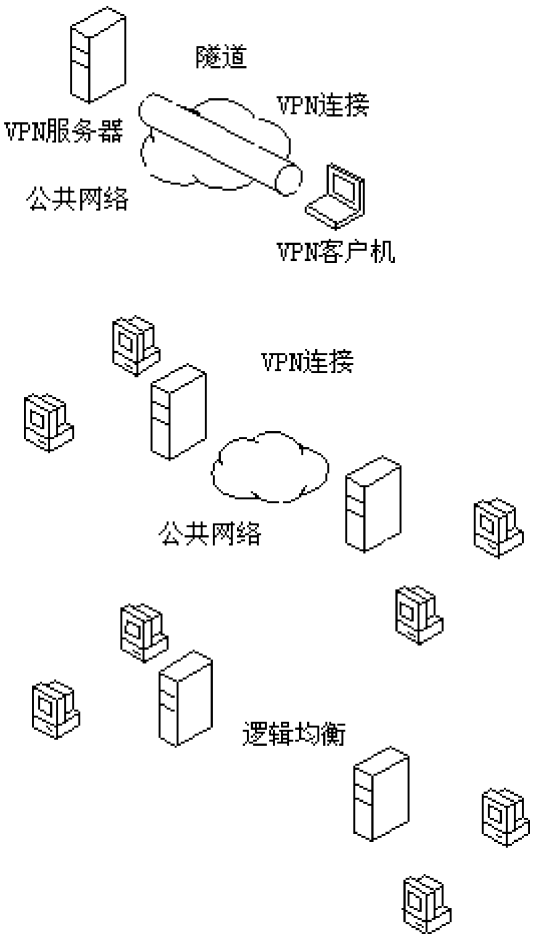
VPN技术学习指导

华 为 技 术 有 限 公 司

第一章 VPN 概 述

1.1 VPN综述

VPN--虚拟专用网（Virtual Private Network）是专用网络在公共网络如Internet上的扩展。VPN通过私有隧道技术在公共网络上仿真一条点到点的专线，从而达到安全的数据传输目的。



单纯仿真一条点到点的连接，数据只要经过封装，再加上一个提供路由信息的报头就可以了。而如果要仿真一条专线，为保证传输数据的安全，通常还要对数据进行加密处理。VPN连接必须同时包含数据封装和加密两方面。

有了VPN，用户在家里或在路途中也可以利用Internet或其他公共网络对企业服务器进行远程访问。从用户的角度来看，VPN就是在用户计算机即VPN客户机和企业服务器即VPN服务器之间点到点的连接，由于数据通过一条仿真专线传输，用户感觉不到公共网络的实际存在，能够像在专线上一样处理企业内部信息。换言之，虚拟专用网不是真正的专用网络，但却能够实现专用网络的功能。

VPN可以使企业通过公共网络在公司总部和各远程分部以及客户之间建立快捷，安全、可靠的信息通信。这种连接方式在概念上等同于传统广域网WAN的运作。

VPN技术的出现，使企业不再依赖于昂贵的长途拨号以及长途专线服务，而代之以本地ISP提供的VPN服务。从企业中心站点铺设至当地ISP的专线要比传统WAN解决方案中的长途专线短得多，因而成本也低廉得多。

第二章 VPN分类介绍

按功能位置：CPE-based VPN、Network-based VPN

按业务构成：Access VPN、Intranet VPN、Extranet VPN

按实现层次：应用层VPN、网络层VPN 、二层VPN

按组网模型：VPDN、VPRN、VPLS、VLL

2.1 CPE-based VPN、Network-based VPN

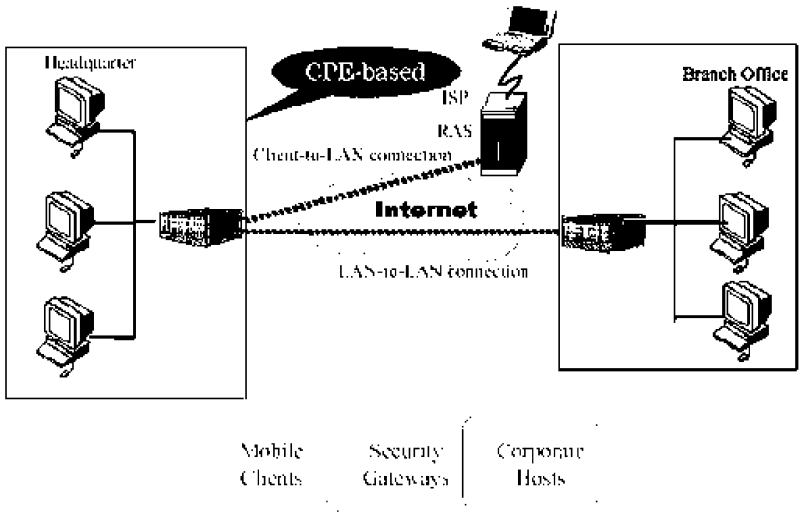
根据是由企业客户还是由服务提供商实施，VPN分为两类：

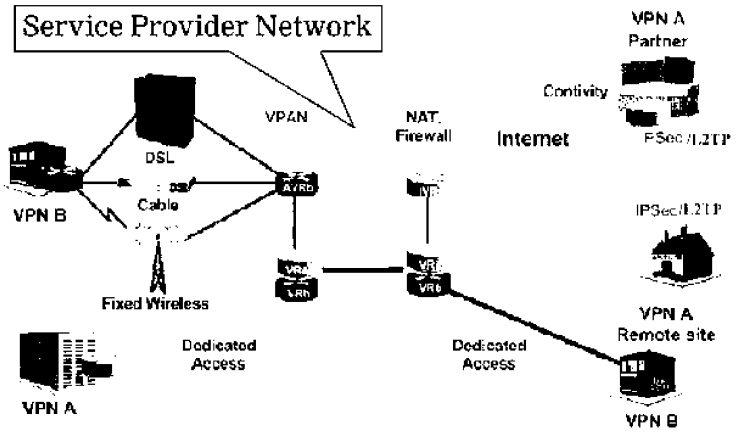
1. CPE-based VPN 基于客户端设备的VPN

2. Network-based VPN 基于网络的VPN

对于CPE-based VPN 基于客户端设备的VPN的特点是：业务扩展能力弱、设备价格昂贵、组网复杂度高。

对于Network-based VPN基于网络的VPN 的特点是：便于管理和维护、降低用户投资、业务扩展能力强、支持网络管理、运营商与用户实现双赢。





Network-based VPN基于网络的VPN

CPE-based vs Network-based VPN

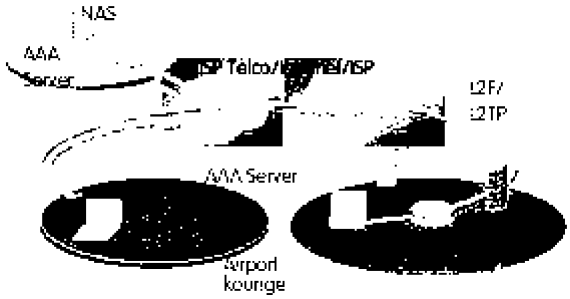
Feature	CPE-based VPN	Network-based VPN
QoS,CoS与SLAs	SLAs局限于网络时延和可用性，不支持CoS	多CoS,综合SLAs覆盖每个CoS
可扩展性	局限于几百条连接	没有限制
用户控制	非常有限（如增加远程接入用户）	多种提供在线修改网络资源的特性
业务类型	数据	关键数据、实时话音和图象

2.2 Access VPN、Intranet VPN、Extranet VPN

用户可以根据自己的情况进行选择：远程访问虚拟网（AccessVPN）、企业内部虚拟网（IntranetVPN）和企业扩展虚拟网（ExtranetVPN），这三种类型的VPN分别与传统的远程访问网络、企业内部的Intranet以及企业网和相关合作伙伴的企业网所构成的Extranet相对应。

2.2.1 远程访问虚拟网（AccessVPN）

AccessVPN通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。AccessVPN能使用户随时、随地以其所需的方式访问企业资源。AccessVPN包括模拟、拨号、ISDN、数字用户线路(xDSL)、移动IP和电缆技术，能够安全地连接移动用户、远程工作者或分支机构。如图所示。

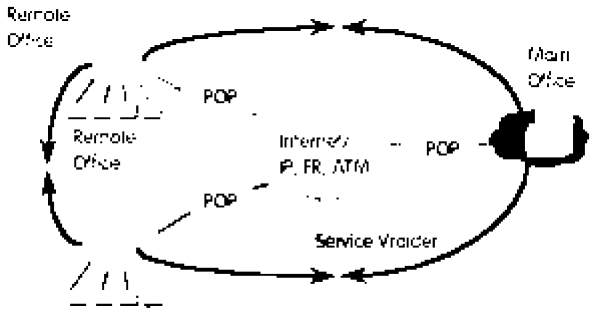


AceessVPN结构图

AccessVPN最适用于公司内部经常有流动人员远程办公的情况。出差员工利用当地ISP提供的VPN服务，就可以和公司的VPN网关建立私有的隧道连接。RADIUS服务器可对员工进行验证和授权，保证连接的安全，同时负担的电话费用大大降低。

2.2.2 企业内部虚拟网（IntranetVPN）

越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司、研究所等，各个分公司之间传统的网络连接方式一般是租用专线。显然，在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵。利用VPN特性可以在Internet上组建世界范围内的IntranetVPN。利用Internet的线路保证网络的互联性，而利用隧道、加密等VPN特性可以保证信息在整个IntranetVPN上安全传输。IntranetVPN通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。如图所示。

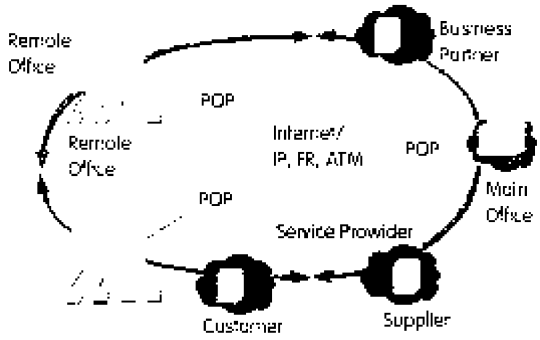


IntranetVPN结构图

2.2.3 企业扩展虚拟网（ExtranetVPN）

各个企业越来越重视各种信息的处理。希望可以提供给客户最快捷方便的信息服务，通过各种方式了解客户的需要，同时各个企业之间的合作关系也越来越多，信息交换日益频繁。Internet为这样的一种发展趋势提供了良好的基础，而如何利用Internet进行有效的信息管理，是企业发展中不可避免的一个关键问题。利用VPN技术可以组建安全的Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全。

ExtranetVPN通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。如图所示。



ExtranetVPN结构图

ExtranetVPN对用户的吸引力在于：能容易地对外部网进行部署和管理，外部网的连接可以使用与部署内部网和远端访问VPN相同的架构和协议进行部署。主要的不同是接入许可，外部网的用户被许可只有一次机会连接到其合作人的网络。

2.3 网络层VPN 、二层VPN

2.3.1 二层VPN

二层VPN服务的主要特征是根据用户数据包的二层地址（如MAC地址、帧中继的DLCI、ATM的PVC等）在网络的第二层对数据包进行转发和发送，服务提供商的网络负责提供CE之间的二层连接，这包括用MAC地址(例如LAN仿真)、点到点的链路层连接(ATM、帧中继、MPLS)、多点到点(用MPLS多点到点的LSP)和点到多点(例如ATM VCC)，而三层的连接例如选路由等由用户负责。PE设备可以是路由器或交换机，从支持二层连接的角度看，交换机更合适一些。VLL及局域网仿真服务VPLS就属于二层VPN。

二层VPN的主要特征

通过链路层地址（必要时也可用链路端口号）转发用户数据包。

SP（服务供应商）主要提供CE之间的链路层连接，一般SP不对IP VPN管理而只对链路的连接进行管理。

SP负责二层链路的连接，而三层的连接例如选路由等由用户负责。

由于VPN是建立在链路层基础上的，SP仅提供链路层连接，所以实际上IP VPN是由用户借助于SP的链路建立的。当然SP为VPN打下基础，它提供用户的链路应该是可靠的，也有较好的安全性(主要是指所提供的链路的专用性，它与公用部分及其他VPN的链路是相互隔离的，不会有用户数据包传送至公网或其他VPN域内)。

2.3.2 三层VPN

三层VPN服务的主要特征是PE转发用户数据包是以其IP地址为依据的，VPRN就属于三层VPN。通常用户网络使用专用的IP地址，所以PE要了解用户的专用IP地址空间。从CE的角度看PE，它是一个IP路由器。在三层VPN中，SP也参与VPN的管理并提供VPN，用户也可在其VPN范围内对其进行管理。

