网络专业人员书库

虚拟专用网的创建与实现

(美) Casey Wilson Peter Doak 著

钟 鸣 魏允韬 等译

刘晓霞 审校

机械工业出版社
China Machine Press

本书系统介绍了虚拟专用网的概念、起源、配置、实现和维护，还对虚拟专用网体系结构、加密工具、有关限制、防火墙结构等内容进行了探讨，并提供了大量实例。本书是网络、MIS管理员必备的参考书。

本书版权登记号：图字：01-2000-1312

图书在版编目（CIP）数据

虚拟专用网的创建与实现 /（美）威尔森（Wilson，C.），（美）杜瓦克（Doak，P.）著；钟鸣等译. - 北京：机械工业出版社，2000.8

(网络专业人员书库)

书名原文：Creating and Implementing Virtual Private Networks

ISBN 7-111-08179-X

Ⅰ.虚… Ⅱ.①威… ②杜… ③钟… Ⅲ.虚拟网络 - 基本知识 Ⅳ.TP393

中国版本图书馆CIP数据核字(2000)第37839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：郭东青

北京昌平奔腾印刷厂印刷 · 新华书店北京发行所发行

2000年8月第1版第1次印刷

787mm × 1092mm 1/16 · 23.5印张

印数：0 001-6 000册

定价：38.00元

前　言

记得曾经在什么地方看到过，“我们今天的技术是从前的学者们不可想象的……”。我忍不住想知道，布勒斯·帕斯卡（1623～1662）面对放在他的机械计算器旁的 400MHz 的奔腾便携电脑会作何感想。如果山姆·摩尔斯将电话线插到他的 56K “猫” 的后背上，阅读来自阿列克谢·贝尔的伊妹儿时，我真想悄悄瞄他一眼，看看他的表情。

撰写这样一本书存在很多困难，可以说是一种挑战。一开始我们就说，本书主要是针对网络管理人员以及对虚拟专用网（Virtual Private Network）感兴趣的人写的。我们希望本书既技术完善而又不至于很复杂（这是一对矛盾）。我们所面对的是一种不断飞速发展的技术，书中的内容随时都在变化，很多东西刚在键盘上打出，但由于理论已成为现实又要对其进行更改。因此在本书中我们对虚拟专用网这一新兴的技术只是进行尽可能全面的介绍，很多内容不能讨论得很深。

VPN远未成熟，4年前，它还带有科幻性质，但现在已具有了相当的实用性。利用现在可以得到的技术，大大小小的具有VPN的工商企业利用Internet连接到任何远距离的设施，或连接到电话能达到的用户。从缅因州的班歌到南非的开普敦，企业只要单击一下鼠标就能够操作业务和共享数据。

本书，我们对大量的信息进行了筛选，给读者提供了将VPN技术投入具体业务所需的东西。根据需要，我们对Novell 和 Microsoft进行了介绍，与其他VPN供应商进行了尽可能经常的接触。我们在对某项技术进行介绍时尽量从技术而不是商业营销的角度出发。Pete是本书的主要策划者，作为德克萨斯Mainland学院的教授，这是他的专长。我们选择网络管理人员、MIS管理员、信息技术人员以及有经验的连网专家作为本书的主要读者对象。我们打算使本书成为设计、实现和维护虚拟专用网的主要参考书籍。我们虚构了两个公司（Specialty Training和Vintage Air）并将它们作为例子。

在第1章，我们使时间倒流，对一些早期的学者进行了拜访，探讨了这些技术是怎样产生的，他们称这些东西为Internet。本章讨论了VPN网的得与失，并说明它能干什么或者不能干什么，它对您的企业有何用途。

用第2章和第3章描述局域网和广域网。假定读者已经拥有一个或多个网络，以保证我们能具有共同的语言。显然，两章的篇幅讲述这些内容是不够的，不可能像教材那样详细。可以说要展开来讲，局域网和广域网的内容用两本书也不够。

在第4章和第5章中，将对开发标准等较深的内容进行探索。读者能了解到连网社区中的规则由谁制定，特别是Internet上的规则由谁制定，以及这些规则怎样存在和为什么存在。如果读者认为它是无序的，那么这种认识是不对的。没有规范，Internet就不能存在。我们列举了一些各供应商如何采用符合其利益的标准，以及有时通过与其表面上的竞争对手合作而受益的例子。

第6章将讨论怎样对现有网络系统进行发展，使其与VPN技术相结合。我们将为把Internet与您公司的网络可接受策略相结合而打下基础。如果您的公司至今尚没有合适的策略，我们

将使您认识到为什么需要策略以及向您提供一个建立它们的基础。本章将开始讨论安全问题，以及安全对您有何意义。接着，是一些关于训练的想法：通过给用户灌输正确的思想，使您的工作更为容易。总之，利用第6章，我们将帮助您确定实现这种令人激动的技术的最佳成本效率方法。

Novell和Microsoft将占用第7和第8两章。每章都将引导您一步步地通过安装和配置 VPN 的过程。在详细解释为什么要求某些录入时，给出的屏幕将显示出工作进行到了何处。我们认为重要的是要认识到为什么要按某种方式做某样事情。在此阶段，将建立简单的站点到站点的VPN，示范怎样通过当地的电话将两个网连接起来。一个站点可能在德克萨斯，另一个站点可能在新西兰，用户可在此两站点间共享数据，而只需支付本地电话费。

然后在第9章中作进一步的提高，引入客户机到站点（client-to-site）用户对VPN进行扩充。这里的目的是针对在家远距离办公和/或可移动用户对系统做进一步的扩充。目的是减少每月的电话费，而且允许您的远程用户对系统进行访问，不管他们位于何处。

