



Cisco 专业技术丛书



Cisco

初学者

指南

Cisco: a Beginner's Guide

(美) Tom Shaughnessy Toby J. Velte 著

孙义 马莉波 张亮 等译



机械工业出版社
China Machine Press



McGraw-Hill

Cisco 专业技术丛书

Cisco初学者指南

(美) Tom Shaughnessy 著
Toby J. Velte

孙 义 马莉波 张 亮 等译



机械工业出版社
China Machine Press

本书讲述了网络基础, Cisco认证, 路由器概念和配置, 交换机和集线器, Internet接入产品, 路由协议, 网络管理, Cisco安全性, 建造Cisco网络以及Cisco网络故障处理等知识。全书内容翔实, 实例丰富。对Cisco认证感兴趣的读者, 可以通过阅读本书了解Cisco专业技术背景、概念、术语和技术。

本书是为Internet网络互连的初学者设计的。本书适合有兴趣学习网络知识的专业人士、计算机行业中网络互连知识薄弱的经理们、计算机软件人员甚至普通大众。

Tom Shaughnessy, Toby J. Velte· Cisco: a Beginner's Guide (0-07-212115-7).

Original edition copyright © 2000 by McGraw-Hill. All rights reserved

Chinese edition copyright © 2001 by China Machine Press. All rights reserved

本书中文简体字版由美国麦格劳-希尔公司授权机械工业出版社独家出版。未经出版者书面许可, 不得以任何方式复制或抄袭本书内容。

版权所有, 侵权必究。

本书版权登记号: 图字: 01-2000-1721

图书在版编目 (CIP) 数据

Cisco 初学者指南 / (美) 邵内斯 (Shaughnessy, T), (美) 威尔特 (Velte, T J) 著; 孙义等译. -北京: 机械工业出版社, 2001 4

(Cisco 专业技术丛书)

书名原文: Cisco. a Beginner's Guide

ISBN 7-111-08779-8

I C… II ①邵… ②威… ③孙… III 计算机网络-基本知识 IV. TP393

中国版本图书馆CIP数据核字 (2001) 第13546号

机械工业出版社 (北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑: 魏立康 徐江红

北京市密云县印刷厂印刷 · 新华书店北京发行所发行

2001年4月第1版第1次印刷

787mm × 1092mm 1/16 · 25.75 印张

印数: 0 001-5 000 册

定价: 40.00 元

凡购本书, 如有倒页、脱页、缺页, 由本社发行部调换

前言

在公司的一次紧急会议上，大家正面临这样一个事实：电子商务项目已经延期，而且超过了预算，并面临着性能等问题。在走进会议室时，VP环顾了一下四周，看到所有与会人员都到齐了，正在焦急地等待着他。

已经花费将近200万美元了，VP想，而且委员会要求仔细认真考虑是否要取消这个项目。他被派来查明什么地方出了差错，以及如何进行弥补。“好”，他边拿开会议桌前的椅子边说，“我正在取消日程的限制。我想知道这个项目的的主要问题是什么，导致问题的原因是什么，解决问题要花多少时间和经费。”他转向CIO和网络经理，接着说，“我们都知道这个项目是我们公司战略的中心，去年没有哪个项目能比它更具有优越性，比它消耗资源更多。然而，我们的两个主要竞争对手已经成功地完成了他们的Web站点，并且更新了商业-商业电子商务。而我们的项目却没有结果。我要提醒你们的是，这不只是另一个小的部门应用，委员会希望Internet变成我们的商业重点。我们的对手已经将商品价格削减了15%以上，上一个季度我们已经丧失了5%的市场份额。我们对已完成了一半、速度很慢的网络并不感到兴奋，更不用提已经超过了预算，但这个周末的安全保障这一块也许是我们最后的机遇。这个项目到底怎么了？”

CIO开始抱怨承包方没有遵照他所需要的三级分层设计，还抱怨后台通道和链妨碍了性能。顾问团反驳说如果当时公司留下他们参加这个项目，那么应用他们严格的管理方法论后，管理事物将会得到更好的控制。一位Web编程小组的成员讽刺地指出，基于上下文的访问控制算法是“每次隐含的拒绝规则碰撞底部都吐回代码”。另一位抱怨道，被选择用于VPN的号称强有力的密码系统正在使用一个过度紧张的DES密钥。顾问们争论说，记录RMON的那些状态可能占用了太多的带有MIB集合的CPU时钟，而且不管怎么样，NMS都比SNMP更胜一筹。网络经理这时发表异议，指出只有当“主升级”被最后送往不同LAN交换机的主干网上的闸口时，最初的EtherChannel线速基准才能被获得，尤其是反馈ATM LANE适配器的那些基准，因为它们在内网内妨碍了广播。当然，现在他们都一致同意在“big honker” Cisco 7500 上的路由分配处理器模型配置是非常欠缺的，但那还不是设计阶段“路由还是交换”大争论中的问题。事实是，如果主干网执行了PIM稀疏模式，则所有的事情都将无所顾虑，但是多点传送使网络应接不暇，这是因为有太多未知的群，尤其是穿过IGX交换的群。没有那些嗡嗡直叫的群，QoS——尤其对于通信量定型和CAR——就没有在夏天出现雪崩的机会，至少不会没有严重的、最后生成给多层交换的一个约定，这个多层交换就像已被推荐的那样。特别是在访问层给出了全部的子网掩码、DHCP和DNS进行处理的情况。顾问们请求不要同意，指出传播延时正引起环路，尤其是在RIP域中，这些环路是他们明确推荐予以反对的。IGRP是较好的选择，或者EIGRP更好一些，而且不论怎样，一旦路由矩阵被正确地调整好，RIP与IGRP比较起来将落到一边。然后陷阱最终被设置成在带宽外操作的警报状态，释放队列将CBAC和ASA算法拧在一起，来确保上周末安全措施崩溃不会复制本身。

