国 际 电 信 联 盟

ITU-T Y.1314

国际电信联盟
电信标准化部门

(10/2005)

Y系列：全球信息基础设施、网际协议问题和下一代网络

互联网的协议问题 — 传输

虚拟专用网络功能分解

ITU-T Y.1314建议书

国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、网际协议问题和下一代网络

全球信息基础设施	
概要	Y.100-Y.199
业务、应用和中间件	Y.200-Y.299
网络方面	Y.300-Y.399
接口和协议	Y.400-Y.499
编号、寻址和命名	Y.500-Y.599
运营、管理和维护	Y.600-Y.699
安全	Y.700-Y.799
性能	Y.800-Y.899
互联网的协议问题	
概要	Y.1000-Y.1099
业务和应用	Y.1100-Y.1199
体系、接入、网络能力和资源管理	Y.1200-Y.1299
传输	**Y.1300-Y.1399**
互通	Y.1400-Y.1499
服务质量和网络性能	Y.1500-Y.1599
信令	Y.1600-Y.1699
运营、管理和维护	Y.1700-Y.1799
计费	Y.1800-Y.1899
下一代网络	
框架和功能体系模型	Y.2000-Y.2099
服务质量和性能	Y.2100-Y.2199
业务方面：业务能力和业务体系	Y.2200-Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250-Y.2299
编号、命名和寻址	Y.2300-Y.2399
网络管理	Y.2400-Y.2499
网络控制体系和协议	Y.2500-Y.2599
安全	Y.2700-Y.2799
通用移动性	Y.2800-Y.2899

欲了解更详细信息，请查阅*ITU-T*建议书目录。

ITU-T Y.1314建议书

虚拟专用网络功能分解

摘　要

本建议书描述建立、操作和维护客户机/服务器和对等层虚拟专用网络（VPN）所需要的一组功能。网络的功能特性是从网络层的观点来描述的，它考虑了 VPN 分层的网络结构、客户特征信息、客户机/服务器的联系、联网拓扑技术和层网络的功能特性。

建议书采用 ITU-T G.805 和 G.809 建议书介绍的模型化方法描述了功能模型。所用的模型化方法独立于网络技术，因而该功能模型和所描述的相关功能将适用于所有的 VPN 层网络技术。

来　源

ITU-T 第 13 研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于 2005 年 10 月 14 日批准了 ITU-T Y.1314 建议书。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目 录

ITU-T Y.1314建议书

虚拟专用网络功能分解

1 范围

本建议书描述建立、操作和维护客户机/服务器和对等层虚拟专用网络（VPN）所需要的一组功能。网络的功能特性是从网络层的观点来描述的，它考虑了 VPN 分层的网络结构，客户特征信息、客户机/服务器的联系、联网拓扑技术和层网络的功能特性。建议书采用 ITU-T G.805 和 G.809 建议书介绍的独立于网络技术的模型化方法描述了功能模型。

2 参考文献

下列 ITU-T 建议书和其它参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的 ITU-T 建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

– ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks.*

– ITU-T Recommendation G.809 (2003), *Functional architecture of connectionless layer networks.*

– ITU-T Recommendation G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*.

– ITU-T Recommendation Y.1311 (2002), *Network-Based VPNs – Generic architecture and service requirements.*

3 定义

本建议书使用 ITU-T G.805 建议书中定义的如下术语：

3.1 access point 接入点

3.2 access group 接入群

3.3 adapted information 经过适配的信息

3.4 characteristic information 特征信息

3.5 client/server relationship 客户机/服务器关系

3.6 connection 连接

3.7 connection point 连接点

3.8 layer network 层网络

3.9 link 链路

3.10 link connection 链路连接

3.11 matrix 基体

3.12 network 网络

3.13 network connection 网络连接

3.14 port 端口

3.15 reference point 参考点

3.16 subnetwork 子网络

3.17 subnetwork connection 子网络连接

3.18 termination connection point 终端连接点

3.19 trail 路径

3.20 trail termination 路径终端

3.21 transport 传送

3.22 transport entity 传送实体

3.23 transport processing function 传送处理功能

3.24 unidirectional connection 单向连接

3.25 unidirectional trail 单向路径

本建议书使用 ITU-T G.809 建议书中定义的如下术语：

3.26 access point 接入点

3.27 access group 接入群

3.28 adapted information 经过适配的信息

3.29 characteristic information 特征信息

3.30 client/server relationship 客户机/服务器关系

3.31 connectionless trail 无连接路径

3.32 flow 信流

3.33 flow domain 流域

3.34 flow domain flow 流域信流

3.35 flow point 流接点

3.36 flow point pool 流接点集

3.37 flow termination 信流终端

3.38 flow termination sink 信流终端信宿

3.39 flow termination source 信流终端信源

3.40 layer network 层网络

3.41 link flow 链路信流

3.42 network 网络

3.43 network flow 网络信流

3.44 port 端口

3.45 reference point 参考点

3.46 traffic unit 业务流单元

3.47 transport 传送

3.48 transport entity 传送实体

3.49 transport processing function 传送处理功能

3.50 termination flow point 终端流接点

本建议书使用 ITU-T G.8010/Y.1306 建议书中定义的如下术语：

3.51 flow domain fragment 流域段

本建议书使用 ITU-Y.1311 建议书中定义的如下术语：

3.52 Layer 1 VPN 第 1 层 VPN

3.53 Layer 2 VPN 第 2 层 VPN

3.54 Layer 3 VPN 第 3 层 VPN

本建议书定义了如下术语：

3.55 VPN client layer network VPN 客户层网络：客户机/服务器 VPN 中的一个拓扑构件，它代表了同类型的一组接入点，它们为传送 VPN 客户层的特征信息而相互关联。

3.56 VPN server layer network VPN 服务器层网络：客户机/服务器 VPN 中的一个拓扑构件，它代表了同类型的一组接入点，它们为传送适配的 VPN 客户层信息而相互关联。

3.57 VPN peer layer network VPN 对等层网络：为一个拓扑构件，它代表了同类型的一组接入点，它们为传送 VPN 对等层的特征信息而相互关联。

4 缩写词和缩略语

本建议书使用如下缩写词和缩略语：

AAA 认证、授权和记账

AAL ATM 适配层

AG 接入群

AI 经过适配的信息

AIS 告警指示信号

AP 接入点

ASON 自动交换光网络

ATM 异步传送模式

BFD 双向转发检测

BGP 边界网关协议

CAC 连接允许控制

CBR 恒定比特率

CC 连通性检查

CE 客户边缘

CI 特征信息

CL-PS 无连接包交换

CO-CS 面向连接的电路交换

CO-PS 面向连接的包交换

CP	连接点
CV	连通性检验
DHCP	动态主机配置协议
DLCI	数据链路连接识别码
DSCP	差别服务编码点
DWDM	密集波分复用
EBGP	外部边界网关协议
E-LMI	外部的 LMI
ES	末端系统
FDF	流域信流
FDFr	流域段
FDI	转发差错指示
FP	流接点
FPP	流接点集
FR	帧中断
FT	信流终端
FTP	信流终接点
GRE	一般性选路包装
IGP	内部网关协议
IKE	互联网密钥交换
IPv4	网际协议第 4 版
IPv6	网际协议第 6 版
ISIS	中间系统到中间系统
L2TP	第二层隧道协议
LDP	标签分配协议
LF	链路信流
LMI	本地管理接口
LOC	失去连续性
LOS	失去信号
LSP	标签交换通道
MAC	媒体接入控制
MP2P	多点到点
MP-BGP	多协议 BGP
MPLS	多协议标签交换
MTU	最大传输单元
NE	网络实体
NF	网络信流

NMS	网络管理系统
NSAP	网络服务接入点
OAM	操作、管理和维护
OOB	带外
OSI	开放系统互连
OSPF	首先打开最短路径
OSS	操作支撑系统
P	提供商（节点）
P2P	点到点
P2MP	点到多点
PCR	峰值信元速率
PE	提供商边缘
PM	性能监测
PNNI	专用的网络到网络接口
PHP	在倒数第二跳弹出
PM	性能监测
PW	伪线
QoS	服务质量
RADIUS	远程认证拨入用户服务
RIP	选路信息协议
RPR	弹性数据包环网
RMON	远程监测
RSVP-TE	有业务量工程扩展的资源预留协议
SCR	持续的信元速率
SDH	同步数字系列
SES	严重误码秒
SLA	服务水平协定
SNC	子网络连接
SNMP	简单网络管理协议
SONET	同步光网络
SPVC	交换的永久虚电路
SSL	安全套接层
STP	生成树协议
SVC	交换的虚电路
TCP	终端连接点
TDM	时分复用
TFP	终端流接点

TTL 生存时间

TTSI 路径终端信源识别码

UNI 用户网络接口

VC 虚电路/通道

VCCV 虚电路连通性检验

VCI 虚通道识别码

VLAN 虚拟局域网（络）

VPI 虚通路识别码

VPN 虚拟专用网（络）

WDM 波分复用

5 客户机/服务器 VPN

客户机/服务器 VPN 有一个两层的体系，在此使用一个 VPN 的服务器层网络来支持一或多个 VPN 的客户层网络。

ITU-T Y.1311 建议书依据 VPN 服务类型和 VPN 的传送描述了客户机/服务器 VPN，在此，术语 VPN 服务类型是指 VPN 的客户层，而 VPN 传送是指 VPN 的服务器层。不同的 VPN 服务（客户机）和传送（服务器）的类型在 ITU-T Y.1311 建议书中进行了分类，如下面表 5-1 所示。

表 5-1/Y.1314 – Y.1311 服务类型

服务类型	描　　述
第 1 层	在属于同一 VPN 的客户站点提供物理层服务。连接可以是基于物理端口、光波长、SDH/SONET VC、频率信道或者时隙。
第 2 层	在属于 VPN 的客户节点之间提供数据链路层的服务。用户数据包的转发是基于数据包数据链路层包头中的信息（如 DLCI、ATM VCI/VPI 或 MAC 地址）。
第 3 层	在属于 VPN 的客户节点之间提供网络层的服务。用户数据包的转发是基于第 3 层包头中的信息（如 IPv4 或 IPv6 的目的地地址）。

ITU-T Y.1311 建议书使用的分类方法有一个缺点，用这种方法 MPLS 无法放入到这些类别中的任何一类，因而必须作为一个独特的层网络技术来处理。另一个缺点是：从功能的观点，同一层的网络技术可以具有很不相同的特征和要求。例如以太网和 ATM，两者都是第 2 层技术；然而，以太网是基于广播的无连接技术，而 ATM 是面向连接的非广播技术。

对网络技术分类的另一种方法是依据它们所属的网络模式来分类。所有网络技术都可以映射到三种模式中的一种：无连接包交换的（CL-PS）、面向连接包交换的（CO-PS）和面向连接电路交换的（CO-CS）。各种模式的功能要求是不同的，因为各种模式具有不同的特征。表 5-2 显示了 VPN 网络层技术的例子及它们所属的模式。

表 5-2/Y.1314－网络的操作模式及其例子

操作模式	例　子
无连接包交换	IP，以太网，MPLS MP2P (注 1)
面向连接的包交换	帧中继，MPLS P2P/P2MP (注 2)，ATM
面向连接的电路交换	SDH/SONET，TDM
注 1 — MPLS 多点到点（MP2P）LSP 是直接跨越相邻的 LDP 同层实体采用工作于下游主动或有序控制方式的 LDP 建立的。 注 2 — MPLS 点到点（P2P）或点到多点（P2MP）LSP 是跨越 RSVP-TE 同层实体采用 RSVP-TE 来建立的，或者 P2P LSP 是在非相邻的 LDP 同层实体之间采用对准目标/直接的 LDP 来建立的。	

5.1　客户机/服务器的组合

基于三种网络模式有九种可能的客户机/服务器组合，尽管某种组合比其他的更为兼容。表 5-3 描述了可能的客户机/服务器组合，并提供了它们间兼容性的一些信息。

一个 VPN 服务器层网络必须支持复用/去复用，以便在多个 VPN 客户层之间提供数据平面的分割。VPN 服务器层还必须支持客户业务流的适配，这种适配是客户机/服务器特定的，并取决于 VPN 客户层和服务器层网络的模式和所采用的特定技术。承载于包交换 VPN 服务器层上的电路交换 VPN 客户的一个重要的适配要求是：这种适配功能必须提供速率去耦（即空闲填充）和 VPN 客户层数据包的定界。在客户机/服务器都为包交换（CO 或 CL）情况下的关键要求是：如果 VPN 服务器层的业务流单位（即数据包的 MTU）小于 VPN 客户层的业务流单位，适配功能必须支持分段和排序。依据所采用的特定的 VPN 客户机/服务器技术还可能需要其他的适配功能，包括编码、速率改变和对齐。

表 5-3/Y.1314－网络客户机/服务器操作模式的组合

	CL-PS VPN 客户层	**CO-PS VPN 客户层**	**CO-CS VPN 客户层**
CL-PS VPN 服务器层	— 理想情况，虽然要提供逐个流传递的保证会在确定比例上带来挑战 — 一个并不提供逐个流传递保证的通常做法是采用过量配置和基于等级的优先级队列（来管理任意点之间突发的业务量和拥塞） 例子：一个以太网的服务器层支持一个 *IP* 的客户层	— 提供逐个流传递的保证会在确定比例上带来挑战 — 一个并不提供逐个流传递保证的通常做法是采用过量配置和基于等级的优先级队列 — VPN客户层必须能对失去顺序的业务流单元进行恢复（由于服务器层对数据包重新定序的可能性） 例子：一个 *IP* 服务器层支持一个 *ATM* 的客户层	— 提供逐个流传递的保证会在确定比例上带来挑战 — 一个并不提供逐个流传递保证的通常做法是采用过量配置和基于等级的优先级队列 — 恢复时钟定时是技术上的挑战 — VPN客户层必须能对失去顺序的业务流单元进行恢复 例子：一个 *IP* 服务器层支持一个 *TDM* 的客户层
CO-PS VPN 服务器层	— 对于按需建立并具有很短保持时间的 VPN，有一个与保持连接，也即 SPVC 的状态相联系的开支 例子：一个 *ATM* 的服务器层支持一个 *IP* 的客户层	— 理想的 例子：一个 *P2P MPLS* 的服务器层支持一个 *ATM* 的客户层	— 恢复时钟定时是技术上的挑战 例子：一个 *ATM* 的服务器层支持一个 *TDM* 的客户层
CO-CS VPN 服务器层	— 在汇聚点之间没有统计复用 — 在递增过程中永久分配的带宽会导致很差的网络利用率 — 对于按需建立并具有很短保持时间的 VPN，连接建立的响应时间缓慢 例子：一个 *SDH* 的服务器层支持一个以太网的客户层	— 在汇聚点之间没有统计复用 — 在递增过程中永久分配的带宽会导致很差的网络利用率 — 对于按需建立并具有很短保持时间的 VPN，连接建立的响应时间缓慢 例子：一个 *ATM* 的服务器层支持一个 *TDM* 的客户层	— 理想的 例子：一个光服务器层（例如一个 *DWDM* 信道）支持一个 *SDH/SONET* 客户层

5.2 VPN 客户层的透明性

在一个客户机/服务器 VPN 中，属于 VPN 客户层网络的功能构件（如选路、信令、OAM、管理等）应该完全独立于 VPN 服务器层网络的功能构件。

虽然有可能对客户机/服务器 VPN 的解决方案进行设计，使 VPN 服务器层网络的功能构件能与 VPN 客户层网络的功能构件进行互动，但这一做法会导致一系列不希望的结果，例如：

1） 如果客户对 VPN 客户层网络的任何功能构件进行改动，VPN 的服务会破坏。

2） VPN 服务提供商需要跟踪客户的 VPN 客户层技术的发展，并在它的网络中实现相应的升级。

3） 在出现差错的情况下，要确定这差错是在 VPN 客户层网络还是 VPN 服务器层网络将变得很困难。

既然要求 VPN 客户层和服务器层网络能相互独立地运行，自然地需要：VPN 服务器层应该透明地传送 VPN 的客户层。例如，如果 VPN 客户层网络是 ATM，VPN 的客户层网络可以实现一些特有的特性（例如 AAL、非 PNNI 的选路和信令、OAM），这些特性如果不能透明地运送，将破坏 VPN 服务。

客户层透明性不仅仅是一个技术要求，它还同时具有商业意义，因为 VPN 服务提供商很可能会认为它的网络的一些细节是商业敏感的，因而希望将这些细节对 VPN 的客户层网络隐藏起来。例如在上述例子中，VPN 的服务器层网络将不希望成为 VPN 客户层网络选路和信令的对等体。

6 对等层VPN

在第 5 节中 VPN 的拓扑是基于 VPN 客户层和 VPN 服务器层之间的客户机/服务器关系。在这个客户机/服务器的 VPN 模型中，VPN 服务器层的信源适配功能将 VPN 客户层的 CI 适配成 VPN 服务器层的 AI，同时 VPN 服务器的信宿适配功能将 VPN 服务器层的 AI 适配成 VPN 客户层的 CI。用基本的术语来讲，这种适配是指用 VPN 服务器层的帧/信号来包装客户层的帧/信号。

然而不是所有的 VPN 拓扑都基于这客户机/服务器的模型。VPN 也可以采用 CL-PS 网络技术，基于另一种模型来提供，在此 VPN 在共享区域内可通达性的隔离是通过客户机/服务器包装以外的其他手段来实现的。本建议书称这种类型的 VPN 为对等层的 VPN。术语“对等层”是指：提供商是在它接收客户数据包的同一个网络层上跨越它共享的基础设施来传送客户的 VPN 数据包的。这并不涉及客户/提供商控制平面的对等关系，客户与提供商可以在控制平面中相互对等，而不论 VPN 的类型如何。只有 CL-PS 的网络模式支持这种类型的 VPN，因为在 CO-PS 和 CO-CS 的情况下，面向连接的特性在技术上会强制可通达性的隔离，也即 NE 只能与属于同一 P2P 或 P2MP 连接的 NE 进行通信。

为了支持跨越共享区域的 VPN，所用的网络技术必须有某种能确保 VPN 隔离的手段，也即 NE 必须只能和属于同一 VPN 的其他 NE 进行通信，或者只能对属于同一 VPN 的 NE 的数据包进行解密。

6.1 包/路由的过滤

跨越共享区域实现 VPN 隔离的一种方法是与由多个客户共享的 PE 一起使用包过滤。采用这种方法，服务提供商网络中的所有节点知道客户的所有路由。它们包括提供商面向客户站点的边缘（PE）节点和核心网中的提供商节点（P）。在这一体系下，PE 节点由不同的客户共享。服务提供商将一部分它的地址空间分配给一个客户，并在 PE 路由器上对包过滤器进行管理，来确保一个客户站点之间的可通达性和客户之间的隔离。

为了克服需要在逐个客户逐个站点的基础上保持相一致的路由表和包过滤器，另有一种方法是与专用的 PE 一起，即一个 VPN 一个 PE，实施基于路由过滤的解决方案，而不是包过滤。在这一架构下，P 节点具备所有客户的路由，但 PE 节点仅具有单个客户的路由。客户路由的隔离由路由过滤来实现。PE 节点将配置路由过滤器，它只允许客户知道属于它们的有关路由。边界网关协议（BGP）是提供商骨干网络中为此而通常使用的协议的一个例子，原因是它的多功能路由过滤工具。路由过滤的一种替代方法是为每一个 VPN 使用不同选路协议的实例。然而采用这种方法，由于 P 节点只能支持有限数量的选路协议实例以及管理多协议实例在操作上的复杂性，共享的网络将只能支持小量的 VPN。

为了克服需要为每一个 VPN 使用一个不同的 PE 节点，一个替代的方法是使用虚拟路由器（VR）。用这种方法，一个物理节点在实际上将被划分为一些虚拟的路由器。可以将一个（或几个）虚拟路由器分配给一个特定客户。这样，一个节点可以为多个用户提供相分割的选路实例。一个单独的虚拟路由器的表现就像分别的专用于一个特定 VPN 的 PE 节点。正如路由过滤方法那样，P 节点包含所有客户的路由，因而需要在 PE 进行路由过滤。[1]

6.2 加密

代替包/路由过滤的另一种选择是与包加密相结合在连接到共享基础设施的所有客户之间提供全通达性。包加密将确保：在客户从一个不是他们所属的 VPN 接收到数据包时，他们得不到包中所包含的信息。客户可以在业务流经由共享网络送出之前对 VPN 数据包加密，管理 VPN 由客户负责。用这种方法，在服务提供商网络内，业务流将同任何其他的 IP 业务流一样进行选路，服务提供商看不到隧道之内的东西。服务提供商网络也不需要以任何专门的方式进行配置。换一种做法，VPN 数据包也可以在提供商的共享网络的边缘用提供商管理的设备（即 PE 或提供商管理的 CE）进行加密。用这种方式，提供商将负责管理 VPN。

[1] 这一方法的自然演化是使用MPLS或其他的隧道方法，使得VPN特定的路由不必要保存于骨干路由器中。然而，这样将形成为客户机/服务器拓扑，因而这种方法适用于第5节，而不是本节。

支持加密架构的一个例子是 RFC 2401 — 网际协议安全架构（IPsec）。IPsec 定义密码算法、认证和密钥[2]管理程序，可用于 IPsec 网关/客户之间建立安全的 IP 业务流隧道。IPsec 在信息跨越共享的基础设施时保证 VPN 中的保密、完整性和对数据源点的鉴别。IPsec 对于跨越像互联网那样的公众网络提供 VPN，用于站点到站点或远程接入的 VPN，是特别有用的。IPsec 的功能特性可以由 PE、CE 或末端的用户装置（例如执行 IPsec 客户程序的膝上型电脑）来提供。

安全套接层（SSL）VPN 是使用加密来提供逐个 VPN 隔离的另一类 VPN。SSL VPN 的典型使用是允许用户经由互联网安全地接入应用和文档。这一方法的优点是不需要对末端的用户系统在配置上做任何修改，只需要支持标准的应用（如 Web 浏览，电子邮件客户端等）即可。同样地对于 VPN 对等层，SSL VPN 是透明的（由于加密是在应用层进行），因而为了支持 SSL VPN，不需要对选路/交换节点进行配置。

6.3 以太网VLAN

标准 IEEE 802.1Q 定义了虚拟 LAN（VLAN）网桥的操作，它允许在桥接 LAN 的基础设施内对虚拟 LAN 的拓扑进行定义、操作和管理。VLAN 使得位于多个物理的 LAN 段上的端站能进行通信，就好像它们是连接在同一个 LAN 段上一样。末端用户和集线器/交换机可以通过改变 VLAN 的配置移动到不同的 VLAN 中，配置在它们所连接的符合 802.1Q 的交换装置的端口/接口上进行。广播和组播帧将受 VLAN 边界的限制，使得端站只能接收来自它们所属的 VLAN 的广播/组播帧。这一点，与如何学习 MAC 地址的机制一起，将确保只有属于同一个 VLAN 的端站可以相互通信，因而可以考虑是同一个 VPN 的成员。

对于跨越共享的基础设施的属于不同的 VLAN 的帧，业务流的分离是通过在每个帧中插入带有 VLAN 识别码（VID）的标记来实现的。对每一个 VLAN 必须分配一个 VID（1 至 4 096），它在同一个物理基础设施内必须是全局地惟一的。这一方法的缺点之一是：客户在它们自己的网络中也使用 VLAN，这会带来 VID 的分配和限制问题。为了解决这一问题，可以在进入提供商网络的客户的带有 IEEE 802.1Q 标记的数据包上附加第二个标记（IEEE 802.1ad 中定义的 Q-in-Q）。这就分开了提供商的 VLAN 空间和客户的 VLAN 空间，允许客户使用它们要用的任何 VID[3]。

