高等学校计算机应用规划教材

组网技术与网络管理
(第三版)

张玉兰　张召贤　编著

清华大学出版社
北　京

内 容 简 介

本书系统地介绍了计算机网络的组网技术和网络管理知识。全书共 12 章，包括计算机网络建设的基本要素、基本概念和特点，网络标准和协议模型，局域网和广域网技术，网络接入技术，网络的规划和设计，网络综合布线和工程施工标准，网络服务器构建技术和各种网络结构的组建方案，网络维护与管理，网络安全和病毒防范技术与方法等内容。

本书内容丰富，结构清晰，把基础理论和具体的工程实例相结合，具有很强的实用性，不仅可作为高等院校计算机网络及相关专业的教材，还可作为计算机网络设计开发、工程建设和系统集成等工程技术人员的参考书。

本书各章对应的电子教案和习题答案可以到 http://www.tupwk.com.cn/downpage/index.asp 网站下载。

图书在版编目(CIP)数据

组网技术与网络管理 / 张玉兰，张召贤　编著. —3 版. —北京：清华大学出版社，2013.9

(高等学校计算机应用规划教材)

ISBN 978-7-302-32197-2

Ⅰ. ①组…　Ⅱ. ①张…　②张…　Ⅲ. ①计算机网络—高等学校—教材　Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字(2013)第 083325 号

责任编辑：胡辰浩　袁建华
装帧设计：牛艳敏
责任校对：邱晓玉
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62794504

印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**24　　**字　　数：**554 千字
版　　次：2006 年 5 月第 1 版　2013 年 9 月第 3 版　　**印　　次：**2013 年 9 月第 1 次印刷
印　　数：1～5000
定　　价：39.00 元

产品编号：

前　言

与计算机组网和网络管理维护的相关技术，涵盖了网络基础理论、网络设备、组网技术和协议、网络布线、网络服务、网络调测和管理维护等相关知识，全方位地向读者介绍计算机网络技术。

本书作为面向高等院校的教材，在讲述基础理论知识的同时，注重结合具体工程和技术实例的讲解，把理论教学和对实践技能的培养结合起来，是一本非常实用的教材。

本书共分为 12 章，按照由浅入深、理论与实例相结合的方式编排内容。

第 1 章对如何进行网络建设进行了概述，并简要说明了网络建设的几个基本要素，为读者阅读后面章节的知识打下一个初步的基础。

第 2 章介绍了计算机网络的基本概念、原理、技术要点和特点，重点讲述计算机网络的分层体系结构，OSI 参考模型和 TCP/IP 协议簇，互联网协议和 IP 地址结构。使读者对计算机网络有一个整体性的认识，为下一步具体讲解网络知识打下基础。

第 3 章介绍网络设备，网络设备是计算机网络的物质基础，包括服务器、交换机、路由器、集线器等，还包括各种网络传输介质，如双绞线、同轴电缆、光纤等。本章重点讲述了各种网络设备的基本概念、工作原理、主要特点，以及网络设备的选择和评价参考要素。

第 4 章重点讲述局域网组网技术，局域网是计算机网络中应用最广泛的一种网络形式。本章讲述了局域网的基本构成和技术特点、拓扑结构、局域网协议标准和分类；此外还介绍了无线局域网技术和虚拟局域网技术；最后结合具体实例讲解了局域网的应用。

第 5 章主要介绍了广域网和网络接入的相关技术，包括广域网技术、DDN、xDSL、SONET、ATM、MPLS、卫星通信技术、无线通信技术、广域网路由等内容，重点讲解了各种技术的标准、协议结构、技术特点，并结合实例讲解了各种技术的应用情况和适用环境。

第 6 章讲述了如何根据用户需求，综合运用前面讲过的技术，结合实际情况进行网络的规划和设计，并介绍了网络工程和网络评估的基本概念。

第 7 章介绍了网络综合布线技术，主要是布线的规范、标准和工程施工标准，以及线缆的架设和测试等技术。

第 8 章主要介绍了网络操作系统和网络应用服务器的架设，首先介绍了网络操作系统的技术特点和常见的几种网络操作系统；然后结合 Windows 操作系统讲述了各种网络服务器的架设，包括 Web、DNS、DHCP 和邮件服务器等。

第 9 章主要介绍了多种形式的网络组建技术，如对等网、C/S 结构网络、家庭网络、企业网、多媒体教室网络和校园网等，结合具体实例讲述了这些网络形式的特点、结构和软硬件配置等内容。

第 10 章讲述了网络和设备的测试技术，包括网络测试的指标和测试工具、测试方法，交换机和路由器的测试标准和测试方法等；网络故障的检测、调试和排除技术，以及网络故障检测的工具和方法。

第 11 章重点介绍了网络管理维护的相关技术，包括网络管理的基本概念和体系结构，简单网络管理协议，网络管理系统的组成，常见的网络管理软件的配置和使用等。

第 12 章主要讲述了网络安全威胁，网络安全的主要目标，网络安全防范体系结构和安全策略，网络安全技术和协议，网络病毒的相关概念和病毒防治技术，网络机房安全常识等内容。

本书内容翔实，结构清晰，作者根据自己长期从事网络设计和建设的经验，设计了丰富的实例讲解。不仅适合作为高等院校计算机网络及相关专业的教材，还可以作为从事计算机网络设计开发、工程建设和系统集成等工程技术人员的参考书。

本书由张玉兰和张召贤执笔编写，参与本书编写和制作的还有张伟娜、唐丽、李敏、李晓辉、张王英、王勇、白新岭、梅胜利、罗峰、宋连凤、孙建伟、李凯红、王新华、白瑞萍、王春英、刘现丽、郭丽、李晓凤、赵瑞杰等同志。在此，编者对以上人员致以诚挚的谢意！

本书在编写过程中参考了很多宝贵的文献，在此，向这些文献的作者表示衷心的感谢！

限于作者水平有限，书中不足之处，还请广大同行和读者给予批评和指正。我们的邮箱是 huchenhao@263.net，电话是 010-62796045。

编　者

2013 年 6 月

目　　录

第1章　网络建设要素

随着信息技术的飞速发展，人们越来越迫切地需要信息资源的共享，然而，由于地区范围的限制，使得资源共享发生了困难，网络技术因此而应运而生。网络技术为人们的生活、工作、娱乐带来了巨大的变化，而网络建设就成为决定人们生活、工作、娱乐的至关重要的一项。本书将为读者详细介绍如何进行网络建设。

为了能够系统地讲述如何进行网络建设，本章将作为一个综述，为读者介绍网络建设的基本要素。在后面的章节中，将会针对具体的要素进行详细分析。

本章要点：

- 如何进行网络建设
- 网络建设的拓扑图
- 网络建设的基本要素

1.1　如何进行网络建设

网络建设听起来似乎很复杂，其实就是将所有的终端设备，包括工作站计算机、服务器计算机、打印机、数码产品等通过网络设备进行相连。当然，真正的网络建设也不是这么简单，它需要考虑网络质量、网络安全、网络负载平衡等因素。从而会引出很多网络建设中所使用到的技术，如 QOS 技术、组播技术、HSRP 技术、服务器负载均衡技术、冗余电源技术等。

在进行网络建设之前，首先必须针对现有的状况进行具体的定位，然后再针对今后的发展趋势进行详细的分析，最后将所有的分析结果汇总，通过拓扑图和方案的方式表现出来，以作为真正网络建设时的依据。

接下来，将对组建网络时针对现状和未来规划所需要的考虑进行详细的分析。

1. 针对现有的状况做以下考虑

针对现有的条件来规划网络时，需要考虑以下几种情况。

- 在针对现有的状况时，需要考虑网络建设所需的费用，尽量使用合适的设备。例如当一个小型局域网对网络流量不是要求很高，选择一般性的交换机设备如 D-LINK、TP-LINK 等即可，而无须选择 3COM、CISCO 等品牌的高端交换机，这样无疑是为用户节省了大量的开支。

- 另外，需要从整个网络的实际情况来进行分析，不要一味地为了节约成本而使用低廉的产品。当一个网络中需要有语音、视频等信息传递时，那么在此网络中，即使只有十几个用户客户端，也需要选择比较高性能的交换机，如果使用了一般性的交换机，就会使得整个网络针对语音、视频、普通数据流量等无法正常地传输，从而使得此网络建设完全失去意义。
- 网络设备使用过程中可能会出现失控、损坏等因素，为了能保障整个网络不受任何一台网络设备故障因素而导致网络瘫痪，必须针对重要网络设备进行冗余。什么是冗余呢？所谓的冗余，也就是备份的概念。针对冗余，有电源冗余技术、路由器冗余技术、引擎冗余技术等。另外，在网络建设中，还会因为链路的故障而导致网络瘫痪，所以，后来又出现了 Port Channel 技术，使用它来满足链路的冗余和带宽的增加。
- 有的企业网络中的用户很多，但是如果需要保证每个用户使用一个公网地址上网却是无法实现的，此时就需要考虑在内部网络使用私有地址，然后将私有地址多对一的将其转换成公网地址，这样就可以使用少数的公网 IP 地址让众多用户上网，这种技术被称为网络地址转换技术，简称 NAT。
- 最后需要考虑的就是网络的安全，网络安全已经成为整个网络建设的至关重要的技术。如果无法保障网络的安全，而让网络一天到晚承受着非法流量的侵入、黑客的不定期骚扰、病毒的长期扫荡等，那么整个网络所面临灾难则是无法让人想象得到的。所以，网络建设中必须要考虑网络安全一项，此时则可以通过架设防火墙、在路由器中使用访问控制列表等技术。

2. 针对今后的发展需要做以下考虑

针对未来的网络发展，有以下几种情况需要考虑。

- 针对今后的发展，首先要考虑是否需要为不同区域进行预留，通俗地讲就是，如果一个部门有 24 个用户，是否只需要配备一个 24 口的交换机呢？是否需要考虑此部门在未来可能需要添加的用户数量？这个就需要网络建设规划者去详细调查。
- 当一个企业网络中暂时只是拥有一些普通的流量，即一般的数据传输，但在未来是否会添加如视频会议、语音电话等的特殊数据？如果企业在未来有可能添加这些项目的话，那就需要按照未来项目的情况规划目前的网络，简单地说，就是将网络配置成可以运行视频会议、语音电话的网络。
- 对于今后的网络发展，是否需要预留足够的接口进行扩容，如今后服务器的存储负担可能会加大，此时可能需要考虑是否为服务器预留一个连接磁盘阵列的接口。

3. 网络建设所要保障的基本要求

网络建设中有许多基本的要求，如下所示：

- 必须保证网络中所有信息点都有备份点，也可以说尽量针对每个信息点备份一个点。
- 必须保证网络中的所有网络设备在有冗余的情况下工作，特别是核心层设备和汇聚层设备。
- 必须保证局域网的自身安全。
- 必须保证网络的流量优先权限，也就是说当有视频或者语音数据传输时，必须要保证这些流量优先通过，防止这些流量的延迟。

在分析过后，接下来就是撰写方案，方案中一般需要包括以下几点内容：

- 网络建设的意义。
- 针对此次网络建设的用户的现状分析。
- 用户的要求。
- 规划出大概的网络拓扑图。
- 针对拓扑图配备相应的网络设备。
- 工程布线的步骤和拓扑图。
- 针对各种布线的线缆，如双绞线、光缆的技术参数给予说明。
- 针对布线施工完毕后的测量仪器说明、测量结果的说明。
- 整个网络的地址规划情况。
- 整个网络建设的造价表。
- 网络建设的项目小组的名称。

当然以上所说的是一个最基本的网络建设方案所需要具备的内容，其实，很多网络建设方案还有更多的内容，包括机房的建设情况、装潢拓扑图等。这个就靠读者去灵活掌握了。

1.2　网络建设的拓扑图

网络建设中的规划拓扑图对于整个网络建设起着尤为重要的作用，它是网络设计者针对网络现状和今后发展的一个初步规划和今后修改的依据，如果网络建设中没有拓扑图，那么一切将会成为纸上谈兵，什么地方需要改进，什么地方需要添加设备等都不会被设计者所注意，一旦网络建设完毕，再发现很多令人不满意的地方就悔之晚矣了。

网络拓扑图分为 3 种，如下所示。

- 广域网拓扑图。
- 局域网拓扑图。
- 详细拓扑图。

下面将详细针对这 3 种拓扑图给出说明和具体的实例。

1. 广域网拓扑图

广域网拓扑图一般来说是针对用户网络如何接入到互联网的示意图，它需要规划如何接入互联网、使用何种技术接入到互联网、使用何种设备接入互联网等。下面将举一个实例。

一个企业的总公司在北京，在美国和新加坡有两家分公司，现在将 3 家公司进行连接，并且将它们接入到互联网中。接下来，先给出如图 1-1 所示的拓扑图，然后再给以详细的分析。

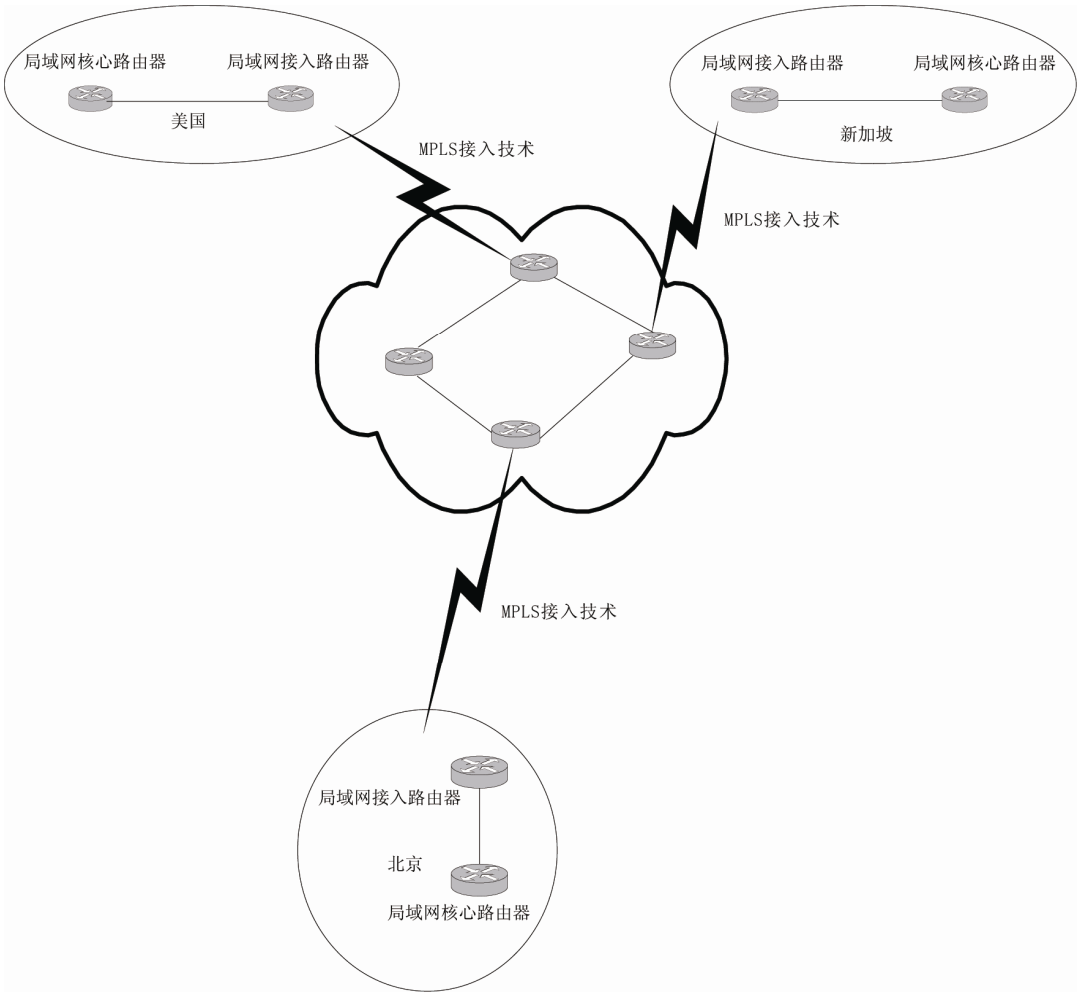

图 1-1　广域网拓扑图

下面来分析上面的拓扑图。

- 首先，必须明确接入到互联网的是路由器还是多层交换机，并且确认其型号。
- 其次，需要明确接入的是哪种方式，是 ATM、MPLS、DDN 或者是光缆直连。
- 接下来，需要明确的就是大概的接入技术的简单拓扑，如图 1-1 中的 MPLS 的简单示意图。

下面再给出一个比较复杂的拓扑图，如图 1-2 所示。

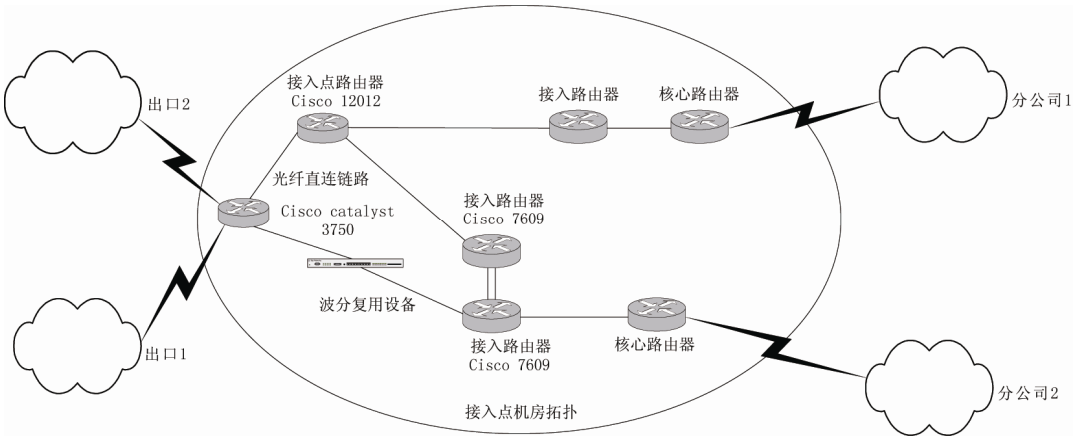

图 1-2　稍微复杂的广域网拓扑图

以上拓扑图是某个企业的广域网接入拓扑图，读者可以根据前面所讲述的认真分析，找出广域网拓扑图的规划技巧。

2. 局域网拓扑图

局域网的拓扑图直接表现出整个局域网中的网络设备的分布情况，网络中的路由情况，以及整个网络中的网络层次。下面将通过一个实例，为读者展示如何具体地规划一个局域网拓扑图。

一个企业中包括了网络管理部、销售部、财务部、售后部、客服部 5 个部门，现在将其规划到一个企业网络中。

由于网络管理部可以管理整个企业的网络，所以将其作为局域网的核心处。其详细如图 1-3 所示的拓扑图。

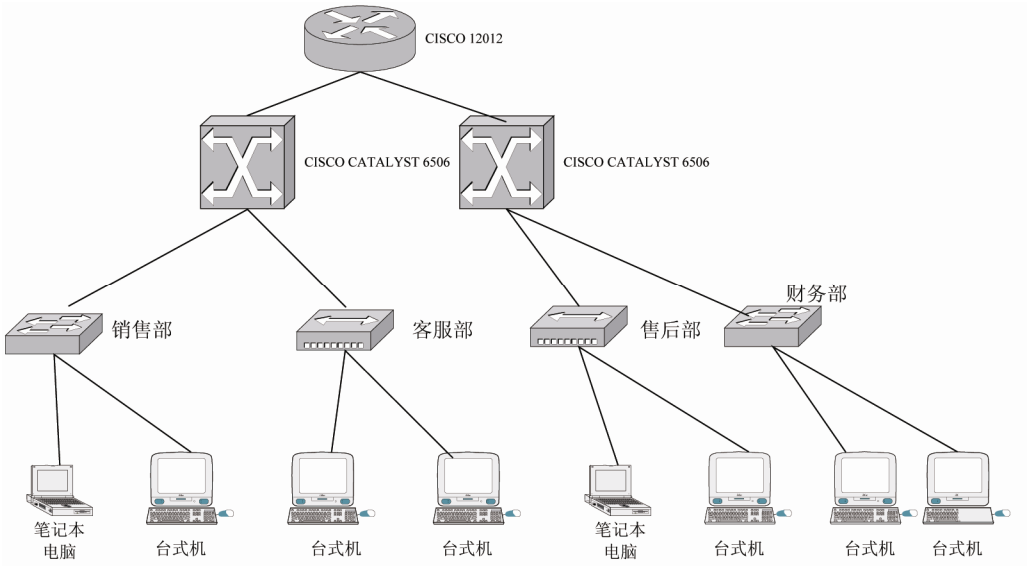

图 1-3　局域网拓扑图

以上的拓扑图将整个用户网络规划得清清楚楚，其中包括了每个部门使用何种接入设备，核心层使用何种接入设备，网络的最前端使用何种接入设备等。下面再给出一个比较复杂的拓扑图，如图 1-4 所示。

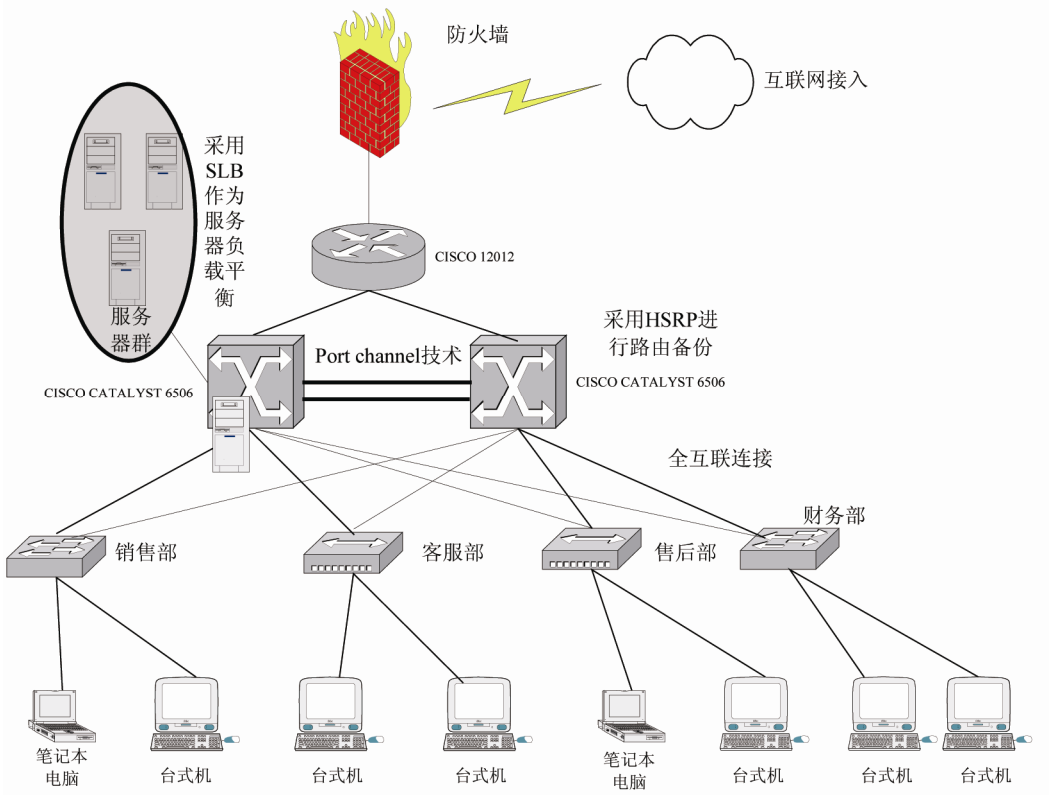

图 1-4　比较复杂的局域网拓扑图

图 1-4 中，不但规划出了局域网的接入方式，而且还将局域网中的连接技术都一一标明在图中，使得设计者在修改网络规划时可以一目了然，针对实际情况做进一步的修改。

3. 详细拓扑图

所谓的详细拓扑图，主要是指针对用户局域网中具体的规划方式进行说明。下面将举一个实例，通过这个实例读者应该能够掌握如何规划详细拓扑图。

在一个企业中有 3 栋楼，每栋楼有 3 层：第一层是技术部，第二层是销售部，第三层是财务部。该企业详细的网络拓扑图如图 1-5 所示。

以上的拓扑图详细地说明了 3 栋楼是如何进行相连的，是使用何种技术进行相连的。所以网络建设的规范拓扑图在每个技术方案中是不可缺少的一部分，希望读者能够自己去详细揣摩。

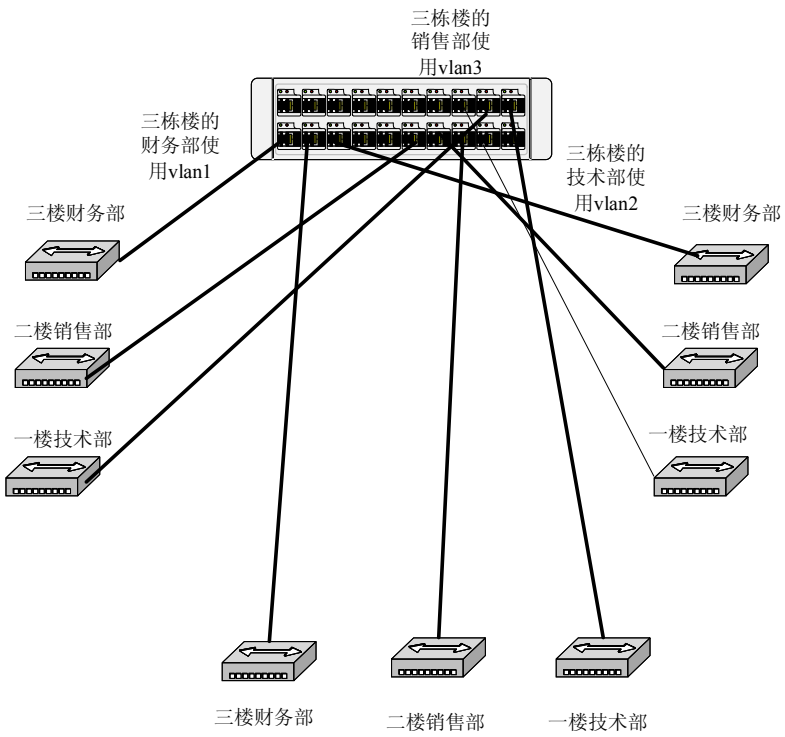

图 1-5　详细拓扑图

1.3　网络建设的要素

网络建设的要素，其实就是网络建设所需要做的几个步骤，分为综合布线、网络设备的选型、地址规划以及网络安全等。工程布线属于基础建设，综合布线的质量好坏直接决定了整个网络的质量好与坏。网络设备的选型决定了网络的规模，以及网络的传输质量。地址规划及路由协议的选择则是能够保证很好地维护和升级整个网络的关键。至于网络安全，则是整个网络的守护神。这些要素都是网络建设中缺一不可的。

1.3.1　综合布线

综合布线是一种模块化的、灵活性极高的建筑物内或建筑群之间的信息传输通道。它既能使语音、数据、图像设备和交换设备与其他信息管理系统彼此相连，也能使这些设备与外部相连。综合布线还包括建筑物外部网络或电信线路的连接点与应用系统设备之间的所有线缆及相关的连接部件，通过按标准的、统一的和简单的结构化方式编制和布置达到所要求的功能。因此，综合布线系统是一种标准通用的信息传输系统。

在进行网络建设时，充分理解用户需求是综合布线系统设计的基础。设计者可以通过现场勘查、阅读招标文件、技术交流会、答疑会等多种方式充分理解用户需求。

接下来的内容将会为读者详细讲述综合布线中，作为一个设计者需要做的最为基本的工作。

1. 布线系统物理链路设计

布线系统的物理链路的设计主要是一些位置的确定，包括了机房、弱电井等，下面将分别进行详细的叙述。

(1) 机房位置确定

一般设计院或用户已经指定了布线机房位置，布线机房大部分都和网络机房共用，也有部分单独设置。在这种情况下，需要查看机房内是否可以满足布线系统的要求。如果用户还没有明确机房位置，需要设计者根据实际现场情况和机房的基本要求确定机房位置，并与用户沟通，获得用户认可。