VP觉得他的胃很不舒服，如坠云雾之中，四周是太多的告警。意识到VP越来越不舒服，顾问们的头头未加思索，脱口提出要将全职干项目的九个人的薪水由160美元/小时减到150美元/小时。没想到VP最后说了下面一段话：“我必须告诉你们，在我的一生中从未听过这么多公牛在讲话。我已经在数据处理领域干了20多年，但是我没弄清今天会上所说的任何一件事情。更让我头疼的是，你们这些搞网络的人都不会说通俗的英语。这个项目进了死循环，我已经找到问题的所在。现在让我们休会，午饭后再聚在一起。”

会议室的后面坐着两个年轻的小伙子，他们参加会议的目的是准备对他们所收集的网络性能统计资料进行说明解释。他们也没弄明白会上都说了些什么，没说一句话，最后他们俩却不由地相互看了看，同为一个想法而吃惊：每小时160美元？

本书的读者对象

本书是为那些网络互连的初学者设计的。它覆盖了Internet技术基础结构的全部内容。你桌面上的所有软件——Web浏览器、FTP 软件或者ICQ消息器——只不过是冰山的一角。在过去的30年中，一支日渐壮大的队伍，包括致力于计算机事业的科学家、通信工程师和程序员，正忙于设计和构造一个全球性的基础结构，这个结构有点像商业和文化的革命。就像在上面的会议情景中看到的那样，网络互连技术呈现出它自身是一种语言——这种语言甚至与被计算机工业普遍使用的语言都不相干。

本书适用于有兴趣学习网络知识的专业人士、计算机行业中网络互连知识薄弱的经理们（有90%或更多的这样的经理）、计算机平台和软件人员，甚至于那些略懂点技术的普通大众们。

本书还适用于那些对Internet和网络互连、而不仅仅是对Cisco感兴趣的人们。在专门钻研Cisco之前，一般必须先了解技术基础。书中全部以Cisco为例，这是因为Cisco公司在该行业拥有最大和最广泛的产品系列，而且，直率地说，他们是目前为止这个领域中最大、最重要的玩家。

那些对Cisco认证感兴趣的人们，可以先阅读本书了解行业背景、概念、术语和技术，然后继续阅读测试预备方面的书籍，来明确CCNA测试。当然，本书的出版商也出版了最好的CCNA测试预备书籍《CCNA Cisco Certified Network Associate Study Guide》，作者Syngress Media公司（Osborne/McGraw-Hill，1998）。

本书主要内容

第1章，“Cisco 与Internet”——Internet代表了历史上最大和最迅速的经济变革，迟早它将深刻地影响我们的整个生活。本章将把Internet作为一种现象纵览，而且要专门讲述Cisco公司和他的IOS操作软件是如何在计算机工业精英中取得一席之地的，是如何与微软、Intel 和IBM并驾齐驱的。本章概述了网络互连行业，解释说明了Cisco的产品系列是如何与行业环境相适应的。

第2章，“网络基础”——现代网络互连是众多复杂技术的顶峰。本章讲解了来自线缆上的东西，从线缆上传输的最基本的比特和字节讲起。讲述了主要的LAN技术，如以太网和令牌环，并透彻地解释了它们的区别，包括如ATM和千兆以太网这样的高速骨干技术。本章还讲述了七

层开放系统互连（OSI）参考模型，包括TCP/IP协议组的内部工作——被用于运行Internet的软件。本章还将介绍面向连接和无连接网络之间的区别，以及域名是如何被翻译成数字IP地址的。还详细讲述了IP寻址和子网掩码的重要网络基础，概述了拨号技术，如DSL和ISDN，WAN干线技术，如T1、T3、帧中继和ATM。

第3章，“Cisco认证”——与微软和Novell一样，Cisco也向使用他们产品的技术人员提供了齐备的认证程序。本章详述了三条途径——路由&交换、WAN交换和ISP拨号，指明了用于设计的新Cisco认证是如何不同于已用在网络支持上的认证。对适用于每一个认证的测试对象都进行了完全的解释。任何对从事网络互连工作有兴趣的人，或者面临重新招聘和管理Cisco保障人员的人，本章是必读的。

第4章，“路由器概览”——本章着重于Cisco路由器的基础知识。本章覆盖了整个路由器的硬件组成，从印刷电路板直到CPU。还讲述了网络管理员如何注册进入Cisco路由器对这些硬件进行操作，甚至连重新启动计算机执行口令的恢复这样基本的操作都予以了说明。本章也涉及了Cisco路由器中的主要软件组成，包括Cisco IOS命令接口和特性设置。还回顾了Cisco路由器的产品系列，包括如何选择最佳的路由器来解决特殊网络问题的一些小技巧。

第5章，“路由器的配置”——现在是研究更高级部分的时候了，尤其是配置文件。本章探究了Cisco IOS操作模式、命令层次、实用性和如何使用IOS帮助子系统。但是重点放在重要的配置文件上，以及如何使用它们设置Cisco路由器和配置网络。阅读本章可以帮助读者了解基本的Cisco路由器命令、命令句法、如何读设备状态以及如何配置关键的路由器参数。此外，还回顾了Cisco的ConfigMaker和FastStep配置软件工具。

