

组织：中国互动出版网 (<http://www.china-pub.com/>)

RFC 文档中文翻译计划 (<http://www.china-pub.com/compters/emook/aboutemook.htm>)

E-mail: ouyang@china-pub.com

译者：于德雷（于德雷 ydl_ldy@sina.com）

译文发布时间：2001-7-1

版权：本中文翻译文档版权归中国互动出版网所有。可以用于非商业用途自由转载，但必须保留本文档的翻译及版权信息。

IP VPN的框架体系

(A Framework for IP Based Virtual Private Networks)

文档状态：

为Internet社区提供信息，不描述任何形式的Internet标准。文档的发布不受限制。

版权声明：

Copyright (C) The Internet Society (2000)。版权保留。

IESG 说明：本文不是IETF工作组的产品，IETF现在还没有进行特别的VPN框架体系标准化。

摘要：

本文描述了基于IP骨干网的VPN框架体系，讨论了不同类型的VPN以及它们具体的要求，提出了用当前的规范去实现这些VPN的机制。本文的目标是，为开发交互VPN解决方案的全范围规范集提供相关协议开发的框架。

目录：

1.0 简介：	2
2.0 VPN 应用和实现要求：	3
2.1 总的要求：	3
2.2 基于 CPE 和基于网络的 VPN	4
2.3 VPN 和外联网	4
3.0 隧道技术：	5
3.1 VPN 的隧道协议要求	5
3.2 建议	9
4.0 VPN 类型：虚拟租用线	9
5.0 VPN 类型：虚拟路由网络	10
5.1 VPRN 特性	10
5.1.3 转发	12
5.2 VPRN 相关的网络	12
5.3 VPRN 总要求	13
5.4 多宿桩路由器	19
5.5 多播支持	19
5.6 建议	20
6.0 VPN 类型：虚拟专用拨号网	20
6.1 L2TP 协议特性	20
6.2 强制隧道	22
6.3 自发隧道	23
6.4 网络主机支持	25
6.5 建议	25
7.0 VPN 类型：虚拟专用 LAN 片 (Segment)	26

7.1 VPLS 要求.....	26
7.2 建议.....	29
8.0 建议总结.....	29
9.0 安全考虑.....	29
10.0 鸣谢.....	29
11.0 参考资料.....	30
13.0 完全版权声明.....	35
鸣谢.....	35

1.0 简介:

本文描述了基于IP骨干网的VPN框架，讨论了不同类型的VPN以及它们具体的要求，提出了用当前的规范去实现这些VPN的机制。本文的目标是，为开发交互VPN解决方案的全范围规范集提供相关协议开发的框架。

在IP骨干网设施上开发VPN有非常重要的现实意义，然而，由于VPN的定义和涉及范围缺乏统一的要求，各种解决方案的描述有许多混淆，互操作性难以实现，VPN的开发也因此受到阻碍。在众多的文档中，VPN经常只是简单的定义为“用IP设施仿真专用广域网”（这里所说的IP设施包括公用Internet，以及专用IP骨干网），因而，VPN的类型就象广域网一样多，也因此产生了好多混淆概念。

在本文中，VPN模型化为一个连接对象，主机可以连接在VPN上，VPN之间可以互联，就像以前的主机连接在物理网络上、物理网络之间可以互联（例如，通过桥或者路由器）一样。网络特性的许多方面，如定址（Addressing）、转发机制（Forwarding Mechanism）、学习（Learning）和广播可达性（Advertising Reachability）、业务质量（Quality of Service）、安全（Security）和防火墙（Firewalling），在物理网络上和虚拟网络上都会有共同的解决方案，VPN中的许多问题都会与原有的物理网络有着类似的实现，引入VPN不是要重新发明一个网络，不会与原来的物理网络截然不同，相反，如果认真考虑一下在物理网络环境下问题的处理方法，再把相同的原理应用在虚拟网络上将会很有帮助，物理网络和虚拟网络运行机制的相似性方便了VPN的引入，减少了标准和协议的开发。

本文档对各种VPN类型进行归类，列出各种类型具体的应用、具体的要求以及实现的具体机制，目的在于作为一个框架体系，为开发全范围互操作VPN解决方案的相关讨论提供指导。

本文首先介绍了一些可能的VPN特例以及它们的实现，同时也将介绍一下基于CPE的解决方案和基于网络的解决方案的不同，然后呈现出VPN的各种类型和它们各自的要求，概要地描述它们的实现方法，指出将来需要标准化的领域。

需要注意的是，本文仅仅讨论在IP骨干网上实现VPN，不论是在专用IP骨干网上，还是在公共Internet上。所描述的机制和模型适用于IPv4以及IPv6。本文不讨论用本地映射交换骨干网手段构建VPN的方法——例如用基于ATM的LAN仿真（LANE）或者多协议传输（MPOA）构建的VPN。IP骨干网通过一些协议用互联路由器建立在交换网络之上，VPN讨论的只是在IP网络之上的操作，因此不直接利用基础网络的本地机制。本地VPN限制在基础骨干网的范围之内，而基于IP的VPN可以伸展到IP可达的任何地方。本地VPN协议显然超出IETF的范围，可以由象ATM论坛这样的组织去应付。（笔者按：该段中的本地是指native，不是local，不当之处，还请指教。）

2.0 VPN 应用和实现要求:

2.1 总的要求:

现在人们非常希望用IP VPN作为建立多站点通信专用网络的有效手段,而不愿意继续使用以前建立物理专用网络的方法。

以前的专用网络大致可以分为两种:专线WAN,可以永久的把多个通信站点连接在一起;拨号网络,可以通过PSTN按需地连接一个或者多个通信点。

WAN一般用租用线路或者专用电路实现——如,用FR和ATM连接多个通信点。处于不同通信站点的CPE路由器或者交换机把这些专用设施连接在一起,进行网络互联。由于这种专用设施的成本、复杂性以及CPE设施配置的复杂性问题,这种网络总起来说无法完全互联,只不过具有某些形式的等级拓扑罢了,例如,远端办公室可以直接连接在最近的区域办公室,区域办公室再进行全互联或者部分互联。

专用拨号网络可以使远端用户通过PSTN或ISDN连接到企业网络上,这一般通过一个或者多个中心站点的NAS来实现,用户拨入这样的NAS,NAS和AAA服务器验证用户身份和被授权接收的业务集。

现在,更多的企业希望自己的专用网络能够快速接入Internet,因此开发基于CPE的VPN的很有意义,因为覆盖范围和通信距离不大影响Internet服务的费用,这样可以比专线和租线大大降低成本。

用Internet进行专用通信不是个新概念,以前就有许多技术能够支持这类应用,如控制路由泄漏。只是在最近才有合适的IP机制来满足用户建立VPN。这些机制的要求包括:

2.1.1 不透明包传输:

运载在VPN上的数据可能与IP骨干网上的毫无关系,一方面因为这些数据是多协议的,另一方面,用户所使用的IP地址与IP骨干网数据传输所使用的IP地址可能就没有什么关系,特别是,用户的IP网络可能使用非唯一IP专用定址方案。

2.1.2 数据安全性

用户使用VPN需要一定形式的数据安全,不同VPN有不同的信任模型,一种模型是用户不相信业务提供商提供的任何形式的安全,他们会用实现了防火墙,使用了安全隧道互联的CPE设备去实现VPN,这种情况下业务提供商被仅仅用来传输IP包。

另一种情况是用户相信业务提供商可以提供一个安全管理的VPN业务,就像用户相信公用FR和ATM交换业务一样,用户相信数据包不会走错方向,不会不经过授权就进入网络,不会被窃听,不会被修改,不会被非授权方进行流量分析。

在第二个模型中,提供防火墙功能和保护包传输的安全是业务提供商的责任,提供商的骨干网中在不同场合下可能需要不同的安全等级。如果VPN的数据交易只发生在一个业务提供商的IP骨干网中,那么就不大需要太高的安全机制(如IPSec)来提供的骨干网节点的隧道安全,如果VPN数据交易横跨了多个管理者的IP骨干网络,启用高安全机制就很有必要了。既然用户认为IP传输网(特别是Internet)是不安全的,即使单个业务提供商也可以为用户数据交易建立高水平安全机制,问题的理解取决于VPN的具体实现。

2.1.3 QoS 保证

除了保证通信的专有性,建立在物理层或者链路层上的专用网络技术也提供不同类型的QoS保证,租用线和拨号线都能够提供带宽和时延的保证,ATM和FR的专用连接也能够提供类似的保证,IP VPN在更广的范围采用之后,市场也需要这样的保证,以便能够保证端到端的应用透明性。IP VPN的QoS保证主要依赖于基础IP骨干网相应的能力,随着它们的发展,VPN框架也必须提供这样的手段,让VPN系统能够利用这种能力。

2.1.4 隧道机制

前面的两条要求已经暗示了VPN的实现必须通过隧道机制,以便VPN的包格式和地址与IP骨干网上的隧道包互不相干,隧道使用特定的格式,可以提供一定水平的数据安全,还可以通过其他一些机制来加强(如IPSec)。

另外,这样的隧道机制可以随着IP数据流量管理机制的发展而发展。现在已经定义了许多IP隧道机制,其中一些非常适合VPN应用,在3.0节中将会有详细讨论。

2.2 基于 CPE 和基于网络的 VPN

现在大多数的VPN实现是基于CPE设备的,VPN的功能都集成在各种各样的CPE设备之中,从防火墙到WAN边缘路由器以及特定的VPN终端设备,这样的设备可以由用户来购买和配置,也可以由ISP以外包业务方式进行配置(常常是远端管理)。

基于网络的VPN也很有意义,这时,VPN的整个操作作为一个ISP的外包资源实现在网络上,而不是用户CPE上。使用这种方案,用户可能减少技术支持费用,ISP可以增加收入。支持基于网络的VPN使得一些高效廉价的解决方案得以奏效,在众多用户之中支持普通的设备和操作。

下面描述的好多机制即可应用于网络VPN也可以应用于CPE VPN,但是一些特殊的机制可能仅仅可以应用于后者,因为它们所利用的工具(如路由协议负载)只能由ISP访问,不能由用户访问,甚至由于CPE节点联合管理问题,连那些拥有和操作CPE的ISP主机也不能访问。本文将指出那些技术仅仅适用于网络VPN。

2.3 VPN 和外联网

外联网的概念是指两个或者两个以上的公司网络可以互相访问对方有限的数据库信息。例如,一个设备制造商可能用一个外联网为它的供应商提供查询数据库,允许后者查询元件价格和用途,以及定购情况。再如,在联合软件开发中,公司A允许公司B的一个开发小组访问它的操作系统代码,公司B允许公司A的一个开发小组访问它的安全性软件。注意,访问策略可以做到任意复杂,例如,公司B可以对自己的安全性软件作出一些内部访问限制,为适应出口控制法律,只允许特定的地理位置进行访问。

外联网的关键特性就是控制访问者和被访问的数据,这是一个策略决策问题,策略决策一般在不同域的互联点上受到加强,例如专网和Internet之间,或者公司的软件测试实验室和公司其余的网络之间。这种加强可以通过防火墙、带有访问表功能和应用网关的路由器或者任何其他任何能够执行传输策略应用的设备来完成,策略控制除了可以实现在公司网络之间,还可以实现在公司网络的内部。网络间的互联也可以是双向链接的集合,或者就是一个独立的网络——由工业组织维护的网络,这个单独的网络本身也可以是一个VPN或者物理网络。

VPN的引入不需要改变这个模型，策略可以应用于两个VPN之间，或者在VPN和Internet之间，就像以前没有VPN一样。例如，两个VPN可以互联，每个都有自己的策略控制，通过一个防火墙，查看进来的流量是来自于另一个VPN还是Internet。

VPN的这个模型提供了一种与包传输基础模式不同的策略，例如，路由器可能把语音流量直接路由到ATM VCC上以保证QoS，非本地内部公司流量路由到安全隧道里，其他流量路由到Internet链路上，在过去，安全隧道是帧中继电路，现在它们也可以是安全IP隧道或者MPLS标记交换通道。

当然还可能有一些其他一些VPN模型，例如，可以有一个应用流集映射进VPN的模型，由于网络管理员给出的策略规则则会相当复杂，在策略规则库中使用的不同应用流集的数目，也就是VPN的数目，就会变得很大，可能造成多重交叉的VPN，然而，引入这种新的复杂性到网络中却实在获得不了什么好处。VPN应该看成是物理网络的直接模拟，这样可以充分利用现有的协议和规程以及现有的网管和用户技术。