(2) 弱电竖井与分配线间位置确定

一般设计院或用户已经指定了弱电竖井与分配线间物理位置。在这种情况下，需要查看配线间内是否可以满足布线系统的要求。如果用户还没有明确分配线间位置，需要设计者根据实际现场情况和机房的基本要求确定机房位置，并与用户沟通，征得用户认可。竖井与分配线间的位置和数量将直接影响工程造价，如发现原有设计不合理(这种情况时常出现)，请直接与用户和设计院沟通，请求作设计变更。

(3) 点位统计表

确定点位图是必须的，这是计算材料清单的必要条件。要详细统计数据节点、语音节点、光纤到桌面节点的数量和分布情况，制作成详细点位统计表。

(4) 路由设计

在工程实施中，路由是很重要的一环，包括水平线缆路由、垂直主干路由、主配线间位置、分配线位置、机房位置、机柜位置、大楼接入线路位置等。

(5) 材料种类

物理路由上可能使用镀锌线槽、镀锌管、PVC 管线槽、PVC 软管、梯形爬线梯、上走线铝合金桥架等。

(6) 障碍物结构

砖墙、混凝土墙、楼板结构、隔断，是否为承重墙等要分别对待。敷设方式如下：

- 暗敷设。
- 明敷设。
- 吊装。
- 沿墙。
- 室外架杆。
- 室外管井。

在确定了上述情况后，作出物理路由图(也称预埋管线图)，包括线路路径、材料种类、材料数量、敷设方式和施工工时等。并且路由设计一定要考虑其他线路路由和消防规定。

2. 布线系统逻辑链路设计

布线系统的逻辑链路的设计包括了线缆的选择、主干的选择、布线区间的设计等。下面将进行详细的叙述。

(1) 铜缆类别选择

包括屏蔽与非屏蔽、超 5 类与 6 类、各种阻燃等级应用等。

(2) 主干类别选择

包括光缆和铜缆。在实际设计中，语音主干一般采用 3 类大对数电缆(25 对、50 对、100 对等)。数据主干可采用 4 对双绞线、5 类 25 对大对数电缆，但光缆现在已被绝大多数工程所采用。根据网络设备类型可采用单模与多模光缆。根据用户数量和带宽要求确定光缆芯数。

(3) 布线品牌选择

现在市场上有很多布线品牌，质量、价格、知名度都有差别，选择质量可靠、价格合理的产品是很重要的。

(4) 各子系统布线材料设计选型

布线子系统一般包括以下子系统：

- 工作区子系统。
- 水平子系统。
- 管理子系统。
- 垂直子系统。
- 设备间子系统。
- 建筑群子系统。

3. 统计与报价

统计和报价是设计工作中比较重要的一环，它决定了整个布线工程中的成本在预计的情况下进行，这步工作主要包括了材料统计和工程报价。下面将针对这些进行详细的讲述。

(1) 布线材料分配表

将各个布线子系统的材料型号和数量详细列表。用 Excel 表格作出布线材料分配表。材料分配表体现了设计者的全部设计思想，同时也体现了确定材料数量的设计依据。

(2) 布线材料统计表

将各个布线子系统的材料型号和数量归类列出最终的布线材料统计表。用 Excel 表格做出规范的布线材料统计表。材料统计表体现了全部材料用量。

(3) 工程报价

根据材料统计表，制定工程报价。当然所有工程报价要和客户的投资预算相符合。工程报价方式有以下几种方式。

- 国家行业管理部门概、预算方式，包括信息产业部和建设部，一般含直接费和间接费两大部分。可参照行业部门出版的定额标准。
- 材料费用和人工费用按照比例报价，如材料费用按照进货成本加价，然后人工费

用按照材料费用的百分比加价。这种方式对于选用国产布线品牌可能会由于人工费用取价较低造成项目亏损，所以要适当调高收费比例。

- 材料费用和人工费用分开报价，人工费用按照点数核算，按照单点造价乘以点数。

4. 设计方案成册

设计方案成册是一个优秀的设计者最基本的工作，因为它是整个布线工程的总依据和总指挥，其中包括了图纸、设计方案等。

(1) 图纸

包括点位图、系统图和路由图等。当然出图纸的费用也是不小的开销，所以做工程报价核算成本时也要考虑进去。

(2) 设计方案

按照以上设计思路编写设计方案文字部分。设计方案一定要在材料分配表、统计表出来以后编写。否则免不了要改来改去，浪费时间。

(3) 装订成册

将以上设计方案、图纸、统计与报价表装订成册。剩下的工作就是交给销售人员进行项目跟进了。

以上就是整个综合布线的基本步骤，在后面的章节中，将会针对综合布线内容进行详细的分析和讲述。

1.3.2　网络设备的选型

在网络建设中，网络设备的选型对于整个网络是否具备高可用性、冗余性、可扩展性都起着决定性的作用。网络设备包括了对交换机、路由器的选择。

所谓的交换机，就是帮助数据包在一个广播域中进行转发的设备。而所谓的路由器，则是帮助数据包能够在不同的网段中进行传输，并且选择路由器认为最佳的路径进行传输的设备。

整个网络按照逻辑来分，可以划分为 3 层，分别为核心层、汇聚层和接入层。

- 接入层为用户提供了网络设备的接入，它通常包括实现局域网的设备(如工作站和服务器)互联的第二层交换机。在广域网环境中，同广域网的接入点即为接入层的节点。
- 汇聚层也可称为分布层，它汇聚了配线架，并且使用第二层和第三层交换进行工作组分段、实施安全策略、限制带宽和隔离各种网络故障等。这些措施能够直接防止汇聚层和接入层对核心层带来的不利影响。
- 核心层主要是用来快速交换的，因为核心层是连通的关键环节，所以必须采用高速传输交换技术才能满足网络的快速有效的传输。

上面所讲述的网络三层逻辑结构如图 1-6 所示。

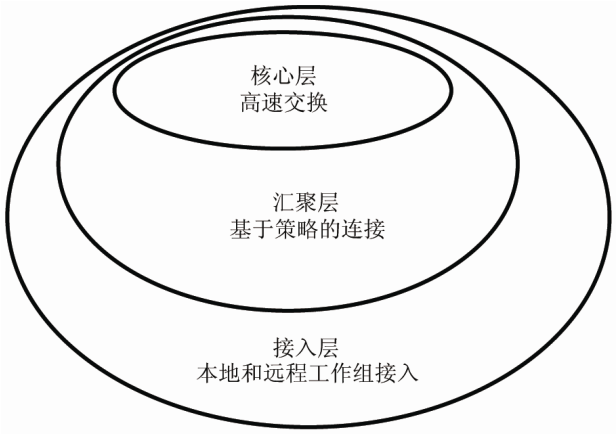

图 1-6　网络逻辑三层结构图

以上给出的是逻辑结构图。接下来，将针对三层逻辑结构举一个实际网络建设的例子，通过这个例子让读者清楚如何划分三层结构。实例的网络拓扑图如图 1-7 所示。

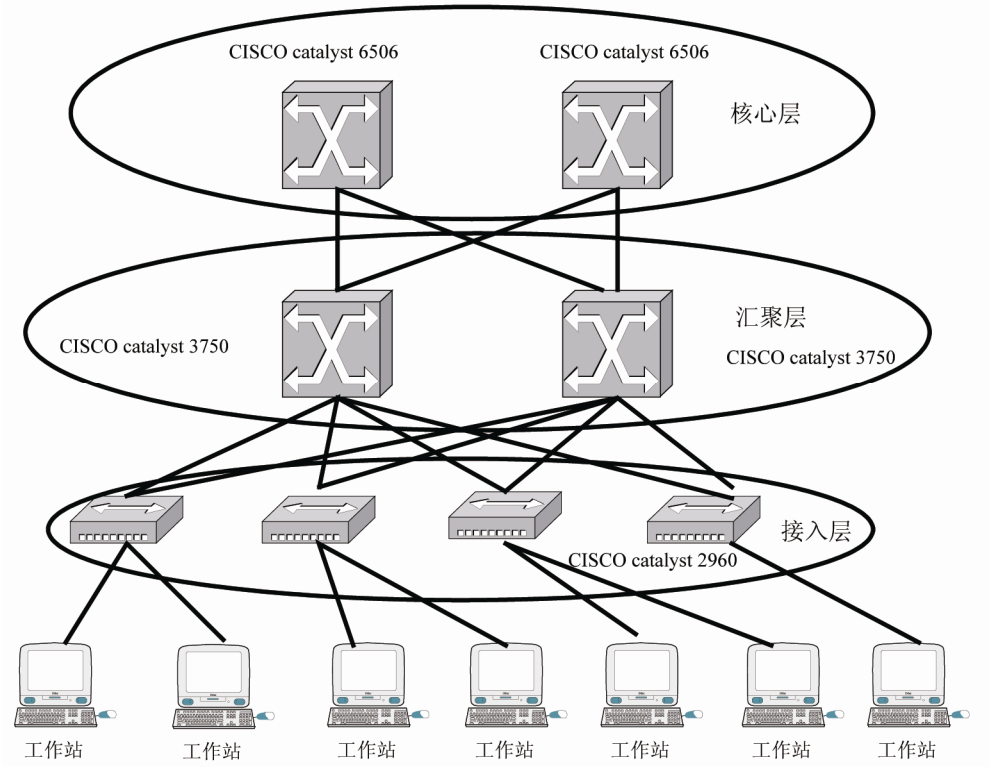

图 1-7　网络建设中的三层逻辑拓扑图

针对不同的逻辑层需要选择不同类型的网络设备。例如，接入层设备只需要实现一般的数据包转换功能，所以对此层的设备要求比较低，一般的普通交换机都可以作为接入层的设备。汇聚层的交换机对于性能要求比较高，需要具备充足的命令集，能够处理工作组分段、实施安全策略、限制带宽和隔离各种网络故障等功能，所以选择这种网络设备一般来说是选择中高端设备。至于核心层的设备就必须要那些转发传输性能最好的设备，所以

一般使用的是高端设备。

读者可以根据实际的网络情况自行分析，结合综合性能、价格、可扩展性、高可用性等特性进行网络设备的选择。

1.3.3　地址规划和路由协议选择

为了确保网络的可扩展性，关键之一是构建可扩展的 IP 编制方案。随着网络的不断增大，所需要的子网数目也相应地不断增加，如果不采用如地址汇总和无类域间路由选择技术等高级 IP 编制技术，则会导致 IP 地址不够用、路由器中的路由选择表庞大、网络设备反应迟钝等不良的影响。后面将会针对 IP 地址的规划进行详细讲述。

路由协议的选择就比较复杂，需要设计者对每个路由协议都十分了解。路由协议包括 RIP、IGRP、EIGRP、OSPF、IS-IS、BGP 等，不同的网络路由协议使用的环境和情形不同，需要设计者根据实际情况来进行选择。在后面的章节中将会为读者详细介绍几种路由协议的知识。

1.3.4　网络安全

计算机网络安全规划可以帮助用户决定哪些信息需要保护、在保护时愿意投资多少、由谁来负责执行该保护等。网络安全规划一般通过以下几种方式。

1. 威胁评估

制定一个有效的网络安全规划，第一步是评估系统连接中所表现出的各种威胁。与网络相关的主要有：非授权访问、信息泄露、拒绝服务。

2. 分布式控制

实现网络安全的一种方法，是将一个大型网络中的各段责任和控制权分配给单位内部的一些小组。这种责任的层次结构从高到低包括网络管理员、子网管理员、系统管理员和用户，在该层次结构的每一点都有人负责和具体执行。

3. 编写网络安全策略

编写一个网络安全策略文件，明确地阐明要求达到什么目的和要求谁来执行是很重要的。一个网络安全策略文件包括如下内容：系统管理员的安全责任、正确地利用网络资源、检测到安全问题时的对策、网络用户的安全责任等。

一个全方位的计算机网络安全体系结构包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。充分利用各种先进的主机安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术、网络反病毒技术、安全审计技术、安全管理技术、系统漏洞检测技术、黑客跟踪技术，在攻击者和受保护的资源间建立多道严密的安全防线，不仅极大地增加了恶意攻击的难度，而且增加了审核信息的数量，利用这些审核信息可以跟踪入侵者。

在实施网络安全防范措施时，要考虑以下几点。

- 要加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞。
- 要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出可能存在的安全隐患，并及时加以修补。
- 从路由器到用户各级建立完善的访问控制措施、安装防火墙、加强授权管理和认证。
- 利用数据存储技术加强数据备份和恢复措施。
- 对敏感的设备和数据要建立必要的物理或逻辑隔离措施。
- 对在公共网络上传输的敏感信息要进行数据加密；安装防病毒软件，加强内部网的整体防病毒措施；建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

为了能够让读者了解网络安全的含义，在后面的章节中将针对网络安全，给以详细的讲解。

1.4　本 章 小 结

本章主要针对整个网络建设进行了总体概念性的讲述，包括了网络建设中的规划方法、网络拓扑图的绘制、网络建设中的几大要素等的知识，具体的内容将会在本书后面的各章中进行详细的讲述。

1.5　思考与练习

1. 填空题

(1) 设计者可以通过_____、_____、_____、_____等多种方式充分理解用户需求。

(2) 整个网络按照逻辑来分，可以划分为 3 层，分别为_____、_____和_____。

(3) 路由协议包括了_____、_____、_____、_____、_____、_____等，不同的网络路由协议使用的环境和情形不同，这个就需要设计者根据实际情况来进行选择。

(4) 网络安全规划一般通过_____、_____、_____几种方式。

2. 选择题

(1) 布线子系统一般包括以下子系统(　　)。

A. 工作区子系统　　B. 水平子系统

C. 管理子系统　　D. 垂直子系统

E. 设备间子系统　　F. 建筑群子系统

(2) A 类地址的范围是(　　)。

A. 1~127　　B. 128~191

C. 192~233　　D. 239 以后

(3) 在工程实施中，路由是很重要的一环，包括(　　)等。

A. 水平线缆路由　　B. 垂直主干路由

C. 主配线间位置　　D. 分配线位置

E. 机房位置　　F. 机柜位置

G. 大楼接入线路位置

3. 问答题

(1) 在实施网络安全防范措施时，需要考虑哪些问题？

(2) 什么是网络的逻辑三层结构？

第3章　网 络 设 备

第 2 章介绍了计算机网络的基础知识和基本理论，可以说第 2 章介绍的协议和模型是计算机网络的理论基础，要构建一个实用的网络，硬件设备是其物质基础。网络不仅仅是由通信电缆、无线电波和接口组成，还有许多的网络传输设备，这些设备使网络成为具有一定功能的拓扑结构。

网络设备多种多样，有的网络设备用来将载波信号放大，以便信号可以到达建筑物中另外的房间或者楼层；有的网络设备可以从一个网络向另一个网络路由载波信号；还有一些网络设备用来转换信息，使得信息可以在不同的网络间进行发送。本章将重点介绍这些网络设备，其中，最重要的网络设备是服务器、交换机和路由器。另外，本章也对其他设备作了简单介绍。

本章要点：

- 网络设备的功能和特点
- 网络设备的分类
- 网络设备的选择
- 传输介质

3.1　计算机网络中的传输介质

在计算机之间联网时，通信线路和通道传输问题也是非常重要的一个方面。OSI 模型的第 1 层包含着传输介质和接口，最基本的通信就是在这个层完成的。目前，共有 4 种基本的介质类型：同轴电缆、双绞线、光纤电缆和无线技术。

3.1.1　双绞线

双绞线(Twisted Pair，简称 TP)是综合布线工程中最常用的传输介质。双绞线是由两根具有绝缘保护层的铜导线组成。当把两根绝缘的铜导线按一定密度互相绞在一起时，每一根导线在传输中辐射出来的电波会被另一根导线上发出的电波抵消，大大降低了信号受干扰的程度。双绞线一般由两根为 22 号、24 号或 26 号绝缘铜导线相互缠绕而成。如果把一对或多对双绞线放在一个绝缘套管中便成了双绞线电缆。与其他的传输介质相比，双绞线在传输距离、信道宽度和数据传输速度等方面均受到一定的限制，但其价格较为低廉。

目前，双绞线可分为非屏蔽双绞线(Unshielded Twisted Pair，简称 UTP)和屏蔽双绞线(Shielded Twisted Pair，简称 STP)两种。屏蔽双绞线电缆的外层由铝泊包裹着，它的价格相对要昂贵一些。

1. 屏蔽双绞线

屏蔽双绞线由成对的绝缘实心电缆组成，在实心电缆上包围着一层编织的或起皱的屏蔽。屏蔽减少了 RFI 和 EMI 对通信信号的干扰，更有效地减少 RFI 和 EMI 干扰，每一对双绞线上的交织距离必须是不同的。而且，为了获得最佳效果，插头和插座必须要屏蔽。STP 中的另一个重要因素是要正确接地，以获得可靠的传输信号控制点。

编织的屏蔽用于室内布线，起皱的屏蔽用于室外或地下布线。在周围有重型电力设备和强干扰源的位置，建议使用屏蔽双绞线。

2. 非屏蔽双绞线

非屏蔽双绞线由位于绝缘的外部遮蔽套内的成对电缆线组成，在一对对缠绕在一起的绝缘电线和电缆外部的套之间并没有屏蔽。与 STP 类似，内部的每一根导线都与另外一根导线相互缠绕，以帮助减少对载有数据的信号的干扰。

UTP 的流行称谓是 10Base-T 电缆，意思是，其最大传输速率为 10 Mb/s(对于某些数据传输而言，真正的速率可达 16 Mb/s)，UTP 使用的是基带通信，为双绞线类型。

3. 双绞线的分类

TIA(电信工业协会)和 EIA(电子工业协会)在 TIA/EIA 568 标准中完成了对双绞线的规范说明。TIA/EIA 568 标准目前覆盖的内容包括电缆介质、设计以及安装规范。TIA/EIA 568 标准将双绞线电线分割成若干类。双绞线被称为 1、2、3、4 或 5 类，后来又出现了 6 类，所有这些电缆都必须符合 TIA/EIA 568 标准，局域网经常使用的是 5 类电缆。

- 1 类线(CAT 1)：一种包括两个电线对的 UTP 形式。1 类线适用于语音通信，而不适用于数据通信。它每秒最多只能传输 20 Kb/s 的数据。
- 2 类线(CAT 2)：一种包括 4 个电线对的 UTP 形式。数据传输速率可以达到 4 Mb/s。但是由于大部分系统需要更高的吞吐量，2 类线很少应用于现代网络中。
- 3 类线(CAT 3)：一种包括 4 个电线对的 UTP 形式。在带宽为 16 MHz 时，数据传输速度最高可达 10 Mb/s。3 类线一般用于 10 Mb/s 的 Ethernet 或 4 Mb/s 的 Token Ring。虽然 3 类线比 5 类线便宜，但为了获得更高的吞吐量，网络管理员正逐渐用 5 类线代替 3 类线。
- 4 类线(CAT 4)：一种包括 4 个电线对的 UTP 形式，它能支持高达 10 Mb/s 的吞吐量。CAT 4 可用于 16 Mb/s 的 Token Ring 或 10 Mb/s 的 Ethernet 网络中，确保信号带宽高达 20 MHz。与 CAT 1、CAT 2 或 CAT 3 相比，CAT4 能提供更多的保护以防止串扰和衰减。
- 5 类线(CAT 5)：用于新网安装及更新到快速 Ethernet 的最流行的 UTP 形式。CAT 5 包括 4 个电线对，支持 100 Mb/s 吞吐量和 100 Mb/s 信号速率。除了 100 Mb/s Ethernet

之外，CAT 5 电缆还支持其他的快速联网技术，如异步传输模式(ATM)。

- 增强 CAT 5：CAT 5 电缆的更高级别的版本。它包括高质量的铜线，能提供一个高的缠绕率，并使用先进的方法以减少串扰。增强 CAT 5 能支持高达 200 MHz 的信号速率，是常规 CAT 5 容量的两倍。
- 6 类线(CAT 6)：包括 4 对电线对的双绞线电缆。每对电线被箔绝缘体包裹，另一层箔绝缘体包裹在所有电线对的外面，还有一层防火塑料封套包裹在第二层箔层的外面。箔绝缘体对串扰提供了较好的阻抗，从而使得 CAT 6 能支持的吞吐量是常规 CAT 5 的 6 倍。

4. 双绞线的特性

STP 和 UTP 有共同的特性，同时也有不同之处。

- 吞吐量：STP 和 UTP 能以 10 Mb/s 的速度传输数据，CAT 5 UTP 以及在某些环境下的 CAT 3 UTP 的数据传输速度可达 100 Mb/s。高质量的 CAT 5 UTP 也能以每秒 1 GB 的速度传输数据。
- 成本：STP 和 UTP 的成本区别在于所使用的铜态级别、缠绕率以及增强技术。一般来说，STP 比 UTP 价格更昂贵，但高级 UTP 也是非常昂贵的。
- 连接器：STP 和 UTP 使用的连接器和数据插孔，看上去类似于电话连接器和插孔。如图 3-1 所示的是一个包含 4 对电线电缆的 RJ-45 连接器。

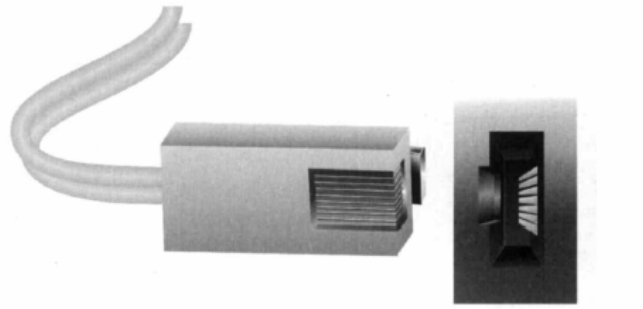

图 3-1　RJ-45 连接器

- 抗噪性：STP 具有屏蔽层，因而它比 UTP 具有更好的抗噪性。
- 尺寸和可扩展性：STP 和 UTP 的最大网段长度都是 100 m，它们的跨距小于同轴电缆所提供的跨距，这是因为双绞线更易受环境噪声的影响。双绞线的每个逻辑段最多能容纳 1 024 个节点，整个网络的最大长度与所使用的网络传输方法有关。

5. 双绞线的做法

- 双绞线的做法共分为 3 类：第一类是直通线，第二类是交叉线，第三类是配置线。
- 直通线的做法是将网线的两端制作成相同线序。所谓的线序，在国际上有两种标准，分别是 T568A 和 T568B。在这里以 T568B 为例。两端的线序如图 3-2 所示。

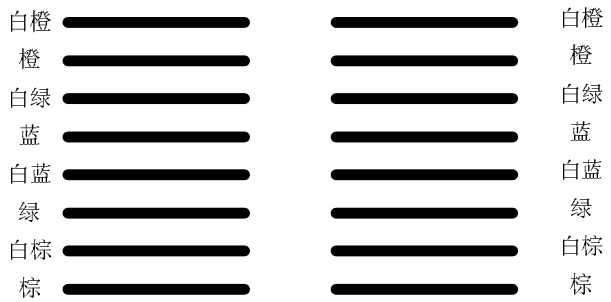

图 3-2　直通线的制作

交叉线的做法将网线的两端制作成不同的线序，其线序对应如图 3-3 所示。

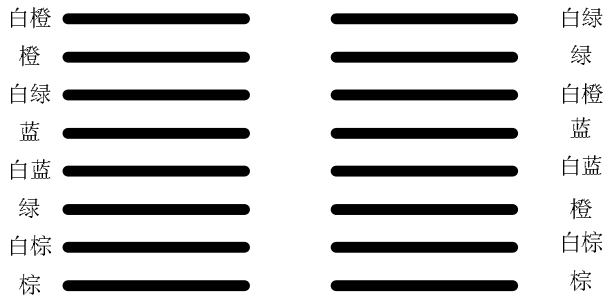

图 3-3　交叉线的制作

配置线又称为反向线，是将两端的线序完全颠倒过来，其线序如图 3-4 所示。

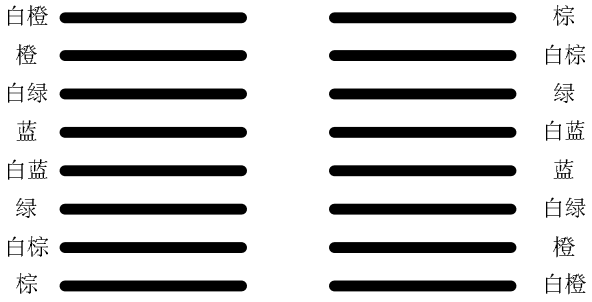

图 3-4　配置线的制作

当相同类型的设备对接，使用交叉线。当不同类型的设备对接则使用直通线。至于配置线则是专门使用在配置路由器上的。例如计算机与计算机相连就是用交叉线，计算机与交换机连接使用的是直通线。这些都希望读者能够引起重视。在结束讲解双绞线知识之前，提醒读者注意，网络双绞线中真正起到作用的是 1、2、3、6 四根线，传输数据时就是使用这四根线。

3.1.2　光纤

光导纤维是一种传输光束的细而柔韧的介质，光导纤维电缆由一捆纤维组成，简称为

光缆。光纤通常是由石英玻璃制成，其横截面积是很小的双层同心圆柱体，称为纤芯，它质地脆，易断裂，需要外加一层保护层，其结构如图 3-5 所示。当光波脉冲由激光或者普通发光二极管(LED)设备发出后，便可以在光纤芯线中向前传输。玻璃包层的作用是将光线反射回芯线中。光纤电缆具有进行高速网络传输的能力，它所支持的传输速度可以从 100 Mb/s 到 1Gb/s，甚至超过 10 Gb/s。光纤电缆的优点在于：它的带宽大、损耗小，可以持续传输很长的距离，一般用作电缆传输主干。

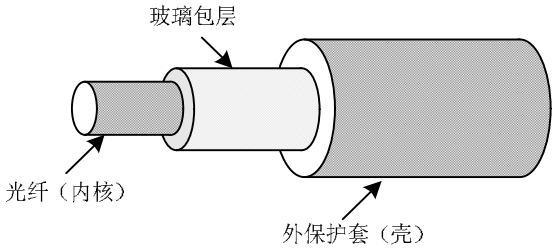

图 3-5　光缆

1. 光纤的分类

光纤主要有两大类，即单模/多模和折射率分布类。

(1) 单模/多模

单模光纤(SMF，全称 Single Mode Fibre)的纤芯直径很小，在给定的工作波长上只能以单一模式进行传输，传输频带宽，传输容量大。光信号可以沿着光纤的轴向传播，因此光信号的损耗很小，离散也很小，传播的距离较远。单模光纤 PMD 规范建议芯径为 8 μm~10 μm，包括包层直径时为 125 μm。

多模光纤(MMF，全称 Multi Mode Fibre)为在给定的工作波长上能以多个模式同时传输的光纤。多模光纤的纤芯直径一般为 50 μm~200 μm，而包层直径的变化范围为 125 μm~230 μm，计算机网络用的纤芯直径为 62.5 μm，包层为 125 μm，就是通常所说的 62.5 μm。与单模光纤相比，多模光纤的传输性能较差。

在导入波长上分为：单模 1 310 nm、1 550 nm；多模 850 nm、1 300 nm。

(2) 折射率分布类

折射率分布类光纤可分为跳变式光纤和渐变式光纤两种。

跳变式光纤纤芯的折射率和保护层的折射率都是常数。在纤芯和保护层的交界面，折射率呈阶梯形变化。

渐变式光纤纤芯的折射率随着半径的增加而按一定的规律减小，到纤芯与保护层交界处减小为保护层的折射率。纤芯的折射率的变化近似抛物线形。

2. 光纤通信系统

光纤通信系统是以光波为载体、光导纤维为传输介质的通信方式，起主导作用的是光源、光纤、光发送机和光接收机。它们的功能分别如下。

- 光源是光波产生的根源。

- 光纤是传输光波的导体。
- 光发送机负责产生光束，将电信号转变成光信号，再把光信号导入光纤。
- 光接收机负责接收从光纤上传输过来的光信号，并将其转变成电信号，经解码后再作相应的处理。光纤通信系统的基本构成如图 3-6 所示。

