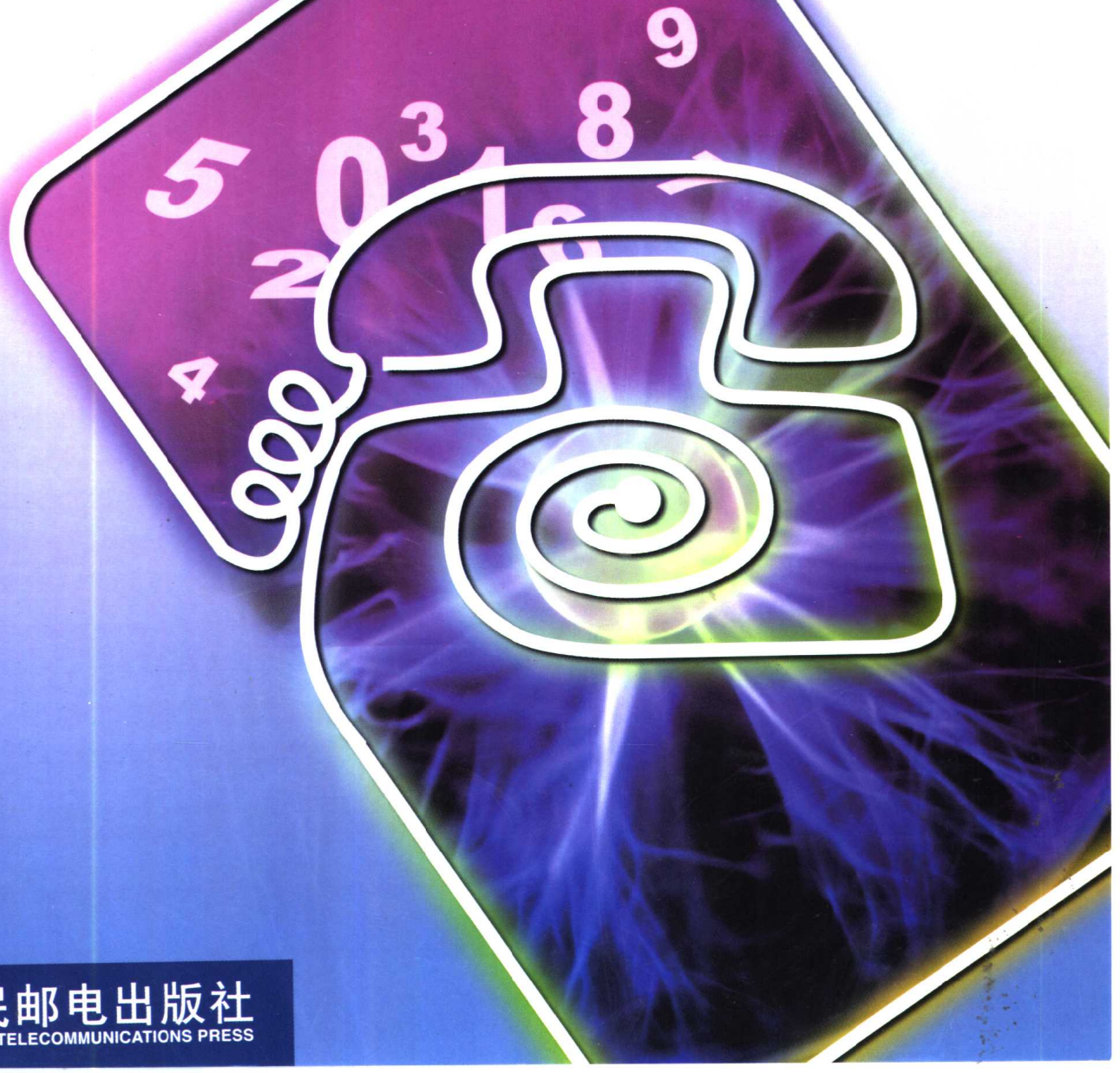
现代IP技术丛书

MODERN IP TECHNOLOGY

IP虚拟专用网技术

何宝宏 编著



人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

现代 IP 技术丛书

IP 虚拟专用网技术

何宝宏　编著

人民邮电出版社

图书在版编目（**CIP**）数据

IP 虚拟专用网技术/何宝宏编著. —北京：人民邮电出版社，2002.4
(现代 IP 技术丛书)
ISBN 7-115-10206-6

Ⅰ.I… Ⅱ.何… Ⅲ. ①虚拟网络—通信技术②计算机网络—通信协议 Ⅳ.TN915.5

中国版本图书馆 CIP 数据核字（2002）第 012629 号

内 容 提 要

本书依据国内外相关的标准，并结合国内外研究和运用 IP 虚拟专用网（VPN）的情况，介绍了 IP VPN 的优势、特点、相关协议以及组网等，使读者能够系统地了解 IP VPN 技术原理与应用。

本书重点内容包括 IP VPN 的概念与类型、技术要求与组成、L2TP 隧道协议与远程接入 VPN、IPSec 隧道协议与组网、MPLS 隧道协议与组网，以及运营商如何开展 IP VPN 等，基本上覆盖了 IP VPN 的各个领域以及目前最新的研究成果。

本书注重原理性说明，力求具有理论性、实用性和系统性，适合通信工程领域的广大技术人员和大中专院校的师生阅读，也可供希望了解 IP VPN 知识的人员参考。

现代 IP 技术丛书

IP 虚拟专用网技术

◆ 编　　著　何宝宏
责任编辑　陈万寿

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www. ptpress.com.cn
读者热线　010-67180876
北京汉魂图文设计有限公司制作
北京顺义向阳胶印厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：16.25
