L2TP虚拟专用网*

余 堃**[1] 谭兴烈[2] 周明天[1]

(1. 电子科技大学计算机科学与工程学院 成都 610054; 2. 四川大学数学学院 成都 610064)

【摘要】从L2TP协定入手，介绍了L2TP协议的基本技术和拨号访问服务器及L2TP网络服务器，详细阐述了在此基础上建立的认证模块、日志模块和LAC模块，并对用L2TP创建VPN进行了探索，在多种UNIX环境下建立了原型，积累了建立VPN的经验，为其他VPN的建立打下了基础。

关 键 词 虚拟专用网; 第二层隧道协议; 隧道; L2TP集中器; L2TP网络服务器

中图分类号 TP393.08

A L2TP VPN

She Kun[1] Tan Xinglie[2] Zhou Mingtian[1]

(1. College of Computer Science and Engineering, UEST of China Chengdu 610054;
2. Mathematics College of Sichuan University Chengdu 610041)

Abstract Virtual private network is the key technology of next generation Internet, L2TP is a dialup virtual private network specification which was defined by IETF. Its design and implementation are very significant. From the L2TP, basic technology and two kinds of servers of L2TP(LAC server and L2TP net server) are introduced and L2TP function models(authentication model、log model and LAC model) on this are expatiated. Based on this, a L2TP scheme was suggested and developed on a few UNIX latforms.

Key words virtual private network; L2TP; tunneling; LAC; LNS

虚拟专用网络(VPN)最简单的定义就是在公众数据网络(如Internet)上建立属于自己的专用数据网路，即不再使用长途数据专线建立专用数据网络，而是将其建立在拥有完善架构的公众数据网络上。虚拟是指企业之间不再拥有物理上直接相连的专用数据线路，而是使用Internet之类的公众数据网络基础设施。专用数据网络是指企业可以做一个最符合自己需求，可以自己控制的网络。

虚拟专用网不是新概念，X.25、Frame Relay等公众数据网络早就提供了VPN服务，但相关的终端通信设备不但成本高，且管理与设定也很烦琐，因此并没有流行起来。现在的Internet虚拟专用网络可以利用廉价的电话网、校园网等，再加上Internet本身的开放性和潜在的安全威胁，Internet 上的VPN则成为下一代Internet发展的关键技术。

虚拟专用网络主要采用隧道、加解密、密钥管理和身份认证四项技术，其中隧道技术是核心，其他三种是用来加强隧道技术的。

隧道技术是为了将专用数据网络的资料在公众数据网络上传输而发展出来的一种资料打包方式(Encapsulation)，亦即在公众网络上建立一条秘密通道。目前隧道技术所使用的协定主要有Ipsec、

2002年5月7日收稿
* 国家863高科技项目
** 男 34岁 硕士 副教授 硕士生导师

PPTP及L2TP等三种[1~3]，Ipsec 为第三层的穿隧技术，专门为IP所设计，不但符合现有Ipv4的环境，同时Ipv6也可使用[4]。PPTP与L2TP均为第二层的穿隧技术，适合具有IP/IPX/AppleTalk等多种协定的环境，前者是用户发起隧道，后者隧道对用户屏蔽，由第三方ISP与企业共同提供。本文只讨论L2TP，其他VPN协议将另撰文讨论。

1 L2TP技术

图1显示了L2TP的网络结构，L2TP提供了拨号VPN服务。LAC(L2TP访问集中器)相当于拨号访问服务器，而LNS(L2TP网络服务器)是企业提供L2TP服务的服务器。LAC与LNS之间是公共数据网络，如Internet、X.25、Frame Relay和ATM等L2TP使用了控制消息和数据消息两种类型。控制消息用于隧道的创建、维护及清空和调用。数据消息用于将隧道上运送的PPP帧打包[5]，控制消息使用可靠的控制信道传输。数据消息使用不可靠的数据信道，在传输过程中有包丢失，不会重传，其协议结构如图2所示。

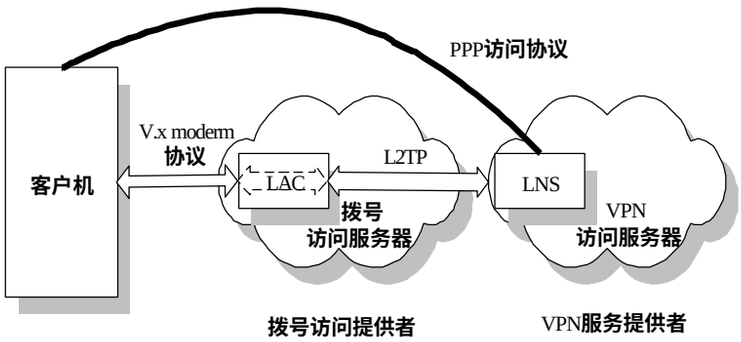

图1 拨号VPN隧道

图2描述了PPP帧在L2TP控制和数据信道上的关系，PPP帧首先加上L2TP头封装，这个包的传输用UDP、帧中继、ATM等，在一个不可靠的信道上传输，控制消息在一个可靠的信道上传输。

