文章编号：1006-4354 (2004) 02-0034-03

虚拟专用网络（VPN）在市县广域网中的应用

程 路

（南京气象学院，江苏南京 210044）

中图分类号：TP393.01 **文献标识码**：B

1 虚拟专用网络简介

虚拟专用网络（VPN）是通过公用网络（如Internet）连接专用网络（如市局局域网络）。VPN使用需身份验证的链路以确保只有授权用户可以连接到您的网络，且使用加密确保通过Internet传送的数据不被其他人侦听和利用。Windows使用点对点隧道协议（PPTP）或第二层隧道协议（L2TP）实现此安全性。

VPN技术使上级单位可以通过公用网络（如Internet）连接到下级单位，同时又可以维护通讯安全。通过Internet的VPN连接从逻辑上讲相当于专用的广域网（WAN）链路。

1.1 VPN的连接组件

VPN服务器：接受VPN客户VPN连接的计算机。

VPN客户：将VPN连接初始化为VPN服务器的计算机。VPN客户可能是一台单独的计算机，也可能是路由器。

隧道：连接中封装数据。

VPN连接：连接中加密数据的部分。对典型的安全VPN连接，数据沿连接的相同部分进行加密和压缩。

隧道协议：管理隧道及压缩专用数据的协议。要成为VPN连接，隧道传输的数据也必须加密。Windows 2000包括PPTP和L2TP信道协议。

隧道数据：数据经常在专用点对点的链接间发送。

传输互联网络：压缩数据所通过的、共享的或公共的网络。对Windows 2000，传输互联网络通常是IP网络。传输互联网络是Internet或基于IP的专用intranet。

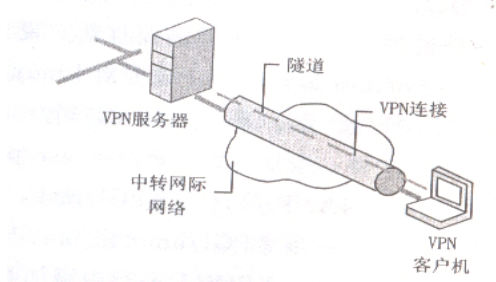

图1 虚拟专用网络的组成

1.2 VPN连接的属性

1.2.1 封装 通过VPN技术提供路由信息的

收稿日期：2003-10-24

作者简介：程路（1968-），男，陕西商南人，学士，工程师，在读硕士研究生，从事短期预报及网络工作。

5.4 Dell Precision450工作站对MM5V3的用户来说是一款非常不错的机器，与普通微机比较，同样的程序运算速度约快2倍以上。

参考文献：

[1] 施威铭研究室. Linux7.2实务应用[M]. 北京：清华大学出版社，2002

[2] Mesoscale and microscal Meteorology Division National Center for Atmospheric Research. PSU/NCAR Mexoxcale Modeling system Tutorial Class Notes and User's Guide: MM5 Modeling system Version 3 [EB/OL]. http://www.mmm.ucar.edu/mm5/mm5-home.html, 2003.

数据头加密数据，允许数据经过网际网络传输。

1.2.2　身份验证方式　①通过 PPP 身份验证的用户级别身份验证。要建立 VPN 连接，VPN 服务器将使用点对点协议（PPP）的用户级身份验证方法来验证试图使用该连接的 VPN 客户的身份，并验证该 VPN 客户是否有适当的访问权限。如果使用互相身份验证，VPN 客户也验证 VPN 服务器的身份，可防止伪装的 VPN 服务器。②使用 ISAKMP 进行的机器级身份验证。要建立 IPSec 安全关联，VPN 客户端和 VPN 服务器使用机器证书和 Internet 安全关联和密钥管理协议（ISAKMP）以及 Oakley 密钥生成协议。③数据验证和完整性。要验证 VPN 连接上发送的数据从连接的另一端开始并且在传送过程中没有更改，数据包含基于只有发件人和收件人才知道加密关键字的加密检验和。数据验证和完整性仅对 IPSec 连接上的 L2TP 启用。

1.2.3　数据加密　为确保数据在通过共享或公用传输网络时的保密性，数据应该由发送者加密而由接收者解密。加密和解密过程依赖于发送方和接收方均使用共同的加密密钥。

1.3　VPN 隧道协议

点对点隧道协议（PPTP）是“点对点协议（PPP）”的扩展，增强了 PPP 的身份验证、压缩和加密机制。PPTP 与路由和远程访问服务程序一起安装。PPTP 和 Microsoft“点对点加密（MPPE）”提供了对专用数据封装和加密的主要 VPN 服务。

基于 RFC 的隧道协议（L2TP）。L2TP 依赖于加密服务的网际协议安全（IPSec）。L2TP 和 IPSec 的组合称为基于 IPSec 的 L2TP。L2TP 与路由和远程访问服务程序一起安装。基于 IPSec 的 L2TP 提供专用数据的封装和加密的主要 VPN 服务。

1.4　VPN 的安全性

1.4.1　授权　只有得到授权的用户和路由器才能创建 VPN 连接。对于 Windows 2000，VPN 连接的授权由用户帐户的拨入属性及远端访问策略决定。

1.4.2　身份验证　机器级身份验证：如果将网际协议安全（IPSec）用于通过 IPSec VPN 连接的 L2TP，机器级别的身份验证将通过 IPSec 安全关联建立过程中的机器证书交换完成。

用户级别身份验证：在通过 PPTP 或 L2TP 隧道发送数据之前，必须对请求 VPN 连接的用户或请求拨号路由器进行身份验证。用户级别的身份验证是通过点对点协议（PPP）身份验证方式进行的。

