

在公共网络上构建专用网的 VPN 技术研究

崔洪刚¹, 谢国波¹, 许 英²

(1. 广东工业大学 计算机学院, 广东 广州 510090;

2. 江苏省武进职业高级中学, 江苏 常州 213021)

摘要: 虚拟专用网(VPN) 是利用公众网资源为客户构成专用网的一种业务. 校园网是一个宽带、具有交互功能和专业性很强的局域网络. 本文以广东工业大学校园网为例, 说明如何采用 VPN 技术实现在多个物理空间上互相分离的校区之间建设一个廉价安全的专用网络.

关键词: 虚拟专用网; 隧道; 加密技术; 授权

中图分类号: TP 393. 18

文献标识码: A

文章编号: 1007-7162(2004) 04-0031-06

广东工业大学是由原广东工学院、广东机械学院、华南建设学院(东院)合并组建的一所以工为主、工理经管文结合的多科性协调发展的省属重点大学, 分为五个校区: 东风东路校区、五山校区、沙河校区、番禺校区、龙洞校区. 校本部设在广州市东风东路 729 号. 学校实行统一领导、统一管理, 按统一的教学大纲和要求组织教学. 从 1995 年到 2000 年, 学校投入校园网建设经费 1 000 多万元, 已在东风路校区、五山校区和龙洞校区建设了校园网, 另外两个校区的校园网也在筹建当中, 并且这两个校区的有关部门的管理系统也已经实现了与校本部的连接. 为了实现各个园区网之间信息安全可靠地进行互换, 需要在各个园区网之间采用相应的连接技术, 构造符合信息安全级别的专用网络. 目前构造专用网的技术主要有两种: 租用专线和虚拟专用网技术. 学校目前采用的是专线方式, 这种方式能够保证专用网络的高度可靠性, 但无论在运营阶段或者扩容阶段, 都需要昂贵的花费和专人的管理, 并且很多时候都不能充分利用网络资源. 虚拟专用网(VPN) 技术利用公众网的资源构成专用网, 它有两层含义: 1) 它是虚拟的网, 即没有固定的物理连接, 网路只有用户需要时才建立; 2) 它是利用公众网设施构成的专用网^[1]. VPN 兼备了公众网和专用网的许多特点, 将公众网可靠的性能、丰富的功能与专用网的灵活、高效结合在一起, 是介于公众网与专用网之间的一种网. VPN 能够充分利用现有网路资源, 提供经济、灵活的连网方式, 为客户节省设备、人员和管理所需的投资, 降低用户的电信费用, 在近几年得到了迅速的应用. 本文将首先简单介绍 VPN 的关键技术, 然后在对学校现有网络结构进行分析的基础上, 给出一个采用 VPN 技术构造的专用网络方案.

1 VPN 技术简介

VPN 通过公众 IP 网络建立了私有数据传输通道, 将远程的分支办公室、商业伙伴、移动办公人员等连接起来. 减轻了企业的远程访问费用负担, 节省电话费用开支, 并且提供了安全的端

收稿日期: 2003-05-28

基金项目: 广东工业大学青年基金资助项目(022037)

作者简介: 崔洪刚(1976-), 男, 助教, 主要研究方向为计算机网络及分布式系统.

到端的数据通讯. 无论是应用在企业内部网还是外部网, VPN 都可以通过采用一个单独连接和对应于每个场所一个设备来代替多重连接和传统设备的办法来节省大量的费用.

在结构不同的公众网络上构造一个统一的 VPN 网络, 一个最关键的技术叫做隧道技术^[2]. 隧道是指采用路由信息对整个传输的数据包进行加密和封装, 使得信息能安全地到达正确的目的地. 隧道协议可分为第二层隧道协议 PPTP、L2F、L2TP 和第三层隧道协议 GRE、IPsec.

L2TP^[3] 主要由 LAC(L2TP Access Concentrator) 和 LNS(L2TP Network Server) 构成, LAC 支持客户端的 L2TP, 它用于发起呼叫、接收呼叫和建立隧道; LNS 是所有隧道的终点.

L2TP 的建立过程如图 1 所示.

1) 用户拨号至本地的接入服务器 LAC; LAC 接收呼叫并进行基本的辨别.

2) 当用户被确认, 建立一个通向 LNS 的拨号 VPN 隧道.

3) 企业内部的安全服务器鉴定拨号用户.

4) LNS 与远程用户交换 PPP 信息, 分配 IP 地址.

5) 端到端的数据从拨号用户传到 LNS.

