VPN网络技术与业务应用

王占京 张丽诺 雷 波 编著

国防工业出版社
National Defense Industry Press

VPN 网络技术与业务应用

王占京　张丽诺　雷　波　编著

国防工业出版社

·北京·

前　言

当前，中国的主流运营商一般拥有以IP为内核的MPLS VPN网络和以ATM技术为内核的基础数据网络，用以承载VPN专线业务。其中，基础数据网以业务安全性高、质量好、可以保证QoS等特点，吸引了很多党政军及金融客户。而IP网络则在费用、组网灵活度、维护难易度上占有优势。但由于IP网在安全、管理和QoS等方面的运营经验不足，一些对丢包、抖动和时延等传输质量指标有较高要求的企业客户一般都选择了基础数据网(ATM/FR)业务的电信服务。出于使用习惯以及网络稳定运行的考虑，客户一般都不会轻易改变所使用的电信业务。因此，无论是从用户群规模还是收入贡献来看，基础数据业务近几年仍将会稳定存在。

而目前各运营商基础数据网普遍存在技术没落、网络老化等问题，如果不尽快对ATM/FR业务替代及网络转网方案进行研究，则不利于对客户感知的提升，无法避免业务质量下降，从而导致客户流失、收入下降以及后续的一系列不利的连锁反应。因此，如何持续保障业务质量，避免上述矛盾的集中爆发，是各大运营商急需解决的重大难题，需要尽快研究基础数据网的演进策略，制定相应的迁移方案。

目前，业界对网络演讲策略与具体方案存在较大分歧，尚未给出具体演进步骤。本书通过从大客户业务需求入手，在对现有VPN技术及组网模式进行梳理的基础上，对现有电信运营商的转网策略进行研究，首次提出了切实可行的基础数据网演进方案，合理利用现有资源，实现基础数据网业务的平稳演进。这样既利于提升电信运营商的网络运营能力，又能保证现网中大量重要客户业务的稳定运行，增强电信运营商的核心竞争能力。

本书第1章简要对VPN技术进行概述，阐述了不同种类的VPN的实现方式；第2章介绍了基于隧道的VPN技术，重点描述了L2TP和IP Sec体系；第3章描述了基于分组交换的VPN技术，包括了二层与三层VPN技术与组网，及其适用的业务、ATM技术及承载业务、帧中继技术及承载业务等；第4章介绍了基

于传送网的VPN技术，包含了SDH、MSTP、PTN、WDM、OTN等专线技术及其在实际业务中的应用等；第5章分析了VPN网络的关键点，对QoS机制、安全机制、时钟机制进行了透彻的分析，并对网络的维护与管理及网络的扩展性进行深入的探讨；第6章回顾了VPN网络的发展历程及应用场景，重点介绍了不同的VPN技术及网络在中国市场的几种典型应用场景；第7章阐述了VPN网络的发展趋势，指出VPN网络演进势在必行；第8章描述了VPN网络的迁移，涉及了客户侧的迁移策略以及运营商侧的迁移策略；第9章推荐了网络迁移的实例，以供参考。

本书融入了编者多年来从事电信VPN网络及业务研究及维护的相关成果和工作经验，也参考了一些相关技术文献及解决方案等。

由于时间仓促，加之编者水平有限，书中偏颇和不当之处在所难免，敬请读者不吝赐教。

编 者

目 录

第 1 章　VPN 技 术

1.1　VPN 概述

VPN(Virtual Private Network，虚拟专用网络)。通常定义为通过公用网络(如Internet)建立一个临时的、安全的连接，可以认为是一条在公用网络穿通并隔离的安全、稳定的隧道。使用这条隧道可以对数据进行加密，以达到安全使用Internet 的目的。在 VPN 中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，而是架构在公用网络平台上。VPN 对用户端透明，用户好像使用一条专用线路进行通信。

VPN 是网络互连技术和通信需求迅猛发展的产物。Internet 的快速发展及其应用领域的不断推广，使得许多部门(如政府、外交、军队、跨国公司)已经广泛地利用廉价的公用基础通信设施构建自己的专用广域网，进行本部门数据的安全传输，客观上促进了 VPN 在理论研究和实现技术上的发展。

VPN 是专用网络的延伸。通过 VPN 可以模拟点到点专用链接的方式，通过共享或公共网络在两台计算机之间发送数据。VPN 是创建和配置 VPN 的行为。要模拟点到点链路，应压缩或包装数据，并加上一个提供路由信息的报头。该报头使数据能够通过共享或公用网络到达其终点。若要模拟专用链接，数据应加密，以进行保密，否则在共享或公用网络上截取的数据包是无法破译的。封装和加密专用数据之处的链接是 VPN 连接。

