

ICS 33.040.40

M 32

YD

中华人民共和国通信行业标准

YD/T 1943-2009

公用三层虚拟专用网业务技术要求

Technique Requirement for Layer 3 Provider Provisioned
Virtual Private Network Service

2009-06-15 发布

2009-09-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 三层PPVPN分类	6
5 通用业务要求	7
6 客户要求	9
7 运营商网络要求	14
8 运营商管理要求	20
9 安全考虑	24

前 言

本标准对应于IETF RFC4031《三层运营商虚拟专用网业务要求》（2005年英文版）。本标准与IETF RFC4031《三层运营商虚拟专用网业务要求》（2005年英文版）的一致性程度为非等效，主要差异如下：

——本标准的第5章修改采用了IETF RFC4031《三层运营商虚拟专用网业务要求》（2005年英文版）第4章；

——本标准第6章修改采用了IETF RFC4031《三层运营商虚拟专用网业务要求》（2005年英文版）第5章；

——本标准第7章修改采用了IETF RFC4031《三层运营商虚拟专用网业务要求》（2005年英文版）第6章；

——本标准第8章修改采用了IETF RFC4031《三层运营商虚拟专用网业务要求》（2005年英文版）第7章。

本标准虚拟专用网（VPN）的系列标准之一，本系列标准的名称及结构如下：

- YD/T 1190-2002 基于网络的虚拟IP专用网（IP-VPN）框架
- YD/T 1471-2006 基于IP的二层虚拟专用网（VPN）业务技术要求
- YD/T 1943-2009 公用三层虚拟专用网业务技术要求
- YD/T 1476-2006 基于边界网关协议/多协议标记交换的虚拟专用网（BGP/MPLS VPN）技术要求
- YD/T 1477-2006 基于边界网关协议/多协议标记交换的虚拟专用网（BGP/MPLS VPN）组网要求
- YD/T 1945-2009 基于边界网关协议/多协议标记交换的虚拟专用网（BGP/MPLS VPN）测试方法
- YD/T 1942-2009 基于标记分配协议（LDP）的虚拟专用以太网技术要求
- 基于标记分配协议（LDP）的虚拟专用以太网测试方法

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、上海贝尔阿尔卡特股份有限公司、华为技术有限公司、中兴通信股份有限公司

本标准主要起草人：田 辉、马 科、高 巍、何宝宏、张立新、李德丰、冯 军

公用三层虚拟专用网业务技术要求

1 范围

本标准从客户和运营商的不同角度出发，规定了运营商提供三层虚拟专用网业务的技术要求，包括通用业务要求、客户要求、运营商网络要求、运营商管理要求和安全考虑等。

本标准适用于运营商提供的三层虚拟专用网业务（包括基于IP的三层虚拟专用网业务），不适用于二层虚拟专用网业务和应用层虚拟专用网业务。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD/T 1190-2002	基于网络的虚拟 IP 专用网框架
ITU-T Y.1311	基于网络的虚拟专用网——通用框架和业务要求
ITU-T Y.1311.1	MPLS 体系结构上的 IP VPN 网
IETF RFC1918	私有因特网地址分配
IETF RFC2205	资源预留协议（v1）：功能规范
IETF RFC2211	负载控制网络业务规范
IETF RFC2212	确保服务质量业务规范
IETF RFC2385	用 TCP MD5 签名选项保护 BGP 回话
IETF RFC2475	差分服务架构
IETF RFC2597	确保转发的每跳行为
IETF RFC2685	虚拟专用网标识
IETF RFC3246	加速转发的每跳行为
IETF RFC3270	多协议标记交换支持差分服务
IETF RFC3809	运营商虚拟专用网（PPVPN）通用要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

站点

对于特定的骨干网，一个不需要通过骨干网就能完成互联的IP网络系统，被称之为一个站点。通常，这些主机和网络设备系统在地理上比较集中。但是两个地理位置较远的站点通过租用线路连接，运行适

当的路由协议来传播路由，并且这个租用线是这两个站点间数据转发的优选通道，那么这两个站点对于PE可以认为是一个VPN站点，即使每个站点有自己的CE路由器。这里的站点是一个拓扑概念，而不是一个地理概念。如果站点间的租用线失效，则一个站点变成两个站点，两个站点间可以使用VPN来通信。

3.1.2

客户

客户是站点的所有者。客户从运营商处得到VPN服务。运营商的VPN客户可以是单个企业、多个企业、一个Internet运营商、一个应用提供商，甚至是同样提供VPN业务的运营商（拥有自己的客户）。

客户还可以指定一组用户，并授权管理客户的VPN，这些用户被称为代理。

3.1.3

运营商

运营商是骨干网的所有者，运营商为客户提供VPN业务。

决定VPN包含哪些站点的管理策略由客户自己决定，某些客户将所有的管理工作交给运营商完成，或者由客户和运营商一起管理。本标准对VPN的讨论仅针对运营商管理的情形。更进一步的策略可能还包含VPN内部的路由策略，如VPN站点内部站点之间存在直达路由（full mesh），或强制两个站点之间的业务必须经过第三个站点（例如第三个站点内包含一个防火墙）。

3.1.4

虚拟专用网

对连接到骨干网上的站点集合施加某种控制策略，生成站点的子集，当某一子集同时包含两个或更多的站点，且这些站点之间通过骨干网连接具有可达性时，称这个子集为VPN。

在站点之间利用共享的骨干网络设施实现三层通信的虚拟专用网称为三层虚拟专用网。

如果运营商参与虚拟专用网业务的管理和运维，则称其为运营商虚拟专用网。

3.1.5

内联网/外联网

当VPN所有站点属于同一客户时，VPN通信被看作是内联网（Intranet）。

当VPN站点属于不同客户时，VPN通信被看作是外联网（Extranet）。

单个站点可以同时属于一个Intranet或多个Extranet。本标准不作特殊说明时，VPN不区分Intranet和Extranet。

3.1.6

用户边缘设备

用户边缘设备位于客户网络的边缘，它通过到一个或多个运营商边缘设备的数据连接链路为用户提供对运营商的接入。这里的连接可以是ATM、帧中继、以太网、PPP以及各种隧道等。

CE设备可以是一台主机、以太网交换机或路由器。通常情况下，CE设备是一台路由器，一个站点可能包含多台路由器，仅将连接到PE的路由器称为CE。CE与直连的PE设备建立路由邻接关系。CE路由器将站点的本地路由广播给PE路由器，并从PE路由器学习远端VPN路由。不同站点的CE路由器之间不能直接交换路由信息。

3.1.7

运营商边缘设备

运营商边缘设备位于运营商网络的边缘，通常是路由器设备。PE路由器使用静态路由、RIPv2、OSPF、或BGP与CE路由器交换路由信息。

为了增强VPN的可扩展性，对于PE路由器来说只需维护与其直接相连的VPN路由信息，而不要求PE路由器维护运营商网络中所有VPN的路由信息。

当使用MPLS对VPN业务进行转发以穿越运营商网络时，入口PE路由器的作用相当于入口LSR，而出口PE路由器的作用相当于出口LSR。

3.1.8

运营商路由器

运营商路由器是运营商网络中不连接CE设备的路由器。

如果骨干网采用MPLS技术，当PE路由器间对VPN数据业务进行转发时，P路由器的功能相当于传输LSR。由于数据在MPLS骨干网中被转发时使用了多层标记堆栈，P路由器只需要维护到达运营商PE路由器的路由，所以P路由器不需要为每个站点维护特定的VPN路由信息。

3.1.9

包交换网络

包交换网络是IP或MPLS网络，该网络上可建立支持VPN业务的隧道。

3.1.10

业务提供商网络

业务提供商网络是指由单个业务提供商管理的、PE和P设备互连的网络，该网络可属于一个AS，也可属于多个AS。

3.1.11

接入网络

在CE和PE设备之间提供连通性的连接被称为接入连接，这种接入连接包括专用物理链路、FR、ATM、VLAN以及其他IP隧道。

在CE和PE设备之间提供连通性的网络被称为接入网络，这种接入网络包括TDM网络、FR网络、ATM网络、以太网以及其他支持隧道技术的IP网络。

3.1.12

隧道

VPN应用中，为支持两个实体之间的数据包传送，用一个封装头封装另一报文的技术称为隧道。常见的隧道协议包括GRE、IPSec、IP-in-IP以及MPLS隧道。

将一个隧道封装到另一个隧道的技术称为层次化隧道，其中最内层隧道协议头定义了两个实体之间的逻辑联系（如CE或者PE之间）。

3.2 缩略语

下列缩略语适用于本标准。

AC	Attachment Circuits	直连电路
AFI	Address Field Identifier	地址字段标识
AS	Autonomous System	自治系统
ASBR	Autonomous System Border Router	自治系统边界路由器

