路径有4跳。由于RIP仅根据跳数值选择路径，因此本例中选择的RIP路径是19.2kbit/s的链路，而不是更快的T1链路。

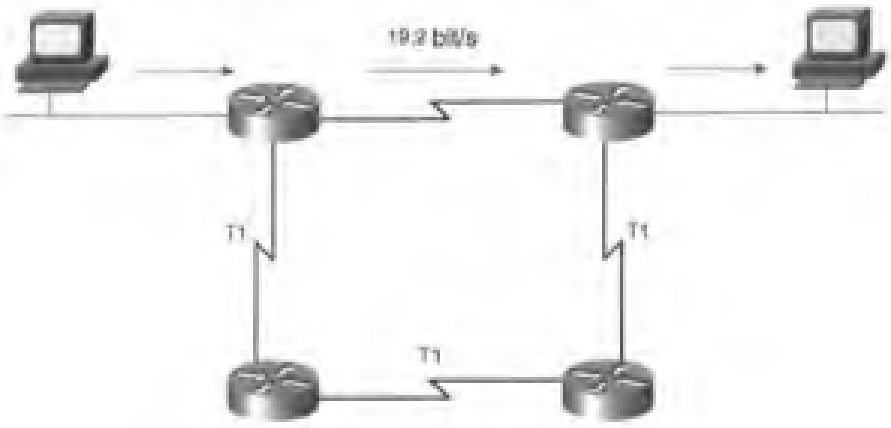


图16-11 使用跳数作为度量标准的RIP

RIP经过若干年的发展，从一个有类路由选择协议——RIP版本1（RIP-1）改进到了无类路由选择协议——RIP版本2（RIP-2）。RIP-2具有以下增强特性：

- 能够承载附加的分组路由选择信息。
- 认证机制以确保表更新的安全。
- 支持子网掩码。

RIP通过限制源和目的间路径的跳数值来防止路由选择环路。一条路径的最大跳数值是15。当路由器收到一条包含新条目或变更条目的路由选择更新时，就将度量标准值加1。如果度量标准值累加超过15，则认为该度量标准值为无穷，并且目的网络不可达。RIP还具有一些与其他路由选择协议相同的特性，例如RIP实现了水平分割和抑制机制来防止传播不正确的路由选择信息。

16.4.1 在IP网络中启动RIP

router rip命令启用RIP作为路由选择协议，然后使用network命令告之RIP通告哪些直连网络。路由选择进程将网络地址与接口关联起来，并在这些接口上使用RIP。

RIP定期发送路由选择更新消息，并在网络拓扑改变时发送触发更新。当路由器收到一条包含变更条目的路由选择更新时，则更新其路由选择表以反映新的路由。该路径的度量标准值加1，更新消息的源接口即为该路由的下一跳。RIP路由器只为每个目的维护其最佳路由，但是RIP路由器可以为每个目的维护多条具有相同度量标准值的路由。

路由器由于配置的改变而更新其路由选择表后，应立即发送路由选择更新信息，将其变化通知其他网络路由器。这些更新独立于RIP路由器所发送的周期性更新。在更新中，RIP仅通告有类网络或主类网络。

在全局配置模式下使用表16-3中的命令来启用RIP。

表16-3 启用RIP的命令

命令	用途
Router(config)# router rip	启动一个RIP路由选择进程，然后切换到路由器配置模式
Router(config-router)# network *network-number*	指定RIP路由选择进程的关联网络

以下命令显示了启用RIP和指定直连网络的过程。

```
BHM(config)# router rip
```

```
! selects RIP as the routing protocol
BHM(config-router)# network 1.0.0.0
! specifies a directly connected network)
BHM(config-router)# network 2.0.0.0
! specifies a directly connected network
```

连接网络1.0.0.0和2.0.0.0的Cisco路由器接口发送和接收RIP更新。这些路由选择更新使得路由器可以从运行RIP的邻居路由器处获悉网络拓扑。

16.4.2　使用ip classless命令

有时，路由器会收到去往未知子网的分组，而该路由器的直连子网与这个未知子网同属一个IP网络。使用ip classless这个全局配置命令能够将这些分组转发给可能的最佳超网路由。ip classless命令在Cisco IOS软件的11.3版本和之后版本中默认启用。如果要禁用该特性，请使用该命令的no形式。

当这个特性被禁用时，路由器会丢弃送往没有所属网络默认路由的子网的分组。图16-12举例说明了这个原理：如果主机发送一个到128.20.4.1的分组，而此时路由器上又没有对应的网络默认路由（即128.20.0.0/16的路由）存在，那么该路由器将丢弃这个分组。

IP无类仅仅影响IOS中的转发进程操作，而不会影响路由选择表的构建。影响路由选择表的构建是有类路由选择的本质：如果知道一个主类网的一部分，而分组所送往的从属于该主类网的目的子网未知，那么该分组将被丢弃。

这条规则最令人迷惑的一点是：路由器仅当路由选择表中没有主类网络目的存在时才使用默认路由。默认情况下，路由器假定直连网络的所有子网都存在于路由选择表中。如果路由器接收到的分组其目的地址属于一个直连网络的未知子网，那么该路由器假定这个子网不存在。因此，即便有一条默认路由存在，该路由器还是要丢弃这个分组。在路由器上配置ip classless可以解决这个问题，即指示该路由器忽略其路由选择表中网络的有类边界，简单地发送到默认路由上，如图16-13所示。

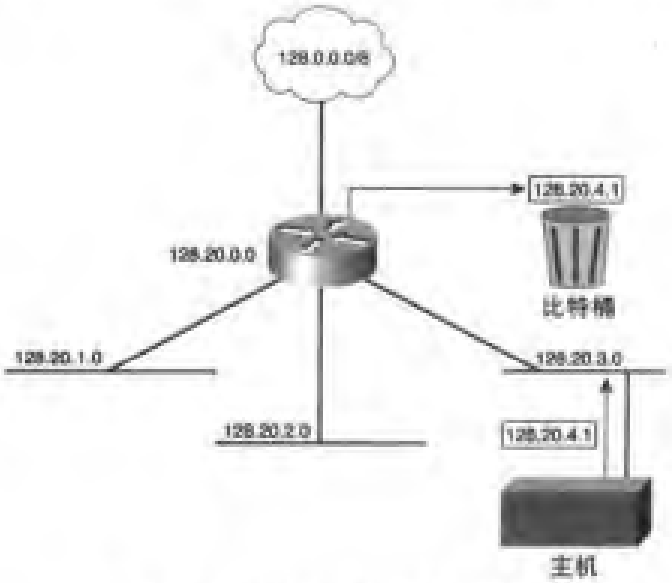


图16-12　没有使用IP无类的路由选择

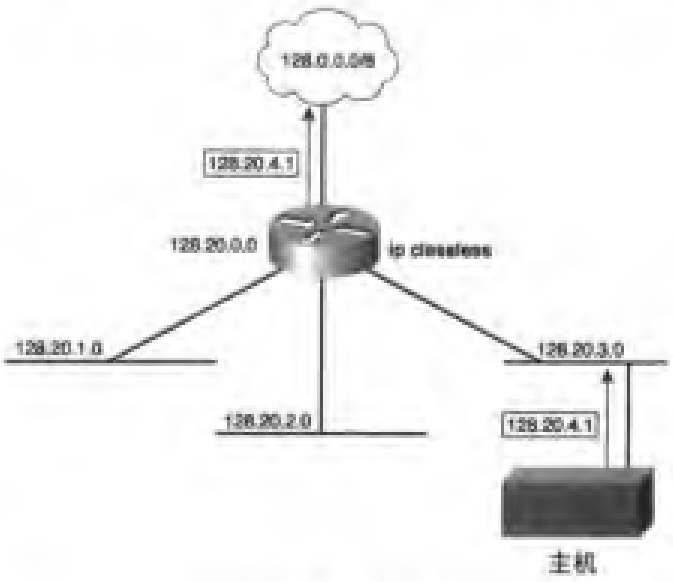


图16-13　IP无类

16.4.3　常见的RIP配置问题

RIP路由器的网络信息必须依赖于邻居路由器。RIP使用距离矢量路由选择算法，而所有的距离矢量路由选择协议具有一些导致慢收敛的问题。

这些问题包括路由选择环路和计数到无穷大，它们都导致了由于在互联网内传播包含过时路由的路由选择更新消息所引起的矛盾。

为了减少路由选择环路和计数到无穷大，RIP使用了以下方法：

- **水平分割**（Split horizon）。
- **毒性反转**（Poison reverse）。
- **抑制定时器**（Hold-down timer）。
- **触发更新**（Triggered updates）。

这些方法有的需要配置，有的不需要或偶尔需要配置。

RIP允许的最大跳数值是15，大于15跳的目的被标记为不可达。RIP的最大跳数限制了RIP在大型互联网络中的使用，但是防止了被称为“计数到无穷大”的这个问题所引起的无止境的网络路由选择环路。

水平分割规则基于这样一个事实：关于某条路由的信息没有必要沿该路由获取方向的反方向发送回去。在有些网络的配置中，可能需要禁用水平分割，其禁用是针对每个接口的。

使用以下命令可以禁用水平分割：

```
Router(config-if)# no ip split-horizon
```

抑制定时器是另一种可能需要某些变化的机制。抑制定时器在防止计数到无穷大的同时也增加了收敛时间。RIP的默认抑制时间是180s。抑制定时器阻止了次等路由的更新，但同时也阻止有效的替代路由的安装。可以减少抑制定时器来加快收敛的速度，但需要谨慎实施。理想的解决方案是将该定时器的值设置得刚好大于互连网的最长更新时间。图16-14中，4台路由器组成了一个环，每个路由器有一个30s的更新时间，可能的最长环时间是120s，因此抑制定时器应该设置为稍大于120s。

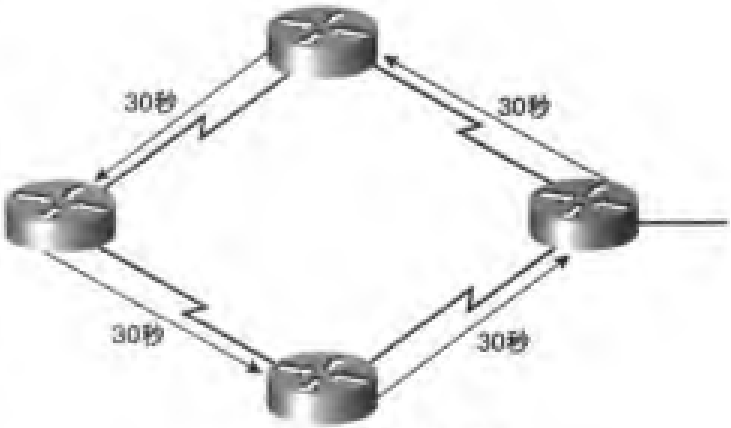


图16-14 抑制定时器

使用以下命令可以修改抑制定时器：

```
CAD(config-router)# holdown-timer seconds
```

一个影响收敛并能够配置的附加项目是更新间隔。Cisco IOS软件默认每30s运行一次IP RIP更新。这个时间可以重新配置得长一些以节约带宽，或者短一些以减少收敛时间。

使用以下命令可以修改更新间隔：

```
CAD(config-router)# update-timer seconds
```

本章的前面部分曾经讨论过路由选择协议的另一个问题是在某个接口上通告不必要的路由选择更新。当使用network命令后，RIP将从所有位于该命令所指网络地址范围内的接口上发送通告。为了控制用来交换路由选择更新信息的接口，网络管理员可以通过配置passive-interface命令来禁止指定接口上的路由选择更新的发送。

网络管理员可能需要在非广播网络（如帧中继）中配置RIP来交换路由选择信息，但是因为RIP是一个广播协议，因此需要明确指定邻居RIP路由器。以下命令可以用来定义用于交换路由选择信息的邻居路由器：

```
CAD(config-router)# neighbor ip address
```

默认情况下，Cisco IOS软件接收RIP-1和RIP-2分组，但是只发送RIP-1分组。网络管理员可以配置路由器只接收和发送RIP-1分组，或者只发送RIP-2分组。在路由器配置模式下使用表16-4中列

出的命令可以配置路由器只发送和接收一种版本。

表16-4　指定RIP版本

命令	用途
(config-router) # version {1|2}	配置整个软件接收和发送的仅是RIP-1或仅是RIP-2分组
(config-if) # ip rip send version 1	配置一个接口仅发送RIP-1分组
(config-if) # ip rip send version 2	配置一个接口仅发送RIP-2分组
(config-if) # ip rip send version 1 2	配置一个接口仅发送RIP-1或RIP-2分组

为了控制如何处理一个接口上收到的分组，可以使用表16-5中描述的命令。

表16-5　控制分组

命令	用途
(config-if) # ip rip receive version 1	配置一个接口仅接收RIP-1分组
(config-if) # ip rip receive version 2	配置一个接口仅接收RIP-2分组
(config-if) # ip rip receive version 1 2	配置一个接口仅接收RIP-1或RIP-2分组



实验活动　配置RIP

在本实验中，使用C类网络设计IP编址方案，并在所有的路由器上配置RIP。

16.4.4　检验RIP的配置

有些命令可以用来检验是否正确配置了RIP，其中最常用的两个命令是show ip route和show ip protocols。

show ip protocols命令输出配置在路由器上的所有IP路由选择协议信息，如例16-5所示。这些输出可以用来检验大部分、但不是所有的RIP配置。一些最普通的检验项目如下：

- 配置了RIP。
- 从正确的接口发送和接收RIP更新。
- 发送和接收的是正确的RIP版本。
- 路由器通告了正确的网络。

例16-5　show ip protocols命令输出

```
GAD# show ip protocols
Routing Protocol is "rip"
! Line above verifies that RIP is configured
  Sending updates every 30 seconds, next due in 5 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
! Line above verifies the RIP version
    Interface    Send   Recv   Triggered RIP   Key-chain
! Line above verifies RIP interfaces
    FastEthernet0/0      1      1 2
    Serial0/0            1      1 2
```

```
  Routing for Networks:
    192.168.1.0
    192.168.2.0
! Lines above verify networks being advertised
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2          120      00:00:11
  Distance: (default is 120)
```

show ip route命令可以用来检验接收并安装在路由选择表中的RIP路由，如例16-6所示。检查该命令的输出来查看标记为“R”的RIP路由。注意，由于网络要经过一段时间后才能收敛，因此这些路由不会立刻出现在路由选择表中。

例16-6 show ip route命令输出

```
GAD# 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

C  192.168.1.0/24 is directly connected, FastEthernet0/0
C  192.168.2.0/24 is directly connected, Serial0/0
R  192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:07, Serial0/0
! Line above verifies RIP routes received
```

最后一条以字母R开头的表项表示网络192.168.3.0是通过RIP获知的，并可以经由连接在该路由器Serial0/0接口的邻接路由器（下一跳）接口192.168.2.2到达该网络。

以下是用来检查RIP配置的一些其他命令：

- **show interface** *interface*
- **show ip interface** *interface*
- **show running-config**

这些命令在检查特定接口的信息时非常有用。使用show interface命令可以显示一个接口的所有信息，包括该接口是开还是关、协议类型、IP地址，以及该接口上所配置的封装类型。基本上，这些命令为管理员提供了关于某个特定接口的所有可用配置信息。show running-config命令用来显示路由器及其所有接口的当前配置。回忆一下，Cisco路由器的每个协议都是独立于其他协议运行的。因此，要仅列出关于指定接口的IP信息就必须在show ip interface命令中包含ip。

16.4.5 RIP的故障排除

大多数的RIP配置错误是包括错误的network语句、不连续的子网或水平分割。用来发现RIP更

新问题的主要工具是debug ip rip命令。

debug ip rip命令显示了发送和接收到的RIP路由选择更新。图16-15和例16-7显示了一个路由器使用debug ip rip命令及其收到的一个更新。

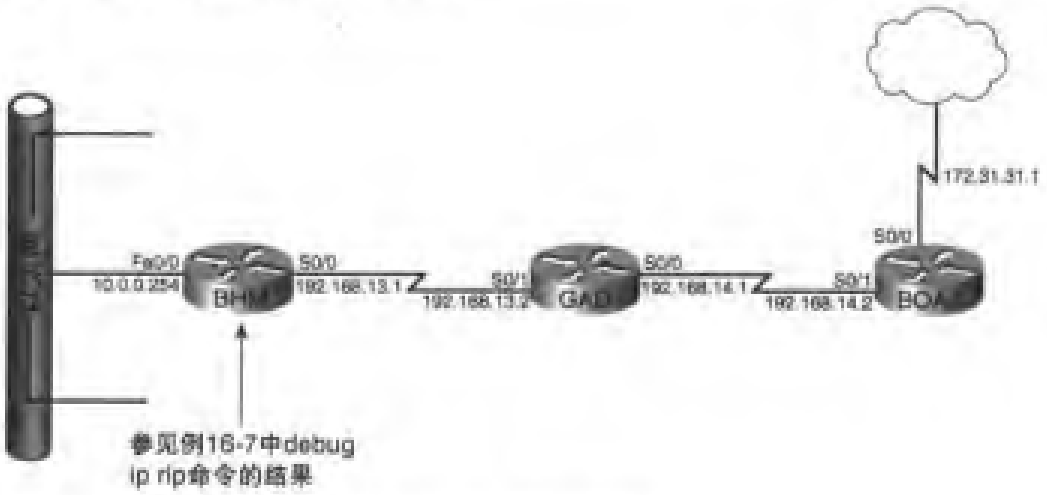


图16-15　调试RIP网络

例16-7　debug ip rip输出

```
BHM#debug ip rip
RIP event debugging is on
BHM#
00:45:36 RIP:received v1 update from 192.168.13.2 on Serial0/0
00:45:36      192.168.14.0 in 1 hop
00:45:36      172.31.0.0 in 2 hops
00:45:36      172.29.0.0 in 15 hops
00:45:36 RIP sending v1 update to 255.255.255.255 via Serial0/0 (192.168.13.1)
00:45:36      network 10.0.0.0, metric 1
00:45:36 RIP sending v1 update to 255.255.255.255 via FastEthernet0/0 (10.0.0.254)
00:45:36      network 192.168.13.0 metric 1
00:45:33      network 192.168.14.0 metric 2
00:45:33      network 172.31.0.0 metric 3
00:45:36      network 172.29.0.0 metric 16
```

在以上图例中，路由器在两个RIP接口上发送更新信息。其输出显示该路由器使用RIP-1，并且广播更新信息（地址255.255.255.255）。阴影部分的圆括号内数字表示封装在IP头中的RIP更新源地址。

在debug ip rip的输出中可以发现几个问题。其中一对可以被诊断出的问题是不连续子网或重复子网。这些问题的症状是路由选择协议所通告的网络路由的度量标准小于接收到的该网络的度量标准。

例16-8显示了debug ip rip命令的输出。

例16-8　debug ip rip命令输出

```
BMH#debug ip rip
RIP event debugging is on
```

```
BHM#
7w2d: RIP: received v1 update from 192.168.13.2 on serial0/0
7w2d:      192.168.14.0 1 hop
7w2d:      172.31.0.0 in 2 hops
7w2d: RIP: sending v1 update to 255.255.255.255 via Serial0/0 (192.168.13.1)
7w2d:      network 172.31.0.0 metric 1
7w2d: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (10.0.0.254)
7w2d:      192.168.13.0 metric 1
7w2d:      192.168.14.0 metric 2
```

另外，还可以使用以下命令对RIP进行故障排除：

- **show ip rip database**——用来显示启用触发扩展RIP时的RIP专有数据库的内容。
- **show ip protocols {summary}**——用来显示IP路由选择协议信息。
- **show ip route**——用来显示路由器上的IP路由选择表。
- **debug ip rip {events}**——将路由器正在处理的RIP信息显示给管理员。
- **show ip interface brief**——在特权EXEC模式下列举接口的IP信息概要和状态概要。可选的brief参数用来显示IP状态和配置的简短提要。

以上这些命令为路由器的故障排除提供了十分有用的信息。

实验活动 RIP的故障排除

在本实验中，使用B类网络设计IP编址方案，并在所有的路由器上配置RIP。然后用debug ip rip命令观察路由选择活动，用show ip route命令检查路由。

16.4.6 RIP的负载均衡

负载均衡概念允许一个路由器使用多条最佳路径到达指定目的。这些路径可以静态或通过诸如RIP这类的动态协议来获得。

RIP最多支持6条等价路径上的负载均衡。默认使用4条路径进行负载均衡。RIP执行的是一种循环负载均衡，也就是说RIP在平行的路径上顺次转发分组。

图16-16显示了具有4条等价路径的RIP路由例子。路由器首先从连接路由器1的接口开始，然后

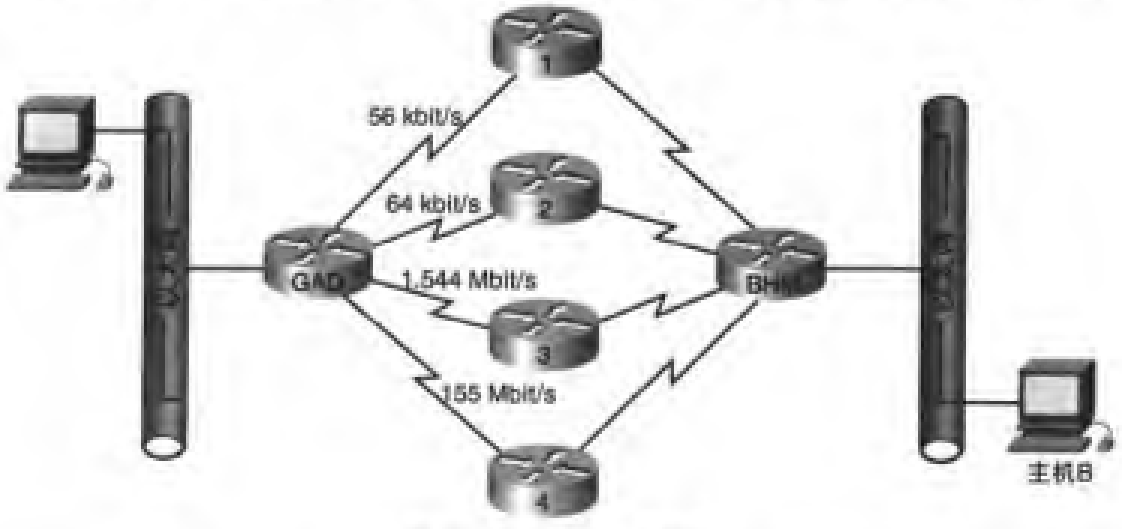


图16-16 RIP的负载均衡

按照一种确定的顺序，如1-2-3-4-1-2-3-4-1顺次循环。由于RIP的度量标准是跳数，而不必考虑链路的速度，因此两个网络间56kbit/s路径上处理的流量与155Mbit/s路径上的流量一样多。

可以使用show ip route命令来发现等价路由。例16-9显示了show ip route所输出的到特定子网的多条路由。

例16-9　通过show ip route命令输出检验等价路由

```
RouterC# show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 192.168.4.2 on FastEthernet0/0, 00:00:18 ago
  Routing Descriptor Blocks:
    192.168.4.1, from 192.168.4.1, 00:02:45 ago, via FastEthernet0/0
      Route metric is 1, traffic share count is 1
  * 192.168.4.2, from 192.168.4.2, 00:00:18 ago, via FastEthernet0/0
      Route metric is 1, traffic share count is 1
```

注意上例中有两个路由选择描述块，每一块是一条路由。星号（*）表示下一个使用的条目，对应于新流量所使用的活动路由。



实验活动　阻止一个接口上的路由选择更新

在本实验中，阻止一个接口上的路由选择更新以控制路由的通告，并观察结果。需要使用*Passive-interface*命令，并添加一条***默认路由***。



实验活动　多条路径上的负载均衡

在本实验中，配置RIP的多路径负载均衡，然后观察负载均衡的过程。

16.4.7　结合静态路由和RIP

静态路由是用户定义的路由，用来强制分组使用指定的路径到达其目的。在Cisco IOS软件不能建立到达特定目的的路由时，静态路由变得十分重要。在指定“最后的可用网关”——用来发送那些没有指定路径的分组时，静态路由也十分有用。

运行RIP的路由器可以通过来自其他运行RIP的路由器的更新接收一个默认网络地址。路由器也可以自己产生一个默认网络。

可以使用全局配置模式下的no ip route命令删除静态路由。管理员可以利用管理距离值将一条动态路由替换为静态路由选择信息。每种动态路由选择协议都有一个默认的管理距离，这使得静态路由可以作为动态路由失效时的备份路由。

指向一个接口的静态路由可以通过RIP通告出去，因为在路由选择表中这种指向接口的静态路由被看作是直连路由，从而丧失了它们的静态本性。如果为一个静态路由所指派的接口不是network命令中所定义的网络，那么动态路由选择协议将不能通告这条路由，除非指定了redistribute static命令。

当一个接口断掉时，需要从IP路由选择表中删除所有经由该接口的静态路由。另外，当软件无法找到静态路由中指定作为转发地址的有效下一跳地址时，也需要从IP路由选择表中删除该静态路由。

静态路由是由管理员特别输入的，所以路由器能确知到目的的路径。动态路由是路由器通过使

用各种路由选择协议学习到的，它不能保证路由器确知到达特定目的的路径。

为了配置静态路由，可以在全局配置模式下使用以下命令：

```
ip route prefix mask {address | interface} [distance] [tag tag] [permanent]
```

图16-17中，在GAD路由器上配置了一条静态路由，用来在RIP路由失效时取代RIP路由。例16-10显示了管理距离值为130的静态路由的添加，该路由也被称为浮动静态路由。浮动静态路由是通过声明该静态路由的管理距离（130）大于RIP管理距离（120）的方式来配置的。图16-17中的BHM路由器需要配置一条默认路由。

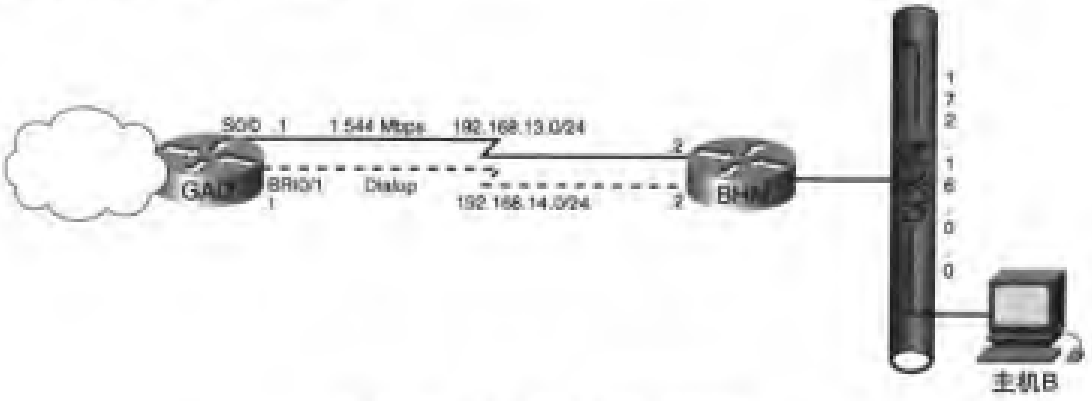


图16-17 使用浮动静态路由的RIP

例16-10显示了图16-17中浮动静态路由的配置。

例16-10 浮动静态路由

```
GAD# configure terminal
GAD(config)# ip route 172.16.0.0 255.255.0.0 192.168.14.2 130
GAD(config)# ^z
GAD# 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

C  192.168.113.0/24 is directly connected, Serial0/0
C  192.168.14.0/24 is directly connected, BRI0/1
R  172.16.0.0/16 [120/1] via 192.168.13.2, 00:00:24, Serial0/0
```

注意，由于指定了下一跳接口，此处的静态路由是作为动态路由对待的。所以用R而不是S开头。

16.5 IGRP

与RIP协议类似，*内部网关路由选择协议（IGRP）*也是距离矢量路由选择协议。与RIP不同的

是，IGRP是Cisco专有协议而不是一个标准协议。虽然它执行起来很简单，但是IGRP是一个比RIP复杂很多的路由选择协议，它能够使用多个因子来确定到目的网络的最佳路由。这一节的内容就是介绍IGRP的配置和故障排除，以及以下的IGRP主题：

- IGRP特征。
- IGRP度量标准。
- IGRP路由。
- IGRP的稳定特性。
- 配置IGRP。
- 从RIP转移到IGRP。
- 检验IGRP的配置。
- IGRP的故障排除。

16.5.1 IGRP特性

IGRP是一个距离矢量的内部网关协议（IGP）。距离矢量路由选择协议通过测量距离来算术地比较路由。这种测量的方法就是*距离矢量*。使用距离矢量协议的路由器必须以固定的时间间隔向它们的邻接路由器发送路由选择更新消息，这个更新消息是该路由器全部或部分的路由选择表。路由选择信息在整个网络中增生扩散时，路由器可以执行以下功能以及其他一些功能：

- 标识新的目的。
- 故障的获知。

IGRP是Cisco研发的一种距离矢量路由选择协议。IGRP每隔90秒发送一次路由选择更新，通告特定自治系统的网络。IGRP的关键设计特征如下：

- 多功能性地自动处理不确定的复杂的拓扑。
- 灵活地支持不同带宽和延迟的网段。
- 大型网络中功能的可伸缩性。

默认情况下，IGRP路由选择协议使用带宽（bandwidth）和延迟（delay）作为度量标准。此外，IGRP可以配置使用多个变量的组合来确定一个复合度量标准。这些变量包括：

- 带宽（Bandwidth）。
- 延迟（Delay）。
- 负载（Load）。
- 可靠性（Reliability）。

16.5.2 IGRP度量标准

show ip protocols命令显示了路由器上所使用的路由选择协议的参数、过滤器和网络信息。你需要这些信息来定义K1-K5的度量标准值，并提供关于最大跳数的信息来计算IGRP的复合度量标准，计算公式如下：

度量标准 = [K1 × 带宽 + (K2 × 带宽) / (256 - 负载) + K3 × 延迟] × [K5/(可靠性+K4)]

度量标准K1表示带宽，度量标准K3表示延迟。默认情况下，度量标准K1和K3的值设置为1，而K2、K4和K5设置为0。

默认的常数值是K1 = K3 = 1和K2 = K4 = K5 = 0。如果K5 = 0，就不使用[K5/(可靠性+ K4)]这个条件。因此，给定K1到K5的默认值，IGRP的复合度量标准计算简化为：

度量标准 = 带宽 + 延迟

这些公式中的K值是常数，可以用下面的路由器配置命令定义：

```
metric weights tos k1 k2 k3 k4 k5
```

带宽的获得是从所有出站接口中找出最小的带宽，然后用10 000 000除以这个值（带宽是以kbit/s为单位与10 000 000的比例）。延迟的获得是把所有出站接口的延迟都加起来，然后再除以10。（延迟以10微秒为单位）。要记住，具有最小度量标准的路径才是最佳路径。

这个复合度量标准在选择到目的的最佳路径时，比RIP的跳数度量标准更精确。具有最小度量标准的路径是最佳路由。

IGRP的度量标准包含以下成分：

- **带宽**（Bandwidth）——路径上的最小带宽值。
- **延迟**（Delay）——路径上的累积接口延迟。
- **可靠性**（Reliability）——到达目的的链路可靠性，通过交换keepalive信息来确定。
- **负载**（Load）——到达目的的链路负载，基于bit/s。
- **最大传输单元**（MTU）——路径上的最大传输单元值。

IGRP使用一个复合度量标准，它通过带宽、延迟、负载和可靠性来计算。默认情况下，只考虑带宽和延迟特性；其他参数值仅在配置启用后才考虑。延迟和带宽不是测量值，但是可以使用delay和bandwidth interface命令来设置。例16-11中的show ip route命令在方括号内显示了IGRP的度量标准值。第一个值表示管理距离，第二值就是计算出来的度量标准值。具有较高带宽的链路拥有较小的度量标准值，具有较小的累积延迟的路由也具有较小的度量标准值。

例16-11 show ip route命令输出显示IGRP的度量标准值

```
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

C  192.168.1.0/24 is directly connected, FastEthernet0/0
C  192.168.2.0/24 is directly connected, Serial0/0
I  192.168.3.0/24 [100/80135] via 192.168.2.2, 00:00:30, Serial0/0
```

16.5.3 内部、系统和外部IGRP路由

IGRP通告三种类型的路由：

- 内部路由是指连接到路由器接口的子网间路由。如果连接到路由器的网络没有划分子网，IGRP就不会通告内部路由。
- 系统路由是在一个自治系统内的网络路由。Cisco IOS软件从直连网络接口，以及其他IGRP通告路由或访问服务器提供的系统路由信息获得系统路由。系统路由不包含子网信息。
- 外部路由是自治系统外的网络路由，在确定最后可用网关时才考虑。Cisco IOS软件从IGRP提供的外部路由中选择一个最后可用网关。如果没有找到最好的路由而且目的也不是直连网络时，软件就使用这个最后可用网关（路由器）。如果该自治系统到一个外部网络有多条连接，不同的路由器

可以选择不同的外部路由器作为自己的最后可用网关。

16.5.4　IGRP的稳定特性

IGRP具有一系列设计用来加强其稳定性的特性，比如：

- 抑制（Holddowns）。
- 水平分割。
- 毒性反转更新。

注释：目前，IGRP已经过时了，它缺乏对变长子网掩码（VLSM）的支持。Cisco已经在IGRP基础上成功地开发了增强的内部网关协议（EIGRP），而不是开发IGRP版本2来纠正这个问题。

Holddowns用来阻止定期更新消息不适当的恢复还没有正常的路由。当一个路由器停止后，邻接路由器通过没有收到周期发送的更新信息来检测到这个状态。

水平分割源于这样一个前提，即通常沿路由来的方向发送该路由信息回去是无益的。水平分割规则帮助防止路由选择环路。

水平分割防止邻近路由器间的路由选择环路，但是毒性反转更新在对抗大规模路由选择环路时是必要的。一般而言，路由选择度量标准的增长预示着路由选择环路。那么，发送毒性反转更新来删除该路由，同时将其置为抑制状态。在IGRP中，毒性反转更新只是在路由度量标准增加到原值的1.1倍时发送。

IGRP协议还维护了一组包含时间间隔的定时器和变量，如下所示：

- *更新定时器（Update timer）*——指定路由选择更新信息发送的频率。该变量的IGRP默认值是90秒。
- *失效定时器（Invalid timer）*——指定路由器在宣告一条特定路由失效之前没有收到其路由选择更新信息的等待时间。该变量的IGRP默认值是3倍的更新时间。
- *保持定时器（Hold-time timer）*——指定忽略较差路由的时间。该变量的IGRP默认值是3倍更新时间加10秒。
- *清除定时器（Flush timer）*——指定一条路由被清除出路由选择表之前的时间。该变量的IGRP默认值是7倍的更新时间。

例16-12显示了show ip protocols命令的输出。注意指出IGRP正在运行及其度量标准值的那些行。

例16-12　IGRP路由选择统计信息

```
RouterB# show ip protocols
Routing Protocol is "igrp 101"
  Sending updates every 90 seconds, next due in 51 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
```

```
IGRP maximum metric variance 1
Redistributing: igrp 101
Routing for Networks:
  192.168.2.0
  192.168.3.0
Routing Information Sources:
  Gateway    Distance    Last Update
  192.168.2.1  100          00:00:54
Distance: (default is 100)
```

16.5.5 配置IGRP

要配置IGRP路由选择进程，可使用router igrp全局配置命令：

```
RouterA(config)# router igrp as-number
```

要关闭一个IGRP路由选择进程，可使用该命令的no形式：

```
RouterA(config)# no router igrp as-number
```

自治系统号可以标识一个IGRP进程，也可以用来标记路由选择信息。

要指定IGRP路由选择进程的网络序列，可使用network路由器配置命令：

```
RouterA(config)# router igrp 101
RouterA(config-router)# network 192.168.1.0
```

要删除一个条目，可使用其命令的no形式：

```
RouterA(config)# no router igrp 101
RouterA(config-router)# no network 192.168.1.0
```

例16-13显示了如何在路由器A和路由器B上配置使用AS 101的IGRP：

例16-13 配置IGRP

```
RouterA(config)# router igrp 101
RouterA(config-router)# network 192.168.1.0
RouterA(config-router)# network 192.168.2.0

RouterB(config)# router igrp 101
RouterB(config-router)# network 192.168.2.0
RouterB(config-router)# network 192.168.3.0
```



实验活动 配置IGRP

在这个实验中，使用C类网络设计一个IP编址方案，并在所有的路由器上配置IGRP。

16.5.6 检验IGRP的配置

要检验IGRP是否配置正确，可输入show ip route命令，查看其中以I标识的IGRP路由。

用来检查IGRP配置的其他命令如下：

- **show interface** *interface*——检验接口配置正确。
- **show running-config**——检验路由器上启用了IGRP。

• **show running-config interface** *interface*——检验接口上使用了正确的IP地址。

• **show running-config | begin interface** *interface*——检验IGRP运行在以指定接口开始的路由器接口上。

• **show running-config | begin igrp**——检验路由器上启用了IGRP。

• **show ip protocols**——检验路由器上启用了IGRP。

要检验Ethernet接口配置正确，可输入show interface fa0/0命令。例16-14显示了该命令的输出。

例16-14 show interface命令输出

```
RouterA# show interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0009.7c89.5620 (bia 0009.7c89.5620)
  Internet address is 192.168.1.1/24
--- Output Omitted ---
```

要查看路由器上是否启用了IGRP，可使用例16-15中显示的命令：

例16-15 show ip protocols和show running-config命令输出

```
RouterA# show ip protocols
Routing Protocol is "igrp 101"
---Output Omitted ---

RouterA# show running-config | begin igrp
router igrp 101
  network 192.168.1.0
  network 192.168.2.0
!
--- Output Omitted ---
```

要检查正确的IP地址，可使用例16-16中显示的命令。

例16-16 show running-config interface命令输出

```
RouterA# show running-config interface fa0/0
Building configuration...

Current configuration:
!
interface FastEthernet0/0
   ip address 192.168.1.1 255.255.255.0
   no ip directed-broadcast
end
```

例16-17显示了show ip route命令的输出，并显示了经由该路由器接口的可用路由。

例16-17 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

C  192.168.1.0/24 is directly connected, Loopback0
C  192.168.2.0/24 is directly connected, Serial0/0
I  192.168.3.0/24 [100/80135] via 192.168.2.2, 00:01:00, Serial0/0
```

16.5.7 IGRP的故障排除

大多数IGRP配置错误一般都是误输入的network语句、不连续的子网，或者是不正确的自治系统号。

以下命令在IGRP故障排除时比较有用：

- **show ip protocols**——以概要形式显示IP路由选择协议的信息。
- **show ip route**——显示路由器上的IP路由选择表。
- **debug ip igrp events**——显示网络上正在运行的IGRP路由选择的信息概要。
- **debug ip igrp transactions**——显示邻居路由器请求更新的请求消息和源路由器向邻居路由器发出的广播。
- **ping**——一个用来确定指定IP地址是否可达的工具。
- **traceroute**——一个用来跟踪从你的计算机到一台Internet主机的分组的工具，显示了分组到达主机所需的跳数以及每一跳所花的时间。

例16-18举例说明了debug ip igrp events命令的输出。

例16-18 debug ip igrp events命令输出

```
RouterA# debug ip igrp events
IGRP event debugging is on

00:21:38: IGRP: sending update to 255.255.255.255 via FastEthernet0/0 (192.168.1.1)
00:21:38: IGRP: Update contains 0 interior, 2 system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 2
00:21:38: IGRP: sending update to 255.255.255.255 via Serial0/0 (192.168.2.1)
00:21:38: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 1
```

例16-19举例说明了debug ip igrp transactions命令的输出。

例16-19 debug ip igrp transactions命令输出

```
RouterA# debug ip igrp transactions
```

```
IGRP protocol debugging is on

00:22:17: IGRP: received update from 192.168.2.2 on Serial0/0
00:22:17:       network 192.168.3.0, metric 80135 (neighbor 110)
00:23:07: IGRP: sending update to 255.255.255.255 via FastEthernet0/0 (192.168.3.1)
00:23:07:       network 192.168.2.0, metric=80125
00:23:07:       network 192.168.3.0, metric=80135
00:23:07: IGRP: sending update to 255.255.255.255 via Serial0/0 (192.168.2.1)
00:23:07:       network 192.168.1.0, metric=110
```

如果发现使用了错误的AS号，如例16-20所示纠正该错误之后产生正确的输出。

例16-20　debug ip igrp transactions

```
RouterA(config)# no router igrp 102
RouterA(config)# router igrp 101
RouterA(config router)# network 192.168.1.0
RouterA(config router)# network 192.168.2.0

00:27:50: IGRP: broadcasting request on FastEthernet0/0
00:27:50: IGRP: sending update to 255.255.255.255 via FastEthernet0/0 (192.168.1.1)
00:27:51: IGRP: Update contains 0 interior, 0 system, and 0 exterior routes.
00:27:51: IGRP: Total routes in update: 0 - suppressing null
00:28:01: IGRP: sending update to 255.255.255.255 via FastEthernet0/0 (192.168.1.1)
00:28:01:       network 192.168.2.0, metric=80125
00:28:01:       network 192.168.3.0, metric=80135
00:28:01: IGRP: Update contains 0 interior, 2 system, and 0 exterior routes.
00:28:01: IGRP: Total routes in update: 2
00:28:01: IGRP: sending update to 255.255.255.255 via Serial0/0 (192.168.2.1)
00:28:01:       network 192.168.1.0, metric=110
00:28:01: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
00:28:01: IGRP: Total routes in update: 1
```



实验活动　RIP和IGRP的默认路由选择

在这个实验中，配置一条默认路由，使用RIP将这个默认信息传播给其他路由器。当你使得这个配置工作以后，将网络从RIP转移为IGRP，并且也配置默认路由选择使其工作。



实验活动　IGRP的非等价负载均衡

在这个实验中，配置并且调整IGRP实现非等价负载均衡，用debug命令观察负载均衡。

16.6　总结

本章学习了以下知识点：

- 网络中拓扑发生改变时，路由选择信息通过更新来维护。

- 网络中路由选择环路的产生是因为交替路由、缓慢收敛和不一致的路由选择更新。
- 定义一个最大值可以防止计数到无穷大。
- 3种防止路由选择环路的方法：水平分割、触发更新和抑制定时器。
- 路由中毒被多种距离矢量协议用来克服大型的路由选择环路，并且提供一些关于一个子网或网络不可以访问的信息。
- 配置路由选择协议：RIP和IGRP。
- 使用ip classless命令。
- 路由选择协议的故障排除：RIP和IGRP。
- 检验路由选择协议：RIP和IGRP。
- 配置默认路由。

关于本章学习的补充内容，请参阅本书附赠光碟中与本章相关的视频、插图和e-Lab实验。

16.7 关键术语

邻近邻居（*adjacent neighbor*） 参与交换路由选择信息的两个直连的路由器被称为邻近的。

收敛（*convergence*） 运行特定路由选择协议的一组网络互联设备在拓扑变化后，对拓扑达到一致意见的速度和能力。

计数到无穷大（*count to infinity*） 发生在路由选择算法上缓慢收敛的一个问题，即路由器持续增加到特定网络的跳数值。一般来说，一些跳数限制被用来防止这个问题。

外部路由（*exterior routes*） 到自治系统外网络的路由，在确定最后可用网关时考虑。

清除定时器（*flush timer*） 指定一条路由被清除出路由选择表之前的时间。该变量的IGRP默认值是7倍的更新时间。

抑制（*holddowns*） 用来阻止定期更新消息不适当的恢复还没有正常的路由。

保持定时器（*hold-time timer*） 指定忽略较差路由的时间。该变量的IGRP默认值是3倍更新时间加10秒。

IGRP（*Interior Gateway Routing Protocol*） Cisco研发的一个IGP，用于解决大型异种网络中的路由选择问题。比较EIGRP。也参见IGP、OSPF和RIP。

内部路由（*interior routes*） 连接到路由器接口的子网间路由。如果连接到路由器的网络没有划分子网，IGRP就不会通告内部路由。

失效定时器（*invalid timer*） 指定路由器在宣告一条特定路由失效之前没有收到其路由选择更新信息的等待时间。该变量的IGRP默认值是3倍的更新时间。

毒性反转更新（*poison reverse updates*） 在对抗大规模路由选择环路时的必要更新。一般而言，路由选择度量标准的增长预示着路由选择环路。那么，发送毒性反转更新来删除该路由，同时将其置为抑制状态。

RIP（*Routing Information Protocol*） UNIX BSD系统提供的IGP。Internet上最常用的IGP。RIP使用跳数作为路由选择度量标准。

路由选择度量标准（*routing metric*） 一个路由选择算法用来确定一条路由好于其他路由的一个方法。该信息存放在路由选择表中，并发送在路由选择更新中。度量标准包括带宽、通信代价、延迟、跳数、负载、MTU、路径代价和可靠性。有时简称为度量标准。

路由选择协议（*routing protocol*） 通过执行一个特定的路由选择算法来完成路由选择的协议。路由选择协议的例子有IGRP、OSPF和RIP。

路由选择表（*routing table*） 存放在路由器上或一些网络互联设备上的一张表，它是用来跟踪到特定网络目的的路由，在有些情况下还有关联这些路由的度量标准。

路由选择更新（*routing update*） 一个路由器发出的消息，它标识网络的可达性和相关的代价信息。路由选择更新一般是定期发送，以及在网络拓扑发生变化后发送。比较瞬时更新（flash update）。

水平分割（*split horizon*） 一种路由选择技术，用于禁止路由信息从其接收接口出去。水平分割的更新对于防止路由选择环路很有作用。

系统路由（*system routes*） 在一个自治系统内的网络路由。Cisco IOS软件从直连网络接口，以及其他IGRP通告路由或访问服务器提供的系统路由信息获得系统路由。系统路由不包含子网信息。

触发更新（*triggered update*） 触发更新是无需等待更新定时器期满就发送的更新。

更新定时器（*update timer*） 指定路由选择更新信息发送的频率。该变量的IGRP默认值是90秒。

16.8 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 初始时路由器使用哪类路由？

A. 关于直连网络或子网的路由

B. 从Cisco IOS软件学习来的路由

C. IP地址和掩码信息已知的路由

D. 从其他路由器学到的路由

2. 下面那一项最恰当地描述了一条静态路由？

A. 用来转发帧的一条路由选择表项，其下一跳没有明确列在路由选择表中

B. 显式配置和添加到路由选择表中的一条路由，优先于动态路由选择协议所选择的路由

C. 能自动适应网络拓扑或通信流量变化的一条路由

D. 在网络拓扑中能不知不觉地进行调整来转发帧的一条路由

3. 下面那一项最恰当地描述了一条默认路由？

A. 用来转发帧的一条路由选择表项，其目的网络没有明确列在路由选择表中

B. 显式配置和添加到路由选择表中的一条路由

C. 能自动适应网络拓扑或通信流量变化的一条路由

D. 在网络拓扑中能不知不觉地进行调整来转发帧的一条路由

4. 外部路由选择协议的用途是什么？

A. 一个网络中节点间的信息传输

B. 在一个单个自治系统内传输信息

C. 自治系统间的通信

D. 建立网络间的兼容性基础

5. 内部路由选择协议的用途是什么？

A. 用于建立网络间的兼容性基础

B. 用于自治系统间的通信

C. 用于一个网络中节点间的信息传输

D. 用于一个单个自治系统内

6. 下面哪一项是全局任务？

A. 通过指定子网值来确定IP网络号

B. 启用路由选择协议，比如RIP或IGRP

C. 分配网络/子网地址和适当的子网掩码

D. 设置路由选择度量标准来发现到达每个网络的最佳路径

7. RIP使用下面哪个度量标准来确定消息传输的最佳路径?

A. 带宽

B. 跳数

C. 根据传递的消息的不同而变化

D. 管理距离

8. 你怀疑网络中的某台路由器在发送错误的路由选择信息，用什么命令来检查?

A. router（config）# show ip route

B. router# show ip route

C. router> show ip protocol

D. router（config-router）# show ip protocol

9. 为什么要显示IP路由选择表的内容?

A. 为了设置路由器的更新时间表

B. 为了识别目的网络和对应的下一跳地址

C. 为了跟踪数据报来自何处

D. 为了设置路由器的参数和过滤器

10. 如果想知道路由器配置了哪种路由选择协议，应使用哪条命令?

A. router> show router protocol

B. router（config）> show ip protocol

C. router（config）# show router protocol

D. router> show ip protocol

11. 在下面这个命令中，最后一个数字代表的是什么含义?

Router（config）# ip route 2.0.0.0 255.0.0.0 1.0.0.2 5

A. 跳数

B. 到达目的网络的路由数量

C. 管理距离

D. 路由选择表中目的网络的参考值

12. 管理距离为15代表了什么含义?

A. IP地址是静态的

B. IP地址是动态的

C. 路由选择信息的来源相对可信

D. 路由选择信息的来源相对不可信

13. 如果想在互联网中添加一个新的局域网，并且通过手工的方式将该网络添加到路由选择表中，你应该使用什么命令?

A. router (config) > ip route 2.0.0.0 255.0.0.0 via 1.0.0.2

B. router (config) # ip route 2.0.0.0 255.0.0.0 1.0.0.2

C. router (config) # ip route 2.0.0.0 via 1.0.0.2

D. router (config) # ip route 2.0.0.0 1.0.0.2 using 255.0.0.0



第17章 TCP/IP差错消息和控制消息

目标

学习完本章之后，你应该能够：

- 描述ICMP。
- 描述ICMP消息格式。
- 识别ICMP差错消息类型。
- 识别特定ICMP差错消息产生的可能原因。
- 识别当今网络中使用的各种ICMP控制消息。
- 确定ICMP控制消息产生的原因。

在学完了路由器的配置过程之后，接下来开始学习传输控制协议/Internet协议（TCP/IP）集中的差错消息和控制消息。本章将学习Internet控制消息协议（ICMP）是如何提供控制和消息功能的。此外，还将学习产生ICMP差错消息的可能原因以及如何识别它们。

请认真查看随书的光盘，这里面有关于这章内容的e-Lab实验、视频和插图。光盘中提供了一些与本章内容相关的素材，帮助读者加深理解和巩固所学知识。

17.1 IP协议在差错控制中的功能和角色

IP协议的功能是便于主机间的网络通信。IP协议的设计允许对主机和网络进行寻址。IP协议与不可路由协议的区别在于不可路由协议虽然可以给不同的主机编址，但不能区分不同的网络。IP协议被广泛接受，它不仅仅用来在因特网中传送数据，也成为很多不需要路由选择功能的小型局域网的默认内部协议。

IP协议的局限性在于它是一个尽力而为的传送系统。IP协议没有任何机制来确保不管网络中出现任何问题都能交付数据。数据可能因为各种各样的原因而无法到达目的，例如硬件故障、不正确的配置，或者是错误的路由选择信息。如果一个诸如路由器之类的中间设备出现了故障，或者目的设备已经从网络上断开，那么都无法递送数据。这就是为什么使用IP协议的应用一般比较快：它们没有TCP协议所具有的差错控制或可靠性机制。为了帮助发现这些错误，IP协议使用*Internet消息控制协议（ICMP）*。ICMP向数据的发送者通报传送过程中出现了一个差错。

以下章节将回顾ICMP差错消息的不同类型以及它们消息的格式。熟悉ICMP差错消息并了解产

生它们的可能原因是网络故障排除的必备基础知识。

17.2　ICMP

ICMP是*TCP/IP*协议栈的一部分，用来指出IP协议的故障以确保数据的递送。ICMP并没有克服IP协议的不可靠性局限。ICMP只是简单地将差错消息发送给数据发送者，指出在数据传送中出现了问题。图17-1显示了ICMP在TCP/IP模型中所处的位置。

本节包含了ICMP的各个方面，包括ICMP消息传送、差错报告与纠正，以及检测和处理可达性问题的方法。

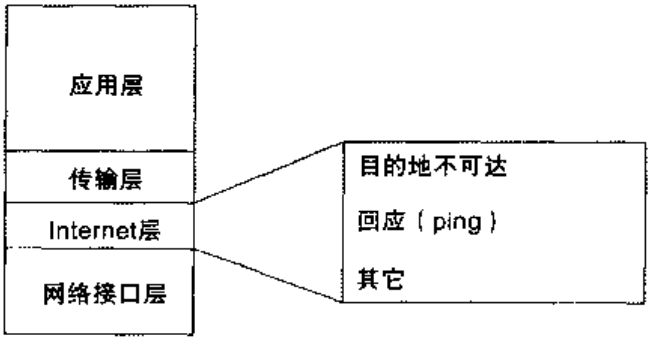


图17-1　ICMP和TCP/IP模型

17.2.1　ICMP消息传送

ICMP消息使用IP传送。与其他使用IP传送的数据一样，ICMP消息被封装在IP数据报内。表17-1显示了ICMP分组被封装在IP数据报的数据域。帧头可能来自一个局域网协议，如以太网，或者一个广域网协议，如高级数据链路控制协议（HDLC）。

表17-1　ICMP封装

帧头	IP数据报头	ICMP头	ICMP数据
帧头	IP数据报头	IP数据报的数据域	
帧头	帧的数据域		

数据到达网络层时被封装在数据报中。在数据链路层，数据报及其封装的数据被进一步封装成帧。ICMP消息有自己的头部信息。但是，这些头部信息与ICMP数据一起被封装在IP数据报中，如同其他数据一样。ICMP消息的传送方式也和其他数据一样。因此ICMP消息也会遇到同样的传送错误。这时就会出现这样一种局面，差错报告将产生更多的差错报告，这让原本已经境况不佳的网络更加拥塞。基于这种原因，ICMP消息所产生的差错不会生成它们自己的ICMP消息。因此有可能一个数据报在传送过程中出现了差错，但是发送者永远也无法收到差错报告。

17.2.2　差错报告与差错纠正

ICMP是IP的差错报告协议。当数据报发生传送差错时，ICMP向该数据报的发送者报告这些差错。例如，图17-2中的工作站1向工作站6发送了一个数据报。如果路由器C上的相应接口断掉了，路由器C则使用ICMP发送一个报文给工作站1，指明该数据报无法成功传送。ICMP并不纠正所遇到的网络问题。

在图17-2的例子中，ICMP并不试图去纠正阻止数据报传送的路由器C上的接口问题。ICMP的惟一功能就是向工作站1报告这些差错。

路由器C不会将传送故障通报给中间设备。因此，路由器C不会向路由器A和路由器B发送ICMP消息。路由器C也不知道这个出现传送差错的***数据报***是经由哪条路径到达这里的。数据报中仅仅包含源和目的IP地址；而没有包含所有中间设备的信息。报告设备只有发送者的IP地址，因此只能与之通信。尽管不能直接通告路由器A和路由器B，但是它们可以意识到路由器C的接口故障。当然，将这一信息传播给邻居路由器不是ICMP的功能。ICMP是向发送者报告分组的传送状态，而不是扩散网络变化的信息。

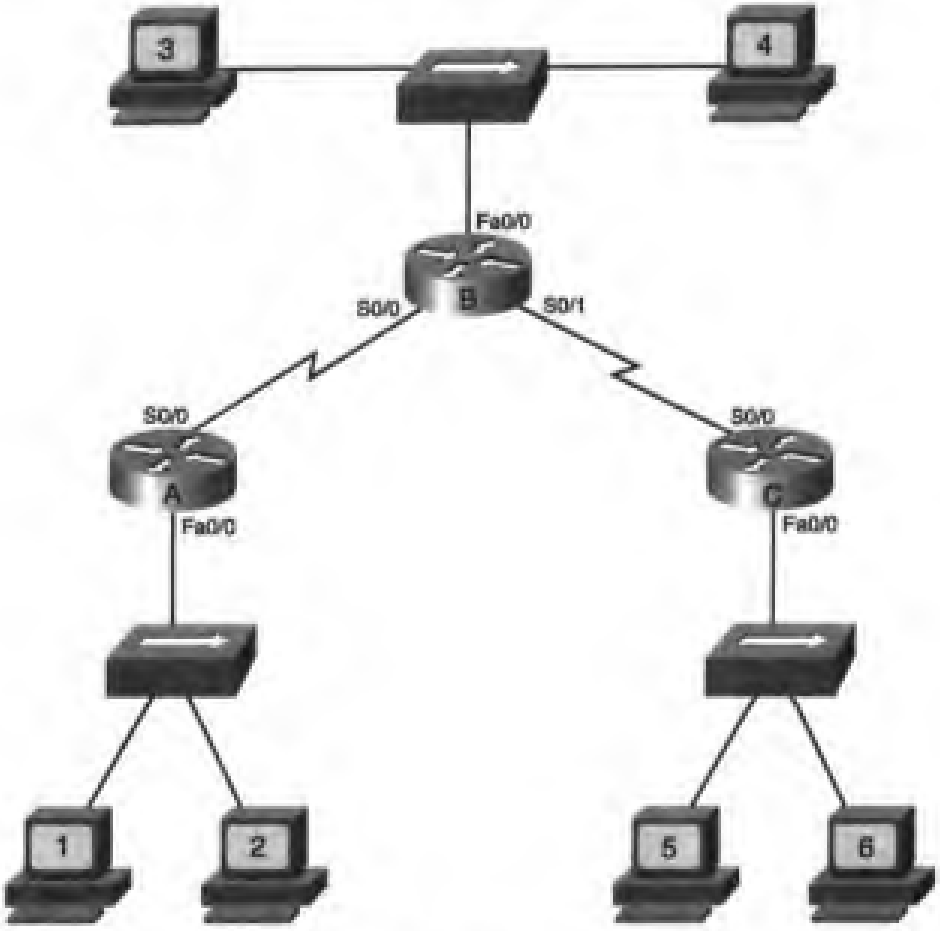


图17-2 更新差错报告

17.2.3 不可达网络

网络通信依赖于一些基本条件：

- 正确配置发送和接收设备上的TCP/IP协议栈。这包括安装TCP/IP以及正确配置IP地址和子网掩码。如果数据报要被传送到本地网络以外，那么还必须配置一个缺省网关。
- 必须安放一些中间设备用来将数据从源设备及其网络路由至目的网络。路由器就是完成这样的功能。
- 路由器接口上必须正确配置TCP/IP协议，并使用适当的路由选择协议或静态路由。

如果无法具备这些条件，网络通信就不能完成。例如，发送设备可能将数据报发送到一个并不存在的IP地址或者已经从网络上断开的目标设备。如果路由器的连接接口断掉或者路由器没有足够的信息来发现目的网络，那么该路由器也会成为故障点。如果一个目的网络无法访问，则称之为*不可达网络*。

目的不可达消息包括以下几种：

- **网络不可达**——这种消息通常表示路由选择或寻址错误。
- **主机不可达**——这种消息通常表示传送错误，例如错误的子网掩码。
- **协议不可达**——这种消息通常表示目的主机不支持分组中所指定的上层协议。
- **端口不可达**——这种消息通常表示TCP/UDP端口（套接字）不可用。

图17-3显示了一个路由器收到一个无法投递到它的最终目的地的分组。分组无法被投递是因为没有到达目的地的已知路由。由于没有已知路由，因此路由器向源发送一个ICMP主机不可达消息。

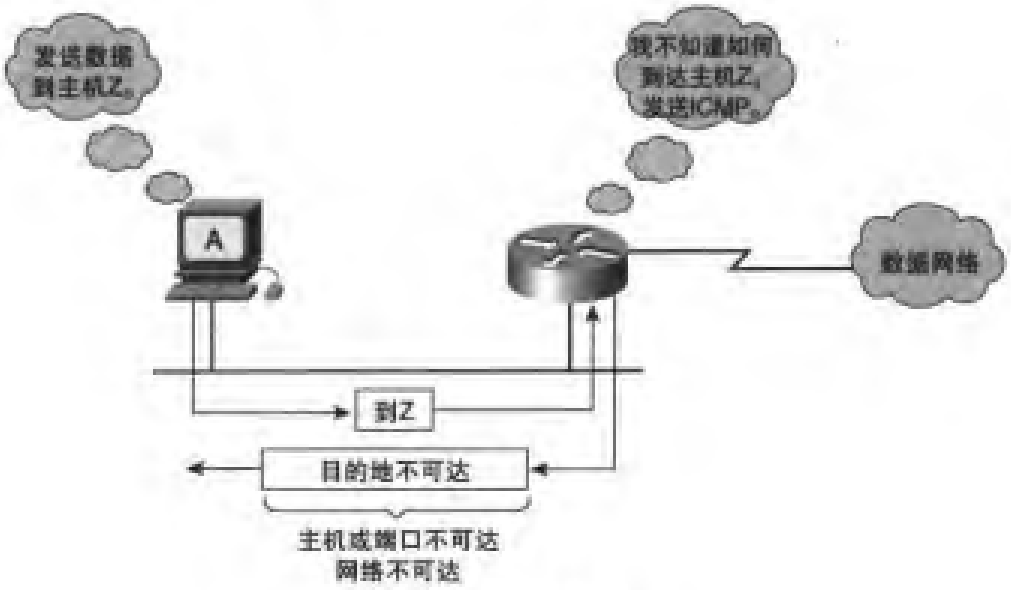


图17-3　ICMP主机不可达

17.2.4　用ping测试目的网络的可达性

ICMP协议可以用来测试特定网络的可达性。图17-4显示了使用ICMP向目的设备发送回应请求消息。目的设备收到一个ICMP回应请求后，它会构造一个回应应答消息返送给回应请求的发送者。如果发送者收到了回应应答，这就能够确定目的设备可以使用IP到达。

回应请求消息典型地使用ping命令发起，如例17-1所示。在这个例子中，该命令与目的设备的IP地址一起使用。例17-1和图17-5显示了一次成功的ping，或者说一次成功的回应请求/应答。

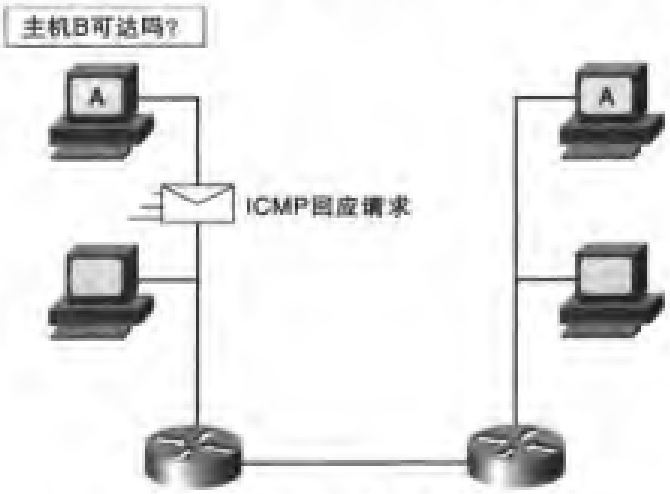


图17-4　回应请求

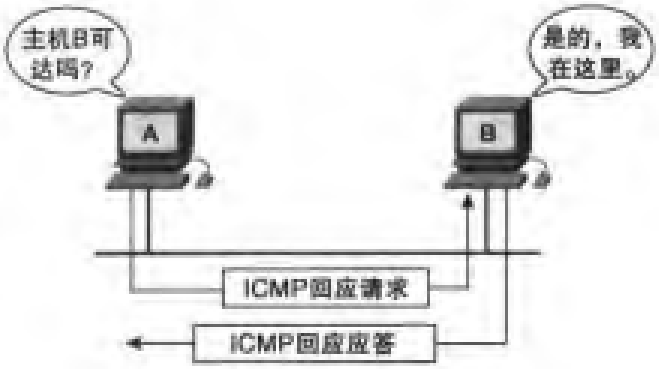


图17-5　ICMP ping

例17-1　ping发起的回应请求

```
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:\>
```

Ping命令也可以像例17-2所示的那样使用目的设备的域名（假定DNS是可用的）。

例17-2 使用目的设备域名的ping

```
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:\>
```

在这些工作站的例子中，ping命令发送了4个回应请求，收到了4个回应应答，可以确认两个设备之间的IP连通性。路由器的ping命令所产生的输出与工作站的ping命令输出有所不同。例17-3分别显示了从路由器A到路由器B（IP地址192.168.100.100）的一次成功和不成功的ping过程。惊叹号（！）表示一个成功的ping，句号（.）表示失败。表17-2列举了Cisco设备间使用ping时的Cisco ping返回代码。

例17-3 路由器ping的例子：成功和失败

```
RouterA# ping 192.168.100.100

Type escape sequence to abort.