安全问题不容忽视。本书第10章的所有内容都与安全问题有关，虽然我们知道，任何有点能力的作者就此问题都可以写整整一本书，而且材料还有富余。我们的一个目的是展示如何利用VPN技术提出在网络间具有一个专用隧道的 Internet。而且，我们还将示出安全不仅仅是对大量的位和字节进行加密的问题，安全保证了数据的完整性并使它们免遭各种破坏。这些破坏可能来自各种意想不到的地方。

M&M（不是糖果）为第11章的议题。M&M（Management and Maintenance）在此表示管理与维护。我们将在本章中介绍使VPN保持正常且性能最好的工具。还给出了一些较为复杂的练习，因为这样做是值得的。本章中安排了一节讲述定期检查，以便在出问题前能及早发现它们。

在第12章总结之后还有好几个附录。例如，我们将首字母缩略词及其定义以一种易于参考的形式编在一起，可将其折起来或夹一张小便条以便今后查找。还提供了一个关于VPN供应商的附录，在需要购买VPN软硬件时可以查找。我们将在各种Internet文档中可得到的2 500多个请求注解（Request for Comments, RFC）中进行挑选，并在某个附录中给出与VPN有关的那些RFC的清单。我们专门用附录D汇编计划、安装、配置、管理和维护VPN时所需的检查表。最后，在附录E中，给出一组推荐读物进行选择，以便您能扩展自己的知识，对VPN网作进一步的探讨。

我们打算在站点 www.sldenterprises.com 上对本书提供技术支持，在本书销售后一段时间内我们都会这样做。欢迎经常提问。只要我们发现新材料，就会设法提供给您。

Casey Wilson (Casey@sldenterprises.com)
Peter Doak (PDoak@sldenterprises.com)

第1章 VPN 介 绍

主要内容：

- 什么是 VPN
- 网络历史回顾
- 某些得失
- 前景展望

虚拟专用网(Virtual Private Networking，VPN)是将Internet作为计算机网络主干的一种网络模式。表面上它似乎不那么令人喜欢，但深入研究就会发现，它提供了巨大的潜力。利用 VPN，很多企业能够省下一大笔为已有网络租用线路的费用。使用VPN不需要到处布置站点，只需将它们放置在你所在的城镇即可。事实上，构造VPN的技术也可用于你所在大楼中的局域网(LAN)上。

1.1 历史回顾

近十年内，Internet的发展相当平静，有一段时间可以说是无声无息，但现在它又刮起了一阵旋风。十年间唯一真正重大的变化是用户数量的增长。近两年，这种势头有增无减，掀起了一个又一个的高潮。 Internet 这次卷土重来，不是孤军深入，还带有一个伙伴，那就是虚拟专用网。

1.1.1 1866——先兆

当第一条2 700英里的电缆横跨大西洋将爱尔兰与纽芬兰岛连接起来时，网络迈出了一小步。对于那些坚韧不拔的通讯先驱们来说，这条电缆意味着第一次可以在两个大陆之间发送消息了。由于这次冒险的成功，出现了更多的海底电缆，开始了信息时代。

电报系统当时唯一可用的电源是电池，发明发电站是几年后的事情。数据格式建立在莫尔斯电码的基础上，利用莫尔斯设计的类似于一系列点划线的东西来表示字符。

电报员根据查尔斯·惠斯通发明的系统将消息译成一些穿在纸带上的孔。然后将该纸带送进电报发送机，电报发送机以光速将纸带所载的信息通过电缆发送出去。

电脉冲以光速传送，但其数据传送率每分钟只有100个字。电传机(也叫传真电报机或干脆叫电传)在19世纪末20世纪初尚未出现，它的发明是在打字机之后。

电缆通讯占统治地位达36年之久，直到一个名叫马可尼的年轻发明家发送了一条从加拿大新斯科舍到英格兰的横跨大西洋的无线电消息后，这种状况才得以改变。这个事件加快了信息时代的进程。

气候对无线电传送有很大的干扰。当时的无线电设备都是手工制造的，并且非常昂贵。所以多数人都对这种小玩意冷眼旁观。

1.1.2 1880——何勒内斯码与制表机

在电缆的敷设与马可尼发明无线电期间，有一个名叫赫尔曼·何勒内斯的美国科学家正

忙着发明一种制表机。何勒内斯负责编制1890年美国的人口普查表，他研制出了一种能够读取穿在卡片上的孔洞的机器。这种机器能根据各种开关的设置汇编信息。

何勒内斯没有发明成第一台计算机。算盘领先了数个世纪。他所做的仅仅是发明了一种机器，这种机器能够按照预先设置的开关产生所需的信息，而操作人员所要做的也只是搬动一个曲柄。实事上，现代计算机也只是根据人们对任务的定义进行工作的。

1.1.3 1945——ENIAC

借助电缆和无线电进行通信已经从横跨大西洋发展到了洲际间的通信。1945年，工程师和物理学家们将大约20 000个电子管、1 500个机械继电器和数十万个电阻器、电容器和电感器装入了宾夕法尼亚大学莫尔电子工程学院的许多机柜中。用数英里长的铜线、数百磅的焊接材料将上述器件绑在一起，最终的造物被称为电子数字积分计算机(ENIAC)。

ENIAC 为美国政府的最机密的研究工具，对公众保密。ENIAC 最初用来计算炮弹的弹道，一个训练有素的数学家利用当时最先进的计算器花20个小时才能完成ENIAC 30 秒的计算量。

