文章编号：1005-8451(2007)09-0043-03

如何实现企业内部网络的远程互联

杨 艳
（太原铁路局 大同电务段，大同 037005）

摘 要：详细介绍网络远程互联技术，重点对VPN技术及其组网方式进行阐述，并根据企业的不同情况和需求提出组网建议。

关键词：网络技术；远程互联；通信协议；虚拟专用网
中图分类号：TP393 文献标识码：A

随着企业规模的不断扩大，企业信息化程度的加深，远程安全访问、协同工作需求的日益明显，企业对信息的获取方式也提出了更高的要求。大量的企业为了适应业务需要，成立了一系列的子公司或分支机构，迫切需要通过网络互联以实现信息共享。

1 企业网络远程互联的方式

实现企业的网络远程互联主要有两种方式：专线方式，虚拟专用网（VPN）方式。

1.1 专线方式

专线方式是指通过租用通信运营商的专线电路实现点到点之间的远程接入，主要的专线方式有：DDN专线，ISDN，2 M电路，PSTN电路，X.25，ATM，FR等，接入方式很多，实现的方式和使用技术均不相同，但共同的一点都是由通信运营商来提供电路实现连接，根据不同的方式，租用费用也不相同。典型网络如铁路和电力系统的各种管理信息系统，视频会议系统等，都是采用专线方式实现连接的。

1.2 虚拟专用网方式

虚拟专用网（VPN）是指在公众数据网络（通常为Internet）上建立属于自己的私有数据网络，以实现远程用户或分支机构对本企业内部网络的访问及资源共享。VPN具有两个方面的含义：（1）VPN是“虚拟”的，不再使用长途专线建立私有数据网络，而是将其建立在分布广泛的公用网络，尤其是Internet上；（2）VPN又是一个“专网”，每个VPN的用户都可以临时从公用网络中获得一部分资源供自己使用。VPN既可以让客户连接到公网所能够达到的任何地方，也可以容易地解决保密性、安全性和可管理性等问题，降低网络的使用成本。

VPN方式因为其投资少，效率高，组网灵活，管理方便，在企业网络的远程互联中得到了广泛的应用。

2 VPN的分类

2.1 PPTP协议和L2TP协议的VPN

PPTP协议是微软公司提出来的，PPTP已被嵌入到NT4操作系统中，并被用于Microsoft的路由和远程访问服务，它是数据链路层上的协议。

L2TP协议是由PPTP协议和Cisco公司的L2F协议组合而成，可用于基于Internet的远程拨号方式访问。它能为使用PPTP协议的客户端建立拨号方式的VPN连接。

PPTP/L2TP协议的VPN不能解决大的内部私网的建网问题，同时由于其用户数受限，不能满足企业发展的需要，其数据安全性也不能得到充分保障。

2.2 IPSec协议的VPN

IPSec协议的VPN是采用IPSec网络层（IP层）隧道协议加密技术，通过在两站点间创建安全隧道提供直接（非代理方式）接入，实现客户与企业内部网络的互连，达到对整个网络的透明访问；一旦隧道创建，用户终端就如同物理地处于企业内部局域网中。

2.3 SSL协议的VPN

SSL（安全套接层）协议的VPN是采用SSL应用层安全协议实现基于Web应用的VPN，它指定了在应用程序协议（如HTTP，Telnet和FTP等）和TCP/IP协议之间进行数据交换的安全机制，为TCP/IP连接提供数据加密、服务器认证以及可选的客户机认证。

SSL协议只对通信双方所进行的应用通道进行加密，而不是对从1个主机到另1个主机的整个通

收稿日期：2007-01-11
作者简介：杨 艳，助理工程师。

道进行加密。

2.4 MPLS协议的VPN

MPLS（多协议标签交换）是由IETF提出的新一代IP骨干网络交换标准，是一种集成式的IP Over ATM技术。它融合了IP路由技术灵活性和ATM交换技术简洁性的优点，在面向无连接的IP网络中引入了MPLS面向连接的属性，提供了类似于虚拟电路的标签交换业务，标签交换技术为介于2层和3层业务之间的传输方式，提高了网络传输速度。

MPLS VPN的组网需要运营商网络的支持，业务的开通也需要运营商制作数据，但从组网方式来说它更类似于专线方式中的ATM。只不过企业对MPLS VPN的可管理性更强一些。

3 组网方式

3.1 IPSec协议的VPN组网方式

IPSec协议的VPN可以采用两种方式进行组网，企业可根据自身情况进行选择。组网方式1：不需要通信运营商过多参与，企业在公司总部部署VPN网关设备，申请一个固定的公网IP地址，在企业的各个VPN业务点上部署一台VPN接入路由器。公司总部及分公司、移动用户连入公共互联网即可。业务点上的VPN接入路由器与公司总部VPN网关通过互联网建立隧道实现互联，组网方式1见图1。组网方式2：运营商给企业提供VPN服务，运营商在局端部署VPN网关设备，在企业的各个VPN业务点上部署一台VPN接入路由器。业务点上的VPN接入路由器，将隧道建到运营商的中心VPN网关上面，由中心VPN网关设备转发IPSec报文，实现VPN隧道的互联互通，组网方式2见图2。

