通过L2TP实现虚拟专用网

国家数字交换系统工程技术研究中心　曾勇军　杨贞斌　罗兴国

虚拟专用网技术是当前的热点技术之一，受到了人们的广泛关注，其研究和开发具有十分重要的意义。本文分析了L2TP协议的特点，并描述了通过L2TP协议实现虚拟专用网的网络结构、隧道实现方式以及会话通信过程。

虚拟专用网技术

虚拟专用网(Virtual Private Network，简称VPN)随着INTERNET以及远程接入技术的发展而得到了广泛的应用。它采用了所谓的“隧道”技术，利用公网的传输带宽建立企业的专用网络，允许移动用户、远程办公用户及小的办公室利用VPN技术建立的隧道访问公司的网络，提供了一种安全、可靠的虚拟组网方式。

基于标准的虚拟专用网技术近年来已经成为网络界的新热点，受到了人们的广泛关注。Infonetics Research公司预言，从现在起到2001年，VPN市场每年至少增长一倍。到了2001年，这个市场将达到120亿美元。VPN的蓬勃发展，使得各个远程接入设备的厂家纷纷加入到相应技术的研究开发中去，形成了自己的产品，同时这又给VPN的发展带来了新的动力。

通过隧道实现的接入VPN技术具有以下的优点：

1. 用户通过本地接入系统建立与INTERNET的连接，本地接入系统可以通过隧道技术与公司的网络相连。故用户只需付本地接入费用，不用长途拨号连接公司本地的接入服务器即可与公司的应用服务器进行通信。VPN利用公网的传输特性作为专网的延续，节省了昂贵的长途通信费用。

2. 传统的远程拨号网络服务只支持注册的IP地址，限定了用户对公司网络的访问。而VPN的实现支持多种网络层协议和没有注册的专用IP地址，利用隧道技术很好地解决了INTERNET公网与专网的兼容性问题。隧道在连接的两端产生，在发送端将数据封装成IP数据报，通过公网传送给遂道的接收端点，接收端点按照同样的顺序解开数据报。专网的特性隐藏在隧道之中，对用户是透明的。

3. 支持多种接入方式，如PSTN/ISDN拨号接入、XDSL、Cable Modem、DDN、FR等。

4. 具有很强的灵活性和扩展性。

支持多种隧道实现方式，并且网络是动态的，可以随时增减用户，便于集中控制访问权限。

5. 节省网络建设费用。各个公司组建自己的网络只需购买少量的设备如路由器、服务器即可，其维护、升级费用较低。

VPN技术的显著优点不仅给公司带来了巨大的利益，而且给ISP和电信运营商提供了新的商业机会，可利用VPN吸引更多的用户，提高竞争力。

L2TP实现VPN的拓扑结构

L2TP协议实现VPN的网络拓扑结构如图1所示:

远端系统为连接到电路交换网(如PSTN)的终端系统或路由器。当远端系统要求与公司网络通信时，隧道的建立发生在LAC与LNS之间，对该系统是透明的。

LAC是L2TP的接入集中器，为远端系统提供隧道服务。LAC一端连接PSTN/ISDN，另一端连接INTERNET，负责将PPP帧封装在L2TP报文中，通过隧道传送给LNS。LAC可以利用隧道传送任何封装在PPP中的网络层协议数据单元，是输入呼叫的起始方和输出呼叫的接收方。典型的，LAC可以是一个配置有L2TP协议的网络接入服务器。

LAC客户是连接到INTERNET上的主机，包含有LAC客户软件，它可以完成隧道的建立、维护及释放的工作，并不需要LAC。LAC客户支持L2TP协议，当LAC客户初始化隧道和呼叫时，LAC客户就成为LAC。

LNS是L2TP的网络服务器，负责建立、维护、释放隧道和呼叫，处理服务器方的L2TP协议，终止L2TP和PPP。LNS连接INTERNET公网和公司的专网，是输入呼叫的起始方和输入呼叫的接收方。