第6章，“交换机和集线器”——PC访问互连网络的地方被称为访问层。本章讲述了网络互连技术基础、线缆规范、带宽，以及怎样区别冲突和广播区域、集线器和访问交换。透过当今行业上最重要的主题之一——是设计路由的网络还是交换的网络，讲述了高端LAN骨干交换。从更多的技术方面介绍了交换网络，包括交换协议、虚拟LAN（VLAN）和多层交换。对Cisco的集线器和交换机产品系列也做了简介。

第7章，“Internet接入产品”——现有三种技术，通过它们可以访问互连网络，即防火墙、访问服务器和虚拟专用网络（VPN）。本章讲解了每一种技术，尤其是防火墙技术。还说明了访问列表，还有适应的防火墙安全算法，及在分组级处于互连网络中心的技术。Cisco销售两种防火墙产品：Cisco PIX Firewall硬件/软件和IOS Firewall软件特性设置，本章对这两种产品都予以详细地说明。涉及了VPN——未来的广域网（WAN）。此外，还涉及到访问服务器是如何工作的以及它们所起的作用。更进一步地，对Cisco访问服务器产品做了介绍。

第8章，“路由协议”——庞大的互连网络，如果没有路由协议将是无法想象的。本章涉及了任何互连网络都面临的基本问题，以及路由协议是如何被用来与移动传输模型、出现的问题和拓扑变化相适应。讲述了基本的路由协议技术，它们是当今使用的不同的主要路由协议，既有开放的标准协议（RIP、OSPF、BGP），还有Cisco所拥有的协议（IGRP和EIGRP）。还描述了Cisco的路由协议直至命令层，在命令层里路由矩阵被设置以调整网络行为来满足企业的需求。

第9章，“网络管理”——由于互连网络变得越来越庞大和复杂，网络管理已成为一项主要

任务。本章讲述了位于网络管理系统底层的规范和技术：简单网络管理协议（SNMP）、远程监控仪器（RMON）和管理信息库（MIB）。还涉及了围绕网络管理规范的一些争论，给出了Cisco实现它们的方法。介绍了命令层SNMP配置。还介绍了Cisco的套装网络管理软件产品——Resource Management Essentials、CWSI Campus和NetSys Baseline。

第10章，“Cisco安全性”——存在于防火墙之外的第二种网络安全类型是基于用户的安全保障，设置和执行口令才能访问网络以及限定使用网络资源的权限。本章首先讲述了用于安全保障的底层行业规范，尤其是AAA（Authentication, Authorization, Accounting）规范。介绍了命令层AAA，然后介绍了CiscoSecure ACS产品套装。Cisco提供了两种基于用户的安全保障产品：RADIUS，一种行业标准以及它的所有者TACACS+。两者都予以详细地介绍。

第11章，“建造Cisco网络”——本章包含了在做出网络设计决定时所必需的基础知识，无论是决定一个全新的互连网络还是对一个已存在的网络进行扩展。本章回顾了已经学过的内容——路由网络与交换网络、VLAN、冗余的需要等等——并且将它们应用于解决网络设计中的问题。按照在访问、分配和骨干层中所需要的内容，回顾了传统的三层分层设计模型。还回顾了关键的设计主题，如拓扑连接、负载平衡和服务质量（QoS）。讲解了如何进行一个综合网络需求分析以及如何使用Cisco产品将分析转化为设计方法，内容包括设计要素，如路由协议、地址设计、路由与交换的比较，WAN服务和传输负载平衡等。

第12章，“Cisco网络的故障处理”——当你能解决一个互连网络上的纷争时，你就是一名网络高手了。本章概述了典型的互连网络上的问题，以及诊断和解决它们的正确方法。按照如何处理连接性问题、性能瓶颈和其他问题，回顾了关键的Cisco IOS解决纷争命令。重点反复在如何跟踪和分离培植问题，如何调谐路由协议矩阵和如何解决WAN服务上的纷争，如串行线链接上的纷争。

附录A，“交换机和集线器的配置”——我们感到路由与交换的争论非常关键，因此有必要通过本附录给读者一种如何配置和维护Cisco的连通性产品的感性认识。还全面回顾了Cisco的Visual Switch Manager和Hub Management Console用户界面，以便让用户清楚设置哪个参数才能正确地配置和管理Cisco交换机和集线器设备。

如何阅读本书

读者可以从本书的任何章节开始阅读。各章所涉及的技术都从基础开始，从某种技术历史背景的起点到它是如何发展的，以及围绕在它周围的问题和趋势是什么都做了讲解。这之后才从IOS命令、Cisco软件工具和Cisco硬件/软件产品等方面，特别对Cisco进行了介绍。

本书并不打算重新创造另一种新的有关Internet的术语和缩略词。书中介绍的每一个术语都在上下文中进行了定义和讲解。可在Cisco的Web站点<http://www.cisco.com>阅览到本书。虽然本书独立成册，但作者决不排斥对它修改、补充新的主题内容。Cisco的Web站点包含有丰富的产品图解，白纸和其他材料供大家补充使用。特别指出的是，本书的读者可使用URL阅读到下面的书页——补充本书的三个优秀的在线术语集锦：

<http://www.cisco.com/warp/public/779/edu/academy/curriculum/demo/glossary-f.html>

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>

<http://www.zdwebopedia.com>

最后，在学习本书的时候，要注意几乎所有的现代计算机网络既发源于事实又发源于理论标准。关于网络互连标准和技术的一个最佳信息源是（<http://www.ietf.org/>）。IETF发布了RFC，几乎对任何可得到的Internet主题技术都做了详细地说明。在阅读本书并且对技术主题内容越来越熟悉时，请浏览<http://www.ietf.org/rfc.html>上的RFC，这些RFC也许能帮助你展望正在被讨论的一些技术。

