

# 爱立信提供 MPLS VPN 方案 为服务提供商带来优势和挑战

爱立信(中国)有限公司 数据骨干网及光纤网络部网络顾问 方周

## 1 VPN 概述

与 Internet 不同，专用网络是由单一组织拥有并管理、且互相共享信息的计算机组成的网络。在专用网络中，不同的站点使用专用租赁线路实现互连，保证站点之间的连接一直是专用的。专线网络拥有独立的 IP 地址和路由。对部署了专用网络的企业，可以保证企业是唯一使用该网络的机构。

传统的专用网络是建于 ATM 或帧中继网络之上，用户路由是在用户端实施。这种运营模式的优点是其基于二层技术，因此相对“安全”。但此模式为服务提供商带来较低的网络建设扩展性和网络管理方面的局限性，同时建网的成本较高，也不是一个完全集成的 IP 解决方案。

由于专线网络的昂贵，因此有了 VPN (虚拟专有网络)的概念。VPN 是指网络拥有独立的 IP 地址使用和路由但并不是一个独立的物理网络。市场上所指的 VPN 一般是指由用户端激发的 VPN 解决方案(CPE-based VPN)。

- 点到点隧道协议 ( PPTP ) ；
- 第 2 层隧道协议 ( L2TP ) (RFC2661) ；
- 类属打包协议 ( GRE ) ； 以及
- IP 安全协议 ( IPsec ) - - 由于 IPsec 通过数据加密提供隧道传输和安全，因而变得越来越普及。它也有利于可信性、真实性、完整性和密钥管理。

CPE Based VPN 是由用户端激起并终结，对网络服务提供商是完全透明。因此对网络服务提供商不能提供太多的盈利机会。

CPE Based VPN 的缺点是扩展性较差，因为它是通过数据包封装方式建立隧道，如果同时加密隧道，速度会更慢。CPE Base VPN 也要求企业拥有维护设备的技术能力。往往这类的维护工作对小型企业相当昂贵。

市场的趋势是企业逐步外包 IT 服务以降低公司运营成本，IDC 能迅速的发展也证明了这方面的趋势。企业也有外包 VPN 服务的趋势，这正好给提供商提供了巨大的商机。

由网络服务提供商激发的 VPN 解决方案称为 Provider Provision VPN 或 PP-VPN。一般业界所指的是 MPLS VPN。MPLS VPN 也分为二层 MPLS VPN 和三层 MPLS VPN。三层 MPLS VPN 是指基于 IETF RFC2547bis 标准。而二层 MPLS VPN 是指 IETF Draft Kompella 或 IETF Draft Martini。在下节会详细介绍其区别。

现在无论是国内外的网络服务提供商都希望能降低建网的成本，同时 IP 技术近年来对 QoS 和流量工程的支持都有相当的改进，因此提供商大多已停止对 ATM 和帧中继网络建设的投资，而转向对 IP 网络的建设。因此 IP/MPLS 的技术也变的越重要。

对网络服务提供商而言是需要一个能支持多业务和为提供商创造更多盈利机会的网络平台，同时也需要支持客户对 VPN 的各种要求。

## 2 MPLS 技术为服务供应商带来的优势

IP 网络服务提供商面临最大的挑战是如何充分利用网络带宽为业务争取最大的回报。通过策略路由等手段未能有效地控制网络流量带宽。IETF 新出版的 MPLS 协议解决了这种挑战，它允许面向分组实现流量工程和多业务功能，同时提供更高的扩充能力。

IETF 努力地对一些最初在 90 年代中期被建议的专用多层交换方案标准化，进而形成 MPLS 标准。

事实上所有的多层交换方案和 MPLS 的转发部分都是基于标记交换转发算法。这个算法与在 ATM 和帧中继交换机中使用的转发数据的算法相同。信令和标记分配是标记交换转发算法运行的基础。

MPLS 为网络提供商带来了以下主要的优势：

- MPLS 流量工程；
- 基于 MPLS 快速迂回路由的网络安全保护；
- MPLS VPN；

## MPLS 流量工程

MPLS 流量工程允许您配置一条路径，不再使用内部网关协议(IGP)计算的最短路径传送流量，而是把流量传送到网络中拥塞程度较低的路径上。流量工程把网络的总流量负载均衡到网络中的各个电路、路由器和交换机上，这样不会致使某个部件利用率偏低或偏高。结果，网络可以更加高效地运行，并提供更加可以预测的服务。此外，这种解决方案可以适应网络的迅速激增及 CoS 要求。