用L2TP服务模块入隧一个PPP会话，其步骤如下：

1) 为一个隧道创建一个控制连接；

2) 通过入、出站的调用请求触发创建一个会话。

隧道和相应的控制连接必须在出、入站调用初始化之前进行创建，一个VPN会话必须在VPN能开始入遂PPP帧之前创建。多个会话可以在一个单一的隧道上存在，同时在一个LAC和LNS之间存在多个隧道，如图3所示。

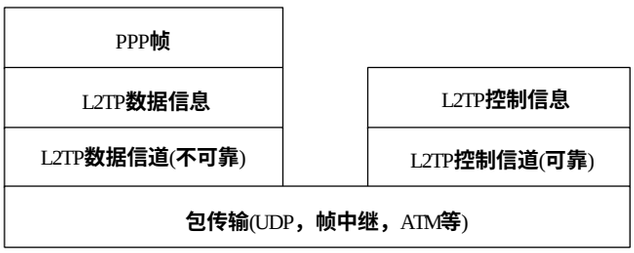

图2 协议结构

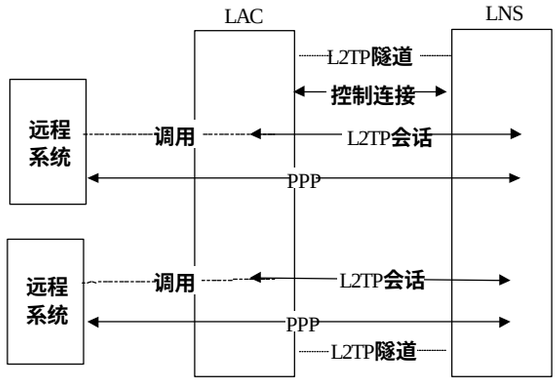

图3 PPP帧的入遂

2 L2TP功能模块

本文的L2TP系统由认证模块、日志模块、LAC模块和LNS模块组成。其中认证、日志模块是共用模块，LAC和LNS都要使用，如图4所示。

2.1 认证模块

认证模块有一个极为重要的数据资源：用户认证数据库，库中由多个用户信息记录组成。每一个用户记录由用户号、用户组、用户真实姓名、用户认证协议、用户使能状态构成和CHAP共享秘密组成[6]。当然，这里的用户对LNS而言是LAC，对LAC而言是LNS，认证服务的工作原理如图5所示。

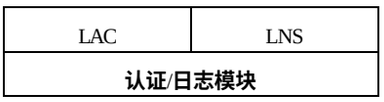

图4　L2TP系统功能模块

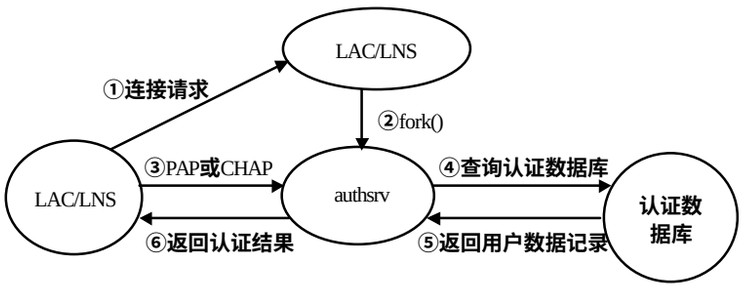

图5　认证服务的工作原理

2.2 日志模块

日志模块作为一个函数库使用，如WrSysLog()接口，日志功能是成熟系统的一大标志。在如此复杂的系统中，日志将在系统审计中起重要作用。本系统不仅提供一般的系统日志，还对L2TP的包进行分类分级，如系统日志、数据包(包括PPP)日志和控制包日志都以独立的日志文件存在，在必要的时候，通过日志级别可审计不同的日志。

2.3 LAC模块

限于篇幅，本文只给出如图6所示的隧道连接工作流程。图中，当一个入站调用请求到达时(如电话拨号)，由LAC生成入站调用消息；检测LNS的连接，如果没有建立，则初始化到LNS的连接，