2.3.3 二层VPN与三层VPN应用的主要特点

CE与PE之间的接入链路

对于二层VPN，CE的接入链路要求统一，例如都是帧中继; 而对于三层VPN，CE的接入链路可以不同，例如某些CE可用帧中继，而另一些CE可用ATM等。

对CE的要求

根据应用的需求不同，二层VPN的CE可为路由器也可以为网桥，三层VPN则通常以CE为路由器。

CE的邻居

当CE为路由器时，三层VPN的CE只需与其相连的PE维持邻居关系，而二层VPN的CE需与其他的CE维持邻居关系，从而增加路由复杂度，规模受限。

支持第三层多协议能力

由于二层VPN只使用SP网络的二层链路，从而为支持三层多协议创造条件，三层VPN也能支持多协议，但不如前者灵活且有一定限制。同理在支持VPLS方面，二层VPN更合适。但如果VPN用户只传送IP包，此特点就不明显。

支持组播能力

二层VPN与三层VPN都支持组播，但二层VPN是依靠CE实施组播的，而三层VPN则依靠PE，因而三层VPN实施组播较简单，同时它还可以充分利用SP网络有关组播方面的能力支持组播，而二层VPN则无法使用SP网络的有关组播方面的能力。

网络管理

VPN服务提供商与用户VPN的管理部门都可进行网络管理，但侧重面不同。对于三层VPN，服务提供商可参与三层的管理；而二层VPN，服务提供商只能对所提供的链路进行管理，无法对三层进行管理。无论是二层VPN还是三层VPN，用户都可以对所属的VPN进行管理。

2.4 VPDN、VPRN、VPLS、VLL

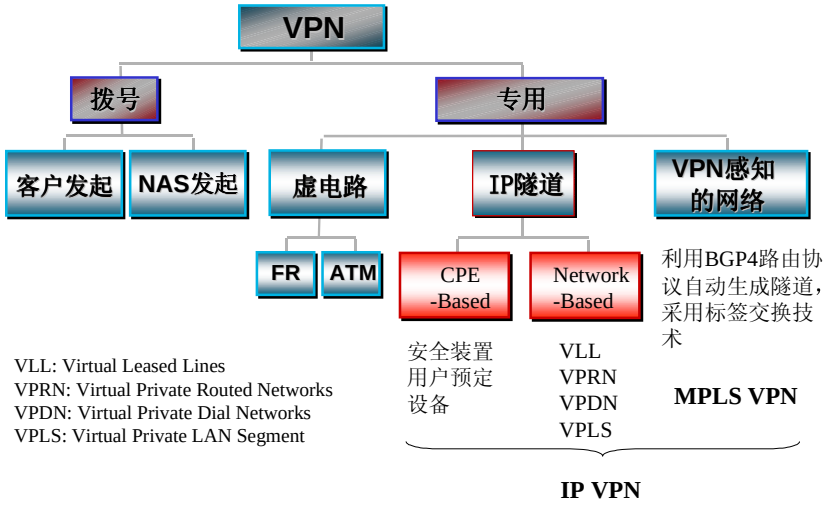
IP VPN-Framework-RFC2764中定义了如下VPN类型。

VPDN：Virtual Private Dial Networks

VPRN：Virtual Private Routed Networks

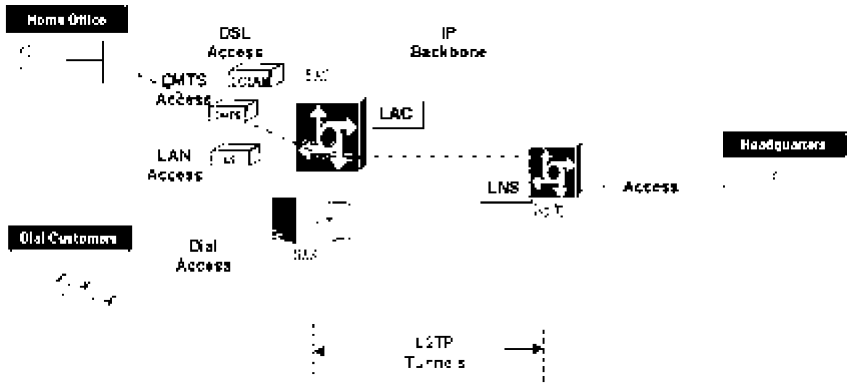
VPLS：Virtual Private LAN Segment

VLL：Virtual Leased Lines



2.4.1 VPDN (Virtual Private Dial Network) 虚拟拨号专网

VPDN的基本特点是：除VPN的总部网络中心采用专线接入VPN服务提供商的网络外，其余的VPN用户通过PSTN或ISDN拨号线路接入网络。另外，虽然拨号用户是通过PSTN或ISDN公网拨入VPN的，但是VPN所属用户仍与外界隔离，有较好的安全保证。VPDN也可以使用IP专用地址等VPN所特有的一些特性，接入范围可遍及PSTN、ISDN的覆盖区域，网络建设投资少、周期短，网络运行费用低。



VPDN有两种设备配置形式，从而导致有两种遂道建立方式。

必备(Compulsory)遂道

必备遂道的基本结构如图所示，该遂道存在于网络访问服务器(NAS/BAS)与网关之间。

通常，必备遂道都采用L2TP遂道协议进行实施，所以该遂道又称为L2TP遂道。必备遂道对特定的VPDN是专用的，即一个VPN有一个或多个专用遂道。主机与网关之间建立的PPP会话也是建立在该专用的L2TP遂道上的。

由于必备遂道采用L2TP协议，所以NAS/BAS与网关都要实施L2TP协议。此时，NAS/BAS要执行L2TP协议的接入控制器功能(LAC)，网关要执行L2TP网络服务器(LNS)功能。

由于LAC和LNS功能可以由多种设备实施，所以存在有多种具体的解决方案。网关实施网络接入功能及LNS功能，必要时，网关还兼有网络地址转换(NAT)功能，对企业总部网络内的专用IP地址与IP网公用IP地址进行转换。网关可以放在企业总部网络内，也可以由IP网的PE兼管。

L2TP遂道建立时要进行识别，如LAC识别LNS，以确保L2TP遂道的正确建立。L2TP遂道主要有封装与隔离功能。隔离功能可以保障VPN之间以及VPN与Internet的数据包不会相互串扰，有一定的安全性能保障。但是，L2TP本身无其他安全措施，用户数据包传送的安全性通过PPP连接的安全措施获得。

从上述必备遂道的结构可以看出，必备遂道是采用PPP对L2TP遂道功能的延伸。L2TP遂道与PPP会话一起构成必备遂道。NAS/BAS实施LAC的功能，且通过L2TP遂道及PPP会话与其他数据流相互隔离。NAS/BAS不只为特定的某个VPN服务，还可以为多个VPN服务。

无论是采用必备遂道还是下面要介绍的自助隧道的VPDN，对用户数据流来说，他们都可以被看成为一种接入方法类型。用户可以利用它实现与不同网络的连接，例如企业总部网络、Internet或者虚拟专用路由网络(VPRN)，都可以使用户通过上述类型的遂道进行接入。

用VPDN接入VPRN是两种VPN类型的结合，这种结合可以使以VPRN为基础的VPN很方便地扩大覆盖范围，满足用户发展业务的需要。

通常，VPN用户接入认证在NAS/BAS或企业总部网络内的安全服务器上实施。当前有很多用于认证的协议，其中Radius协议用得较多。

自助遂道(Voluntary Tunnels)

自助遂道也要使用拨号电路，但它与必备遂道主要不同之处是：用户在主机与远端网关之间建立遂道，而不是在NAS/BAS(LAC)与远端网关之间建立遂道。也就是说，自助隧道由用户主机处起始，而必备遂道是由LAC处起始，当然，隧道的终结点都是网关。

与必备隧道一样，自助隧道也有多种实施方案。用户主机接入企业总部网络是通过L2TP或IPSec协议所构成的隧道。必备隧道一般都用L2TP，但自助隧道可以采用L2TP或IPSec，用户可根据自己对传送信息安全性的需求进行选用。对于安全性要求较高的用户可以选用IPSec，一般用户可选用L2TP。

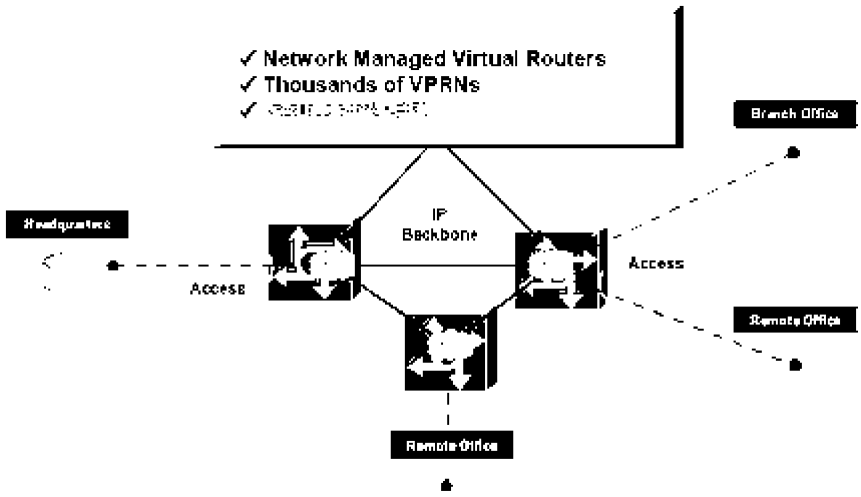
实际上，若把必备隧道中作为隧道起始处的LAC的功能模块放在用户主机处，而不放在网络节点(如NAS/BAS)处，则L2TP便能支持自助隧道模式。

这里必须注意，主机此时有两个IP地址，一个用于LAC-LNS IP隧道，另一个用于指定该网络通过PPP所连接的主机。L2TP用于自助隧道的好处是：原有被PPP使用的认证和地址分配机制无须修改仍能使用。例如，一个LNS可以包括一个Radius客户机，并且与Radius服务器通信，以认证PPP的相关信息。同时，它还可以检索主机的配置信息，如IP地址和所使用的DNS服务器为列表，这些信息随后通过PPP、IPCP协议送至主机。

自助隧道一般用L2TP协议构成，当用户需要高级别的安全性时，用户可以在链路层工作的L2TP协议基础上，在网络层上再使用IPSec协议。此时，L2TP构成自助隧道，而IPSec的ESP用于网络安全。

2.4.2 VPRN(Virtual Private Routed Networks) 虚拟专用路由网络

VPRN定义为：用IP设施仿真出一个专用多站点广域路由网。它是在IP公用网络(如Internet)基础上实施的。像VPN结构一样，VPRN也可以分为基于网络的VPRN及基于CE的VPRN。



相类似地，基于网络的VPRN及基于CE的VPRN的主要区别在于IP隧道与何种类型的节点连接。若PE边缘路由器之间用IP隧道按全连接或部分连接构成

主干网，而CE用支干链路(Stub link)与邻近的PE边缘路由器相连。这种方式所构成的VPRN称为基于网络的VPRN。假如CE用IP隧道按全连接或部分连接构成VPRN，则称为基于CE的VPRN。

VPRN与其他类型的VPN相比，其主要区别在于VPRN数据包的转发是在网络层实现的。VPRN是由PE路由器之间用IP隧道所组成的网状主干网和在每个VPRN节点接收的数据流转发至合适的目的站点所需的路由能力所组成。CE通常为路由器。

PE路由器与CE路由器是通过一条或多条支干链路相连接的。每个PE路由器为每个VPN建立专用路由表(注意，每个PE可以为多个VPN服务)。数据流在PE路由器之间的转发以及PE路由器和用户站点之间的转发都是依据这些转发表进行的。转发表包含网络层可达性信息(与VPLS相对照，VPLS的转发表包含MAC层可达性信息)。

通常，中小规模的基于网络的VPRN，其PE路由器用IP隧道两两相连构成全连接的网状结构的主干网。这种方式的最大优点是每对节点都有直达通道，在一般情况下，由于有直达路由器，无需第三方转发，网络的拓扑结构信息即可简化，一般只要确定PE路由器的数量就可以隐含拓扑结构。但由于全连接的网状结构需要n×(n-1)/2个IP隧道，当n较大时，由于n**2链路的关系，网络很难接受全连接方式。此时，网络可采用部分连接，甚至一个中心节点的星形拓扑结构。

VPRN应用的主要特性

支持非惟一的专用IP地址。与其他形状的VPN一样，VPRN内的IP地址可与公用IP网的IP地址无关，可以使用VPRN内部专用的IP地址。这些地址可以不是惟一的，可与其他VPN或其他专用系统的IP地址重叠。

VPRN主要支持TCP/IP协议。VPRN是在IP网基础上建立起来的，主要为支持传送IP包而设计，数据包在网络层实现转发。VPRN虽然也可以支持其他协议的数据包，但由于VPRN在网络层实现转发，所以单个VPRN只能直接支持一个网络层协议。若要求VPRN支持多协议环境，一般可以有两种实施方法，一种是通过封装技术，在一个已建隧道上再建一个隧道，使不同协议的数据包分别在不同隧道上传输，两者相互隔离。另一种方法是在相同物理设备上建立多个VPRN，每个VPRN分别支持特定的协议，即通过各个VPRN相互隔离。另外，如果特别强调要支持多协议，也可以在VPRN基础上稍加修改，变成虚拟专用LAN网段(VPLS)的形式。