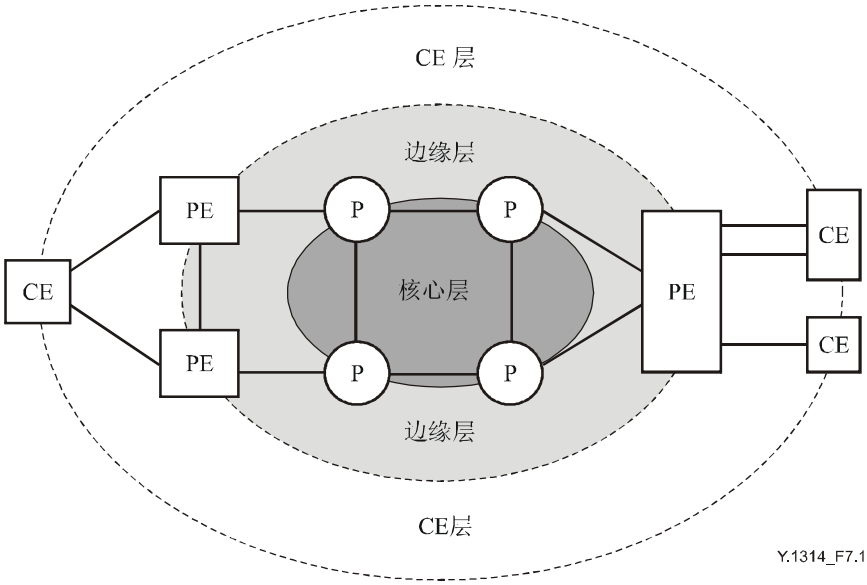
---

2 密钥是控制加密/解密算法操作的信息片。

3 另一个选项是使用MAC-in-MAC方法（如IEEE 802.1ah所定义的），在此提供商在客户数据包上附加第二个以太网包头。然而这一选项建立的是一个客户机/服务器VPN而不是一个对等层VPN，因为客户帧是包装在一个提供商的帧之内。

7 VPN的功能结构

出自 ITU-T Y.1311 建议书的 VPN 参考模型如图 7-1 所示。



CE 客户边缘
PE 提供商边缘
P 提供商

图 7-1/Y.1314－ITU-T Y.1311建议书 的VPN参考模型

这一模型虽然显示了物理拓扑和不同的网络构件，但它并没有显示不同的 VPN 服务器层和客户层的拓扑或层间适配功能的位置。

另一种表达客户机/服务器 VPN 网络的方法是使用功能模型。面向连接的（CO-PS/CO-CS）和无连接的（CL-PS）的层网络的功能结构可以分别采用 ITU-T G.805 建议书“传送网络的一般性功能结构”和 ITU-T G.809 建议书“无连接层网络的功能结构”来描述。

ITU-T G.805 和 G.809 建议书提供了一种一般化的方法从功能的和结构体系的观点将网络模型化。定义的术语是独立于技术的，可用于描述给定的任何一种网络的物理和拓扑构件。由于可以对整个网络的视图做模型描述，从管道中的光纤直到在上面运行的 VPN 服务，这对于网络的盘点和管理将是特别有用的。

一个 VPN 网络可以分解为一系列独立的层网络，相邻的层网络间具有客户机/服务器关系。正如 ITU-T G.805 建议书所说明的，采用功能模型定义的层网络不应该与开放系统互连（OSI）模型（ITU-T X.200 建议书）中的层相混淆。OSI 模型中的每一个层提供特定的功能，为每一个层定义的协议执行对应于那个层的特定功能，例如传送层（第 4 层）从会晤层接受数据，将它传送给提供端到端传递服务的网络层。与之相反，基于 ITU-T G.805 或 G.809 建议书的功能模型中的每一个层网络提供的是同样的服务，也即在输入和输出之间进行比特/帧的传送。通常地采用了抽象，将细节隐藏起来，而关注于感兴趣的层/构件，但网络可以模型化直到网元，例如以太网交换机、铜线对、SDH 交叉连接等。

7.1 面向连接的VPN层网络

VPN 客户层和服务器层网络，各自有其自己的连通性的输入和输出组，称为接入点（AP）。它们可以相互关联从输入到输出跨越层网络来透明地传送信息。对于 CO 层网络，AP 之间关联的有效拓扑构造是点到点（P2P）和点到多点（P2MP）。

VPN 服务器层的 AP 标志着 VPN 服务器层和客户层网络之间的功能性边界。从 VPN 服务器层的观点，一个 VPN 服务器层的 AP 代表了可以支持路径的一个选路的目的地。从 VPN 客户层的观点，一个 VPN 服务器层的 AP 代表了可能获得链路能力的一个点。CO 网络层中的功能构件和参考点已示意于图 7-2 中。

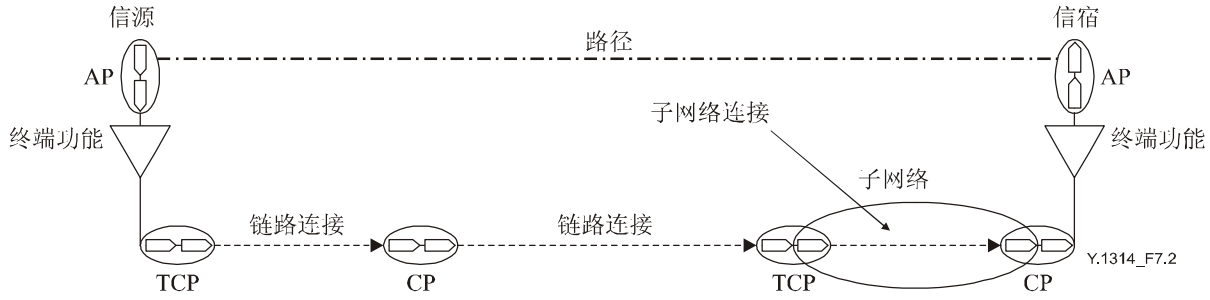


图 7-2/Y.1314－CO的功能构件和参考点

连接是 CO 层网络中的传送实体，它由一对相关联的单向连接组成，两者能在相反方向上在它们各自的输入和输出之间同时传送信息。网络连接是 CO 层网络中的传送实体，它由终端连接点（TCP）之间一系列邻接的链路连接和/或子网络连接构成。

子网络是 CO 层网络中的一种拓扑构件，用于实现特定特征信息的选路；子网络在单个 CO 网络层中包含有一组与管理功能相关联的点。子网络连接能跨越子网络传送信息，它由子网络边界上的端口（路径终端信源的输出/路径终端信宿的输入）之间的联合所构成。

链路连接互连拓扑上相邻接的子网络，它们具有共同的点的子集。链路连接的输入被连到另一个链路连接输出的点是连接点（CP）。CO 层网络中一个路径终端的信源输出被连接到网络连接输入的点是信源 TCP，而路径终端的信宿输入被连接到网络连接输出的点是信宿 TCP。CP 和 TCP 都具有与它们相关联的管理对象，因而有可能为了管理的需要而将属于同一 VPN 的 TCP 和 CP 点组合在一起。

7.2 无连接的VPN层网络

与 CO 层网络不同，CL 层网络支持多点到多点（MP2MP）或任意到任意的拓扑。CL 层网络使用信流，而不是连接，它们是一个或多个具有共同选路项的业务流单元的集合。信流可以是单向的或双向的，双向信流由方向相反的两个单向信流所组成。网络信流是 CL 层网络的一个传送实体，它由终端流接点（TFP）之间一系列邻接的信流构成。CL 层网络的功能构件和参考点如图 7-3 所示。

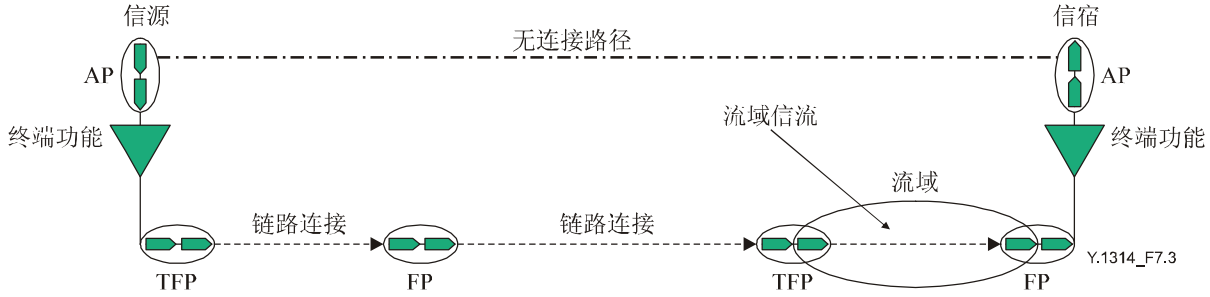


图 7-3/Y.1314－CL的功能构件和参考点

流域是 CL 层网络的一个拓扑构件，用于实现特定特征信息的选路。流域信流是跨越流域传送信息的传送实体，它由流域边界上的端口间的联合所构成。流域在单个 CL 网络层中包含有一组与管理功能相关联的点。

链路信流互连拓扑上相邻接的流域，它们具有共同的点的子集。链路信流的输入被连到另一个链路信流输出的点是流接点（FP）。CL 层网络中一个无连接路径终端的信源输出被连接到网络信流输入的点是信源 TFP，而无连接路径终端的信宿输入被连接到网络信流输出的点是信宿 TFP。和 CO 情况下的 CP 和 TCP 一样，在 CL 情况下，FP 和 TFP 都具有与它们相关联的管理对象，因而有可能为了管理的需要而将属于同一 VPN 的 TFP 和 FP 点组合在一起。

7.3 VPN的客户机/服务器关系

从功能的角度，一个 VPN 客户层网络是客户机/服务器 VPN 中的一个拓扑构件，它代表了同一类型，为了传送 VPN 客户层特征信息而相关联的一组接入点，这些接入点受 VPN 服务器层路径或无连接路径的支持。VPN 客户层连接/信流的信源/信宿 TCP/TFP 可以位于 CE 节点，或者在客户网络其他的节点/末端系统中。例如 ATM VPN 客户层的 TCP 很可能位于 CE 节点，而以太网 VPN 客户层的 TFP 很可能位于末端用户的计算机或服务器中。从客户的角度，VPN 客户信流/连接的 TFP/TCP 的位置是重要的，因为这是客户网络中 VPN 客户层和更高层之间必须进行适配的地点。从 OAM 的角度，它同样是重要的，因为它是与 VPN 客户层信流/连接相关联的路径/无连接路径的信源和信宿 AP 的所在地。TFP/TCP 位于不同地点的客户机/服务器 VPN 的例子已在附录一中提供。

一个 VPN 服务器层网络是客户机/服务器 VPN 中的一个拓扑构件，它代表了为了给一个或多个 VPN 客户层信流或连接传送经适配的客户层信息而相关联的同一类型的一组接入点。VPN 服务器层包含有信源/信宿的适配功能，它们将 VPN 客户层的特征信息适配成 VPN 服务器层中经过适配的信息或反之。VPN 的客户层和服务器层可以属于同一种模式（即客户层和服务器层都是 CO，或者都是 CL），但两种模式的组合也是可能的，也即 CO 的 VPN 服务器层可以支持 CL 的客户层，同样 CL 服务器层也可以支持 CO 的客户层。图 7-4 显示了支持 CL VPN 客户层的一个 CL VPN 服务器层的例子，它从功能的角度出发，并基于图 7-1 所示的 ITU-T Y.1311 建议书网络模型的物理拓扑。这一模型中的底层是 VPN 服务器层，顶层是 VPN 客户层。为了简便起见，图中仅示意了 VPN 的客户机/服务器层，客户的高于 VPN 客户层的客户层以及低于 VPN 服务器层的服务器层并没有显示。在这一例子中 VPN 服务器层是 CO（例如 ATM），而 VPN 的客户层是 CL（例如以太网），尽管 CO 或 CL 对的任何组合都是可能的。

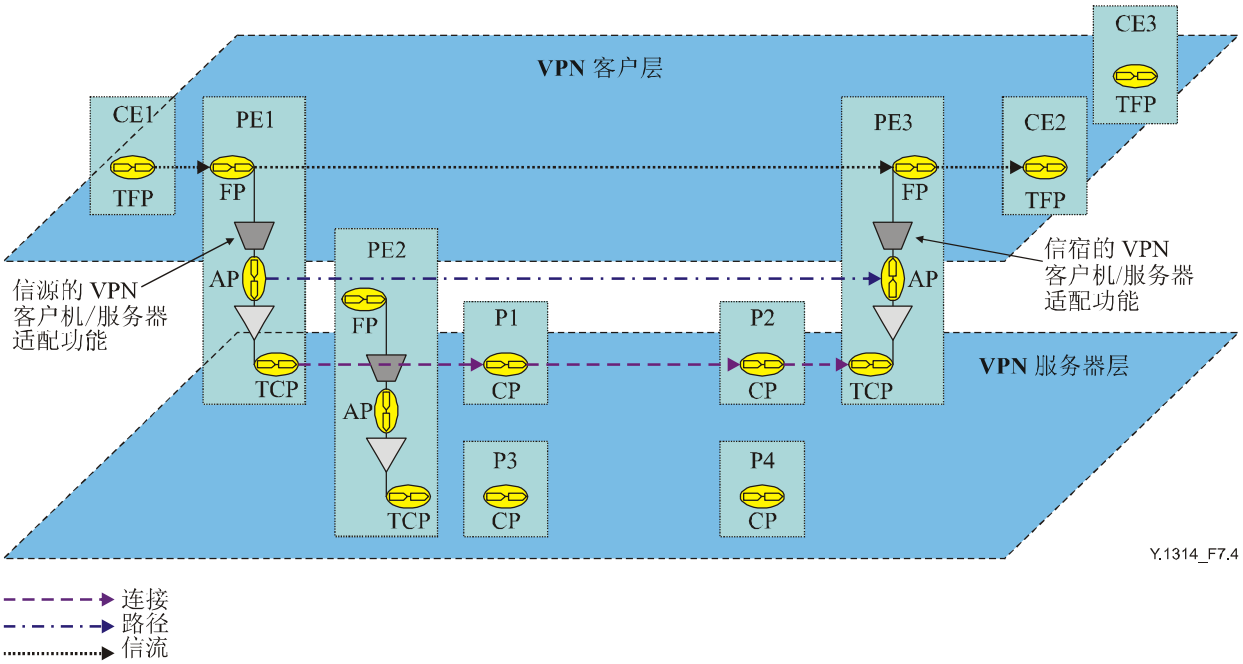


图 7-4/Y.1314－客户机/服务器 VPN的功能模型

图 7-4 突出显示了哪些功能和网络参考点存在于哪个网元（即 CE、PE 或 P 节点）中，由此显示了功能模型与图 7-1 中的网络图形之间的联系。CE 和 P 节点分别属于 VPN 的客户层和服务器层，而 PE 节点同时属于这两个层。在 VPN 客户层中的 TFP 标识 P2P VPN 客户层信流从哪里（在本例中即从那个 CE 节点）开始（它的信源）和终结（它的信宿），而 FP 标识 P2P 信流要通过哪些 PE 节点。类似地，VPN 服务器层中的 TFP 标识 VPN 服务器层连接的信源和信宿，而 FP 标识信流要通过哪些 P 节点。VPN 服务器层中的 AP 标识 VPN 服务器层路径的信源/信宿。

随后的子节将采用功能模型对 4 种可能的客户机/服务器 VPN 组合进行逐一的介绍，并描述客户机/服务器 VPN 适配功能的作用。

7.3.1 由CO VPN服务器层支持CO VPN客户层

由 CO VPN 服务器层网络支持的一个 CO VPN 客户层网络的例子如图 7-5 所示。

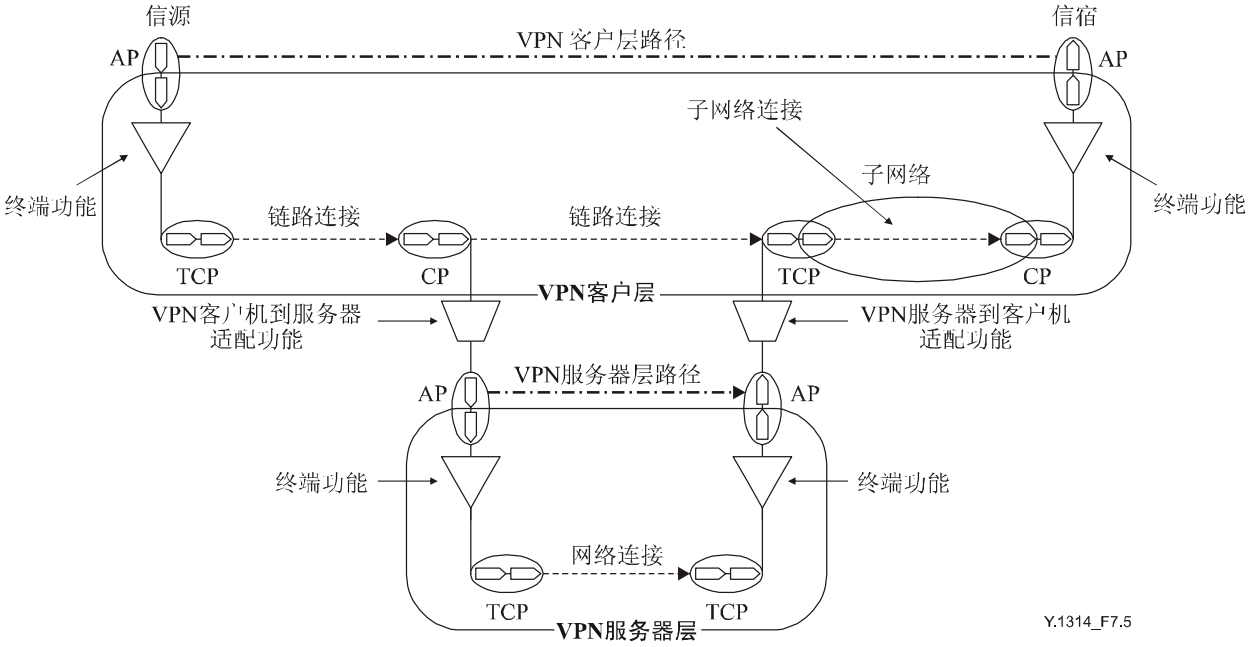


图 7-5/Y.1314－具有CO VPN客户机的CO VPN服务器层

在这一例子中，CO VPN 客户层连接是由 CO VPN 服务器层路径来支持的。CO VPN 服务器层的信源适配功能将 CO VPN 客户层的特征信息（CI）适配成 CO VPN 服务器层中经过适配的信息（AI）。CO VPN 服务器层的信宿适配功能将 CO VPN 服务器的 AI 适配成 CO VPN 客户层的 CI。

7.3.2 由CL VPN服务器层支持CL VPN客户层

由 CL VPN 服务器层网络支持的一个 CL VPN 客户层网络的例子如图 7-6 所示。

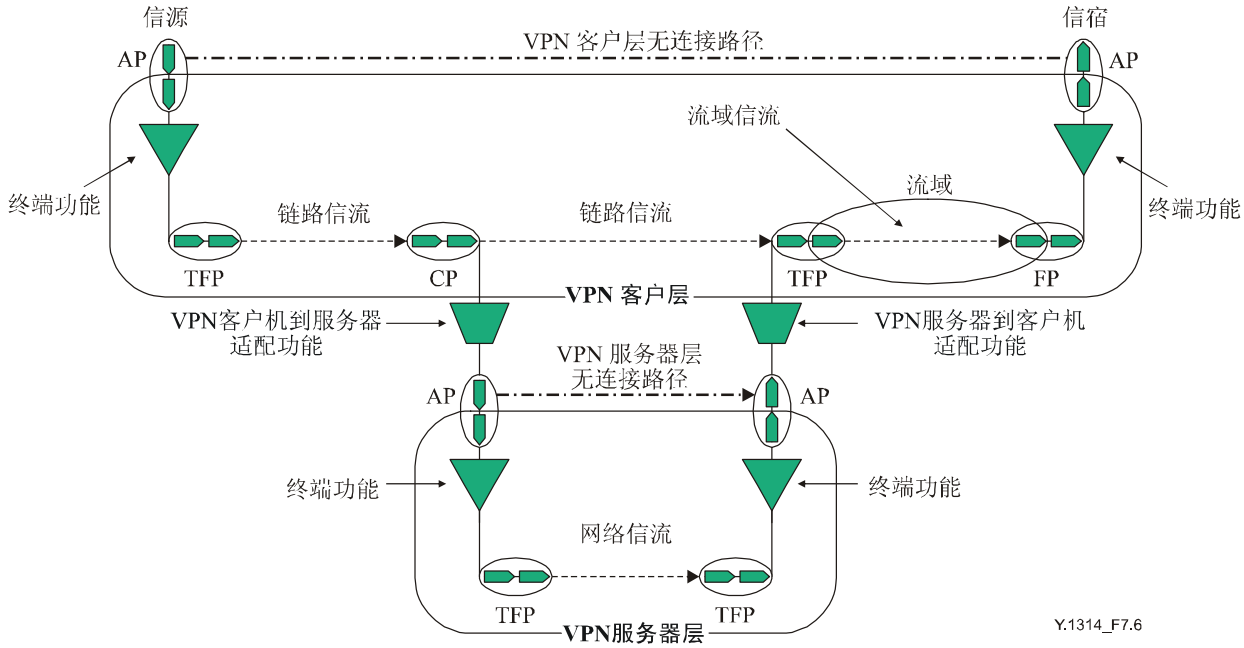


图 7-6/Y.1314－具有CL VPN 客户机的CL VPN服务器层

在这一例子中，CL VPN 客户层信流是由 CL VPN 服务器层无连接路径来支持的。CL VPN 服务器层的信源适配功能将 CL VPN 客户层的特征信息（CI）适配成 CL VPN 服务器层中经过适配的信息（AI）。CL VPN 服务器层的信宿适配功能将 CL VPN 服务器的 AI 适配成 CL VPN 客户层的 CI。

