文章编号：1005-8451（2009）11-0029-03

VPN技术在铁路办公系统的应用

张 燕

（中国铁通 南昌铁道通信事业部，南昌 330003）

摘 要：L2TP VPN和MPLS VPN都是IP VPN技术，L2TP VPN利用公用数据网建立数据传输隧道，在远程用户之间提供对第2层协议的中继，提供实现远程专用虚链路的技术，MPLS VPN将ATM快速交换技术和IP动态路由协议结合起来，简化核心路由器的路由选择方式，构造宽带的Intranet，Entranet，满足多种灵活的业务需求。介绍这2种VPN技术在铁路局站段VPN办公系统的应用。

关键词：L2TP；MPLS；办公系统；研究

中图分类号：C931.4 文献标识码：A

Application of VPN technology to Raiway Office System

ZHANG Yan

(Nanchang Railway Communication Department of China Tietong Telecommunication Corporation, Nanchang 330003, China)

Abstract: L2TP VPN and MPLS VPN were IP VPN technology, L2TP was a technique which forwarded layer 2 Protocol Data Units (PDUs), especially PPP, through a data transfer tunnel established on top of public data network services, so as to provide a means for setting up layer 2 virtual leased links. MPLS technique, combined with the fast ATM and dynamic IP routing protocol, was simplified route choose of core routers, constructed wideband Intranet, Extranet, and satisfied flexible applications. It was introduced the application of L2TP VPN and MPLS VPN in VPN System of railway administration.

Keyword: L2TP; MPLS; Office System; research

办公自动化是企业信息化的重要部分，实现对企业办公事务的科学管理。本文主要介绍L2TP VPN和MPLS VPN 2种IP VPN技术以及它们在铁路局管内站段办公系统中的研究应用。

1 L2TP VPN概述

1.1 L2TP简介

L2TP（Layer Two Tunneling Protocol，第2层通道协议）是一种工业标准的Internet隧道协议，它利用公用数据网建立数据传输隧道，在远程用户之间提供对第2层协议（特别是使用极广的点到点协议（PPP））的中继，提供实现远程专用虚链路的技术，即将第2层数据单元，如点到点协议（PPP）数据单元，封装在IP或UDP载荷内，以顺利通过包交换网络（如Internet），抵达目的地。

1.2 L2TP VPN组成

（1）VPN用户

指通过L2TP协议连入VPN的用户。

（2）L2TP访问集中器（LAC）

L2TP Access Concentrator，为L2TP的接入设备，它提供各种用户接入的AAA服务，发起隧道和会话连接的功能，以及对VPN用户的代理认证功能，它是提供VPN服务的接入设备，在物理实现上，它既可以是配置L2TP的路由器，或接入服务器也可以是专用的VPN服务器。

（3）L2TP网络服务器（LNS）

L2TP Network Server，为L2TP企业侧的VPN服务器，该服务器完成对用户的最终授权和验证，接收来自LAC的隧道和连接请求，并建立连接LNS和用户的PPP通道。

1.3 L2TP VPN工作原理

图1说明L2TP协议在TCP/IP层次结构中位置。以一个用户侧的IP报文的传递过程来描述VPN工作原理。

在LAC侧的链路层将用户数据报文加上PPP和封装，然后传递给L2TP协议，L2TP再封装成UDP报文，UDP再次封装成可以在Internet上传输的IP报文，此时的结果就是IP报文中又有IP报文，但2个IP地址不同，一般用户报文的IP地址

收稿日期：2009-07-30

作者简介：张 燕，工程师。

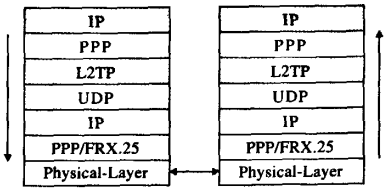

图1 L2TP协议在TCP/IP协议栈中的位置图

是私有地址，而LAC上的IP地址为公有地址，至此完成了VPN的私有数据的封装。

在LNS侧，收到L2TP/VPN的IP报文后将IP、UDP和L2TP报文头去掉后就恢复了用户的PPP报文，将PPP报文头去掉就可以得到IP报文，至此用户IP数据报文得到，从而实现用户IP数据的透明隧道传输，而且整个PPP报头/报文在传递的过程中也保持不变。

