VPN 技术应用研究

杨永斌
(重庆工商大学计算机科学与信息工程学院　重庆400067)

摘　要　随着网络经济、电子商务、电子政务、远程教育等的迅猛发展，各单位对外联系业务及合作范围越来越广，传统的联网方式已难以适应现代业务发展的需求。VPN 技术可以让各单位利用 Internet 来建立自己安全的内部网，将其分散在各地的网络通讯通过现有的公网安全地连接起来。本文介绍了 VPN 的概念、技术、优势，并探讨了 VPN 在券商广域网备份系统中的应用。

关键词　虚拟专用网，隧道技术，身份验证，加密，广域网，备份

The Research of VPN Technique Application

YANG Yong-Bin
(College of Computer Science and Information engineer, Chongqing Technology and Business University, Chongqing 400067)

Abstract　With the rapid development of network economy, E-Business, E-Government, distance education, etc., and with the ever-enlarging scope of business and cooperation, it is difficult for the tradition way of linking network to adapt to the requirements of the developing modern business. VPN technique enables network users to establish their secure Intranets based on the Internet, linking securely together notwork in different places. This paper focuses on the VPN concept, technique and its advantages, and discusses about its application in backup system of WAN of security companies.

Keywords　Virtual Private Network (VPN), Tunnel technique, Identity validate, Encrypt, WAN, Backup

1　引言

随着网络经济、电子商务、电子政务、远程教育等的迅猛发展，各单位对外联系业务及合作范围越来越广。面对业务数据流量的不断增长，单位对网络的灵活性、安全性、经济性和可扩展性等方面提出了更高的要求，使得传统的基于固定地点的专线(DDN、ATM/帧中继)联网方式已难以适应现代业务发展的需求，尤其对于一些特殊应用更加力不从心，如：野外作业和远程作业的人员向办公室传输数据等情况。VPN 技术价格低廉、灵活、安全的联接方式，非常适合中小规模单位低成本扩展自身业务。

根据预测，国内分支机构间使用 VPN 将为用户节省的20%～80%的通讯费用，跨国公司使用 VPN 节省的国际通信费用比例则更高。随着 VPN 技术的不断发展和完善，用户中许多业务完全可以承载于 VPN 中，这都为 VPN 的广泛应用奠定了坚实的基础。

2　VPN 概述

虚拟专用网技术(Virtual Private Network，VPN)是利用开放性网络作为信息传输的媒体，通过加密、认证、封装以及

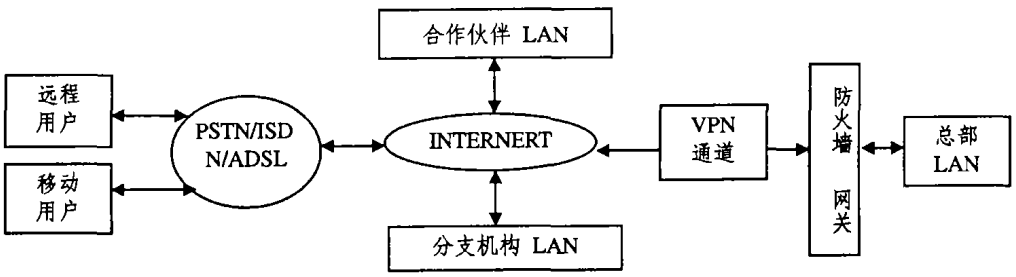

图1　典型的 VPN 系统组成

杨永斌　讲师，主要研究方向：计算机算法、计算机网络、数据库技术、网络教育。

参考文献

1　Ballew S M 著，夏昊，洪峰译. CISCO 路由管理[M]. 北京：中国电力出版社，2000
2　Helo G L, Hundley K 著，前导工作室译. CISCO 访问表配置指南[M]. 北京：机械工业出版社，2000
3　CISCO SYSTEMS 公司著，希望图书创作室译. 网络核心技术内幕—CISCO 网络安全解决方案(上、下)[M]. 北京：北京希望电子出版社，2000
4　CISCO SYSTEMS 公司著，希望图书创作室译. 网络核心技术内幕—网络协议解决方案(上、下)[M]. 北京：北京希望电子出版社，2000
5　张琳，李璇华著. 网络组建、原理与安全[M]. 北京：人民邮电出版社，2000
6　Mcqueny A 著，谈利群，胡爱民译. 组网用网：CISCO 网络设备互联解决方案[M]. 北京：电子工业出版社，2001