YD/T 1943-2009

ASN	Autonomous System Number	自治系统编号
ASP	Application Service Provider	应用业务提供商
ATM	Asynchronous Transfer Mode	异步转移模式
BE	Best Effort	尽力而为
BGP	Border Gateway Protocol	边界网关协议
CE	Customer Edge	用户边缘设备
CHAP	Challenge Handshake Authentication Protocol	质询握手认证协议
CLI	Command Line Interface	命令行接口
COS	Class of Service	业务类型
DLCI	Data Link Connection Identifier	数据链路连接标志符
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name Service	域名服务
DOS	Denial of Service	拒绝服务攻击
DSCP	Diffserv Code Point	区分服务编码点
DUT	Device Under Test	被测设备
EAP	Extensible Authentication Protocol	可扩展认证协议
EF	Expedited Forwarding	加速转发
ER	Explicit Routing	显式路由
FCAPS	Fault Configuration Accounting Performance Security	差错/配置/计费/性能/安全
FEC	Forwarding Equivalence Class	转发等价类
FR	Frame Relay	帧中继
GRE	General Route Encapsulate	通用路由封装
GW	Gateway Router	网关路由器
IETF	Internet Engineer Task Force	因特网工程任务组
IGMP	Internet Group Management Protocol	互连网组管理协议
IGP	Interior Gateway Protocol	内联网关协议
IP	Internet Protocol	互连网协议
IPLS	IP-only LAN-like Service	只支持IP的类似LAN业务
IPSec	IP Security	IP安全协议
IPSECIM	IPSec Policy Information Model	IPSec策略信息模型
IPv4	Internet Protocol Version 4	互连网协议—第四版
ISP	Internet Service Provider	互连网业务提供者
ITU	International Telecommunications Union	国际电信联盟
LAN	Local Area Network	局域网
LIB	Label Information Base	标记信息库
LDP	Label Distribution Protocol	标记分发协议
LSP	Label Switched Path	标记交换路径

LSR	Label Switching Router	标记交换路由器
LUT	LSR Under Test	被测LSR
L2 VPN	Layer 2 Virtual Private Network	二层虚拟专用网
L3 VPN	Layer 3 Virtual Private Network	三层虚拟专用网
MD5	Message Digest 5 Algorithm MD5	消息摘要算法
MIB	Management Information Base	管理信息库
MPLS	Multiprotocol Label Switching	多协议标记交换
NAT	Network Address Translate	网络地址翻译
NHRP	Next Hop Route Protocol	下一跳路由协议
NMS	Network Management System	网络管理系统
NLRI	Network Layer Reach ability Information	网络层可达性信息
NTP	Network Time Protocol	网络时间协议
ORF	Outbound Route Filtering	出口路由过滤器
OSPF	Open Shortest Path First	开放最短路径优先
P	Provider Router	运营商路由器
PAP	Password Authentication Protocol	密码认证协议
PE	Provider Edge	运营商边缘设备
PHB	Per Hop Behavior	每一跳行为
PPVPN	Provider Provision Virtual Private Network	运营商运营虚拟专用网
PSN	Packet Switched Network	包交换网络
PVC	Permanent Virtual Circuit	永久虚电路
QoS	Quality of Service	服务质量
QPIM	QoS Policy Information Model	服务质量策略信息模型
RADIUS	Remote Authentication Dial-In User Service	远程认证拨号接入用户业务
RD	Routing Distinguisher	路由区分器
RIP	Routing Information Protocol	路由信息协议
RR	Routing Reflect	路由反射
RSVP	Resource Reservation Protocol	资源预留协议
RT	Route Target	路由目标
SAFI	Sub Address Field Identifier	子地址字段标识
SLA	Service Layer Agreement	业务等级协定
SLS	Service level Specification	业务等级规范
SP	Service Provider	业务提供商
TCP	Transmission Control Protocol	传输控制协议
TMN	Telecommunications Management Network	电信管理网络
TTL	Time-To-Live	生存时间
UDP	User Datagram Protocol	用户数据报协议

VFI	Virtual Forwarding Instance	虚拟转发实例
VLAN	Virtual Local Area Network	虚拟局域网
VPLS	Virtual Private LAN Service	虚拟专用LAN业务
VPWS	Virtual Private Wire Service	虚拟专用线路业务
VPN	Virtual Private Network	虚拟专用网
VPN-IPv4	VPN-IPv4	VPN IPv4地址
VRF	VPN Routing and Forwarding	VPN路由转发表
VSI	Virtual Switching Instance	虚拟交换实例

4 三层 PPVPN 分类

根据VPN隧道终结点的不同，可以将PPVPN分为两类：基于PE的三层VPN和基于CE的三层VPN。

4.1 基于 PE 的三层 VPN

三层VPN隧道终结点为PE时，称为基于PE的三层VPN。

在基于PE的三层VPN业务中，运营商为客户提供IP层的服务。此时，CE设备将PE看作为一个三层设备（IPv4或IPv6路由器），而PE设备接入一个或多个CE设备，并根据IP包头（包括IPv4和IPv6）信息转发用户数据包。

在基于PE的三层VPN业务中，通过PE和CE之间的路由交互，PE设备为每个VPN创建并维护一个VFI。该VFI终结与其他VFI互连的隧道，同时终结相应CE的接入连接。根据VFI中所包含的转发信息，PE设备从CE-PE接入连接上收到数据，并转发到相同VPN的其他PE，因此VFI应包含三层VPN的路由信息库和转发信息库。对VFI的支持，使得路由器从功能上看仅为单个VPN提供独享的服务，可以实现VPN路由与转发的隔离，并允许不同VPN之间使用重叠的地址空间。

基于PE的三层VPN中，PE设备可以使用隧道和层次化隧道为VFI提供通信连接。

图1为PE使用独立隧道承载不同VPN的参考模型，此时每个隧道为不同PE设备上的VFI建立通信连接。

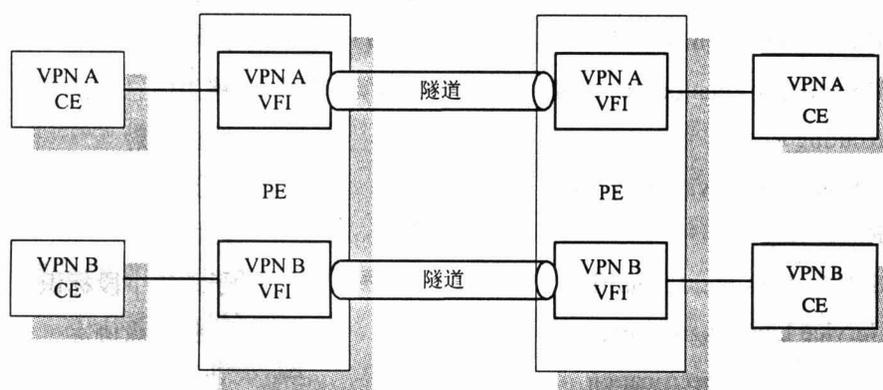


图1 基于 PE 的 VPN（独立隧道）

图2为PE使用层次化隧道承载多个VPN的参考模型，该共享隧道为不同VPN提供通信连接。PE设备通过对最内层协议封装头的分析，判断数据包到底属于哪个VPN。

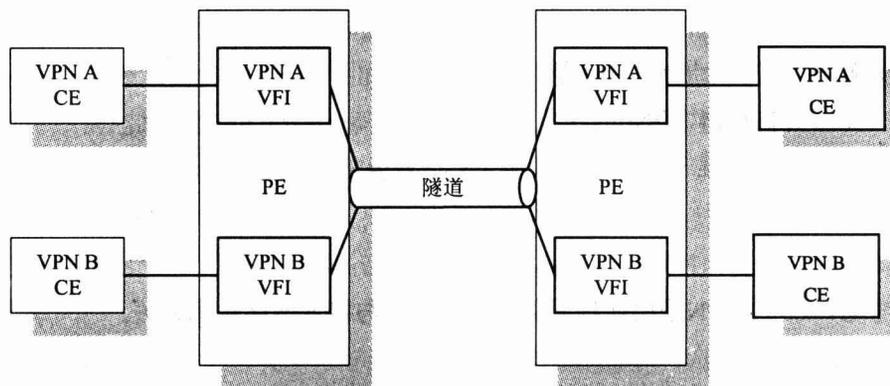


图2 基于 PE 的 VPN (共享分级隧道)

4.2 基于 CE 的三层 VPN

三层VPN隧道终结点为CE时，称为基于CE的三层VPN。

在基于CE的三层VPN业务中，CE通常仅为单个客户站点服务，因此可从物理上实现与其他客户VPN路由与转发的隔离。此时，所有VPN功能由CE设备实现，VPN对PE设备保持透明，PE设备不感知VPN中CE设备的成员关系，PE和P设备仅提供CE设备之间的路由和转发。

