HZ BOOKS

Cisco专业技术丛书

Implementing Cisco VPNs: A Hands-On Guide

实现 Cisco VPN 实践指南

(美) Adam Quiggle 著
云舟工作室 译

机械工业出版社
China Machine Press
Mc Graw Hill Education

Cisco专业技术丛书

实现Cisco VPN实践指南

（美） Adam Quiggle 著
云舟工作室 译

机械工业出版社
China Machine Press

本书全面讲述了使用具有加密手段的VPN(虚拟专用网)在公用设施上安全地进行各种数据传输的技术。主要内容包括CBco(VPN)概论，拨号的Windows支持，通过Cisco路由器拨号，VPN安全性入门，GRE和CET等。本书内容深入浅出，细致周到，实例丰富，适合实现VPN的网络设计人员和网络工程师，以及想要通过CCIE考试的人员参考。

本书版权登记号：图字：01-2001-3953

图书在版编目(CIP)数据

实现Cisco VPN实践指南/(美)奇歌(Quiggle,A.)著；云舟工作室译．－北京：机械工业出版社，2001.10

(Cisco专业技术丛书)

书名原文：Implementing Cisco VPNs : A Hands-On Guide

ISBN 7-111-09339-9

Ⅰ.实… Ⅱ.①奇…②云… Ⅲ.虚拟网络－通信技术 Ⅳ.TN915.5

中国版本图书馆CIP数据核字(2001)第065378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：张鸿斌 许 萍

北京忠信诚胶印厂印刷·新华书店北京发行所发行

2001年10月第1版第1次印刷

787mm×1092mm 1/16·25.25印张

印数：0001-5000册

定价：43.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

译 者 序

随着网络技术的不断发展以及网络互连环境不断复杂化，人们对其应用的需求也在不断地提高，这尤其体现在安全地进行IP传输方面。本书所讲述的VPN(虚拟专用网)就可通过加密手段，在公用TCP/IP上安全地进行IP传输。

Cisco的端到端硬件和Cisco IOS软件互联产品为在公用设施上传输保密数据、QoS、支持宽带数据的可行性以及网络管理提供了成熟的安全保障。本书共分为9章和5个附录，其中，第1章“Cisco虚拟专用网概论”介绍了VPN的简明定义及其基本原理；第2章“拨号的Windows支持”，介绍了如何使用由Microsoft提供的标准工具来设置远距离工作人员/移动用户的计算机，从而建立拨号连接；第3章“通过Cisco路由器拨号”，介绍了用来支持拨号环境的电路转换技术(物理层)以及封装方法(数据链路层)；第4章“VPN安全性入门”，介绍了使数据更加安全所需的因素、需要防止的常见袭击类型，以及使得数据在Internet中传递时更加安全的技术；第5章“GRE和CET”，介绍使用通用路由封装(Generic Routing Encapsulation, GRE)隧道和Cisco加密技术(Cisco Encryption Technology,CET)来设置伪VPN强制隧道的内容；第6章“IPSec”,介绍IPSec服务；第7章“PPTP”，介绍一种主动隧道VPN技术——PPTP；第8章“L2TP”，介绍另外一种VPN技术——L2TP；第9章“PIX防火墙VPN”，介绍如何配置PIX防火墙，以便使得它能够支持IPSec以及PPTP；附录A～C分别列出了VPN协议比较、命令和Cisco 2000/2500/3000/4000以及7000系列路由器口令恢复；附录D列出了本书使用的词汇表；附录E列出了本书所使用的参考书目。

本书主要适合实现VPN的网络设计人员和网络工程师，而且它还是那些想要通过CCIE考试的人员的最佳选择。

本书由云舟工作室组织翻译，韦菲菲、丘博、包岩、张益革、田芳芳、许文静等人承担了主要翻译工作，另外，方雪斌、陈薇、蔡翔元等同志也参加了部分翻译和校对工作。由于译者水平所限，书中难免有误解和疏漏之处，恳请广大读者批评指正，以帮助我们改进翻译的水平。

2001年7月

目　录

第1章 Cisco虚拟专用网概论

在当今世界上，交换信息已是司空见惯的事。要想通过计算机进行信息交换，需要进行网络连接。在最近10年里，计算工业的局域网（Local Area Network，LAN）和广域网（Wide Area Network，WAN）的网络产品数量增长飞快。