1.4 L2TP VPN协商交互过程

为了在VPN用户和服务器之间传递数据报文，必须在LAC和LNS之间建立传递数据报文的隧道和会话连接，隧道是保证具有相同会话连接特性的一组用户可以共享的连接属性所定义的通道，而会话是针对每个用户与企业VPN服务器建立连接的PPP数据通道，多个会话复用在一个隧道连接上，隧道和会话是动态建立与删除的。

会话的建立是由PPP模块触发，如果该会话在建立时没有可用的隧道结构，那么先建立隧道连接，会话建立完毕后开始进行数据传输。

2 MPLS VPN

2.1 MPLS简介

MPLS（Multiprotocol Label Switching，多协议标记交换）是由IETF（互联网工程任务组织）提出的新一代网络交换标准。它采用一种特殊的转发机制，为进入网络中的IP数据包分配标签（Label），并通过对标签的交换来实现IP数据包的转发。它将第3层路由与第2层交换合而为一，把第3层的智能、灵活性和可扩展性与第2层的交换机制有机结合起来。在帧模式链路上，Label位于2层头与IP报文之间，结构如图2。

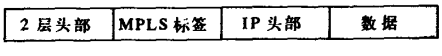

图2 MPLS Label结构示意图

一个MPLS标签是一个短的、长度固定的数值，由报文的头部携带，不含拓扑信息，只有局部意义。

MPLS包头的结构如图3。

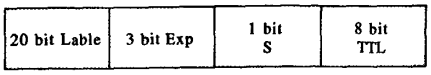

图3 MPLS Label包头结构示意图

通常，MPLS包头有32 bit，其中：20 bit用作标签（Label），0到15系统保留；3 bit EXP，协议中没有明确，通常用作COS；1 bit S，用于标识是否是栈底，表明MPLS的标签可以嵌套；8 bit TTL。

在网络内部，MPLS在数据包所经过的沿途通过交换标签而不是按IP包头来实现转发。当数据包要退出MPLS网络时，数据包被解开封装，继续按照IP包的路由方式到达目的地。

2.2 MPLS VPN的网络组成

图4是MPLS VPN的网络示意图。

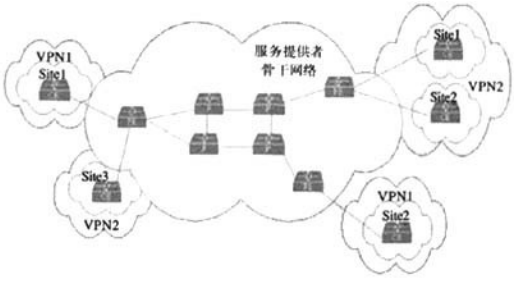

图4 MPLS VPN网络示意图

CE（Custom Edge）客户边缘路由器：为用户提供到PE路由器的连接。

PE（Provider Edge Router）：指骨干网上的边缘路由器，与CE相连，它根据存放的路由信息将来自CE路由器的VPN数据处理后转发，同时负责和其它PE路由器交换路由信息。