7.3.3 由CL VPN服务器层支持CO VPN客户层

由 CL VPN 服务器层网络支持的一个 CO VPN 客户层网络的例子如图 7-7 所示。

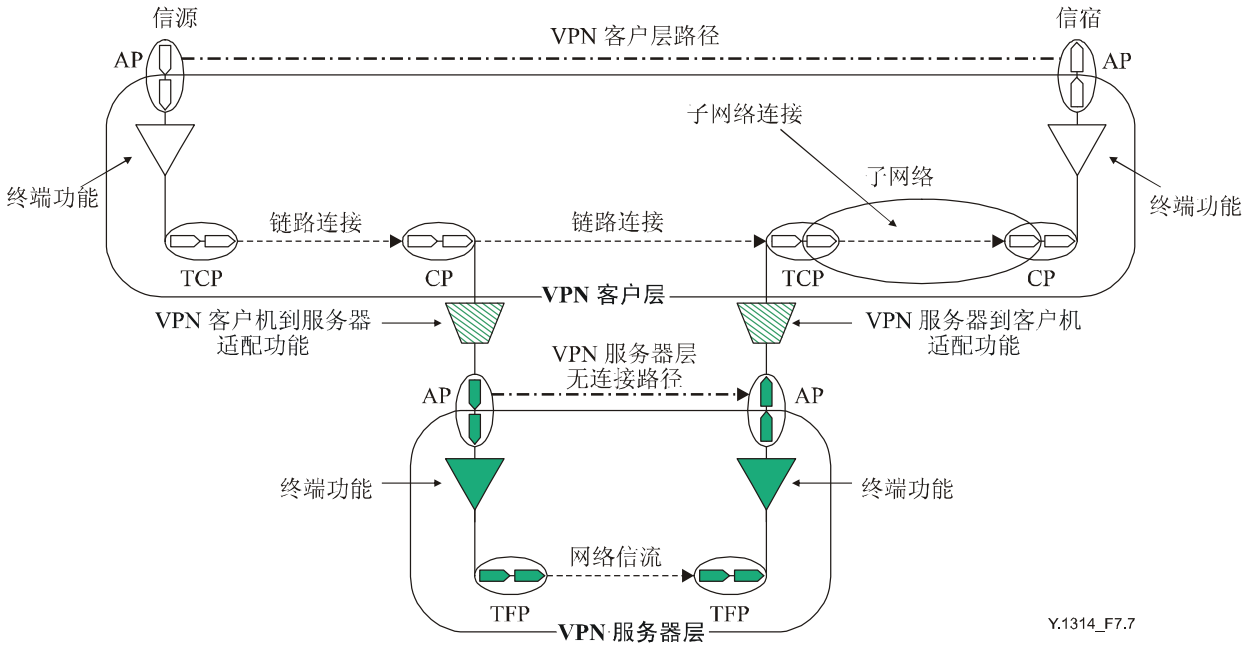


图 7-7/Y.1314－具有CO客户机的CL VPN服务器层

在这一例子中，CO VPN 客户层连接是由 CL VPN 服务器层无连接路径来支持的。CL VPN 服务器层的信源适配功能将 CO VPN 客户层的特征信息（CI）适配成 CL VPN 服务器层中经过适配的信息（AI）。CL VPN 服务器层的信宿适配功能将 CL VPN 服务器的 AI 适配成 CO VPN 客户层的 CI。

7.3.4 由CO VPN服务器层支持CL VPN客户层

由 CO VPN 服务器层网络支持的一个 CL VPN 客户层网络的例子如图 7-8 所示。

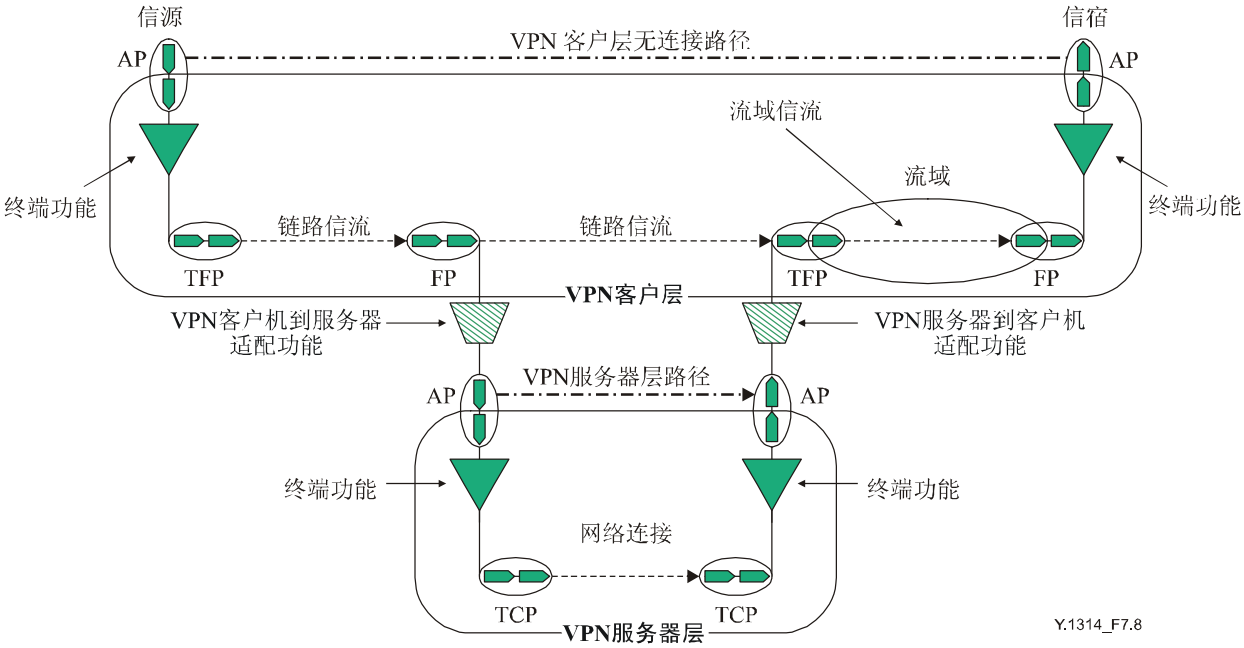


图 7-8/Y.1314－具有CL客户机的CO VPN服务器层

在这一例子中，CL VPN 客户层信流是由 CO VPN 服务器层路径来支持的。CO VPN 服务器层的信源适配功能将 CL VPN 客户层的特征信息（CI）适配成 CO VPN 服务器层中经过适配的信息（AI）。CO VPN 服务器层的信宿适配功能将 CO VPN 服务器的 AI 适配成 CL VPN 客户层的 CI。

7.4 多个VPN客户层

本节中到此为止的例子中，端到端使用的都是单个的 VPN 客户层。但情况并不总是这样，一个客户可能愿意在 VPN 的一侧使用 VPN 的一个客户层类型，而在 VPN 的另一侧使用不同的 VPN 客户类型。例如在一侧，VPN 的客户层可能是 IP，而在另一侧可能是 MPLS，或者在一侧是帧中继（FR），另一侧是 ATM。在这样的情况下，两个不同的 VPN 客户层网络必须在对等层的基础上进行联网。

应该注意：这里使用的术语“VPN 客户层网络”是指客户机/服务器 VPN 中的一个拓扑构件，它代表为传送 VPN 客户层 CI 而相关联的同类型的一组接入点。它并不是第 1 层、第 2 层和第 3 层意义上的网络分层，也即在 VPN 客户层上要互通的两种技术可以都是第 2 层技术（例如一个可能是 ATM，另一个是 FR），但它们被认为是不同的层网络，因为它们包含不同的接入点，这些接入点是不同类型的。

互通功能可以处于 VPN 服务器层信源适配功能之前，或者在 VPN 服务器层信宿适配功能之后。图 7-9 显示了客户机/服务器 VPN 网络的物理拓扑，它在 VPN 的各侧使用了不同的 VPN 客户层。

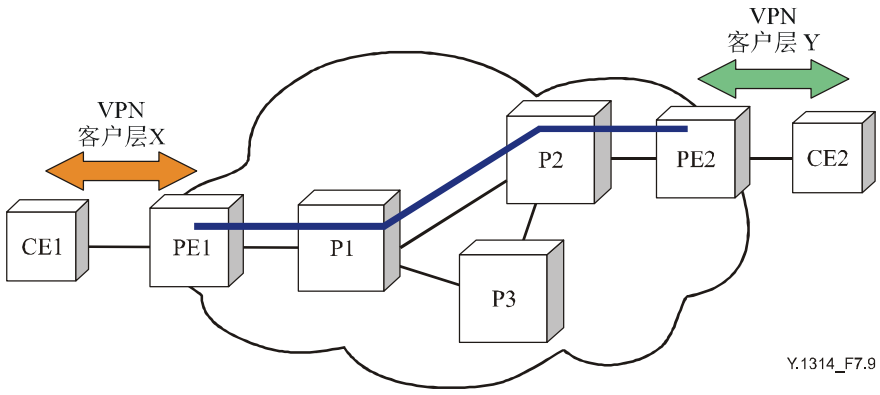


图 7-9/Y.1314－VPN 客户机对等层互通的物理拓扑

图 7-10 依据图 7-9 的物理拓扑，提供了对等层 VPN 客户机互通的一般性功能模型，在此互通功能处于 VPN 服务器层信源适配功能之前。

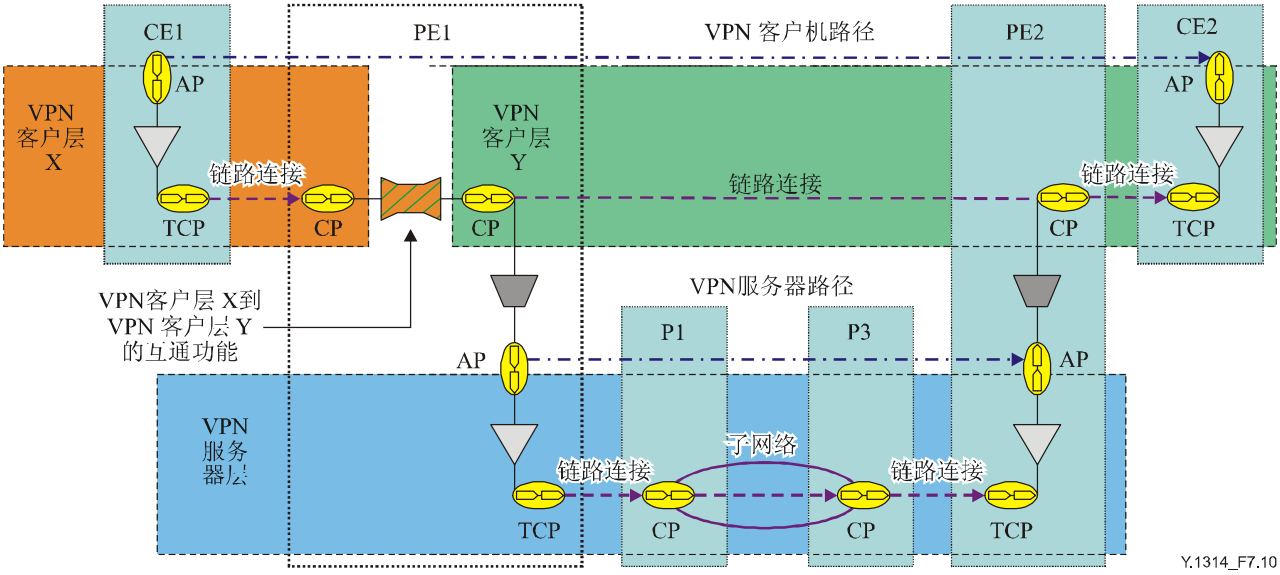


图 7-10/Y.1314－VPN客户机对等层的互通
（在VPN服务器信源适配之前）

在这一模型中两个异构的 VPN 客户层是 VPN 客户层 X 和 VPN 客户层 Y。在这一例子中，PE 执行互通功能，但它也可以用单独的装置来执行。互通功能将 VPN 客户层 X 的 CI 转换为 VPN 客户层 Y 的 CI。VPN 服务器层的信源适配功能将 VPN 客户层 Y 的 CI 适配到 VPN 服务器层的 AI，而 VPN 服务器层的 AI 跨越 VPN 服务器层路径进行发送。在 VPN 服务器层的信宿，适配功能将 VPN 服务器层的 AI 适配到 VPN 客户层 Y 的 CI。作为例子，假如 VPN 客户层 X 是 FR，而 VPN 客户层 Y 是 ATM，那么信源 PE 将把 FR 的业务流转换成 ATM 的业务流（例如使用 FRF.8），同时 VPN 客户层业务流将作为 ATM 运载于 VPN 的服务器层。

图 7-11 提供了对等层 VPN 客户互通的一般性功能模型，在此互通功能处于 VPN 服务器层信宿适配功能之后。

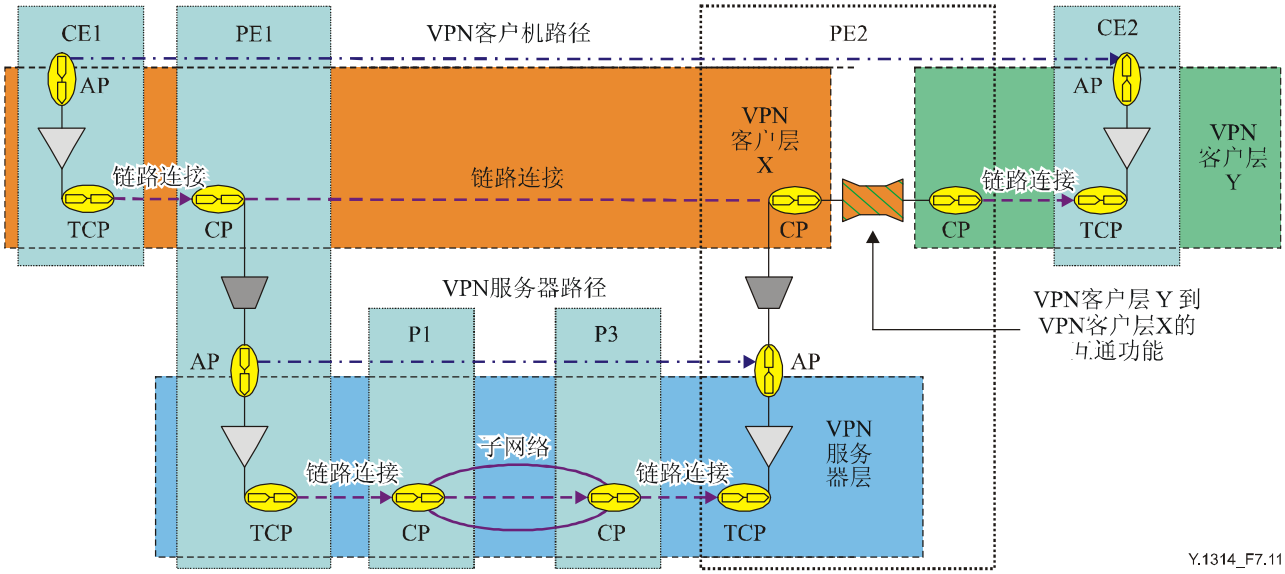


图 7-11/Y.1314－VPN客户机对等层的互通
（在VPN服务器信宿适配之后）

VPN 服务器层的信源适配功能将 VPN 客户层 X 的 CI 适配到 VPN 服务器层的 AI，而 VPN 服务器层的 AI 跨越 VPN 服务器层路径进行发送。在 VPN 服务器层的信宿，适配功能将 VPN 服务器层的 AI 适配到 VPN 客户层 X 的 CI。互通功能将 VPN 客户层 X 的 CI 转换为 VPN 客户层 Y 的 CI。如果 VPN 客户层 X 是 FR，而 VPN 客户层 Y 是 ATM，那么 VPN 客户层业务流将作为 FR 运载于 VPN 的服务器层，并由信宿 PE 转换成 ATM。

7.5 多个VPN服务器层

在前面的例子中，端到端使用单个的 VPN 服务器层来跨越提供商网络支持 VPN 的客户层。但情况并不总是这样，例如一个提供商由于网络覆盖的不足，用单个 VPN 服务器层有可能不能提供端到端的连通性，或者一个 VPN 客户层可能需要跨越多个提供商网络。在这些情况下，将需要多个 VPN 服务器层。依据特定的网络技术和提供商设备的互通能力，分别的 VPN 服务器层可以在对等层的基础上进行互通，或者在客户机/服务器的基础上与 VPN 客户互通。

尽管使用多个 VPN 服务器层是可能的，但在考虑使用多个 MPLS VPN 服务器层时有一些因素需要考虑。要考虑的因素具体取决于所需互通的类型和要用的 VPN 服务器层技术。在附录二中提供了多个服务器层对等层和客户机/服务器互通的例子以及对每一种情况的一些考虑。

应该注意：在 VPN 服务器层之下使用多个服务器层不应与采用多个 VPN 服务器层的情况相混淆。例如，如图 7-12 所示，一个服务提供商可以端到端地使用单个 MPLS VPN 服务器层，但在这 VPN 服务器层之下在一部分网络中使用 MPLS 服务器层（采用 MPLS 标记堆栈），而在另一部分网络中使用 IP 服务器层（例如采用 GRE 封装）。

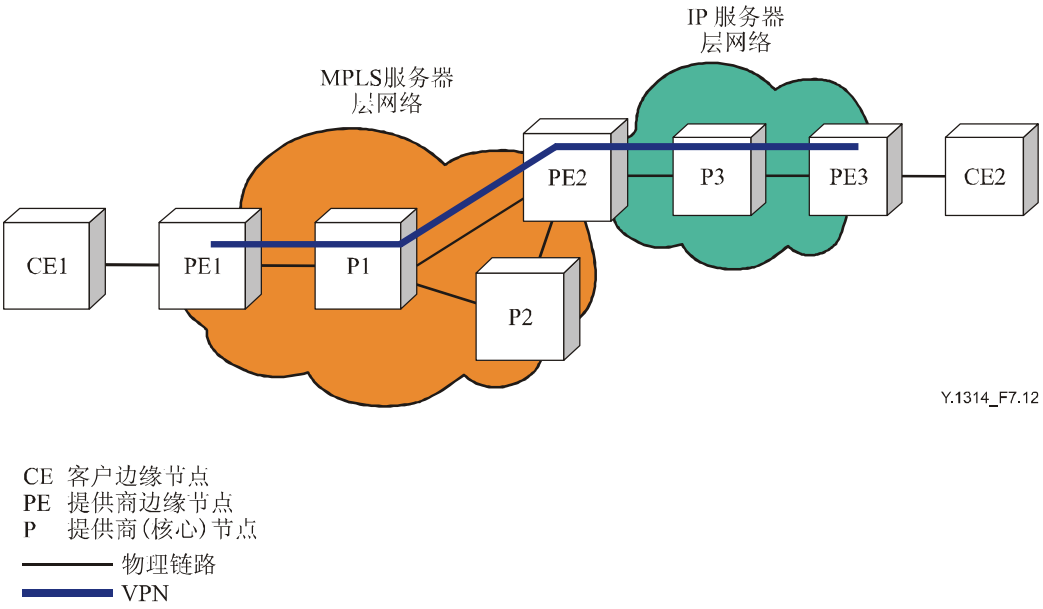


图 7-12/Y.1314－采用MPLS和IP服务器层的客户机/服务器VPN

在 MPLS 服务器层网络中 PE 和 P 路由器必须都支持 MPLS，然而在 IP 服务器层中只有 PE 路由器需要支持 MPLS，P 路由器不需要支持 MPLS。与图 7-12 示意的网络相关的功能模型在图 7-13 中描述。

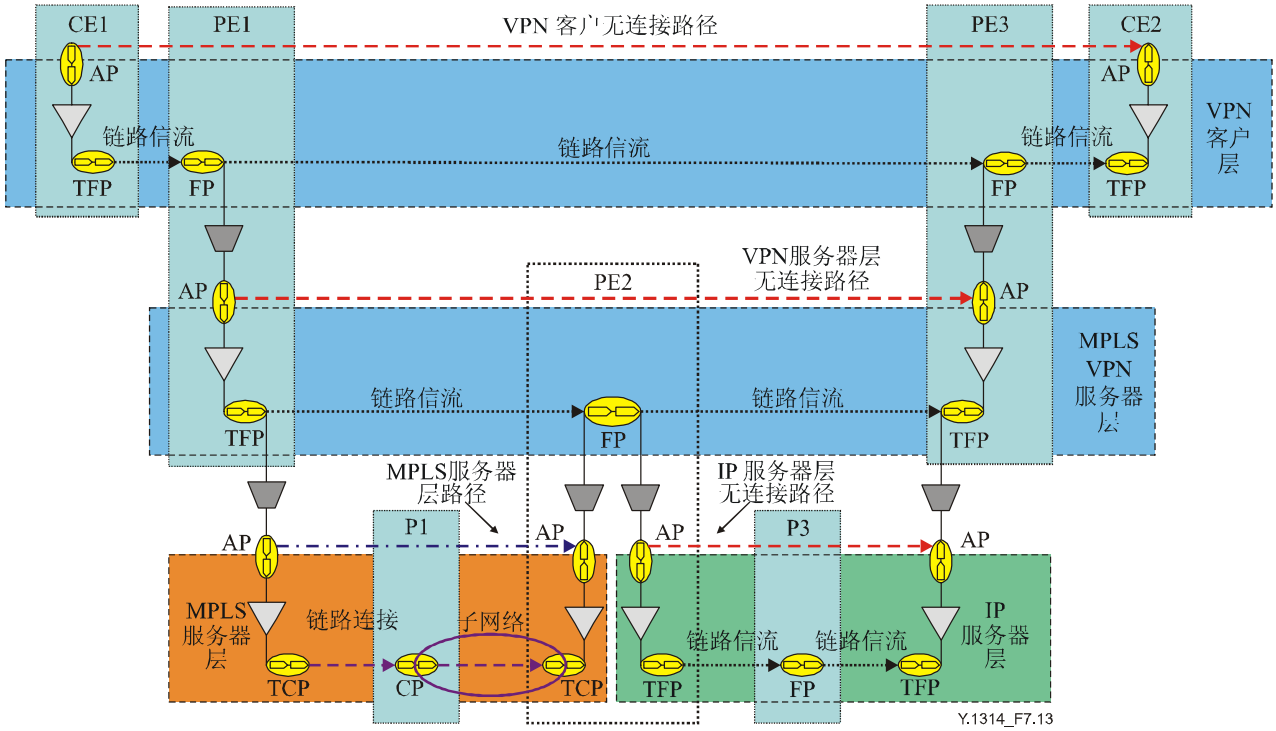


图 7-13/Y.1314－由多个服务器层支持的VPN服务器层

在这一例子中，MPLS 服务器层信源适配功能将 MPLS VPN 服务器层的 CI（它是 MPLS 服务器层的一个客户）适配到 MPLS 服务器层中的 AI，而 MPLS 服务器层信宿适配功能将 MPLS 服务器层 AI 适配到 MPLS VPN 服务器层的 CI。IP 服务器层信源适配功能将 MPLS VPN 服务器层的 CI 适配到 IP 服务器层中的 AI，而 IP 服务器层信宿适配功能将 IP 服务器层的 AI 适配到 MPLS VPN 服务器层的 CI。

7.6 采用分区的VPN模型描述

前面章节中提供的功能模型是采用分层的方法形成的。将网络分解为一系列独立的层网络可以为相邻层网络之间的客户机/服务器关系建立模型，并对对应的适配、终端和互通功能进行描述。

另一种建立模型的方法是分区，它用于定义一个层网络内的网络结构和网络区域间管理/选路的边界，这种网络区域可能是不同运营商拥有的网络。在要分解的一个层次上，分区可以将一个子网络分成为它包含的一些子网络以及它们间的链路。这种分区可以一直继续，直到达到递推的极限，也就是一个网元内的单个子网络。正如 ITU-T G.805 建议书所描述的，它被称为基体。在图 7-14 中对分区做了示意。