允许用户接入Internet 。一般VPRN内的用户只能相互通信，不能与Internet用户通信或不能接入Internet。但是当需要时，网络可以允许某些用户接入Internet。 具体的实现方法有几种。一种方法是在PE边缘路由器处实施，该路由器可以负责区别两种不同的数据流，并分别引导至VPRN及Internet。同时，它可以在VPRN与Internet两个域之间提供防火墙功能。另一种方法是在

用户处实施。此时，由CE设备区分两种不同的数据流，并分别引导两个不同的域：一个通过PE边缘路由器接入VPRN，一个通过不包含在VPRN内的ISP路由器接入Internet。同时，CE设备可以提供防火墙功能。

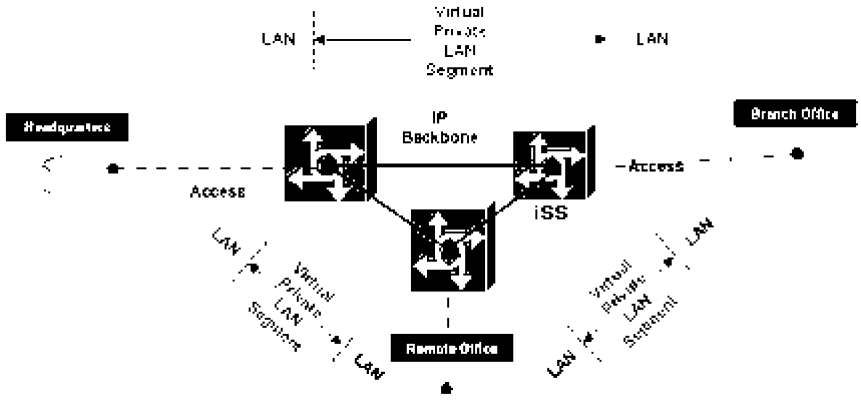
一个用户可以同时作为多个VPRN成员。很多情况都要求一个用户同时属于多个VPRN，该用户可以与不同的VPRN的用户通信，但不允许多个VPRN通过该用户转发。

安全性有保障。从总体上说，基于CE的VPRN的安全性要优于基于网络的VPRN。但是，基于网络的VPRN至少可获得类似帧中继、ATM网络的安全性。在采取适当措施后，基于网络的VPRN可以获得通常用户所需的安全性。

2.4.3 VPLS(Virtual Private LAN Segment)虚拟专用LAN网段

VPLS是用Internet设施仿真LAN网段。VPLS可用于提供所谓的透明LAN服务(TLS)。

TLS可用于以协议透明方式互连多个支干CE节点(如桥或路由器)。VPLS在IP上仿真LAN网段，类似于LANE在ATM上仿真LAN网段。它的主要优点是协议完全透明，这在多协议传送和传送管理上是很重要的。VPLS的样例如图所示。



PE节点一般是LAN交换器，CE设备可以是网桥也可以是路由器。CE与PE边缘节点之间的支干链路可以是ATM VCC、帧中继电路，当距离较短时也可以是物理线路，如5类线。

VPLS的拓扑与工作模型，除VPLS边缘节点实现链路层桥接而不是网络层转发外，基本上等效于VPRN(虚拟专用路由网络)。VPRN的隧道和构造机制也适用于VPLS，只是数据包和编址信息需要做适当改变。因为VPLS是在链路

层上工作，用链路层代替网络层，所以，网络信息的改变一般用帧代替包，用MAC地址代替IP地址即可。

VPLS应用的主要特性

支持非惟一的专用IP地址。虽然VPLS仿真LAN网段使用MAC地址，但是链路层MAC地址只标识站点，站点内的用户网络仍用IP地址标识。

所以，VPLS与其他类型VPN一样，采用隧道封装技术，VPLS内的IP地址可以与公用IP网的IP地址无关，也可以使用VPLS内部专用的IP地址。这些地址可以不是惟一的，可与其他VPN或其他专用系统的IP地址重叠。

完全支持多协议数据流传送。支持VPLS的ISP网络因为提供的是第二层的连接，ISP网络用于仿真多入口的LAN网段，所以用户网络可以更灵活。例如，任何的IGP或任何协议可以在用户站点运行。

VPRN由于在网络层实现转发，所以在通常条件下，一个单一的VPRN仅直接支持一个单一的网络层协议，为了支持多协议数据流传送需要采取某些特殊措施。而VPLS可全面支持多协议数据流传送，当然，这种多协议数据流传送需要有支持多协议的隧道协议的支持。

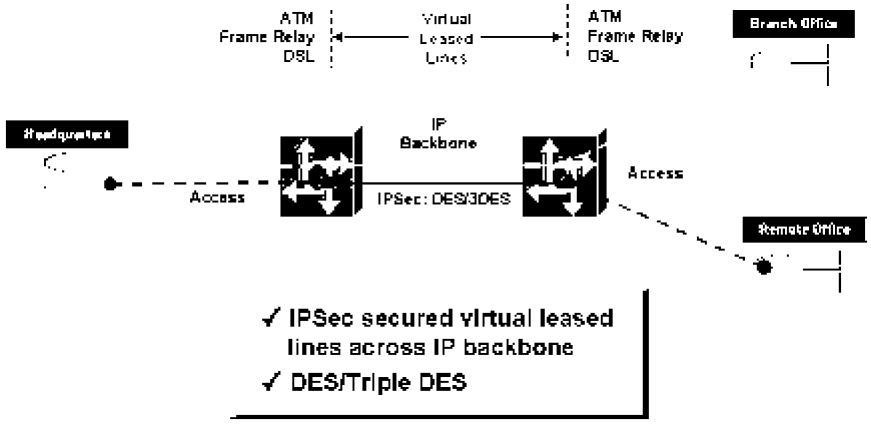
VPLS因为是用Internet设施仿真LAN网段，这就是说VPN服务提供商的基础网络是IP网，它要在IP网上通过相关设施在VPLS边缘节点实施链路层桥接而不是网络层转发，即在二层网络基础上提供透明的LAN服务。

CE节点可以是网桥也可以是路由器。在网桥情况下，所有支干站点的主机都在链路层上工作。一般来说，这些主机都在同一网络层子网内，帧的转发都是以链路层地址如MAC地址为依据，所以，VPLS要求支持广播数据流，实施地址解析(ARP)。

在CE路由器情况下，每个CE路由器的互连在同一个网络层子网中进行。CE路由器传送数据包通过VPLS至对等路由器时，使用下一跳的、路由器网络层地址映射的链路层地址识别路由器。

2.4.4 VLL(Virtual Leased Lines) 虚拟租用线

VLL是VPN中最简单的网络类型，可以说它是VPN中的一个特例。



VLL是服务提供商在IP网上为用户提供的点到点的链路业务，例如提供ATM VCC或帧中继电路等租用电路业务。发展VLL的主要原因是由于VPN服务提供商的基础网络是IP网，但有些用户需要一条或多条ATM VCC或帧中继电路的专线，由此诞生了VLL业务。

VLL的工作原理是，用户的CE设备通过本地专线接入网络边缘设备PE，在PE之间建立专用隧道，PE实施IP与ATM或帧中继协议转换，使PE的CE侧提供ATM或帧中继接口，从而建立两个CE之间的ATM VCC或帧中继电路通路，供用户使用。

第三章 VPN安全算法

3.1 常用加密(Encryption)算法

在公网上传输数据不能保证数据不被窃听。为了避免因为数据窃听而造成的信息泄漏，有必要对所传输的信息进行加密，只有与之通信的对端才能对此密文进行解密。通过对路由器所发送的报文进行加密，即使在Internet上进行传输，也能保证数据的私有性、完整性以及报文内容的真实性。对于利用公网构建VPN的情况，数据加密能够保证通过隧道传输的数据安全。

3.1.1 DES(Data Encryption Standard)

最著名的保密密钥或对称密钥加密算法DES(Data Encryption Standard)是由IBM公司在70年代发展起来的，并经过政府的加密标准筛选后，于1976年11月被美国政府采用，DES随后被美国国家标准局和美国国家标准协会(American National Standard Institute，ANSI) 承认。

DES是一种对称分组密码算法，以64bit分组的方式对输入数据（明文）进行加密，输出64bit的密文，密钥长度为8Byte（有效长度为56bit）。

CBC（Cipher Block Chaining）则是一种分组密码算法的工作模式。它需要在加密当前明文块之前，先与上一次加密后的密文块进行异或操作。对于第一个数据块，参与异或运算的应该是初始化向量IV（Initialization Vectors）。随ESP使用的所有加密算法必须以CBC模式工作，DES-CBC即是采用DES算法进行CBC运算。相关详细描述，请参看RFC2405（The ESP DES-CBC Cipher Algorithm）。

3.1.2 3DES

3DES-CBC （Triple Data Encryption Standard - Cipher Block Chaining）是DES-CBC加密算法的扩展算法。它和DES-CBC的区别在于它所使用的密钥长度是112位或168位（对长度为64位的数据块进行加密并产生64bit的密文），比DES-CBC具有更好的保密效果。

这种方式里使用三或两个不同的密钥对数据块进行三次或两次加密加密一次要比进行普通加密的三次要快三重DES 的强度大约和112- bit 的密钥强度相当三重DES 有四种模型

a. DES- EEE3 使用三个不同密钥顺序进行三次加密变换

b. DES- EDE3 使用三个不同密钥依次进行加密- 解密- 加密变换

c. DES- EEE2 其中密钥K 1 =K 3 顺序进行三次加密变换

d. DES- EDE2 其中密钥K 1 =K 3 依次进行加密- 解密- 加密变换

到目前为止还没有人给出攻击三重DES 的有效方法对其密钥空间中密钥进行蛮干搜索那么由于空间太大这实际上是不可行的若用差分攻击的方法相对于单一DES 来说复杂性以指数形式增长要超过10**52

3.1.3 对称密钥加密的理解

对称密钥加密我们可以做如下理解：

设加密算法函数为E，解密算法函数D，明文为M，密钥为key，加密后的密文为C。

在加密端有C=E(M，key)，在解密端M=D(C,key)。

对于加密算法有以下特性

a. 每一个加密函数E和每一个解密函数D 都能有效地计算

b. 破译者取得密文后将不能在有效的时间内破解出密钥key或明文M

c. 一个密码系统是安全的必要条件穷举密钥搜索将是不可行的即密钥

空间非常大。

对称密钥加密的算法是公开的，密文的保密性是依赖于双方保存相同的密钥key，key的长度越长则安全性越高，但计算的强度就要增加。

3.2 常用验证(Authentication)算法

3.2.1 HMAC-MD5

HMAC-MD5-96

MD5（Message Digest 5）是由Ron Rivest设计的散列算法，它以一个任意长度的报文作为输入（MD5实际处理的报文长度为K mod 64 bit，K为初始报文长度(bit)），输出一个128bit的摘要。MD5按照512bit的分组来处理输入消息，输出由4个32bit分组级联而成。

HMAC（Keyed-Hashing for Message Authentication）则是一种特殊的密钥散列算法，它需要完成两次Hash运算。对于密钥为K，输入消息为M，散列算法为H的HMAC定义如下：HMAC（K，M）=H（K XOR opad，H（K XOR ipad，M））， ipad是数值为0X36的64元素数组，opad是数值为0X5c的64元素数组。IPSec中进行的所有消息验证工作都用HMAC完成的。

HMAC-MD5-96采用MD5算法进行HMAC运算，输出结果取截断后的高96bit。有关在ESP和AH中应用HMAC-MD5-96的详细描述参见RFC2403（The Use of HMAC-MD5-96 within ESP and AH）。

3.2.2 HMAC-SHA1

HMAC-SHA-1-96

SHA-1（Secure Hash Algorithm 1）是由NIST（美国国家标准和技术协会）设计的散列算法，它要求输入报文的最大长度不超过 64 bit，输出一个160位的摘要。SHA1按照512bit的分组来处理输入消息，输出由5个32bit分组级联而成。

HMAC-SHA-1-96采用SHA-1算法进行HMAC运算，输出结果取截断后的高96bit。有关在ESP和AH中应用HMAC-SHA-1-96的详细描述参见RFC2404（The Use of HMAC-SHA-1-96 within ESP and AH）。

3.2.2 对验证算法理解

对验证算法我们可以做如下理解：

数字签名算法

Hash签名是最主要的数字签名方法，也称之为数字摘要法（digital digest）、数字指纹法（digital finger print）。该数字签名方法是将数字签名与要发送的信息紧密联系在一起下面我们将详细介绍Hash签名中的函数与算法。

单向函数

单向函数的概念是计算起来相对容易，但求逆却非常困难。也就是说，已知x，我们很容易计算f（x）。但已知f（x），却难于计算出x。在这里，"难"定义成：即使世界上所有的计算机都用来计算，从f（x）计算出x也要花费数百万年的时间。