流量工程参与将业务流映射到网络物理拓扑上的任务，它提供了将业务流重通过内部网关协议 ( IGP ) 计算出的最短路径转移到一条具有更少阻塞的路径上去的能力 ( 图 1 )。流量工程的目的

图 1：流量工程

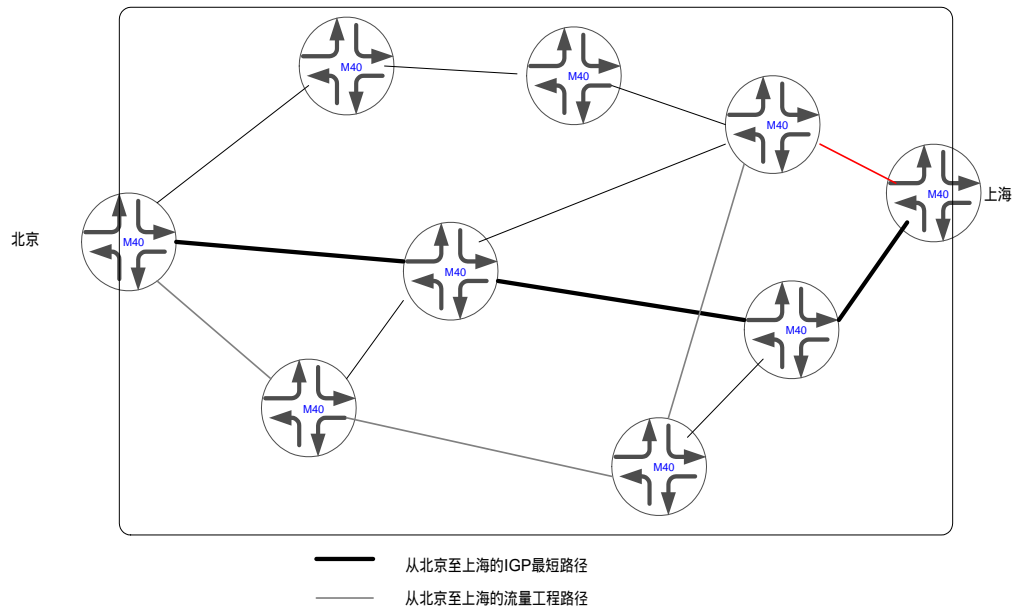


Figure 1 MPLS Traffic Engineering

在于在网络中的不同链路，路由器及交换机之间均衡业务流，使这些网络组成部分不会被过分使用或未被充分使用。流量工程使网络服务提供商能够充分使用他们的网络基础结构。

## MPLS 快速迂回路由

在沿着预定的 MPLS 路径（称为标记交换路径 LSP）上的任何电路或路由器发生故障时，MPLS 快速迂回路由可以提供快速恢复能力。沿着 LSP 的每台路由器会计算一条备用迂回路径，避免其下行站。如果一条电路发生故障，最近的上行路由器会自动激活迂回路径，见图(二)。