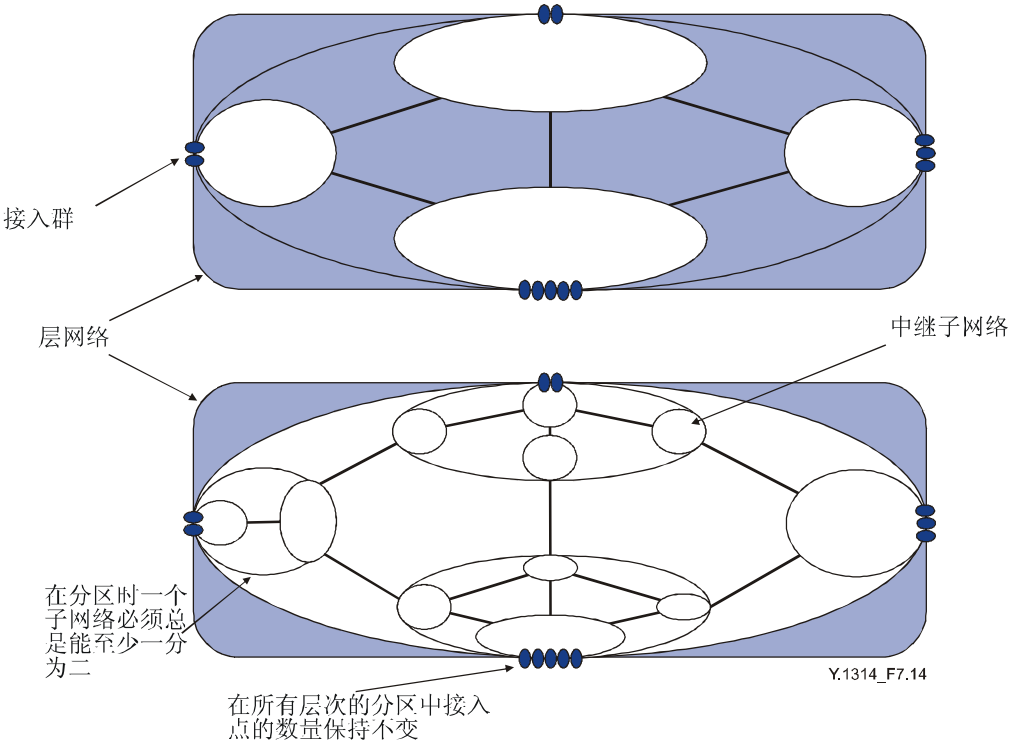


图 7-14/Y.1314－在层网络内对子网络进行分区

作为分区进程的一部分，最大的子网络中的流/连接点的数量在分区中是保持不变的，而它内部的连接点在下一层的分区中会展现出来。从连通性的角度，子网络（流域）代表了它输入与输出间的一个有弹性的点（如信源/信宿接入点或流/连接点）。一般地讲，它允许任何的一个输入可以连接到任何的一个输出。

这一模型对于公众网络是充分的，在此，资源可以假定都总是可用的。然而，它对于虚拟专用网络并不适合。原因是：子网络/流域输入和输出间的连通性将限制于属于同一 VPN 的输入和输出。为了支持用分区方法来建立 VPN 模型，可采用由 ITU-T G.8010 建议书描述的流域段（FDFr）的构造和子网络连接（SNC）的构造。FDFr/SNC 是通过将它的输入和输出分割成不同的组群的办法来进行分段的。连通性被限制于同一组群的成员之间。这样一种组群可以是以太网网桥上的 VLAN（一个以太网流域）或者是子网络或流域上的 VPN。一个 FDFr/SNC 可以用它相关联的层网络的名称和段号来标记，或通过将流接点分组为特定的段，例如用 VLAN 识别码来标记。用 VLAN 来提供 VPN 隔离的一个网络的例子如图 7-15 所示。

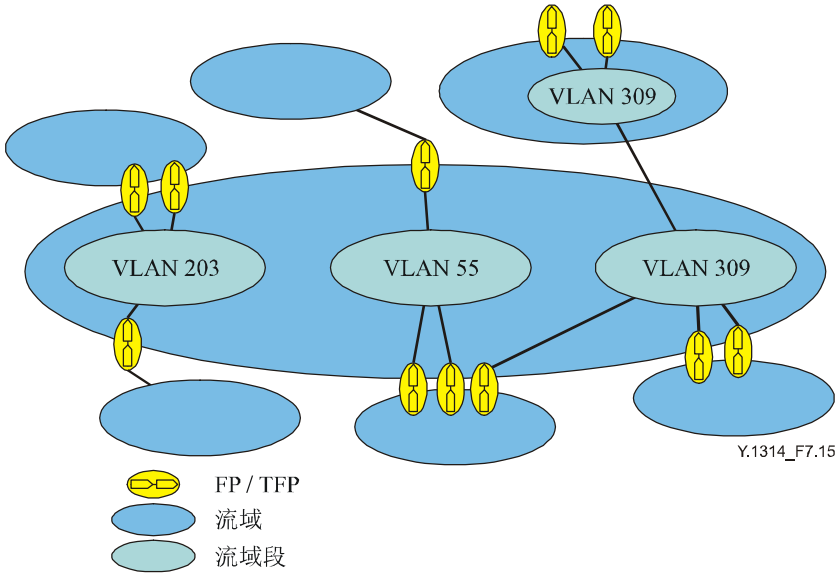


图 7-15/Y.1314－VPN分区功能模型的例子

流域中的一个 FDFr 是通过互连的构件链路与另一流域中的 FDFr 相关联的。类似地，子网络中的一个 SNC 是经由互连的链路连接与另一个子网络中的 SNC 相关联的。这样将使这构造可以分区或者聚合，与子网络的模型相一致。由于这样，这一模型非常灵活，使得 VPN 的结构可以在子网络分区的任何层次上进行显示。

7.7 VPN对等层

图 7-16 显示了一个对等层 VPN 的物理拓扑。在这一例子中，网络云雾表示共享的网络区域，而灰线表示一个 P2P 的 VPN。VPN 的隔离可以通过第 6 节中定义的任何方法来实现，如以太网的 VLAN、IPsec 的隧道等。

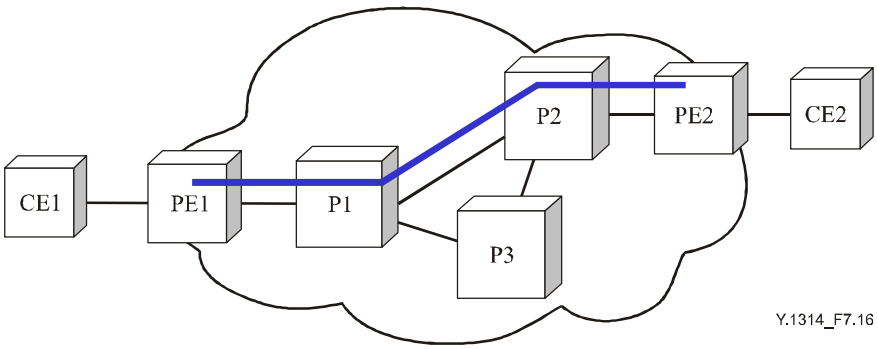


图 7-16/Y.1314－对等层VPN物理拓扑的例子

图 7-17 从功能的角度描述了图 7-1 的 VPN 拓扑，显示了 VPN 层和 PE 之间底下的单个服务器层。在这一例子中，服务器层是 CO，但它也同样地可以是 CL。

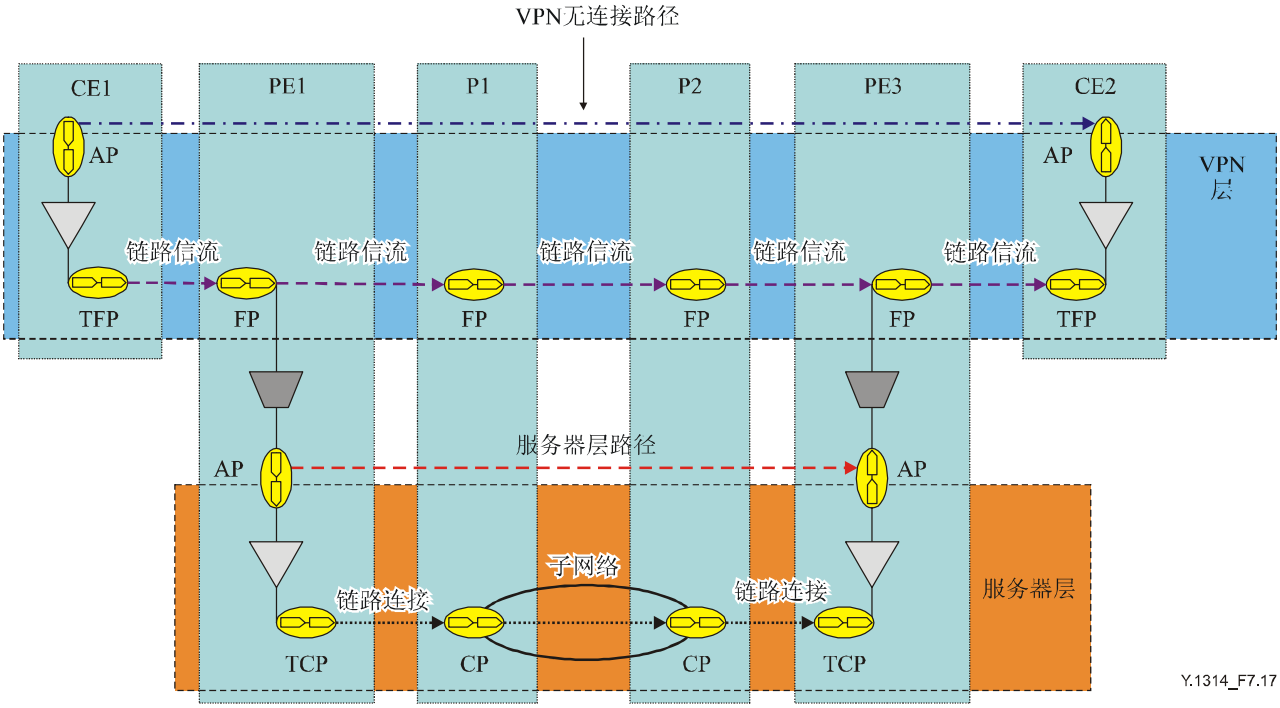


图 7-17/Y.1314－一个单层VPN的分层模型

正如图 7-17 所示，网络中的所有节点（包括 P 节点）都属于 VPN 层，因此它们必须能够利用 VPN 层包头中的信息将数据包转发到正确的目的地。由于单层的 VPN 架构，这一层次模型并未提供它在用于客户机/服务器情况下所提供的那么多的信息。尤其是图 7-17 的呈现格式没有提供有关 VPN 在何处开始和终结的任何信息。加入这种信息的方法之一是进一步叙述 VPN/服务器层的适配功能。图 7-18 示出 VPN/服务器层适配功能的两个不同的例子，一个采用 IPsec，另一个采用以太网 VLAN 标记。

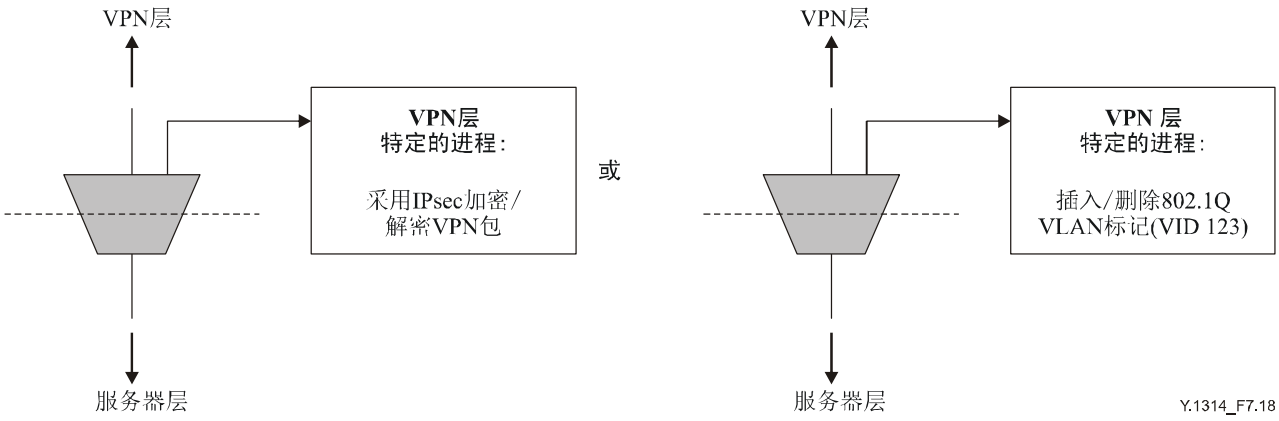


图 7-18/Y.1314－VPN/服务器层适配功能的扩展

描述对等层 VPN 的另一种方法是采用第 7.6 节引入的分区的概念。如何用这种方法使用分区的一个例子已在图 7-19 中提供。

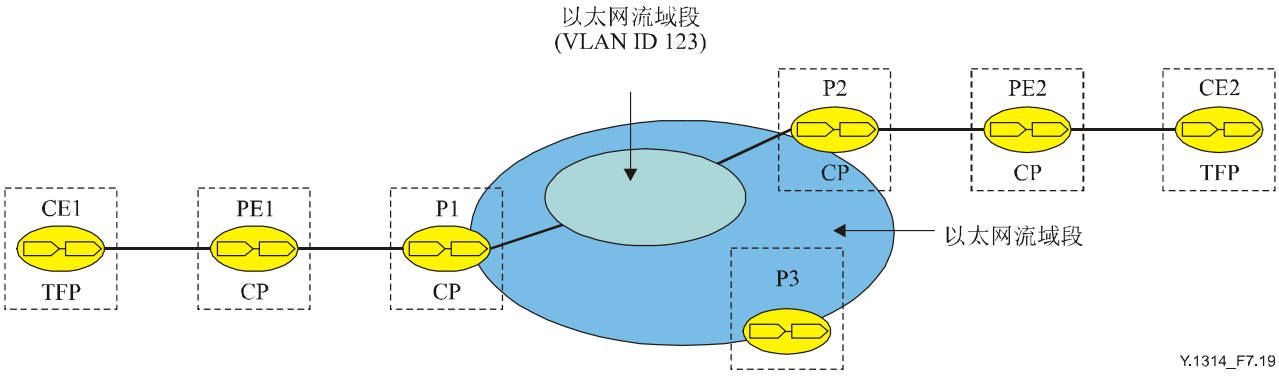


图 7-19/Y.1314－用分区进行模型描述的对等层VPN

图 7-19 描述了对等层 VPN 的拓扑，还显示了对应的 VLAN（123），但没有提供有关 VPN 在何处开始和终结，也即 IEEE 802.1Q VLAN 标记在何处插入/删除的信息。从图 7-19 的模型很容易看出：节点 P1 和 P2 是 VLAN 的一部分，但尽管 PE1 和 PE2 是 VPN 的开始/终结点，模型恰并没有给出这一信息。然而，只要将 VPN/服务器层的适配功能加入这分区模型，并进一步描述 VPN 层特定的进程就可以提供这种信息（如图 7-18 所示）。

8 VPN拓扑的支持

本建议书所用的术语“VPN 拓扑”是指从 VPN 客户角度来看的 VPN 拓扑，也即 VPN 站点之间的拓扑，VPN 站点可以是 CE 节点或末端系统。VPN 站点之间的连通性只有在它们之间的 VPN 服务器层或对等层的路径已经建立时才能提供。一般地，在 n 层的拓扑决定于在 n-1 层上服务器层路径所提供的拓扑。一旦 VPN 服务器或对等层的路径已经建立，如果 VPN 客户层或对等层的技术是包交换的，那么就有可能通过限制 VPN 内某些站点之间的连通性来修剪 VPN 的拓扑。限制 VPN 成员间连通性的一种方法是控制 VPN 客户层上的路由分配（VPN 站点，如果相互间没有路由可以通达，就不能通信）。另一种可用于限制连通性的方法是使用包过滤（例如基于 VPN 客户层和对等层上的源/目的地地址）。如第 8.1、8.2 和 8.3 节所描述的，有三种基本的 VPN 拓扑，它们是全互连、部分互连以及中心和幅条。

8.1 全互连的VPN拓扑

在全互连的 VPN 拓扑中，正如图 8-1 所描述的，每一个 VPN 站点都有一个路由/连接通往其他的每一个 VPN 站点。

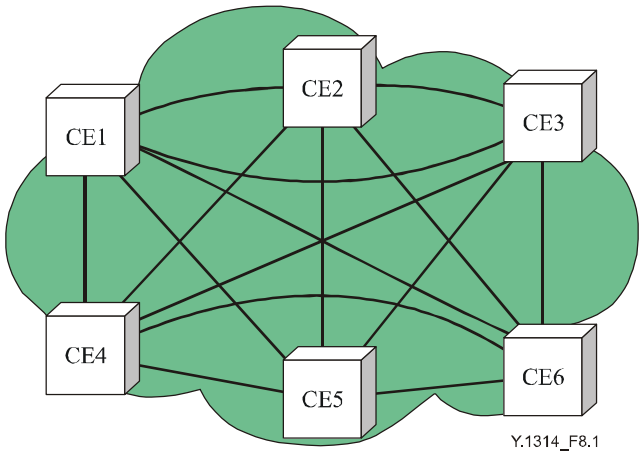


图 8-1/Y.1314－全互连VPN拓扑的一个例子

全互连拓扑提供了完整的冗余，由于 VPN 站点可以使用最短/最好的路由相互通达，它也能提供高效的网络利用率和性能。全互连的一个缺点是：全互连要实现可能会很贵，尽管这一点决定于所采用的 VPN 网络模式/技术（例如由 ATM VC 全互连构成的 VPN 网络很可能会贵于支持任何到任何连通性的以太网 VPN）。另一个缺点是：随着全互连站点数的增加，连接/路由和控制面邻接关系的数量会成比例地增长（设 n 为 VPN 的站点数，那么全互连中的连接数量为 n(n–1)/2）。要支持大量的连接/路由和控制平面的邻接关系，由于所需带宽和 CPU 资源的增加，会带来扩展性问题。

8.2 部分互连的VPN拓扑

在部分互连的 VPN 拓扑中，VPN 站点有路由/连接通往一些 VPN 站点，但不是所有的站点。图 8-2 提供了部分互连拓扑的一个例子。

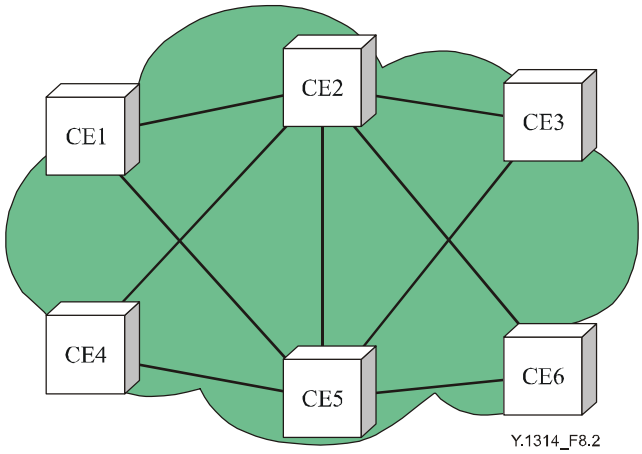


图 8-2/Y.1314－部分互连VPN拓扑的一个例子

在某些情况下，VPN 站点有可能能经由中转的 VPN 站点通达没有直接路由/连接的其他 VPN 站点。然而，在其他情况下，如果 VPN 站点没有直接的路由/连接可相互通达，那么它们之间就可能不能通信。在没有直接路由/连接相互通达的节点之间，进行通信的能力取决于 VPN 服务器层或对等层路径的存在以及对拓扑连通性的任何限制（例如选路策略或包过滤）。由于所需带宽和 CPU 资源减少了，部分互连的拓扑比全互连更能扩展，尽管这是以牺牲最佳路由和高效的网络利用为代价的（如果某些 CE 要用于作为中转节点）。尽管部分互连网络在设计上通常会在最需要的场合使用冗余的路由/连接，网络的冗余也同样减少了。例如，在图 8-2 中，CE 节点 CE2 和 CE5 可以作为核心节点，而其他 CE 节点作为边缘节点。这一拓扑在这种情况下，边缘节点将有冗余的路由/连接通达核心。客户通常由于开支（也即全互连比较昂贵）或地理限制等因素而被迫使用部分互连的拓扑。

8.3 中心和幅条的VPN拓扑

在中心和幅条（或星型）的拓扑中，一个 VPN 站点，对于一个特定的 VPN 而言，可以是一个幅条或者是一个中心（如果一个 VPN 站点属于多个 VPN，它对于某些 VPN 可以是中心，而对于其他是幅条）。中心和幅条拓扑中的所有幅条都有直接的路由/连接通达中心，但没有直接的路由/连接可以相互通达。图 8-3 显示了中心和幅条拓扑的一个例子，在此 CE2 是中心，所有其他的 CE 节点是幅条。

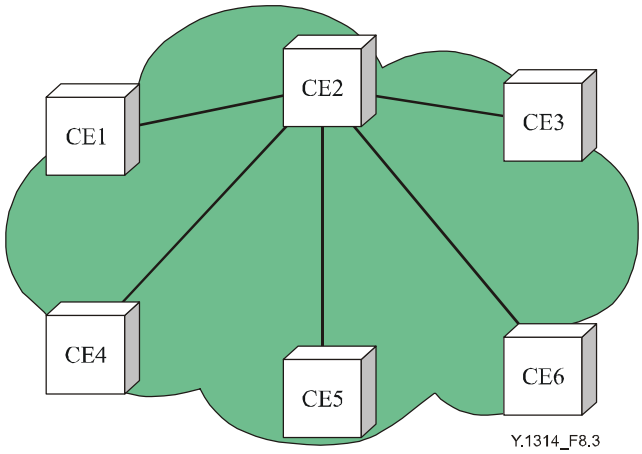


图 8-3/Y.1314－中心和幅条VPN拓扑的一个例子

在某些情况下，可以将中心配置成中转节点，使得幅条可以经由中心相互通信。然而在其他情况下，幅条之间的连通性可能是不允许的。中心和幅条拓扑一种普遍的使用是将办公点（幅条）连接到公司的总部（中心）。采用中心和幅条的拓扑将可以使用集中的网络资源（例如互联网的接入、防火墙和电子邮件服务器），它与分布的网络资源配置相比可以带来开支的节省。

9 VPN QoS的考虑

关于服务质量（QoS）有大量的信息资源，它们对于 QoS 到底是什么具有不同的定义。ITU-T E.800 建议书将 QoS 定义为服务性能集合的效果，这种集合效果决定了服务用户的满意程度。ITU-T G.1000 建议书提供了通信服务质量的框架和定义，而 ITU-T G.1010 建议书定义了基于用户观点的多媒体服务质量的等级模型。在这些建议书以及它处所定义的满足服务质量要求所需的功能将决定于网络的操作模式。因此对于服务质量的要求对于 VPN 服务提供商选择 VPN 服务器层的技术以及可以支持的 VPN 客户层的技术可能会有影响。

9.1 电路交换的层网络

在面向连接电路交换的层网络中，在连接持续期间将建立一个基于物理链路、光波长、SDH/SONET VC 或 TDM 时隙的通道，专门用于 AP 间的单个连接。当一个新连接被请求时，网络必须确定是否接受该连接，如果接受，进而确定如何经由网络为它选路以及为连接保留什么资源。将使用连接接纳控制（CAC）机制在带宽可用时接受连接，或者在请求的连接带宽超过可用带宽时加以拒绝。

数据是以恒定的比特速率按它送出时完全相同的顺序发送的。连接可以采用静态指配人工地建立，或者用信令机制或自动的指配工具动态地建立。能否建立新连接的能力决定于网络是否有空余能力。如果连接已经建立，那么跨越连接的数据传递是有保证的。

在如同 PSTN 那样的 CO-CS 网络中，时延主要地是传输距离的函数。CO-CS 网络节点的交换时延与传输（传播）时延相比相对较小，尤其是当呼叫跨越长距离的干线时。

9.2 包交换的层网络

在包交换网络中，数据包是按照包头中的信息转发的。包交换在提供连通性的同时，通过由许多用户共享网络资源（它假设：不是所有用户所有时间都需要使用资源的）使网络资源得到高效的利用。信流或连接的包转发行为可以用一组被称为业务流描述语的参数来描述。业务流描述语的例子有包/比特速率，最大的突发长度/包长度和数据包在固定时间间隔内到达的概率。用户的质量要求通常用可接受的包丢失率、时延和抖动来表达。