单向Hash函数

Hash函数长期以来一直在计算机科学中使用，无论从数学上或别的角度看，Hash函数就是把可变输入长度串（叫做预映射，Pre-image）转换成固定长度

（经常更短）输出串（叫做hash值）的一种函数。简单的Hash函数就是对预映射的处理，并且返回由所有输入字节异或组成的一字节。

单向Hash函数是在一个方向上工作的Hash函数，从预映射的值很容易计算其Hash值，但要产生一个预映射的值使其Hash值等于一个特殊值却是很难的。好的hash函数也是无冲突的：难于产生两个预映射的值，使他们的hash值相同。

Hash函数是公开的，对处理过程不用保密。单向hash函数的安全性是它的单向性。无论怎么看，输出不依赖于输入。预映射单个比特的改变，平均而言，将引起hash值中一半的比特改变。已知一个hash值，要找到预映射的值，使它的hash值等于已知的hash值在计算上是不可行的。

哈希函数，即对于任意长度的信息m，经过哈希函数运算后，压缩后固定长度的数，比如64比特HASH函数的特殊要求是：

a. 已知哈希函数的输出，要求它的输入是困难的，即已知c=Hash（m），求m是困难的。这表现了函数的单向性。

b. 已知m，计算Hash（m）是容易的。这表现了函数的快速性。

c. 已知，构造m2使Hash（m2）=c1是困难的。这是函数的抗碰撞性。

d. c=Hash（m），c的每一比特都与m的每一比特有关，并有高度敏感性。即每改变m的一比特，都将对c产生明显影响。这就是函数的雪崩性。

e. 作为一种数字签名，还要求哈希函数除了信息m自身之外，应该基于发信方的秘密信息对信息m进行确认。

f. 接受的输入m数据没有长度限制；对输入任何长度的m数据能够生成该输入报文固定长度的输出；

曾有数家统计计算结果表明，如hash(m)的长度为128位(bit)时，则任意两个分别为M1．M2的输入报文具有完全相同的h(m)的概率为10－24，即近于零的重复概率。它较人类指纹的重复概率10－19还要小5个数量级。而当我们取hash(m)为384(bit)乃至1024(bit)时，则更是不大可能重复了。

另外，如输入报文M1与输入报文M2全等,则有h(m1)与h(m2)全等，如只将M2或M1中的某任意一位(bit)改变了，其结果将导致h(m1)与h(m2)中有一半左右对应的位(bit)的值都不相同了。这种发散特性使电子数字签名很容易发现（验证签名）输入报文的关键位的值被人篡改了。

第四章 IPsec协议

4.1 IPSec协议简介

4.4.1 IPSec协议概述

IPSec (IP Security)是IETF 制定的一系列协议，以保证在Internet 上传送数据的安全保密性能，特定的通信方之间在IP 层通过加密与数据源验证来保证，数据包在Internet 上传输时的私有性、完整性和真实性。

IPSec 通过AH Authentication Header 和ESP Encapsulating Security Payload 这两个安全协议来实现对IP 数据报或上层协议的保护。而且此实现不会对用户、主机或其它Internet 组件造成影响，用户还可以选择不同的加密算法而不会影响其它部分的实现

AH（Authentication Header） 是报文验证头协议主要提供的功能有数据源验证数、据完整性校验和防报文重放功能ESP（Encapsulating SecurityPayload）是封装安全载荷协议，它除提供AH 协议的所有功能之外， 还可提供对IP 报文的加密功能。AH 和ESP 可以单独使用，也可以同时使用。

IPSec 提供的安全服务需要用到共享密钥因特网密钥交换协议(Internet Key Exchange IKE) 为IPSec 提供了自动协商交换密钥建立和维护安全联盟的服务能够简化IPSec 的使用和管理。

4.1.2 IPSec提供的安全服务

私有性 — IPSec在传输数据包之前将其加密.以保证数据的私有性；

完整性 — IPSec在目的地要验证数据包，以保证该数据包在传输过程中没有被修改；

真实性 — IPSec端要验证所有受IPSec保护的数据包；

防重放 — IPSec防止了数据包被捕捉并重新投放到网上，即目的地会拒绝老的或重复的数据包，它通过报文的序列号实现。

4.1.3 与IPSec实现相关的几个概念

a. 安全网关，是指具有IPsec功能的网关设备（这里当然就是指我们安全加密路由器了）。安全网关之间可以利用IPsec对数据进行安全保护，保证数据不被偷窥或篡改。

b. 安全策略，由用户手工配置，规定对什么样的数据流采用什么样的安全措施。 一条安全策略由“名字”和“顺序号”共同唯一确定。

c. 安全策略库是所有具有相同名字的安全策略的集合。当一个接口需要对外建立多条安全隧道时，必须采用此种形式。一个原则需要明确，任何端口都只能应用一个安全策略库，任何一个安全策略库同时都只能应用在一个端口之上。

d. 安全联盟（SA）包括协议、算法、密钥等内容，具体确定了如何对IP报文进行处理。安全联盟是单向的，在两个安全网关之间的双向通信，需要两个安全联盟来分别对输入数据流和输出数据流进行安全保护。安全联盟由一个三元组来唯一标识，这个三元组包括安全参数索引（SPI）、IP目的地址、安全协议号（AH或ESP）。安全联盟可以由用户手工配置和维护，但需要用户配置比较多的参数；安全联盟也可以由IKE生成和维护，IKE根据安全策略能够不需要用户干预而自动地建立和维护安全联盟，后者将是我们使用的重点。

e. 安全隧道是点对点的安全“连接”。通过在安全隧道的两端，本端和对端，配置（或者自动生成）对应的安全联盟，实现在本端对IP报文加密，在对端解密。安全隧道可以跨越多台路由器和多个网络，只有安全隧道的两端共享了秘密，对于隧道中间的路由器和网络，所有的加密报文和普通报文一样被透明地转发。

f. 安全参数索引（SPI）是一个32比特的数值，在每一个IPsec报文中都携带有该数值。安全参数索引（SPI）和IP目的地址、安全协议号一起组成一个三元组，来唯一标识一个特定的安全联盟。（手工配置安全联盟时，需要手工指定安全参数索引（SPI），为保证安全联盟的唯一性，必须使用不同的安全参数索引来配置安全联盟；IKE协商产生安全联盟时，使用随机数来生成安全参数索引（SPI））。

g. 转换方式的内容包括安全协议、安全协议使用的算法、安全协议对报文的封装形式，规定了把普通的IP报文转换成IPsec报文的方式。在安全策略中，将引用一个转换方式来规定该安全策略采用的协议、算法等。

4.2 建立IPSec 的准备工作

a. 确定在哪些安全网关之间对哪些数据流建立安全隧道

安全隧道是两个安全网关之间端对端的隧道，必须为一条安全隧道指定一个本端和一个对端。一条安全隧道对应着一种受保护的数据流，两个安全网关之间可以建立多条安全隧道。安全隧道建立在两个安全网关的接口之间，例如以太网口同/异步串口。安全隧道的本端地址及对端地址是指接口的IP 地址。

根据需要在安全策略(crypto map)中配置正确的本端地址(set local-address) 及对端地址(set peer)设置好访问控制列表(access-list)确定需要保护的数据流，并在安全策略中引用访问控制列表（match address）

b. 确定建立安全联盟选用的协商方式

有两种方式建立安全联盟，一种是手工方式（manual） 一种是IKE 自动协商(isakmp)方式前。者配置比较复杂，安全策略的信息和创建安全联盟所需的全部信息都必须手工输入而且IPSec 的一些高级特性（例如定时更新密钥)不被支持，但优点是可以不依赖IKE 而单独实现IPSec 功能。而后者则相对比较简单，只需要配置好安全策略的信息，由IKE 自动协商来创建和维护安全联盟推荐使用IKE 协商建立安全联盟。

在创建一条安全策略时就必须指定协商方式，一旦创建了安全策略就不能再改变协商方式。如果要改变协商方式，只能先删除安全策略再创建一条新的安全策略。

c. 确定在安全隧道上采用的安全协议算法和报文的封装形式

安全协议有AH 协议和ESP 协议。AH 协议支持MD5 验证算法和SHA-1 验证算法ESP 协议支持MD5 验证算法，SHA-1 验证算法和DES 3DES 加密算法在。安全隧道的两端设置的安全策略必须采用同样的协议和算法。

IPSec 对IP 报文的封装有两种形式：传输模式（transport mode） 和隧道模式（tunnel mode）。 对于传输模式，IPSec 对原IP 报文的数据部分加以保护，不对IP 报文头进行保护，对于隧道模式，IPSec 对整个IP 报文进行保护，并在原IP 报文的前面增加一个新的IP 头，新IP 头的源地址和目的地址分别是安全隧道的两个端点的IP 地址。

根据需要配置好一个安全转换方式(crypto ipsec transform)， 然后在安全策略（crypto map ）中引用这个转换方式（set transform）。

d. 确定密钥和安全参数索引（SPI）

如果是通过IKE 协商安全联盟，则上述信息由IKE 协商生成，无须手工输入。如果是通过手工方式建立安全联盟，则必须事先确定以上信息。

在安全隧道的两端，本端的输入安全联盟的SPI 及密钥必须和对端的输出安全联盟的SPI 及密钥一样，本端的输出安全联盟的SPI 及密钥必须和对端的输入安全联盟的SPI 及密钥一样。

4.3 IPsec加密传输流程

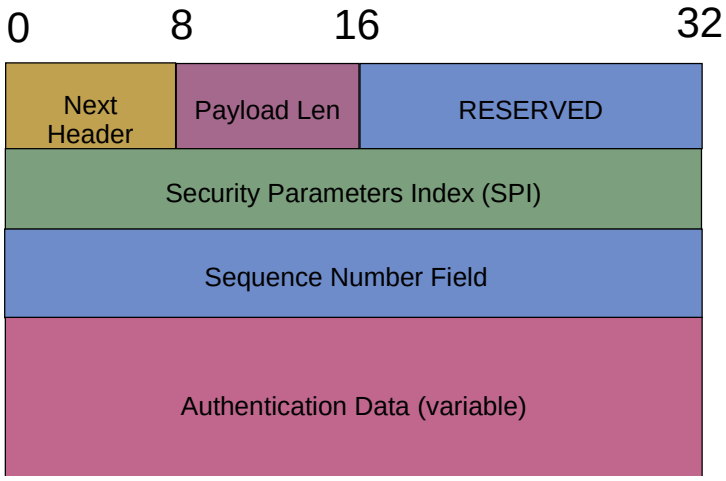
为直观起见，我们先来看一个数据包通过安全隧道的传输过程。本过程的一个前提是安全网关之间的安全联盟已经建立好，请留意前面概念涉及到的一些对象在此过程中所发挥的作用。

一个IP包到达了安全加密路由器的端口1，路由器首先根据此数据包的源、目的IP地址，端口号，协议号，查本端口引用的访问列表，允许通过（假设），再察路由表，然后将此数据包送到指定的端口2。数据包到达此端口2后，访问列表将数据包的IP包头提取出来与访问控制列表对照，发现此数据包属于需要加密之列，便将其交给IPsec来处理。IPsec首先根据访问列表对照的结果，将对应的SA的信息与包头放到IPsec队列中排队，逐一处理。之后，IPsec将根据该数据包指定的SA的配置进行如下操作：

a. 检查此SA所用的传输模式，如果是TUNNEL模式，则将原IP包整个当作数据交给“加密部分”，如果是TRANSPORT模式，则将IP包头提出来，只送数据段到“加密部分”；

b. 不论是TUNNEL还是TRANSPORT模式，加密部分处理送过来的数据的方式是一致的，此阶段有两种方式供选择（由SA决定，具体是由SA引用的转换方式配置决定的），一种是AH协议方式，另外一种是ESP协议方式，AH即 Authentication Header，报文验证头协议，ESP 即 Encapsulating Security Payload，报文安全封装协议，AH协议主要提供的功能有数据源验证、数据完整性校验和防报文重放功能，ESP在此之外还提供了对IP报文加密的功能。下面我们来看看两种协议是怎样工作的。

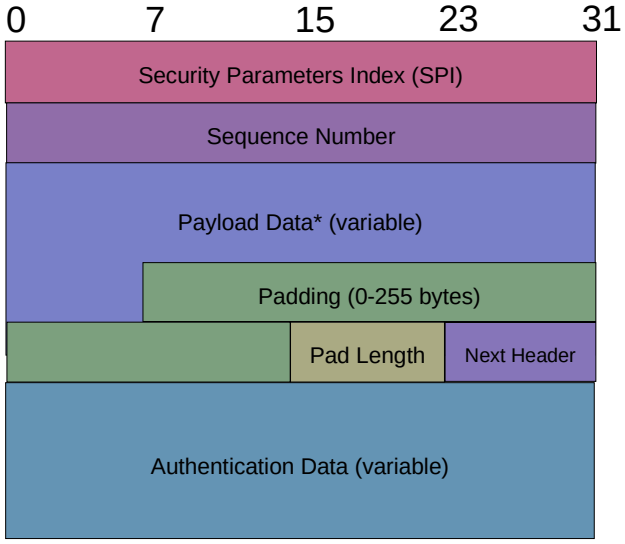
AH协议方式：在Quidway安全加密路由器系列中，目前提供了两种散列算法可选择，分别是：MD5和SHA1，这两种算法的密钥长度分别是128bit和160bit，散列算法并不改变实际的数据，它们的作用是用SA提供的密钥与数据内容进行一种复杂的散列运算，生成一个验证字段(authentication data)，当原数据段任何内容的很小的改变包括顺序的变化都会导致该字段的值发生巨大的变化。AH协议方式会首先在原数据前生成一个AH报文头，报文头中包括一个递增的顺序号（Sequence number)与验证字段（空）、安全参数索引（SPI）等，然后，AH协议将对此报文头和数据进行这种散列算法运算，生成的验证字段填入AH头后，发送端的AH过程结束。