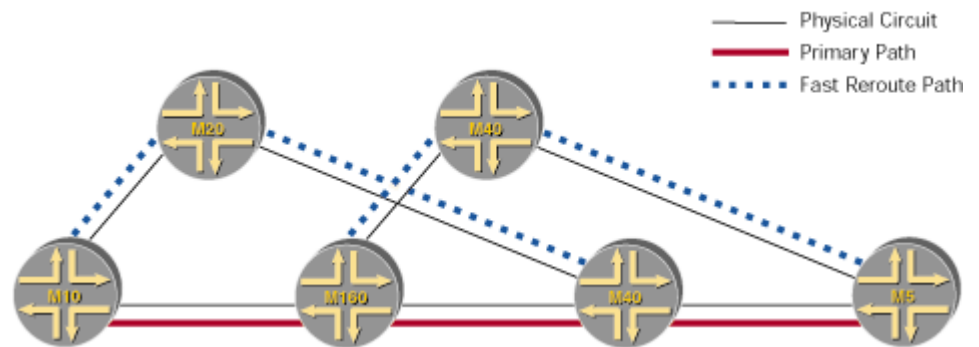


Figure 2 MPLS Fast Reroute

### MPLS VPN

通过 MPLS，网络提供商可以在一个多元融合的 IP 网络中运行二层 VPN、三层 VPN、流量工程、Diffserv 及许多其它服务。

下节介绍二层 MPLS VPN 和三层 MPLS VPN 的运营模型和实现方式。

## 3 MPLS VPN 的运营模式和实现方式

### 三层 MPLS VPN

RFC 2547bis 定义了一种机制，允许服务提供商使用自己的 IP 骨干，为客户提供 VPN 服务。RFC 2547bis VPN 也称为 BGP/MPLS VPN，因为它使用 BGP 把 VPN 路由信息分布到供应商的骨干中，并使用 MPLS 把 VPN 流量从一个站点转发到另一个站点上。

### 网络组成部分

在 RFC 2547bis 中，VPN 是一种策略集合，这些策略控制着一套站点中的连接能力。客户站点通过一个或多个端口连接到服务供应商网络上，其中服务供应商把每个端口与 VPN 路由表关联起来。在 RFC 2547bis 中，VPN 路由表称为 VPN 路由和转发(VRF)表。图 3 说明了 BGP/MPLS VPN 的基本构件。

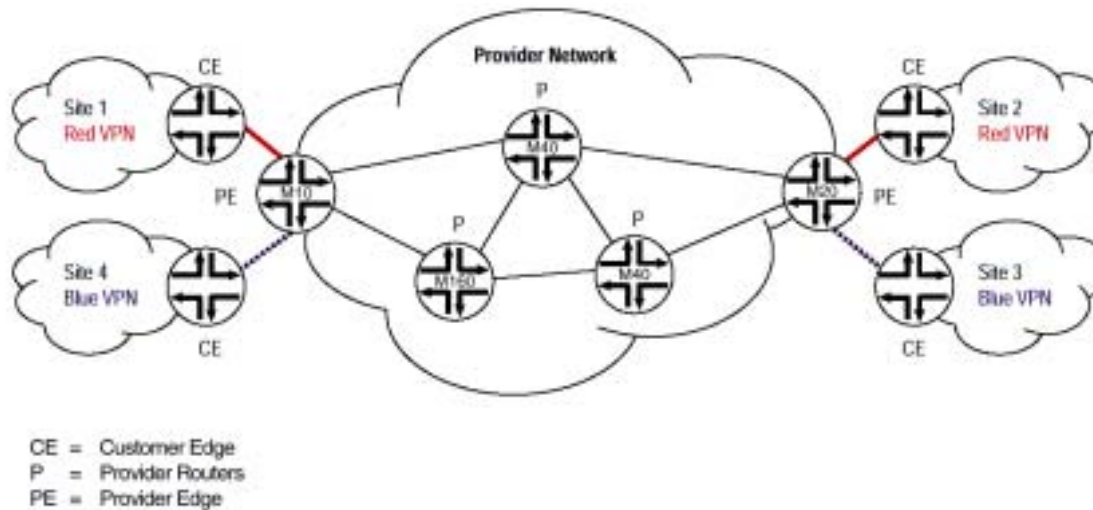


Figure 3 RFC 2547bis 网络组成部分

### 客户边缘设备

客户边缘 (CE) 设备允许客户通过连接一台或多台供应商边缘 (PE) 路由器的一条数据链路接入服务供应商网络。CE 设备可以是一台主机或一台第二层交换机，但典型的 CE 设备是一台 IP 路由器，它与其直接连接的 PE 路由器建立邻接关系。在建立邻接后，CE 路由器把站点的本地 VPN 路由广播到 PE 路由器，并从 PE 路由器上学习远程 VPN 路由。

### 供应商边缘路由器(PE)

PE 路由器使用静态路由、RIPv2、OSPF 或 EBGP 与 CE 路由器交换路由信息。尽管 PE 路由器维护着 VPN 路由信息，但它只需为其直接相连的那些 VPN 维护 VPN 路由。这种设计增强了 RFC 2547bis 模型的扩充能力，因为 PE 路由器不需维护服务供应商的所有 VPN 路由。