根据VPN客户需求和流量模型，CE之间的隧道拓扑可以是Full Mesh的，也可以是Partial Mesh的。

图3为基于CE的VPN参考模型。

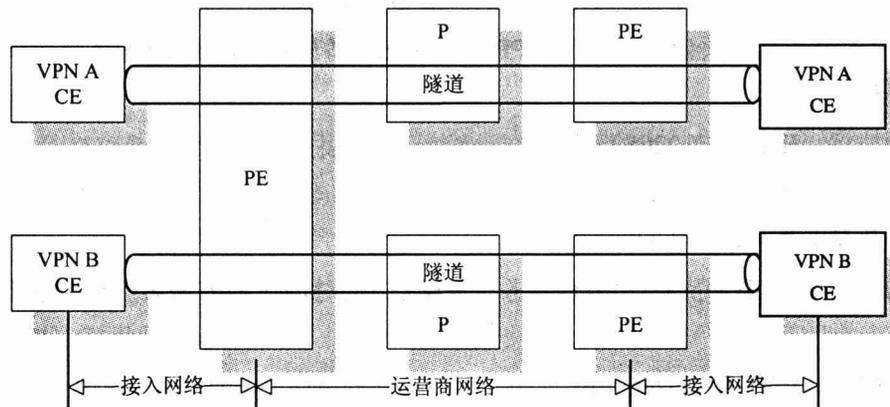


图3 基于 CE 的 VPN

5 通用业务要求

本章是对L3 PPVPN的通用业务的要求，既适用于客户，也适用于运营商。

5.1 隔离

PPVPN应提供VPN相关站点路由可达性信息的隔离机制，L3 VPN应提供解决方案，阻止VPN内部路由器与非授信实体发生路由交互，避免不良路由信息的引入对VPN路由信息库产生干扰。

PPVPN应提供手段，利用路由信息和配置方法，约束、隔离VPN数据仅分发至VPN站点。

PPVPN应支持单个站点属于多个VPN的应用场景，此时VPN解决方案必须确保站点的数据仅在相同VPN站点间传送。

VPN内部拓扑结构不应通告或泄漏给外部网络。

VPN隔离要求数据转发和路由信息的交互仅限于VPN内部站点之间，是PPVPN安全的重要组成。

5.2 地址

单个VPN内所有站点的IP地址必须保证唯一性。

PPVPN解决方案应支持IPv4、IPv6的封装和被封装协议。

若客户使用私有地址或非唯一的IP地址，那么VPN业务应提供客户地址翻译功能，保证VPN客户能够与公网互通。

5.3 服务质量

出于扩展性考虑，L3 PPVPN采用何种服务质量技术应与接入网络技术无关。

5.3.1 服务质量标准

本标准不定义新的服务质量协议，也不对已有协议进行扩展。L3 PPVPN应能支持以下一种或多种服务质量模型：

- 尽力而为的服务质量（必须支持）；
- 聚合CE接口级别的服务质量；
- 站点到站点的服务质量；
- Interserv信令；
- Diffserv标记；
- 跨包交换接入网络。

以上所有QoS机制需要CE和PE设备实施相应的流量整形及策略。

对于特定客户的语音及视频会话应用，L3 PPVPN的CE设备应实现Interserv服务质量模型。此时，CE设备应支持以下标准：

- 资源预留协议（IETF RFC2205）；
- 负载控制网络业务规范（IETF RFC2211）；
- 确保服务质量业务规范（IETF RFC2212）。

L3 PPVPN的CE和PE设备应支持Diffserv服务质量模型。此时，CE和PE设备应支持以下类型的每跳行为标准：

- 加速转发PHB（IETF RFC3246）；
- 确保转发PHB（IETF RFC2597）。

支持L3 PPVPN业务的CE和PE设备应根据以下IP头字段将数据包分类映射至Interserv、Diffserv业务模型：

- 协议ID；
- 源端口号；
- 目的端口号；
- 源地址；
- 目的地址。

对于特定的Internet流量，L3 PPVPN设备应支持随机早期检测机制，避免网络发生拥塞。

5.3.2 服务模型

运营商必须能够为客户提供有服务质量保障的VPN服务，应提供以下通用业务类型：可管理的接入VPN服务和边缘到边缘的QoS VPN服务。

可管理的接入VPN服务：该业务在CE和PE的接入连接上提供服务质量保障，对于Diffserv，要求仅在CE和PE的用户侧接口使能Diffserv，而不要求运营商骨干网实施。运营商应支持在PE设备上实施入口流量整形，还应支持数据包分类和Diffserv标记。运营商应支持根据客户选择进行数据包分类，或根据客户特定需求定制，其他更加复杂的服务质量策略可由客户自行实现。

边缘到边缘的QoS VPN服务：该业务根据运营商和客户驻地网业务划分点的不同，在本端CE到远端CE，或本端PE到远端PE之间提供服务质量保障。边缘到边缘的QoS服务应支持跨域和跨运营商的应用。

5.4 SLS 和 SLA

除IETF RFC3809所规定的SLA要求以外，Diffserv方案的SLS服务质量测量应遵循ITU-T Y.1311的分类：

- 点到点SLS（Pipe模型）：该模型结合VPN站点之间流量交互的服务质量目标，界定流量参数。点到点SLS提供与点到点帧中继、ATM PVC以及边缘到边缘MPLS隧道类似的SLS，对VPN可达站点的SLS规格集中应包括对某一特定站点所有点的点SLS定义。

- 点到云SLS（Hose模型）：该模型结合CE和PE之间流量交互的服务质量目标，界定流量参数。点到云SLS根据VPN站点向SP网络发送数据包的汇聚角度制定要求，而不考虑数据包的具体目的VPN站点。

- 云到点SLS：该模型结合PE和CE之间流量交互的服务质量目标，界定相关流量参数。但未定义从多个源地址向特定站点发送数据的流量参数，这种应用可能导致站点接口发生拥塞。

SLS应根据业务提供商和客户站点的划分，定义上行和下行流量的流量参数和转发行为。这时需要在入口定义流量策略，出口进行流量整形。

5.5 管理

L3 PPVPN业务必须是可管理的，应提供给运营商和客户管理VPN能力和特性的手段。进一步考虑，业务还应支持标准管理平台上的自动化操作和互操作能力。

要求L3 PPVPN网络管理符合ITU-T电信管理网络模型，满足以下通用的架构：

- 从网络（网元网管）角度看，网管系统应能够对开展业务所需的各种资源进行设计、部署和管理，这些资源包括交换、路由和传输等；

- 从业务网管角度看，网管系统应能够管理以上资源上所开展的VPN，包括VPN业务管理以及VPN商务管理（主要提供VPN客户的相关管理、计费信息）。

PPVPN管理应符合电信管理网络的“FCAPS”功能要求，包括故障、配置、计费、规定和安全。

5.6 互通

L3 PPVPN应支持不同VPN解决方案之间的互通，且具有良好的扩展性。

L3 PPVPN的互通应满足VPN流量和路由的隔离、安全、服务质量、接入和管理方面的要求，在网络迁移过程中，保障分属网络不同部分站点的服务连续性。

6 客户要求

本章从客户的角度提出对L3 PPVPN的业务要求。

6.1 VPN 成员

L3 PPVPN方案应支持VPN成员之间的Intranet和Extranet应用场景。

外联网方案中，应支持各个组织的客户代理根据多方的商业决策，批准VPN站点的添加、删除与管理。此外，还应提供手段，允许各个组织控制站点之间的流量和路由信息交互。

6.2 跨运营商

客户可能需要跨越多个管理域或运营商网络的VPN服务，因此PPVPN服务必须支持跨越多个AS或者SP网络，且对VPN客户保持透明（客户感觉单一的、同质的VPN服务）。

在应用初期，客户可能仅要求单一AS内VPN的SLA保障，但可能还需要将VPN扩展到跨AS/SP的应用场景中。这种情况下，与所有跨AS/SP应用相同，PPVPN业务应为客户的所有站点保障一致的SLA（不考虑站点的具体AS/SP归属）。

6.3 地址分配

客户可能要求L3 PPVPN支持以下地址分配方案：

- 客户自行分配重叠地址或私有地址，参见IETF RFC1918；
- 客户自行获得的全球唯一地址；
- 运营商静态分配的全球唯一地址；
- 运营商按需分配的全球唯一地址（如DHCP），包括临时性的远程接入和永久性的专线接入。

在非唯一地址/私有地址和Internet接入组合应用的情况下，L3 PPVPN方案应支持客户地址空间和全球唯一Internet地址空间之间的流量交换。运营商和客户可以部署NAT技术来满足这个要求。