密钥交换技术在公网上开辟一条隧道，使得合法的用户可以安全地访问单位的私有数据。它可以替代专线，把单位的移动员工、远程分支机构、供应商和合作伙伴连接到单位的内部网，从而为单位和个人节省了昂贵的长途通信费用。典型的VPN系统组成如图1所示。要实现VPN连接，单位内部网络中必须配置一台基于Windows NT或Windows 2000 Server的VPN服务器。VPN服务器一方面连接单位内部专用网络，另一方面要连接到Internet，也就是说，VPN服务器必须拥有一个公用的IP地址。当客户机通过VPN连接与专用网络中的计算机进行通信时，先由ISP(Internet服务提供商)将所有的数据传送到VPN服务器，然后再由VPN服务器负责将所有的数据传送到目标计算机。

3 VPN使用技术

VPN使用隧道协议、身份验证和数据加密等三个方面的技术保证了通信的安全性。客户机向VPN服务器发出请求，VPN服务器响应响应请求并向客户机进行身份质询；客户机将加密的响应信息发送到VPN服务器，VPN服务器根据用户数据库检查该响应。如果帐户有效，VPN服务器将检查该用户是否具有远程访问权限，如果该用户拥有远程访问权限，VPN服务器接受此连接。在身份验证过程中产生的客户机和服务器公有密钥将用来对数据进行加密。

1. 隧道技术

隧道技术的基本过程是在源LAN与公网的接口处将数据作为负载封装在一种可以在公网上传输的数据格式中，在目的LAN与公网的接口处将数据解封装，取出数据。被封装的数据包在公网上传递时所经过的逻辑路径称为“隧道”。要使数据顺利地被封装、传递及解封装，通信协议是保证的核心。VPN隧道协议有4种：点到点隧道协议PPTP、第二层隧道协议L2TP、网络层隧道协议Ipsec以及SOCK v5。各协议工作在OSI七层模型的不同层次，不同的网络环境适合不同的协议。

一种趋势是将L2TP和IPSec结合使用，用L2TP作隧道协议，用IPSec保护数据。目前多采用此方式。

2. VPN的身份验证方法

(1)CHAP。是通过使用MD5(一种工业标准的散列方案)来协商一种加密身份验证的安全形式，CHAP在响应时使用质询-响应机制和单向MD5散列。用这种方法，可以向服务器证明客户机知道密码，但不必实际地将密码发送到网络上。

(2)MS-CHAP。同CHAP相似，微软开发MS-CHAP是为了对远程Windows工作站进行身份验证，它在响应时使用质询-响应机制和单向加密。而且MS-CHAP不要求使用原文或可逆加密密码。

(3)MS-CHAP V2。这是微软开发的第二版的质询握手身份验证协议，它提供了相互身份验证和更强大的初始数据密钥，而且发送和接收分别使用不同的密钥。如果将VPN连接配置为用MS-CHAP V2作为唯一的身份验证方法，那么客户端和服务器端都要证明其身份的验证，以确定连接是否被断开。

(4)EAP。其开发是为了适应使用其它安全设备的远程访问用户进行身份验证的需求。通过使用EAP，可以增加对许多身份验证方案的支持，其中包括令牌卡、一次性密码、使用智能卡的公钥身份验证、证书及其它身份验证。对于VPN来说，使用EAP可以防止暴力或词典攻击及密码猜测，提供比其它身份验证方法(例如CHAP)更高的安全性。

3. VPN的加密技术

(1)对于PPTP服务器，将采用MPPE加密技术。MPPE可以支持40位密钥的标准加密方案。只有在MS-CHAP、MS-CHAP V2或EAP/TLS身份验证被协商之后，数据才由MPPE进行加密，MPPE需要这些类型的身份验证生成的公用客户和服务器密钥。

(2)对于L2TP服务器，将使用IPSec机制对数据进行加密。IPSec是基于密码学的保护服务和安全协议的套件。IPSec对使用L2TP协议的VPN连接提供机器级身份验证和数据加密。在保护密码和数据的L2TP连接建立之前，IPSec在计算机及其远程VPN服务器之间进行协商。IPSec可用加密标准DES和56位密钥的三倍DES(3DES)。