每台 PE 路由器为其直接相连的每个站点维护一个 VRF。每个客户连接(如帧中继 PVC、ATM PVC 和 VLAN) 映射到某个 VRF 上。因此，PE 路由器上的一个端口 ( 而不是一个站点 ) 与 VRF 相关。注意，PE 路由器上的多个端口可以与一个 VRF 相关。PE 路由器能够维护多个转发表，支持按 VPN 分隔路由信息。

在从 CE 路由器上学习本地 VPN 路由后，PE 路由器使用 IBGP 与其它路由器交换 VPN 路由信息。PE 路由器可以保持到路由反射器的 IBGP 会话，作为全网状 IBGP 会话的替代方案。部署多个路由反射器增强了 RFC 2547bis 模型的充能力，因为它不需任何单个网元维护所有 VPN 路由。

最后，使用 MPLS 在供应商骨干中转发 VPN 数据流量时，入口 PE 路由器作为入口 LSR 使用，出口 PE 路由器作为出口 LSR 使用。

### **供应商路由器(P)**

供应商路由器是没有连接 CE 设备的供应商网络中的任何路由器。在 PE 路由器之间转发 VPN 数据流量时，供应商路由器作为 MPLS 转接 LSR 使用。由于是在采用两层标记堆栈的 MPLS 骨干中转发流量，因此供应商路由器只需维护到供应商 PE 路由器的路由，而不需维护每个客户站点专用的 VPN 路由信息。

### **基于 MPLS 的第二层 VPN**

基于 MPLS 的第二层 VPN 是服务供应商为客户提供第二层服务的一种网络。在客户端，客户使用帧中继等电路连接各个站点，每个客户边缘 ( CE ) 设备配置一个 DLCI，并通过这个 DLCI 与其它 CE 通话。但在服务供应商网络内部，第二层分组是在 MPLS 标记交换路径 ( LSP ) 内部传送的。服务供应商不必参与客户的第三层网络 ( 特别是在路由方面 )，从而为服务供应商和 PE 路由器提供了多种优势。

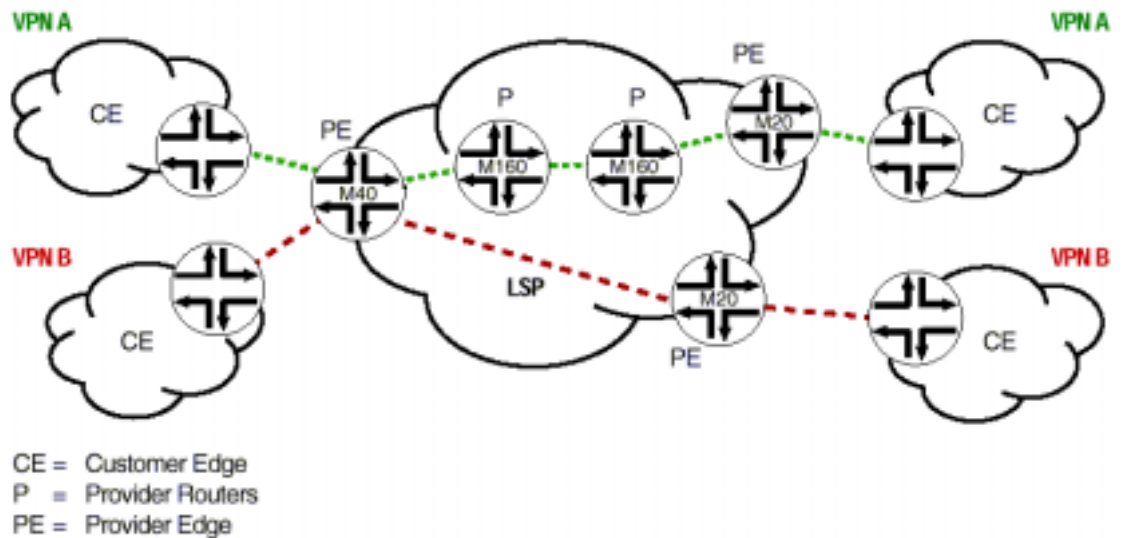


Figure 4 基于 MPLS 的第二层 VPN

CE=客户边缘路由器

P=供应商路由器

PE=供应商边缘路由器

#### 管理职责的划分

在第二层 VPN 中，服务供应商负责第二层连接；客户负责第三层连接，其中包括路由。如果客户认为站点 A 中的主机 x 不能到达站点 B 中的主机 y，服务供应商只需说明站点 A 是连接到站点 B 上的。至于主机 y 的路由怎样到达主机 x 的具体细节，则由客户负责。