Sending 5, 100byte ICMP Echoes to 192.168.100.100, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/36 ms

RouterA# ping 192.168.100.100

Type escape sequence to abort.
```

```
Sending 5, 100byte ICMP Echoes to 192.168.100.100, timeout is 2 seconds:
. . . . .

Success rate is 0 percent (0/5)
```

表17-2　Cisco ping命令的返回代码

代码	含义	可能的原因
!	每个惊叹号代表接收到一个ICMP回应应答	ping成功完成
.	每个句号表示等待一个应答时网络服务超时	这个消息可能指示以下问题：
		• ping被访问列表或防火墙阻隔；
		• 路径上的一台路由器没有到达目的的路由，也没有发送ICMP目的不可达消息；
		• 路径上的某处发生了物理连接问题
U	收到一条ICMP不可达消息	路径上的一台路由器没有到达目的的路由
C	收到一条ICMP源抑制消息	路径上的一台设备——可能是目的——收到过多的流量；检查输入队列
&	收到一条ICMP超时消息	可能发生路由环路

17.2.5　检测超长的路由

在网络通信中可能会出现几种故障情况。一种情况是，数据报在一个环中传送，永远无法到达目的。另一种情况是，根据路由选择协议的限制，源和目的之间没有可用路径。第一种情况的一个例子是数据报在两个路由器之间来回路由。在这种情况下，每个路由器都认为另一个路由器是到目的的下一跳。导致这种错误的一种可能原因是错误的路由选择信息。路由选择协议还可能限制一个分组所能经过的最大距离。例如，RIP跳数限制为15，简单地说就是一个分组最多只能经过15个路由器。

以上这些情况都可能导致超长路由的出现。无论事实上是路径中包含太多的跳数还是出现了路由选择环路，分组最终都会达到它的寿命期。当一个分组到达了它的寿命期，也就是到达了它的存活时间（TTL）。TTL值一般匹配于路由选择协议所定义的最大跳数值。在每个数据报中都会定义一个初始TTL值。每个路由器处理该数据报时，就将TTL值减1。当该数据报的TTL值为0时，则丢弃该分组。ICMP使用一个超时消息来通告源设备TTL已经过期。

17.2.6　ICMP消息格式：回应消息

与任何类型的分组一样，ICMP消息也有特定的格式。表17-3中所显示的每种ICMP消息类型都有自己独一无二的特点。不过，所有ICMP消息格式都以如下三个字段开始：

表17-3　ICMP消息类型

ICMP	消息类型
0	回应应答
3	目的地不可达
4	源抑制
5	重定向/改变请求
8	回应请求
9	路由器通告
10	路由器恳求
11	超时
12	参数错误

续表

ICMP	消息类型
13	时间戳请求
14	时间戳应答
15	信息请求
16	信息应答
17	地址掩码请求
18	地址掩码应答

- 类型。
- 代码。
- 校验和。

类型字段表示所发送的ICMP消息类型。代码字段包括用来指明消息类型的进一步信息。校验和字段，与其他类型分组中的一样，用来验证数据的完整性。

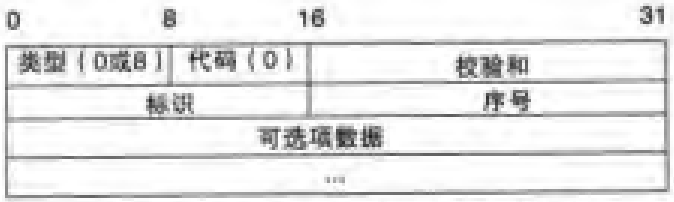


图17-6 回应请求和回应应答消息的格式

图17-6显示了ICMP回应请求和回应应答消息的格式。每种消息都显示了相关的类型和代码数字信息。回应请求和回应应答消息中的标识和序号值字段都是惟一的。标识和序号字段用来匹配回应应答和与之对应的回应请求。数据字段包含回应应答或回应请求消息中的附加信息。

17.2.7 ICMP消息格式：目的不可达消息

不是总能将数据报转发到它们的目的地，如图17-7所示。硬件故障、不正确的协议配置、接口



图17-7 目的地不可达消息

故障，以及不正确的路由选择信息都可能成为数据报无法成功传送的原因。在这些情况下，ICMP向发送者传送一个目的地不可达消息来指示数据报无法正常转发。

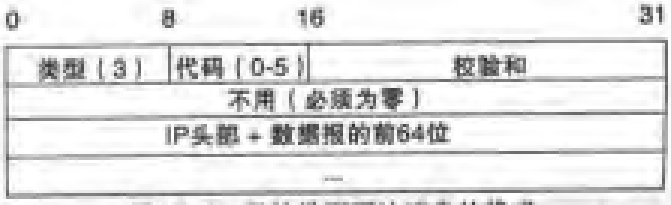


图17-8 目的地不可达消息的格式

图17-8显示了一个ICMP目的地不可达消息

的头部。类型字段值为3表示这是一个目的地不可达消息。代码字段的值说明了数据报无法传送的原因。代码字段值为0表示是网络不可达。表17-4列举了代码值及其说明。

表17-4　代码值及其描述

代码值	说明
0	网络不可达
1	主机不可达
2	协议不可达
3	端口不可达
4	需要分片但DF置位
5	源路由失败
6	目的网络未知
7	目的主机未知
8	源主机被隔离
9	与目的网络的通信被管理禁止
10	与目的主机的通信被管理禁止
11	对所请求的服务类型，网络不可达
12	对所请求的服务类型，主机不可达

当分组需要分片转发时也有可能发送目的地不可达消息。数据报从令牌环网络转发到以太网时通常需要分片。如果该数据报不允许分片，就无法转发分组。因此，就会发送一个目的地不可达消息。当一些IP相关的服务，例如FTP或者网页服务不可用时也会发送目的地不可达消息。要想有效地排除IP网络故障，就必须了解ICMP目的地不可达消息产生的各种原因。

17.2.8　其他差错报告

处理数据报的设备无法正确转发一个数据报的原因可能是数据报头部的一些差错。这些差错与目的主机或网络的状态无关，但仍会阻碍数据报的处理和传送。这时，就要发送一个ICMP类型为12的参数错误消息给数据报的源。图17-9显示了参数错误消息的头部。

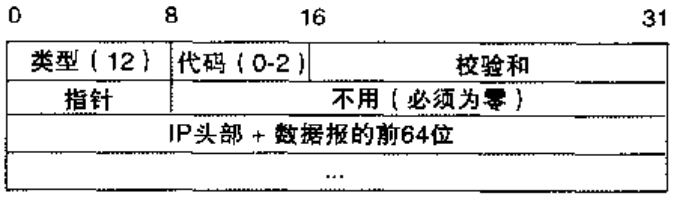


图17-9　参数错误消息的格式

参数错误消息的头部包含一个指针字段。当代码字段值为0时，指针字段表示数据报中产生差错的8位组。

17.3　TCP/IP协议集控制消息

与差错消息不同，控制消息的产生不是由于分组的丢失或分组传递中出现的差错。控制消息而是向主机通告一些状况，比如网络的拥塞或者到远程网络有一个更好的网关。与所有ICMP消息一样，ICMP控制消息被封装在IP数据报中穿越多个网络。

ICMP使用多种类型的控制消息，表17-3列出了最常见的一些类型。这些控制消息将在以下章节中详细讨论。

17.3.1　ICMP重定向/改变请求

最常见的ICMP控制消息是ICMP重定向/改变请求。这种类型的消息只能由网关发出。所有主机与其他IP网络通信时必须配置一个缺省网关。缺省网关是路由器连接主机所在网络的接口地址。图17-10显示了一个主机通过一个路由器访问Internet。

主机B将Fa0/0接口的IP地址配置为自己的缺省网关后，就可以使用这个IP地址访问任何非直连的网络。通常主机A只连接一个网关。但是在有些情况下，一个主机有可能连接到具有两个或更多直连路由器的网段。在这种情况下，主机的缺省网关就可能需要使用重定向/改变请求来通知主机到特定网络的最佳路径。

缺省网关仅在以下情况下发送ICMP重定向/改变请求：

- 分组进出路由器的接口相同。
- 分组路由的下一跳IP地址和源IP地址的子网/网络相同。
- 数据报不进行源路由（也就是说，不是根据数据所携带的信息来路由该数据）。
- 重定向的路由不是另一个ICMP重定向或缺省路由。
- 路由器被配置发送重定向消息。默认情况下，Cisco路由器要发送ICMP重定向。接口子命令no ip redirects用来禁止ICMP重定向。



图17-10 重定向请求

ICMP重定向/改变请求使用的格式如图17-11所示。该请求的ICMP类型值为5。另外，该请求的代码值为0、1、2或3。表17-5列举了这些代码值所请求的具体动作。

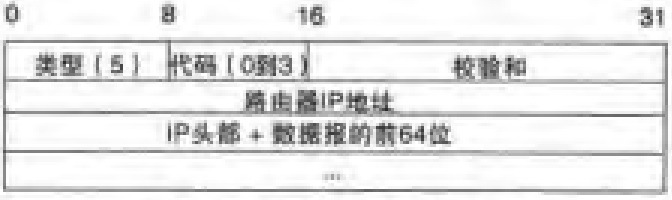


图17-11 重定向请求消息的格式

表17-5 代码值及其请求动作

代码值	请求的动作
0	对网络重定向数据报
1	对主机重定向数据报
2	对网络和服务的类型重定向数据报
3	对主机和服务的类型重定向数据报

重定向的接收者使用ICMP重定向中的路由器IP地址作为转发分组到特定网络的网关IP地址。在图17-10所示的例子中，路由器A发送给主机A的ICMP重定向中的路由器IP地址为192.168.12.2，这个地址实际上是路由器B的IP地址。

17.3.2 时钟同步和传送时间估计

TCP/IP协议集允许系统之间穿过多个网络进行远距离的连接。每个独立的网络以自己的方式提供时钟同步。当不同网络中的主机试图使用需要时间同步的软件进行通信时，就会出现一些问题。ICMP时间戳消息类型就是用来帮助解决这一问题的。



图17-12 时间戳请求

ICMP时间戳请求消息允许主机请求远程主机的当前时间。远程主机使用一个ICMP时间戳应答消息来回复这一请求。图17-12显示了ICMP时间戳请求或应答的格式。

ICMP时间戳消息的类型字段值为13表示时间戳请求，值为14表示时间戳应答。因为没有任何可用的附加参数，所以代码字段值总是为0。ICMP时间戳请求中包含有一个初始时间戳，用来指定

发送时间戳请求时请求主机的时间。接收时间戳是目的主机收到ICMP时间戳请求的时间。传送时间戳在ICMP时间戳应答报文即将返回时填入。初始、接收和传送时间戳计算的是从世界时间（UT）的零点开始的毫秒值。

所有的ICMP时间戳应答消息都包含初始、接收和传送时间戳。产生ICMP时间戳请求的主机可以使用这三个时间戳计算穿越网络的传输时间：

发送时间 = 接收时间戳 - 初始时间戳

接收时间 = 时间戳应答消息返回的时间 - 传送时间戳

往返时间 = 发送时间 + 接收时间

不过，这只是一个大概推测的时间，实际的传输时间可能变化很大，要取决于网络的流量和拥塞。产生ICMP时间戳请求的主机还可以使用这三个时间戳估算远程主机的本地时间。

ICMP时间戳消息为远程主机的时间和总的网络传输时间的估算提供了一个简单途径。但是，这并不是获得这些信息的最好方法。像网络时间协议（NTP）这样位于TCP/IP协议栈的高层协议，可以用更可靠的方式完成时钟同步。

17.3.3　信息请求和应答消息的格式

ICMP信息请求和应答消息原本是用来让主机发现自己所在网络的网络号的。图17-13显示了ICMP信息请求和应答消息的格式。

这种消息有两种类型。类型15表示信息请求消息。类型16表示信息应答消息。这种特定的ICMP消息类型已经过时。现在主要使用BOOTP和动态主机配置协议（DHCP）来让主机获得它们所接入网络的网络号。

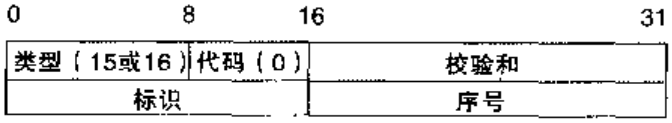


图17-13　信息请求和应答消息的格式

17.3.4　地址掩码请求

当一个网络管理员使用子网划分过程将一个主类网络划分成多个子网时，就要创建一个新的子网掩码。这个新的子网掩码在区分IP地址中的网络、子网、主机位时非常重要。如果一个主机不知道子网掩码，它就向本地路由器发送一个地址掩码请求。如果主机知道该路由器的地址，那么这一请求就以**单播**的方式发送。如果不知道该路由器的地址，那么这一请求就以**广播**的方式发送。当路由器收到这个请求时，它就响应一个地址掩码应答。地址掩码应答中给出了正确的子网掩码。例如，假设一台主机位于一个B类网中，其IP地址是172.16.5.3。这台主机不知道子网掩码，于是它广播一个地址掩码请求：

```
Source address          172.16.5.3
Destination             255.255.255.255
Protocol                ICMP=1
Type                    Address Mask Request=AM1
Code                    0
Mask                    0
```

本地路由器168.5.5.1收到了这个广播。该路由器响应一个地址掩码应答：

```
Source address          172.16.5.1
Destination address     172.16.5.3
Protocol                ICMP=1
Type                    Address Mask Reply=AM2
```

```
Code                    0
Mask                    255.255.255.0
```

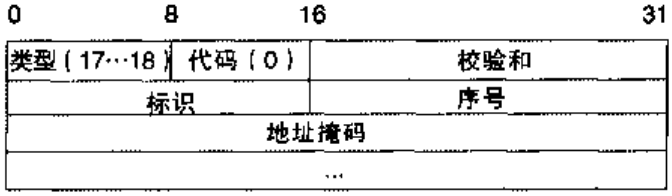


图17-14 地址掩码请求

图17-14显示了地址掩码请求消息的格式。表17-6列举了地址掩码请求消息。注意地址掩码请求与应答使用同样的消息格式。只是地址掩码请求的ICMP类型值为17，而应答的类型值为18。

表17-6 ICMP地址掩码请求消息

ICMP域	说明
类型17	地址掩码请求消息
类型18	地址掩码应答消息
代码0	地址掩码请求消息
代码0	地址掩码应答消息
校验和	从ICMP消息类型部分开始的16位数据的反码和再取反。计算校验和时，校验和字段值应为0。然后将计算出的校验和填入该字段
标识	标识的目的是为了匹配请求和应答。值可以为0
序号	序号的目的是为了匹配请求和应答。值可以为0
地址掩码	一个32位的掩码。一个网关收到地址掩码请求后，将一个32位的掩码填入该字段，标识请求主机的子网和网络。如果请求主机不知道自己的IP地址，可以将源字段置为0；应答则用广播方式。但是，这种情况应该尽量避免，因为这将引入过多的广播报文到网络上。而且当应答为广播时，根本就不需要匹配请求和应答，因为一个子网只有一种可能的地址掩码。标识和序号字段也可以忽略。网关或主机都可以发送类型为AM1的消息。网关或者代替网关主机可以发送类型AM2的消息

17.3.5 路由器发现消息

当主机上没有手动配置的缺省网关时，它可以通过路由器发现过程发现可用的路由器。这一过程由主机发送一个*组播*的路由器恳求消息开始，使用的地址为224.0.0.2。当包含没有配置组播的路由器时，路由器恳求也可以用广播的方式发送。RFC 1812中规定，路由器应该支持所有直连网络的路由器发现过程。但是，这种支持并不是一直这样的。如果一个路由器恳求消息送往一个并不支持发现过程的路由器，那么该恳求将不会被响应。

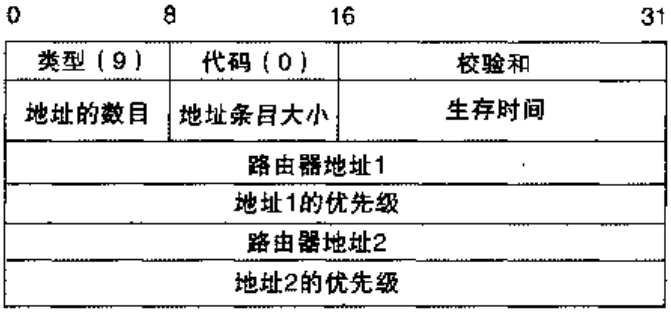


图17-15 路由器发现消息

当支持发现过程的路由器收到路由器恳求消息时，就会回送一个路由器通告，如图17-15所示。表17-7解释了消息格式中的每个字段。

表17-7 路由器通告消息的格式

ICMP字段	说明
类型	9
代码	0
校验和	从ICMP消息类型部分开始的16位数据的反码和再取反。在计算校验和时，校验和字段值应为0
地址数目	该消息中所通告的路由器地址数目
地址条目大小	每个路由器信息的32位字的数量（在这里所描述的协议版本中，值为2）
生存时间	路由器地址的最大有效时间（秒）
路由器地址	发送的路由器IP地址。 发送该消息的接口地址

续表

ICMP字段	说明
优先级	每个路由器地址的优先级。 标志该地址相对于同一子网的其他地址谁更应该是缺省路由器地址。用二进制反码表示；值越高表示越可取

17.3.6　路由器恳求消息

当主机没有缺省网关时就会生成一个ICMP路由器恳求消息。这一消息采用组播方式发送，是路由器发现过程的第一步。本地路由器响应一个路由器通告用来告知本地主机的缺省网关。

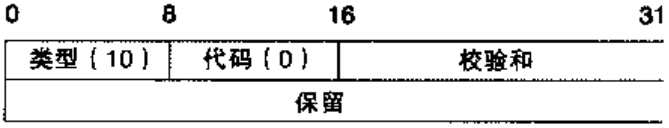


图17-16　路由器恳求消息的帧格式

图17-16表示了该消息的格式，表17-8给出了每个字段的解释。

表17-8　路由器恳求消息各字段的说明

ICMP字段	说明
类型	10
代码	0
校验和	从ICMP消息类型部分开始的16位数据的反码和再取反而得。在计算校验和时，校验和字段值应为0
保留	发送时置0；接收时忽略

17.4　拥塞和流控消息

如果多台计算机试图访问同一个接收者，那么该接收者将会出现流量冲突。当数据流从一个高速的局域网流向低速的广域网时也可能出现拥塞。网络或主机的拥塞将导致分组的丢弃，从而引起数据的丢失。为了减少数据丢失量，必须向发送者发送关于拥塞的ICMP消息。这种类型的ICMP消息被称为*源抑制消息*。源抑制消息向发送者通告拥塞，并要求发送方降低分组发送速率。在大多数情况下，拥塞会在很短的时间内平息。源主机在没有收到其他的源抑制消息时会逐渐提高发送速率。大多数Cisco路由器在默认情况下不发送源抑制消息。这是因为源抑制消息本身会加剧网络拥塞。

ICMP源抑制消息可以有效地用在小型办公室，即家庭办公室（SOHO）中。这样一个SOHO可能由使用5类双绞线连接在一起的4台计算机组成，并通过一个56kbit/s的调制解调器实现Internet连接共享（ICS）。很容易看出，10Mbit/s带宽的SOHO局域网很容易导致56kbit/s带宽的广域网链路过载。这将导致数据丢失和重传。在ICMP消息的帮助下，作为ICS网关的主机可以要求其他主机降低传输速率到一个可使用的程度。降低传输速率就阻止了连续的数据丢失。

17.5　总结

本章学习了以下知识点：

- IP协议采用尽力而为的传递方法，使用ICMP消息警告发送者数据没有到达目的地。
- ICMP回应请求和回应应答消息帮助网络管理员在故障排除过程中测试IP的连通性。
- ICMP消息使用IP协议传递，因此是不可靠传送。
- ICMP分组有自己的开始于类型字段和代码字段的特定头部信息。
- ICMP控制消息的功能。
- ICMP重定向/改变请求消息。
- ICMP时钟同步和传送时间估计消息。

- ICMP信息请求和应答消息。
- ICMP地址掩码请求和应答消息。
- ICMP路由器发现消息。
- ICMP路由器恳求消息。
- ICMP拥塞和流控消息。

关于本章学习的补充内容，请参阅本书附赠光碟中与本章相关的视频、插图和e-Lab实验。

17.6　关键术语

广播（*broadcast*）　数据分组发送给网络上的所有节点。

数据报（*datagram*）　在IP网络中，分组通常被称为数据报。

ICMP（*Internet*消息控制协议）　网络层的IP协议，用来报告差错以及提供IP分组处理过程中的其他信息。该协议定义在RFC 792中。

组播（*multicast*）　一个分组被网络复制并发送给网络地址的一组特定子集。

ping（分组网际探测器）　ICMP回应请求消息及其应答。经常用在IP网络中测试一个网络设备的可达性。

TCP/IP（传输控制协议/Internet协议）　美国国防部于20世纪70年代开发的可构建全球互联网络的协议集的通用名称。TCP和IP是这个协议集中最广为人知的两个协议。

单播（*unicast*）　消息只发送给网络上的一个单一目的地。

17.7 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. ICMP是IP协议的差错报告协议。正确还是错误？
   A. 正确
   B. 错误
2. ICMP代表什么？
   A. Internal Control Message Protocol
   B. Internet Control Message Portal
   C. Internal Control Message Protocol
   D. Internet Control Message Protocol
3. ICMP消息和其他使用IP协议传送的数据一样被封装在数据报中。正确还是错误？
   A. 正确
   B. 错误
4. 如果数据报要传送到本地网络以外，则必须配置一个缺省网关。正确还是错误？
   A. 正确
   B. 错误
5. TTL代表什么？
   A. Time-To-List
   B. Time-To-Live
   C. Terminal-To-Live
   D. Terminal-To-List
6. 所有的ICMP消息格式都以下面的哪个字段开始？
   A. 类型
   B. 代码
   C. 校验和
   D. 以上全部
7. 只有出现下列哪种情况时，缺省网关才会发送ICMP重定向/改变请求？
   A. 分组的进出接口相同
   B. 源IP地址所在的子网/网络与下一跳IP地址的子网/网络相同
   C. 数据报不是源路由的
   D. 重定向的路由不是另一个ICMP重定向或缺省路由
   E. 以上全部
8. ICMP时间戳消息的类型字段值可以是13（时间戳请求）或者是多少？
   A. 14，时间戳应答
   B. 14，时间
   C. 14，应答
   D. 26，时间戳应答
   E. 以上全部
9. 所有的时间戳应答消息都不包含初始、接收和传送时间戳。正确还是错误？
   A. 正确
   B. 错误

10. 路由器恳求消息的ICMP类型值是哪多少?

A. 9

B. 10

C. 17

D. 18



第18章　基本路由器故障处理

目标

学习完本章之后，你应该能够：

- 执行基本网络测试。
- 使用ping命令执行基本网络连通性测试。
- 使用telnet命令验证源和目的主机之间的应用层软件。
- 根据OSI模型各层测试进行故障处理。
- 使用show interfaces命令确认第1层和第2层问题。
- 使用show ip route和show ip protocol命令检查路由问题。
- 使用show cdp命令验证第2层连接性。
- 使用traceroute命令显示分组在网络间经过的路径。
- 使用show controller serial确保已连接正确的电缆。
- 使用基本debug命令显示路由器的动作。

本章提供了进行网络测试的简介，并且重点介绍了故障排除采用结构化方法的必要性。本章同时介绍了路由器故障处理的基本方法。

请务必在本书配套的光盘中查看与本案相关的e-Lab实验活动、视频和插图。这些光盘资料提供了补充材料，能够强化本章中涉及的概念。

18.1　网络测试介绍

网络基本测试应按照OSI参考模型顺序进行，如图18-1所示。

如果有必要的话，最好从第1层开始一直进行到第7层。从第1层开始检查简单的故障，例如电源没有插到插座上。

第2层的问题可能包括不正确地配置串行接口或以太网接口，在串行接口上设置不恰当的时钟速率，或者网络接口卡（NIC）故障。

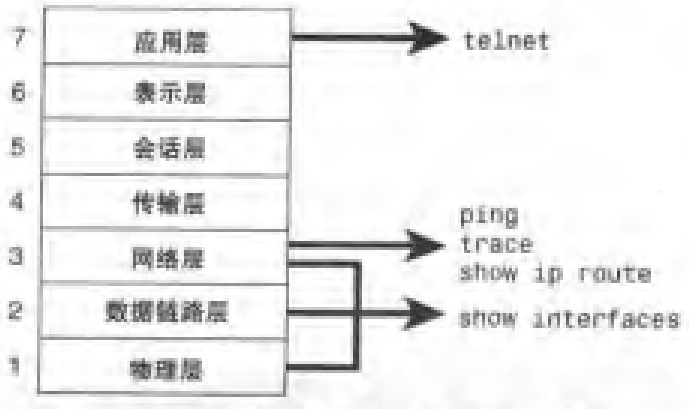


图18-1　测试工具和OSI参考模型

在IP网络中发生的最常见的故障主要由寻址方案中的错误导致，这是第3层的问题。

本章后面会讨论OSI模型所有层上可能发生的各种故障。在继续更进一步的配置步骤前对地址配置进行测试是很重要的。

本节的每个测试都针对OSI模型的某一个特定层的网络操作。

18.1.1　故障排除的结构化方法

故障排除是一个帮助用户发现网络故障的过程。在由管理员恰当地规定的网络标准基础上，应当执行一个有秩序的排除故障过程。文档是故障处理过程中非常重要的一个组成部分。图18-2中的流程图推荐了一个解决网络故障的逻辑顺序。

图18-3显示了网络故障排除的方法。

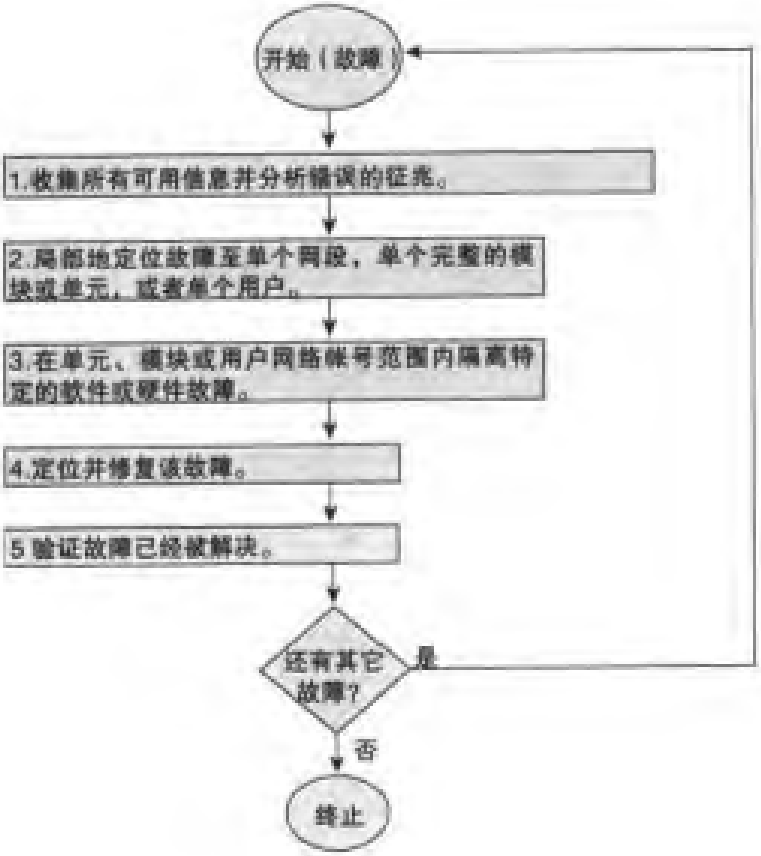


图18-2　故障排除方法

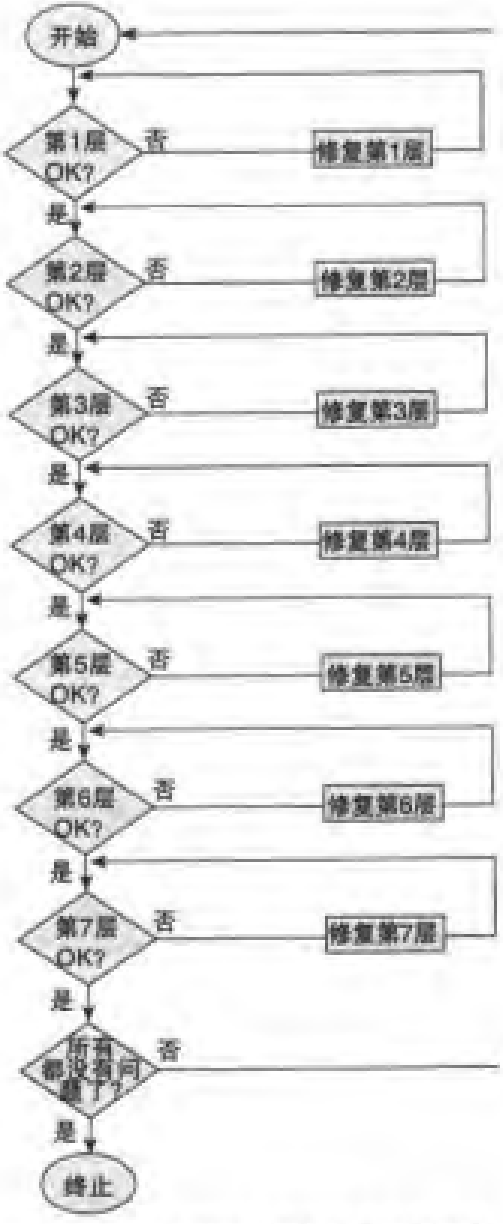


图18-3　按OSI模型各层的顺序故障处理

有了结构化的方法，网络的成员就知道其他成员为解决一个故障曾做过什么处理。如果没有任何组织地使用多种方法，问题的解决就会变得非常混乱。没有一个结构化的方法，几乎不能解决任何故障。

图18-2和图18-3的流程图并不是故障排除的惟一方法；然而，一个有秩序的处理过程对于确保网络平滑地、有效率地运行是非常重要的。

18.1.2 OSI各层的测试

如果有必要的话，最好从第1层开始一直进行到第7层。

第1层（物理层）的故障可能包括以下各项：

- 电缆被损坏。
- 未连接电缆。
- 电缆连接到错误的端口。
- 电缆连接间歇性中断。
- 对于当前任务使用了错误的电缆（必须使用正确的全反连接、交叉连接以及直通连接方式的电缆）。
- 收发器故障。
- DCE电缆故障。
- DTE电缆故障。
- 设备掉电。

排除了所有因第1层故障而导致网络故障的可能性后，下一个步骤就应该检查第2层故障的可能性。

第2层错误可能包括以下各项：

- 不正确地配置串行接口。
- 不正确地配置以太网接口。
- 不正确的封装设置（高级数据链路控制［HDLC］是串行接口的缺省设置）。
- 串行接口上不正确的时钟设置。
- *NIC*故障。

排除了所有因第2层故障而导致网络故障的可能性后，下一个步骤就应该检查第3层故障的可能性。

第3层错误可能包括以下各项：

- 路由选择协议没有启用。
- 启用了错误的路由选择协议。
- 不正确地配置路由选择协议。
- 不正确的IP地址。
- 不正确的子网掩码。
- 不正确的缺省网关。

如果错误或者问题与网络上出现的连通性有关，那么就要首先使用像ping或者telnet之类的连通性测试工具通过层进行检查，以确定网络中分组丢失的地点。Ping命令可用于测试第3层的连通性，在第7层，Telnet命令可以用于检测源和目的工作站之间的应用层软件。这些命令将在本章的后面详细讨论。

18.1.3 使用指示灯排除第1层的故障

指示灯是排除故障的有用工具。大部分接口或者NIC都有指示灯显示连接是否正常。这种指示灯通常称为链路灯（*link light*）。接口可能也有这样的灯用于指示是否有发出（TX）或者收到（RX）的流量。如果接口的指示灯显示为无效连接，可以关闭设备电源并重启接口卡。NIC工作在第1层和

第2层。

许多指示灯认为网络中第1层的故障包括以下各项：

- 电缆被损坏。
- 未连接电缆。
- 电缆连接到错误的端口上。
- 电缆连接间歇性中断。
- 对于当前任务使用了错误的电缆。
- 收发器出现问题。
- 设备掉电。

使用有毛病或者错误的电缆会导致链路灯指示为不正常的连接或者无连接。

检查并确认所有的电缆都连接到了正确的端口。检查所有的交叉连接都使用了适当的电缆和连接方法。检查所有的交换机或者集线器的端口都设置在正确的VLAN域或者冲突域中，并为生成树和其他各项设置了适当的参数。

检查使用了合适的电缆，如果在两个末端系统间直连——比如PC和路由器之间或者两台交换机之间——可能就需要使用一条专门的交叉线。检查来自源端接口的电缆连接正确并处于良好的状态。如果电缆看起来连接得不好，需重新接插电缆并确保可靠连接。尝试用一根已知正常工作的电缆去替换原来的电缆。如果电缆是连接到墙上的插座，使用电缆测试器来确保插座布线正确。

同时检查所有使用的收发器，确保它们的型号正确并且连接和配置都正常。当替换了电缆后仍未解决问题，如果使用了一个收发器的话，尝试替换转发器。

在进行诊断和排除复杂的故障之前，一定要检查以确保设备已接通电源。有些问题往往就是由这些最简单的错误产生的。

18.1.4 使用show interface命令排除第2层的故障

Show interface命令也许是发现路由器第1层和第2层故障的最重要的一个工具。该命令的第一个输出参数（或线路）与物理层有关。第二个输出参数（或协议）表明控制线路协议的Cisco IOS软件进程是否认为接口可用。这取决于是否成功接收到存活（keepalive）消息。如果接口连续三次丢失keepalive消息，则线路协议标志为down。

如果线路标记为down，则协议也一定为down。这是因为没有可用的介质供协议使用。当由于硬件问题而接口为down或者因为配置问题而导致“管理性的down”时，就会发生这种现象。

如果接口是up，而线路协议是down，则问题出在第2层。以下是一些可能引起故障的原因：

- 没有keepalive。
- 没有配置时钟频率。
- 封装类型不匹配。

当输入show interface命令后出现一行消息为“interface is up and the line protocol is down”时，则可能是由这些原因引起的。使用clockrate和encapsulation命令来确保接口间没有不匹配的情况。

在配置完一个串口之后，应该用show interface serial命令来查看接口的改变并确保接口可运作。

18.1.5 使用ping命令排除第3层的故障

Ping命令是测试网络连通性的一个有用的工具。为了支持对网络基本连接情况进行故障诊断，许多网络协议都支持echo协议，用来检测协议分组是否可路由。Ping命令发送一个分组到目的主机，然后等待目的主机的回应。Echo协议返回的结果可以帮助衡量到达目的地路径的可靠性，确定路径

上的时延，决定主机是否可达到或者是否正常工作。Ping命令的输出显示了一个ping分组到达指定系统的最小、平均和最大往返时间。Ping使用Internet控制消息协议（ICMP）来验证硬件的连通性和网络层的逻辑地址。这是一种基本的测试机制。

对于图18-4中的网络，ping命令对目标172.16.1.5所发出的5个数据报都得到了成功的响应，如例18-1所示。

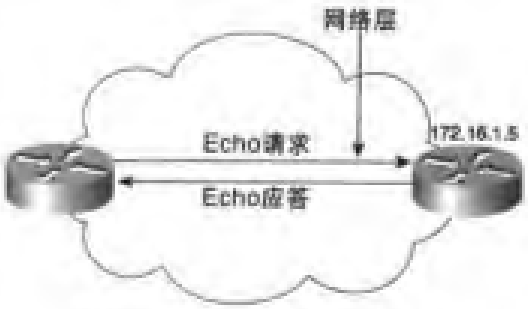


图18-4 使用ping命令测试网络

例18-1 ping目的172.16.1.5的结果

```
Router>ping 172.16.1.5

Type escape sequence to abort

Sending 5, 100 byte ICMP Echos to 172.16.1.5,

timeout is 2 seconds:

!!!!!

Success rate is 100 percent,

round-trip min/avg/max=1/3/4 ms

Router>
```

惊叹号（！）表示一个成功的回应。如果显示句号（.）而不是惊叹号，表明路由器在等待ping的目标对某个分组回应时产生了超时。Ping命令可以用来对网络的基本连通性进行诊断。

Ping通过向目标主机发送ICMP回应请求并等待应答来测试网络连接。测试一个连接时，ping跟踪发送的分组数量、接收到的应答数量、丢失的分组百分比、以及分组到达目的端和收到应答所需的时间总和。这个信息使得用户能够确认他们的工作站是否能与其他主机通信，并确定是否丢失任何信息。

Ping命令在用户和特权EXEC模式下都可以使用。ping命令可用于在AppleTalk、ISO无连接网络服务（CLNS）、IP、Novell、Apollo、VINES、DECnet或XNS网络上确认基本的网络连接性。

ICMP使用消息来完成各种任务。表18-1显示了ICMP消息类型的列表。

表18-1 ICMP消息类型

消息	目的
目的不可达	告诉源主机分组传递有问题
超时	传递分组的时间太长，分组被丢弃
源抑制	源发送数据的速度比路由器转发的速度快。这个消息要求发送者降低发送速率
重定向	路由器接收到一些分组，由其他路由器发送会有更好路由时，则向发送者返回一个消息，告诉它用更好的路由
回应	ping命令用来检验连接性
参数问题	用于识别不正确的参数
时间戳	用来测量到特定主机的往返时间
地址掩码请求/应答	用来查问和获悉将使用的恰当的子网掩码
路由器通告和选择	允许主机动态学习连接到该子网的路由器IP地址

Ping命令的扩展模式允许使用者指明所支持的IP报头选项。这使得路由器可以执行更广泛的测试选项。要进入ping命令的扩展模式，在特权模式下键入ping命令，不加任何选项后按回车。然后出现和扩展命令选项一样的一些基本选项提示，在扩展命令提示符下指定各种扩展ping选项后键入yes。扩展ping和常规ping 使用同样的工作方式，但是扩展ping支持对不同的参数进行修改，例如分组的大小和频率。

在网络运行正常的时候使用ping命令是一个好方法，可以看到网络在通常状态下命令如何工作，以便处理故障时有数据进行参考对比。

18.1.6　使用traceroute排除第3层的故障

Traceroute命令用于发现分组到达目的地过程中所经过的路由器。Traceroute也用于检测网络层或第3层，在逐跳的基础上提供性能基准。

Traceroute命令列出成功到达的跳，如例18-2所示。如果数据成功到达想去的目的地，则输出会显示数据报所经过的每一个路由器。这个输出可以保存用于将来的网络故障处理。

例18-2　traceroute 命令输出

```
Cougars>traceroute 168.71.8.2
traceroute to pc-b.cisco.com (168.71.8.2), 30 hops max, 40 byte packets
1   routerb (168.71.6.3)    3 ms 3 ms 3 ms
2   *   *   *
3   *   *   *
4   *   *   *
5   *   *   *
Cougars>
```

Traceroute的输出也指出在哪一跳发生故障。对于路径中的每一台路由器，在终端生成一行输出，指出数据所到接口的IP地址。如果显示一个星号（*），则分组转发失败。通过从traceroute的输出结果中获得最后一个正常跳的位置，并将它与网络图相对比，可以隔离问题区域。

Traceroute也提供信息以显示链路的相对性能。往返时间（RTT）是发送一个回应分组和得到一个响应所需要的往返时间，如例18-2所示。在这个例子中，发出去的每一个分组都有一个3 ms的RTT。对链路的延迟有个大致的了解是很有用的。虽然这些数字对于一个准确的性能评估来说不够精确；然而这个输出可以保存下来用于将来网络性能的故障处理。

收到traceroute的设备也必须知道如何发送应答给traceroute的源。由于traceroute或ping数据成功地完成路由器之间的来回旅程，因此一定存在两个方向的已知路由。一个失败的响应并不总是代表有故障存在，因为ICMP消息可能被主机限制或者过滤掉。跨过Internet的时候尤其如此。

当traceroute从路由器发出一系列UDP数据报给远程主机的一个无效端口地址时，对于发送的第一个序列的三个数据报，生存时间（TTL）字段设为1。TTL值设为1，使得数据报达到路径中第一个路由器就会超时。这个路由器则响应一个ICMP的超时消息（TEM）表示数据报已过期。

又有三个TTL值设为2的UDP消息被发送，这使得第二台路由器返回ICMP TEM。这个过程继续进行下去直到分组到达目的。

因为这些数据报试图访问一个目的主机上的无效端口，所以返回ICMP端口不可到达消息，而不是ICMP TEM。这表示一个不可到达端口，并发通知给traceroute程序以终止该程序。

18.1.7　使用Telnet处理第7层的故障

Telnet是一个虚拟终端协议，属于TCP/IP协议集的一部分。Telnet允许检验源和目的工作站之间的应用层软件。这是最完整有效的测试机制。Telnet允许建立连接到远程设备上，以收集信息并运行命令和应用程序。

Telnet是最完整的测试工具，因为它在网络层使用了IP和在传输层使用了TCP来建立一个与远程

主机的会话。如果Telnet能成功，则IP连通性必定是好的。

Telnet命令提供一个虚拟的终端，以便管理者能够通过Telnet操作连接到其他运行TCP/IP的网络设备（例如路由器和交换机）。如果一台路由器能够通过Telnet被远程访问，那么可以确定至少有一个TCP/IP应用能够达到远程路由器。一个成功的Telnet连接能够表明高层应用和低层服务都是正常工作的。图18-5演示了一个Telnet连接。

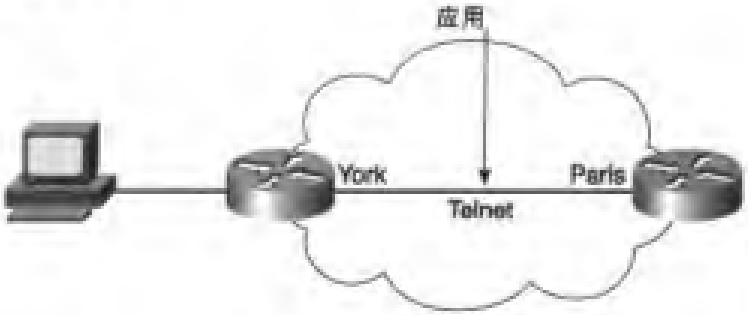


图18-5 使用Telnet

如果管理员能够Telnet到一台路由器而不能到另一台路由器，则Telnet失败很可能是由于特定的寻址、命名或访问权限等问题造成的。这些问题可能出现在管理员的路由器上，也可能出现在作为Telnet目标的路由器上。

如果从一台主机到一台特定的服务器Telnet失败，可以尝试从路由器和其他设备上去连接。也可以尝试使用ping命令做更基本的测试。如果可以ping到主机，但Telnet时却不能出现登录提示，可检查以下方面：

- 通过反向DNS查客户端地址是否能被解析？许多Telnet服务器不允许来自无DNS条目的IP地址的连接。这对于使用DHCP分配地址的方式来说是个常见的问题，管理员没有为DHCP地址池添加DNS条目。
- Telnet应用程序也许不能协商合适的选项，因此无法连接。在Cisco路由器上，这个协商过程可以通过debug telnet来观察。查找错误的信息、无效的IP或DNS地址，看是什么导致了这个问题。
- 还有一种可能是Telnet被禁用，或是在目的服务器上Telnet端口被移到了另一个不是23的端口。回顾前面章节，23端口是Telnet的缺省端口。

实验活动 利用ping和telnet处理故障

在这个实验中，将用到OSI模型中第1、第2和第3层的知识，通过使用ping和telnet工具诊断网络配置错误。

18.2 使用show interface和show interfaces命令处理路由器的故障问题

Cisco IOS软件包含了许多处理故障的命令。其中比较广泛使用的是show命令。使用一条或多条show命令可以查看路由器的各个方面。Show interface命令用于检查接口的状态和统计数据。这条命令的各种变化可以用于检查不同类型接口的状态。要查看FastEthernet接口的状态，可使用show interfaces fastethernet。这条命令也可以用于查看一个特定接口的状态。要查看Serial 0/0接口的状态，可使用show interface serial0/0。要查看接口FastEthernet 0/0的状态，可使用show interface fa0/0。

使用show interfaces命令能显示接口两个重要部分的状态。这将涉及到第1层和第2层的功能：

- **物理（硬件）部分**——硬件包括线缆、连接器和接口，显示设备间的物理连接情况。
- **逻辑（软件）部分**——软件状态显示消息的状态（如*keepalives*）、控制信息和相邻设备之间传递的用户信息。这涉及在两个直连的相邻路由器接口之间传递的数据链路层协议的状态。

Show interface serial命令的输出中最重要的部分是关于线路和链路状态的信息，如例18-3所示。

例18-3 show interface serial命令

```
Cougar5# show interface serial 0
Serial0 is up, line protocol is up
```

```
Hardware is HD64570
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:02:57
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
   Conversations 0/0/256 (active/max active/max total)
   Reserved Conversations 0/0 (allocated/max allocated)
   Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 packets output, 0 bytes, 0 underruns
   0 output errors, 0 collisions, 8 interface resets
   0 output buffer failures, 0 output buffers swapped out
   0 carrier transitions
   DCD=up DSR=up DTR=up RTS=up CTS=up
```

第一个参数（Serial0 is up）与硬件层有关，本质上反映了接口是否在接收来自另一端（DCE）的载波检测信号。如果线路是down的，那么在背靠背的连接情况下可能是线缆故障，也可能另一端是“管理性down”。如果接口是管理性down，则是在配置中被手动地禁用了。

Show interfaces serial命令同样也能提供信息帮助诊断其他不容易确定的第1层问题。

下面的问题会引起串行链路上的载波转换不断增长：

- 服务提供商网络线路中断。
- 有故障的交换机、DSU或路由器硬件。

如果在show interface serial输出中显示输入错误不断增长，会有几个原因存在。与第1层相关的常见问题如下：

- 电信公司设备故障。
- 串行线路噪声。
- 使用错误电缆或电缆长度不合适。
- 电缆或连接受损。
- CSU或DSU缺陷。
- 路由器硬件缺陷。

另一个检查的区域是接口重置数目。接口置启是由于太多keepalive 丢失的结果。第1层的问题也可以由以下原因引起：

- 坏的电话线引起CD转换。

• CSU、DSU或交换机可能存在硬件故障。

错误的数目还与路由器处理的流量数量及统计数字的捕捉时间相关。路由器跟踪提供接口信息的统计数字。这些统计数字反映了路由器启动以后或上一次计数器清零以后的运行情况，如例18-4所示。

例18-4 统计数字积累

```
Cougars# show interface serial 0
Serial0 is up, line protocol is up
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     rellability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:02:57
```

如果show interface输出显示计数器上次的清除时间是“never”，那么使用show version检查路由器已工作了多长时间，如例18-5所示。

例18-5 路由器正常运行时间

```
Cougars# show version
Cisco Internetwork Operating System Software
IOS (tm) 2600 Software (C2600-BNSY-L), Version 12.2 (6h), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 26-Aug-02 23:23 by kellythw
Image text-base: 0x8303ED8C, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0 (10c), SOFTWARE
BOOTLDR: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0 (10c), RELEASE SOFTWA
RE (fc1)

Cougars uptime is 14 minutes
```

使用clear counter命令对计数器清零，如例18-6所示。在接口问题处理完毕后总是应清除计数器。从0开始能比较准确地把握网络状态并帮助验证问题是否已解决。

例18-6 clear counters命令

```
Cougars# clear counters
Clear "show interface" counters on all interfaces [confirm]yes
Cougars#
00:17:24: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
Cougars#
```

18.3 使用show cdp neighbors命令处理路由器的故障问题

Cisco Discovery Protocol（CDP）向直接邻居发布信息，包括MAC、IP地址和发送接口。

Show cdp neighbors命令的输出显示了直接相连的邻居信息，如例18-7所示。

例18-7 show cdp neighbors命令输出

```
routerA# show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge,
B   Source Route Bridge,
S - Switch, H - Host, I   IGMP

Device ID   Local Interface   Holdtime   Capability   Platform   Port   ID
routerB     Eth 0             151        R            2501       Eth    0
routerB     Ser 0             165        R            2501       Ser    0
```

这些信息对调试连接问题有帮助。如果怀疑电缆有问题，进行其他任何配置之前，使用no shutdown命令启用接口然后执行show cdp neighbors detail命令，如例18-8所示。这个命令显示了指定设备的详细信息，如活动接口、端口ID和设备信息。

例18-8 show cdp neighbors detail命令

```
routerA# show cdp neighbors detail
Device ID: routerB
Entry address(es):
   IP address: 198.92.68.18
Platform: 2501, Capabilities: Router
Interface: Ethernet0, Port ID(outgoing port): Ethernet0
Holdtime: 143 sec
```

如果物理层工作正常，所有直接相连的Cisco设备都应能显示出来。如果一个已知设备没有出现，很可能是第1层问题。

CDP关心的另一个领域是安全。CPD协议所提供的大量有用信息对安全性存在很大的潜在危险。基于安全理由，CDP应该只配置在Cisco设备之间，并且在普通用户端口和非本地管理链路上应该禁用。

18.4 使用show ip route和show ip protocols命令处理路由器的故障问题

show ip protocols和show ip route命令显示路由选择协议和路由选择表的信息。这两个命令的输出可以验证路由选择协议的配置。

show ip route命令也许是进行路由故障处理最重要的一个命令了。这个命令显示了路由选择表的内容。例18-9显示了所有已知的网络和子网的条目以及这些信息是如何获得的。

例18-9 Show ip route命令输出

```
Cougars> show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
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
```

```
* - candidate default

Gateway of last resort is not set

     144.253.0.0 is subnetted(mask is 255.255.255.0), 1 subnets
C  144.253.100.0 is directly connected, Ethernet1
R  153.50.0.0 [120/1] via 183.8.128.12, 00:00:09, Ethernet0
    183.8.0.0 is subnetted(mask is 255.255.255.128), 4 subnets
R      183.8.0.128 [120/1] via 183.8.128.130.00, 00:00:17, Serial0
                   [120/1] via 183.8.64.130, 00:00:17, Serial1
C  183.8.128.0 is directly connected, Ethernet0
C  183.8.64.128 is directly connected, Serial1
C  183.8.128.128 is directly connected, Ethernet0
```

如果到达特定网络的一台主机存在问题，show ip roiute命令可以验证路由器是否有到该网络的路由。

如果show ip route命令的输出没有预期所应学习到的路由或没有路由输出，则问题可能是没有路由选择信息交换。在这种情况下，通过show ip protocols命令检查路由器上的路由选择协议配置是否有误，如例18-10所示。

例18-10 show ip protocol命令输出

```
Router> show ip protocols
 Routing Protocol is rip
 Sending updates every 30 seconds, next due in 13 seconds
 Invalid after 180 seconds, hold down 180, flushed after 240
 Outgoing update filter list for all interface is not set
 Incoming update filter list for all interface is not set
 Redistributing: rip
 Routing for Networks:
 183.8.0.0
 144.253.0.0
Routing Information Sources:
 Gateway         Distance      Last Update
 183.8.128.12         120           0:00:14
 183.8.64.130         120           0:00:19
 183.8.128.130        120           0:00:03
Distance: (default is 120)
```

show ip protocols命令显示了整个路由器上IP路由选择协议相关的信息。这个命令可以验证配置了哪些协议、公布了哪些网络、哪些接口正在发送更新消息，以及路由选择更新消息的发送源。show ip protocols命令的输出还能显示路由选择协议关于计时器、过滤器和其他信息的路由选择参数。当存在多路由选择协议配置时，每一种协议的信息都会分开列出。

show ip protocols命令的输出可以用于诊断许多路由选择问题，例如确认一台怀疑在发送错误

路由器信息的路由器。该命令输出也能用于确认预期的协议、公布的网络和路由选择邻居是否存在。与所有故障处理过程一样，如果没有一个预期结果的输出文档，就可能很难定位故障。



实验活动 用show ip route检查路由选择表

在这个实验中，在路由器上配置RIP和IGRP并使用show ip route命令检查多路由选择协议的路由选择表结果。



实验活动 通过show ip route和show ip protocols处理路由选择问题

在这个实验中，通过show ip route和show ip protocols命令诊断路由选择配置错误。



实验活动 最终定向网关（缺省网关）

在这个实验中，在路由器上配置RIP路由选择协议并添加缺省路由（网关）。然后删除RIP和缺省路由后，重新在路由器上配置IGRP和添加缺省路由（网关）。



实验活动 最新路由更新

在这个实验中，收集路由选择更新和路由选择协议信息，判断找出最新更新的路由选择表。

18.5 使用show controllers serial命令处理路由器的故障问题

路由器的配置和故障处理多数是远程进行的，因此通常不可能直接地检查路由器连接情况。show controllers serial命令可用来判断线缆连接类型而无需检查线路的连接，如例18-11所示。

例18-11 show controllers serial命令输出