IPSec 协议^[4] 把多种安全技术集合到一起, 可以建立一个安全、可靠的隧道. 提供了在公共网络上安全传输数据所需要的封装技术、鉴别技术和访问控制技术.

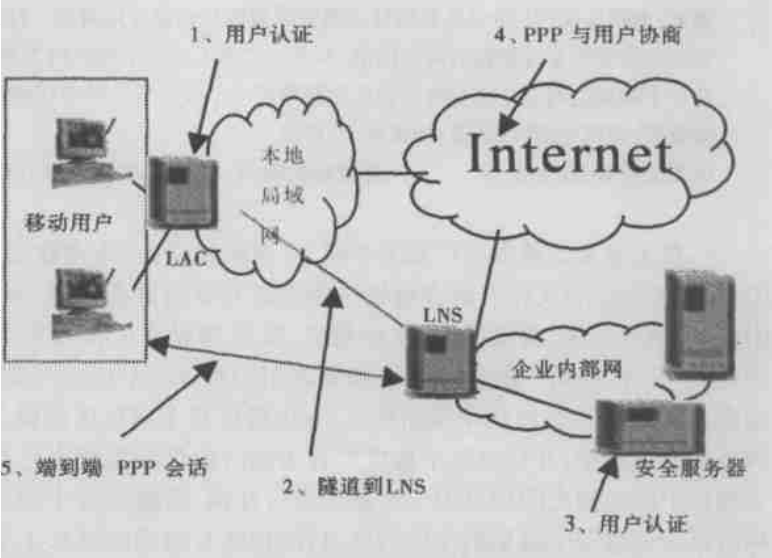


图 1 通过 L2TP 构造 VPN 的连接过程

2 广东工业大学原有校园网概况

广东工业大学是由原广东工学院、广东机械学院、华南建设学院(东院)于 1995 年 6 月合并组建的省属重点工科大学, 分为五个校区: 东风东路校区、五山校区、沙河校区、番禺校区、龙洞校区. 是广东省首批接入国际互联网的高校之一, 早在 1995 年 8 月就成立了网络信息中心, 并于同年 10 月接入中国教育和科研计算机网. 网络信息中心除了负责广东工业大学的校园网络与综合信息管理系统的建设, 还负责为广州市龙洞地区大中专院校和中小学提供校园网接入和网络服务, 并且承担了广东省教育科研计算机网龙洞地区汇接点的工作. 从 1995 年到 2000 年, 学校投入校园网建设经费 1000 多万元, 已在东风路校区、五山校区和龙洞校区建设了校园网, 下面以东风路校区为例, 讨论学校已有的网络结构.

东风路校区包括教学区和生活区二部分, 生活区目前尚未联网, 教学区是由 6 个楼房组成的建筑群: 2 号教学楼、4 号教学楼、5 号教学楼、7 号教学楼、图书馆和行政楼. 中心交换机放置在 7 号教学楼的网络中心, 各个楼房里面都放置有二级交换机, 并通过光纤与中心交换机相连. 二级交换机再通过 100 Mb/s 双绞线连接到桌面交换机或者集线器. 整个校园网拓扑结构如图 2 所示.

东风路校区作为广东工业大学的校本部, 需要和其它校区有网络线路连接, 构造安全可靠的学校内部专用网络. 目前采用的是专线方式, 在电信局租用专用的微波线路, 每个校区都安装有相应的微波发送和接收设备, 从而把几个校区的局域网连接成一个大的园区网, 并在其上实现了信息的安全交流和共享.

3 利用 VPN 技术构造新的校园网

随着各个校区内部网络的完善, 以及在相互间进行流动的信息量的迅速增大, 微波通信的固有弊端^[5]就逐渐暴露出来了. 主要有以下一些问题:

- 1) 微波经过的路线中出现新的建筑群, 会严重影响通信质量, 甚至出现通信中断情况;
- 2) 网络的运营和升级都需要专门投资和专人管理. 不能分享公众网的先进技术和业务;
- 3) 网络资源在业务量不饱和时得不到充分利用, 而在业务高峰时间可能又不够用;
- 4) 接入单个用户不经济.

学校对网络的需求也在变化, 主要表现在下面一些方面:

- 1) 各校区校园网的建设和完善, 必然对各校园网之间的连接提出新的要求;
- 2) 学生宿舍上网工程的展开, 引起学校网络访问的流量迅速增大;
- 3) 随着教师公寓的建成, 将会出现教师希望在家办公的需求.