与三层 MPLS VPN 不同，IETF 并没有对二层 MPLS VPN 进行最终的标准化的，但业界普遍承认 IETF Draft Martini (draft-martini-l2circuit-trans-mpls-06)和 IETF Draft Kompella (draft-kompella-ppvnp-l2vpn-00.txt)并提供相应的产品支持。两个草案都以作者姓名命名。

两种 IETF 草案不同的地方主要是 IETF Draft Martini 建立 VPN 时是采取了 LDP 信令方式而 IETF Draft Kompella 采用了 LDP 信令和扩展性 BGP 方式建立 VPN。IETF Draft Kompella 基本解决了如何部署大规模 L2 VPN 的问题。它描述了如何通过扩展性 BGP 进行 VPN 的部署工作，某些内容与 RFC2547 相似。但 RFC2547 描述如何利用扩展性 BGP 传递 VPN 之间的路由信息，而 KOMPELLA 描述了如何利用扩展性 BGP 部署 VPN。

因为二层 MPLS VPN 和三层 MPLS VPN 各有优点缺点，因此所针对的应用也不同。

### **MPLS/L2 VPN**

#### 优点

- 一个统一的多业务平台
- 减小运营商管理复杂度
- VPN 路由由 CPE 设备完成
- 安全隐患少
- 多协议支持
- 支持 VPN 之间的 Multicast 服务

#### 限制

- 一般情况下用户端需配置路由设备

总结以上各优缺点，MPLS/L2 VPN 更适合于以下两种客户：

- 网络安全性要求较高和有足够能力自己维护 VPN 内网络路由的专有用户如金融和公安等。
- 现有专线用户(E1、ATM 或帧中继等)。这类用户以有足够能力维护自己网络和已有现成的设备。同时也容易接受 MPLS/L2 VPN 概念，因此运营商很容易把这类用户升级为使用 MPLS/L2 VPN 以降低成本和增强竞争性。

### **MPLS/L3**

#### 优点

- 将用户的工作量减到最小
- 将用户的设备减到最简单
- 为运营商带来较多的商机

#### 限制

- 运营商需增加人力资源为客户维护虚拟主干

综合以上各优缺点，MPLS/L3 VPN 更适合于以下用户：

- 一般中小型企业，无能力管理自己 VPN 内的网络。VPN 内的网络规模为中小型。

## 5 安全程度

对基于 IP 网络安全造成威胁的主要原因有两点：一是用户网络拓扑被学习，骇客会利用学习到的网络拓扑对企业网络进行攻击；二是用户网络数据被窃听。

MPLS VPN 利用二层标签技术代替帧中继或 ATM VPN 业务并提供同样适当的安全性。MPLS 的标记切换性质使第三方不能将数据包送入 MPLS 隧道中。因为数据包的整个标记交换路径是在入口点预先确定的，客户可以确信送入 MPLS 隧道的通信不会偏离该隧道。数据包自身不会偏离提供商的骨干网。因此防止了用户数据被窃听。

对 MPLS L2 VPN 而言，网络服务提供商不会管理用户拓扑结构，因此拥有与传统专用网同等的安全程度。对 MPLS L3 VPN，用户只能对网络服务提供商赋予信任。假设网络服务提供商采取了适当的安全过程，泄密范围仅限于服务提供商的工作人员。服务提供商所用的 PE 路由器必须是高端核心网路由器，因为这类路由器能提供可靠的路由器管理性和网络安全性。