参加本书翻译工作的还有：杨宝欣、蒋晓莉、王卫东、陈丽坤、侯晓明、张洪兵、于晓佳、孙建平、刘春艳、康文卓、马骏伟、高建华、蒋华明、熊萍、许宏林、吴亚平、周世龙等。

目 录

前言

第一部分 Cisco概览

第1章 Cisco 与Internet	1
1.1 Cisco在计算机行业中的地位	2
1.2 Cisco的贡献	12
1.2.1 Cisco硬件设备	13
1.2.2 Cisco解决方案	17
第2章 网络基础	19
2.1 比特和字节	19
2.2 OSI参考模型	22
2.2.1 7层栈	22
2.2.2 分层的OSI实现	24
2.3 网络技术	26
2.3.1 以太网	27
2.3.2 令牌环	29
2.3.3 ATM	30
2.3.4 千兆以太网	34
2.3.5 FDDI	35
2.4 WAN技术	36
2.4.1 拨入技术	37
2.4.2 WAN主干技术	38
2.5 TCP/IP	41
2.5.1 TCP/IP消息传递	42
2.5.2 传输层	45
2.6 IP寻址	48
2.6.1 IP地址格式	50
2.6.2 IP地址类	51
2.6.3 私人寻址	52
2.6.4 子网	53
2.7 小结	59
第3章 Cisco 认证	60

3.1 认证概述	61
3.1.1 Cisco职业途径概述	61
3.1.2 支持与设计科目	62
3.1.3 CCIE途径	63
3.2 路由与交换技术路线	64
3.2.1 路由与交换的支持认证	64
3.2.2 路由与交换的设计认证	67
3.2.3 路由与交换CCIE	69
3.3 WAN交换技术路线	69
3.3.1 WAN交换支持认证	70
3.3.2 WAN交换设计认证	73
3.3.3 WAN交换CCIE	74
3.3.4 ISP拨号CCIE	74
3.4 职业专业认证	75
3.4.1 安全认证	75
3.4.2 网络管理认证	76
3.4.3 LAN ATM认证	77
3.4.4 语音访问认证	78
3.4.5 SNA/IP集成认证（用于CCNP）	79
3.4.6 SNA/IP网络管理认证	80
3.4.7 SNA/IP集成认证（用于CCDP）	81

第二部分 Cisco网络互联工具

第4章 路由器概览	83
4.1 与路由器通信	84
4.1.1 控制台端口	85
4.1.2 辅助端口	86
4.1.3 Telnet	87
4.1.4 HTTP服务器用户界面	88
4.2 路由器的安全性	89
4.3 路由器硬件	91
4.3.1 路由器的存储器	92

4.3.2 路由器端口和模块	93
4.4 基本文件	96
4.4.1 IOS: 互联网络操作系统	96
4.4.2 配置文件	100
4.5 口令恢复	102
4.5.1 恢复Enable口令	102
4.5.2 从老式Cisco路由器恢复口令	105
第5章 路由器的配置	106
5.1 配置文件的中心作用	106
5.2 启动Cisco路由器	108
5.2.1 与IOS通信	109
5.2.2 使用IOS命令	110
5.2.3 路由器模式概述	114
5.3 基本的路由器命令	117
5.4 路由器的逐步配置	118
5.4.1 安装模式	118
5.4.2 给路由器一个身份	121
5.4.3 检查设备状态	122
5.4.4 Cisco Discovery Protocol	123
5.5 使用应用程序帮助配置路由器	125
5.5.1 ConfigMaker	125
5.5.2 Fast Step	129
第6章 交换机和集线器	135
6.1 网络拓扑结构	136
6.1.1 网络域的重要性	138
6.1.2 布线决定了网络的速度与距离	141
6.2 集线器和交换机的用途, 有何区别	145
6.3 Cisco 集线器	147
6.3.1 Cisco 集线器基础	148
6.3.2 Cisco集线器产品	151
6.4 Cisco交换机	152
6.4.1 单个交换机如何工作	153
6.4.2 交换网络基础	154
6.4.3 设计交换是网络	155
6.4.4 VLANs	158
6.4.5 Cisco 交换网络产品	159
6.4.6 配置和管理Cisco交换机	161

第7章 Internet接入产品	164
7.1 防火墙	164
7.1.1 防火墙基础	165
7.1.2 防火墙如何工作	167
7.1.3 IOS防火墙特征集	173
7.1.4 Cisco PIX防火墙	179
7.2 虚拟专用网络	184
7.2.1 什么构成了VPN	184
7.2.2 为什么大多数WAN不久会成为VPN	186
7.3 访问服务器	186

第三部分 Cisco网络的设计

第8章 路由协议	191
8.1 路由协议概述	191
8.1.1 路由协议基础	192
8.1.2 路由表的中心角色	192
8.1.3 路由协议是互联网络的一个智能	192
8.1.4 路由网络与交换网络的比较	194
8.1.5 路由更新是控制报文	194
8.1.6 动态路由与静态路由	195
8.1.7 收敛	196
8.1.8 路由器如何发现拓扑结构的变化	196
8.1.9 路由更新如何收敛	197
8.1.10 传播延时	199
8.1.11 路由循环	200
8.1.12 保持网络互联无循环的机制	201
8.1.13 路由指标	204
8.2 路由算法体系结构	204
8.2.1 距离向量路由算法	205
8.2.2 链路状态路由算法	206
8.2.3 混合路由算法	208
8.3 路由协议的实现	208
8.3.1 自治系统	208
8.3.2 内部网关协议和外部网关协议之间的差别	209
8.3.3 允许自治系统互联的方法	210
8.3.4 路由域、路由区和管理域	211