3.0 隧道技术：

如2.1所述，VPN需要用某些形式的隧道机制来实现，本小节讨论VPN隧道机制的要求，比较链路层协议的特性和现有隧道协议的特性，提供协议差异比较的基础，突出隧道协议特点，更好的支持VPN环境运作。

连接两个VPN端点的IP隧道是一个基本的构件，基于它各种不同的VPN才得以建立。IP隧道运行在IP骨干网之上，发送到隧道中的数据流量对IP骨干网络是不透明的，在效果上IP骨干网用作了链路层技术，隧道形成了点到点连接。

VPN设备可以终止多个IP隧道，在这些隧道和不同的网络接口之间以各种方式转发数据包，在后面不同类型VPN的讨论中，数据包在接口（如桥或者路由器）间的转发方式是造成类型差异的主要原因，非常类似于以前网络设备的特性。两端口转发器直接转发数据包，不检查包的内容；桥使用MAC层信息来转发数据包；而路由器用第三层地址信息来转发，如本文后面所述，这三个场合都有和VPN的直接相似性。要注意，IP隧道被视为另一种链路，可以和其他链路串连，绑定在桥转发表中，或者绑定在IP转发表中，具体根据VPN的类型而定。

下面的章节就看一看建设不同类型VPN的基础构件——IP隧道协议。

3.1 VPN 的隧道协议要求

有许多种IP隧道机制，IP/IP，GRE、L2TP、IPSec、MPLS。虽然有些协议没有被视作隧道协议，但是它实际上做的也是建立隧道的事情，都是从封装包的地址域提取转发信息，允许不透明帧作为包载荷通过IP网络传输。

然而要注意的是，MPLS和其他隧道协议有所不同，它是一种专门的链路层协议，MPLS只能在MPLS网络范围内应用，而IP可以伸展到任何可以达到的地方，基于MPLS隧道建立的VPN机制从定义上就不能伸展到MPLS网络之外，就像基于ATM机制如LANE不可以伸展出ATM网络一样。可是，MPLS可以横跨许多不同的链路层技术，就像IP网络，它的范围也不是限定在特定的链路层之上。现在已经提出了许多机制允许基于MPLS网络建设交互VPN。

VPN隧道机制有好多要求，当前的隧道机制还没有完全满足这些要求，它们包括：

3.1.1 复接

在相同的两个IP端点之间可能要求建立多个VPN隧道，基于网络的VPN就有这种需求，每个端点支持多个用户。在两个相同的物理设备上，不同用户的数据通过各自独立的隧道，应

该有一个复接域标识数据包所属的那个隧道，或者以类似的方式共享一个隧道，这样可以减少隧道建立的负担和时延。在现有的IP隧道机制中，L2TP（通过隧道标识和会话标识）、MPLS（通过标签）和IPSec（通过安全参数索引）有复接机制；严格地讲，GRE没有复接域，但是它的钥匙域可以用来认证信息包源，有时可以作为复接域；IP/IP没有复接域。

IETF和ATM论坛都标准化了全局唯一的标识符VPN-ID，用来标识一个VPN。VPN-ID可以放在控制平面，在隧道建立时间中绑定一个隧道和VPN，或者放在在数据数据平面，基于数据包来标识该数据所关联的VPN。在数据平面中，VPN封装头可以用在MPLS、MPOA和其他一些隧道机制上，为不同VPN在一个隧道上收集数据包。在这种情况下，VPN-ID显式地包含在每一个数据包中，隧道不需要特别的复接域；在控制平面上，VPN-ID可以包含在任何隧道建立信令协议上，让隧道（如，由SPI域标识）和VPN关联，在这种情况下，不需要在每个数据包中包含VPN-ID，5.3.1中将做进一步讨论。

3.1.2 信令协议

在隧道建立之前端点必须知道一些配置信息，如远端IP地址以及隧道所要求的相关隧道属性（如安全水平），一旦这些信息配置完成，隧道便可以通过两种方式完成建立，可以通过管理操作，或者也可以通过信令协议，信令协议可以动态建立隧道。

管理操作的例子如用SNMP MIB配置不同隧道参数，如MPLS标记、IP/IP或者GRE隧道的源地址，L2TP的隧道标识、会话标识，或者IPSec的安全连接参数。

信令协议可以减轻管理负担，在许多场合下这非常重要，它可以减少需要配置的工作量，如果VPN横跨多个管理域，可以减少管理协同的必要。例如，上面描述的复接域的值，节点分配时为本地化，通过信令协议可以在发布后仍保持本地化，而不是首先配置在管理站，然后发布到相关节点。信令协议也允许移动节点或者间歇连接的节点按需建立隧道。

在VPN环境下，信令协议应该允许VPN-ID的传输，让产生的隧道关连到特定的VPN，也应该允许隧道属性交换和协商，例如帧序列和多协议传输的使用，注意，信令协议的角色只是协商信道属性，而不是运载隧道如何使用信息，如隧道中的帧是在层2转发还是在层3转发，（就像Q.2931 ATM信令——除LANE的又一种建立IP逻辑子网络的信令）。

在各种IP隧道协议中，下列协议支持适应此目的的信令协议，L2TP（L2TP控制协议）、IPSec（IKE协议）、和GRE（移动IP隧道）。还有两种MPLS信令协议可以用来建立LSP隧道，一个是MPLS标签分布协议（LDP）的扩展，叫做受限路由LDP，CR-LDP，另一个是LSP隧道的资源保留协议RSVP的扩展。

3.1.3 数据安全

VPN隧道协议必须支持用户所要求的任何档次的安全，包括认证和不同强度的加密能力。除了IPSec，其他的协议都没有内在的安全机制，它们依赖于基础IP骨干网络本身的安全特性。特别是，MPLS依赖显式的标记交换通道来保证它的信息包不会传错方向，其他的隧道协议可以用IPSec来提供安全保障。对于是实现在非IP骨干网上的VPN（如，MPOA，FR和ATM VC），数据安全隐式的由层2交换结构提供。

从总体来看，VPN不仅仅包括隧道的安全能力，还包括在边缘路由器中信息包是如何进入隧道的，例如，用虚拟路由器实现的VPN中，独立的路由表、转发表实例保证了VPN之间的隔离，一个VPN上的数据包，不会错误的路由到另一个VPN的隧道上，因为这些隧道对于第一个VPN的转发表是不可见的。

如果VPN端点使用某些形式的信令机制和另一端点动态建立隧道，那么就要求认证试图建立隧道的实体，IPSec为了这个目的形成了一系列的方案，例如，允许使用预共享密钥来进行认证对方，也可以用数字签名和身份验证。其他一些隧道协议的认证能力比较弱，但在一些情况下可能根本就不需要认证，例如，如果隧道是预分配而不是动态建立的，或者如果系统根本不需要信任模型。

现在IPSec ESP可以建立SA即能支持加密又能支持认证，或者二者都支持，然而如果不用认证和加密，协议也可以不使用SA。在一个VPN环境中，这个“NULL/NULL”选项是非常有用的，因为可能有时仅仅需要协议的其他方面（如，支持隧道和复接）可能都是必需的。在效果上，“NULL/NULL”可以视为另外一种水平的数据安全。

3.1.4 多协议传输

许多应用中，VPN可以承载不透明多协议数据，因此，隧道协议必须能够支持多协议传输。L2TP可以传输PPP包，而PPP包可以运载多协议，因此L2TP可以传输多协议。GRE也提供隧道协议标识，而IP/IP和IPSec隧道没有这样的协议标识域，因而只能建立IP协议隧道。

扩展IPSec协议集允许传输多协议是完全可能的，例如，可以通过扩展IPSec的信令组件IKE来实现IPSec的多协议传输，指示隧道里传输的协议类型，或者在每个隧道包里运载一个包复接头，（例如，一个LLC/SNAP头或者GRE头）等等。这种方法类似ATM网络，它使用信令来指示VCC里面的封装，VCC发送的数据包使用一个LLC/SNAP头，或者直接放在AAL5载荷中，后者就是VC复接。

3.1.5 帧序列

用户所要求的QoS属性之一便是VPN帧序列，类似于物理租用线或专线的特性。特定端端协议和应用的有效操作可能需要帧序列，为了实现帧序列，隧道机制必须支持序列域，L2TP和GRE都有这样一个域，IPSec有一个序列号码域，但是它是由接收者执行反重播检验，不是为了保证数据包的有序传送。

扩展IPSec允许使用已有的序列域来保证有序包传送是完全可能的，例如，用IKE协商来确定序列是否使用，定义保留包序列的端点行为。

3.1.6 隧道维护

VPN端点必须监视VPN隧道的运作，保证连接不丢失，如果发生意外应该采取适当的措施（如路由重计算）。

有两种可能的方法，一种是让隧道协议自身周期性地检查隧道连接，提供显式的失败指示，例如，L2TP有一个保持存活机制选项来检测不运作的隧道。

另一种方法不需要隧道协议自身来执行这个功能，而是依赖于一些外部机制来确定连接的丢失，例如路由协议RIP和OSPF运行在一个隧道上，在一定的周期里侦听到邻通道的失败后，便在路由协议上报告隧道的关闭。还有一种方法是不断的执行ICMP ping，这也可以确保隧道运作特性，因为隧道本身也是在同一个IP骨干网上运行。

当隧道动态建立时，我们需要了解动态和静态隧道信息的不同，一个隧道建立之前，节点需要知道一些静态信息，例如远端的验证，所发起或者接受的隧道的属性等等。一般这都是配置操作，作为建立隧道的信令交换结果，在每一个端点都形成了一些动态状态，如复接域的值，密钥等，例如，在IPSec中，SA建立后，在它生存时间里的密钥也得以建立。

建立动态隧道时将会用到不同的策略，一种是数据驱动机制，当数据需要传输时，就启动隧道建立，没有数据传输，就发出隧道超时信息，当为QoS分配隧道时，这种方法非常有效。另一种方法是每当静态隧道配置信息安装完毕时，就建立隧道，然后努力保持该隧道存在。

3.1.7 MTU 问题

一个IP隧道关联一个MTU，就像常规的链接一样，可以想象，这个MTU可能比通道上任何两端点之间的单跳或多跳的MTU都要大，这样在隧道中就可能要求某些形式的帧分割。

如果帧映射在一个IP包里面，当IP数据报到达一个MTU小于IP隧道MTU的节点时，就会进行正常的IP分割。这种隧道中间分割可能会在路由器上造成意料不到的性能牵连。

一种可选的方法是让隧道协议本身包含隧道级分拆和重组的能力，例如，可以用隧道序列号和某种类型的消息终止符，（注意，多链接PPP就是用这种类似的机制分割信息包），避免IP层隧道自身的分割。现在还没有什么协议支持这样的机制。

3.1.8 最小隧道开销

减少隧道机制的开销有许多好处，特别是传输诸如音频视频包等对抖动和时延比较敏感的数据。另一方面，如果使用IPSec安全机制，也会强加自己的开销，因此目标对象应该尽量减少安全所需的开销，不要加重那些对安全要求不太强烈的隧道负担。

当远端拨号用户使用自发隧道连接VPN时，由于拨入链接带宽较低，开销的大小就更显得重要了。6.3将讨论这个问题。

3.1.9 流量和拥塞控制

L2TP协议的开发过程已经制定了流量和拥塞控制的规程，这主要是因为在使用与IPComp【28】不同的PPP压缩时，要求在有损网络上提供足够的性能。另一个动机是让设备尽量使用较少的缓存，例如可以终止低速拨号线。然而，L2TP规范的最后版本仅仅为控制信道定义了流量和拥塞控制机制，而没有为数据信道定义。

总的来说，多层流量和拥塞控制的交互作用是非常复杂的，但是当今占主导地位的TCP还是有其自身的端到端流量和拥塞控制机制，但是真正在隧道协议中实现类似的机制却不见得到底会有多大好处，开发测试适应所有网络条件的流量和拥塞控制方案是很困难的，有其自身的原因，也有和其他类似方案理解上的原因。然而，让发送者能够知道接收者的接收能力，提供协议机制、允许接收者把它的能力通过信令发送给发送方是很有帮助的。对该领域做进一步研究可以获益不少。

也请我们注意一下IETF PILC工作组的工作，它正在对不同网络链路的正确性如何影响Internet协议在那些链路上的操作进行检查。

3.1.10 QoS/流量管理

如上所述，客户可能要求VPN就丢失率、抖动、时延和带宽保证等QoS参数提供同物理租用线和专线一样的保障，如何实现，是VPN节点自身和以及它所连接的接入和骨干网的流量管理功能。