MPLS L3 VPN 的跨域问题增加了 VPN 网络安全的困难，因为 VPN 会经过其他网络提供商。PE 路由器上的 VPN 路由因此可能广播至其他网络提供商的 ASBR(自治系统边缘路由器)上，因此网络提供商之间必须有足够的协调，通过 ASBR 路由器上进行策略避免 VPN 路由泄漏。或使用 RFC2547bis 对跨域 MPLS VPN 的建议，采取 Multi-hop BGP 的手段交换点到点 PE 路由器上的 VPN 路由。在利用 Multi-hop BGP 手段的情况下，其他网络服务提供商的 ASBR 路由器只负责转发骨干网路由器之间的路由，并不负责转发 VPN 路由。

## 6 MPLS VPN 技术面临的挑战

### **厂家之间的兼容性问题**

大多数的路由器厂家和交换机厂家都认为 MPLS VPN 是未来 VPN 发展趋势 同时也相应支持。对三层 MPLS VPN 来说，各厂家都会支持 RFC2547bis 标准，但对标准支持的程度因开发力量而有异，因此造成设备兼容性问题。

对二层 MPLS VPN 来说，市场上多数厂家支持 IETF Draft Martini，相信是因为 Draft Martini 相对 Draft Kompella 简单。但 Draft Kompella 通过扩展性 BGP 交换对端信息和支持 Over Provision 功能对大规模部署 VPN 有利。相信这是未来二层 MPLS VPN 的发展方向。

由于各厂家面对的市场不同因此对二层封装的支持种类也不尽相同。例如交换机厂家一般不支持帧中继和 ATM 的封装。

### **MPLS VPN 网管**

对 MPLS VPN 业务进行性能管理可通过 SNMP 协议采集路由器 MIB 库，因此不存在网管问题。路由器厂家可提供专有 MIB 库对采集 LSP 上的流量有较多的支持。各种性能管理应用软件对采集来的数据可能有不同的表现方式，有些能根据服务提供与 VPN 客户所定的 SLA 进行报表。服务提供商可根据自己需求选择适合的网管软件。

对 MPLS VPN 告警管理可通过 SNMP Trap 或 Syslog，市场上有不少告警管理软件可供选择。

由于各设备厂家没有统一的设备配置标准，因此市场上很少支持多厂家的 VPN 部署应用软件。而且 VPN 部署应用软件对 VPN 的支持一般落后网络设备对 VPN 的支持一至两个季度。同时 VPN 的部署工具涉及到网络服务提供商的业务层面，因此很难选择到完全适用的软件。某些路由器能提供网络设备配置的 API 接口如 XML，因此网络服务提供商能很容易地开发适合自己的 VPN 部署软件。

### **网络提供商经营模式**

由于 MPLS VPN 与传统 VPN (ATM/帧中继)不同, 这为网络提供商带来经营模式改变的挑战。与客户签的 SLA 再不能向过去般如 ATM 提供 Burst Rate、Commit Rate、等。基于 MPLS VPN 的 SLA 会更复杂因为不能以简单的包月方式对用户进行收费, 服务商要提高自己的竞争力, SLA 必须包括时延、丢包率、QoS 等内容。在 IP 网络上对客户保证网络带宽是服务提供所面临的巨大挑战。

MPLS VPN 为提供商带来的不只是向客户提供简单的专线服务, 而是为用户提供 VPN 路由交换的服务, 同时也可按客户需求提供其他如 Internet Access 服务和外包防火墙等增值服务。

仅在单一运营商内提供 VPN 服务, 对用户而言其吸引力较小, 跨运营商, 跨省或跨国的 VPN 服务才能体现 VPN 的意义。目前多数运营商的骨干网络未必支持 MPLS, 对网络的升级和改造所需要的时间和带来的风险也是影响其他老式运营商支持 MPLS 的阻力, 这无疑为经营 MPLS VPN 带来巨大的挑战。

## 7 MPLS VPN 的市场发展

现时实现 MPLS(L2/L3) VPN 的运营商不多。北美有运营商正使用基于厂家非公开性的 L2 MPLS VPN 技术解决如何通过 IP 骨干网连接边缘的 Legacy ATM 网络 (i.e. Uunet、MCI、...)。暂时没有运营商使用公开性的 Draft Kompella 或 Draft Martini。北美使用 RFC2547 的运营商有 Global One、AT&T 等。RFC2547 在欧洲似乎比在北美流行, 运行 RFC2547 的运营商有 Deutsche Telekom, BT Belgium, DiAx in Switzerland 等, BT UK 正在试验。这些运营商都以小范围提供 VPN 服务。因此市场上缺乏经营 MPLS VPN 业务的经营。