8.4 Cisco路由协议概述	212	9.3.5 CiscoWorks交换互联网络	259
8.4.1 Cisco的内部网关路由协议	212	9.3.6 NetSys Baseline	263
8.4.2 Cisco路由协议的一般配置步骤	214	第10章 Cisco安全性	266
8.4.3 EIGRP的配置	215	10.1 网络安全概述	267
8.5 RIP 2的配置	216	10.1.1 基于数据流的安全性	267
8.6 开放最短路径优先协议的配置	217	10.1.2 基于用户的安全性	269
8.6.1 OSPF路由区域	217	10.2 验证、授权和记账	271
8.6.2 变长子网掩码	218	10.2.1 AAA模型概述	271
8.6.3 边缘网关协议	219	10.2.2 AAA的工作方式	276
8.6.4 Cisco的路由协议策略	220	10.3 CiscoSecure ACS	289
第9章 网络管理	222	10.3.1 CiscoSecure ACS体系结构	290
9.1 网络管理概述	222	10.3.2 CiscoSecure ACS的使用	291
9.1.1 网络管理工具的发展	223	10.4 动态访问列表	301
9.1.2 今天的网络管理工具	225	第11章 建造Cisco网络	302
9.1.3 企业系统管理的发展趋势	227	11.1 互联网络设计基础	302
9.2 SNMP是IP的公共管理平台	229	11.1.1 网络互联基础	302
9.2.1 什么是SNMP	229	11.1.2 三层次式的设计模型	307
9.2.2 SNMP轮询与被管理对象	230	11.1.3 设计方法	311
9.2.3 MIB	230	11.2 适合需要的设计	314
9.2.4 轮询组和数据聚集	235	11.2.1 理解现有的互联网络	315
9.2.5 SNMP命令	236	11.2.2 网络的特征化	316
9.2.6 阈值	237	11.3 CISCO网络设计	319
9.2.7 事件与陷阱	238	11.3.1 逻辑网络设计	320
9.2.8 RMON: 交换网络的硬件探测器	239	11.3.2 园区网络设计	324
9.2.9 网络管理技术的发展趋势	241	第12章 Cisco网络的故障处理	335
9.2.10 Cisco的SNMP和RMON实现	243	12.1 网络故障处理的机制	335
9.3 CiscoWorks2000	246	12.1.1 网络故障处理的方法	336
9.3.1 CiscoWorks2000概述	247	12.1.2 主机IP配置的故障处理	337
9.3.2 CiscoWorks2000 Resource Manager Essentials	248	12.1.3 隔离连接问题	340
9.3.3 CiscoView: 管理个别设备的工具	250	12.1.4 处理WAN链路的故障	350
9.3.4 Resource Manager Essentials应用 程序	256	12.2 Cisco硬件的故障处理	353
		附录A 交换机和集线器的配置	356

第一部分 Cisco概览

第1章 Cisco 与 Internet

Internet令人吃惊，找不到合适的语言描述这一技术，十年前它还默默无闻，如今却引起人们如此大的关注。对Internet的狂热使1849年加利福尼亚的淘金热相形见绌。毫无疑问，人们肯定听过这样的分析和陈词滥调——Internet是历史上增长最快的市场；是历史上发展最快的技术；是第一个真正全球化的，实时的集商品、服务和思想于一处的场所；Internet将给各行各业带来深远的变化，从商业到教育到娱乐；Internet是我们通往未来的信息高速公路；Internet将变革社会；等等。

在所有令人透不过气的Web广告中最令人吃惊的是广告的大部分都是真实的。考虑这样一组数字：在今后的几年中，Internet用户的总和将从现在的2亿增长到5亿，几乎是美国人口数的两倍。注册的Internet域名每年至少翻一番。现在大约有1 000万个Web站点，比前两年多得多。1998年，美国商业系统花费了100多亿美元来更新他们的网络。每小时就有1 000个美国家庭注册访问Internet。去年花在Internet上的广告费用达30多亿美元，在一些构想的计划中，在今后几年内要将这一数字增加到300多亿美元。许多学者严肃地预计，到2005年，“Internet经济”将超过10 000亿美元。不管我们如何厌倦听那些冗长而枯燥的陈述，这些数字是令人生畏的。

尽管大多新闻报道偏爱可见的技术，如浏览器和WebTV，但真正的关键还是在于Internet基础设施。一些严肃的玩家已经投资了数十亿去建设基础设施，他们预见到终有一天所有的介质（广播、电视、电话）都会会集到Internet上。这种会集将把Internet作为唯一的“管道”，通过它几乎所有的信息都可以传输。Internet通道是否将在电话线，有线电视传输线或者在卫星之外运行，还存在着异议。这是一场大的赌博，因为赢得Internet基础设施这场游戏将意味着不可预知的财富。

但是，在天堂里也会有麻烦事。由于越来越多的人跳上这辆流行花车，所以管道的直径（称之为带宽，是衡量有多少数据可以在一个链接上传输的指标）变得越来越需要仔细审查。新的用户和较大的应用程序不停地吞占着带宽（如图1-1），其速度与向Internet基础设施中添加额外网络设备的速度一样快。全球迷宫般的远程链接和互联网络设备使带宽的需求持续增长。Internet已经承受住长期的带宽恐慌，专家们仍担心额外的负担会最终使整个网络陷于中断。这种担心虽然还没有发生过，但是庞大的财力和精力都被集中到Internet基础设施上。