AH协议报文头结构

ESP协议方式：在ESP协议方式下，数据同样要通过散列算法获得验证数据字段，可选的算法同样是MD5和SHA1。与AH协议不同的是，在ESP协议中还可以选择序列密钥加密算法，国外一般常见的是DES系列序列算法，但在国内该系列算法未得到国家商密认证机构的许可，不能使用，Quidway一块专用加密卡完成，不需占用系统资源。此算法突出的特点是加密强度高，支持一次一密，即用来加密每一个IP报文的密钥都可以不一样。序列密钥加密算法要从SA中获得密钥，对参加ESP加密的整个数据的内容进行加密运算，得到一段新的“数据”。完成之后，ESP将在新的“数据”前面加上SPI字段、Sequence number字段，在数据后面加上一个验证字段和填充字段等，如此，ESP过程结束。在这个过程中注意到散列算法和序列算法都需要密钥，那么它们使用的是同一个密钥吗？显然不是。如果我们的SA是由手工建立的，那么在建立时，我们就需要为其分别设置密钥；如果是使用IKE方式的话，ESP将会自动获得不同的密钥。

c. 加密部分的工作完成后，IPsec还要进行最后一步工作，就是根据转换方式的不同（TUNNEL/TRANSPORT）为新的“数据”打上一个新的IP包头。对于TUNNEL模式，IPsec会将SA配置中设置的TUNNEL的入口与出口IP地址作为新的源与目的地址根据使用的协议产生一个新的IP包头；TRANSPORT模式中，IPsec将把原来的IP包头直接放在数据的前面使用，但协议号已经修改成了AH或者ESP。

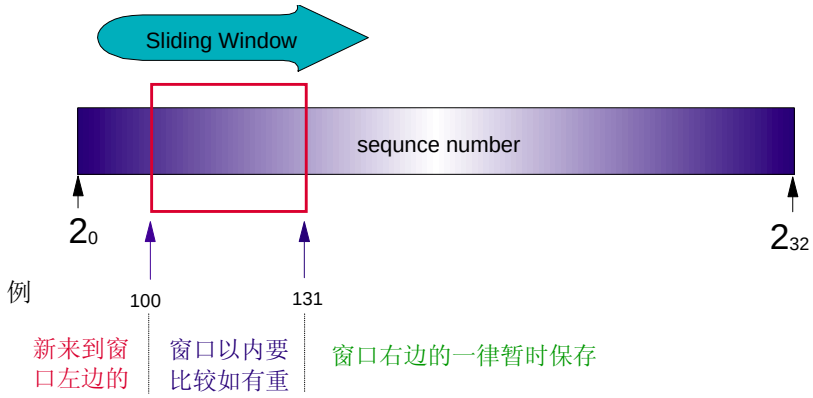


ESP包结构示意图

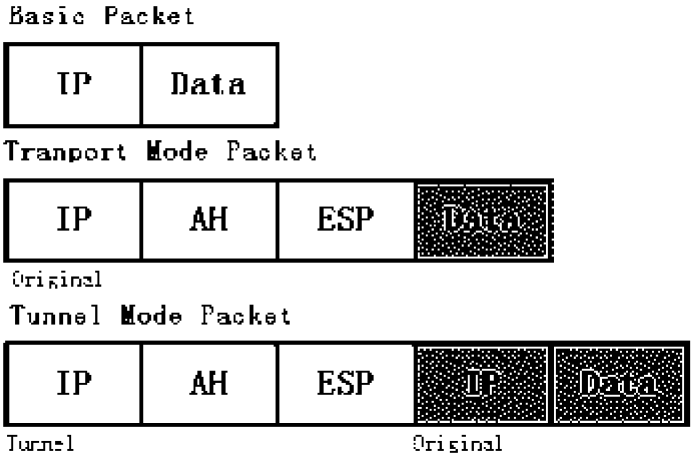
这样，发端的工作就完成了，收端的工作与之类似，只是处理的方式相反。但值得注意的是，收端怎样发现和处理可能被篡改和重放的数据包呢？前面我们提到了AH和ESP均具有此两方面的防范功能。

防篡改（即数据完整性校验，同时提供数据源验证功能）：发端使用散列算法与每一位数据作运算但不改变数据原文，生成一个一一对应的验证字段，当数据在传输中被截获修改后再发过来的时候，收端使用事先协商好的密钥和散列算法再对数据进行运算，如果得到的新的验证字段与传送过来的不一致，则可以断定，数据已经被修改过了，或者数据包的身份不合法。这样，我们可以轻易的发现被篡改过的数据包，丢掉。

防重放：在AH和ESP报文头里都有一个 Sequence number 字段，这个字段内的值是单调递增的，共32bit，用来一一标识每一个发出的数据包。那是不是任何新的数据包到来都和已有的成千上万的数据包的Sequence number进行比较呢？当然不是，在AH和ESP协议中定义了Sliding Windows （滑动窗口）的概念，这个窗口的尺寸可以定义，最小使用32，一般推荐为64。滑动窗口的作用是什么呢？限制比较范围。窗口随着IPsec包的不断到来而向右滑动，遵照这样一个规则：假设当前滑动窗口尺寸为32，当前位置为X ，范围从X到 X+31，此时，如果新到的IPsec包的sequnce number值小于X，则无条件丢弃；如果值大于X+31，则一律暂时保存；当此值落在窗口之内时，则需与窗口内已有的IPsec包的sequnce number值进行一一比较，发现有重复，则认为是重放的数据包，丢掉；如果发现新来的IPsec包的sequnce number恰好为X+1，则窗口右移一位，范围变为X+1到X+32，这样将可以证明，窗口左边的IPsec包一定是唯一的。



AH协议不能提供对报文内容的加密，只要被截获，报文的内容就一览无遗，虽然不能非法修改，但始终是秘密泄漏了，而ESP协议解决了这个问题，方法很简单，用很长的密钥对报文内容进行一些复杂的幂模运算，这样截获者即使得到报文只要没有密钥，同样无从下手。 ESP将需要保护的用户数据进行加密后再封装到IP包中，ESP可以保证数据的完整性、真实性和私有性。



IPSEC Packet 在IP报文中的结构

第五章 IKE协议

5.1 IKE 协议简介

IKE Internet Key Exchange 是因特网密钥交换协议，它属于一种混合型协议，建立在由Internet 安全联盟和密钥管理协议ISAKMP 定义的一个框架上。IKE为IPSec 提供了自动协商交换密钥、建立安全联盟的服务能够简化IPSec 的使用和管理。

安全隧道的确比较“安全”，但所有的安全都来自密钥的保护，一旦密钥泄漏，前面的一切防范措施都将失效，所以，对于安全加密路由器来说，密钥的管理是非常重要的。前面我们提到过，在手工配置SA时，密钥由隧道两端的网络管理员来相互协调，人与人之间交互信息有多种方式，但要确认安全却十分的繁琐，对于目前高超的窃密手段来说，任何有人参加的密钥协商都不可能百分之百安全，更何况在特殊情况下，密钥需要频繁的更改，要做到就更为困难了。这个至关重要的问题如何来解决呢？我们让路由器自己来全权处理它。这就是我们将要讨论的IKE协议。

IKE，（INTERNET KEY EXCHANGE PROTOCOL）互联网密钥交换协议，是一个密钥管理协议标准，与IPsec一起使用提供了用户身份鉴别, 密钥协商, 和协商创建安全连接的功能。 IKE的特点就是它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。所以，IKE名为交换（exchange）而非传送（transfer）正体现了这一特点。

在介绍IKE协商之前有必要提一下ISAKMP： Internet Security Association and Key Management Protocol，互联网安全连接和密钥管理协议，它定义了身份验证， SA创建和管理， 密钥生成和防止攻击的概念和过程。ISAKMP定义的是一个结构，按照这个结构可以定义多个密钥交换协议， IKE是其中之一。

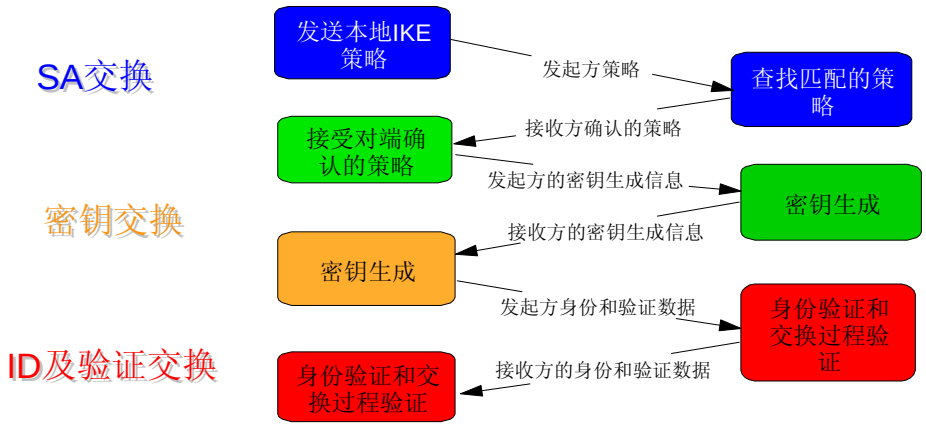
5.2 IKE协商流程

两台安全加密路由器要能够通过IKE方式协商密钥，必须具有以下两个条件：两端配置有匹配的POLICY；两端配有匹配的安全策略（此安全策略当然不用配置验证与加密密钥）。在POLICY中我们定义了一些IKE协商的自保护措施，他们包括：协商报文的加密算法，验证方法，散列算法，使用的DH组

标识，安全连接的生存时间等等。验证方法的定义非常重要，我们以pre-share这种验证方法为例，这是一种秘密密钥验证方法。

我们来看具体的协商，IKE协商分为两个阶段，分别称为阶段1和阶段2。阶段1中，主要协商出一个称为“加密物”的“密钥池”，并对双方进行身份的验证。阶段2将在阶段1的基础上取得共同的密钥，并使用此密钥来进行具体的IPsec的SA的协商。

首先看阶段1协商。阶段1中IKE需要协商三对数据，流程如下图所示：



IKE阶段1 协商流程简图

第一对数据协商的是双方的IKE策略。IKE的发起方将本地配置的IKE策略联同一个随机数A一块以明文的方式发送给接收方，接收方收到以后，将其策略一一与自己的策略库进行比较，当发现第一条匹配的策略时，接收方将记住随机数A(将其与匹配的策略关联）并产生一个新的随机数B，与A一块发回给发起方，这样，双方均知道了使用什么样的IKE策略，以及该策略关联的唯一标识（随机数），接着，将进行下一步协商，如果此过程未找到匹配的策略，那么协商就此失败。

第二步要进行的是密钥交换，是整个IKE协商过程的重点。在此过程介绍之前有必要简单介绍一下DH交换技术。 DH交换（Diffie-Hellman Exchange），过程如下：

a. 须进行DH交换的双方各自产生一个随机数，如a和b；

b. 使用双方确认的共享的公开的两个参数：底数g和模数p各自用随机数a,b进行幂模运算，得到结果c和d，计算公式如下：

$c = g^{a} \ mod \ p$，$d = g^{b} \ mod \ p$；

c. 双方进行模交换；

d. 进一步计算，得到DH公有值： $d^a \ mod \ p = c^b \ mod \ p = g^{ab} \ mod \ p$此公式可以从数学上证明。

若网络上的第三方截获了双方的模c和d，那么要计算出DH公有值$g^{ab} \ mod \ p$还需要获得a或b，a和b始终没有直接在网络上传输过，如果想由模c和d计算a或b就需要进行离散对数运算，而p为素数，当p足够大时（一般为768位以上的二进制数），数学上已经证明，其计算复杂度非常高从而认为是不可实现的。所以，DH交换技术可以保证双方能够安全地获得公有信息。

回到第二步协商上来，发起方和接收方分别产生一个随机数，与第一步协商好一起使用的公开数 p ,g进行幂模运算，将得到的结果交换后，再进行一次运算，从而得到双方共有的一个DH公有值，此公有值在IKE协商中就称为“加密物”。值得提一下的是，公开数p，g在配置IKE策略时通过选择group参数已经确定，参数：1，2分别对应的参数p，g分别为768位和1024位的两个常数。

第三步要进行的是身份验证和交换过程验证。具体内容包括：发起方将本端的pre-share密钥、随机数（A/B)等，作为参数参与此阶段验证、加密密钥的选取算法，对加密物运算， 从而取得需要的密秘密钥。由于双方的加密物、验证字以及随机数均相同，所以可以断定，双方得到的密秘密钥是一致的。得到的密钥用于加密、验证双方的身份信息，并在此阶段进行交互。

