

基于MPLS的第二层虚拟专用网

Juniper 网络公司，爱立信公司，2001 年 3 月

内容提要

尽管基于帧中继或ATM电路的虚拟专用网 (VPN)运转良好，但为Internet流量和VPN维护不同网络的成本及开通VPN的管理负担导致了许多不同的备选解决方案。本文介绍了多种解决方案中的一种方案，即从客户的角度，在基于MPLS的第二层电路上建设VPN。本文进一步解释了Juniper Networks公司是怎样提供解决方案，来满足第二层VPN要求的。

在基于MPLS的第二层解决方案中，服务供应商可以为IP、第三层(MPLS/IP)和第二层VPN维护和管理一个基于MPLS的网络。通过MPLS，您可以在多元融合网络中运行第二层VPN、第三层VPN、流量工程、Diffserv及许多其它服务。

角度

第一种公司网络基于专用的租赁线路，这些租赁线路把公司的各个办公室连接起来。除连接能力外，这种网络几乎没有提供其它功能。这种网络成本高昂，开通速度缓慢耗时。

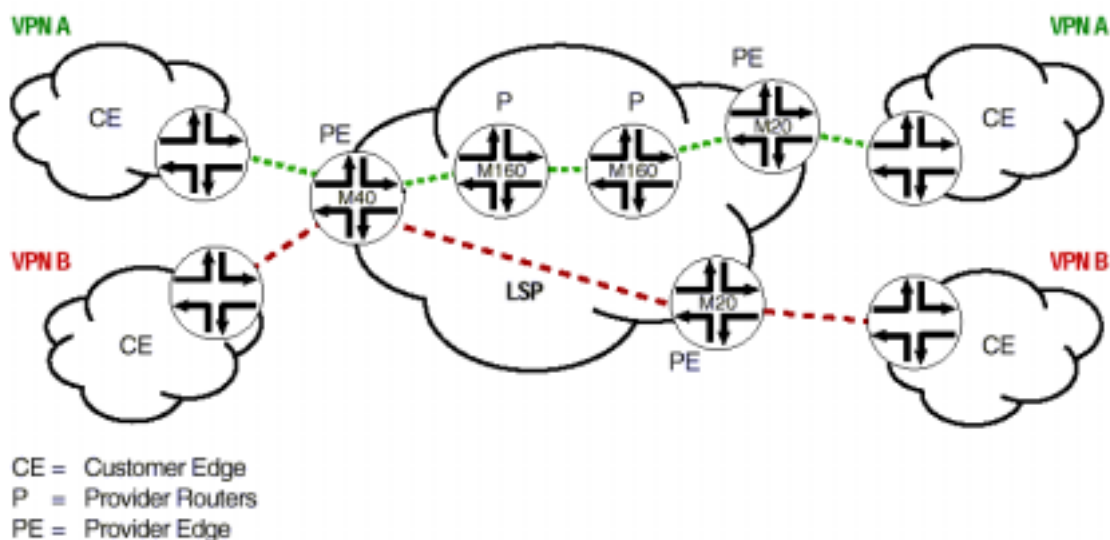
第一种VPN基于第二层电路：在一定程度上基于X.25协议，另外还可以基于帧中继及ATM。这些第二层VPN开通起来比专线简单，虚电路允许所有VPN共享公共设施。它节约了成本，而服务供应商则把节约的成本部分让渡给客户，从而使得客户能够从中受益。但是，尽管第二层VPN较专线是一个重大进步，但它们仍存在着缺点。

- 它们的速度不够快。由于不支持OC-192c/STM-64，因此它们不能跟上Internet日益提高的速度要求。
- 它们把VPN设施局限在一种介质上，如ATM上。如果Internet设施共享相同的物理链路，那么这种负担会随之提高。
- Internet设施和VPN设施即使共享相同的物理网络，但仍需要分别进行管理和维护。
- 尽管相对于专线来说，这种VPN的开通要简便得多，但其仍然十分复杂，特别是在现有的VPN中增加站点时，这一点表现得尤为明显。

基于MPLS的第二层VPN解决方案保留了第二层VPN的优势，同时允许为IP、第三层(MPLS/IP)和第二层VPN维护和管理单一的基于MPLS的网络。它还降低了开通复杂度。特别是在现有的VPN中增加站点时，在大多数情况下只需把供应商边缘(PE)路由器连接到新站点上即可。

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。



图一：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。

一旦PE为连接的CE提供了第二层连接，那么它的工作就完成了。在最坏情况下，行为有误的CE会拍打其接口。另一方面，第三层VPN中行为有误的CE可能会拍打其路由器，从而导致PE路由器、甚至整个服务供应商网络不稳定。因此，服务供应商必须积极控制CE上的路由拍打。这种事件在外部BGP对等中非常常见，但在VPN中，问题的规模要大得多。此外，CE-PE路由协议不能是BGP，因此没有BGP的拍打抑制控制功能。