对QoS和VPN的全面的讨论超出了本文档的范围，然而如果把VPN隧道模型化为另一种类型的链路层，许多为原来物理链路所开发的QoS机制仍然可以应用，如，可以在一个VPN节点上，用VPN参数、队列和接口把策略机制、标记机制、队列机制、整形机制和进程机制和应用到VPN流量上，就象非VPN流量一样，Diffserv、Intserv和MPLS流量工程开发的技术在VPN流量上仍然可用。见【29】对QoS和VPN的讨论。

然而，应该注意的是，这个隧道操作模型不必和现在已经模型化的隧道协议相一致，模型只不过用来帮助理解，不是协议规范的一部分，如果模型不同会使讨论复杂化，特别是当

模型作为协议规范的一部分或者作为实现方法的强制性选择被曲解时，例如，IPSec隧道处理过程可以模型化为接口，也可以模型化为特别数据包流属性。

3.2 建议

需要强加密或者强认证就需要IPSec，IPSec也支持复接和信令协议——IKE，然而，为了支持VPN环境的隧道要求，扩展IPSec使其可以覆盖下面的领域将会有更多好处。

- 建立SA时，传输VPN-ID (3.1.2)
- 空加密和空认证 (3.1.3)
- 多协议操作 (3.1.4)
- 帧序列 (3.1.5)

L2TP自身不提供数据安全，PPP的任何安全机制并不应用到L2TP自身，因此，为了提供强安全性，L2TP必须运行在IPSec之上，定义IPSec支持L2TP数据传输的专用操作模式将会有助于互操作性，L2TP的工作组正在做这样的事情。

4.0 VPN 类型：虚拟租用线

最简单的VPN形式是“虚拟租用线”（VLL）业务，在这种情况下，用户仅仅得到了点到点链接，连接了两个CPE设备，如下图所示。连接CPE设备到ISP节点的链路层可以是任何类型，如ATM VCC或者FR电路等，CPE设备可以路由器、桥或者主机。

两个ISP节点都连接在IP骨干网上，IP隧道建立在二者之间，每个ISP节点在第二层（如ATM VCC和IP隧道）配置绑定桩链路和IP隧道，帧在两条链路之间中继，例如，ATM AAL5载荷封装在IPSec隧道中，AAL5载荷的内容对ISP节点是不透明的，不被检查。

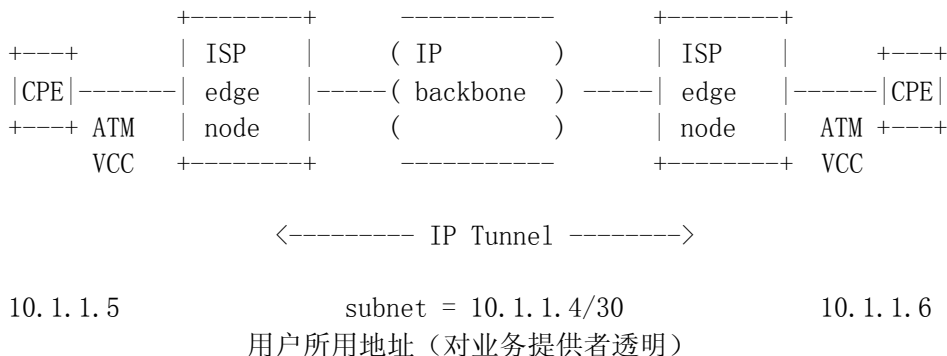


图4.1: VLL用例

对于用户来说，就好像真的有一条ATM VCC或者FR电路连接两个CPE似的，用户感觉不到电路部分实际上实现在IP骨干网上，这种做法有时候非常有好处，例如，业务提供者想用ATM作为网络接口提供LAN互联业务，但是却没有直接连接所有用户站点的ATM网络。

连接CPE设备到ISP节点的两条链路可以不是同一种介质类型，但这时ISP节点不能以如上所述的不透明方式进行数据传输。相反，ISP节点必须在两种介质类型（如ATM和帧中继）中间执行设备互联功能，如LLC/SNAP到NLPID转换，进行不同的ARP协议转换，执行CPE设备期望的任何媒介处理，（如，ATM OAM信元或者帧中继XID交换）。

IP隧道协议必须支持多协议操作，如果序列功能对用户数据传输很重要，可能还需要支持序列。如果隧道是用信令协议建立的，当从用户链路收到一个帧并且这时隧道不存在，它们可能以数据驱动方式启动，或者，也可以预分配并且永久保持隧道。

注意这里用到的VLL和Diffserv EF—PHB（Expedited Forwarding Per Hop Behaviour）定义不同，后者指的是低时延、低抖动、保证带宽的通道，可以由PHB提供，因此它的重点

放在链路时间特性上。在这篇文档里，VLL并不暗示任何特殊的如Diffserv或者其他的QoS机制，相反，其重点是放在链路拓扑上，（如，建立一个包含一个IP隧道的链路）。对于完全的链路层仿真，时间和拓扑特性都需要考虑。

5.0 VPN 类型：虚拟路由网络

5.1 VPRN 特性

VPRN定义为用IP设施仿真广域路由网络，本节介绍如何提供基于网络的VPRN业务，基于CPE的VPRN也是可能的，但在这儿不作特别讨论。基于网络的VPRN所要解决的问题主要是配置和操作，必须在业务提供商和业务用户之间划分管理责任。

VPRN和其他VPN的不同之处就在于数据包转发在网络层，VPRN就是由ISP路由器之间的隧道网组成，每个VPRN节点转发数据的路由能力。附着在ISP路由器上的是通过一条或者多条链路（称为桩链路）连接的CPE路由器。在每个ISP路由器中有一个VPRN专用转发表，VPRN的成员都连接在上面，通过路由转发表，数据可以在ISP路由器之间、ISP路由器和用户站点之间转发，表中包含网络层可达性信息（可以和VPLS比较，它的转发表中包含MAC层可达性信息，7.0小节）。

下图是了一个VPRN的例子，示意了3个ISP边缘路由器通过IP隧道网络连接，互联了4个CPE路由器，其中一个CPE路由器在网络上有多宿，它有多条桩链路，所有的链路可以都激活，也可以让其中的主链路激活，如果发生意外，备用链路再激活，术语“后门”链路指的是两个用户之间没有通过ISP网络的链路。

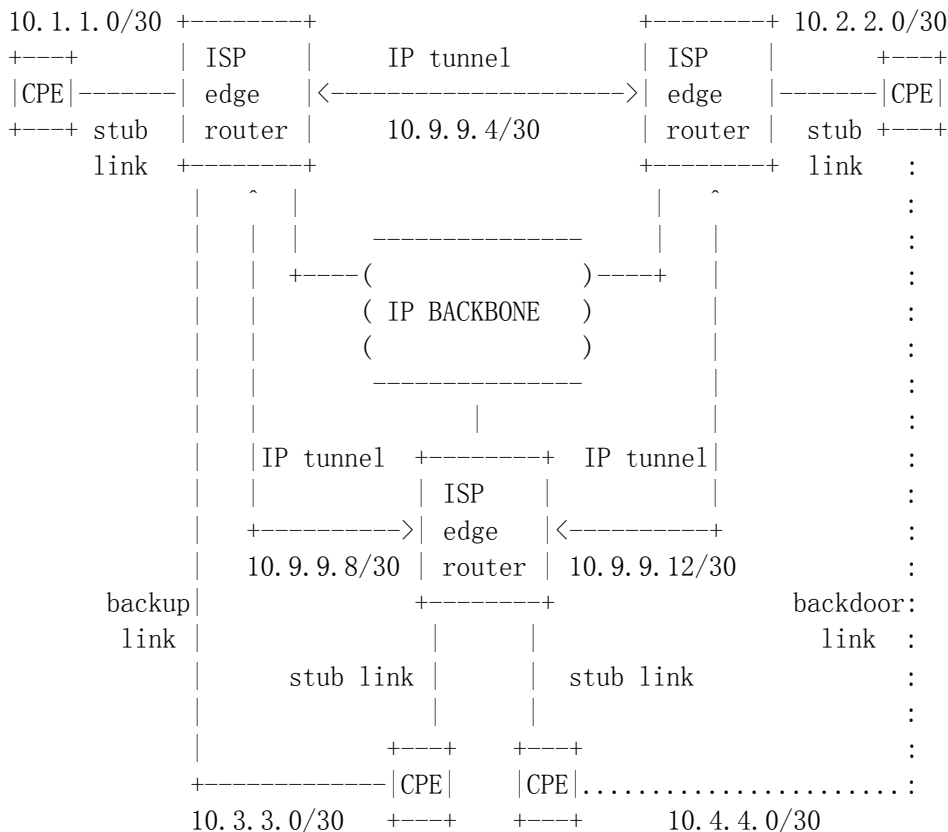


图5.1:VPRN实例

VPRN的主要好处是CPE路由器的配置及其复杂性得到简化, 对于一个CPE路由器, ISP边缘路由器好像是用户网络的邻路由器, 它用缺省路由向其发送数据。数据传输隧道网的建立仅延伸到ISP边缘路由器, 而不是CPE路由器, 在效果上, 隧道建立、维护和路由配置的负担都交给了ISP, 此外, VPN所要求的其他服务如防火墙的提供、QoS处理也可以由一小部分ISP边缘路由器处理, CPE设备种类繁多, 不适合处理这些功能, 引入和管理新的业务也可以很容易解决, 不必去为CPE设备升级, 当本地使用VPN业务接入专用公司网络的用户非常多的时候, 这样做的好处就更大了, 该模型就像电话业务, 不需改变用户设备就可以引入新业务(如呼叫等待)。

VPRN不同于那些把隧道口延伸到CPE路由器的VPN类型, 那不过是由ISP提供层2连接罢了, 可以通过CPE路由器之间的VLL(见4.0)实现, 即ISP网络提供一系列的层2点到点链接; 也可以作为一个VPLS——ISP仿真一个多接入LAN片, 这种情况下用户可能有更多的灵活性(如, 任何IGP或者任何协议可以运行在用户站点), 但是配置复杂性造成了成本的昂贵, 因此, 需要根据用户的具体要求, 有可能是VPRN, 也有可能是VPLS。

因为VPRN在网络层转发, 一个VPRN仅仅直接支持一个网络层协议, 对于多协议支持, 可以在各种网络层协议上建立独立的VPRN, 或者让一种协议在另一个网络上(如, 非IP网络隧道到IP VPRN)建立隧道, 或者, 让ISP网络仅提供层2连接, 就像上面提到的VPLS。

VPRN要解决的问题包括初始配置, 就是ISP边缘路由器所要确定的每个VPRN的链路集、在VPRN拥有成员的其他路由器集、通过每个桩链路可达的IP地址前缀集, 还包括CPE路由器确定的准备转发到ISP边缘路由器的IP地址前缀集、正确发布桩链接可达性信息的机制和运载数据隧道的建立和使用等等, 还要注意的, 虽然我们在这里首先讨论了VPRN, 但是这里的许多问题也适合于后面的VPLS, 只要把网络层地址替换成链路层地址即可。

注意, VPRN的操作类似于用户站点访问Internet的机制, 一般情况情况是ISP边缘路由器即要为用户提供VPRN连接, 又要为用户提供Internet连接, 这时CPE路由器里有一个到ISP边缘路由器缺省的路由点, 负责把私有数据转送到VPRN, 其他的数据流通转送到Internet, 在这两个域之间提供防火墙功能。当然, 用户也可以通过不涉及VPRN的ISP路由器建立Internet连接, 甚至通过一个不同的ISP, 这时的CPE设备要完成不同域数据的分离以及提供防火墙功能。

5.1.1 拓扑

VPRN的拓扑可能包括所有VPRN节点之间整个的隧道网, 或者也可以是某些隧道的随机拓扑, 如一系列远端办公室连接到最近的地区站点, 地区站点再进行整个或者部分的连接。在IP隧道建立的VPRN中, 使用全网拓扑可以比直接分配物理资源(如, 租用线)节省很大的费用, 也比那种要求资源分配在设备上的隧道方法(如, FR DLCI)要好。全网拓扑产生出优化路由, 消除了经过第三个节点为两个直接相连的站点传输数据的必要性, 全网拓扑的另一个吸引人的地方是不需要配置VPRN的拓扑信息, 对于VPRN的成员路由器来说, 拓扑是隐式的。如果ISP边缘路由器的数量十分巨大, 全网拓扑可能不太适合, 因为这时涉及到升级问题, 如, 站点之间的隧道数目会随之增长, (n 个站点, $n(n-1)/2$ 个隧道), 每个路由器的路由对也会急剧增长。当然也可能也会使用非全网拓扑的网络策略, 如网络管理员可能希望两个站点的流量经过中心站点, 而不是直接传输数据。对于IP骨干网, 也需要考虑到由于某些错误造成的部分连接问题(如, A可到B, B可到达C, 但是A不能直接到达C), 可以运用策略路由来解决这个问题。