到这里，双方的IKE协商第一阶段已经完成，如果是第一次发起协商，双方将继续进行第二阶段的协商，相对而言，如果不是第一次发起协商的话，将由访问列表指定的用户IP报文来触发第二阶段的协商，但协商的过程都一样。

首先是发起方将本端的IPsec策略，连同本端的用户身份信息、密钥生成信息（一般是用户主机的IP地址）用第一阶段产生的验证密钥和序列密钥加密传送给接收方，接收方收到验证、解密以后，将其与本身的IPsec策略、密钥生成信息进行匹配，然后将匹配后的结果连同密钥生成信息、身分信息加密传给发起方，这样发起方收到的信息已经足够验证出该用户是否为指定用户并能从加密物中算出与接收方相同的密钥，这样，此密钥将永远不需要在网络中直接传输，可见其安全性是很高的。到这里，IPsec需要的各种密钥和顺序号均得到了，双方的IPsec SA便可以顺利建立起来了。

双方的IKE协商结束，IPsec SA协商结束。

值得说明的是，在IKE和IPsec SA协商过程中的生存时间的定义非常重要，前者决定了多长时间后自动重新协商“加密物”（阶段1协商），后者决定多长时间或流量后重新协商IPsec SA（阶段2），这是IKE方式比起手动方式建立SA来说最大的好处之一，一旦策略建立，双方的密钥交换、更改将完全不用人工参与。

另一方面，从IKE协商的全程来看，pre-share方式在协商两端仍然依赖了一个共同的秘密密钥，就是pre-shared- KEY，此密钥泄漏，将对双方的内部网络安全造成危害，因为这样的话，攻击者将有机会利用地址欺骗与双方之一建立新的“安全”隧道，当然过程将非常复杂。

第六章 L2TP VPN

6.1 VPDN相关协议简介

VPDN(Virtual Private Dial Network 虚拟私有拨号网)是指利用公共网络(如ISDN 和PSTN) 的拨号功能及接入网来实现虚拟专用网，从而为企业、小型ISP、 移动办公人员提供接入服务。VPDN 隧道协议可分为PPTP、L2F和L2TP三种目前最广泛使用的是L2TP。

PPTP（Point to Point Tunneling Protocol，点对点通道协议）

PPTP 提供PPTP 客户机和PPTP 服务器之间的加密通信。PPTP 客户机是指运行了该协议的PC 机，如启动该协议的Windows95/98；PPTP 服务器是指运行该协议的服务器，如启动该协议的WindowsNT 服务器。PPTP 可看作是PPP 协议的一种扩展。它提供了一种在Internet 上建立多协议的安全虚拟专用网（VPN）的通信方式。远端用户能够透过任何支持PPTP 的ISP 访问公司的专用网络。

通过PPTP，客户可采用拨号方式接入公共IP 网络Internet。拨号客户首先按常规方式拨号到ISP 的接入服务器（NAS），建立PPP 连接；在此基础上，客户进行二次拨号建立到PPTP 服务器的连接，该连接称为PPTP 隧道，实质上是基于IP 协议上的另一个PPP 连接，其中的IP 包可以封装多种协议数据，包括TCP ／IP、IPX 和NetBEUI。PPTP 采用了基于RSA 公司RC4 的数据加密方法，保证了虚拟连接通道的安全性。对于直接连到Internet 上的客户则不需要第一重PPP 的拨号连接，可以直接与PPTP 服务器建立虚拟通道。PPTP 把建立隧道的主动权交给了用户，但用户需要在其PC 机上配置PPTP，这样做既增加了用户的工作量又会造成网络安全隐患。另外PPTP 只支持IP 作为传输协议。

L2F（Layer 2 Forwarding，二层转发协议）

L2F 是由Cisco 公司提出的可以在多种介质如ATM、帧中继、IP 网上建立多协议的安全虚拟专用网（VPN）的通信方式。远端用户能够透过任何拨号方式接入公共IP 网络，首先按常规方式拨号到ISP 的接入服务器（NAS），建立PPP 连接；NAS 根据用户名

等信息，发起第二重连接，通向HGW服务器。在这种情况下隧道的配置和建立对用户是完全透明的。

L2TP（Layer 2 Tunneling Protocol，二层通道协议）

L2TP结合了L2F和PPTP的优点，可以让用户从客户端或访问服务器端发起VPN连接。L2TP是把链路层PPP帧封装在公共网络设施如IP、ATM、帧中继中进行隧道传输的封装协议。

Cisco、Ascend、Microsoft和RedBack公司的专家们在修改了十几个版本后，终于在1999年8月公布了L2TP的标准RFC2661。

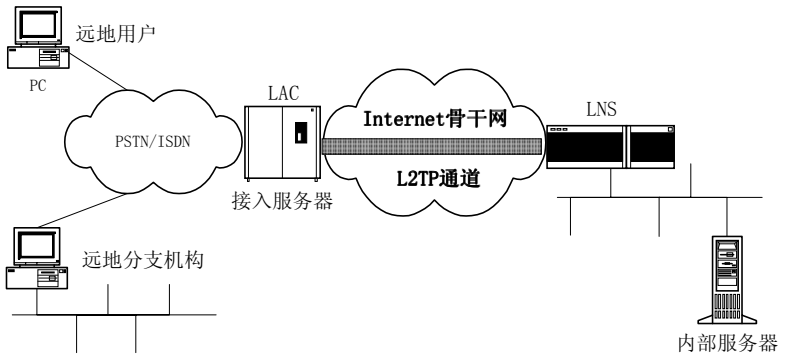
目前用户拨号访问Internet时，必须使用IP协议，并且其动态得到的IP地址也是合法的。L2TP的好处就在于支持多种协议，用户可以保留原有的IPX、Appletalk等协议或公司原有的IP地址。L2TP还解决了多个PPP链路的捆绑问题，PPP链路捆绑要求其成员均指向同一个NAS，L2TP可以使物理上连接到不同NAS的PPP链路，在逻辑上的终结点为同一个物理设备。L2TP扩展了PPP连接，在传统方式中用户通过模拟电话线或ISDN/ADSL与网络访问服务器(NAS)建立一个第2层的连接，并在其上运行PPP，第2层连接的终结点和PPP会话的终结点在同一个设备上(如NAS)。L2TP作为PPP的扩展提供更强大的功能，包括第2层连接的终结点和PPP会话的终结点可以是不同的设备。

L2TP主要由LAC(L2TP Access Concentrator)和LNS(L2TP Network Server)构成，LAC(L2TP访问集中器)支持客户端的L2TP，他用于发起呼叫，接收呼叫和建立隧道；LNS(L2TP网络服务器)是所有隧道的终点。在传统的PPP连接中，用户拨号连接的终点是LAC，L2TP使得PPP协议的终点延伸到LNS。

6.2 L2TP 协议结构

6.2.1 典型L2TP组网应用

使用L2TP协议构建的VPDN应用的典型组网如下图所示：



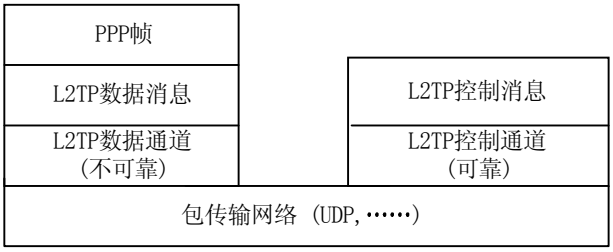
应用L2TP构建的VPDN服务

其中，LAC表示L2TP访问集中器（L2TP Access Concentrator），是附属在交换网络上的具有PPP端系统和L2TP协议处理能力的设备，LAC一般是一个网络接入服务器NAS，主要用于通过PSTN/ISDN网络为用户提供接入服务。LNS表示L2TP网络服务器（L2TP Network Server），是PPP端系统上用于处理L2TP协议服务器端部分的设备。

LAC位于LNS和远端系统（远地用户和远地分支机构）之间，用于在LNS和远端系统之间传递信息包，把从远端系统收到的信息包按照L2TP协议进行封装并送往LNS，将从LNS收到的信息包进行解封装并送往远端系统。LAC与远端系统之间可以采用本地连接或PPP链路，VPDN应用中通常为PPP链路。LNS作为L2TP隧道的另一侧端点，是LAC的对端设备，是被LAC进行隧道传输的PPP会话的逻辑终止端点。

6.2.2 L2TP协议技术细节

L2TP协议结构



L2TP协议结构

上图所示L2TP协议结构描述了PPP帧和控制通道和数据通道之间的关系。PPP帧首先被封装L2TP头部并在不可靠数据通道上进行传输，然后进行

UDP、Frame Relay、ATM等包传输过程。控制消息在可靠的L2TP控制通道内传输。

通常L2TP以UDP报文的形式发送。L2TP注册了UDP 1701端口，但是这个端口仅用于初始的隧道建立过程中。L2TP隧道发起方任选一个空闲的端口（未必是1701）向接收方的1701端口发送报文；接收方收到报文后，也任选一个空闲的端口（未必是1701），给发送方的指定端口回送报文。至此，双方的端口选定，并在隧道保持连通的时间段内不再改变。

隧道和会话的概念

在一个LNS和LAC对之间存在着两种类型的连接，一种是隧道（Tunnel）连接，它定义了一个LNS和LAC对；另一种是会话（Session）连接，它复用在隧道连接之上，用于表示承载在隧道连接中的每个PPP会话过程。在同一对LAC和LNS之间只可建立一个L2TP隧道，该隧道由一个控制连接和一个或多个会话（Session）组成。会话连接必须在隧道建立（包括身份保护、L2TP版本、帧类型、硬件传输类型等信息的交换）成功之后进行，每个会话连接对应于LAC和LNS之间的一个PPP数据流。控制消息和PPP数据报文都在隧道上传输。

L2TP使用Hello报文来检测隧道的连通性。当隧道空闲一定时间后，LAC和LNS开始向对端发送Hello报文，若在一段时间内未收到Hello报文的应答，该会话将被清除。

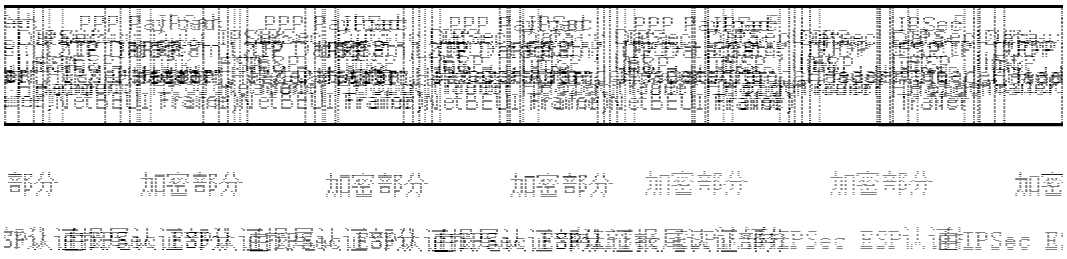
控制消息和数据消息的概念

L2TP中存在两种消息：控制消息和数据消息。控制消息用于隧道和会话连接的建立、维护以及传输控制；数据消息则用于封装PPP帧并在隧道上传输。控制消息的传输是可靠传输，并且支持对控制消息的流量控制和拥塞控制；而数据消息的传输是不可靠传输，若数据报文丢失，不予重传，不支持对数据消息的流量控制和拥塞控制。

控制消息和数据消息共享相同的报文头。L2TP报文头中包含隧道标识符（Tunnel ID）和会话标识符（Session ID）信息，用来标识不同的隧道和会话。隧道标识相同、会话标识不同的报文将被复用在一个隧道上，隧道标识符与会话标识符由对端分配。