```
Cougar#4 show controllers serial 0/0
QUICC Serial Unit 0
idb at 0x20A31A8, driver data structure at 0x20A4C60
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x0
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x0006
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
... output omitted ...
DTE V.35 serial cable attached.
--- output omitted ---
```

能够确定控制器检测的线缆类型对于寻找不带有连接线缆、错误类型线缆或者缺陷线缆的串口是很有用的。

show controllers serial命令查询控制串口的集成电路或芯片，并显示有关这个物理接口的信息。不同的控制器芯片中这些输出信息可能不同。甚至同一个路由器类型，也可能使用不同的控制器芯片。

不考虑控制器类型，show controllers serial命令产生大量的输出信息。除了线缆类型之外，输出的许多信息是关于控制器芯片状态的内部技术细节。如果没有关于集成电路的专业知识，这些信息是没有用的。

18.6 debug介绍

debug命令有助于隔离协议和配置问题。debug命令通常显示动态数据和事件。由于show命令仅仅显示静态信息，所以它们提供的是路由器操作的历史性描述。而debug命令输出信息能够洞察路由器当前的事件。这些事件包括接口流量，网络节点产生的错误信息，协议专用诊断分组，以及其他有用的故障诊断数据。例18-12显示了debug ip rip命令的输出例子。

例18-12 debug ip rip命令

```
Router# debug ip rip
RIP Protocol debugging is on
Router#
RIP:     received update from 183.8.128.130 on Serial0
183.8.0.128 in 1 hops
183.8.64.128 in 1 hops
0.0.0.0 in 16 hops (inaccessible)
RIP:     received update from 183.8.64.140 on Serial1
183.8.0.128 in 1 hops
183.9.128.128 in 1 hops
0.0.0.0 in 16 hops (inaccessible)
RIP: received update from 183.8.128.130 on Serial0
183.8.0.128 in 1 hops
183.8.64.128 in 1 hops
0.0.0.0 in 16 hops (inaccessible)
RIP:   sending update to 255.255.255.255 via Ethernet0 (183.8.128.2)
subnet 183.8.0.128, metric 2
subnet 183.8.64.128, metric 1
subnet 183.8.128.128, metric 1
default 0.0.0.0, metric 16
network 144.253.0.0, metric 1
RIP:   sending update to 255.255.255.255 via Ethernet1 (144.253.100.202)
default 0.0.0.0, metric 16
network 153.50.0.0, metric 2
network 183.8.0.0, metric 1
```

例18-12中突出显示的部分显示了RIP debugging已经开启并显示哪些路由、网络和接口是可到达的，哪些是不可到达的。

debug命令的动态输出会造成性能消耗，性能消耗会导致处理器的高负载，破坏正常的路由器操作。因此，应适当地使用这个命令。可以使用debug命令来检查指定类型的流量或者在故障已经被缩减到少数的可能性后用作参考。换言之，debug命令应该用于隔离特定的故障，而不是用于监控正常的网络操作。

注释：尤其是debug all命令应谨慎地使用，因为这个命令可能破坏路由器的运作。

默认情况下，路由器发送debug输出和系统消息到控制台。如果一个Telnet会话被用于检查路由

器，debug输出和系统消息可以被重定向到远程终端。通过使用terminal monitor命令，可以通过Telnet会话来实现这个功能。从Telnet会话选择debug命令时应格外小心。不应选用任何可能使debug输出造成额外流量的命令。如果发生了这种情况，Telnet会话会马上使链路充满流量，或者使路由器耗尽一种或多种资源。要防止这种流量的产生应遵守的一个好的规则是永远不要在建立了会话的端口上调试任何活动。

不同的debug命令的输出是不同的。一些命令会频繁地输出许多行信息，但另外一些可能隔几分钟才输出一行或两行。例18-13显示了debug ip packet detail命令。

例18-13　debug ip packet detail命令输出

```
Router# debug ip packet detail
10w6d: TCP src=1075, dst=80, seq=785595392, ack=3448593899, win=64240 ACK
10w6d: IP: s=192.168.120.145 (Ethernet0/0), d=192.168.119.9 (Ethernet0 /0),
  g=192.168.119.9, len 60, forward
10w6d:     TCP src=1075, dst=80, seq=785595392, ack=3448599739, win=64240 ACK
10w6d: IP: s=192.168.120.145 (Ethernet0 /0), d=192.168.119.9 (Ethernet0 /0),
  g=192.168.119.9, len 60, forward
10w6d:     TCP src=80, dst=1075, seq=3448603559, ack=785595392, win=8446 ACK PSH
10w6d: IP: s=192.168.120.145 (Ethernet0), d=192.168.119.9 (Ethernet0 /0),
  g=192.168.119.9, len 60, forward
10w6d:     TCP src=1075, dst=80, seq=785595392, ack=3448604710, win=64240 ACK
10w6d: IP: s=10.1.1.82 (Serial0 /0), d=224.0.0.10, len 64, rcvd 2, proto=88
10w6d: IP: s=210.107.197.105 (Serial0 /0), d=192.168.119.255, len 1028,
  access denied
10w6d: ICMP type=8, code=0
10w6d: IP: s=10.1.1.82 (local), d=224.0.0.10 (Serial0 /0), len 22,
  sending broad/multicast, proto=88
10w6d: IP: s=0.0.0.0 (Ethernet0 /0), d=255.255.255.255, len 590, rcvd 2
10w6d:    UDP src=68, dst=67
10w6d: IP: s=192.168.120.50 (Ethernet0 /0), d=192.168.120.255 (Ethernet0 /0),
  len 241, rcvd 3

Router# undebug all
All possible debugging has been turned off
GAD#
```

前面这个例子中突出显示的内容指出了相关的网络并显示210.107.197.105收发的分组访问被拒绝。

另一个能增强debug输出的有效性的Cisco IOS软件服务是timestamps命令。这个命令在调试消息中放置一个时间戳。这个信息提供debug事件发生的时间和事件之间的持续时间。service timestamps debug uptime命令能够提供输出信息的时：分：秒，测定自从路由器上次通电启动后的时间数值，或者确定什么时间执行了reload命令。

no debug all命令和undebug all命令关闭所有的诊断输出信息。要关闭某个特殊的debug命令，使用命令的no形式。例如，如果用debug ip rip命令启动了监控RIP的调试进程，那么可以用no

debug ip rip来关闭。要了解当前正在用debug命令检查的那些内容，使用show debugging。



实验活动 利用debug进行路由选择问题的故障诊断

在本实验中，要使用系统化的OSI故障诊断流程和不同的show命令来收集信息以便诊断路由选择故障。然后可以使用不同的debug命令来协助进行故障诊断。

18.7 总结

本章学习了以下知识点：

- 应利用网络测试来维持一个网络平滑和有效地运行。应该逐层进行测试。
- 应使用一个结构化的方法来进行故障诊断。
- 在进行网络故障诊断、排除时，ping和telnet是两个有用的命令。
- traceroute命令可用于检测路由器之间链路的状态。
- 不同的show命令可以帮助确定第1层和第2层故障。
- show ip route和show ip protocols命令有助于识别路由选择问题。
- 基本的debug命令有助于发现关于路由器活动的信息。

为了补充本章你所学内容，参考本书所附CD - ROM中指定章节的视频、插图和e-Lab实验活动。

18.8　关键术语

keepalive——由一个网络设备发出的消息，目的是知会另一个网络设备它们两者之间的虚拟电路仍然是活动的。

网络接口卡（*network interface card*，*NIC*）——为一个计算机系统提供网络通信能力的电路板。

ping——Packet Internet groper。ICMP回应消息及其应答。在IP网络中使用，用于测试网络设备的可达性。

Telnet——TCP/IP协议集中标准的虚拟终端协议。Telnet被用于远程终端连接，使用户能够像连接到本地系统一样登录到远程系统并且使用其资源。

traceroute——在许多系统上都可用的程序，用于跟踪一个数据分组传递到目的地的路径。它经常被用于调试主机之间的路由故障。

18.9 复习题

完成所有复习题以测试你对本章主题和概念的理解。答案在附录C中。

1. 当技术人员进行基础的网络测试时，下列哪一项是对的？
   A. 该技术人员应按顺序从OSI参考模型的一个层到下一个层来进行。
   B. 该技术人员可以在任何希望的OSI层上进行。
   C. 该技术人员应从管理层进行。
   D. 该技术人员以随机的方式对OSI参考模型的层进行测试。
2. 当一个技术人员对网络进行故障诊断时，他/她应该开始一种什么方法？
   A. 该技术人员应该开始一种结构化的方法。
   B. 该技术人员应该开始一种他自己选择的方法。
   C. 该技术人员应该开始任何方法。
   D. 该技术人员应该开始一种碰巧的方法。
3. 当一个技术人员排除一个网络故障时？
   A. 从第1层开始
   B. 从第2层开始
   C. 从第3层开始
   D. 从第4层开始
4. 如果一个技术人员想测试网络的连通性，应使用哪个基本命令？
   A. telnet
   B. ping
   C. debug
   D. traceroute
5. 当一个网络管理员想在源和目的工作站之间验证应用层的软件，应使用以下哪个命令？
   A. ping
   B. telnet
   C. debug
   D. traceroute
6. 你怀疑你的网络上某个路由器正发送错误的路由选择信息。那么可以使用哪个命令来检查？
   A. router（config）**#show ip route**
   B. router**#show ip route**
   C. router**>show ip protocol**
   D. router（config-router）**#show ip protocol**
7. 为什么要显示IP路由选择表？
   A. 为了设置路由器的更新时间表
   B. 为了确定目标网络地址和下一跳的匹配
   C. 为了跟踪数据报从什么地方来
   D. 为了设置路由器的参数和过滤器
8. 如果你想在路由器发送和接收RIP路由选择更新时查看这些信息，你应该使用哪个命令结构？
   A. router# **show ip rip**
   B. router# **debug ip protocols**
   C. router# **debug ip rip**
   D. router# **show ip rip update**

9. Debug命令的动态输出会导致_____处理器负载从而造成性能的浪费?
   A. 高
   B. 低
   C. 中等
   D. 最大
10. 默认情况下，路由器发送debug的输出信息和系统信息到哪里?
   A. 控制台
   B. 交换机
   C. PC
   D. 用户
11. telnet命令提供哪种类型的终端?
   A. Register
   B. Virtual
   C. Cisco IOS Software
   D. Command
12. ICMP代表什么?
   A. Internet Control Message Parameter
   B. Internal Control Message Protocol
   C. Internet Control Message Protocol
   D. Internet Control Message Performance
13. 许多网卡的接口用于显示是否存在一个合法连接的指示灯是以下哪种类型?
   A. Indicator
   B. Catalyst
   C. Responsive
   D. Inactive
14. telnet在OSI参考模型的哪一层上使用?
   A. 第1层
   B. 第5层
   C. 第6层
   D. 第7层
15. 如果路由选择协议没有启用或者IP地址检测不到，管理员应从OSI模型的哪一层开始检查?
   A. 第1层
   B. 第2层
   C. 第3层
   D. 第4层



第19章 深入理解TCP

目标

学习完本章之后，你应该能够：

- 描述TCP及其作用
- 描述TCP的同步和流控制功能
- 描述用户数据报协议（User Datagram Protocol，UDP）的操作和处理过程
- 识别公共端口号
- 描述主机之间的多重会话
- 描述端口编号方式以及知名的端口号
- 比较MAC地址、IP地址及端口号

本章介绍TCP/IP如何在各种类型的互联网络上确保通信。此外，还介绍关于TCP/IP协议栈组件的相关知识，例如支持文件传输、电子邮件、远程登录及其他应用的协议。此外，本章还介绍可靠的和不可靠的传输层协议以及网络层上无连接数据报（分组）的传输。最后，介绍ARP和RARP协议如何工作。

请注意应配合本书附带CD-ROM上的e-Lab实验、视频和插图一起观看本章内容，CD-ROM上的素材就是用于支撑本章内容和增强概念的理解。

19.1 TCP/IP协议集

TCP/IP协议集是美国国防部高级研究规划署（Defense Advanced Research Projects Agency，DARPA）所作研究的一部分。起初是为了提供DARPA内部的通信而开发的。后来，TCP/IP包含在BSD UNIX中。现在，TCP/IP已经成为互联网络通信的事实标准，并成为Internet上的传输协议栈，这使得全球范围内的数以百万的计算机能够互相通信。

本章关注TCP/IP的原因在于：

- TCP/IP应用普遍，你将来在工作中可能要用到它。
- TCP/IP可以作为理解其他协议的有用参考，因为它包含了很多有代表性的元素，这在其他的协议中也可以出现。

• TCP/IP被路由器用作一种配置工具，因此很重要。

TCP/IP协议集的功能是将信息从一个网络设备传送到另一个网络设备。为了实现这一功能，TCP/IP协议集在下层与OSI参考模型进行严格的映射，并支持所有标准的物理层和数据链路层协议（见图19-1）。

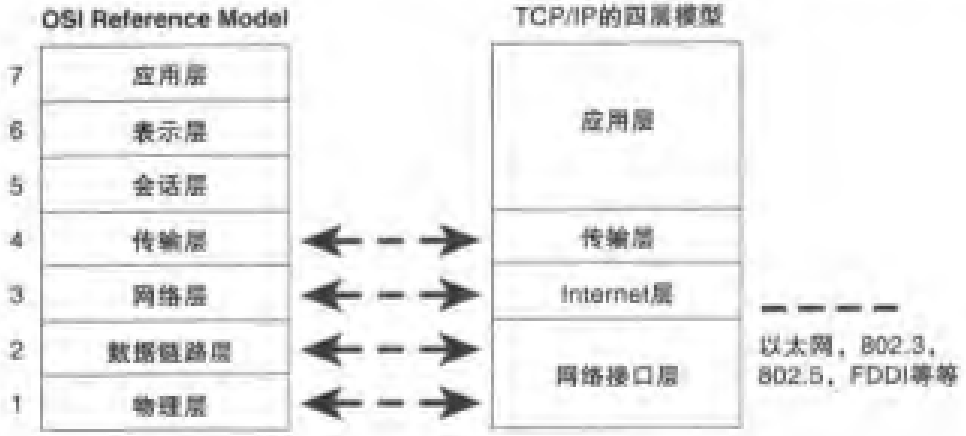


图19-1　TCP/IP的四层模型

OSI的各层中与TCP/IP紧密联系的是第7层（应用层）、第4层（传输层）、第3层（网络层）。这些层中包含了用于完成各种功能的协议，但它们都与信息传输有关。TCP/IP的各层能与OSI模型进行很好的映射：TCP（位于传输层或主机-主机层）映射到OSI的传输层，Internet层映射到OSI的网络层。

TCP/IP能够完成任何互相连接的网络内的通信，也同样适用于LAN和WAN的通信。TCP/IP不仅包括第3层和第4层的规范（例如IP和TCP），而且还包括一些用来支持常见应用的规范。这些应用包括电子邮件、远程登录、终端仿真和文件传输。

19.1.1　TCP/IP协议栈与应用层

TCP/IP的应用层合并了OSI模型中的会话层、表示层和应用层的功能。TCP/IP有支持文件传输、电子邮件和远程登录的各种协议，包括（见图19-2）：

• **域名系统**（*Domain Name System，DNS*）是在Internet中用于将公开发布网络节点名字转换为IP地址的系统。这可看作是传输层功能，因为它为上层（应用层）提供服务，使用下层（Internet层）的服务。

• Windows Internet命名服务（*Windows Internet Naming Service，WINS*）是微软开发的一个标准，用于自动地将NT工作站同Internet域名关联。

• HOSTS是由网络管理员创建并放在服务器上的一个文件。该文件提供了IP地址和计算机名字之间的静态映射。

• **邮局协议**（*Post Office Protocol，POP3*）一种Internet标准，用来在邮件服务器上存放电子邮件，直到你访问邮件服务器并将邮件下载到自己的计算机上。它允许用户使用多种安全级别从收件箱接收邮件。



图19-2　应用层协议

• **简单邮件传输协议**（*Simple Mail Transfer Protocol，SMTP*）管理计算机网络中电子邮件的发送。它只支持纯文本数据的发送。

• **简单网络管理协议**（*Simple Network Management Protocol，SNMP*）提供监视和控制网络设备、管理配置、数据收集、性能和安全等功能。

• **文件传输协议**（*File Transfer Protocol，FTP*）是一种可靠的面向连接的服务，使用TCP来在支持FTP的不同系统间传送文件。它支持双向的二进制和ASCII文件的传送。

• **简单文件传输协议**（*Trivial File Transfer Protocol，TFTP*）是一种采用UDP的无连接服务。TFTP用于路由器上配置文件和IOS映像的传递，以及支持TFTP的系统之间的文件传递。TFTP在某些局域网中非常有用，因为在稳定的环境下，它的传送速度比FTP快。

• **超文本传输协议**（*Hypertext Transfer Protocol，HTTP*）是用于万维网和内联网上信息交换的Internet标准。它支持多种文件类型，包括文本、图形、声音和视频。它所定义的通信过程首先由Web浏览器发出信息请求并发送到Web服务器。

下面列出一些用于故障诊断的协议：

• **Telnet**是一个标准的终端仿真协议。客户端利用telnet可以向Telnet服务器发起远程的终端连接。它使得用户能远程连接到路由器并输入配置命令。

• **Ping**（*Packet Internet Groper*）用于判断某个计算机是否可达。Ping使用了ICMP的echo请求和echo应答消息。

• **Traceroute**程序在很多系统上都有，它的功能和ping类似，但提供的信息更多。Traceroute可以跟踪分组到达目的地的路径，用于调试有关路由的问题。

你也应熟悉一些基于Windows的工具：

• **NBSTAT**——用来对NetBIOS名字解析进行故障排除的工具，可以用来查看和删除名字缓存的内容。

• **NETSTAT**——用来提供有关TCP/IP统计信息的工具；通过它，可以查看有关TCP/IP连接的状态信息以及关于TCMP、TCP、UDP的统计信息。

• **ipconfig/winipcfg**——用来查看某个设备上所有网卡的当前网络设置的工具；可以用来查看MAC地址、IP地址、子网掩码和网关，以及DNS和动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）信息。

19.1.2 TCP/IP协议栈与传输层

本节介绍***传输控制协议***（Transmission Control Protocol，TCP），即TCP/IP协议集中的第4层协议。TCP是一种可靠的、面向连接的协议，通过使用同步、窗口技术和窗口大小、序列号和确认来确保可靠的数据传输。

传输层使用户设备能够把从各种上层应用接收的数据进行分段，以便放在同一个第4层数据流上传送，并使得接收设备能重新对这些数据段进行组装。第4层的数据流是网络中两个终端点之间的逻辑连接；它提供了从源主机到目的主机的传输服务。这种服务有时也被称作*端到端服务*（*end-to-end service*）。传输层提供了以下两种协议（见图19-3）：



图19-3 传输层协议

• **TCP**——一种面向连接的可靠协议。通过滑动窗口提供流量控制，通过序列号和确认提供可靠性。TCP重发一切没有收到确认的数据，并在终端用户的应用程

序之间提供一条虚电路。TCP的优势在于能提供分段的可靠传输。

• **用户数据报协议**（*UDP*）——一种无连接的不可靠协议，它可用于传送消息但是在段的传输过程中不提供软件检查。UDP的优势在于传输速度。因为UDP不使用确认，通过网络发送的控制通信量更小，因此传输速度更快。

19.1.3　TCP和UDP分段格式

TCP是一个面向连接的协议。面向连接意味着终端工作站均知道对方并就该连接保持经常的通信。从非技术性角度，面向连接通信的一个经典的例子就是两个人之间通过电话进行通话。而无连接会话的一个很好的例子就是美国邮政服务，用户把信函放到邮件中然后期待邮政处理流程来传递这个邮政包裹。图19-4显示了TCP分段报头格式，其中字段定义如下面的列表所示。



图19-4　TCP分段格式

• **源端口**（*Source port*）——分段的源端口编号。

• **目的端口**（*Destination port*）——分段的目的端口编号。

• **序列号**（*Sequence Number*）——用来保证到达数据顺序的编号。它是用户数据字段中第一个字节所分配的编号。

• **确认号**（*Acknowledgment number*）——所期望的下一个TCP字节的编号。

• **报头长度**（*Header length*）——报头的字数，字长为32位。

• **保留域**（*Reserved*）——设为0。

• **编码位**（*Code bits*）——用于控制功能（比如建立和终止一个会话）。

• **窗口**（*Window*）——发送方愿意接收的字节数目。

• **校验和**（*Checksum*）——根据报头和数据字段计算出的校验和。

• **紧急指针**（*Urgent*）——指向紧急数据的末尾。

• **选项**（*Options*）——目前定义的一项是：TCP分段的最大长度。

• **数据**（*Data*）——上层协议的数据。

当使用UDP时，如果需要，应用层协议必须提供可靠性。UDP不采用任何的窗口和确认机制。它是为那些不需要将分段组装在一起的应用而设计的。图19-5显示了UDP的头部。

源端口（16）	目的端口（16）	长度（16）	校验和（16）	数据（长度可变）

图19-5　UDP的头部格式

19.1.4 TCP运作

IP地址允许网络之间分组的路由。IP地址支持在网络间对数据包进行路由选择。然而，IP不保证传递成功。传输层负责可靠传输并调节源和目的之间的数据流。这种可靠性是通过滑动窗口（sliding windows）、顺序编号（sequencing numbers）和一个保证每个主机都准备好并愿意进行通信的同步过程实现的，如图19-6所示。



图19-6 TCP运作

为了理解可靠性和流量控制，可以设想谈话中的两个人。首先它们需要会面，并可能需要握手来相互表示准备开始一个会话，将要发送信息。在他们交谈和交互信息的过程中，如果一个词或短语没听见或没有到达对方，对方可能会要求说话方重复他的话（可靠性），以便他或她能跟上对方的话（流量控制）。传输层，OSI模型的第4层通过TCP为第3层提供这些服务。

19.1.5 三次握手

TCP是一种面向连接的协议。在数据传输前，两台通信主机会经过一个同步过程来建立一个虚拟连接。

同步过程确保了双方都为数据传输做好了准备，并使得设备能确定初始序列编号（ISN，initial sequence numbers）。这个过程被称为三次握手（three-way handshake）。

同步是通过交换带有ISN和一个SYN（代表“同步（synchronize）”）控制比特的数据包实现的。成功的连接需要一种适当的机制选择初始的序列号，也会涉及一些握手交换ISN的内容。同步要求每一方都发送自己的ISN并收到来自连接另一方的确认和ISN。

各方都必须收到另一方的ISN，并以特定的顺序发送一个确认回应（ACK）。三次握手使用下列的三步过程来在两台设备间建立一个虚拟连接：

1. 主机通过发送一个SYN数据包来发起一个连接，该数据包表示了自己初始的顺序编号x。包头中的某个比特也进行了设定，表示是一个连接请求。这个比特是TCP头中的code字段。

2. 另一方的主机收到该数据包，记录顺序编号x，用编号为x+1的确认进行回应，并表示自己的初始顺序编号是y。确认编号x+1表示主机收到了直到x的所有八位组，接下来希望接收编号为x+1的八位组。

3. 发起方主机用一个顺序编号为y+1（对方的顺序编号+1）的简单确认（ACK）进行回应，表示收到了前一个ACK，这就完成了连接过程。

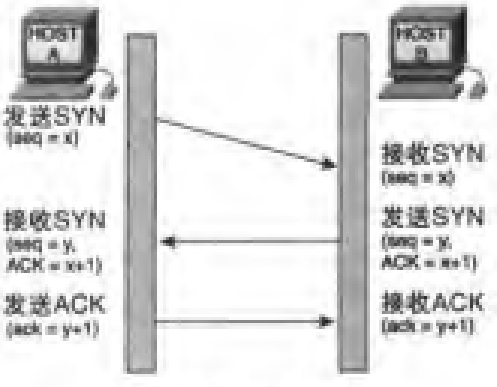


图19-7 三次握手

由于第二步和第三步合并为一个消息，因此这个信息交换过程称为三次握手/建立连接。如图19-7所示，连接双方就三次握手/建立连接的顺序编号实现了同步。

序列号是两个设备之间开始通信的一部分，理解这点是非常重要的。序列号被用作两台设备之间的参考起始号。序列号提供每台主机一个确认SYN的途径，以便接收者知道发送者正在对正确的连接请求做出响应。

由于TCP可能使用不同的机制来挑选ISN，因此三次握手是必需的。接收方接收到第一个SYN时无法识别这个分段究竟是不是一个延迟了的老分段，除非它能记得上一次通信中的序列号，但这

又并非总是可能的。因此，接收者必须要发送者来确认这一次的SYN。此时，因为TCP是点对点（平衡）的通信方式，任何一方都可以开始通信，任何一方也能终止通信。

19.1.6　同步中的拒绝服务攻击

*拒绝服务（DoS）*攻击是指拒绝为合法主机建立连接提供所需的服务。DoS攻击是黑客们经常使用的一种使系统响应暂时中止的方法。SYN泛洪就是其中一种DoS攻击的类型，它发生在TCP的三次握手同步过程中。

在三次握手中，发起通信的主机发送一个SYN分组。这个SYN分组就像其他的分组一样包含源IP地址和目的IP地址。接收者使用这个源端和目的端地址信息给发起通信方发送SYN/ACK分组。

在一个DoS攻击中，黑客发起一个同步请求但是伪造一个源IP地址。接收方的回应将发到一个不存在的不可达的IP地址，于是在等待发起通信方的最终ACK时就会被挂起。等待请求报文都位于连接队列或者内存中。这种等待状态要求受攻击的设备委托系统资源（比如内存）进入等待进程直到连接计时器超时。黑客们发送大量的假SYN请求给受攻击的主机，使它们在响应和等待虚假的连接中消耗大量的资源，从而阻止它们进行正常合法的通信。

为了防御这些攻击，管理员可以减少超时的周期并且增加连接队列的长度。而且，软件也可以检测到这类攻击并启动防御措施。图19-8显示了同步中的一个DoS攻击。



图19-8　DoS攻击

19.1.7　窗口技术和窗口大小

在许多例子中，需要传输的数据都太大了以至于不能用一个数据段来传送。这时，数据必须分成小段以适合传送。TCP负责将数据进行分段。这个过程类似于给孩子喂食。因为大部分小孩子一次不能吃很大一口，于是喂食者就把食物切成小块使得小孩子的嘴可以容纳它们。另外，接收方也许不能以发送方发送数据的速率来接收数据。这种差异有时是因为接收方正在处理别的工作，有时只是因为发送方是一台更强的设备。

数据分段后，它必须被发送到目的设备。*流量控制*是TCP提供的服务之一，它规范了在一个传送周期内可以发送多少数据。流量控制的方法称为*窗口技术*。

窗口的大小决定了在收到目的主机的确认之前可以发送的数据量。一台主机发送了窗口大小的字节后，在发送更多的信息之前主机必须等待一个所发的数据已经收到的确认。比如，对于大小为1的窗口，主机在发送下一个分段之前必须收到前一个分段的确认，如图19-9所示。

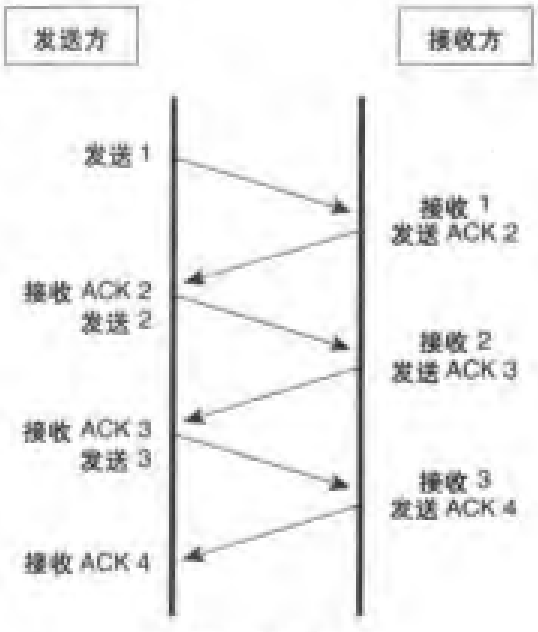


图19-9　大小为1的窗口

在决定传输长度时TCP使用滑动窗口。滑动窗口技术使得设备之间可以协商一个窗口的尺寸大小，使得每次可以传输不止1个字节的数据，如图19-10所示。滑动窗口技术也使得目的设备可以和源设备进行通信。如果目的设备无能力处理所收的数据，它可以要求减少数据的发送量。相反，如果目的设备可以处理比当前收到的数据量更多的数据，它也可以指示源设备发送更多的数据。

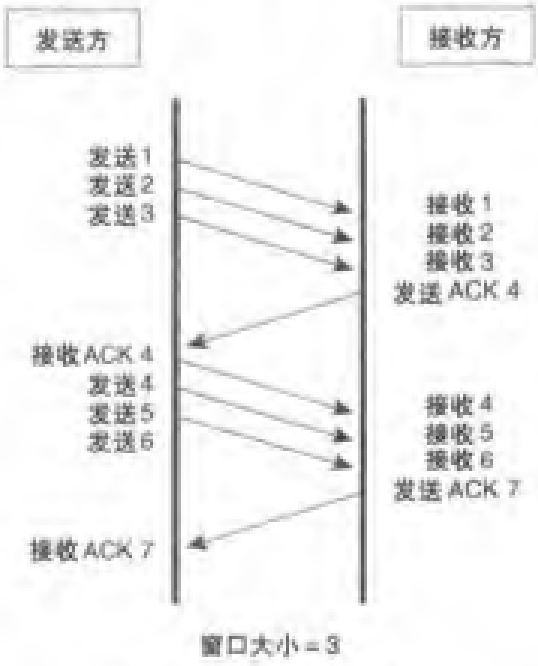


图19-10 更大的窗口尺寸

19.1.8 序列号

TCP将数据进行分段，接着，发送方将数据段发送给接收方。数据是同步传输的，并且窗口的大小可以协商以决定一次可以传输多少字节。一旦所有的数据传送结束，接收方必须重组所接收的数据段。在传输过程中，数据段到达的顺序是无法保证的，所以TCP使用序列号来解决这个问题。由于TCP给每个数据段使用了序列号，接收方可以按原来的顺序正确地重组所有的字节。序列号显示了目的设备如何在收到字节时正确地重组它们。

如图19-11所示，序列号也像参考号一样使接收方知道是否接收了全部的数据并通知发送方重传丢失的数据片断。因为发送方只需要重传丢失的数据段而非所有的数据，所以这个特性有利于提高传输效率。

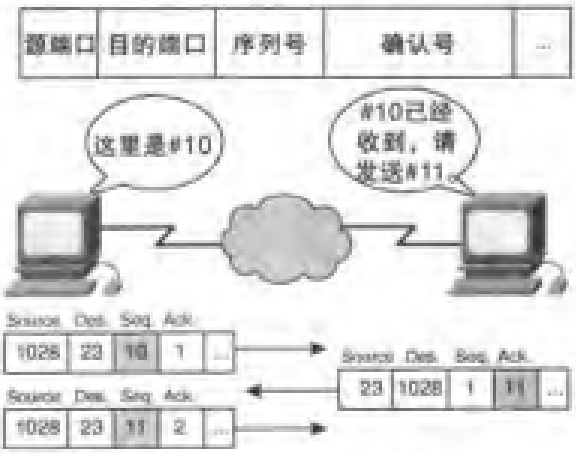


图19-11 序列确认号

TCP分段在传送前，都会被编号。本章前面的图19-4显示了TCP分段的格式。图中显示了序列号部分紧跟在目的端口后面。TCP使用序列号在接收方将数据段重组为一条完整的信息，如果某个数据段中的序列号丢失了，该数据段将被要求重传。

19.1.9 正确的ACK

确认是同步过程、滑动窗口和数据编序中共同的步骤。在一个TCP数据段中，序列号字段后面紧跟着就是确认字段，该字段也称为代码字段。这里存放的是ACK和SYN的值。

IP协议是不可靠的协议，无法验证数据段是否真的到达了目的地。因此，数据段必须在不知道它们是否可以真正到达目的地的情况下进行传输。TCP使用正确的确认和重传机制来控制数据流和确保数据的传输。

许多协议通常都使用正确的确认和重传（PAR）机制来保证传输的可靠性。在PAR中，源端发送一个分组之后就启动一个计时器，并且等待一个确认才能发送下一个分组。如果在等到一个确认之前计时器超时，则源端重传该分组并重新启动计时器。TCP采用期待确认的方法，也就是说确认号指的是所期望收到的下一个字节号。

窗口技术是一种流量控制机制。在窗口技术中，要求源端设备在发送一定量的数据后必须收到目的端的一个确认。比如当窗口大小为3时，源端设备一次可以发送3个字节给目的端，然后它必须等待一个确认。如果目的端收到了这3个字节，它会发送一个确认告诉源端现在可以发送更多的字节

了。如果目的端因为缓存溢出或别的原因没有收到这3个字节，它不会发送确认。如果源端没有收到确认，它知道这些字节必须重传，于是传输速率就会变慢。

19.1.10　UDP运作

TCP/IP协议栈包含许多执行不同的特定任务的协议。在OSI模型中，IP协议提供了第3层的无连接的传输，TCP保证了第4层的面向连接的可靠的分组传输，UDP提供了在第4层的无连接的不可靠的分组传输。

TCP和UDP都使用IP作为第3层的协议。而且TCP和UDP都被不同的应用层协议所使用。TCP提供给应用层的协议包括FTP、HTTP、SMTP和DNS。UDP是DNS、TFTP、SNMP和DHCP所使用的传输层协议。图19-12阐明了TCP/IP应用层、传输层和网络层各种协议的关系。

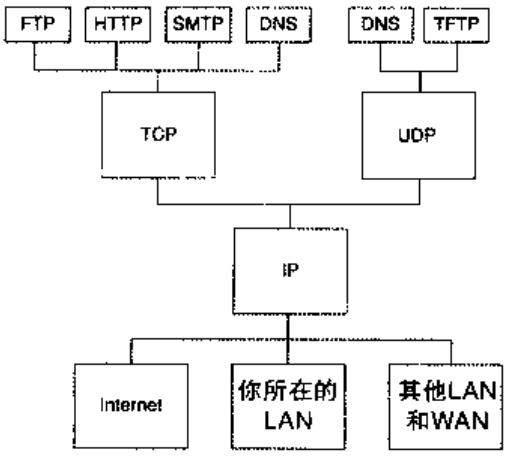


图19-12　TCP/IP应用层、传输层和网络层协议

当应用层需要分组完整、有序和不重复地传输时就必须使用TCP协议。然而，使用TCP协议时，有时用于确保分组传输的总开销过大是一个问题。并非所有的应用层都需要有保证的传输，因此，有些应用层协议使用UDP提供的更快的无连接的传输机制。RFC 768中所描述的UDP是一个没有确认和保证的分段交换简单传输标准。比如，TFTP可以用来从一个TFTP服务器传输一个配置文件或者Cisco的IOS软件镜像文件到以太网上的一台路由器。由于物理层的连接通常都很好，所以TCP的确认和重传能力是不必要的，因此TFTP使用有效的UDP传输层协议。

UDP不使用窗口和确认技术。因此，应用层协议必须提供错误校验。UDP是为那些不需要重组分段的应用层协议服务的。

本章前面的图19-5描述了UDP分段的格式。源端口是一个可选项，只有当信息需要返回给发送的主机时才使用该字段。目的端口字段规定了UDP提供服务的应用层协议。从主机到一个DNS服务器的DNS请求的目的端口值是53，这是DNS的UDP端口号。长度字段定义了UDP分段中的字节数。UDP检验和是可选字段，一般用来确保传输中的数据没有损坏。UDP是封装在IP分组中在网络中传输的。

在UDP分段到达目的IP地址后，接收端的主机必须有一种机制来决定该分段的目的地应用层协议。端口就是用于这个目的。如果一台主机同时运行TFTP和UDP服务，它必须对到达的UDP分段所需要的服务做出决定。UDP报头中的端口号字段值就可以决定UDP分段被传送到哪个应用层协议。

19.2　传输层端口综述

传输层端口是一个16比特的号码，用来标识通信设备双方的连接端点。一个特定的网络连接是由4部分（源地址、源端口、目的地址、目的端口）序列规定的。原则上，这一规则允许任何两个主机之间只有惟一的一个UDP连接。UDP仍然是无连接和不可靠的。为了支持那些需要可靠的、有序的数据流的面向连接的应用层协议，就必须使用TCP。与UDP一样，TCP也使用端口来定义连接端点。

19.2.1　主机之间的多会话

在任一瞬间都有成千上万的提供数百种不同服务的分组在一个现代的网络中传输。通常，服务器都同时提供几种不同的服务，这就引起了分组地址的惟一性问题。比如，对于一台同时运行

SMTP和WWW的服务器，客户就不能仅使用TCP协议构造出一个目的IP地址是该服务器的分组，因为SMTP和WWW都使用TCP作为它们的传输层协议。为了使分组能到达服务器上适当的服务程序，主机之间的每个会话都必须与一个端口号相关联。如果没有办法来区分不同的会话，客户则无法使用同一台服务器同时发e-mail和浏览网页。必须有一种方法来区别传输层的会话。

运行TCP/IP协议的主机都会在传输层将端口和某些应用关联起来。端口号用来跟踪网络中不同的会话。当一台主机与一台同时运行多种服务的服务器通信时，端口号就是必不可少的。TCP和UDP都使用端口号将信息传递给上层。图19-13显示了一个TCP和UDP端口的例子。

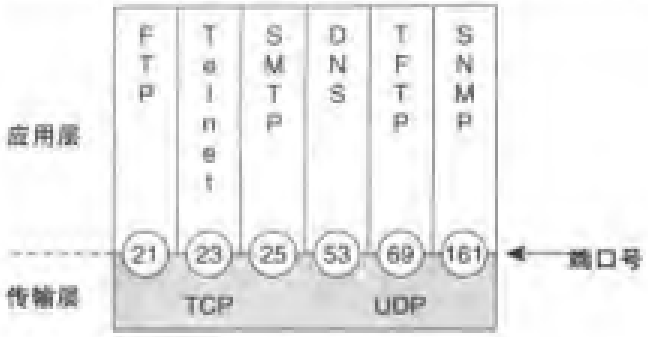


图19-13 TCP和UDP端口号

应用软件开发人员已经协商使用RFC 1700中定义的一些知名端口号。比如FTP使用的端口号为21。那些不涉及带有知名端口号的应用的会话则使用从一个特定范围内随机选取的端口号。在TCP分段中这些端口号可以作为源和目的地址。表19-1列出了保留的TCP和UDP端口号。

表19-1 保留的TCP和UDP端口号

十进制数	关键字	说明
0	-	保留
1-4	-	未分配
5	rje	远程作业入口（RJE）
7	echo	回应
9	discard	丢弃
11	users	活动用户
13	daytime	白天
15	netstat	Who is up或netstat
17	quote	日期引用
19	chargen	字符发生器
20	ftp-data	文件传输协议（数据）
21	ftp	文件传输协议
23	telnet	终端连接
25	smtp	简单邮件传输协议
37	time	时间
39	rlp	资源定位协议
42	nameserver	主机名字服务器
43	nickname	Who is
53	domain	域名服务器
67	bootps	Bootstrap协议服务器
68	bootpc	Bootstrap协议客户端
69	tftp	简单文件传输协议
75	-	任何专用拨号服务
77	-	任何专用RJE服务
79	finger	Finger
80	HTTP	超文本传输协议
123	ntp	网络时间协议（NTP）
133-159	-	未分配
160-223	-	保留
224-241	-	未分配
242-255	-	未分配

端口号的指定范围如下：

- 低于255的端口号用于公共应用。
- 255到1023的端口号分配给各公司用于其销售的应用程序。
- 1023以上的端口号未作规定。

终端系统利用端口号来选择合适的应用。如图19-14所示，源端口号1028是由源主机动态分配的，通常这些端口号都大于1023。Internet地址分配机构（IANA）控制分配0到1023之间的端口号。

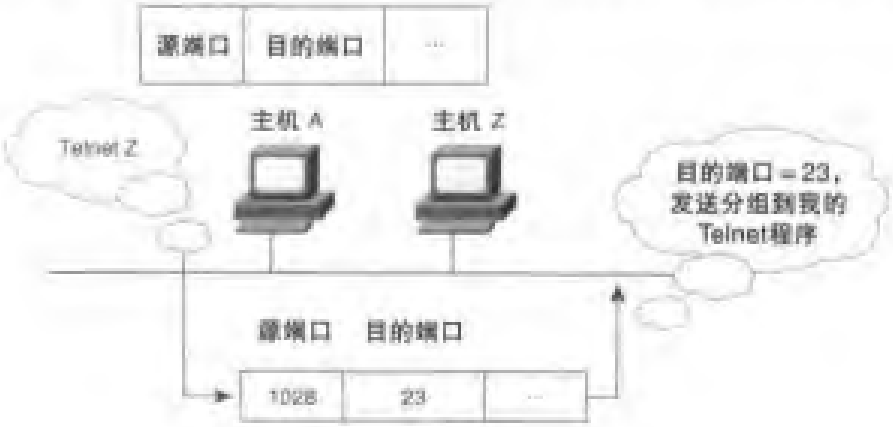


图19-14　源和目的端口

19.2.2　服务端口号

通信中的任何一种服务都必须有一个端口号。一个远端的主机要想获得服务器上的某种运行在一定的传输层协议上的服务就必须使用端口号。在RFC 1700中定义的某些端口号是***知名的端口号***。这些端口保留在TCP和UDP中。

这些知名的端口号可以用来区别传输层之上的某些应用。比如，一台FTP服务器使用端口号为20和21的TCP连接为客户提供FTP服务。这样服务器就可以确切地知道用户所请求的服务是什么。TCP和UDP都用端口号来决定正确的服务类型以便传递正确的服务请求。

19.2.3　客户端口号

客户想请求服务器上的任何服务时都必须提供源和目的端的端口号。TCP和UDP分段中都包含有源和目的端的端口号字段。目的端口号或称为服务端口号通常都是一些已定义的知名的端口号，而由客户定义的源端口号则是动态分配的。

一般来说，源端口号是由客户从1023以上的号码中随机分配的。比如，一个客户想用TCP与Web服务器通信，可以使用目的端口号80并给源端分配端口号1045。当这个分组到达服务器时，它将被传递给传输层并根据端口号80最终可以到达万维网服务器。万维网服务器会响应这个客户的请求，并在传输层使用源端口号为80，目的端口号为1045的分段。这样，客户和服务器就可以根据端口号来辨别各个分段所关联的进程。如果一个客户同时有两个浏览器对两个不同的Web服务器会话，这两个会话的目的端口号都是80。然而，它们的源端口号却不相同（比如一个是1045，另一个是1048）。不同的源端口号使客户可以跟踪不同的会话。

19.2.4　端口编号和知名的端口号

端口号是由TCP或UDP报头中的两个字节来表示的。这16比特产生的端口号可以从0到65,535。这些端口号分为三类：

- 知名端口号
- 已注册的端口号
- 动态或专用的端口号

前1023个端口号是知名端口号。正如前面所讨论的，这些端口号是用于一些众所周知的网络服务，比如TFP、Telnet、DNS或者HTTP。已注册的端口号范围从1024到49151，这些端口号是用于像Cisco-NET-Mgmt协议和日程接入协议。而从49151到65535之间的端口号则是用作动态或专用的端口号。

19.2.5 主机之间的多会话例子

端口号可以用于跟踪主机之间的多会话。一个端口号和一个网络地址组合起来可以形成一个套接字。一对套接字（每台主机一个），可以形成一个惟一的连接。例如，一台主机可以通过23端口建立一个telnet连接，同时通过80端口浏览网页。因为来自同一台主机，分组的IP地址和MAC地址是相同的，但是端口号是不同的，因为它们是不同的协议，所以套接字不同。



实验活动 多活动主机对话

在此实验中，在路由器上启用HTTP服务，在单个主机上用netstat命令观察多个HTTP和Telnet会话。



实验活动 知名端口号和多会话

在此实验中，在单个主机上用netstat命令观察多个会话的知名端口号。

19.2.6 比较MAC地址、IP地址和端口号

MAC地址、IP地址和端口号常被混淆，但这个混淆可以通过参照OSI参考模型解释地址来避免。端口号在传输层，由网络层提供服务。网络层指定逻辑地址，或IP地址。网络层由数据链路层提供服务，数据链路层指定物理地址或MAC地址。

19.3 TCP/IP与Internet层

Internet Protocol（IP）是第3层协议，负责通过地址设置在企业内部网和Internet上正确地传送分组到目的地，路由器使用IP报头里的IP地址信息来决定分组为了到达目的地应该从哪个接口被交换，IP不提供任何服务确保分组到达目的，IP被描述为一个不可靠、无连接的协议，分组可能会在路由中被丢弃、顺序错误地到达，或发送速度快过接收者的能力，IP没有办法克服这些或其他传递问题。

TCP/IP协议栈的Internet层对应于OSI模型中的网络层，网络层负责通过软件地址在网络上传送分组。

图19-15显示了运行在TCP/IP的Internet层上的一些协议，它们对应于OSI中的网络层。

- IP——为数据报提供无连接的、尽最大努力传递的路由功能，它不关心数据报的具体内容，只是寻找一条能把数据报发送到目的端的路径。
- ICMP——提供控制和消息传递功能。
- **地址解析协议（*ARP*）**——为已知IP地址确定数

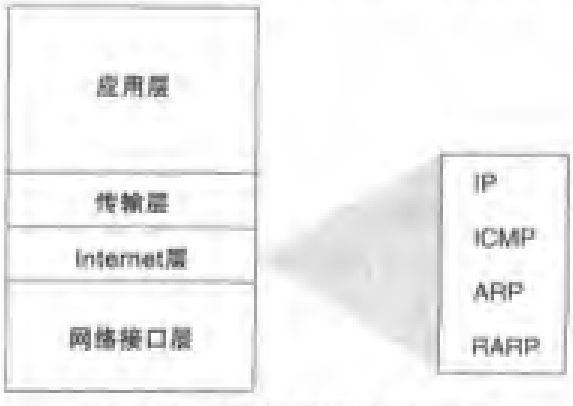


图19-15 TCP/IP模型的Internet层

据链路层（MAC）地址。

- **反向地址解析协议**（*RARP*）——当数据链路层地址已知时，确定网络地址。

19.3.1　ARP如何工作

ARP用来解析或映射一个已知的IP地址到MAC子层地址。这种映射是为了能够通信。因为数据链路硬件只会接收所含MAC地址与之相匹配的帧（或广播MAC地址）。要为数据报确定一个目的MAC地址，必须检查ARP缓存表。每个在TCP/IP网络中的主机（路由器、工作站、服务器等）都维护一个ARP缓存表。如果地址不包含在表中，ARP就发送一个网络上每一个主机都能收到的广播来找目的主机。术语本地*ARP*是指当发送请求的主机和目的主机共享同一介质或线路时的搜索过程。如图19-16所示，发送ARP之前，必须知道子网掩码，以便确定节点是否在同一个子网上。

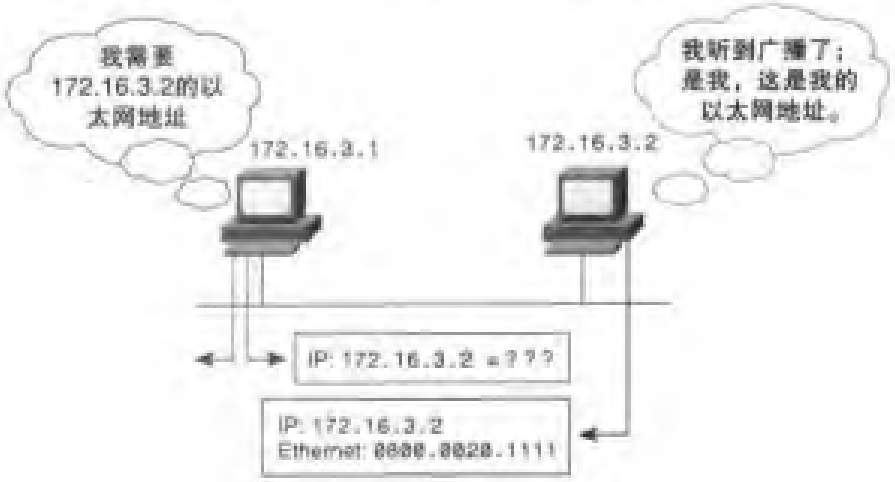


图19-16　OSI模型的网络层

*RARP*是一个TCP/IP协议，使物理地址（如以太网地址）转换为IP地址。因此，该协议是与ARP相反的。像无盘工作站这样的主机，在启动时经常只知道它们的硬件接口地址或MAC地址，却不清楚自己的IP地址，它们必须从外部源来发现自己的IP地址。通常，运行RARP协议的RARP服务器来解决这个问题。

19.4　总结

本章学习了以下知识点：

- TCP是一种面向连接的传输层协议，对不可靠的IP协议提供必要的服务质量处理。
- TCP提供可靠性、流量控制和虚拟连接服务。
- TCP利用三次握手建立主机间同步通信。
- 滑动窗口实现动态数据流量控制。
- 序列号确保接收主机正确组装数据。
- UDP是一种无连接的传输层协议。
- UDP和TCP用端口号区分上层应用。

为了补充你在本章所学的知识，请参考本书配套光盘中对应章节的视频、插图和e-Lab实验活动。

19.5 关键术语

地址解析协议（*Address Resolution Protocol, ARP*） 用于将IP地址映射MAC地址的Internet层协议。

拒绝服务（*denial-of-service, DoS*） 网络上的一种攻击类型，通过泛洪无用流量造成网络崩溃。

反向地址解析协议（*Reverse Address Resolution Protocol, RARP*） TCP/IP协议栈中的协议，提供基于MAC地址查找IP地址的方法。

传输控制协议（*Transmission Control Protocol, TCP*） 一种面向连接的传输层协议，提供可靠的全双工数据传送，TCP是TCP/IP协议栈中的一部分。

用户数据报协议（*User Datagram Protocol, UDP*） TCP/IP协议栈中的无连接传输层协议。UDP是一种简单的协议，交换数据报时无需确认或保证重传。错误处理和重传需要由其他协议解决。

知名端口（*Well-know ports*） 这些端口定义在RFC 1700文档中，保留在TCP和UDP中，这些知名端口号能够区分运行在传输层上的应用。

窗口技术（*windowing*） 管理流量，接收者以字节为单位向发送者报告它目前能接收的窗口大小。然后发送者就发送这么多字节给接收者。

19.6 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 下面哪一项最准确地描述了TCP/IP?
   A. 用于跨越各种互联网络进行通信的一套协议
   B. 用于将局域网接入广域网的一套协议
   C. 用于跨越多个网络进行数据传输的一套协议
   D. 用于通过互联网共享不同设备的一套协议
2. 下面哪一个属于传输层协议?
   A. UCP
   B. UDP
   C. TDP
   D. TDC
3. 端口号的作用是什么?
   A. 跟踪网络中同时发生的不同会话
   B. 源系统使用端口号来组织会话并选择适当的应用
   C. 终端系统根据终端用户所使用的应用，使用端口号动态地指定特定会话
   D. 源系统产生端口号来预报目的地址
4. 下面哪一项最准确地描述了UDP?
   A. 确认破损或不完整数据报的协议
   B. 检测错误并请求源端重传的协议
   C. 处理数据报并在需要时请求重传的协议
   D. 交换数据报无需确认或传输保证的协议
5. 下列TCP/IP的哪一层包含文件传输、电子邮件、远程登录和网络管理的功能?
   A. 传输层
   B. 应用层
   C. Internet层
   D. 网络层
6. 为什么使用三次握手建立连接?
   A. 确保发生问题后丢失数据可以恢复
   B. 确定工作站一次可接收的数据量
   C. 用户用来有效使用带宽
   D. 将二进制ping响应转换成上层信息
7. TCP滑动窗口的作用?
   A. 使得窗口尺寸变大，一次可以传送更多的数据，从而更有效利用带宽
   B. 窗口尺寸根据每个数据报进行滑动以接收数据，从而更有效利用带宽
   C. 在TCP会话中允许动态协商窗口尺寸，从而更有效利用带宽
   D. 限制进入的数据，使每个数据段必须逐个发送，不是对带宽的有效利用
8. UDP分段使用什么协议提供可靠性?
   A. 网络层协议
   B. 应用层协议
   C. Internet协议
   D. 传输控制协议

9. 下面哪一个最好地描述了窗口尺寸?
   A. 软件支持并能迅速处理的窗口大小的最大值
   B. 等待确认时能传输的消息字节数
   C. 必须提前设置，数据才能被发送的窗口大小
   D. 显示器上打开的窗口大小，不一定和显示器大小一样
10. ARP的功能是什么?
   A. 完成搜索第3层目的地址的任务
   B. 用于生成一个第4层地址资源表的缓存
   C. 用于建立一个IP地址到MAC地址的映射
   D. 用于发送一个广播消息寻找路由器的IP地址



第20章　访问控制列表

目标

学习完本章之后，你应该能够：

- 理解访问控制列表（ACL）的目的
- 描述ACL如何工作
- 决定应该使用什么通配符掩码位
- 描述并使用标准ACL、扩展ACL和命名ACL
- 描述一个简单的防火墙结构

本章将学习使用标准访问控制列表和扩展访问控制列表作为控制网络流量的手段，以及访问控制列表如何作为安全解决方案的一部分。

此外，本章还包括有关如何使用ACL的提示、注意事项、建议和使用指南，以及创建ACL所需的命令和配置操作。最后，还提供了标准ACL和扩展ACL及在路由器接口应用ACL的例子。

请注意应配合本书附带CD-ROM上的e-Lab实验、视频和插图一起观看本章内容，CD-ROM上的素材就是用于支撑本章内容和增强概念的理解。

20.1　ACL概述

网络管理员必须能够拒绝不希望的访问连接，同时又要允许正常的访问。尽管一些安全工具，如密码、回叫信号设备及物理的安全设备很有帮助，但它们经常缺乏基本的流量过滤的灵活性和特定的控制，而这些正是管理员最需要的。例如，网络管理员可能想允许用户访问Internet，但是却不允许外部用户通过Telnet进入到本地局域网。

路由器提供了基本的流量过滤能力，例如通过*访问控制列表（access control lists，ACL）*。ACL是一个连续的允许和拒绝语句的集合，关系到地址或上层协议。

正确配置ACL和明确在网络什么地方放置ACL是非常重要的。ACL在网络中可实现多样功能，一般来说包括：

- 内部过滤分组。
- 保护内部网络受到来自Internet的非法入侵。
- 限制对虚拟终端端口的访问。

ACL是应用在路由器接口的指令列表。这些指令告诉路由器哪些分组可以接收以及哪些分组需要拒绝。接收和拒绝基于一定的条件，例如源地址、目标地址以及TCP/UDP端口号等。

注意：ACL会消耗路由器的CPU资源，因为每一个分组必须交给CPU处理。

ACL通过应用访问控制列表到路由器接口来管理流量和审视特定分组。任何经过该接口的流量都要接受ACL中条件的检测。

ACL适用于所有的路由协议，如IP、IPX等，当分组经过路由器时进行过滤。可在路由器上配置ACL以控制对某一网络或子网的访问。

ACL通过在路由器接口处控制被路由的分组是被转发还是被阻塞来过滤网络流量。路由器基于ACL中指定的条件来决定转发还是丢弃分组。ACL中的条件可以是流量的源地址、流量的目的地址、上层协议、端口号或应用等。

ACL的定义必须基于每个协议。换句话说，如果想在某个接口控制某种协议的数据流，必须对该接口处的每一个协议定义单独的ACL。（注意，有些协议把ACL叫做*过滤器*。）例如，如果路由器接口配置成支持3种协议（IP、AppleTalk及IPX），那么至少需要定义3个ACL。如图20-1所示，通过增加灵活性，为每个协议的ACL创建一个编号范围或方案，ACL将成为网络控制的工具，用于过滤进出路由器接口的分组。本章后面将讲述更多有关ACL号的内容。

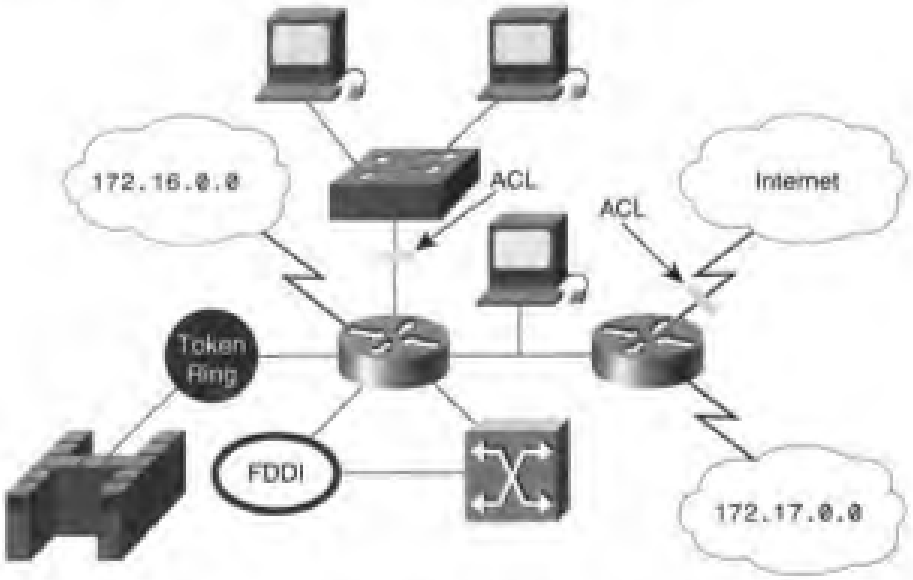


图20-1　ACL例子

20.2　为什么建立ACL

建立ACL的原因很多，ACL可以用来：

- 限制网络流量，提高网络性能。例如，ACL能够基于分组的协议，指定一定分组的级别可被路由器优先处理。*这叫做排队*。排队确保路由器不去处理那些不需要的分组。结果，排队限制了网络流量，减少了网络拥塞。
- 提供流量控制。例如，ACL能够限定或简化路由选择更新的内容。这些限定常用于限定关于特定网络的信息通过网络传播。

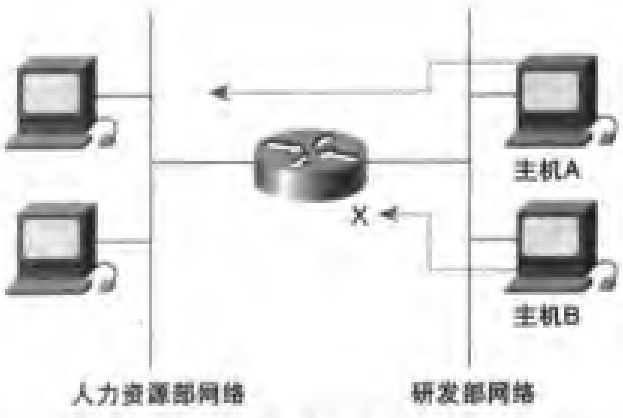


图20-2　限制网络流量

• 提供网络访问的基本安全级别。ACL允许一个主机访问你的网络的一部分，而阻止其他主机访问相同的区域。如图20-2所示，允许主机A访问人力资源部网络，而拒绝主机B访问人力资源部网络。如果不在路由器上配置ACL，那么所有经过路由器的分组都能够到达网络的所有部分。

• 在路由器接口决定哪种流量被转发或被阻塞。例如，可以允许e-mail流量被路由，但同时阻塞所有Telnet流量。

注意：经验法则是每个接口每个方向一个ACL。

20.3 创建ACL：为什么顺序至关重要

当创建一个ACL时顺序是至关重要的。当流量进入或流出应用了ACL的路由器接口时，Cisco IOS软件会将分组跟ACL中定义的规则相比较。比较判断是按照网络管理员在ACL中输入的语句顺序执行的。当比较分组时，一次一句按顺序比较，直到与某一条语句匹配。一旦与某一条语句匹配，就执行匹配的语句行中所指定的动作，不再检查其他条件语句。

例如，如果你创建了一个允许所有通信流量通过的条件语句，那么加在它后面的语句将永远不会被检查。如果需要增加另外的语句或是语句需要改变，你就必须删掉该ACL，然后再重新建立一个带有新语句的ACL。一个好的办法是，使用PC上的文本编辑器创建或修改ACL，然后再通过简易文件传输协议（TFTP）或超级终端的发送文本文件将ACL传到路由器。

注意：当一个ACL被创建后，新的语句行都会被加到ACL的最后。无法删除列表中的单独一行，只能删除整个ACL列表。

20.4 使用ACL

对每个路由器接口，你可以为想要过滤的每一种协议都创建一个ACL。对于某些协议，可以建立一个ACL来过滤流入的流量，同时建立另一个ACL来过滤流出的流量。

在使用了访问组的接口上，当分组跟ACL中的语句相匹配时，分组将被接口拒绝通过或允许通过。Cisco ISO软件ACL检查分组和上层协议报头，如图20-3所示。

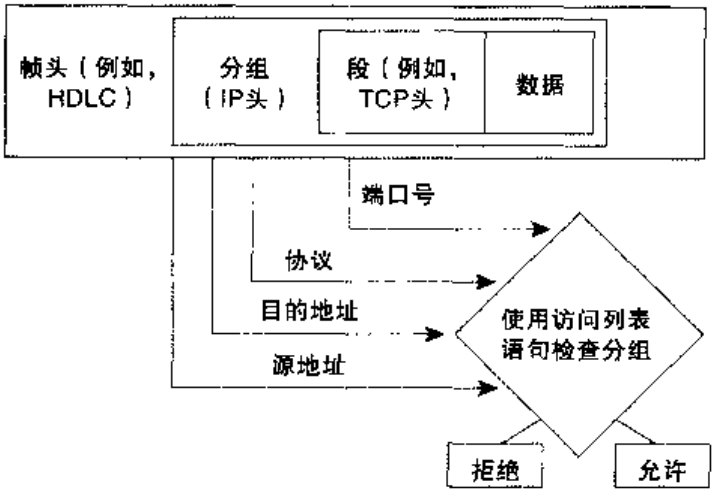


图20-3 检查分组以及上层协议报头

20.5 ACL如何工作

ACL是一组语句，定义了分组的下列行为：

• 进入入站路由器接口。

• 通过路由器转发。

• 流出出站路由器接口。

如图20-4所示，无论是否使用ACL，通信处理过程的开始都是一样的。当一个分组进入某一个接口时，路由器首先检查该分组是否可路由或可桥接。然后路由器检查是否在入站接口上应用了ACL。如果有ACL，就将该分组与列表中的条件语句相比较。如果分组被允许通过，就继续检查路由选择表条目以决定转发到的目的接口。ACL不过滤由路由器本身发出的分组，只过滤别的来源的分组。

下一步，路由器检查目的接口是否应用了ACL。如果没有应用，分组被直接送到目的接口。例如，如果使用E0接口，E0接口没有应用ACL，分组就直接通过E0接口。

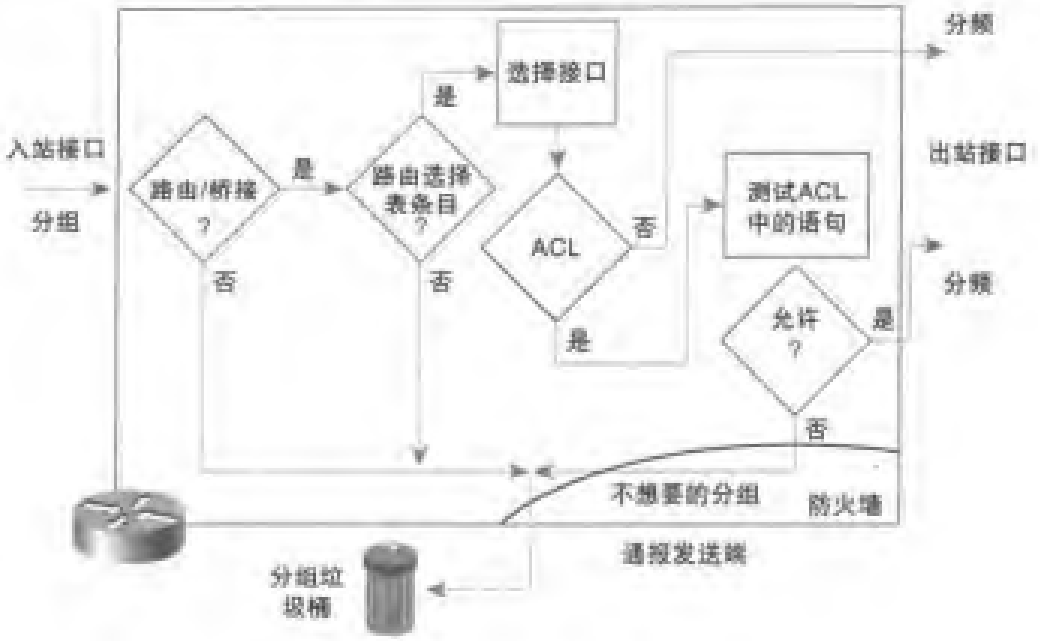


图20-4　ACL如何工作

ACL语句按照逻辑次序顺序执行。如果与某个条件语句相匹配，分组就被允许通过或被拒绝通过，而不再检查剩下的条件语句。如果所有的条件语句都没有被匹配，则最后将强加一条拒绝全部流量的暗含语句。即使这条拒绝全部流量的语句在ACL中最后一行是看不到的，缺省的情况下在最后也是拒绝所有的流量。如图20-5，如果分组跟第一条语句相匹配，被拒绝通过到目的地，分组则被丢弃扔进*比特垃圾桶*。它不会再跟ACL中其余的任何语句进行比较。如果分组与第一条语句没有匹配，将继续与下一条语句进行比较。

ACL能够控制哪些客户端可以访问你的网络。ACL文件中的条件语句能实现：

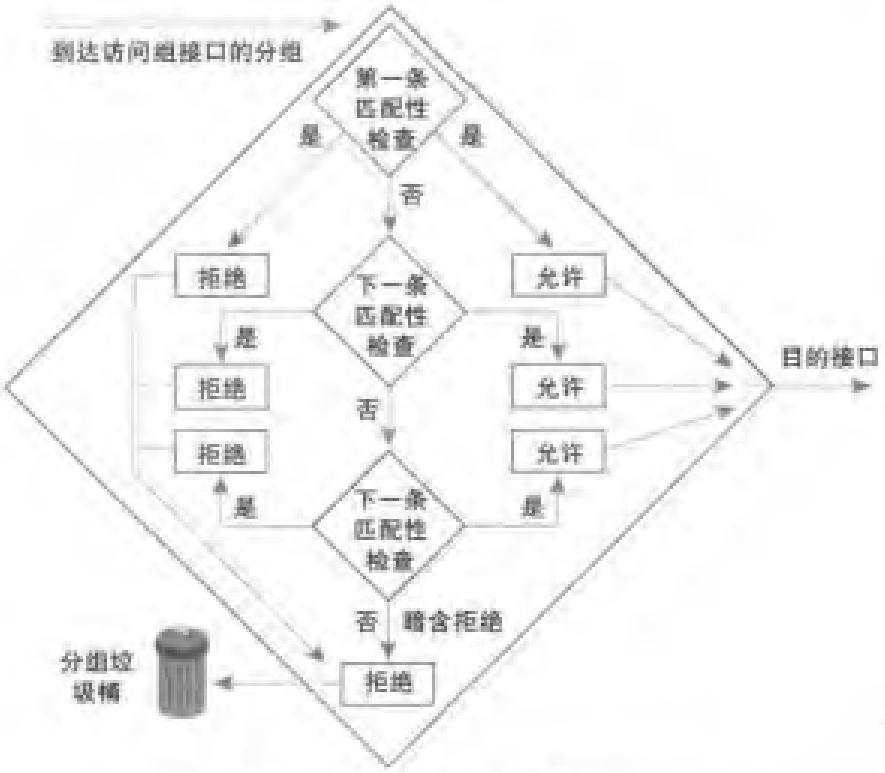


图20-5　ACL匹配性检查和暗含deny any

• 筛选出某些主机，允许或者拒绝它们访问你的网络的某一部分。

• 允许或拒绝用户访问某种类型的应用，例如FTP或HTTP。

20.6 ACL配置任务

实际上，访问控制列表命令可能是冗长的字符串。本节将要讲述的有关创建ACL的主要任务包括下列内容：

• 使用通常的全局配置模式来创建ACL。

• 指定一个范围在1到99之间的ACL号，为IP定义一个标准ACL，并指示路由器接受标准的ACL语句。

• 指定一个范围在100到199之间的ACL号，为IP定义一个扩展ACL，并指示路由器接受扩展的ACL语句。

• 网络管理员必须小心地选择ACL语句，并且要特别注意它们之间的逻辑顺序，以便能实现预期的控制。必须明确地指出所允许的IP协议，而所有其他TCP/IP协议都将被禁止。

• 选择所要检查的IP协议，任何其他的IP协议都不被检查。在这个过程的后期，网络管理员可以为更高的精确度而指定一个可选的目的端口。

• 应用ACL到接口。

尽管每个协议要求有自己的一套特定任务和规则来提供流量过滤，一般来说，大部分协议需要两个基本步骤：

步骤一：创建ACL定义。

步骤二：把ACL应用于某一个接口。

ACL应用到一个或多个接口上，根据配置和如何被应用来过滤入站或出站的流量。出站ACL通常比入站ACL更高效，因此优先选用出站ACL。带有入站ACL的路由器在把分组交换到出站接口前必须检查每个分组是否跟ACL条件判断语句相匹配。

20.7 为每个ACL分配惟一的编号

在路由器上配置ACL的时候，必须为每一协议的ACL分配一个惟一的编号，以便标识每个ACL。如果使用数字来标识ACL，必须保证这个数字在协议所允许的合理范围之内。例20-1定义了ACL1和2并且把这些ACL应用于接口Ethernet 0上：

例20-1 应用ACL到某个接口