对于一个面向网络的VPRN, 假设用户通过一条或者多条点到点链路(如, 租用线, ATM或者FR连接)连接到ISP边缘路由器, ISP路由器要负责学习和发布它们之间可达性信息, CPE路由器通过每条桩链路学习可达目的地集, 虽然这可以象缺省路由一样简单。

桩链路可以是预分配的专线, 也可以是象用PPP、自发隧道(见6.3节)或者ATM信令等按需分配的动态链路。动态链路需要认证用户, 确定用户可以接入(如, 用户可以加入VPRN)

的授权资源。VPRN机制和业务可以由任何类型的用户以任何方式使用，而不是让用户初始绑定VPRN，（这种处理可能包括专门的考虑，如动态IP地址分配）。

5.1.2 定址

VPRN里使用的地址和IP骨干网上的地址没有什么关系，特别是VPRN可以使用非唯一专用IP地址，多个VPRN可以实现在同一套物理设备上，它们可以使用相同的或者交叠的地址空间。

5.1.3 转发

对于一个VPRN，隧道网形成了IP骨干网上的交叠网络，在每个ISP边缘路由器中，必须有VPN专用的转发状态来转发从桩链路接收到的信息包，传送到下一跳路由器，当ISP边缘路由器支持属于同一VPRN的多链路时，作为本地事件，隧道可以终止在边缘路由器上，也可以终止在桩链路上，前者需要VPN专用的转发路由表转发流出的数据，后者不需要。为了把接收到的数据流量导向正确的隧道，在数据来的方向中需要VPN专用转发表。

也因为VPRN工作在互联网的网络层，在隧道上发送的IP包也将有TTL域，以正常的模式操作，防止信息包在VPRN的路由环中打转。

5.1.4 多并发 VPRN 连接

注意一个用户站点也可能同时属于多个VPRN，可能同时传输数据到一个或者多个VPRN或者到缺省的Internet上，这一切都可以发生在同一个桩链路上。对于这个问题有好多解决办法，但是这超出本文的范围。

5.2 VPRN 相关的网络

VPRN的要求和机制在前面许多文档中讨论过了，其中的一个是【10】，讨论的是如何在MPLS和非MPLS网络上实现相同的VPN功能，其他的一些在下面简单描述。

提供VPRN成员资格和可达性功能的机制有两种主要的方式——交叠式和背载式，下面的5.3.2、5.3.3和5.3.4将详细讨论。【14】里描述了一个交叠式例子，讨论的是通过分离每个VPN路由协议实例和路由转发表来实现VPRN功能，另一种办法是通过虚路由来实现。每个VPN的路由实例隔离于另一个VPN的路由实例，也隔离于骨干网的路由实例，结果是任何路由协议（如，OSPF，RIP2，IS-IS）都可以运行在任何VPRN上，独立于其他VPRN所运行的路由协议，也独立于骨干网自身的路由协议。【12】中描述的VPN模型是一种使用虚路由的交叠VPRN模型，重点放在了在MPLS骨干网上提供VPRN功能，描述了基于MPLS隧道网的VPRN成员如何实现MPLS骨干网上的自治。【31】扩展了虚路由模型，包括VPN区域，以及在VPN区域之间负责路由的VPN边缘路由器，VPN区域可以由管理以及技术原因定义，如不同的基础网络结构（如，ATM，MPLS，IP）。

相反，【15】描述了用背载方法提供成员资格和可达性信息发布等VPN功能，这些信息在BGP【32】协议包上以背载方式操作，VPN用BGP策略构建，由它来控制哪些站点可以互相通信，【13】也使用BGP背载成员信息和背载可达性信息来建立MPLS LSP（CR-LDP或者扩展RSVP），然而不像其他的建议那样，这个建议需要CPE实现VPN的某些功能。

5.3 VPRN 总要求

基于网络的VPRN解决方案有许多通用要求，也有许多机制可以用来满足这些要求：

- 1) 全局唯一的VPN标识符，用来指一个特定的VPN。
- 2) VPRN成员资格的确定。一个边缘路由器必须学习本地每个VPRN桩链路，必须学习在该VPRN中拥有成员的其他路由器集合。
- 3) 桩链路可达性信息。一个边界路由器通过每个桩链路必须学习可达地址集和地址前缀集。
- 4) 内联VPRN可达性信息，一旦边缘路由器确定关联于每个桩链路的地址前缀集，那么这个消息必须发布到VPRN的每个边缘路由器。
- 5) 隧道机制，一个边缘路由器必须构建必要的隧道到另一个拥有VPRN成员的路由器，必须执行必要的封装和解封装。

5.3.1 VPN 标识符

IETF和ATM论坛已经为标识VPN的全局唯一标识符标准化了一个独立的格式——VPN-ID，现在只定义了VPN-ID的格式，没有定义它的语法和用法。目标是允许它用于不同的目的，让不同技术以及机制使用同一个标识符。例如，一个VPN-ID可以包含在MIB中，标识一个VPN；VPN-ID也可以用在控制平面上起到控制作用，例如在隧道建立时间绑定一个隧道，所有穿过隧道的包就会隐式地关联于标识了的VPN；VPN-ID也可以用在数据平面封装，显式地标识一个VPN包。如果VPN用不同的技术实现，（如IP和ATM），可以用同一个VPN-ID在不同技术上标识VPN，同样，如果VPN横跨几个管理域，同一个标识符可以在任何域使用。

大多数的VPN方案（如，【11】，【12】，【13】，【14】）都要求使用VPN-ID，或载在控制包里，或载在数据包里，其作用是和特定VPN关联一个数据包。虽然以这种方式VPN-ID的使用非常普遍，但是却并不普遍。【15】描述了一种没有VPN协议标识域的方案，这个方案里，VPN由用户理解，行政式的构建，用BGP策略建立。有许多关联于VPN路由的属性，如路由区别符号、源或者目标“VPN”，由基础协议机制使用，消除歧义，扩大使用范围，这在用BGP策略机制构建VPN中也使用，但是在其他的文档中没有相应的VPN-ID。

也请注意，【33】也定义了一种使用标准VPN-ID格式在ATM AAL5上进行多协议封装的格式。

5.3.2 VPN 成员资格信息配置和发布

为了建立一个VPRN，或者在VPRN中插入新的客户，ISP边缘路由器必须确定哪一个桩链路关联于哪一个VPRN，对于静态链路（如，ATM VCC），这个消息必须配置进边缘路由器，由于边缘路由器不能由自身推断这样的绑定，让SNMP MIB允许本地桩链路和VPN身份之间的绑定不失为一个解决方法。

对于用户来说，动态地连接在网络上（用PPP或者自发隧道），可以把桩链路和VPRN关联，作为终端用户认证处理的一部分，例如用户所要绑定的VPRN可以继承PPP认证处理的域名。如果用户成功的通过认证（如，用Radius服务器），新创建的动态链路可以绑定到正确的VPRN上，注意，静态的配置信息仍然是必要的，如为了维护每个VPRN的授权用户表。但是静态信息的位置可以是认证服务器，而不是ISP的边缘路由器，不论链路是静态创建还是动态创建，VPN-ID都可以关联到那条链路上，标识绑定的VPRN。

知道了哪条桩链路绑定在哪个VPRN上之后，每个边缘路由器必须学习每个边缘路由器支持桩链路的身份，或者至少是可以到达它们的路由。后者暗示了这样一个概念，那就是当前的配置边缘路由器所使用的机制，可以用边缘路由器和桩链路身份信息建立合适的隧道。边

缘路由器的VPRN成员资格发布问题，可以通过不同的途径解决，将在后面讨论。

5.3.2.1 目录查找

特定VPRN的成员，即支持桩链路的边缘路由器身份，以及每个边缘路由器绑定在这个VPRN的静态桩链路集，可以配置进一个目录，通过在启动时定义某些机制（如，LDAP），边缘路由器可以查询它。

使用目录允许配置全网拓扑或者随机拓扑，对于全网拓扑，VPRN中所有路由器成员表发布到任何地方，对于一个随机拓扑，不同的路由器可能收到不同的成员表。

使用目录也可以使认证校验优先于VPRN成员信息的发布，当VPRN跨过几个管理域时，这就非常有必要了。这种情况下，目录到目录的协议机制可以在多管理域系统中传播授权的VPRN成员信息。

为了让所有的边缘路由器知道插入进激活VPRN的每一个新配置站点的身份，以及原有站点从VPRN中的移出，需要某种数据库形式的同步机制（如，触发目录查询，信息更新）。

5.3.2.2 显式管理配置

一个VPRN MIB定义为，允许一个管理系统把每个参与的边缘路由器的身份、每个静态桩链路的身份配置每个边缘路由器。就象使用目录一样，这种机制允许全网配置和随机配置。另一种机制是用一个中心管理系统，通过策略服务器和COPS协议【35】发布VPRN成员和策略信息，如建立隧道时使用隧道属性，如【36】所述。

注意，这个机制允许管理站加强严格的认证控制，另一方面，在管理域之外配置边缘路由器却十分困难，管理配置模型可作为一个目录方法子集，这样管理目录可以用MIB把VPRN信息压到参与的边缘路由器中，可以作为本地桩链路配置过程的结果或部分结果。

5.3.2.3 路由协议背载操作

VPRN成员信息背载到边缘路由器在IP骨干网上运行的路由协议中，因为这是一种通过网络向其他参与的边缘路由器传播信息的有效手段。特别是，每个边缘路由器的路由通告可以包含关联于每个边缘路由器VPN标识符集，以便让另一个边缘路由器确定特定边缘路由器身份和路由的足够信息。其他边缘路由器将检查接收到路由通告，确定是否包含了支持VPRN的相关信息，可以通过查找匹配于本地配置VPN的VPN标识符来完成。背载信息的特性、相关的问题（如范围）以及节点广播特定VPN成员资格的方法将会得到确定，都将是路由协议和基础传输的功能。

使用这种方法，网络中所有的路由器都将拥有VPRN成员信息的相同视图，可以很容易的支持全网拓扑，然而，要支持一个随机拓扑却比较困难的，需要某些形式的剪除。

背载方案的好处在于它有效的信息发布能力，但是它要求不仅仅参与到边缘路由器上的节点，而是通道上所有的节点，都要接受修改的路由广播，这样做的不好之处在于，这可能要求复杂的配置范围机制，既能允许又能限制背载广播，这会加重配置负担，特别是如果VPRN跨越几个路由域（如，不同自治系统、ISP）。

另外，除非为路由更新使用某些安全机制，允许所有相关的路由器读取背载广播，否则，只能由这个方案隐含一种信任模型，所有的路由器必须绝对地被授权知道这个信息。根据路由协议的特性，背载也要求中间路由器，特别是自治系统边缘路由器高速地缓冲这些广播，也要求多路由协议之间重发布他们。

每个方案都在特定场合下有它们自身的优点，注意在实际中，几乎总是有中心目录或者管理系统来维护VPRN成员信息，如允许支持一个特定VPRN的边缘路由器集，支持静态桩链路

到VPRN的绑定，支持通过动态链路为用户接入网络的认证和授权信息。这些信息需要配置存储在某种形式的数据库中，因此也需要额外的步骤方便这种信息到边缘路由器的配置，可能不是特别繁重。

5.3.3 桩链路可达性信息

桩站点可达性有两个方面——VPRN边缘路由器确定VPRN地址集和地址前缀可达桩站点的手段，以及CPE路由器通过桩链路学习目的地可达性的手段。无论是那一种情况，ISP边缘路由器需要的信息都是一样的——VPRN在客户站点的可达地址，但是CPE路由器需要的信息各异。

5.3.3.1 桩链路连接的不同情况

5.3.3.1.1 双 VPRN 和 Internet 连接

CPE路由器通过一条链路连接到ISP边缘路由器，得到VPRN和Internet连接的服务。这对于CPE路由器是最简单的情况，它仅仅需要一个到ISP边缘路由器缺省的路由点。

5.3.3.1.2 VPRN 连接

CPE通过一条链路连接到ISP边缘路由器，仅仅得到VPRN连接，而不是Internet。

CPE路由器必须知道通过那条链路可达的非本地VPRN目的地集，可能是一个简单的前缀，也可能是一系列的非结合前缀。CPE路由器可以是静态配置，也可以通过IGP动态学习，为了简单，假定用于IGP的是RIP，其实也可以是其他IGP。ISP边缘路由器将插入VPRN路由RIP的实例，该实例就是通过5.3.4描述的内联VPRN可达性机制学习获得的。注意运行载CPE的RIP实例以及任何用于学习内联VPRN可达性（甚至RIP）的路由协议实例都是独立的，由ISP边缘路由器从一个实例把路由重发布到另一个边缘路由器。