字数：384 千字　　2002 年 4 月第 1 版
印数：1-5 000 册　　2002 年 4 月北京第 1 次印刷

ISBN 7-115-10206-6/TN・1855

定价：28.00 元

前　言

IP VPN 是指通过开放的 IP 网络建立私有数据传输通道，将远程的分支办公室、商业伙伴、移动办公人员等连接起来的一种专用网络技术。IP VPN 具有性能/价格优势和灵活性等优势，因此具有巨大的市场潜力。2001 年 Forrester Research 的研究报告指出，它所调查的用户有 55%计划建立 IP VPN，到 2002 年全球将有 90%的公司运用 IP VPN 连接其远程用户和分支机构。美国通信杂志将 IP VPN 技术评选为 2001 年的十大热门技术之一。我国的信息产业部已经将 IP VPN 业务明确定义为一种电信增值业务，向社会开放。

对企业而言，IP VPN 可以替代传统租用线来连接计算机或局域网，也可以提供传统租用线的备份、冗余和峰值负载分担等。研究表明，在国内分支机构间使用 IP VPN 能够为企业节约 20%～40%的通信费用；把远程办公室通过 IP VPN 连接起来可以节省 60%～80%的长途通信费用和交通费；跨国公司使用 IP VPN 节省的国际通信费用的比例会更高。另外，在 IP 网上组建 VPN 可能也就仅几分钟的事情，而传统的租用线和帧中继业务的建立则需要几天甚至几个星期的时间。

就服务供应商而言，IP VPN 是其未来数年内保持竞争力的重要法码。随着 IP VPN 的广泛运用，服务提供商有了商机来增加收入，扩大业务范围。在国外，IP VPN 业务发展很快，很多大型的运营商都已经推出了此项业务，使得其 IP 资源得到进一步增值，获得了更高的利润。在国内，到 2001 年底，中国网通和中国电信已经推出了此项业务，其它很多大型和小型运营商正在做研究、测试和实验等的准备工作，计划在不久的将来开展此项业务。