各种机构的可用信息来源不再局限于自身的集体网络，取而代之的是他们对因特网上无穷无尽的信息源进行访问。因此，因特网成为集体网络的一个巨大的延伸。既然各个企业已经对使用因特网来交换非机密数据的观念很适应，他们就会考虑使用因特网来传送高度机密的内部资料。为什么？与其他任何企业一样，他们希望自身富于竞争性。通过将杠杆作用应用于因特网的巨大的基础结构，企业可以减少接到远程站点甚至商业合作伙伴的专用线路的相关费用。

可惜的是对于商业来说，在因特网上所运行的协议通常都不太安全。记住，因特网上的最大用户是综合大学而不是商业组织，在那里信息和思想能进行自由交换，不存在如大型企业所要求的安全性。

在本章中我们将给出虚拟专用网（Virtual Private Network，VPN）的简明定义，说明虚拟专用网的基本原理，定义在本书的后续部分一直使用的这个术语。在阅读本书之前，需要完成这3个重要任务。否则，既使开始你认为这些不必完成，但后来还是会觉得实际上应该完成。

1.1 谁应该阅读本书

本书的主要读者是要实现VPN的网络设计人员和网络工程师。然而，随着近年来在Cisco认证网络专家（Cisco Certified Internetwork Expert，CCIE）路由和交换实验室中包含了Internet安全性协议（IPSec）部分，以及在Cisco认证网络专家服务提供者实验室中包含了第二层隧道协议（L2TP）部分，我们希望Cisco认证网络专家的报考者也可以使用本书作为参考资料。

如果你已经拿起本书，那么无疑已理解了安全的重要性。因此，你不会觉得安全部门或商情讨论为什么需要拥有VPN是一件很有趣味的事。这并不意味着在实现VPN前不需要完成别的工作。事实上，在实现任何VPN前，应该对解决方案有一个完整的商情理解，该解决方案应该包括规定可接受风险的良好的安全策略，以及对需要保持机密的业务流说明文档的理解。

本书并不是建立VPN的根据，也不是决定好的安全策略的依据。假定读者已经完成其他工作并了解所要解决的问题，现在想知道的是如何解决问题。本书的特点是“具有针对性”。你会看到VPN的不同类型及其使用的场合。

因此，读者可能会想“在读此书之前需要知道些什么？”。早在写本书时，作者就决定只讨论与VPN相关的主题，而不考虑OSI模型、Cisco构造基础、TCP/IP基本原理以及IP路由。由于已经有许多相当不错的书深入地研究了这些主题，因此本书就不需要包含跟网络专业基础相关的内容，而只是将重点放在VPN的实现方面以及注意事项上。但是，如果需要复习其中的个别主题，请参看优秀参考资料列表中列出的参考书目。

注意 对于熟悉Cisco认证途径的读者来说，Cisco认证网络专业人员（Cisco Certified Network Professional，CCNP）——特别是构建Cisco远程接入网络（Building Cisco Remote Access Network）考试中列出的目标）——对阅读本书很有帮助。这并不意味着要理解本书，你必须先要通过构建Cisco远程接入网络(BCRAN)考试，它只是作为本书的推荐入门资料而已。

1.2 章节简介

为了便于整体上更好地理解VPN，本书分为两部分：

- VPN入门。
- VPN案例研究。

VPN入门这部分是为了能更好地理解构建CiscoVPN的基本原理，例如基本的加密原理以及如何在Cisco硬件和不同的Windows平台上配置拨号服务。VPN案例研究这部分向读者介绍不同的VPN协议，给出各种格式的详细解释，指出如何在Cisco硬件上进行配置，并为读者实际操作新掌握的知识提供了一个案例研究。

1.2.1 VPN简介

这些章节有助于理解那些支持VPN的组件。虽然本书已经假设读者知道如何在Cisco路由器上配置IP地址，但假设读者不知道如何在Cisco路由器上配置综合业务数字网（ISDN），也不理解密码术和加密之间的不同之处。这些章节将给出了理解VPN案例研究所需要的知识。

