 随着互联网的广泛应用，企业分支机构的联网应用也越来越多。但是，租用专线的费用是很多中小企业无法承受的。通过使用本文中介绍 的VPN技术，可以轻易构建企业之间的联网应用。 VPN，全称“ 虚拟专用网 ”。这是相对于实际的专有网络而言的。实际的专有网络比如银行，政府机构，大型企业等等。通过租用专有的线路进行互联。而VPN是通过公共互联网传播私有数据的一种技术。这种技术通常使用在如下的网络： 下面首先简单介绍一下各种VPN技术和各自长短。 GRE：通用路由封装技术。这种技术是在IP数据包的外面再加上一个IP头。通俗的说，就是把私有数据进行一下伪装，加上一个“ 外套 ”，传送到其他地方。因为企业私有网络的IP地址通常是自己规划，无法和外部互联网进行正确的路由。而在企业网络的出口，通 常会有一个互联网唯一的IP地址。这个地址可以在互联网中唯一识别出来。GRE就是把目的IP地址和源地址为企业内部地址的数据 报文进行封装，加上一个目的地址为远端机构互联网出口的IP地址，源地址为本地互联网出口的IP地址的IP头，从而经过通过互联 网进行正确的传输。这种技术是最简单的VPN技术。 L2tp ：全称二层隧道传输协议。这是一种在特定链路层实现的VPN技术。具体是把二层协议PPP的报文封装在IP 报文中，进行传输。这种技术主要是提供了企业员工出差在外通过拨号网络直接访问企业内部网络的方式。在Windows2000中，也提供了这项功能。但是，用户要使用

这种技术，必需ISP提供支持。 IPsec ： 网络安全协议。这个协议提供了互联网的验证，加密等功能，实现了数据的安全传输。同时，可以使用这种协议构建VPN网络。原理也 是对IP包进行封装（可以提供多种方式），并且进行加密，然后在互联网中进行传输。与前面两种相比，这种技术提供了更好的安全性 。但是，协议的复杂性导致了处理Ipsec 的网络设备（如路由器）需要占用大量的资源，效率较低。如果使用专门的加密硬件，又会增加成本。 其他还有一些最新的技术，如MPLS VPN，但是都需要ISP提供相应的服务。 下面，以目前互联网现状最简单，成本最低，最有效的VPN技术GRE为例，说明如何实际的构造中小企业的VPN网络。 现在，许多中小企业都有一个互联网出口供上网，查找资料，处理邮件等。所使用的技术差不多都是NAT网络地址转换。虽然，这 种技术可以让内部网络访问互联网，却不能访问其他的内部网络。 公司的两个机构原来都使用NAT访问互联网。上网路由器可以通过ISDN，普通拨号电话线，卫星专项等上网。如果原来是 使用Linux或者Windows网关上网，要实现下面的功能，必须购买路由器（目前国产的地端路由器不过几千元）。 分支A和分支B都有一个上网使用的公共IP地址。分支A的内部网段为 172.17.1.0/24 ，分支B内部网段为 172.17.20/24。现在需要实现分支A的计算机能访问分支B的服务器Server B，分支B机能访问分支A的服务器Server A。为了实现这个目的，我们需要在Router A 和Router B上进行相应的配置，其他一切不变。 在Router A上 ： 1 配置一个虚接口（逻辑的接口，不是实际的物理接口），配置IP地址，本例中为172.17.10.1/24。 2 然后配置通道的目的地址193.64.2.1，配置

通道的源地址202.38.1.1。 3 配置路由：到网段172.17.2.0 255.255.255.0 的下一跳为172.17.10.2。 在Router B上： 1同样配置一个虚接口，配置IP地址172.17.10.2/24。 2然后配置通道的目的地址202.38.1.1，配置通道的源地址193.64.2.1。 3 配置路由：到网段172.17.1.0 255.255.255.0 的下一跳为172.17.10.1。 配置完成以后，从Router A如果可以ping 通 Router B 上的地址172.17.10.2，就大功告成了。分支A 和分支 B上就可以进行如专线一样的联网应用了。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com