L2TP数据封装

L2TP用户传输数据的隧道化过程采用多层封装的方法。图中表示了封装后在隧道中传输的基于IPSec的L2TP数据包格式。



L2TP数据包封装

a. L2TP封装

初始PPP有效载荷如IP数据报、IPX数据报或NetBEUI帧等首先经过PPP报头和L2TP报头的封装。

b. UDP封装

L2TP帧进一步添加UDP报头进行UDP封装，在UDP报头中，源端和目的端端口号均设置为1701。

c. IPSec封装

基于IPSec安全策略，UDP消息通过添加IPSec封装安全负载ESP报头、报尾和IPSec认证报尾（Auth trailer），进行IPSec加密封装。

d. IP封装

在IPSec数据报外再添加IP报头进行IP封装，IP报头中包含VPN客户机和服务器的源端和目的端IP地址。

e. 数据链路层封装

数据链路层封装是L2TP帧多层封装的的最后一层，依据不同的外发物理网络再添加相应的数据链路层报头和报尾。例如，如果L2TP帧将在以太网上传输，则用以太网报头和报尾对L2TP帧进行数据链路层封装；如果L2TP帧将在点-点WAN上传输，如模拟电话网或ISDN等，则用PPP报头和报尾对L2TP帧进行数据链路层封装。

f. 基于IPSec的L2TP隧道化数据的解封装过程

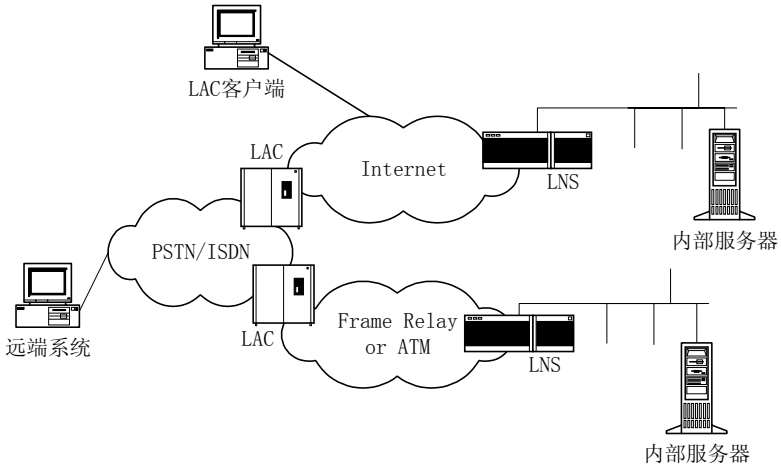
在接收到L2TP帧后，L2TP客户机或服务器将做如下解封装处理：

处理并去除数据链路层报头和报尾；处理并去除IP报头；用IPSec ESP认证报尾对IP有效载荷和IPSec ESP报头进行认证；用IPSec ESP报头对数据报的加密部分进行解密；处理UDP报头并将数据报提交给L2TP协议；L2TP协议依据L2TP报头中Tunnel ID和Call ID分解出某条特定的L2TP隧道；依据

PPP报头分解出PPP有效载荷，并将它转发至相关的协议驱动程序做进一步处理

6.3 两种典型L2TP隧道模式

远端系统或LAC客户端（运行L2TP协议的主机）与LNS之间对PPP帧的隧道模式如下图所示：



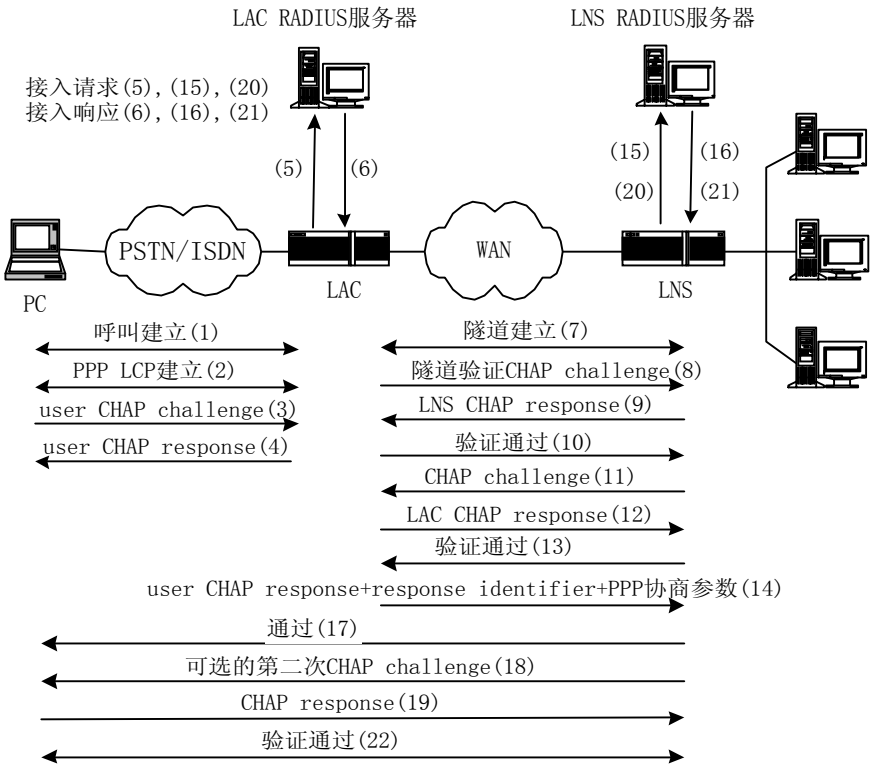
两种典型的L2TP隧道模

由远程拨号用户发起。远程系统通过PSTN/ISDN拨入LAC，由LAC通过Internet向LNS发起建立通道连接请求。拨号用户地址由LNS分配；对远程拨号用户的验证与计费既可由LAC侧的代理完成，也可在LNS侧完成。

直接由LAC客户（指可在本地支持L2TP协议的用户）发起。此时LAC客户可直接向LNS发起通道连接请求，无需再经过一个单独的LAC设备。此时，LAC客户地址的分配及AAA验证均由LNS来完成。

6.4 L2TP隧道会话建立过程

L2TP通道的呼叫建立流程可如下图所示：



b. 当用户被确认为合法企业用户时，就建立一个通向LNS的拨号VPN隧道。

c. 企业内部的安全服务器如RADIUS鉴定拨号用户。

d. LNS与远程用户交换PPP信息，分配IP地址。LNS可采用企业专用地址(未注册的IP地址)或服务提供商提供的地址空间分配IP地址。因为内部源IP地址与目的地IP地址实际上都通过服务提供商的IP网络在PPP信息包内传送，企业专用地址对提供者的网络是透明的。

e. 端到端的数据从拨号用户传到LNS。

在实际应用中，LAC将拨号用户的PPP帧封装后，传送到LNS，LNS去掉封装包头，得到PPP帧，再去掉PPP帧头，得到网络层数据包。

6.5 L2TP协议特点

灵活的身份验证机制以及高度的安全性

L2TP协议本身并不提供连接的安全性，但它可依赖于PPP提供的认证（比如CHAP、PAP等），因此具有PPP所具有的所有安全特性。L2TP可与IPSec结合起来实现数据安全，这使得通过L2TP所传输的数据更难被攻击。L2TP还可根据特定的网络安全要求在L2TP之上采用通道加密技术、端对端数据加密或应用层数据加密等方案来提高数据的安全性。

多协议传输

L2TP传输PPP数据包，这样就可以在PPP数据包内封装多种协议。

支持RADIUS服务器的验证

LAC端通过用户名和密码向RADIUS服务器进行验证申请，RADIUS服务器负责接收用户的验证请求，完成验证。

支持内部地址分配

LNS可放置于企业网的防火墙之后，它可以对远端用户的地址进行动态的分配和管理，可支持私有地址应用（RFC1918）。远端用户所分配的地址不是Internet地址而是企业内部的私有地址，这样方便了地址的管理并可以增加安全性。

网络计费的灵活性

可在LAC和LNS两处同时计费，即ISP处（用于产生帐单）及企业网关（用于付费及审计）。L2TP能够提供数据传输的出入包数、字节数以及连接的起始、结束时间等计费数据，可根据这些数据方便地进行网络计费。

可靠性

L2TP协议支持备份LNS，当一个主LNS不可达之后，LAC可以重新与备份LNS建立连接，这样增加了VPN服务的可靠性和容错性。下面把L2TP的配置分为LAC配置和LNS配置。

第七章 GRE VPN

7.1 GRE协议简介

GRE（Generic Routing Encapsulation，通用路由封装协议）在RFC1701/RFC1702中定义，它规定了怎样用一种网络层协议去封装另一种网络层协议的方法。GRE是VPN（Virtual Private Network）的第三层隧道协议，即在协议层之间采用了一种被称之为Tunnel（隧道）的技术。GRE的隧道由两端的源IP地址和目的IP地址来定义，它允许用户使用IP封装IP、IPX、AppleTalk，并支持全部的路由协议如RIP、OSPF、IGRP、EIGRP。通过GRE，用户可以利用公共IP网络连接IPX网络、AppleTalk网络，还可以使用保留地址进行网络互联，或者对公网隐藏企业网的IP地址。

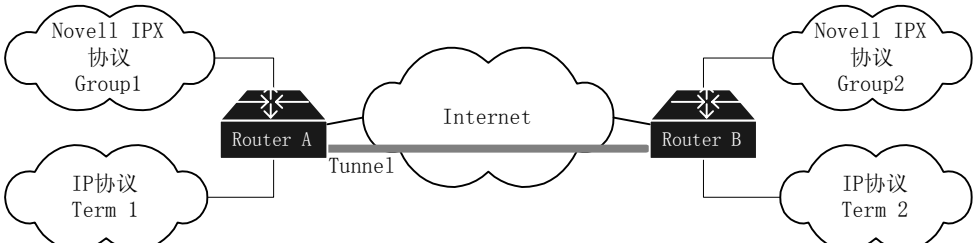
GRE在包头中包含了协议类型，这用于标明乘客协议的类型；校验和包括了GRE的包头和完整的乘客协议与数据；密钥用于接收端验证接收的数据；序列号用于接收端数据包的排序和差错控制；路由用于本数据包的路由。

GRE只提供了数据包的封装，它并没有加密功能来防止网络侦听和攻击。所以在实际环境中它常和IPsec在一起使用，由IPsec提供用户数据的加密，从而给用户提供更好的安全性。

7.2 GRE协议结构

7.2.1 GRE典型组网应用

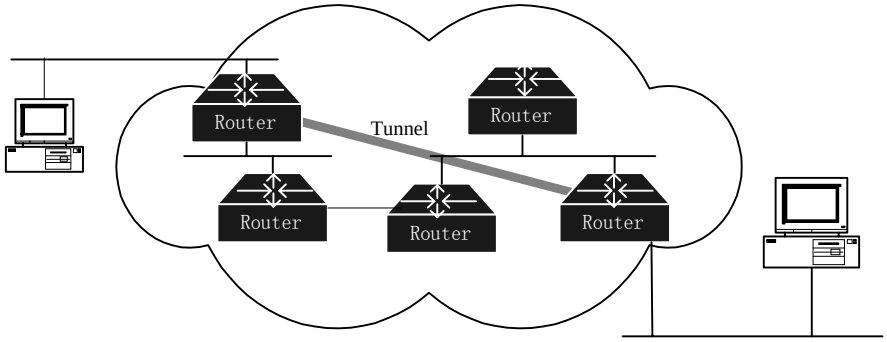
多协议的本地网通过单一协议的骨干网传输



上图中，Group1和Group2是运行Novell IPX协议的本地网，Term1和Term2是运行IP协议的本地网。通过在Router A和Router B之间采用GRE协议封装的

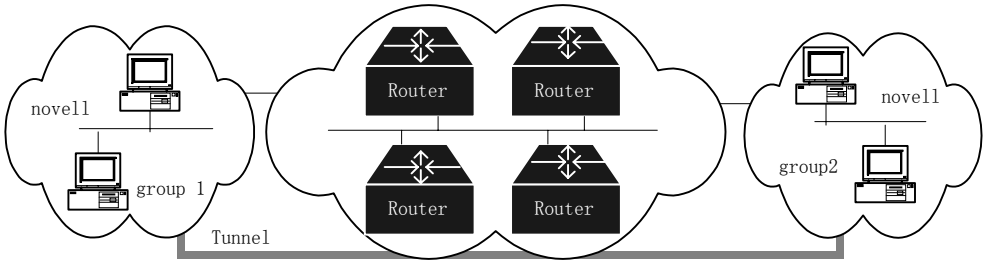
隧道（Tunnel），Group1和Group2、Term1和Term2可以互不影响地进行通信。

扩大了步跳数受限协议（如IPX）的网络的工作范围



若上图中的两台终端之间的步跳数超过15，它们将无法通信。而通过在网络中使用隧道（Tunnel）可以隐藏一部分步跳，从而扩大网络的工作范围。

将一些不能连续的子网连接起来，用于组建VPN



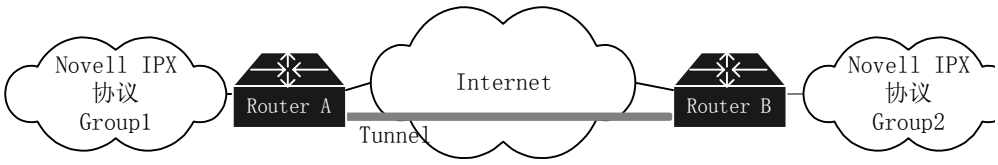
运行Novell IPX协议的两个子网group1和group2分别在不同的城市，通过使用隧道可以实现跨越广域网的VPN。