图 3-6　光通信系统构成

3. 光纤通信系统的主要优点

光纤通信系统的主要优点包括：

- 传输频带宽和通信容量大，在短距离传输数据时达几千兆的传输速率。
- 线路损耗低、传输距离远。
- 抗干扰能力强，应用范围广。
- 线径细、质量小。
- 抗化学腐蚀能力强。
- 光纤制造材料丰富。

在网络工程中，一般使用 62.5 μm/125 μm 规格的多模光纤，有时也使用 50 μm/125 μm 和 100 μm/140 μm 规格的多模光纤。户外布线大于 2 km 时可选用单模光纤。

3.1.3　同轴电缆

同轴电缆是 Ethernet 网络的基础，并且多年来一直是最流行的传输介质。同轴电缆由有绝缘体包围的一根中央铜线、一个网状金属屏蔽层和一个塑料封套组成，图 3-7 所示是一种典型的同轴电缆。

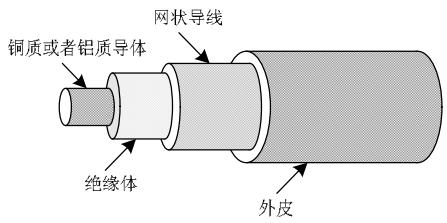

图 3-7　同轴电缆结构示意图

在同轴电缆中，铜线传输电磁信号。网状金属屏蔽层一方面可以屏蔽噪声，另一方面可以作为信号地。绝缘层通常由陶制品或塑料制品组成(如聚乙烯(PVC)或特富龙)。它将铜线与金属屏蔽物分隔开，若这两者接触，电线将会短路。塑料封壳可使得电缆免遭物理性的破坏，它通常由柔韧性好的防火塑料制品制成。

同轴电缆的绝缘体和防护屏蔽层，使得电缆对噪声干扰有较高的抵抗力。在信号放大

之前，同轴电缆与双绞线电缆相比，能将信号传输得更远；另一方面，同轴电缆要比双绞线电缆昂贵得多，并且通常只支持较低的吞吐量。同轴电缆还要求网络段的两端通过一个电阻器进行终结。这种类型的电缆存在许多不同的规格。

同轴电缆有粗、细两种类型，粗同轴电缆(Thicknet)又称为粗线或粗电缆网，其中心为铜导体或敷铜箔膜的铝导体。粗同轴电缆用于传输速度为 10 Mb/s 的总线网络上。根据 IEEE 标准，最大长度可延伸为 500 m。这一标准可以写为 10Base5。10 表示电缆传输速率为 10 Mb/s，Base 指的是使用基带而非宽带。与粗同轴电缆一样，以太网规范要求细同轴电缆的阻抗为 50 Ω。细同轴电缆贴有 RG-58A/U 标签，说明这是 50 Ω 的电缆。一般网络管理员称之为 10Base2，因为理论上其最大的网络速度为 10 Mb/s，布线可达 185 m，使用基带类型的数据传输。

在细同轴电缆的中心，有一个铜的或敷铜箔膜的铝导线，并在中轴上附着一层绝缘泡沫材料。有一种高质量的电缆是编织的铜网，由铝箔的套管附着，缠绕着绝缘泡沫材料，而且电缆由外部的 PVC 或特氟纶套覆盖以绝缘。

细同轴电缆安装起来要比粗同轴电缆容易而且便宜得多，但是双绞线柔性较好，所以更加利于安装和使用。细同轴电缆优于双绞线之处在于可以抵抗 EMI 和 RFI。

3.1.4　无线传输介质

在传输网络包时，有许多无线介质可以替代电缆：无线电波、红外线信号以及微波等。所有这些技术都是通过空气或大气来传输信号的。在使用电缆非常困难或者说根本不可能时，无线通信可以出色地替代电缆。但是使用无线进行通信有一个非常重要的限制：同一介质的其他信号、太阳黑子的运动、电离层变化和其他大气干扰都会对通信信号形成干扰，从而会产生许多问题。

无线局域网通常使用红外或射频(RF)信号传输信息，微波和卫星连接也可通过空气传输数据，这些可以跨越更远距离的方法主要应用于广域网通信。

1. 无线电技术

网络信号可以通过无线电波进行传输，这种方式与本地电台广播的手段非常相似，但是应用于网络时，信号频率要远高于电台发射频率。例如，AM 电台发送频率为 1 290 kHz， FM 的播送范围为 88~108 MHz，但在美国，网络信号的传输频率可高达 902~928 MHz、2.4 GHz 或 5.72~5.85 GHz。

在无线电网络传输中，根据信号采用的天线类型，可以沿一个方向或多个方向进行传输，如图 3-8 所示。由于无线电的波长比较短，而且强度也较低，这就意味着无线电传输最适用于短程的视线(line-of-sight)传输。在视线传输中，信号是从一点向另一点进行传输的，而不是在国家间或各大洲间进行传输。视线传输的限制在于信号会被高的物体(如山峰)中断。低功率的单频信号传输数据的能力在 1~10 Mb/s 之间。

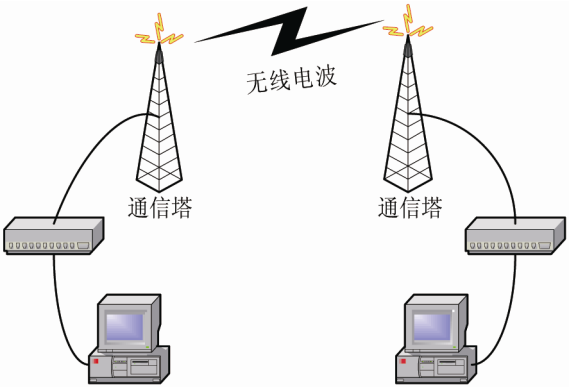

图 3-8　无线电通信

大多数网络设备采用扩展频谱(spread spectrum)技术进行包的传输。在这种技术中，使用了一个或多个邻接的频率以跨越更大的带宽来传输信号。扩展频谱的频率范围非常高，可达到 902~928 MHz 或更高。扩展频谱传输通常以 2~6 Mb/s 的速度传输数据。

当铺设电缆成本很高且很困难时，使用无线电通信可以大大节省费用。与其他无线通信的手段相比，无线电通信比较便宜而且易于安装。但是无线电通信也有其显而易见的缺陷：一是许多网络安装要实施高速(100 Mb/s)的通信来处理拥挤的数据流量，基于无线电的网络速度不能满足这类需求；另一个缺点是，使用的频率难以控制，许多无线电爱好者和蜂窝电话公司使用的频率与无线电通信的频率在相似的范围内，从而干扰信号。此外，自然的障碍物(如山峰)，也会减弱或干扰信号的传输。

2. 红外线技术

红外线也可以作为网络通信的介质。这种技术在电视和立体声系统的远程控制设备上对用户而言最为熟悉。红外线可以沿单方向也可以沿所有的方向进行传播，可以用 LED 进行传输，用光电二极管来接收。传输频率为光的频率(100 GHz~1 000 THz)。

与无线电波相同，在电缆连接比较困难或者有移动用户的情况下，红外线技术是一个成本不高的解决方案，优点在于信号可以在别人不知道时介入。当然这种通信介质也有其显著的缺点，其中一个缺点是在有方向的通信中，数据传输速率仅达 16 Mb/s，在各个方向上传输时速度也不过 1 Mb/s；另一个缺点是红外线不能穿越墙壁，如果把立体声系统拿到另一个房间，然后再试图进行通信时即可发现这一缺点。而且，强光源也会对红外线通信造成干扰。

3. 微波技术

微波系统的工作方式有两种：一种是地面微波，它是在两个盘状的定向天线间传输信号。这种传输的频率为 4~6 GHz 和 21~23 GHz，要求操作人员具备 FCC 许可证；另一种是卫星微波，它是在 3 个定向天线间传输信号，3 个天线之一是空间的一颗卫星，如图 3-9 所示。对于采用这种技术的公司来说，发射卫星或者租用提供这种技术的公司的服务是非常重要的。这类传输的频率范围为 11~14 GHz。

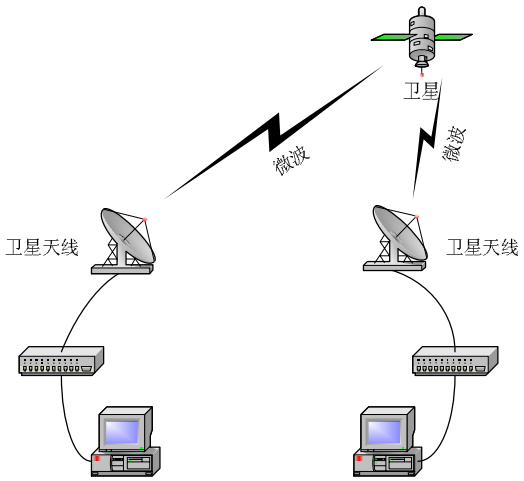

图 3-9　卫星通信

与其他无线介质相同，当布线耗费巨大或者根本不可能布线时就可采用微波通信解决方案。采用地面微波在城市的两个大建筑物之间进行通信是很优秀的解决办法。卫星通信用于跨国或在两个洲之间连接网络。

地面微波和卫星微波的微波介质传输速度可达 1~10 Mb/s，当需要更高的网络速度时，就暴露出了它的局限性。当然，微波技术还有其他的限制，如安装和维护的成本很高。微波传输还极易受到大气环境、恶劣的天气和 EMI 等的影响。

3.1.5　传输介质的选择

在布线基础设施时，有两个最重要的原则，一是为支持网络转型计划提供所需要的性能标准，二则是提供最经济高效的解决方案。

除无线技术外，所有介质类型都支持转向千兆以太网的网络转型计划。千兆以太网是工作站上部署要求最高的以太网系统，但它仍可在所有铜缆和光纤介质上运行。尽管目前几乎没有企业在工作站上使用千兆以太网，但随着用户对数据吞吐量需求不断提高，以及有源设备的成本下降，千兆以太网将会越来越流行。

那些考虑将来转向千兆以太网的用户则可以考虑安装其他介质，以获得资金优势。这就涉及到第二个因素：经济高效性。在大多数网络中，最昂贵的部分是有源硬件：交换机和网络界面卡(NIC)。这在千兆以太网中最为明显，随着选择的介质不同，有源设备的每端口成本最高可以是布线成本的十倍。研究表明，以超五类布线为传输介质的千兆以太网(1000base-t)是所有介质类型中成本最高的。这是因为有源设备极其复杂，其成本相对高于其他型号。研究表明，以多模光纤为传输介质的千兆以太网(1000base-sx)成本相对比较低，而成本最低的是 1000base-tx。它是一种较新的千兆以太网版本，最低要在六类双绞线布线上运行。美国的 TIA 标准委员会正在开发这种新型千兆以太网 1000base-tx，它的技术不如 1000base-t 先进，但仍可支持 1 000 Mb/s 的带宽。

因此，选择传输介质最关键是要根据实际用户的要求、投入的资金、以后扩展升级的方便三方面的因素来决定的。

3.2　计算机网络中的连接设备

计算机网络中有各种不同的连接设备，根据 OSI 七层模型不同，也分成不同的连接设备，其中常用的网络连接设备包括第一层设备集线器和网络设备器、第二层设备网桥和网络交换机、第三层设备路由器等。下面将会分成几节为读者详细讲述。

3.2.1　网络适配器

网络适配器(或被称之为网络接口卡)是一种连接设备。它能够使工作站、服务器、打印机或其他节点通过网络介质接收并发送数据。网卡将来自传输介质的数据信号打包成帧，所以网卡是应该属于数据链路层的设备。在有些情况下，网络接口卡也可以对承载的数据做一些基本的解释，而不只是简单地把信号传送给 CPU 以便让 CPU 进行解释。

网络适配器技术中的先进之处在于它使得这种网络适配器更加智能化。所有的网络适配器不仅能够正确读出数据传送的目标地址信息(而且在以太网中还能检测出冲突)，而且许多网络适配器还具有优化、网络管理和过滤等功能。

网络适配器的类型根据它所依赖的网络传输系统不同(如以太网与令牌环网)而不同。网络适配器与网络传输速率(如 10 Mb/s 与 100 Mb/s)、连接器接口(如 BNC 与 RJ-45)以及兼容的主板或设备的类型有关。

在一个网络设备中安装一块网络适配器之前，用户需要搞清楚该设备需要什么类型的网络适配器。对于一台桌面计算机而言，网络适配器必须与它的总线相匹配。总线是主板用来向其他部件传送数据的电路。总线的能力是由总线的数据通道的宽度(用位表示)和数据传输速率(用 MHz 表示)来决定的。总线的数据通道宽度等于总线在任何时候都能并行传输的数据位数。

- ISA(工业标准结构)：这种最初的个人计算机总线是在 20 世纪 80 年代早期开发出来的。它支持 8 位数据传输，后来扩展至 16 位。ISA 总线不支持 100 MHz 的数据传输，尽管可以在经济型 PC 或者工控机中使用它们，但是它们通常都不能被新式 PC 的网络接口卡所接纳。
- MCA(微通道结构)：IBM 在 1987 年为个人计算机开发的优化的 32 位总线，后来被标准的 EISA 和 PCI 总线所代替。
- EISA(扩展的工业标准结构)：一种兼容以前的 ISA 设备的 32 位总线，它采用更深的两层引脚插槽，因而可以更快地进行传输。EISA 总线是在 20 世纪 80 年代后期为了与 IBM 的 MCA(微通道结构)总线竞争而开发的。
- PCI(外围部件互联)：一种 32 位或 64 位的总线结构，自 20 世纪 80 年代引入以来，已经几乎成为所有新式个人计算机的网络接口卡所采用的总线结构。它比 ISA、MCA 或 PCI 板卡更短，但能以更快的传输速率传输数据。目前，128 位的 PCI 总线正在开发之中。

网络接口卡也可以用于连接其他接口，而不仅仅是用于连接计算机总线。对于便携式

计算机而言，PCMCIA 也可以用于连接网络接口卡。

从目前的市场上来看，网络接口卡分为有线网络接口卡和无线网络接口卡两种。有线网络接口卡也就是前面为读者讲述的几种总线型的网络接口卡，而无线网络接口卡则是使用在无线网络中的。无线网络接口卡有两种不同的接口：一种是 USB 接口的无线网络接口卡，它可以使用在台式机和便携式计算机上；另一种则是 PCMCIA 接口的无线网络接口卡，这种卡只能使用在便携式计算机上。随着便携式计算机硬件不断升级，目前拥有 PCMCIA 接口的便携式计算机越来越少了，所以本着节约成本的角度，建议使用 USB 接口的无线网络接口卡。

3.2.2　交换机

交换机是按照通信两端传输信息的需要，用人工或设备自动完成的方法将需要传输的信息传送到符合要求的相应路由上的技术统称。在计算机网络中，交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。交换机对于因第一次发送到目的地址不成功的数据包，会再次对所有节点同时泛洪该数据包，同时交换机会记录下源 MAC 地址到自己的地址表中，于是，就通过这样的泛洪的方法记录出所有连接在其上的主机 MAC 地址。

1. 交换机的工作原理

要明白交换机的基本工作原理，最重要的是要理解“共享”(Share)和“交换”(Switch)这两个概念。在计算机网络系统中，交换概念的提出是对共享工作模式的改进。在共享式网络中，当同一个局域网中的 A 主机向 B 主机传输数据时，数据包在网络上是以广播方式进行传输的，对网络上的所有节点同时发送同一信息，然后由每一台终端通过验证数据包头部的地址信息来确定是否接收该数据包。因为接收数据的终端节点一般来说只有一个，而现在对所有节点发送该数据包，那么绝大部分数据流量是无效的，这样就造成整个网络数据传输效率低下网络堵塞。另一方面，由于所发送的数据包每个节点都能侦听到，容易出现一些不安全的因素。

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有端口都挂接在这条背部总线上。当交换机从某一节点收到一个以太网帧后，将立即在其内存中的地址表(端口号—— MAC 地址)进行查找，以确认该目的 MAC 的网卡连接在哪一个接口上，然后将该帧转发至相应的接口。如果在地址表中没有找到该 MAC 地址，也就是说，该目的 MAC 地址是首次出现的，交换机就将该数据包广播到所有节点上。拥有该 MAC 地址的网卡在接收到该广播帧后，将立即做出应答，从而使交换机将其节点的“MAC 地址”添加到 MAC 地址表中。

使用这种方式传输数据，一方面效率高，不会浪费网络资源，由于只对目的地址发送数据，一般来说不易产生网络堵塞；另一个方面数据传输安全，因为它不是对所有的节点都同时发送数据，在发送数据时其他节点很难侦听到所发送的信息。

交换机还有一个重要的特点就是，它的每一端口都是独享交换机的一部分总带宽，这

样在速率上对于每个端口来说有了根本的保障。另外，使用交换机也可以把网络进行“分段”，通过对照地址表，交换机只允许必要的网络流量通过交换机，这就是后面将要介绍的 VLAN(虚拟局域网)。通过交换机的过滤和转发，可以有效地隔离广播风暴，减少误包和错包的出现，避免共享冲突。这样交换机就可以在同一时刻进行多个节点对之间的数据传输，每一节点都可视为独立的网段，连接在它上面的网络设备独自享有固定的一部分带宽，无须同其他设备竞争使用带宽。

交换机的主要功能包括物理编址、网络拓扑结构、错误校验、帧序列以及流量控制。目前一些高档交换机还具备一些新的功能，如对 VLAN(虚拟局域网)的支持、对链路汇聚的支持，甚至有的还具有路由和防火墙功能。

交换机除了能够连接同一种类型的网络之外，还可以在不同类型的网络(如以太网和快速以太网)之间起到互联作用，当然这就必须要是多层交换机设备。目前许多交换机都能够提供支持快速以太网或 FDDI 等的高速连接端口，用于连接网络中的其他交换机或者为带宽占用量大的关键服务器提供附加带宽。

2. 生成树协议

通常为了能够保证网络的正常运行，在网络中会再接入一台交换机作为冗余，如图 3-10 所示。

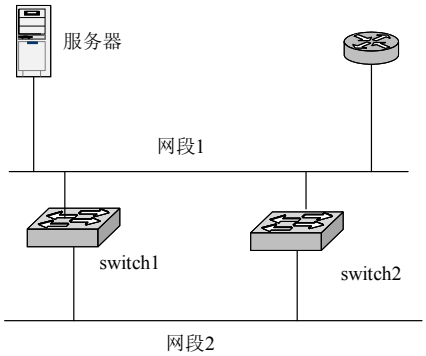

图 3-10　交换机冗余拓扑图

上面的拓扑结构，主要目的是为了防止单点故障，但是同时也带来了几个问题。

(1) 广播风暴

当服务器向网络中发送一个广播帧时，switch1 和 switch2 都会从网段 1 中收到此帧。Switch1 收到帧后，由于是广播地址，所以也会泛洪出去的。Switch2 又从网段 2 处收到此广播帧，这样就形成了一个广播帧不断地被泛洪。如果发送的帧多，就会造成整个网络的广播风暴。

(2) 多个帧的复制问题

如果服务器发送一个单播帧时，那么交换机 MAC 表中无此地址，该单播帧会发给网段 2，与此同时，路由器也收到了一次帧，然而 switch2 在网段 2 中收到帧后，又会转发给路由器，于是路由器就重复接收到了两次帧。这对于一些路由协议计算路径来说，是个很

严重的问题。

(3) MAC 地址库不稳定

当一个单播帧发出，分别在 switch1 和 switch2 上被学习，switch1 学习到服务器连在 switch1 上的某个接口，而 switch2 也学习到了服务器连接在 switch2 上的某个接口，于是就使得 MAC 地址表出现错误，因为一个 MAC 地址不可能接在两个接口上。

由于冗余交换拓扑会形成环路，所以出现了 STP 技术来解决这个问题。STP 又称为生成树协议，它通过将其中一条环路暂时给封闭起来，让它处于休眠状态，等到主链路发生故障后，这条链路就会自动由休眠状态转为可用状态，如图 3-11 所示。

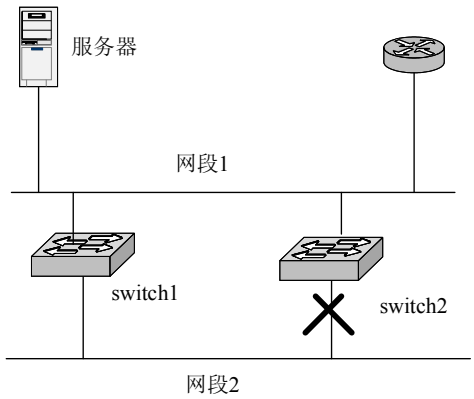

图 3-11　使用 STP 技术的冗余网络

3. 交换机的分类

由于交换机具有许多优越性，随着网络技术的发展，出现了各种类型的交换机，满足了各种不同应用环境的需求。下面将简单介绍交换机的主流分类。

(1) 根据网络覆盖范围划分

根据网络的覆盖范围进行划分，可以将交换机分为广域网交换机和局域网交换机两大类。

其中，广域网交换机主要用于电信城域网互联、互联网接入等领域的广域网中，提供通信用的基础平台；局域网交换机应用于局域网，用于连接终端设备，如服务器、工作站、集线器、路由器、网络打印机等网络设备，以提供高速独立通信通道。

(2) 根据传输介质和传输速度划分

根据交换机使用的网络传输介质及传输速度的不同，一般可以将局域网交换机分为以太网交换机、快速以太网交换机、千兆(G 位)以太网交换机、10 千兆(10 G 位)以太网交换机、FDDI 交换机、ATM 交换机和令牌环交换机等类型。

(3) 根据交换机的结构划分

如果根据交换机的端口结构进行划分，交换机大致可分为固定端口交换机和模块化交换机两种不同的类型。其实还有一种是两者兼顾的交换机，那就是在提供基本固定端口的基础上再配备一定的扩展插槽或模块的交换机。

(4) 根据交换机工作的协议层划分

网络设备都在 OSI 这一开放模型的一定层次上进行工作，工作所在的层次越高，说明其设备的技术性越高，性能也越好，档次也就越高。交换机也一样，随着交换技术的发展，交换机由原来在 OSI 的第 2 层工作，发展到了可以在第 4 层工作，所以，根据工作的协议层，交换机可分第 2 层交换机、第 3 层交换机和第 4 层交换机。

此外，根据交换机所应用的网络层次的不同，还可以将网络交换机划分为企业级交换机、校园网交换机、部门级交换机、工作组交换机和桌机型交换机 5 种。还可以按交换机是否支持网络管理功能进行划分，将交换机分为“网管型”和“非网管理型”两大类。

4. 交换机的选购

以上对交换机的几种主流分类方法逐个进行了简单介绍，读者对交换机的主要类型有了一个基本的了解，以下将介绍交换机的主要交换技术及选购注意事项。

(1) 转发方式

数据包的转发方式主要分为“直通式转发”(现为准直通式转发)和“存储式转发”两种。由于直通式转发只需检查数据包的包头而不需要存储，所以切入方式具有延迟小和交换速度快的优点。存储转发方式在处理数据时延时大，但它可以对进入交换机的数据包进行错误检测，并且能支持不同速度的输入/输出端口间的交换，有效地改善网络性能。同时这种交换方式支持不同速度端口间的转换，保持高速端口和低速端口之间的协同工作。

由于不同的转发方式适用于不同的网络环境，因此，应当根据需要作出相应的选择。通常情况下，如果网络对数据的传输速率要求不是太高，可以选择存储转发式交换机；如果网络对数据的传输速率要求较高，可选择直通转发式交换机。

低端交换机通常只拥有一种转发模式，或是存储转发模式，或是直通模式，只有中高端产品才兼具两种转发模式，并具有智能转换功能，可根据通信状况自动切换转发模式。

(2) 延时

交换机的延时(Latency)也称延迟时间，指的是从交换机接收到数据包到开始向目的端口发送数据包之间的时间间隔。造成延时的主要原因是受所采用的转发技术等因素的影响。延时越小，数据的传输速率越快，网络的效率就越高。特别是对于多媒体网络而言，较大的时间延迟，往往会导致多媒体在播放时的短暂中断，所以交换机的延迟时间越小越好，但是，延时越小的交换机价格也就越贵。

(3) 管理功能

交换机的管理功能(Management)指的是交换机如何控制用户访问交换机，以及系统管理人员通过软件对交换机的可管理程度如何。如果需要以上的配置和管理，则需选择网管型交换机，否则只需选择非网管型的。

(4) MAC 地址数

交换机之所以能够直接对目的节点发送数据包，最关键的技术就是交换机可以识别连在网络上的节点的网卡 MAC 地址，形成一个 MAC 地址表。这个 MAC 地址表存放在交换机的缓存中，当交换机需要向目的地址发送数据时，就可以在 MAC 地址表中查找到这个

MAC 地址的节点位置，然后直接向这个位置的节点发送数据。

不同档次的交换机每个端口所能够支持的 MAC 数量不同。在交换机的每个端口，都需要足够的缓存来保存这些 MAC 地址，所以缓存容量的大小就决定了相应交换机所能记忆的 MAC 地址的数量。

(5) 背板带宽

在选购交换机时，应该注意交换机背板带宽。背板带宽越宽越好，它将为用户的交换器在高负荷下提供高速交换。由于所有端口之间的通信都需要通过背板完成，所以背板所能够提供的带宽就成为端口间并发通信时的总带宽。带宽越大，能够给各个通信端口提供的可用带宽就越大，数据交换速度就越快；带宽越小，能够给各个通信端口提供的可用带宽就越小，数据交换速度也就越慢。因此，在端口带宽和延迟时间相同的情况下，背板带宽越大，交换机的传输速率就越快。

(6) 交换机的协议功能

第 4 层交换技术相对原来的第 2 层和第 3 层交换技术具有明显的优点，从操作方面来看，第 4 层交换是稳定的，因为它将包控制在从源端到宿端的区间中。另一方面，路由器或第 3 层交换，只针对单一的数据包进行处理，不清楚上一个数据包从哪里来、也不知道下一个数据包的情况，它们只是检测数据包报头中的 TCP 端口数字，根据应用建立优先级队列，路由器根据链路和网络可用的节点决定数据包的路由；而第 4 层交换机则是在可用的服务器和性能基础上先确定区间。

(7) 端口

交换机与集线器一样，也有端口带宽之分，但这里所指的带宽与集线器的端口带宽不一样，因为交换机的端口带宽是独享的，而集线器上端口的带宽是共享的。交换机的端口带宽目前主要包括 10 M、100 M 和 1 000 M 3 种，现在高端的交换机端口甚至达到 10 G，但根据这些带宽又有不同的组合形式，以满足不同类型网络的需要。

(8) 光纤解决方案

如果用户的布线中必须选用光纤，则在交换机选择方案中可以有以下两种方案：第一种方案是选择具有光纤接口的交换机，第二种方案是在模块结构的交换机中加装光纤模块。第一种性能比较好，但不够灵活，而且价格较贵；第二种方案具有较强的灵活配置能力，性能也较好，但价格较贵。

5. 交换机的品牌

目前，市场上流行的交换机有 CISCO、3COM、华为、D-LINK、TP-LINK 等很多品牌。每种品牌的交换机都可以使用在不同的环境下。D-LINK、TP-LINK 的交换机是智能型交换机，也就是说只需将网线插到交换机上的接口上即可。而 CISCO、3COM 和华为的交换机则不是简简单单将网线插到其接口上，还需要在其中进行配置。目前，中大型网络多数使用 CISCO、3COM 和华为的交换机。在这里读者可能会有疑问，既然有那种可以直接插上去不用配置的交换机，人们为什么还要使用那些需要配置的交换机呢？在一个小的网络里，工作站的台数不多，流量自然也就不大，这种情况下，无须对其流量进行规划。然

而在中大型网络中，工作站的台数众多，流量很大，而带宽资源有限，在这种情况下，就必须合理地规划流量。特别是在一个拥有语音、视频等数据需要传输的网络，因为这些数据是实时性的，必须要求很小的延迟，当流量没有经过规划，都是满足 FIFO 的默认传输流量的方式，就会使得这些语音、视频数据无法得到很好的传输。