4 VPN的优势

VPN除了能有效地降低网络通讯费外，还具有以下优势：

(1)*安全保障* 通过提供身份认证、访问控制、数据加密及数据完整来保障其安全可靠性。

(2)*服务质量保证(QoS)* QoS指包在一个或多个网络的传输过程中所表现的各种性能的具体描述，如丢包率、延迟等。VPN网应根据用户需求为用户提供不同等级的服务质量保证，为重要数据提供可靠的带宽。VPN与一些网络技术(如IPSec、MPLS)的结合能够为需要服务质量保证的用户提供不同程度的QoS保证。

(3)*可扩充性和灵活性* VPN必须能够支持通过Intranet和Extranet的任何类型数据流，方便增加新的结点，支持多种类型的传输媒介，可满足同时传输语音、图像和数据等新应用对高质量传输及带宽增加的需求。

(4)*可管理性* 在VPN管理方面，VPN要求用户将管理功能从LAN无缝地延伸到公网，甚至是客户和合作伙伴。虽然可将一些次要的网络管理任务交给服务供应商完成，用户任需完成许多网络管理任务。VPN网管理的目标是：减小网络风险、具有高扩展性、经济性、高可靠性等优点。事实上，VPN的管理主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS管理等。

5 VPN应用实例

广域网对于券商来说已经是至关重要，一旦A/B股交易、网上交易、开放式基金、自营等基本业务都在广域网上运行，广域网自然就成为券商的生命线，不得有任何闪失。目前的广域网主要面临两个问题：线路带宽以及设备和线路的备份。

带宽问题比较容易解决。以目前的网络流量来及其增长趋势，只要将带宽升级到2Mbps，并合理地实施QoS技术，2Mbps完全能胜任语音、视频和其它业务数据的传输。

设备和线路备份的目的是消除广域网上的单点故障，简言之就是要实现“双路由器+双线路”。双路由器就是使用两台路由器互为备份。线路备份才是真正困扰券商的关键问题。目前选择的线路常有“专线”和“ISDN”。备份线路采用专线(DDN/SDH)应当是最理想的方式，带宽及稳定性都很好，但费用太贵，这会给整个公司的运营成本造成负担。而采用ISDN作为备份线路(目前在券商广域网中非常普遍的方式)，但是带宽低，因为它只有128kbps，所以在做备份时难以承载

所有业务流量，必须将一些非紧要的流量过滤掉；更严重的是ISDN线路不稳定，经常处于一种非激活状态，这就导致主线路中断时，ISDN由于没有被激活而无法拨号。那么有没有一种线路能够满足券商的需求：既要带宽高，又要稳定性好，而且还要便宜。回答是肯定的，这就是宽带VPN解决方案。

国内宽带业务发展迅猛，其增长态势已超过了ISDN。宽带是Internet带宽接入的简称，主流的技术包括ADSL、以太网、有线的Cable Modem等，在线路带宽、线路质量和运维服务方面都已达到了比较好的水平，而且费用相当低廉，512kbps的ADSL每月只需200至300元。对券商而言，现在就将广域网构建在Internet(VPN)上还为时过早，与专线相比，VPN在两个方面还存在问题。首先，Internet上的带宽没有保证，无法实施End-to-End的QoS；第二，Internet宽带接入的稳定性还无法与专线相比。所以，VPN目前还不适合作为主线路，但是与ISDN和专线相比，VPN却更适合作为备份线路。表1是三种备份方式的比较。

表1 三种备份方式的比较

比较	专线(DDN/SDH)	VPN	ISDN
带宽	64k～2M	512k～2M	128k
延时	小于10ms	小于20ms	大于30ms
稳定性	非常稳定	比较稳定	较稳定
备份方式	保持常在线，依靠动态路由协议触发	保持常在线，依靠动态路由协议触发	平时不在线，主线路中断时拨号
故障切换速度	快	快	较慢
负载均衡	支持	支持	不支持
技术复杂性	低	较高	低
维护管理	简单	简单	需时常注意线路状态
运行成本	高	低	低

通过比较可以看出，VPN在一些关键的特性上与专线很接近，而且费用方面又非常低廉。与专线相比，VPN能够更好地平衡线路备份的需要和公司运营成本之间的矛盾。典型的广域网VPN备份方案的网络拓扑结构如图2所示。