RADIUS(Remote Authentication Dial In User Service)服务器完成用户的身份认证、授权及计费的功能。用户的身份认证可以发生在LAC的RADIUS服务器和LNS的RADIUS服务器。LAC的RADIUS服务器承担部分认证的任务，成为RADIUS的代理，是LNS的RADIUS服务器的客户机。而LNS的RADIUS服务器则完成用户身份的认证及地址分配、呼叫授权的功能。

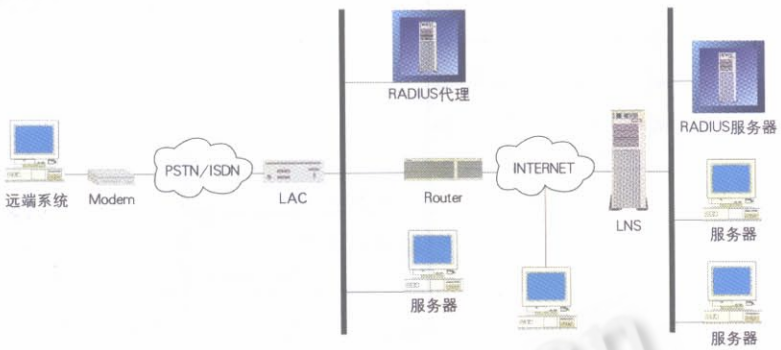

图 1 L2TP实现VPN的网络拓扑结构

隧道的实现方式

基于L2TP的VPN技术包含有两种隧道实现方式: 一种是LAC或LAC客户初始化的隧道实现方式，完成输入呼叫的功能; 另一种是LNS初始化的隧道实现方式，完成输出呼叫的功能。

1. 输入呼叫的隧道实现方式

(1)LAC初始化方式。这种方式的隧道建立过程是由LAC来完成的。远端系统只需向LAC拨号，建立PPP的连接，然后由LAC建立一条通往目的LNS的隧道。

在这种隧道建立方式中，由于隧道在LAC和LNS之间产生，因而对远端系统的软件构成没有限制，只需加载TCP/IP协议以及普通的远程拨号软件即可; 并且远端系统可以同时建立多条隧道，与多个公司同时通信。其主要缺点在于这种通信方式只能依赖于支持L2TP协议的服务提供者ISP，不能随意选择。

(2)客户初始化方式。这种方式由LAC客户自己完成隧道的建立、控制与管理的工作，对ISP是透明的。这种隧道的实现方式也称为“自愿”隧道。由于LAC客户是INTERNET上的一台主机，因此在通信过程中建立了一个虚拟的PPP连接，形成一条通往目的LNS的隧道，通过该隧道在LAC客户与LNS之间传送PPP帧。

这种方式只能用于隧道技术，可实现端到端的安全隧道，不依赖ISP提供的服务。但是这种方式的每一个工作站都有自己的隧道，因而LNS需要大量的隧道满足用户的连接请求，并且每一个客户同时只能开通一条隧道。

2. 输出呼叫的隧道实现方式

L2TP提供了一种输出呼叫的功能，

可以由LNS建立通往某个LAC或LAC客户的隧道，完成公司与移动用户或小型办公室的通信。

这种通信方式中隧道以及呼叫的建立是由LNS来触发完成的。隧道的建立可以使用相同的控制报文交换机制，而会话的建立过程可以使用一组输出呼叫控制报文来完成。

典型的L2TP会话通信过程

典型的L2TP会话通信过程如图2所示。此处主要考虑了远端系统(如远程拨号用户)通过LAC初始化的隧道与公司的服务器通信的情形，并对隧道的建立过程进行了详细的描述。

1. 呼叫建立

远程用户首先在自己的PC机上配置TCP/IP协议并形成一拨号程序，运行该程序拨入LAC的号码。若呼叫成功，则在用户与LAC之间建立了一条物理链路，以承载数据信息。

2. 会话建立过程

远程用户的PC与LAC的PPP协议交换LCP(Link Control Protocol)配置请求分组，以在物理链路上建立、配置和测试数据链路连接。当远程用户的PC与LAC均发送和接收了LCP配置确认分组后，LCP自动机进入了OPENED状态，PPP进入认证阶段。此时可以使用LCP协商的认证协议如PAP、CHAP完成用户的身份验证。图2描述了PAP协议的认证过程。RADIUS代理服务器可以根据用户输入的用户名决定是否需要建立隧道以及确定LNS的IP地址。例如，若用户输入的用户名为zyj@ndsc.com.cn，则LAC知道用户为远程用户，需要建立隧道