VPN 是对企业内部网的扩展。VPN 可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，用于经济有效地连接到商业伙伴和用户的安全外联网。VPN 主要采用隧道技术、加解密技术、密钥管理技术和使用者与设备身份认证技术。

VPN 通过特殊加密的通信协议链接到 Internet 上，在位于不同地方的两个或多个企业内部网之间建立一条专有线路，就像通过安全隧道到达目的地，而不用为隧道的建设付费。但是它并不需要真正地去铺设光缆之类的物理链路。这就像是去电信局申请专线，但是不用给铺设链路的费用，也不用购买路由器等硬件设备。VPN 技术原是路由器具有的重要技术之一，在交换机、防火墙设备或 Windows 2000 及以上操作系统中都支持 VPN 功能。简言之，VPN 的核心

就是利用公共网络建立虚拟私有网。

总的来说，VPN 就是将分布(物理分布)在不同地点的网络通过公用骨干网，(Internet/FR/ATM 等)连接而成的逻辑子网。并且采用了鉴别、访问控制、保密性、完整性等措施，以防止信息被泄露、篡改和复制，从而保障信息的安全。

1.1.1 VPN 的产生

IT 技术越来越多地影响现代企业的业务流程，如企业资源规划、基于 IP 的语音、基于网络的会议和教学活动等，为企业的自动化办公和信息的获取提供了构架。随着网络经济的发展，越来越多的企业的分布范围日益扩大，合作伙伴日益增多，公司员工的移动性也不断增加。这使得企业迫切需要借助电信运营商网络连接企业总部和分支机构，组成自己的企业网，同时移动办公人员能在企业以外的地方很方便地访问企业内部网络。

最初，电信运营商是以租赁专线的方式为企业提供二层链路，这种方式的主要缺点：建设时间长、价格昂贵、难于管理。

此后，随着 ATM(Asynchronous Transfer Mode)和帧中继技术的兴起，电信运营商转而使用虚电路方式为客户提供点到点的二层连接，用户再在其上建立自己的三层网络以承载 IP 等数据流。虚电路方式与租赁专线相比，其运营商提供服务的时间短、价格低，能在不同专网之间共享运营商的网络结构。这种传统专网的缺点在于：

(1) 依赖于专用的介质(如 ATM 或 FR)。为了提供基于 ATM 的 VPN 服务，运营商需要建立覆盖全部服务范围的 ATM 网络；为了提供基于 FR 的 VPN 服务，又需要建立覆盖全部服务范围的 FR 网络。在网络建设上造成了浪费。

(2) 其速率较慢，达不到当前 Internet 中已实现的速率。

(3) 部署复杂、尤其是向已有的私有网络加入新的站点时，需要同时修改所有接入此站点的边缘节点的配置。

传统专网的应用使得企业的效益日益增长。但难以满足企业对网络的灵活性、安全性、经济性、扩展性等方面的要求。这导致了新的替代方案的产生，在现有 IP 网络上模拟传统专网。这种新的解决方案就是 VPN。VPN 是依靠 Internet 服务提供商 ISP(Internet Service Provider)和网络服务提供商 NSP(Network Service Provider)，在公共网络中建立的虚拟专用通信网络。

1.1.2 VPN 的特征

VPN 具有以下两个基本特征：

(1) 专用：对于 VPN 用户，使用 VPN 与使用传统专网没有区别。一方面，

VPN 与底层承载网络之间保持资源独立，即一般情况下，VPN 资源不被网络中其他 VPN 或非该 VPN 用户所使用；另一方面，VPN 提供足够的安全保证，确保 VPN 内部信息不受外部侵扰。

(2) 虚拟：VPN 用户内部的通信是通过一个公共网络进行的，而这个公共网络同时也被其他非 VPN 用户使用。即 VPN 用户获得的是一个逻辑意义上的专网。这个公共网络称为 VPN 骨干网。

根据 VPN 的专用和虚拟的特征，可以把现有的 IP 网络分解成逻辑上隔离的网络。这种逻辑隔离的网络的应用非常广泛：可以用在解决企业内部互连、政府的相同或不同办事部门的互连；也可以用来提供新的业务，如为 IP 电话业务专门开辟一个 VPN，以此解决 IP 网络地址不足、QoS 保证及开展新业务等问题。

在解决企业互连和提供各种新业务方面，VPN 尤其是 MPLS(Multiprotocol Label Switching)VPN，越来越受运营商的青睐，成为运营商在 IP 网络提供增值业务的重要手段。