优选的方案是分配全球唯一的公有地址，包括IPv4和IPv6。

对于不愿意进行网络重编号的客户，PPVPN方案应支持NAT技术。

6.4 路由协议

PPVPN不限制在CE和PE路由器、CE路由器之间使用何种路由协议，但应支持静态路由、IGP路由协议（如RIP、OSPF和IS-IS）以及BGP。

6.5 服务质量

L3 PPVPN业务的服务质量保障能力是客户关注的重要环节，对服务质量的要求应覆盖内联网、外联网以及VPN站点和Internet共享接入的应用场景。

6.5.1 应用级服务质量

L3 PPVPN解决方案应为客户提供应用级服务质量保障机制。

语音、交互式视频和多媒体应用期望要求严格的QoS保障，这些实时应用对时延、时延抖动、丢包、可用性和可靠性比较敏感。其他应用，如多媒体交互式视频应用、高性能Web浏览以及文件传输应用，要求近似于实时的性能。尽力而为的应用对网络性能的降低不太敏感，具有一定的弹性，并且能够适应网络性能的降低。

为满足特定应用的需求，合理处理运营商网络的拥塞，选择合适的服务质量技术和业务类型尤为重要。对于敏感业务，PPVPN解决方案应支持逐流的Interserv服务模型，为客户提供精细的SLA保障。对于非敏感业务，可以采用Diffserv服务质量模型。

L3 PPVPN解决方案应支持独立流的Interserv服务质量和汇聚流的Diffserv服务质量。

即使同一L3 PPVPN客户站点采用不同的接入网络技术，VPN解决方案应为客户应用提供一致的服务质量体验。

6.5.2 DSCP 透明性

L3 PPVPN解决方案应支持DSCP的透明性。

L3 PPVPN入口CE接收到用户设置的DSCP码点，VPN服务质量策略应支持将该码点透明地中继到出口CE上，见IETF RFC3270和ITU-T Y.1311.1。即使差分服务模型允许在服务质量域内或边界点上修改DSCP码点，客户对L3 PPVPN还可能有以下要求：

- VPN应用采用区别于运营商网络的DSCP方案；
- 客户在VPN内部站点采用多于运营商网络支持的DSCP分级；
- 在运营商的应用中，L3 PPVPN方案应该允许子运营商向客户分销VPN业务，并采用独立于父运营商的DSCP解决方案。

对DSCP透明性的支持，要求不对QoS和SLA产生影响。如果支持DSCP的透明性，运营商需要在管理域内透明携带VPN客户的DSCP值，但也允许在自身管理域内进行DSCP映射，以实施服务质量保障。

6.6 SLS 和 SLA

客户利用SLA监督运营商L3 PPVPN业务的实施和管理。

对于购买特定SLA业务的客户，VPN业务应提供手段，允许客户/客户代理接入网络，对业务的SLA实施状况进行测量。

6.7 客户管理

L3 PPVPN方案应提供方法，允许客户查看自己的VPN拓扑、运行状态、订购状况以及其他参数。

VPN方案应允许经过认证、授权的客户代理，配置和维护VPN相关信息，这些信息包括CE设备的管理信息以及运营商管理的客户属性。但应防止管理系统对敏感信息（如加密密钥等）的读写。

VPN方案应允许客户代理动态请求改变流量参数，客户也应支持接收运营商网络的实时响应。ITU-T Y.1311.1规定了动态带宽管理服务，该机制支持客户对VPN带宽分配变化请求的实时响应。

对不具备管理自身VPN站点能力的客户，VPN方案应提供外包服务，由运营商完成全部的VPN管理。

6.8 隔离

L3 PPVPN隔离包括流量和路由信息的隔离，并提供等同于一层和二层VPN的隔离能力（包括专线、FR以及ATM）。

6.9 安全

L3 PPVPN解决方案应支持一系列的安全属性，应支持高级别的安全服务，包括边缘到边缘的加密、认证以及防重放攻击。

除远程或临时用户的VPN接入应用，VPN服务的安全应该尽可能对客户保持透明，在第6.11.2节中进行详细描述。

除运营商安全机制以外，VPN客户还应支持实施自己的安全机制，为特殊应用或流量提供比站点到站点更好的安全粒度。

如果客户VPN需要服务质量保障，那么这些请求必须通过非加密域或协商认可的安全联盟通告给运营商。为支持Interserv，应支持使用明文或协商密钥的加密方式发送RSVP信息。在IPSec隧道中，应支持将被加密的内层IP头DSCP值复制到外层隧道的IP头中。

6.10 迁移影响

在客户从已有专用网络（CE路由器接入物理或虚拟的专网）迁移到L3 PPVPN网络过程中，应尽量减小迁移的代价以及通信的中断。

VPN解决方案应支持所有站点的全面迁移以及部分站点的迁移,参见ITU-T Y.1311.1。在部分迁移中,应保障未迁移的遗留站点与已迁移站点之间保持三层的可达性。

6.11 网络接入

L3 PPVPN应为用户提供等效于专网的服务。

6.11.1 物理/链路层

L3 PPVPN应该支持广泛的物理和链路层接入技术,包括PSTN、ISDN、xDSL、电缆Modem、租用线路、以太网、以太网VLAN、ATM、FR、无线本地环以及移动无线接入等。且保障VPN能力和服务质量与特定的接入技术无关。

6.11.2 临时接入

L3 PPVPN服务应允许已认证用户永久或临时地接入一个或者多个L3 VPN,且支持多种接入技术。远程或临时VPN接入应支持包括ISDN、PSTN拨号、xDSL或经由其他SP网络接入。且允许客户选择临时接入用户的认证方式,包括运营商提供、第三方提供以及客户自己提供的认证。

临时接入的VPN用户需要经常切换VPN附着站点,因此VPN解决方案应提供对VPN用户进行认证、授权的方法。VPN客户代理和运营商应为VPN远程接入用户实施认证,并为授权用户自动完成网络激活、加入VPN的操作。

VPN方案应支持用户经由具有Internet接入的网络接入L3 VPN。

移动用户可以在L3 VPN站点内移动,还可以临时接入同一VPN内的不同站点。在上述情况中,VPN方案都必须提供认证手段。

6.11.3 接入网络共享

在基于PE的L3 VPN中,如果VPN流量与其他流量共享接入网络(如Internet接入),那么接入网络中的数据安全由VPN客户负责。

6.11.4 接入连通性

L3 PPVPN客户端必须支持不同类型的物理连通性,例如:多归属站点、用户站点由后门链路连接、设备归属多个运营商网络等。VPN解决方案至少应支持图4所示的6种接入场景,确保它们在物理及链路上保持连通性。

若在多种物理、逻辑链路上,提供从CE到其他CE和PE的访问,接入方案必须支持冗余链路和负载均衡。VPN应支持冗余链路接入方案,保障CE站点与其他CE站点之间的连通性,为VPN接入提供了更多的可选路径。VPN应支持负载均衡接入方案,并支持实施流量工程技术,利用空闲的冗余资源使网络性能得到提升。

对于多归属、单运营商网络接入,VPN PE设备应支持在CE到PE的链路提供负载均衡功能。如图4A所示的连接到CE的两个PE应该提供负载均衡;图4C所示的连接到两个CE的两个PE应该提供负载均衡。

根据客户需求,运营商应该向客户提供不同负载均衡参数(包括多个负载均衡链路上的业务比例、指定链路上的业务比例等)。在接入连接出现问题的时候,负载平衡功能应为客户提供弹性的接入应用。如图4B所示的CE可以通过两个不同的接入网连接到两个不同的运营商;图4D所示的CE通过后门链路也可以连接到其他运营商网络,这种接入具有更强的弹性。进一步可以对以上方法进行任意组合,如图4E、图4F所示,PPVPN都应进行支持。