5.3.3.1.3 多宿连接

CPE路由器对于ISP网络来说是多宿的，提供VPRN连接性。

这种情况下，所有的ISP边缘路由器可以把相同的VPRN路由广播到CPE路由器，后者便可以通过所有链路认知所有可达VPRN前缀。当然还有其他特殊的重发布，ISP边缘路由器对CPE路由器广播不同的前缀集。

5.3.3.1.4 后门连接

CPE路由器连接到ISP网络上，后者提供VPRN连接，但也可以由一个后门链接直接通往客户站点。

这种情况下，ISP边缘路由器将广播VPRN路由到CPE设备上。然而现在相同的目的地是如何通过ISP边缘路由器和后门链接达到的呢？如果连接到后门链路上的CPE路由器运行了客户IGP，那么后门链路总是作为优先链路，就像一个内部链路一样，而通过ISP边缘路由器插入的目的地就好像是外部通道（对于客户IGP来说），为了避免这种情况，假设客户希望自己的数据流量通过ISP网络，就需要一个独立的RIP运行在后门链路两端的CPE路由器上，就如RIP运行在桩链路或者备份链路（在CPE路由器和ISP边缘路由器之间）一样，这便使得后门链路像向外部通路一样，通过适当调整该链路的费用，ISP通道可以总是可以优先，除非它关闭，后门链路才启用。

上面就等于描述了ISP边缘路由器和CPE路由器各自的可达性信息要求，以及传送这些信息的机制。下面的小节将详细介绍这些机制。

5.3.3.2 路由协议实例

路由协议可以运行在CPE边缘路由器和ISP边缘路由器之间，交换可达性信息，这样可以使ISP边缘路由器在客户站点学习可达VPRN前缀，以及让CPE路由器通过业务提供商网络学习可达目的地。

虽然客户也运行相同的协议，就像它的IGP，但是这个协议路由域的只扩展到ISP边缘路由器和CPE路由器，域可以扩展到客户站点，如果客户站点正在运行一个不同的路由协议，CPE在ISP边缘路由器实例和客户站点实例之间重发布路由。

考虑到这个路由实例的限制，一个简单的协议就足够了，RIP可能是最普通的协议，其他也可，如OSPF或者BGP运行在内部模式（IBGP）。

注意桩链路路由协议的实例是不同于内联VPRN可达性路由协议实例的，例如，如果ISP边缘路由器用路由协议负载操作，通过内核发布VPRN成员资格和可达性信息，那么它就可以由CPE路由实例到核心路由协议实例重发布合适标签的路由，用于每个实例的路协议弱化了，任何合适的协议可以用在每个场合。不需要相同的协议，甚至不需要相同的桩链路可达性信息收集机制，不需要它运行在CPE路由器和某一VPRN关联的ISP边缘路由器之间，因为这纯粹是本地事务。

这种弱化允许ISP使用一种普通的内联VPRN机制，通过这些机制，各个VPRN互相隔离，也隔离于客户网络的IGP。在第一种情况中，ISP可以不和桩链路操作，就能获得和内联VPRN可达性机制的隔离；第二种情况，ISP不需要知道客户站点的IGP。还有其他一些情况，如ISP边缘路由器和客户站点运行相同的IGP，但这很不实际，因为这样便失去了VPRN简化CPE路由器配置的目的。如果要让客户在多站点上运行IGP，VPLS方案比较合适。

注意，如果某一客户站点同时属于几个VPRN（或者希望同时与VPRN和Internet通信），ISP边缘路由器必须映射桩链路地址前缀到特定的VPRN。简单一点，可以在每个VPRN中使用多条桩链路，通过确保（或者，通过配置ISP边缘路由器，使其知道）某一非结合的地址前缀映射到单个的VPRN，或者由用合适的VPN标识标记来自于CPE路由器的路由广播，从而可以在同一条桩链路上运行多个VPRN。如，MPLS传送桩链路可达性信息，不同的MPLS标记将用来区别不同的VPRN所分配的前缀。不论如何，这种协同都需要一些管理规程。

5.3.3.3 配置

跨过每一个桩链路的可达性信息可以手工配置，当地址集和前缀集很小或者为静态时比较合适。

5.3.3.4 ISP 管理的地址

每一个桩站点的地址集可以由VPRN的边缘路由器管理和分配，当客户站点比较小的时候比较合适，特别是包含单主机或者单子集。地址分配可以由PPP或者DHCP【37】来完成，如，边缘路由器作为一个Radius客户，检索客户IP地址，或者作为一个DHCP中继，检查DHCP消息，中继给客户站点，这时的边缘路由器需要建立桩链路可达性信息表。虽然这些IP地址分配机制一般用于分配给单个的主机，一些销售商加了一些扩展，使其可以分配地址前缀。在某些情况下，让CPE设备可以作为一个小型DHCP服务器，在客户站点为主机分配地址。

注意在这些方案下，地址分配服务器有责任保证VPN的每个站点收到不同的地址空间，也要注意，ISP通常只为小的桩站点使用这种机制，小站点不太可能有后门链路。

5.3.3.5 MPLS LDP

CPE路由器运行MPLS时，LDP可以在桩站点传送前缀集给VPRN边缘路由器。用下行标记发布的主动模式，CPE可以从头站点的每个路由器发布一个标记。然而需要注意的是，由于是LDP学习新路由，而不是从存在的路由器学习标记——通过标准路由机制学习，边缘路由器执行的处理就不仅仅是普通的LDP处理过程。

5.3.4 内联VPN可达性信息

一旦边缘路由器确定了联结每个桩链路的前缀集，这个信息便必须马上发布到每个边缘路由器。这里也有一个隐含的要求，那就是可达地址集本地唯一，也就是说，每个VPRN桩链路（不执行负载共享）维护与任何其他地址空间无关的一个地址空间。实际中虽然不是要求这样，但至少希望这样，这个地址空间要很好的分割开，如，每个边缘路由器用一个特殊的地址前缀，以便消除维护发布大数量主机路由的必要。

内联VPN可达性信息的发布可以通过许多途径解决，下面将分别叙述一下它们其中的几个。

5.3.4.1 直接查找

和VPRN成员信息一起，中心目录可以维护连接每一个客户站点的地址前缀列表，这样的信息可以由服务器通过边缘路由器协议的交互作用获得，注意5.3.2讨论到的目录同步问题也可以应用在这个场合。

5.3.4.2 显式配置

地址空间可以显式配置，但是这样不容易升级，特别是当使用随机拓扑时，同时这也提出了管理系统如何学习这些信息的问题。

5.3.4.3 本地内联 VPRN 路由实例化

在这种方法中，每个边缘路由器运行一个路由协议（一个“虚路由”）的实例，通过VPRN隧道到每个对端边缘路由器，发布内联VPRN可达性信息。由于路由协议自身可以运行在任何拓扑上，全网拓扑和随机拓扑都可以很容易的得到支持。内联VPRN路由广播可能不同于普通的隧道数据包，它可以直接定址对端边缘路由器，或者使用隧道特殊机制。

注意这里的内联VPRN路由协议可以和任何客户站点的IGP协议以及ISP在IP骨干网的其他路由协议不发生任何关系。根据VPRN尺寸的大小和规模，不论是简单的RIP协议还是复杂的OSPF协议都可以使用。由于内联VPRN路由协议运行在IP骨干网之上，对于任何中间路由器完全透明，对于不在VPRN内的任何其他边缘路由器也完全透明，这也暗示了这样的路由信息可以对这样的路由器保持不透明，在一些场合下这提供了必要的安全要求。也要注意，如果路由协议象数据一样直接运行在同一个隧道上，那么它和数据流量有同等水平的安全，例如强加密或者认证。

如果内联VPRN路由协议所运行的隧道对于特定VPN（如，一个不同的复接域）是专用的，那么就不需要改变路由协议自身；另一方面，如果使用了共享隧道，那么就很有必要扩展路由协议，以允许VPN-ID包含在路由更新包中，允许前缀集连接到特定的VPN上。

5.3.4.4 链路可达性协议

链路可达性协议就是允许两个节点通过点到点链路连接，相互交换可达性信息，对于全网拓扑，每个边缘路由器可以运行链路可达性协议，例如MPLS CR-LDP的一些变种，通过隧

道到每个对端边缘路由器，在两个边缘路由器之间通过隧道运载VPN-ID和可达性信息。如果VPRN成员信息已经发布到边缘路由器，那么就不再需要传统的邻路由发现协议，因为邻节点集已经知道了。TCP连接可以用来互联邻接点，提供可达性。这个方法可以减少每个VPRN的路由协议实例的处理负担，可以支持多VPRN使用共享隧道机制连接边缘路由器时。

另一个链路可达性协议的方法可以基于IBGP，这时链路可达性协议需要解决的问题与IBGP非常相似——在边缘路由器之间可靠传送地址前缀。

用链路可达性协议可以直接支持全网拓扑——每个边缘路由器传送它的本地可达性信息到其他所有的路由器上，但是却决不把从其他路由器接收来的信息重发布。然而，一旦需要支持随机拓扑，链路可达性协议需要开发成一个全路由协议，由于需要避免死环，重新发明一种路由协议没有什么好处。为什么在一个隧道环境中也需要部分连接网已经在5.1.1中讨论过。

5.3.4.5 IP 骨干网路由协议的背载操作

VPRN成员资格和关联于每个头接口的地址前缀也背载在从每个边缘路由器的路由广播和网络的传播中。其他路由器就像它们获得VPRN成员资格信息那样（隐含在每个路由广播源的标识中）抽取该信息。注意，由于所设计路由协议的特性，这个方案可能要求中间路由器——如边缘路由器，缓存内联VPRN路由信息，以便重发；同时，这也隐含了安全要求，提出了内联VPRN路由信息可能的安全水平。

注意，上面所说的任何情况，边缘路由器都要以某种方式发布桩链路前缀，以允许从远端边缘路由器直接流出桩链路的隧道传输。它也可以发布这些信息，以便让边缘路由器关联所有的前缀，而不是特定的桩链路。这种情况下，边缘路由器需要实现一个VPN特殊转发机制以导出流量，确定正确的桩链路。这样做的一个好处就是可以很大程度上减少不同隧道的数目以及需要创建和维护隧道的标签信息。注意，这个选择只是本地事件，对于远端边缘路由器是不可见的。

5.3.5 隧道机制

一旦VPRN成员资格信息得到发布，包含VPRN内核的隧道就可以构建了。

建立隧道网的一种方法是用点到点IP隧道，这种隧道的要求和存在的问题已经在3.0节中讨论过了，例如，虽然隧道的建立可以通过手工配置，但是却不容易升级（数量级 $O(n^2)$ ）。象这样的话，隧道的建立需要用某些形式的信令协议，以允许两个节点构建隧道，能够知道双方的身份。

另一种方法是用多点到点的隧道，如MPLS。如【38】所提到的，MPLS可以视为某种形式的IP隧道，由于MPLS包的标记允许路由，弱化了数据包本身地址信息的作用。MPLS标记发布机制可以用来关联MPLS标记集和出口点（如桩链路和边缘路由器）的VPRN地址前缀，因而允许其他路由器显式地标记和路由，把流量导向特定的VPRN头链路。

MPLS的引人之处在于，作为一种隧道机制，它仅仅要求很少的处理，这主要是因为MPLS网络的数据安全隐含在显式的标记绑定中，而不象面向网络的连接，如帧中继。因而使得用户不必为数据安全的处理做过多考虑，比如IPSec。然而，MPLS却有其他潜在的安全问题，它没有直接的认证、机密性和完整性这样的安全特性，MPLS的信任模型意味着需要通过中间路由器，（可能属于不同管理域）来传送成员资格和前缀可达性信息，因而中间路由器必须得到信任，而不仅是边缘路由器本身。

5.4 多宿主路由器

这里假定桩路由器仅仅连在一个VPRN边缘路由器，总起说来，如果市场因为可靠性或者其他原因，这个限制可以减少VPRN操作。特别是如果桩路由器支持多宿主冗余链路，一次只有一个运行，链路连在同一个VPRN边缘路由器上，或者两个或多个不同VPRN边缘路由器上，那么桩链路可达性机制既要能够发现活动链路的丢失，又要主要备份链路的活动。在前一种情况，前一个连接的VPRN边缘路由器将停止广播可达性信息，而带有活动链路的VPRN边缘路由器将开始广播可达性，然后存储连接。