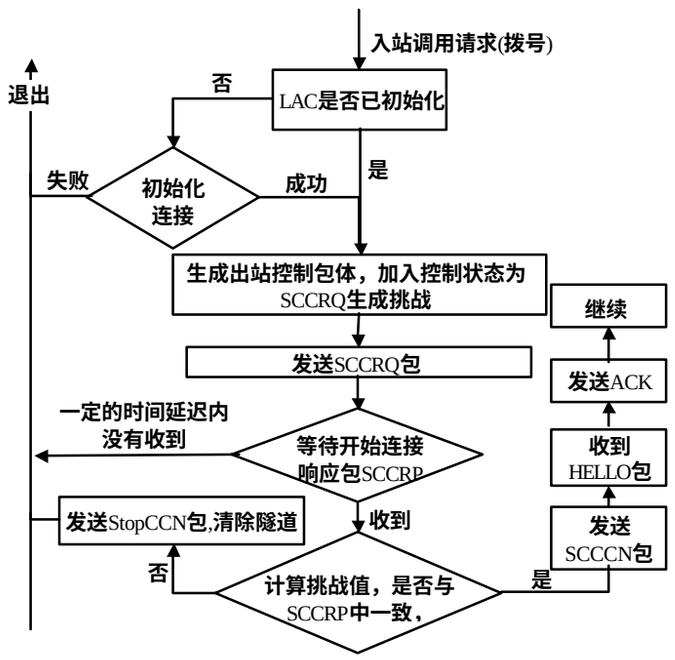

图6　LAC端控制连接的实现流程图

构造滑动窗口队列的大小；生成新的出站控制包，加入控制消息，设置状态为SCCRQ，生成挑战，并标示要挑战对方的位为真，但此时并不能预测响应，因为不知道对方的主机名；发出开始控制连接请求包(SCCRQ)，等待开始控制连接响应包(SCCRP)；当收到一个开始连接的响应，如果一切正常，根据SCCRP的主机名和本文的主机名计算挑战值，如果与SCCRP中的期望值一致，就发送开始控制连接包(SCCCN)，否则发送停止控制连接包(stopCCN)，清除隧道；等待HELLO包；在一定的时间延迟内，如果收到HELLO包，则创建成功，发出ACK包，否则创建控制连接失败，清除隧道。

2.4 LNS模块

图7给出了LNS端控制连接的实现过程。图中，当收到一个SCCRQ的请求时，首先检查SCCRQ是否可以接收，如果是，则生成一个新的控制连接响应包，生成挑战值，并在包中指明期望的响应值，发出SCCRP包，否则发出stopCCN包，清除隧道；等待接收SCCCN包，看是否可以接收，如果是则计算挑战值，如果与SCCCN中的期望值一致，发出HELLO包，等待；如果收到ACK包表明控制连接创建成功。

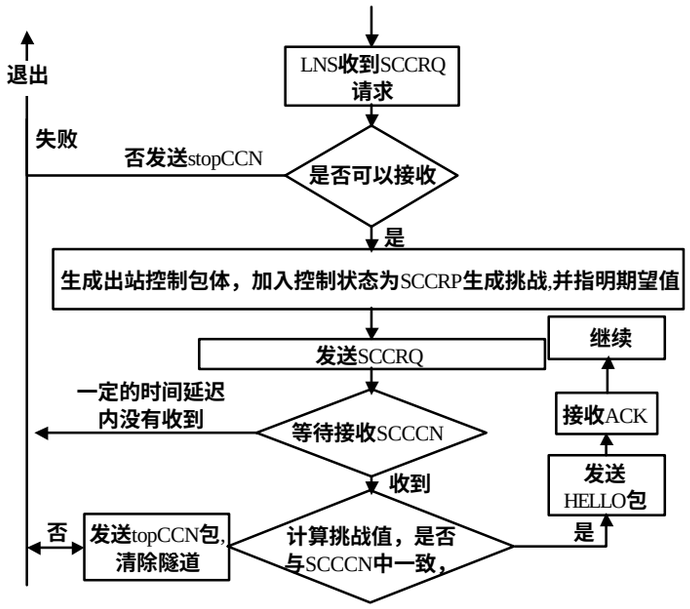

图7 LNS端控制连接

3 结 束 语

随着L2TP的不断完善， VPN技术得到了广泛的应用。本文对L2TP创建VPN进行了探索，并在多种UNIX环境下建立了原型，积累了建立VPN的经验，为其他VPN的建立打下了基础，基于L2TP的虚拟专用网技术的前景十分光明。

参 考 文 献

1 Kent S, Atkinson R. Security Architecture for the Internet Protocol(RFC 2401), 1998

2 Hamzeh K, Pall K, Verthein W, *et al.* Point to Point Tunneling Protocol(draft-ietf-pppext-pptp-0.2.txt), 1998

3 Townsley W M, Valencia A, Rubens A, *et al.* Layer Two Tunneling Protocol — L2TP(draft-itef-pppext-12tp-10.txt), May, 1999

4 Deering S, Hinden S. Internet Protocol, Version 6 (IPv6) Specification(RFC 1883), 1995

5 Simpson W. The Point-to-Point Protocol(RFC 1661), 1994

6 Simpson W. PPP Challenge Handshake Authentication Protocol(RFC 1994), 1996