1. 第1章——CiscoVPN实现简介

本章为读者提供了本书使用的术语。由于那些声称其产品是VPN的卖主，其天花乱坠的广告和狂热已经在市场上造成许多混乱，因此第1章包含以下内容：

- VPN的定义。
- 什么不是VPN。
- VPN的分类。
- VPN的基本组件。
- 什么时候不需配置VPN。

通常人们认为书本的第1章不是很重要，但对于不熟悉VPN术语的人来说，本书的第1章是必读的。

2. 第2章——拨号的Windows支持

通常VPN强制隧道需要对客户机进行配置，以便支持标准的点对点协议（PPP）连接。本章的重点放在3个不同的Microsoft操作系统上：Windows 95、Windows NT和 Windows2000。每一部分都将重点放在每个操作系统的点对点协议（Point-to-Point Protocol，PPP）配置方面。熟悉MS-Windows的读者可以跳过这个部分。

3. 第3章——通过Cisco路由器拨号

本章回顾了拨号所需的各种设备。与第2章相似，由于VPN主动隧道利用了拨号特征的重要部分，我们应该知道如何配置Cisco路由器，使之能支持拨号接入（简易老式电话服务（POST）

和综合业务数字网（ISDN）接入）。

4. 第4章——VPN安全性入门

本章主要将重点放在案例研究所需的概念和配置命令。深入地讨论了加密、密码术，以及鉴别、授权及账户处理（AAA），便于读者理解后续章节中的知识。

1.2.2 VPN案例研究

这些章节对知识进行了深入说明，它们除了有可靠的知识基础外，还对技术进行了深入的说明。每一章都有技术概论包含基本原理因特网标准和每种技术后的相关概念。读者可以看到如何使用Cisco设备来实现VPN。最后还提供了3个案例研究，让读者可以对知识有一个更好的理解。

1. 第5章——GRE和CET

使用通用路由封装（Generic Routing Encapsulation，GRE）隧道以及在Cisco路由器上的有效载荷加密可以创建伪VPN，即使并没有一致认为它是VPN的一种。另外，对隧道技术基本原理的了解有利于更好地理解这些基本原理和领悟其他章节。

2. 第6章——IPSec

本章讲述Internet安全性协议(Ipsec)的历史，并说明它与VPN协议之间的根本区别。利用第4章中学到的知识，便于了解其基本构成。本章还对配置Internet安全性协议时每个命令的使用方法和使用原因进行了说明。

3. 第7章——PPTP

本章的重点是由某个集团（Microsoft领导下）开发的VPN协议PPTP。第7章讨论了PPTP的很多优缺点。虽然你不用知道如何将Microsoft Windows NT Server作为VPN服务器来配置传统的PPTP VPN，你将会看到Cisco最新的一项VPN线路新增功能，并学习如何将Cisco路由器配置为PPTP VPN服务器。

4. 第8章——L2TP

VPN协议的最后内容是L2TP。L2TP利用来源于PPTP以及L2F的最优秀技术，来提供非常实用的VPN协议。我们将说明在L2TPF如何配置Cisco硬件。

5. 第9章——PIX防火墙VPN

本章中，我们不想研究新的VPN协议，但是将学习在PIX防火墙上如何配置点对点隧道协议和Internet安全性协议。另外，我们还会学习一些PIX命令，这样就可以在PIX防火墙上配置Ipsec和PPTP了。本章并不讲述配置PIX防火墙的所有知识——只介绍为支持VPN，配置PIX防火墙的一些必要命令。

1.3 什么是VPN

最近几年来，VPN这个术语已经广为流传，成为最新的时髦话。许多公司试图介入这种最新、最伟大的技术。可惜的是，其结果是迷惑或误导了那些做出决定的领导。

VPN试图利用公用网和专用网的所有优势。公用网络的优点是它拥有一个共享的环境，与建立私有的国际网络相比较其费用相对要低一些。专用网的优点在于它很安全。由于它是私有

的网络，可以控制对它的访问。

1.3.1 VPN定义

要理解本书使用的VPN的定义，就要将首字母缩写词分解为几个基本的组成部分。第一个词“虚拟”在韦氏词典中定义为“具有特定物理功效的”。在这种情况下，“虚拟”指的是经由公用网的两个远程节点之间的动态连接，如图1-1所示。这个“虚拟”连接赋予了两个路由器之间的逻辑连接。