从传统第二层VPN转型

由于从客户角度来看，并不能区分传统第二层VPN(例如连接多个站点的实际帧中继电路)与基于MPLS的VPN，因此从一种VPN过渡到另一种VPN导致的问题非常小。通过第三层VPN，服务供应商直接涉及专用网络的路由，这具有多种意义(如可以使用特定解决方案，

比较骨干路由器与第三层VPN路由器)。

路由的保密性

在第二层VPN中，由于服务供应商不参与路由，因此可以自然而然地实现客户路由的保密性。您的路由不需采取任何专门措施，就可以把客户路由与其它客户的路由或与Internet分开。它不需要使用逐个VPN的路由表，也不会给PE路由器带来额外的复杂性。

独立于第三层

由于服务供应商只提供第二层连接能力，因此客户可以运行其选择的任何第三层协议。如果服务供应商参与客户路由，那么很重要的一点是，服务供应商和客户都必须采用相同的第三层协议和路由协议。

扩充问题

在第二层VPN方案中，每个PE把与PE连接的每个CE有关的少量单一信息传送到每个其它的PE上。也就是说，在每个VPN中，每个PE只需维护每个CE发出的一片信息，并在每个VPN中与每个站点保持一条路由。转发信息库和路由信息库都可以与站点数量和VPN数量一起很好地扩充。此外，服务供应商网络的扩充特点与客户无关；唯一密切相关的数量是VPN站点的总数。（如欲了解客户的扩充问题，请参阅路由备选方案部分）

第三层比较

在第三层VPN中，对连接了一个CE、并具有相关路由协议（BGP、OSPF、RIP）例程的每个VPN，PE为其维护和保持一个VPN路由和转发（VRF）表的状态。它还需要生成BGP标记捆绑，并与其MP-BGP对等交换信息。对路由器来说，保持潜在数量非常大的VRF的状态，对处理器和内存会提出非常密集的要求，进而可能导致路由性能问题。

此外，在第三层VPN中，每个CE可能有服务供应商需要承载的任意数量的路由。其中一个问题是，每个PE中存储的信息和PE在VPN中为CE安装的路由数量可能(在原则上)非常大；因此，在实践过程中，PE必须在安装与其目前所属VPN有关的路由数量方面对自己作出限制。另一个问题是，CE可能在没有发出警告的情况下，开始向PE发送大量的、并且越来越多的路由，因此PE必须防止这种情况的发生。这样，服务供应商必须对从CE上接收的前缀数量实施一个限额，因此要求PE路由器提供这种控制功能。

第三层VPN的扩充问题主要集中在BGP路由反射器上。如果服务供应商拥有大量的VPN客户或大型的VPN客户，那么代表客户网络维护的路由总数可能非常大，以至一台路由反射器不能维护所有通知的VPN路由。必需使用下述解决方案，来解决这个问题：

- 路由反射器可以分区，这样每个路由反射器都为一个VPN子集服务，任何一个路由反射器都不必承载所有路由。这种方法的缺点是，改变VPN隶属关系的PE可能会强制改变路由反向器配置，这将要求认真构建路由反射器拓扑结构。
- 路由反射器可以使用预先配置的路由目标列表，实现入局路由过滤。路由反向器可能还

需要安装出局路由过滤器，其中在每个对等上了包含上述路由目标列表，这样，它们不会发送不必要的VPN路由。这种方法还要求重大扩展，另外需要多个路由反向器，以服务不同的VPN集合。

配置简便

配置传统的第二层VPN是一项负担，主要因为该任务的 n^2 的特点。如果在一个帧中继VPN中有 n 个全网状CE，那么必须在服务供应商网络中开通 $n*(n-1)/2$ 个DLCI PVC。在每个CE上，必须配置 $(n-1)$ 个DLCI，以到达每个其它的CE。此外，在增加新的CE时，必须开通 n 个新的DLCI PVC，并使用新的DLCI更新每个现有的CE，以到达新的CE。

在基于MPLS的第二层解决方案中，LDP和RSVP-TE信令协议处理网络中PVC的开通工作，减少了很大一部分的开通负担。此外，与网络中的标记一样，CE边缘的DLCI成本相对低廉。因此，服务供应商可以超额开通VPN。例如，在只需要20个CE时，服务供应商可以为一个VPN分配50个CE。通过超额开通VPN，在VPN中增加新的CE只需配置新的CE及相关的PE；而不需要重新配置现有的CE及其PE。

第二层相关性

在第二层VPN中，一个主要限制是一个VPN借以连接多个站点的第二层介质必须统一。其必然的结果是，第二层技术提供的第二层电路数量决定了第二层VPN中的站点数量。例如，如果第二层技术是带有2字节DLCI的帧中继，那么一个CE最多可以连接一个VPN中大约1000个其它的CE。

路由备选方案

在第二层VPN中，路由负担(维护路由邻居、传播和更新路由及转发分组)完全落在CE路由器上。例如，在带有 n 个轮辐的“轮轴和轴辐”拓扑结构中，轮轴必须维护 n 个路由对等。如果 n 太大， n 倍路由对等对CE路由器来说可能是一个问题。此外，客户必须解决所有路由问题。