可以使用业务流的整形机制来调节网络所接纳的业务流量，这种调节一般地是在逐个队列/信流、逐个连接或逐个接口的基础上进行的。在基于数据包的网络中，如果业务流量超过了网络实体（NE）的转发能力或可用的网络容量，会发生拥塞。当网络变得拥塞时，数据包可能被缓冲存储或者丢弃，缓冲存储将引入时延。

在包交换网络中，时延决定于与底下的物理的服务器层相关联的传输距离，再加包交换层的一些其他因素。在包交换层引入时延的因素有包长度、链路速度、逐跳的转发时延（它又可以分解为装包、压缩/解压、交换/选路以及缓冲存储的时延），还有跳数。在基于数据包的网络中为了保证范围广泛的质量水平，优先级控制是需要的。一般地讲，优先级控制是通过逐个连接、逐个信流和每一接口上逐个 QoS 等级地采用分别的队列，并控制每一队列的优先级来实现的。可以采用包排序机制将数据包按照特定的策略分配到具体的队列。

9.2.1 面向连接包交换的

在面向连接包交换的层网络中，连接将建立，并保持到连通性不再需要时为止（而不管数据是否要发送）。正像面向连接的电路交换层网络一样，连接可以经由人工的指配、管理系统或信令协议来建立。网络当前的状态可以通过监测网络资源的利用和/或对已接纳连接行为的特征描述来确定。可以用 CAC 机制来为恒定比特率（CBR）的业务流信源预留需要的连接的峰值带宽。另一种做法是与 CAC 机制一起采用统计复用的方案，分配的带宽小于所需的峰值带宽，以提高网络效率。然而，由于所需的带宽会随时间有很大的变化，要描述所请求连接的带宽特征是很困难的。

在 CO-PS 网络（例如 ATM 网络）中，如果要支持的是 CBR 服务（而且没有过度的预订），逐跳的转发时延将保持恒定，因而时延/抖动将可以计算/保证。然而，如果为了提高网络利用率，服务会过度预订（服务通常是这样），那么在拥塞的节点由于缓冲存储或者丢弃超过契约的业务流，将会引入时延/丢失。尽管逐跳的转发时延变成为可变的，但其他因素，如链路速度、距离/跳数（以及 ATM 情况下的包长）将保持不变。

9.2.2 无连接包交换的

在无连接包交换的网络中，数据一旦送出，连接就中断了，直到有进一步的信息要发送或接收（一个数据包可以看成是一个连接，它在数据包被发送和接收所用的时段内存在）。这里没有储存的连接状态，因而，相继的数据包不必要遵循同一个路径，或者按它们送出的顺序到达。业务流是以可变的比特速率送出的，资源通常是按先来先服务的原则分配的。

在 CL-PS 网络（如 IP 网络）中，决定时延的因素，如包长度、链路速度、跳数和逐跳的转发时延都是可变的，尤其是当采用提供负荷平衡的技术时。可以在边缘实现速率限制/业务流整形以限制进入网络的业务流量，但由于 CL-PS 业务流任意到任意的特性（以及对等联网的增长），将很难预测跨越 CL-PS 网络逐个链路的带宽利用率。可以采用业务流监测连同模型化技术一起来获得业务流矩阵，并抓取 IGP 的性能来提高链路利用率，但由于 CL-PS 业务流的突发性和不可预测性，要使服务保证得到满足的一个最为简单/最为安全的方法是过量地装备网络。

然而，即使是过量装备，由于无连接业务流的不确定性，CL-PS 网络中节点/链路仍可能会拥塞，尤其是当发生链路/节点故障和拒绝服务攻击（DoS）时。不仅如此，链路/节点故障的影响还不只限于穿越这故障链路/节点的业务流，重新选路还会导致网络中其他地点的拥塞。一个保护重要业务流免遭拥塞的通常做法是采用基于优先级的队列（例如基于 RFC 2475 用于 IP 的差别服务架构）来控制逐个等级的转发行为，也即较高优先级的业务流将得到比较低优先级业务流更为优先的处理。这使得提供商可以向客户提供多层次的服务（例如，首要的、实时的、尽力而为的），并据此对服务定价。差别服务（Diffserv）方法的一个缺点是：带宽只是在逐个集合的基础上预留的，因而集合中单个信流的传递将不能保证。

另一个可供选择（或补充）的方法是采用综合的服务架构（基于 RFC 1633），在此将采用资源预留协议（RSVP、RFC 2205），它通过在数据包发送前先传送有关信流要求的信令来沿着端到端的路径预留能力。由于带宽是在逐个信流的基础上预留的，将有可能为单独的信流提供有保证的传递。这一点再现了 CO 网络中使用的 CAC 模型，在 CO 网络中为了保证网络有足够的能力，在 CAC 已执行之前是不发送业务流的。这种方法的主要缺点是：它会给核心路由器带来相当的（RSVP）处理负荷，这种负荷随着需要资源预留的包信流数量的增加将成正比地增加。

另一种支持在逐个流基础上预留资源的方法是使用基于信流的路由器。基于信流的路由器保持每个流的状态，它只在有足够的可用资源时才接受新的信流。如同用 RSVP，这一方法的挑战是处理负荷将随着信流数的增加而增加。然而，至今还没有可用的路由器，能为大量的信流支持逐个流的选路。

10 客户机/服务器VPN建立所需要的功能

在客户机/服务器 VPN 的建立过程中，对于必定要发生的事件有一个严格的顺序。VPN 客户层信流/连接在 VPN 服务器层信流/连接已经建立之前是不能建立的。同样地，VPN 服务器层信流/连接在服务器层连接/信流（对于它 VPN 服务器层是一个客户）已经建立之前是不能建立的。采用这种信流/连接的建立顺序的原因：客户层的拓扑是由下面的服务器层的拓扑确定的，这种情况可以循环下去直到管线。

10.1 VPN服务器层的建立

这里假设：下层的服务器层拓扑已经建立，而且 VPN 服务器层的 TCP/TFP 和 CP/FP 已经用地址进行了配置，那么在 VPN 客户层成员之间 VPN 服务器层连通性的建立将涉及 3 个主要的步骤：

步骤 1：发现 VPN 成员，并存储 VPN 成员信息。

步骤 2：计算 VPN 服务器层上 VPN 成员之间的路由。

步骤 3：在 VPN 服务器层上 VPN 的成员之间建立连接/隧道/VLAN。

支持 VPN 服务器层建立和保持所需要的每一个功能以及各单独的功能实体已经进一步在表 10-1 中描述。

表 10-1/Y.1314－VPN服务器层功能

功　能	功能实体	网　元	服务器层的工作模式
VPN 成员关系的发现	VPN 成员（属于同一 VPN 的 VPN 客户层 CP/FP）的发现	PE	所有
	VPN 成员信息（包括加入、离开、可用性）的分发/收集	PE	所有
	VPN 成员信息的保持	PE	所有
	VPN 客户层 CP/FP 到 VPN 服务器层 AP 的映射	PE	所有
VPN 服务器层选路	VPN 服务器层通达性/拓扑/资源信息的分发/收集	PE, P	所有
	VPN 服务器层通达性/拓扑/资源信息的保持	PE, P	所有
	VPN 服务器层 AP 之间最佳路由的计算	PE, P	所有
VPN 服务器层隧道/连接的建立	连接接纳控制（CAC）	PE, P	所有
	连接/隧道请求成功/失败的通告	PE, P	所有
	VPN 服务器层去复用字段的分配和配置	PE, P	所有
	连接/隧道的信息，如 QoS、去复用字段、带宽等的分发	PE, P	所有

10.1.1 VPN成员关系的发现

为了建立PE之间VPN服务器层的拓扑，首先有必要确定哪些PE是连接到哪个特定客户机/服务器VPN成员的CE的。这一功能可以由操作人员依据已知的网络拓扑人工地执行。或者，这一功能也可以经由集中的服务器/系统或分布式协议动态地执行，以便使指配进程能自动化/简化。为了支持动态的发现，PE 必须配置以 VPN 识别码，来指示它们要连接到特定 VPN 的一个或多个 CE。用于发现的集中的服务器/系统的例子是使用认证服务器（例如 RADIUS），用它作为客户认证进程的一部分来分发关于 VPN 成员的信息。分布式协议的例子是将 BGP 用于 RFC 2547 VPN，它用路由目标作为 VPN 识别码，确保 PE 只接收那些是成员的 VPN 的信息。

10.1.2 VPN服务器层的选路

在信源/信宿 VPN 服务器层端点之间，如果底下的服务器层（VPN 服务器层底下的层）是单个一跳的P2P 连接/信流，由于只有单个路由/通路可用，不需要进行选路。但另一方面，如果有可选择的路由/通道能经由中间点到达同一个目的地，或者底下的服务器层提供一个 P2MP[4]拓扑，那么就必须在 VPN 服务器层上进行选路，以找到拓扑和/或计算通达目的地的最佳路由。

10.1.2.1 选路的需要

在 CO 层网络的情况下，在给定层上的路由/通道已经算出之前，信令是不能进行的。在 CL 层网络的情况下，在到达目的地的路由已经算出/配置之前，数据包是不能转发的。这并不是说，网络的每一个节点都需要有明确的路由通往网络中其他的每一个节点。网络地址的归纳通常与选路区域的等级架构相结合使用来改善可扩展性。地址归纳的最终形式是使用默认路由，它可以作为一种“百达”机制来转发数据包，而不论其目的地地址。

对于 CL 数据包在路由计算完（或默认路由已配置）以前不能转发这一规则的一个例外是当 CL 技术支持广播时。广播是指将数据包跨越拓扑中所有的服务器层路径（不包括收到数据包的路径）复制和转发到未知的目的地地址。支持这种功能特性的技术的一个例子是以太网。这种规则的另一个例外是令牌环网的运行模式。在令牌环层网络中，当节点接收到数据包时，它重发这数据包将它送往环中的下一个节点，直到数据包环回到源节点时被删除。目的地节点保留一个数据帧的拷贝，并通过在帧中设置响应比特来指示它已经接收到数据帧。尽管有一些技术，它们不需要选路，但应该指出：这些技术作为 VPN 服务器层技术是不理想的。对于那些扩展到很大的地理地区包含有大量节点的层网络、选路，连同分等级的地址结构都是很基本的要求。从 VPN 的角度，诸如广播和令牌传送等机制是固有地不安全的，而且对于单播（P2P）的业务流传输效率也是很低的。

4 这里对P2MP的引用从单个源点PE而言是指出网的服务器层拓扑。基于PE间双向连接/信流的全互连/部分互连，整个层网络实际的拓扑可以是任意到任意的。

10.1.2.2 需要选路的网络拓扑例子

图 10-1 示出一个有两个可选择的路由/通路（A 和 B）通往同一目的地的网络的例子。

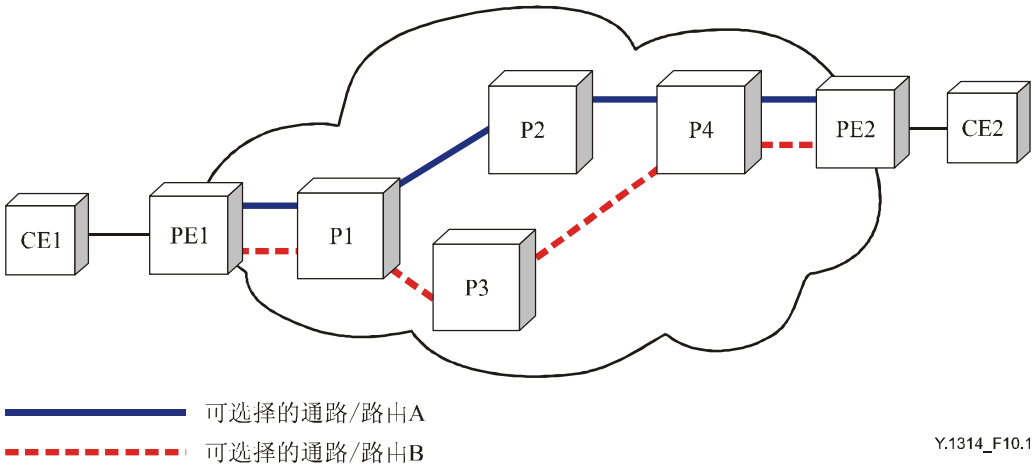


图 10-1/Y.1314－多个路由/通路通往同一目的地

正如图 10-1 所示，从 CE1 到 CE2 的路由 A 穿越了 PE1、P1、P2、P4 和 PE2，而路由 B 穿越的是 PE1、P1、P3、P4 和 PE2。这一信息在图 10-2 中用功能模型进行了描述。

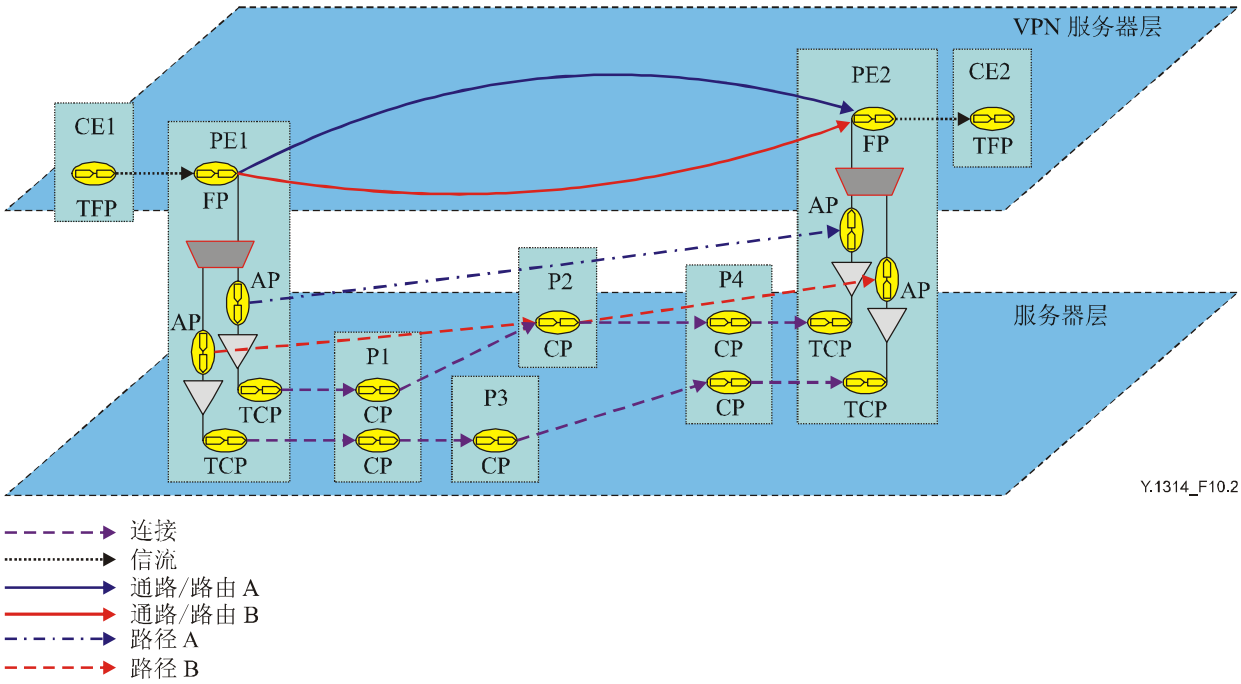


图 10-2/Y.1314－多通路/路由的功能模型

图 10-2 示出两个可供选择的服务器层路径（A 和 B），可以由 VPN 服务器层使用。依据由 VPN 服务器层选路功能计算的路由，有一个服务器层路径将被选出（或者两个，如果需要负荷平衡），以便在位于 CE1 的 VPN 服务器层信源 TFP 和位于 CE2 的信宿 TFP 之间传送 VPN 服务器层的信流。

图 10-3 示出服务器层从 CE1（源点）到 CE2、CE3 和 CE4（P2MP 拓扑中的信宿分支）提供 P2MP 连通性的案例。

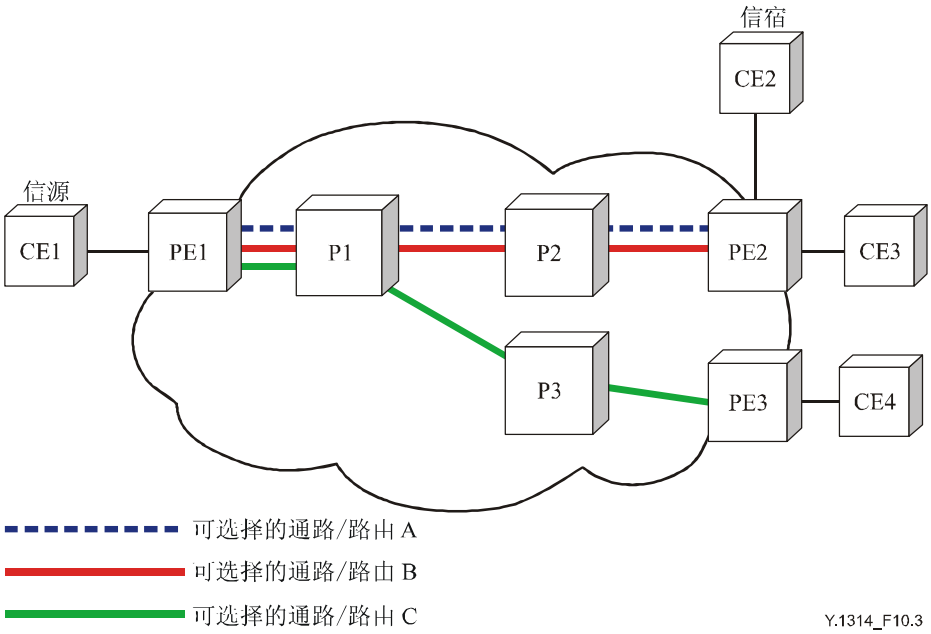


图 10-3/Y.1314－P2MP服务器层拓扑

图 10-3 中的网络被作为功能模型在图 10-4 中示出。

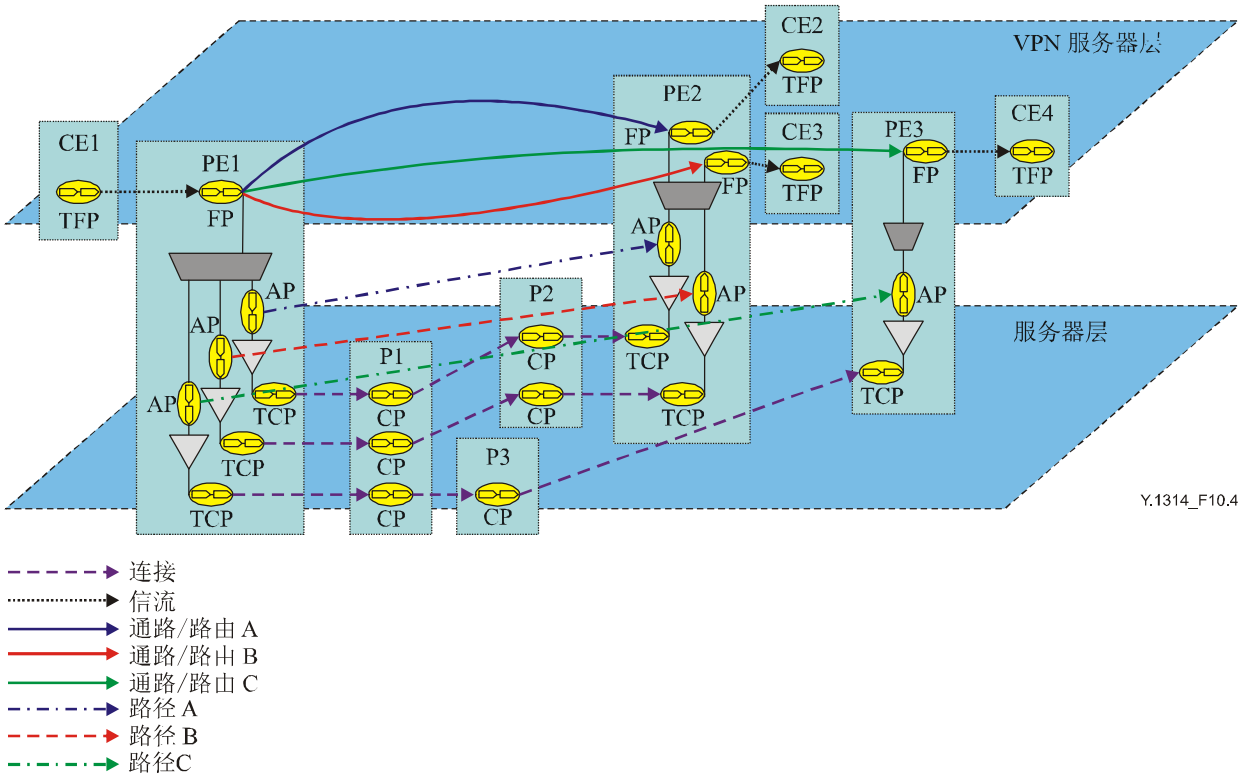


图 10-4/Y.1314－P2MP服务器层拓扑的功能模型

如果 CE1 是一个特定 VPN 服务器层信流的信源，CE2 是它的信宿，那么 CE1 需要知道用什么路由通达 CE2。然而，图 10-4 中显示的 VPN 服务器层中的路由/通路是由底 F 的服务器层中的 P2P 路径提供的，也即在 P2MP 拓扑中只有一个路由存在，它从信源的 TFP 到每一个分支信宿的 TFP。这意味着选路功能只需要将拓扑弄明白；它不需要进行路由计算（因为到每一个信宿只存在一个路由）。随着拓扑的发现，从 CE1 去往 CE2 的信流将使用由服务器层路径 A 提供的路由/通路 A。

10.1.2.3 可选择的选路方法

当需要选路时，一个操作人员可以执行选路功能，在这种情况下，操作人员基于已知的拓扑和资源利用信息计算跨越网络的路由。选路可以人工地执行的一个例子是当 VPN 客户层基于 IP 时对双宿的 CE 节点进行配置。在这一例子中，有意义的是使用静态路由（也即一个主用，一个浮动的默认路由），因为只有两个可选择的路由存在。

如果使用网络管理系统来执行选路功能，那么管理系统必须通过请求或收集可通达性/拓扑/资源信息来寻找网络拓扑，然后利用这些信息计算路由并将选路信息分发给网络节点。选路由 NMS 执行的一个例子是跨越基于 SDH 的层网络建立 P2P 的连接。在连接可以建立之前，NMS 必须首先计算穿越网络的最佳路由。

如果使用动态的选路协议来执行选路功能，那么可通达性/拓扑/资源信息将经由选路协议跨越网络分发到每一个节点，并用来计算通达目的地的最佳路由。动态选路协议的一个例子是用于 ATM 层网络的 PNNI 构件（它也可以和其他的网络技术一起使用），它用于寻找网络拓扑并为动态连接计算路由。另一个例子是 RPR，它使用拓扑消息来弄清环路拓扑。当一个节点接收到拓扑消息时，它将它的 MAC 地址附在上面，并传递给环上的下一个节点，最终数据包将带着环路拓扑图（地址清单）返回到它的源点。

在控制面上使用动态选路协议的另一种方法是使用数据平面上的地址学习，利用这种操作模式的网络技术的例子是以太网。以太网采用生成树（通过网络拓扑的删改避免环路）和数据平面上透明的桥接（基于源地址的学习）来将数据包转发到正确的目的地，而不必要将它们广播到所有的节点/端站。然而，如果要使用数据平面上的地址学习，为了将数据包转发到还不曾得知的目的地地址，这网络技术就也必须支持广播。由于路由在带有它相对应地址的数据包已经接收之前是不知道的，数据平面上的地址知识不能用于执行 CO 层网络的选路功能，它只适合于 CL 层网络。