1.4.3　数据加密　必须使用数据加密来保护在 VPN 客户和 VPN 服务器或者共享或公共网络之间发送的数据，因为这些网络通常有未授权拦截的危险。可以将 VPN 服务器配置为强制执行加密的通讯。连接到该服务器的用户必须对数据进行加密，否则不允许建立连接。对 VPN 连接，Windows 2000 使用有点到点隧道协议（PPTP）的 Microsoft 点到点加密（MPPE）及使用第二层隧道协议（L2TP）的网际协议安全（IPSec）加密。

1.4.4　数据包筛选　要保证 VPN 服务器在 Internet 接口上发送或接收除 VPN 通信之外任何通信的安全，需要在响应与 Internet 连接的接口上的 IPSec 输入和输出筛选器上配置 PPTP 或 L2TP。对于路由器到路由器 VPN 连接，还必须使用 IPSec 数据包筛选器上的 PPTP 或 L2TP 配置呼叫路由器（VPN 客户）。

2　组建基于 Internet 的地县虚拟专用网络连接

2.1　基于 Internet 的 VPN 连接

在地市气象局端，有安装 Windows 2000 Server 的计算机作为路由和远程访问服务器，和到 ISP 的专用链接，如光纤或 ADSL 专线；在县气象局端，有安装 Windows 98 以上操作系统的计算机作为 Internet 共享服务器，和到 ISP 的专用或拨号链接，如 163，169，ADSL 拨号。

2.2　地市端配置

2.2.1　配置到 Internet 的连接　从运行 Windows 2000 Server 的计算机连接到 Internet 是使用安装在计算机中 WAN 适配器的专用连接，如光纤接入或 ADSL 宽带接入。在 WAN 适配器上，需要配置以下 TCP/IP 设置：从 InterNIC 或 Internet 服务提供商（ISP）指派的 IP 地址和子

网掩码；ISP 路由器的默认网关；域名服务器地址。连接命名为“Internet”。

2.2.2 配置到 Intranet 的连接 从运行 Windows 2000 Server 的计算机连接到 Intranet 是安装在计算机上的 LAN 适配器。需要在 WAN 适配器上配置以下 TCP/IP 设置：从网络管理员指派的 IP 地址和子网掩码；Intranet 名称服务器的 DNS 和 WIN 名称服务器地址。连接命名为“本地连接”。

2.2.3 路由和远程访问服务器配置为有网络地址转换（NAT）路由协议的 Internet 连接路由器

在“路由和远程访问”控制台（MMC）中，把当前计算机添加为服务器，打开“路由和远程访问”安装向导页，在“公共设置”，选择“Internet 连接服务器”，在“Internet 连接服务器设置”，选择“设置有网络地址转换（NAT）路由协议的路由器”，在“Internet 连接”，将 Internet 连接设置为“Internet”。完成配置后，启用 Internet 连接服务器。

2.2.4 将路由和远程访问服务器配置为 VPN 远程访问服务器 在“路由和远程访问”控制台（MMC）中，打开服务器的属性，在“常规”选“远程访问服务器”，配置此服务器：在“安全”选“Windows 身份验证”，在“身份验证方法”中，选“Microsoft 质询握手身份验证协议版本 2（MS-CHAP v2）”，去掉其他选项。在“IP”中“IP 地址分配”项，选“静态地址池”，并添加 VPN 客户可用的 IP 地址；在 VPN 客户获取 DHCP，DNS 和 WINS 地址的“适配器”项上选“本地连接”。

设置完成后，路由和远程访问服务器将重新启动，重启动，继续配置：在“端口”属性中，将“WAN 微型端口（PPTP）”，设置成满足需要的值，如 20，将“WAN 微型端口（PPTP）”设为 0。在“远程访问策略”属性，授予 VPN 客户“远程访问权限”。VPN 远程访问服务器配置完毕并已启用。

2.2.5 建立 VPN 访问用户 新建 VPN 访问用户，将其权限设置成“Users”，“远程访问权限（拨入或 VPN）”设置为“通过远程访问策略控制访问”。

2.3 *县局端配置*

2.3.1 配置 Internet 共享连接服务器 在 Windows2000 系统，将连接到 Internet 的网络适配器设置为共享即可启用 Internet 共享连接服务。在 Win98 系统，添加“Internet 连接共享”组件，可建立 Internet 共享连接服务。

2.3.2 配置 VPN 客户端 对 Windows 2000 系统，在“网络和拨号连接”，新建连接，打开网络连接向导，选“通过 Internet 连接到专用网络”，输入远程访问服务器的 Internet IP 地址，可建立 VPN 连接。打开连接的“属性”项，打开“安全措施”项，在“安全措施选项”中，选择“高级”选项，在“设置”中，将数据加密选为“最强大的加密”，在“登录安全措施”中，选择“Microsoft CHAP 版本 2（MS-CHAP v2）”。打开连接，输入用户 ID 和密码，登录到地市局域网并可通过地局访问省局网络。

对 Win98 系统，需要增加“虚拟专用网络适配器”组件，新建基于适配器的拨号连接，亦可建立到地市局的 VPN 连接。

3 小结

商洛市气象局 VPN 网络 2002 年 10 月组建并投入使用，不仅满足业务需要，还将 Notes 等办公应用延伸到县局。使用表明，VPN 地县远程连接开通费用和维护费用低廉，联网稳定，安全性好，是 X.25，162 拨号等的很好替代方案，也将是陕西气象光纤网的廉价备份。