本书共分 9 章。第 1 章概要介绍了 IP VPN 的起源、历史、类型和应用等。第 2 章重点介绍组建 IP VPN 的核心——隧道机制的基本概念和典型的隧道协议。第 3 章介绍使用隧道协议组建 IP VPN 的通用模型和体系结构等。第 4 章和第 5 章分别介绍了 VPN 的两个重要基石——服务质量(QoS)和安全技术。第 6 章介绍了隧道协议 L2TP 以及远程接入 VPN。第 7 章介绍了隧道协议 IPSec 以及基于 IPSec 组建 VPN 的方法。第 8 章介绍隧道协议 MPLS 以及基于 MPLS 的 VPN 组网技术。第 9 章介绍运营商组建 VPN 的技术。

参与本书编写的人员分别来自信息产业部电信传输研究所、深圳华为技术有限公司、中国移动通信集团等，这些单位有的是权威的标准研究机构，有的是国内知名的运营商或设备制造商，具有很强的技术实力。本书主要由何宝宏执笔，参加编写的还有张宝峰、田辉、袁琦、吴江等，他们有的参与了中国 IP VPN(系列)标准的制订工作，有的参与了有关 IP VPN 政府管制政策的研究等，他们为本书的问世付出了大量的心血，在此一并表示感谢。

由于 IP VPN 技术目前还在快速发展中，加之作者水平有限，书中难免有不妥甚至错误之处，希望读者不吝赐教。

何宝宏

2002 年 1 月 1 日

目　录

第 1 章　VPN 综述

VPN 是虚拟专用网(Virtual Private Network)的缩写，是从专用网业务发展而来的，用以替代专用网的一种广域网(WAN)技术。而 IP VPN 是 VPN 的一种，是指通过开放的 IP 网络建立专用数据传输通道，将远程的分支办公室、商业伙伴、移动办公人员等连接起来的一种网络。同样地，可以把基于异步传输模式(ATM)组建的虚拟专用网称为 ATM VPN，把基于帧中继(Frame Relay)组建的虚拟专用网称为 FR VPN。

随着 IP VPN 技术的日趋成熟，越来越多的用户和运营商都将目光转向了这种极具竞争力和市场前景的 VPN。对企业而言，IP VPN 可以替代租用线(无论是物理的或 ATM/FR 虚电路)来连接计算机或局域网(LAN)，也可以提供租用线的备份、冗余和峰值负载分担等。IP VPN 的采用会明显降低组网和运行费用。另外，与传统的租用线和 ATM/FR VPN 相比，在 IP 网上组建 VPN 也非常快捷。

本章是对 VPN 技术的一个概要介绍，目的是能够使读者对 VPN 有一个直观的感觉，便于学习后面的章节。本章首先介绍了什么是 VPN 以及 IP VPN 的含义。在此基础上，简单介绍了从开始的租用物理专用线，到后来的 ATM/FR VPN，直到现在的 IP VPN 的发展历程。IP VPN 要替代传统的租用线，就必须具有很大的优势，这在第 3 节做了介绍。第 4 节对 IP VPN 的不同应用方式做了介绍，包括远程接入 VPN、内联网 VPN 以及外联网 VPN 的组网等。VPN 引起很大混乱的一点是它的分类方式，不同的生产厂家和运营商都采用了不同的分类方式，为了澄清这些概念，本章第 5 节做了这方面的介绍，并在第 6 节介绍了 VPN 的基本组成。另外，究竟具有什么样特征的产品和服务才能被认为是真正的 VPN 产品和服务呢？本章第 7 节回答了这个问题。

1.1　什么是 VPN

1.1.1　理解 VPN 的含义

简单地讲，VPN 就是利用开放的公众网络建立专用数据传输通道，将远程的分支办公室、商业伙伴、移动办公人员等连接起来，并且提供安全的端到端的数据通信的一种广域网技术。VPN 本质上是一种网络互联型业务，通过共享的网络基础架构满足企业互联需求，在共享使用网络资源的同时具有与专网一样保证用户网络的安全性、可靠性、可管理性。VPN 业务并不限制网络的使用，它既可以构建于因特网或互联网运营商(ISP)的 IP 网络之上，也可以构建于帧中继(FR)或异步传输模式(ATM)等网络基础架构之上，如图 1.1 所示。