P（Provider Router）：指骨干网上的核心路由器，它根据分组的外层标签对VPN数据进行透明转发。

由于网络规模不同，网络中可能不存在P路由器。PE路由器也可能同时是P路由器。

2.3 MPLS几个关键名词

VRF：VPN Routing & Forwarding Instance，

VPN路由转发实例（又名VPN-Instance）；

PE上维护若干独立的路由转发表，包括一个公网路由转发表，以及一个或多个VRF；

VRF可看作一个独立的虚拟路由器—有独立的地址空间、有连接到该路由器的端口；

RD：Route Distinguisher 路由标识符用来标识VRF，与RF一一对应，64 bit，用来解决用户地址复用问题；

RT：Route Target 路由目标利用RT来判断VPNV4路由信息的取舍，注入到哪个VRF中。

3 南昌铁路局站段VPN网络的典型应用

南昌铁路局江西管内各站段，包括几条支线都已建成VPN办公系统，实现铁路局各站段（含班组）办公生产管理信息化功能，包含安全管理、班组管理、公文管理、材料管理、教学管理和邮件管理等功能模块，实现了从铁路局机关、站段到班组的三级管理。系统网络依托铁通的IP网络，用户层主要采用L2TP VPN技术，骨干层主要采用MPLS VPN技术。

图5是南昌铁路局站段VPN网络示意图。

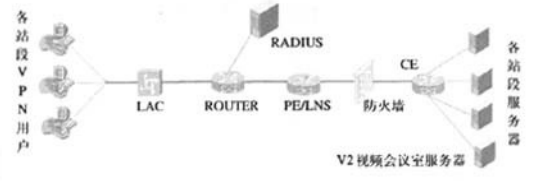

图5　南昌铁路局站段VPN网络示意图

3.1 用户层

站段VPN用户在LAC上按L2TP协议建立传递数据报文的隧道和会话，隧道对应各个站段VPN，会话对应各接入用户，不同的VPN建立不同的隧道，保证数据的安全隔离，隧道建立后，用户的身份验证信息通过隧道传送到LNS，由LNS向RADIUS发起身份验证请求，验证通过后，LNS将VPN地址分配给用户，并将建立的站段VPN隧道与骨干层MPLS VPN的VRF建立对应关系。

3.2 骨干层

各站段VPN服务器均放置在骨干网络层，VPN服务器的数据报文通过CE分配不同的VLAN标识，经防火墙设备，数据报文传送到PE设备，防火墙设备可控制进出网络的信息流向和信息包；防止网络上的DDOS攻击等各类攻击，隐藏内部IP地址及网络结构的细节，使得骨干层网络安全性得到进一步增强。

由PE设备根据VLAN标识分配MPLS标签，MPLS标签与VRF建立对应关系，同时还要设置RD、RT参数，RD用来识别不同的VPN用户，RT用来实现不同VPN的访问控制。MPLS标签转发后，由于用户层站段VPN隧道也已与VRF建立对应关系，通过VRF的对应关系，可以实现各站段VPN用户对VPN服务器的访问。

3.3 视频会议业务

南昌铁路局VPN办公系统还开展了视频会议业务，实现站段日常视频会议、网络远程教学、数据共享协作等功能，将视频会议系统从站段开到班组也成为铁路局VPN办公系统的一大特色，视频会议服务器也作为一台VPN服务器，而各站段VPN用户均可访问它，各站段VPN服务器又作为视频会议服务器的从服务器，其路由转发原理与各站段VPN服务器相似，更加灵活运用MPLS VPN的RT属性来实现视频会议服务器的路由选择功能，实现各站段到班组VPN用户的视频会议功能。

4 结束语

铁路局站段VPN办公系统根据站段分布特点，在用户层采用L2TP技术，具有用户接入方便、网络维护简单、节约投资成本以及安全保障有效等优点，而在骨干层采用MPLS VPN技术，满足用户对信息传输安全性、实时行和宽频带的要求，提高了运营和管理的灵活性。站段VPN办公网络的建设可以较好地实现将信息化建设推进到班组的要求，伴随铁路信息化程度的加深，必将更加灵活深入利用各类网络技术为铁路信息化建设服务，适应铁路发展新的需求和新的形势，为铁路发展做出贡献。

参考文献：

[1] 蒋朝辉. 下一代Internet技术[M]. 北京：国防工业出版社，2005，8.