为了能够解决这些问题，在 CISCO、3COM 和华为的交换机中就拥有众多的命令集，通过配置这些命令，来使得交换机在网络中能够保证网络的 QOS(质量服务)。这个配置是可以按照管理员的自身意志和目前网络的现状来配置的。所以，这种交换机能够很好地规划一个网络，并且能够让网络中的流量得到合理分配。

由于网络技术的发展，CISCO、3COM 和华为按照 OSI 七层协议将交换机分为两层交换机(也就是普通的交换机)、三层交换机(带路由功能的交换机)和多层交换机(包括四层交换机、七层交换机等)。在实际网络规划中，会将这些交换机按图 3-12 所示进行规划。

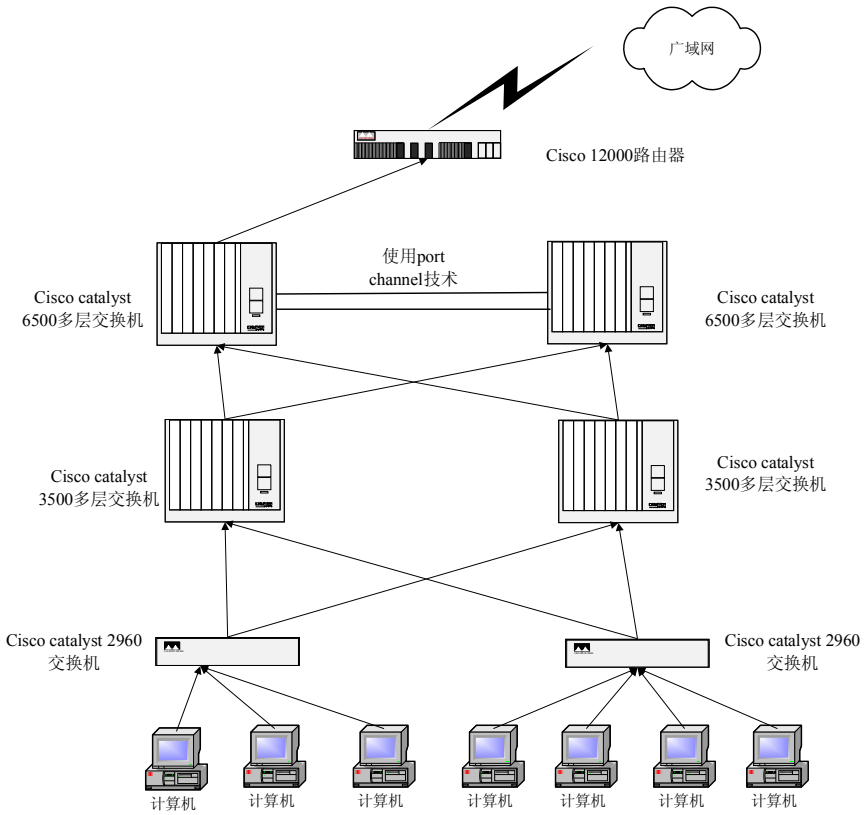

图 3-12　网络规划图

3.2.3　路由器

路由器是一种用于连接多个网络或网段的网络设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使路由器之间能够相互“读懂”对方的数据，从而相连成一个更大的网络。路由器与交换机不同，它不是应用于同一网段的设备，而是应用于不同网段或不同网络之间的设备，属于网际设备。路由器之所以能在不同网络之间起到“翻译”的作

用，是因为它不是一个纯硬件设备，而是具有相当丰富的路由协议的软、硬结构设备，如 RIP 协议、OSPF 协议、EIGRP 和 IPV6 协议等。这些路由协议用于实现不同网段或网络之间的相互“理解”。

1. 路由器的工作原理

路由器通过识别不同网络的网络 ID 号识别不同的网络，所以为了确保路由成功，每个网络都必须有一个唯一的网络编号。路由器要识别另一个网络，首先就要识别对方网络的路由器 IP 地址的网络 ID，看是否与目的节点地址中的网络 ID 号相一致，如果相同则立即向这个网络的路由器发送数据，接收网络的路由器在接收到源网络发来的报文后，根据报文中所包含的目的节点的 IP 地址中的主机 ID 号来识别需要将数据发送给哪一个节点，然后直接发送。

为了更清楚地说明路由器的工作原理，假设有这样一个简单的网络：其中一个网段的网络 ID 号为 A，在同一个网段中有 4 台终端设备连接在一起，每台设备的 IP 地址分别为：A1、A2、A3 和 A4。连接在这个网段上的一台路由器是用来连接其他网段的，路由器连接于 A 网段的那个端口的 IP 地址为 A5。同样，路由器连接另一网段为 B 网段，这个网段的网络 ID 号为 B，那连接在 B 网段的另外几台工作站设备的 IP 地址可以设为 B1、B2、B3 和 B4，同样连接于 B 网段的路由器端口的 IP 地址可以设置为 B5，结构如图 3-13 所示。

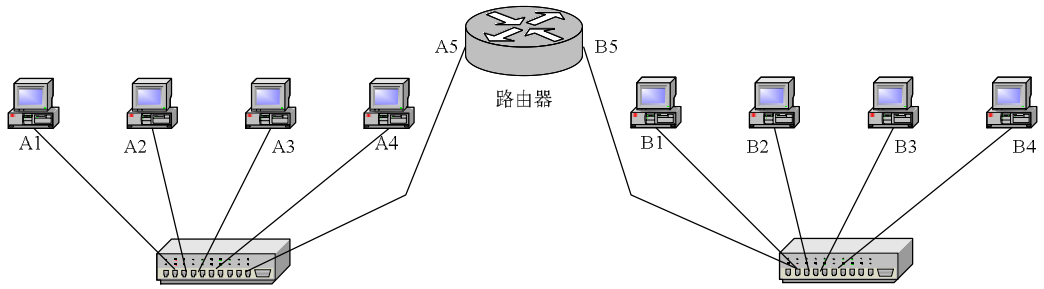

图 3-13　由路由器连接起来的两个网络

在这个简单的网络中同时存在着两个不同的网段，现在，如果 A 网段中的 A1 用户需要发送一个数据给 B 网段的 B2 用户，有了路由器就变得非常简单了。

首先，A1 用户把需要发送的数据及报文准备好，以数据帧的形式通过集线器或交换机广播发给同一网段的所有节点，路由器在侦听到 A1 发送的数据帧后，分析目的节点的 IP 地址信息，如果得知数据不是本网段的，就把数据帧接收下来，进一步根据其路由表进行分析，得知接收节点的网络 ID 号与 B5 端口的网络 ID 号相同，这时路由器的 A5 端口就直接把数据帧发送给路由器 B5 端口。B5 端口再根据数据帧中的目的节点 IP 地址信息中的主机 ID 号来确定最终目的节点为 B2，然后再将数据发送到节点 B2。这样，一个完整的数据帧的路由转发过程就完成了，数据也被正确、顺利地发送到了目的节点。

(1) 路由选择表

每个路由器中都保存有一个路由表，路由表为路由器存储到达网络上任何一个目的地

所需要的一切必要的信息。如图 3-14 所示的是一个路由表的实例，它的每一项都包含以下信息。

- 目的 IP 地址(Destination)，如图 3-14 所示的第 1 列所示，它既可以是一个完整的主机地址，也可以是一个网络地址，具体由该表中的标志字段来指定，或者使用一个默认的地址(default)。主机地址包含一个非 0 的主机号，用于指定某一特定的主机，而网络地址中的主机号为 0，用于指定网络中的所有主机(如以太网、令牌环网)。
- 下一跳(Next-Hop)，如图 3-14 中的第 2 列所示，该值可以是直接连接的网络 IP 地址，也可以是一个在直接相连网络上的路由器，通过它可以转发数据报。下一跳路由器不是最终的目的，但是它可以把用户传送给它的数据报转发到最终目的。
- 标志(Flags)，其中的一个标志用于指明目的 IP 地址是网络地址还是主机地址，另一个标志用于指明下一跳路由器是否为真正的下一跳路由器，还是一个直接相连的接口。
- 接口(Interface)，它为数据报的传输指定一个网络接口。

路由器基本上有两种获得路由信息的途径：静态路由选择和动态路由选择。在路由表中的手动添加表项是静态路由选择的例子。当路由器是自动控制获得信息时，称为动态路由选择。

Destination	next-hop	Netmask	Flags	Interface
202.112.10.0	*	255.255.255.224	U	eth0
default	202.112.10.1	0.0.0.0	UG	eth0

图 3-14　路由表实例

(2) 路由选择的步骤

IP 路由选择是逐跳地(Hop-By-Hop)进行的。IP 并不知道到达任何目的的完整路径(除了那些与主机直接相连的目的)。所有的 IP 路由选择只为数据报的传输提供下一站路由器的 IP 地址，它假定下一站路由器比发送数据报的主机更接近目的主机，而且下一站路由器与该主机是直接相连的。

IP 路由选择按如下操作步骤进行。

- 搜索路由表，寻找能与目的 IP 地址完全匹配的表目(网络号和主机号都要匹配)，如果找到完全匹配的表目则把报文发送给该表目指定的下一站路由器或直接连接的网络接口(取决于标志字段的值)。
- 搜索路由表，寻找与目的网络号相匹配的表目，如果找到该表目，则把报文发送给该表目指定的下一站路由器或直接连接的网络接口(取决于标志字段的值)。目的网络上的所有主机都可以通过这个表目进行处理。这种搜索网络的匹配方法必须考虑可能的子网掩码。
- 搜索路由表，寻找被标为“默认”(default)的表目，如果找到该表目，则把报文发送给该表目指定的下一站路由器。

如果以上这些步骤都没有被成功执行，那么数据报就不能被成功传送。如果不能传送的数据报来自本机，那么本机一般会向生成数据报的应用程序返回一个“主机不可达”或“网络不可达”的错误信息。

完整主机地址匹配工作在网络号匹配之前进行。只有当这两项匹配工作都失败后才选择默认路由。默认路由以及下一站路由器发送的 ICMP 间接报文(如果用户为数据报选择了错误的默认路由)，是 IP 路由选择机制中的功能强大的特性。为一个网络指定一个路由器，而不必为每个主机指定一个路由器，这是 IP 路由选择机制的另一个基本特性。

(3) 路由选择协议

路由选择协议指的是那些执行路由选择算法的协议，即通过互联网络操纵网络的协议，其中包括内部网关路由选择协议(IGRP)、增强型内部网关路由选择协议(Enhanced IGRP)、开放最短路径优先(OSPF)、外部网关协议(EGP)、边缘网关协议(BGP)、中介系统到中介系统(IS-IS)和路由选择信息协议(RIP)等。

路由选择协议可以分为两种：内部协议和外部协议。内部协议在自治系统(AS)内部路由，如 OSPF 和 RIP；而外部协议则是在自治系统之间路由，最常见是外部网关协议 EGP(External Gateway Protocol)和边缘网关协议 BGP(Border Gateway Protocol)。BGP 是较新的协议，将逐渐取代 EGP。

① 自治系统

从路由选择的角度来讲，处于一个管理机构控制之下的网络和路由器群被称为一个自治系统(Autonomous System)。

在一个自治系统内的路由器可以自由地选择寻找路由、广播路由、确认路由以及检测路由的一致性。在这样的定义下，核心路由器本身也构成了一个自治系统。一个自治系统可以自由地选择其内部的路由选择体系结构，但是必须收集其内部所有的网络信息，并责成若干个路由器把这些可达信息发送给其他的路由系统。整个因特网使用核心体系结构，每个与之相连的自治系统都要把可达信息发送到因特网的核心路由器。

② RIP(Routing Information Protocol)

RIP 是广泛使用的路由选择协议。RIP 使用距离向量算法，所以其路由选择是基于两点间的“跳(hop)”数，穿过一个路由器就是一跳。主机和路由器都可以运行 RIP，但是主机只是接收信息，并不发送信息。路由信息可以从指定路由器请求，但是通常每隔 30 秒广播一次以保持其正确性。RIP 使用 UDP 通过端口 520 在主机和路由器之间通信。路由器之间传送的信息用于建立路由表，由 RIP 选定的路由距离目的地跳数最少。如果到达信宿的路径有多条，根据 RIP 协议，路由器选择步跳数最少的路径。因为跳数是 RIP 协议决定最佳路径时使用的唯一路由选择度量，所以它不一定是到信宿的最快路径。另外，RIP 并没有任何链接质量的概念，所有的链路都被认为是相同的，低速的串行链路与高速的光纤链路被认为是相同的，所以，跳数最少的路由并非最畅通。

使用 RIP 协议还会带来另一个问题：信宿的距离可能很远而无法定位。在 RIP 协议中，数据转发能够通过的跳数最多为 15 跳。因此，如果信宿网络超出 15 个路由器的距离，就被认为是无法到达的网络。

③ OSPF(Open Shortest Path First)

与采用距离向量的 RIP 协议不同的是，OSPF 是一个链路状态协议。OSPF 意味着开放最短路径优先，这个内部网关协议使用了一些标准来确定到达目的地的最佳路径，这些标准包含有费用度量，其中包括路由速度、业务量、可靠性和安全性等因素。在一个链路状态协议中，路由器并不与其相邻站交换距离信息，它采用的方法是，每个路由器主动地测试与其邻站相连链路的状态，将这些信息发送给它的邻站，而邻站将这些信息在自治系统中广播出去。每个路由器接收到这些链路状态信息时，建立起完整的路由表。

OSPF 与 RIP 以及其他路由选择协议的不同之处在于，OSPF 直接使用 IP，它并不使用 UDP 或 TCP。对于 IP 头部的 Protocol 字段，OSPF 有自己的值。另外，作为一种链路状态协议而不是距离向量协议，OSPF 还有着一些优于 RIP 的特点，如下所示。

- OSPF 可以对每个 IP 服务类型计算各自的路由集。这意味着对于任何目的地，可以有多个路由表表项，每个表项对应着一个 IP 服务类型。
- 给每个接口指派一个无维数的费用。可以通过吞吐率、往返时间、可靠性或其他性能来进行指派。可以给每个 IP 服务类型指派一个单独的费用。
- 当同一个目的地址存在着多个相同费用的路由时，OSPF 在这些路由上平均分配流量，称之为流量平衡。
- 路由器之间的点对点链路不需要每端都有一个 IP 地址，我们将它称为无编号网络。这样可以节省 IP 地址。
- OSPF 采用多播，而不是采用广播形式，这样可以减少不参与 OSPF 的系统负载。

随着大部分计算机厂商支持 OSPF，在很多网络中，OSPF 将逐步取代 RIP。

2. 路由器的分类

路由器发展到今天，为了满足各种应用需求，出现过各式各样的路由器。以下将按照不同的标准对各式各样的路由器进行分类。

(1) 按性能档次划分

按性能档次划分，可将路由器分为高、中和低档 3 类路由器，不过各厂家对路由器的档次划分并不完全一致，通常将背板交换能力大于 40 Gb/s 的路由器称为高档路由器；背板交换能力在 25~40 Gb/s 之间的路由器称为中档路由器；背板交换能力低于 25 Gb/s 的为低档路由器。

(2) 按结构划分

按结构划分，可将路由器分为模块化结构与非模块化结构两种。模块化结构可以灵活地配置路由器，以适应企业不断增加的业务需求；非模块化的路由器只能提供固定的端口。通常情况下，中高端路由器为模块化结构，低端路由器为非模块化结构。

(3) 从功能上划分

从功能上进行划分，可将路由器分为核心层(骨干级)路由器、分发层(企业级)路由器和访问层(接入级)路由器 3 种。

(4) 从应用上划分

从应用上进行划分，路由器可分为通用路由器与专用路由器两种。一般所说的路由器都是通用路由器。专用路由器通常用于实现某种特定功能，对路由器接口、硬件等作专门优化。例如，VPN 路由器用于为远程 VPN 访问用户提供路由，它要求在隧道处理能力以及硬件加密等方面具备特定的功能；宽带接入路由器则强调接口带宽及种类。

(5) 从所处的网络位置划分

根据路由器所处的网络位置进行划分，通常将路由器划分为“边界路由器”和“中间节点路由器”两类。“边界路由器”是处于网络边缘、用于不同网络路由器的连接；而“中间节点路由器”则处于网络的中间，通常用于连接不同的网络，起到一个数据转发的桥梁作用。

3. 路由器的选购

因其价格昂贵且配置复杂，所以绝大多数用户对路由器的选购显得非常茫然。路由器的选购主要从以下几个方面加以考虑。

(1) 吞吐量

路由器的吞吐量指的是路由器对数据包的转发能力，如较高档的路由器可以对较大的数据包进行正确而快速地转发；而较低档的路由器则只能转发较小的数据包。对于较大的数据包，需要将其拆分成许多小的数据包进行分别转发，这种路由器的数据包转发能力较差，与下面所讲的背板容量有非常紧密的关系。

(2) 背板能力

背板能力通常指的是路由器背板容量或者总线带宽能力，这个性能对于保证整个网络之间的连接速度是非常重要的。如果所连接的两个网络速率都比较快，但是路由器的带宽较小，这将直接影响到整个网络之间的通信速度。所以，一般来说，如果是连接两个较大的网络，网络流量较大时应该格外注意路由器的背板容量。

(3) 丢包率

丢包率指的是在一定的数据流量下，路由器不能正确进行转发的数据包在总的数据包中所占的比例。丢包率的大小会影响到路由器线路的实际工作速度，严重时甚至会使线路中断。

(4) 转发时延

转发时延指的是需转发数据包的最后一比特进入路由器端口到该数据包的第一比特出现在端口链路上的时间间隔，它与背板容量、吞吐量参数也是紧密相关的。

(5) 路由表容量

路由表容量指的是路由器在运行中可以容纳的路由数量。一般来说越高档的路由器其路由表容量就越大，因为它可能要面对非常庞大的网络。这一参数与路由器自身的缓存大小有关。

(6) 路由器所支持的路由协议

因为路由器所连接的网络的类型不同，这些网络所支持的网络通信、路由协议也就有可能不一样，对于在网络之间起到连接桥梁作用的路由器来说，如果不支持任意一方的协

议，那就无法实现它在网络之间的路由功能，因此在选购路由器时，需要注意所选路由器所能支持的网络路由协议有哪些，特别是在广域网中的路由器，因为广域网的路由协议非常多，网络也相当复杂，例如，目前电信局提供的广域网线路主要有 X.25、帧中继、DDN 等多种协议。

(7) 可靠性

可靠性指的是路由器的可用性、无故障工作时间和故障恢复时间等指标，当然新买的路由器暂时无法验证这些指标。不过可以优先选购信誉较好、技术较先进的品牌。

此外，选购路由器还要考虑路由器的安全性、可管理性和成本等因素。

4. 路由器的品牌

和交换机一样，市场上也有很多不同品种的路由器。目前，市场上的路由器分为两种：一种是智能路由器，这种路由器主要是用来为小型网络设计共享上网而生产的低端产品；另一种主要是以 CISCO 为主的高端路由器产品，这种路由器含丰富的命令集，能够帮助管理员或网络设计者以人性化的角度设计网络，保证网络的安全、便捷、快速。

路由器主要是使用在网络的前端，作为网络的接入设备，它直接和运营商的接入光纤相连。

一般普通路由器只是将运营商网络同内部网络进行一个简单的连接，并且将内网的地址进行一个简单的 NAT 转换出去，让内部网络可以访问外部网络。而以 CISCO 为主的高端路由器不但具有以上普通路由器的功能，而且还可以充当部分防火墙的功能，它可以通过在路由器上配置不同的访问控制列表(ACL)，来达到控制网络上的流量的进与出。这样可以有效防止内网非法访问外网，以及外网攻击内网，当然，路由器必定不是专业的防火墙，不可能做到跟防火墙一样的功效。另外，路由器可以在大中型网络中，使用不同的路由协议来规划不同的网络路径，从而使得数据能够以最短路径发送的目的地。

3.2.4　集线器

集线器(Hub)是一种特殊的中继器，它与中继器的区别在于集线器能够提供多端口服务，所以集线器也称为多口中继器。

集线器的基本功能是信息分发，它把一个端口接收到的所有信号向其他所有端口分发出去。一些集线器在分发信号之前将弱信号重新生成，一些集线器整理信号的时序以提供所有端口间的同步数据通信。

作为网络传输介质间的中央节点，集线器克服了介质单一通道的缺陷。以集线器为中心的优点是：当网络系统中的某条线路或某节点出现故障时，不会影响到网络上其他节点的正常工作。

下面来看看集线器是怎么嵌入到网络中进行工作的。

如图 3-15 所示的是基本的 10Base-2 网络，机器间通过电缆直接相连，其中有一条主电缆(或者称为总线)，任何设备发送数据都要通过总线到达其他设备。如果主电缆(总线)发生故障，将影响到整个网络中的数据传输。

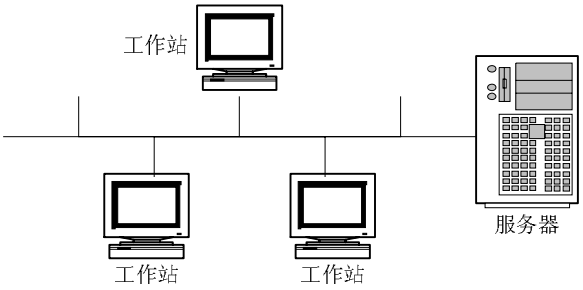

图 3-15　基本的 10Base-2 网络

如图 3-16 所示的是 10Base-T 网络，每一台设备仅和集线器连接在一起，各台设备通过集线器连接在一起，构成了一个星型的拓扑网络。这时网络中的某条链路或者某个端点出现故障时不影响到其他链路。细心的读者可能会注意到，如果集线器出现故障，整个网络也受到影响，这也正是星型拓扑的缺点所在。

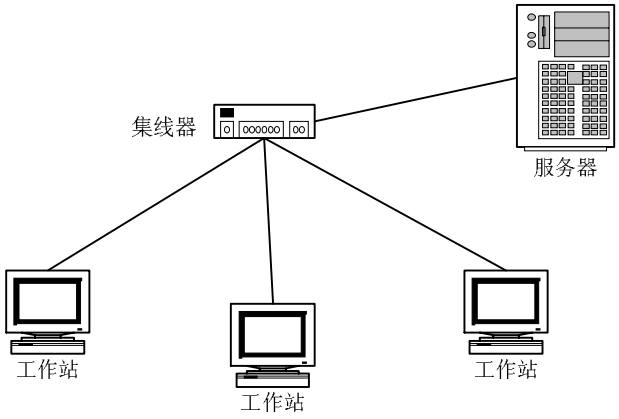

图 3-16　基本的 10Base-T 网络

在 10Base-T 网络中，所有设备需要用非屏蔽双绞线连接到一个或多个集线器上，集线器应该有多个端口甚至有多种类型的端口。集线器在星型拓扑网络中起着重要的作用。

集线器有多种类型，各种类型的集线器具有特定的功能并提供不同等级的服务。集线器可分为被动(Passive)集线器、主动(Active)集线器和智能(Intelligent)集线器 3 种。

1. 被动集线器

被动集线器不能用来提高网络性能，也不能帮助用户检测硬件错误或性能瓶颈。它只是简单地从一个端口接收数据并通过所有端口分发数据。被动集线器是星型拓扑以太网的入门级设备。

被动集线器通常有一个 10Base-2 端口和一些 RJ-45 接头，其中 10Base-2 端口可以用于连接主干。

2. 主动集线器

主动集线器除了拥有被动集线器的所有性能，还能监视数据。它在以太网实现存储转

发技术中扮演着重要的角色。它在转发数据之前检查数据，但并不区分数据的优先次序，而是纠正损坏的分组并调整时序。

如果信号比较弱但仍然可读，主动集线器在转发信号前将其恢复到较强的状态。主动集线器还可以报知哪些设备失效，从而提供一定的诊断能力。

有些线缆可能有电磁干扰，使分组不能按正常时序到达集线器。主动集线器可以将转发的分组重新同步。有时数据根本就到达不了目的地，这时主动集线器通过在单个端口重发分组来弥补数据的丢失。主动集线器可以调整时序以适应较慢的、错误率较高的连接。这样做虽然会降低连接到该集线器上的设备的整体网络速度，但是，不会造成数据的丢失。此外，时序调整实际上可以减少局域网中的冲突次数，数据不需要重复广播，局域网就可以传输新的数据。

主动集线器提供一定的优化性能和一些诊断能力，它的价格比简单的被动集线器昂贵，可以配置多个或多种端口。

3. 智能集线器

与前两种集线器相比，智能集线器可以使用户更有效地共享资源。智能集线器技术近些年才出现，它除了有主动集线器的特性外，还提供了集中管理功能。如果连接到智能集线器上的设备出了问题，用户可以很容易地进行识别、诊断和修补。在一个大型网络中，如果没有集中的管理工具，那么用户常常需要一个线盒一个线盒地跑，查找出问题的设备。

智能集线器另一个出色的特性是，可以为不同设备提供灵活的传输速率。除了连接到高速主干的端口外，智能集线器还支持到桌面的 10 Mb/s、16 Mb/s 和 100 Mb/s 的速率，即以太网、令牌环和 FDDI(光纤分布式数据接口)的速率。

4. 高级特性

高级集线器除了提供上述各种类型集线器所具有的功能外，还提供了其他的一些特性，如冗余交流电源、内置直流电源、冗余风扇，还有线缆连接的自动中断、模块的热插拔、自动调整 10Base-T 接头的极性，以及冗余配置存贮、冗余时钟等。有些集线器还集成了路由和桥接功能。

3.3 服 务 器

服务器是计算机网络上最重要的设备。服务器指的是在网络环境下运行相应的应用软件，为网络中的用户提供共享信息资源和服务的设备。服务器的构成与微机基本相似，有处理器、硬盘、内存、系统总线等，但服务器是针对具体的网络应用特别制定的，因而与微机在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面存在很大的差异。通常情况下，服务器比客户机拥有更强的处理能力、更多的内存和硬盘空间。服务器上的网络操作系统不仅可以管理网络上的数据，还可以管理用户、用户组、安全和应用程序。

本节将主要介绍服务器的一些基本特性、分类以及评议一台服务器的性能指标和如何选购服务器等内容。

3.3.1 服务器的特性

服务器是网络的中枢和信息化的核心，具有高性能、高可靠性、高可用性、I/O 吞吐能力强、存储容量大、联网和网络管理能力强等特点。

1. 可用性

服务器的可用性(Usability)指的是服务器应该具有高可靠性和高稳定性，不要频繁出现死机、故障和停机待修现象。因为多数情况下服务器被要求连续工作，所以它的可靠性非常重要，一旦服务器发生故障，将会造成大量数据丢失、许多重要业务停顿，甚至造成整个网络的瘫痪，其损失是难以估量的。

目前，提高服务器可靠性的一个普遍做法是部件的冗余配置和内存查、纠错技术。服务器一般采用具有查、纠错能力的 ECC 内存，如 IBM 的服务器，有的服务器还采用了专门的具有 ChipKill 超强查、纠错能力的内存，从而提高服务器的可靠性。硬件的设备冗余通常支持热插拔功能，如冗余 CPU、RAM、PCI 适配器、电源、风扇等，可以在单个部件失效时自动切换到备用设备上，保证系统运行。

2. 可扩展性

服务器的可扩展性指的是服务器的硬件配置可以根据需要灵活配置，如内存、适配器、硬盘和处理器等由于不同时期的网络配置可能会发生变化，所以服务器的硬件配置也要随之改变。服务器需要具有较多的 PCI、PCI-X 插槽以连接多个板卡；因为需要高容量磁盘来存储服务器数据，所以还需要有较多的驱动器支架。一般的服务器机箱都设有七八个硬盘托架，可以放置更多的硬盘。

3. 可管理性

服务器的可管理性指的是服务器具有非常高的可管理性能，从而为用户提供十分方便、及时的网络管理，服务器的可管理性包括硬件和软件方面的管理，但主要是软件方面的管理。

在服务器硬件的可管理性方面，多数是在服务器主板上集成了各种传感器，用于检测服务器上的各种硬件设备，同时配合相应的管理软件，远程监测服务器，从而使网络管理员对服务器系统进行及时有效的管理。