尽管这种管理分离的前景非常乐观，但许多客户希望外包其路由。第三层VPN为您提供了一个机会，可以作为一种增值服务提供外包路由。在第三层VPN中，CE只有一个路由邻居，即PE路由器，这最大限度地降低了路由负担。此外，CE把所有分组发送到PE路由器上，简化了转发决策。另外，它还简化了客户的管理负担，因为服务供应商基本上承担了所有这些职责。

基于信令 MPLS 的第二层 VPN

支持第二层VPN的供应商路由器可以采用LDP或RSVP进行信令处理。后者提供了额外的流量工程优势，其代价则是在网络中拥有更多的状态。另外还可以实现混合解决方案：在边缘采用LDP，在核心采用RSVP。这种备选方案提供了一个良好的折衷方案，也是许多人正在考虑的一个方案。

第二层VPN可以以两种方案进行信令处理：LDP或BGP4。尽管业内在首选哪种协议上还没有达成一致，但BGP4提供了许多优点。第一个优点是边缘路由器几乎无一例外地运行BGP4；第二个优点是BGP4是为承载大量的各类路由而设计的；最后，BGP4处于较好的位置，可以处理域间路由，而多个供应商的VPN和运营商的运营商VPN都需要这种域间路由。

Juniper Networks基于MPLS的第二层VPN

Juniper Networks实现的基于MPLS的第二层VPN称为MPLS电路交连。这种第二层封装方法允许您在一个构建的MPLS核心上透明地传输任何流量类型，而不必参与核心的IP路由方案。这种技术构成了Juniper Networks员工(Kireeti Kompella, Manoj Leelanivas, and Quaizar Vohra)及多家服务供应商编写的名为“基于MPLS的第二层VPN”的IETF建议书基础。(请参阅<http://www.ietf.org/internet-drafts/draft-kompella-mpls-l2vpn-02.txt>。)

这种特性允许透明地连接不同网络边缘的两条第二层电路。由于没有实现任何第三层解析或查表，因此电路交连支持在分组有效载荷中传输任何第三层协议。电路交连包括把进入逻辑端口、虚电路或DLCI静态映射到输出逻辑端口、虚电路或DLCI上。

考虑到每个客户网络上的路由协议对服务供应商网络中的路由都是不可视的，因此各种客户网络本身不能共享流量，但能够支持VPN之间重叠的IP地址。电路交连消除了客户网络之间或客户网络与骨干网络之间潜在路由耦合的不稳定性，而这种不稳定性在多个路由表实现方案中十分常见。