1946年，ENIAC 在取得巨大成功之后，让位于通用自动计算机(UNIVAC)。主持人是 Mauchly 博士和一个大学毕业生 Eckert。这两个人是ENIAC的主要参加者，他们认为自己会做得更好。他们的顾客只有美国人口普查局，1946年美国人口普查局为 UNIVAC 预付了 30 万美元。

Mauchly和Eckert过于乐观了，基础研究耗掉了预计的双倍时间。商定的工作延迟到了1948年；政府拒绝进一步投资。到1950年人口普查工作开始时，Mauchly和Eckert甚至在考虑申请破产。

1.1.4 1951——雷明顿·兰特的加盟

电动剃须刀公司的这个有远见的合伙者进行了风险投资，1951年4月，第1台UNIVAC 运抵人口普查局。它几乎价值100万美元，美国政府拒绝支付超出预算的部分，坚持只付原协议所定的40万美元。

UNIVAC是一个技术奇迹。其中电子管的数目削减了1/3还多。系统压缩在更小、更好看的机柜中。前面提过赫尔曼·何勒内斯制作了人口普查中广泛使用的穿孔卡片。其80列的卡片可直接读入UNIVAC。这时来自卡片的信息甚至可以直接传送到磁带，结果计算速度更快了。科学家和工程师们曾经认为ENIAC的1KHz的时钟频率是一个了不起的壮举。因此，在UNIVAC的时钟频率提高到2MHz 后，可以想象他们有多高兴了。

1952年，UNIVAC被用来预测艾森豪威尔的总统选举。来自全国各地的记者都盯着UNIVAC的结果；有的记者认为竞争太激烈，结果难以预测，多数人很讨厌用一台机器来预测这件事。但选举结果出来后，UNIVAC 预测的准确性使政治评论家们大为吃惊。

“计算机”一词逐渐地从作业描述中去掉而成为专门的机器了。这时，IBM(蓝色巨人)插了进来，一门新兴的工业诞生了。当时没有一个人能预料到，今后的十年中会发生什么。

1.1.5 1957——ARPA的诞生

在苏联发射人造地球卫星时，比尔·盖茨只有两岁。艾森豪威尔忧心忡忡。为使美国在军事科技上处于领先水平，他批准建立了“高级研究规划局”(ARPA)。从此展开了空间军备竞赛。

计算机的工作不止是计算炮弹的弹道，而且还被用来进行弹道导弹(核武器运载系统)的瞄准。轨道动力学与亚轨道动力学是其核心部分。计算时，宽行(132 列)打印机每小时要用掉数箱打印纸。

越来越多的政府机构装备了计算机。大学也开始安装它们。政府和大学之间进行着数据的交换。多数交换工作是秘密进行的；武装信使长距离运载机密的资料，这件事情不可能依赖美国邮政。

一小群折衷主义者解决了怎样将计算机连到一起以共享信息，这样，信息时代已作好了再次起飞的准备。

1.1.6 1962——ARPANET 投入运作

美国空军由于担心对美国的核攻击可能会中断重要的通信线路，因此委托兰德公司进行生存研究。1962 年提出的问题是怎样建立一个分散的网络，使得如果某个站点或路径被毁坏，对核轰炸机和导弹发射器的命令和控制仍然可以进行。

在几个可选择的方案中选择了包交换技术，在发报的计算机上将数据分成几块，然后通过现有电话线或无线电发送出去。每个包都含有分立的地址和最终的报文部分，这些包将由目标计算机进行组装。如果发送者与接收者之间的通信链路中断，路由器将会选择另一条不同的路径。如果某个包被破坏，接收者将发送一个消息给发送者要求重发。重新发送一个包比重新发送整个报文节省时间。

1968年，ARPA将一个合同给予了Bolt、Beranek 和 Newman(BBN)，要求连接四台计算机，这四台计算机分布在：斯坦福研究所，加利福尼亚大学座落在洛杉矶和圣·巴巴拉的分校，以及犹他大学。早期的大多数时间花在系统性事故的调试上。先驱们最终将它搞成了，并建立了第一个有效的协议，称为网络控制协议(NCP)。这样 ARPANET 以 56Kbps 的速度投入了运行，表面上是作为一种研究方法。只有少数人知道真正的原因。

紧接着下一年，尼尔·阿姆斯壮和布兹·阿尔德林就登上了月球。他们在月球探测飞船(LEM)上携带的计算机在他们登上月球表面时不断发出执行超载的警报，折腾得他们够呛。完成所需任务的电量几乎不够。

1.1.7 1972——ARPA改名

1972 年发生了几件事。ARPA归入了美国国防部并马上改名为 DARPA。主计算机的数量增到了 24 台。最重要的事件是由BBN的 Ray Tomlinson引发的；他在地址中加了一个@符号，创造了电子邮件。

第二年，斯坦福来的Vinton Cerf和DARPA来的Bob Kahn开始研究一种新的协议。他们为其起名为传输控制协议(TCP)。在一篇关于TCP的论文中，Cerf和Kahn杜撰了术语 Internet。增加ARPANET上的用户数目和要求在不同平台间进行通信使TCP进一步改进为 TCP/IP，即Internet协议组。

1.1.8 1976——TCP/IP入伍

由于连接到ARPANET的计算机数量达到了100台，国防部命令将TCP/IP作为系统协议。同年，卫星网(SATNET)将美国与欧洲连接了起来。总部设在瑞士的欧洲粒子物理研究所