对于多归属、多运营商的网络环境，不同运营商也应该支持负载平衡的功能。多运营商的负载平衡需要运营商之间的互操作达成服务策略和协定。

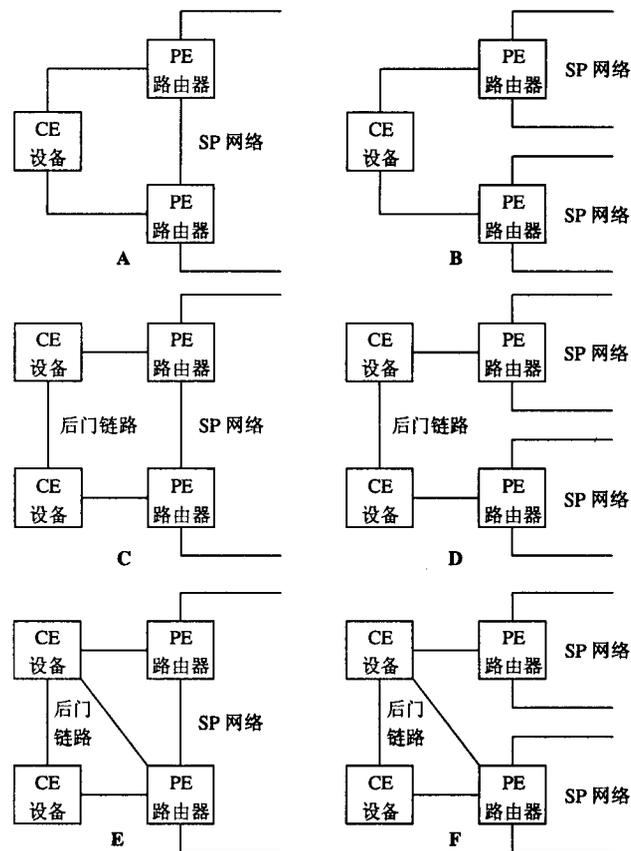


图4 典型接入类型

6.12 业务访问

除VPN业务之外，VPN客户还可能访问其他业务。

6.12.1 Internet

运营商应支持使用相同接入网络，将一个或多个客户站点同时接入L3 PPVPN和Internet。

客户可以通过PPVPN站点集合直接将Internet流量传送到拥有防火墙（或其他安全设备）、拥有NAT功能的用户站点，处理Internet与客户VPN之间的各种业务。

VPN用户应该可以访问不属于VPN的、使用公有地址的Internet站点，如企业的公共网站服务器。

如果客户网络使用非唯一地址或私有IP地址，那么客户或运营商必须提供NAT（或类似机制）实现地址的转换。

6.12.2 应用业务提供商

L3 PPVPN方案应支持用户访问其他主机集合、应用业务以及应用业务提供商，此时要求应用业务提供商加入客户所在的VPN。

6.12.3 其他业务

结合VPN服务，客户还可能要求访问其他服务，包括DNS、FTP、NNTP、SMTP、LDAP、VoIP、NAT、视频会议、共享应用、电子商务、流媒体、电子词典以及防火墙等。实现上述应用的资源可以使用专用物理链接，也可以使用逻辑共享链接，若使用逻辑共享则应按照VPN方案考虑不同接入的隔离。

6.13 混合 VPN 业务

Intranet或Extranet客户可能需要多个VPN解决方案的混合应用，包括以下应用场景：

- VPN迁移；
- VPN合并；
- 使用不同类型VPN的Extranet用户接入；
- 不同站点集合的VPN能力需求不同；
- 临时接入；
- 由不同运营商提供的VPN解决方案。

在避免网络提供服务、扩展、性能等管理过度复杂的前提下，VPN框架结构和解决方案中应满足不同L3 VPN解决方案的互联、互通以及可达要求。

7 运营商网络要求

本章从运营商的角度提出对L3 PPVPN的业务要求。

7.1 扩展性

IETF RFC3809对PPVPN的容量、扩容以及度量提出了要求。以外，L3 PPVPN还应从方案承载VPN数目、每VPN的接口数目、每VPN的路由数目以及VPN配置变化的速度等角度，考虑VPN网络的建设容量。

- VPN方案应提供VPN网络数目的升级能力，允许每个运营商网络提供大量的VPN。
- VPN方案应为每个VPN接入站点提供接口数目升级能力（由客户机构大小和组织结构决定）。
- VPN方案应为每个VPN支持的路由条目提供升级能力。
- VPN方案应支持灵活的配置、设置变化，支持单个VPN在时间单元内增加、删除站点拓扑。

考虑一些复杂的网络应用（如跨自治域VPN、跨管理域VPN以及运营商的VPN），VPN方案应该注意网络规模与性能的结合。还应该考虑其他方面的问题，例如容量的需求与限制、管理系统支持相互作用实例的数目以及升级对管理系统带来的影响。

7.2 地址

如5.2节通用业务要求，运营商必须支持公有和私有IP地址（IPv4和IPv6地址的单播和组播地址）。为支持这些地址方案，要求运营商的L3 PPVPN方案达到以下要求。

- 支持从自己拥有的公共IP地址空间为PPVPN的客户站点分配地址块，并以高效的方式向其他运营商、站点集合提供路由通告。
- 支持客户指定的地址，这些地址可以是公有的或私有的。
- 使用私有IP地址时，VPN方案应提供将保留地址转换为公网地址的方法（如NAT），保证与其他使用重叠地址的VPN或Internet之间的正常通信。

7.3 标识符

运营商在管理、控制以及路由协议中需要使用标识符，L3 PPVPN方案应支持以下标识符：

- 支持可扩展为多运营商的VPN，在互联的SP网络中至少为SP域分配一个唯一的标识。理想情况下，应该为SP域分配一个全球唯一的标识（如AS号码）。
- 支持为每个VPN分配唯一的标识，至少在一个SP网络中保证唯一。理想情况下，考虑VPN可能扩展到跨SP域的VPN，应为VPN分配一个全球唯一的标识，且符合IETF RFC 2685的规定。

- 支持为每个CE设备分配唯一的标识，至少在一个SP网络中保证唯一。
- 支持为每个PE设备分配唯一的标识，至少在一个SP网络中保证唯一。
- 支持在前述网络的集合中，确保互联SP网络的设备具有唯一的标识。
- 支持为每个站点分配唯一的标识，至少在每个PE路由器的接口上保证唯一。
- 支持为每个隧道分配唯一的标识，至少在每个路由器的隧道上保证唯一。

7.4 VPN 相关信息学习

VPN CE和PE设备的配置是运营商的重要工作，为减小配置的复杂度，VPN方案应支持PE和CE设备的自学习能力，允许VPN信息的自动学习动态配置网络。L3 PPVPN解决方案应支持以下功能。

- VPN中的每个设备应该可以在VPN中标识并认证自己，通过对其他VPN成员的学习，设备应可以安全地交换配置信息。这些配置信息包括PE的IP地址以及其他扩展信息。

- VPN中的每个设备应该可以判断其他设备是否属于同一VPN，这种成员发现机制应支持基于源地址的认证，并防止非授权用户访问网络。

- VPN相关设备应限制对VPN信息的分发仅限于VPN内部。
- 在基于PE的VPN中，方案应提供手段，对接入CE进行认证，并验证VPN配置是否正确。
- VPN方案应提供机制，保证对VPN成员关系的变化实现快速响应。
- VPN方案应为站点和客户 provide 动态创建、改变以及管理VPN的方法。

7.5 SLS 和 SLA 支持

典型情况下，与5.4节和IETF RFC3809要求一致，运营商应将特定SLS做为VPN服务协议的组成部分一起提供给客户。这个SLA约定要求运营商对SLS参数进行监测，这些参数包括服务质量、网络可用性、响应时间以及配置时间间隔。

7.6 服务质量与流量工程

L3 PPVPN应提供服务质量保障。

VPN方案中运营商可以控制网络资源的提供、PE和P路由器的配置（甚至包括CE设备），所以运营商应负责为客户提供5.3.2节所述的服务质量模型，包括可管理的QoS接入服务和边缘到边缘的QoS服务。

VPN方案必须描述为满足QoS指标所提供的流量工程的可用性，该流量工程描述中应量化升级能力和实施效率因素。流量工程可以在整网提供，也可以基于每个VPN提供。

采用安全机制不应影响QoS实施带来影响。如IETF RFC 2983要求，使用IPSec隧道，不应影响DiffServ策略带来影响。

在VPN服务中，运营商网络应提供从用户DiffServ标记到运营商网络标记的映射功能，见IETF RFC 2475所述。

符合6.5.2节要求，当客户需要提供DSCP码点的透明性时，VPN从客户接收到数据包，并由出口发往目的地，必须保证IP头中的DSCP字段数值不发生变化。

7.7 路由

VPN方案应限制路由策略和路由可达性信息仅在VPN成员站点内部分发。

VPN方案可采用认证机制（如MD5鉴权）保障路由信息的安全交互。

VPN方案还应提供其他方法将运营商网络和客户VPN与异常路由行为隔离，如防止路由振荡、过滤路由前缀、设置CE发布路由的条目数量或设置CE发布路由的速率等。

当VPN客户使用重叠地址时，VPN方案应该能够区分不同VPN的重叠地址。

VPN解决方案应提供选项，以确定是否允许将VPN路由向Internet通告。

基于PE的VPN方案中，运营商内部网关协议不应受到PE与CE路由器之间的路由协议限制。运营商可以选择使用不同的IGP路由协议。

每个L3 PPVPN方案中，必须清楚地分析VPN业务对运营商网络所带来的额外路由负担。

7.8 隔离

外部网络（Internet或其他相连的VPN）不应看到PPVPN的内部结构。

从运营商角度出发，基于PE的PPVPN必须确保业务、路由信息在得到VPN鉴权、授权的成员之间交换；基于CE的PPVPN中，确保业务、路由信息在站点互联的隧道中交换，有效地实现隔离的要求。