用户与Internet基础设施上的服务器相连接，然而很少有人关注它是如何工作的。带宽并不是电信介质在高速光缆上运行的唯一一件事情。位于电缆每一端的网络设备，每一个比特都同样重要。在许多情况下，这些设备的速度和电信介质一样，也是Internet带宽中的一大要素。

本书从“地基”入手，纵览了互联网络的基础设施，从底层技术开始一直到产品层都有讲

述。如果是初学者，那么阅读本书将了解互联网络的基础。本书是从互联网络技术的首要生产者——Cisco公司的观点写作的。由于技术的覆盖面非常广泛，所以要清楚需要各种各样的技术和组件才能使任何一种互联网络正常运行，而不仅仅只使用Cisco的产品才能建造网络。但绝对不会错的是，本书是关于基础设施，即互联网络上操作的各种设备的：

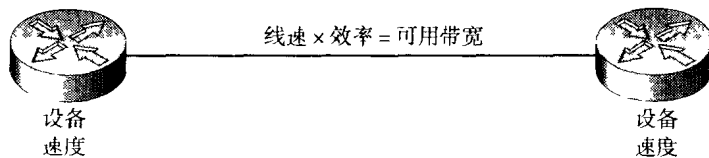


图1-1 网络设备之间的可用带宽

- 路由器。这些设备在局域网（LAN）之间进行路由选择、传输数据。路由器放置在互联网络内部；没有它们，Internet将不可能实现。路由器使用网际协议（IP）地址来断定如何选择最佳的路由，将包传输通过互联网络。
- 交换机。这些设备也是在局域网之间转发数据的。交换机的速度比路由器快，但是它们不使用IP地址，因此没有路由器那种在庞大的互联网络中寻找路径的能力。
- 防火墙。这是一些基本的路由器，被特别装备用以过滤包，来保障一个企业内部互联网络的重要数据处理的安全。
- 访问服务器。这些专用设备响应来自远程用户的呼叫，并将它们连接到互联网络上。大多数访问服务器被Internet服务供应商（ISP）用以将家庭用户和小公司连接到Internet上。
- 集线器。低级的集线器接受来自PC机和服务器的电缆，创建一个独立的LAN，称之为LAN段，互联网络的基础建设部分。

总之，这五种类型的设备构成了Internet的基础设施，唯一的其他主要因素是连接广域网（WAN）的远程通信链接。本书讲述了全部五种类型的设备，这些设备都是Cisco产品线上的产品，还回顾了WAN技术。透过Cisco的产品系列进行讲述，能更仔细地看到互联网络设备内部的工作情况。

1.1 Cisco在计算机行业中的地位

我们都知道，微软的Windows是世界上最重要的计算机操作系统。这儿有个小测验：你能说出第二个最重要操作系统的名称吗？做出一个选择：

- MVS。IBM的专有操作系统，在大型计算机上运行。MVS仍然在中央社团和处理金融账目和其他敏感事物的政府数据中心上占主导地位。
- UNIX。实际上有许多UNIX专有版本，分属于Sun、惠普、康柏、Novell和IBM等计算机生产商。无论如何，UNIX是企业级代理服务器应用中起主导作用的服务器操作系统。
- IOS。互联网络操作系统的缩写，它是Cisco专有的、用于自身互联网络硬件系列的操作系统。

IOS是第二个最重要的操作系统，而且具有广泛的影响力。下如此断言的一部分原因是因为UNIX和MVS都已丧失了它们的部分市场——UNIX的市场份额已被Windows NT抢走，而MVS

虽然仍是关键任务的技术，但已经停止了进一步的发展。至于IOS这样重要的主要原因是Cisco在Internet路由器市场上占有80%的份额，且Internet是历史上发展最快的市场。

更进一步看，Cisco在路由器技术上拥有和Intel在Windows（或者说是Wintel）硬件平台上享有的同样的市场份额。Wintel体系已经作为一个垄断体受到竞争者的攻击，微软和Intel最近被美国司法部门以所谓的垄断行为反托拉斯侵害的名义起诉。但Wintel还是被两家卖主垄断着，出现了两家公司平分硬件和软件的局面。

这些情况对于Cisco都不会出现。IOS是属于Cisco公司所有的操作系统（OS）结构，而且它只在自己的硬件上运行。这意味着Cisco 80%的份额在软件和硬件的收入上，使公司能控制住其产品的全部结构。Cisco的管理队伍也许在考虑适当退缩一下，但是已经开始有谣传说Cisco将是行业上的下一个垄断体。公司赢得占优势的市场份额是公平和合理的，但是有些人害怕IOS之于互联网络就像Windows之于桌面计算机。Cisco将毫不犹豫地向着制定的500亿或更高的目标前进。