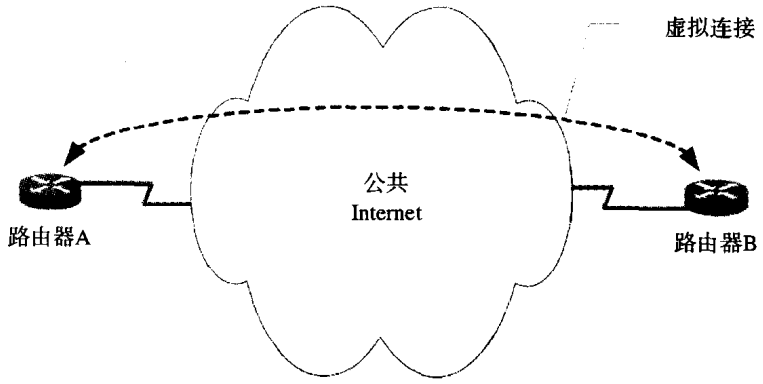

图1-1　通过网络的虚拟连接

第二个词“专用”在韦氏词典中定义为“仅限特定的人或组织使用”。VPN的这个方面通常是通过鉴别和加密这两个组件实现的。

鉴别是标识个体或节点的过程，通常在访问网络以及由网络提供的各种服务之前完成。加密是转换信息实体的一种方式，其目的是隐藏原有的含义。图1-2表明没有经过数据加密的消息是以明文的形式传送的。对消息进行数据加密后，消息不可读，除非你知道如何进行解密。

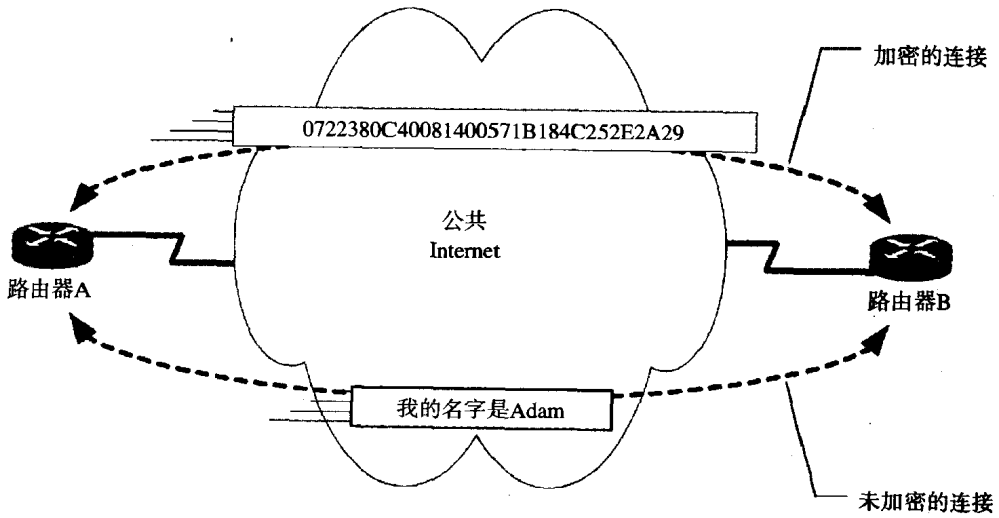

图1-2　经过加密和解密的数据通过网络的实例

最后一个词“网络”在韦氏词典中定义为“由通信线路进行连接的计算机、终端以及数据库组成的系统”。这是VPN最基础也是最明显的方面。网络使得计算机能够通过不同的媒介进行沟通。

1.3.2 什么不是VPN

给出了这些宽范围的定义后，为了理解本书，接下来是有关什么不是VPN，或至少不能看做是VPN解决方案。

点到点连接：一些人主张专用点到点连接可以看做是一种VPN。考虑到租用线路基础设施使用多路复用器对多用户物理层数据进行组合，并通过公共长距离线路传送。用户物理层信号随即多路分解，并通过用户本地回路传送到用户路由器中。虽然你可以明确地将这个范例看做是数据使用了共享的公共基础设施，但根本不具备虚拟的特征。