而 VPN 技术在解决这些问题的时候具有得天独厚的优势:

- 1) VPN 是构造在公众网上面的, 能快捷廉价的应用到最新的网络技术;
- 2) 构造 VPN 只需增加有限的一些设备, 不需要对原有网络结构进行改动;
- 3) 不需要专门的经营费用和专门的网络管理员, 节省大量的费用;
- 4) 远程用户可以随时通过拨号 VPN 接入到校园网来, 实现在家办公.

下面采用 VPN 技术对东风路校区校园网进行改造, 改造后的网络拓扑结构如图 3 所示.

跟原来的网络结构相比, 需要改动的只有外联网子网和网络中心子网.

在网络中心子网中增加了一个 Raduis 服务器和一个拨号接入服务器. 其中 Raduis 服务器作为用户数据库, 普通用户和 VPN 拨号用户的资料都存放在 Raduis 服务器上, 远程用户通过 PSTN 连接到拨号接入服务器时, 接入服务器从 Raduis 服务器中取出用户资料, 并分配相应 IP 给远程用户, 建立 PPP 连接.

外联网子网中增加了一台 VPN 服务器. VPN 服务器一般由专用的防火墙服务器担任. 这次学校网络升级采用的是广东天海威数码技术有限公司开发的蓝盾防火墙. 用户建立 PPP 连接之后, 中心交换机根据 IP 地址将用户分类, 普通用户通过路由器连上公众信息网, 虚拟拨号网络用户则连接到 VPN 服务器上, 通过各个校区的 VPN 服务器之间建立的 IPSEC 安全通道访问整