服务器的可管理性主要体现在软件方面。在服务器软件的可管理性方面除了网络操作系统自身所具有的各种可管理性外，服务器厂商还可以针对特定的需求或者硬件结构，设计开发特定的管理软件。

4. 可利用性

服务器的可利用性是从服务器的处理能力上来说的，因为服务器所要承担的负荷比较

重，要面向整个网络，所以要求服务器具有较高的运算处理能力和处理效率。

在服务器的处理能力方面，目前最主要的技术是通过采用对称多处理技术和群集技术来实现。对称多处理器(SMP)技术指的是在一个计算机上汇集多个处理器(多 CPU)，各个 CPU 之间共享内存子系统以及总线结构。虽然同时使用多个 CPU，但是从管理的角度来看，它们的表现就像一台单机一样。需要注意的是，所使用的 CPU 必须是成对出现，即必须是如 2、4、6、8 之类的双数，除了单 CPU 的服务器之外。

服务器群集技术也是提高服务器性能的一项技术措施，一个服务器群集包含多台拥有共享数据存储空间的服务器，各服务器之间通过内部局域网进行相互通信。当其中的某台服务器发生故障时，它所运行的应用程序将由其他服务器自动接管。在大多数情况下，群集中所有的计算机都拥有一个共同的名称，群集系统内的任意一台服务器都可以被所有的网络用户所使用。服务器群集将一组相互独立的计算机通过高速的通信网络而组成的一个单一的计算机系统，并以单一系统的模式进行管理。

3.3.2　服务器的分类

服务器发展到今天，可以适应各种不同功能、不同环境的服务器不断地涌现，分类标准也变得多样化，主要有如下几种分类标准。

- 按应用层次进行划分，服务器可以分为入门级服务器、工作组级服务器、部门级服务器和企业级服务器 4 类。
- 按处理器架构进行划分，可以分为 X86、IA-64、RISC 等几种架构。
- 如果按服务器的处理器所采用的指令系统划分，可以把服务器分为 CISC 架构服务器、RISC 架构服务器和 VLIW 架构服务器 3 种。
- 服务器按用途进行划分，可分为通用型服务器和专用型服务器两类。
- 按服务器的机箱结构进行划分，可以把服务器划分为“台式服务器”、“机架式服务器”、“机柜式服务器”和“刀片式服务器”4 类。

3.3.3　服务器的选择

服务器是整个网络的核心，如何选择与本网规模相适应的服务器，是决策者和技术人员都需要考虑的问题。下面是配置采购网络服务器需要注意的几点。

1. 性能要稳定

为了保证网络能正常运转，所选择的服务器首先要确保稳定，因为一个性能不稳定的服务器，即使配置再高、技术再先进，也不能保证网络能正常工作，后果严重的话可能还会给使用者造成难以估计的损失。另一个方面，性能稳定的服务器意味着为公司节省维护费用。

2. 以够用为准则

由于本身的信息资源以及资金实力有限，不可能一次性投入太多的经费去采购档次很

高或技术很先进的服务器。对于中小规模的网络而言，最重要的就是根据实际情况，并参考以后的发展规划，有针对性地选择既能满足目前信息化建设的需要又不至于投入太多资源的解决方法。

3. 应考虑扩展性

由于网络处于不断发展之中，快速增长的应用不断地对服务器的性能提出新的要求，为了减少更新服务器带来的额外开销和对工作的影响，服务器应当具有较高的可扩展性，可以及时调整配置来适应发展。

4. 便于操作和管理

所谓便于操作和管理，指的是采用相应的技术来提高系统的可靠性能，简化管理因素和降低维护费用成本。一般的公司通常没有专业人员来维护和管理服务器，这就要求服务器必须具有非常好的易操作性和可管理性，当出现故障时无须专业人员也能将故障排除。

5. 满足特殊要求

不同的网络应用其侧重点不同，对服务器性能的要求也不一样。例如，VOD 服务器要求具有较高的存储容量和数据吞吐率，而 Web 服务器和 E-mail 服务器则要求 24 小时不间断运行。如果在网络服务器中存放的信息属于机密资料，就要求所选择的服务器有较高的安全性。

6. 配件搭配合理

为了能使服务器更高效地运转，要确保所购买的服务器的内部配件的性能必须合理搭配。例如，当我们购买了高性能处理器的服务器，却用低速、小容量的硬盘、小容量的内存时，就会制约系统的整体性能。一台高性能的服务器不是一件或几件设备的性能优异，而是所有部件的合理搭配。

3.3.4 服务器的技术细节

服务器的技术非常复杂，在这里只是针对一些较为简单的专用服务器的技术细节展开论述。其中，包括了硬件冗余技术、热插拔技术、双处理技术、对称多处理技术、RISC 和 CISC 处理架构技术、I2C 串行总线技术、智能输入/输出技术和智能管理技术等。

1. RISC 和 CISC 处理架构技术

所谓的 RISC，其全称 Reduced Instruction Set Computing，又称为精简指令集计算。而 CISC 的全称为 Complex Instructino Set Computer，又称复杂指令系统计算机。它们都是服务器处理器的指令系统执行方式，通常被称为服务器处理器架构技术。

RISC 指令架构技术以 IBM、HP 和 SUN 公司的 RISC 服务器为代表，而 CISC 则是以 Intel 的 IA 处理器为代表。从执行效率方面来对比，RISC 架构比 CISC 的效率高。所以，目前一般把 IBM、HP、Compaq 和 SUN 公司的 RISC 服务器称为高性能服务器，它们几乎

垄断了整个高端服务器市场，而采用 CISC 架构的服务器目前只能算中低端服务器。

为什么 RISC 架构的服务器比 CISC 架构的服务器性能要好呢？在实际测试中发觉：在 CISC 众多的指令中，只有 20%的指令使用频率达到了 80%，而其余的指令使用频率非常低。这样在一个处理器中容纳了如此多的使用频率低的指令时就会大大地降低整个处理器的处理性能。RISC 架构的处理器集合了平时使用频率非常高的指令，从而大大增强了处理器的处理性能。这也就是目前，一些大型企业的网络中，如果对于服务器要求比较高，多半是采用 IBM、HP 或者 SUN 的服务器的原因。

2. 对称多处理技术

对称多处理技术又称 Symmetrical Muti-Processing，简称 SMP 技术。在日常不是很讲究的网络系统中，为了节约成本，会使用单个处理器或者服务器集群技术来构建服务器，而这种服务器被称作非对称多处理技术。

目前，工作组级别以上的服务器绝大多数是使用 SMP 技术。当同一个服务器中的主板上提供的处理器的个数是偶数时，就会被称作是对称性。

使用对称多处理技术的原因是由于随着网络规模的发展，对于服务器的要求越来越高。单单使用单个处理器已经完全不能满足网络的要求。于是就出现了双路服务器、4 路服务器、8 路服务器、12 路服务器，甚至是 64 路服务器，这些服务器分别是指服务器具有 2 个、4 个、8 个、12 个、64 个处理器。这些处理器会平等地访问内存、I/O 和外部中断，并且系统资源会被所有的处理器共享、工作负载被均匀地分配到所有处理器上。

当然，不是随便几个处理器放在一起就可以实现 SMP 技术的。实现 SMP 技术的处理器要符合下面的要求。

- 处理器必须内置 APIC(Advanced Programmable Interrupt Controllers，即：高级可编程中断控制器)单元。这是 Intel 多处理器规范的核心，处理器之间彼此之间通过互相发送中断来完成彼此的通信，从而能够使得多个处理器能够协调地共同完成任务。
- 处理器的型号必须相同，因为只有同一个型号的处理器才会具有相同的 CPU 核心，不同型号的处理器即使都具有内置的 APIC 单元，也很难彼此之间建立协调。
- 相同的运行频率，只有相同的运行频率才可以使得系统正常启动。
- 保持相同的产品序列号，这样会更好地使得处理器之间协调运行。

在实际应用中，所有支持 RISC 的处理器都支持 SMP 技术，另外，Intel 的 Xeon MP/Nocona 等处理器也支持 SMP 技术。

3. 双处理技术

双处理技术(Dual Processor，简称 DP)支持两个处理器，在中低档服务器更多的是采用 DP 技术。

4. I2C 总线技术

I2C(Inter-Integrated Circuit，即：内部集成电路)总线技术是由菲利普公司开发的一种串行总线，是一种具有多端控制能力的双线双向串行数据总线系统。它广泛地被应用在音频、

视频电路中，如彩电就是用了这一技术，而目前，一些服务器也采用了这个技术。

通过一个带有缓冲区的接口，数据可以被 I2C 总线发送或接收，控制和状态信息则通过一套内存映射寄存器来传送。利用 I2C 总线技术可以对服务器的所有部件进行集中管理，可以随时监控内存、硬盘、网络、系统温度等多个参数，增加了系统的安全性，方便了管理。

标准的 I2C 总线的传输速度可以达到 100 Kb/s，通过 7 位地址码，能够支持 128 个设备。而加强型的 I2C 总线用了 10 位地址码，可以支持 1024 个设备，其传输速度已经达到了 400 Kb/s，最高能达到 3.4 Mb/s。I2C 总线是多主控总线，所以任何一个设备都可以像主控一样作为发送器或接收器工作。I2C 总线上每个设备都有一个独一无二的地址。正是由于 I2C 总线的出现，从而增强了服务器处理数据的能力。

5. 智能监控管理技术

智能监控技术不是一个单一的服务器技术，它是一系列智能管理技术的总称，包括了应急管理端口(EMP)、Intel 服务器管理(ISC)、智能平台管理接口(IPMI)和简单网络管理协议(SNMP)。

- EMP(Emergency Management Port)技术是服务器主板上所带的一个用于远程管理服务器的接口。远程控制机可以通过 Modem 与服务器连接，控制软件安装在控制机上。控制机通过控制软件来远程操纵服务器，例如打开、关闭、重设服务器、设置主板的 CMOS 和 BIOS 参数等。
- ISM(Intel Server Management)技术是一种网络监控技术，它只适用于使用 Intel 架构的带有集成管理功能的主板的服务器。通过这种技术，管理员可以使用一台普通的客户机通过网络远程对服务器进行启动、关闭或重新置位，同时也可以监控网络上 Intel 主板服务器的运行状况，其中包括了电源、内存、处理器，系统信息等等。
- IPMI(Intelligent Platform Management Interface)技术同样也是一种远程管理服务器的技术。
- SNMP(Simple Network Management Protocol)技术定义了一系列网络管理协议，利用它可以远程管理所有支持这种协议的网络设备，包括了监视网络状态、修改网络设备的配置和接收网络事件的警告等。

6. 智能输入/输出技术

智能输入/输出技术把任务分配给智能 I/O 系统，在这些子系统中，专用的 I/O 处理器将承担中断处理、缓冲存取以及数据传输等繁琐的任务，从而使得系统的吞吐能力得到很大的提高。

这个系统中的 I/O 子系统完全独立于网络操作系统，并不需要外部设备的支持，这样一方面减轻了操作系统的负担，另一方面也提高了 I/O 通信效率。

7. 硬件冗余技术

硬件冗余技术能够很好地保证服务器安全有效地运行，其中包括了单机容错冗余技

术、双服务器冗余技术、电源冗余技术、磁盘冗余技术、风扇冗余技术、网卡冗余技术等等。

8. 热插拔技术

热插拔技术也就是指可以在系统带电的情况下对部分设备进行插拔操作。由于有些服务器是不能关闭的，所以有了热插拔技术，就可以在系统开启的情况下，更换损坏的设备。

当然，服务器技术不仅仅是上面这些，由于本书不是专门讲述服务器的书籍，因而不再赘述。有兴趣的读者可以参阅相关的书籍。

3.4 工 作 站

工作站(work station)指的是具备强大的数据运算与图形、图像处理能力的高性能计算机，性能上的差别决定了工作站和 PC 机使用领域的不同，工作站主要面向的是专业应用领域，主要有工程设计、动画制作、科学研究、软件开发、金融管理、信息服务和模拟仿真等领域。

工作站根据软、硬件平台的不同，可分为基于 RISC(精简指令系统)架构的 UNIX 系统工作站和基于 Windows、Intel 的 PC 工作站两种。

UNIX 工作站是一种高性能的专业工作站，具有强大的处理器(以前多采用 RISC 芯片)、优化的内存、I/O(输入/输出)和图形子系统，并使用专有的处理器(Alpha、MIPS、Power 等)、内存等硬件系统，专有的 UNIX 操作系统，针对的是特定硬件平台的应用软件，彼此互不兼容。

PC 工作站是基于高性能的 X86 处理器，使用稳定的 Windows NT、Windows 2000 以及 Windows XP/Vista/7 等操作系统，采用符合专业图形标准(OpenGL)的图形系统，并使用高性能的存储、I/O(输入/输出)和网络等子系统，以满足专业软件运行的要求。以 Windows NT、Windows 2000 和 Windows XP/Vista/7 为架构的工作站采用的是标准、开放的系统平台，能最大程度地降低成本。

3.5 本 章 小 结

本章介绍了主要的网络设备和连接设备。通过本章的学习，读者应了解各种设备的主要功能和它们之间的异同之处，同时掌握一些网络中的关键设备的基本工作原理和分类，以及一些设备的选购要素，如服务器、交换机和路由器等。

3.6　思考与练习

1. 填空题

(1) 按服务器的处理器所采用的指令系统进行划分，可以把服务器分为_____、RISC 架构服务器和_____ 3 类。

(2) 光纤通信系统是以光波为载体、光导纤维为传输介质的通信方式，起主导作用的是光源、_____、_____和_____。

(3) _____是最简单的网络互联设备，主要完成物理层的功能，负责在两个节点的物理层上按位传递信息，完成信号的复制、调整和放大功能，以此来延长网络的长度。

(4) 网桥(Bridge)是数据链路层的连接设备，它根据_____地址来转发帧。

(5) 交换机在传送源和目的端口的数据包时，通常采用直通式交换、_____和 3 种数据包交换方式。

(6) 每个路由器中都存有一个路由表，路由表为路由器存储了到达网络上任一目的地所需要的一切必要信息，这些信息主要包括目的 IP 地址、_____、_____和为数据报的传输指定一个网络接口等。

2. 选择题

(1) 为了提高服务器的可靠性，可以采用多种措施。下面这些措施无助于提高服务器系统可靠性的是(　　)。

A. CPU 的冗余配置

B. 服务器系统具有多个 PCI 插槽的主板

C. 采用具有查、纠错能力的 ECC 内存

D. 采用双电源，互为备份

(2) 网络适配器(或被称之为网络接口卡)是一种连接设备，它能够使工作站、服务器、打印机或其他节点通过网络介质接收并发送数据。它只传输信号而不分析高层数据，属于 OSI 模型的(　　)层。

A. 网络　　B. 数据链路

C. 物理　　D. 传输

(3) 路由选择协议指的是那些执行路由选择算法的协议，下列各项不属于路由选择协议的是(　　)。

A. ARP　　B. RIP

C. OSPF　　D. BGP

(4) 双绞线是综合布线工程中一种最常用的传输介质，它的连接器适用的是(　　)接头。

A. RJ-11　　B. DB-25

C. RJ-45　　D. USB

3. 问答题

(1) 简述网桥的基本工作原理。

(2) 交换和路由的主要区别有哪些?

(3) 简述交换机和集线器的主要区别。

(4) 什么是智能输入/输出技术?

4. 实践题

假如读者的一位朋友是一家公司的老板，拥有员工 50 多人，并设立了 6 个部门。目前公司希望建立自己的网络系统，在公司的各部门之间形成不同的子网，同时公司又要建立共享的 Mail 和文件服务器。请读者运用本章的知识，向身边的朋友解释要实现这样的网络所需要的主要设备有哪些，如何选择合适的设备。请读者针对这些问题给你的朋友写封邮件，谈谈你的建议。

第10章　网络调测与故障排查

一个网络建成后，人们总是希望了解它的实际运行情况，如网络的最大吞吐量、延时情况等基本的网络性能指标。要实现这个目的，就需要使用到网络的测试技术。通过网络测试，不仅可以客观地评价这个网络的性能，还可以在网络出现故障时，及时地寻找到故障点。所以，网络测试是网络维护工作的一项重要内容。

本章要点：

- 网络测试内容
- 网络测试的工具
- 交换机和路由器测试技术
- 网络故障排查和排除

10.1　网络综合测试

近年来，以 TCP/IP 为核心的 Internet 取得了飞速的发展。随着网络规模的扩大、网络带宽的增加、异构性和复杂性的不断提高、网络新业务的不断出现，人们对互联网的流量特征、性能特征、可靠性和安全性特征、网络行为模型缺乏理解和精确描述的问题日益突出，严重影响到网络的科学发展和有效利用。

建立高效、稳定、安全、可靠、互操作强、可预测、可控的网络是网络研究的目标，而网络测试是获得网络行为第一手指标参数的有效手段，在测量和测试的基础上建立网络行为模型，并用模拟仿真的方法建立理论到实际的桥梁，是理解网络行为的有效途径。网络测试和网络行为分析是高性能协议设计、网络设备开发、网络规划与建设、网络管理和操作的基础，也是开发高效网络应用的基础。

10.1.1　网络测试的范围

网络测试技术的研究涵盖了网络协议测试、网络设备测试、网络系统测试、网络应用测试、网络安全测试等方面。

1. 网络协议测试

网络协议指的是计算机在网络中进行通信时必须遵守的约定，即通信协议。通信协议主要是对信息传输的速率、传输代码、代码结构、传输控制步骤、出错控制等作出规定并

制定出标准。只有运行相同的网络协议的计算机才能进行信息的沟通与交流。

协议测试是从软件测试的基础上发展而来的，它是一种功能性测试，即黑盒测试。协议测试有 3 种类型：一致性测试、互操作性测试和性能测试。一致性测试指的是通过观察具体实现在不同的环境和条件下的反应行为，来验证协议实现与相应的协议标准是否一致。一致性测试只关心协议实现呈现于外部的性能。要保证不同的协议在实际网络中能成功地进行通信，还需要检测某一协议与其他系统之间的交互过程是否正常，这就是互操作性测试。另外，还要对协议的性能进行测试，如健壮性、吞吐量等。

2. 网络设备测试

网络设备是网络组成的物质基础，设备的性能直接关系到网络的整体性能，网络的设备测试也是网络测试的一个重要组成部分。设备测试的对象是网络中的所有设备，包括路由器、交换机和服务器等设备，还包括网络的链路，如双绞线、光纤等。设备测试的内容可能因设备的不同而不同，如交换机的交换能力、背板容量等，光纤的测试则侧重于其传输性能。

3. 网络系统测试

网络系统的测试主要是对网络性能的总体测试，包括数据传输速率，链路的利用率、流量特性等。对各个网段进行利用率及错误状态分析，主要是为了分析当前网段的网络带宽利用率、冲突、广播和错误的帧情况，对网段物理层和数据链路层的健康状况进行评估。对各网段进行流量分析，可以知道各网段的网络带宽的最大占用者，以便于今后的网络管理和用户跟踪。

4. 网络应用测试

网络测试的最终目的是确保网络能够承载各种各样的业务。目前网络测试越来越重视网络应用测试，特别是在大型的网络中。例如，在宽带城域网中测试语音、数据、图像、多媒体、IP 接入和各种增值业务、智能业务流量和性能及其用户行为，建立网络应用与用户行为模型，从而验证网络对业务的承载能力。

5. 网络安全测试

网络安全性测试是目前网络测试中的一项日益被关注的重点内容。网络的安全性主要是从终端的安全性做起，然后是防火墙，目前的路由器设备普遍集成了安全功能。当网络中间的中转设备(至少要在各网络的入口设备上)具备安全能力时，安全问题才有可能得到更好的解决。安全功能的转移给测试工作带来了很多新的课题，如安全和性能之间如何平衡等。

10.1.2　网络评测指标

网络测试的目的在于全面评价网络的功能和性能。网络性能的评测需要有客观的指标，才能从量化的角度评价一个网络的性能。网络的测试指标很多，从测试内容的角度来看，网络测试的指标包括以下几个方面。

- 吞吐量：指的是网络设备处理各种尺寸的数据封包的能力。吞吐量通常有两种表达方式，一种是在网络测试点处监测到的单位时间内通过的数据包数量；第二种是在网络测试点处监测到的单位时间内通过的所有数据包的字节数量。例如，在以太网中，以太网吞吐量的最大理论值被称为线速，指的是交换机有足够的能力来全速处理各种尺寸的数据封包转发，千兆交换机产品都应达到线速。
- 时延：指的是数据包穿过一个基本段或网络段集合所需要的时间，与该包传送成功与否无关。平均传输时延指的是一个数据流中的所有数据包的传送时延的算术平均值。
- 时延变化：也称时延抖动，它是反映网络稳定性的一个重要指标。在同一条网络路径中，所有的数据包从原节点到目的节点所经历的时延并不是固定的，可能由于各种因素的影响，导致时延的变化。在 IP 数据包传送应用中，利用 IP 包时延变化范围的信息可以避免出现节点缓冲的溢出和读空; IP 包时延变化会导致 TCP 层重传定时器门限的增高，也可能导致数据包重传的时延或造成没有必要的数据包重传。
- 带宽：带宽一般分为瓶颈带宽和可用带宽两种。瓶颈带宽指的是当一条路径(通路)中没有其他背景流量时，网络能够提供的最大吞吐量。可用带宽指的是在网络路径(通路)存在背景流量的情况下，网络能够提供给某个业务的最大吞吐量。瓶颈带宽反映了路径的静态特征，而可用带宽反映了在某一段时间内链路的实际通信能力，所以，可用带宽的测量具有更重要的意义。但是，因为背景流量的出现与否和它所占用的带宽都是随机的，所以可用带宽的测量比较困难。
- 丢包率：指的是丢失的数据包与所有数据包的比值。许多因素会导致数据包在网络中传输时被丢弃，如数据包的大小和在发送数据时链路拥塞状况等。网络的丢包率，一般采用直接发送测量包来进行测量。
- 误差率：指的是错误数据包传送结果与成功数据包传送加错误数据包传送结果之和的比值。传输错误通常是由于网络物理环境造成，目前有一些技术(如校验和重传等机制)可以降低误差率。

上述是评测一个网络的主要参数指标，针对协议的不同层次，这些指标的具体含义也有差别。此外，在网络测试中，按照具体的协议层，不同的协议层测试的重点也有所不同。

- 物理层：在物理层最值得关注的是网络的连通性、物理带宽(传输介质的传输能力)、误码率等信息。
- 链路层：链路层的数据传输的单元是帧，测试的重点是帧吞吐量、帧传输时延、帧丢失率等信息。
- 网络层：网络层的数据传输单元是数据包，最值得关注的是包吞吐量、传输时延、包丢失率等。此外，在网络层上还要测试路由协议、包转发能力等指标。
- 传输层：传输层的数据传输单元主要是 TCP 和 UDP 数据报，在传输层上最值得关注的是 TCP/UDP 报文的处理能力。
- 应用层：在应用层进行的主要是网络应用测试，如 Telnet、FTP、Web 等。

10.1.3　网络测试范畴

网络测试的概念非常广泛，前面介绍了网络评测的一些指标，从网络测试的范畴角度来看，包括节点测试、链路测试、路径测试和网络测试 4 个范畴。

- 节点测试：节点测试是针对网络中的具体节点或设备所进行的测试。例如，对交换机、路由器和服务器等进行测试。节点测试关注的是网络中单点的吞吐量、延时等性能指标和协议处理能力、接口类型等功能指标，节点的性能将直接影响到网络性能。
- 链路测试：链路指的是两个直接相邻节点之间的连接，链路测试首先关注的是链路的连通性，这是最基本的能力。链路测试还要测量链路的带宽、丢包率和误码率等指标。
- 路径测试：路径指的是从原点到目的点所经过的节点和链路的集合。路径测试也要测试路径的连通性，但这里不仅指物理上的连通性，还包括逻辑上的连通性。此外，还要测试路径的带宽、延时、丢包率等性能指标，还要测量其最大的传输单元(MTU)、传输协议等功能指标。
- 网络测试：网络测试的范畴最大，它是前面 3 种测试的组合，反映的是整个网络的性能。

10.1.4　网络测试方法

网络测试的方法很多，针对不同的测试项目需要不同的测试方法，在网络测试中，需要根据实际的情况选择合适的测试方法。网络测试的方法可以概括为以下 4 种类别。

1. 从选择的网络测试点可分为入点测试和出点测试两种

测试网络时通常需要选择一个监测点，当监测点选择在网络或者链路的入口处时，称为入点测试；反之，如果测试点选择在网络的出口处，称为出点测试。但是在测试过程中，这两者并不是相互独立的，在很多测试中需要将两者结合起来才能实现。例如，要测试一条网络路径的丢包率，就要在入口处监测流入网络的数据包数量，在出口处测量实际收到的数据包数目，两者之比就是丢包率。

2. 从测试手段可分为主动测试和被动测试两种

主动测量指的是在选定的测量点上，利用测量工具有目的地主动产生测量流量，注入网络，并根据测量数据流的传送情况来分析网络的性能。被动测量指的是在链路或设备(如路由器，交换机等)上，利用测量设备对网络进行监测，而不使用产生多余流量的测量方法。

主动测量的优点是对测量过程的可控性比较高，灵活、机动，易于进行端到端的性能测量；缺点是，注入的测量流量会改变网络本身的运行情况，使得测量的结果与实际情况存在偏差，且测量流量还会增加网络负担。被动测量的优点在于理论上它不产生多余流量，不会增加网络负担；其缺点在于，被动测量基本上是基于对单个设备的监测，很难对网络

端到端的性能进行分析，并且可能实时采集的数据量过大，另外还存在用户数据泄漏等安全性和隐私问题。

主动测试和被动测试各有优缺点，因此适用的范围不同。主动测试在性能参数的测试中应用得比较广泛，被动测试主要用于流量测试。

3. 从网络测试的路径角度可以分为单程测试和环回测试两种

单程测试用于测试网络路径上源端到目的端的单向网络情况；环回测试用于测试从源端向目的端发出请求，直到目的端返回相应的双向网络情况。单程测试主要用于网络流量、吞吐量、速率等性能的测试，环回测试主要用于功能性的测试。但是，有些项目在单程测试和环回测试中都有重要的意义。如网络时延，其中，单程时延反映了网络中一个方向的延时，环回测试则反映了网络中的双向延时，但因受到网络中各种因素的影响，环回时延通常并不是单程时延的两倍。

4. 从网络测试对业务的影响情况看可以分为离线测试和在线测试两种

在线测试不影响当前网络的运行，主要用于测试网络或设备的实际性能指标；离线测试则是将网络或设备脱离当前的业务环境，测试网络规定的性能指标。离线测试通常用于测试设备或网络的理想指标。

10.1.5　网络测试工具

网络测试的方法和手段因测试的目的不同而不同，所采用的网络测试工具也各不相同。用于进行网络测试的工具很多，针对不同的测试内容，既有专门的测试工具，也有综合性的测试工具，既有专业化的测试仪器，也有免费的软件测试工具，很多系统本身还集成了简单的网络测试工具。一般来说，广义上的网络测试工具可以分为物理线缆测试仪、网络运行模拟工具、协议分析仪、专用网络测试设备、网络协议的一致性测试工具和网络应用分析测试工具等。

1. 主要的测试仪器

目前，网络测试的仪器很多，这些仪器通常是由专业测试设备厂家生产，既有主要用于网络性能测试的网络性能分析仪，如 SmartBits 2000、IXIA 1600 等；又有针对网络协议进行测试的专业网络协议分析仪，如 Agilent J6800A 网络协议分析仪等；还有针对网络系统的布线、物理连通性和故障监测的专门测试工具，如 Fluck Nettool 网络万用表等。下面简单介绍几种常用的测试仪器。