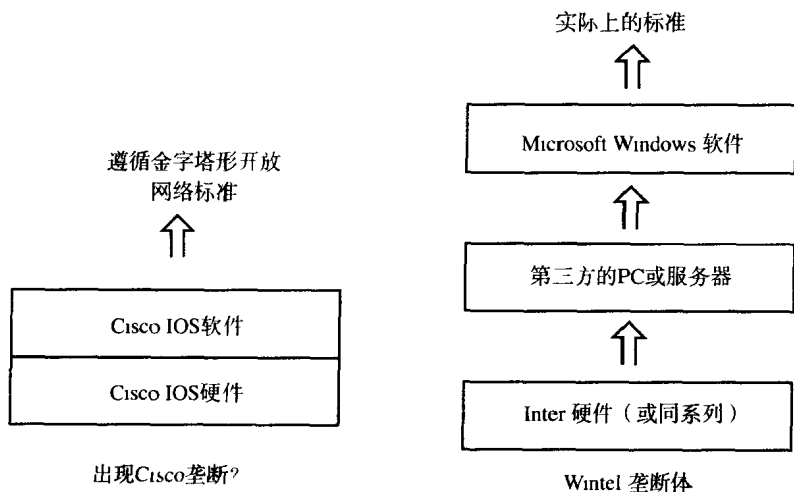


图1-2 Cisco与Wintel的比较

Cisco当前的地位与Wintel垄断体相比（如图1-2），既有自己的强项又有自身的弱点。从反面说，Cisco的产品被用于执行真正的开放标准协议，这些协议削减了他们平衡产品结构以控制市场的程度。Cisco不会对任何设计圈子之外的竞争者冻结他们准备实现已有技术的产品，这是因为有技术实现开放标准。从正面说，Cisco是一家制造自己产品的公司。这和Wintel形成了良好的对比，Wintel是靠成千上百的PC制造商将他们各自的产品推向市场的两个公司。

投资团体没有任何损失。他们特别喜欢看到这样的事实，即在每一个主要的互联网络硬件市场中，Cisco都占有第一或第二位的份额。例如，本地数据交换市场是互联网络中最热门的部分之一，Cisco拥有40%的份额，而它最有竞争力的对手，其份额还不到10%。Cisco处于如此重要的地位，以致于其CEO John Chambers声称“Cisco是计算机行业历史上发展最快和获利最多的公司”。显然他的话有一定的价值。本书编写之际正值1999年秋，此时许多Internet股票已经下跌，而Cisco的全部资本稳定在2 200亿美元上。

本书不是一本吹捧Cisco的书。像任何行业企业一样，这家公司也有自己的缺点，本书也适

时地给予适当的批评。但是不管是寻找工作的个人，还是决定公司Internet战略的经理们，学习Cisco技术是如何工作的都将可能是对互连网络世界最好的认识。

Internet的风景

Internet不是唯一的一种技术，它是使互连网络成为可能的相关技术的一个集合（如图1-3）：

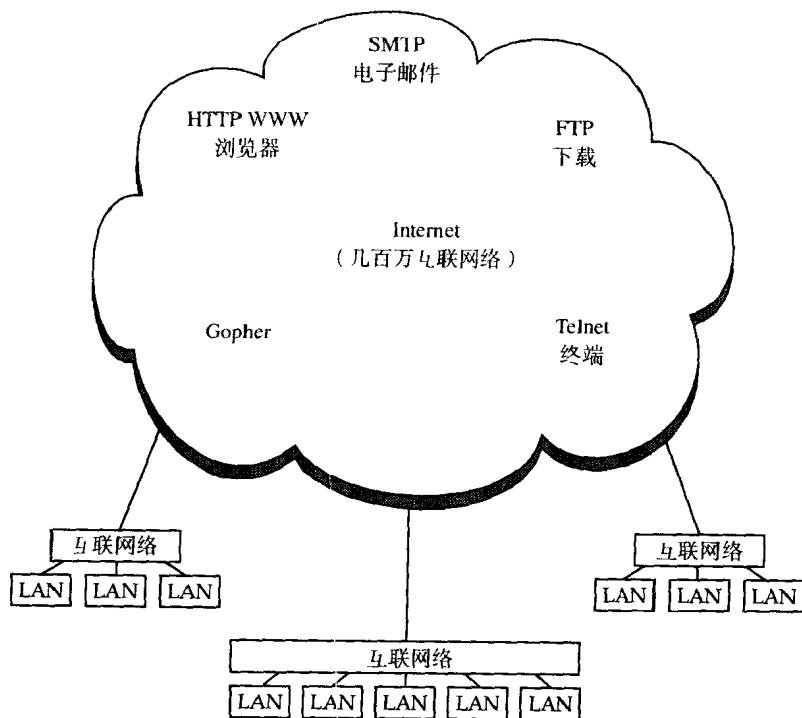


图1-3 Internet的组成

- 物理介质。从连接器、电缆到高速光缆，将所有事物连接在一起的物理链接是网络的基础。
- 网络技术。LAN协议执行电话线上发生的事情。最著名的是以太网，但是还有其他重要的网络。
- TCP/IP。传输控制协议网际协议将Internet绑在一起。IP处理地址，而TCP处理消息。
- 操作技术。互连网络依靠一定数目的底层标准和协议使自己运行起来，没有它们互连网络将不能付诸实施。
- 应用程序协议。网络应用程序协议定义了各种互连网络能做的有用工作，从文件传输到网页下载。

为了制造自己的产品，网络行业使用一个7层的结构框架，称之为开放系统互连（OSI）参考模型。它不是一个一致性模型，但前面所列出的技术从物理层向上，或多或少地遵照了OSI模型。

在继续往下进行之前，先用简短的话语明确清楚以下术语：Internet是指独立的互连网络的一个全球性互连网络。互连网络是指在单一管理权下本地网的任何连接——通常是一个企业或

一个ISP。一个私人的网络机械地说和开放的Internet一样。主机是用户的设备，如PC、服务器、大型机或打印机。设备是指一件网络装备，如路由器。一般而言，节点和站既指主机又指设备。LAN段是主机共享的一种网络介质，大多数LAN段是用一个集线器组成的。应用程序协议是运行类似Web浏览器、文件传输、电子邮件和其他有用函数的一种软件标准。内联网是指作为一个私有Web运行的内部互联网络，Web浏览器使用的是企业应用程序软件，而不是更普通的图形用户界面（GUI），Windows。