1.1.3 VPN 的优势

与传统的数据专网相比，从用户角度看，VPN 具有如下优势：

(1) 安全：在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的连接，保证数据传输的安全性。这对于实现电子商务或金融网络与通信网络的融合特别重要。

(2) 廉价：利用公共网络进行信息通信，企业可以以更低的成本链接远程办事机构、出差人员和业务伙伴。

(3) 支持移动业务：支持驻外 VPN 用户在任何时间、任何地点的移动接入，能够满足不断增长的移动业务需求。

(4) 服务质量保证：构建具有服务质量保证的 VPN(如 MPLS VPN)，可为 VPN 用户提供不同等级的服务质量保证。

从运营商角度看，VPN 具有如下优势：

(1) 可运营：提高网络资源利用率，有助于增加 ISP 的收益。

(2) 灵活：通过软件配置就可以增加、删除 VPN 用户，无需改动硬件设施。在应用上具有很大的灵活性。

(3) 多业务：SP 在提供 VPN 互连的基础上，可以承揽网络外包、业务外包、客户化专业服务的多业务经营。

VPN 以其独具特色的优势赢得了越来越多的企业的青睐，使企业可以以较少的精力关注网络的运行与维护，从而致力于企业的商业目标的实现。另外，运营商可以只管理、运行一个网络，并在一个网络上同时提供多种服务，如

Best-effort IP 服务、VPN、流量工程、差分服务，从而减少运营商在建设、维护和运行方面的费用。

VPN 在保证网络的安全性、可靠性、可管理性的同时提供了更强的扩展性和灵活性。在全球任何一个角落，只要能够接入到 Internet，即可开展 VPN。

1.2 VPN 的分类

随着网络技术的发展，VPN 技术得到了广泛的应用，同时也得到了很大的发展，涌现了许多 VPN 新技术。按照不同的角度，VPN 可以有多种分类。

(1) 按组网模型；
(2) 按业务用途；
(3) 按实现层次；
(4) 按运营模式。

1.2.1 按组网模型分类

根据组网模型的不同，VPN 可以分为：VPDN(Virtual Private Dial Network)、VPRN(Virtual Private Routing Network)、VPWS(Virtual Virtual Pseudo Service)、VPLS(Virtual Private LAN Service)。

1. VPDN

VPDN 利用公共网络的拨号功能及接入网，为企业、小型 ISP 和移动办公人员提供接入服务。VPDN 也可以使用私有 IP 地址等 VPN 的一些特性接入网，接入范围可遍及 PSTN(Public Switched Telephone Network)、ISDN(Integrated Services Digital Network)的覆盖区域，网络建设投资少、周期短、网络运行费用低。主要采用点到点的连接方式。通过 L2TP(Layer 2 Tunneling Protocol)、PPTP(Point-to Point Tunneling Protocol)等协议实现。图 1-1 是 VPDN 的示意图。远程用户(如企业驻外机构或出差人员)可以通过 ISDN 或 PSTN 网络接入 Internet，并在网络接入服务器和企业网关之间建立一条虚拟隧道，从而接入到企业内部。

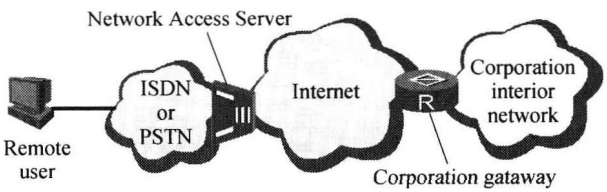

图 1-1 VPDN 示意图

VPDN 比其他类型的 VPN 具有更加灵活的身份验证机制、网络计费方式及高度的安全性，并支持动态地址分配。此外，VPDN 采用二层隧道，能支持多种三层传输协议。

2. VPRN

VPRN 是总部、分支机构和远端办公室之间通过网络管理虚拟路由器互连。VPRN 与其他类型的 VPN 相比，其主要区别在于 VPRN 数据包的转发是在网络层实现的。公网的每个 VPN 节点需要为每个 VPN 建立专用路由转发表。该表包含网络层可达性信息。数据流在公网的 VPN 节点之间的转发，以及 VPN 节点和用户站点之间的转发都是基于这些专用路由转发表。

VPRN 的实现方式包括两种：一种是使用传统 VPN 协议，如 IPSec(Internet Protocol SECurity extensions)、GRE(Generic Routing Encapsulation)等；另一种是使用 MPLS。