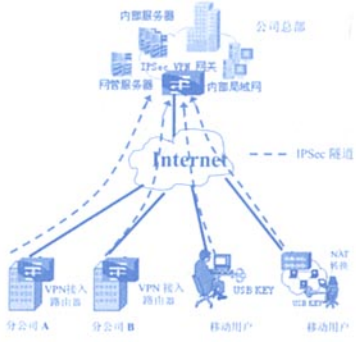

图1 IPSecVPN组网方式1

图2 IPSecVPN组网方式2

3.2 SSL协议的VPN组网方式

SSL协议的VPN组网方式如图3所示。

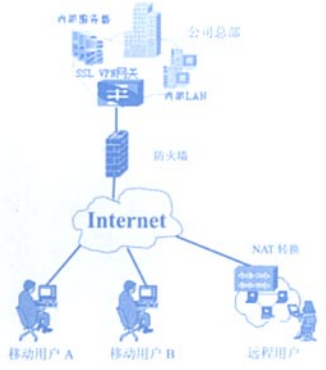

图3 SSL协议的VPN组网方式

4 各种连接方式的特点

（1）通过专线建立独立的专用网络无疑是安全性高，服务质量有保障的连接方式，但它的租用价格和维护成本也非常昂贵。

（2）PPTP/L2TP协议的VPN用于Microsoft的路由和远程访问服务以及基于Internet的远程拨号访问，但它并不能解决形成大的内部私网的问题，同时由于其用户数受限，也不能适应企业发展。

（3）IPSec协议的VPN采用隧道和加密机制以及严格的验证方式。能够真正解决局域网之间的互联，形成一个真正的私有网络，但IPSec协议的VPN网络部署相对复杂，投资较大。

（4）SSL协议的VPN网络部署相对简单，企业用户可以通过标准的Web浏览器就可以访问重要的企业应用。但SSL协议的VPN身份认证是基于证书的，认证方式比较单一，用户对于非Web页面的

文章编号：1005-8451(2007)09-0045-04

分散自律调度集中系统中车次追踪算法的研究

王建英，刘 隽，张一军
（铁道科学研究院 通信信号研究所，北京 100081）

摘 要：车次追踪主要包括原始车次号的获取、逻辑追踪和定点校核3个方面。对于客车的原始车次号采用列车运行调整计划的车次顺序进行匹配；对于货车的原始车次号，通过始发车站货票管理系统获得。逻辑追踪的基本原理是同一时刻同一地点有且只有一列列车在运行或者停车，其关键技术就是依据列车运行的情况、当前时刻、当前地点来自动推算当前运行或者停车的列车的车次号。定点校核则是采用其他第3方系统获得的车次号有选择地对追踪结果进行校核。当原始车次号、逻辑追踪车次号和校核车次号三者一致时，任取其一作为正确的车次号；否则报警，由人工介入干预，得到正确的车次号。

关键词：车次追踪；分散自律；调度集中；算法
中图分类号：U284.5：TP39 **文献标识码：**A

Study on train number logical tracing algorithm in Decentralized Self-regulated CTC System

WANG Jian-ying, LIU Jun, ZHANG Yi-jun
(Signaling & Communications Research Institute, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: Train number logical tracing algorithm was included acquiring to original train number, logically tracing and regularly checking. Facing with passenger trains, the matching of original numbers and the trains were relied on the trains operation rescheduling sequence. Facing with freight trains, the matching was relied on the data from freight invoice system of start station. The principal of logical tracing was at a certain time, there was no more than one train which was passing by or halting at certain position on the line. The key technique was to automatically calculate the train's number according to its operation status, its position and the time. Regularly checking was to check the tracing results with the train numbers provided by other systems. When the original train number, the logical tracing train number and the checking train number were identical, any of them could be used as the true train number; otherwise, the System was alarmed, and manual operation was involved to provide the true train number.

Key words: train number logical tracing; decentralized self-regulated; CTC; algorithm

车次号是列车进路自动控制的基础，是调车作业自律交互控制的基础，是列车运行计划自动调整和实际运行图自动生成的保障，是实现调度命令和行车凭证不停车交付和接车进路信息自动预告的前

收稿日期：2006-06-18
作者简介：王建英，副研究员；刘 隽，助理研究员。

文件访问，往往要借助于应用转换。

（5）MPLS协议的VPN通过运营商来完成企业各个分公司的互联，其标签交换技术提高了网络传输速度，同时双重封装提高了网络的安全性。

5 结束语

根据接入技术的特点，企业可以根据自身情况和业务需求选择不同的互联接入方式，如果是大型企业，又有雄厚的资金，或者企业对安全和服务的要求特别高，可以选择专线接入方式或MPLS协议的VPN方式；如果是大中型企业，对安全和服务有较高的要求，接入方式可采用IPSec协议的VPN技术组网，具体组网方式可采用如图1所示的企业自建方式，如果企业维护力量不足，也可以采用如图2所示的与运营商共同建设的方式；若企业为小型企业，用户多是以远程访问方式连接企业网络，查看内部网页信息（HTTP应用），下载和上传有关文件，则企业可以考虑采用SSL协议的VPN技术组网或IPSec协议的VPN和SSL协议的VPN混合组网。