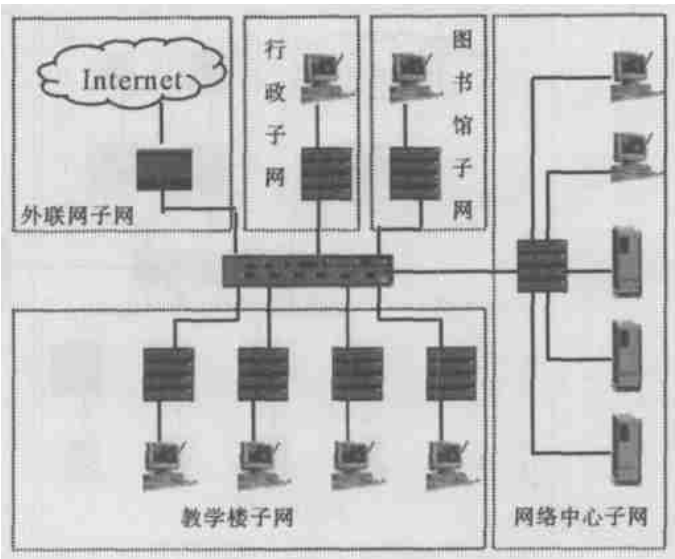


图2 东风路校区网络拓扑结构

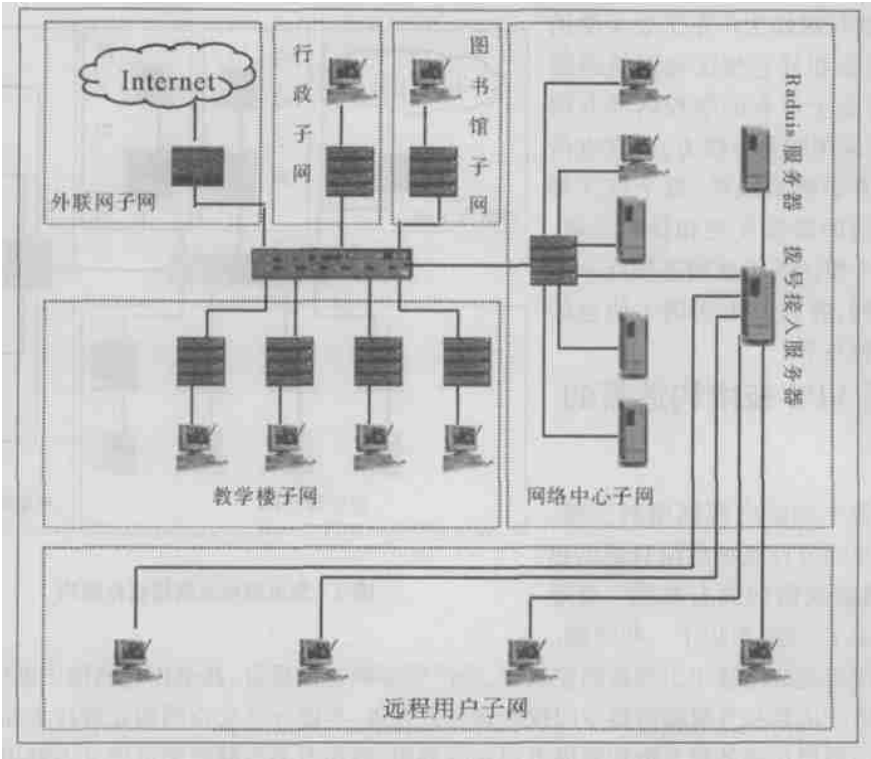


图 3 改造后的东风路校区网络拓扑结构

个校园网的资源。
各校区之间的互连如图 4 所示。

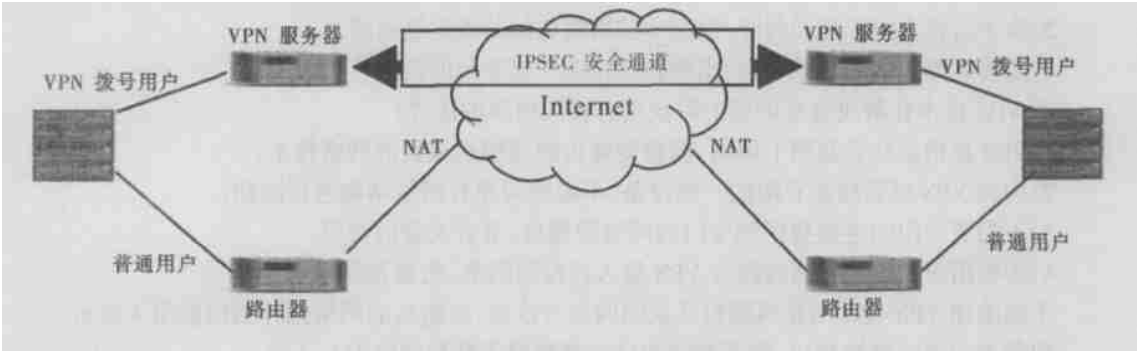


图 4 各校区之间的互连示意图

4 VPN 技术的安全隐患及对策

通过隧道技术和加密技术,已经能够建立起一个具有安全性、互操作性的 VPN. 但是该 VPN 性能上不稳定,管理上不能满足企业的要求,这就要加入 QoS 技术. 实行 QoS 应该在主机网络中,即 VPN 所建立的隧道这一段,这样才能建立一条性能符合用户要求的隧道.

网络资源是有限的,有时用户要求的网络资源得不到满足,需要通过 QoS 机制对用户的网络资源分配进行控制以满足应用的需求. QoS 机制具有通信处理机制以及供应(Provisioning)和

配置(Configuration)机制。

通信处理机制包括 802.1p、区分服务(differentiated service per-hop behaviors, DiffServ)、综合服务(integrated services, IntServ)等等。现在大多数局域网是基于 IEEE802 技术的,如以太网、令牌环、FDDI 等,802.1p 为这些局域网提供了一种支持 QoS 的机制。802.1p 对链路层的 802 报文定义了一个可表达 8 种优先级的字段。802.1p 优先级只在局域网中有效,一旦出了局域网,通过第 3 层设备时就被移走。DiffServ 则是第 3 层的 QoS 机制,它在 IP 报文中定义了一个字段称 DSCP (DiffServ codepoint)。DSCP 有 6 位,用作服务类型和优先级,路由器通过它对报文进行排队和调度。与 802.1p、DiffServ 不同的是,IntServ 是一种服务框架,目前有两种:保证服务和控制负载服务。保证服务许诺在保证的延时下传输一定的通信量;控制负载服务则同意在网络轻负载的情况下传输一定的通信量。典型地,IntServ 与资源预留协议(Resource reservation Protocol, RSVP)相关。IntServ 服务定义了允许进入的控制算法,决定多少通信量被允许进入网络中。

供应和配置机制包括 RSVP、子网带宽管理(subnet bandwidth manager, SBM)、政策机制和协议以及管理工具和协议。这里供应机制指的是比较静态的、比较长期的管理任务,如:网络设备的选择、网络设备的更新、接口添加删除、拓扑结构的改变等等。而配置机制指的是比较动态、比较短期的管理任务,如:流量处理的参数。