另一种可能的情况是，桩节点使用某些形式地负载共享算法，支持多活动链路，这样，多个VPRN边缘路由器便可能有几条活动通道，从而可以通过VPRN广播。如果内联VPRN可达性机制可以提供多通道到相同的前缀，并且有适当的机制避免死锁——如，为每个广播前缀关联一个距离向量矩阵，这种方式不会造成可达性的任何问题，

5.5 多播支持

多播和广播包括两种，一是在VPRN上通过骨干网边缘复制，二是本地多播支持。下面讨论这两种情况。

5.5.1 边缘复制

VPRN边缘路由器在VPRN的每条链路上复制多播数据，这种操作与CPE路由器终止物理链路或专线的操作相同。对于CPE路由器，多播路由协议可以运行在每个VPRN边缘路由器，以确定多播流量的发布树，进而减少泛播的必要性。可以由标准多播路由协议实例运行来实现，如PIM【39】或者DVMRP【40】，在每个边缘路由器上或者它们之间，通过VPRN隧道，与内联VPN单播可达性路由协议一样，如5.3.4所述。还可以这样，如果一各链路可达性协议运行在VPRN隧道上，那么就让VPRN边缘路由器既指示特定多播组，又支持多播源。

无论那种情况，都必须有某些机制让VPRN边缘路由器确定站点要求哪个多播组、那个多播源，如何实现这个功能是每个站点CPE桩路由器的事情。如果运行多播路由协议，那么它们可以和等同的协议在每个VPRN边缘路由器直接交互，然后在缺少IGMP代理【41】的情况下，客户站点将通过桥设备把到VPRN边缘路由器的连接限制在一个子集，然而，使用IGMP代理，CPE路由器可以不必运行多播路由协议就能完成转发多播转发。在客户站点的接口处，CPE路由器执行IGMP路由功能，在VPRN边缘路由器的接口处，执行IGMP主机功能。

5.5.2 本地多播支持

这是指，VPRN边缘路由器映射内联VPRN多播流量到本地IP多播发布机制。注意，内联VPRN多播同骨干网的内联VPRN单播有相同的要求。目前，具有多播本地支持的IP隧道机制只有MPLS。另一方面，在MPLS支持IP多播包的本地传输时，将需要额外的机制来支持内联VPRN多播。

例如，每个VPRN路由器可以为多播组地址加前缀，然后重发布，其实就是把VPN-ID/内联VPRN多播地址组作为普通的多播地址，用在骨干多播路由协议上。MPLS多播标记发布机制可以用来建立合适的多播LSP，互联VPRN支持多播组地址的站点。然而需要注意的是，这要求每个中间LSR不仅要知道每个内联VPRN多播地址，而且也要具有解释修改的广播的能力。

另外，也可以定义映射内联VPRN多播地址到骨干多播组的机制。

其他的IP隧道机制没有本地多播支持，这可以通过把IP多播组地址作为一个整体分配给VPRN来实现，此时将在骨干多播数据包上封装内联VPRN多播数据，边缘VPRN路由器可以过滤出不想要的多播组。还有一种情况是，也可以定义一种机制，为特定内联VPRN多播组分配骨干多播组地址，通过骨干多播协议，把内联多播数据限定在组的节点上。

使用本地多播支持的问题就在于这些多播数据的安全性，边缘复制集成了基础隧道的安全特性，而本地多播不同于边缘复制，它将需要某些特殊形式的安全多播机制。安全多播解决方案的开发是一个非常活跃的领域，见【42】和【43】，安全多播组（SMuG），IRTF，都已经建立了解决方案的开发模型，然后将通过IETF IPsec工作组来标准化。

5.6 建议

支持VPRN功能的建议大体可以分为两大类——一是使用路由背载方法发布VPN成员资格和可达性信息（【13】，【15】），二是使用虚路由方法（【12】，【14】）。许多情况下，协议的机制依赖于特定基础结构的特性（如，MPLS），而仅仅是IP。

在虚路由方法的场景中，基于目录或者MIB开发成员资格发布协议很有用处，当和3.2所述的IP隧道协议扩展结合时，便可以提供一个完全的协议集和运作机制，支持IP骨干网上横跨几个管理域的可操作的VPRN，当然还需要其他的功能——学习发布客户可达性信息，这可以由标准路由协议实例执行，而不需要任何协议扩展。

因为全网拓扑的限制，需要考虑一下链路可达性协议开发的用处，如果标准路由可以工作的话，全网拓扑的限制和升级问题可能使得开发工作不太值。

也需要考虑扩展路由协议，以便在路由更新包中传送VPN-ID，但是如果使用了VPN专用隧道，这就不太需要了。

6.0 VPN 类型：虚拟专用拨号网

VPDN允许一个远端用户可以通过ad hoc隧道按需地接入到另外一个站点。用户通过拨号PSTN或者ISDN链路连接到公共IP网络上，用户数据包通过公众网络隧道传输到所要到达的站点，对用户来说就好像直接连接到那个站点，这种ad hoc连接的一个关键特性就是需要为用户认证，因为任何用户可能通过交换拨号网络接入这样的站点。

现在许多公司网络允许远端用户通过PSTN接入，让用户建立通过接入网到网络接入服务器的PPP连接，在接入服务器上PPP会话使用AAA系统（如，RADIUS【44】）认证，由于这种系统已经非常普遍采用，VPDN系统必须能够对这些已有系统透明复用。

IETF开发了L2TP【8】，使用户的PPP会话能够从L2TP LAC传输到远端L2TP LNS，L2TP依赖于它以前两个协议，即L2F【45】和PPTP【46】，这也恰好反映了L2TP的两种不同的应用方法——强制隧道和自发隧道，在下面的6.2和6.3节中将进一步讨论。

本文的重点在于L2TP over IP（用UDP），其实L2TP还可以直接运行在其他协议上，如ATM和FR，对于L2TP运行在非IP网络上的问题，如非IP隧道安全的保证等，在本文不作叙述。

6.1 L2TP 协议特性

本节用3.0的分类方法来看一下L2TP隧道协议的特性。

6.1.1 复接

L2TP支持复接,可以在一个单独的链路上复接不同用户的呼叫,也就是在同两个IP端点上,可以有多个L2TP隧道,由Tunnel ID来标识,在一条隧道上可以复接许多个会话,由Session ID来标识。

6.1.2 信令

由内建控制连接协议来支持,允许隧道和会话的动态建立。

6.1.3 数据安全性

通过允许PPP从用户通过LAC到LNS的透明伸展,使用普通的PPP连接,L2TP对连接建立数据传输都允许使用任何形式的安全机制。然而这没有对L2TP控制协议本身提供安全,L2TP可以进一步与IP骨干网的IPSec或者非IP骨干网的其他一些相关机制结合来实现隧道安全。

L2TP和AAA系统为用户认证和授权的交互作用是L2TP所拥有的特别功能,是支持LAC和LNS设备的本质所在,在【50】中有对这一问题的详细讨论。

主机如何连接到正确的LAC,以及LAC如何确定那个用户所连接的隧道、LNS和每个用户如何协商参数等,都已经超过了VPDN的操作范围,可以由像发展Internet漫游规范【51】那样来解决它。

6.1.4 多协议传输

L2TP传输PPP包(仅仅PPP包),PPP本身可以传输多协议。

6.1.5 序列

L2TP支持包的序列传送,这是一种可以在会话建立时协商的能力,可以由LNS在会话期间打开或者关闭,L2TP的序列号域也可以用来提供丢失包指示,许多PPP压缩算法的运作都需要这项功能。如果没有使用压缩,LNS确信使用(由PPP NCP协商显示)中的协议能够处理序列包(如IP),序列可以禁止。

6.1.6 隧道维护

L2TP使用了一种保持存活协议,能够区分隧道超时和隧道非活动状态时间的延长。

6.1.7 MTU 问题

L2TP本身没有拆装支持,但是运行在UDP/IP上,IP拆分可以在需要时启用。注意如果知道LAC和LNS通道上的MTU,LAC和LNS可以调整PPP协商的MRU以消除拆分,后来就有了L2TP隧

道传输IP帧的MTU发现建议【52】。

6.1.8 隧道开销

L2TP运行在IP网络上时,要在UDP上传输PPP数据,导致了很大的开销,不仅仅存在于UDP、L2TP和PPP头的数据平面里,而且存在于L2TP和PPP控制平面里,这在6.3节里将进一步讨论。

6.1.9 流量和拥塞控制

L2TP为控制协议支持流量和拥塞控制,但是不为数据传输协议提供支持,详见3.1.9。

6.1.10 QoS/流量管理

L2TP头包含1比特的优先级域,可以为在本地排队和传输中需要优先处理(如,保持存活)的数据包设立;也可以通过透明扩展PPP,让L2TP支持如多链路PPP【53】和联合控制协议【54】的PPP机制,来按需满足用户要求的带宽。

另外,L2TP呼叫可以映射到任何拥有的基础流量管理机制的网络中,有建议允许通过L2TP信令实现请求特种业务行为【55】。

6.1.11 其他

由于L2TP透明传输扩展PPP,它不打算代替PPP提供的普通地址分配机制,因此,发起PPP会话的主机将由LNS按PPP规程分配地址,这个地址与LAC和LNS的地址无关,LNS也要支持远端主机数据路由所需的任何形式的转发机制。

6.2 强制隧道

强制隧道是指这种情况:一个网络节点——如拨号服务器或者网络接入服务器,作为LAC,把PPP会话通过骨干网伸展到远端LNS,如下图示。这对于向LAC发起PPP会话的用户来说是透明的,终止拨号呼叫的modem池的位置和拥有权不再那么重要,因为通常都是从站点到modem用户提供接入。这正是L2F规范的所支持一种情形情况,L2TP规范基于此保留了这项支持。

强制隧道有许多应用场合,如下图所示,用户主机拨入NAS,NAS作为一个LAC,通过IP网络(如Internet)隧道连接到一个LNS网关,网关提供到公司网络的接入,可以是公司网络自身,也可以是ISP边缘路由器——用户把LNS功能的维护包给了ISP。还有一种情况是ISP用L2TP提供用户接入Internet,用户主机拨入NAS(作为LAC),通过一个接入网接入到ISP边缘路由器(用作LNS),ISP边缘路由器将用户数据流量馈送到Internet上。再者,就是ISP用L2TP提供用户接入VPRN,或者同时提供VPRN接入和Internet接入。

VPDN,不论是用强制隧道还是自发隧道,都可以视为一种用户数据接入方法,从而提供不同类型网络的接入,如,公司网络、Internet或者VPRN,接入VPRN也就实现了这样一个实例,那就是结合不同类型的VPN为用户提供VPN业务。

10.0.0.1

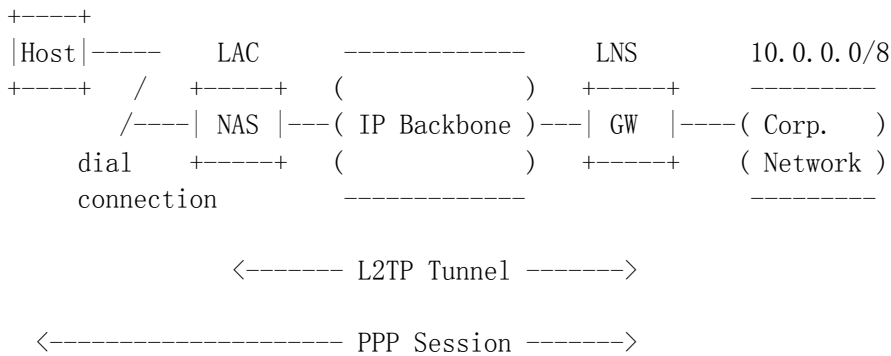


Figure 6.1: Compulsory Tunneling Example

强制隧道起先是要让网络接入服务器支持批发拨入业务，允许远端拨号接入通过普通的设施接入到一个企业站点，而企业不需要使用它自己的拨入服务器。另一个例子是，ISP把自己的拨入连接卖给接入网络提供商（如本地交换载波），ISP不必再维护自己的拨号服务器，这样做的好处还在于可以允许LEC服务于多个ISP。最近，也有人建议发展DSL强制隧道【56】，【57】，寻求对现存AAA结构的充分利用。

强制隧道的呼叫路由要求允许LAC确定LNS的身份的一些PPP建立的特征，如【50】所注，包括用户身份——通过接入网络的某些方面确定，包括呼叫方号码，或者还包括被叫方的一些属性——如PPP认证期间的身份声明FQDN等。