10.1.3 VPN服务器层的信令

为了本建议书的需要，信令是指建立 CL 隧道（例如 L2TP 隧道）和 CO 连接（例如 ATM VPI/VCI）所需要的信息交换。所需要的信息包括诸如复用/去复用字段、QoS（例如时延、抖动）、带宽、加密密钥和恢复力（例如 1+1 保护）等参数。

隧道和连接之间的一个关键的不同点是：连接，在任何用户数据可以发送之前，总需要有信令（或者人工的指配）来建立连接。尽管某些隧道技术（例如：L2TP 隧道，明确配置的 GRE 隧道）在用户数据发送以前也需要信令传送隧道的参数，但其他的，如软/动态的 GRE、IP-in-IP 隧道都不需要任何信令。这些隧道技术只是依据本地的策略/选路信息简单地将 VPN 客户层数据包装入到 VPN 服务器层的包头内。在隧道信源/信宿端点之间遇到的中间节点（P）只是查看 VPN 服务器层的包头来确定是否以及如何将这数据包转发到 VPN 服务器层的信宿（目的地 PE）。VPN 客户层包头仅当数据包到达 VPN 服务器层信宿所在的目的地 PE 时才使用。还请注意：在内部的 VPN 客户层包头中，中间节点通常是不能有任何意义的（例如能够选路）。

在连接建立时要执行连接接纳控制（CAC）来确定在底下的服务器层上是否有足够的带宽以维护客户层的 QoS 要求。客户层信令期间将使用业务流描述语（如 ATM 中用的峰值信元速率（PCR）和持续信元速率（SCR））从底下的服务器层请求适当的资源。依据客户层的请求确定在服务器层有多少带宽可用的能力意味着：在控制平面上 CAC 功能与服务器层和客户层必须都是对等的关系。

在 CO-CS 服务器层的情况下，CAC 是依据被请求的服务器层上可用的物理带宽的数量（例如空闲的 TDM 时隙或 WDM 波长）。在 CO-PS 服务器层的情况下，CAC 是依据未被现有连接使用的空闲的带宽数量。这种信息是通过在那个特定层网络的每个节点上保持有关每个连接的状态信息（例如：建立/中断，所用资源的数量）而得到的。与可用带宽受限于可用的物理带宽的 CO-CS 层网络不同，在 CO-PS 网络中，在网络的每一个节点必须要逐个连接地进行管制，以保证每个连接只发送/接收连接建立时约定的业务流量。

在 CL-PS 服务器层网络的情况下，CAC 可以依据物理/逻辑接口或队列/信流/服务等级水平的可用带宽来执行。如同 CO-PS 层网络，管制必须在网络的每个节点上依据所请求的带宽来执行。然而，与 CO-PS 上为每一个连接保持状态的情况不同，相当的（也即逐个信流的）信息在 CL 层网络上通常不保存[5]。这一点，再加上 CL 业务流不确定的任意到任意的特性，意味着：CL 层网络中的 CAC 将取决于广泛使用业务流监测和模型描述来求得业务量矩阵以及网络的过量装备来保证带宽是可用的，尤其是在故障情况下。如果需要逐个 VPN 的严厉的 CAC 以及严格的 SLA，那么应该使用 CO 的服务器层网络，而不是 CL 的服务器层网络。

10.2 VPN客户层的认证/配置

在 VPN 客户层 CE 和 PE 节点之间建立连通性所需要的功能可以使用静态的指配或动态的协议来实现。静态指配可以通过人工配置或自动的网络管理系统来实现。建立 VPN 客户层连通性所涉及的功能实体如表 10-2 所示。

[5] 例外的情况有使用RSVP RFC 2205（基于端到端信令的解决方案）和信流状态的选路（逐跳的解决方案），在此将保持每个信流的状态，在没有足够的带宽可用时将拒绝新的信流。

表 10-2/Y.1314－VPN 客户层认证和配置功能

功　　能	功 能 实 体	网元	VPN 客户层模式
CE/用户认证、授权和记账（AAA）	认证：基于认证参数的 CE/用户识别，认证参数的例子有有效的用户名和口令	CE, PE	所有
	授权：允许或拒绝接入 VPN 客户层网络的资源/服务	CE, PE	所有
	记账：所用资源/服务的测量	CE, PE	所有
VPN 客户层网元配置	跨越 VPN 客户层 CP/FP 和 TCP/TFP 对 VPN 客户层网络的地址进行分配和配置	CE, PE	所有
	跨越属于同一 VPN 的 VPN 客户层 CP/FP 对 VPN 识别码进行分配和配置	PE	所有
	逐个 VPN 概况和策略的配置	CE, PE	CO-PS, CL-PS

10.2.1 CE/用户的AAA

CE/用户的 AAA 功能控制 VPN 客户层的接入，对策略进行强制，支持对使用的审核，并提供 VPN 服务必要的记账信息。AAA 功能可以由 CE 连接的 PE 装置来执行，由单独的装置来执行，或者两者的混合。

在某些情况下可能需要集中的认证服务器用于用户/CE 的认证，而在另一些情况下可能只有 CE 和 PE 与认证进程有关。前者的一个例子是将 IEEE 802.1X 用于以太网 CE 装置的认证。在这一例子中，PE 是认证者，集中的认证服务器则将用于执行认证。后者的一个例子是对来自 CE 的控制消息（例如 BGP 消息）的认证，目的是鉴别消息源点，防止欺骗。

10.2.2 VPN客户层网元的配置

在 VPN 客户层指配期间，在客户和提供商网络边缘的网元必须用下列参数进行配置：VPN 客户层网络地址，VPN 客户层网络去复用字段，VPN 识别码，逐个 VPN 的策略/特性。配置可以在认证/授权的进程中进行，或者单独地执行。前者的一个例子是：在成功的认证之后，CE 可以依据从认证服务器收到的信息自动地以特定的带宽分配和数据包标记特性进行配置。后者的一个例子是使用人工配置或动态主机配置协议（DHCP）给 CE 分配 IP 地址。

要在 PE CP/FP 和 CE TCP/TFP 或 CP/FP 配置的 VPN 客户层地址是属于 VPN 客户层网络的地址（例如：IP VPN 客户机的 IP 地址，或者 ATM VPN 客户机的 ITU-T E.164/NSAP 地址）。

客户层网络去复用字段仅在有多个 VPN 客户机要跨越同一个 CE 到 PE 的链路进行运载，或者所用的 VPN 客户层网络技术总是带有去复用字段时，才有需要。前者的一个例子是以太网 VPN 层网络，它在需要支持多个 VPN 时只需要使用 VLAN 标记。后者的一个例子是 ATM，它在业务流单元（信元）的头部总是使用 VPI/VCI 值。在某些情况下，去复用字段的配置将决定于物理的配置，而不是包头中一个值的配置（例如在 PE 将一根光纤连接到正确的入口接口上对应于出口上正确的 DWDM 波长）。

虽然 VPN 识别码是用于识别一个特定 VPN 的一个名字，它只在需要支持动态 VPN 成员发现和信令时才需要分配/配置，但从运行的角度（例如协助故障处理、记账）也可能是有用。VPN 识别码用于动态发现和信令的一个例子是 RFC 2547 VPN 中使用的路由目标属性。在 PE 上 VPN 识别码可以经由人工/OSS 指配静态地进行配置，或者动态地配置（例如使用 RADIUS 作为认证进程的一部分）。如果 VPN 识别码要用于发现/信令，那么它至少在单个选路/信令区域内应该是惟一的（如果需要支持 AS 之间/提供商的 VPN，理想地应该全球惟一）。

对于基于数据包的 VPN 客户，可能需要在 CE 装置、PE 装置或者在两者中进行逐个 VPN 概况和策略的配置。依据 VPN 服务可能需要进行配置的 VPN 的特性和策略包括：速率限制/业务流整形，数据包标记/分类，多宿站点路由/连接的选择（也即一个主用，一个备用）。

10.3 VPN客户层的选路和信令

如同 VPN 服务器层，当在信源和信宿 TCP/TFP 之间存在有多个路由/通路时，或者当 VPN 服务器层路径在 VPN 客户层上建立 P2MP 拓扑时，VPN 客户层的选路是需要的。如果 VPN 客户层是 CO，并且 VPN 客户层上要支持动态的指配，那么信令也是需要的。

这里有一点很重要需要说明：在 VPN 客户层选路/信令能进行之前，VPN 服务器层的路径必须先建立。VPN 客户层数据平面的拓扑是基于底下的 VPN 服务器层路径的拓扑，因此，在 VPN 服务器层路径建立之前，不可能执行路由的计算或连接/隧道的信令。

VPN 客户层的选路和信令功能以及各单独的功能实体已经在表 10-3 中描述。

表 10-3/Y.1314－VPN客户层的选路和信令功能

功　　能	功 能 实 体	网元	VPN 客户层模式
VPN 客户层选路	VPN 客户层可通达性/拓扑/资源信息的分发/收集	CE, PE	所有
	VPN 客户层可通达性/拓扑/资源信息的保持	CE, PE	所有
	VPN 客户层 AP 之间最佳路由的计算	CE, PE	所有
VPN 客户层隧道/连接信令	连接接纳控制（CAC）	PE, P	CO-CS, CO-PS
	连接/隧道请求成功/失败的通告	PE, P	所有
	VPN 客户层去复用字段的分配和配置	PE, P	所有
	VPN 客户层连接/隧道信息，如 QoS、去复用字段、带宽等的分发	PE, P	所有

10.3.1 任意到任意CL-PS VPN客户层连通性

如果 VPN 服务器层路径为有多个站点的 CL-PS VPN 客户层网络提供一个任意到任意的全互连/部分互连的拓扑，那么包含有 VPN 客户层 TFP/FP 的节点（也即 PE/CE 节点，但不是 P 节点）必须依据 VPN 客户层的地址信息对于往何处转发数据包做出转发决定。这意味着：CE 和 PE 节点必须经由控制面采用动态选路协议交换 VPN 客户层的选路信息，或者采用人工的或 OSS 指配对静态路由进行配置。动态选路协议或静态路由以外的另一种方法是使用数据平面上的地址学习，以太网就是这种情况，它使用基于源点的地址知识将业务流单播到正确的目的地。

每个 VPN 的选路信息必须与其他 VPN 的选路信息相隔离。这是为了提供 VPN 转发的分离（也即确保数据包不转发给属于不同 VPN 的节点），并允许使用重叠的 VPN 客户层地址空间。这一点可以逐个 VPN 采用物理上分离的 PE 来实现，或者采用共同的 PE，但它具有逻辑/虚拟分离的选路信息数据库。另一种方法是使用共同的 PE 和路由表，但为每一个 VPN 客户分配不同的地址空间[6]。支持 VPN 客户层选路的 VPN 解决方案的一个例子是 RFC 2547。RFC 2547 使用动态或静态的 CE 到 PE 的选路，连同 MP-BGP，在 PE 之间分发 VPN 客户层的选路信息，并使用分离的虚拟路由表提供 VPN 客户层路由的分离。

10.3.2 按需的VPN客户层动态连接的建立/拆除

在大多数情况下，CO-CS 和 CO-PS VPN 客户层连接是经由人工的或 OSS 指配静态地配置的。然而，如果需要动态按需的连接建立，那么在 VPN 客户层所有的 CP 和 TCP 之间（也即 PE 和 CE 节点之间）必须建立控制面对等交换（选路和信令）的对等关系。此外在连接建立时还必须执行 CAC 以确定在 VPN 客户层是否有足够的带宽用于 VPN 客户层连接。这意味着：CAC 功能与 VPN 服务器层网络和 VPN 客户层网络的控制面都必须是对等的。如果 VPN 服务器层和客户层的技术不同，那么在 VPN 客户层和服务器层之间必须进行对等的控制面互通。

10.3.3 客户控制的按需连接

客户控制按需动态的连接是指客户对 CE 节点有某种（或全部）控制的情况，这种控制使它们可以建立新的 VPN 客户层连接。从客户的角度，这种能力的优点是：这将给它们以灵活性可以在它们需要时动态地建立 VPN，并据此对它们的使用收费。例如，客户会希望短时地建立一个按需的连接来下载/上载一个大的文档（例如一个应用或一个电视文档），或者建立一个可靠的连接用于电视会议。按需动态 VPN 客户层连接建立的一个使用例子是使用 PNNI 来建立/拆除跨越 VPN 服务器层路径的用虚通路提供的 SPVC。

在考虑加入对按需动态 VPN 客户层连接的支持时，一个要考虑的重要因素是地址/拓扑信息的分发。服务提供商由于安全的原因不大愿意向客户暴露它们的网络拓扑或内部的网络寻址。因此对于 PE 的选路功能，要求将可通达性信息只分发到 CE。另一个重要的考虑是做出决定：连接建立时如果带宽不可用应采取什么动作。建立 VPN 客户层新连接的能力取决于信源和信宿端点之间服务器层路径的可用性。如果路径不存在，或没有足够的带宽，那么，必须或者拒绝连接，或者建立新的 VPN 服务器层连接/隧道（或给现有的连接/隧道增加带宽）。为了建立新的 VPN 服务器层连接/隧道，或者增加现有连接/隧道的带宽，必须要执行 CAC 以保证底下的服务器层的带宽是可用的。

---

6 这一方法有多个重要的缺点：它需要服务提供商仔细地管理地址空间，需要客户对使用服务提供商分配的地址取得一致（客户可能要求使用他们自己的地址），需要包过滤以保证VPN间的隔离，而这是件冗长乏味容易出错的工作。

如果服务器层是 CL，要执行严厉的 CAC 是不可能的，为此网络必须要过量装备以允许新的 VPN 服务器层隧道能得以建立。这一方法的缺点是：它需要细致的网络规划和控制/强制，以保证现有 VPN 服务器层的隧道不受任何影响。如果底下的服务器层是 CO，那么可以执行严厉的 CAC 来确保对于建立新的 VPN 服务器层连接/隧道带宽是可用的。然而，在 n 层的每一个连接请求对 n-1 层可用的带宽会有影响，这一点将循环一直到管线。随着我们接近管线，带宽颗粒度和指配/保持的时间将增加。一般地，如果底下的服务器层没有足够的能力支持新的连接，这连接就应该拒绝。服务器层的能力应该按照能力的规划活动（包括网络模型描述和应用分析/预测）的结果来提供的。

10.3.4 服务提供商控制的按需连接

服务提供商控制的按需动态的连接是指：服务提供商管理 CE 节点，并使用选路/信令动态地建立新的 VPN 客户层连接的情景。从服务提供商的角度，这一能力的优点是：它允许它们动态地建立 VPN 端到端的客户层连接，而不必使用静态配置（即人工的或 OSS 指配）。VPN 客户层动态连接建立可能有用的情景的一个例子是：两个或多个 ATM 接入网经由 MPLS 核心网相互连接。在这一例子中，可以用 PNNI 在 VPN 客户层跨越 MPLS 的 VPN 服务器层路径建立/拆除 SPVC。由于这 VPN 客户层和服务器层的技术不同，在控制面必须进行对等的互通。

在服务提供商控制的按需动态连接的情况中，即使提供商代替客户管理 CE 节点，将内部的寻址和拓扑信息分发到 CE 也会伴随有危险，例如 CE 位于客户的住所，而不是提供商的。避免这种安全危险的一个方法是在 CE 装置和邻近的提供商网络的中间节点之间采用静态/人工的指配，从那个节点回到 PE 使用动态的选路/信令。例如，如果 VPN 客户层是 ATM，那么在 CE 和它连接的提供商的 ATM 交换机之间可以人工地配置 VC，并在 ATM 交换机之间端到端地使用 PNNI。关于层网络等级架构中对不同层上连接/隧道建立的控制，由于是提供商控制按需的连接，提供商对于网络中将发生什么会有更多的控制。然而，细致的网络规划和对每一层连接的 NMS 监测仍必须进行，尤其是当公司中负责管理 VPN 客户层的部门和负责管理 VPN 服务器层（和下面的服务器层）的部门不相同时。

11 对等层VPN建立所需要的功能

这里假设：下层的服务器层拓扑已经建立，而且 VPN 对等层的 TFP 和 FP 已经用地址进行了配置，那么在 VPN 成员之间，VPN 对等层连通性的建立将涉及 3 个主要的步骤：

步骤 1：发现和认证 VPN 成员，并存储 VPN 成员关系的信息。

步骤 2：在 VPN 对等层上计算 VPN 成员之间的路由。

步骤 3：配置 VPN 对等层网络的网元以提供 VPN 的隔离。

支持 VPN 对等层建立和保持所需要的每一个功能以及各单独的功能实体已经进一步在表 11-1 之中描述。

表 11-1/Y.1314－VPN服务器层

功　能	功能实体	网　元
VPN 成员关系的发现	VPN 成员的发现	CE/PE
	VPN 成员关系信息（包括：加入，离开，可用性）的分发/收集	CE/PE
	VPN 成员关系信息的保持	CE/PE
CE/用户认证、授权和记账（AAA）	认证：基于认证参数的 CE/用户识别，认证参数的例子有有效的用户名和口令	CE, PE
	授权：允许或拒绝接入 VPN 客户层网络的资源/服务	CE, PE
	记账：所用资源/服务的测量	CE, PE
VPN 对等层的选路	VPN 对等层可通达性/拓扑/资源信息的分发/收集	CE, PE, P
	VPN 对等层可通达性/拓扑/资源信息的保持	CE, PE, P
	VPN 对等层 AP 之间最佳路由的计算	CE, PE, P
VPN 对等层网元的配置	逐个 VPN 数据包过滤器的配置	PE
	逐个 VPN 路由过滤器的配置	PE
	逐个 VPN/CE 加密密钥的配置与交换	ES, CE, PE
	VLAN ID 的分配和配置	CE, PE, P

11.1 VPN成员关系的发现

在客户配备的对等层 VPN 的情景中，VPN 对提供商而言是透明的（例如互联网上的 IPsec VPN），在这 VPN 建立之前，首先有必要确定哪些 CE 属于这一 VPN。在提供商配备的 VPN 的情景中（例如基于 VLAN 的 VPN），提供商需要发现哪些 PE 是连接到作为 VPN 成员的 CE 的。发现可以由操作人员依据已知的网络拓扑人工地执行，或者经由集中的服务器/系统或分布的协议动态地来执行。

11.2 CE/用户的认证、授权和记账（AAA）

CE/用户的 AAA 功能在提供商配备的 VPN 情景中用于控制 VPN 对等层资源的接入。AAA 也用于政策的强制，支持对使用的审核，并提供对客户使用 VPN 服务进行记账的必要信息。AAA 功能可以由 PE、单独的装置或使用两者的混合来执行。例如，如果 IEEE 802.1X 在基于以太网 VLAN 的 VPN 中用于对 CE 的认证，这 PE 将是认证者，而一个集中的认证服务器可用于执行认证。

11.3 VPN对等层的选路

在 VPN 成员间有可以选择的通路/路由时，在 VPN 对等层中必须执行选路，以发现拓扑和/或计算 VPN 成员间的最佳路由。由于 CE、PE 和 P 节点都属于 VPN 对等层，所有这三类节点都将参与到任何路由/通路的计算中。选路功能可以由操作人员人工地执行，或者经由集中的服务器/系统或分布的选路协议动态地来实现。为了本建议书的需要，选路将包括基于数据平面源地址知识的透明的网桥连接。

11.4 VPN对等层网元的配置

有一些可选的不同功能可提供 VPN 隔离。一个选项是在共享的 PE 节点上配置逐个 VPN 的包过滤器来确保单客户站点间的完全可通达性，但客户间是分离的。另一个选项是使用专门的 PE 节点并配置路由过滤器，使得 P 节点可包含所有客户的路由，但 PE 节点仅包含单个客户的路由。包/路由过滤仅适用于提供商配备的 VPN 的情景，因而必须由 PE 节点来执行。

在客户之间存在连通性时，替换路由/包过滤的另一种方法是采用包加密。采用包加密将确保：如果客户从它们并不属于的 VPN 接收到数据包，它们将不能得到包中包含的数据。对于提供商配备的 VPN，包加密可以由 PE 节点来执行；而对于客户配备的 VPN，可以由 CE 节点或末端系统来执行。

常用的支持加密/解密的密码术包括秘密密钥和公钥密码术。秘密密钥密码术最适合于封闭用户群，在此秘密密钥可以由单个管理机构所持有和秘密地进行分发，例如在企业 VPN 的环境中。公钥密码术的优点是：它允许用户秘密地进行通信，而不必预先接入共享的秘密密钥。这种方法使用两个密钥：一个私钥，它要保持秘密，另一个公钥，它需要分发到所有的 VPN 成员。公钥和私钥是数学上相关联的，不持有特定私钥的任何人将不能对加密数据包中的信息进行解密。公钥密码术的一种通常的使用是交换秘密密钥密码术所用的秘密密钥。

当以太网用于作为 VPN 的对等层技术时，VPN 的隔离可以通过分配和配置 VLAN 来实现。VLAN 虽然也可用动态的协议来配置，但通常是人工地或经由 OSS 来分配与配置的。为了在 CE 间提供端到端的连通性，VLAN 必须正确地在 CE、PE 和 P 节点上进行配置。

12 VPN的OAM功能

在大范围的网络中，OAM 工具和功能对于保持运营的效率是不可少的。经由 OAM 功能传送的网络连接/信流的重要特性有质量、完整性和有效性等。如果一个层网络不支持 OAM，或者缺少某个 OAM 功能性，那么这个特定的层网络，就那一 OAM 功能性而言，在功能上就是不完善的。较高/较低层的 OAM 功能/工具不能用于作为替代品来提供同样的功能特性，尤其当遇到故障定位时。这并不是说不可能用那些缺少 OAM 功能的网络技术来提供 VPN 服务。然而，缺少 OAM 功能很可能会大大提高运营的开支和操作的复杂性。

