基于校园网络的 VPN 方案设计

摘要：

我校经过校区合并和扩建后，现有 5 个校区。现我校校园网网络出口有 2 条，一条为老校区到教育网的千兆出口，这条为校园网内访问外网的统一出口，另外一条为在**校区的千兆电信出口，这一条出口用作 VPN。我校因为有多校区，在双出口的网络构架中为了实现 VPN 与服务器的有效访问而使用了路由策略。本文针对当前**高校跨地域分布导致的校园网建设中所遇到的问题，分析了当前**高校在校区互联、移动办公、校际交流等需求，得出了 VPN 工程上马的必要性。文中结合 VPN 技术的特点，给出了本校网络建设中的一种基于 VPN 技术的高安全性网络解决方案，用于提供高效、安全、灵活和经济的网络数据传输，该技术的应用还可以提供可靠的校区互联、移动办公和校际交流三个方面的拓展功能。

正文：

我校为部属的 985 工程和 211 工程大学，2000 年合并了多个学校，现在拥有 5 个校区。2000 年因此启动了多校区互联工程将各分校区利用各种手段如直接敷设光纤，租用电信线路等方式连接在一起，2005 启动了多校互联工程，将**省**市的几所大型的高校连接在一起。2008 年开始，由于设备的老化又启动了新一轮的校园网建设的工程。该工程主要是增加新老校区校园网络覆盖率、启动**大学数字化校园建设工程，其中设计一个供学校老师访问的 VPN 系统是该工程的一部分。我为该学校信息部部长，负责该工程的设计和招标工作。

我校存在地理上跨地域分布，为了保证学校逻辑和管理上的统一性要求，导致了位于不同地域的校区间网络信息交换呈现出信息交流量大、交换频率高和信息涉密程度大等特点，这就要求校园网络体系必须满足分布性、高效性和安全性。网络既要保证高效运转，又要保证数据的绝对安全，此外，由于经费限制，还要保证建设和运行的低成本等，解决这些问题的关键在于如何实现不同校区间的子网互联。结合对于 VPN 主要技术及优点的分析，该技术恰好可以用来解决以上问题，应用于校园网络的构建，可以方便地提供校区互联、移动办公及校际交流等服务。

1. VPN 构建前需求分析

在方案构建前需要对 VPN 进行一定的需求分析，确定上马该项目的必要性，通过分析我校对 VPN 有以下几点需求：

（1）校区互联

在不同地域的分校区子网与主校区子网间或分校区与分校区间，利用相应的 VPN 设备，可以建立 VPN 网络。一方面，使得各分校区与主校区间方便、安全地共享资源和进行数据交流；另一方面，VPN 技术还提供了一种虚拟的专用网环境，使得原本在地域上相对分散校区的网络连成一体，在逻辑上保持了统一性。此外，还可以节省大量的建立专用网而必须支付的用于租用通信线路的费用。

（2）移动办公

对于出差在外或是在家的学校工作人员，利用相应的 VPN 客户端软件，采用拨号方式或本地 ISP，接入学校的 VPN 网络，可以实现传统物理专用网所不能实现的移动办公等功能，从而提高工作效率。

（3）校际交流

在**市不同的多所高校间，往往存在着一些资源共享和信息交流的需求，在这样的高校间，基于一所高校，完全可以建立起我校与多所高校间类似于企业扩展 VPN 的 VPN 网络，用于进行校际资源安全共享和信息的交流，而这一点如果使用专用网络实现，其投入和成本都是不可接受的。

2. VPN 建设方案

基于以上对校园网现状的分析，我们的实施采用了 Access VPN 和 Intranet VPN 两类方案。

（1）Access VPN 的应用

该方式下远端用户不再像传统的远程访问那样，要通过长途电话拨号到本地网络的远程访问端，而是拨号接入远端用户本地的 ISP，利用 VPN 系统在公用网络上建立一个从远程用户端到本地网关的安全传输通道，这样既经济又安全。

从校园网的安全策略来讲，有些校内网络资源是只允许校内网络用户访问的。由于在校外需要访问校园网内资源的远程用户的 IP 地址是不固定的，所以，为了使远程用户通过 VPN

接人校园网，我们采用的方法是，在用户端使用 VPN 功能的软件，配置为隧道开通器，通过 ISP 接人 Internet 并访问校园网内的 VPN 网关及服务器。即在校园网内建立 VPN 网关及服务器，远程用户使用软件进行 VPN 配置后访问校园网内的 VPN 网关及服务器。

由于目前校园网络用户使用的操作系统平台多为 Windows 系列，而 Windows 200X Server 中的 RRAS（路由和远程访问服务）可以被用来建立使用 PPTP 或 L2TP 的 VPN 连接，因此，可以选择在校园网内使用 Windows 200X建立 VPN服务器，而终端用户只要在 Windows 系列的平台上配置 VPN 客户端，便可通过远程的 VPN 服务器访问校园专用网。

（2）Intranet VPN 的应用

该方式可以在 Internet 上组建世界范围的虚拟 Intranet，利用 Internet 的公共线路保证网络的连通性，用 VPN 的隧道、加密特性，确保信息在 Intranet VPN 上的传输安全性。

在主校区和分校区之间建立 Intranet VPN，可以通过 Internet 这一公共网络将其相连，以便学校的资源共享、信息交流和数据传送。这样既可以克服使用开放路由器方法时对访问范围的限制，也可以对数据的传输起到保护作用，还不用租用专线而节省了开支。在两个校区之间建立 Intranet VPN，我们采用的方式是，使用带 VPN 功能的路由器来实现。通过对两地的路由器进行路由、账户、地址池及协议的适当配置，在主校区路由器和分校区路由器之间建立虚拟专用链路。

当分校区的用户访问主校区网络时，根据分校区 VPN 路由器上的静态路由，用户可以通过在两个校区之间建立的虚拟隧道，到达主校区的路由器，主校区的路由器分配给该用户一个主校区校园专用网的 IP 地址，并根据用户的账户名等信息检查自身的配置，然后根据检查结果赋予用户相应的访问权限。

分校区与其它高校利用 VPN 网关经由 Internet 与主校区的 VPN 网关完成校区与校间互联，可实现资源共享和信息交流，出差或在家的教职工使用笔记本电脑或 PC 机中内置的 VPN 软件通过本地 ISP 连人 Internet，再与主校区或相应校区的 VPN 设备相连来实现移动或家庭办公。另外，为了保证系统的安全性，在此方案中，各子网都装有防火墙，在主校区设置了置于主校区校园网 DMZ 区域中的认证服务和置于主校区校园网内部网中的 CA 中心，用于向网络中心合法用户授权和验证访问用户或设备的身份，加强了访问控制，最大程度加强了系统的安全性。

3. 结语

目前 VPN 建设极大的解决了师生远程访问的问题。但是现在由于没有和学校其他系统统一起来，需要新建用户和密码。由于没有做到用户名统一的问题，将在数字化校园项目的建设中解决。