```
access-list 1 permit 5.6.0.0.0.0.255.255
access-list 1 deny 7.9.0.0.0.0.255.255
!
access-list 2 permit 1.2.3.4
access-list 2 deny 1.2.0.0.0.0.255.255
!
interface ethernet 0
ip address 1.1.1.1 255.0.0.0
!
ip access-group 1 in
ip access-group 2 out
```

表20-1列出了有效的协议ACL号。

表20-1　协议、ACL及相应的编号

协议	范围
IP	1到99
Extended IP	100到199
AppleTalk	600到699
IPX	800到899
Extended IPX	900到999
IPX Service Advertising Protocol	1000到1099

20.8　使用通配符掩码位

*通配符掩码*是一个32比特的数字字符串，它被用点号分成4个8位组，每个8位组包含8个比特。在通配符掩码位中，0表示“检查相应的位”，而1表示“不检查（忽略）相应的位”。如图20-6所示。

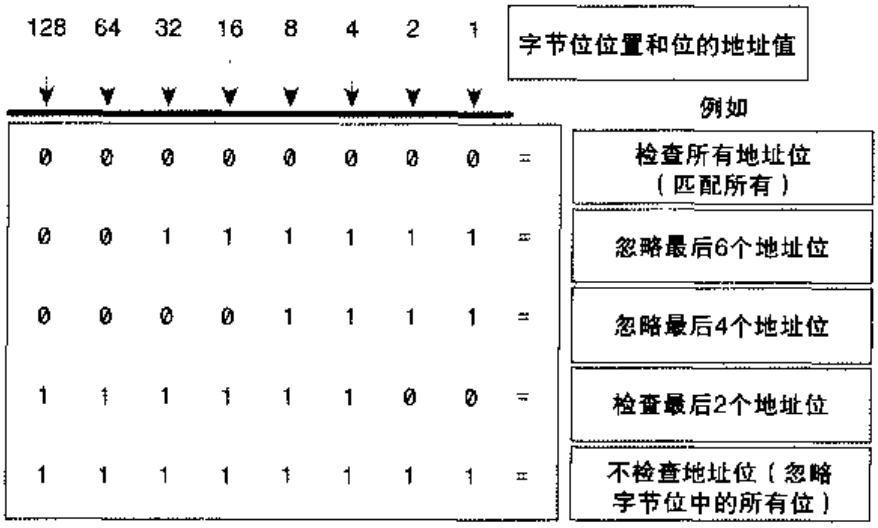


图20-6　通配符掩码位的匹配

通配符掩码跟IP地址是成对出现的。在通配符掩码的地址位使用1或0表明如何处理相应的IP地址位。

ACL使用通配符掩码来标志一个或几个地址是被允许，还是被拒绝。术语“*通配符掩码*”是“ACL掩码位匹配过程”的缩写，它是从纸牌游戏中引申过来的一个比喻。

尽管都是32比特的数字字符串，ACL通配符掩码跟IP子网掩码的工作原理是不同的。在IP子网掩码中数字1和0用来决定是网络、子网还是相应的主机IP地址。正如刚才所讲的，在ACL通配符掩码中，掩码位是1还是0，用来决定相应的IP地址被忽略，还是被检查。

我们已经知道，在ACL的通配符掩码位上的0或1导致ACL检查或者忽略IP地址中的相应位。图20-7说明了通配符掩码的应用过程。

现在想通过测试一个子网的IP地址来决定该子网是被允许还是被拒绝。假设这个IP地址是一个B类地址（前面两个字节表示网络号），它还包括一个8位的子网号（第3个字节表示子网号）。

你想通过使用ACL的通配符掩码来匹配从172.30.16.到172.30.31.0的子网，以便允许它们通过。图20-7给出了示例说明。

首先，为了测试IP地址的前两个8位组（172.30），通配符掩码需要在相应的通配符掩码位上置0。

另外，由于没有必要检测每个独立的主机地址（有效的主机ID的地址最后不可能是.0），所以通配符掩码把相应位置为1，以便忽略对最后一个字节的测试。

在第3个8位组，通配符掩码是15（00001111），而相应的子网网络地址部分是16（00010000）。

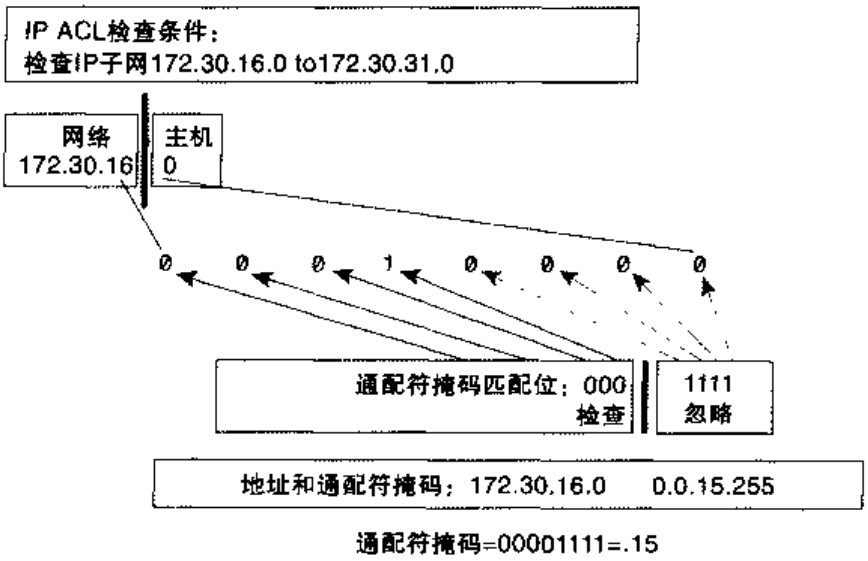


图20-7 通配符掩码举例

这里通配符掩码的前4位为0，表示要检查IP地址的第3个8位组的前4位（0001）；因为后4位被忽略，可以匹配从16（00010000）到31（00011111）的所有子网，因为它们IP地址的第3个8位组都以0001开头的。

通配符掩码的后4位为1，表示忽略IP地址第3个8位组的后4位，这样IP地址相应位的值可以为二进制的0或者1，而相应的通配符掩码位为1。在这个例子中，通配符掩码告诉路由器去匹配IP地址的前4位，而剩余的4位被完全忽略。因此，172.30.16.0及其通配符掩码0.0.15.255匹配从172.30.16.0到172.30.31.0的所有子网，而拒绝其他的一切子网。

20.8.1 使用通配符any

使用二进制通配符掩码位的十进制表示方法是一件单调乏味的事。最普遍的通配符掩码使用方式是使用缩写字。当网络管理员配置测试条件时，可用缩写字来代替冗长的通配符掩码字符串，这些缩写大大地减少了输入量。假设你想要在一个ACL测试中允许访问任何目的地址。为了指出是任何IP地址，你将要输入0.0.0.0，如图20-8所示。然后，还要指出ACL将要忽略（允许不测试）任何值，相应的通配符掩码位是全1（也就是255.255.255.255）。

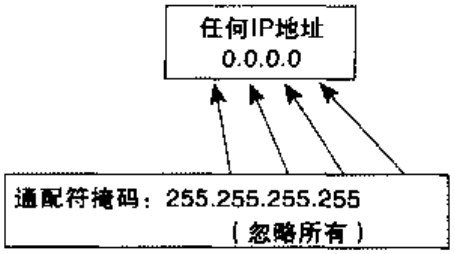


图20-8 通配符any

你可以使用缩写字any把上述的测试条件表达给Cisco IOS软件的访问控制列表软件。这样就不需要输入0.0.0.0和255.255.255.255，而只要使用通配符any本身就行了。

例如，要替代下面的用法：

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

可以这样使用：

```
Router(config)#access-list 1 permit any
```

20.8.2 使用通配符host

Cisco IOS软件所允许的第二种普遍的情况是：当想要与整个IP主机地址的所有位相匹配时，Cisco IOS软件允许在访问控制列表的通配符掩码中使用缩写词。假设想要在ACL的测试中允许一个

特定的主机地址。为了表示这个主机IP地址，要输入全部的地址（例如172.30.16.29，如图20-9所示）。然后指出这个ACL将要测试这个地址的所有位，相应的通配符掩码位全为零（也就是0.0.0.0）。



图20-9　通配符host

可以在Cisco IOS软件的访问控制列表中使用缩写词host来表达上面所说的这种测试条件。在这个例子中，可以不用输入172.30.16.29和0.0.0.0，而只需在地址前面添加通配符host。

例如，要替代下面的用法：

```
Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0
```

可以这样使用：

```
Router(config)#access-list 1 permit host 172.30.16.29
```

20.9　标准访问控制列表

标准ACL检查可以被路由的IP分组的源地址并且把它与ACL中的条件判断语句相比较，如图20-10所示。

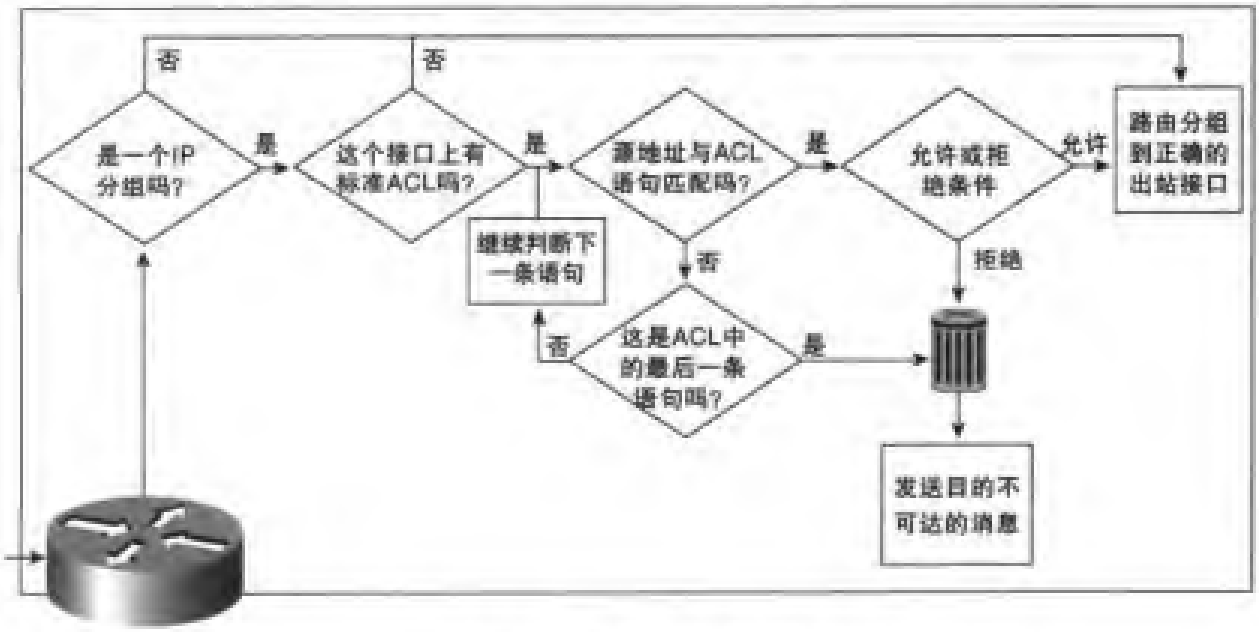


图20-10　标准ACL工作过程

标准ACL可以基于网络、子网或主机IP地址允许或拒绝整个协议组（如IP）。例如，从接口E0或Fa0/0处进来的分组经过检查其源地址和协议类型，并且与ACL条件判断语句相比较，如果匹配，则执行允许或拒绝。如果该分组被允许通过，就从路由器的出口转发出去；如果该分组没有被允许，就简单地丢弃它。

下面列出标准ACL命令的详细语法：

```
Router(config)# access-list access-list-number {deny | permit} source
[source-wildcard] [log]
```

可以通过在access-list命令前加no的形式，来消除一个已经建立的标准ACL，使用语法格式如下：

```
Router(config)#no access-list access-list-number
```

表20-2列出了语法中参数的描述。

表20-2 标准ACL参数

参数	描述
access-list-number	访问列表编号。是一个从1到99或从1300到1999的十进制数字
deny	在匹配条件语句时，拒绝分组通过
permit	在匹配条件语句时，允许分组通过
source	发送分组的源地址，可以是网络地址或是主机地址。有两种方式用来指定源地址： • 采用32比特数字，用点十进制分为四部分的表示方式。 • 使用关键字any作为0.0.0.0 255.255.255.255的源地址和源地址通配符的缩写字
source-wildcard	（可选项）通配符掩码位用来跟源地址一起使用。有两种方式来指定源地址的通配符掩码： 采用32比特数字，用点分十进制分为四部分的表示方式。通配符掩码1的位置对应源地址的位不进行匹配性检查。 使用关键字any作为0.0.0.0 255.255.255.255的源地址和源地址通配符的缩写字
log	（可选项）生成有关分组匹配情况的日志消息，发送到控制台（送到控制台日志消息的等级由logging console命令来控制）。 日志消息包括访问列表的编号，分组是被允许还是被拒绝，源地址和包的数量。日志消息在第一个分组匹配时生成，然后每隔5分钟生成一次，记录每5分钟之内被拒绝或被允许的分组的有关消息。 使用ip access-list log-update命令可以配置当匹配数目到达阈值时就生成日志消息（从而替代等待5分钟间隔）。要了解关于ip access-list log-update命令的更多信息，可以访问Cisco网站查找下列资源：www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cger/cbkixol.htm。 如果记录日志的设备有太多消息而处理不过来或者每秒钟超过一条日志消息要处理时，设备就可能会丢掉一些日志消息分组。这种做法防止路由器因为处理太多记日志消息分组而崩溃。因此，记录日志的设备不能用于计费工具或用于精确计算访问列表匹配的数目的来源

使用标准版本的全局配置命令access-list来定义一个标准的ACL，并给它分配一个数字编号，其编号范围从1到99。例20-2显示了ACL2的四个条件判断语句，尽管它们的组合不像图解那样清楚地阐述几种不同的语句如何工作。如果分组不能与任何一个条件判断语句相匹配，则在ACL的末尾隐含对所有访问的拒绝。

例20-2 标准ACL语句

```
access-list 2 deny 172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny 172.16.1.1 0.0.255.255
access-list 2 permit 172.16.1.1 0.255.255.255
```

注意到在ACL的第1条判断语句中没有通配符掩码。像这种情况，缺省掩码0.0.0.0就被使用，这个语句拒绝了IP地址为172.16.1.1的访问。

ACL的第2条判断语句允许特定主机172.16.1.0或从172.16.1.0子网来的任何主机的访问。

第3条判断语句拒绝了172.16.0.0网络的任何主机的访问，而第4条语句则允许来自172网段的任何主机的访问。

ip access-group命令把某个现有的ACL与某个接口联系起来。配置时必须先进入到目的接口（例如，s0/0）的接口配置模式下。命令格式如下：

```
Router(config if)# ip access-group access-list number {in | out}
```



实验活动 标准访问控制列表

在这个实验中，将规划、配置、应用一个标准的ACL来允许或者禁止特定的通信流量，

然后测试这个ACL是否达到预期结果。

20.10　扩展访问控制列表

*扩展ACL*比标准ACL使用得更多，因为它提供了更大的弹性和控制范围。扩展ACL既可检查分组的源地址和目的地址，也检查协议类型和TCP或UDP的端口号。图20-11举例说明了路由器根据扩展ACL来检查分组的过程。

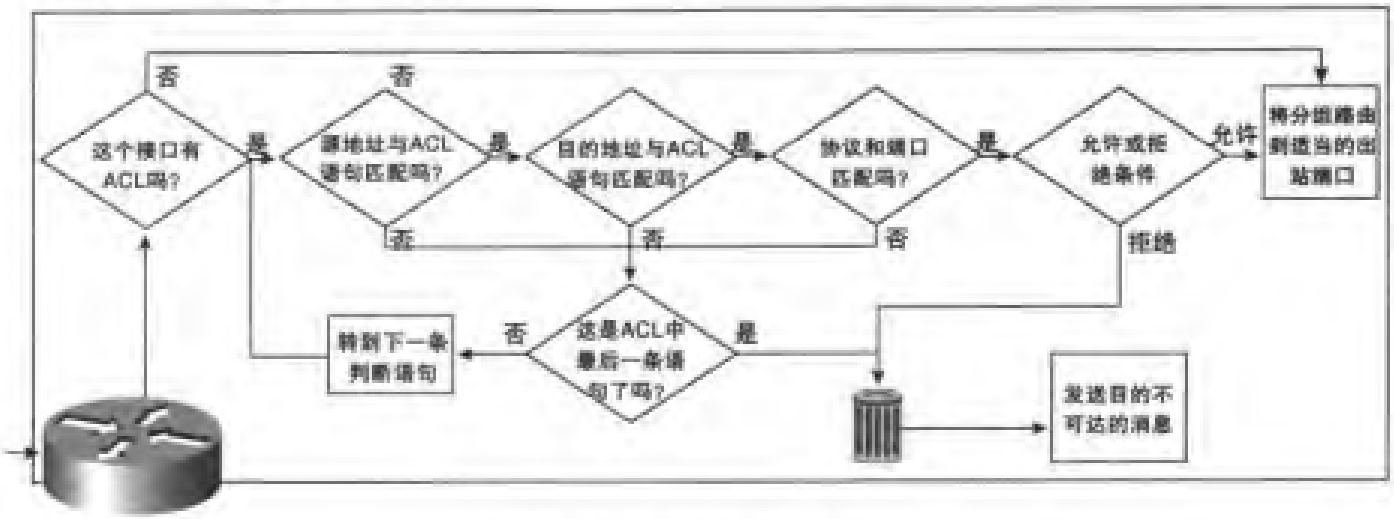


图20-11　扩展ACL工作过程

扩展ACL可以基于分组的源地址、目的地址、协议类型、端口地址和应用来决定访问是被允许或者被拒绝。扩展ACL可以在拒绝文件传输和网页浏览的同时，允许从Fa0/0的e-mail通信流量抵达目的地S0/0。一旦分组被丢弃，某些协议将返回一个回应分组到源发送端，以表明目的不可达。

扩展ACL比标准ACL提供了更广阔的控制范围和更多的分组处理方法。标准ACL只能禁止或拒绝整个协议集，但扩展ACL可以允许或拒绝协议集中的某些协议。例如，允许HTTP而拒绝FTP。

以下是扩展ACL命令的完整语法：

```
Router(config)# access-list access-list-number [dynamic dynamic-name [timeout
minutes]] {deny | permit} protocol source source-wildcard destination destination-
wildcard [precedence precedence] [tos tos] [log | log-input] | time-range time-
range-name] [fragments]
```

这个命令的no形式用来删除标准ACL。以下是该命令的no形式的语法：

```
Router(config)# no access-list access-list-number
```

扩展ACL语句的语法很长而且限制在终端窗口中。该命令有关参数的详细说明见表20-3。

表20-3　扩展ACL参数

参数	描述
access-list-number	访问控制列表编号。使用一个100到199或2000到2699之间的数字来标识一个访问控制列表
dynamic *dynamic-name*	（可选项）把ACL定义为动态的ACL。查阅*cisco IOS Security Configuration Guid*一书中"Configuring Lock-and-Key Security（Dynamic Access Lists）"章节中的锁和密钥访问的内容
timeout *minutes*	（可选项）指定时间的绝对长度，准确到分钟的一个临时访问列表入口可以保持在动态访问列表中的时间。默认的是一个无穷大的时间，并允许一个入口保持不变。

续表

参数	描述
deny	如果条件符合就拒绝访问
permit	如果条件符合就允许访问
protocol	Internet协议的名称或号码。它可能是以下关键字中的一个eigrp, gre, icmp, igmp, igrp, ip,ipinip, nos, ospf, pim, tcp或udp。 或者是一个0到255之间的整数，用来代表IP协议。可以通过使用ip这个关键字来匹配所有的Internet协议（包括icmp, tcp和udp）。部分协议允许更多的控制
source	发送分组的网络号或主机。有三种方法来定义分组的源地址： 使用十进制的32比特数字表示，每8位为一组，中间用点号“.”隔开。 使用关键字any作为一个源地址和源地址通配符（如0.0.0.0 255.255.255.255）的缩写字。 使用关键字host作为源通配符掩码0.0.0.0的缩写字
source-wildcard	应用于源地址的通配符位。通配符位0表示源地址中相应的位的位置。通配符位设为1表示分组的IP地址的相应的位置中的0和1都被认为与这个访问列表入口匹配。 有三种方法来指定源通配符： 使用十进制的32比特数字表示，每8位为一组，中间用点号“.”隔开。如果某位为1，表明某位不需要检查。 使用关键字any作为一个源地址和源地址通配符（如0.0.0.0 255.255.255.255）的缩写字。 使用关键字host作为源通配符掩码0.0.0.0的缩写字。 在源地址通配符中不必把连续的位都设成1。例如，源通配符0.255.0.64是有效的
destination	分组的目的网络号或主机。 有三种方法来定义分组的目的地址： 使用十进制的32比特数字表示，每8位为一组，中间用点号“.”隔开。 使用关键字any作为一个目的地址和目的地址通配符（如0.0.0.0 255.255.255.255）的缩写字。 使用关键字host作为目的通配符掩码0.0.0.0的缩写字
destination-wildcard	应用于目的地的通配符位。有三种方法来指定目的地： 使用十进制的32比特数字表示，每8位为一组，中间用点号“.”隔开。 使用any关键字作为代表目的地址和目的通配符掩码0.0.0.0 255.255.255.255的缩写字。 使用关键字host作为目的通配符掩码0.0.0.0的缩写字
precedence *precedence*	（可选项）分组可基于优先级（一个0到7的数字）来过滤。这可用于QoS（服务质量）机制
tos *tos*	（可选项）分组可基于服务类型的级别（一个0到15的数字）来过滤。这可用于QoS（服务质量）机制
log	（可选项）生成关于匹配入口的分组的日志消息，以发送到控制台（发送到控制台的日志消息的级别由命令logging console控制），日志消息包括访问控制列表的编号， 分组是被拒绝还是被允许；协议类型，是TCP、UDP还是ICMP，或协议号；如果合适，还包括源地址和目的地址，以及源端口和目的端口。 一旦有分组跟测试条件匹配，就产生日志消息。缺省地，log功能每隔5分钟就产生一条日志消息，其中包括在这5分钟内被允许或被拒绝的分组个数。 当被允许或拒绝分组个数到达可配置的上限时可使用命令ip access-list log-update去生成日志消息（而不是等待5分钟间隔）。 可通过命令ip access-list logupdate command了解更多的信息。 如果需要处理的日志消息太多或者同一时间有超过一个需要处理的日志消息的话，日志消息工具将有可能丢弃部分日志消息分组。这个操作可以避免路由器由于要处理过多的日志消息分组而崩溃。因此，日志消息不能作为付账的工具或用来作为匹配访问控制列表的编号的确切源地址

续表

参数	描述
log-input	（可选项）日志的输出消息包括输入接口和源MAC地址或者虚拟信道
time-range time-range-name	（可选项）应用于该语句的时间范围的名称。时间范围的名称及其要求由time-range命令指定
icmp-type	（可选项）基于ICMP消息类型来过滤ICMP分组。该类型为0到255的一个数字
icmp-code	（可选项）基于ICMP消息代码来过滤ICMP分组。该代码为0到255的一个数字
icmp-message	（可选项）基于ICMP消息的类型名或者ICMP消息类型和代码名称来过滤ICMP分组
igmp-type	（可选项）基于IGMP消息类型或者消息名称来过滤ICMP分组，消息类型是一个从0到15的数字
operator	（可选项）比较源和目的端口，可用的操作符包括lt（小于），gt（大于），eq（等于），neq（不等于）和range（包括的范围） 如果操作符位于源地址和源地址通配符之后，那么它必须匹配源端口。 如果操作符位于目的地址和目的地址通配符之后，那么它必须匹配目的端口。 range操作符需要两个端口号，其他操作符只需要一个端口号
port	（可选项）指明TCP或UDP端口的十进制数字或名字。端口号可以从0到65535。TCP端口号只被用于过滤TCP分组。UDP端口号只被用于过滤UDP分组
established	（可选项）只针对TCP协议，指一个已经建立的连接。如果TCP数据报中的ACK、FIN、PSH、RST、SYN或者URG等控制位被设置，则匹配。如果是要求建立连接的初始数据报，则不匹配
fragments	（可选项）该ACL入口应用于分组的非初始部分。这个段将被允许或拒绝

对于单独的一个ACL，可以定义多个条件判断语句，每个条件判断语句都包含相同ACL编号，以便把这些语句与同一个ACL相关联，如例20-2所示。另外ACL中条件判断的语句是无限的，其数量的大小只受内存的限制。当然，条件判断语句越多，该ACL的执行和管理就越困难。例20-3的ACL共包含3条判断语句，它们允许位于172.16.6.0网段的机器通过使用telnet、ftp和ftp-data访问其他任意网段。

例20-3　扩展ACL语句

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

扩展ACL功能非常强大，对于所使用的不同协议提供了不同的参数选项，根据所使用的协议，语法也会不同。下面是可以使用的协议：

- Internet控制消息协议（ICMP）。
- Internet组管理协议（IGMP）。
- 传输控制协议（TCP）。
- 用户数据报协议（UDP）。

下面几小节描述基于所使用的协议而不同的扩展ACL语法。

20.10.1　为ICMP配置扩展ACL

对ICMP的ACL语法格式如下：

```
access-list access-list-number [dynamic dynamic name [timeout minutes]] {deny |
permit} icmp source source-wildcard destination destination-wildcard [ icmp-type
[icmp-code] | icmp-message] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name] [fragments]
```

20.10.2 为IGMP配置扩展ACL

对IGMP的ACL语法格式如下：

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny |
permit} igmp source source-wildcard destination destination-wildcard [igmp-type]
[precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]
[fragments]
```

20.10.3 为TCP配置扩展ACL

对TCP的ACL语法格式如下：

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny |
permit} tcp source source-wildcard [operator [port]] destination destination-
wildcard [operator [port]] [established] [precedence precedence] [tos tos] [log |
log-input] [time-range time-range-name] [fragments]
```

20.10.4 为UDP配置扩展ACL

对UDP的ACL语法格式如下：

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny |
permit} udp source source-wildcard [operator [port]] destination destination-
wildcard [operator [port]] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name] [fragments]
```

20.10.5 默认状态下的扩展ACL

一个扩展ACL默认状态下是拒绝所有通信的列表，在列表的最后暗含一条拒绝所有流量的语句。

扩展ACL的判断语句末尾，有一个字段指定可选的TCP和UDP端口号，从而增加了精确性。

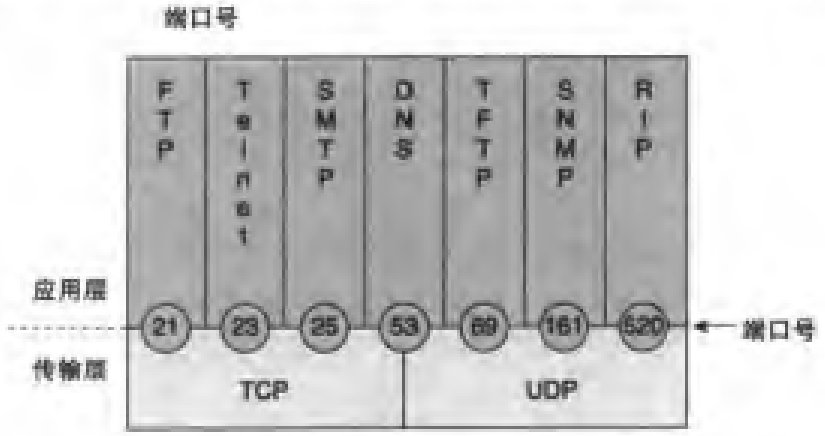


图20-12 传输层/应用层端口号

表20-4列出了更多常用的保留UDP和TCP端口号。

命令ip-access group将现有的扩展ACL链接到一个接口。如图20-13所示，针对某种协议，每个接口的一个方向只允许放置一个ACL，命令的格式如下：

表20-4　一些保留的TCP/UDP端口号

端口号	关键字	描述
0		保留
1到4		未指定
5	RJE	远程作业登录
7	ECHO	回显
9	DISCARD	丢弃
11	USERS	在线用户
13	DAYTIME	时间
15	NETSTAT	谁在线，网络状态
17	QUOTE	每日引用
19	CHARGEN	字符发生器
20	FTP-DATA	文件传输协议（数据）
21	FTP	文件传输协议（控制）
23	TELNET	终端连接
25	SMTP	简单邮件传输协议
53	DOMAIN	域名服务器（DNS）
69	TFTP	简易文件传输协议
80	HTTP	超文本传输协议（www）

```
Router(config-if)# ip access-group access-list number {in | out}
```

20.11　命名访问控制列表



对于每种协议，在一个端口的一个方向上只能设置一个列表

图20-13　ACL规则

Cisco IOS软件11.2版本中引入了IP命名ACL，命名ACL允许在标准ACL和扩展ACL中，使用名字代替数字来表示ACL编号。使用命名ACL有以下的好处：

- 通过一个字母数字串组成的名字来直观地表示特定的ACL。
- 不受99条标准ACL和100条扩展ACL的限制。
- 使得网络管理员可以方便地对ACL进行修改而无需删除ACL之后再对其进行重新配置。

使用ip access-list命令可创建命名ACL，语法格式如下：

```
ip access-list {extended | standard} name
```

这将用户置于ACL配置模式下。在ACL配置模式下，通过指定一个或多个允许及拒绝条件，来决定一个分组是允许通过还是被丢弃。语法格式如下：

```
Router(config-ext-nacl)#permit | deny protocol source source-wildcard [ operator
[port]] destination destination-wildcard [operator [port]] [established]
[precedence precedence] [tos tos] [log] [time-range time-range-name]
```

ACL配置命令中，permit或deny操作符用于通知路由器当一个分组满足某一ACL语句时应执行转发操作还是丢弃操作。

例20-4演示应用一个命名ACL。

例20-4　命名ACL语句

```
! Named ACL created:
Rt(config)# ip access-list extended server-access
Rt(config-ext-nacl)# permit tcp any host 131.108.101.99 eq smtp
Rt(config-ext-nacl)# permit tcp any host 131.108.101.99 eq domain
Rt(config-ext-nacl)# deny ip any any log
```

```
Rt(config-ext-nacl)# ^Z
! Named ACL Applied:
Rt(config)# interface fastethernet0/0
Rt(config-if)# ip access-group server-access out
Rt(config-if)# ^Z
```

在例20-4中，一个被命名为server-access的ACL被应用到接口FE0/0，该ACL只允许用户访问e-mail和DNS服务器，而其他请求将被拒绝。

如例20-5所示，命名ACL允许删除任意指定的语句，但新增的语句只能被放到ACL的结尾处。

例20-5 命名ACL语句

```
router# configure terminal
  Enter configuration commands, one per line.
  router(config)# ip access-list extended test
  router(config-ext-nacl)# permip ip host 2.2.2.2 host 3.3.3.3
  router(config-ext-nacl)# permist tcp host 1.1.1.1 host 5.5.5.5 eq www
  router(config-ext-nacl)# permit icmp any any
  router(config-ext-nacl)# permit udp host 6.6.6.6 10.10.10.0 0.0.0255 eq domain
  router(config-ext-nacl)# ^Z
  1d00h:%SYS-5-CONFIG-1:Configured from console by consoles-1
  router# show access-list
  Extended IP access list test
      permit ip host 2.2.2.2 host 3.3.3.3
      permit tcp host 1.1.1.1 host 5.5.5.5 eq www
      permit icmp any any
      permt udp host 6.6.6.6 10.10.0 0.0.0.255 eq domain

  router# configure terminal
  Enter configuration commands, one per line. End with CNTL'Z.
  router(config)# ip access-list extended test
  !--The following command deleles anared ACI entry.
  router(config-ext-nacl)# no permit icmp any any
  !--The following command adds a named ACL entry.
  router(config-ext nacl)# permit gre host 4.4.4.4 host 8.8.8.8
  router(config-ext nacl)# ^Z
  1d00h: %SYS 5-CONFIG I: Configured from console by consoles 1

  router# show access-list
  Extended IP access list test
      permit ip host 2.2.2.2 host 3.3.3.3
      permit tcp host 1.1.1.1 host 5.5.5.5 eq www
      permit udp host 6.6.6.6 10.10..0.0 0.0.255 eq domain
      permit gre host 4.4.4.4 host 8.8.8.8
```

在实现命名ACL之前，需要考虑：

• 11.2之前版本的Cisco IOS软件不支持命名ACL。

• 不能够以同一个名字命名多个ACL，例如，同时将一个标准ACL和一个扩展ACL都命名为George是不允许的。

例20-6中的命令首先创建一个名字为Internetfilter的标准ACL和一个名字为marketing_group的扩展ACL。这些命令然后访问接口e0/5，分配一个IP地址，并将这两个ACL都应用到接口Ethernet 0/5。

例20-6 命名ACL的创建

```
. . .
ip access-list standard Internetfilter
permit 1.2.3.4
deny any
ip access-list extended marketing-group
permit tcp any 171.69.0.0 0.255.255.255 eq telnet
deny tcp any any
deny udp any 171.69.0.0.0.255.255.255 lt 1024
deny ip any log
ip interface Ethernet0/5
ip address 2.0.5.1 255.255.255.0
ip access-group Internetfilter out
ip access-group marketing-group in
```



实验活动 命名ACL

在这个实验中，可以创建一个命名ACL以允许或者拒绝指定的通信流量，并且测试这个ACL是否达到期望的效果。

20.12 放置ACL

在一个网络中，ACL是通过过滤分组和拒绝那些不需要的通信流量来实现流量控制的。放置ACL需要考虑的一个重要条件是应该在什么地方放置访问控制列表。当ACL被放置在正确的地方时，它不仅可以过滤通信流量，而且可以使整个网络更有效地运作。为了过滤通信流量，ACL应该放置在对网络增长影响最大的地方。

参考图20-14，假设企业的策略要求是：把从路由器A通过以太网LAN访问路由器D的Fa0/0的telnet或者FTP流量都拒绝，与此同时，其他的通信流量都是允许通过的。这个策略可以用多种方法实现。我们推荐最好的方法是使用一个扩展ACL，指定源地址和目的地址。假如这个扩展ACL被放置在路由器A上，被拒绝的分组就不能通过路由器A的以太网口或者路由器B或者路由器C的串行口了，那样也就无法到达路由器D了。这样就减少了路由器A和路由器D链路上的通信流量。其他源地址和目的地址的流量仍然被允许通过。

放置ACL的一般原则是，尽可能把扩展ACL放置在距离要被拒绝的通信流量近的地方。标准ACL由于不能指定目的地址，所以它们应该尽可能放置在距离目的地最近的地方。例如，标准ACL应该放置在路由器D的Fa0/0上，以阻止来自路由器A的通信流量。

注意：ACL的应用会降低路由器的路由性能。路由器在转发分组时不得不读取更多的分组和比较更多的参数。

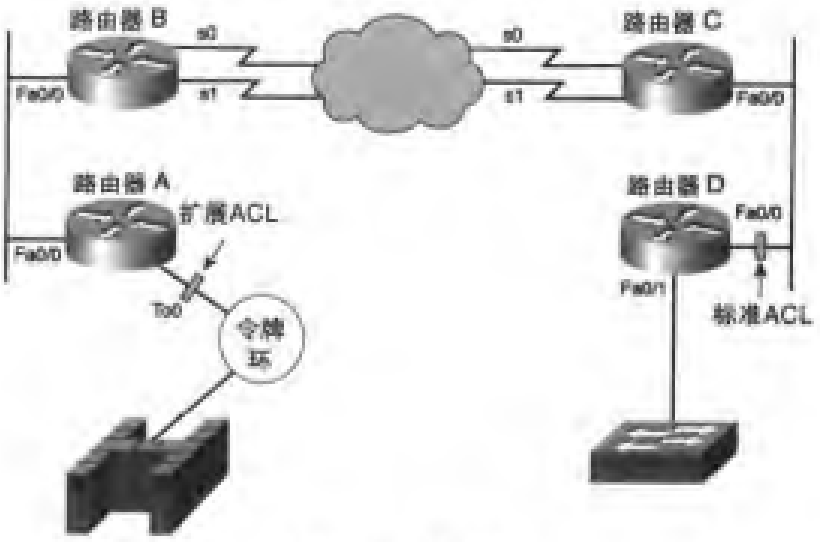


图20-14 放置ACL

在高级的配置中，有一种叫Turbo ACL的特性用于编译ACL，可以加快这一进程。Turbo ACL使用一种更有效的查找算法，它使用一种更高效的方式解析列表。

实验活动 扩展ACL

在这个实验中，必须计划、配置和应用一个扩展ACL实现允许或拒绝指定的通信流量。测试ACL是否达到期望的效果。

20.13 防火墙

*防火墙*是存在于用户和外部世界之间，用于保护内部网络免受外部入侵者攻击的一种计算机或者网络设备。在大多数情况下，入侵者来自与全球性的互联网以及与其相连接的成千上万的远程网络。典型的情况下，一个网络防火墙由几个不同计算机组成，以防止不希望和不合法的访问。如图20-15显示了一个简单的防火墙结构。

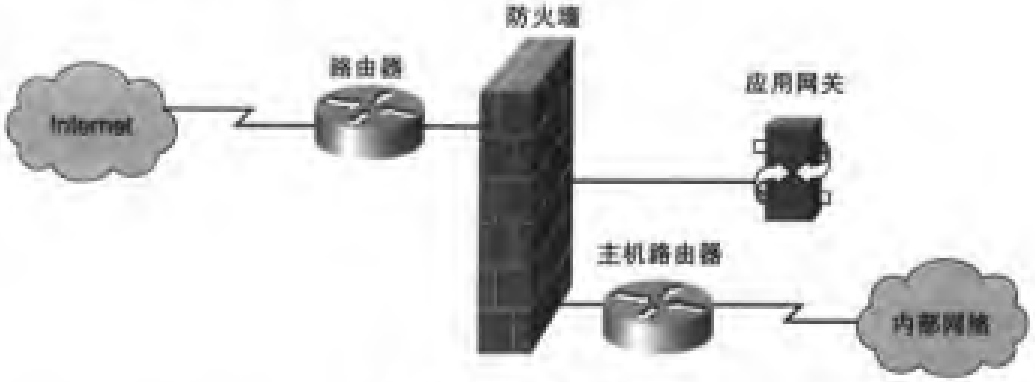


图20-15 防火墙结构

在防火墙结构中，连接互联网的路由器（*外部路由器*）强迫所有流入的通信流量经过应用网关。而连接内部网络的路由器（*内部路由器*）仅仅接受来自应用网关的分组。实际上，网关控制着那些流入和流出内部网络的网络服务的传递。例如防火墙只允许指定的用户连接到互联网，或者只允许特定的应用程序能够在内部主机和外部主机之间建立通信。如果被允许的服务是email，那么只有email的分组被允许通过路由器。这样不但保护了应用网关，也避免了未经认可的分组太多而造成负荷过载。

20.13.1　带防火墙的ACL

ACL应该用在位于内部网络和外部网络（例如互联网）之间的防火墙路由器上。防火墙路由器提供一个孤立的节点，使内部网络的结构不受影响。也可以在两个网络之间的路由器中使用ACL，用于控制指定的内部网络通信流量的出入。

由于ACL提供安全性方面的用途，所以我们应该马上在*边界路由器*上配置ACL。边界路由器是指被放置在网络边界的路由器，通常称为*防火墙路由器*。这样可以提供基本的安全性能，控制外部网络或者缺乏控制的网络区域的流量进入专用的网络区域。

在边界路由器中，可以针对路由器接口上配置的每种网络协议来创建ACL。可以在每个接口上配置ACL，过滤流入方向、流出方向或者两个方向的通信流量。

20.14　限制虚拟终端访问

标准ACL和扩展ACL的应用可以使分组通过路由器。它们不是设计用于把分组阻塞在路由器中的。在默认的情况下，一个允许出站Telnet通信流量的扩展ACL不会阻止路由器发出的Telnet会话。

此外，路由器上的物理端口或接口，例如Fa0/0和S0/0，都是虚拟端口。这些虚拟端口被称为虚拟终端连接（vty line）。路由器上一共有5个虚拟终端连接，它们的编号从0到4，如图20-16所示。出于安全方面的考虑，用户可以被允许或者拒绝通过虚拟终端访问路由器，也可以拒绝从路由器上访问某个目的地址。例如，管理员可以配置ACL，允许通过终端访问路由器以达到管理或者处理故障的目的，与此同时限制路由器以外的访问。

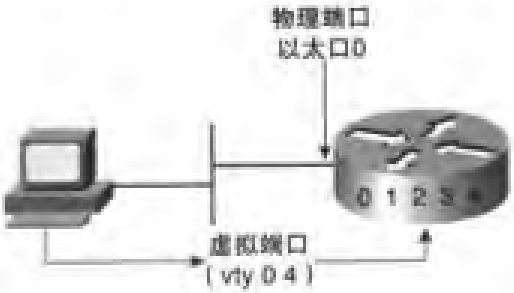


图20-16　用ACL限制vty的访问

限制vty的访问不是普通的通信流量控制机制，相反，它是用于增加网络安全性能。Vty的访问是使用Telnet协议，与路由器产生一个非物理性的连接。因此，只有一种类型的vty ACL。同样，这种限制应该被放置在所有的vty连接中，因为它不能控制用户使用哪个连接登录路由器。

然而，vty ACL的创建和在端口上建立ACL是一样的，只是应用vty ACL到虚拟连接时，用命令access-class代替命令access-group。例20-7显示了创建和应用一个虚拟终端访问控制列表。

例20-7　用ACL限制vty的访问

```
! Creating the standard list:
Rt1(config)# access-list 2 permit 172.16.1.0 0.0.0.255
Rt1(config)# access-list 2 permit 172.16.2.0 0.0.0.255
Rt1(config)# access-list 2 deny any
! Applying the access list:
Rt1(config)# line vty 0 4
Rt1(config)# login
Rt1(config)# password secret
Rt1(config)# access-class 2 in
```

在配置vty连接的访问控制列表时要记住以下各项：

- 在配置接口的访问时可以使用带名字的或者数字的ACL。
- 只有数字的访问列表才可以应用到虚拟连接中。

• 因为用户可以连接所有的虚拟终端，因此所有的虚拟终端连接都应用相同的ACL。

20.15 验证访问控制列表

命令show ip interface用于显示IP接口信息，并指出ACL是否正确设置。例20-8显示了show ip interface命令的输出内容。在例20-8中的第9和10行可以看到，ACL 10设置在接口Ethernet 0上的通信流量流出的方向。通信流量流入的方向没有设置ACL。

例20-8 show ip interface 命令

```
Router>show ip interface
Ethernet0 is up, line protocol is up
Internet address is 192.54.22.3, subnet mask is 255.255.255.0
Broadcast address is 255.255.255.255
Address determined by nonvolatile memory
MTU is 1500 bytes
Helper address is 192.52.71.4
Secondary address 131.192.115.2,subnet mask 255.255.255.0
Outgoing ACL 10 is set
Inbound ACL is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are never sent
ICMP mask replies are never sent
IP fast switching is enabled
Gateway Discovery is disabled
IP accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Router>
```

命令show access-lists显示所有ACL的内容。通过输入一个ACL的名字或数字作为命令的可选参数，可以看到一个具体的列表。

20.16 总结

本章学习了以下知识点：

• 两种主要的ACL类型：标准ACL和扩展ACL。
• 命名ACL允许用名字代替数字，并与数字的ACL具有相同的用途。
• ACL可以针对所有的被路由网络协议进行配置。
• ACL的典型应用是用于放置在内部网络和外部网络（互联网）之间的防火墙路由器上。
• ACL也可以用于限制虚拟终端访问路由器。
• ACL在Cisco的路由器中完成几个重要的功能，包括实现安全访问过程。

• ACL用于控制和管理通信流量。

• 对于某些协议，可以在同一个接口上应用两个ACL，一个是流入方向的ACL，另一个是流出方向的ACL。

• 通过使用ACL，一旦某个分组与ACL测试条件相匹配，它要么被拒绝要么被允许使用一个相应的接口。

• 通配符掩码位通过使用数字“1”和“0”来指示如何处理相应的IP地址位。

为了补充本章所学内容，参考本书所附CD－ROM中指定章节的视频、插图和e-Lab实验活动。

20.17 关键术语

访问控制列表（*access control list, ACL*） 用于控制和限制网络通信流量而根据通信流量特征设定的一套规则。

比特垃圾桶（*bit bucket*） 放置路由器决定丢弃的比特的地方。

边界路由器（*border router*） 网络边界的边缘或末端的路由器，提供了基本的安全保护，防止外界网络或者从缺乏网络控制的区域进入到专用网络区域。

扩展访问扩展列表（*extended ACL*） 一种既检查分组源地址又检查分组目的地址的访问控制列表

外部路由器（*exterior router*） 在防火墙结构中，连接互联网的路由器，常称为外部路由器。它强迫所有流入的通信流量经过应用网关。

防火墙（*Firewall*） 它是指一个路由器或者一个访问服务器或者几个路由器或者访问服务器，它们被设计为在任意相连的公用网络和专用网络之间的缓冲区。防火墙路由器使用访问控制列表和其他方法保证专用网络的安全

内部路由器（*interior route*） 它用于连接内部的网络。内部路由器只从应用网关处接受分组。网关控制那些流入和流出内部网络的网络服务的传递。

命名访问控制列表（*named ACL*） 它指那种带有名字的标准ACL或者扩展ACL。

排队（*queuing*） 在协议的基础上，ACL可指定某些分组在其他通信流量之前被路由器处理的过程

标准ACL（*standard ACL*） 一种访问控制列表，它基于分组的源地址和通配符掩码来过滤分组。

20.18 复习题

完成下面的复习题，以考核你对本章主题和概念的掌握情况。答案请参见附录C“复习题答案”。

1. 普通ACL功能包括内部地过滤分组，保护内部网络免受互联网的非法访问，限制虚拟终端的访问。这种说法是否正确？

A. 对

B. 错

2. ACL是一种：

A. 可达性的控制列表

B. 可计算性的控制列表

C. 可估计性的控制列表

D. 访问控制列表

3. 哪种ACL通过比较源地址来定义ACL的规则？

A. 扩展型

B. 命名型

C. 标准型

D. 路由器

4. 哪种ACL通过比较源地址、目的地址或者其他参数来定义ACL的规则？

A. 扩展型

B. 命名型

C. 标准型

D. 路由器

5. 哪种ACL用名字代替数字？

A. 扩展型

B. 命名型

C. 标准型

D. 路由器

6. 作为一般原则，ACL应该放置在网络的哪里？

A. 互联网中

B. 网络的核心层中

C. 靠近被控制的通信流量

D. 以上都不是

7. 在防火墙体系结构中，哪种路由器最有可能配置ACL？

A. 最强大的路由器

B. 内部路由器

C. 外部路由器

D. 以上全部

8. 命名ACL在Cisco IOS 11.2版本中引入进来。这种说法是否正确？

A. 对

B. 错

9. 哪条命令可以把ACL应用到VTY的端口中？

A. ip access-list

B. ip access-class

C. ip access-group

10. 哪个命令可以查看在端口上应用了哪些ACL?