(1) Fluck Nettool 网络万用表

Fluck 公司推出的 Nettool 网络万用表将电缆测试、网络测试、PC 设置测试集成在一个手掌大小的工具中，它可以迅速验证、诊断 PC 与网络的连通性问题，判定插口的类型和以太网、电话、令牌环等接口类型，还可以检查连接脉冲、网络速度、通信方式(半双工或全双工)、电平和接收线对。同时还能迅速显示 PC 所使用的网络关键设备(如服务器、路由器和打印机等)，并检查 PC 到网络的连通设置问题(如 IP 地址、默认网关、E-mail 和 Web

服务器)，显示 PC 和网络之间不匹配的问题，识别那些浪费网络带宽的不需要的协议。此外，NetTool 万用表还可以对 PC 和网络通信的每个帧进行计数，同时监测全双工网络的健康问题(如发送的帧、利用率、广播、错误、冲突等)，连续记录所发现的 PC 和网络问题。

(2) Agilent J6800A 网络分析仪

J6800A 网络分析仪用于安装部署、维护与优化当前数据网络，适用于电信运营商的现场安装与维护、企业网络的网络管理与设备制造商研发部门的各类工程技术人员。该分析仪既支持集中式的网络故障诊断，又支持分布式网络状况监测，它涵盖了局域网、广域网、ATM、IP 电话、移动(包括 3G)、NGN 等各类应用。

J6800A 可以对速率高达 1Gb/s 接口的数据全线速率捕获、实时传送、处理、显示和存储，支持 LAN/WAN/ATM/VoIP/WCDMA/CDMA2000 等多个应用领域的测试。该仪表可以嵌插和更换各种通用测试接口，其中，包括 10/100/1000M 以太网、STM-1、E1/E3 和 V 系列接口等，由同一个控制平台实现测试控制。J6800A 支持监测分析 OSI 参考模型 7 层的 400 余种协议，其中包括协议解码、参数统计、网络节点自动发现、带宽使用方式和通信过程统计分析。支持的协议种类覆盖多种协议体系，包括以太网、FDDI、ATM、Frame Relay 等，还能够实现 3G 协议与信令的测试分析。其先进的流量发生、智能缓存捕获功能，多任务处理功能可以在流量发生的同时监测网络。

此外，J6800A 能实现集中式故障定位和分布式监测分析功能。集中式测试具备双端口测试功能，能实现 LAN-LAN、LAN-WAN、LAN-ATM 等多种组合测试；分布式测试能够同时测量网络中多个测试点的协议与网络性能状况，采集网络数据信息，排查间隙性与深层网络问题，全方位的管理与监测网络。

(3) Spirent SmartBits 2000

思博伦通信(Spirent Communications)的 SmartBits 系列数据网络测试平台提供了以太网业务所必需的测试功能，它能快速地验证以太网业务，可选择的 POS 和 ATM 接口卡还可以完成部分 SDH 和 ATM 的功能及性能测试。

SmartBits 可以用于测试设备及网络性能，如吞吐量、延迟、丢包等指标，还可以在一个端口中模拟上千、上万个网络的数量，并对它们各自的性能进行分析，测试出在不同的 QoS 下不同流量的表现。

SmartBits 测试系统可分为 2X 系列和 6X 系列两大类机箱，每个系列中又分别有机架式和便携式两种机箱。2X 系列机架式机箱有 20 个槽位，最多可以支持 20 个 10/100 Mb/s 接口；2X 系列便携式机箱有 4 个槽位，最多可以支持 4 个 10/100 Mb/s 接口；6X 系列机架式机箱有 12 个槽位，最多可以支持 96 个 10/100 Mb/s 接口；6X 系列便携式机箱有两个槽位，最多可以支持 16 个 10/100 Mb/s 接口。 SmartBits 提供了丰富的接口：包括 10 Mb/s USB 接口、10 Mb/s/100 Mb/s/1 000 Mb/s 以太网接口、E1/25M/ OC 12 ATM 接口、OC12/ OC 48/ OC 192 POS 接口和 1 G/2 GB/s Fiber Channel 接口。

SmartBits 支持不同接口类型之间的互通测试，还提供了丰富的测试软件，用户可以通过已安装测试软件的 PC 机(Windows NT/2000/XP)控制 SmartBits 设备，这种控制既可以是本地的也可以是来自远程的。

SmartBits 可以结合 Spirent 的其他软件，如 SmartWindow、Smart Applications、SmartFlow，以提供更加丰富的测试功能。

(4) IXIA 1600

IXIA 公司作为数据通信领域内网络及其设备性能测试的主要供应商，提供了支持多端口的流量发生及性能分析系统，具有业界领先的技术水平。IXIA 产品提供了极大的端口密度，支持广泛的接口类型。IXIA 1600T 支持 16 个插槽，能够同时测试 64 个 10/100Base-T 端口、32 个 1000Base-T 端口、32 个 OC3/OC12 端口、16 个 OC48 端口或 16 个 OC192 端口。IXIA 的接口模块支持 OC-3、OC-12、OC-48 和 OC-192 的 PoS 接口以及 10M、100M、1000M 和 10G 的以太网接口，此外，IXIA 采用上行和下行 FPGA 技术，在每个端口上，实现线速的流量发生和统计分析，包括时延的实时测试。利用 FPGA 技术，可通过硬件实时计算 IP、TCP 和 UDP 的 Checksum。

IXIA 提供了两种主要的图形化用户管理软件：IxExplorer 用户自定义管理软件和 Scriptmate 自动测试管理软件。其中，IxExplorer 用户自定义软件工具可以通过本地或 TCP/IP 网络对 IXIA 性能测试系统平台进行管理，并且可以编辑和控制流量的发生，进行统计及解码分析。Scriptmate 自动测试管理软件提供一系列工业化的自动性能测试软件套。提供的自动测试软件套包括：RFC2544、RFC2285、QoS 测试套、IP 多播测试套、服务器负载均衡测试套、路由能力及路由收敛测试套等。IXIA 提供了灵活的路由协议的仿真功能，可以满足广泛的测试应用需求，包括 RIP、IS-IS、MPLS RSVP-TE、OSPF 和 BGP 等。

针对智能化的网络设备(如 Web 服务器、防火墙、负载均衡系统)，IXIA 提供了 4 层至 7 层的模拟会话功能，从而可以进行 4 层到 7 层的性能测试。IXIA 的 Web 测试系统可以模拟几十万用户以及几百万用户的并发呼叫连接；模拟虚拟客户终端访问 Web 服务器的 HTML 页面；通过发出 HTTP(1.0/1.1)呼叫连接来模拟电子商务应用。

针对网络监测及优化，IXIA 也提出了相应的解决方案。为了监测 IP 网络的核心部分，IXIA 可以对骨干路由器的 metrics 进行统计，并监测网络单向的时延、包丢失率、包抖动等性能指标。为了监测 IP 网络的边缘部分，IXIA 可以监测网络环路的时延、包丢失率、路由可达性及稳定性。对于网络流量，IXIA 可以进行如网络协议分布、流量大小分布等的分析，并可用于 ISP 的网络管理，有效地区分网络设备的物理地址，因此它可用于安全分析、认证及网络管理，并且可以确认是否有 IP 新业务出现。

2. 常见测试软件

除了测试仪器外，还有很多网络测试软件可供选择，这些软件有的要结合测试仪器使用，帮助分析测试结果。有的软件是专门的网络测试软件，具有强大的测试和分析功能，如 Sniffer Portable 和 SolarWinds Toolset。

(1) Sniffer Portable

Sniffer 实际上是一种网络嗅探器，是一种监视网络数据运行的软件设备，既能用于合法的网络管理，也能用于窃取网络信息，如监视网络流量、分析数据包、监视网络资源利用、执行网络安全操作规则、鉴定分析网络数据和诊断并修复网络问题等。

Sniffer Portable 可用于网络故障与性能管理，在网络界的应用非常广泛。目前，其最新版本是 Sniffer Portable 4.8，被称为多拓扑纯软件解决方案，它使用专家分析技术管理和调试局部网段，利用全线速捕捉功能，Sniffer Portable 能分析信息包并实时报告数据，允许网络管理员迅速响应网络性能问题。如图 10-1 所示的是 Sniffer 实时分析网络中各节点间的报文信息。

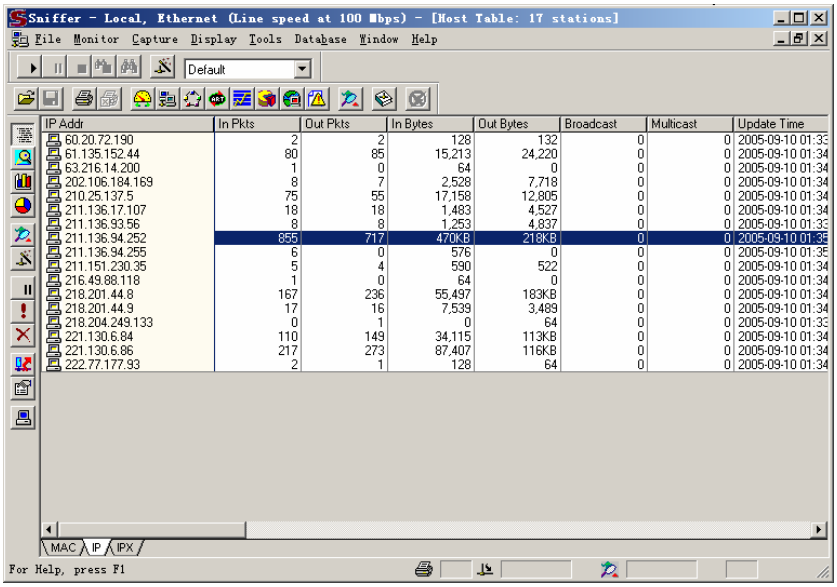

图 10-1　Sniffer 实时分析网络中各节点间的报文统计

Sniffer Portable 可以用于捕获网络中的数据包，还可以使用过滤器过滤数据包，针对捕获的数据包进行协议分析，可以实现简单的网络协议测试。如图 10-2 所示的是 Sniffer 分析数据包的各层协议。

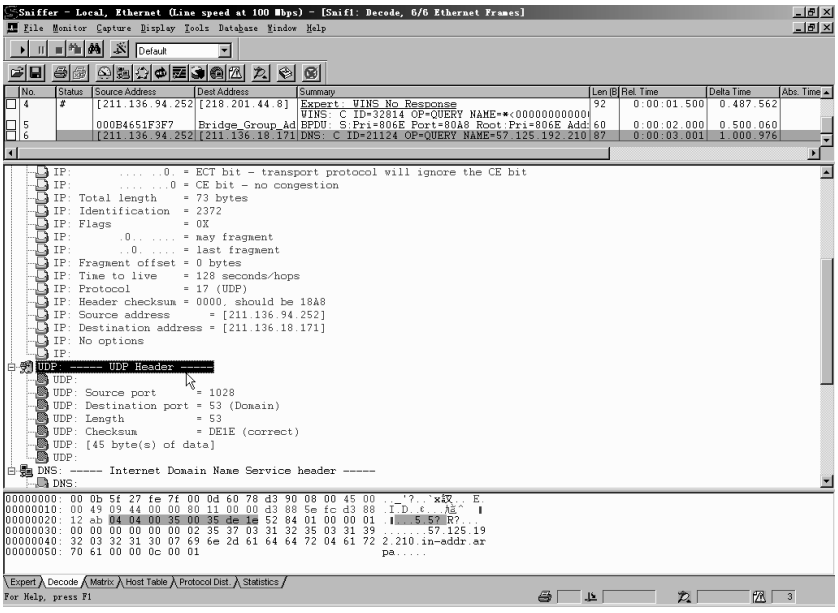

图 10-2　Sniffer 分析网络数据包协议

Sniffer Portable 软件可以在桌面机、便携式计算机或者笔记本等硬件平台上运行，并且可以利用高级自定义硬件组件确保全线速的捕获能力。Sniffer Reporter 可以生成基于 RMON1/RMON2 的图形报告，以及由 Sniffer Portable 应用程序收集的类似数据。从带宽使用率到潜在的网络衰减，Sniffer Reporter 提供了详尽数据来帮助用户规划未来的网络需求。有关以太网和令牌环的可用报告包括：主机表、矩阵、协议分发、全局统计和其他报告。

(2) SolarWinds Toolset

SolarWinds Toolset 是一套网络管理软件，包括网络发现、错误监控、性能管理等工具。SolarWinds Toolset 包括 Professional Edition、Engineer's Edition 等版本，根据版本的不同，所提供的工具库也有所不同，但基本的工具库都包括网络和错误管理软件、安全和 Cisco 路由器管理工具、MIB 浏览器等，如图 10-3 所示。网络性能监控器能够对带宽、错误、性能门限进行查询、图示和警告。

① 网络性能监控工具

SolarWinds 的网络性能监控器能够对有效性、带宽利用率、CPU 负载、内存和硬盘空间的利用情况进行监控和警告，当发生中断或达到性能门限时，它的自定义警告功能还可以向用户的数字电话发送提示信息。SNMP Graph 能够监视任何 SNMP 设备，实时界面监控器可以同时显示路由器和转换器的统计信息表，CPU Gauge 显示单个转换器、服务器或路由器的 CPU 性能，而高级 CPU Gauge 可以监控路由器的实时负载。如图 10-4 所示的是 SolarWinds 对网络带宽进行的实时监控。

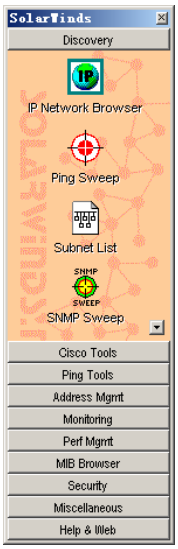

图 10-3　SolarWinds Toolset 工具库

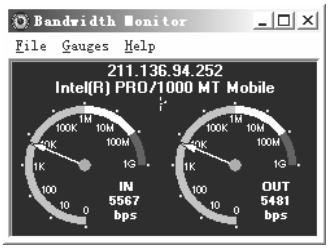

图 10-4　网络带宽实时监控

② 网络发现工具

SolarWinds 提供了业界性能最好、速度最快的发现引擎。IP 网络浏览器和网络定位是最流行的发现工具。新的 Switch Port Mapper 可以自动映射到 Layer2 和 Layer3，此外，还包括了其他发现工具，如 MAC Address Discovery、Subnet List、SNMP Sweep 和 DNS Audit。

③ Cisco 路由器工具

SolarWinds Toolset 专门为 Cisco 路由器管理设计了一个简单的图形界面。通过 Config Downloader、Config Uploader 和 Config Editor/Viewer 简化路由器的配置管理工作，还可以在远程 Cisco 路由器上对运行和启动配置进行比较。高级 CPU 负载监控器允许用户浏览路由器的实时负载。其他的工具还有：Proxy Ping、路由器密码解译、路由器安全检查、配置管理和 CPU 核查。

④ 故障监控工具

该工具是完全的交互式管理程序，允许用户监控所选择的设备，并发送中断警告。Watch It 是另一个便利的工具，该工具可以控制网络波动。除此之外，还包含有系统日志服务器(Syslog Server)。

⑤ MIB 浏览器工具

MIB 浏览器含有 220 000 个预编译的 OID(对象标志符)。通过 MIB 浏览器，查询引擎能够通过 SNMP 查询任何远程设备的软件和硬件配置，利用 MIB Walk，还可以获得 MIB 树，如图 10-5 所示。通过系统 MIB 更新和 MIB 浏览器，用户不仅能够浏览 MIB 细节，还可以进行远程更改。用户可以利用 SNMP Graph 远程图示和监控任何 MIB。

⑥ 安全和入侵工具

通过 SNMP Brute Force Attack 和 Dictionary Attack，用户可以测试自己的 Internet 安全性，利用路由器安全检查(Router Security Check)也可以验证用户 Cisco 路由器的安全性。远程 TCP Reset 可以显示设备上的所有活动会话，密码解译程序允许用户破译 Type 7 Cisco 密码。端口扫描器可以用于测试所有开放的 TCP 端口，包括整个 IP 地址和端口范围或者所选择的专门机器和端口。

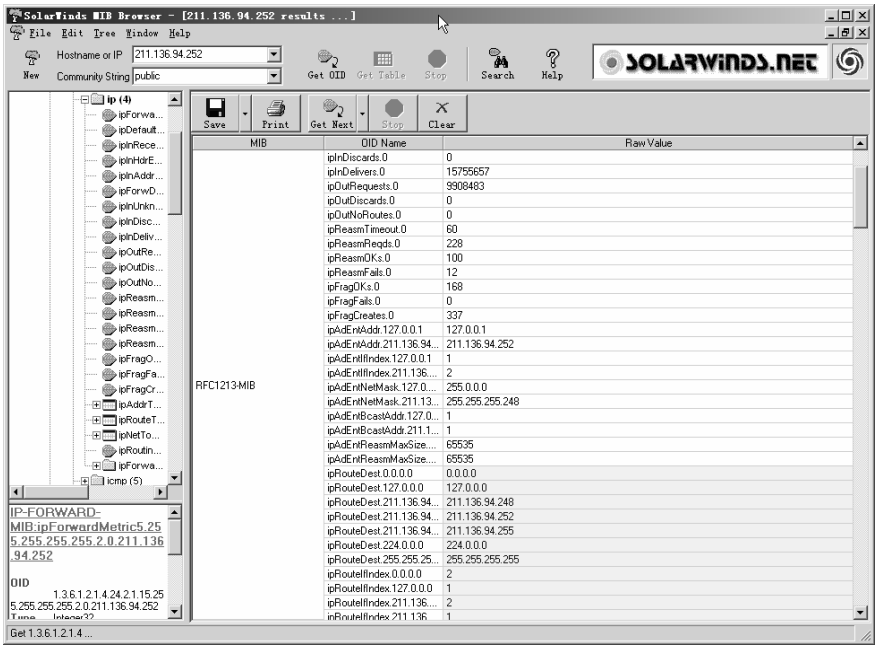

图 10-5　MIB 浏览器

⑦ SNMP trap 工具

SolarWinds 的 Trap 接收器用来接收、存储和浏览 SNMP trap，而它的 Trap 编辑器则可以用于修改网络管理工具的 SNMP trap 模板。

⑧ Ping 和诊断工具

SolarWinds Toolset 包含的许多工具可以用来管理用户网络的日常操作，它们并非是基本的标准工具，如其中的多线程工具。SolarWinds Toolset 所包括工具有：Ping、Ping Sweep、高级 Ping、跟踪路由、Proxy Ping、TFTP 服务器、WAN Killer 和 Wake-On-LAN(可以远程开、关服务器)。如图 10-6 所示的是使用 ping 工具测试到 sina 的连通性。

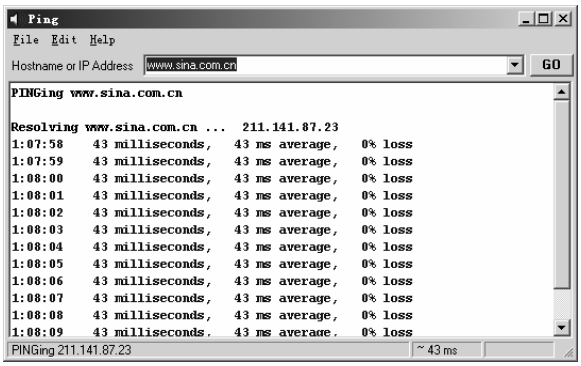

图 10-6　ping 工具

⑨ IP 地址管理工具

该工具用于管理用户的 IP 地址空间。SolarWinds 的自动发现功能可以证实用户的 IP 地址空间。所包括的工具有：IP 地址管理、DHCP 范围监控、高级子网计算器、DNS/WhoIs 解答器、DNS 分析器和 DNS 核查。

⑩ 其他工具

TFTP 服务器是唯一的多线程 TFTP 服务器，WAN Killer 对于装载和测试网络是非常有用的数据源发生器。另外，SolarWinds 还包含有一系列的免费工具，这些工具可以从网上下载。

3. 系统自带的调测工具

一些系统自带的工具可以用于简单的网络测试，如 Windows、Unix 等系统都提供了 ping、netstat、traceroute 等工具。

(1) ping

ping 命令是 Windows、Unix 系统中集成的一个专门用于 TCP/IP 协议的测试工具，用于测试网络连接状况以及信息包发送和接收状况，是网络测试中最常用的命令之一。ping 利用 ICMP 协议，向目标主机(地址)发送一个回送请求数据包，要求目标主机收到请求后给予答复，从而判断网络的响应时间和本机是否与目标主机(地址)连通。如图 10-7 所示的是使用 ping 命令测试到 sina 的连通性。如果执行 ping 不成功，则可以预测故障出现在以下几个方面：网线故障、网络适配器配置不正确和 IP 地址不正确。

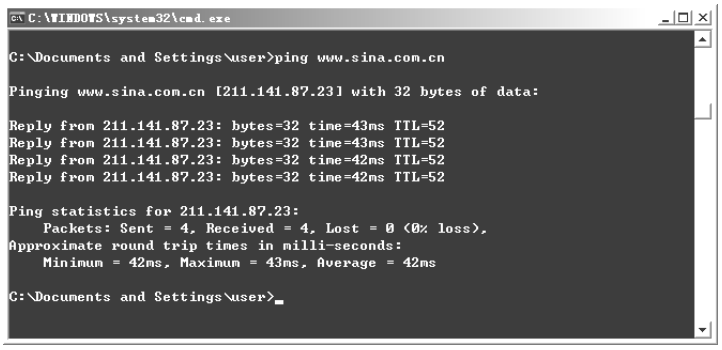

图 10-7　使用 ping 命令测试网络的连通性

此外，ping 命令有很多复杂的参数，如-t、-n、-l 等。使用这些参数可以实现复杂的测试情景。

(2) netstat

netstat 命令可以帮助网络管理员了解网络的整体使用情况。它可以显示当前处于活动状态的网络连接的详细信息。例如，显示网络连接、路由表和网络接口信息，并可以统计目前总共有哪些网络连接正在运行。如图 10-8 所示的是使用 netstat -an 命令查看系统当前活动的网络连接。

利用命令参数，命令可以显示所有协议的使用状态，这些协议包括 TCP 协议、UDP 协议和 IP 协议等，另外，还可以选择特定的协议并查看其具体信息，还能显示所有主机的端口号以及当前主机的详细路由信息。

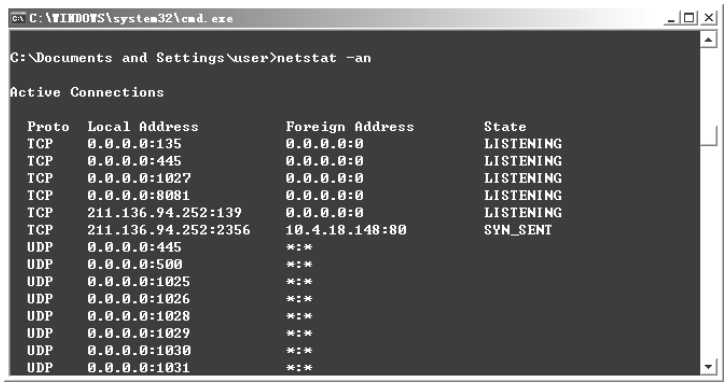

图 10-8　使用 netstat -an 查看系统当前活动的网络连接

(3) traceroute/tracert

traceroute/tracert 命令用于显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。命令功能与 ping 类似，但它所获得的信息比 ping 命令更详细，它把数据包所经过的全部路径、节点的 IP 以及花费的时间都显示出来。如图 10-9 所示的是在 Windows 命令行下使用 tracert 命令测试本机到 IETF 网站的路径。该命令比较适用于大型网络。

在 tracert 命令后面加上一些参数，还可以检测到其他更详细的信息。例如，使用参数-d，可以指定程序在跟踪主机的路径信息时，同时解析目标主机的域名。

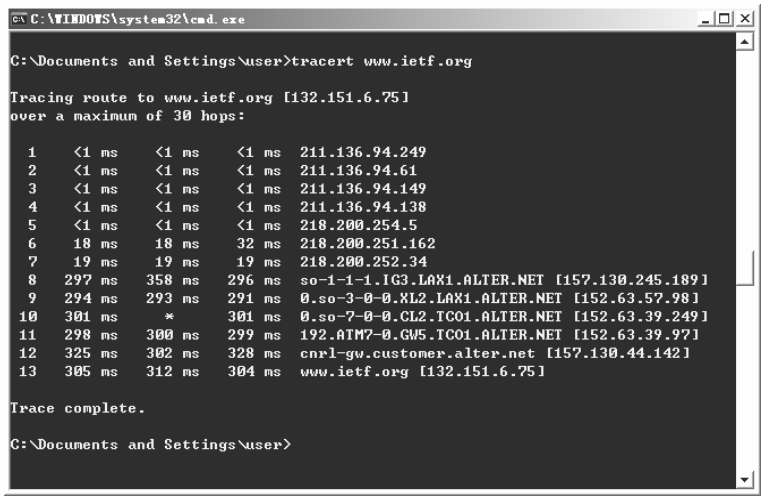

图 10-9　使用 tracert 命令测试本机到 IETF 网站的路径

10.2　交换机测试

设备测试是网络测试中非常重要的一部分，网络设备的功能和性能决定着整个网络的功能，也影响着网络的性能。网络中用于互联的设备主要有交换机和路由器。本章将分别介绍交换机和路由器的测试技术。

典型的网络设备的测试方法有两种：一种是将设备放在一个仿真的网络环境中，通过分析该产品在网络中的行为来对其进行测试；另一种方法是使用专用的网络测试设备对产品进行测试，如专用的性能分析仪器 SmartBits 2000 和 IXIA 1600 等。

10.2.1　交换机测试内容

交换机是重要的网络连接设备，随着技术的进步，交换机的性能、功能等都有了较大的进步，所采用的技术也不断发展，与之相应的测试技术也在不断地进步，其内容复杂性随之增加。从测试所关注的内容上分，交换机测试可以分为功能性测试、协议一致性测试与互操作测试、性能测试、安全性测试和异常环境测试。

功能测试主要是针对交换机的功能所进行的测试，包括管理功能测试、维护功能测试、技术功能测试等方面，还包括了组网能力的测试。广义上讲，功能测试还需要包括交换机附带的文档、帮助文档、产品标识和附件等的检查。

协议一致性测试指的是测试交换机对指定协议的遵从性，需要仪器或相关的一致性软件来完成。通常，测试仪器会将协议过程分解为若干个测试用例(Test Case)，通过执行这些测试用例与被测试交换机的交互来判断交换机对协议的遵从性。对于 2 层交换机，需要进行基于以太网协议、生成树、组播协议等的测试；对于 3 层交换机测试，需要进行如 RIP、OSPF、BGP4 等路由协议的测试，支持 IPv6 的设备还要对 IPv6 协议及 IPv6 路由协议进行

测试。经过一致性的测试后，还需要进行交换机的互通性测试，尤其是当采用了新的协议后。

交换机性能测试需要遵从一定的测试协议，包括 RFC 2544/1242、RFC 2889/2285 等。RFC 2544/1242 是针对目前互联网络设备的通行测试标准，主要包括吞吐量、延迟、丢包和背对背 4 项指标。这 4 项指标是目前交换机测试的主要指标，按照测试应用的不同，交换机测试包括 2 层交换测试、3 层交换测试、静态路由测试、动态路由测试、QoS 测试等，在这些测试中采用的指标包括吞吐量、延迟和丢包。在 RFC 2889/2285 中定义了 2 层交换机的主要测试指标，包括转发能力、拥塞控制、MAC 地址表深度、错误过滤能力、广播转发能力、广播延迟、转发压力等。对于 3 层交换机，需要测试不同路由协议的路由表容量(RIB 或 FIB)、路由转发能力(吞吐量和延迟)、路由震荡能力(丢包和震荡时间)和路由汇聚时间等。

越来越多的用户开始关心交换机的安全性，在安全性测试中，既要检查交换机是否存在管理上的安全漏洞，又要对有抗攻击能力的交换机进行如 DoS 的攻击测试。

10.2.2　交换机评测指标

交换机的评测是一个综合的度量，其中既有定量衡量标准(如吞吐量、包丢失、延迟等)，又有定性衡量标准(如安装和管理是否简单、可靠性等)。

针对交换机的性能测试有相应的标准作为依据。例如，RFC2544、RFC 2285 以及中国通信行业千兆以太网测试规范制定的 9 项测试指标，它们是吞吐量、帧丢失率、背对背、延迟、部分网状、全网状、背压、线端阻塞、错误帧过滤，基本上涵盖了用户在选择千兆以太网交换机时需要考虑的主要性能指标。