另外，GRE还支持由用户选择记录隧道接口的识别关键字，和对封装的报文进行端到端校验。

由于GRE收发双方加封装、解封装处理及由于封装造成的数据量增加等因素的影响，这就导致使用GRE会造成路由器数据转发效率有一定程度的下降。

7.2.3 GRE封装过程

一个报文要想在Tunnel中传输，必须要经过加封装与解封装两个过程，下面以图的网络为例说明这两个过程：



IPX网络通过GRE隧道互连

a. 加封装过程

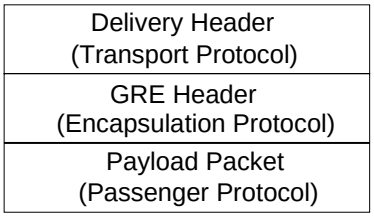
连接Novell group1的接口收到IPX数据报后首先交由IPX协议处理，IPX协议检查IPX报头中的目的地址域来确定如何路由此包。若报文的目的地址被发现要路由经过网号为1f的网络（Tunnel的虚拟网号），则将此报文发给网号为1f的tunnel端口。Tunnel口收到此包后进行GRE封装，封装完成后交给IP模块处理，在封装IP报文头后，根据此包的目的地址及路由表交由相应的网络接口处理。

b. 解封装的过程

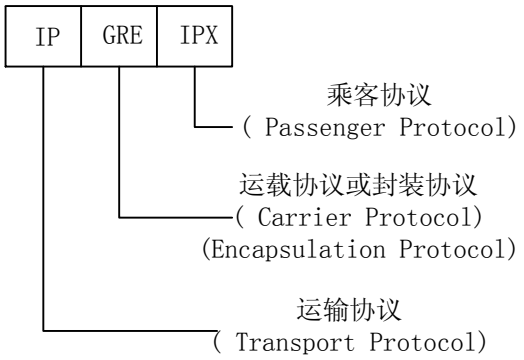
解封装过程和加封装的过程相反。从Tunnel接口收到的IP报文，通过检查目的地址，当发现目的地就是此路由器时，剥掉IP报头，再交给GRE协议模块处理后（进行检验密钥、检查校验和及报文的序列号等），剥掉GRE报头后，再交由IPX协议模块象对待一般数据报一样对此数据报进行处理。

系统收到一个需要封装和路由的数据报，称之为净荷(Payload)，这个净荷首先被加上GRE封装，成为GRE报文；再被封装在IP报文中，这样就可完全由IP层负责此报文的向前传输（Forwarded）。人们长把这个负责向前传输IP协议为传输（Delivery）协议或传输（Transport）协议。

封装好的报文的形式如下图所示：



举例来说，一个封装在IP Tunnel中的IPX传输报文的格式如下：



7.3 GRE VPN特点

优点：

加密为可选的，不象IPSec中加密是必须的，而加密方法是可选，所以大幅度减低了芯片的工作量，提高了系统性能。

更细化的QoS服务能力，包含应用层QoS。

IP层的可见性使得对应用层的带宽管理成为可能。

能封装非IP协议，如IPX和DECnet。

缺点：

通信只局限在服务商的网络中。

平面网状结构需要更多的准备开销，与基于VC的VPN具有相同的问题，就是在大型VPN上会引起N的平方问题。所以不适合大型网络的拓展。

准备与管理的开销相对昂贵。

第八章 MPLS VPN

本文对MPLS VPN只做简单的介绍，有关MPLS及MPLS VPN的内容将会有详细文档介绍。

8.1 MPLS的概念

ATM技术具有高带宽、快速交换、服务质量可靠的优点，利用ATM实现第二层的交换传输已是共识。而Internet的迅速发展也使IP成为计算机网络应用环境中既成事实的标准和开放的系统平台。因此宽带网络发展的主线是把最先进的ATM交换技术和最普及的IP技术融合起来，这种融合如果以时间发展和先进性为主线，则集中体现在IP交换、TagSwitchARIS和MPLS(Multiprotocol Label Switching多协议标签交换)技术。MPLS技术是当前最具有发展前景的宽带网络传输交换技术。

MPLS工作原理

简单来讲，MPLS技术是指：

a. 在LDP(标签分发协议)控制下，LSR(标签交换路由器)根据IP路由技术产生具有一定语意的代表数据传输路径及属性的标签(Label);

b. 应用本地标签于媒介(ATM、FR、PPP、…);

c. 多层的标签置换传输(标签堆栈);

d. 转发基于标签、入口压入标签、出口剥离标签、分组QoS、CoS等的分析仅在入口做一次，中间节点只分析标签的含义。

MPLS技术将3层网络层技术和2层交换技术完美地结合在一起，使网络既具有3层的智能，又具有2层的快速交换特性，与其他解决方案相比较，MPLS技术将第3层(路由层)的智能、灵活性和可扩展性与第二层的交换机制(不包括它面向连接的服务)结合起来，具有高效、节约资源、配置简单、减少单点故障等优点。

MPLS技术是一种创造性的高性能包发送新技术，它将"标签"分配给多协议的数据帧，以便在基于包或信元的网络中传输。MPLS是建立在"标签交换"概念的基础之上的，数据单位(例如包或信元)携带一固定长度的短标签来告诉交换节点如何处理该数据。

MPLS互联网络的构成部件

a. 标签边缘路由器(LER)：边界边缘路由器位于服务提供商网络的边界，执行增值的网络服务并将标签加到数据包上。

b. 标签交换机：标签交换机根据包或信元标签进行交换。除了支持MPLS外，它们还可能支持全面的第3层路由或第2层交换。

c. 标签分布协议(TDP)：与标准的网络层路由协议相结合，TDP用来在标签交换网中分配标签信息。

MPLS的技术核心

MPLS的核心思想：边缘的路由，核心的交换。

标签交换机是MPLS互联网络的核心。标签即是短的固定长度的标签，使IP+ATM交换机能进行简单快速的表查询。这样就使得标签交换机能利用快速的硬件技术(包括ATM信元交换)完成查表和发送功能。

MPLS技术可在各种介质上使用。由于MPLS技术隔绝了标签分布机制与数据流的关系，它支持众多的物理和链路层技术。对于ATM，标签放置在虚拟路径标识符 虚拟隧道标识符(VPI/VCI)字段的ATM信元报头中。如果在点对点协议(PPP)中使用，标签就安置在第2层和第3层(即IP)报头之间。这种设置使得MPLS技术可在各种介质上使用，包括ATM链路、SONET包传输链路、以太网等。

MPLS并不只是面向IP的，由于路由协议是分开的，标准的MPLS技术可用来支持多个第3层协议(如IPv4和IPv6)。标准的路由器配置了MPLS软件后，就可起标签交换机的作用。能通过支持TDP，并根据标签值将各种功能添加到交换机的包上，Internet核心路由器就可加入到标签网络的主干网中。对于现有的路由器，这种方式将MPLS的显式路由和IP VPN功能引入到纯路由器的Internet中，这对目前的功能来说是很大的加强。要获得这些流量规划的好处并不需要单独的第2层交换主干网。

MPLS的主要特点

a. 结构的灵活性。它可以同时支持路由器与ATM交换机，从而不会失去B-ISDN的原有功能。另外，MPLS不受制于硬件平台，同样支持POS技术。因此，它可以随硬件技术共同发展。MPLS与B-ISDN使用同样的交换，它不受制于传输介质。网络层同时也不受制于链路层。

b. 增强的可扩展性传统的IP与ATM的结合是依靠中间层的翻译。这种方式带来了一系列的后果，如虚电路"N的平方"问题等。而MPLS有效地解决了这一系列的问题，使ATM的可扩展性得到了提高。

c. 直接在ATM交换上进行IP服务，这就允许提供RSVP、多点广播以及未来IP的服务。MPLS已被证明是大型网络可扩展性的最佳解决方案。

8.2 MPLS VPN技术

基于MPLS的VPN的组成

MPLS VPN模式支持网内所有地点之间的全互连通信。当多个用户共享同一个IP骨干网时，可以通过使用边界网关协议BGP的归属群体(community-of-interest)属性来指定属于同一个VPN的路由器。服务供应商则可以设置策略来规定VPN网内的路由信息的传播只限于网内的路由器。

用户端路由器只与服务供应商本地POP的路由器相连，而不是与VPN中的每一个其它的节点相连，POP的路由器只接收并保持与其直接相连的路由器的有关VPN的路由信息。所以用户在管理自己的VPN时会发现使用MPLS模式时路由配置非常简单。他们可以把服务供应商的骨干网当作到他们所有地点的缺省路由来使用，而不需要与非常复杂的、包括了大量第二层PVC或第三层路由表的网络打交道。

基于MPLS的VPN的工作过程

基于MPLS的VPN，其框架结构的基本思想是：定义供应商核心路由器PE(ProviderEdge)、用户端路由器CE(CustomerEdge)、骨干网核心路由器P(Provider)三种路由器。其中在CE/PE、PE/PE之间使用BGP协议作为路由控制协议，这其中CE/PE之间属于BGP自治域间会晤，即EBGP;PE/PE之间属于BGP自治域内会晤，即IBGP。PE/P之间可以使用IETF为MPLS定义的任何路由控制协议，即可以使用LDP(标签分配协议)/RSVP(资源保留协议)或其它控制协议。

第一，用户端路由器(CE)首先通过静态路由或BGP将用户网络中的路由信息通知供应商路由器(PE)，同时在PE之间采用BGP的Extension传送VPN-IP的信息以及相应的标记(VPN的标记，称作内层标记)，而在PE与P路由器之间则采用传统的内部网关协议IGP协议相互学习路由信息，采用LDP协议进行路由信息与标记(骨干网络中的标记，称作外层标记)的绑定。此时CE、E以及P路由器中基本的网络拓扑以及路由信息已经形成了。PE路由器拥有了骨干网络的路由信息以及每一个VPN的路由信息。

第二，当属于某一VPN的CE用户数据进入网络时，在CE与PE之间连接的接口上可以识别出该CE属于哪一个VPN，从而到该VPN的路由表中去读取下一跳的地址信息，与此同时，在前传的数据包中打上相应VPN的VPN标记(内层标记)。这时得到的下一跳地址为与该PE作Peer的PE的地址，为了达到这个目的端的PE，此时在起始端PE中需读取骨干网络的路由信息，从而得

到下一个P路由器的地址，同时采用LDP在用户前传数据包中打上骨干网络中的标记(外层标记)。

第三，在骨干网中，初始PE之后的所有P均只读取数据包中的外层标记的信息来决定下一跳，因此在骨干网中P路由器只是作简单的标记交换。P路由器上不运行BGP，也不区分不同的VPN。

第四，在达到目的端PE之前的最后一个P路由器时，该P路由器将数据包的外层标记去掉，读取内层标记(VPN标记)，从而确定数据包所属的VPN，随之将该数据包送至相关的接口上，进而将数据包传送到VPN的目的地址处。

基于MPLS的VPN的优点

MPLS能识别不同种类的应用的数据包这点，保证了QoS的实现，而且实现方法比IP隧道和基于VC的网络简单。因为在IP网络上建设VPN需要隧道或加密，而基于VC的网络(如ATM和帧中继)所建的VPN是点对点的，需要为每个CPE进行单独的配置。另外因为在这种网络上的IP数据包的传输是在VC通道内进行的，所以整个VPN并不知道通信的内容和种类。这种方式下，需要智能化和有策略配置的边界设备，可以给每个通信最大的VC带宽。而且这种方式是以连接为中心的，不具备可扩展性。而且还与IP的商业应用是冲突的，因为IP的商务应用是围绕无连接的TCP/IP协议的。VPN还应当能识别通信的类型，从而将通信根据应用分类。而且VPN应当对VPN的整个网络的存在有了解，这样服务商可以将不同用户和服务分组到IntranetVPN或ExtranetVPN。

MPLS完全可以隔离无关用户的通信，使得无关用户的通信不会混杂，从而提高了安全性。这是在不必使用隧道和加密的前提下就能完成的。MPLS根据服务类型区分的传输方法和完全的QoS策略使得服务商的原来面向传输的服务模型转变成为重点集中于服务变化的模型。

基于MPLS的网络能够将数据流分开，无需建立隧道或加密即可提供保密性，基于MPLS的网络，以网络到网络的方式提供保密性，为用户提供服务。这将支持服务供应商实现从面向传输的模式到面向服务的模式转变。基于MPLS的VPN提供了逻辑上最大的安全性，网络的安全性是由BGP、IP地址方案、可选的IPSec加密三方面结合而成的。

MPLS VPN不仅满足VPN用户对安全性的要求，还减少了网络方和用户方的工作量，可以建立任意的连接，且具有很好的网络可扩展性。VPN用户可以延用原有的专用地址，不需要作任何修改，在骨干网络采用VPN-ID，可以保持全网的唯一性。MPLSVPN还易于提供增值业务，如不同的COS等。

VPN技术参考读物

1. VRP3R001M03配置指导-07-VPN-VPN配置

Quidway路由器的IP Sec、IKE、L2TP VPN、GRE VPN配置命令及详细配置案例。

2. RFC2764

是IP VPN的一个框架性文件，对VPN的体系结构有详细的描述。

3. 网络基础知识培训教材-课程13 VPN、L2TP协议

介绍了VPN的一些基本概念和原理，并介绍了VPN的重要组成部分L2TP协议。在Support网站上数通工程师资料上可以找到。

4. 网络安全与VPN技术V10

介绍了常用的网络安全技术和VPN技术。在Support网站上数通工程师资料上可以找到。

5. http://www.cisco.com/pcgi-bin/Support/PSP/index.pl?i=Technologies

Cisco 网站上有关技术的介绍。不单是对Cisco产品的介绍，对技术标准和相关技术参考读物都有链接或介绍。在Security部分有关于Generic Routing Encapsulation (GRE)、IP Security (IPSec) 、Layer Two Tunneling Protocol (L2TP) 、MPLS for VPNs等的详细资料和参考读物链接。值得一看。