表 12-1 提供了一些关键的 OAM 功能，并识别了哪些网元应该支持其相关联的功能。

表 12-1/Y.1314－客户机/服务器OAM功能

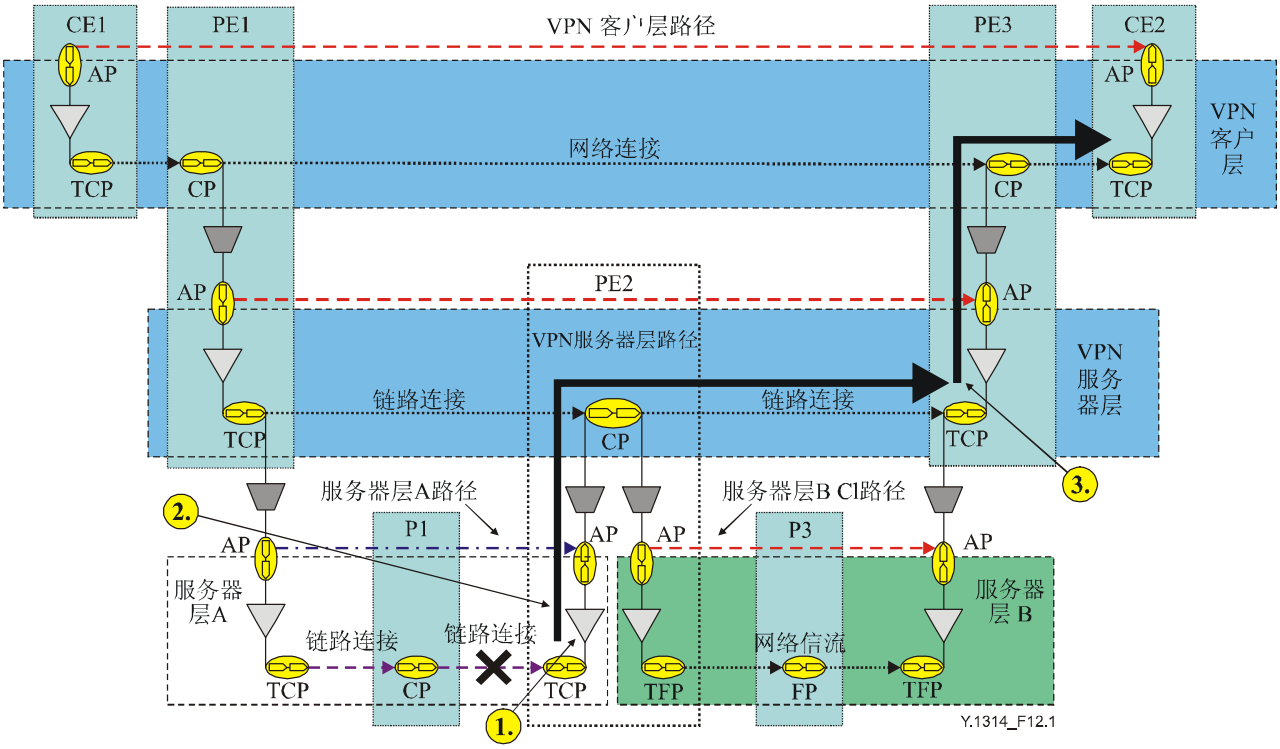
功　能	功能实体	网　元
VPN 客户层 OAM	VPN 客户层故障检测/管理	CE 和 PE
	VPN 客户层性能监测	CE 和 PE
	VPN 客户层 OAM 激活和去激活	CE 和 PE
VPN 服务器层 OAM	VPN 服务器层故障检测/管理	PE 和 P
	VPN 服务器层性能监测	PE 和 P
	VPN 服务器层 OAM 激活和去激活	PE 和 P
VPN 对等层 OAM	VPN 对等层故障检测/管理	CE，PE，P（所有）
	VPN 对等层性能监测	CE，PE，P（所有）
	VPN 对等层 OAM 激活和去激活	CE，PE，P（所有）

12.1 故障管理

故障管理包括故障检测、定位、纠正和按需的诊断测试。故障必须在它们发生的层网络中在连接/信流的信宿端点处检测和处理。不能做到这一点将导致模糊的故障指示，而这将大大增加操作的复杂性和处理故障所花的时间。一旦检测到故障，除了生成和发出给 NMS 的告警以外，为了防止客户层网络上的告警风暴，应采用受影响的特定客户层技术使用的适当的 OAM 句法（如果有的话）向客户层网络传送 FDI（前向故障指示）或 AIS（告警指示信号）。

最重要的故障检测机制是使用连通性检验（CV），它是一个所在三种网络模式都通用的要求。简单地说，它要求：一个业务流的信源能确定地（以某种方式）向信宿标识它自身。如何实现这一点决定于网络的模式，这将在随后的章节中进行解说。故障定位是所有这三种模式的另一个关键要求，为的是确定故障根源，除了初始的故障信息外，可以用按需的诊断测试工具来定位故障。

图 12-1 从功能的角度描述了在 VPN 服务器层中故障情景的一个例子。



1. 服务器层依据未收到CV数据包检测LOS
2. 服务器层A将FDI转发给VPN服务器层
3. VPN服务器层接收到FDI, 并将它传播到VPN客户层

图 12-1/Y.1314－客户机/服务器FDI的传播

在这一例子中，服务器层 A 中由信宿终端功能对链路故障的检测导致 FDI/AIS 的生成并传送到 VPN 服务器层。这 FDI 被传播给 VPN 服务器层的信宿终端功能，又由它发送 FDI 给客户层。这一行为将反复直到不支持 FDI 的层网络。因此，尽管这里没有显示，VPN 客户层在收到 FDI 后，可能会发送 FDI 到上一层，具体取决于上一层是什么技术（例如：ATM、以太网、IP 等）。

应该发出告警的仅有的地点是检测到始发故障的层网络路径的终端点。尤其是，在受影响的任何客户层中不应该发出告警（这是向它们发送 FDI 的主要目的）。此外，如果需要两个方向的单端监测时，那么可以在另一方向上发送 BDI（反向故障指示）。有关故障指示/告警更一步的细节（包括故障细节、不可用性状态进入和离开的准则以及随后的动作）可以从处理特定层网络技术 OAM 的建议书中找到，如用于 MPLS OAM 的 ITU-T Y.1711 建议书。

故障纠正负责故障的修复和对使用冗余资源替代故障的设备或装置的规程的控制。例如，在光纤切断或节点故障时，可以用保护转换或连接的重新选路来恢复/保持服务。

按需的诊断测试工具一般地用于故障定位，但也可以用于连接/隧道投入服务前对正确的连通性/配置进行验证。环回是诊断测试的一个例子，其间网络连接上的一个环路从信源经由一个连接或终端连接点返回到信源，从而将那一段连接隔离开来。

12.2 性能管理

性能监测（PM）是性能数据的收集、分析和报告。这种数据用于估价和维护网络以及对提供给客户的服务质量进行归档。如果要支持多个层次的服务等级（例如基于差别服务的架构），那么性能监测应该在逐个服务等级的基础上来执行。其中，性能监测包括信号恶化的检测、延迟/抖动监测和丢失数据包的计数。性能监测有一些不同的目标，包括 SLA 的保持、业务流工程的支持、逐个客户的记账和服务的恢复/保护转换（例如由于信号恶化）。

在故障、有效性和 PM 之间建立关系是很重要的。这里有一个特别的顺序，可以归纳如下：

1） 网络模式确定相关的故障（它们对于每一种模式是不同的）以及所需 OAM 的性质。

2） 所有的故障应该用标准化的进入/离开准则以及随后的动作来定义。

3） 当故障或不可接受的性能恶化连续地持续数秒后进入不可用状态。在 SDH 中，在连续的 10 个严重误码秒[7]（SES）以后进入不可用状态，并在连续的 10 个非 SES 之后离开。为了保持协调，不可用周期对于所有层网络应该相同，也即 10 秒。

4） 用于 SLA 的 PM 仅当在可用状态下才是有效的，因此用于 SLA 的 PM 在进入不可用状态时应该暂停。

在可用状态下，用于 SLA 的 PM 是单向测量的。然而大多数应用需要双向工作（上行和下行），因而从应用的角度，有任一方向故障，两个方向就认为是故障了。这意味着不可用性与每一个方向是“或”的关系，因而只要有任一方向进入不可用状态，用于 SLA 的 PM 就应该在两个方向上暂停。

12.3 OAM的激活/去激活

对于 CO-CS 和 CO-PS 模式，故障检测/处理基本的 OAM 机制应该与路径建立和拆除同步地激活/去激活，路径建立和拆除可经由 NMS/OSS 的指配或信令来实现。例如，CV 的发生可以在信宿点激活 CV 检测之前先在信源点激活，以避免无意义的告警。建立路径所用的指配或信令方法也应该能告知路径信宿点对一个具体的路径在数据平面上可以期望的信源识别码（例如 ITU-T Y.1711 建议书中的 TTSI）是什么，以确定它接收的 OAM 数据包属于哪条路径。

---

7 一个SES是一个一秒钟的时段，其比特差错率等于或高于1E-3，或者在其间检测到LOS或AIS。

12.4 与各种网络模式相关的故障

可能发生在 VPN 客户层或服务器层网络中潜在的传送故障决定于层网络技术所属的网络模式。下面对由模式决定的潜在故障进行归纳：

— **CL-PS**：仅中断；

— **CO-PS**：中断，调换和混合；

— **CO-CS**：中断，调换（但只在类似的实体之间）。

在以下章节中，将对每一种网络模式进行更细的描述，以明确对一个特定模式哪些是关键的 OAM 要求和考虑。需要说明：这并不是要成为每种模式 OAM 要求的一个深入的清单。这里只突出了那些基本的功能差别，以便显示 VPN 客户层和服务器层所属的网络模式如何影响所需要的 OAM 功能/工具。

12.4.1 CL-PS层网络

假设选路信息是一致的和有效的（这实际上适用于所有的模式），那么连通性错误的故障（也即调换或混合）在 CL-PS 层网络中不会发生。每个数据包既包含有源地址（这是 CV 功能），又包含有目的地地址；后者具有在每个网络节点为数据包选路所需要的所有信息。因此，在 CL-PS 层网络中可能有的仅有的故障是出现中断的情况（例如由于选路、链路或节点的故障）。在 CL-PS 层网络中，由于每个数据包具有网络惟一的源/目的地地址，CV 功能是数据包包头整体的组成部分。在 CL-PS 网络中，控制和用户数据通常共享同一个数据路径，因而如果在控制平面上有故障（例如选路邻接关系的丢失），那么蕴含地可以假设：连通性已经丢失，用户数据也不能发送。这就是 CL-PS 层上故障一般地是如何检测和纠正的，例如，控制平面上收不到选路的 hellos，指示数据平面有故障，因而必须采用纠正的操作（如选择另一个路由）。然而有一种情况是例外，那是当在 IP 层网络上采用负荷平衡时。在这种情况下，将存在多个路由通往同一目的地，因而在一条路由变得不可用时，由于控制业务流可以简单地使用另一条可用路由，这情况不能由控制平面检测出来。为了在采用负荷平衡时检测故障，必须用 OAM 机制来测试跨越所有路由的连通性。

12.4.2 CO-PS层网络

在 CO-PS 情况下，仅层网络的接入点是识别网络惟一的地址的，这种地址由选路功能用来为连接计算经由网络的最佳路由/通路。一旦路由/通路已经算出，将采用信令（或人工的指配）来分配和配置局部有意义的入口/出口复用/去复用字段（或链路连接识别码），它们在数据平面上用于将数据转发到正确的目的地。由于复用/去复用字段只在局部有意义，同样的数值可重新用于同一连接的上行/下行节点，或者不同的连接。复用/去复用字段的重新使用再加上数据平面上没有网络惟一的地址将意味着：在 CO-PS 层网络中，除了中断，我们还能够遭遇调换和混合的差错。由于 CO-PS 数据包是异步传送的，需要以某种确定的方式将 CV 功能加入，通常是以特定的速率发送 CV 数据包。对 CV 数据包的发送速率要仔细加以考虑，以保证在出现暂态的突发误码时不会采取不必要的动作。

12.4.3 CO-CS层网络

CO-CS 层网络，由于复用/去复用字段是基于物理时间/空间/频率的链路连接识别码并具有恒定的比特速率，并不会遭遇混合问题。在 CO-CS 层网络中可能发生的差错包括中断和连接被调换，然而，调换连接的差错将只发生于严格相同的路径之间，例如，调换不会发生在 SDH 的 VC12 和 VC4 之间。在 CO-CS 层网络的情况下，如同 CO-PS 的层网络，CV 功能必须以某种确定的方式加进去。由于 CO-CS 帧以恒定的比特速率发送（不管是否有数据发送），CV 信息可以载于每个帧中，以帧的速率作为 CV 发送速率，例如在 SDH VC4 的帧中，J0 跟踪消息具有以 125 μs 为基数的插入速率。在 CO-CS 情况下，控制业务流总是以 OOB 方式运载，因此必须在逐个连接的基础上为用户数据平面和控制数据平面提供 OAM 功能。

12.4.4 控制和用户数据平面的分离

在 CO-PS 网络中，控制数据和用户数据可以采用不同的数据平面来传送（通常被称为带外（OOB）控制）；正如前一节所说的，在 CO-CS 模式下这一点总是被迫这样做的。有很多理由说明：这种控制和用户数据平面的分离是有利的，尤其是从安全和网络稳定的角度，因为它可以保护控制平面免受来自用户平面的攻击，免受用户平面业务流造成的过载/拥塞问题。当用户和控制数据平面分开时，显然已不能假定：控制平面的故障表明用户数据平面有故障（或反之）。因此，在使用 OOB 的 CO-PS 层网络中，OAM 机制必须在逐个数据平面的基础上使用。情况也是这样，如果控制业务流有可能和一些用户业务流使用同一数据平面，但不是所有的（例如在 MPLS 中，可以用业务流工程（TE）来为某些业务流类型提供明确选路，因而，用户数据业务流不需要与用来建立 TE 隧道的控制数据包遵循同一路径）。

使用基于数据平面的 OAM 机制的失效会导致以下情景：运载用户数据包的连接遭遇故障，而控制业务流由于使用单独的连接发送，控制信息仍继续流动，因而这故障不能由控制平面检测出来。没有数据平面 OAM 检测机制，连接的信源将继续发送用户数据，形成一个业务流的黑洞，或者更加糟糕，将业务流送往错误的地点从而损害客户数据的安全。

为了明确地确定故障发生在哪个方向，支持 P2P 和 P2MP 连接正确的故障处理，OAM 应该单向操作。此外，如果可能，也应该支持在两个方向上对故障的单端监测。这在客户或提供商对连接/隧道的一端有控制，而对另一端没有时尤其重要，例如在一个跨提供商的 VPN 的情景中，在此 P2P VPN 客户层连接的各端将位于不同的服务提供商网络。

13 功能的融合和服务情景

将 VPN 的服务要求映射到本建议书描述的功能将使得网络运营商可以选择提供他们希望提供的 VPN 服务所需要的最适合的技术和机制。为每一种功能选择品种最好的机制/协议将使单独的功能构件能独立地发展。这一方法还支持一些共有的机制/协议在不同的 VPN 网络技术（在适合时）间得到重用，以减少开支和复杂性。

13.1 客户机/服务器VPN服务的情景

支持客户机/服务器 VPN 所需要的功能（以及其机制/协议）取决于客户机/服务器网络的模式以及实际要提供的 VPN 服务。例如，一些客户会要求能在多个站点间，在需要时，建立按需的 SVC，而其他客户可能基于已知的静态拓扑只要求永久的连接。又比如，一些客户会要求使用逐个用户/CE 的认证来提高安全性，而另一些客户可能相信：限制对网络基础设施的物理接入就足够了。表 III.1 和 III.2 提供了不同服务情景的一些例子，并标识了例举的机制/协议，可用于提供所需的功能。

13.2 对等层VPN的情景

支持对等层 VPN 所需要的功能取决于对等层网络的技术和要提供的 VPN 服务的类型。例如，在基于加密的 VPN 情况下，为了使用正确的密钥，认证是必备的；而在基于以太网 VLAN 的 VPN 情况下，认证（如采用 IEEE 802.1X）可提供额外的安全，但并不是必不可少的。表 III.3 提供了不同服务情景的一些例子，并标识了例举的机制/协议，可用于提供所需的功能。

14 VPN的安全考虑

本建议书并不引入任何新的安全问题。然而，在设计/开发 VPN 网络时为了选择能满足客户安全要求的网络技术和功能构件，安全是一个要考虑的基本因素。由于一个共享的基础设施要用于传送多个客户的业务流，会有一些固有的安全风险与所有的 VPN 技术相关联。

网络安全其本身是一个巨大的领域，因而在本建议书中没有深入地加以研究。从高层次上看安全，物理的 VPN 网络基础设施必须防止非授权的访问或恶意攻击（例如限制对有网络设备的建筑物进行访问）。此外，也要防止从 VPN 网络基础设施外部进行非授权的远程接入（例如采用防火墙防止来自互联网的攻击源）。

在客户机/服务器 VPN 情况下，正如第 5.1 节所描述的，一个 VPN 服务器层网络必须支持复用和去复用，以提供多个 VPN 客户层之间数据平面的分离。这种业务流的分离必须与网络边缘基于逐个客户 VPN 策略的有效的 VPN 接入控制相结合。

在对等层 VPN 的情况下，正如第 6 节所描述的，为了支持跨越共享区域的 VPN，所用的网络技术必须具有某种提供 VPN 隔离的手段。CE 将只能与属于同一 VPN 的其他 CE 进行通信，或只能解密属于同一 VPN 的 CE 的数据包。

对于客户机/服务器的和对等层 VPN，用加密法对用户/控制业务流单元进行加密都可以提高安全性，同时可以用认证对用户和网络节点进行鉴别。关于客户机/服务器和对等层 VPN 的认证已在第 10.2.1 和 11.2 节中分别进行了较细的描述。在第 6.2 和 11.4 节中也对加密进行了更进一步的描述。

附　录　一

VPN客户层TCP/TFP的位置

图 I.1 给出了客户机/服务器 VPN 网络的一个例子，它示出了该网络的物理拓扑，在此，黑线表示 VPN 服务器层，灰线表示节点间的物理链路。

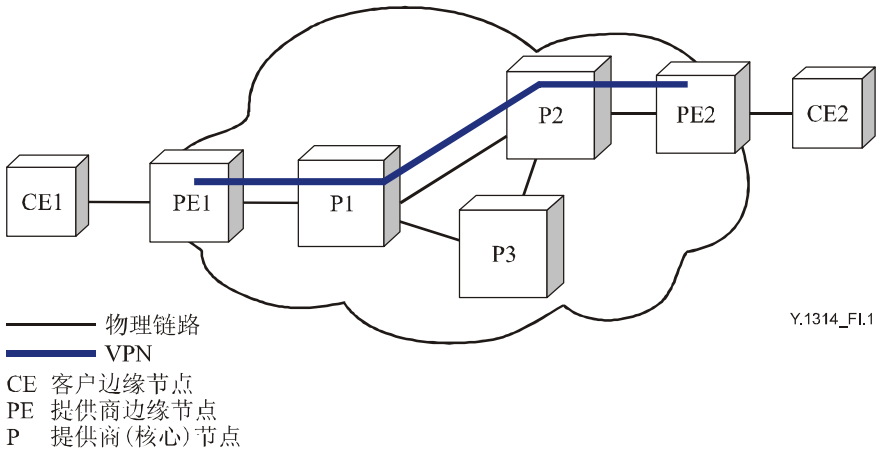


图 I.1/Y.1314－客户机/服务器VPN的物理拓扑 — 例子 1

虽然图 I.1 示出了物理拓扑和 VPN 服务器层，它并没有显示分离的 VPN 客户层和服务器层的拓扑，或 TCP/TFP 位于何处。图 I.2 示出基于图 I.1 物理拓扑的功能模型，图中 TFP 位于 CE 节点。在这一例子中，VPN 服务器层是 CO（例如 ATM），而 VPN 客户层是 CL（例如以太网），尽管 CO 或 CL 对的任何组合都是可能的。

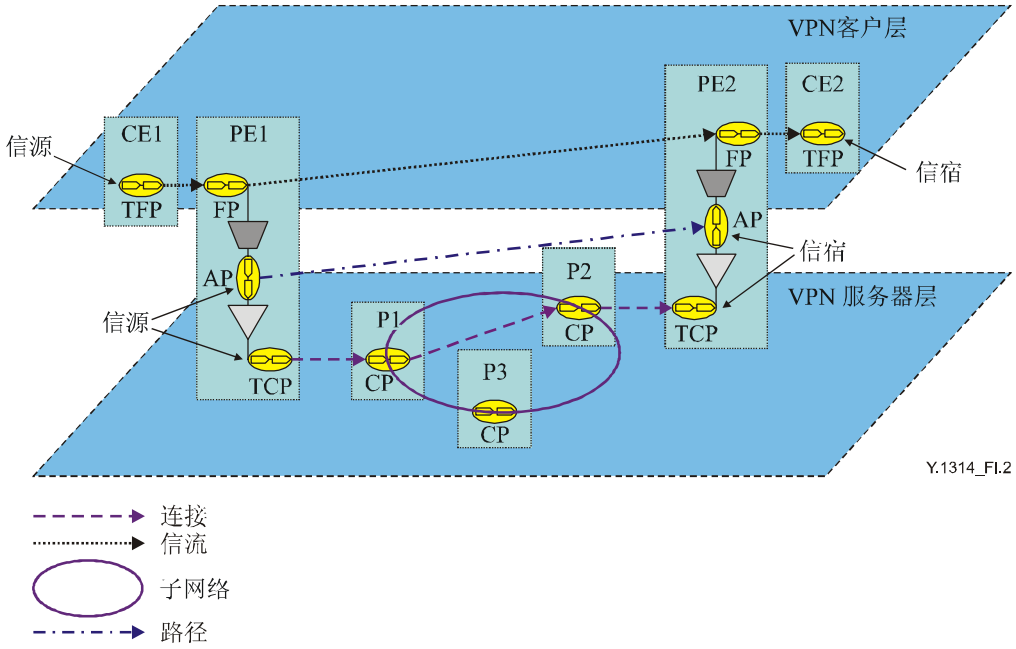


图 I.2/Y.1314－位于CE节点的VPN客户层TFP

CE 节点和 P 节点分别属于 VPN 的客户层和服务器层，而 PE 节点同时属于两个层。VPN 客户层中的 TFP 标识 P2P VPN 客户层信流从何处（本例中即哪个 CE 节点）开始（它的信源）和终结（它的信宿），而 FP 标识 P2P 信流通过哪些 PE 节点。类似地，VPN 服务器层中的 TFP 标识 VPN 服务器层连接的信源和信宿，而 FP 标识信流通过哪些 P 节点。VPN 服务器层中的 AP 标识 VPN 服务器层路径的信源/信宿。

在前一例子中，VPN 客户层 TFP 是位于 CE 节点（CE1 和 CE2），然而这并不是所有 VPN 客户机/服务器关系的情况。例如，VPN 客户层可以是以太网或 IP 层网络，在此 TFP 是位于主机/末端系统。

图 I.3 显示了一个客户机/服务器 VPN 网络的物理拓扑。如果 VPN 客户层是以太网，那么 C 节点将是以太网交换机，而末端系统/主机将是具有以太网接口的计算机/服务器。