首先，总部和营业部都要增加网络设备。总部需要新增一台中高端的防火墙如PIX 515E/525和一台专门用于VPN路由的路由器如Cisco 2651XM；每个营业部需要新增一台低端防火墙如PIX 506E和一台备份路由器如Cisco 2611XM。

总部以专线方式接入Internet，而且必须具有静态的公网IP，带宽应大于2Mbps。营业部以ADSL方式接入Internet，带宽有512kbps就足够。PIX 506E防火墙具有PPPoE拨号功能，只要将从ADSL Modem出来的RJ-45网线直接连接到PIX 506E的outside端口即可。

ADSL上网获得的是动态IP地址，所以在构建VPN时是采用Cisco EzVPN技术，由营业部端的防火墙向总部防火墙发起连接请求，以建立IPSec VPN，这种方式称为动态VPN。所谓动态是指每次ADSL重新拨号后，IPSec VPN也要重新建立。

要在VPN上传输数据，仅仅有防火墙是不够的，还必须通过复杂的路由配置，保证当专线中断时，业务流量能够被快速地重新定向到VPN线路上。使用OSPF(或EIGRP)动态路由协议，并且通过GRE技术，将动态路由协议OSPF扩展到VPN上。

考虑到网络系统的安全性，建议保留原有的ISDN线路，以便有多种备份手段，只是新的备份策略与以前不同：专线中断后，所有的流量会切换到VPN上，如果这时VPN线路也意外中断，备份路由器会马上启动ISDN线路，保证在专线和VPN都中断时，业务依然能够传输。所以，ISDN将成为第三备份手段。

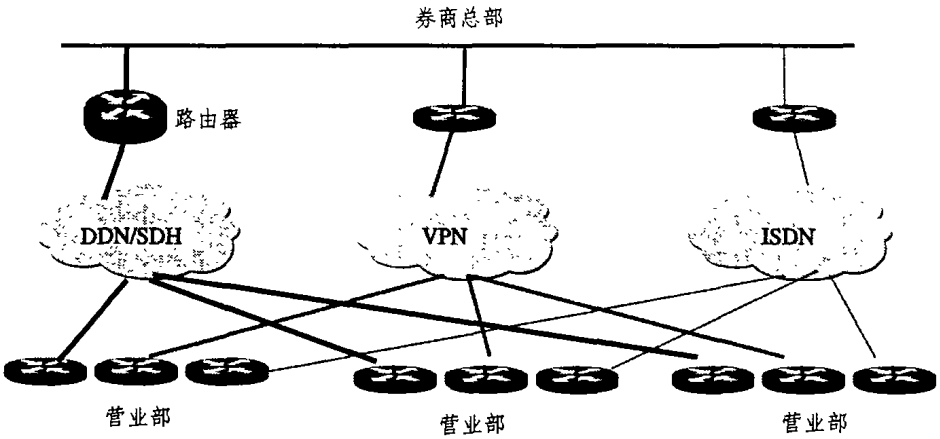

图2 典型的证券公司广域VPN备份方案

VPN备份方案能够实现以下的备份功能：营业部到总部的专线出现故障时，流量能够在2秒内切换到VPN线路上；营业部的主路由器发生故障时，备份路由器能够自动在20秒内恢复广域网连接；总部主路由器发生故障时，所有业务在2秒内切换到VPN线路上，实现针对整个广域网的备份。

结束语 现在，利用公网来构造企事业单位的虚拟专用网络的技术很热门。VPN技术的应用将极大降低网络系统的运营成本，提高资源的利用效率，具有明显的应用价值。随着国民经济信息化进程的加快，特别是政府上网、电子商务以及网络教育等应用的推动，VPN技术将会有更大的用武之地，使之发挥最大的优势，但还有待研究VPN技术与其它网络技术的结合，进一步实现网络安全，提高传输性能等功能。

参考文献

1 [美] SaadatMalik等，著. 王宝生，等译. 网络安全原理与实践[M]. 北京：人民邮电出版社，2003

2 [美] Sam Brown等，著. 王军，等译. Cisco IOS的IPv6配置[M]. 北京：电子工业出版社，2003

3 石淑华. 用Windows 2000实现企业VPN的分析与研究[J]. 微机发展，2002(5)：69～71

4 肖玲. VPN在远程教育中的应用[J]. 计算技术与自动化，2003(3)：61～64