- 吞吐量：作为用户选择交换机和衡量交换机性能的最重要指标之一，吞吐量的高低决定了交换机在没有丢帧的情况下发送和接收帧的最大速率。在测试吞吐量时，需要在满负载状态下进行。该测试的配置为一对一映射。
- 帧丢失率：该测试决定交换机在持续负载状态下应该转发，但由于缺乏资源而无法转发的帧的百分比。帧丢失率可以反映交换机在过载时的性能状况，这对于反映在广播风暴等不正常状态下交换机的运行情况非常有用。
- 背对背(Back-to-Back)：该测试用于测试交换机在不丢帧的情况下能够持续转发数据帧的数量。该测试能够反映出数据缓冲区的大小。
- 延迟：该项指标能够决定数据包通过交换机的时间。延迟如果是 FIFO(First in and First Out)，即计算被测设备从收到帧的第 1 位达到输入端口开始到发出帧的第 1 位达到输出端口结束的时间间隔。计算时间间隔时，将发送速率设定为在吞吐量测试中获得的速率，并在指定的时间间隔内发送帧，在每一个特定的帧上自动设置时间标记帧。标记帧的时间标签在发送和接收时都被记录下来，二者之间的差就是延迟时间。
- 错误帧过滤：该测试项目决定了交换机能否正确地过滤某些错误类型的帧，如过小帧、超大帧、CRC 错误帧、Fragment 错误、Alignment 错误和 Dribble 错误。过小帧指的是小于 64 字节的帧。包括 16、24、32、63 字节帧。超大帧指的是大

于 1 518 字节的帧，包括 1 519、2 000、4 000、8 000 字节帧。Fragment 指的是长度小于 64 字节的帧。CRC 错误帧指的是帧校验和错误。Dribble 帧指的是在正确的 CRC 校验帧后有多余字节。交换机对于 Dribble 帧的处理通常是将其更正后转发到正确的接收端口。Alignment 结合了 CRC 错误和 Dribble 错误，指的是帧长不是整数的错误帧。

- 背压：决定交换机能否阻止将外来数据帧发送到拥塞端口，并且避免丢包。一些交换机在发送或接收缓冲区开始溢出时，通过将阻塞信号发送回源地址从而实现背压。交换机在全双工时使用 IEEE 802.3x 流控制达到同样的目的。该测试通过多个端口向一个端口发送数据来检测交换机是否支持背压。如果端口设置为半双工并加上背压，则应该检测到没有帧丢失和碰撞。如果端口设定为全双工并且设置了流控，则应该可以检测到流控帧。如果未设定背压，则发送的帧总数不等于收到的帧数。
- 线端阻塞(Head of Line Blocking，简称 HOL)：该测试决定拥塞的端口如何影响非拥塞端口的转发速率。在进行测试时，采用端口 A、B 向端口 C 发送数据形成拥塞端口，而 A 也向端口 D 发送数据形成非拥塞端口。结果将显示收到的帧数、冲突帧数和丢帧率。
- 全网状：该测试用于决定交换机在自己的所有端口都接收数据时，所能处理的总帧数。交换机的每个端口在以特定速度接收来自其他端口数据的同时，还以均匀分布的循环方式向所有的其他端口发送帧。在测试千兆骨干交换机时可以采用全网状方法获得更为苛刻的测试环境。
- 部分网状：该测试在更严格的环境下测试交换机最大的承受能力，通过从多个发送端口向多个接收端口以网状形式发送帧来进行测试。该测试方法用于千兆接入交换机测试中，其中将每个千兆端口对应 10 个百兆端口，而剩余的百兆端口实现全网状测试。

10.2.3　交换机测试工具和方法

交换机的测试工具很多，针对不同的测试需求，有不同的测试工具可供选择。例如，交换机性能的测试可以使用 SmartBits 2000；协议测试可以使用协议分析仪，如 Agilent J6800A 等。

交换机的测试既可以使用仿真环境进行测试，也可以使用专用的网络测试设备对产品进行测试。下面以一台 3 层交换机的测试为例，介绍交换机的测试方法。

选择 Spirent 公司的 SmartBits 6000B 作为测试仪器，SmartBits 6000B 可以同时插 12 个不同的模块，我们使用了 4 个 10/100Mb/s Ethernet SmartMetrics 模块、4 个 1000Base-X SmartMetrics 模块和 1 个 TeraMetrics 10/100/1000 Mb/s 以太网模块。其中，每个 10/100 Mb/s Ethernet SmartMetrics 模块有 6 个 10/100Base-TX 端口，TeraMetrics 模块有两个 10/100/1 000 Mb/s 的 RJ45 端口，1000Base-X SmartMetrics 的每个模块可接 1 个 1000Base-SX/LXGBIC。使用一台笔记本计算机作为控制台，安装测试软件 SmartWindow 7.30、Smart Applications

2.50、SmartFlow 1.50。如图 10-10 所示。

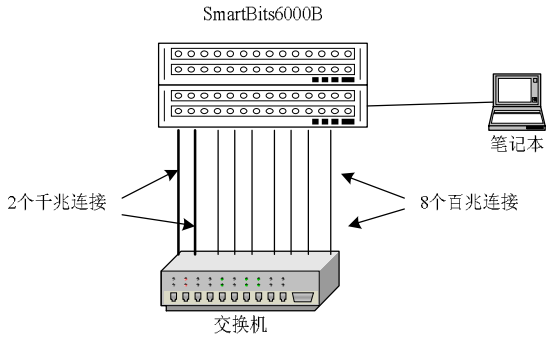

图 10-10　交换机测试示意图

本次测试主要依照 RFC2544(网络互联设备的基准测试方法)。在性能测试中，选用 64 字节、512 字节、1518 字节 3 种长度的帧。在进行 2 层交换机的吞吐量、丢包率、背对背、延迟测试时，拓扑结构为端口 1 对 1，满负载。在进行延迟测试时，分别测试了百兆端口同模块、跨模块时的延迟和千兆端口之间的延迟，测试速率在被测设备的吞吐量下。需要说明的是，对于在吞吐量的速率下测试的延迟结果为异常的交换机，可以将速率降到 90%线速来测试它的延迟。

网状测试是对交换机性能更为残酷的考验。在网状测试中，设置每个千兆端口与 10 个百兆端口作为双向传输，剩余的百兆端口用于实现全网状测试。

在 3 层交换机的性能测试时，将被测交换机的每个端口设置成一个独立的 VLAN，并分配一个独立的 IP 网段，在进行吞吐量、丢包率、延迟、B to B、网状测试时的拓扑结构测试与 2 层性能测试相同。

需要强调的是，大部分测试项目包括吞吐量、丢包率、延迟和网状测试项目的测试时间都设置成 120 s，这是为了体现出测试严谨性。在实际的测试中将测试时间设为 60 s 和 120 s 进行比较，发现在网状测试时，有的交换机在 60 s 的情况下不丢包，但在 120 s 时却丢包。这表明，120 s 的测试时间能够在更严格的情况下检验交换机的性能。在进行背对背测试时，将测试时间设置为 2 s，共测试 10 次。

路由测试也是 3 层交换机评测的重点，这项测试包括两部分：路由表容量测试和路由收敛测试。

路由表容量指的是路由表内所能容纳的路由表项数量的极限，它是交换机路由性能的重要体现，因为这意味着第 3 层交换设备能够在一个多大规模的网络中工作。在测试时，通过仪器向被测设备广播一定数量的路由表，考察被测设备是否能够收到并维持相应的路由表项。

路由收敛测试是体现 3 层交换机路由性能的一个重要部分。在测试时，给交换机灌入被测设备路由表容量的 80%左右的虚拟路由，并通过测试仪给交换机加入 90%线速的虚拟网络的传输流，在被测交换机完全收到广播的路由表并稳定一段时间后，撤销 50%的路由，待稳定一段时间后再恢复被撤销掉的路由，通过这样的一个过程考察被测交换机是否能够

及时地维护路由表，并且正确进行转发数据。

10.3　路由器测试

路由器作为计算机网络的核心设备，在网络中得到了广泛的应用。高端路由器现已由企业级设备成为公众网上重要的电信级设备。随着互联网络的逐步普及以及它在生活中的重要性的增加，路由器的性能、功能、安全性、可靠性等指标变得越来越重要。所以对路由器的测试有其重要性与必要性。

10.3.1　路由器性能技术指标

路由器的测试也有一些具体的指标作为标准，其中包括以下几个方面。

1. 路由器类型

该表项主要用于比较路由器是否是模块化结构。模块化结构的路由器的可扩展性较好，可以支持多种端口类型，如以太网接口、快速以太网接口、高速串行口等，各种类型的端口的数量一般可以选择。固定配置路由器的可扩展性较差，只用于固定类型和数量的端口。

2. 路由器配置

路由器的配置主要是指接口种类、用户可用槽数、CPU 和内存等的设置。

路由器能支持的接口种类，体现在路由器的通用性方面。常见的接口种类有：通用串行接口、10/100 Mb/s 以太网接口千兆以太网接口、ATM 接口(2 Mb/s、25 Mb/s、155 Mb/s、633 Mb/s 等)、POS 接口(155 Mb/s、622 Mb/s 等)、令牌环接口、FDDI 接口、E1/T1 接口、E3/T3 接口、ISDN 接口等。

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

通常在中低端路由器中，CPU 负责交换路由信息、路由表查找和转发数据包。在上述的路由器中，CPU 能力直接影响到路由器的吞吐量(路由表查找时间)和路由计算能力(影响网络路由收敛时间)。在高端路由器中，包转发和查表由 ASIC 芯片完成，CPU 只负责路由协议、计算路由和分发路由表。由于技术的发展，路由器中许多工作都可以由硬件来完成(专用芯片)。CPU 的性能并不能完全反映路由器的性能。路由器的性能指标包括路由器吞吐量、时延和路由计算能力等。

在路由器中可能有多种内存，如 Flash、DRAM 等。内存用来存储配置、路由器操作系统、路由协议软件等内容。在中低端路由器中，路由表可能被存储在内存中。路由器的内存越大越好(不考虑价格)。

端口密度体现了路由器制作的集成度。由于路由器的体积不同，该指标应当折合成机架内每厘米端口数。

3. 路由协议支持

路由协议的支持性指的是对 RIP/RIPv2、OSPF、IS-IS、BGP4 等路由选择协议的支持，为了支持下一代网络技术，还需要验证其对 IPv6 的支持。此外，还包括对 IEEE 802.3、IEEE 802.1Q 的支持、源地址路由支持、策略路由支持、PPP、PPPoE 的支持，以及对除 IP 以外的其他协议的支持，如 IPX、DECnet 等。

4. 对组播的支持

对组播的支持主要是对 IGMP 和 DVMRP 的支持，IGMP(Internet Group Management Protocol)是 IP 主机用来向相邻的多目路由器报告其多目组的成员。DVMRP 是基于距离矢量的组播路由协议，基本上是基于 RIP 开发。DVMRP 利用 IGMP 与邻居交换路由数据包。协议无关组播协议(PIM)PIM 是一种组播传输协议，能在现有的 IP 网上传输组播数据。

5. 路由器性能

性能指标是路由器的重要衡量指标，路由器测试规范主要阐述了下面几个主要性能指标。

(1) 全双工线速转发能力

路由器最基本且最重要的功能是数据包的转发。在同样端口速率下转发小包是对路由器包转发能力的最大考验。全双工线速转发能力指的是以最小包长(以太网 64 字节、POS 口 40 字节)和最小包间隔(符合协议规定)在路由器端口上进行双向传输且不引起丢包。

(2) 吞吐量

吞吐量指的是路由器的包转发能力。吞吐量与路由器端口的数量、端口速率、数据包长度、数据包类型、路由计算模式(分布或集中)以及测试方法有关，一般泛指处理器处理数据包的能力。吞吐量又分为设备吞吐量和端口吞吐量两种。

设备吞吐量指的是设备整机包转发能力，是设备性能的重要指标。路由器的工作是根据 IP 包头或者 MPLS 标记路由选择，所以其性能指标是每秒转发的包数量。设备吞吐量通常小于路由器所有端口的吞吐量之和。

端口吞吐量指的是端口的包转发能力，通常使用 pps(包每秒)来衡量，它是路由器在某端口上的包转发能力。通常采用两个相同速率的接口进行测试。但是测试接口可能与接口位置及关系相关。例如，同一插卡上端口间测试的吞吐量可能与不同插卡上端口间吞吐量值不同。

(3) 路由表能力

路由器通常依靠其所建立及维护的路由表来决定如何转发数据包。路由表能力指的是路由表内所能容纳路由表项数量的极限。由于 Internet 上执行 BGP 协议的路由器通常拥有数十万条路由表项，所以该项目也是路由器能力的重要体现。

(4) 背板能力

背板指的是输入与输出端口之间的物理通路，背板能力是路由器的内部实现，目前路

由器通常采用共享背板技术。背板能力体现在路由器的吞吐量上：背板能力通常大于依据吞吐量和测试包场所计算得到的值。

(5) 丢包率

丢包率指的是测试中所丢失的数据包数量占所发送的数据包数量的比率，通常在吞吐量范围内进行测试。丢包率与数据包长度以及包发送频率相关。在一些环境下可以加上路由抖动、大量路由后再进行测试。

(6) 时延

时延指的是数据包第一个比特进入路由器到最后一个比特从路由器输出的时间间隔。在测试中，通常使用测试仪表来测试从发出测试包到收到数据包的时间间隔。时延与数据包的长度相关，通常在路由器端口吞吐量范围内进行测试，超过吞吐量进行测试时，该指标没有意义。

(7) 时延抖动

时延抖动即时延变化。数据业务对时延抖动不敏感，只有当 IP 上多业务，包括语音、视频业务出现时，该指标才有测试的必要性。

(8) VPN 支持能力

通常情况下，路由器都能支持 VPN。其性能差别一般体现在所支持的 VPN 数量上。一般情况下，专用路由器所支持的 VPN 数量较多。

(9) 内部时钟精度

拥有 ATM 端口做电路仿真或者 POS 口的路由器互联通常需要同步。如果使用内部时钟则其精度会影响到误码率。

6. Qos

Qos 也是路由器测试的一项重要指标，其中包括以下内容。

(1) 队列管理机制

队列管理控制机制通常指的是路由器拥塞管理机制和队列调度算法。常见的方法有 RED、WRED、WRR、DRR、WFQ、WF2Q 等。

(2) 端口硬件队列数

通常路由器中所支持的优先级由端口硬件队列以保证。每个队列中的优先级由队列调度算法进行控制。

(3) 分类业务带宽保证

体现路由器是否能对各种业务等级作出带宽保证。该指标可以由队列调度算法等方式实现。其中，包括 RSVP、IP Diff-Serv 支持。RSVP 是资源预留协议，用于端到端路径上资源的预留。PSVP 使用软状态刷新，是一种流驱动工作方式。该协议一般不能在大规模的全国范围网络上运行。但是通常情况下路由器支持该协议，一些著名厂商将该协议用于 MPLS。IP Diff-Serv(区分服务)用于对 IP 服务质量进行分级，是对 QoS 的一种简化。

7. 网络管理

网络管理指的是网络管理员通过网络管理程序对网络上的资源进行集中化管理的操作，包括配置管理、计账管理、性能管理、差错管理和安全管理。设备所支持的网管程度体现在设备的可管理性与可维护性，通常使用 SNMPv2 协议对网络进行管理。网管粒度指的是路由器管理的精细程度，如管理到端口、到网段、到 IP 地址、到 MAC 地址等粒度。管理粒度可能会影响到路由器的转发能力。

8. 可靠性和可用性

可靠性和可用性包括设备的冗余设计，冗余包括接口冗余、插卡冗余、电源冗余、系统板冗余、时钟板冗余、设备冗余等。冗余用于保证设备的可靠性与可用性，冗余量的设计应当在设备可靠性要求和投资之间折中。路由器可以通过 VRRP 等协议来保证路由器的冗余。

此外，还包括热插拔组件，由于路由器通常要求 24h 不间断地工作，所以，更换部件不能影响到路由器的工作。部件热插拔是路由器 24h 工作的保障。

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

10.3.2　路由器测试规范

路由器测试规范主要由下面通信行业标准来进行规范：YD/T 1156-2001《路由器测试规范-高端路由器》；YD/T 1098-2001《路由器测试规范-低端路由器》。以上标准分别参照下列的标准进行制定：YD/T 1097-2001《路由器设备技术规范-高端路由器》；YD/T 1096-2001《路由器设备技术规范－低端路由器》。

低端路由器设备测试主要包括：常规测试，即电气安全性测试；环境测试，包括高低温、湿度测试和高、低温存储测试；物理接口测试，即测试低端路由器可能拥有接口的电气和物理特性；协议一致性测试，即测试协议实现的一致性；性能测试，即测试路由器的主要性能；管理测试，主要测试路由器对无大项网管功能的支持。

高端路由器测试主要包括：接口测试，即高端路由器可能拥有的接口测试；ATM 协议测试，即测试 ATM 协议要求；PPP 协议测试，即测试 PPP 协议的一致性；IP 协议测试，即测试 IP 协议的一致性；路由协议测试，即测试路由协议一致性；网管功能测试，验证测试网关功能；性能和 QoS 测试，即测试路由器性能和 QoS 能力验证；网络同步测试，即测试设备同步定时的能力；可靠性测试，即验证设备可靠性；供电测试，即测试整机功耗等内容；环境测试，包括高低温、湿度测试和高低温存储测试。

10.3.3　路由器测试的类型和方法

路由器测试一般可以分成以下几类：功能测试、性能测试、稳定性和可靠性测试、一致性测试、互操作性测试以及网络管理测试。

1. 功能测试

路由器功能通常可以划分为如下几个方面。

(1) 接口功能：该功能用于将路由器连接到网络中。可以分为局域网接口和广域网接口两种。局域网接口主要包括以太网、令牌环、令牌总线、FDDI 等网络接口；广域网接口主要包括 E1/T1、E3/T3、DS3、通用串行口等网络接口。

(2) 通信协议功能：该功能负责处理通信协议，包括 TCP/IP、PPP、X.25、帧中继等协议。

(3) 数据包转发功能：该功能主要用于按照路由表内容在各端口(包括逻辑端口)之间转发数据包并且改写链路层数据包的头信息。

(4) 路由信息维护功能：该功能负责运行路由协议，维护路由表。路由协议包括 RIP、OSPF、BGP 等协议。

(5) 管理控制功能：路由器管理控制功能包括 5 个功能：SNMP 代理功能、Telnet 服务器功能、本地管理、远端监控和 RMON 功能。管理控制通过多种不同的途径对路由器进行控制管理，并且允许记录日志。

(6) 安全功能：用于完成数据包过滤、地址转换、访问控制、数据加密、防火墙、地址分配等功能。

路由器并非必须完全实现上述功能，但是由于路由器作为网络设备，存在最小功能集，对最小功能集所规定的功能，路由器必须给予支持。因为绝大多数的功能测试可以由接口测试、性能测试、协议一致性测试和网管测试所涵盖，所以，路由器功能测试一般可以仅对其他测试无法涵盖的功能进行验证性测试。路由器功能测试一般采用远端测试法。

2. 性能测试

路由器是 IP 网络的核心设备，其性能的好坏直接影响到 IP 网网络规模、网络稳定性和网络可扩展性。由于 IETF 没有对路由器性能测试作出专门的规定，一般来说，只能按照 RFC2544 进行测试。但是，路由器区别于一般简单的网络互联设备，因此，在性能测试时还应该加上路由器特有的性能测试，如路由表容量、路由协议收敛时间等指标。路由器性能测试应当包括以下指标。

(1) 吞吐量：测试路由器包转发的能力。指的是路由器在不丢包的条件下每秒转发包的极限，一般可以采用二分法查找该极限点。

(2) 时延：测试路由器在吞吐量范围内从收到包到转发出该包的时间间隔。时延测试应当重复 20 次，然后取其平均值。

(3) 丢包率：用于测试路由器在不同负荷下丢弃包占收到包的比例。不同负荷通常指从吞吐量测试到线速(线路上传输包的最高速率)，步长一般为线速的 10%。

(4) 背靠背帧数：测试路由器在接收到以最小包间隔传输时不丢包条件下所能处理的最大包数。该测试实际上是考验路由器的缓存能力，如果路由器具备线速能力(吞吐量=接口媒体线速)，则该测试没有意义。

(5) 系统恢复时间：测试路由器在过载后恢复正常工作所需要的时间。测试方法可以

采用向路由器端口发送吞吐量 110%和线速间的较小值，持续 60s 后，将速率下降到 50%的时刻到最后一个丢包的时间范围。如果路由器具备线速能力，则该测试没有意义。

(6) 系统复位：测试路由器从软件复位或关电重启到正常工作的时间间隔。正常工作指的是能以吞吐量转发数据。

在测试上述 RFC2544 中规定的指标时应当考虑以下因素。

- 帧格式：建议按照 RFC2544 所规定的帧格式进行测试。帧长变化为从最小帧长到 MTU 顺序递增，如在以太网上采用 64、128、256、512、1 024、1 280、1 518 字节；认证接收帧用于排除收到的非测试帧，如控制帧、路由更新帧等；广播帧用于验证广播帧对路由器性能的影响，在进行上述的测试后，在测试帧中夹杂 1%广播帧时再测试；管理帧用于验证管理帧对路由器性能的影响，在进行上述的测试后，如果在测试帧中夹杂每秒一个管理帧，再重新进行测试。
- 路由更新：路由更新即下一跳端口的改变对性能的影响。
- 过滤器：在设置过滤条件下对路由器性能的影响，建议设置 25 个过滤条件测试。
- 协议地址：测试路由器收到随机处于 256 个网络中的地址时对性能的影响。
- 双向流量：测试路由器端口双向收发数据对性能的影响。
- 多端口测试：测试流量全连接分布或非全连接分布对性能的影响。
- 多协议测试：测试路由器在同时处理多种协议时对性能的影响。
- 混合包长：除了测试所建议的递增包长之外，检查混合包长对路由器性能的影响，RFC2544 除了要求包含所有测试包长之外，没有对混合包长中各个包长所占的比例进行规定。建议按照实际网络中各包长的分布测试，如在没有特殊应用要求时，以太网接口上可采用 60 字节包 50%、128 字节包 10%、256 字节包 15%、512 字节包 10%和 1 500 字节包 15%。

除上述 RFC2544 建议的测试项外，路由器还需要测试以下内容。

- 路由震荡：测试路由震荡对路由器转发能力的影响。路由震荡程度即每秒更新路由的数量，可以根据网络条件而定。路由更新协议可以采用 BGP。
- 路由表容量：测试路由表的大小。骨干网路由器通常运行 BGP，路由表包含全球的路由。一般来说要求超过 10 万条路由，建议通过采用 BGP 输入导出路由计数进行测试。
- 时钟同步：在包含相应端口(如 POS 口)的路由器上测试内钟精度和同步能力。
- 协议收敛时间：测试路由变化通知到全网所用的时间。该指标虽然与路由器单机性能有关，但是一般只能在网络上进行测试，而且会因配置的改变而变化。可以在网络配置完成后，通过检查该指标来衡量全网性能。测试时间应当根据具体项目和测试目标而定。一般认为测试时间应当介于 60~300 s 之间。

3. 一致性测试

路由器一致性测试通常采用“黑箱”方法，被测试设备 IUT 叫做“黑箱”。测试系统通过控制观察点 PCO 与被测试设备接口来进行测试。

不同的测试事件是通过不同的 PCO 来控制和观察的，按照其应答是否符合规范，即定时关系和数据匹配限制，测试的结果可分为通过、失败、无结果 3 种。路由器是一种复杂的网络互联设备，需要在各个通信层上实现多种协议。例如，相应接口的物理层和链路层协议、IP/ICMP 等互联网层协议、TCP/UDP 等传输层协议、Telnet/SNMP 等应用层协议和 RIP/OSPF/BGP 等路由协议。

协议一致性测试应当包含路由器所实现的所有协议。由于该测试内容繁多且测试复杂，在测试中，可以选择重要的协议以及所关心的内容进行测试。由于骨干网上的路由器可能影响到全球路由，所以，在路由器测试中，应特别重视路由协议一致性测试，如 OSPF 和 BGP 协议。由于一致性测试只能选择有限测试例进行测试，一般无法涵盖协议的所有内容。所以，即使已通过测试也无法保证设备能完全实现协议的所有内容，所以最好的办法是在现实环境中进行测试。路由器一致性测试一般采用分布式测试法或远端测试法。

4. 互操作测试

由于通信协议、路由协议非常复杂并且拥有众多的选项，因此，实现同一协议的路由器并不能保证互通、互操作。并且因为一致性测试的能力有限，即使可以通过协议一致性测试也未必能保证完全实现协议，所以，有必要对设备进行互操作测试。

互操作测试实际上是将一致性测试中所使用的仪表替换成需要与之互通、互操作的设备，选择一些重要且典型的互联方式进行配置，观察两台设备是否能按照预期的计划正常工作。

5. 稳定性、可靠性测试

路由器的稳定性和可靠性很难进行测试。其一般可以通过以下两种途径得到。

- 厂家通过关键部件的可靠性以及备份程度来计算出系统的可靠性。
- 用户或厂家通过大量相同产品在使用中的故障率来统计产品的稳定性和可靠性。

当然，用户也可以通过在一定时间内，对试运行结果的要求来保证路由器的可靠性与稳定性。

6. 网管测试

网管测试一般用于测试网管软件对网络和网络设备的管理能力。由于路由器是 IP 网的核心设备，所以必须测试路由器对网管的支持度。如果路由器附带有网管软件，可以通过使用所附带的网管软件来检查网管软件所实现的配置管理、安全管理、性能管理、计账管理、故障管理、拓扑管理和视图管理等功能。如果路由器不附带有网管软件，则应当测试路由器对 SNMP 协议实现的一致性和对 MIB 实现的程度。由于路由器需要实现的 MIB 非常多，每个 MIB 都包含有大量的内容，很难对 MIB 实现完全测试。一般可以通过抽测重要的 MIB 项来检查路由器对 MIB 的实现情况。

10.3.4　路由器测试

由于路由器设备非常复杂，采用的接口和协议多种多样，所以对路由器进行测试所采

用的仪表和仪表的配置，必须根据测试内容和路由器的实际配置来决定。一般来说，路由器测试所使用的仪表可以分为性能测试仪表、协议测试仪表和其他种类的仪表。

(1) 性能测试仪表主要用于测试 IP 包转发能力。最典型的有 NetCom 公司的 SmartBit、安捷伦公司的 Router Tester 等。性能测试仪表有时也要求一些协议仿真能力，如对 BGP、OSPF 的仿真。

(2) 协议测试仪表主要用于测试路由器对协议实现的一致性。主要的路由协议一致性测试仪表有安捷伦公司的 Router Tester 等。其他的协议，如 TCP/IP、ATM、ISDN、SNMP 等，可选用各种专用或通用仪表。

(3) 其他仪表主要包括一些通用仪表，如示波器、万用表、率耗器、光功率计等。在测试仪表的选择中，还应当考虑仪表的精度以及误差范围。

综上所述，路由器的测试是一项复杂且非常重要的工作，对路由器的测试，只有在研究测试方法的基础上，结合具体的测试情况，制定正确的测试方案，选择合适的测试仪表，认真地进行测试才能达到测试目的。

下面以某公司的一款路由器为例，使用 SmartBits 6000B 测试其转发性能。在测试中，使用 SmartBits 6000B 测试仪和 SmartApplication 2.50 测试软件，并用一台 PC 作为 SmartBits 6000B 的控制台。

根据网络互联设备的基准测试标准 RFC 2544，完成吞吐量、延迟、帧丢失率以及 Back to Back 测试。在测试时，将被测路由器的两个以太网端口与测试仪的相应端口连接起来，测试它在 100 Mb/s 速率下的双向全双工转发性能，如图 10-11 所示。