(CERN)用CERNET网在欧洲步入了领先地位，CERNET在大量的主机和小型机间用2Mbps 的串行线和包交换技术提供文件传输服务。这是一种在通过双绞线和RS-232端口连接在一起的数百台哑终端的现有系统上进行的重要改进。

我们打算离开CERN和欧洲返回美国。不过，可以看出信息时代并不只是一种局限于某地的冒险。我们在几年后还要再次访问 CERN。

1977年，一个称为Commodore 的小公司带着个人电子处理器(PET)进入了市场。其后是VIC-20，然后又是Commodore C-64。一位计算机史专家估计，当时制造和销售了两千万台C-64。

UNIX到UNIX拷贝协议(UUCP)的研制导致了世界性的新闻组网络系统和新闻组的建立，它是1979年进入这个领域的。

1.1.9 1981——PC出现

某些企业家认为这时的世界所需要的是某种更好的东西，于是这种东西就出现了。

蓝色巨人于1981年将 IBM PC投放市场。在数年内，又提供了IBM XT。这是当时的技术奇迹。它几乎占据了桌面系统的全部市场，这种机器有10MB硬驱，其RAM可扩展为2MB。

两年后，在史蒂夫·乔布斯引入了Apple Macintosh(Mac)时，个人机市场的竞争进入了白热化状态。Mac利用其用户友好的操作系统争得了一大块市场份额。Mac的用户无需费劲地从键盘启动应用程序，然后再打开要处理的文件，他们只需在某个图标上点击一下，机器会做其余的工作。

XT和Macintosh比阿姆斯壮和阿尔德林带到月球的那台计算机完善多了。

1.1.10 1984——用户数量开始增多

在国家科学基金会(NSF)的大力支持下，这五年中，连接世界教育单位的计算机网(BITNET)、计算机科学网(CSNET)、军用网(MILNET)等相继出现。组成了Internet活动委员会(IAB)。这段时间中最引人注目的进展是CSNET的升级，它采用了T1线，允许数据的速率从56K跳到1.5Meg。当年用户数就达到了1 000 左右，次年达到了2 000。

1.1.11 1988——用户数剧增

到1988年，Internet用户数超过了56 000。多数都是专用连接。NSF 禁止Internet用于商业目的，但禁令的打破只是个时间的问题，因为电子商务时代就要到来了。

业务用线串了起来。局域网的黄色电缆在公司的办公室间穿进穿出。Appletalk 和Ethernet说着悄悄话。医疗机构不用图表就能传递病人的信息。你可以进入银行的任一家分行查对自己储蓄户头的余额或支付信用卡帐单。保险公司可在任何需要的地方共用精算员。网络的潜在应用简直不胜枚举。

像Fido Net这样的专用电子公告牌建立了一种将世界各地的人员连接在一起的方法。在一个月内，你可以和过去不可能有机会相识的人交换好几次意见。任选一个主题，都能找到有关它的许多资料。这在调制解调器制造者之间激起了极大的竞争，看谁能在普通电话线上最先达到2 400波特。

1.1.12 1992——World Wide Web

还记得瑞士CERN的那些人吗？当他们在1992年发表World Wide Web时，域名几乎已经

有十年了。也就是在同一年，注册主机的数目超过了一百万。

迄今为止，我们已经追述了Internet成长过程的一小部分，但是非常重要的一部分。本书或其他书都不可能完全记载清楚这个即将到来的潮流。

创新思想是构成Internet的基本要素。E-mail是第一个创新；它产生了imagery、telephony和聊天室(一种发泄过剩精力的地方)。发展了一批新词：电脑空间(cyberspace)、连接、虚拟世界、nethead(有经验的Internet用户)、网民(netizen)以及 geek。有各种方言词汇，如桥接、路由器、交换机以及加密等。

在创造了Web后仅仅两年，国家科学基金会就放弃了它加在 Internet上的商业限制。这个举动导致了一次实际的大爆发。商务活动乘机大举进攻，在 Intermet网上攻城掠地。

此时，ARPANET 已经退役多时。第一根横跨大西洋的电缆怎么样了呢？这根伟大的跨大西洋电缆在30年前发送了最后一条报文，然后被送进了博物馆。

据报道，Internet在1998 年末已经有7 400万个以上的域名。

1.1.13 现在——巨大的飞跃

本书的所有内容都是关于连通的电脑空间——虚拟专用网的。Internet已经发展成为一个巨大的商业冒险场所，数百万人将他们的家用计算机连到了Internet上，成千上万的组织机构也连了进去。软件和硬件开发者，3Com、Novell、Microsoft、Cisco等已经看出了集中于VPN的需求。

几乎有十年的时间，Internet发展平稳，一段时间可以说是无声无息。唯一真正重大的变化是用户数量的增长。

下一个重要事件将是VPN，而这也正是本书所要介绍的内容。VPN像一辆松开离合器往坡下滑的汽车，获得了动力但省了电，正向下一个高峰迈进。VPN建立了Internet的另一个新目标，为VPN编写了新的协议，设计了新设备，还有许多设备正在研制中。大约再有一两年就会轮到VPN大显身手了。

1.2 VPN的优缺点

根据权威人士的观点，如果一个行业可以利用虚拟专用网，它在起跑线上就占有了优势。每个行业，或大或小，都能够以这样或那样的形式利用VPN。

VPN的一个重要优点是能够在不同平台之间传输数据，而无需对专门的设备及其相关协议操心。

我问过Fortress公司的业务发展经理Howard Myers，是否能想得出某类行业或企业，不管其大小，将不使用VPN。“任何不想节省电话费和/或不担心安全问题的行业！”他答道。他说，“实际上，今天VPN尚未为需要巨大带宽的极大的设施作好准备。现在，它一般对T3速度的调制解调器性能最好，不过变化会很快。”