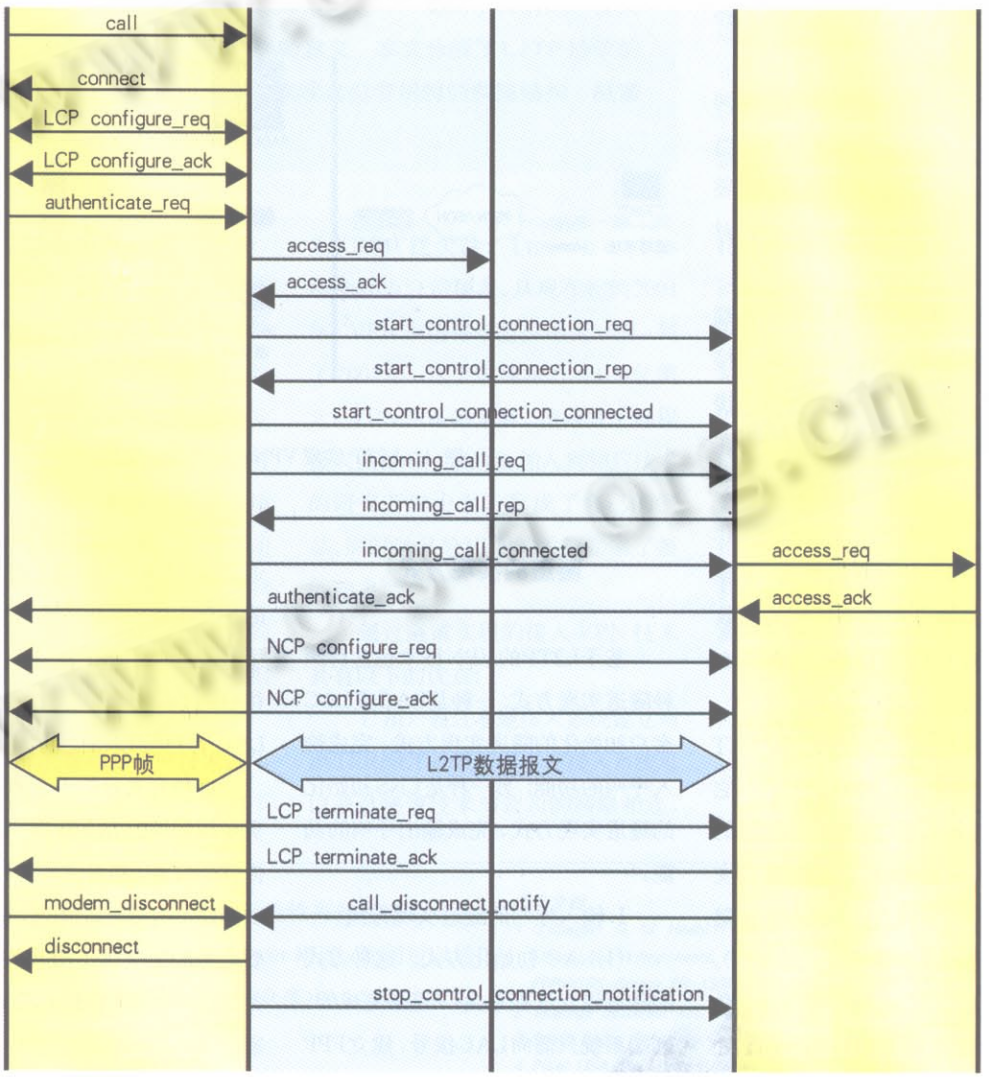

图 2 会话建立过程

承载用户数据。目的端点的地址为ndsc.com.cn,验证其合法性并查找对应的IP地址。LAC能确定到目的LNS的隧道是否存在。若隧道存在，则直接进行会话通信；若隧道不存在，则使用控制连接管理报文建立一条隧道，并使用RADIUS代理服务器分配的隧道标识号识别该隧道。为了建立一个隧道，LAC发送一个Start-Control-Connection-Req报文给LNS服务器，请求建立一条隧道，LNS回答Start-Control-Connection_Req，指示接受隧道建立的请求。最后，LAC发送控制报文Start-Control-Connection-Connected完成隧道建立的工作。在此阶段，可以完成可选的隧道端点认证的工作。