3. VPWS

VPWS 是对传统租用线业务的仿真，使用 IP 网络模拟租用线，提供非对称、低成本的 DDN(Digital Data Network)业务。从虚拟租用线两端的用户来看，该虚拟租用线近似于传统的租用线。VPWS 也兼容传统专网(如 ATM、FR)，运营商可以从 ATM、FR 等传统专网向 VPWS 平滑升级。VPWS 作为一种虚拟租用线路的实现方法，主要是在接入层和汇聚层使用。VPWS 又分为 CCC(Circuit Cross-Connect)、SVC(Static Virtual Circuit)、Martini 和 Kompella 等方式。PWE3 也是一种端到端的二层业务承载技术，是对 Martini 方式 VPWS 的一种扩展。

VPWS 模型适合星形连接的 VPN，对于需要全连接的 VPN，推荐采用 VPRN。

4. VPLS

虚拟专用局域网业务 VPLS 是局域网之间通过虚拟专用网段互连，是局域网在 IP 公共网络上的延伸。VPLS 也称为透明局域网服务(Transparent LAN Service，TLS)。不同于普通 L2VPN 的点到点业务，利用 VPLS 技术，服务提供商可以通过 MPLS 骨干网向用户提供基于以太网的多点业务。以太网技术由于其灵活的 VLAN 逻辑接口定义、高带宽、高成本比等优势，越来越广泛地被使用。VPRN 和 VPWS 也能提供局域网服务，但以太网技术的局限性如下：

(1) 无法限制未知 MAC 的广播泛滥。

(2) 生成树协议 STP(Spanning Tree Protocol)扩展受限。

(3) VLAN 地址空间有限。

突破传统以太网技术的限制，VPLS 骨干网不需要运行 STP，而是使用全连接和水平分割来消除骨干网的环路。对于单播或多播不可知帧，可采取丢弃、

本地处理和广播的处理方式。因此，VPLS 将实现 VLAN 的范围扩展至全国各地，甚至世界各地。尤其是 Q-in-Q(802.1q-in-802.1q)方式的 VPLS，不受 VLAN 地址空间的限制，更加扩大了 VPLS 的地域范围。

1.2.2 按业务用途分类

根据业务用途不同，VPN 可分为三种类型：企业内部虚拟专网(Intranet VPN)、扩展的企业内部虚拟专网(Extranet VPN)、远程访问虚拟专网(Access VPN)。

1. Intranet VPN

Intranet VPN 通过公用网络进行企业内部的互连，是传统专网或其他企业网的扩展或替代形式。使用 Intranet VPN，企事业机构的总部、分支机构、办事处或移动办公人员可以通过公有网络组成企业内部网络。VPN 也可用来构建银行、政府等机构的 Intranet。典型的 Intranet 例子就是连锁超市、仓储物流公司、加油站等具有连锁性质的机构。

2. Extranet VPN

Extranet 利用 VPN 将企业网延伸至供应商、合作伙伴与用户处，拥有共同利益的不同企业间通过公网构筑 VPN，使部分资源能够在不同 VPN 用户间共享。在传统的专线构建方式下，Extranet 通过专线互连实现，需要维护网络管理与访问控制，甚至还需要在用户侧安装兼容的网络设备。虽然可以通过拨号方式构建 Extranet，但此时需要为不同的 Extranet 用户进行设置，这样降低不了复杂度。因合作伙伴与用户的分布广泛，拨号方式的 Extranet 需要昂贵的建设与维护费用。因此，企业常常放弃构建 Extranet，使得企业间的商业交易程序复杂化，商业效率被迫降低。

Extranet VPN 以其易于构建和管理的特点为以上问题提供了有效的解决方案，其实现技术与 Intranet VPN 相同。目前，企业间通常使用 VPN 来构建 Extranet。为了保证 QoS，企业外部通信一般不直接使用 Internet。并且，企业间的通信数据通常是敏感的，而 Extranet 的安全性比 Internet 强。Extranet VPN 的访问权限可以由各个 Extranet 用户通过防火墙等手段来设置与管理。

3. Access VPN

Access VPN 使出差流动员工、家庭办公人员和远程小办公室可以通过廉价的拨号介质接入企业内部服务器，与企业的 Intranet 和 Extranet 建立私有网络连接。Access VPN 也称 VPDN。Access VPN 有两种类型：一种是用户发起的 VPN 连接，另一种是接入服务器发起的 VPN 连接。