其支持的封装包括：

- ATM
- 以太网802.1Q VLAN
- 帧中继
- HDLC
- PPP

这种机制允许通过一个MPLS骨干网络云在CP路由器之间创建隧道，如图2和图3所示。

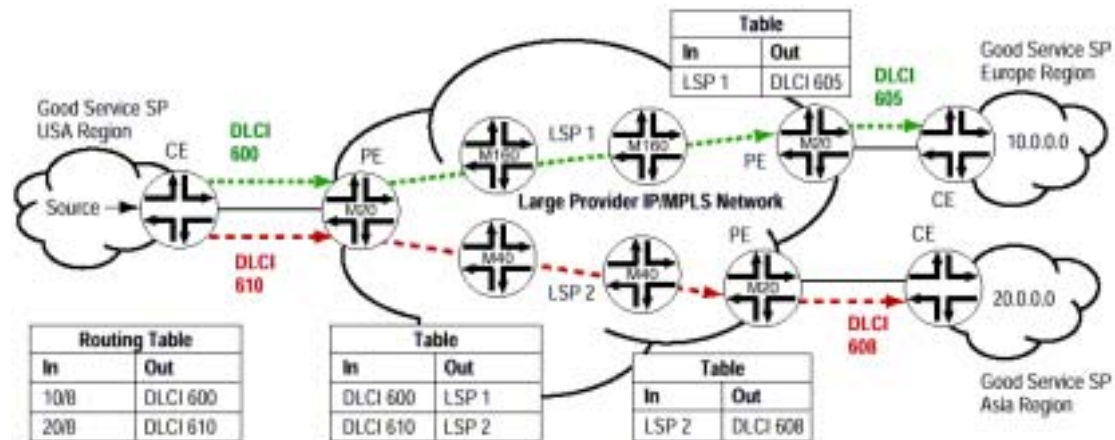


图2：采用电路交连的帧中继网络实例

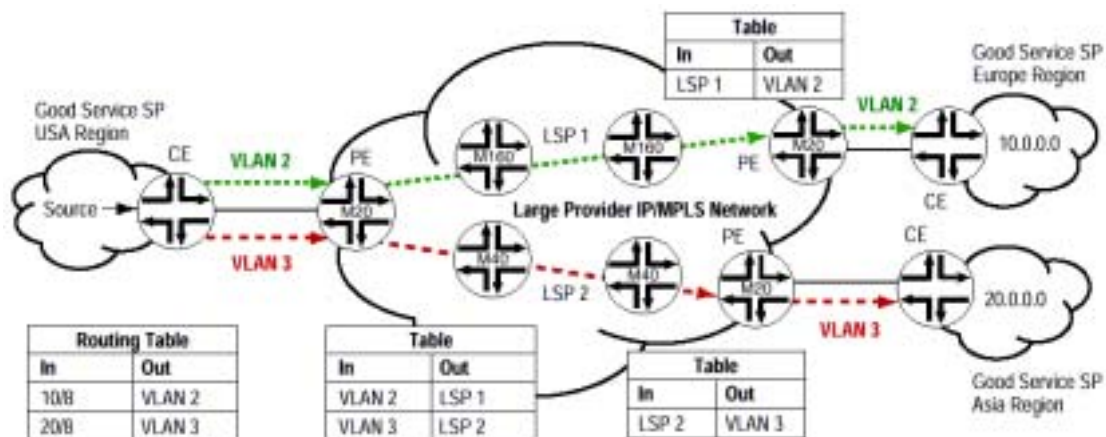


图3：采用电路交连的以太网802.1Q VLAN实例

对ATM AAL/5 VPN，传输AAL/5 PDU，而不需表明VPI/VCI。在接收PE上，AAL/5 PDU被分片，然后在每个信元中增加一个VPI/VCI，然后把信元发送到CE上。

对帧中继VPN (带有两个八位字节DLCI)，先剥去两个DLCI八位字节，然后传输其余的第二层帧。在接收PE上，新的DLCI增回到帧上，然后发送到CE。

对PPP、Cisco HDLC和以太网VLAN VPN，传输整个第二层帧，而没有任何修改。第二层帧不包括HDLC标记、以太网pre-amble或CRC。其假设还没有完成比特/字节填充。在接收PE上，帧被发送到CE上。

增值服务

服务供应商可以使用基于MPLS的第二层VPN，在一个核心基础设施上构建和销售增值服务，如运营商的运营商服务、第二层VPN、第二层企业外部网访问、高速局域网到局域网服务及Internet交换局服务。

运营商的运营商服务

服务供应商可以为其它运营商提供透明的带宽服务，允许后者部署核心骨干，而不必构建自己的传输网络 (图4)。服务供应商可以在地区、全国或全球部署这些服务，可以把这些服务简称为虚拟核心服务。运营商可以继续管理自己的网络设备，把其作为连接到PE节点上的一个CE站点，简单地连接到服务供应商网络上。CE和PE之间采用的第二层协议可以是帧中继、ATM、PPP、HDLC或以太网，但前提条件是所有点到点连接都实现相同的访问协议。服务供应商只需为运营商维护任何点到点互连之间的MPLS LSP。服务供应商可以应用流量工程，从而可以提供SLA (服务水平协议)。与采用租赁线路或光纤相比，这种服务对运营商来说要经济得多。当服务供应商在一对PVC或VLAN之间建立映射时，一个CE可以连接到多个远程CE上。此外，服务供应商可以以任何速度提供带宽，因为本地连接的速率可以从 E1 到 OC-48c/STM-16 以及OC-192c/STM-64。

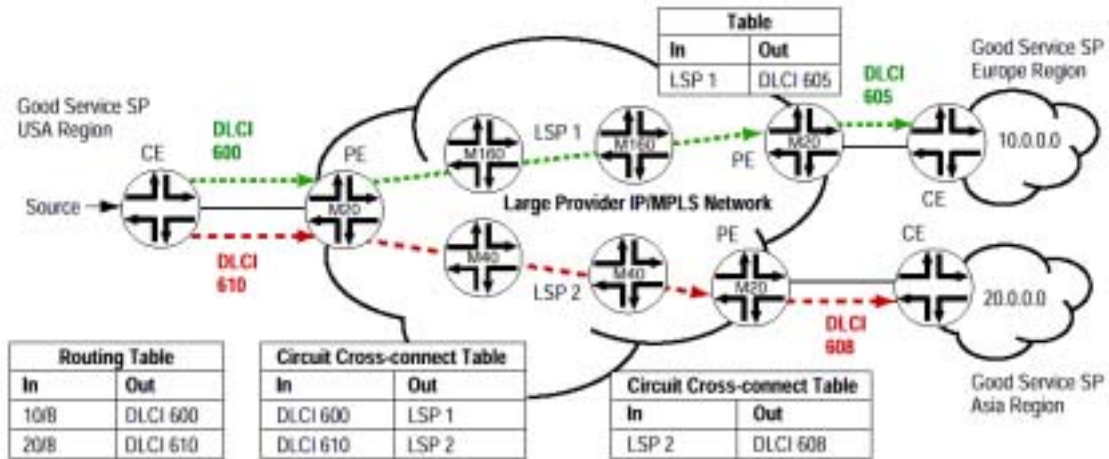


图4：运营商的运营商

通过采用Juniper Networks的LSP缝合功能（图5），服务供应商还可以在MPLS基础上提供服务。在LSP缝合功能中，服务供应商把运营商的入口LSP映射到自己骨干上的核心LSP，然后映射到远端的运营商出口LSP。通过使用这种方法，运营商可以实现一个端到端MPLS解决方案，而不必维护整个网络。