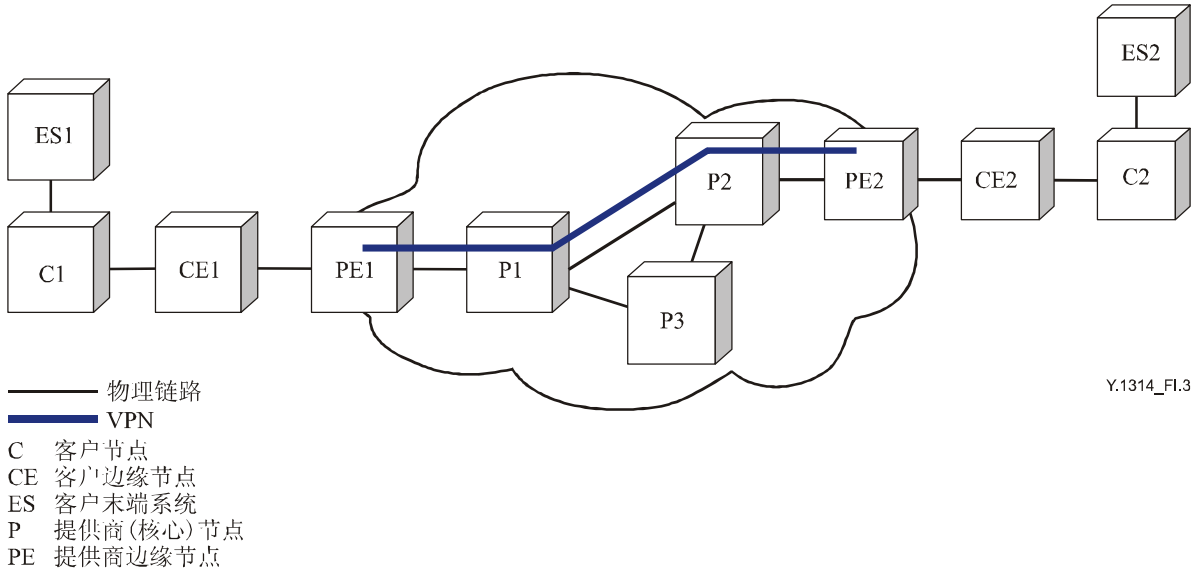


图 I.3/Y.1314－客户机/服务器VPN的物理拓扑 — 例子 2

基于图 I.3 描述的物理网络的功能模型已在图 I.4 中提供，在此 VPN 客户层的 TFP/TCP 位于末端系统/主机而不是 CE 中。

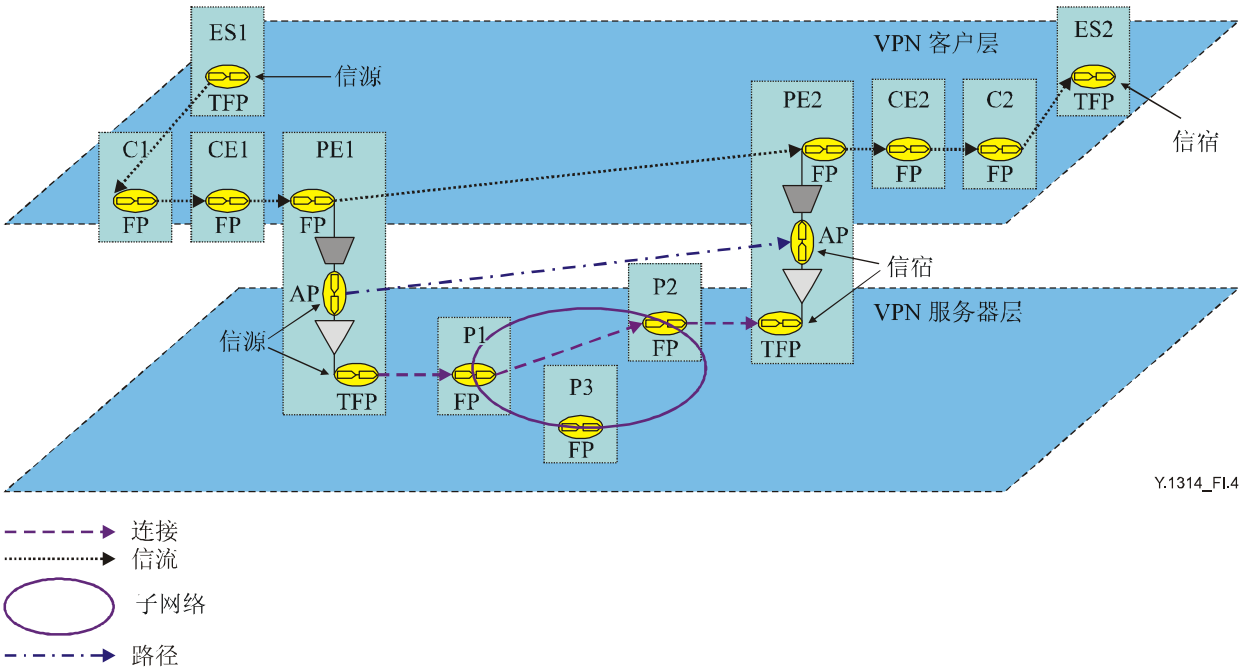


图 I.4/Y.1314－位于末端系统/主机中的VPN客户层TFP

C 和 CE 节点与 ES 一起属于 VPN 客户层。PE 节点属于 VPN 服务器层和客户层，而 P 节点只属于 VPN 服务器层。VPN 客户层的 TFP 标识 VPN 客户层信流的信源和信宿（也即分别为 ES1 和 ES2），FP 标识信流通过哪些 C、CE 和 PE 节点。

尽管在前一例子中没有示意，但也有可能在 VPN 的一侧一个信源或信宿的 TFP/TCP 位于 CE，而在另一侧 TFP 并不位于 CE，也即 CP/FP 位于 CE，TFP/TCP 位于客户节点或 ES 中。

附　录　二

有多个VPN服务器层的客户机/服务器VPN

图 II.1 示出了一个客户机/服务器 VPN 网络的物理拓扑，它使用了两个 VPN 服务器层，X 和 Y。节点 PE1、P1 和 P2 属于 VPN 服务器层 X，而节点 P3 和 PE3 属于 VPN 服务器层 Y。节点 PE2 同时属于两个服务器层，并在两者间充当网关。

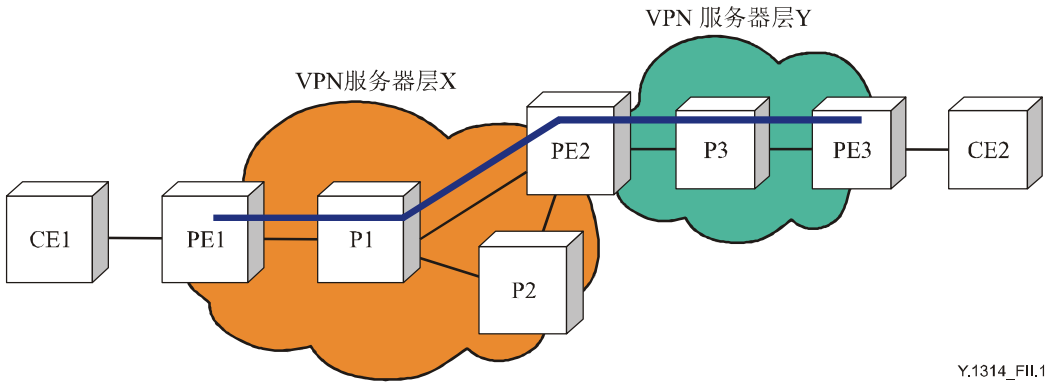


图 II.1/Y.1314－VPN服务器层互通的物理拓扑

VPN 服务器层 X 和 Y 之间互通的方法之一，如图 II.2 所示，是使用客户机/服务器互通。在这一模型中，节点 PE2 属于 VPN 服务器层 X 和 Y，同时所有 3 个 PE 节点都属于 VPN 客户层。

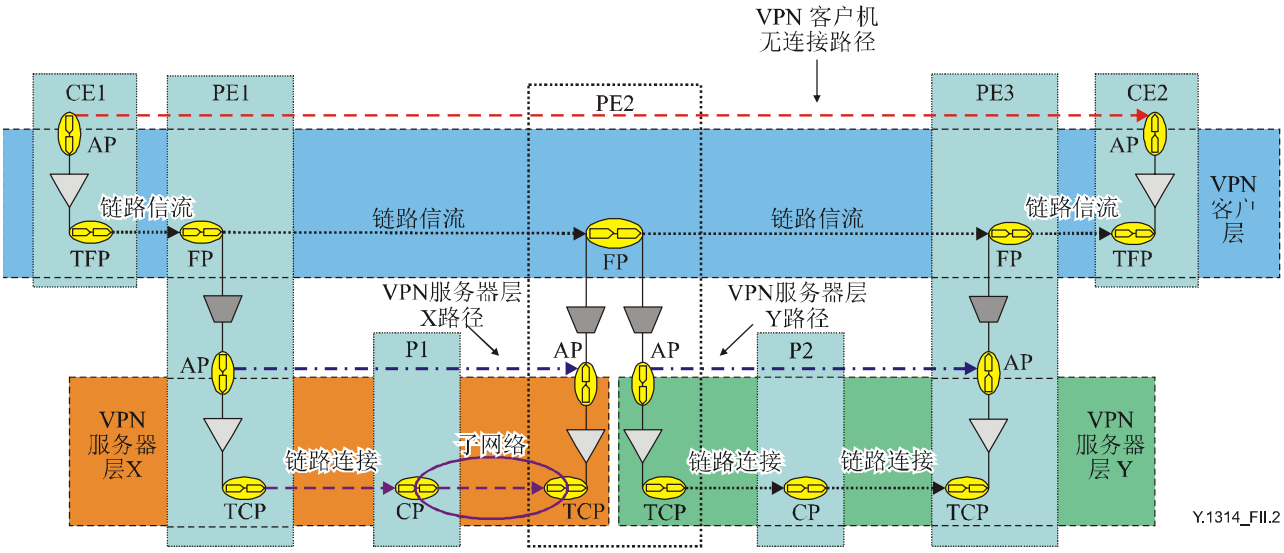


图 II.2/Y.1314－VPN服务器层客户机/服务器互通

VPN 服务器层 X 的信源适配功能将 VPN 客户层的 CI 适配成 VPN 服务器层 X 的 AI，而信宿适配功能将 VPN 服务器层 X 的 AI 适配到 VPN 客户层的 CI。类似地，VPN 服务器层 Y 的信源适配功能将 VPN 客户层的 CI 适配到 VPN 服务器层 Y 的 AI，信宿适配功能将 VPN 服务器层 Y 的 AI 适配到 VPN 客户层的 CI。

进行客户机/服务器适配的网元包含有属于 VPN 客户层的 FP 或 CP，它们必须用 VPN 客户层的地址加以标识。因此，假如 VPN 客户层是 IP、PE1、PE2 和 PE3 将都需要属于 VPN 客户层的 IP 地址。

将带有客户机/服务器适配的多个 VPN 服务器层用于 CO VPN 客户层意味着：一个跨越 CP 的路由/通路必须动态/人工地进行计算，至少有两个链路连接将在提供商网络中在 VPN 的客户层端到端地建立起来。将带有客户机/服务器适配的多个 VPN 服务器层用于 CL VPN 客户层意味着：一个跨越 FP 的路由/通路必须动态/人工地进行计算，CL 业务流单元（也即数据包）必须依据 VPN 客户层的地址信息进行转发。这和在 VPN 客户层的两个 CP/FP 之间跨越提供商网络已经端到端地建立有单个 VPN 服务器层的情况形成对照。在这种情况下，在提供商网络中在 VPN 服务器层路径的信源和信宿之间只需要单个链路连接/信流，因而不需要在 VPN 客户层计算跨越提供商网络的路由/通路。

图 II.2 中 VPN 服务器层 X 和 Y 之间互通的另一种可选的方法是使用图 II.3 所示的对等层的互通。在这一模型中，节点 PE2 属于 VPN 服务器层 X 和 Y，但不属于 VPN 客户层。PE1 和 PE3 分别地属于 VPN 服务器层 X 和 Y，同时也属于 VPN 客户层。

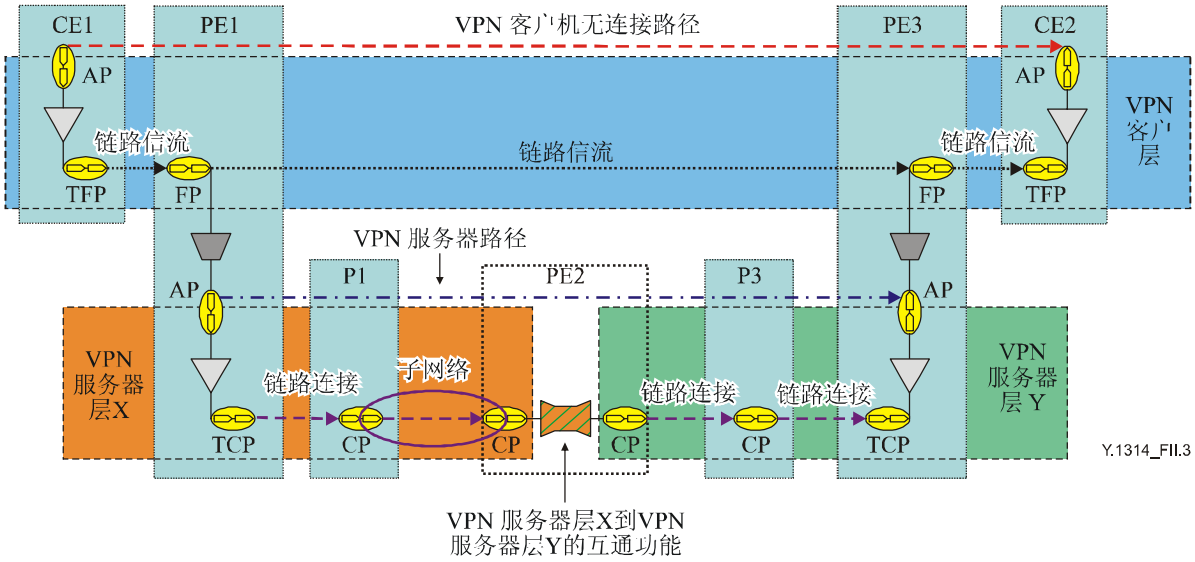


图 II.3/Y.1314－VPN服务器层的对等层互通

VPN 服务器层 X 的信源适配功能将 VPN 客户层的 CI 适配到 VPN 服务器层 X 的 AI。VPN 服务器层 X 到 VPN 服务器层 Y 的互通功能将 VPN 服务器层 X 的 AI 适配到 VPN 服务器层 Y 的 AI。VPN 服务器层 Y 的信宿适配功能将 VPN 服务器层 Y 的 AI 适配到 VPN 客户层的 CI。

在考虑对等层互通时要考虑的主要因素是：只有某些网络技术能够在对等层的基础上互通，例如 ATM 和帧中继网络可以在对等层的基础上互通（使用 FRF.8），但 IP 和 TDM 不能。对等层互通不仅需要数据平面的互通，还需要就诸如选路、信令和 OAM 等功能在控制平面进行互通。

附 录 三

客户机/服务器和对等层VPN服务情景的举例

以下表格例举了一些不同的 VPN 服务的情景，并说明了可以用来提供所需要功能的机制/协议的例子。

注 — 与本附录中这些表格相关的补充的参考文献在参考资料中提供。

表 III.1/Y.1314－客户机/服务器VPN服务情景 1

	载于MPLS的第2层帧中继服务	**载于IP/L2TPv3的第2层以太网VPWS服务**	**第3层RFC 2547 IP VPN服务**
VPN 客户层	帧中继	以太网	IP
VPN 服务器层	MPLS PW	IP/L2TPv3	MPLS
VPN 成员关系的发现	RADIUS, BGP, 人工, NMS	RADIUS, BGP, LDP, RSVP-TE, 人工, NMS	BGP
VPN 服务器层选路	IGP, BGP, 人工, NMS	IGP, BGP, 人工, NMS	BGP
VPN 服务器层隧道/连接的建立	LDP, BGP, 人工, NMS	L2TPv3 信令	BGP
CE/用户的认证、授权和记账（AAA）	RADIUS, IEEE 802.1X, RMON, SNMP, NMS	RADIUS, IEEE 802.1X, RMON, SNMP, NMS	CE-PE 选路协议（例如使用 MD5 的 EBGP），RMON, SNMP, NMS
VPN 客户层网元的配置	NMS, 人工	NMS, 人工, E-LMI	DHCP, NMS, 人工
VPN 客户层选路	NMS, 人工	MAC 地址的知识	EBGP, OSPF, 人工/静态
VPN 客户层隧道/连接的信令	NMS, 人工	不需要，因为客户是 CL-PS	不需要，因为客户是 CL-PS
VPN 客户层 OAM	帧中继 LMI	IEEE 802.1ag, E-LMI, IEEE 802.3ah, ITU-T Y.1731 建议书	IP ping/路由跟踪
VPN 服务器层 OAM	ITU-T Y.1711 建议书, ITU-T Y.1713 建议书, MPLS, VCCV, BFD/LSP ping	IP ping/路由跟踪	ITU-T Y.1711 建议书, ITU-T Y.1713 建议书, LSP ping/路由跟踪

表 III.2/Y.1314－客户机/服务器VPN服务情景 2

	载于OTN的第1层SDH VPN服务	载于MPLS的第1层TDM VPN服务	载于SDH的第2层ATM VPN服务
VPN 客户层	SDH（例如 STM-16）	TDM（例如 E1）	ATM
VPN 服务器层	光通路 /光通道（OCh）	MPLS PW	SDH（例如 VC4）
VPN 成员关系的发现	ITU -T G.7714.1/ Y.1705.1 建议书, 人工, NMS	RADIUS, BGP, LDP, 人工, NMS	人工, NMS
VPN 服务器层选路	GMPLS/ASON 选路协议, 人工, NMS	IGP, BGP, 人工, NMS	GMPLS/ASON 选路协议, 人工, NMS
VPN 服务器层隧道/连接的建立	GMPLS/ASON 信令协议, 人工, NMS	LDP, BGP, 人工, NMS	GMPLS/ASON 信令协议, 人工, NMS
CE/用户的认证、授权和记账（AAA）	GMPLS/ASON 协议, SNMP, NMS	RMON, SNMP, NMS	ATM, PNNI/UNI 安全, RMON, SNMP, NMS
VPN 客户层网元的配置	NMS, 人工	NMS, 人工	ATM UNI, 人工, NMS
VPN 客户层选路	GMPLS/ASON 选路协议, 人工, NMS	人工, NMS	人工/静态, NMS, PNNI
VPN 客户层隧道/连接的信令	GMPLS/ASON 信令协议, 人工, NMS	人工, NMS	人工, NMS, PNNI
VPN 客户层 OAM	SDH 开销（例如 J0/J1/J2 跟踪字节, G1 通路状态字节）	ITU-T G.775 建议书, AIS/LOS	F4 和 F5 故障管理, 环回和连续性检查（CC）
VPN 服务器层 OAM	OCh 开销（例如在通路/段监测（PM/SM）中使用的路径跟踪识别码（TTI））	ITU-T Y.1711 建议书, ITU-T Y.1713 建议书, MPLS, VCCV, BFD/LSP ping	SDH 开销（例如 J0/J1/J2 跟踪字节，G1 通路状态字节）

表 III.3/Y.1314－对等层VPN服务情景

	载于互联网的IPsec VPN	**以太网 VLAN VPN**
VPN 对等层	IP	以太网
VPN 成员关系的发现	人工, NMS	人工, NMS, RADIUS
CE/用户的认证、授权和记账（AAA）	IKE 首次认证（基于预共享的密钥或数字签字）, RMON, SNMP, NMS	IEEE 802.1x, RADIUS, RMON, SNMP, NMS
VPN 对等层选路	IGP 选路协议（例如 ISIS, OSPF, RIP）, BGP, 人工, NMS	STP 拓扑修剪和数据平面地址学习（透明的网桥连接）
VPN 对等层网元配置	配置预共享的密钥，或向证书管理机构申请证书。	采用人工配置，NMS 或动态的协议配置 VLAN
VPN 对等层 OAM	IP ping/路由跟踪	IEEE 802.1ag, E-LMI, IEEE 802.3ah, ITU-T Y.1731 建议书

参 考 资 料

所指明的参考文献会进行修改。本建议书的使用者应探讨使用这些参考文献的最新版本/草案。

ATM UNI: ATM Forum UNI 4.1 (2002), "*ATM User Network Interface (UNI) Signalling Specification version 4.1*", af-sig-0061.001.

ATM Forum PNNI 1.1 (2002), *Private Network-Network Interface Specification v.1.1,* af-pnni-0055.001.

IEEE 802.1ad (2005, Draft 6.0), *Virtual Bridged Local Area Networks – Amendment 4: Provider Bridges.*

IEEE 802.1ag (2005, Draft 4.1), *Virtual Bridged Local Area Networks – Amendment 5: Connectivity Fault Management*, status: PAR approved, Task Group ballot in progress.

IEEE 802.1ah (Aug 2005, Draft 1.2), *Virtual Bridged Local Area Networks – Amendment 6: Provider Backbone Bridges*, status: PAR approved, Task Group ballot.

IEEE 802.1Q (2005), *Virtual Bridged Local Area Networks*, status: published.

IEEE 802.1X (2004), *Port-Based Network Access Control*, status: published.

IEEE 802.17 (2004), *Specific requirements – Part 17: Resilient packet ring (RPR) access method and physical layer specifications*, status: published.

IEEE 802.3ah (2004), *Specific requirements – Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications* Amendment: *Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks*, Ethernet in the First Mile amendment to IEEE Std 802.3.

IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: an Overview.*

IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification.*

IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol.*

IETF RFC 2409 (1998), *The Internet Key Exchange (IKE).*

IETF RFC 2475 (1998), *An Architecture for Differentiated Services.*

IETF RFC 2547 (1999), *BGP/MPLS VPNs.*

IETF RFC 3036 (2001), *LDP Specification.*

IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels.*

IETF draft-ietf-bfd-base-03.txt (2005), *Bidirectional Forwarding Detection*, work in progress.

IETF draft-ietf-bfd-mpls-02.txt (2005), *BFD For MPLS LSPs*, work in progress.

IETF draft-ietf-l2tpext-l2vpn-05.txt (2005), *L2VPN Extensions for L2TP*, work in progress.

IETF draft-ietf-l2vpn-radius-pe-discovery-01.txt (2005), *Using RADIUS for PE-Based VPN Discovery*, work in progress.

IETF draft-ietf-l3vpn-bgpvpn-auto-06.txt (2005), *Using BGP as an Auto-Discovery Mechanism for Network-based VPNs*, work in progress.

IETF draft-ietf-l3vpn-rfc2547bis-03.txt (2004), *BGP/MPLS VPNs*, work in progress.

IETF draft-ietf-mpls-lsp-ping-09.txt (2005), *Detecting MPLS Data Plane Failures*, work in progress.

IETF draft-ietf-pwe3-control-protocol-17.txt (2005), *Pseudowire Setup and Maintenance using the Label Distribution Protocol*, work in progress.

IETF draft-ietf-pwe3-frame-relay-05.txt (2005), *Encapsulation Methods for Transport of Frame Relay Over MPLS Networks*, work in progress.

IETF draft-ietf-pwe3-vccv-06.txt (2005), *Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)*, work in progress.

ITU-T Recommendation E.164 (2005), *The international public telecommunication numbering plan*.

ITU-T Recommendation E.800 (1994), *Terms and definitions related to quality of service and network performance including dependability*.

ITU-T Recommendation G.775 (1998), *Loss of Signal (LOS), Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) defect detection and clearance criteria for PDH signals*.

ITU-T Recommendation G.826 (2002), *End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections*.

ITU-T Recommendation G.827 (2003), *Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths*.

ITU-T Recommendation G.1000 (2001), *Communications Quality of Service: A framework and definitions*.

ITU-T Recommendation G.1010 (2001), *End-user multimedia QoS categories*.

ITU-T Recommendation G.7714.1/Y.1705.1 (2003), *Protocol for automatic discovery in SDH and OTN networks*.

ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions.*

ITU-T Recommendation Q.933 (2003), *ISDN Digital Subscriber Signalling System No. 1 (DSS1) – Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*.

ITU-T Recommendation Q.2931 (1995), *Digital Subscriber Signalling System No. 2 – User-Network Interface (UNI) layer 3 specification for basic call/connection control.*

ITU-T Recommendation X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model.*

ITU-T Recommendation Y.1413 (2004), *TDM-MPLS network interworking – User plane interworking.*

ITU-T Recommendation Y.1415 (2005), *Ethernet-MPLS network interworking – User plane interworking.*

ITU-T Recommendation Y.1711 (2004), *Operation & Maintenance mechanism for MPLS networks.*

ITU-T Recommendation Y.1713 (2004), *Misbranching detection for MPLS networks.*

ITU-T Draft Recommendation Y.1731, *OAM functions and mechanisms for Ethernet based networks*, COM13-D211 August 2005.

MEF ETH OAM (2003), *Ethernet Services* OAM, Draft.

Frame Relay Forum FRF.8 (1995), *Frame Relay/ATM PVC Service Interworking Implementation Agreement*.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	**全球信息基础设施、网际协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2006年，日内瓦