但是，不同的人或组织对 VPN 的含义有不同的理解。VPN 产品供应商和服务提供商非常喜欢使用这个首字母缩写，因为这个“标签”能够满足他们提供产品/服务时的需要，但用户可能还是一头雾水。“虚拟”的意思比较好理解，即建立隧道或虚电路把不同的物理网络或设备连接起来，不再使用物理上的长途专线建立专有数据网络，而是将其建立在分布广泛的公用网络，尤其是在因特网上。“虚拟”是相对于 DDN(数字数据网)网络而言的，VPN 业务中使用网络资源并不是为一家用户所独占。虽然从用户看来是自己独享网络，但是实际用户网络只是叠加在公网中的虚拟层面。

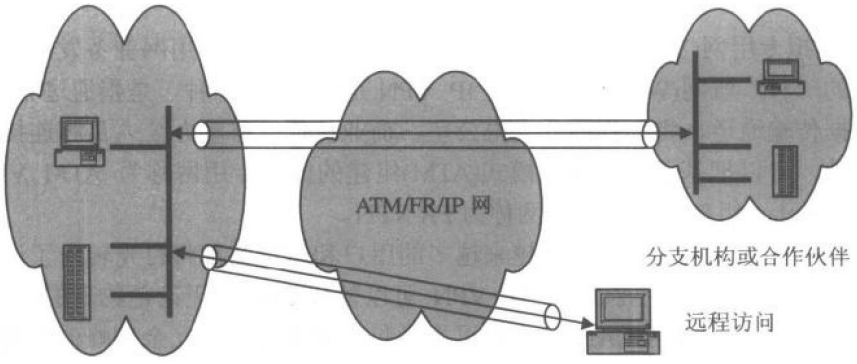


图 1.1 VPN 的含义

为了便于下面对“专用”概念的介绍，这里有必要首先来看一下“闭合用户群(CUG)”的含义。闭合用户群指很多特定的用户站点形成一个闭合的用户群体，通过基于用户“专用”网络的业务来保证其间的通信，并防止未经授权的其他站点访问这些站点。特定 CUG 内部可以使用专用的地址，不同的 CUG 之间的地址空间可以重用。CUG 的这种特性可以防止未经授权的包扩散到特定 CUG 网络的内部，防止欺骗以及在传输中修改数据包等安全攻击，并可以对不同类型的包进行不同的处理、统计和计费等。

对“虚拟”的含义，大家的理解比较一致，但对“专用”至少存在两种不同的理解方式。对于 ATM 和帧中继，一般将“专用”理解为电路连接的是一组闭合的用户或社区，具有服务质量(QoS)的保证，但不提供认证和加密等安全服务，“专用”的含义中更多的强调服务性能而不怎么考虑安全问题。对于 IPSec 等的 VPN，一般将“专用”理解为连接的也是一组闭合的用户或社区，但这时“专用”的含义中更多地强调安全服务，在性能方面仅提供“尽力而为(best effort)”的服务，位于站点之间的 IP 流量相互竞争 IP 网的网络资源(为了改善 IPSec 的服务质量，可以将 IPSec 和 DiffServ 等技术结合使用)。

1.1.2 IP VPN 的含义

有了对 VPN 含义的了解，理解 IP VPN 就比较容易了，因为 IP VPN 其实是 VPN 的一种类型。简单地讲，IP VPN 就是一种基于 IP 的 VPN。更准确地讲，IP VPN 是指利用 IP 基础设施(包括公用的因特网或专用的 IP 骨干网等)实现专用广域网设备专线业务(远程拨号、DDN 等)的业务仿真。