1.2.1 它对所有人都适用吗

也有一些VPN不能对企业投资给出回报的情形。假如某个公司有一个已经启用和运行的拨入网络。如果所有通信都在本地，不需要长途电话费，此时VPN没有多大意义。

对于上述相同的网络设施，如果只有少量的短距离通信，正如在局部访问传送区(Local

Access Transport Area, LATA)中一样，信息技术管理人员需要进行复杂的分析以搞清分期偿还VPN技术方面的投资需要多长时间。

怎样实现VPN以及能节约多少费用依赖于正确的决策。不同条件下的结果各不相同。Myers认为VPN对只有一两个拨入人员且无自己的网络专家的非常小的公司没有用。

在阅读本书时，请注意，对某些VPN用户是优点的东西可能对另外一些用户不是优点，甚至可能是缺点。某一机构如何实现这个发展中的技术将依赖于信息技术(IT)管理人员怎样分配可用资源。

要点是，IT 管理人员必须确定其优点是什么和在何处，如何避开其不利之处。IT 管理人员必须不落入范例的陷井。他或她必须估计可利用的VPN技术并计划好怎样使其在自己的环境中起作用。观摩其他公司实现VPN的方法没有什么坏处，只要能保证其他公司的方法适用于自己即可。

1.2.2 实现

VPN的实现有三种。一种是打电话给Internet服务商(ISP)，将任务完全传送给服务商。另一种相反的选择是IT管理人员只购买拨入服务连接并在公司的范围内提供VPN的所有元素。第三种选择是外购部分作业并维持其余的作业。正如后面的章节所要介绍的那样，这样可在不同的程度上完成VPN的实现。

在第一种情况下，IT管理人员和企业人员完全依赖于 ISP，因为本书中讨论的VPN的各个方面都移交给了ISP。另一方面，在内部维持所有VPN操作使企业具有完全的控制权。

如果由ISP完成所有工作，它将在连接和连接的质量方面作出某种保证。企业不用支付雇人管理和维护运行的费用，不用为培训和保持最新技术而花钱。另一好处是具有硬件和软件变化的透明性。在ISP升级其系统时，顾客可能不会意识到已经作了更改。ISP一般还具有其他优点，尤其是如果它首先是一个电话公司时更是如此。如果T1线开始运行时不正常，ISP可以快速地更改线路，以保证顶层的服务。

如果决定在企业内部保持部分或全部控制，我们还将考虑实现VPN的不同方法。例如，某个IT管理人员可会选择通过软件完成所有VPN的工作，另一 IT 管理人员可能决定用软件或硬件一起完成VPN的工作；而其他人可能选择全部用硬件来完成VPN的工作。

1.2.3 用于intranet的VPN

顺便说一下，VPN技术并不一定都用于超大网络通信，可将其用于公司内部以允许雇员访问某些特定的数据，但限制他们访问其他数据。

假定有一个医疗保健机构，记帐部门有一个员工可能需要知道在 Joe Doak 的身体检查之后，还要进行什么检查过程，但不能够私下查看由验血确定的胆固醇含量。

可能允许该员工查看由该医疗机构人事部门保存的他或她的个人记录，但限制查看其同事的记录。

IT管理人员要做的事是利用VPN技术更好地服务于他的公司。

1.2.4 无限的应用

远程办公正越来越流行。雇用最好的人员来完成工作不再受地域的限制。雇员可在家中

工作，而公司则减少办公开支。使用移动电话，一个房地产中介公司可以利用VPN将数据传给他的驻场代表。在货运业中同样的移动电话也可以用来跟踪货物。将电话和卫星通信相结合，可以将VPN扩展到全球任何水域的船上。

1.2.5 软件方案

如果你决定在企业内保持部分或全部 VPN，就必须选择硬件或软件系统，选择基于防火墙的VPN或独立的VPN应用程序包。

利用现有的内部路由器并装入VPN软件是一种快速且相对经济的入手方法。顶不济可以采用利用处理器循环的纯软件VPN方案，增加用户数目则需要更多的循环。处理器不仅要负责它当前的事务，而且还要另外担负验证和加密的任务。

另一问题是有可能难以增加设备。随着VPN的流行，在系统上引来越来越多的用户，处理器为处理他们而被占满。临界期一般是在大量用户企图同时登录时出现，如在上午所有远程办公人员都要进行工作连接时出现。

作为一种评价工具并用来学习 VPN，基于软件的系统可能是一种经济的学习工具。如果你发现此系统存在不足，可以升级到硬件方案。

本书以后会讨论这个问题，附录C将给出一份供应商清单，其中有关于怎样用Web和普通邮件与他们联络的信息。

1.2.6 硬件方案

此方案与软件方案相反，它涉及那些提供VPN运作的承包商。他们的设备可以完全处理你的所有VPN需求。验证、加密及密钥管理、路由、内务处理以及登录等全都打包在一个装配紧密的部件中，将其插入即可。不过，你需要完成一些操作；例如，像所有设备一样，必须装载自己的操作参数并访问数据库。

有一件需要考虑的事情，就是作为这些承包设备的补偿，它们只需要很少的培训和维护，甚至不需要培训和维护。所必须的仅仅是偶尔监督一下。维护协议的花费可能比雇用一个员工的开销要小。