将两个L2TP隧道拴在一起也是可能的，如，一个LAC发起一个隧道到中继设备，该中继设备作为第一LAC的LNS，同时是后一个LNS的LAC，其实这就是某种程度的隧道串连，当在接入网提供商、IP骨干网提供商和企业用户之间划分管理、组织和调整责任时，往往需要这种隧道串连。

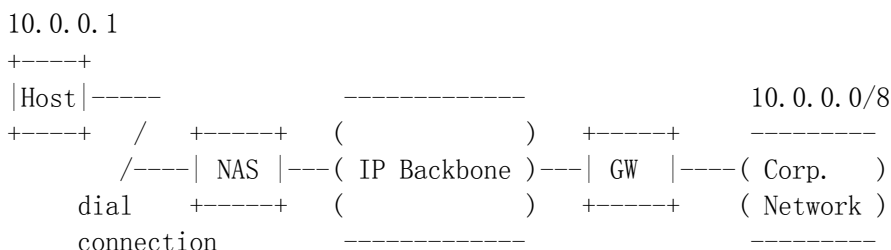
6.3 自发隧道

自发隧道是指这种情况，一个主机通过本主机发起的隧道连接远端站点，不需要中间网络站点的介入，如下图所示，PPTP规范是基于自发隧道模型的，L2TP集成了PPTP的一部分。

就像强制隧道一样，它也有许多不同的应用场合，下图示意的是用户用L2TP或者IPSec作为自发隧道机制接入一个公司网络。另一种场合是使用自发隧道为用户接入VPRN。

6.3.1 L2TP 自发隧道的问题

L2TP规范支持自发隧道，LAC可以位于主机之上，当然也可以是一个网络节点，注意，这样的主机有两个IP地址——一个是为LAC—LNS IP隧道的IP地址，一个是通过PPP获得的，是为该主机接入到它所连接的网络的IP地址。L2TP自发隧道的好处是PPP的认证和地址分配机制可以重利用，如，一个LNS可以包含一个Radius客户，与Radius服务器通信，认证PPP PAP或者进行CHAP交换，为主机检索配置信息，如IP地址，以及用到的DNS服务器列表等，然后这些信息可以通过PPP IPCP协议送到主机上。



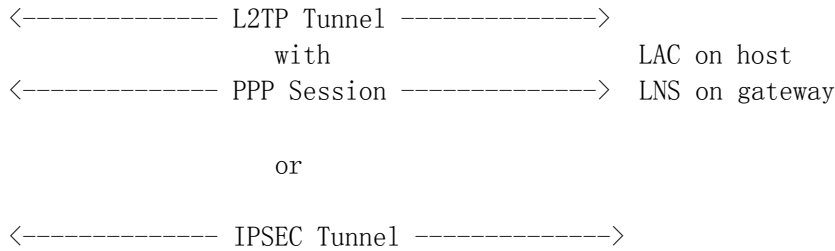


Figure 6.2: Voluntary Tunneling Example

上面的规程并不是没有成本问题，这样的协议栈需要考虑开销问题，特别是为了安全使用了IPSec时，而主机又是通过低带宽拨入链路连接，此时开销显得十分重要。开销中包含了额外的头，无论是在数据平面上，还是再控制平面上，用L2TP发起自发隧道，用IPSec来保障安全，意味着Web应用将工作在如下的协议栈上：

HTTP/TCP/IP/PPP/L2TP/UDP/ESP/IP/PPP/AHDLC

在【58】中建议IPSec单独使用，减少开销，用下面的协议栈：

HTTP/TCP/IP/ESP/IP/PPP/AHDLC

这种情况下，IPSec工作于隧道模式下，隧道终止在企业站点的IPSec边缘设备上，或者连接企业站点的提供者边缘路由器上。主机的IP地址有两种可能性，其一，用两个IP地址，就像L2TP一样；其二，主机用一个公用的IP地址作为源地址，无论是内部IP头还是外部IP头，都由网关在向企业网转发数据时执行NAT，对于企业网的其他主机来说，该主机好像有一个“内部”IP地址。使用NAT有一些限制，在【58】也有说明。

PPP还有一个潜在问题是通过L2TP隧道在IP骨干网上实现链路层的特性与在串行线上的链路层很不相同，就如L2TP规范本身所讨论的那样。如，选择PPP参数不慎会导致频繁地重新启动和超时，特别是使用了压缩操作之后。这是因为L2TP隧道可能弄乱了数据包，也可能静丢弃，而这二者在串行线路中都不会发生。数据包的丢失率很大程度上也受网络拥塞的影响，L2TP头使用序列号时可以解决错序问题，当LAC和LNS同时和PPP端点一致时，如自发隧道，序列号域可以用来检测丢包情况，给压缩实体传送适当的指示，而这一般都要要求这种信息以保持两端同步的压缩记录。（事实上，这对强制隧道更是一个问题，因为LAC可能故意地损坏PPP主机的帧，再给出丢包指示。一些硬件不允许这样。）

6.3.2 IPSec自发隧道的问题

如果自发隧道由IPSec实现，L2TP通过PPP所获得的用户认证和主机配置功能仍然需要承载，需要区别在于用户认证和机器认证，“二因素”认证基于用户所共同拥有的东西实现，如数字签名的机器或者信用卡，或者其他用户知道的东西，如口令。（还有一个例子就是从ATM机上取款——需要卡号和PIN号。）许多已有的用户认证系统都有着天然的不对称性，不被IKE支持。对于远端接入，最常用的用户认证机制就是使用PPP协议（用户和接入服务器之间）和Radius（接入服务器和认证服务器之间）。发生在这种场合的认证交换，如PAP或者CHAP交换，都是不对称的。CHAP也支持重认证，当会话已经建立了一段时间之后，重认证可以保证当前用户仍然是发起会话的同一人。

而IKE支持机器认证，它只有很少的一点用户认证功能，并且根本就没有不对称认证功能。虽然用户口令可以衍生出一个与共享密钥，然而这缺不能用于远端接入环境的IKE主模式，用户将不能拥有一个固定IP地址，野蛮模式下可以使用，可以不提供身份保护。后来已经有了许多支持不对称用户水平认真的IPSec方案，【59】定义了一种新的IKE消息交换——交易交换——它允许请求/应答和设立/认可消息序列，也定义了客户IP栈可以使用的属性。

【60】和【61】描述了交易消息交换、或者一系列这样的交换的机制，执行用户认证。【62】描述的是另一种方法，这种方法没有扩展IKE协议本身，用这种方法用户和安全网关建立阶段1 SA，然后再建立阶段2 SA到王国，在其上运行当前的认证协议，网关扮演了代理的角色，中继协议消息到认证服务器。

另外，也有一些协议允许远端主机在IPSec上配置IP地址和其他信息，如【63】，它描

述的方法是，远端首先和安全网关建立阶段1 SA，然后建立阶段2 SA到网关，在其上运行DHCP协议，网关扮演了代理的角色，中继协议消息到DHCP服务器。同样，像【62】，该协议不包括IKE协议自身的扩展。

PPP的另一个特性就是支持多协议操作，可以在运载其他的网络层协议，而不仅仅是IP；甚至运载链路层协议（如，Ethernet），支持IPSec上的桥。参见3.1.4。

在远端接入环境重支持用户认证和主机配置能力的方法现正由IPSec工作组讨论。

6.4 网络主机支持

当前的PPP拨号网络模型假定主机直接连接到一个拨号接入网络上，现在的一些工作如DSL似乎要复制这个模型【57】，以便允许AAA系统的重利用，家庭或者小型公司的个人计算机、打印机和其他一些网络应用却冲击着这种直接连接的主机模型，慢慢地，大多数地主机将通过小型的以太网、本地区域网接入Internet。

因此必须让业务提供商现有的AAA结构也能够支持每个客户站点的多网络主机。这种情况主要的复杂性在于对登录对话的支持，通过它交换适当的AAA信息。有许多建议能够满足于此：

6.4.1 通过 L2TP 扩展 PPP 到主机

已经有好多建议（如，【56】）在Ethernet上扩展了L2TP，因此PPP会话可以从网络主机连接到网络上，就像直接连接似的。

6.4.2 PPP 直接扩展到主机

PPPoE【64】是一种映射PPP到Ethernet的规范，它使用广播机制让主机发现合适的接入服务器，服务器便根据需要用L2TP或其他类似机制建立隧道传输PPP会话。

6.4.3 使用 IPSec

上面讨论的基于IPSec的自发隧道既可以用在网络上，也可以用在直接连接的主机上。注意，所有这些方法都需要另外增加主机软件，以实现LAC、PPPoE或者IPSec客户功能。

6.5 建议

L2TP规范的制定已经结束，将广泛的应用于强制隧道，如3.2节所述，让IPSec为L2TP提供安全的定义一个特殊模式将会很有意义。

并且，对于IPSec自发隧道，完成下列工作的支持将会很有用处：

- 不对称/原用户认证（6.3）
- 主机地址分配和配置（6.3）

描述就基于此假定。

7.1.2 多播和广播支持

VPLS需要有广播能力，因为需要帧广播以及链路层泛播（flooding）——即一个单播帧因为到达链路层地址的目的地不清楚而进行的泛滥。在桥网络上用到的地址解析协议通常是广播帧（如，ARP），虽然太高频率的使用广播可能增加本地多播支持的压力，（例如，在VPLS边缘节点上的复制负担），先前VPRN中讨论的多播隧道机制集仍适用于VPLS。

7.1.3 VPLS 成员配置和拓扑

VPLS成员配置和VPRN的相似，由于在任何给定的VPLS边缘节点上都只要求本地VPN链路分配的信息，以及其他边缘节点的身份或路由，特别是，这样的配置独立于每个VPN边缘节点转发的自然特性，这样的话，任何为VPRN配置的VPN成员配置和发布机制都适用于VPLS配置。也类似于VPRN，VPLS的拓扑也可以通过控制VPLS边缘节点对端的配置来操纵，假定成员资格发布机制允许这样做的话。典型的VPLS很可能是全网拓扑，然而，为了消除两个VPLS节点通过另一个VPLS节点传输数据的需要，将会要求使用Spanning Tree协议防止环。

7.1.4 桩 CPE 节点类型

VPLS对桥CPE设备和路由器CPE设备都支持。

CPE路由器可以跨过VPLS相互之间透明，不需要任何其他的路由器和任何节点。VPRN应用在全网拓扑的升级问题在这里也适用，只不过对等点路由器现在可能数目要多一些，因为此时ISP边缘设备不再作为汇聚点。

在CPE桥设备中，广播域包含了所有的CPE站点，以及VPLS本身，由于数据包泛播的要求，以及桥域任何拓扑改变都不是本地化，这时会有很重要的升级限制，但是在整个域中是可见的，这样的话，这种场合通常只适用于非可路由协议的支持。

CPE的性质影响了封装、地址、转发和VPLS种可达性协议的性质，这将在后面分别讨论。

7.1.5 桩链路封装

7.1.5.1 桥 CPE

在这种情况下，通过桩链路的包是链路层帧，适合接入链路封装。最普通例子如以太网帧，用适合特定接入技术的封装，如ATM，连接CPE桥到VPLS边缘节点，这些帧然后在2层转发到VPLS的隧道，如前所述，这必须使用IP隧道协议，要求隧道能够传输链路层帧。然而需要注意，隧道包协议身份域的使用不是必需的，因为封装数据（如以太网帧）可以在隧道建立时得到指示。

7.1.5.2 路由器 CPE

这种情况下，CPE路由器通过桩链路传输链路层包，目的地是它们对端CPE路由器链路层

的地址。然而，由于VPLS需要的相关受限地址空间允许其他形式的封装，因此还有其他一些可行的封装方式，下面进一步讨论。

7.1.6 CPE 定址和地址解析

7.1.6.1 桥 CPE

由于VPLS工作在链路层，对于桥CPE，所有桩站点的所有主机，将在同一个网络层子集，（多网络，多个子集工作在同一个LAN片上，也是可能的，但是那不多见）。帧在VPLS上基于链路层地址转发——如，连接个人主机IEEE MAC地址。VPLS需要支持广播流量，如地址解析机制，映射网络地址到它们相应的链路层地址，VPLS转发和可达性算法也需要支持泛播流量。

7.1.6.2 路由器 CPE

一个网络层子集一般就是要通过一个VPLS互联路由器CPE设备，在每个CPE路由器之后是不同网络层子集的主机，CPE通过映射下一跳路由器的网络层地址到它相应的链路层地址，实现VPLS上的数据包传输。链路层封装，通常为以太网，如前面所述的桥。