A. show running-config

B. show ip protocols

C. show ip interface

D. show ip network

11. 在访问控制列表中，附加的32位信息称为：

A. 通配符位

B. 访问位

C. “0”位

D. “1”位

12. 如果希望允许通过的通信流量是基于地址或者协议类型，那么应该使用下面的那个命令?

A. Router #access-list *access-list number* {permit | deny} {*test conditions*}

B. Router（config）#access-list *access-list number* {permit | deny} {*test conditions*}

C. Router（config-if）#access-list *access-list number* {permit | deny} {*test conditions*}

D. 以上都不是

13. 标准的IP访问控制列表是基于分组的源地址和使用的协议来决定允许或者拒绝分组通过。这种说法是否正确?

A. 对

B. 错

14. 访问控制列表能够增加网络安全性是基于下面的哪些因素?

A. 分组的数据内容

B. 分组的目的子网、目的主机或者目的网络

C. 分组的源子网、源主机或者源网络

D. 被路由通过的网络类型

15. 下面哪种网络设备可以使用访问控制列表增加网络的安全性?

A. 集线器

B. 路由器

C. 网桥

D. 交换机

16. 命令access-list 1 permit 204.211.19.162 0.0.0.0可以实现以下哪种功能?

A. 只拒绝本网段地址

B. 允许一个指定的主机

C. 只允许本网络通过

D. 以上都不是

目标

学习完本附录之后，你应该能够：

- 了解结构化布线的基础。
- 在设计和安装的时候遵循结构化布线的规则以提供可扩展性。
- 认识结构化布线的子系统，包括分界点、电信间和设备间（如MC、IC和HC）。
- 认识在工作区内的特殊布线要求。
- 熟悉各种标准化组织，包括电信工业协会（TIA）、电子工业联合会（EIA）TIA/EIA、欧洲电工标准化委员会（CENELEC），还有各种世界级的组织，比如国际标准化组织（ISO）。
- 在注意安全的情况下进行低电压电信操作，并保证用电安全。
- 了解梯子安全性的基本要点，还有合适衣服对布线工作的重要性。
- 熟悉一些用于安装工作的基本的专门工具，还有基本的通信测试和测量设备。
- 了解在一个典型的项目里，哪个阶段对应哪些布线的任务。
- 了解使布线结构成功的基本业务过程。

第三部分　附录

附录A　结构化布线
附录B　术语表
附录C　复习题答案



附录A　结构化布线

目标

本附录包含以下几个主题：

- 结构化布线系统、标准和规程。
- 安全性。
- 布线行业的工具。
- 布线安装过程。
- 完成阶段。
- 布线业务。
- 案例分析。

这部分的材料，以及*Cisco Networking Academy Program CCNA 1 and 2 Lab Companion, Third Edition*里面与这部分内容相关的实验，对结构化布线安装的各个方面提供了广泛的介绍。

A.1　结构化布线系统、标准和规程

结构化布线系统是指以标准和经核准的方式建立的电信布线。它从***分界点***开始，穿过不同的***设备间***，并延伸到***工作区***。另外，它还包含可扩展性的问题。

学员应该注意的重要事项包括以下内容：

- 结构化布线的规则。
- 结构化布线的各个子系统。
- 可扩展性。
- 分界点。
- 电信间和设备间。
- 工作区。
- 主交叉连接（MC）、中间交叉连接（IC）和水平交叉连接（HC）。
- 电信工业协会（TIA）和电子工业联合会（EIA）。
- 欧洲电工标准化委员会（CENELEC）。
- 国际标准化组织（ISO）。

- 美国的规程。
- 各种标准的发展历程。

A.1.1 局域网结构化布线的规则

*结构化布线*是一种布线的系统化方法。它是一种创建有组织的布线系统的方法。安装工人、网络管理员及其他与布线相关的技术员都容易理解它。

以下的三条规则有助于确保结构化布线的设计计划是经济而有效的：

- **寻找一个完善的连接方案**——最佳的网络连接方案包括所有被设计用于连接、选路、管理和标识结构化系统的系统。符合标准的布线施工会有助于确保当前和将来的技术都能被支持。遵循标准可以确保项目长期保持高性能和高可靠性。
- **为将来的发展作打算**——安装的线路的数量也要满足将来的要求。为确保可以满足将来的需求，应该考虑使用超5类、6类非屏蔽双绞线和光纤。另外，应该使物理层的安装能工作十年以上。
- **保持选择厂商自由**——虽然一个封闭和专有的系统在开始的时候会比较便宜，但长远来说，它最终可能会变得非常昂贵。单个厂商的非标准化系统可能会使稍后的移动、增加和更改变得更加困难。

更多信息

如果想获得更多关于结构化布线规则的信息，请访问：
www.panduitncg.com/NCG_SYSSOL/ncg_syssol_pm/ncg_syssol_pm_markets/Finance/rules.asp

A.1.2 结构化布线的子系统

有7个子系统是跟结构化布线系统有关的（如图A-1所示）。每个子系统都负责一些特定的功能，为整个布线系统提供语音和数据服务。

- 位于设备间的入口设施（entrance facility，EF）内的分界点（分界）。
- *电信间（TR）*。
- *骨干布线*，也称为垂直布线。
- 分布（distribution）布线，也称为水平布线。
- 工作区。
- 设备间（ER）。
- 管理部门。

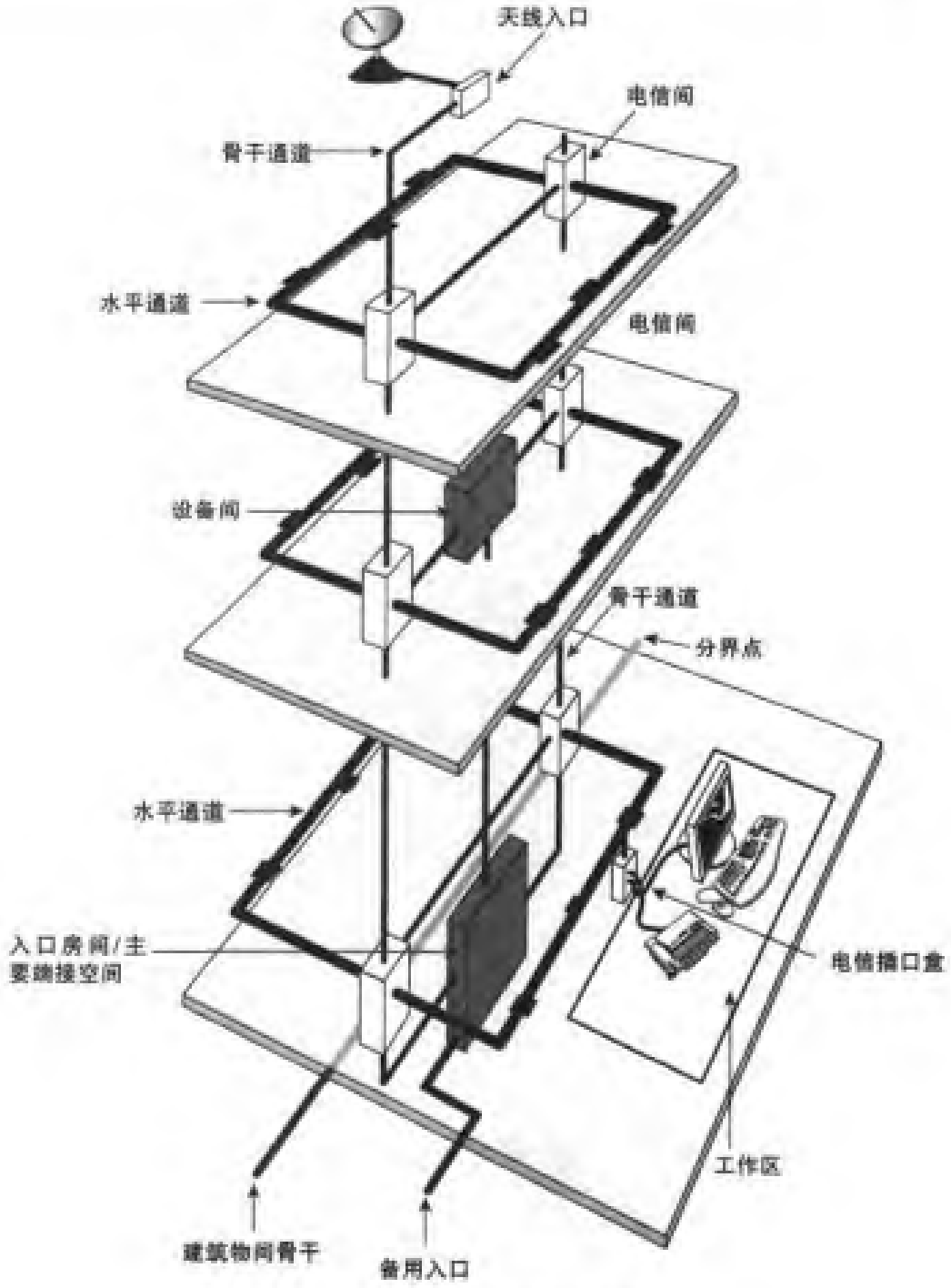
*分界（demarc）*是布线设施里，外部的服务提供商线缆与用户线缆连接的地方。

骨干布线是从分界到设备间，再到遍及整座建筑物的各个电信间的干线电缆。水平布线是从电信间引出的、通向各个工作区的布线。电信间是骨干布线转变为分布布线的地方。

这些子系统使结构化布线从本质上成为了一个分布式的结构，并提供了限制各种活动装置（PC、交换机、集线器等）的管理能力。设计一个可以正确路由、保护、标识和端接铜线或光纤介质的结构化布线设施，对网络性能和将来的升级来说都是至关重要的。

A.1.3 可扩展性

如果一个局域网在规模上能适应将来的发展，那它就是可扩展的。当对一个工作区内所需电缆和接入点的数目进行估算的时候，预先计划是很重要的。安装额外的电缆但暂时不用，总比需要时



图A-1 结构化布线的子系统

却没有足够的电缆好。

除了在骨干区域安装额外的线缆以便将来的发展之外，为每一台工作站或桌面型计算机安装一条额外的线缆以便将来使用也是很常见的。这可以保护线缆不受可能出现的安装失败的影响，同时也提供了扩充能力。

骨干可扩展性

如果要确定牵引多少额外的铜质电缆，首先要确定现在必需的电缆数量，然后再在这个数目上额外增加大约20%。

一种获得保留扩充能力的方法是：在建筑物的骨干使用光纤线缆和设备。升级终端设备（例如加入更高速的激光器和装置）可以适应将来光纤的发展。

工作区可扩展性

显然每一个工作区都需要一条线缆传输语音，一条线缆传输数据，而其他设备也可能需要一个到达语音系统或数据系统的连接。网络打印机、传真机、笔记本电脑或其他在工作区里的用户都可能需要他们自己的网络线缆接入点。

当线缆就位后，就要在插座上使用多端口墙壁板了。有很多安装方式都可以用于墙壁或隔断墙（partition wall）。此外，应使用那些以颜色编码的插座，以便使线路的类型更容易识别。管理标准要求每一条线路都应该贴上清晰的标签以便接线和排错。

一种叫做*IP语音（VoIP）*的新技术正变得越来越普及。这种技术使一些特别的电话可以通过数据网络进行呼叫。这种技术的一个很大的优点是，通过在现有的网络连接上使用这种服务，可以避免昂贵的长途话费。其他的设备，例如打印机和计算机，也可以接到IP电话上。IP电话也因此成为了工作区的集线器或交换机。但是，即使计划使用这些类型的连接，也应该安装足够的线缆以备将来的发展。特别要注意的是，IP电话和IP视频的流量在将来可能会共享网络的电缆。



图A-2　容许增长

为了适应办公室用户不断变化的需求，把至少一条备用电缆连接到工作区的插口上是比较好的做法。办公室可能会从单人使用变为多人使用。在这种情况下，如果只安装了一条通信电缆，那么工作区就会变得很低效。所以，应该假定将来每一个工作区都有可能容纳多个用户（如图A-2所示）。

A.1.4　分界点

分界点（demarc）提供了一个室外布线接口与楼内骨干布线的连接点（如图A-3所示）。它代表了服务提供商与客户的责任分界线。在很多建筑物里，分界点离其他设施（例如电力和用水）的接入点很近。

从服务提供商的设备到分界点之间的一切都由服务提供商负责。从分界点到建筑物里的一切就是由用户负责了。

通常要求本地电话线路端接到建筑物15米（49.2英尺）以内，并提供基本的电压保护。这通常都由服务提供商安装和提供。

*电信工业协会（TIA）*和电子工业联合会（EIA）制定和公布了很多行业（包括布线行业）的标准。因此，为了



图A-3　分界点

确保布线安装的安全性，在进行任何语音或数据布线的安装或维护时都一定要遵守这些标准。

TIA/EIA-569-A指定了用于分界点区间的各项标准。这些用于建筑和分界点区间规模的标准视建筑物的尺寸而定。例如，如果一座建筑物的可用面积超过2000m2，那么最好有一个上锁的、专用的和密封的房间。

以下是设立分界点区间的一些通常的规则：

- 允许建筑物内每20m²（215.3平方英尺）安装一块1m²的夹板墙。
- 在安装了分布设备的表面，必须覆盖防火级夹板或涂有两层防火漆的夹板。
- 防火夹板或终端设备的覆盖物应该涂成橙色，表示那是分界点。

A.1.5 电信间和设备间

线缆通过分界点进入建筑物后，就会到达入口设施（EF），EF通常是在设备间（ER）里。设备间是语音和数据网络的中心。设备间实际上就是一个大型的电信间，里面可能有主分布机柜、网络服务器、路由器、交换机、电话交换机、二级电压保护装置、卫星信号接收器、调节器、高速Internet设备，等等。TIA/EIA-569-A标准指定了设备间设计的各个方面。

在大型的设施里，设备间可能会为整座建筑物内的一个或多个电信间（TR）提供服务（如图A-4所示）。



图A-4 电信间

电信间里面的接线头和接线板可以安装在墙上的活动托架、分布架（如图A-5所示）或设备机柜里。

- 如果选择的是活动托架，那么托架必须固定在覆盖了底层墙面的胶合板上。使用活动托架的目的是使设备可以向外拉，这样工人和维修人员可以很容易进入墙的后面。但是应该注意的是，托架拉出后，离墙应该有48cm（18.9英寸）。
- 如果选择的是机架，那么机架的前后都必须至少有1m（3英尺）的空间作为工作区。一块用于安装分布架的55.9cm（22英寸）支撑板可以提供稳定性，并确定了分布架最终离墙的最小距离。
- 如果*接线板*、集线器和其他的设备被安装在同一个设备机柜里，那么机柜前方最少要有76.2cm（28.6英寸）的空间，以便机柜门可以打开。通常这种机柜的尺寸为1.8m高×0.74m宽×0.66m深（5.9英尺×2.4英尺×2.17英尺）。



图A-5 泛达（Panduit）牌分布式机架

设备必须小心地放置在设备架上。放置时要考虑的问题包括：设备是否要用电力工作、线缆的走向、线缆的管理和使用线缆的易用性。例

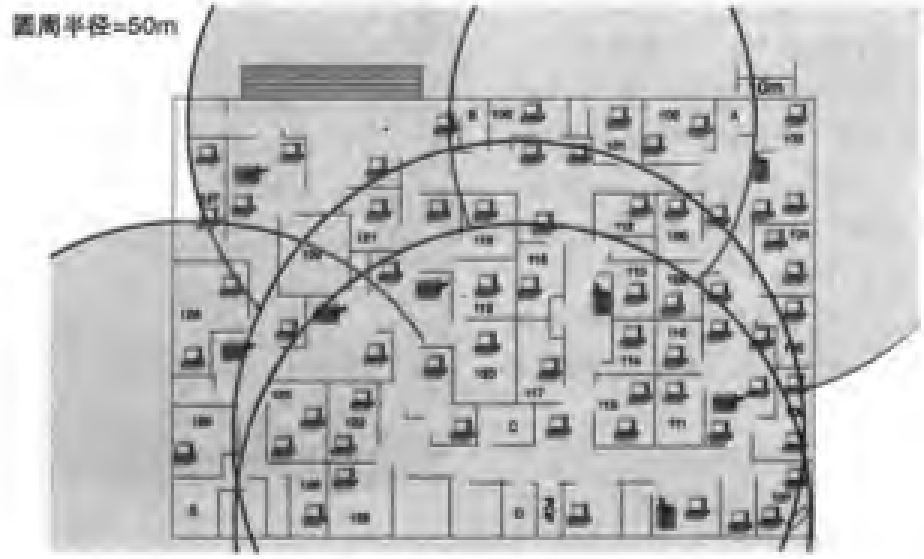
如，如果在布线系统安装完成后会发生一系列重大的改动，那么接线板就不要放置在设备架的高处。当设计设备布局的时候，易用性是一个很重要的考虑因素。

为了能适应将来的发展，在进行设备布局的时候，可扩展性也是一个需要考虑的因素。在设备架上必须留有一定空间以便日后摆放更多的接线板；在进行初次布局的时候，也要留下一定的地方以便日后安装更多的设备架。

如果能在电信间里正确地安装设备架和接线板，那么将来与布线安装有关的改动和修正就会比较容易了。这在考虑工作区的设计和布局的时候是非常重要的。

A.1.6　工作区

由一个单独的电信间提供服务的区域叫做工作区。在大多数情况下，工作区占了一座建筑物的整一层，或者是一层楼的一部分（如图A-6所示）。



图A-6　工作区

从电信间端接点到工作区插座的线缆的最大长度不能超过90m（295英尺）。这90m的最大水平布线长度被称为永久线路。每一个工作区都必须至少有两条线缆，一条用于传输数据，另一条用于传输语音。正如前面所提到的那样，工作区布线也要考虑到适应将来其余设备或扩展的需要。

其实这个最远距离通常都会少于90米，因为线缆不能直接穿过地板——它们通常都要在布线管理设备（例如线槽、配线架、楼梯和配线管道）里面穿行。这些设备使线缆从工作区的上方（通常是在悬置的天花板上方的*隔层*）经过。这意味着预计工作区半径要减去两倍的天花板高度（一次是线缆到布线管理设备上面去，一次是线缆从布线管理设备上下来）。

此外，ANSI/TIA/EIA/-568-B标准规定了从跳线到互连设备接线板之间的距离可以有5m，从墙上的线缆端接点到电话或者计算机的距离也可以有5m。这额外的10m最大长度，再加上永久线路，被称为水平通道。一条水平通道的最大长度是100m——最大长度为90m的永久线路加上最大长度为10m的跳线。

最后，线缆实际走的线路不一定是直接到达目的地的。布线管理设备可能会很昂贵，而且加热、通风和空调设备，还有变压器和照明设备的位置也可能会增加线缆的长度。这进一步减少了工作区的半径。通常来说，如果把所有因素都考虑在内，实际的半径大概会是60到70m（196.9到229.7英尺），而不是100m（328.1英尺）。在设计的时候，工作区半径通常会是50m（164英尺）。

工作区的维护

如果要经常进行连接的改变，或预见到会有这种改变，那么就要进行临时性接线了。比起从连

接着的设备中移走终端线缆，并把线缆重新端接在另一条线路上来说，从工作区插口上把线接到电信间的新位置会容易得多。跳线也用于连接网络设备与电信间里的交叉连接。根据TIA/EIA-568-B.1标准，跳线的长度不能超过5m（16.4英尺）。

必须在整个接线板系统里使用统一的布线设计。就是说，所有的插座和接线板都应该按照相同的布线设计来布线。如果信息插口或插座使用了T568A的布线设计，那么就应该使用T568A的接线板。对于T568B的布线设计来说也一样。

接线板可以用于非屏蔽双绞线（UTP）、屏蔽双绞线（STP）或光纤的连接。其中，用于UTP的接线板是最常见的。这种接线板使用的是RJ-45插座，带有RJ-45插头的跳线会被插在这些端口上。

在多数的机构里，并没有规定经授权的维护人员不能在线路上安装未被授权的连接板或集线器。然而，有一些新型的接线板可以在简化移动、增加和改变的规定之余，提供广泛的网络监控能力。在这些接线板上，任何需要移走的跳线旁都会有一盏指示灯，一旦跳线被拔出，电缆应该被重新插上的地方的那个插孔旁的另一盏灯就会亮起来。通过这种方法，系统可以自动引导一个相对来说不那么熟练的员工进行线缆的移动、增加和改变。

这种机制可以发现操作员拔掉了某个插座上线缆，也可以发现一个插座被插上了线缆。一个未经授权的对接线板的改动可以触发系统日志产生一个事件，如果需要的话，甚至还可以触发一个警报。例如，如果在凌晨两点半，连接到工作区的6条线缆被显示断开了连接，那么这就是一个值得调查的事件了，因为很有可能发生了盗窃。

连接线缆的类型

跳线（如图A-7所示）包含不同的接线方案。其中最普遍的是直通线，它的两端有着相同的接线方案。换句话说，一端的引线1连接着另一端的引线1；一端的引线2连接着另一端的引线2，以此类推。这种类型的线缆用于连接PC和网络集线器。

如果要连接通信设备与网络集线器，那么通常都要使用交叉线。交叉线的一端使用T568A的接线方案，而另一端则使用T568B的接线方案。



图A-7 UTP跳线

实验活动 检查线缆端接类型

本实验中，你将复习T568A、T568B和RJ-45 USOC接线标准，并学会端接一条超5类线缆终端的方法。

线缆管理

线缆管理设备用于路由线缆，为线缆提供一个整齐有序的路径，并确保维护线缆的最小弯曲半径。线缆管理设备也可以使布线系统中的线缆增加和更改变得更容易。电信间里的线缆管理设备有很多种。当需要简易轻便的安装时，可以选择线缆筐（cable basket）。如果需要支撑一束很重的线缆，那么通常可以使用梯形架。不同类型的管道可以使线缆在墙壁、天花板和地板里穿过；或者是走明线的时候，管道可以为线缆提供保护。线缆管理系统用于从电信架到分布电缆之间的垂直或水平布线，它使布线工程显得整齐而有序（如图A-8所示）。

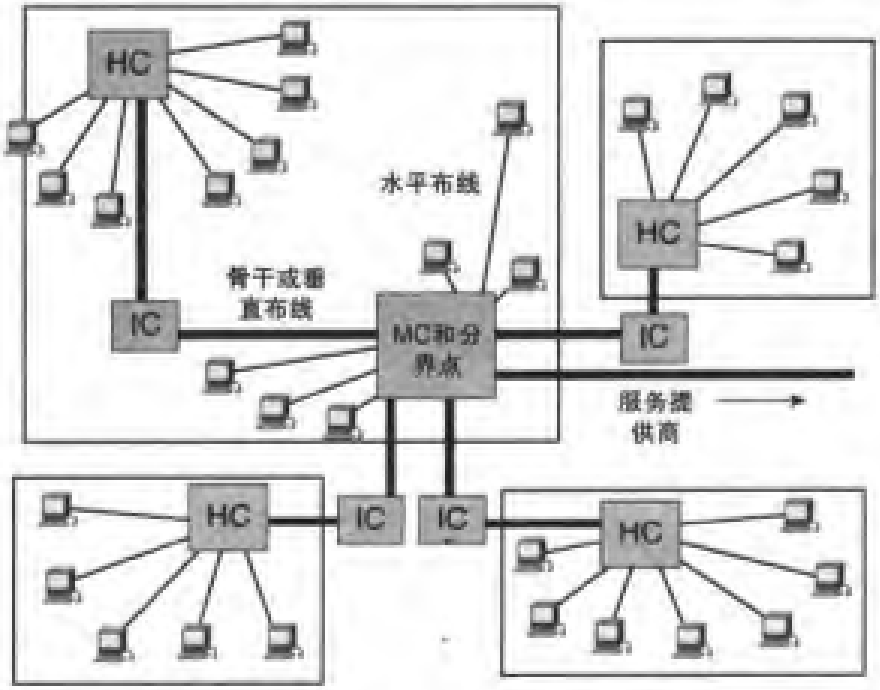
A.1.7　主交叉连接、中间交叉连接和水平交叉连接



图A-8　安装了机架的泛达（Panduit）纵垂直和水平线缆管理系统

由于各种原因，大多数的网络里电信间的数量都不止一个。首先，一个中型或大型的网络通常会覆盖很多楼层或建筑物。因此每一层楼或每一座建筑物都需要一个电信间（如图A-9所示）。其次，信号在传输介质中传播的时候会降级和衰减。因此，遍布整个局域网的电信间之间会隔开预先规定的距离，以提供集线器和交换机之间的互连和交叉连接，并保证网络能发挥人们所期望的性能。而放置在电信间里的中继器、集线器、网桥或交换机等设备则用于信号的再生。

并非所有电信间的地位都是相等的。主要的电信间被称为***主交叉连接***（*main cross-connect, MC*），它是网络的中心。所有的布线都从这里出发，而且大多数的设备都放置在这里。***中间交叉连接***（*intermediate cross-connect, IC*）与主交叉连接相连，里面放置着供一座建筑物或一个园区使用的设备。***水平交叉连接***horizontal cross-connect,（*HC*）提供了骨干与水平线缆（位于一层楼内或一座建筑物内）的交叉连接。



图A-9　MC、HC和IC的规划

主交叉连接

主交叉连接（MC）是整座建筑物或整个园区的主要集中点。实际上，主交叉连接就是主电信间。它是控制建筑物或园区内其余电信间（中间交叉连接和水平交叉连接）的房间。在某些网络里，它是内部线缆与外部连接的地方（分界点）。

所有的中间交叉连接或水平交叉连接都与主交叉连接以星形拓扑相连。骨干布线，或**垂直布线**，被用于连接那些位于其他楼层的中间交叉连接和水平交叉连接。当整个网络被限制在一座多层建筑物里的时候，主交叉连接通常会位于建筑物中部的某一层——即使分界点可能会位于一楼或地下室的入口设施里。

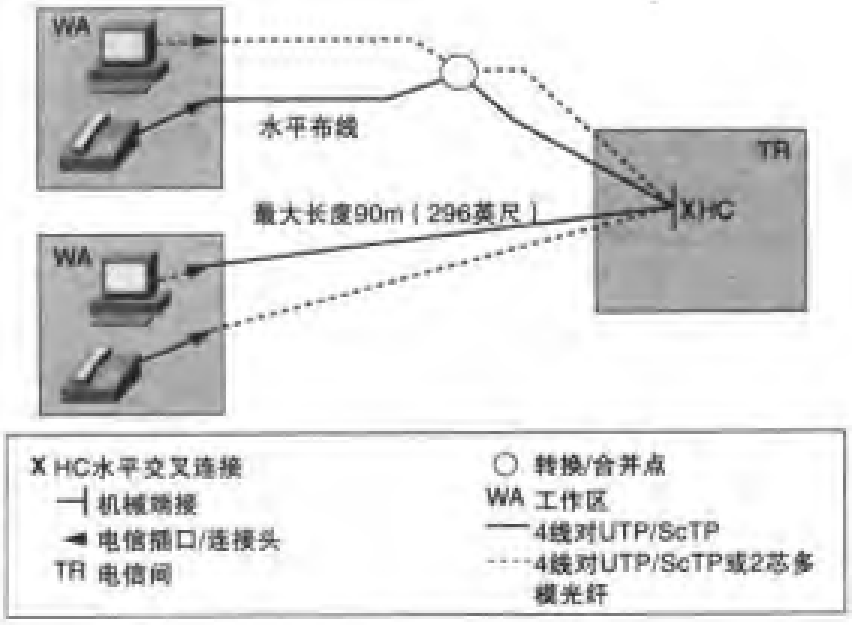
当网络由多座建筑物组成时，主交叉连接通常会位于它们的其中一座里。每一座建筑物通常都会有它自己的主交叉连接，称为中间交叉连接（IC）。中间交叉连接与建筑物内所有的水平交叉连接相连。中间交叉连接使骨干布线可以从主交叉连接延伸到各个水平交叉连接，因为这个互连节点不会使通信信号降级。在整个结构化布线安装里面，只能存在一个主交叉连接。主交叉连接为各个中间交叉连接服务，而各个中间交叉连接又为多个水平交叉连接服务。在主交叉连接和水平交叉连接之间只能有一个中间交叉连接。

骨干布线（图中的红线）从主交叉连接延伸到每一个中间交叉连接。中间交叉连接位于园区的每一座建筑物内，而水平交叉连接则为工作区服务。从水平交叉连接延伸到工作区的水平布线，在图中以黑线表示。

水平交叉连接

水平交叉连接（HC）是最靠近工作区的电信间。就像所有的铜质交叉连接那样，水平交叉连接通常是一个接线板或一个冲压模块，另外再加上各种网络设备，例如中继器、集线器或交换机。它也可以是一个安装在房间或机柜里的架子。由于一个典型的水平布线系统包含了多条连接到各个工作站的线缆，因此它代表了建筑设施里最大的线缆集中点。一座有1000台工作站的建筑物里面的水平布线系统，它所包含的线缆可以轻易达到2000甚至3000条。

水平布线包括铜线或光纤这些网络传输介质，它们用于从配线室延伸到工作站的区域（如图A-10所示）。水平布线包括沿着水平路径到达通信插口，工作区里的连接头，还有水平交差连接里的跳线等网络传输介质。



图A-10 水平布线和符号

任何安装在主交叉连接和另一个电信间之间的线缆都被称为骨干线缆。布线标准里明确定义了水平线缆和骨干线缆的不同之处。

实验活动 在超5类接线板上端接一条超5类线缆

本实验中，你将在超5类接线板上端接一条超5类线缆，并学会110型冲压工具和剥线工具的正确使用方法。

骨干布线

任何安装在主交叉连接和另一个电信间之间的线缆都被称为骨干线缆。布线标准里明确定义了水平线缆和骨干线缆的不同之处。骨干布线也被称为垂直布线。它由骨干线缆、中间交叉连接和主交叉连接、机械终端和用于骨干到骨干的交叉连接的跳线组成。骨干布线包括以下几个部分：

- 同一楼层里面的各个电信间（主交叉连接到中间交叉连接，中间交叉连接到水平交叉连接）。
- 不同楼层间的各个电信间之间（主交叉连接到中间交叉连接）的垂直连接（线缆）。
- 电信间和分界点之间的线缆。
- 在有多座建筑物的园区里，建筑物之间的线缆。

各种线缆的最大铺设距离是不同的。对骨干布线来说，最大铺设距离还会受到骨干布线被如何使用的影响。举个例子，假设现在决定使用单模光纤进行骨干布线。如果这种传输介质将被用于连接水平交叉连接和主交叉连接，那么它用于骨干布线的最大铺设距离为3000m（9842.5英尺）。

在某些时候，用于骨干布线铺设的3000m（9842.5英尺）最大距离必须被分成两部分。这种情况发生在骨干布线用于连接水平交叉连接与中间交叉连接，还有连接中间交叉连接与主交叉连接的时候。在这种情况下，从水平交叉连接到中间交叉连接的骨干线缆的最大铺设距离为300m（984英尺），从中间交叉连接到主交叉连接的骨干线缆的最大铺设距离为2700m（8855英尺）。

光纤骨干

光纤是一种用于传输骨干流量的极其有效的方法。这是因为光纤不会受到电噪声和无线电频率干扰的影响。而且光纤不导电，因此也不会引起接地环路。同时，光纤系统有着很高的带宽，可以工作在很高的速度下。这意味着由于光纤骨干有着某些特性，现在安装的光纤在将来可以升级到具有更高的性能——只要终端设备有这样的能力。这使光纤具有很高的性价比。

在使用光纤作为骨干传输介质的时候，它还有一个额外的优点：它的传输距离远远超过了铜线。多模光纤在用于骨干时，最大传输距离可以达到2000m。单模光纤甚至可以达到3000米。虽然光纤，特别是单模光纤，可以把信号传输到远远超过上面所说的距离（借助终端设备可以传输60到70英里），但如此长的距离被认为是超过了局域网标准的范围。

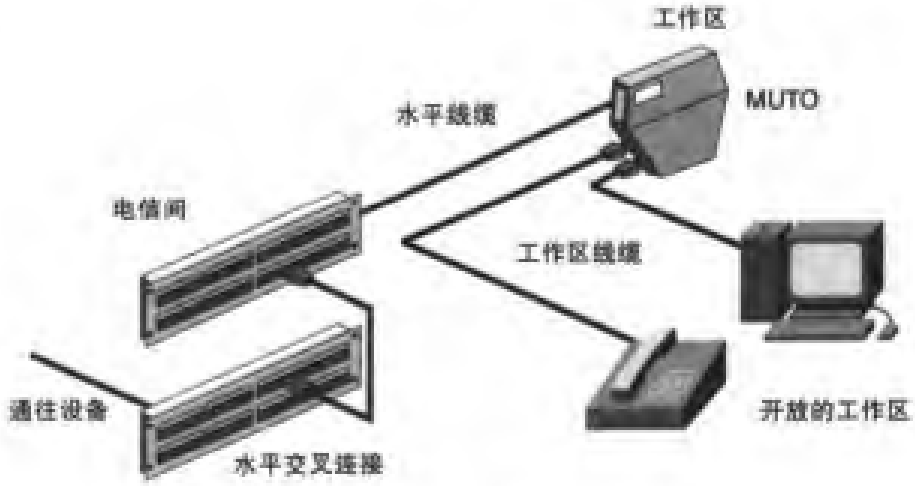
多用户电信插座组件和集合点

架空的地板和吊顶的天花板内都可以放置接线板。它们通常都用作聚集点（consolidation point）或***多用户电信插座组件（multiuser telecommunications outlet assemblies，MUTOAs）***。

在TIA/EIA-568B.1里，对含有可移动家具和隔板的工作区的水平布线作了额外的规定。通过MUTOA和集结点，水平布线方法规定了一个“开放办公室”环境（如图A-11所示）。这些方法是为了使得那些需要频繁配置的开放办公室工作区的布线安装能更灵活和更经济。

集集点（CP）和MUTOA的出现并不是要取代为工作区服务的整个水平布线系统，它们的作用是：处于靠近开放办公室区域的位置，当设备需要重新安放的时候，可以避免从办公室到电信间的整段线缆的重新铺设——只需要把新的工作区域插口与CP或MUTOA之间的线缆重新铺设就行了。这样一来，从CP或MUTOA到TR的那段长距离线缆就可以保持不动了。

MUTOA可以使用户在移动或者添加设备，以对模块化设备的设置进行更改的时候，不需要重新进行线缆的铺设。***跳线***可以从MUTOA直接牵引到工作区设备上（如图A-12所示）。MUTOA摆放



图A-11 典型的MUTOA安装



图A-12 典型的集合点安装

的位置必须固定，而且易于接近。另外，不能把它安装在天花板或地板里。类似地，不能把它安装在设备内部——除非该设备对整个建筑结构来说是安全而且保持不动的。

聚集点（CP, Consolidation points）为一个有限的区域提供了连接接入功能。通常，由一个固定的、足够用的、安装在墙上、天花板上或支撑柱上的配线板为多个模块化装修的工作区提供服务。面板必须没有障碍，能畅通无阻地访问而不需要移动任何固定装置、设备或沉重的家具。聚集点与MUTOAs不同，工作站和工作区的其他设备不会像插入到MUTOA中一样插入到CP中。工作站插入到插孔中，然后连接到CP。

TIA/EIA-569标准规定了下列内容：

- 每个装修群集子少需要一个CP。
- 每个CP最多服务12个工作区。
- 跳线长度最多为5m（16.4英尺）。

当使用MUTOA的时候，TIA/EIA-568-B.1有以下的几项规定：

- 每一个设备群里面都要有最少一个MUTOA。
- 每一个MUTOA最多可以连接12个工作区。
- 工作区跳线的两端要贴上惟一的标识。
- 跳线的最大长度是22m（72.2英尺）。

对于集结点和MUTOA，TIA/EIA-568-B.1标准建议在电信间和CP，或者电信间和MUTOA之间

的设备相隔最少15m（49英尺）。这可以避免串扰和回波损耗问题。

A.2 结构化布线的标准和规程

标准是指一系列的规则或程序，它们被广泛使用或正式指定，并被当作衡量标准或卓越的典范。标准可以有很多种形式。它们可以由一个单独的厂商指定，或者作为行业标准用于支持不同厂商之间的协同工作：

- 用于骨干和水平布线的标准化传输介质和布局的描述。
- 标准的用于设备物理连接的连接界面。
- 遵循系统的计划和基本的设计原则来进行的统一规范的设计。

众多的公司和组织，甚至政府机构都调整和指定了线缆的使用。此外，很多组织，还有地方、州、国家和国际的政府机构都提出了各种规范、要求和规程。

标准的力量在于：遵循标准组建的网络可以与其他的标准网络设备一起很好地工作。很多网络布线系统的长期表现和投资价值已经被那些不知道或不遵循强制性和建议性标准的安装者严重地降低了。

这些标准会被经常复核和周期性更新，以便反映新的技术和日益增长的语音和数据网络的需求。了解这一点是很重要的。一旦新技术被添加到标准里面，旧的技术就会被放弃或逐渐销声匿迹。很多情况下，一个网络可能含有一些已经不再符合当前标准，又或者正在被逐渐淘汰的技术。通常并不要求这种网络一定要马上进行彻底的转变，但是这些陈旧和落后的技术最终是会被新技术所取代的。

各种标准通常是由一些国际性组织研究出来的，又或者是在它们的指导下被研究出来的，这些国际性组织这么做的原因是设法使它们成为通用的标准。这些组织的例子有IEEE、ISO和IEC等国际性标准化团体。这些国际性标准化组织由很多来自各个国家的成员组成，每一个组织都有它们自己的制定标准的过程。

在很多国家里，国家规程是州/省机构制定相应标准的样板，自治市和其他政府单位也把它们合并到自己的法律和条例里。于是，强制性被移到了大多数的本地权威机构里。记得到本地的权威机构里了解一下哪些规程是强制性的。在大多数情况下，本地规程凌驾于国家规程之上，而后者又凌驾于国际规程之上。

A.2.1 电信工业协会和电子工业联合会

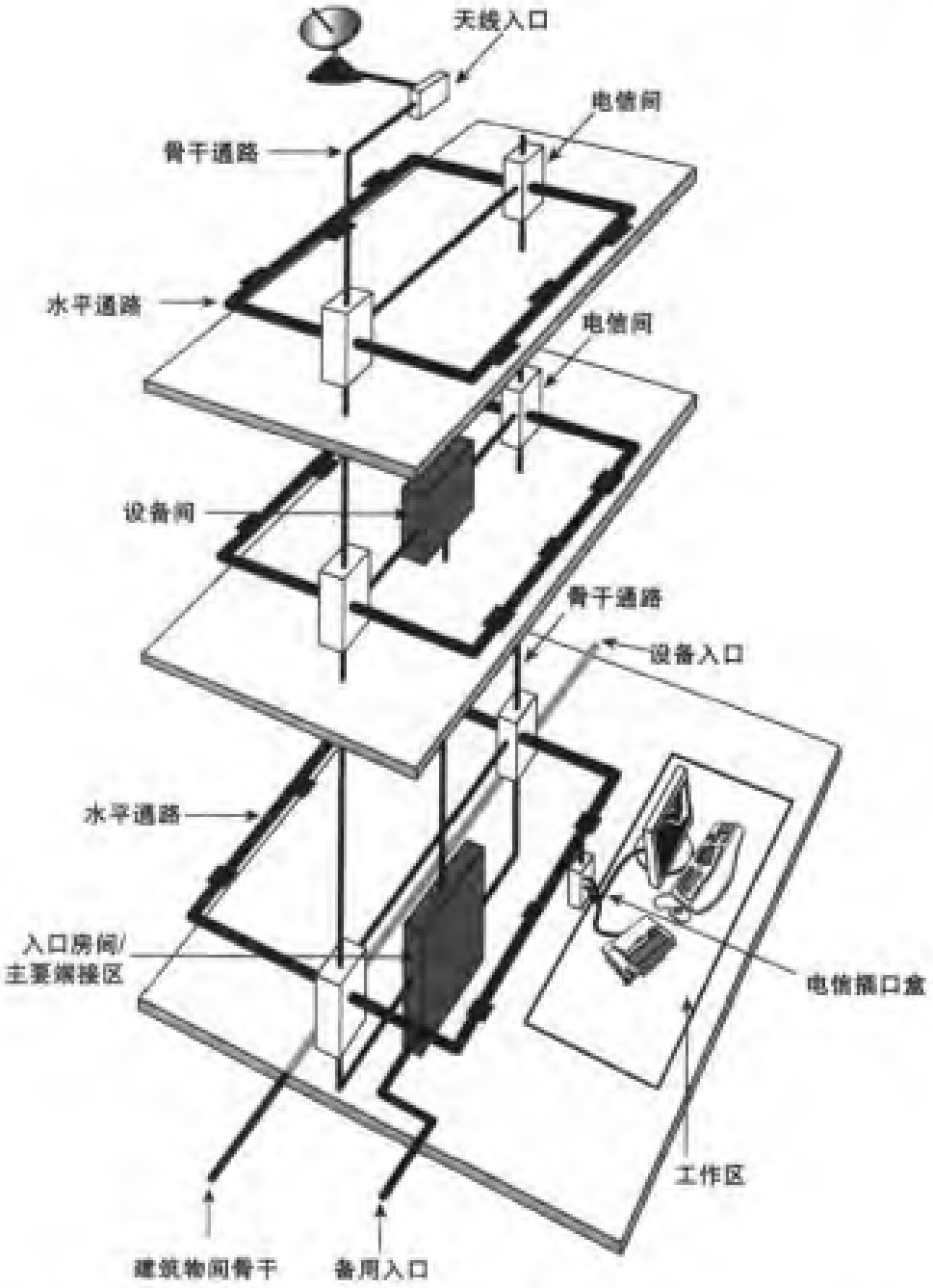
电信工业协会（TIA）和电子工业联合会（EIA）是两个行业协会，它们联合制定和公布了一系列的标准。这些标准覆盖了局域网结构化语音和数据布线的各个方面（如图A-13所示）。

注意：要想获得关于TIA和EIA的更多信息，请访问www.tiaonline.org和www.eia.org。

美国国家标准协会（ANSI，见第6.2.7节）委托TIA和EIA去研究用于多种通信产品的非官方的工业标准。这意味着很多标准的名称都是以ANSI/TIA/EIA开头的。TIA/EIA有很多委员会和子委员会，它们负责制定关于光纤、用户前端设备、网络设备、无线通信和卫星通信方面的各种标准。

虽然存在很多标准和补充标准，但以下这些标准是线缆安装者最常使用的（如图A-14所示）。

- TIA/EIA-568-A是用于通信布线的商业建筑标准。这个标准指定了通信布线、推荐拓扑和传输距离限制方面的最小要求，传输介质和连接硬件的性能规范，还有连接头和插脚的指定。
- TIA/EIA-568-B是关于布线的标准。这个标准指定了传输介质的组件和传输要求。TIA/EIA-568-B.1指定了一种用于商业建筑的通用的通信布线系统。这种系统适用于多设备和多厂商的环境。



图A-13 用于建筑物的TIA/EIA标准

TIA/EIA-568-B-1.1是一个补充标准，它规定了由四对线组成的非屏蔽双绞线（UTP）和金属箔屏蔽双绞线（ScTP）跳线的弯曲半径。TIA/EIA-568-B-2指定了布线的组件、传输、系统模型和用于检验双绞线的测量过程。TIA/EIA-568-B.2.1是一个关于6类线缆的补充标准。TIA/EIA-568-B.3指定了光纤布线系统里的组件和传输要求。

• TIA/EIA-569-A是关于通信路径和空间的商业建筑标准。该标准指定了建筑物内和建筑物间的设计和构筑方法，从而使它们能支持通信介质和设备。

• TIA/EIA-606-A是商业建筑的通信构造方法的管理标准，另外它还包含了为线缆做标记的标准。该标准指定了每一个硬件终端单元都必须有某种惟一的标识。该标准也对网络管理方面的记录保存和文档维护作了概述。

• TIA/EIA-607-A是关于通信方面的商业建筑接地和连接要求的标准。它支持多厂商、多产品的环境，也支持那些可能会安装在用户前端的不同系统的接地方法。这个标准指定了建筑物接地系统和电信设备接地配置之间精确的分界点，也指定了需要为该设备提供支持的建筑接地配置。

A.2.2 欧洲电工标准化委员会

*CENELEC*的意思是*欧洲电工标准化委员会*。1973年它根据比利时法律的规定，以非营利性机构的形式成立。CENELEC制定了大多数用于欧洲的电气标准。它与来自19个国家的35000名技术专家一起合作，公布了很多欧洲市场的标准。欧洲经济共同体在它的第83/189/EEC号文件里把CENELEC正式指定为欧洲标准化组织。很多CENELEC的布线标准都借鉴了ISO的布线标准，而且只是做了很小的改动。

注意：*要想获得关于CENELEC的更多信息，请访问*www.cenelec.org。



图A-14 TIA/EIA结构化布线标准

虽然CENELEC和国际电工委员会（IEC）工作在两个不同的层面上，但由于它们是欧洲电工领域里最重要的两个标准化团体，因此它们的行动都能产生强烈的相互影响。CENELEC和IEC之间的合作被称为德累斯顿协定——双方于1996年在德国城市德累斯顿核准和签署了该协定。该协定的目的在于加速国际标准的出版和通常修订，并应市场要求加速标准指定的准备过程。该协定也用于确保资源的合理使用。因此，有关标准内容的详尽的技术考虑更适宜在国际层次上制定。

A.2.3 国际标准化组织

国际标准化组织（ISO）是一个由来自超过140个国家的国家标准化团体组成的国际性组织。例如，美国国家标准协会（ANSI）就是ISO的一个成员。ISO是一个非政府组织，它的建立是为了促进标准化的发展以及一些相关的活动。ISO的工作导致了国际性协定的产生，后者以国际性标准的形式公布。ISO定义了许多重要的计算机标准，其中最重要的可能就是用于网络设计的一个标准化体系——开放系统互联（OSI）模型了。

注意：*要想获得关于ISO的更多信息，请访问*www.iso.org/iso/en/ISOOnline.frontpage。

A.3 美国的规程

某些网络项目需要一张执照来确保工作是按正确方式完成的。这种情况下，最好联系当地的有关部门，咨询一下有关执照要求的信息。

为了获得当地或州的建筑规程的副本，可以联系负责管辖当地建筑的官员。在美国被广泛采用的所有基本建筑规程（CABO、ICBO、BOCA、SBCCI、ICC等）都可以从建筑管理局国际联合会（ICBO）处购买。

很常见的情况是：规程需要当地的检查，并强制与州或省政府的规程合并，而且这种情况很有可能在市和镇的执行单位里出现。建筑规程、消防规程和用电规程就是其中的一些例子。跟职业安全规程一样，这些规程本来是地方问题，但标准的不一致和通常缺乏强制性，导致了国家标准的出现。当这些标准被州或当地权威机构采纳并且在适当的层次上强制执行的时候，它们就会被移交到更低级的权威机构实行。

值得注意的是，触犯这些规程的代价通常都会很高——无论是在罚款方面还是在延误项目的代

价方面。

> **注意：** 美国残障人法案（ADA）使网络和电信在进行新的构筑、改造和革新方面有了几项重大的更改，根据使用工具的不同，这些更改可以是强制性的，而罚款数目会根据不遵守规定的程度而定。

不同城市、县和州的机构会强制推行不同的规程。这意味着，一个城市里的项目会由相应的市机构处理，而在该市外的项目可能会由县机构处理。例如，在某些地方，防火规程可能由该县的建筑许可部门强制推行，而在其他地方，防火规程却由当地防火部门负责。

虽然地方机构会检查和强制推行这些规程，但规程通常都不是由本地机构制定的，而是由标准制定机构制定的。例如，《美国国家用电规程》（NEC）就被写成了一个听起来合法的条例。这使当地政府有可能通过投票决定是否采纳它。但这种情况并不一定会经常出现，而且政府可能会拖后腿。记得去了解一下你所在的地方所强制推行的NEC的版本。

> **注意：** 多数国家都有类似的规程制定机构。如果你要进行跨国的项目实施，那么了解当地的规程将是一件很重要的事。

A.3.1 标准的发展过程

随着网络带宽从10Mbit/s增加到1000Mbit/s，甚至更高，它为布线带来了新的要求。旧式的线缆通常不能满足当今快速网络的使用需要。基于这个原因，随着时间的过去，网络所使用的线缆的类型不断地改变，而且这也反映在标准的制定上。以下是一些TIA/EIA-568-B.2里面使用的标准：

- 对于双绞线缆，只认可100b的3类、超5类和6类线缆。在进行新的布线安装时已经不再推荐使用5类线缆了，而且它也从标准的正文被移到了附录里。现在在需要使用100Ω双绞线缆的环境里，推荐使用的是超5类或更好的类别。
- 6类标准指定了一些性能参数，以确保产品符合这些标准：组件间互相适应、向后兼容、不同厂商间的产品能共同使用。
- 当进行超5类或更高级电缆的端接时，从端点开始算起，线对不应该被解开缠绕超过13mm（0.5英寸）。UTP水平布线的最小弯曲半径是电缆直径的4倍。UTP跳线的最小弯曲半径可以与电缆的直径相等，因为它包含绞合的电线，所以比用于水平布线的实心铜线更柔韧。

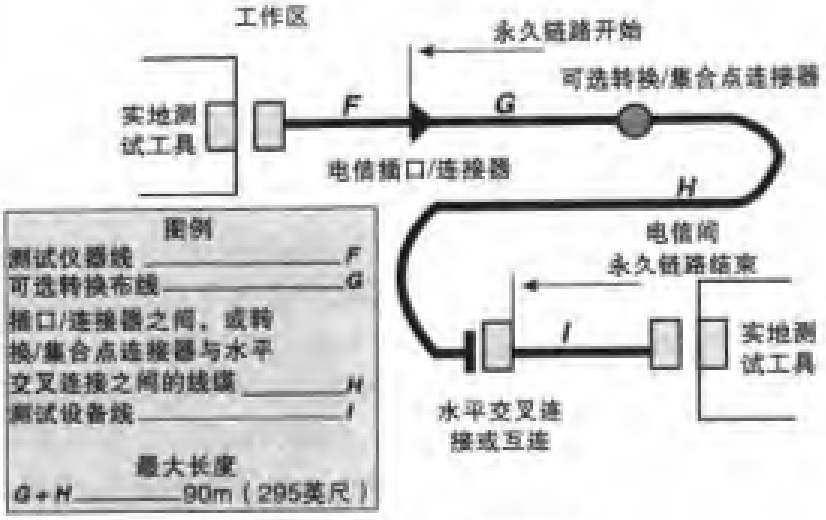
用于电信间跳线的最大长度从6m（19.7英尺）变成了5m（16.4英尺）。用于工作间跳线电缆的最大长度从3m（9.8英尺）变成了5m（16.4英尺）。水平线缆长度保持90m（295.3英尺）不变。如果使用了MUTOA，而且水平线缆长度可以减少，那么工作区跳线的长度可以相应增加——只要线缆总长度不超过100m（328.1英尺）（如图A-15所示）。

如果使用了MUTOA或集合点，则要求电信间与MUTOA或集合点之间的最小距离为15m（49英尺），这是为了减少噪声和回波损耗问题。

在以前，所有跳线和交叉连接跳线都要求使用绞合线缆以提供柔韧性，以便即使在不断插拔的情况下也不会出现问题。而现在，考虑到绞合导线的使用，所有与该主题有关的文章里，措辞都从“要”变成了“应该”。这允许了实心导线电缆的设计使用。

跳线是网络系统中的关键组成部分。有关在施工现场制作跳线和跳线的那部分描述，现在仍然允许当场制作这些线缆，但强烈建议网络设计者购买事先制作好并经过测试的电缆。

6类和7类是最新的铜质电缆类型。由于6类线缆使用得更加频繁，因此对线缆安装者来说，了解它的好处是很重要的。



图A-15　水平布线标准的更改

在保持线缆内部线对间距离的方法上，超5类和6类线缆有着显著的不同。有些6类线缆用从线缆的中心把线对从物理上分隔开。另一些则用一个特别的外套把线对固定起来。还有一些6类线缆用金属屏蔽箔把里面的线对包裹起来。这种电缆通常被称为金属箔屏蔽双绞线，或ScTP。

为了达到比6类线缆更高的性能，7类线缆使用了一种完全屏蔽结构以限制线对之间的串扰。每一对线都被包裹在一个金属箔套里，四对包裹了金属箔的导线外面还围绕着一层编织外套。将来的电缆可能还会加上一条排绕线（drain wire）提供接地功能。

结构化布线的标准会继续向前发展。标准关注的焦点是对那些集中在数据网络上的新技术的支持，例如以下这些：

- 在传输中利用电力信号的IP电话和无线技术，这种技术可以为IP电话或接入点供电。
- 使用10GB以太网传输的存储区域连网（storage area networking）。
- 大都市以太网的“最后一英里”问题的解决方案，这需要优化的带宽和对距离的要求。

利用以太网供电（Power over Ethernet，PoE）标准现在正在研究中，并且在不久的将来会成为现实。PoE在用于以太网传输的线缆上嵌入一个电力信号，这种电力信号可以使IP电话和无线接入点不需要通过交流电插座供电，从而简化了网络部署，并节约了成本。

A.4　安全性

安全性是一个非常重要的概念，它包含了在低压电通信布线里经常被忽视的信息。还不习惯在实际工作场所进行操作的学员可以从实验或训练中受益。与安全有关的其他重要问题包括：

- 美国的安全规程和标准。
- 带电操作的安全问题。
- 实验室和工作场所的安全守则。
- 个人安全装备。

A.4.1　美国的安全规程和标准

绝大多数的国家都有致力于保护在危险环境下工作的工人的规则。在美国，主管工人安全和健康的机构是*职业安全与健康管理局（OSHA）*。自从这个机构在1971年创立之后，工作中的死亡事故减少了一半，工伤和生病率也下降了40%。与此同时，美国的就业工人数目几乎翻了一番：从在350万个工地工作的5600万名工人增加到在690万个工地工作的1亿零500万名工人。

OSHA的责任是通过强制执行美国劳工法来保护工人。从技术上来说，OSHA并不是一个与建立规程或许可证有关的机构。然而，如果OSHA的调查员发现一个施工场所严重违反了安全规程，那他们可以对它处以很重的罚金并关闭它。

注意：要想获得关于OSHA的更多信息，请访问www.osha.gov。

物资安全记录表（MSDS）

*物资安全记录表（MSDS）*是一份文档，它含有与使用、存放和处理危险物资有关的信息。具体来说，它提供了与危险物资有关的详细信息：危险物资泄漏对健康的潜在的影响，还有如何对危险物资进行安全操作。它讲述了危险物资的危险所在，如何安全地使用它，如果不按照建议去做的话会有什么后果，如果意外发生了该怎么办，如何辨别危险物质过度泄漏的征兆，还有如果这样的事件发生了该怎么办。

保险商实验所公司

保险商实验所公司（Underwriters Laboratories, Inc., UL）是一个独立的、非营利的产品安全性测试和认证组织。UL为公共安全而测试产品已经超过一个世纪了。UL所关注的是安全性标准，但它已经把认证项目的范围扩展到了评估LAN双绞线的性能。评估的依据是IBM和TIA/EIA（电信工业协会/电子工业联合会）的性能规范，还有美国国家用电规程（NEC）的安全规范。UL还建立了一个项目来为屏蔽和非屏蔽局域网双绞线作评价，这应该可以简化确保用于安装工程的材料达到指标这一复杂的工作。UL的列表还指示了应该对线缆进行初始和周期性测试，以确保线缆一直符合标准。

注意：要想获得关于保险商实验所公司的更多信息，请访问www.ul.com。

UL对线缆的样本进行测试和评估，按照UL的列表进行评级，然后再进行重复的测试和检查。这种独立和坚持到底的测试使UL成为了购买者的重要参考标志。

UL的LAN认证项目不但代表了安全性，还代表了高性能。获得UL认证的公司会把UL的评级记号印在它们的线缆的外层封套上（例如Level I，LVL I或LEV I）。

美国国家用电规程

*美国国家用电规程（NEC）*的目的是保护人员和财物免遭用电过程中引起的危险。该规程是在*美国国家标准化组织（ANSI）*的资助下，由*美国国家防火协会（NFPA）*倡议的。该协议每三年修订一次。