大多数多合一的(all in one)VPN 系统提供最小配置，在用户数目增多时还可以追加。例如，VPNet公司(1995 年在加利福尼亚的圣何塞创办)提供初始为1 000个用户，可升级到 2 000或5 000个用户。此公司说他们的系统“结合了基于标准的加密、验证、密钥管理以及压缩技术，对大型企业、中小规模的企业、分支机构和远程站点提供了VPN支持”。

1.2.7 混合搭配

另一方案是混合方法，其中IT管理人员增加某些设备处理VPN的部分工作，并将其中一些工作分配到现有硬件上。

不管怎样实现虚拟专用网，都应该用一种开放的思想和良好的方法进行工作。我们将在本书其余部分尽力帮助你作出最明智的选择。

1.3 展望

本书不对未来作过多的预测。我们只是详细分析了许多供应商并且评述(不披露其专利机

密)他们为迎接新千年作了什么准备。请抓牢你的帽子，这将是一次风驰电掣般的旅行。

正如前面所述，Internet最近一些年相当平静。虚拟专用网将改变这种情况。只需看看那些主要的电话服务商在干什么就会得到启示。

AT&T、MCI、Sprint、GTE、Atlantic Bell、Southwestern Bell 都正在积极采取行动。对他们以及其他传统的电话服务公司进行的投资不能视为等闲。全方位服务的VPNISP 今天已经出现，而明天它将会抓住越来越多的商机。

Novell、Microsoft 以及其他公司正向VPN市场投入新的和改进了的软件。明天将会出现处理更大通信量和更安全的软件。

今天，可以从Cisco、3Com、Fortress Technologies、Internet Dynamics、Assured Digital、VPNet Technologies 和其他公司那里购买VPN硬件。随着开发步调的加快，明天将会看到大量的风险资金投向更多的硬件公司。各种联盟与伙伴公司正在形成，以抢占VPN供应的制高点。

这种潮流正将虚拟专用网推向产业化发展的方向，就像汹涌的大海将波涛推向海岸一样，随着虚拟专用网的盛行，Internet将再次加速。保守的企业作为旁观者捞不到好处，而那些有眼光的企业将感到刺激与兴奋，会发起新的一轮冲刺。

1.3.1 增长情况

据 Internet 年鉴(www.i-i-a.com)，2000 年末将有3.27亿人使用Internet ，而1997年末只有1亿。美国计划2000年有1.39亿Internet用户，占总人口的 40%。这些数字包括企业、教育机构和在家上网者。

IIA(信息产业协会)不是唯一预测增长的研究机构。根据来自INTECO公司(www.inteco.com)的调查数据，7 600万用户能够在家中上网，5 100万用户在工作中访问Internet，2 200万从朋友或亲戚处访问，而2 400万从其他地方(如学校、图书馆或社区活动中心等)访问。此项调查还显示有39%的 Internet 用户年龄在18~34岁之间，而39%的用户年龄在35 ~ 49岁之间。

INTECO 在1998年12月采样了16 500户具有代表性的美国家庭，算出全国成年人中大约55%(1.8亿)的人在前30天内至少访问过一次 Internet。1998年12月的数据比 1998年3月的7 800万增加了38%，而较1997年9月的6 100万上升了 71%。

根据来自INTECO的另一个报告，PC家庭金融从1997年第三季度的380万上升到了 1998年末的700万。根据INTECO的高级财务服务分析员George Barto的观点，驱动连机金融迅速增长有两个因素，一个是访问Internet的美国家庭数目上升了68%(从1997年第三季度的220万上升到1998年末的3 700万)。另一因素是金融机构所采用的“建立它，他们就会来”的方法。

可从表1-1中看到这种增长的例子。其中数据来自位于加利福尼亚 Menlo Park 的 Network Wizards(www.nw.com)。他们自1990年就开始这项业务，专攻与计算机和通信有关的产品。该公司设计并销售独特的硬件和软件产品，或者是自己销售，或者通过转手商或OEM销售。

表1-1 1991年与1999年1月1日的前15个域名使用情况对照

域	类 别	1999	1991
com	商业	12140747	181361
net	网络	8856687	4109
edu	教育	5022815	243020
jp	日本	1687534	8579

(续)

域	类 别	1999	1991
us	美国	1562391	127
mil	美国军方	1510440	27492
uk	英国	1423804	18984
de	德国	1316893	31016
ca	加拿大	1119172	27052
au	澳大利亚	792351	31622
org	组织	744285	19117
gov	政府	651200	46463
nl	荷兰	564129	12770
fi	芬兰	546244	11994
fr	法国	488043	13011

1. 这与VPN有何关系

让我们来看看远程办公。位于纽约的研究和咨询公司FIND/SVP(www.findsvp.com)报告，到1999年1月为止，美国远程办公的人数仅在两年间就从850万上升到了1 100万，增长率大于15%。

“许多公司，或大或小，都发现允许员工部分时间在家工作很有好处，”指导此项研究的FIND/SVP的副总裁 Thomas E.Miller说道。“电子邮件、语音邮件以及 Internet 的增长，再加上重新强调工作成效而不是在工作场所的表现，已经使管理人员认识到，兼职的员工不会比在正式工作场所工作的员工差。最重要的事情是工作是否完成。”

FIND/SVP的调查表明，今天有35%的远程办公人员使用Internet ，包括在家有规律地使用Internet的31%的人员，总共有340万家庭用户。这个数字反映连接到办公室的远程办公人员的年平均增长率为50%还要多。

远程办公中心(Telecommuter Central，www.tcentral.com)报导提高了员工的生产效率和士气。他们还列举了容易招聘和保留人才等诸多好处。