分组交换连接：另一些人主张应该将帧中继看做是一种VPN。毕竟可以认为帧中继是一种公共基础结构。并且当使用帧中继时，用户数据链路层帧会被封装到单元转换业务中，并通过帧中继群进行传送。一旦单元达到远程帧转换器，就会将单元重组以形成原来的帧，然后传送到用户本地回路。虽然这几种服务类型可以用来构建专用内联网，但是它们仍缺少前面标识的能使VPN保密的一个成分：加密。另外，由于这个过程包含的是数据链路层而非网络层，因此不需要防火墙来避免帧中继用户数据网受到另一个连接用户的攻击。

1.4 VPN的类别

现在已经了解了本书中使用的VPN的定义，再来看一看VPN所属的不同类别。记住这些分类都是通用的定义，这一点是很重要的。所拥有的基础结构和所要解决的问题决定了对VPN类型的选择。

注意 虽然作者在本节没有定义商业术语，但是本书的目的之一是促使你思考此类可以用VPN解决的问题。

通常使用的5种VPN类型为：远程访问VPN、内联网VPN、外联网VPN、增强的Voice/IP VPN和企业VPN。

1.4.1 远程访问VPN

远程访问VPN为那些通过因特网服务供应商（Internet Service Provider，ISP）并主要连接到公司网络的远程用户提供连接。企业可以通过向ISP购买远程访问基础设备来实现费用的精简。无论是远程工作人员还是交警都可以从这些类型的VPN中受益。

1.4.2 内联网VPN

通过在因特网上为某个组织的远程站点提供站到站的连接，可以降低企业在广域网上的费用。使用内联网VPN的优点在于安装它们很容易，其缺点是当使用因特网时，服务水平得不到保证。

1.4.3 外联网VPN

外联网与内联网基本上相同，只是封装节点通常是商业合伙人，而不属于同一个机构。虽然从技术上讲，解决方案是一样的，但是内联网VPN和外联网VPN之间的主要区别在于安全性。例如，虽然外联网允许职工浏览网络资源，但它可能不想让商业合伙人也能进行此类访问。

1.4.4 增强的Voice/IPVPN

增强的Voice/IP VPN支持安全的因特网电话。这与因特网VPN相似，除了因特网封装的是经过加密的语音而不是经过加密的数据之外。

1.4.5 企业VPN

企业VPN在公共Internet上安全地支持语音和数据应用程序的收敛性。他们将数据VPN（通常只是内联网VPN）与语音VPN结合起来。

本书并没有将重点放在语音技术上，因此同样也不将重点放在增强的Voice/IPVPN或者企业VPN上。要想知道这几种VPN的更多信息，请参考Robert Caputo所著的《Cisco Packetized Voice & Data Integration》这本相当出色的书。

1.5 VPN隧道的类型

图1-1显示了两个设备之间的逻辑连接。这种逻辑连接称为隧道，它提供了VPN的“虚拟”组件。“VPN隧道类型”这个短语指3种设备之间的隧道类型：VPN用户、VPN启动器和VPN服务器。

注意 这一部分详细说明了本书中所使用的术语。在一些例子中所使用的不一定是广泛使用的术语。但是，描述得越准确，这些术语越明确，这样就能更清晰地理解。在前面的段落中，VPN客户这个术语可以用来描述VPN启动器和VPN用户。在特定的例子中可能行得通，但是指示不明会造成对所讨论对象辨别不清。例如，当VPN客户的职责是拆分，就像强制隧道（请参看本章后面与强制隧道有关的部分）中那样，读者可能很难理解讨论的到底是哪些设备。

下面看一看3种设备构造中使用的两种不同类型的VPN隧道：主动隧道和强制隧道。

1.5.1 主动隧道

主动隧道要求用户能够管理本身的VPN隧道，如图1-3所示。在这种情况下，当数据流向企业通信网时，通过客户建立的隧道进行路由。

这个范例的优点在于VPN用户同样是VPN启动器，从而允许接入因特网的VPN用户建立VPN。因特网的连接也可以通过多种不同的业务，如本地拨号ISP、x类数字用户线（x-Type Digital Subscriber Line，xDSL）业务、电缆调制解调器连接，甚至于通过商业合伙人。这种配置对机动的劳动力特别有利。另一个优势在于VPN服务器不一定要有一个路由器，如图1-3所示。VPN服务器可以很容易地成为网路服务器B或工作站B。