VPN方案应提供满足QoS的SLA要求的方法，将非VPN客户业务对VPN业务的影响隔离。同样，PPVPN方案应提供将某VPN业务站点产生的拥塞与其他VPN隔离，减少拥塞对其他VPN的影响。

7.9 安全

本节从运营商角度规定了VPN安全要求，包含对客户的数据安全，如何为临时、远程或移动用户服务提供鉴权以及如何保护运营商的网络资源。

7.9.1 客户数据安全

VPN方案应向客户提供整套的安全选项，满足通用的安全要求。每个VPN方案必须清楚地说明配置选项如何进行相互协调工作。

当VPN方案运行在Internet之上时，为保证客户VPN业务流的安全性，VPN应对业务流支持以下一个或多个标准的IPSec功能：

- (1) 加密，只允许授权的设备解密业务流；
- (2) 完整，确保数据不被修改；
- (3) 认证，确保业务发送者真正是宣称的发送者；
- (4) 防止重放攻击，防止中间人的攻击。

VPN方案应在客户的业务流中实现上述功能，这些业务包括站点之间、临时用户与站点之间以及临时用户之间的业务。同时也应在控制流中实现上述功能（如路由信息的交换）。这些安全功能应对用户保持透明，不为客户所感知。

VPN方案应支持这些安全功能，并在不同设备之间具有可配置性，包括CE-CE、PE-PE以及CE-PE。方案可选为支持每条路由、每个VPN进行安全配置。

VPN方案应支持一种或多种加密方案，包括AES、DES、3DES。加密、解密及密钥管理都应在安全管理系统中得到支持。

7.9.2 鉴权服务

如6.11.2节临时接入要求所述，为支持临时用户接入的需求，VPN方案必须提供鉴权服务。

VPN内部的业务交互涉及不同种类的设备，必须保证设备能够协调工作提供服务，参见ITU-T Y.1311.1。这些网络设备包括CE、PE、防火墙、骨干路由器、服务器以及管理工作站等。如7.4节所述，这些设备可以通过手工静态配置或动态发现协议互相学习、标识其他设备。当设备协同工作时，在提供服务之前，需要对等设备进行鉴权。该认证功能也可以应用到访问网络资源的控制之中。

上述对等实体之间的鉴定、认证功能只适用于同一VPN的网络设备，包括：

- CE和PE之间的业务；
- 相同VPN的CE之间的业务；
- CE或PE为VPN处理路由布告；
- 策略决策点和网元；
- 管理工作站和SNMP代理。

VPN方案应为每项对等体的认证功能进行说明，包括：

- 哪里需要认证；
- 如何实现认证；
- 必须达到什么级别的安全认证；
- 配置、维持设备标识的方法；
- 执行认证需要的认证信息。

7.9.3 资源保护

如3.1.5节定义，一个站点可以属于某个组织的内联网，也可以属于其他组织的外联网，可以访问Internet，也可以是前者的组合。在这样的情况下，VPN站点可能受到来自不同源地址的攻击。潜在的攻击源包括：

- 公有IP骨干网连接的用户；
- Internet用户；
- 属于内联网或外联网的临时站点的用户。

站点可能遇到的安全威胁包括以下情况：

- 拒绝服务攻击，包括垃圾邮件、接入连接阻塞、TCP同步攻击已经Ping攻击等；
- 非法入侵，最终可能导致拒绝服务攻击（如特洛伊木马攻击）。

为了应付以上的安全威胁，运营商应控制对站点的访问，这些方法包括防火墙过滤、监控以及告警，还应建立日志记录所有可疑行为。

VPN方案中的网络设备必须为运营商提供报告非法侵入的手段。

7.10 跨域 VPN

L3 PPVPN方案必须支持跨自治域的应用，可选支持跨运营商的应用，并提供标准的解决方案（包括基于CE的VPN和基于PE的VPN）。

VPN跨域方案中，应满足非跨域PPVPN对运营商提出的所有业务要求，包括业务/路由的隔离、SLA协定、管理以及安全等。跨域方案必须清楚地描述运营商之间的网络接口、封装方法、路由协议以及所有的应用参数。

跨自治域VPN解决方案应在运营商之间或运营商内部建立一个协定，该协定明确不同管理实体之间的信任、经济以及管理责任。本标准不涉及对该协定的要求。

全面可升级的VPN服务应支持多达数百个运营商的PPVPN业务，对每个运营商规模的具体要求可参见IETE RFC 3809。

7.10.1 路由协议

如果自治域之间的链路不可信，那么运行在这些自治域之间的路由协议必须支持某些形式的认证手段。如在TCP选项中携带MD5数字摘要，可以加强BGP的安全性，见IETE RFC 2385。

VPN方案应将BGP作为标准的跨域路由协议，并以此控制VPN业务传输路径。

7.10.2 管理

对单个自治域VPN的管理要求同样适用于串联的跨自治域的VPN应用，最小化管理子系统应具备以下能力：

- 分析工具，例如ping、traceroute；
- 从一个AS安全地接入到另一个AS的管理系统；
- 配置请求和状态查询工具；
- 差错通知和问题定位工具。

7.10.3 服务质量

跨域VPN方案应提供手段，判断跨域能否建立保证统一服务质量的VPN业务。

VPN从单域扩展到跨域时，需要建立代理机制，通过该机制向不同自治域网络请求或通告SLA参数，包括带宽和QoS等。

代理机制应支持手工配置，运营商在这种情况下可以向其他运营商提出要求，获得给定站点往返业务的带宽和QoS参数；代理机制也应支持自动配置，这种情况下由设备动态地请求/接收特定的SLA参数。在L3 MPLS VPN中，PE在与相邻自治域中的PE通信时，可以为不同等级的业务协商标签；代理机制也应支持手工、自动相结合的配置方式。

为了提高代理机制的扩展性，跨域VPN方案必须提供自治域之间的QoS汇聚、代理申请带宽的手段，避免以单个VPN为单位实现代理。可以由运营商制定服务协定，并说明为所有VPN客户提供特定QoS参数时的最大带宽。也可以在不同自治域的PE之间支持三层PPVPN服务时，在层次化隧道基础上实现QoS汇聚。

7.10.4 安全

如果隧道跨越多个运营商网络，并穿越不安全的SP、PoP、NAP或IX，那么就必须实施安全机制，包括加密、鉴权、资源保护以及安全管理。

7.11 VPN 批发

L3 PPVPN应支持Carrier's Carrier架构，包括运营商向另一个运营商提供VPN业务以及VPN服务的批发和零售。

Carrier's Carrier架构中，要求批发商VPN对分销商VPN的地址、路由保证透明性。

Carrier's Carrier架构应支持层次结构，VPN的分销商可以将从批发商处购买的VPN服务再向另一个运营商出售。

L3 PPVPN应支持以下几种Carrier's Carrier：

- 客户的运营商不负责为客户操作PPVPN服务；
- 客户的运营商负责为客户操作PPVPN服务，但这些服务与运营商提供的PPVPN业务不存在关联；
- 客户的运营商负责为客户操作PPVPN服务，而且这些服务与运营商提供的PPVPN业务相互关联。

7.12 隧道封装

为提供CE站点或PE设备之间的连通性，L3 PPVPN骨干网应支持多种隧道技术，包括L2TP、IPSec、GRE、MPLS及IP-in-IP等。

VPN应用需要建立隧道承载业务，PE路由器必须支持隧道建立协议，并支持隧道的静态配置。如果实施隧道技术，隧道建立协议必须传递以下相关信息：

- 相关标识符；
- QoS/SLA参数；
- 复位信息；
- 复用标识符；
- 安全参数。

隧道技术还应提供监测方法，监控以下信息：

- 静态特性，如隧道状态up、down所花费的时间；
- 隧道up、down之间经过的状态迁移数；
- 隧道事件，如隧道up、down状态之间的迁移。

VPN运营商使用的隧道技术以及相关的隧道建立、复用及维护机制必须符合本标准的各项要求，包括扩展性、隔离、安全、服务质量以及管理要求等。

7.13 接入网和骨干网

本节规定L3 PPVPN对运营商接入网和骨干网技术的要求。

运营商可以使用单一底层网络承载多种业务，包括Internet、VPN、流量工程以及区分服务等。

7.13.1 专用接入网

L3 PPVPN服务应与接入网络采用何种物理层、链路层以及网络层技术保持无关。但若指定VPN业务SLA/QoS时，就必须对接入网络的特性进行说明。

7.13.2 按需接入网

如6.11节网络接入的要求，运营商应支持临时用户访问VPN。

VPN方案必须支持用户通过本运营商接入网接入，直接访问VPN。运营商还应支持如何从其他运营商接入网络，访问VPN服务。

在内联网应用中，客户应储存、维护所有的用户识别、认证信息。在外联网应用中，客户应维护鉴权服务器，或将外联网用户的鉴权工作转包给运营商维护。

为方便运营商对接入网的控制，运营商应可以获得客户的识别、认证信息，或查询客户维护的服务器。运营商还应为其他VPN运营商提供接入服务，若接入运营商代表VPN运营商对用户进行识别/认证，则运营商之间应达成满足通用要求的协定。