注意：要想获得关于美国国家防火协会（NFPA）的更多信息，请访问www.nfpa.org/Home/index.asp。

好几个组织（包括UL）都建立了用于建筑物内网络布线的防火防尘标准，然而地方执照和检查机关最广泛支持的是NEC所包含的标准。

NEC类型代码

NEC类型代码列出在线缆和补充物品的目录中。这些代码把特定用途的产品归到特定的目录下，如表A-1所示。

表A-1　NEC线缆类型代码

线缆类型	描述
OFC（光导纤维）	含有用于增加强度的金属导体
OFN（光导纤维）	不含金属
CMP（天花板隔层通信电缆）	通过了暴露于有限度蔓延火焰和低浓度烟雾中的测试。天花板隔层通信电缆通常都具有以特殊材料（比如特氟纶）制成的外套。代码里面的“P”定义了一种用于处理空气的，类似于通道或管道系统的通风送气系统
CMR（垂直通信线缆）	“R”表示该线缆通过了与CMP类似的暴露于有限度火焰和低浓度烟雾中的测试，但这种测试与CMP的测试又稍有不同。比如它主要测试垂直电缆在垂直位置的燃烧性质。根据规程，在使用穿过地板和天花板的线缆时，必须使用经评定可用于垂直用途的电缆。垂直电缆通常都有聚氯乙烯（PVC）外套

通常内部网络线缆会以CM类（代表“通信”）或MP类（代表“多用途”）列在分类目录里。有些公司会选择安装那些经过了远程控制测试，或CL2、CL3（2类或3类）限制功率（power-limited）电路线缆测试的电缆，而不是通过了CM或CP测试的电缆。但在所有的测试中，火焰和烟雾标准通常都是相同的。这些测试标准的不同之处在于：在最坏的情况下，可以通过线缆的电量。MP电缆能通过最高电量处理能力的测试，而CM、CL3和CL2能通过的电量处理能力的测试等级则逐渐降低。

A.4.2　带电操作的安全性

除了要对工业安全组织有所了解之外，线缆安装工人还应该学习一些基本的安全条例。因为每天的工作都会用到这些安全条例，而且它们对于课程实验来说也是必需的。由于安装电缆时会存在很多危险，所以安装工人应该对所有的情况都有所准备，以避免事故或伤害的发生。

高压电

线缆安装工人使用的线缆是为低压电系统设计的。加到一条数据线缆里的电压对大多数人来说都几乎感觉不到。然而，插数据线缆的网络设备的电压可以是100到240V（北美地区）。如果电路出现故障，使高压电变得可以触及，那么它可能会使安装工人受到危险的电击——而且这种电击可能是致命的。另外，低压电安装工人由于不小心剥掉高压电导线的绝缘外套而触电也不是没有听说过的。

不要因为大多数的工作都与低压电有关，就不关心附近的高压电线的危险。如果有人突然接触到高压电，那么他/她就很难控制自己的肌肉，或者没有能力脱身。

闪电和高压电的危险

高压电并不只是来自于电力线，闪电也是高压电的另一个来源。由于闪电是致命的，而且会对网络设备造成损害，所以必须小心防止它进入网络线缆。必须实施以下的防范措施以防人员或网络设备受到闪电和电线短路的伤害：

- 所有室外线缆都必须在它们进入建筑物的那一点（称为入口点）配备合适的接地和已注册的信号电路保护装置；必须依照当地电话公司的要求及相应的规程来安装这些保护装置。不应该使用未经授权的电话线。如果已经获得授权，不要移除或更改电话线路的保护装置或接地线路。
- 绝对不能在没有合适保护措施的建筑之间铺设线缆。事实上，在建筑物之间使用光纤的最大好处或许就是它能避免闪电的影响。
- 避免在潮湿的地方，或靠近潮湿的地方进行布线。
- 绝对不能在雷暴其间进行铜线的安装或连接。没有正确保护的铜线可以把致命的闪电浪涌传输很远的一段距离。

高压电安全性测试

电压是不可见的，但是它的影响可以从使用它的工具、操作它的设备或遭电击导致的不愉快经历中看出来。

在使用任何插上电源的设备时，最安全的操作应该是：在接触它们之前，先检查一下它们表面和各部分的电压。在开始工作前，用确定可靠的电压测量设备（比如*万用表*或者检电器）做一下电压的测量。在重新开始工作前（无论是第二天还是休息了片刻之后）要重新进行测量，因为可能别人会作了某些改动。当工作完成后，重新进行一次测量。

某些形式的电是无法预见的，例如闪电和静电。永远不要在雷暴期间进行铜线的安装或连接，因为铜线可以把闪电浪涌传输很远的一段距离。当有外部线缆在建筑物间或地下延伸的时候，这会是一个很显著的问题。因此，要为所有的外部线缆安装合适的接地或被认可的信号电路保护装置。这些保护装置的安装必须依照当地的规程进行。而在多数情况下，这些规程会与国家规程统一。

接地

接地是指为电流提供一条直接与地面相连的通路。设备设计者故意使设备与外壳在电路安装部分绝缘，因为任何从设备内部泄露到外壳的电压都不应该停留在外壳上。接地装置会把所有游离的电压传导到地面，并且不会让设备受到损害。如果没有与地面连接的合适通路，游离的电压会利用另外的通路（比如人的身体）到达地面。

接地电极是一根金属棒，它埋在靠近建筑物入口点（也就是电流进入建筑物的地方）的地下。而接地系统与地面连接的方法则通常是另一回事了。多年以来，从地下自来水总管进入建筑物内部的冷水管被认为是非常好的接地。把大型的建筑构件（比如工字钢和横梁）作为接地也是可以接受的。虽然这些可以为接地提供足够的通路，但现在多数的地方规程都要求有一个专门的接地系统，比如连接着设备和接地电极的接地导体。

要对实验室和工作点的接地系统有所了解。核实一下真正起作用的接地系统。有时可以发现，接地系统被错误地安装了，又或者根本没有安装，而这样的情况并不少见。一种更常见的情形是，安装工人采取了一些捷径，完成了技术上可行，但事实上却不符合标准的接地工作。随后网络其他部分的改动，或者建筑物本身的改动或许会破坏或除去这套非标准的接地系统，从而使设备和人员处于危险之中。

连接

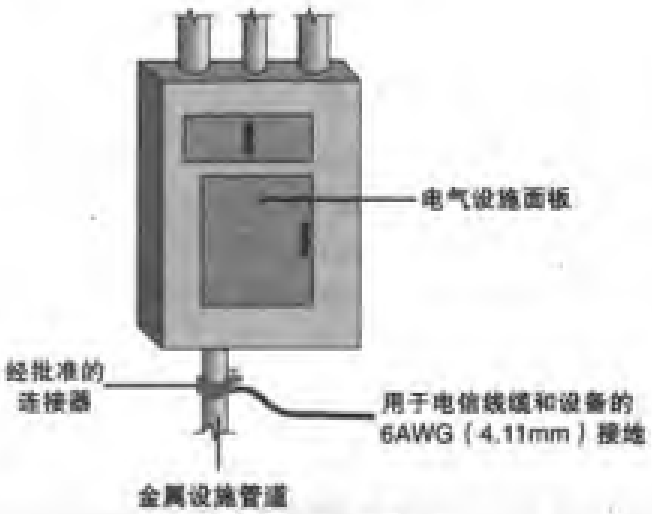
连接是提供一种方法使不同类型的线缆支架与接地系统互连（如图A-16所示）。可以认为它是接地系统的延伸。一台设备（比如交换机或路由器）可能有一块连接板，这块连接板处于设备箱和接地电路之间，以保证有一个好的连接。

正确安装的连接和接地可以实现以下几点：

- 最小化电涌（尖峰）的影响。
- 维持电气接地设备的完整性。
- 提供一条更安全和更有效的接地通路。

电信连接通常用于以下几个方面：

- 入口设施。
- 设备间。



图A-16 连接

• 电信间。

接地和连接的标准

国家电气规程里包含了很多关于接地和连接的信息。TIA/EIA标准里与接地和连接有关的部分——TIA/EIA-607-A（“用于电信的商业建筑接地与连接要求”）把接地和连接扩展到了电信结构化布线系统里。TIA/EIA-607-A制定了建筑物接地系统与电信设备接地配置之间的精确接口点。它支持一个多厂商、多产品的环境。该环境适用于那些可能会被安装在用户前端的不同系统的接地操作。它也指定了在建筑物中用于支持设备的必需的接地和连接配置。

A.5 实验室和工作区的安全性操作

虽然线缆安装通常是一项安全的职业，但是仍然存在很多受伤害的可能。很多伤害都是由接触游离的电压来源造成的。这些游离的电压来源被称为外来电压，比如闪电、静电或其他由于安装失误或网络电缆上的感应电流造成的电压。

在墙壁、天花板或阁楼工作时，第一件要做的事应该是切断所有可能会经过工作区的电路的电源。如果不清楚哪些电线会经过工作区，可以遵循一条很好的规则——切断所有的电源。另外，永远不要接触电力线缆。因为即使该区域的所有电源都被切断了，也无法知道是否有电路仍在通电。

大多数国家都有一个或多个机构专门负责制定和管理安全标准。其中有些机构是为了保证公共安全，其他则是为了保护工人。那些保护工人的机构的管理范围通常包括实验室安全、普通工作场所安全、与环境规则保持一致，还有危险性废物的处理。

A.5.1 工作区安全性

以下是一些使工作区保持安全的指导方针：

• 在开始工作前，了解区域内所有灭火器所在的位置。如果不能快速找到灭火器的位置，那么一次小型的可扑灭的火灾可能会变得失去控制。

• 一定要预先找到当地的规程。某些建筑规程可能会禁止在某些区域（比如防火墙或天花板）钻孔。施工点的管理员或设备工程师可以帮忙确定哪些区域是禁止施工的。

• 在楼层之间安装线缆的时候要使用专门的垂直线缆。垂直线缆外有一层起阻燃作用的氟化乙丙烯（FEP）橡胶外套，因而可以防止火焰通过线缆从一层楼蔓延到另一层楼。

• 室外线缆通常都有一层聚乙烯外套。聚乙烯很容易燃烧，并且会放出有毒气体。因此NEC规定聚乙烯入口线缆不能进入建筑物内部超过15m（大概49英尺）。如果需要更长的距离，那么线缆必须装在金属导管里。

• 咨询建筑物的维护工程师，查明工作区内是否有石棉、铅或多氯联苯（PCB）。如果有的话，按照政府的规定去处理这些物质。这些物质由于某些原因被称为危险物质。不应该有任何人由于在这些区域内不受保护地工作而使健康遭到威胁。

• 最后，如果线缆必须经过空气流通区域的话，一定要用防火型（耐热阻燃型）的线缆。最常用的隔热阻燃型线缆是以特氟纶（Teflon）或海拉尔（Halar）为外套的线缆。隔热阻燃型线缆燃烧的时候不会像以聚氯乙烯（PVC）为外套的普通线缆那样放出有毒气体。

A.5.2 梯子的安全性

梯子有很多种不同的尺寸和形状，用于很多特定的用途。它们可以由木、铝或玻璃纤维制成，并被设计用于轻型或工业用途。最常见的两种梯子是直梯和活梯。无论是使用哪种类型，都要确保

梯子上有标签证明它符合美国国家标准协会（ANSI）和美国保险商实验室（UL）的有关规定。

• 为工作选择合适的梯子。要确保梯子足够长，工作起来足够舒适，而且足够坚固，能承受多次重复使用。玻璃纤维梯子是线缆安装中最常用的梯子。虽然铝梯更轻，但铝梯不够坚固，而且绝对不能带电操作。如果在靠近电气设备的地方工作，只能选用玻璃纤维梯子。

• 首先检查一下梯子。任何梯子都有可能存在致使它变得不安全的问题。检查一下梯子是否有松动，横档、踏板、扶手或支架有没有损坏。确保活梯的支杆能固定在适当的位置，另外梯子要有安全的梯脚，因为梯脚可以提供更好的稳定性，并减少工作中梯子滑动的可能性。千万不要使用有缺陷的梯子。

• 活梯应该完全打开，铰链也要锁定。直梯应该以4:1的比率放置。也就是说，从支撑点算起，一直到梯子的顶端，高度每增加1m（3英尺），梯子底部离墙或其他垂直表面的距离就应该增加0.25m（10英寸）。如果可能的话，确保直梯与支撑点尽量靠近，以免梯子移位。梯子应该始终放置在坚固水平的表面上。

• 切勿爬得高于活梯的第二块踏板，或直梯的第三块踏板（从梯顶往下数）。

• 用警戒线隔离工作区域，并配以合适的标记，比如锥形交通路标或警告带。贴上标记可以使人们知道梯子的存在。锁上或阻塞所有附近的门，以免在门打开的时候向梯子方向摆动。

A.5.3 光纤的安全性

由于光缆含有玻璃，所以对它采取适当的防范措施是很重要的。光纤碎屑非常锋利，必须妥善处理。就像其他玻璃产品一样，光纤破裂了会断成或碎裂成细小的长条。这些长条会扎进皮肤里。所以操作光纤时必须遵循以下的规则，以免受到伤害：

• 一定要戴上侧面有保护物的防护眼镜。

• 在桌面上放一块垫子或一块胶布，使所有落下的玻璃碎片都更容易看到。

• 操作光纤系统的时候不要碰眼睛，除非双手已经彻底干净。类似地，不要触摸隐形眼镜，除非双手已经彻底洗净。

• 把所有切割完后的光纤碎片放到安全的地方并进行妥当的处理。

• 如果光纤碎片粘到衣服上，用胶布或者胶带把它除去。用胶带除去手指和手上的碎片。

• 不要在工作区进食或喝饮料。

• 不要直接对着光缆的末端看。某些光纤里传输的光线可以对眼睛造成永久的伤害。

A.5.4 灭火器的使用

切勿在不知道如何使用灭火器之前就尝试去灭火。一定要预先阅读灭火器的使用说明书并检查阀门。在美国，条例规定用于商业建筑的灭火器必须定期检查，如果它们不是处于正常状态的话就要替换掉。

注意：如果有人身上着火了，记住一个技巧："停、跌、滚"：

• 停下，不要跑动。身上着火了的人跑动的话，火会快速蔓延。如果身上着火了的人由于惊慌失措而跑动，要把那人捉住。

• 跌倒在地上。在地板上滚动，以便熄灭火焰。

灭火器上会有标签说明它适合扑灭哪种类型的火灾。在美国，这被称为分级。在美国，火灾可以被划分成四种类型：

• A类火灾是指由普通物质（比如烧着的纸张、木材、纸版或塑料等）引起的火灾。

• B类火灾是指由可燃或易燃液体（比如汽油、煤油或实验室使用的普通有机溶剂）引起的火灾。

• C类火灾是指由带电设备（比如仪表、开关、配电箱、电动工具、轻便电炉和其他大多数电器设备）引起的火灾。在扑灭C类火灾的时候绝对不能用水，因为这样会很容易触电。

• D类火灾是指易燃金属（比如镁、钛、钾和钠）引起的火灾。这些物质燃烧温度很高，并且会与水、空气和其他化学物质发生剧烈的反应。

A.5.5　个人安全设施

在进入工作区安全地工作前先做好决定。具有安全工作态度包括选择合适的工作服。穿上保护服或保护装备可以防止受伤，或者减轻受伤害的程度。比如，在使用电动工具进行工作的时候，避免飞溅的碎片进入眼睛和震耳欲聋的噪音伤害耳朵是非常重要的。如果没有使用护目镜和耳塞，视力或听力有可能会受到永久的伤害。

工作服

长裤和长袖衣服可以保护手臂和双腿，使其免遭划伤、擦伤和其他危险。避免穿着过于宽松或宽大的衣服，因为它们有可能会碰到突出的物体，或被电动工具扯住。工作时穿上大小合适的鞋子。而且鞋子应该是耐用和全封闭的。它们应该能保护脚底，避免脚底被地上的尖锐物扎伤。如果工作时周围有钉子、金属碎片和其他可以刺破普通运动鞋鞋底的物质，那么最好穿上厚底鞋。脚趾部分镶嵌了钢铁的鞋可以使脚趾避免被落下的重物压伤。另外要确保鞋底有纹路，这样可以避免滑倒。

眼睛的保护

保护眼睛要比治疗眼睛容易得多，因此当切割、钻孔、锯切或在槽隙里工作的时候一定要戴上防护眼镜（如图A-17所示）。在为某些线缆进行端接的过程中，随着材料的切割、准备和丢弃，小颗粒很容易在空气里漂浮。在操作光纤的时候，玻璃纤维、粘合剂和溶剂有可能会接触到眼睛。另外，小颗粒或化学物品可能会粘到手上，并由于用手擦眼睛而意外地进入眼睛。因此，护目镜也保护了眼睛免遭双手的污染。在槽隙里或吊顶天花板上工作的时候戴上护目镜是一个很好的主意。如果上方有东西落下，双眼就可以受到保护了。很多施工现场都要求工作人员始终戴上护目镜。



图A-17　对眼睛的保护

在所有的实验室里都应该戴上眼睛保护装置。在进行任何实验操作前，记得回顾一下安全指示和所需的安全设备。

安全帽的使用

就像其他安全设备一样，安全帽可以使使用者免遭伤害。施工现场可能会要求工作人员戴上安全帽，特别是那些建筑施工现场。很多雇主都会提供安全帽，也有一些雇主要求安装工人自己去买。雇主提供的安全帽可能会有公司的特别颜色，或者配备公司的标志，以便标识佩戴者所属的组织。即使安全帽是自己买回来的，而且把它用于个人用途，那也不要在还没获得雇主同意的情况下装饰它。另外，OSHA（职业安全与健康管理局）不允许在安全帽上贴标签，因为这样有可能会掩盖安全帽上的裂痕。

要周期性地对安全帽上的裂痕进行检查。破裂了的安全帽可能保护不了头部的安全。由于安全帽需要提供有效的保护，所以必须对它们进行适当调整。花点时间去调整一下安全帽内部的带子，确保它能正常发挥作用。另外，确保安全帽能贴紧头部并保持舒适。在梯子顶端或新建好的环境下工作的时候，安全帽是必需的。

A.6 行业工具

与其他行业一样，结构化布线行业所用的工具能使困难的工作变得简单，使普通的成果变得突出显著。学员应该对低压电线缆安装工人所使用的几种工具有实际操作经验，以便能获得专业的效果。

学员应该精通以下工具的使用：

- 剥线和剪线工具。
- 端接工具。
- 诊断工具。
- 安装维护工具。

A.6.1 剥线和剪线工具

剥线工具用于把线缆的外套和绝缘层切开。泛达（Panduit）牌UTP剥线工具（如图A-18所示）用于把四对线组成的线缆的外套除去，它也可以用于大部分的同轴电缆。该工具的特点是，它可以调整切割刀片的位置以适应不同线缆外套的厚度。只需要把线缆插进去，然后把剥线工具一扭就行了。刀片只会切开外层胶套，使安装工人很容易就能把外层胶套从线缆上扯开，从而露出里面的双绞线。



图A-18 泛达（Panduit）牌UTP剥线工具

电工剪刀和线缆刀套件（如图A-19所示）同样可以用于除去线缆的外套。小刀用于除去大型线缆（比如那些从电话公司或ISP那里进入建筑物的线缆）的外套。这种小刀非常锋利，所以使用的时候要特别小心。建议使用时戴上手套，因为这样可以防止小刀滑落时把手弄伤。剪刀可以用于切断线缆、除去小型线缆的外套和导线的绝缘层。这种剪刀的特点是，在刀片的背面有两种尺寸的凹口（图中并没有显示出来），这使它可以剥去22到26口径线缆的绝缘层。

A.6.2 端接工具

端接工具用于切割和端接特定类型的线缆。多线对端接工具（如图A-20所示）用于端接和切割UTP线缆并固定接线板。这种工具的特点是，根据人体工程学设计的把手可以减轻修整线缆或把接线板固定在配线基座上时的疲劳。另外，它还有以下的特点：

- 可以同时端接五对线缆。
- 既可以端接连接块的电缆端也可以端接连接块的交叉连接端。
- 可以替换切割刀片。
- 可以用于切割和非切割（noncut）位置。



图A-19 电工剪刀和线缆刀

• 在进行端接时能清晰显示“CUT”记号以便能按正确的方向操作。

• 含有可靠的冲压机械装置。

• 具有根据人体工程学设计的橡胶把手，该把手的边缘有棱纹，可以防滑。

冲压打线工具（如图A-21所示）的刀片是可以替换的，所以它可以用66型或110型部件对线缆进行端接。与多线对端接工具不同的是，该工具一次只能端接一条线。它上面的可替换刀片的其中一边具有打孔和剪线功能，而另一边只有打孔功能。



图A-20　泛达（Panduit）牌多线对冲压工具



图A-21　泛达（Panduit）牌冲压工具

实验活动　工具的用法和安全性

本实验中，你将会学习到用于线缆安装的工具的识别、检查和使用。

A.6.3　诊断工具

有时需要接触电信插口或插座中个别的线缆。组合适配器，或“班卓”（banjo），被用于提供对这些线缆的接触（如图A-22所示）。只需要把一条普通的绳索插进适配器并插到插座里面就行了。这样技术员就可以在不拆开插座的前提下用欧姆表或其他测试工具进行测试了。班卓有三对（three-pair）和四对（four-pair）两种。



图A-22　组合适配器（班卓）

如果要定位金属管、木螺栓或横梁，或者其他藏于墙后或地板下的设施，可以使用本质或金属探测器。探测应该在所有布线项目的钻孔工作开展之前进行。一个深层扫描金属探测器可以找到金属螺栓、导管、钢管、电线、钢筋、电话线、电缆线路、钉子和其他金属物体。这种工具扫描非金属表面（比如混泥土、灰泥、木材或乙烯板壁）的时候通常可以深入15cm（大概6英寸）。另外，它可以鉴别30cm（大概12英寸）深的管道或钢筋的位置和深度。

另一种探测器是螺栓探测器（如图A-23所示）。这种探测器用于定位墙壁后面的木螺栓和横梁。这种工具能帮助安装工人对安装接口或配线管道时的最佳钻孔或锯切位置作出正确的判断。这种螺栓和横梁探测器也可以探测金属，它甚至可以找到深入水泥达100cm的钢筋。所有的探测模式都可以探测出交流电线并警告安装工人，以防钻孔或钉钉子时钻进或钉进带电导线里。



图A-23　螺栓探测器

A.6.4　安装维护工具

线缆安装工人会发现其他工具也是很有用的。测量轮可以用于估计线缆铺设的长度（如图A-24所示）。轮子的旁边装有计数器。安装工人只需按照线缆的预定路径滚动轮子就行了。当到达终点后，计数器会显示轮子所走的距离。

线缆安装工人还需要清洁施工现场的工具和材料。扫帚、簸箕和吸尘器可以使清洁过程变得迅

速。清洁是完成布线项目的最后几步之一，同时它也是很重要的一步。车间吸尘器可以用于工业或繁重的任务。

A.6.5 鱼状带

一种用于快速简便地从墙壁里取回线缆的设备是鱼状带（如图A-25所示）。鱼状带可以穿过墙壁和导管。把鱼状带放到某个适宜的中间点作为预定终点，把要拉出的线缆固定到鱼状带的末端。通过拉和绕取回鱼状带，这样线缆就会随着它出来了。



图A-24 测量轮



图A-25 鱼状带

对布线工作来说，玻璃纤维做的鱼状带要比钢铁做的好。另外，很多经验丰富的线缆安装工人在进行线缆牵引的时候，会连同一条细绳一起拉。这可以使随后的线缆牵引过程变得更方便。

A.6.6 线缆树

在施工的初始阶段，可以使用***线缆树***、千斤顶和滚轮来支撑线缆卷轴。它们可以使线缆的铺设更快捷、更容易，还可以使施工人员免于受伤。线缆树可以支撑许多小线缆卷轴（如图A-26所示）。这使线缆安装工人可以同时拉动多条线缆。由于所有的线缆都会在电信间终止，所以应该把线缆树放置在线缆的集结区域。一旦线缆被拉到插座所在的位置，就可以剪断线缆处于卷轴的那一端，并把它拉到电信间里面。



图A-26 线缆树

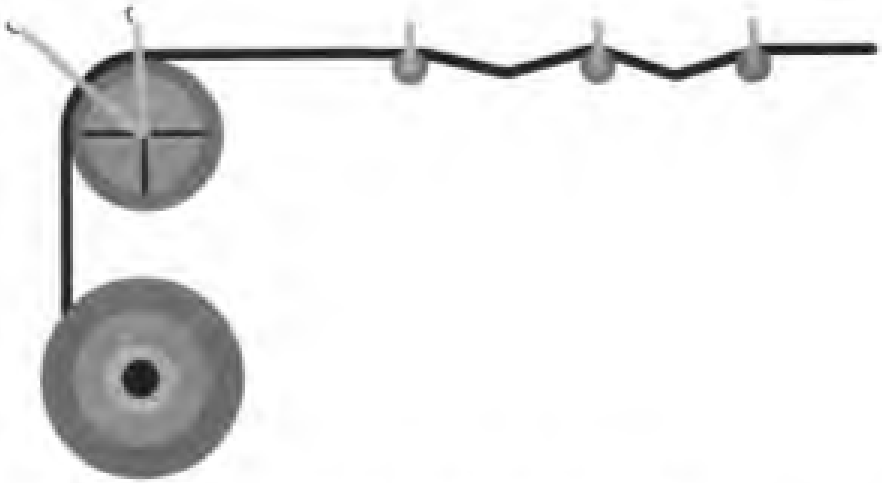
线缆千斤顶和卷轴滚轮用于支撑那些缠绕了骨干线缆的大型卷轴。由于大型卷轴通常都又大又重，所以很难用手提起它们，而线缆千斤顶有杠杆装置，从而使两个人就可以升起卷轴。当卷轴升起后，千斤顶使卷轴可以在拉线过程中自由而安全地转动。滚轮由两部分组成，每一部分支撑卷轴的一边。滚轮安装在轴承上，使卷轴很容易转动。当从卷轴滚轮上拉线的时候，通常要有一个安装工人站在卷轴旁帮助卷轴的滚动。

A.6.7　大导轮

大导轮通常专门用于在线缆铺设路径的开始和结束处帮助线缆拐弯，但它也可以用于在电缆铺设的中心点使线缆偏移和转向。大导轮是一个大直径的滑轮，它被用于线缆的机械牵引过程。大导轮很少会用于那些用手来牵引线缆的场合。大导轮通常由铝制成，直径最少0.3m（大概1英尺），而且它的构架只支持某些型号的轴承。大导轮与滑轮的不同之处在于，它通常有两个作为附加装置的锁扣，使它可以固定在某一点。另外，可以把大导轮从构架里拆下来，以便使它可以从线缆的中间位置放进线缆的铺设路径里。

A.6.8　滑轮

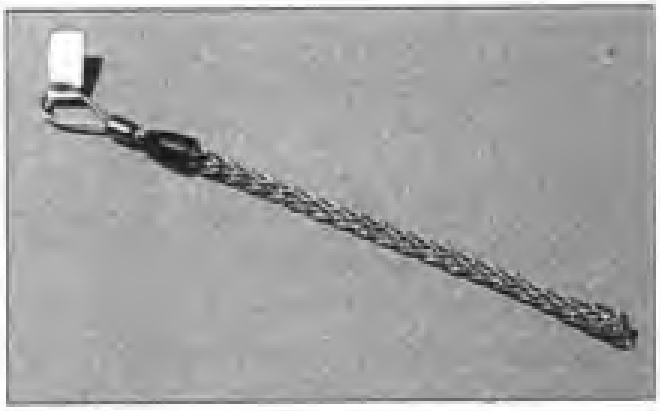
滑轮被用于长距离开放线缆的铺设中。它可以支撑线缆，防止它们由于在地上拖曳而使护套受损。滑轮也被用于一些可能会由于线缆牵引而受损的表面。滑轮用于直线线缆的铺设，它可以支撑线缆的重量并减少摩擦。滑轮也可以帮助对线缆铺设做少量的偏移（如图A-27所示）。在用手、拉出器或绞车进行线缆牵引的时候都可以使用滑轮。但如果线缆沿铺设方向转弯的角度超过45°的话就需要用大导轮了。滑轮既可以用于多网络线缆的铺设，也可以用于沉重的骨干线缆的铺设。虽然进行网络线缆铺设的时候可以用轻型滑轮，但是铺设骨干线缆的时候就应该用重型滑轮了。骨干线缆滑轮有大型的构架，而且滑轮的轮子直径也很粗。



图A-27　使用大导轮和滑轮进行线缆牵引

A.6.9　线缆套或Kellem夹具

线缆套或Kellem夹具可以附在线缆的末端，那么牵引绳就可以绑在线缆的末端了（如图A-28所示）。夹具沿着线缆的末端滑动，上面要结实地缠上优质的乙烯绝缘带，而且最少要缠15cm（大概6英寸）。由于在线缆上施加了压力，夹具拖曳的时候可以把线缆的护套夹得更紧。这些夹具只能用于单一的线缆，它们通常不能用于一束网络分布线缆。这些夹具有很多不同的尺寸，以适合不同尺寸的线缆。



图A-28　线缆套或Kellem夹具

当接触不到线缆末端的时候，Kellem夹具可以一分为二使用。这被用于牵引线缆中部额外松弛的部分。拆分的夹具也用于支持大型骨干线缆的垂直线缆安装——也就是说当线缆在楼层之间牵引的时候。打开夹具，使它环绕线缆，然后就可以把夹具缚在线缆上了。另外还需要用一条特别的棒穿过线缆套来紧紧线缆。

A.7 安装过程

安装过程包含了很多安装的要素，它从施工的初始阶段，即线缆刚被牵引到适当位置的时候开始。在安装过程中，垂直线缆会被加工，在火焰通过防火级墙壁时所用到的挡火物也一样；铜线的终端会被包裹住，而墙壁适配器和其他固定装置也一样。

将会讨论到的话题包括以下这些：

- 初始（rough-in）阶段。
- 垂直线缆的安装。
- 挡火物。
- 铜介质的端接。
- 修整（trimout）阶段。

四个阶段涵盖了布线项目的各个方面：初始、删除、完成和用户支持。各个阶段的特点如下：

- **初始阶段**——在初始阶段，所有的线缆都被安装到天花板、墙壁、地板管道和垂直管道中。
- **修整阶段**——这个阶段的主要任务是线缆的管理和端接。
- **完成阶段**——完成阶段的主要任务是对线缆进行测试、排错和认证。
- **用户支持阶段**——项目的最后阶段集中在使用户觉得满意上。在这个阶段，会与用户一起进行网络的试运行，然后用户会提供正式的测试报告和其他文档，比如楼宇建成后的修订图则。如果用户对工程项目满意的话，就可以签收了。随后，如果布线出现问题的话，布线公司会对用户提供长期的支持。

A.7.1 初始阶段

初始阶段中的任务是从一个被称为集结区域的工作区中把线缆牵引到各个房间或工作区。集结区域通常就在电信间的外面。每一条线缆的两端都要贴上标签以便辨认。在工作区里，一定要牵引足够数量的线缆，以便有大量的线缆可以用于端接。如果线缆铺设在墙壁里，那么应该把它的两端拉出来，以便下一个阶段的端接工作。

在多数情况下，新的建筑环境并没有改建项目那么具有挑战性，因为前者里面没有那么多障碍物。在这样的环境里通常都不需要什么特别的规划，因为建筑都能支持线缆的铺设，而且各种终端也通常能按照需要去设立。然而，与施工现场的其他行业配合是很重要的。其他工人必须知道数据线缆的位置，以免他们对新安装的线缆造成损害。

集结区域是线缆安装操作的起点。这个区域通常都位于电信间附近，也就是每一条线缆的其中一端所在的位置。在线缆牵引阶段，正确的设备安装可以节省时间。不同类型的线缆铺设需要不同的安装过程。网络分布线缆的铺设通常需要安装多个小型线缆卷轴。与此相反，骨干线缆的铺设则需要安装一个大型的线缆卷轴。



实验活动 线缆的识别

本实验中，你将会学习识别在CCNA 1和CCNA 2里所用到的不同类型的线缆。

水平线缆安装

水平线缆是指从HC（水平交叉连接）到工作区插口的那一段线缆。线缆可以是水平走向或垂直走向。在安装水平线缆的时候，遵循以下的原则是很重要的：

- 任何情况下线缆都应该平行于墙壁铺设。
- 绝对不应该使线缆以走对角线的形式穿过天花板。

- 在选择线缆所经过的路径时，应该选择最直接的路径，而且拐弯数量要尽可能少。
- 不要把线缆直接铺在天花板瓷砖的顶端。

骨干线缆安装好之后，必须安装水平网络分布线缆。网络分布线缆为用户和设备提供了来自骨干线缆的网络连接性。通常这种分布线缆是从工作站回到电信间，也就是与骨干线缆互连的地方。

管道中的水平线缆安装

在管道中安装水平线缆的步骤和过程与在敞开的天花板里安装线缆类似。安装过程中并不需要滑轮提供暂时的支持，因为管道本身可以做到这一点。虽然初始的设置都是一样的，但在管道中牵引线缆的时候还是要考虑一些特别的技术和因素。

首先，管道必须足够粗大，能容纳所有需要牵引的线缆。管道所容纳的线缆绝对不应该超过它最大容量的40%。可以通过建筑图表算出特定管道可以容纳的最大线缆数目或尺寸。其次，必须考虑线缆铺设的距离和管道中90°弯的数量。普遍的看法是，在没有引线盒的情况下，管道线缆铺设不应该超过30m（98英尺），而且90°弯的数量不应该超过2个。最后，大型线缆的牵引要求管道弯曲部分的半径要大。比如10cm（4英寸）管道的标准弯曲半径是60cm（24英寸）。但对于大型电信分布线缆（比如起码包含了400对线的线缆）来说，这是不够的。在进行这样的大型牵引时，起码需要90cm（35英寸）半径的管道。



图A-29　管道鼓风系统

有一种特制的真空吸尘器附件可以帮助完成线缆的牵引工作（如图A-29所示）。一种特别的泡沫橡皮发射物（有时被称为“老鼠”）可以被放到管道里，在它的后面绑着一条很轻的牵引绳。在发射物上涂上少量的普通家用清洁剂作润滑，高功率真空吸尘器（就像那些用于商业用途的吸尘器那样）就可以吸着发射物（后面绑着牵引绳）穿过整条需要铺设线缆的导管了。对于一些特别难铺设线缆的管道，可以在一端用吸尘器吹，另一端用吸尘器吸。当牵引绳到达管道的另一端之后，可以用它拉着牵索穿过管道。而牵索就从反方向拉着线缆穿过管道。

配线管道

配线管道是安装时容纳线缆的管道的统称。配线管道包括普通的电气管道、特制的线缆盘或梯架、楼内输送管系统，还有塑料或金属表面安装（surface-mounted）配线管道。表面安装配线管道用于没有隐藏的路径可以铺设线缆的场合（如图A-30所示）。塑料表面安装配线管道有很多种尺寸，这可以使它们容纳任意数量的线缆。而且它们比金属导管容易安装得多，



图A-30　配线管道

所以非常具有吸引力。

把线缆牵引到插座里

在线缆处于工作区的那一端，必须把线缆牵引到插座或者插口位置。如果从天花板到配线箱的导管是从墙壁后面经过的话，可以把鱼状带从导管的末端伸进配线箱，然后把导管往上推，直到它从敞开的天花板里冒出来。线缆可以直接附在鱼状带上，从天花板上牵引下来，并从配线箱里拉出来。

有些墙壁，比如用水泥和砖头堆砌的墙壁，显然不能让线缆从它们的后面经过。这时就需要用表面安装配线管道了。在线缆安装之前，应该按照制造商的建议把表面安装配线管道固定在墙上。当线缆从插口处牵引出来之后，线缆安装工人就可以回到电信间里完成最终的线缆牵引了。

固定线缆

初始阶段的最后一步工作是永久地把线缆固定。固定装置有很多种，比如J形钩和钩环带（hook and loop tie）。网络线缆绝对不能与电力线缆绑在一起。虽然这看起来好像是最实用的方法——特别是对单独的或一小束的线缆来说，但是这会破坏电信号的传输。另外，线缆也绝对不能与水管或洒水管绑在一起。



图A-31 泛达（Panduit）牌钩环带

由于高性能网络线缆有一个四倍于线缆直径的最小弯曲半径，因此应该选择一些支持该最小弯曲半径的固定装置（如图A-31所示）。固定装置之间的间隔可以由工作说明书指定。如果没有指定间隔，固定装置之间的距离不应该超过1.5m（4.9英尺）。

如果天花板里装有线缆盘或篮，那么就不需要永久固定装置了。

水平布线的预防措施

如果不注意的话，线缆的牵引有可能会对线缆的护套造成损害。把线缆压得太紧，或者在拐角处绑得太紧以致超过了弯曲半径都会使线缆传输数据的能力下降。驻守在牵引路径上的安装工人应该留意各种障碍和可能出问题的地方，以防线缆外套破损。

以下是一些在水平线缆牵引过程中需要做的预防措施：

- 线缆进入导管后，可能会在导管的末端被绊住或磨损。要用塑料导管防护装置或防护垫避免这种类型的护套磨损。
- 90° 弯周围的非常大的拉力会使线缆被压平——即使使用了大导轮和滑轮也没用。因此如果牵引压力太大，那就必须缩短牵引的距离，并且分阶段进行牵引。对于双绞线，牵引拉力不要超过25英尺/磅（约16.8m/kg）；对于光纤，牵引拉力不要超过50英尺/磅（约33.6m/kg）。
- 在使用线缆牵引器或绞车进行牵引的时候，保持牵引动作的平稳是很重要的。当牵引开始后，如果有可能，把牵引动作持续到结束为止。牵引中的停顿和开始会对线缆造成额外的压力。

A.7.2 在干式墙上安装插座

安全规则

无论什么时候，在墙壁、天花板或阁楼里工作时，首先要做的事情就是切断所有可能经过工作

区的电路的电源。如果不清楚哪些电线会经过你所工作的建筑物的那部分，可以遵守一条很好的规则——切断所有的电源。

警告：绝对不要碰触电力线缆。因为即使切断工作区内所有线路的电源，你也没有办法知道是否还有带电的线缆。

在开始工作前要了解区域内所有灭火器所在的位置。

穿上合适的衣服。长裤和长袖衣服有助于保护腿和手臂。不要穿过度宽松或宽大的衣服，因为这样会有可能挂住某些物体。

如果是在架空的天花板区域工作的话，要先调查一下整个区域。举起一些天花板瓷砖并周围看看。这个过程可以帮助你定位电气管道、通风管道、机械设备和其他随后有可能会引起问题的东西。

在切割和锯物体时，用护目镜保护眼睛。在槽隙里或架空的天花板上工作的时候，戴上护目镜也是一个很好的主意。如果有东西从高处或暗处落下，护目镜可以保护眼睛。

咨询建筑物维护工程师，查明工作区内是否有石棉、铅或多氯联苯（PCB）。如果有的话，按照政府的规定去处理这些物质。

使工作区保持整齐清洁。不要把工具放在容易绊倒人的地方。对于有延长绳的工具要使用警告牌。因为它们很容易使人绊倒。

注意：在墙壁、天花板或阁楼工作时，切断所有到达或经过该区域的线缆的电源是非常重要的。如果不清楚是否有电线经过该区域，可以遵循一条很好的规则：切断所有的电源。

在干式墙上安装RJ-45插座的时候，要遵循以下的步骤：

1. 在高于地板30-45cm（10-15英寸）的地方选择一个安装插座的位置。在所选的位置钻一个小孔。把一条线弯曲，伸进孔里，转一圈，看看孔后面有没有什么障碍物。如果线碰到了障碍物，你必须重新选择一个远离刚才那个孔的位置。然后重复以上过程，直到找到一个没有障碍物的位置为止。

2. 确定存放插座的盒子所需的开口的尺寸。描绘出包含了盒子或支架的模板轮廓。

3. 在凿开墙壁之前，用木匠的水平仪确保开口垂直。用实用刀把开口切开。在模板轮廓内，用刀插穿干式墙，直到开口足够容纳锌孔锯（keyhole saw）或干式墙锯的刀片为止。

4. 把锯插进孔里，沿着用铅笔划的轮廓锯。小心地一直沿着线锯，直到可以拔出干式墙的这一部分。另外，要确保盒子或支架的大小与开口符合。

如果使用盒子去平直地安装插座，不要把盒子固定，直到把线缆牵引到开口处为止。

A.7.3　在灰泥墙上安装插座

切开灰泥墙要比切开干式墙困难得多。为了达到最好的效果，要遵循以下的步骤：

1. 确定安装插座的合适位置。

2. 用锤子和凿子从墙上除去灰泥，以便让灰泥后面的板条露出来。

3. 用实用刀小心地把板条周围的灰泥削去。

4. 把模板贴紧板条，使其与三块板条重叠，并使它与开口的顶端和底端距离相等。沿着模板描绘出一个轮廓。从开口的中心用电锯锯开整块露出来的板条。

5. 在整块板条上锯几个小切口，先在一边锯，然后再到另一边。一直这样一点一点地锯，直到把中间的板条整个切出来。

通过除去板条顶端和底端那些需要除去的部分来完成开口的准备工作。垂直地切开孔的边缘，然后就像之前所做的那样，在一边切几个小的切口，然后再在另一边切。就这样一直切下去，直到

孔的顶端和底部的切口都平齐为止。然后，在底部那块板条处切一条曲线，方法是从右上角切到左下角。在曲线到达左下角之前，要使曲线回升，以便使它在刚好到达左下角的时候变平。当切口到达左下角时，除去那一部分可以自由掉下的板条。把锯子转向，沿着孔的底部齐平地锯，直到到达另一个角为止。这样剩下的那部分板条应该也可以自由掉下了。然后再在上部的板条上重复以上的过程。

> 注意：在进行这一步工作的时候要非常小心。如果先切完一边再切另一边，那么在切另一边的时候，锯子会使板条摇摆。这种摇摆会使开口附近的灰泥松动，从而使灰泥从板条上剥落。

A.7.4 在木材上安装插座

要在木材上平直地安装插座的话，必须遵循以下的步骤：

1. 选择一个想安装盒子的位置。如果要把RJ-45插座安装在护壁板上，不要在护壁板底部5cm（1.5英寸）的地方锯盒子的开口。

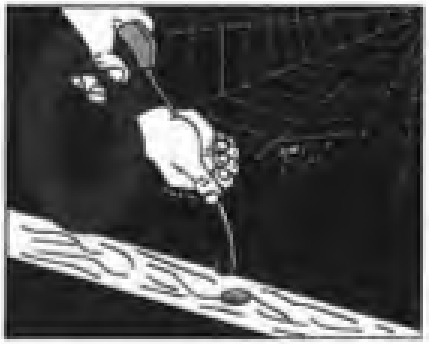
2. 把一个盒子当作模板，在它的外部描绘出轮廓。在轮廓的每一个角钻一个作为起始位置的孔。把铰孔锯或竖锯插进孔里，沿着轮廓锯下去，直到锯子到达下一个孔。把锯子转向，继续锯下去，直到可以把木块除去为止。

A.7.5 在墙壁上平直地安装插座

在准备好开口之后，就可以把插座安装到墙壁上了。如果是用盒子来安装插座的话，握住线缆，把它通过其中一条槽放进盒子里。然后，把盒子推进墙壁的开口里。用螺丝钉把盒子固定在墙壁的表面。在旋紧螺丝钉之后，盒子就可以紧贴在墙壁上了。如果要把插座安装在一个扁平的低压电安装支架（有时称为“墙板适配器”或“老式工作盒”）里，现在就把它安置进去。把支架贴紧墙壁的开口，光滑的一边朝外。把顶端和底部的凸缘向后压，以便使支架可以夹紧墙壁。然后把一边向上推，另一边向下推，以便把支架安装固定。

A.7.6 把线缆牵引到插座里

在线缆处于工作区的那一端，你必须把线缆牵引到插座或者插口的位置。如果导管在墙壁后面从天花板到达出线盒，你可以把一条鱼状带从出线盒伸进导管的末端，把它从导管里往上推，直到它从敞开的天花板里露出来。然后你可以把线缆直接绑在鱼状带上，把鱼状带从天花板上往下拉，最终把它从出线盒拉出来（如图A-32所示）。



图A-32 利用鱼状带把线缆牵引到插座去

如果导管是在墙壁里面的话，可以从墙壁后面牵线。首先，在干式墙需要安装插座的地方的钻一个孔。要小心的是，不要把孔钻得太大。在墙壁的顶板上再钻一个孔。这个孔的直径应该为1-2cm（0.37-0.39英寸）。把鱼状带从顶端的孔伸进去，从底端的孔抽出来。有些安装工人会用砝码和细线代替鱼状带。把砝码系在细线上，从顶端的孔慢慢放下，以防砝码意外地越过底端的孔。在底端的（插口）孔，安装工人可以用钩或衣架找到细线。

抓住鱼状带处于插口位置的那一端后，把牵引绳绑在上面。然后，从初始位置把鱼状带往回拉，把牵引绳拉出来，再把线缆绑在牵引绳上。最后，在插口位置把附有线缆的牵引绳往下拉。

有些墙壁，比如水泥或砖头堆砌成的墙壁，线缆显然不能从它们的后面走过。在这些墙壁上可

以使用表面安装配线管道。在线缆安装之前，应该按照制造商的建议把表面安装配线管道固定在墙上。当线缆从插口处牵引出来之后，就可以回到电信间里完成最终的线缆牵引了。

A.7.7　从墙壁底下把线缆“钓”出来

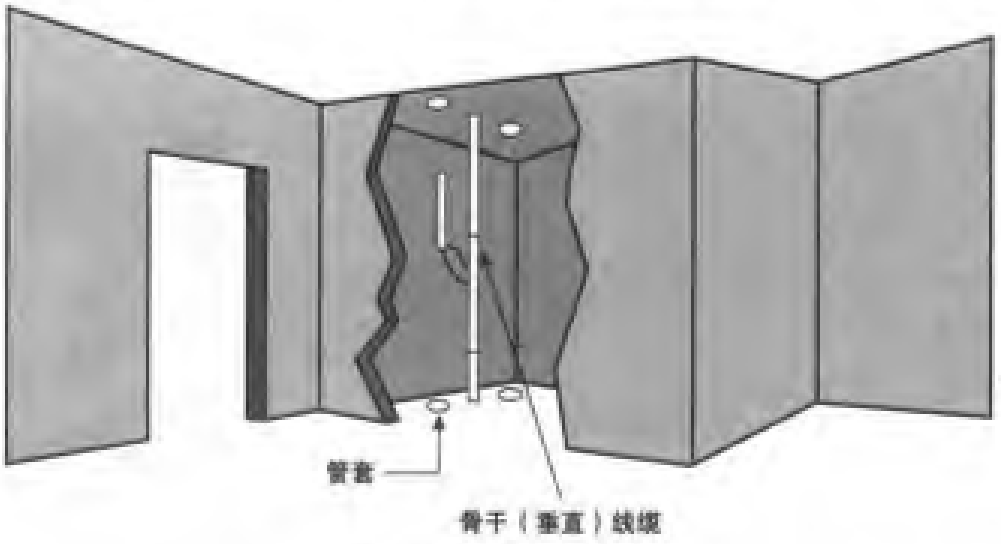
在有地下室的建筑物内铺设水平线缆的时候，要把线缆从地下室“钓”到首层的工作区里。依照以下的步骤完成这项工作：

1. 以一定的角度钻一个3.2mm（1/8英寸）的孔，使它穿过贴近护壁板的地板。
2. 把衣架或硬的线伸进孔里，以便在地下室里指示孔的位置。
3. 到地下室去，找到线缆。
4. 用卷尺在墙壁下面的区域做一个标记。这个标记与孔的距离应为57mm。
5. 在这个点上钻一个新的孔。这个孔的直径应为19mm。与第一个钻的有角度的孔不同，这个孔应该垂直地钻穿底层地板和承梁板。
6. 从第二个孔把线缆插进去，直到你想安装工作区插口的墙壁开口处。
7. 确保留出足够长度的线缆，以便使它可以到达地面，并继续延伸60-90cm（2-3英尺）。

A.7.8　垂直线缆的安装

线缆的垂直牵引要比水平牵引困难得多。垂直线缆的安装包括网络分布线缆和骨干线缆。虽然骨干线缆也可以水平牵引，但是还是把它们看成是垂直分布系统的一部分。而另一方面，网络分布线缆则是水平分布系统的一部分。

垂直安装通常在导管里完成——从导管套或线槽里穿过楼层。地板上的矩形开口被称为槽沟或管槽。天井是地板上一连串的洞，直径通常10cm（3.9英寸），而且很可能装上了导管套（如图A-33所示）。导管套可以在地板的上方和下方各突出10cm（3.9英寸）。另外，并非所有的天井都能重合得很好，有时它们会有偏移，所以应该在初始阶段前检查天井有否校正。



图A-33　典型的垂直线缆

垂直布线的安装要么从高层向低层进行，要么从底层向高层进行。在大多数情况下，从高层向低层牵引线缆会更容易——因为其中有重力的帮助，而且通常不需要诸如绞车或线缆拉出器之类的工具的帮助。但有时把大型的线轴抬到建筑物的高层不太可行，因此某些情况下必须把线缆从低层向上牵引。在向上牵引的时候，通常都不需要诸如绞车或线缆拉出器之类的工具，但需要一个卷轴制动器以防线缆自由下落。

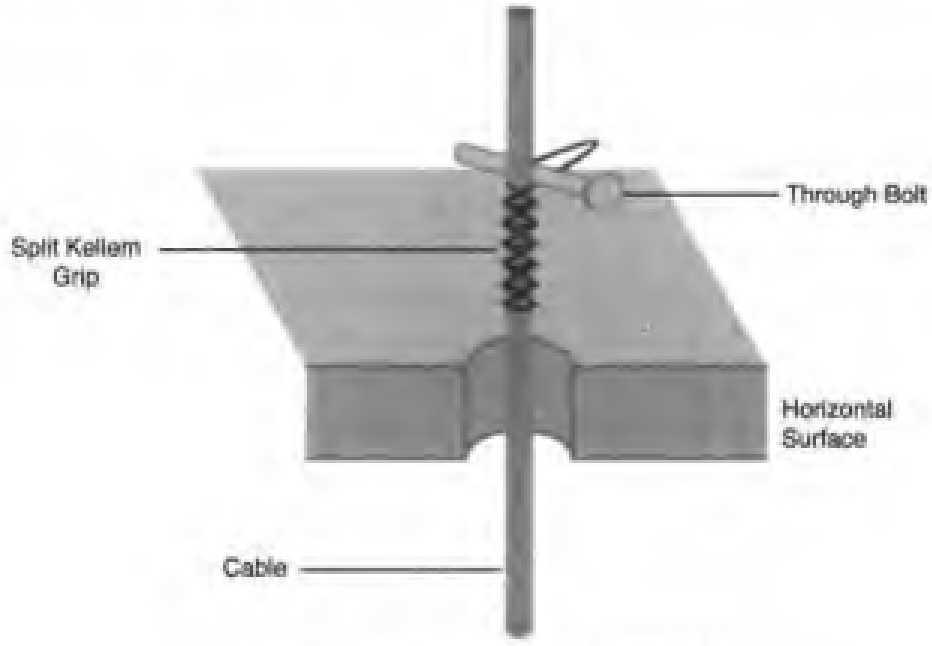
线缆绞车

垂直牵引工作中，下放线缆的时候要非常小心，免得线缆下放得太快以致失去控制。卷轴制动器的使用有助于提供额外的压力。升高线缆的时候，通常都会用到线缆绞车（如图A-34所示）。由于用于牵引线缆的装置可能会对线缆安装工人和旁观人员造成危险，所以在工作区域内只应该有线缆安装队的工作人员。用线缆绞车牵引大型线缆会对线缆造成巨大的压力。如果线缆突然断了，在工作区域内的人员有可能会受伤。那些富有经验的线缆安装工人知道不应该太靠近承受着巨大压力的线缆。



图A-34 绞盘

可以从工厂里定制安装有拉孔的线缆。拉孔对于大型或重型的牵引特别有用。如果办不到的话，可以用Kellem夹具代替。要再次强调的是，当牵引开始后，整个过程应该缓慢而稳定。如非绝对必要，千万不要中断牵引过程。当线缆被牵引到相应位置后，用牵引绳和绞盘控制住它，直到它被支撑系统、摩擦夹钳或带有螺钉的Kellem夹具永久地固定在楼层之间为止（如图A-35所示）。



图A-35 用穿透螺钉固定的分离Kellem夹具

固定垂直线缆

固定垂直线缆的其中一种方法是使用分离网孔线夹具（split wire-mesh grip），它类似于Kellem夹具，有一颗大的螺钉，长度在25到30cm（9.8到11.8英寸）之间。夹具尺寸与线缆束相符是很重要的。在绞盘或卷轴制动器支撑着线缆的时候，建筑物的每一层都安装着一个分离网孔线夹具，而螺钉则穿在夹具的环上。然后线缆会慢慢下放，直到它能被夹具支撑位置。这是一个永久安装的过程。

线缆安装技巧

以下是一些牵引线缆的技巧：

• 无论何时，只要有可能，集结区域应该靠近第一个90° 拐弯处。在线缆刚从线箱或卷轴里抽出来的那个拐弯处牵引线缆会比在线缆末端的那个拐弯处牵引线缆容易得多。这是因为安装工人必须牵引从他所在那一点算起直到集结区域的整段线缆的重量。

• 在进行长距离和困难的牵引时应该使用牵引润滑剂，以免线缆受损。

• 调整卷轴，使线缆从卷轴的顶端而不是底部牵引出来。

• 如果鱼状带卡在导管的拐弯处，要一面旋转鱼状带一面往前推。

• 牵引线缆的时候，在线缆上绑上一条额外的牵引绳。如果以后需要安装额外的线缆的话，这条牵引绳就可以派上用场了，因为它可以避免使鱼状带再次穿过这个场所。

• 如果必须盘绕地板上的线缆，以便为下一次牵引做准备的话，要把线缆盘绕成“8”字形，以免解缠绕的时候线缆缠在一起。在盘绕线缆的时候，要用两个安全圆锥（safety cone）甚至桶作为引导。

• 支撑垂直穿过多个楼层的线缆是一项挑战。在楼层间布上钢索或铁链，并在两端固定。然后垂直线缆就可以缠绕在作为支撑的钢索上了。

A.7.9　挡火物

线缆材料的选择和线缆的安装方法可以对火焰在建筑物内的移动、释放出的烟雾和气体的类型，还有烟雾和火焰的蔓延速度产生巨大的影响。在有需要的地方采用耐热阻燃线缆，线缆穿过防火墙时缺口应该尽量小，当必须穿透防火墙时使用合适的防火物。这些都可以减少和降低烟雾和火焰蔓延的速度。致人死亡的通常是烟雾而不是火焰。

防火墙

防火墙由特殊材料和技术制成，它可以防止烟雾和气体从一个区域蔓延到另一个区域。防火墙壁也可以限制火焰从火灾起源的区域蔓延到没有受到直接影响的区域。如果一个区域真的发生了火灾，防火级的墙壁可以减慢火焰向新的区域蔓延。这些措施可以避免建筑物里的居住者和消防员暴露在有毒的烟雾中，而且可以使他们有额外的时间撤出建筑物。

防火墙穿透

有时线缆必须穿过防火墙。这就要求有一个特殊的，被称为“穿透”（penetration）的开口（如图A-36所示）。

有几种建筑材料被用于建筑防火墙。其中最常用的可能是清水墙（drywall）或石棉水泥板（sheetrock）。在从地板到天花板都使用了防火材料后，每一层这样的材料可以抵挡火焰的蔓延大概半小时。两层重叠的材料可以提供双倍时间的保护。其他常见的防火墙材料包括混凝土块（concrete block）和浇注混凝土（poured concrete）。

当线缆要穿过防火墙时，必须先在防火墙上钻一个洞。这叫做穿透（penetration）。穿透可以从防火墙的各个方向进行，也可以只是穿透其中的一面，这种情况下的穿透被称为表层（membrane）穿透。



图A-36　典型的防火墙穿透

在钻好孔后，通常都会在穿透上加上管套，方法是把一小截的导管插进洞里。导管必须足够大，能够容纳所有的线缆，而且还要有额外的空间容纳日后增加的线缆。这根导管还必须在墙的两边各突出0.3m（11.3英寸）。这样线缆就可以穿过导管了。在线缆穿过导管后，必须使用被认可的防火材料密封好导管。这可以防止火灾通过防火墙的洞口从建筑物的一个部分蔓延到另一个部分。

如果要在已有的防火墙穿透上安装新的线缆，必须先去掉原来的防火材料，为新的线缆腾出空间。当新的线缆穿过防火墙后，空口和导管要用防火材料重新密封。

A.7.10 端接铜介质

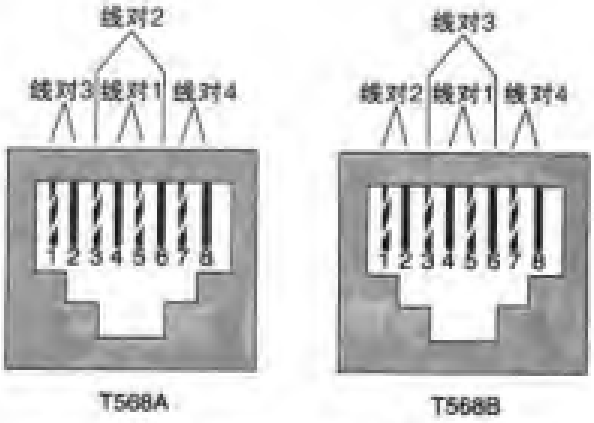
通信线缆上都有不同的颜色标记，以便识别。在北美地区，所有通信线缆的颜色标记方法都是相同的。颜色标记的使用可以确保识别单独线对时的一致性。每一对有颜色标记的线都与一个特别的数字有关。

四对线（four-pair）的颜色标记

大多数的语音和数据布线都使用UTP线缆。每一条UTP线缆里都有四对互相缠绕的导线。这四对线的颜色标记如下：

- **第1对**——白/蓝。
- **第2对**——白/橙。
- **第3对**——白/绿。
- **第4对**——白/棕。

第1对线一定是处于8引脚插座或插头的第4和第5个位置（或者说“引脚”）。第4对线一定是处于8引脚插座或插头的第7和第8个位置（或者说“引脚”）。其他线对会根据不同的标准（T568A或T568B）而处于不同的位置（如图A-37所示）。



图A-37 TIA/EIA T568A和T568B布线方案

布线方案一定要使用T568A或者T568B标准。绝对不应该再创造其他新的布线方案，因为每一条线都有它特定的用途。如果线的排列顺序不正确，两端的设备要不就无法通信，要不通信质量就会严重下降。