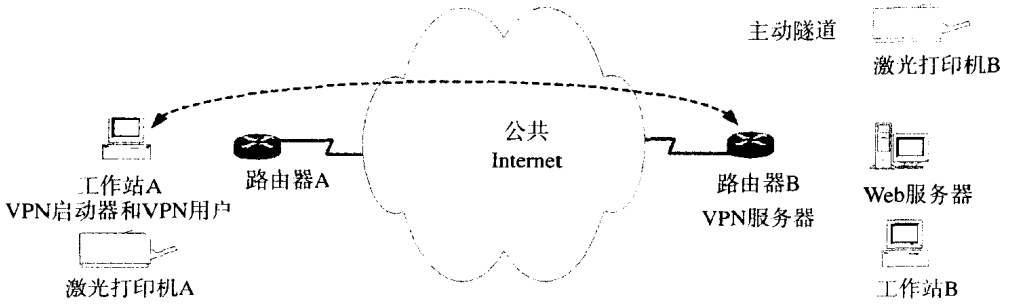

图1-3 使用主动隧道的虚拟专用拨号网

注意 拥有因特网连接不一定就够了。如果在企业通信网之间有防火墙，要通过企业通信网进行连接时就必须要重新设置防火墙。

由于这些隧道是动态的，一旦管理员建立起VPN服务器，VPN启动器就负责建立隧道。你可能认为这个范例与远程访问服务器（Remote Access Server，RAS）类似，在远程访问服务器中客户可以拨号连接到网络上。VPN服务器管理员唯一需要注意的事是，除了排除与VPN启动器的连接故障外，还要确认VPN服务器的硬件容量是否足够大。

注意 许多Cisco路由器可以作为VPN服务器使用。本书提到的VPN服务器包括通过Cisco因特网操作系统(IOS)来支持VPN的VPN服务器。但是所说的Cisco路由器不一定指VPN服务器。这是需要阐明的重要而微妙的一个区别。

由于对于每个优点都有其不利的一面，隧道的缺点在于用户计算机必须安装特殊的软件，以便管理自身的VPN。这使得配置过程相当繁琐，特别是当要将此服务加入已经配置好了的便携式电脑时。这是因为VPN客户需要在操作系统中安营扎寨，而这会与用户机器上已经存在的服务发生冲突。加之在配置之前不能对所有可能的情况进行测试，你应该有对付延迟转出，或更糟的停止转出情况的方法。当配置主动隧道时，新客户机的配置应该加以考虑。这样能在配置之前给IT组进行彻底检验配置的机会，以减少对使用主动隧道转出的VPN支持程序的调用。

主动隧道经常与远程访问VPN共同使用。因为移动用户不可能知道网络连接的来源，所以有了机动的劳动力对他们来说特别有用。主动隧道对于远程工作人员也有帮助，特别是对不属于同一地域的人员来说。允许远程工作人员使用ISP能节省直接拨号访问企业通信网时的长途费用。虽然主动隧道通常不与其他VPN类型进行配置，但是可以将主动隧道配置成为外联网VPN。

使用主动隧道的另一大显著优点在于通常可以相当快地对其进行配置。在组织管理严密的应用程序或业务需要的情况下，如图1-4所示，建立主动隧道可能会更好。

这并非因为主动隧道所需要的组件能设置的更快（此种情况较罕见），而是因为减少了有关人员人数的缘故。在外联网VPN中进行短期项目或基础设施不支持VPN的这两种情况下，主动隧道可能是最合适的解决方案。