IP VPN 的“专用性”是相对于因特网而言的。因特网是一个开放的网络，而在 IP VPN 网络中，所有的信息都被限制在网络内部传送，不能将数据信息扩散到不安全或未授权的网

络中去。当然，这也不是要求 IP VPN 网络与外界完全隔离，而只是说无论从外界访问 IP VPN 内部网络，还是从 IP VPN 内部网络访问外部网络，都有很高的安全措施来保证安全性，这些措施包括用户身份验证、访问列表和防火墙过滤等。

1.2 VPN 的发展简史

随着社会的进步和技术的发展，信息的分布式处理的趋势越来越明显。从 20 世纪 70 年代末期开始，在基础科学和工程领域开始使用个人计算机处理信息。后来随着个人计算机的普及和发展，局域网技术应运而生，它将公司内的多台个人计算机连接起来，能够实现信息在本地的共享和分布式的处理。随着局域网应用的不断扩大，局域网的范围也不断扩大，从本地开始延伸到跨地区、跨城市甚至是跨国家，于是就诞生了能够将地理上分布的 LAN 连接起来的广域网技术。

专用网是一种能够把 LAN 连接起来的 WAN 技术。早期的数据业务并不是十分发达，专用网互联的介质一般采用租用电缆，用户数据信息根据事先约定的协议，在固定的时隙以预先设定的通道带宽和速率顺序传输，业务一旦开通，相关网络资源便为该用户独有，不管他是否真正在使用。专用网可以同时支持多种协议，比如帧中继、ATM 和 IP 协议等。高性能、高速度、高安全性、支持多种承载技术是专用网的明显优势，但由于专用网的专用性和严格性，专用网的费用也非常昂贵；而且一旦建成专用网，要在其上增加新的站点、合作伙伴或获得广泛的国际连接都将需要巨大的工程量和投入；另外，也不容易升级专用网。

随着分组技术的不断发展以及用户终端的日益智能化，出现了替代传统的租用物理线路的帧中继技术。帧中继传输链路使用逻辑连接而不是物理连接，可以在一个物理连接上支持多个逻辑连接，实现了对信道的动态复用，因此带宽利用率高了很多；另外，帧中继技术通过支持虚呼叫建立虚电路连接传送服务，逻辑连接可以按需建立。因此人们开始使用帧中继技术组建专用网络。从帧中继网络的特性上说，可以认为它是最早的 VPN 业务(即基于帧中继的 VPN)，因为基于帧中继的网络已经不再是对物理资源的独占了，而是开始变成“虚拟”的专用网络了。

后来出现的 ATM 技术，虽然摈弃了电路交换中采用的同步时分复用，改用了异步时分复用，具有了高带宽，综合传送话音、数据和图像等业务的能力等优势，但其逻辑连接的特性与帧中继没有什么不同，因此仍然是一种二层逻辑链路层技术。随着 ATM 技术的不断发展和成熟，组建专用网络时越来越多的使用 ATM 技术。

基于 ATM/帧中继的 VPN 都能够降低租用线路的费用，同时达到专用网络的要求，因此在全球目前得到了广泛使用。但基于 ATM/帧中继的 VPN 仍然存在费用较高，维护和升级困难的问题。随着网络经济、电子商务的迅猛发展，企业规模越来越大，所跨地域越来越广，合作伙伴越来越多，传统企业网基于固定地点的专线或虚拟专线的连接方式，已难以适应现代企业发展的需求。企业用户已经不仅仅满足于基本的网络互联能力，而是在网络的灵活性、安全性、经济性和可扩展性等方面都提出了更高的要求。面对数据流量的不断增大，用户需求的不断提高，运营商也不能停留在以往的 DDN 专线和 ATM/帧中继业务上，必须能够更为有效地利用自己网络资源，更为迅速地响应客户需求。