对用户的接入鉴权应支持多种认证协议，包括PAP、CHAP和EAP。

7.13.3 骨干网

L3 PPVPN服务应与骨干网采用何种物理层、链路层技术保持无关。但若指定VPN业务SLA/QoS时，就必须对骨干网的特性进行说明。

7.14 保护与恢复

若L3 PPVPN方案提供主要和备份接入链路，那么VPN方案必须提供保护与恢复连接的功能。任何时候CE站点接入PE的主要连接发生中断时，应实现接入流量的切换。VPN方案应支持自动的链路保护功能，当监测到主要连接发生中断时，业务流应迅速地转换到备份连接上。若配置故障恢复时仍然使用主要连接，那么也应动态地将业务流切换回主要连接上。

按照6.11节网络接入的要求，VPN方案使用多归属接入PE时，应支持负载均衡提供一定的网络冗余。当一个或多个（但不是全部）接入连接中断时，负载均衡参数应支持动态地、快速地将业务流从故障链路转接到剩余链路上。一旦故障恢复，负载均衡功能应自动地将负载比例调整回故障前的配置。

在运营商骨干网的基础架构上，运营商应可以实现保护、恢复机制，提高VPN服务的可靠性和容错度。这些技术应支持升级能力，因此运营商不应以单个VPN为目标实施这些功能，而从全网的角度来考虑这个问题。

VPN方案应支持监测和报警功能，来显示网络保护和恢复功能是否正常工作。

7.15 互操作

L3 PPVPN方案的互操作性应支持：

- 在一个运营商网络内，方便地使用PE设备、管理CE设备；
- 在多个运营商互联的网络中，实现L3 VPN服务；
- 使用不同的L3 VPN技术，或使用相同技术的不同实施中，完成客户站点的互联、互通。

VPN方案必须清楚地说明能否满足上述要求。如果可以，方案中必须说明对具体互操作性的实施方法，还必须说明VPN互操作方案的网络接口、封装方法、路由协议、安全策略、隔离、管理以及所有VPN方案其他的应用要求。

7.16 迁移支持

运营商必须为客户提供良好的VPN迁移方案，以保证客户在site-by-site基础上，将服务中断的损失减小到最低程度。

若VPN方案支持互连互通，那么运营商也应提供迁移支持。在互联互通发生变化时，保障客户以最小的代价完成迁移。

8 运营商管理要求

L3 PPVPN方案必须提供手段给运营商，来浏览每个客户VPN的拓扑、运行状态、订购状态以及其他相关参数。VPN方案还应提供方法给运营商，来浏览VPN设备的下层逻辑和物理拓扑、运行状态、服务情况以及其他相关参数。

VPN管理方案应提供切实可行的、基于标准的管理接口，避免使用私有的管理方法，尽量减少为管理工作带来额外的负担。

VPN管理方案应符合ITU-T Y.1311.1运营商网络管理系统的要求，包括差错管理、配置管理、计费管理、性能管理和安全管理。

8.1 差错管理

VPN差错管理应支持：

- 客户出现错误的指示；
- 错误的探测(事件报告、示警以及错误可视化)；
- 错误的定位（分析示警报告及诊断）；
- 事件记录或日志（对异常产生记录）；
- 纠正操作（对业务、路由以及资源进行重新分配）。

基于PE的VPN依赖于公用网络的下层结构，网络管理系统必须提供方法，通知运营商由于骨干网下层结构故障给客户所带来的影响。网管系统还应提供指向相关用户配置信息的指针，协助进行故障隔离和排障工作。

配置错误可能导致VPN服务失败，或无法满足各项业务要求（如业务、路由的隔离），网络管理系统应提供配置错误发现机制。由于配置错误往往涉及不止一个节点，甚至会达到全球范围，这种配置错误的探测十分困难。为降低配置错序探测的难度，网管系统应为其制定协议，在不同端节点上系统地、强制地、连续地检查全部隧道的配置参数。

为了方便地诊断错误，网管系统必须提供三层可达性的验证功能。网管系统还应支持对VPN设备配置参数正确性的验证功能。

8.2 配置管理

网络管理系统必须支持L3 PPVPN的三层可达性配置，必须提供各种VPN组件的配置管理，包括PE、CE、嵌套VPN隧道、接入连接、路由以及服务质量等。如果VPN支持共享访问Internet，那么网管系统必须支持对该功能选项的配置。

VPN的具体配置和拓扑依赖于客户的组织构成，因此VPN系统应支持客户提出的特定要求。网管系统必须确保VPN设备和协议配置的一致性和正确性。

网管系统应支持本地化的、自动化的增加和删除站点。

网管系统应支持根据运营商定义的服务模板来配置管理VPN，服务模板包括明确的服务要求和策略。IPSec隧道模板应包括隧道端点、鉴权模式、加密方案以及鉴权算法，若需要还应包括预共享密钥、流量过滤等；BGP/MPLS服务模板应包括组成VPN的站点等；SLA模板应包括满足SLA所需的时延、抖动、吞吐量以及丢包率门限等。客户的VPN服务订单可以看作是一系列示范服务模板的组合，依次组合这些服务模板，可以定义客户VPN的逻辑业务架构。

运营商应支持使用服务模板定义运营商网络的服务架构，OSPF模板应包括组成区域的子网、区域号以及区域类型；BGP模板应包括为特定目的地优先选择出口路由器。

运营商应提供方法，将服务模板翻译为相关设备支持的配置信息。

人工配置错误、入侵攻击以及服务要求冲突可能导致配置错误，配置管理应提供配置错误的诊断方法，并监测提供给客户的服务是否满足要求。

8.2.1 基于 PE VPN 的配置管理

除以上配置管理要求之外，对基于PE的VPN的配置管理还有以下要求。

- 网管系统必须支持三层PE路由器的配置功能，包括内联网成员、外联网成员、接入连接的CE路由协议、路由度量以及隧道的配置。
- 网管系统应支持对VPN标识的要求，包括运营商、L3 VPN、PE、CE、层次化VPN隧道以及接入连接的标识。
- 网管系统应支持PE和P路由器之间的隧道配置，包括隧道标识符的协商、层次化VPN隧道、VPN、QoS/SLA服务以及相关服务信息。
- 网管系统应支持对PE和CE之间的路由协议进行配置。
- 网管系统应支持对PE之间、PE与P之间的路由协议进行配置。
- 若支持组播业务，网管系统应支持对组播路由协议进行配置。

- 网管系统应协调L3 PPVPN的配置与下层网络结构的配置之间的配合，下层网络包括VPN连接的物理层和链路层网络。

8.2.2 基于CE VPN的配置管理

除以上配置管理要求之外，对基于CE VPN的配置管理还有以下要求：

- 网管系统应支持CE之间的隧道配置，包括隧道标识符的协商、VPN、QoS/SLA服务以及相关服务信息；
- 网管系统应支持对PE和CE之间的路由协议进行配置；
- 若支持组播业务，网管系统应支持对组播路由协议进行配置。

8.2.3 路由

网管系统应提供手段，向VPN运营商提供IGP路由协议参数，这些参数包括链路级度量值、容量、服务质量能力以及恢复参数。

8.2.4 网络接入

网管系统应提供手段，允许运营商管理PE和CE之间的接入网络。

8.2.5 业务安全

网管系统应提供手段，允许运营商提供安全服务的实体和相关参数。在IPSec服务中，应提供PE和CE的隧道、选项、密钥以及其他参数；在入侵检测服务中，应提供过滤和检测规则。

8.2.6 VPN资源参数

网管系统应提供手段，允许运营商动态提供VPN服务资源。在基于PE的VPN服务中，应支持动态管理VSI、VFI表所支持的用户数。

对于客户需求的频繁变化（如站点加入、离开时拓扑结构变化）以及网络升级的支持，网管系统应支持动态分配VPN资源。对于拨号、无线VPN服务，PE设备应支持VPN资源的动态分配。