1.2.3 按实现层次分类

根据实现层次的不同，VPN 可分为 L3VPN(Layer 3 VPN)、L2VPN(Layer 2 VPN)和 VPDN。

1. L3VPN

L3VPN 也就是 VPRN。它包括多种类型，如 IPSec VPN、GRE VPN、基于 RFC2547 的 BGP/MPLS VPN、以 IPSec 或 GRE 作为隧道的 BGP/MPLS VPN。其中 MPLS/BGP VPN 主要应用在主干转发层，IPSec VPN、GRE VPN 在接入层被普遍采用。

2. L2VPN

随着网络技术的发展，运营商网络越来越复杂，人们迫切希望出现新的技术，将传统的交换网(如 ATM、FR)与 IP 或 MPLS 网络融合，L2VPN 因此而诞生。L2VPN 包括前述的 VPWS 和 VPLS。VPWS 适合较大的企业通过 WAN 互连，而 VPLS 适合小企业通过城域网互连。VPLS 中存在广播风暴的问题，同时，PE 设备要进行私网设备的 MAC(Medium Access Control)地址学习，其协议、存储开销较大。

由于二层 VPN 只使用 SP 网络的二层链路，从而为支持三层多协议创造了条件。L3VPN 也能支持多协议，但不如 L2VPN 灵活，有一定限制。

3. VPDN

严格来说，VPDN 也属于二层 VPN，但其网络构成和协议设计与其他 L2VPN 有很大不同。在对 IP 报文进行封装时，VPDN 方式需要封装多次。第一次封装使用隧道协议 L2TP，第二次封装使用 UDP(User Datagram Protocol)。

1.2.4 按运营模式分类

根据运营模式的不同，VPN 可分为由用户控制的 CPE-based VPN(Customer Premises Equipment based VPN)、由 ISP 控制的 Network-based VPN 两种。

1. CPE-based VPN

在 CPE-based VPN 模式下，由用户控制 VPN 的构建、管理和维护。用户设备需要安装相关的 VPN 隧道协议，如 IPSec、GRE、L2TP 和 PPTP，并负责 VPN 的维护。CPE-based VPN 中，依靠用户侧的网络设备发起 VPN 连接，不需要运营商提供特殊的支持就可以实现 VPN。CPE-based VPN 方式复杂度高、业务扩展能力弱，主要应用于接入层。

传统的利用公有 IP 网络构建的 VPN(传统 IP VPN)属于 CPE-based VPN。其实质是在各个私有路由器之间建立 VPN 安全隧道，来传输用户的私有数据。

Internet 是典型的公有 IP 网络。使用 Internet 构建的 VPN 是最为经济的方式，但服务质量难以保证。企业在规划 IP VPN 建设时，应根据自身的需求对各种公用 IP 网络进行权衡。

2. Network-based VPN

在 Network-based VPN 模式下，VPN 的构建、管理和维护由 ISP 控制，允许用户在一定程度上进行业务管理和控制。功能特性集中在网络侧设备处实现，用户网络设备只需要支持网络互连，无需特殊的 VPN 功能。Network-based VPN 方式可以降低用户投资、增加业务灵活性和扩展性，也为运营商带来新的收益。

基于 MPLS 的 VPN 属于 Network-based VPN。MPLS VPN 由于在灵活性、扩展性和 QoS 方面的优势，逐渐成为最主要的 IP-VPN 技术，在电信运营网和企业网中都获得了广泛的应用。MPLS VPN 主要运用于骨干核心网及汇聚层，是对大客户互连及 3G、NGN 等业务系统进行隔离的重要技术。MPLS VPN 对于城域网同样重要：城域网内部署 MPLS VPN 技术已成为提升 IP 城域网的价值、为运营商提供更高收益的重要技术。

MPLS VPN 中，客户站点可以使用 T1、帧中继、ATM 虚电路、DSL 等链路接入 MPLS VPN 骨干网。并不需要在客户设备上进行特殊配置。

CPE-based VPN 与 Network-based VPN 的对比见表 1-1。

表 1-1　CPE-based VPN 与 Network-based VPN 的对比

项 目	CPE-based VPN	Network-based VPN
业务扩展能力	弱	强
用户投资	多	少
用户设备支持隧道的情况	需要支持	无需支持
性能要求	功能特性集中于 CE 设备，对 CE 设备要求高	功能特性集中于 PE 设备，对 PE 设备要求高

将 CPE-based VPN 和 Network-based VPN 无缝集成，可以给用户提供更可靠、更安全、更丰富的 VPN 业务。

1.3　VPN 的实现

1.3.1　VPN 的典型网络结构

典型的 VPN 组网分为三级结构：接入层、汇聚层和骨干层。