如上所述，在所有连接到VPLS的CPE节点都是路由器的情况下，那么就有可能由于VPLS的受限地址空间，需要用不同地址控制而不是普通的MAC地址的封装方式。例如，【11】，VPLS over MPLS，仿照以前的VPRN over MPLS，把MPLS作为隧道机制，以本地分配标记作为链路层地址方案，标识连接到VPLS的CPE LSR路由器。

7.1.7 VPLS 边缘节点转发和可达性机制

7.1.7.1 桥 CPE

这种情况下，唯一比较实际的VPLS节点转发机制可能就是标准链路层泛播和MAC地址学习，如【65】。这样的话，虽然需要广播机制，但它却并不需要内联VPLS可达性协议。如果VPLS拓扑上任何节点不需要在任何其他的边缘节点之间转发数据，也就是说，实现了全网拓扑，根本就没有转发的必要，那么总的说来，也不需要VPLS节点之间实现Spanning Tree协议；另一方面，CPE桥最好实现Spanning Tree协议，以防止“后门”通道绕过VPLS连接。

7.1.7.2 路由器 CPE

这种情况也可以用标准桥技术，另外，由于VPLS的链路层地址空间较小，因此也可以利用其他一些技术实现在在CPE路由器之间的显式链路层路由上。例如【11】，建议在所有CPE LSR之间插入任何新的CPE路由器到VPLS时建立MPLS LSP，这样便不再需要包泛播。更一般的情况是，如果使用桩链路可达性机制为VPLS边缘节点配置链路层地址，那么任何上面为VPRN所讨论的任何内联—VPN可达性机制，经过修改都可以用来给每个VPLS边缘节点广播信息，这将允许不需要泛播就可以实现数据包再VPLS的转发。

可以开发一些机制，进一步从桩链路到CPE路由器广播链路层地址和相应的网络层地址，

这样的信息可以插入到CPE路由器的地址解析表中。这也可以消除在VPLS上广播地址解析协议的必要。

很明显，如果链路层路由由VPLS确定，那么就不需要支持spanning tree protocol。如果使用了泛播机制，spanning tree将仅仅在全网拓扑不可行时才需要，此时VPLS节点将不得不运载转发数据。

7.2 建议

VPRN和VPLS有很大的共性，可以减少开发和配置的复杂性，特别是，VPLS应该充分利用类似的隧道和成员配置机制，其改变之处只需反应VPLS的特性即可。

8.0 建议总结

本文分别讨论了不同类型的VPN，对于所有类型的VPN，它们有着许多共同的要求和机制，许多网络上将会同时包含多个不同类型的VPN，让不同类型的VPN尽可能有共同的特性很有好处，特别是，通过标准化相关的几个关键机制，便能够实现许多类型的VPN。

支持下列机制的好处值得好好考虑一下：

IKE/IPSec：

- 在SA建立时传输VPN-ID (3.1.2)
- NULL加密和NULL认证选项 (3.1.3)
- 多协议操作 (3.1.4)
- 帧序列 (3.1.5)
- 不对称/原用户认证 (6.3)
- 主机地址分配和配置 (6.3)

对于L2TP

- 定义支持L2TP时IPSec特殊操作模式 (3.2)。

对于通常意义上的VPN

- 定义VPN成员信息配置和发布机制，用了某些形式的目录或者MIB (5.3.2)
- 尽可能保证方案开发适用于不同类型的VPN，而不是只面向特定类型的VPN。

9.0 安全考虑

关于安全的考虑是VPN机制的一个重要集成部分，有关它的讨论在VPN机制描述的相应章节中已经有所阐述。

10.0 鸣谢

感谢北电的Anthony Alles，在本文的产生过程中，他为我们提供了太多的帮助，他所研究的许多东西是本文的早期版本的基础所在。也感谢Joel Halpern，谢谢他提出的见解和评论。

11.0 参考资料

- [1] ATM Forum “LAN Emulation over ATM 1.0”, af-lane-0021.000, January 1995.
- [2] ATM Forum. “Multi-Protocol Over ATM Specification v1.0”, af-mpoa-0087.000, June 1997.
- [3] Ferguson, P. and Huston, G. “What is a VPN?”, Revision 1, April 1 1998; <http://www.employees.org/~ferguson/vpn.pdf>.
- [4] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. and E. Lear, “Address Allocation for Private Internets”, BCP 5, RFC 1918, February 1996.
- [5] Kent, S. and R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, November 1998.
- [6] Perkins, C., “IP Encapsulation within IP”, RFC 2003, October 1996.
- [7] Hanks, S., Li, T., Farinacci, D. and P. Traina, “Generic Routing Encapsulation (GRE)”, RFC 1701, October 1994.
- [8] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Palter, “Layer Two Tunneling Protocol “L2TP””, RFC 2661, August 1999.
- [9] Rosen, E., et al., “Multiprotocol Label Switching Architecture”, Work in Progress.
- [10] Heinanen, J., et al., “MPLS Mappings of Generic VPN Mechanisms”, Work in Progress.
- [11] Jamieson, D., et al., “MPLS VPN Architecture”, Work in Progress.
- [12] Casey, L., et al., “IP VPN Realization using MPLS Tunnels”, Work in Progress.
- [13] Li, T. “CPE based VPNs using MPLS”, Work in Progress.
- [14] Muthukrishnan, K. and A. Malis, “Core MPLS IP VPN Architecture”, Work in Progress.
- [15] Rosen, E. and Y. Rekhter, “BGP/MPLS VPNs”, RFC 2547, March 1999.
- [16] Fox, B. and B. Gleeson, “Virtual Private Networks Identifier”, RFC 2685, September 1999.
- [17] Petri, B. (editor) “MPOA v1.1 Addendum on VPN support”, ATM Forum, af-mpoa-0129.000.

- [18] Harkins, D. and C. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
- [19] Calhoun, P., et al., "Tunnel Establishment Protocol", Work in Progress.
- [20] Andersson, L., et al., "LDP Specification", Work in Progress.
- [21] Jamoussi, B., et al., "Constraint-Based LSP Setup using LDP" Work in Progress.
- [22] Awduche, D., et al., "Extensions to RSVP for LSP Tunnels", Work in Progress.
- [23] Kent, S. and R. Atkinson, "IP Encapsulating Security Protocol (ESP)", RFC 2406, November 1998.
- [24] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.
- [25] Perez, M., Liaw, F., Mankin, A., Hoffman, E., Grossman, D. and A. Malis, "ATM Signalling Support for IP over ATM", RFC 1755, February 1995.
- [26] Malkin, G. "RIP Version 2 Carrying Additional Information", RFC 1723, November 1994.
- [27] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.
- [28] Shacham, A., Monsour, R., Pereira, R. and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 2393, December 1998.
- [29] Duffield N., et al., "A Performance Oriented Service Interface for Virtual Private Networks", Work in Progress.
- [30] Jacobson, V., Nichols, K. and B. Poduri, "An Expedited Forwarding PHB", RFC 2598, June 1999.
- [31] Casey, L., "An extended IP VPN Architecture", Work in Progress.
- [32] Rekhter, Y., and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.
- [33] Grossman, D. and J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", RFC 2684, September 1999.
- [34] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.
- [35] Boyle, J., et al., "The COPS (Common Open Policy Service)

- Protocol”, RFC 2748, January 2000.
- [36] MacRae, M. and S. Ayandeh, “Using COPS for VPN Connectivity”
Work in Progress.
- [37] Droms, R., “Dynamic Host Configuration Protocol”, RFC 2131,
March 1997.
- [38] Heinanen, J. and E. Rosen, “VPN Support with MPLS”, Work in
Progress.
- [39] Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S.,
Handley, M., Jacobson, V., Liu, C., Sharma, P. and L. Wei,
“Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol
Specification”, RFC 2362, June 1998.
- [40] Waitzman, D., Partridge, C., and S. Deering, “Distance Vector
Multicast Routing Protocol”, RFC 1075, November 1988.
- [41] Fenner, W., “IGMP-based Multicast Forwarding (IGMP Proxying)”,
Work in Progress.
- [42] Wallner, D., Harder, E. and R. Agee, “Key Management for
Multicast: Issues and Architectures”, RFC 2627, June 1999.
- [43] Hardjono, T., et al., “Secure IP Multicast: Problem areas,
Framework, and Building Blocks”, Work in Progress.
- [44] Rigney, C., Rubens, A., Simpson, W. and S. Willens, “Remote
Authentication Dial In User Service (RADIUS)”, RFC 2138, April
1997.
- [45] Valencia, A., Littlewood, M. and T. Kolar, “Cisco Layer Two
Forwarding (Protocol) “L2F””, RFC 2341, May 1998.
- [46] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and
G. Zorn, “Point-to-Point Tunneling Protocol (PPTP)”, RFC 2637,
July 1999.
- [47] Patel, B., et al., “Securing L2TP using IPSEC”, Work in
Progress.
- [48] Srisuresh, P., “Secure Remote Access with L2TP”, Work in
Progress.
- [49] Calhoun, P., et al., “Layer Two Tunneling Protocol “L2TP”
Security Extensions for Non-IP networks”, Work in Progress.
- [50] Aboba, B. and Zorn, G. “Implementation of PPTP/L2TP Compulsory
Tunneling via RADIUS”, Work in progress.

- [51] Aboba, B. and G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999.
- [52] Shea, R., "L2TP-over-IP Path MTU Discovery (L2TPMTU)", Work in Progress.
- [53] Sklower, K., Lloyd, B., McGregor, G., Carr, D. and T. Coradetti, "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.
- [54] Richards, C. and K. Smith, "The PPP Bandwidth Allocation Protocol (BAP) The PPP Bandwidth Allocation Control Protocol (BACP)", RFC 2125, March 1997.
- [55] Calhoun, P. and K. Peirce, "Layer Two Tunneling Protocol "L2TP" IP Differential Services Extension", Work in Progress.
- [56] ADSL Forum. "An Interoperable End-to-end Broadband Service Architecture over ADSL Systems (Version 3.0)", ADSL Forum 97-215.
- [57] ADSL Forum. "Core Network Architectures for ADSL Access Systems (Version 1.01)", ADSL Forum 98-017.
- [58] Gupta, V., "Secure, Remote Access over the Internet using IPsec", Work in Progress.
- [59] Pereira, R., et al., "The ISAKMP Configuration Method", Work in Progress.
- [60] Pereira, R. and S. Beaulieu, "Extended Authentication Within ISAKMP/Oakley", Work in Progress.
- [61] Litvin, M., et al., "A Hybrid Authentication Mode for IKE", Work in Progress.
- [62] Kelly, S., et al., "User-level Authentication Mechanisms for IPsec", Work in Progress.
- [63] Patel, B., et al., "DHCP Configuration of IPSEC Tunnel Mode", Work in Progress.
- [64] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D. and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.
- [65] ANSI/IEEE - 10038: 1993 (ISO/IEC) Information technology - Telecommunications and information exchange between systems - Local area networks - Media access control (MAC) bridges, ANSI/IEEE Std 802.1D, 1993 Edition.

12.0 作者信息

Bryan Gleeson
Nortel Networks
4500 Great America Parkway
Santa Clara CA 95054
USA

Phone: +1 (408) 548 3711
EMail: bgleeson@shastanets.com

Juha Heinanen
Telia Finland, Inc.
Myrmaentie 2
01600 VANTAA
Finland

Phone: +358 303 944 808
EMail: jh@telia.fi

Arthur Lin
Nortel Networks
4500 Great America Parkway
Santa Clara CA 95054
USA

Phone: +1 (408) 548 3788
EMail: alin@shastanets.com

Grenville Armitage
Bell Labs Research Silicon Valley
Lucent Technologies
3180 Porter Drive,
Palo Alto, CA 94304
USA

EMail: gja@lucent.com

Andrew G. Malis
Lucent Technologies
1 Robbins Road
Westford, MA 01886
USA

Phone: +1 978 952 7414
EMail: amalis@lucent.com

13.0 完全版权声明

Copyright (C) The Internet Society (2000). 版权保留。

本文及其译本可以提供给其他任何人，可以准备继续进行注释，可以继续拷贝、出版、发布，无论是全部还是部分，没有任何形式的限制，不过要在所有这样的拷贝和后续工作中提供上述声明和本段文字。然而，该文档本身不可做任何修改，例如删除版权声明或者参考资料等，除非是为开发Internet标准的开发目的，那时，版权定义在Internet标准过程里，或者翻译成其他语言。

上述有限许可是永久性的，不会被Internet社区或者其后继者收回。

本文和包含在这里的信息以“As is”基础提供，Internet社区和Internet工程任务组不做任何担保、解释和暗示，包括该信息使用不破坏任何权利或者任何可商用性担保或特定目的。

鸣谢

RFC编辑活动现在由Internet社界资助。