员工是怎么看待远程办公的呢？远程办公中心说，人们都认为提高了个人的生产效率，减少了乘车上班的时间，提高了生活的质量。灵活的工作时间与灵活的管理很不错，反映了公司对员工的理解。

远程办公还减少了公司的营业成本；包括减少了设施维护和能源消耗。

1.3.2 Voice-Over Internet Protocol

Voice-Over Internet Protocol(VoIP)已经建立一种方法，即将推广。座落在宾夕法尼亚的一个名叫Voicenet的ISP，在Internet上为使用传统的本地和长距离呼叫电话的家庭和企业提供Internet 电话服务。

“Voicenet 通过提供这种利用最新 Internet 技术使打电话成本低质量高的革命性的新方法，已经改变了通信的面貌，” Voicenet公司的一个客户Dante Mattioni说道，“数字质量是很优越的，而且费用的节省也相当可观”。

在1999年1月Internet上召开的一个VoIP研讨会上，德州仪器的一位数字信号处理专家说，“VoIP仍然是一门新兴的技术，正处于市场开拓的早期阶段。但是由于其技术的先进性，软件

和硬件现在都允许在受控分组网上得到全面高质量的声音，我们看到公司或企业的客户表现出了极大的兴趣。”

Yankee Group(www.yankeegroup.com)对VoIP世界范围市场的预测是2002年达到16亿美元。这是基于1998年的1.93亿美元且1999年估计为3.1亿美元作出的预测。这些数据建立在从长途直拨服务变为本地拨入且VoIP可跨国的基础之上。

像Cisco(www.cisco.com)这样的硬件公司正在销售VoIP系统，并将它们的产品投向全美国。这表示 VoIP 与VPN相结合，作为一种并行的或集成的成份，将具有很大的市场价值。

1.4 本章小结

虚拟专用网并不是一种未来的东西，它已经有了。企业以及政府已经使用它们，而且每天都有更多的机构利用它进行连接。新的硬件与新的软件正在研制出来，正在现有设备中对其进行实现和制作。

VPN具有节省标准拨入成本的40%～80%的潜力，具体节省多少要视实现而定。作出是否使用它的正确决定是 IT 管理人员的职责。

在ARPA为最初的连网研究提供经费时，任何人也不会想到Internet会发展得如此之快。从1960年的4个用户发展到现在的1.5亿用户，几乎是每1.75秒就增加一个新用户。

Internet 上的商务活动在 2000 年时将会达到数十亿美元。

第2章　局域网概述

主要内容：

- 标准化及其影响
- 网络模型
- 协议组
- 网络传输介质
- 物理设备——硬件
- 逻辑设备——软件

本章将对局域网(LAN)进行讨论。有关广域网(WAN)的内容将在下一章介绍。

局域网是复杂的实体，对其所有内容进行详细的讨论不是本书的真正的目的。然而，有必要使每个人都了解一些适用于所有网络的基本原理。如果你是一位工作在技术支持服务岗位上的网络支持人员，并且感到自己所掌握的关于局域网如何工作的知识够用，则可以跳过本章直接进入第3章。另一方面，如果你感到这部分知识有某些欠缺，那么本章将有助于你填补这些空白。

2.1　LAN的概念

网络是用标准化组织(standards organzation)开发的协议进行定义的。首先来了解一下这些组织。为了简化标准各个过程的说明，标准化组织建立了模型(model)；我们将简略地了解由网络标准中的三种主要标准建立的LAN模型：

- ISO/OSI网络模型。
- IEEE 802委员会的网络模型。
- Internet协议组，它是在ARPA下进行开发的。

标准化组织确定用什么规则定义网络如何实现实体之间通信所需的过程。这些规则称为协议(protocol)，它们定义网络应何时、在哪里、为什么，最重要的是怎样执行它的给定的任务。协议通过硬件和软件的某种结合来实现。然后我们从协议到硬件，再从硬件到软件地进行分析，这是一个逻辑进程。

2.2　体系结构

今天，几乎所有出售的计算机都可配置在LAN上运行。更令人惊讶的是，大多数只有基本操作系统的廉价计算机都能够在一个小的工作组——LAN上很好地工作。但并不总是这样的。在早期的个人计算机中，每个制造商都根据自己的思路制造品牌机。由于每个人对PC概念的理解都不一致，企图用LAN将这些早期的机器连接起来会带来严重的问题，因此在这些机器之间信息共享几乎是不可能的。

这种情况的改变始于80年代初IBM PC的诞生。IBM在计算机工业中产生了如此大的力量，即在PC的体系结构发布后，几乎整个计算机工业都跟着效仿起来。这种情况一直延续下去，

直到IBM将体系结构改变为IBMPS2时，计算机工业才打算摆脱IBM的束缚。但到那时，IBM PC的体系结构实际上已经成为标准。

2.2.1 体系结构标准

PC产业共同认识到，如果打算在市场上获得成功，必须制造支持真标准而非只是事实上的(de facto)标准产品。因此，针对个人计算机，产生了工业标准结构(ISA)和扩展工业标准结构(EISA)。通过以标准结构制造计算机，与它们接口的其他产品有了成功的机会。这些标准不是偶然产生的；它们是经过了一个很长的咨询、调研和测试过程后开发出来的。

