 VPN(虚拟专用网络)技术对大型的跨地域企业内部同步使用ERP、MRP等信息化管理系统有着极大的帮助作用和可观的经济意义，不过受到流量问题的限制，VPN技术也面临一个网络带宽“ 供不应求 ”的难题，现在很多企业都是采用ADSL网络接入方式，而基于ADSL线路由于技术本身的限制，单条的上行速率只能达到几百K，如果是一些数据量较大的企业信息系统，要求信息流是双向的，上传和下传的速度都要快，那么单条ADSL就显得力不从心了。于是，一种既可以不改动原有ADSL线路，又可以有效提升VPN系统性能的技术呼之欲出采用多路捆绑，这种技术现在在国内也已经十分成熟。 好处 多线路捆绑技术不仅可以帮助用户大幅提升带宽和网速，还可以增强系统的稳定性，方便网络的运营维护。在目前大多数的VPN系统应用中，都是总部的一条线路，需要应对来自几个甚至几十个分支机构、移动用户的数据量。尤其在类似ADSL的非对称线路中，上行带宽本来就较窄，造成总部数据量不堪重负。为了解决带宽不平衡的问题，有些企业不得不在总部耗费巨资申请高速的专用线路，成本高昂。 VPN支持各种不同方式的线路绑定，用户可以申请多条动态IP的ADSL上网线路，也可以申请ADSL及其他宽带线路甚至无线连接等等。通过多线路防火墙/NAT模块，还可以实现多条线路共同访问Internet，成倍地提高了上网的速度。 多线路捆绑的另一个好处就是，如果是单条线路，一旦中断，整个系统就会陷入瘫痪，VPN

系统的稳定性非常依赖于线路本身的稳定性。通过多线路捆绑技术，尤其是对不同方式的线路捆绑，在任何一条线路出现故障时，数据可以无缝切换到其他正常线路，保证了整个系统的持续可靠运行。优秀的VPN路由还进一步实现了多条Internet线路的QOS管理，并能根据不同线路的带宽情况智能分配负载，最大限度地提高带宽利用率。 问题 从表面上看，多线路捆绑似乎是一种非常理想的技术，但真正实现起来，还存在不少困难。 数据要同时在多条线路上传输，如何能保证相同的业务数据分配到不同线路时，仍然不受影响呢？比如一串视频数据，发送时通过多条Internet线路，在接收端，传输的数据顺序必须准确有效，并能还原成发送前的状态。 线路的中断和恢复 也是一个必须解决的问题。一旦一条线路出现故障，所承载的数据要立刻无缝切换到其他线路，并保证业务不受影响。同样，线路恢复后，也要能够在新恢复的线路上建立VPN隧道，并能够重新调整负载均衡策略。 由于Internet连接方式也多种多样，用户为了进一步增强系统稳定性，往往倾向于从不同的运营商处申请线路，就会存在各种不同方式的Internet线路(如ADSL、宽带、DDN等等)需要能够实现带宽的捆绑和叠加。 组合 在一个路由器上做多条线路捆绑的方式有多种组合：多条ADSL线路捆绑，多条光纤线路捆绑，光纤和ADSL线路进行捆绑。这种捆绑是一种带宽相加式的捆绑，而不是线路互相备份。一些产品在参数上写着“……可以进行多路捆绑，还支持互相备份……”其实这句话是要分开来看的，因为2条ADSL线路使用多路捆绑模式的时候是不能实现互相备份的，就像两个硬盘使用RAID0加速的时候不能实现RAID1备份一样。 从实际应用的角度去分析，

两条线路进行捆绑后，上下行的流量是不可能达到1 1=2的效果的，2条以上的线路也是同样道理，原因大致如下： 当每一个数据包进行传输时，它必须先选择其中一条线路，这个选择的过程就是路由器进行调度分配的过程，路由器会按照预先设定的算法将每一个数据包根据一定的条件(这个条件通常不是固定的)分配到一条线路，这个过程会占用路由器的处理器资源，需要耗费一定的时间，当然耗时是非常短的，但是大量的数据包耗费的时间累加起来就比较可观了，加上现在中低端路由器的处理能力还比较有限，所以这种资源的消耗是不能忽略的。如果你捆绑两条2M的线路和一条4M的线路做对比，就会发现捆绑两条2M线路的速度不会快过那条4M的线路，其中一个重要因素就是路由器上对数据包进行调度而耽误了数据转发的时间。 RAID0阵列的容量是取决于容量小的那个硬盘，因为数据是同时在两个硬盘上进行读写的；而在VPN多路捆绑中也有类似情形如果两条线路的带宽不一样，也就是一条大些，一条小些，这时情况就比较复杂了。因为如果路由还是按照1：1的比例将数据包分别派发给两条线路的话，就会造成带宽大的那条线路发完时带宽小的那条还没发完，于是带宽大的线路得等待带宽小的线路，这样会造成效率的降低，因此很多支持不对称多路捆绑的路由器都允许设置路由器调度分配的比例，例如接入1条1M的ADSL和1条2M的ADSL时，就可以把这个比例设成1：2，这样两条线的带宽就可以充分利用起来；当然，由于数据分配的比例不会是完美的1：2，而两条线路的实际流量也不是准确的1：2，因此宽带资源还是没有被完全地利用起来，所以最终1M和2M两条ADSL线路捆绑之后的实际效果依旧小于3M

线路的实际效果。 如果两条线路进行捆绑，在下载时和上传时得到的带宽其实是不同的，因为在上传时你是两条线路同时传送数据，可以理解为1 1=2；但在下载时，对方并不知道你将线路进行了捆绑，他也无法控制数据包往哪条线路上传送，所以每次对方的数据包发送过来都是由其中一条线路承担接收任务，在这种情况下，两条1M的线路进行捆绑后其实效果大概也是1M，也就是1 1=1，因此，将多路捆绑简单地理解为带宽的叠加其实是不对的。 安全 多条线路同时连接时，局域网也同时面临着多条与Internet连接的通道。这就给各种网络攻击、病毒提供了更多的可乘之机，所以很多VPN路由都是直接结合了比较专业的防火墙功能，不但能够支持多条线路的捆绑上网，还能对带宽进行智能动态分配，防护来自多条线路的攻击。 由于很多VPN网络的结构非常庞大，内部成员的权限问题也就非常复杂，因此一些优秀的VPN产品可以对各成员接入后的可访问资源做严格而详细的限定来杜绝这些安全隐患。例如Sinfor的DLAN方案就可以针对每个用户设定不同的接入访问权限，如某些用户只能访问总部的库存系统，不能访问财务系统等，不同的VPN用户可以设定对不同资源的访问权限，避免因为VPN用户权限过大造成的安全隐患。 