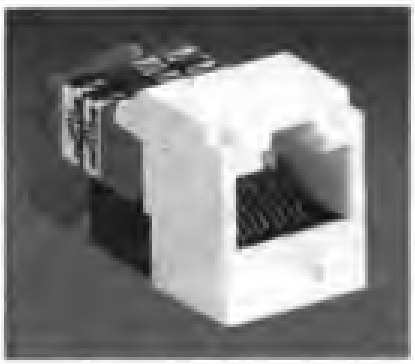
如果线缆的安装在新建的楼宇里进行的话，要根据合同的指示来决定是使用T568A还是T568B标准。如果标准的选择是由安装工人决定的话，可以使用区域内最普及的方案。如果建筑物内已经有布线系统的话，应该遵照已有布线系统的方案。记住，工程组里每一个安装工人都应该使用相同的布线方案。

可能偶尔会有人对线的编号和引脚的编号感到迷惑。一根引脚是插头或插座里的一个特定的位置。而涂了颜色的线对永远都是相同的。比如，第2对线永远都是白/橙线对。然而在一个RJ-45的插座里，第2对线会与第3和第6根引脚，又或者是与第1和第2根引脚相连，这要视所用的标准是T568A还是T568B而定。

RJ-45插头和插座

RJ-45插座是有8根导线的插座，RJ-45插头或者RJ-11插头可以插到它里面（如图A-38所示）。插座的排线应该遵循T568A或T568B标准。

RJ-45插头有8根引脚，可以容纳4对线。如同RJ-11插头和插座一样，第1对线一定端接在中间的引脚，即第4和第5根引脚上。第4对线（白/棕）一定端接在第7和第8根引脚上。第2和第3对线的端接位置会由于所用布线方案的不同而不同。如果用的是T568B，第2对线（白/橙）端接在第2和第3根引脚上。第3对线（白/绿）端接在第3和第6根引脚上。T568A的第2和第3对线的端接位置刚好反过来——第2对线端接在第3和第6根引脚上，而第3对线端接在第1和第2根引脚上。



图A-38　8P8C（RJ-45）插座

RJ-45插座可以端接水平线缆的一端。线缆的另一端通常端接在一个带有110型连接器或110型连接块的接线板上。

实验活动　超5类插座的端接

本实验中，你将会学习到使用布线工具的正确的安全步骤，而且也会学习到如何使用T568B标准把超5类线缆端接到一个模块化的接线板上的模块插座上。

110型模块

110型模块是高密度的端接模块，适用于语音和数据应用（如图A-39所示）。它的绝缘位移连接提供了一个低阻力的气密连接。110型模块有很多种配置类型。模块被设计为可以以多种组合形式来堆叠，以适应不同尺寸的要求。110型系统还包括线缆管理槽，这种槽可以作为模块的间隔装置。110型模块可以作为一个特别的多头冲压工具，利用它可以同时冲压多达5对线。然而，注意在含有印刷电路板的配线板上不要使用这种工具进行冲压，因为冲击力有可能会对内部的布线造成损害。



图A-39　110型模块

实验活动　把超5类线缆端接到110型模块上

本实验中，你将会学习到如何把超5类线缆端接到110型端接模块上，另外也会学习到110型冲压工具和110型多头冲压工具的正确使用方法。

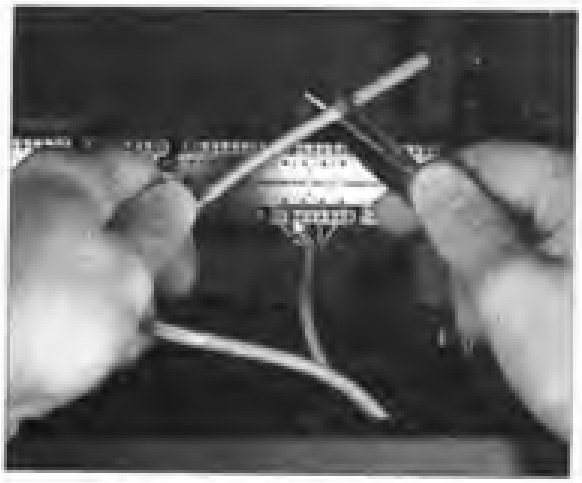
A.7.11　修整阶段

在线缆安装的初始阶段，线缆铺设的两端会留下额外的线缆。这些卷起来的线缆被称为维护绳圈（service loop），它们既可以使线缆不会松弛，也可以使以后的更改更容易。EIA/TIA标准并不鼓励使用维护绳圈。然而在初始阶段完成时，在墙边插座挂出1m（3英尺）的线缆终端并不少见。在有数百条线缆端接的电信间（TR）里，每条线缆留出2到3m（6到10英尺）的长度也很常见。

虽然这项措施看起来好像很浪费，但经验丰富的安装工人会知道，额外富余的线缆能为线缆铺设提供更多灵活性，也能在评定（测试）每一条线缆时都能更容易接触到它。缺乏经验的安装工人常犯的一个错误是把线缆剪得太短。记住，额外富余的线缆可以随时被剪短，但不够长度的线缆却没办法延长。如果一条线缆太短，唯一的解决办法就是使用另一条线缆，而这却是一个非常消耗人力和时间的解决办法。

如果从墙边插座位置伸出来的线缆有1m（3英尺）长，最好把伸出来的部分剪为大概25cm（9.8

英寸）。应该在一条新线缆从末端算起大概15cm（5.9英寸）的地方贴上标签。然后把外套剥开大概5到7cm（2到2.8英寸），把里面的双绞电线暴露出来。线缆端接完成后，剥去护套而暴露出来的导线长度不应该超过1.5cm（0.6英寸），而线缆解缠绕了的部分也不应该超过1.5cm（0.6英寸）。最终端接时，所有额外的导线都应该被剪掉（如图A-40所示）。



图A-40 把线缆剪到合适的长度

端接插座时，线缆从墙里伸出来的部分大概要留出15到20cm（6到8英寸）。在安装插座后，这些额外的线缆要小心地卷好并放到墙壁或暗线箱里。这些额外的线缆可以用于日后插座的重新端接，或者使去掉面板并在插口多加一个插座成为可能。在工作站的一端，插座里面的电线经常会接触不到引脚，因为连接到工作区的跳线经常会被工作站使用者拔出、踢中或拉紧。

端接或冲压

电信线缆在电信间一端的端接被称为冲压（punching down）。墙上的端接面板和交叉连接面板背后的线缆也需要被冲压。

把线缆插到端接面板的合适位置，然后把冲压工具放到线缆上。根据所使用的端接工具的类型，端接工具里的可替换刀片可以替换成适合的端接类型（如图A-41所示）。



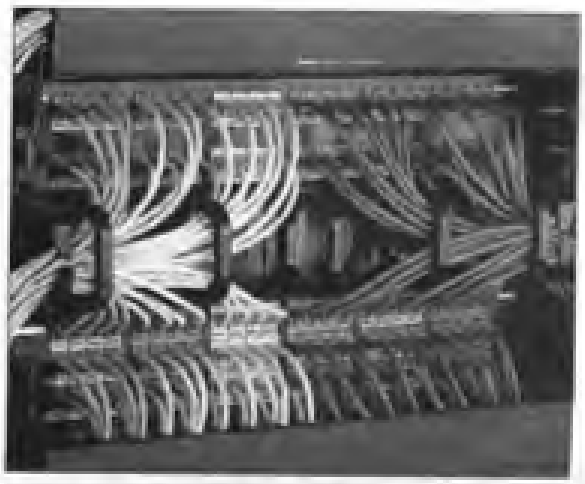
图A-41 可替换端接刀

在工具上施加压力后，弹簧的压力增加到某一点时，类似于撞针的机械装置就会释放弹簧里储存的能量。导线马上被压到两个绝缘位移（insulation-displacement）连接之间，而且额外的导线也会在同一操作里被切断。连接之所以被称为绝缘位移是因为绝缘层会在端接工具的接触点被挤出去。

绝缘位移连接提供了一个安全和不透气的连接，这意味着实际的连接并不会暴露在空气中，因为被移位的绝缘层紧紧地压在了模块上。这对于提供长期的抗腐蚀连接来说是必需的。接线板通常都用于数据网络，就像110型模块那样，但它们也可以用于语音方面的应用。

线缆管理

有些端接系统里内置了线缆管理装置。110型模块在模块间使用了塑料线槽和间隔装置。线槽可以水平或垂直地使用，而架子的安装可以加入多种的线缆管理特性（如图A-42所示）。另外，有时会组合使用D型环和线槽。



图A-42 泛达（Panduit）牌线缆管理装置

在购买线缆管理系统时，考虑以下几个方面：

- 系统应该保护线缆不被挤压，而且应该维持它的最大弯曲半径。
- 系统是可伸缩的，以便当需要更多线缆时，系统有能力处理。
- 系统是灵活的，以便线缆可以从各个方向进入系统。

• 系统可以提供通向水平路径的平滑转移，以便线缆不会被损坏，或者不会超过最大 弯曲半径。
• 系统是耐用的，它应该可以与安装在它上面的线缆和设备那样持久地工作。

小心地贴上标签

贴标签是结构化布线系统里另一个很重要的部分。如果线缆两端没有被清晰地贴上标签，就有可能产生混乱。TIA/EIA-606指定每一个硬件终端单元都必须有某种类型的惟一标识。标识符必须被标记于每一个硬件终端单元或它的标签上。在工作区使用标识符的时候，工作站终端必须把标签贴在面板、机架或连接器自身上。多数的提案申请（Request For Proposal）和规范都要求标签要由机器制造，以便使标签耐久和易读，并且使其看起来更专业。

使用的标签要使多年以后在该系统上工作的人仍然能够理解。很多网络管理员会把房间号码加入到标签信息里。他们会为通向房间的每一条线缆指定字母。有些标签系统，特别是那些在大型网络里面的标签系统，还会在标签上使用颜色编码。

为了确保以后标签不会被擦除或（在末端）剪掉，可以在线缆的非固定端贴几个标签，每个标签相隔大概60cm（23.6英寸）。线缆铺设好之后，在线箱或线轴的那一端重复该过程。为了使线缆能稳固地绑在一起，可以使用绝缘胶布。把牵引绳的末端与线缆的末端绑在一起。贴胶布前在线缆上用牵引绳打几个半结，以防松动。不要吝啬胶布的使用。如果日后因为这个而使牵引绳或线缆松开了的话，恢复它会导致时间和金钱的浪费。

当线缆沿着选定的路径铺设好之后，把它牵引到电信间里面。必须留有足够长度的线尾，以使线缆可以从各个方向到达插座的位置。另外还要为线缆保持足够的松弛度，使它们可以触及地面，并且还可以延伸60到90cm（23.6到35.4英寸）。

回到处于中心点或电信间的线轴。以每个线轴的标签为参考，在相应电缆的末端标上合适的房间号和字母。在还没贴完标签前不要切断线缆。如果遵循这些步骤，那么用于水平线缆铺设的网络传输介质两端应该会被贴上标签了。

A.8　完成阶段

完成阶段是指安装工人测试并在某些情况下认证他们工作的那个阶段。测试能确保所有的线缆都通向了指定的目的地，而认证则是一项关于布线和连接质量的声明。

完成阶段包括以下几个重要方面：

• 线缆的测试。
• 时域反射计（TDR）。
• 线缆的认证和文件编制。
• 系统切换。

在确定网络布线安装中已有和潜在的问题和错误时，诊断工具是非常重要的。

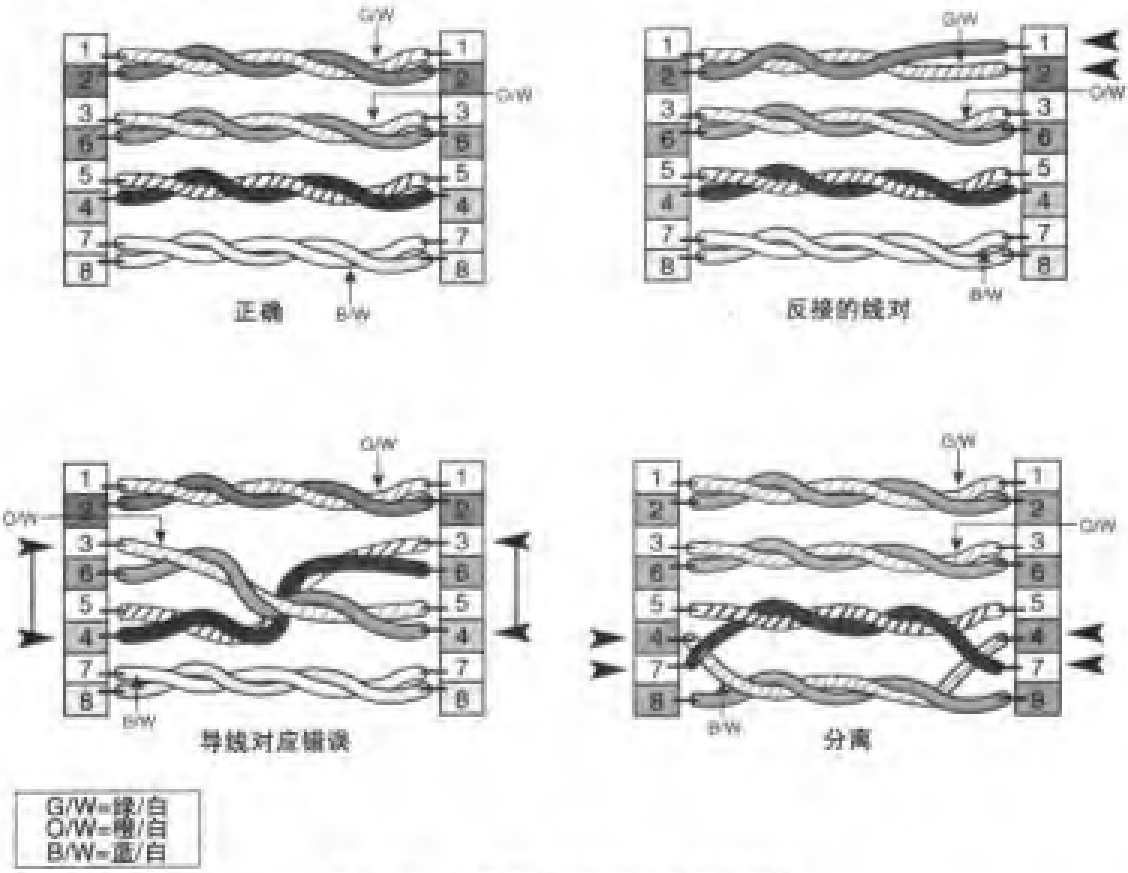
A.8.1　线缆的测试

线缆测试器被用于测试线缆的开路、短路、裂开以及其他问题。在线缆安装工人进行一条线缆的端接后，应该把线缆插到测试器上，检验一下端接是否正确。如果导线被意外地接到了错误的引脚上，测试器会指示出这个布线错误。类似地，它可以测试其他的线缆问题，比如短路或并路。每一个线缆安装工人的工具箱里都应该有一个线缆测试器。用线缆测试器测试完线缆的连通性后，可以继续用认证测量仪对线缆进行认证。

测试是线缆安装完成阶段里最重要的一步。通过测试可以验证所有的线缆都工作正常，用户日

后也不会发现线缆存在问题。毕竟在一个小问题变成主要问题前就抓住它总是好的。

与线缆功能有关的测试可以在TIA/EIA-568-B.1里面找到。通常需要进行测试的各个方面包括以下这些（如图A-43所示）：



图A-43 由不正确端接造成的布线错误

- **开路**——线缆里面的导线不能保持端到端的连通性。这通常是由不正确的端接或断开造成的。另外，开路偶尔是由于线缆本身的问题。
- **短路**——线缆里面的导线互相接触，造成电路的短路。
- **线对的分离**——线对里的导线混杂在一起。
- **导线对应错误**——多线对（multipair）线缆里面的导线在处于远端的连接器里端接得不正确。

在大多数情况下，可以只从线缆的一端完成开路、短路、分离的线对和导线对应错误的简单功能测试。

短路的测试

当一对线里的两条导线互相接触时，就造成了短路，而短路为信号流提供了一条不希望有的捷径（如图A-44所示）。这条捷径是在电压到达预期目标前形成的电路。



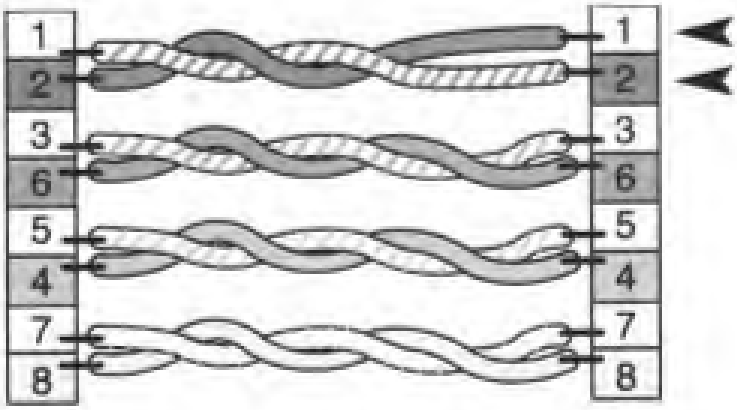
图A-44 导线短路

为了确定是否存在短路，可以测量一下导线间的连通性或电阻。在正常情况下不应该测量到它们之间有任何的连通，而且它们之间的电阻应该是无穷大的。可以用一个低电阻、带刻度的欧姆表进行这些测试。如果使用了高电阻的欧姆表，当导线接触到探针时，安装工人相当于冒着有可能在无意中测量了自己身体的电阻的危险。有些安装工人觉得，如果能发明一个可以防止这个问题的小测试装置会很有用。因此，很多测试探针都装有易拆卸弹簧夹。它们可以夹紧导线，使导线不会同时被接触。

反接的测试

当一对线缆的尖端（或者环）被端接在相反的位置时，反接就发生了（如图A-45所示）。

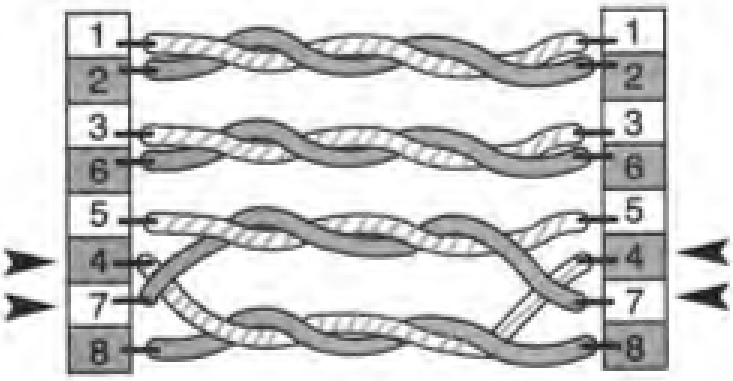
为了修复线缆里面逆转的线对，必须把RJ-45连接头去掉，而且有线对逆转的线缆要重新端接。



图A-45　反接

线对分离的测试

当线缆里面的线对混在一起时，线对的分离就发生了（如图A-46所示）。测量分离的其中一种方法是使用欧姆表。首先，测试线对是否存在短路。如果没有发现任何短路，那么使每一对导线短路。如果是使用欧姆表进行测试的话，预期的结果应该是有短路产生。如果发现开路，则肯定出现了问题。线对要不就是分离的，要不就是开路了。这时可以用音频发生器来判断到底是哪一种情况。而高端的测试器则通过测量***线间串扰***来探测线对的分离。



图A-46　分离的线对

一个简单的线缆测试器也可以用于检查线对的分离。如果存在极性或连接性问题，这种测试器所使用的发光二极管可以马上通知安装工人。

要修复线对分离的话，必须去掉一边或两边的连接器，然后重新端接线缆。

A.8.2　时域反射计

时域反射计（TDR）的工作方式是：向导线发送一个脉冲，然后监听由于线缆故障而造成的线缆上的电回声。TDR会根据这个判断线缆是否失效，如果是的话，到底是开路还是短路；另外它也可以确定从测量点到故障点的距离。它的工作原理是：信号到达线缆末端后会被反射回来，另外，当它沿着线缆传递时，如果碰到一个故障点，它也会被反射回来。信号传播的速度称为额定传播速度。对于不同类型的线缆，额定传播速度是一个已知量。当设置好之后，测试器就能知道信号传播的速度，并且可以通过测量信号从发送到反射回来所经历的时间来测量线缆的长度。TDR的读出装置通常都要进行校准。虽然仪器必须被正确校准，而且使用时也需要技巧，但是在定位线缆故障时，这会是一项非常有效的方式。

A.8.3 线缆的认证和文档编制

测试与认证并不相同。测试是为了功能性——换句话说，它确定线缆能否把信号从一端传送到另一端。认证，或性能测试，则是一项关于线缆性能的声明。它回答了这些问题：信号沿着线缆传输的质量如何？信号有没有免于受到干扰？信号到达线缆另一端时强度是否足够？

认证测试器

认证包含的内容比功能性测试要多。另外还必须进行性能测试。遵守安装标准的结构化布线系统必须被认证。认证仪表可以根据ANSI/TIA/EIA-568-B标准进行所有必需的性能测试（如图A-47所示）。仪表具有自动测试功能，因此可以通过按一个按钮来完成所有的测试。这些测试包括近端串扰（NEXT）、导线图、阻抗、长度、DC回路电阻、传播延迟、回波损耗、延迟偏差、衰减和衰减串扰比（attenuation-to-crosstalk ratio）。仪表会把多项测试结果放在内存里，因此可以把测试结果下载到计算机上，然后生成一个测试报告，并把报告提供给用户。除了认证之外，这些仪表还具有一些诊断特性。这些特性不但能鉴别故障，还能显示被测量线缆的末端离故障点有多远。



图A-47 福禄克（Fluke）牌Networks 4000型线缆认证测试仪

性能测试通常都会在某个指定的测试频率下进行。所选择的用于测试线缆的频率是线缆预期工作频率的一部分。比如，用1000MHz测试超5类线缆，用250HMz测试6类线缆。性能测试的内容由TIA/EIA-568-B的各种附录描述。现代的测试硬件和软件可以提供文本和图形输出，从而可以对结果进行快速比较，而且能一眼就看出分析结果。

线缆认证方法构成了布线系统的基本测量法。在合同签署后，工作结果所遵循的认证标准通常都是合同的一部分。安装工程必须符合或超过所使用的线缆等级规范。而表明布线已经达到这些标准的详细文档会交给用户。

认证程序是完成布线工作的重要一步。它可以使安装工人明确地表明：在某天的某个时间，线缆的性能达到了某种规范。任何日后在线缆性能方面的更改都必须可以归因于某个原因，而如果之前能有关于线缆状况的明确证明的话，找出这个原因就会变得更容易了。不同等级的线缆所要求的可接受的最小测试结果是不同的。通常线缆类别越高，制造公差就越紧；品质越高，性能就越好。

认证测试

为了通过认证，线缆必须符合适用于它们等级的最小测试结果。换句话说，线缆必须符合或超过这些规范。通常遇到的情况是，真实测试结果会比最低要求要好。真实测试结果与最小测试结果之间的差别称为净空（headroom）。如果结果显示净空有很多，那么将来的线缆维护可以少一点，而且网络更能忍受等级不高的跳线和设备线缆。

通常使用的规范包括以下这些：

- **指定的频段**——每一条线缆都会在一个频段内进行测试，该频段通常是线缆进行日常应用时的频段。线缆的等级越高，频段就越高。
- **衰减**——线缆衰减的衡量标准是线缆吸收的信号量。衰减越低，导线越好，而且线缆的质量也越高。
- **近端串扰（NEXT）**——当处于线缆近端的其中一对导线的信号受到另一对导线的信号的干扰

时，近端串扰就发生了。串扰会影响线缆传输数据的能力。每一个等级的线缆都被指定了它可以承受的近端串扰的总量。

• **近端串扰功率总和**——在使用了所有导线的线缆里（比如吉比特以太网），信号会受到几对导线的干扰，而不是一对。需要考虑线缆里所有线对的相互作用才能计算这些干扰所产生的效果。可以用近端串扰功率总和的计算方程式来进行计算。

• **衰减串扰比**（*ACR*）——衰减串扰比（ACR）表明了与同一条线缆上的近端串扰或噪音相比，接收到的信号有多强。有时这项衡量标准被称为信噪比（SNR）。需要注意的是，SNR把外部的干扰也计算在内了。

• **衰减串扰比功率总和**——当使用了一条线缆里所有的线对时，线对之间的相互作用就变得更加复杂了。这是因为，更多线对的参与意味着存在更多的相互作用。

• **等电平远端串扰**（*ELFEXT*）——等电平远端串扰是发生在导线远端的串扰量的计算标准。如果该特征是高的话，意味着线缆不能很好地传输信号，而且ACR（信噪比）没有受到很好的控制。

• **等电平远端串扰功率总和**——就像其他功率总和的衡量标准那样，在同一线缆里的多对导线之间的相互作用增加了等电平远端串扰特性的复杂性。衡量标准中功率总和的计算方法把这个复杂性考虑在内了。

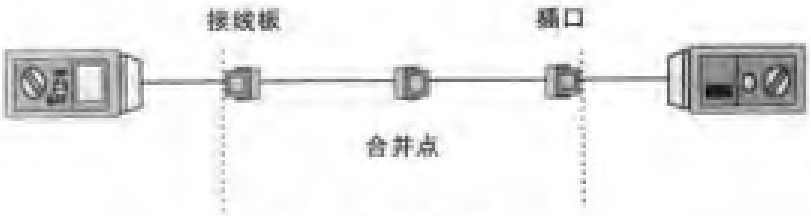
• **回波损耗**——有些沿着导线传播的信号会反射一些导线里的缺陷，比如阻抗不匹配。它会反射回发送端并形成干扰源。这称为回波损耗。

• **传播延迟**——线缆的电气特性会影响信号的传播速度。这个延迟值必须通过某些测量工具（比如时域反射计）获知。线缆的传播延迟通常被指定为一个以毫秒为单位的最大允许延迟量。

• **延迟偏差**——由于线缆里的每一对导线都有一个不同的绕数，当同时进入线缆的信号到达远端时，它们肯定会有轻微的不同步。相邻线对里领先和落后的信号到达远端的时间差被称为延迟偏差。这个问题可以被不整齐的端接掩盖起来，就是说线缆对于连接器的引脚来说并不对称。最后，如果线缆里的线对之间存在传播延迟的差异的话，会由于延迟差异而影响信号。

信道测试和链路测试

测试时使用的方法有两种：信道测试和链路测试。信道测试是真正的从工作站或电话到电信间（TR）设备的端到端的测试。信道测试会测量所有的线缆和跳线，包括从插座到用户设备的线绳和从接线板到电信设备的跳线。而作为另一种测试方法的链路测试就只是测试从墙壁到接线板的线缆。链路测试有两种：基本链路测试和永久链路测试。基本链路测试不包括任何的连接器，测量点从故障诊断装置附近开始，到处于链路另一端的故障诊断装置的远端单元附近结束。永久链路测试不包括线缆的现场诊断装置单元部分，但包括线缆两端与适配器线缆相连的部分（如图A-48所示）。



图A-48　永久链路测试

永久链路测试也考虑了集合点，而这正是开放办公布线安装所需要的，而且也更实用。

惟一被接受的测试是永久链路测试。而信道测试已经在TIA/EIA-568-B.1里被正式废除了。

认证技巧

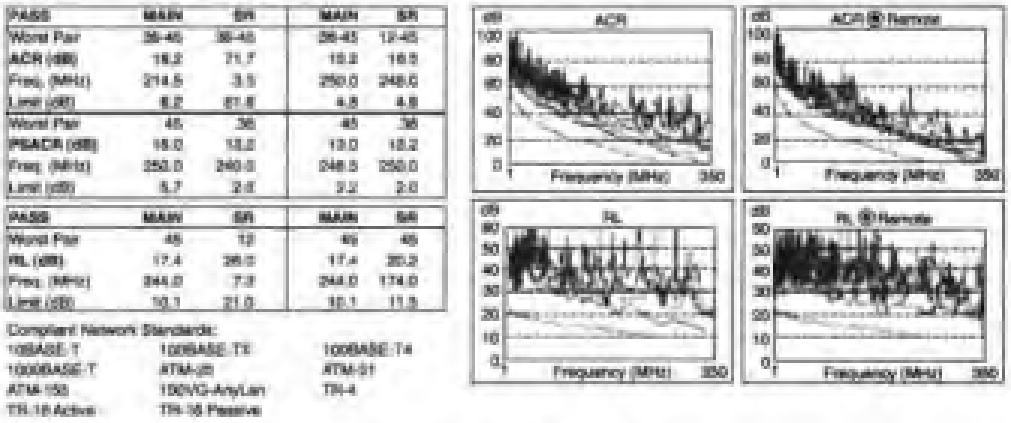
理解测试结果与发现问题同样重要。学习如何理解测试结果的最佳途径是使用测试设备测试好的线缆的电路。这可以使安装工人对如何正确使用测试设备和当线路工作正常时测试会有怎样的测

试结果有一个基本的认识。

如果想积累关于排错和问题鉴别方面的经验，可以特意制造一些具有某些特定问题的线缆，然后观察一下测试器是如何对这些问题作出反应的。接下来，通过随机选择这些有问题的线缆进行测试来练习根据测试器的测试结果来鉴别问题。花时间去练习，以便能快速鉴别问题是值得的，因为安装工人必须有能力快速定位问题并把它修复。

专业认证文档

很多线缆认证工具都具有以数据库格式输出测试结果的能力。在个人计算机上可以利用这个来生成高质量的文档（如图A-49所示）。



图A-49 线缆认证文档

高级的认证测试器通常都会提供与线缆安装有关的软件。这些软件使承包者可以为客户提供整齐像样的测试结果。有了这些软件，就不必手工把测试结果输入到电子制表软件里了。这些软件包把测试结果以“通过”或“不通过”的形式储存起来。当不足之处被发现并更正后，有关的项目要被重新测试并提交给用户。而用户通常都既想要测试结果的电子版，也想要测试结果的书面版。

如果要使文档真正有用，那么它必须容易获得。以电子版发布的文档能确保那些需要测试结果的人能随时得到它。另外，还应该以书面形式为用户提供完工（as-built）文档和认证结果，而且这两者还要保存在安装工人的永久记录里。

当布线系统接受认证测试时，应该把测试结果收集起来，并且根据测试结果编写完工文档。如果出现了对布线工作在质量或准确性方面的疑问，认证文档对于安装工人来说就变得很重要了。因为它能显示在某一个确定的日期，线缆以特定的顺序排列，并且可以以特定的质量传输信号。随着时间的过去，那些影响线缆传输信号能力的改变可以通过把当前与以前的测试结果相比较而显示出来。

由于不可预料的障碍、改变了的计划、还有最后一刻才进行的设备升级，用于构建网络布线系统的文档可能不能反映真正构建的系统。因此，任何时候如果有人被安排对布线系统进行更改，那么那个人一定要知道当前系统的真正状况。否则，所做的更改有可能会造成无法预料的后果。完工文档可以有助于避免这种麻烦的发生。另外，在真正进行更改的时候，一定要预先创建更改文档。

A.8.4 系统切换

系统切换是指从现有设施转换到新的布线系统，或者在最近铺设的布线系统上安装新设备的过程。

系统切换指导方针

好的系统切换需要周详的计划、组织和对详情的细心留意。在进行切换时，要遵循以下的指导

方针以确保成功：

• 保存安装的详细记录。这些记录可以对所有线缆已经被安装好，而且已经被安装到了正确的位置进行核实。

• 对每一条已安装的线缆进行测试。

• 编写正确的介绍文档和线路图，以及与它们对应的线缆或线路。安装管理员通常要按照从用户处接收到的信息来编写介绍文档。

• 为系统切换做好计划安排，尽量减少它对用户带来的不便。由于系统切换通常需要使某些系统离线，因此最好把它安排在晚上或周末进行。

清除废弃的线缆

根据2002年版的美国国家用电规程，当符合了规程里定义的某些标准后，所有废弃的线缆都必须被清除。至于清除线缆的费用包括在总费用里是否合理这一问题，目前由用户和线缆安装承包商共同协商决定。但是用户和承包商必须确保遵守当地的法规。因此，在开始翻新前，必须到当地管理部门核实，并且要与用户讨论细节问题。

在清除任何废弃的线缆前，要先确保没有任何线路要使用该线缆。要做到这一点，可以通过向用户核实并使用万用表或电话测试装置验证。在清除废弃的线缆时必须特别小心，以免破坏天花板瓷砖或悬置天花板的支撑结构。

A.9 布线工作

布线工作需要引起广泛的关注，就像任何其他企业的工作方面那样。在线缆安装前必须要进行投标，而在进行投标前又必须要求有一个提案和预演，以便确定工作的准确范围。而且也可能需要一份有关项目描述以及如何完成项目的文档。开展布线工作需要许可证，可能还需要是工会的成员。所有的项目必须及时开展，而且要把时间和物资的浪费减到最低程度。而这通常是一项要使用计划管理应用的项目策划工作。

在布线工作领域里特别重要的事项或主题包括以下这些：

• 现场调查。

• 劳动力状况。

• 合同的修订和签署。

• 项目策划。

• 最终文档。

与其他大多数工作一样，布线安装工人的形象和行为会影响用户、上司和同伴对他的印象。一个布线安装工人在工作方面的选择可以影响他被提职或者甚至被解雇。作为公司的一名职员，线缆安装工人在工作上是代表公司的。他的形象和行为反映出公司的形象。因此，你一定要保持专业形象和行为。

在工作当中要遵循以下的指导方针：

• 要尊重施工现场。注意不要造成损坏，也不要随便抛弃垃圾。如果杂物影响到其他人，要马上把它们清理干净，或者是在当天工作结束后进行清理。

• 穿上整齐清洁的工作服到达施工现场。

• 在约定的时间出现在工作地点。记住，准时是非常重要的。

• 要对噪音考虑周到。进行翻新工作时，正常的工作仍然在进行中的话，不要放音乐、吹口哨、唱歌或大喊大叫。

• 要尊重客户、建筑物居住者、同事和上司。

A.9.1 现场调查

现场调查（或项目走查）是对项目成本预算进行准备之前的最重要的几件事之一。它使承包商有机会发现任何有可能影响安装工程的问题。而客户提供的图纸和说明书可能不会指出这些问题或困难。

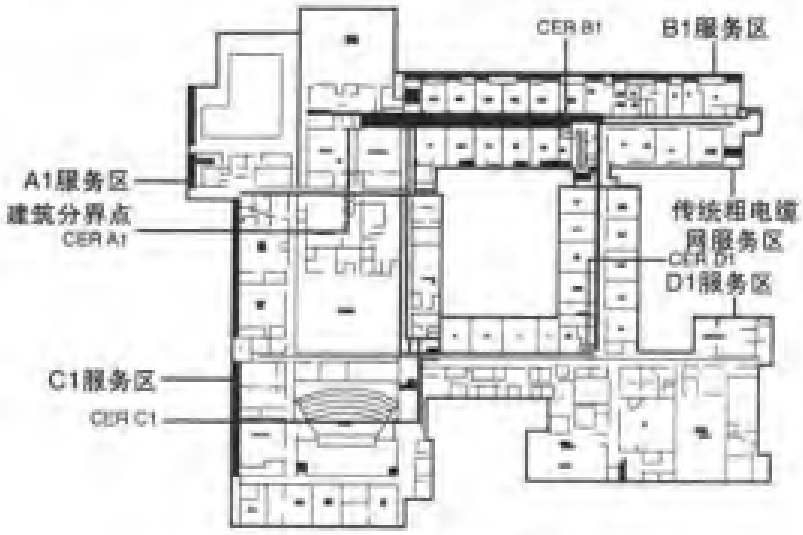
在进行走查时，绘制项目的草图是明智的。当真正进行评估时，草图会有助于问题区域的认证。

在进行现场调查时，需要搞清楚以下的关键问题：

- 存在通风天花板区域吗？
- 存在物资集结或存储区域吗？
- 是否要求特别的工作时间？
- 存在特别的安全要求吗（在工厂环境下这个问题有特别重大的意义）？
- 哪些墙壁是防火墙？
- 在建筑物内有石棉吗？
- 当天花板瓷砖损坏时，用户会提供备用的瓷砖吗？
- 存在需要考虑的特别的劳动力问题吗？

需求文档

蓝图是根据比例划出的图纸，它提供了决定线缆铺设长度所需的距离信息（如图A-50所示）。蓝图也应该标出设备插口和电信间的位置。但它们不一定会标出可行的路径或选路的信息。选路的信息通常是通过现场调查收集得到的。大多数的结构化布线系统都规定每一个位置都需要最少两条四线对的线缆，但很多用户的要求都比这个要高。这种信息应该复制到项目说明书里。

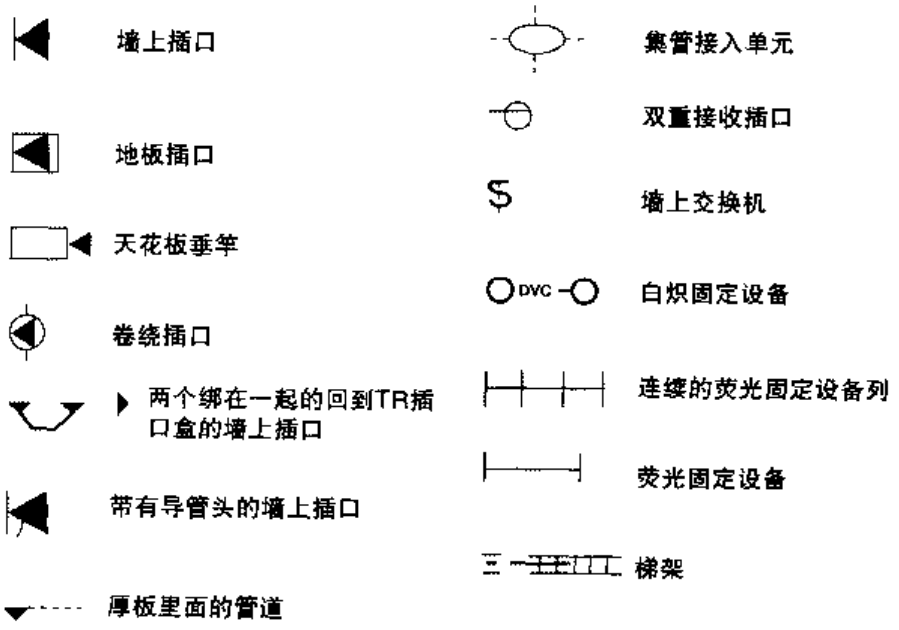


图A-50 典型的建筑蓝图

在蓝图上统计插口的位置和测量线缆的长度称为估算。估算要求很高的准确性，因为它会为投标提供物资需求。现在，自动化的测量仪器可以有助于把犯错的机会减到最低程度。

安装图标和符号

蓝图和图表会使用标准图标和符号来识别线路的铺设、不同类型的配线管道，还有插口和插座的有关信息（如图A-51所示）。这些标准图标和符号在蓝图上提供了图形识别需求的统一方法。



图A-51 线缆安装图标

图纸类型

建筑蓝图遵循一个标准的格式。图纸根据类别来分组。图纸会以前缀作为标记，而这个前缀则与图纸所属的类别有关。比如，所有与电系统有关的图纸都会被归为一组，并且它们的前缀为“E”，表示“与电有关的”。而建筑部分的图纸以“A”开头，管道设备图纸以“P”开头，以此类推。电话和数据图纸通常被分在同一组，并且以“T”作为前缀：

- T0——园区或工地布置图：外部路径和建筑物之间的骨干。
- T1——整座建筑物每一层楼的平面图：服务区域边界、骨干和水平路径。
- T2——服务区域的图纸：接入点的位置和线缆的标记。
- T3——通信设备间：机架的俯视图和墙壁的立视图。
- T4——典型的细部图：面板的标记、挡火物和安全特性。
- T5——系统切换的计划（布线和设备的电子表格）。

除了以上这些，或许还有别的图纸，比如设备图。设备图可以在A类图纸或者杂项类别里面找到。估算人员要求图纸要包含以下这些方面：

- 一张建筑平面图，根据它来获得对项目的总的看法。
- 楼面布置图。
- T类（电话）图纸。
- E类（与电有关的）图纸，作为参考。
- 设备图，帮助确定插口的布置。
- 一张（建筑）图纸，用于协助找出可用的路径。

设计文档提供了关于项目的叙述性描述。它可能会包含要安装的布线系统的功能性的描述。比如，它可能会含有类似于“该系统必须支持1000BASE-T（双绞线吉比特以太网）”之类的陈述。

设计文档通常也会含有一些行业的专门术语，还有对行业或准备安装的系统来说具有惟一含义的缩写词。估算人员应该对设计文档里的所有术语都有透彻的了解。术语表和缩写词表都是可以得到的。国际建筑业咨询服务公司（BICSI）的网站就含有一个这样的术语和缩写词表。

设计文档会指明系统的需求和需要使用的物资的类型。每一个信息插口或插座所需的线缆数目的信息也会在设计文档里面提供。设计文档还会描述测试规范和标记的规范和格式。

示意图

*示意图*并不需要按照比例绘制。它用于描述连通性——也就是事物之间连接的方式。一张典型的示意图显示了主电信间或主交叉连接（MC）和中间交叉连接（IC）。它也会显示这些点之间的线缆类型和尺寸。它通常不会详细标出在这些地方的实际端接点，也不会显示单独一条通向信息插口或插座的线缆，而只会显示通向某些特定设备（比如在项目里需要用到的服务器或其他主要组成部分）的线缆。

A.9.2 劳动力状况

每一家线缆安装公司都需要处理各种劳动力问题。有些劳动力问题会造成线缆安装公司与工会的矛盾。因此安装公司必须对涉及工会或许可证等方面的规则和法令很清楚。

工会

有些项目需要使用工会劳工。工会是代表工人的组织。虽然工会劳工的使用在新的建筑项目里更常见，但是却不只限于新的建筑。工会劳工的使用可能会是合同内容的一部分。如果客户明确要求必须使用工会劳工，那么承包商就必须使用工会劳工。

其他的劳动力状况规定了工作分类和允许的工作。在工会环境里，通常不允许监督者进行任何的安装工作。类似地，也不允许线缆安装工人去安装配线管道。不过有时候，线缆安装工人也可以去安装不超过某个尺寸或长度的配线管道，而超过这个尺寸或长度的配线管道就一定要由电工去安装。这些规则是由工会协议所定义的，而且通常是由不同行业间的工会协商后决定的。

承包商的许可证

并不是所有的国家或州都需要承包商具有许可证。在美国，不同州的承包商许可证规定会有不同。有些州要求承包商必须把他的许可证编号显示在所有的广告、名片和信笺头上面，以此证明他是获得了许可的。在需要出示许可证的地方，如果有承包商不出示许可证的话，那么将被罚款。而且他们也有可能会失去某些权利，比如在客户不对实施的服务付款时提出扣押权的申请。

承包商获得许可证的条件包括技术知识、商业知识和所在州的劳动法知识。而知道在某个州或国家里承包商是否需要许可证是承包商自己的责任。

A.9.3 合同的修订和签署

当所有的协商完成后，必须修订合同以反映双方都同意的更改。而且双方也要重新对合同进行详细的审核。合同的协商是一项口头的工作，双方必须确保他们的目的都准确地反映在书面形式的文档里。随着工程的开展，合同内容的改变更改以合同修订的形式提出。而修订必须获得双方的同意，而且由双方签署。

来自客户组织和承包商组织的、经认可的责任团体负责合同的签署，以使其成为一份有效的协定。当双方都签署了合同之后，约定就生成了。而在合同签署之前，不应该订购任何物资，也不应该开展任何工作。

普通的文档，比如变更通告，可以作为模板被预先创建，并且只需要简单地填写一些正确的信息。这些模板可以带到项目现场，并且在最初的会议或不同的走查期间填写。

在项目启动后，任何的更改都只能由书面形式的变更通告作出。不允许仅根据口头指示就作出对原计划的更改。另外，合同应该有变更通告表。而且项目经理应该把这些表放在施工现场。无论

什么时候，只要有可能，变更通告导致的额外工作应该包含在额外劳动力和物资的成本里。如果办不到，那么变更通告里应该包含一条声明：客户同意为额外的工作付款。

A.9.4 项目策划

项目策划阶段真正开始的时间是在项目被授予之后、正式合同被签署之前。在这个阶段要进行投标和评估信息的编制、特别需求的记录、资源安置的制定，还要对提案申请作最后的审查，以确保所有的组成部分都会被提及。

以下是所有在策划阶段应该采取的步骤：

步骤1 在策划布线项目时，第一步要做的是选择项目经理或监督者。

步骤2 必须根据项目的大小、完成项目所需的时间数、对技能的要求以及完成项目所允许的时间来选择工作人员。

步骤3 必须确定和安排子承包商。

步骤4 必须做好物资交付的计划。

步骤5 必须制定出废弃物品的处理规定。

供应商

评估人员通常会基于成本、交货和服务来选择供应商。评估人员会根据以下的问题来确定物资总成本：

- 供应商的报价包含运费吗？
- 根据以往的记录，供应商可以在承诺的时间内交付货物吗？
- 在退货问题上，供应商的政策是怎么样的？
- 供应商可以及时提供货物说明和工程图样吗？
- 供应商可以提供技术上的建议和支持吗？

订购物资

在合同签署之后，应该以书面订购单的形式从供应商处订购物资。订购单应该包含对物资的描述、生产商的零件号码、质量、价格、送货日期和送货地点。

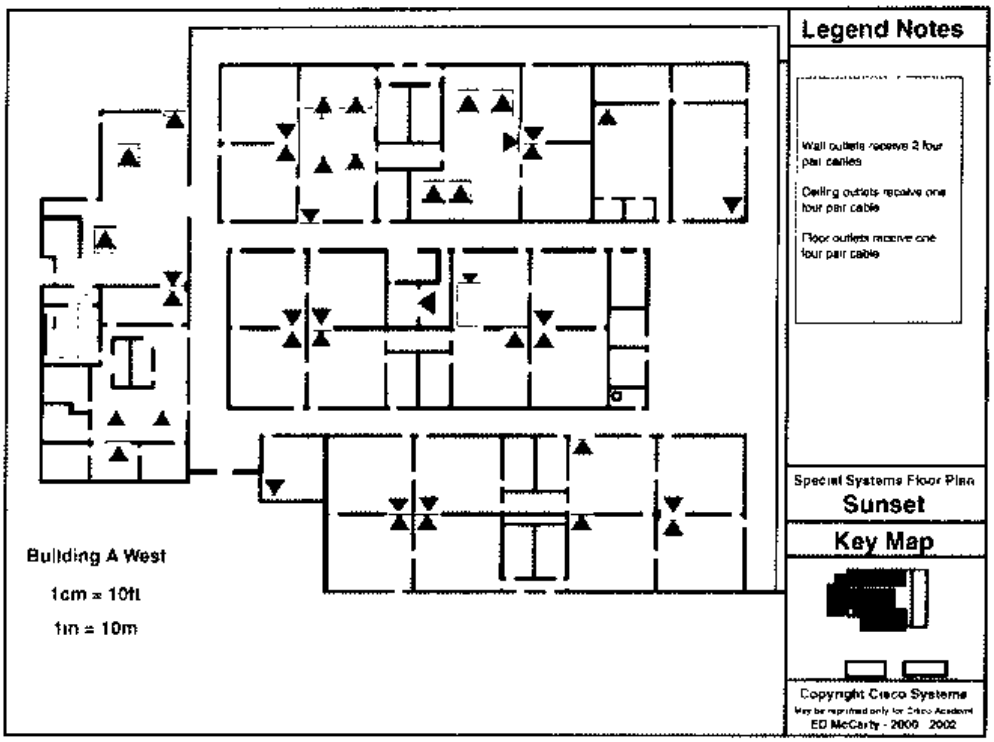
通常情况下，订购者都会选择那些报价最低而又可以提供所需数量的指定线缆和设备的供应商。在评估最低成本时，必须把运费考虑在内。而供应商必须保证在一段固定的时间内不更改报价。通常情况下，供应商会保证在最少30天内不对报价进行更改。另外，监督者或承包商负责人必须注意的是，不允许有任何未经批准的、意在降低成本的替换行为。

A.9.5 最终文档

向客户提供完工图纸是完成布线项目的最重要部分之一。图纸里要显示线缆的走向、端接点，还有实际安装的线缆的类型。在多数情况下，由于遇到障碍物或困难，会有些原计划需要安装的线缆并没有被安装。典型的更改包括增加或删除线缆的铺设或插口，或者是采用另一条通路去铺设线缆。完工图纸为客户提供了真正执行的工作的图表（如图A-52所示）。

当所有的线缆都铺设好、所有的插座都安装好、所有线缆都端接好之后，才能绘制完工图纸。在进行最终测试的时候就可以开始绘制图纸了，但必须确保此后不会进行任何没有正确反映在图纸上的改动或额外的工作。

楼面布置图、设备图和T类图纸通常会作为完工图纸的绘制基础。承包商并不需要为完工图纸



图A-52 完工图纸

重新绘制建筑平面图。承包商需要绘制的包括所有铺设的电缆、端接点和插口，还有安装时所提供的所有标签信息。

工程项目清单（punch list）是当承包商认为项目完成时，客户向承包商提供的清单（如图A-53所示）。

工程项目清单

工程项目清单是一份记录，里面包含了所有承包商必须更正或完成的项目任务。只有当任务更正或完成后，屋主才会觉得满意，而承包商的工作才算完成。

在项目结束和最后付款之前，屋主和承包商或建筑师应该一起进行项目走查，以便找出所有需要更正或完成的任务。

与项目有关的各方都知道：当屋主同意以下详细列出的工程项目清单已经完成了，而且他或她对此感到满意，那么整个项目就完成了，而所有的款项都应该支付给承包商和/或建筑师。

工程项目清单项	日期	核准

图A-53 典型的工程项目清单

工程项目清单是一个关于还没完成的项目（比如没有安装的插口或没有铺设的线缆）、完成得不满意的项目（比如线缆没有固定在阶梯形齿条上，或插口不能正常工作），或客户要求在最终付款

前纠正的清理项目的列表。工程项目清单可以表现为客户对项目的最终接受程度的形式。当用户对工程项目清单里的项目感到完全满意时，就是付款的时候了。

A.10 案例学习：FARB软件开发有限公司：网络设计与实施

实验练习使你有机会练习结构化布线安装的手工技巧。这个案例学习让你能有实践机会去参与一个假想的软件开发公司的结构化布线系统的设计。该公司拥有一栋新的三层建筑物，而且这栋建筑物需要扩建。

A.10.1 概述

为了完成该案例学习，你应该能够：

- 为安装前的准备工作收集资料，为安装过程拟定计划。
- 为组建实际网络编写所需的文档。
- 遵守TIA、EIA和各项电气标准。

利用这个附录，并且掌握了CCNA第3学期的知识后，你就可以完成很多与实际网络组建有关的任务了。在该案例学习中，这些目标在来自Cheryl Farb的信中有详细的说明。Cheryl Farb是FARB软件开发有限公司的总裁，而这家软件开发公司在本案例学习中是客户公司。

接下来是一些有助于你进行本案例学习的内容回顾。

A.10.2 通常的设计过程框架

网络设计最好能依照一个框架来进行。线缆的走向的决定需要对网络结构有所了解。在开始草拟一个可行的网络前，你需要知道用户所在的位置和他们使用的应用程序的类型。必须设计出一个第1层LAN的逻辑和物理拓扑。这个设计要包括所选择的线缆类型和物理（布线）拓扑，还有网络里作为基础设施的连接点的物理布置。

第2层的分段设计图必须覆盖在之前设计的第1层拓扑上。这一层的设计图包括为了提高网络性能和功能而增加到拓扑上的设备，比如交换机和网桥。这一层也包括了诸如微分段、虚拟LAN（VLAN）和生成树协议（STP）之类的技术的使用，以增加网络的性能和可靠性。

第3层的层次化设计图要覆盖在之前的两层上。这个设计图包括了第3层设备的增加，以便为网络提供网络内和网络间的功能性，另外也包括了网络地址分配计划的设计。路由器和防火墙都应用在第3层，它们增强了网络的逻辑结构。另外，它们也被用于划分冲突域和广播域。

对第3层设计图的扩展也可以被认为是一个第4层的设计图。这个设计图会覆盖在前三层之上，它会严格限制软件的应用，并且控制着网络的接入和可用性。它包括了访问列表和防火墙的配置。虽然一个完整的网络设计会继续涉及OSI模型的更高层次，但是这已经超出了该项目的讨论范围了。

这个设计会把精力集中在以太网、IP、第1层、第2层和第3层（本学期的重点内容）上。而设计的过程在逻辑上会沿着OSI模型从低到高进行。

布线系统必须能在服务期内经受住对它的更改和扩大。对大多数公司来说，当结构化布线系统老化时，它们很有可能已经搬到其他地方去了。这意味着必须注意不要太遵循当前的网络布局，以免线缆不适合用于以后的其他组织。一个合适的结构化布线系统既要适合当前的网络，也要能容易地适应将来的网络。

网络设计和操作里最重要，而通常又最容易忽略的一个部分就是文档编制了。该项目的一个主要焦点就是网络设计的文档编制。用于这个项目的文档应该包含布线图、编址方案、任何灵机一动的好主意、问题解决模型，还有在进行这些决定时所作的任何其他记录。

A.10.3 初步设计过程

在设计一个网络之前，必须收集设计网络所需的数据。为了使网络能有效工作，并能满足用户的需要，应该根据一系列系统化的、预先计划好的步骤来收集数据。这些步骤为完全发现用于组建网络的数据提供了指南。

在这个过程中，第一步要做的是收集与组织有关的信息。这些信息应该包括以下内容：

- 组织的历史和现状。
- 预计的发展。
- 运作政策和管理程序。
- 建筑图表（蓝图）。
- 现有的网络图表和文档编制。
- 办公室系统和程序。
- 要使用该局域网的人们的观点。

在紧接本部分内容的信息包里，你可以找到来自FARB软件开发有限公司的总裁概述的通信。这份文档存在于FARB Software Development LTD.doc文件里。

在这封信里，Farb简要地说明了她对这个项目的特别要求。

第二步要做的是，为在第一步里收集的当前和预计需求做详细的分析和评估。这一步确定和定义了需要解决的问题或困难（比如建筑物里的一个偏僻的房间可能还没有网络接入）。它也提供了有关未来网络扩展需要、接入和安全性的信息。

第三步要做的是，确定组织的资源和约束。对新的LAN系统的实施有影响的组织资源包括硬件、软件和人力资源类别。如果这个项目是网络的扩展或升级，那么一定要把现有的计算机硬件和软件配以文档说明。而且也必须对那些计划中的需要作出认证和定义。以下问题的答案也有助于确定：需要多少培训？需要多少人员来维护这个LAN？这些问题包括：

- 组织的资金来源是什么？
- 这些资金来源当前的联系如何？它们是如何分配的？
- 有多少人会使用这个网络？
- 网络用户的计算机水平如何？
- 对计算机和计算机应用的态度如何？

遵照这些步骤，在正式报告的框架中把这些信息写成文档会有助于为LAN的实施进行成本的估算和预算。

A.10.4 网络的设计方法和交付使用

根据现在所提供的材料，你应该已经对层次化通信模型的概念有深厚的基础和透彻的认识了。如果以OSI模型作为框架，那么还应该对支持各层工作的功能和设备有所了解。

为了进行这个案例学习，必须学习与网络的物理设计和安装有关的材料。就像前面所提供的材料那样，各种规则和标准支配着网络的设计和组建。在案例学习能真正进行之前，必须对这些规则和标准进行学习。

完成了这一课学习的学员应该能够：

- 设计一个第1层和第2层的拓扑。
- 收集预备过程和真正施工过程的信息。
- 在施工过程中设计文档。
- 遵循TIA、EIA和其他电气标准。

注意，设计出来的网络要符合Farb对她的公司的项目的要求。

A.10.5 标准化组织

在设计和组建网络时，确保符合所有适用的防火规范、建筑规范和安全标准是很重要的。网络设计过程中最重要的部分或许就是根据EIA/TIA和ISO/IEC等工业标准进行设计了。本学期的学习重点在于由以下团体制定并公布的各种网络传输介质的标准：

- ISO——国际标准化组织（这并不是一个首字母缩写词——参见术语表）。
- IEEE——电气与电子工程师协会。
- UL——（美国）保险商实验室。
- EIA——电子工业联合会。
- TIA——电信工业协会。

最后两个组织联合公布了一系列被称为“TIA/EIA标准”的标准。除了这些组织以外，很多地方的、州的、国家的和国际的政府机构也公布了很多对局域网线缆类型有影响的各种规范和要求。

另外，这些标准会被定期检查和更新，以反映新技术和日益增长的对语音和数据网络的需要。知道这一点也是很重要的。当一项新技术被增添到标准里面的时候，其他的旧的技术就会被抛弃或逐步淘汰。在很多情况下，一个网络有可能会含有一些不符合当前标准或正在被淘汰的技术。通常并不要求马上对这一情况进行完全的改变，但是这些陈旧的、缓慢的技术最终还是会被那些更新更快的技术取代的。

A.10.6 标准的制定

对层次化设计有影响的各种基本标准已经由TIA/EIA制定了。电信工业协会（TIA）和电子工业联合会（EIA）是两个行业协会，它们联合制定并公布了一系列覆盖了LAN结构化语音和数据布线的标准。1984年美国电话行业的管制被取消后，房屋内的布线变成了建筑物拥有者的职责，于是导致了这些工业标准的发展。而在此之前，AT&T垄断了该行业的电话装备和系统。

美国国家标准协会（ANSI，见第6.2.7节）委托TIA和EIA去制定用于多种通信产品的建议性的工业标准。这意味着很多标准的名称都以ANSI/TIA/EIA开头。TIA/EIA有很多委员会和子委员会，它们负责研究关于光纤、用户前端设备、网络设备、无线通信和卫星通信方面的各种标准。

TIA/EIA-568-A是用于通信布线的商业建筑标准。这个标准指定了通信布线、推荐拓扑和传输距离限制方面的最小要求，传输介质和连接硬件的性能规范，还有连接器和插脚的指定。它的一些附录覆盖了一些更新更快的铜介质电缆。这个标准已经被TIA/EIA-568-B取代了。

TIA/EIA-568-B是关于布线的标准。这个标准制定了传输介质的组件和传输要求。TIA/EIA-568-B.1指定了一种用于商业建筑的通用的通信布线系统。这种系统适用于多设备和多厂商的环境。TIA/EIA-568-B-1.1是一个补充标准，它规定了由四对线组成的非屏蔽双绞线（UTP）和金属箔屏蔽双绞线（ScTP）跳线的弯曲半径。TIA/EIA-568-B-2制定了布线的组件、传输、系统模型和用于检验双绞线的测量过程。TIA/EIA-568-B.2.1是一个关于6类线缆的补充标准。TIA/EIA-568-B.3指定了光纤布线系统里的组件和传输要求。

TIA/EIA-569-A是关于通信路径和空间的商业建筑标准。该标准指定了建筑物内和建筑物间的设计和构筑方法，使它们能支持通信介质和设备。它给出了一些特定的标准，规定了安装在（或经过）房间、区域或通道的通信设施和传输介质。

TIA/EIA-606-A是商业建筑的通信构造方法的管理标准，另外它还包含了为线缆贴标签的标准。该标准指定了每一个硬件终端单元都必须有某种惟一的标识。在工作区使用标签的时候，工作站终端必须把标签贴在面板、机架或连接器自身上。所有的标签必须符合UL969里面所制定的清晰性、磨损性和粘附性的要求。

TIA/EIA-607是关于通信方面的商业建筑接地和连接要求的标准。它支持多厂商、多产品的环

境，还支持那些有可能会安装在用户前端的不同系统的接地方法。这个标准指定了建筑物接地系统和通信设备接地配置之间的精确的分界点，也指定了需要为该设备提供支持的建筑接地配置。

更多信息
要想知道有关各种EIA/EIA标准的更多信息，请访问以下网址： www.rvcomp.com/wiring/EIA/organizations_codes.htm

A.10.7 用电安全

通常情况下，电流会沿着电阻最小的路径流动。由于金属（比如铜）的电阻很小，所以通常把它们作为传输电流的导体。其他物质（比如玻璃、橡胶和塑料）的电阻比较大，所以它们是电的不良导体。事实上，这些物质通常都作为绝缘体使用。它们被用于与导体绝缘，以免触电、火灾或短路的发生。

全世界有很多不同类型的电源插座。它们使用三个连接点中的两个来提供电源电路。第三个连接点保护人和设备免遭触电和短路。这个连接点被称为安全接地连接。在使用了这个连接点的电器设备中，安全接地导线会与设备的任何暴露的金属部分相连。如果设备内部有接线错误，接地连接可以保护人们免于暴露在危险的电压下。

网络设备中有可能发生的接线错误的其中一个例子是：通电的电线与机箱偶然连接在一起了。如果发生了这种错误，与设备连接的安全接地导线会成为通向地面的低电阻通路。由于安全接地连接的电阻比人体电阻低，所以降低了人们触电或被电击致死的危险。

在进行正确的安装之后，由安全接地导线提供的低电阻通路能提供足够的低电阻和承载电流的能力，从而防止了危险的高电压的积累。也就是说，这条通路直接把带电的连接引向了地面。

A.10.8 对电信间的要求

第1层的设计是整个网络设计里面最大的组成部分。它包含了组建结构化布线系统的初步设计的实现。这些设计是在网络设计的准备阶段进行的。这包括（但不局限于）创建逻辑拓扑、画布线图、选择布线间和选择线缆。另外，这个设计必须与相应的标准化组织用于设计方面的规则相符。

完成这一课学习的学员应该能够：

- 列出电信间的位置和设计要求。
- 解释线缆管理的设计和规范。
- 列出选择和安装设备架时的需要考虑的因素。
- 解释在考虑电信间的位置、设计和安装时的主要环境、安全性和电力因素。

工作区布线

工作区的布线从房间的电信插口一直延伸到用户的工作站。在连接性方面，工作区的布线设计相对来说比较简单，因此可以相当容易地移动或更改。每一个工作区负责的最大可用楼层空间是10m2。

工作区的设备包括以下几个组成部分：

- 工作站设备，比如计算机、数据终端、电话、传真机和打印机。
- 线缆，比如跳线、模块化线缆、PC适配器线缆和光纤跳线。
- 电信插口外部的适配器。

TIA/EIA-568-B标准规定，每个工作区最少要有两个电信插口。第一个插口必须是四线对

(four-pair)、100Ω的非屏蔽双绞线(UTP)或金属箔屏蔽双绞线(ScTP)和连接器。推荐在这种插口上使用超5类标准。而对于第二个插口，该标准允许的选择有三种：

- 四线对的100Ω的非屏蔽双绞线(UTP)或金属箔屏蔽双绞线(ScTP)和连接头(推荐使用超5类标准)。
- 两芯62.5/125μm或50/125μm光纤和连接器。
- 150Ω的非屏蔽双绞线(STP)和连接头(不推荐用于新的安装工程)。

A.10.9 FARB里的网络应用

如果要对网络所承受的总流量进行估计，那么要先理解流量的本质。比如，数据库的数据传输要消耗很多带宽，视频会议也一样；而Web应用对带宽的占用通常都不高，但涉及音频和视频流的应用除外。

FARB里的IT组已经收集了一份他们经常使用的应用软件的列表。哪一组人需要用什么软件，就由那一组的人自己准备。

你可以在本书附带光盘的Case Study Materials部分找到与FARB和所需软件列表有关的信息。

A.10.10 一切该如何进行?