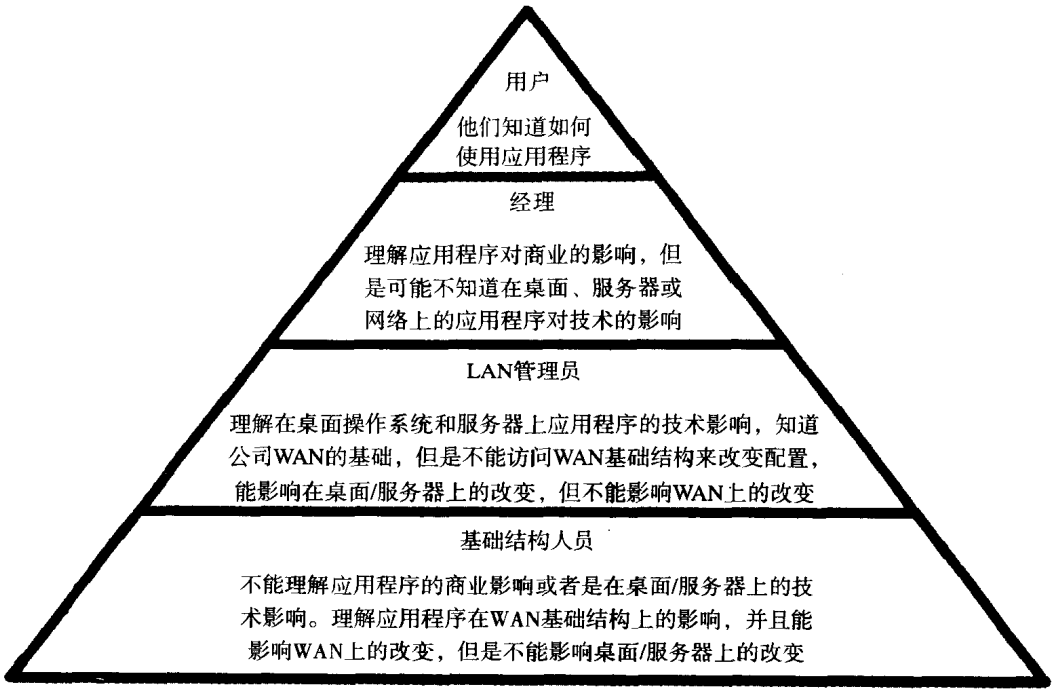

图1-4 从技术观点考虑的商业层

1.5.2 强制隧道

强制隧道通常称为命令隧道，对终端用户是完全透明。图1-5给出了使用强制隧道的VPN实例。在该例中，连接到路由器A的资源（工作站A、电子邮件服务器，以及激光打印机A）需要使用隧道来访问连接到路由器B的资源（工作站B、网络服务器，以及激光打印机B）。这种隧道需要路由器A的管理员和路由器B的管理员进行合作。

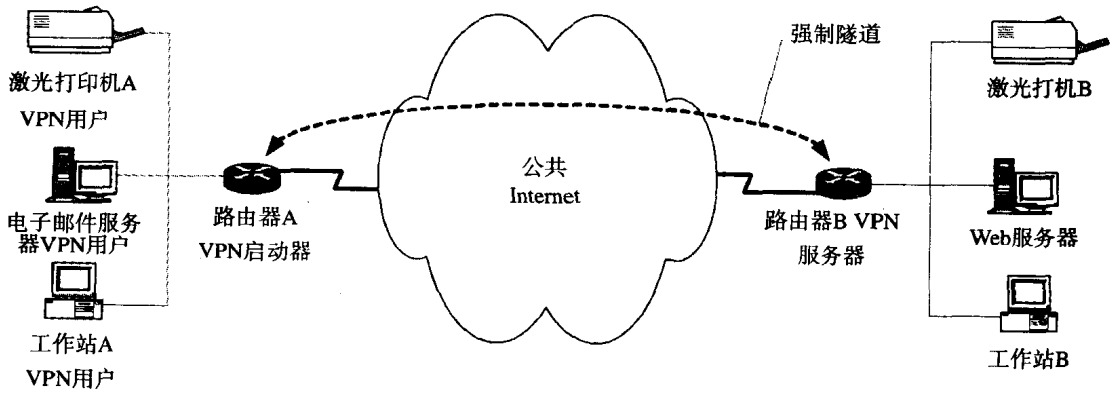

图1-5 使用强制隧道的VPN

强制隧道的优点是，要使用此种VPN，网络双方不需要进行任何重新配置或拥有特定的软件。这对于没有VPN软件的设备（例如打印机或较低版本的操作系统）来说，具有显著的优点。