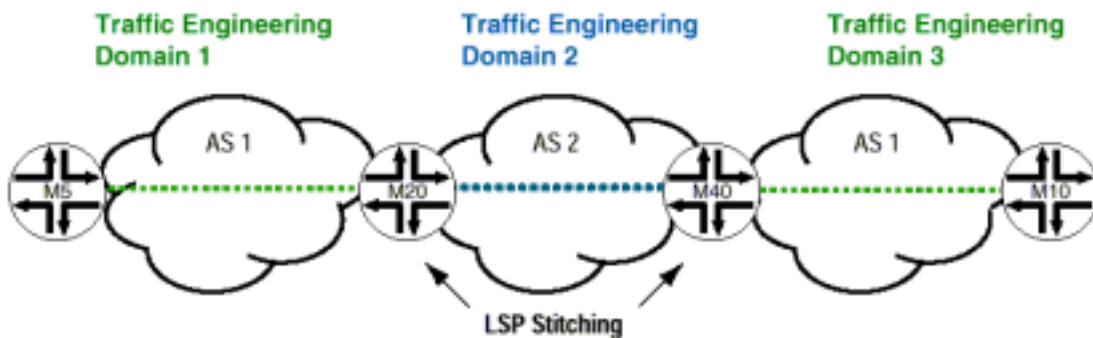


图5：LSP 缝合

基于 MPLS 的第二层 VPN

服务供应商可以提供基于MPLS的VPN服务，以此作为相同的MPLS核心网络上的第二层传输机制（图6）。路由器要求PE支持基于MPLS的第二层VPN，要求核心路由器支持传统的MPLS交换（供应商功能）。在这种实现方案中，MPLS堆栈技术创建了两级标记堆栈：

- 一个外部标记，这是到信宿PE的一条LSP隧道(图6中的LSP 5)
- 一个内部标记，这指明了到CP的PVC (图6中的LSP 2 或 LSP 6)

PE上的信令协议如下：

- LDP/RSVP，用来建立PE之间的LSP
- LDP/BGP，用来交换本地CP VPN信息

这种方法对服务供应商和客户都有许多好处。使用标记堆栈降低了配置复杂度，减少了要管

理的LSP数量。VPN路由在CE级执行。由于PE和核心路由器不必维护VPN路由，因此保证了PE路由器性能和服务扩充能力。通过在IP路由、第三层IP VPN和第二层VPN中使用相同的多元融合核心骨干，服务供应商可以利用所有MPLS特性，如使用流量工程来管理带宽，提高扩充能力等等。客户则可以运行任何第二层或第三层协议，而不会影响核心骨干，实现新客户站点也变得非常简单。

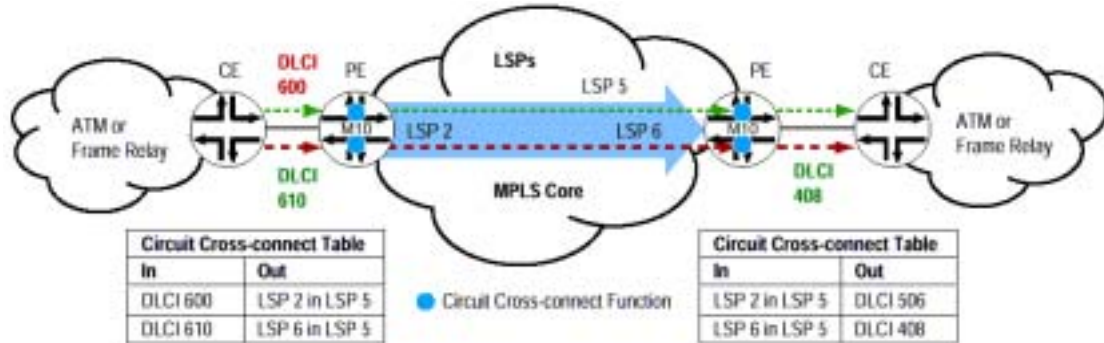


图6：基于MPLS的第二层VPN

第二层企业外部网访问

如果服务供应商拥有一个xDSL或拨号接入网络，那么可以以间接模式，为不希望部署这种基础设施的其它服务供应商提供这种服务。通过把MPLS作为第二层技术，服务供应商可以以透明的方式为另一家服务供应商提供虚拟的RAS或BAS服务(图7)。对于用户连接，根据目标服务供应商，BAS 或 RAS 把数据流指向第二层VPN (如果在RAS或BAS和MPLS核心之间采用以太网连接，那么则是一个VLAN ID)。通过使用MPLS LSP，PE路由器把流量透明地传送到目标服务供应商。对服务供应商来说，这就象所有BAS或RAS都通过一个远程PVC直接连接一样。服务供应商可以为自己的服务供应商客户提供服务水平协议 (SLA)，在核心使用MPLS流量工程，通过各种第二层技术 (如PPP、HDLC、帧中继、ATM或以太网802.1Q.)，同时提供低速和高速吞吐量。此外，在同一条链路上，服务供应商可以在IP/MPLS核心基础上，为其它服务供应商或客户提供其它服务，如Internet接入或IP VPN。