网络管理员基于一定的政策进行 QoS 机制配置。政策组成部分包括:政策数据,如用户名;有权使用的网络资源;政策决定点(policy decision point, PDP);政策加强点(policy enforcement point, PEP)以及它们之间的协议。传统的由上而下(TopDown)的政策协议包括简单网络管理协议(Simple Network Management Protocol, SNMP)、命令行接口(Command Line Interface, CLI)、命令开放协议服务(Command Open Protocol Services, COPS)等。这些 QoS 机制相互作用使网络资源得到最大化利用,同时又向用户提供了一个性能良好的网络服务。

5 总结

世界经济的全球化给网络界带来了新的机遇和挑战,企业管理的信息化成为提高企业管理水平、降低运作成本的必然选择。在国内,政府上网、电子商务将成为今后应用的热点。但是,昂贵的话费和网络维护费用将是 IT 决策者最为关注的焦点。在数据业务飞速增长的今天,他们会发现自己很难构造和维护一个能满足不断增长需求的企业广域网。这些客观原因将迫使企业主管选择基于电信服务商提供的广域网建立自己的 VPN(虚拟专用网)。

本文根据学校当前的需求和考虑到未来的发展,在充分保护现有的网络设施和提供良好的可扩展性两个前提下,通过增加有限的硬件设备,在 5 个校区两两之间建立了 IPSec 安全通道,实现了一个覆盖整个广东工业大学的虚拟专用网。而远程 VPN 用户也可以通过拨号登录网络,达到共享资源的目的。

参考文献:

- [1] W Townsley. Layer Two Tunneling Protocol (L2TP) [DB/OL]. <http://www.ietf-editor.org/rfc/rfc2661.txt>, 2003-04-10.
- [2] S Kent, R Atkinson. Security Architecture for the Internet Protocol [DB/OL]. <http://www.ietf-editor.org/rfc/rfc2401.txt>, 2003-04-10.
- [3] D Piper. The Internet IP Security Domain of Interpretation for ISAKMP [DB/OL]. <http://www.ietf-editor.org/rfc/rfc2407.txt>, 2003-04-10.

- [4] C Madson, R Glenn. The Use of HMAC-MD5-96 within ESP and AH [DB/OL]. <http://www.ietf-editor.org/rfc/rfc2403.txt>, 2003-04-10.
- [5] C Madson, R Glenn. The Use of HMAC-SHA-1-96 within ESP and AH [DB/OL]. <http://www.ietf-editor.org/rfc/rfc2404.txt>, 2003-04-10.

The VPN Technology of Building Private Network over the Public Network

CUI Hong-gang¹, XIE Guo-bo¹, XU Ying²

(1. Faculty of Computer, Guangdong University of Technology, Guangzhou 510090, China;

2. Wujing Senior High School, Changzhou 213021, China)

Abstract: Virtual Private Networks promise to help organize support sales over the Internet more economically and safely. It can almost provide the same security, reliability, priority level and manageability as the private network. It can be built over the IP network, frame relay network and ATM network. The approach to build a VPN over the IP network and correlation protocols are described. This paper gives an example of VPN of Guangdong University of Technology.

Key words: Virtual Private Networks; tunnel; encryption; authentication

(上接第 4 页)

参考文献:

- [1] 李优新. 一种可调磁永磁无刷直流电机的研制 [J]. 中小型电机, 2000, (2): 16-19.
- [2] 王鸿贵, 李优新, 何鸿肃, 等. 混合励磁无刷直流机的应用 [J]. 微电机, 2001, (3): 51-57.
- [3] 李钟明, 刘卫国, 刘景林, 等. 稀土永磁电机 [M]. 北京: 国防工业出版社, 1999.
- [4] 张琛. 直流无刷电动机原理及应用 [M]. 北京: 机械工业出版社, 1996.
- [5] Sun FengChun, Chen Yong, Zhang Chengning, et al. Study on performance of Electric Bus [A]. THE 18TH INTERNATIONAL ELECTRIC VEHICLE SYMPOSIUM (EVS-18) [C], Germany: Berlin, 2001 A2d: 028-033.

Application of a New Type of Brushless DC Motor With Adjustable-magnetic Field in Electric Vehicle

LIANG Xi+ling, LI You+xin, WANG Hong+gui, HE Hong+su, LIU Fang+ming, YAO Zhen

(Faculty of Information Engineering, Guangdong University of Technology, Guangzhou 510643, China)

Abstract: The article presents a new kind of EV drive technology-adjustable-magnetic field motor control technology. Such a home-made brushless DC motor is used as a sample to analyse its structure and theory. In the end, the experimental data of a prototype is given in the paper.

Key words: adjustable-magnetic field; brushless DC motor; electric vehicle; drive system