如果SP支持动态带宽管理服务，考虑到计费的要求，那么必须对要求的带宽分配变化记录日期、时间、变化量和时间间隔等日志。

如果运营商支持动态带宽管理服务，则VPN系统必须支持在SLA规定的范围内，按照客户要求进行资源的动态分配（SLA参数包括响应时间和满足服务要求的概率）。

8.2.7 增值业务访问

在公共骨干网上，L3 PPVPN提供站点之间的控制访问功能。运营商还可能向客户提供其他增值服务，如Internet访问、防火墙业务、入侵检测、IP电话、IP交换中心、集群应用以及远程备份等。VPN解决方案必须为不同增值业务提供访问接入，但本标准不规定如何解决增值业务同VPN之间的互操作性（如寻址、数据完整及安全问题）。

VPN运营商应支持向一个或多个客户提供IP数据业务，VPN服务应支持多种类型的标准IP数据业务（包括DNS、NTP和RADIUS等），并提供对网络的操作和管理功能。

Internet访问VPN时，VPN应支持防火墙功能对访问进行限制。可管理的防火墙服务必须区分不同等级，从功能上包括丢弃特定协议类型、入侵保护、业务速率限制以及防止恶意攻击等。考虑冗余和故障恢复，防火墙必须提供故障保护机制。

即使同一物理设备可能支持多个VPN（如基于PE的VPN），但仍要求运营商支持基于每个VPN提供可管理的防火墙。管理防火墙应设置在VPN的主要访问点处，管理防火墙服务可以内嵌于CE或PE设备之中，也可以由单独设备实现。

网管系统应允许客户外包IP数据业务的管理，可以是VPN的运营商或第三方。

为满足客户的订单需求，网管系统应支持为最优分配IP服务收集必要的信息。

网管系统应支持Internet和VPN站点之间的可达性配置，可以通过路由策略的配置，控制VPN路由向Internet的通告。

8.2.8 混合VPN业务

网管系统应支持不同L3 PPVPN方案之间的互联互通配置，并确保客户获得一致的安全性和端到端的服务质量保障。

8.3 计费管理

出于VPN计费考虑，运营商需要收集网络资源的监测资料。运营商需要网管系统能够提供与计费信息相关的性能管理、差错管理信息，以确保给出的计费账单中，充分考虑到SLA协定，有多少时间达到客户的SLS指标要求。

网管系统应说明以下计费功能如何实现：

- 资源利用率的监测；
- 计费信息的采集；
- 存储、管理监测数据。

网管系统可选提供给运营商准实时的监测信息报告，并将该报告作为客户网络管理服务的一部分提供给客户。

如果运营商支持动态带宽管理服务，出于监控、计费需要，网管系统应支持对动态带宽分配的数据进行跟踪和记录，包括日期、时间、带宽变化的量以及带宽变化的时间间隔等。

8.4 性能管理

网管系统性能管理应包括监测、收集VPN网络性能数据的功能，这些数据包括设备、易用性、服务、SLS满足程度以及服务质量等。

性能管理还应支持VPN重要参数的分析，包括带宽利用、响应时间、可用性、服务质量统计以及收集数据所体现的趋势。

8.4.1 性能监视

为评估性能度量是否达到给定的SLA协定，网管系统应支持对VPN设备行为的监视。根据业务SLA提供的各项指标，网管系统应支持多种监测技术，包括服务质量、安全性、组播以及临时接入等。监视这些参数可能会对VPN服务带来影响，网管系统应将影响降低到最小限度。

对于未规定SLA参数的VPN，网管系统也必须提供监控手段，包括资源使用、设备状态、传送设备以及监控资源的控制（如网络接入访问点处，客户和移动用户使用的探针和远端代理等）。

8.4.2 SLA/QoS 管理特性

网管系统应根据SLA协定内容，监测相应SLS的指示标记，来支持运营商与不同客户之间所签订的SLA。

网管系统应使用服务质量参数的测量定义、技术和方法，并符合IETF IP性能量测工作组对于时延、丢包率和时延抖动的规定。

网管系统应支持端到端服务质量参数的分配和测量，这种分配和测量应覆盖一个或多个VPN网络应用场景。

网管系统应支持为VPN SLA提供实时的性能监测，内容包括指示和门限报警，同时应支持报警门限的配置。

8.5 安全管理

网管系统的安全管理功能应包括VPN网络设备、接入连接以及协议的安全管理特性，同时应符合6.9节对客户数据和控制平面的安全要求。

8.5.1 资源访问控制

安全管理应支持VPN资源的访问控制功能，以此决定用户是否可以访问网络应用和VPN网络资源。缺少这种控制，VPN方案只能保护数据平面和控制业务的安全性，而不能保护提供VPN业务的设备安全。VPN方案应支持访问控制功能，确保授权用户对网络资源和应用的访问，可以保护VPN业务设备的安全。

为了防止和减轻恶意攻击的影响，安全管理应支持对交换、路由资源进行严格的访问控制。

8.5.2 认证

网管系统应支持标准的方法，对访问管理服务的用户进行有效的认证，验证发送者的真实身份。

随着游牧/移动用户的迅速增长，对VPN的升级能力要求日渐迫切，网管系统对移动用户的鉴权方案必须支持足够多的用户数和VPN接入点。

为确保VPN访问点到VPN访问点（PE到PE）、客户到VPN访问点（CE到PE）之间的安全性，防止中间人攻击，VPN必须支持强有力的鉴权认证机制。

8.6 管理信息技术

管理信息数据库是网管方案的重要组成部分，L3 PPVPN方案必须详细规定所有网络构件的管理信息数据库模块。为了满足VPN通用要求，即使标准MIB库未包含，VPN网管方案应识别所有的MIB信息。

L3 PPVPN策略信息模型应支持对IP策略信息模型（专门为IP网络开发）的重用，包括服务质量策略信息模型和IPSec配置策略模型。

VPN信息模型应适用于不同规模的VPN组网方案，并允许运营商以最小的影响改变网络的规模。对VPN信息模型的其他要求应符合PPVPN信息模型的要求。

网管系统可选支持提供给运营商可视的、可听的管理手段，或以合理的方式将FCAPS信息提供给内部操作者或客户。

9 安全考虑

L3 PPVPN的安全要求包括完整性、机密性、认证机制以及隔离机制等。对客户和运营商的安全要求应符合6.9节和7.9节的要求，对控制及转发平面的隔离应符合6.1节和7.8节的要求，对运营商安全管理的要求应符合8.5节的要求。

9.1 系统安全

VPN客户使用共享的运营商骨干网，因此运营商必须确保网络系统安全。VPN方案还应防止未授权用户获得控制VPN网络元件（如PE/CE设备）的权限。

9.2 接入控制

VPN是客户的私有网络，VPN方案应把对该网络（或部分网络）的访问限制在客户范围之内。

9.3 端点认证

从特定实体收到数据时，VPN方案应支持对发送者身份的鉴权。在基于PE的VPN中，PE从客户站点收到的数据，以及PE经过运营商网络收到的目的地是客户网络的数据都需要进行认证。

VPN方案应支持多种不同的认证方法。方案应支持使用特定客户接口识别用户身份；临时接入（拨号）应用中，需要支持一个认证流程；IPSec远程接入情况下，必须对每个数据包进行认证。

9.4 数据完整性

VPN方案应支持数据传输的完整性，确保接收数据与发送信息完全一致。

在基于PE的VPN中，运营商应通过保证每个网络构件的安全性来确保数据完整性，可选支持IPSec隧道技术。

在基于CE的VPN中，承载封装数据隧道的底层网络不值得信赖，由建立隧道的CE设备负责保障数据的完整性，可选支持IPSec隧道技术。

9.5 保密性

VPN方案应支持用户数据的保密性，即使受到中间人攻击，也保障攻击者无法解读用户的数据。

在基于PE的VPN中，运营商网络（PE设备）参与客户VPN数据的路由和转发，因此运营商应负责用户数据的保密性。通过在PE设备中实现VFI/VSF，以及建立隧道穿越位于PE设备之间的共享网络基础设施，可以保障VPN数据与其他数据实现隔离。当VPN隧道穿越非信任或非受控网络时（如跨运营商VPN），VPN方案还应支持更强的保密方法（如对数据进行加密）。

对基于CE的PPVPN，运营商网络仅提供IP连通性，不负责保密性。数据的保密性将由CE提供，可通过在CE间建立隧道（数据隔离）或使用加密机制（使用IPSec）中实现。

9.6 用户数据与控制数据

VPN方案还应支持对控制数据的保护，包括VPN隧道建立、配置VFI/VSF以及设备的控制数据等。

9.7 跨运营商 VPN

VPN方案可能需要穿越多个运营商，边缘到边缘的数据通路处于多个运营商的控制之下，需谨慎设置相互之间的安全关联。

此外，还应避免不同运营商的VPN配置信息发生冲突。