从技术的角度讲，私有网络的组成部分和Internet一样。Internet和一个大型互连网络的唯一区别在于其开放程度。

1. 互联网络的五种主要设备

集线器是一种无源设备，它连接来自个体主机（主要是PC、服务器和打印机）的电缆，形成一个独立的LAN段，扮演着中心连接点的角色（如图1-4）。连接到同一个集线器上的主机成为该LAN段的成员，它们共享集线器的带宽进行彼此之间的通信。集线器只是简单地将输入的信号重复发给连接在它端口上的所有设备。

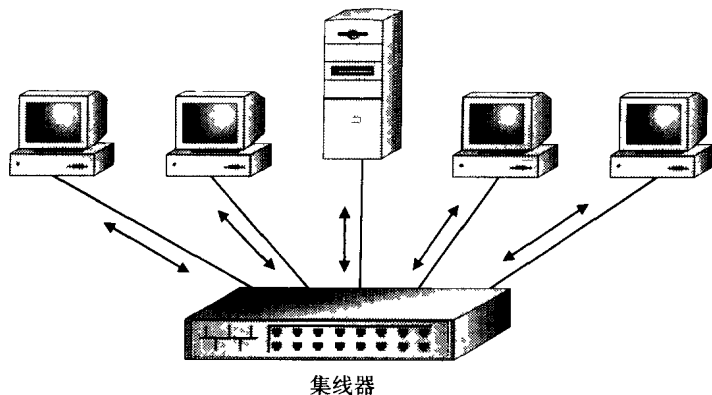


图1-4 主机通过电缆连接在集线器端口上

交换机将主机连接到互联网络上，连接方式和集线器很相似（如图1-5）。但是两者的根本区别在于交换机在发送和接收主机之间形成了一个虚电路。换句话说，交换机的带宽是保留给两个主机之间唯一的交换连接的，就好像它被100%地分配给了那个虚电路。交换机能够很好地做到这一点，方法是通过使用比集线器更高级的电子技术，将带宽时间分成许多条——称之为信道——对每一个交换端口的服务都足够大。交换机比集线器的速度快很多，但是它造价更高，而且结构和管理上更复杂。

访问服务器是一个专门的设备，粗略地说，它的一端像一个调制解调器，而另一端像一个集线器（如图1-6）。访问服务器将远程用户连接到互联网络上。全世界有成千上万个访问服务器，绝大部分都被ISP操作着，接受来自Internet用户的电话呼叫。其中一些执行着更为特殊的功能，但是访问服务器的主要目的还是将远程拨入用户连接到Internet上。

路由器是一个智能设备，它基于消息的IP地址进行传输。集线器和交换机上有给单个主机插入的端口，而路由器上有给LAN段添加的接口。简短地说，路由器的工作就是在添加的LAN段

之间传输包（如图1-7）。

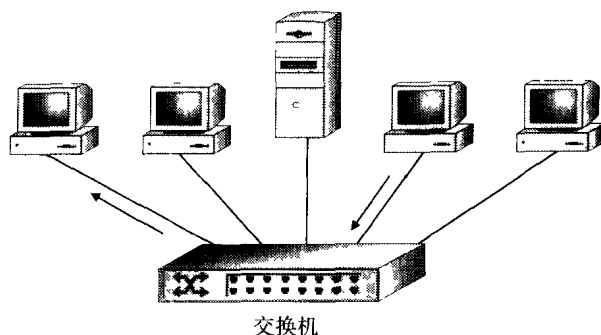


图1-5 交换机连接类似于集线器连接

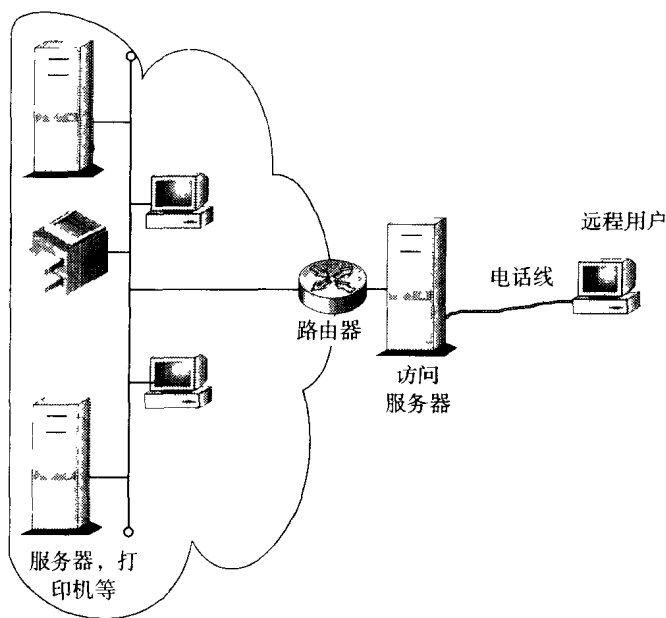


图1-6 访问服务器

在互联网中，路由器是唯一一个最重要的设备类型。它具有的灵活机动性和作出决定的能力，使复杂的互联网络运行成为可能。如果没有路由器提供的逻辑能力，Internet将比现在慢数百倍，而且会更昂贵。互联网络结构分为7层：集线器在第一层操作，交换机在第二层操作，路由器在第三层操作。这将在下一章详细讲述。路由器还有按照源地址、目的地址、网络应用程序和其他参数过滤数据流的能力。

防火墙是专门的路由器，它们在互联网络 and 外界之间起检查点的作用（如图1-8）。它们依照已被编程好、必须被执行的安全政策，检查每一个包。防火墙形成了一个有意设置的数据流挤压点，并且为安全起见一直持续监控着内部/外部的连接。任何连接在Internet上的企业都应该