在L2TP隧道中存在许多标识符识别参与会话的每一个用户，该标识符的分配是由L2TP控制报文中的一组呼叫管理报文来完成的。LAC向LNS发送一个L2TP的Incoming-Call-Req报文，请求建立一个会话。LNS发送报文Incoming-Call-Req响应用户的请求，LAC发送了Incoming-Call-Connected完成会话的建立的工作。此后，可以用分配的会话标识识别该用户对应于哪一个会话，以正确地传送数据报。

完成了隧道及会话的建立之后，用户和LNS之间的端到端的连接已经存在，PPP链路可以重新开始协商。一旦LNS和用户之间的LCP选项被重新协商，LNS使用Set-Link-Info控制报文通知LAC已经改变的选项。

对于没有信任关系的LAC和LNS，隧道服务器必须对用户的身份进行认证。LNS的认证机制可以与LAC的认证机制一致。根据LAC传送来的用户信息，LNS的RADIUS服务器查找用户数据库，验证用户的身份，并进行授权的操作。

在认证结束之后，用户和LNS之间必须协商PPP的NCP(Network Control Protocol)协议配置选项，如分配IP地址、协商TCP/IP头部压缩选项，以配置网络层协议。此后，远程用户与LNS可以进行实际的数据通信。

3. 数据传输

从用户来的数据首先封装在PPP帧中，然后发送给LAC。LAC识别对应于该用户的端口，选择合适的隧道和会话标识，将PPP帧封装在L2TP的数据报文中，转发给LNS。LNS收到该报文后，去掉L2TP的封装，取出PPP帧的信息域，递交给合适的网络层协议，按目的地址传送给对应的LAN服务器。

下行数据传输时，LNS将IP数据报路由到合适的PPP会话，执行L2TP封装的工作，然后将L2TP数据报文递交给对应的LAC。LAC根据隧道标识和会话标识能够识别将数据递交给哪一个接口，传送给远程用户。

4. 终止会话

当用户想断开链路时，可以向LNS发送LCP Terminate_Req分组，请求断开PPP连接。该分组与其他分组一样，封装在L2TP隧道中传送给LNS。LNS收到该分组，发送LCP Terminate-Ack终止链路。LNS知道用户已经终止了本次会话，于是发送L2TP Call_Disconnect_Notify控制分组给LAC，以释放会话。

LAC和LNS可以设置一个超时计时器，在足够长的时间内没有数据传送时，将自动释放一个会话。这确保了在用户关闭了他的PC但没有发送LCP终止分组的情况下，仍然可以终止L2TP会话。

当隧道中不存在会话时，可以发送控制报文Stop-Control-Connection-Notification拆除隧道，以节省网络资源。

结束语

L2TP协议的出现和完善，不仅能为虚拟专用网的实现提供了一种统一的标准，而且为多个厂商的产品互相通信提供了可能。L2TP实现加上IPSec技术，则为用户提供了一个安全、可靠、价格低廉的虚拟专用网络实施方案。目前，Cisco、Microsoft、Ascend、3com及Cabletron公司都宣布支持L2TP协议，可见，基于L2TP的虚拟专用网络技术的前景十分光明。■

参考文献

1 Townsley W,M,Valencia A,Pall G,S,Zorn G,and Palter B "Layer Two Tunneling Protocol L2TP",RFC2661,August 1999.

2 Simpson W The Point-to-Point Protocol(PPP),RFC1661,1994

3 Rigney C,Rubens A,Simpson W,Willens S Remote Authentication Dial In User Service (RADIUS),RFC2138,1997

4 Lloyd B,Simpson W PPP Authentication Protocol,RFC2334,1992