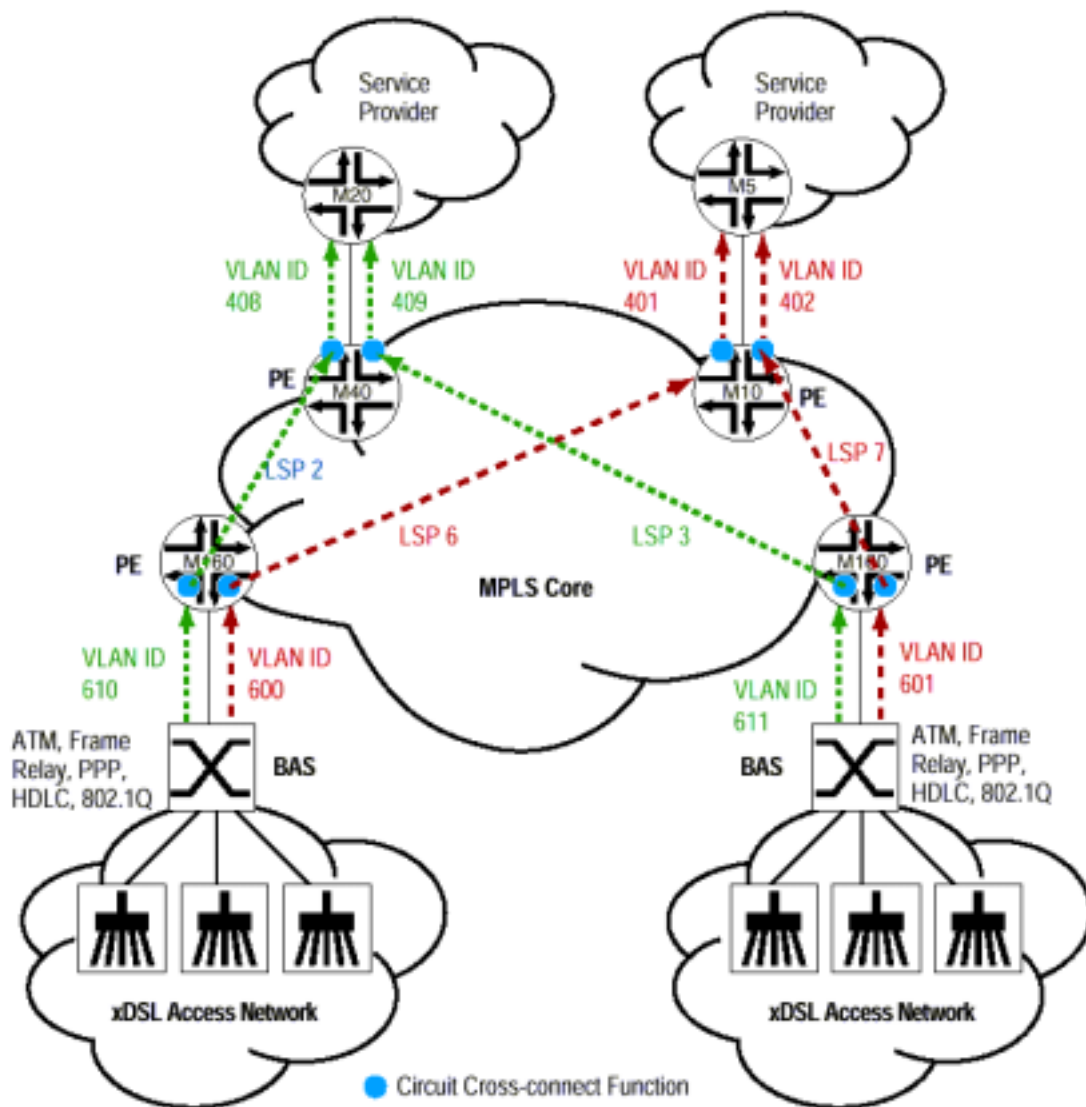


图7：第二层企业外部网访问

高速局域网到局域网服务

在城域环境中，服务供应商可以使用相同的IP/MPLS基础设施，利用简单的局域网接口（如快速以太网和千兆以太网），为客户提供高速站点互连。一旦采用核心IP/MPLS，部署这种服务则变得非常简单。服务供应商可以提供IP服务，另外还可以在相同的本地环路访问上，在第二层提供局域网到局域网互连(图8)。服务供应商可以使用VLAN访问IP服务；或者访问提供IP VPN服务的另一个VLAN，如全国或全球企业内部网服务；或访问连接到同一城市中多个站点的其它VLAN。CE可以是以光纤为介质的远程以太网连接(如连接到现有的局域网交换机)、一台租赁的以太网集中器(同一大楼中的多个客户可以共享这台集中器)、或者是一台Juniper Networks路由器，以各种速度把一个或多个客户连接起来。