缺点是配置新隧道时需要更多的时间。这是因为与主动隧道不同，强制隧道必须要对每个新隧道进行配置。

这种隧道通常与5种不同类型的VPN共同使用：远程访问VPN、内联网VPN、外联网VPN、语音VPN以及企业VPN。但是，当和远程访问VPN共用时，它的基础设施稍有不同。当使用强制隧道和远程访问VPN时，ISP和办公室之间必须共同协作。如图1-6所示，VPN用户连接到本地ISP，同时本地ISP从路由器A（VPN启动器）到路由器B（VPN服务器）中穿过连接。

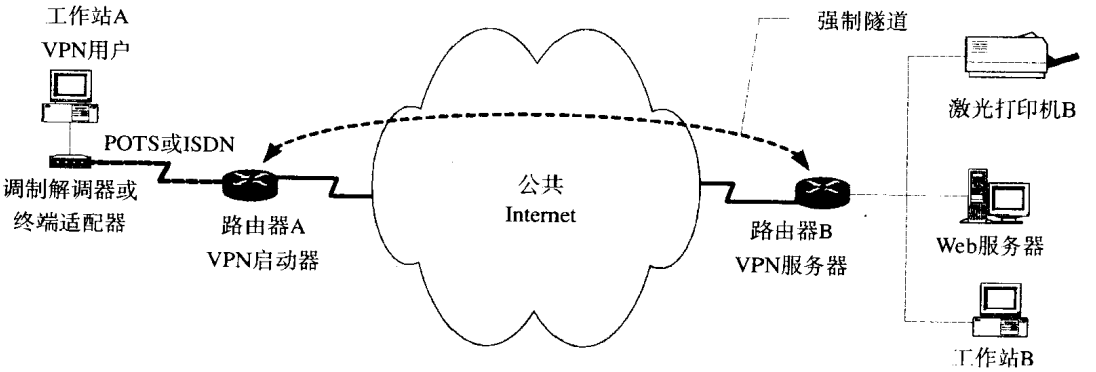

图1-6 使用强制隧道的远程访问VPN

在这里，路由器B负责分配IP地址以及支持拨号连接所需要的任何其他属性。这样，VPN用户就可以直接拨号访问路由器B了。

这个方法的优点是不需要对客户机进行配置。只要客户能使用相同的ISP,将通信费用控制到最低，这倒是一个很大的优点。

与其他隧道不同，多个拨号客户可以共享远程访问强制隧道。当另外一个用户拨号接入图1-6所示的ISP时，不需要建立一个新隧道。新用户的数据可通过现有的隧道进行传送。由于多个用户可以同时使用同一个隧道，这样在隧道的最终用户断开之前，隧道都不会中止。

广泛使用强制隧道的潜在问题是所有信息的封装完全没有区别（这会产生额外的管理费用）。图1-7给出了更糟的情况，即工作站A需要远程登录到路由器A上的情况。

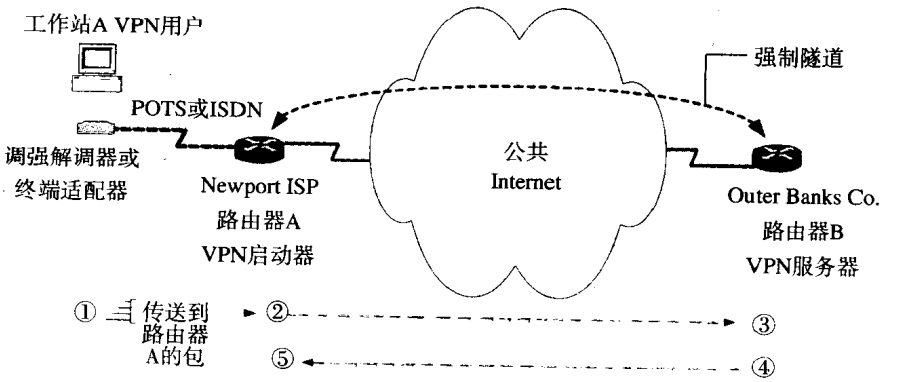

图1-7 不好的VPN设计例子