FARB并没有对它的计划做准备，它没有告诉你用户所处的位置，甚至没有告诉你各部门在建筑物里的哪个区域。但是它已经向你提交了一些设计好的蓝图，在项目中是可以根据它们来决定电信间的位置。

在本书附带光盘的Case Study Materials部分，你可以找到用于指定桌子、管道设备、供热、通风和空调系统、房间，还有电话和照明系统位置的图纸，另外也有建筑物的设计图例、房顶截面俯视图和侧视图。

通常情况下，没有任何一张图纸能包含你所需要的所有信息。而且，有些图纸看上去对你的设计需求并没有太大的作用。然而，它们对于设计出一个符合FARB要求的网络来说是一个很好的开始。

需要留意的是，在这些图纸中，除了在第一层的入口设施和作了标记的接入点之外，并没有任何关于如何确定电信间位置的提示，而且也没有关于哪个部门占用建筑物哪个区域的提示。你可以向教师或者实验教员咨询有关的信息。

下一小节包含了一些提示，学员可以通过这些提示的帮助解决以上的某些问题。

A.10.11 结构化布线案例学习提示

本案例学习可以向你提供在组网和布线技巧练习方面的经验。在进行本案例学习时，目标是为FARB软件开发有限公司设计一个网络的布局。可以通过完成几项任务来达到这个目标，这些任务包括了解对信息的需求，还有从图纸中获得所需的信息。

进行设计时，所需的文档有四种：

1. 一份文件，里面详细说明了总裁Cheryl Farb对将要落成的新FARB办公楼里的网络设施的想法。
2. 一份由内部IP工作组整理的需求文档，而你是这个工作组的成员。该文档列出了哪些东西需要连接到哪里去。
3. 几套关于这栋四层建筑物每一层结构的图纸。
4. 一些详细的图纸，它们可以让你想出一些关于所使用的建筑方法的主意。

建议你多花点时间进行本案例的学习。当你尝试用几种不同的方法去解决问题时，你会发现能从中学到很多有用的东西。另外，与你的同学或同组成员讨论可以有助于巩固你对本案例学习所提

出的重要问题的理解。

指示：找到总裁Cheryl Farb写给内部支持小组的信。这份文件显示了你需要考虑的10个方面的内容。信的最后一部分还有关于公司发展的预测。

以下是这10个方面（其中的一些方面还含有几个小的方面）：

1. 关于网络设备的建议。
2. 关于网络布线的建议。
3. 任何建筑需求。
4. 网络设备的位置。
5. 含有以下几个方面的线路敷设图：
   ——水平和垂直的逻辑布局图。
   ——水平和垂直的逻辑布线布局图。
   ——服务器房间的线路敷设图。
   ——所有MDF和IDF的布局图。
   ——工作区线缆插口的标示图。
6. 服务器房间、MDF和IDF的安全和防火建议。
7. 对设备的电气保护。
8. 网络里所有设备的IP地址安排。
9. 网络实施的成本计划，它包括以下几个方面：
   ——设备购买成本。
   ——布线和测试成本。
   ——设备安装成本。
   ——培训和支持成本。
10. 网络实施的时间线。

接下来是一个含有提示的学习指南，它可以帮助你完成任务。

A.10.12 提示

你可以从附录C“复习题答案”里找到以下问题的答案。

关于网络设备的建议

查看FloorPlan1-Desk-Assignments-building floor1（ground floor）的第一页，回答以下的问题：

这一层的作用是什么？

_____

_____

工人运送货物时会通过哪一扇门？

_____

_____

客人会通过哪些门进来？

_____

_____

在客人签到后，他们很可能会去哪里？

_____

_____

你对使用无线技术的看法如何？

如果有一天，你的部门要为公司安装布线IP安全摄像机，你希望监视哪个区域？

电话公司会从哪里为这栋建筑物铺设电话线路？

需要什么样的锁？

对服务器来说，POP的位置好不好？

如果决定了服务器房间必须与POP分开，那么应该如何选择服务器房间的位置？

可以在POP安装垂直线缆吗？

你会在哪里安装垂直线缆？

水平布线的铺设一定要与墙壁平行。如果通向1.2号房间的线缆要与墙壁平行铺设的话，线缆需要多长？这样可行吗？

2楼

2楼布满了办公室，另外还有一个大会堂的底层。大会堂不但有可能会使用无线设备，而且也会影响线缆的铺设，因为它有几层楼高。

你会把2楼的电信间放在哪个位置？你可能需要考虑使用其中的两个位置。

3楼

3楼的3.1和3.2房间有很大的未规划的空间。如果要把电信间放在3.10房间，你如何为这些空间提供服务，特别是处于远端的3.2房间？

4楼

你留意到在4楼有一块很大的甲板，还有一个宴会区，宴会区里有一台钢琴。你应该如何为这个区域提供网络连接性？

_____

_____

你会把电信间放在哪里？

_____

_____

现在你可以准备去工作了。统计一下每一个电信间需要为多少张桌子提供服务，把这个数字乘以2（每张桌子需要2个插口），再除以16，把结果四舍五入，然后订购这个数量的16口交换机。这是你的网络设备清单里的第一项内容。

你需要机架去放置这些交换机。在开始的时候，为每一个房间订购两个机架。

为特定线路订购足够数量的接线板。记住，有一些网络设备（比如交换机和路由器）必须装配在电信间里。为了正确计算所需接线板的数量，你可以把信息输入到电子制表软件里。

网络布线

在第1步里，你已经确定了每一电信间里所需的工作区插口的数目了。在进行布线时，要使用等级高的线缆，比如超5类或更高。用一把尺子为这些线缆的铺设制定路线。把这些路线的长度全部加起来，以1000为单位进行四舍五入，加上1000，然后再除以1000，这就是你所需的线缆的箱数（每箱线缆1000英尺）。

能进行有效的线缆牵引是很重要的。不要因为节省而使购买的线缆不足，这会导致线缆的重复铺设，而在已有线缆的基础上铺设新的电缆有可能会对原有线缆造成损坏。

其实这里有一个窍门。查看一下名字为“FloorPlan2-Plumbing-and-HVAC-building floor4”的图纸，里面有用水和空调的管道支架。留意一下，里面既有供气管道也有回风管道，而天花板并不是一个隔层天花板。你可以不使用耐热阻燃或垂直线缆。这可以节约相当可观的投资。

建筑要求

你已经决定了要在每一层楼之间使用垂直线缆。这需要在每一层钻洞，而且信号线要穿越楼层，而这又需要导管。

你也已经通过在4楼增加电信间而对其中的一些房间进行了改动。

接下来的步骤

现在你已经对案例学习的其余部分做好准备了。放松，享受一下余下的过程。记住，思考、计划、不成功的开始，还有与小组成员的讨论是这个练习的真正价值所在。

A.11 总结

各种标准的编写都是以促进性能提升为宗旨的。对各种标准的遵循也可以使建筑和安装方法达到统一。比如，电信设施进入用户前端的那一点几乎总是被称为入口设施（EF）；而线缆和设备从由网络供应商负责变为由用户负责的那一点被称为分界点。EF和分界点通常会被安装在一个特意建造的房间里，这个房间被称为电信间（TR）。TR可以具有几个功能中的一个。主交叉连接（MC）把信号分发到一个或多个中间交叉连接（IC）。而中间交叉连接又把信号传到一个或多个水平交叉

连接（HC）处，后者把信号传输到靠近用户的区域（称为工作区）。

工作必须以不伤害工人、公众和环境的方式进行。通常这要求工作区必须标有警告路过人员的记号或锥形桶。另外，梯子的安全性也很重要。一定要确保梯子状况良好，没有任何松动或破损的部分。在使用直梯时，如果可以的话，把它牢固地靠在某种建筑上，另外还要有人扶稳梯子，而且要绝对确保不会有人由于开门而把你从梯子上推下来。如果使用的是活梯，一定要确保梯脚牢固与地面接触，而且横撑杆要完全伸直并固定。不要把活梯当成直梯使用，而且在任何梯子上都不要站得太高。

布线需要专门的工具。布线工人都知道布线时最好使用专门的布线工具，而不要使用替代品。剥线工具的作用是把导线的绝缘外套剥去；导线有很多种，以便安装到不同的连接头里。剪线工具用于把导线剪断，并且不会把里面的线压住。端接工具用于把连接头固定在一条准备好的线缆的末端。每一个安装工人的工具包里都应该有这些基本的工具，但更重要的工具或许是那些用于诊断的工具。一个线缆测试器可以显示线缆里面的每一条导线有没有处在正确的位置，以及是否被正确地端接。

在把线缆牵引到合适的位置时，记住不要穿透防火墙，除非有材料可以补上防火墙的洞。作为挡火物的工具和材料有很多种，不过它们通常都由可以阻止烟雾和火焰蔓延的物质制成。在初始阶段之后，线缆会被牵引和端接，并在修整和完成阶段被安装到接线板和盖板里。完成阶段也是线缆被测试和认证的阶段。认证是指通过把特定的信号发送到线缆上，然后判断特定频率的衰减和净空（headroom）量是否可以接受。认证结果通常会作为布线设备文档的一部分向建筑物所用者提供。

如果在投标中没有中标，就不会有任何的布线工作；面投标中准确地出价需要对施工场所进行彻底的调查和仔细的估算。劳动法规和工会的约束有可能会对项目实施的时间选择造成影响，因此要把这两者考虑在内。每一项工作的外部因素都会对预期的获利造成巨大的影响。

在本材料里提供的案例学习包含了使用一家公司的书面需求和一套蓝图去为一座四层的办公/仓库综合建筑的网络安装制定必需的计划、评估和文档。

A.12 关键术语

ANSI 美国国家标准协会。

骨干（*backbone*） 电信间（TR）与建筑物之间的通路或线缆。

蓝图（*blueprint*） 一张建筑设计图或技术图纸，它提供了建筑项目或已有建筑物的详细情况。

大导轮（*bullwheel*） 一个直径很大的滑轮，通常用于线缆的机械牵引过程。

线缆树（*cable tree*） 一个可以支持很多小型线缆卷的设备。它可以使线缆安装工人同时对多卷线缆进行牵引。

CENELEC 欧洲电工标准化委员会。

串扰（*crosstalk*） 线对里或线对间的信号从发送端到达接收端之后互相结合了。串扰多数发生在电路的发送端。

分界（*demarc*） 服务提供商的线缆与建筑物分布线缆之间的那一点。

分界点（*demarcation point*） 通常是接入提供商设施终止和用户拥有的结构化布线开始的那一点。

设备间（*equipment room*） 存放设备的地方，也可以作为电信间使用。

水平交叉连接（*horizontal cross-connect, HR*） 用接线板或冲压模块把来自工作区的线缆与MC相连的地方。HC可以是电信间、机柜，或者是地面或天花板的安装。

中间交叉连接（*intermediate cross-connect, IC*） 从MC延伸到HC的骨干线缆之间的连接点。

主交叉连接（*main cross-connect, MC*） 通常位于主电信间或主设备间的交叉连接。

物资安全记录表（*material safety date sheet MSDS*） 一份关于使用、存储和处理危险物资的信息的文档。它提供了有关暴露在这些物质下对健康的潜在的影响，以及如何安全地处理这些物质的详细信息。

万用表（*multimeter*） 一个用于确保电信线路上没有电压的测试工具，大多数的这种设备可以测量交流电和直流电的电压、电流、电阻、二极管、连续性和晶体管。

多用户电信插座组件（*multiuser telecommunications outlet assembly, MUTOA*） 在那些使用了模块化设备的工作区使用的一带有多个插口的设备，计算机和电话的插头可以直接插到MUTOA里。

NEC（美国） 国家电气规程。

NFPA（美国） 国家防火协会。

OSHA（美国） 职业安全与健康管理局。

接线电缆（*patch cable*） 两端都有连接头的线缆，用于把信号从一台网络设备传输到另一台。

跳线（*patch cord*） 在交叉连接里用于连接不同线路的线缆。

接线板（*patch panel*） 用于把数据网络或语音系统与物理线缆网络相连的设备。接线板背后是经过冲压的网络线缆，而接线板的前面是某种类型的、出厂时已端接好的接口。

天花板隔层（*plenum*） 作为空气回流管道使用的敞开的天花板，用于加热、通风和空调系统。

配线管道（*raceway*） 用于承载线缆的管道。配线管道包括普通电气线路、特别的线缆盘或梯架、地板内管道系统、还有塑料或金属表面安装（surface-mounted）管道。

结构化布线系统（*structured cabling system, SCS*） 综合的布线计划，其中包含了连接头、线缆布设、

分布中心和由特定公司制定的安装技术的内容。

结构化布线（*structured cabling*）　遵循了各种标准的统一的布线系统。这些标准定义了实际线缆、布线距离、线缆类型和端接设备的类型。

时域反射计（*time domain reflectometer, TDR*）　可以测量安装线缆的长度并定位出错点的设备。工作时，它往线缆发送一个信号，测量信号返回的时间，从而完成任务。

TIA　电信工业协会。

电信间（*telecommunications room, TR*）　建筑物内用于存放电信线缆系统设备的区域。

垂直布线（*vertical cabling*）　用于骨干之间交叉连接的骨干线缆、中间和主交叉连接、机械端接和跳线。

工作区（*work area*）　使用计算机、电话和其他网络设备的地方。



附录B　术语表

术语表见随书附盘。



附录C 复习题答案

本附录中包含了各章末尾“复习题”的答案。

第1章

1. 因特网中的连接可以分为以下哪些部分？
   D. 以上全部
2. 计算机的主要线路板是指什么？
   B. 主板
3. 什么是PCMCIA插槽？
   A. 膝上型电脑插槽
4. 什么是NIC？
   B. 一种可以提供网络连接的印刷电路板
5. 安装网卡时，以下哪些能力是必须具备的？
   D. 以上全部
6. 什么数制是基于2的乘方的？
   C. 二进制
7. 匹配以下短语以及它们的定义
   （1）比特
   （2）字节
   （3）kbit/s
   （4）MHz
   a. 计算机数据的最小单位
   b. 计算通过网络连接传输的数据量的标准单位
   c. 频率单位，用于描述状态转换速度，声波、交流电、其他循环波形的周期
   d. 用于描述数据文件大小、磁盘或者其他存储介质空间、通过网络传输的数据量的单位
   答案：1-A，2-D，3-B，4-C
8. 1字节可以表示的最大十进制数是多少？
   C. 255
9. 十进制数151转化成二进制数的结果是多少？
   B. 10010111

10. 二进制数11011010转化为十进制数的结果是多少?

C. 218

11. 二进制数0010000100000000转化为十六进制数的结果是多少?

A. 0x2100

12. 十六进制数0x2101转化为二进制数的结果是多少?

A. 0010 0001 0000 0001

13. 以下关于ping的说法，哪个是正确的?

D. 以上全部

第2章

1. 下面哪一项是首个实现的微型计算机网络类型?

C. 局域网

2. 如果使用modem连接10台计算机，需要多少个modem?

C. 10

3. 写入到网络接口卡上的编码是什么?

B. MAC地址

4. 哪种物理拓扑结构的所有节点直接连接到一个中心节点且在节点之间没有其他连接?

C. 星型

5. TIA和EIA代表什么?

B. 电信工业协会（Telecommunications Industry Association）和电子工业联盟（Electronic Industries Alliance）

6. 局域网完成以下哪些工作?（选择所有正确的项）

A. 在一个有限的地理范围内运作

B. 允许多个用户同时接入高带宽物理介质

D. 提供本地服务器的全时连接

7. 下面哪个句子最好地描述了广域网?

A. 它连接被大的地理区域分割开的局域网络

8. 下面哪个句子正确地描述了城域网?

C. 城域网是跨越一个城市（都市或郊区）的网络

9. 下面哪一项不是存储区域网（SAN）的特征?

D. 存储区域网使系统和数据的可用性最小化

10. 以下哪个在共享的公共网络基础设施上提供安全、可靠的连接?

B. 虚拟专用网

11. 下列哪个在共享基础网络设施上把企业总部、远程办事处以及分支机构连接成一个内部网络?

B. Intranet VPN

12. 公司网络中可以用来选择诸如雇员、客户和合作伙伴之类的团体的那一部分网络叫什么?

B. 企业外部网

13. 对象在模型各层间的运动叫什么?

B. 流（flow）

14. OSI参考模型有几层?

D. 7

15. OSI参考模型是什么?

D. 以上全部

16. 下面哪一项是网络各层的正确顺序?

B.

（1）物理层

（2）数据链路层

（3）网络层

（4）传输层

（5）会话层

（6）表示层

（7）应用层

17. OSI模型的哪一层涉及物理寻址、网络拓扑结构、网络介质访问以及流量控制?

B. 数据链路层

18. 以下哪一项最好地定义了封装?

D. 把数据打包在一个特定的协议报头中

19. 在一个局域网上从主机A向主机B发送一封电子邮件，在开始发送电子邮件以前，必须对数据进行封装。下面哪一项最好地描述了在生成一个分组以后所发生的事情?

B. 分组被放到一个帧里

20. 在TCP/IP模型中，哪一层处理关于可靠性、流量控制和错误校正等问题?

B. 传输层

21. 对于下面的哪些问题中继器可以提供一个简单的解决方案?

D. 过多的节点或线缆不足

22. 关于网桥和它的转发决策，下面哪一项是正确的?

C. 它们运行在OSI的第2层而且使用MAC地址来做出转发决策

23. 关于交换机的功能下面哪一项是正确的?

B. 结合了集线器的连接功能和网桥的流量管理功能

24. 路由器会对什么作出路由选择?

C. 第3层的分组

25. 下面哪一项是正确的?

C. DSLAM 充当无数用户设备和通信公司网络之间的接口

26. 下面哪些是AAA服务器的功能?（选择所有正确的项）

D. 上述答案都正确

27. 下面哪些是防火墙的功能?（选择所有正确的项）

A. 基于软件的

B. 基于硬件的

C. 过滤通信流

第3章

1. 搭配左右两列：

1）中子　A）带负电荷的粒子

2）质子　B）不带电荷（中性）的粒子

3）电子　C）带正电荷的粒子

C. 1-B，2-C，3-A

2. 下列关于电的描述哪项不正确？

D. 以上都不是。

3. 搭配下列的度量和其各自的单位：

1）电压　A）欧姆

2）电流　B）安培

3）电阻　C）伏特

D. 1-C，2-B，3-A

4. 电子在_____环路里流动，叫作_____。

D. 闭合；电路

5. STP的最大缆线长度是多少？

C. 100米

6. 多少对线组成一条UTP电缆？

B. 4

7. UTP使用哪种接头？

C. RJ-45

8. 同轴电缆相比STP或UTP的优点是什么？

C. 在不增压的情况下能传输更远的距离。

9. 双绞线电缆中电线相互绞合的作用是什么？

C. 减弱噪声问题。

10. EIA/TIA的标准的重要性是什么？选择所有适合的。

B. 为制造商保证兼容性提供了可以遵守的指导原则。

C. 提出了多产品和多厂商环境下最低的介质要求。

11. _____光缆传输多束发光二极管产生的光。

A. 多模

12. 在网络中使用光缆的一个优点是什么？

D. 相比同轴或双绞线电缆，传输速率更高。

13. 哪种光缆通常用于室外安装？

D. 松套型。

14. 通常用于单模光纤的光源是哪种？

B. 激光

15. 哪一个术语描述了光线射到玻璃表面的角度？

C. 入射角

16. 调制是改变振幅、频率或周期的过程，哪一个缩写代表一种调制类型？

D. RM

17. 下列哪一个范围没有正确标识一个无许可证的频率？

C. 9GHz

18. 哪一项不是关于扩频技术优点的描述？

A. 扩频传输的速率高。

19. 以下哪一项没有描述顺序扩频（DSSS）的特征？

C. DSSS技术的数据吞吐量低，接入范围小。

20. 下列哪一项不是有线对等保密（WEP）的特征？

C. WEP的一个目标是拒绝没有适当WEP密钥得未经授权用户接入网络。

第4章

1. 下列哪一项属于802.3u的规范？
   C. 100BASE-TX
2. 下列哪一项是关于以太网连接的最恰当描述？
   C. 在用户级与网络设备间使用快速以太网作为链路，以支持接入链路上来自各个以太网段的聚集通信。
3. 下列哪个标准组织制定了用于支持以太网实现的线缆和接头规定？
   C. TIA/EIA
4. 下列关于介质接头的描述，哪项不正确？
   A. RJ-45连接接头是一个主要用于终结同轴电缆的8针接头。
5. 以下哪一项不需要配备交叉线缆？
   B. 连接路由器和交换机
6. 哪项技术不属于无线通信？
   B. 宽带
7. 下列哪项不是有线对等保密（WEP）的特征？
   B. WEP是在802.3标准中定义的安全机制。
8. 以下哪项不属于广域网实现？
   D. 以太网
9. 广域网使用哪种类型的数据传输方法？
   B. 串行
10. 哪一项对DCE的描述最恰当？
    D. 组成用户-网络接口中网络端的设备
11. 下列哪种介质用于连接ISDN BRI端口到服务提供商的设备？
    A. CAT 5 UTP直通线缆
12. 哪种接头用于DSL连接？
    B. RJ-11
13. 哪种接头用来连接路由器和有线电视系统？
    C. F
14. 哪种线缆用来连接终端和控制台端口？
    B. 反转

第5章

1. 下面哪个不是被当成IEEE的子层之一？
   B. 数据链路层
2. IEEE子层与OSI参考模型中的哪层相关？
   B. 1和2
3. 子层中的LLC，执行_____进程。
   B. 封装
4. MAC地址的前6个16进制数代表_____。
   B. 组织惟一标识符
5. MAC地址有_____位长。
   C. 48

6. 解释以太网工作的访问方法的名称是?

B. CSMA/CD

7. MAC地址位于?

C. NIC

8. 下列哪个叙述将局域网中两台设备之间的通信描述得最好?

A. 源设备将数据封装在帧中并传送出去，该帧包含有目标设备的MAC地址。局域网中的每个人都可以看到，但那些地址不匹配的设备将忽略该帧

9. 哪些功能与帧有关?

D. 以上全部

10. 局域网上的计算机如何判断帧中的错误?

C. 它检查帧中的FCS与计算机从帧内容计算出来的是否一致。

11. 介质访问控制是指什么?

C. 决定在共享介质环境中的计算机是否被准许传输数据的协议。

12. 下面哪个描述最符合CSMA/CD网络?

A. 一个节点的传输内容在整个网络中传送，网络上每个节点都接收和检查该内容。

13. 在以太网或者IEEE 802.3局域网中，什么情况下会发生冲突?

B. 当两台主机侦听流量信息，都侦听到没有流量，于是同时传输数据时。

14. 下列哪一个是第2层数据链路层的重要功能?

D. 以上全部

15. 下列哪个是以太网帧错误类型?

D. 以上全部

16. 那个协议是非确定性协议?

B. CSMA/CD

17. 关于确定性MAC协议哪个说法是正确的?

C. 在传输数据时它允许主机“排队”发送数据。

18. 数据分组产生和冲突的网络区域被称为_____?

A. 冲突域

19. 下列哪个描述广播最准确?

A. 同时传送一个帧到多个主机。

20. 使用中继器会_____冲突域。

C. 扩展

21. 使用复杂的网络设备，像网桥、交换机和路由器来划分冲突域的过程被称为：

B. 分段

第6章

1. 以太网中采用何种方法来阐明以太网的工作?

B. CSMA/CD

2. 不使用中继器的粗以太网的最大距离是多少?

C. 500 m（1640.4英尺）

3. 10Mbit/s以太网的工作受到计时限制，这是由不超过_____个中继器所划分的一系列不超过_____个分段所提供的。

C. 4，5

4. 快速以太网所支持的传输速率达到多少?

C. 100Mbit/s

5. 识别出两个吉比特以太网电缆规范。

C. 1000BASE-SX

D. 1000BASE-LX

6. 1000BASE-SX的传输介质是什么?

D. 多模光纤上短波激光

7. 4D-PAM5编码方法用于下列何种吉比特以太网?

C. 1000BASE-T

8. 10 Gbit以太网的IEEE标准是什么?

C. 802.3ae

9. 下列哪一个不是微分段的特点?

D. 它增加了冲突

10. 下列哪一个被LAN交换机用于转发决定?

B. MAC地址

11. 下列哪一个是全双工传输的特点?

D. 以上全部

12. 三种常见类型的交换方法是_____、_____和_____。

答案：存储转发、直通式和无碎片式

13. 生成树协议容许下列哪一种情况?

B. 一条冗余的网络路径，不受网络中环路的影响

14. 下列哪一个不是STP端口状态?

D. 传输

15. 下面哪一个关于网桥和其转发决定是正确的?

C. 网桥工作在OSI第2层，用MAC地址来作决定

16. 下列哪一个不是网桥的特点?

C. 它们不作任何转发决定

17. 下列哪一个是微分段的正确陈述?

A. 每个工作站得到自己专用的分段通过网络

18. 下列哪一个关于LAN交换机是正确的?

B. 它们是很高速的多端口网桥

第7章

1. TFTP使用传输层的哪种协议?

C. UDP

2. 下面哪个是传输层的基本服务?

D. 以上全部

3. 下面哪种协议工作于TCP/IP Internet层?

D. 以上全部

4. DHCP客户端启动时发生的第一件事情是什么?

C. DHCPDISCOVER

5. 网络层是怎样从源向目的转发分组的?

A. 通过使用路由表

6. 如果一台设备不知道相邻网段上的另一台设备的MAC地址，那么它将向谁发送ARP请求？

D. 以上全部

7. RARP请求中有什么？

A. 一个MAC头和RARP请求消息

8. IP地址的两个部分各是什么？

A. 网络地址和主机地址

9. 哪种Internet协议将一个已知的IP地址映射到一个未知的MAC地址？

C. ARP

10. 下面哪个会发起ARP请求？

D.在ARP表中无法定位目的MAC地址的设备

11. 下面对ARP表的描述哪个是最佳的？

D. 每个设备上都有的一段映射IP地址和MAC地址的内存

12. 下面对ARP回应的描述哪个是最佳的？

A. 设备将自己的MAC地址发送回源主机以响应其ARP请求

13. 为什么保持当前更新ARP表非常重要？

B. 可以限制广播的数量

14. 为什么要产生RARP请求？

A. 源主机知道自己的MAC地址，但不知道自己的IP地址

15. 下列对TCP/IP的描述哪个是最佳的？

A. 一套可以用来穿越许多相互连接的网络进行通信的协议

16. 下列哪个不是描述TCP/IP协议栈的？

A. 非常接近的对应OSI参考模型的上层

17. TCP/IP协议集指定了OSI模型的哪一层？

C. 3、4层以及5到7层

18. 下列哪个不是网络层的功能？

D. UDP提供无连接的数据报交换，并无确认机制

19. 下列哪个协议可以在传输层中找到？

B. UDP

第8章

1. 一个IP地址由多少比特构成？

B. 32

2. IP地址中每个8比特字节的最大值是多少？

B. 255

3. 在IP地址中网络号扮演什么角色？

A. 它确定了主机所属的网络

4. 在IP地址中主机号扮演什么角色？

B. 它确定了子网络中哪一个节点存在编址

5. 二进制数101101转换为十进制数是多少？

C. 45

6. 将十进制数192.5.34.11转换为二进制数是

A. 11000000.00000101.00100010.00001011

7. 将二进制数IP地址11000000.00000101.00100010.00001011转换为十进制是

D. 以上都不是

8. 下面哪一部分是B类地址154.19.2.7的网络地址?

B. 154.19

9. 下面哪一部分是IP地址129.219.51.18的网络地址?

A. 129.219

10. 下面哪一个地址是带有子网掩码255.255.0.0的网络123.10.0.0的广播地址?

B. 123.10.255.255

11. 一个C类网络中有多少个可用主机地址?

B. 254

12. 一个B类网络中最多可以有多少个子网?

D. 以上都不是

13. 在划分子网时至少可以借几位?

B. 2

14. 使用子网的主要原因是什么?

C. 减少广播域的尺寸

15. 子网掩码由多少比特构成?

C. 32

16. 对IP地址131.8.2.5和255.0.0.0执行与运算，得到的网络地址是多少?

D. 以上都不是

17. 在C类网络中划分子网最多可借多少位?

C. 6

18. 对于C类网络地址197.15.22.31和子网掩码255.255.255.224，在划分子网时最多可借多少位?

C. 3

19. 对IP地址172.16.2.120和255.255.255.0执行与运算，得到的子网地址是多少?

C. 172.16.2.0

20. 下面哪一条是对OSI模型第3层——网络层的最佳描述?

C. 它决定数据在网络中传输时的最佳路径

21. 路由器的哪个功能是用来评估路径并确定转发数据报的首选路径?

B. 路径选择

22. 网络层是如何将分组从源发送到目的地的?

A. 通过使用IP路由选择表

23. 网络层地址的哪两个部分被路由器用来在网络中传送数据?

A. 网络地址和主机地址

第9章

1. 当你和母语不同的人交谈时，也许需要重复你所说的话并且放慢讲话速度。重复谈话可以比喻成传输层_____功能，放慢说话的速度可以比喻成传输层_____功能。

A. 可靠性；流控

2. 以下特点描述了哪种TCP／IP协议：面向连接；重传任何没有接收到的数据；将向外发送的消息分成数据分段。

B. TCP

3. TCP数据分段中的窗口字段表示什么含义?

D. 接收设备期望接收的8位字节的数量

4. 哪种传输协议交换数据报，不需要确认和传送保证机制?

A. UDP

5. TCP和UDP使用什么在同一时间对网络的不同会话进行跟踪?

A. 端口号

6. 开始传输数据前，TCP如何对源设备和目的设备之间的连接进行同步?

B. 三次握手

7. 哪个范围的端口号没有进行规定?

D. 1023以上

8. 在TCP传输过程中，如果某个数据分段发送之后在一定时间内没有接收到确认信息，会发生什么情况?

D. 开始重传

9. 下面哪个选项最佳描述了流控?

C. 防止缓冲溢出的方法

10. 下面哪个选项最佳描述了TCP / IP协议栈的功能?

C. 按照数据报的序号把消息从一台主机传送到另一台主机

11. 下面哪个协议是传输层协议?

B. UDP

12. 端口号的作用是什么?

A. 跟踪在同一时间通过网络的不同上层会话

13. 为什么要使用TCP三次握手/开放连接？选择所有可能的选项。

A. 如果以后传输中有错误出现，可以恢复丢失的数据

B. 决定接收设备每次能够接收多少数据

14. 动态TCP窗口字段的功能是什么?

C. 在TCP会话中允许动态协商窗口大小，从而更有效地利用带宽

15. UDP数据分段利用什么协议提供可靠性?

B. 应用层协议

16. 网络重定向器使得数据传送到_____?

D. 以上都不是

17. 客户端/服务器应用程序的实例是?

A. 电子邮件

18. 在客户端/服务器应用中，客户端的角色是?

B. 服务请求者

19. 以下哪个选项最佳描述了域名?

A. 代表Internet站点的数字地址

20. COM域名通常分配给_____?

D. 公司

21. 在一个Telnet连接过程中，远程主机负责什么?

B. 处理工作

22. Telnet主要工作在OSI参考模型的哪3层?

D. 应用层、表示层、会话层

23. 一般来说，匿名FTP会话使用_____作为登录ID，使用_____作为密码？

A. Anonymous；用户E-mail地址

24. 重定向器不和特定应用程序协同工作，那它和什么协同工作？

A. 计算机操作系统

第10章

1. 下面哪一项最准确地描述了广域网？

A. 连接地理上相隔很远的局域网

2. 广域网和局域网的区别是什么？

A. 广域网主要是通过低速的串行接口访问

3. 下列哪些是广域网技术的例子？

B. 帧中继，ISDN

4. 广域网标准描述了OSI模型的哪些层？

D. 物理层和数据链路层

5. 下列哪项最准确地描述了数据电路终结设备（DCE）？

D. 由位于广域网连接末端的物理设备组成

6. 下列哪些部件提供了与语音级服务的接口，与T1/E1接口的信道服务单元/数字服务单元（CSU/DSU），与综合业务数字网（ISDN）接口的终端适配器/网络终端器（TA/NT1）？

C. 调制解调器

7. 下列哪种设备主要用于提供拨入和拨出的用户连接？

D. 通信服务器

8. 广域网物理层和数据链路层的标准包括：

D. 以上全部

9. 将下面的部件与功能进行匹配

1）RAM/DRAM

2）NVRAM

3）ROM

4）闪速存储器

5）接口

选项：

a. 当一个单元断电后仍能保持其内容的RAM

b. 可以被微处理器读写的易失性内存

c. 可以被微处理器读但不可写的易失性内存

d. 可以电擦除和重新编程的非易失性存储器，可以根据需要存储、启动和重写软件映像

e. 两个系统或设备之间的连接

选择你的答案：

D. 1-b, 2-a, 3-c, 4-d, 5-e

10. 互联网络可能提供：

D. 以上全部

11. 下列哪些是广域网的数据链路层的封装：

D. 以上全部

12. 路由器的主要功能有哪些？

D. A与B

13. 哪一项是IBM设计的，针对系统网络结构（SNA）环境设计的，现在已大多被更通用的HDLC替代的广域网数据链路？

C. 同步数据链路控制协议

14. 那种广域网数据链路协议用于ISDN D信道的信令和呼叫建立？

A. LAPD

15. 哪些属于广域网电路交换服务：

D. A和C

16. 哪一种服务已经成为非常流行的广域网技术？它比X.25的效率更高但提供的服务类似，最大带宽为44.736Mbit/s，并能提供非常受欢迎的56-Kbit/s和384-Kbit/s。

A. 帧中继

17. 哪些属于信元交换技术：

D. A和B

18. 哪些属于常见的DSL技术？

D. 以上全部

19. 下列哪项是一个甚高速物理层技术家族，它能提供一系列的数据速率并且都有专用的标识，它可以实现在从51.84Mbit/s（OC-1）到9952Mbit/s（OC-192）的不同光载波（OC）上，能通过波分复用（WDM）实现这些令人惊奇的数据速率？

A. SONNET

20. 下列哪种类型的路由器构成了用于源自其他网络或发往其他网络的流量的主要路径？

C. 骨干路由器

第11章

1. 路由器初始化时会完成下列那项？

C. 加载自举程序、setup程序和操作系统

2. 在路由器的setup过程中，哪个组合键可以用于退出该过程？

C. Ctrl-C

3. 将右边的配置参数设定与左边这些建立一个超级终端会话所需的项进行匹配：

A. 波特率　　无
B. 数据位　　1
C. 奇偶校验　8
D. 停止位　　无
E. 流控制　　9600

答案：波特率 = 9600
数据位 = 8
奇偶校验 = 无
停止位 = 1
流控制 = 无

4. 针对初始启动的输出，下列哪一项是正确的？

A. 能看到路由器使用的Cisco IOS软件版本

5. 针对初始启动的输出，下列哪一项是正确的？

A. 能看到Flash存储器的容量

6. 将左侧的命令与右侧的描述进行匹配。

Ctrl + a	退出配置模式
Ctrl + b	移动到命令行的末尾
Ctrl + e	向后移动一个词
Ctrl + f	移动到命令行的起始位置
Esc + b	向前移动一个字符
Esc + f	向前移动一个词
Ctrl + z	向后移动一个字符

答案：

Ctrl + a	移动到命令行的起始位置
Ctrl + b	向后移动一个字符
Ctrl + e	移动到命令行的末尾
Ctrl + f	向前移动一个字符
Esc + b	向后移动一个词
Esc + f	向前移动一个词
Ctrl + z	退出配置模式

7. 将左侧的命令与右侧正确的描述进行匹配。

Tab	启动高级编辑功能
Ctrl + p	设定命令缓冲区的大小
Ctrl + n	重用最近的命令
show history	显示命令缓冲区
terminal history size #	重用上一条命令
terminal editing	完成输入
no Terminal editing	禁用高级编辑功能

答案：

Tab	完成输入
Ctrl + p	重用上一条命令
Ctrl + n	重用最近的命令
show history	显示命令缓冲区
terminal history size #	设定命令缓冲区的大小
terminal editing	启动高级编辑功能
no Terminal editing	禁用高级编辑功能

8. 典型路由器配置的主要元素包括：

A. 口令、接口、路由选择协议、DNS

9. 下列哪项正确地描述了一种用于指定路由器如何装载Cisco IOS软件的方法？

A. 在NVRAM中指定路由器可以使用的回退软件来源序列[w4]

10. 下列哪项不是一个可以通过配置寄存器的启动字段设定的启动选项：

C. Cisco IOS软件自动从TFTP服务器上启动

11. 下列哪一项是通过Cisco IOS软件show version 命令显示的信息？

B. 系统映像的名称

12. 下列哪一项中包含一个受限版本的路由器Cisco IOS 软件？

A. ROM

13. 如果你想彻底退出配置模式，需要输入下列哪一项？

A. Exit

14. 如果你计划配置一个接口，路由器应该处于哪个提示符？

D. router（config-if）#

15. 下面哪个缩写用于描述Cisco路由器的基于文本的用户界面？

A. CLI

16. 对于Cisco路由器，存在哪两种访问路由器命令的模式？

A. 用户与特权

17. 在Cisco路由器上，你用哪种模式改变路由器的配置

B. 特权

第12章

1. 什么是标准？

B. 广泛使用或者官方规定的一套规则或规程

2. 接口上描述信息的用途？

C. 显示关于接口的注视信息。

3. 哪一项是一个好的登录横幅？

C. 只允许授权的访问

4. 什么是主机名解析？

A. 将名称与网络位置相关联的过程

5. 配置备份和文档说明对组织维护一个高效网络是必需的。正确还是错误？

A. 正确

6. 配置文件的备份不是必需的。正确还是错误？

B. 错误

7. TFTP服务器是备份文件惟一能存放的位置。正确还是错误？

B. 错误

8. 如果你计划配置一个接口，应该在哪种提示符下进行？

D. router（config-if）#

9. 下列哪一项是配置路由器过程的正确顺序？（假设你已经在配置模式下对路由器进行了变更。）

B. 检查结果，决定变更是否是想要的结果，保存变更到备份，检查备份文件

10. 下列哪项命令能用于将路由器配置保存到备份？

A. Router# copy running-config tftp

11. 下列哪项正确地描述了路由器上口令的配置？

C. 可以为所有的入向Telnet会话设定相同的口令

12. 下列哪一项没有正确描述路由器上的口令配置？

A. 每个配置模式下都可以设定口令

13. 哪种模式用于改变整个路由器的单行命令？

A. 全局配置模式

14. 在提示符为Router（config-if）的配置模式下，exit命令的作用是什么？

A. 退出当前的接口配置模式

15. 哪些是典型路由器配置的要素？

A. 口令、接口、路由选择协议、DNS

16. 口令恢复过程中，在路由器启动时执行Ctrl-Break后，紧接着配置寄存器的设置应该为

多少？

B. 0x2142

17. 在口令恢复过程中，在保存运行配置之前，在启用的新加密口令之后，配置寄存器的值应该是多少？

A. 0x2102

第13章

1. 什么是telnet的定义？

C. 一个用来检查源和目的站点间应用层软件的命令，是最全面的可用测试机制

2. 使用show interfaces serial命令测试网络时，会提供什么信息？

A. 显示线路和数据链路协议的状态

3. show cdp neighbors命令为每个CDP邻居提供了什么信息？

D. 以上全部

4. show cdp interface命令显示以下哪项？

D. A和B

5. 关于show cdp entry [*device name*]命令的输出，以下哪项是正确的？

A. 显示邻居路由器的所有第3层地址

6. 为了显示show cdp neighbors和show cdp entry [*device name*]命令的共同信息，使用以下哪个命令？

A. show cdp neighbors detail

7. show cdp neighbors命令显示什么信息？

D. 以上全部

8. 使用ping命令后获得的4项重要信息是什么？

A. ICMP分组的数量和大小；超时时限；成功率；往返时间的最小值、平均值和最大值

9. 使用traceroute命令测试网络时，将提供哪些信息？

C. 映射分组传输到目的网络过程中经过的每个路由器

10. 在应答ping命令时，惊叹号（!）表示什么含义？

A. 成功回应的数量

11. 关于路由器debug命令，下面哪个描述是正确的？

D. A和B

第14章

1. 下面哪一项正确描述了指定一个路由器如何加载Cisco IOS软件的方法？

A. 从NVRAM中按顺序指定路由器可以使用的后退源。

2. 下面哪一项不是可以配置寄存器引导字段所设置的引导选项？

C. 从TFTP服务器自动引导Cisco IOS软件。

3. 下面哪一项是show version命令显示的信息？

B. 系统映像的名称。

4. 哪一个命令用来发现配置寄存器的设置？

C. show version

5. 哪一个信息不是在Cisco映像文件名系统中提供的？

D. 映像的大小

6. 从TFTP服务器加载新的Cisco IOS软件映像到闪存中时，下面的哪一项不是该推荐进程的一部分？（该进程按照正确的顺序列举）

B. 输入copy flash tftp命令，开始从服务器下载新的映像。

7. 如果配置寄存器设置为0x101，哪一项是路由器的初始引导尝试？

C. ROM

8. 下面的哪一项拥有一个受限版本的路由器Cisco IOS软件？

A. ROM

9. 如果配置寄存器设置为0x102，哪一项是路由器的初始引导尝试？

D. 检查boot system命令

10. 下面的哪一项是路由器用来自动后退定位Cisco IOS软件的顺序？

D.（1）TFTP服务器，（2）闪存，（3）NVRAM

11. 下面哪一项不是show version命令显示的信息？

A. 配置接口的统计信息

12. 下面哪一项正确描述了使用TFTP服务器将软件复制到闪存的准备工作？

A. TFTP服务器必须是一个可连接的路由器或主机系统，例如一个UNIX工作站或一个膝上型电脑。

13. 为什么要创建一个Cisco IOS软件映像备份？

D. 为了在更新新版本之前创建当前映像的一个后退拷贝。

14. 如果想要从TFTP服务器下载一个新映像来升级一个旧版本Cisco IOS软件，应该使用下面哪个命令？

B. copy tftp flash

第15章

1. 下面哪一项正确描述了OSI模型中第3层（网络层）的功能？

C. 为通过网络的通信流量确定最佳路径

2. 下面哪一功能允许路由器估计到达目的地的可用路由，并建立分组的优先处理操作？

B. 路径确定

3. 网络层如何从源向目的转发分组？

A. 使用一个IP路由选择表

4. 路由器使用网络层地址的哪两个部分转发穿越网络的流量？

A. 网络地址和主机地址

5. 下面哪一项正确描述了被路由协议？

A. 为主机间的分组传送提供足够的信息

6. 下面哪一项正确描述了路由选择协议？

A. 一种通过执行一个算法来完成路由选择的协议

7. 距离矢量路由选择算法的优点之一是：

D. 计算简单

8. 下面哪一项最好地描述了链路状态算法？

A. 重建整个互联网络的精确拓扑

9. 路由环路为何会发生？

A. 互联网络发生变化后缓慢收敛的发生

10. 下面哪一项正确描述了平衡混合路由选择？

A. 确定最佳路径，但是拓扑变化会触发路由选择表更新

11. 只有一条路径到路由器的网络称作什么？

D. Stub网络

12. 哪一项最好地描述了默认路由？

C. 当目的网络没有明确列在路由选择表中时使用

第16章

1. 初始时路由器使用哪类路由？

A. 关于直连网络或于网的路由

2. 下面那一项最恰当地描述了一条静态路由？

B. 显式配置和添加到路由选择表中的一条路由，优先于动态路由选择协议所选择的路由

3. 下面那一项最恰当地描述了一条默认路由？

A. 用来转发帧的一条路由选择表项，其目的网络没有明确列在路由选择表中

4. 外部路由选择协议的用途是什么？

C. 自治系统间的通信

5. 内部路由选择协议的用途是什么？

D. 用于一个单个自治系统内

6. 下面哪一项是全局任务？

B. 启用路由选择协议，比如RIP或IGRP

7. RIP使用下面哪个度量标准来确定消息传输的最佳路径？

B. 跳数

8. 你怀疑网络中的某台路由器在发送错误的路由选择信息，用什么命令来检查？

B. router show ip route

9. 为什么要显示IP路由选择表的内容？

B. 为了识别目的网络和对应的下一跳地址

10. 如果想知道路由器配置了哪种路由选择协议，应使用哪条命令？

D. router> show ip protocol

11. 在下面这个命令中，最后一个数字代表的是什么含义？

Router（config）# ip route 2.0.0.0 255.0.0.0 1.0.0.2 5

C. 管理距离

12. 管理距离为15代表了什么含义？

C. 路由选择信息的来源相对可信

13. 如果想在互联网中添加一个新的局域网，并且通过手工的方式将该网络添加到路由选择表中，你应该使用什么命令？

B. router（config）# ip route 2.0.0.0 255.0.0.0 1.0.0.2

第17章

1. ICMP是IP协议的差错报告协议。正确还是错误？

A. 正确

2. ICMP代表什么？

D. Internet Control Message Protocol

3. ICMP消息和其他使用IP协议传送的数据一样被封装在数据报中。正确还是错误？

A. 正确

4. 如果数据报要传送到本地网络以外，则必须配置一个缺省网关。正确还是错误?

A. 正确

5. TTL代表什么?

B. Time-To-Live

6. 所有的ICMP消息格式都以下面的哪个字段开始?

D. 以上所有

7. 只有出现下列哪种情况时，缺省网关才会发送ICMP重定向/改变请求?

E. 以上全部

8. ICMP时间戳消息的类型字段值可以是13（时间戳请求）或者是多少?

A. 14，时间戳应答

9. 所有的时间戳应答消息都不包含初始、接收和传送时间戳。正确还是错误?

B. 错误

10. 路由器恳求消息的ICMP类型值是哪多少?

B. 10

第18章

1. 当技术人员进行基础的网络测试时，下列哪一项是对的?

A. 该技术人员应按顺序从OSI参考模型的一个层到下一个层来进行。

2. 当一个技术人员对网络进行故障诊断时，他/她应该开始一种什么方法?

A. 该技术人员应该开始一种结构化的方法。

3. 当一个技术人员排除一个网络故障时?

A. 从第1层开始

4. 如果一个技术人员想测试网络的连通性，应使用哪个基本命令?

B. ping

5. 当一个网络管理员想在源和目的工作站之间验证应用层的软件，应使用以下哪个命令?

B. telnet

6. 你怀疑你的网络上某个路由器正发送错误的路由信息。你可以使用那个命令来检查?

B. router#show ip route

7. 为什么要显示IP路由选择表?

D. 为了设置路由器的参数和过滤器

8. 如果你想在路由器发送和接收RIP路由选择更新时查看这些信息，你应该使用哪个命令结构?

C. router# debug ip rip

9. debug命令的动态输出会导致_____处理器负载从而造成性能的浪费?

A. 高

10. 默认情况下，路由器发送debug的输出信息和系统信息到哪里?

A. 控制台

11. telnet命令提供哪种类型的终端?

B. Virtual

12. ICMP代表什么?

C. Internet Control Message Protocol

13. 许多网卡的接口用于显示是否存在一个合法连接的指示灯是以下哪种类型?

A. Indicator

14. telnet在OSI参考模型的哪一层上使用?

D. 第7层

15. 如果路由选择协议没有启用或者IP地址检测不到，管理员应从OSI模型的哪一层开始检查?

C. 第3层

第19章

1. 下面哪一项最准确地描述了TCP/IP?

A. 用于跨越各种互联网络进行通信的一套协议

2. 下面哪一个属于传输层协议?

B. UDP

3. 端口号的作用是什么?

A. 跟踪网络中同时发生的不同会话

4. 下面哪一项最准确地描述了UDP?

D. 交换数据报无需确认或传输保证的协议

5. 下列TCP/IP的哪一层包含文件传输、电子邮件、远程登录和网络管理的功能?

B. 应用层

6. 为什么使用三次握手建立连接?

A. 确保发生问题后丢失数据可以恢复

7. TCP滑动窗口的作用?

C. 在TCP会话中允许动态协商窗口尺寸，从而更有效利用带宽

8. UDP分段使用什么协议提供可靠性?

B. 应用层协议

9. 下面哪一个最好地描述了窗口尺寸?

B. 等待确认时能传输的消息字节数

10. ARP的功能是什么?

C. 用于建立一个IP地址到MAC地址的映射

第20章

1. 普通ACL功能包括内部地过滤分组，保护内部网络免受互联网的非法访问，限制虚拟终端的访问。这种说法是否正确?

A. 对

2. ACL是一种:

D. 访问控制列表

3. 哪种ACL通过比较源地址来定义ACL的规则?

C. 标准型

4. 哪种ACL通过比较源地址、目的地址或者其他参数来定义ACL的规则?

A. 扩展型

5. 哪种ACL用名字代替数字?

B. 命名型

6. 作为一般原则，ACL应该放置在网络的哪里?

C. 靠近被控制的通信流量

7. 在防火墙体系结构中，哪种路由器最有可能配置ACL?

C. 外部路由器

8. 命名ACL在Cisco IOS 11.2版本中引入进来。这种说法是否正确?

B. 错的。

9. 哪条命令可以把ACL应用到VTY的端口中?

A. ip access-list

10. 哪个命令可以查看在端口上应用了哪些ACL?

C. show ip interface

11. 在访问控制列表中，附加的32位信息称为：

A. 通配符位

12. 如果希望允许通过的通信流量是基于地址或者协议类型，那么应该使用下面的那个命令?

B. Router（config）#access-list access-*list number* {permit | deny} {*test conditions*}

13. 标准的IP访问控制列表是基于分组的源地址和使用的协议来决定允许或者拒绝分组通过。这种说法是否正确?

A. 对

14. 访问控制列表能够增加网络安全性是基于下面的哪些因素?

C. 分组的源子网、源主机或者源网络

15. 下面哪种网络设备可以使用访问控制列表增加网络的安全性?

B. 路由器

16. 命令access-list 1 permit 204.211.19.162 0.0.0.0可以实现以下哪种功能?

B. 允许一个指定的主机

附录A中“提示”的答案

这一层的作用是什么?

答案：仓库、接待区

工人运送货物时会通过哪一扇门?

答案：建筑后面最大的车库门

客人会通过哪些门进来?

答案：设有接待处的大厅前门

在客人签到后，他们很可能会去哪里?

答案：邻近接待处的会议室

你对使用无线技术的看法如何?

答案：客人可以在接待处和会议室通过无线登录到Internet。仓库职员可以使用无线技术来盘存。

如果有一天，你的部门要为公司安装布线IP安全摄像机，你希望监视哪个区域?

答案：两个安全区域，穿行的后门和接待区。

电话公司会从哪里为这栋建筑物铺设电话线路?

答案：邻近机械间的接入点（POP）

需要什么样的锁?

答案：能从里侧打开的优质锁

对服务器来说，POP的位置好不好?

答案：也许好——当然这个位置要足够大，并且邻近电梯，进出方便。

如果决定了服务器房间必须与POP分开，那么应该如何选择服务器房间的位置?

答案：位置应该选择在电信间，并且选择一个中间的楼层。

可以在POP安装垂直线缆吗？

答案：不可以。查看上一层，你会发现是一个会议室。

你会在哪里安装垂直线缆？

答案：邻近每段楼梯的位置都有一个小的走廊，看看那里。

水平布线的铺设一定要与墙壁平行。如果通向1.2号房间的线缆要与墙壁平行铺设的话，线缆需要多长？这样可行吗？

答案：距离大约94米。这刚够铺设这段水平距离，下到墙内并连接工作区的接头。设计者必须确定是否要要一点小聪明，或者利用安装在仓库或会议室的无线技术。这可能会引起关于安全性的争论，但将能解决一个主要问题。

你会把2楼的电信间放在哪个位置？你可能需要考虑使用其中的两个位置。

答案：2.31房间，因为通过其天花板能进入3.10房间，也可以通过底板进入下面的机械间。你可能需要在2.7增加一个电信间，以便为紧挨着的办公室提供服务。

3楼的3.1和3.2房间有很大的未规划的空间。如果要把电信间放在3.10房间，你如何为这些空间提供服务，特别是处于远端的3.2房间？

答案：就目前的情况，无线是较好的一种解决方案。然后，当房间扩建时，可在其中的任何一间内设立第二个电信间。

你留意到在4楼有一块很大的甲板，还有一个宴会区，宴会区里有一台钢琴。你应该如何为这个区域提供网络连接性？

答案：你只需要一个TR和一些无线接入来为该区域提供网络服务。

你会把电信间放在哪里？

答案：这很难说。4.5房间看起来像一个办公室。但是，4.8房间是空的。而且，在靠4.10房间楼梯的旁边是带外门的走廊。由于是4层，你可能怀疑存在错误。另外，所示的4.10房间有一个朝楼梯的门。这样的话，你可能指出这些明显的错误，并同时请求将TR安装在4.4房间和4.5房间之间。