在这种解决方案中使用Juniper Networks路由器的好处包括：

- Juniper Networks路由器的转换延迟特别低、特别稳定，因此服务供应商可以规划任何网状或环形结构，并可以简便地扩容和发展，而不必重新考虑整个网络设施。
- 服务供应商可以无缝地提供从100 Mbps 到 1 Gbps的接入速度，并可以获得100%使

用提供的带宽的保障。

- 通过使用先进的远程千兆以太网技术，可以在最远43.50 英里/70公里距离上提供服务。
- 服务供应商可以在提供局域网到局域网服务中，从MPLS核心固有的冗余性中受益。例如，在核心中继线或节点发生故障时，MPLS快速迂回路由技术可以在不到100毫秒内迂回路由LSP，使得故障对用户流量是透明的。

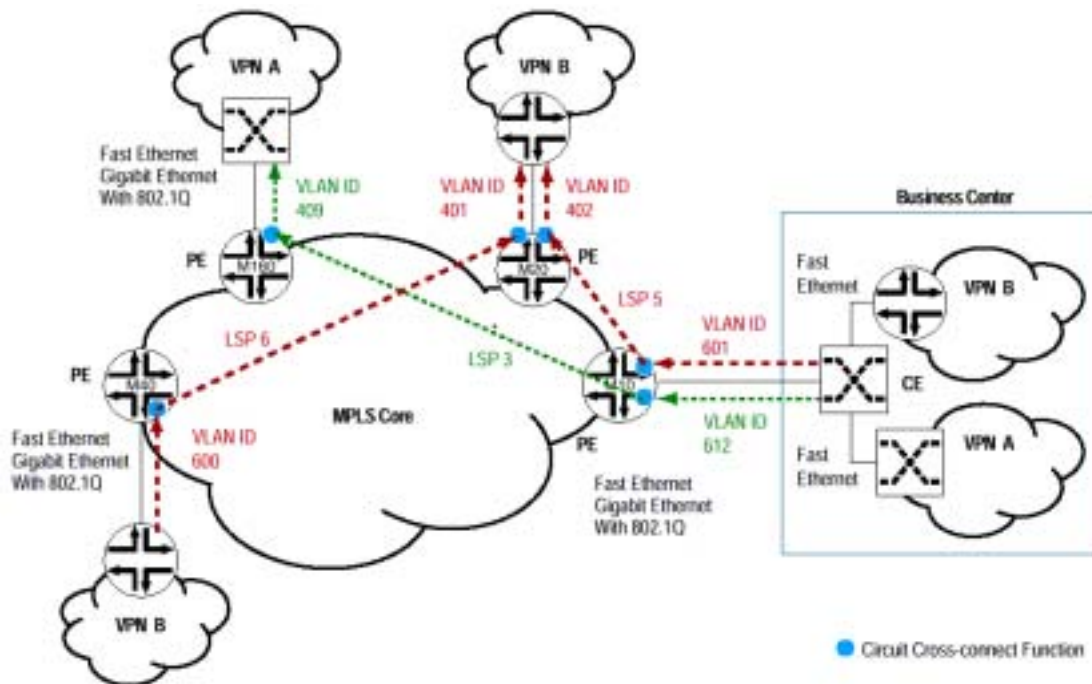


图8：高速局域网到局域网服务

MPLS Internet 交换局

目前，许多Internet交换局都遇到了扩充能力问题，通过使用基于MPLS的Internet交换局服务，服务供应商可以解决这一问题(图9)。例如，服务供应商可以满足下述要求：达到Gbps的高速度；在第二层执行，以控制对等关系；允许远程对等连接；保持带宽管理，如速率限制和服务等级。

对于对等连接，MPLS的速率高达OC-192c/STM-64，避免了ATM信元税，同时仍在任何介质或第二层协议上运行，如SONET/SDH (使用帧中继、PPP或HDLC)、ATM或以太网。ATM技术在速度超过OC-48c/STM-16 (由于SAR芯片局限性)时会发生容量问题，而以太网则很难设计远程对等连接。

服务供应商可以使用两种方法提供MPLS Internet交换局服务：

- 采用端到端流量工程的隧道交换机，其中交换局路由器只交换MPLS LSP，不提供任何BGP路由功能；LSP则在对等路由器之间进行端到端信令处理；
- MPLS电路交连，其中交换局路由器采用静态配置把来自对等路由器的LSP互连起来。