在国内, 中国电信和网通积极地对 MPLS VPN 进行测试和小规模使用。广东移动将要建立的 MPLS VPN 网络将成为中国移动首个商用的 MPLS VPN 网络。

## 8 MPLS VPN 技术的未来发展

对于三层 MPLS VPN 来说，市场会继续向 IETF RFC 2547 标准发展和对此标准进行完善化。例如市场上已有厂家对 RFC 2547 支持组播功能。为提高三层 MPLS VPN 的安全性，市场上已有 PE 路由器支持 IPSec 功能，这使网络服务提供商能向客户提供 IPSec 外包服务(加密 LSP 上的数据流)。

对于二层 MPLS VPN 而言，相信市场会朝向支持 IETF Draft Kompella，因为 IETF Draft Kompella 除了能支持所有 IETF Draft Martini 的功能外，它的 "Over Provisioning"功能解决部署大规模的 MPLS L2 VPN 网络。相信 IETF Draft Martini 只是许多厂家的过渡方案。MARTINI 不适宜用于部署大规模的 L2 VPN 应用。

市场上又刚提出了 VPSN (Virtual Private Switch Network)的新概念。VPSN 概念的提出是想在 MPLS 网络上建立如传统 TLS (Transprant Lan Service) 基于 Ethernet 技术的网络。现时的 MPLS L2 VPN 虽然也支持 Ethernet 封装但只是点到点隧道连接关系，低效率也不太灵活。因此 Draft-vkompella-ppvnp-vpsn-mpls-00 提出了 VPSN 的概念。VPSN 描述了如何在已建好的 MPLS/L2 VPN 全网状网络上互相学习 MAC 地址以达到 TLS 的效果。原理是在各个 PE 路由器上通过 LDP 信令互相学习生成一个"VC Label" 和 Mac 地址的对照表。当网络包从节点到另一节点，先会寻查此对照表，此对照表会根据网络包的目的 MAC 地址打上适当的"VC Label"。

VPSN 的概念仍处于初期，仍然存在不完善的地方，例如如何处理大量 MAC 地址学习时对骨干网造成的负载、如何处理 MAC 地址对照表更新问题(当一台 CE 与 PE 断开时，对方的 PE 必须更新 MAC 对照表)和如何处理当 PE 路由器上的 MAC 对照表与 CE 路由器上的 MAC 地址表(通过 ARP 学习到的) 发生不同步现象等等。

VPSN 的技术仍然有待发展，暂时也没有厂家支持。VPSN 的概念不支持虚拟电路的接入方式。虚拟电路接入是指 CE 与 PE 是以传统电路的连接方式如 ATM、帧中继和专线等。把这类利用传统接入方式的用户升级至 MPLS/L2 VPN 用户会为网络提供商带来很大的商机。

早在 2001 年初爱立信为中国移动集团公司建立了一个全国 IP 骨干网，范围包括全国 31 个省并提供了多台 AXI580 (基于 Juniper M160) 和 AXI520-4 (基于 Juniper M20) 骨干网路由器连接各省。其后又为中国移动公司建立多个省骨干网包括广东移动公司的省数据网并提供了 AXI580 (基于 Juniper M160)和 AXI520-4(基于 Juniper M20)骨干网路由器连接广东省共 22 个城市。

在今年爱立信再向广东移动公司提供多台 AXI520 系列骨干路由器分别放置在广东省的广州、深圳、珠海、东莞等 9 个城市作为网络服务提供商的边缘路由器 (PE)。这些 PE 路由器会与当地节点的省骨干网路由器(P)相连成为一个 MPLS 网络。在同一个 MPLS 网络上会同时提供基于 IETF RFC2547bis 的三层 MPLS VPN 业务和基于 IETF Draft Kompella 的二层 MPLS VPN 业务，同时也利用 IETF RFC2547bis 建议的 Multi-hop BGP 解决跨域的问题 (中国移动全国网拥有一个公开的自治系统号，而每个移动省网都拥有一个私有的自治系统号)。这为将来中国移动实现全国 MPLS VPN 业务做好准备。