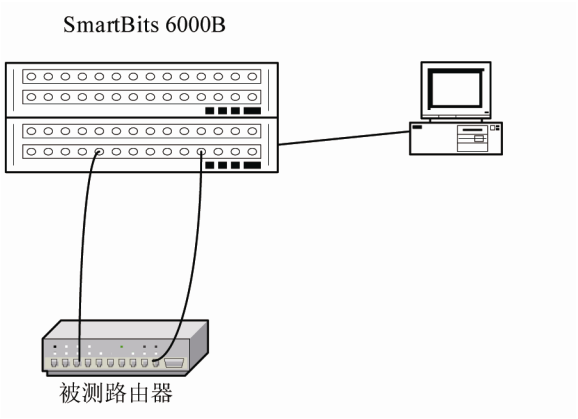

图 10-11　路由器转发性能测试示意图

为了测试该路由器的转发性能，在测试过程中，选用 64 字节、512 字节和 1518 字节 3 种帧。针对吞吐量测试，设置允许的丢包率为 0，分别以 3 种长度的数据报注入路由器，逐渐加大流量，直到出现丢包的临界，这时，测量的流量就是该路由器的最大吞吐量。

为了测试路由器的时延，设置一个统一的测试速率，在 6%、35%和 80%线速下分别测试 64、512 和 1 518 字节帧长下的延迟。测试时间设置为 120 s。

10.4　网络故障检测

网络故障往往与许多因素相关，维修人员要认真学习有关网络技术理论；掌握网络的结构设计，包括网络拓扑、设备连接、系统参数设置和软件的使用；了解网络正常运行状况，注意收集网络正常运行时的各种状态和报告输出参数；熟悉常用的诊断工具，准确地描述故障现象。

10.4.1　网络故障排查方法

网络故障诊断的目的是为了确定网络的故障点，恢复网络的正常运行；发现网络规划和配置中欠佳之处，改善和优化网络的性能；观察网络的运行状况，及时预测网络通信质量。

网络故障诊断应该从故障的现象出发，以网络诊断工具为手段获取诊断信息，确定网络故障点，查找故障的根源，排除故障，以恢复网络的正常运行。

网络故障通常有以下几种可能：物理层中的物理设备相互连接失败或者硬件及线路本身的问题；数据链路层的网络设备的接口配置问题；网络层的网络协议配置或操作错误；传输层的设备性能或通信拥塞问题；以上 3 层的网络应用程序错误。诊断网络故障的过程应该沿着 OSI 7 层模型的物理层开始向上进行。首先检查物理层，然后检查数据链路层，以此类推，设法确定通信失败的故障点，直到系统通信恢复正常为止。一般故障排除模式如下。

第一步，当分析网络故障时，首先要了解故障现象。应该详细说明故障的症结和潜在的原因。因此，要确定故障的具体现象，然后确定造成这种故障现象的原因。为了与故障现象进行对比，了解网络的正常运行状态也是非常重要的。例如，了解网络设备、网络服务、网络软件、网络资源在正常情况下的工作状态，同时还要了解网络拓扑结构、网络协议，熟悉操作系统和所使用的应用程序，这些都是在排除故障过程中不可缺少的。

第二步，收集利于帮助隔离可能故障的信息。向用户、网络管理员、管理者和其他关键人物提出和故障有关的问题。广泛地从网络管理系统、协议分析跟踪、路由器诊断命令的输出报告或软件说明书中收集有用的信息。

第三步，根据收集到的情况分析可能的故障原因，根据出错的可能性，将所有导致故障的原因逐一列举出来，并且不要忽略其中任何一个故障产生的原因。然后根据相关情况排除某些故障原因。例如，根据某些资料可以排除硬件故障，把注意力集中在软件原因上。设法减少可能的故障原因，以便于尽快策划出有效的故障诊断计划。

第四步，根据最后可能的故障原因，建立一个诊断计划。开始仅用一个最可能的故障原因进行诊断活动，这样可以容易恢复到故障的原始状态。如果同时考虑一个以上的故障原因，试图返回故障原始状态就困难得多。

第五步，执行诊断计划，认真做好每一步测试和观察，直到故障症状消失为止。每改变一个参数都要确认其结果。分析结果以确定问题是否已解决。如果故障没有得到解决，继续进行诊断与排除，直到问题解决为止。

10.4.2　网络故障分层检测方法

除了 10.4.1 节介绍的网络故障的一般排查方法之外，在分析和排查网络故障时，应充分利用网络的分层结构特点，快速准确地定位并排除故障。

TCP/IP 的层次结构为管理员分析和排查故障提供了非常好的组织方式。由于其各层相对独立，按层排查能够有效地发现和隔离故障，因而一般使用逐层分析和排查的方法。

逐层排查方式通常有两种：一种是从低层开始排查，适用于物理网络不够成熟稳定的情况，如组建新的网络、重新调整网络线缆、增加新的网络设备；另一种是从高层开始排查，适用于物理网络相对成熟稳定的情况，如硬件设备没有变动。无论使用哪种方式，最终都能达到目标，只是解决问题的效率有所差别。

具体采用哪种排查方式，可根据具体地情况来选择。例如，遇到某客户端不能访问 Web 服务的情况，如果管理员首先去检查网络的连接线缆，就显得太悲观了，除非明确知道网络线路有所变动。比较好的选择方法是直接从应用层着手，按照以下方法进行排查。首先检查客户端的 Web 浏览器是否正确配置，可以尝试使用浏览器访问另一个 Web 服务器。如果 Web 浏览器没有问题，可以在 Web 服务器上测试 Web 服务器是否正常运行。如果 Web 服务器没有问题，再测试网络的连通性。即使是 Web 服务器问题，从底层开始逐层排查也能最终解决问题，只是花费的时间太多了。如果碰巧是线路问题，从高层开始逐层排查也要浪费时间。

在实际应用中往往采用折中的方式，凡是涉及到网络通信的应用出了问题，直接从位于中间的网络层开始进行排查，首先测试网络的连通性，如果网络不能连通，再从物理层(测试线路)开始进行排查；如果网络能够连通，再从应用层(测试应用程序本身)开始进行排查。在 TCP/IP 网络中，排查网络问题的第一步通常是使用 ping 命令。如果能够成功地 ping 到远程主机，就排除了网络连接出现故障的可能性。只要成功地 ping 到远程主机，即可判断网络问题一般发生在更高层次。

每个网络层次都有相应的检测排查工具和措施，在最底层的物理层，通常采用专门的线缆测试仪，没有测试仪时可通过网络设备(网卡、交换机等)信号灯进行目测。数据链路层的问题不多，对于 TCP/IP 网络，可以使用简单的 arp 命令来检查 MAC 地址(物理地址)和 IP 地址之间的映射问题。网络层出现问题的可能性大一些，路由配置容易出现错误，可以通过 route 命令来测试路由路径是否正确，也可以使用 ping 命令来测试其连通性。协议分析器具有很强的检测和排查能力，能够分析链路层及其以上层次的数据通信，也包括传输层。至于应用层，可以使用应用程序本身进行测试。

10.4.3　常用网络命令工具

网络诊断可以使用包括局域网或广域网分析仪在内的多种工具和路由器诊断命令。除了专用的仪表外，很多系统内置命令是获取故障诊断有用信息的网络工具，如前面介绍过的 ping、netstat、tracert。本节将介绍其他几种常用的网络故障检测工具。在实际操作中，

可能需要多个命令，或者使用命令与专业仪表配合才能完成故障的检测，此时应根据特定的情况，确定需要使用的命令和工具。

1. ping

ping 命令可以测试计算机名和计算机的 IP 地址，通过向对方主机发送“网际消息控制协议(ICMP)”回响请求消息来验证与对方 TCP/IP 计算机的 IP 级连接。回响应答消息的接收情况将和往返过程的次数一起显示出来。ping 是用于检测挽留过连接性、可到达性和名称解析的疑难问题的主要的 TCP/IP 命令。ping 命令使用很简单，只要在 ping 命令后面加上所需要 ping 的地址即可。如果需要获得 ping 后的一些数据，则需要在后面添加上一些参数。要获得参数的知识，输入 ping 命令后按下回车键即可显示帮助信息。

下面将举个带参数 t 的实例，指定在中断前 ping 可以持续发送回响请求信息到目的地。要中断并显示统计信息，可按 Ctrl+Break。要中断并退出 ping，请按 Ctrl+C。效果图如图 10-12 所示。

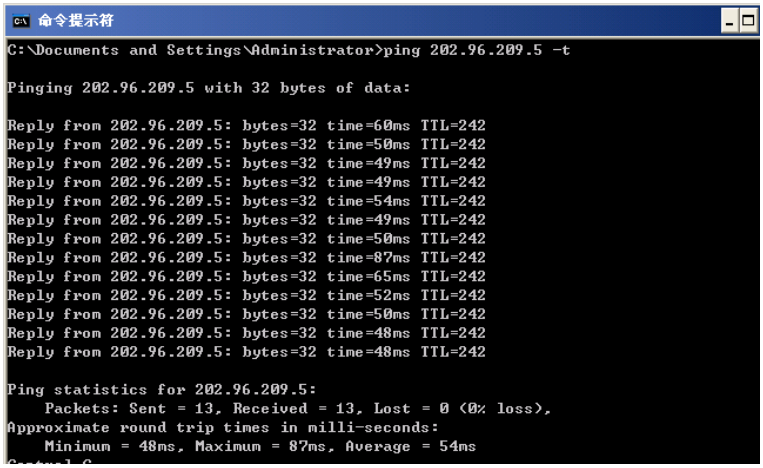

图 10-12　带参数 t 的效果图

从图 10-12 可以知道信息。首先知道从本地到 202.96.209.5 这个地址是通畅的，其次可以知道本地到这个地址的延迟平均值为 54 ms，最大值为 87 ms，最小值为 54 ms。

2. ipconfig

该命令主要是显示所有当前的 TCP/IP 网络配置。该命令在运行 DHCP 系统上的特殊用途是允许用户决定 DHCP 配置的 TCP/IP 的配置值。

它可以附带一个参数/all，这个参数就是显示所有内网和外网的网络配置情况。其效果图如图 10-13 所示。

图 10-13 中通过使用 ipconfig/all 命令将本地所有与网络相关的参数都显示出来，以方便为管理员进行网络排错。

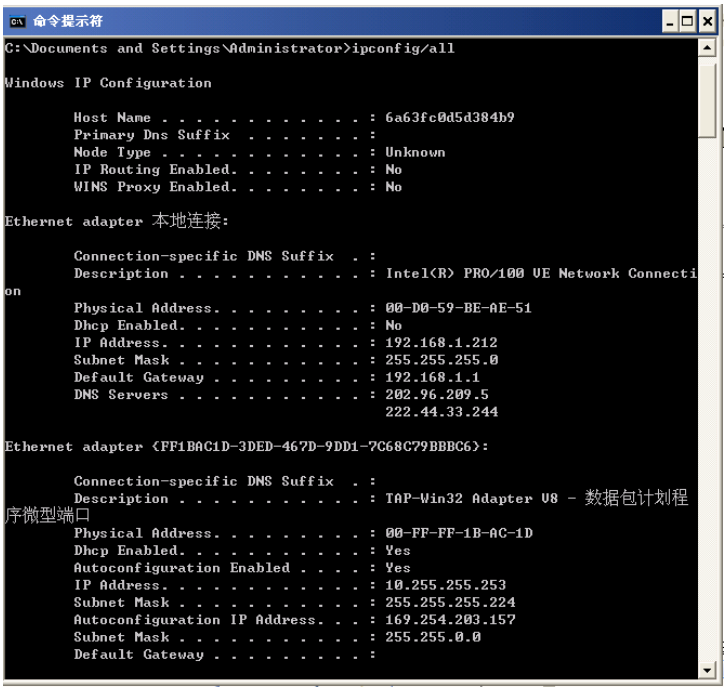

图 10-13　ipconfig 的运行效果图

3. net

net 命令有着非常强大的功能，管理着计算机的大部分管理级操作和用户级操作，包括管理本地和远程用户组数据库、管理共享资源、管理本地服务、进行网络配置等使用操作。下面将为读者详细介绍这个命令的用法。

(1) net view：该命令可以显示当前网络中的域列表和计算机列表，还可以显示用户指定的某台计算机上的共享资源状况。

- 当使用 net view\\计算机名称，会显示当前计算机中所有的共享资源。
- 当使用 net view/domain，显示当前网络中可用的域。

(2) net accounts：该命令将用户账户数据库升级并修改所有账户的密码和登录请求。该操作要在需要更改用户账户参数的计算机上进行。

- 当使用 net account/minpwdlen:NUMBER，设置用户密码长度最短不得小于 NUMBER 个字符。
- 当使用 net accounts/focelogoff:NUMBER，设置当用户账户或有效登录时间到期时在结束用户域服务器的会话前要等待的分钟数 NUMBER。
- 当使用 net accounts/minpwage:NUMBER，表示设置在用户可以更新密码前的最小天数为 NUMBER。
- 当使用 net accounts/maxpwage:NUMBER，表示设置在用户可以更新密码前的最大天数为 NUMBER。

(3) net computer：该命令是从域数据库中添加或删除计算机。

- 当使用 net computer\\计算机名称/add，表示将该计算机添加到当前域中。
- 当使用 net computer\\计算机名称/del，表示将该计算机从当前域中删除。

(4) net config：显示了正在运行的可配置服务，或者显示和更改服务设置。

(5) net pause：暂停运行中的某服务。

(6) net continue：重新激活被暂停的服务。

(7) net config server：显示服务器的当前配置。

(8) net config workstation：显示或更改服务运行时有关工作站服务的设置。

(9) net file：显示服务器上所有打开的共享文件名称以及每个文件的文件锁定码。该命令也关闭单独的共享文件并删除文件锁定。

- 当使用 net file 5 时，它指定标识号为 5 的打开文件属性。
- 当使用 net file/close 时，将关闭打开的文件并释放锁定的记录。通过共享文件的服务器键入该命令。

(10) net group：显示服务器名和服务器上组的名称。

(11) net name：添加或删除消息名称，或显示计算机将接受消息名称列表。

(12) net print：显示和控制打印队列和正在进行的打印任务。

当然，还有很多相关的其他命令，限于篇幅，不再讲述，希望读者自己能够查阅相关的资料。

4. netstat

netstat 用于显示域 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。netstat 命令有一些常用的参数，每个参数代表着不同的含义。

- netstat –s：该命令能够按照每个协议分别显示其统计数据。
- netstat –e：该命令用于显示有关以太网的统计数据。
- netstat –r：该命令可以显示有关路由表的信息。
- netstat –a：该命令显示一个所有的有效连接信息列表。
- netstat –n：该命令显示所有已建立的有效连接。

下面给出一个带参数 n 的效果图，如图 10-14 所示。

```
C:\Documents and Settings\Administrator>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1097         127.0.0.1:1110         CLOSE_WAIT
  TCP    127.0.0.1:1098         127.0.0.1:1110         CLOSE_WAIT
```

图 10-14　带参数 n 的 netstat 命令效果图

从图 10-14 中可以看出，本地的有效连接为本地连接，因为它没有连接任何网络所以没有其他的以太网连接。

5. nbtstat

nbtstat 命令主要用于显示本地计算机和远程计算机的基于 TCP/IP 协议的 netbios 统计

资料、netbios 名称表和 netbios 名称缓存。它可以刷新 netbios 名称缓存和注册 WINS 服务名称。此命令也拥有很多参数，如下所示。

- -a remotename：显示远程计算机的 netbios 名称表，其中 remtename 是远程计算机 netbios 名称。
- -A ipaddress：显示远程计算机的 netbios 名称表，其名称由远程计算机的 IP 地址指定。
- -c：显示 netbios 名称缓存内容、netbios 名称表及其解析的各个地址。
- -n：显示本地计算机的 netbios 名称表。
- -r：显示 netbios 名称解析统计资料。
- -R：清除 netbios 名称缓存的内容并从 Lmhosts 文件中重新加载带有#PRE 标记的项目。
- -RR：重新释放并刷新通过 WINS 注册的本地计算机的 Netbios 名称。
- -S：显示 netbios 客户和服务器会话，只通过 IP 地址列出远程计算机。
- -s：显示 netbios 客户和服务器会话，并试图将目的 IP 地址转换为名称。

6. nslookup

nslookup 是对 DNS 的故障进行排错的一个强大工具，nslookup 最简单的用法就是查询与域名对应的 IP 地址，包括 A 记录和 CNAME 记录，如图 10-15 所示。nslookup 命令会采用先反向解释获得使用的 DNS 服务器的名称。

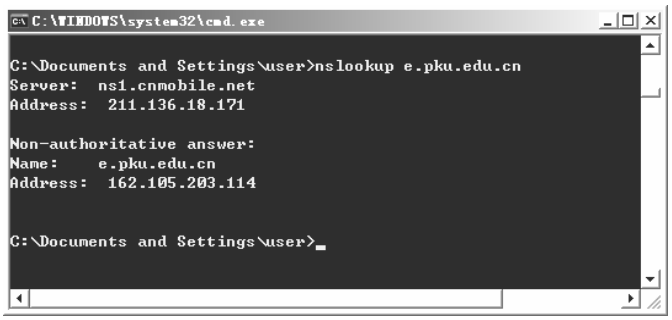

图 10-15　使用 nslookup 测试 DNS

如果查到的是 CNAME 记录，系统还会返回别名记录的设置情况。此外，nslookup 使用参数可以进行反向查询、MAIL 域查询、IPv6 地址查询等。

7. traceroute

互联网遍布全球几万个局域网和数百万的计算机，如果要想知道从本地到某个地址中间需要经过哪些局域网和服务器主机的话，那么就可以使用 traceroute 命令。

通过使用 traceroute 可以知道信息从本地计算机到互联网的另一端的主机究竟是如何路由的，走的是什么路径。在 Windows 系统中则是使用 tracert 命令。这个命令使用的方法也很简单，只需要在命令后添加一个远端主机的名称或者 IP 地址即可。下面将给出一个从本地到 www.yahoo.com 这个地址的 tracert 结果，如图 10-16 所示。

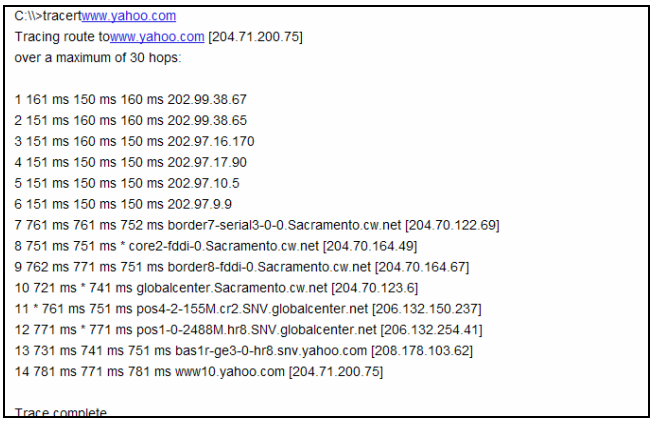

图 10-16　从本地到 www.yahoo.com 的 trace 结果

8. arp

arp 是一个重要的 TCP/IP 协议，用于确定对应 IP 地址的网卡物理地址。使用 arp 命令，可以查看本地计算机或另一台计算机的 arp 高速缓存中的当前内容，如图 10-17 所示。按照默认设置，arp 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，arp 便会自动添加该项目。一旦高速缓存的项目被输入，它们就已经开始走向失效状态。

此外，使用 arp 命令，也可以用人工方式输入静态的网卡物理/IP 地址对，用户使用这种方式对默认网关和本地服务器等常用主机进行操作，有助于减少网络上的信息量。

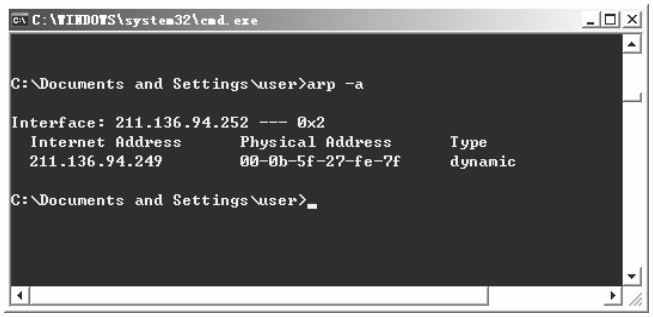

图 10-17　arp 命令查看本机高速缓存

9. route

route 命令主要是用来管理本机路由表，可以查看、添加、修改或者删除路由表条目。该命令在 Windows 2000 以上的系统都可以使用。该命令的命令格式如下所示：

route [-f][-p][command][destination][Mask netmask][gateway][METRIC metric][interface]

下面将详细给出这些参数的解释。

- Command：可以是列出当前列路由表(print)、删除路由表(delete)或者添加路由表(add)和修改路由表(change)。

- -f：清空所有路由表的网关条目。
- -p：这个选项与 add 一起使用，用于添加永久的静态路由表条目。如果没有这个参数，则重启电脑时，该添加的路由表条目会消失。
- destination、gateway、netmask、metric 和 interface 分别表示路由表中的目标 IP 地址段、网关地址、子网掩码、度量值和网络接口。

下面给出一个此命令的实例，如下所示：

```
Route add 192.168.0.0 MASK 255.255.0.0 10.10.10.1 METRIC 3 IF 2
```

此命令的含义是：添加到达 IP 为 192.168.0.0、掩码为 255.255.0.0 的目标网络的路由，指定网关为 10.10.10.1，跳数定义为 3，使用网络界面 2。

10.4.4　常见网络故障的表现和分析

在现实的网络中，所出现的网络故障各种各样，既可能是硬件故障，也可能是软件故障；既可能是协议错误，也可能是应用问题。以下介绍几个常见的例子，结合前面介绍的网络故障排查方法，给出网络故障检测的一些思路。

1. 连接故障的表现和分析

网络连接故障是网络故障发生后首先需要考虑的原因。连接性的故障一般涉及到卡、跳线、信息插座、网线、集线器、调制解调器等设备和通信介质。然而，网络的硬件设备发生损坏，都会导致网络连接中断。连通性通常可以使用软件和硬件工具进行测试验证。

例如，当一台计算机不能打开网页时，首先要考虑的是网络的连通性。首先可以使用前面介绍的 ping 命令来测试与网络中其他计算机的连通性。如果能 ping 得通的话，说明连通性没有问题，如果 ping 不通的话，就要考虑以下两个方面：第一个方面是对方的计算机是否打开，第二个方面就是两台计算机与网络设备是否连接成功。通过这种方法，可以判断网络连接性的故障是否存在。

一般来说，连通性的故障有以下几种情况。

- 计算机无法登录服务器。
- 计算机无法通过局域网接入 Internet。
- 计算机“网上邻居”中只能看到自己，而看不到其他计算机，从而无法使用其他计算机上的共享资源。
- 计算机无法在网络内实现访问其他计算机上的资源的操作。
- 网络中的部分计算机运行速度异常的缓慢。

而导致以上连通性的原因主要有以下原因，如下所示。

- 网卡未安装，或未安装正确，或与其他设备有冲突。
- 网卡硬件故障。
- 网络协议未安装，或设置不正确。
- 网线、跳线或信息插座故障。

- 集线器电源未打开，集线器硬件故障或端口硬件故障。
- UPS 电源故障。

可以针对上面的原因进行排错和解决故障。

2. 软件配置故障的表现和分析

网络故障除了连通性故障外，还存在着软件配置故障。软件配置故障一般来说有以下几种。

- 服务安装问题：局域网中，最重要的服务是“Windows 系统中共享文件和打印机”，当网络无法共享时，要首先检查此服务是否被选中。
- 网络标识问题：Windows 对等网和带有 Windows　NT 域的网络中，如果不正确设置用户计算机的网络标识，也会造成不能访问网络资源的问题。
- 网络应用中的问题：有关应用中的问题，如路由的设置，会导致网络无法使用或者无法迅速的响应。

管理员可以针对以上几种情况，进行逐一排查。

3. 网络协议故障的表现和分析

网络协议配置问题：协议作为计算机之间通信的“语言”，如果没有所需的协议、协议绑定不正确、协议的具体设置不正确，同样会发生网络故障。通常一般出现的协议配置问题的是 TCP/IP 协议，协议配置包括了 IP 地址的设置是否冲突、DNS 服务器设置是否正确、网关设置是否正确以及子网掩码设置是否正确。

4. 网卡常见故障及处理

局域网中网络不通的现象是比较多的。一旦遇到类似问题，应该认真检查各连入设备的网卡设置是否正常。可检查有无中断号及 I/O 地址冲突(最好将各台机器的中断设为相同)。当网络适配器的属性中出现“该设备运转正常”，并且在“网络邻居”中能找到自己，说明网卡的配置是正确的。否则，说明网卡出现故障，应该针对设置来重新设置网卡的相关参数。

以上介绍的是网卡的软件设置，但是有的时候所有的参数都设置正确，这时就应该考虑是否是网卡硬件出现了故障。网卡的硬件故障可以从网卡上的灯的显示情况来判断。

5. 交换机常见故障及处理

交换机故障总共分为以下几种。

- 电路板损坏。此种故障唯一的解决办法就是更换电路板。
- 连接电缆和配线架跳线问题：连接电缆和配线架的跳线是用来连接模块、机架和设备用的，如果这些连接电缆内的缆心或跳线发生短路、断路或虚接的话，会形成通信系统故障。唯一能够解决的方法是使用测试仪测试跳线的连通性和交换机模块的可用性。
- 程序缺陷：交换机中的软件程序设计存在的缺陷，此时唯一的解决办法是重新刷 BOIS。
- 设备的电源问题：这种情况将会导致交换机交换机无法正常的工作。

- 当遇到交换机故障时，首先要检测是否是以上的原因之一，如果是的话则考虑让厂家上门维修，或者更换交换机。

6. 总结

以上讲述了网络故障的一般发生的几种情况，其实，现实网络中的故障是五花八门，可能是几种情况的综合表现。所以说，要想能够真正的解决好网络故障，关键就是长期的故障解决经验。希望读者能够根据以上所说的内容为基础，在实际维护工作中不断的总结经验教训。

10.5　本 章 小 结

本章主要介绍了网络测试和调试的技术。首先介绍了网络评测的技术指标，网络测试的常用工具和方法。然后介绍了交换机和路由器测试的基本技术和测试方法。通过本章的学习，用户需要掌握网络测试的基本技术，同时还要掌握网络故障的监测和排查技术。

10.6　思考与练习

1. 填空题

(1) 网络协议测试包括 3 种类型测试的是：_____、_____和_____。

(2) 瓶颈带宽指的是_____。

(3) 路由器测试一般可以分成以下几类：_____、_____、稳定性可靠性测试、_____、_____和网管测试。

(4) 网络测试从所选择的网络测试点可分为：_____和_____。

2. 选择题

(1) (　　)指的是标志网络设备处理各种尺寸的数据封包的能力的指标。

A. 吞吐量　　B. 带宽

C. 时延　　D. 丢包率

(2) 针对网络协议的测试可以使用专业的网络协议分析仪，如(　　)。

A. SmartBits 2000　　B. IXIA 1600

C. Agilent J6800A　　D. Fluck Nettool

(3) 可以用来显示数据包到达目标主机所经过的路径的命令是(　　)。

A. Ipconfig　　B. Tracert

C. Netstat　　D. Nslookup

(4) 交换机背对背测试的主要目的在于(　　)。

A. 测试交换机在没有丢帧的情况下发送和接收帧的最大速率

B. 测试数据包通过交换机的时间

C. 测试交换机最大的承受能力

D. 考量交换机在不丢帧的情况下能够持续转发数据帧的数量

3. 问答题

(1) 根据本章的内容，阐述 3 层交换机测试的主要指标和这些指标的意义。

(2) 描述路由器性能测试的主要方法。

(3) 简答网络故障分层检测的方法。

4. 实践题

假设现在在公司里网络发生了故障导致无法上网，读者作为一名网管，应该如何排除故障。