有两个标准化组织，一个是国际标准化组织，也就是著名的ISO，另一个是电气和电子工程师协会，即IEEE。IEEE主要建立电气和电子设备的标准。

尽管这两个组织建立了大量的设备及范围标准，但这里是他们已经正式通过的有关计算机网络的标准。ISO是一个国际化组织，由美国国家标准化组织(ANSI)全权代表。

还有其他一些标准化和相关的组织，它们在本行业方面的标准都不如ISO和IEEE颁布的重要。只在本书需要的地方进行介绍。

2.2.2 开放式标准——公共域

由各种组织建立的标准一般都成为公共域，或称开放式标准(open standards)。制造商可以生产与这些开放式标准相适应的产品，而不必付任何版税。

历史悠久的传输控制协议/网际协议(TCP/IP)就是开放式标准的例子。由于TCP/IP的开发是受美国国防部高级研究计划局(DARPA)资助的，而该组织是受税款资助的美国政府机构，因此该协议始终属于公众，即公共域(public domain)范畴。当DARPA完成资助后，TCP/IP由美国国防部发布并作为开放式标准使用。

关于开放式标准应注意到的是，一旦作为开放式标准被采用，制造商就可以设计和制造符合该标准的产品。因而，对于已经采用的标准的修改将遭到极大的反对。尽管所建议的修改是重大的改进，但是这种修改也将给生产部门带来极大的混乱。取而代之的是，当需要实现某个改进时，就采用一个全新的标准。该标准可以吸纳前一个版本的许多或全部特性，但尽管如此，它仍是一个单独的和完整的标准。这个规定允许设计人员和制造商在已有的产品上进行改进，而无须使已有的结构无效或作废。

2.2.3 事实上的标准

有时，某公司开发一个产品，该产品或者是获得专利权或版权的，或者由于某种原因决定保持在公司所有权范围内的。当这样的产品由于受到市场广泛接受和良好的销售而获得巨大成功时，它就会成为事实上的标准。微软的Windows操作系统就是一个例子，另外Novell的Net Ware网络操作系统也是如此。

但是，事实上的标准都存在着缺陷和问题。假定ABC公司依据XYZ公司建立的事实上的标准开发了一个新的和已有技术组成的部件。XYZ公司将依据专利法向ABC公司征收使用费，毕竟XYZ公司为建立该标准花费了工程费用和生产力。而ABC公司几乎在任何情况下都将许可使用费加到最终用户的头上。结果如何？增加了顾客的成本。

事实上的标准所引起的另一个问题是，XYZ拥有在任何时候修改其产品设计的自由。如

果采用事实上的标准的产品被广泛地使用并支配该项技术，则除了紧跟这种变化以及购买新的软硬件升级版来保持技术的领先或至少保持竞争力外，最终用户没有别的选择。

并非所有的事实上的标准最后都是成功的。IBM发现当它决定停止制造具有开放式结构的IBM-PC，并开始制造有微通道结构的IBM-PS2时失败了，公众拒绝微通道的结构。分析家认为PS2缺乏成功的原因最终是由于成本的增加，其中一些就是专利使用费。

2.3 网络模型

为了简化包含在定义网络中的复杂性，标准化组织建立了称为模型(model)的图表。这些模型以逻辑方法定义网络系统的结构。ISO和IEEE都对网络模型进行了开发。但是，这两个模型完全不同并且不能覆盖网络结构的相同范围。

2.3.1 计算机网络的OSI模型

70年代中期，几个大型计算机厂商，包括IBM、美国数字设备公司(DEC)公司，都已开发出了支持上百个用户的大型计算机。每个大型计算机制造商都有其优势和弱势。

在这种环境中，每个公司的计算机结构都被看做是一个虚拟的网络系统；只有一个中央处理器，但它可为多用户服务。每个制造商都有属于自己的结构，并且每个结构都是其制造商的专利。

对于只购买单一制造商产品的企业公司来说，上述情况没有什么问题。但是，另一方面，如果某公司想要购买两个以上制造商的产品以便利用其优势，则信息技术管理人员试图在不同的组成之间传递数据时将会遇到某些问题。

这些问题导致了几个组织的形成，这些组织的共同目标是建立在不同的计算机系统之间进行接口的标准。这些组织包括：

- 国际电信同盟(ITU)。
- 电气和电子工程师协会(IEEE)802委员会。
- 电子工业联合会(EIA)。
- 国际标准化组织(ISO)。

在这里，先快速浏览他们的成果以及不同组织间是如何相互影响的。然后，通过全书，将了解这些机构之间的密切合作关系。

为了减少由不兼容引起的连接性问题的另一项努力是，ISO在70年代末成立了一个小组委员会，以开发多厂商间互操作性的数据通讯标准。

与此同时，IBM成为大型计算机工业的重要的计算机制造商。在这个计算机发展时期，蓝色巨人(IBM的绰号)发布了它首选的系统网络构架(Systems Network Architecture)，这就是贯穿该行业的著名的SNA(见图2-1)。目前，SNA结构在全球范围内依然是有效的。

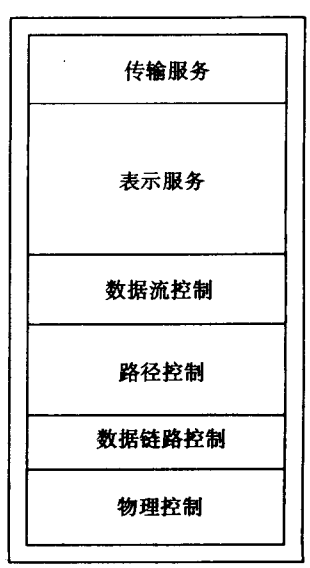

图2-1 IBM的系统网络构架模型

ISO小组委员会继续朝着网络连接开放式标准的最终发展进行努力，在1984年发布了开放式系统互连(Open Systems