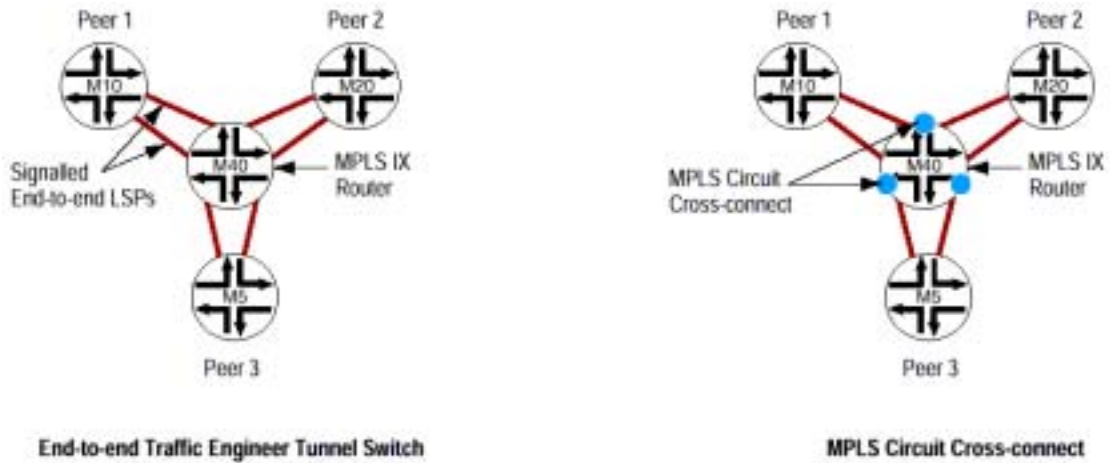


图9：MPLS Internet 交换局

与基于以太网或基于ATM的交换局相比，MPLS通过一个独立于介质的核心网络扩展了对等连接。服务供应商可以在以太网、帧中继、ATM或串行网段基础上构建MPLS核心；它只需作为公共的传输层来运行MPLS。

目前这种功能特别重要，因为Internet交换局正面临着指数级增长，需要扩充，其大多数时间都是在复制物理托管站点，怎样透明地把站点高速互连起来成为一个问题。因此必需使用多条物理光纤或lambda，来解决这种问题。客户通常需要连接一个站点或另一个站点，而不能自由地与任何人实现对等，在要求应变能力的商业环境中，则不能迅速部署对等连接。

MPLS的优点是在站点之间提供了OC-192c/STM-64的速度。通过使用基于MPLS的第二层VPN简单地扩展两个站点之间的LSP，可以实现远程对等。服务供应商甚至可以作为一项服务，或者在两个站点中租赁托管空间时，在两个站点之间提供MPLS Internet交换局。服务供应商在全国或全球范围内查看这个远程对等服务，其中采用转换连接与位于完全不同的区域或国家中的服务供应商建立对等关系（图10）。

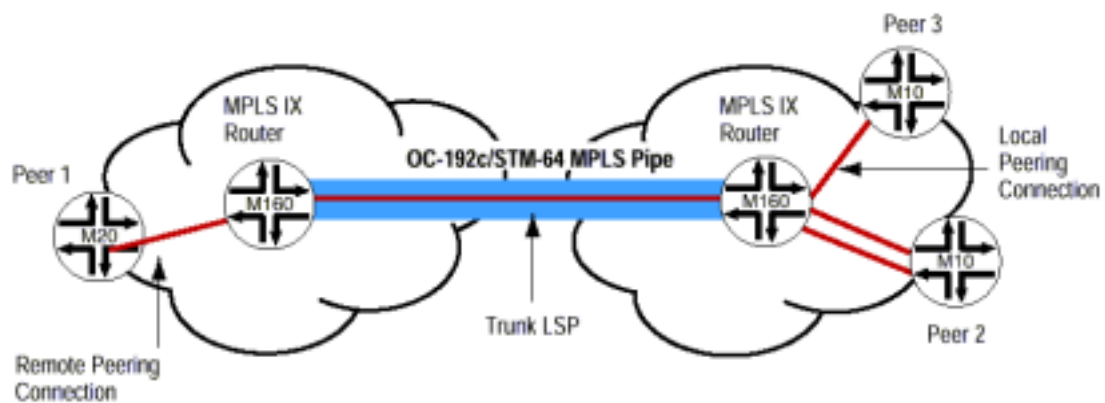


图10：本地和远程对等实例

结论

Juniper Networks基于MPLS的第二层VPN解决了当前最明显的VPN问题：

- 可以简便地进行配置和维护，因此非常经济；
- 提供了具有可预测性能的增值服务；
- 专用的任意间VPN连接，提高了扩充能力；
- 服务等级功能，按客户提供不同的流量。

其结果是可以留住现有的客户群体，同时能够吸引新客户，并迅速可靠地开通新的服务。

缩略语

AAL	ATM适配器层
ATM	异步传输模式
BAS	宽带接入服务器
BGP	边界网关协议
CE	客户边缘
CRC	循环冗余代码
DLCI	数据链路连接标识符
FEC	转发同等类别
HDLC	高级数据链路控制
IP	网际协议
LDP	标记分布协议
LSP	标记交换路径
MPLS	多协议标记交换
OSPF	开放最短路径优先
PE	供应商边缘
PDU	协议数据单元
PPP	点到点
PVC	永久虚连接
RAS	远程接入服务器
RIP	路由信息协议
RSVP	资源预留协议
SAR	分段与重组
SLA	服务水平协议
TE	流量工程
TLV	类型长度值
VCI	虚电路标识符
VPI	虚路径标识符
VLAN	虚拟局域网
VPN	虚拟专用网
VRF	VPN路由和转发