解决VPN路由设置不能访问外网的问题思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_A7_A3_E5_86_B3VPN_E8_c101_644337.htm 在进行VPN路由设置的过程中，我们会遇到很多问题，不能访问外网是其中比较常见的一个，这里就给大家介绍一下解决方法。VPN虚拟专用网技术，对于实现远程访问公司的信息资源而言，相比拨号连接服务具有被广大用户认可的优势，目前在实际运用中正在逐渐取代拨号连接服务。 VPN能够提供高级别的远程访问服务，为用户和基础设施提供一个安全的通信机制。这篇文章我主要对在使用VPN路由设置过程中经常出现的一类问题进行详尽的分析。相信通过VPN路由设置?客户机远程访问公司内部网的网友都曾经碰到过这种问题，即当你的路由器设置连接成功后，虽然能访问总部公司的内部网这时却不能访问外网了，看了下面我的详细介绍之后，大家就可以了解到这是由于VPN路由设置引起的。 （一）VPN客户机不能访问外网的原因初探 我们知道，VPN客户机是通过Internet连接到VPN服务器的，就是说通过VPN对Internet的访问物理意义上说是可以实现的。那么为什么会出现VPN连接建立后就不能访问外网的现象呢？出现了这种问题，很多用户都知道是路由表发生了变化，因此大家都通过在VPN连接的“ 高级TCP/IP设置 ”中取消“ 在远程网络上使用默认网关 ”选项来达到访问外网的目的。这种方法虽然表面上看来可行，觉得解决了一个VPN路由设置问题，但有所不知可能会带来新的路由问题，甚至给公司内网带来严重的安全隐患。大家想一下，我们采用VPN的最初目标是为了保证安全，结果却可

能因为使用VPN而让整个公司网络面临外界攻击的境地，那么这样就背离了我们的初衷。 那么怎样才能更好并且安全的解决这个问题？以下我就先对VPN客户端的路由做一个初探，使大家对这一个知识点有一个较为全面地了解。我们已经通过分析认为是VPN路由设置问题，现在我们从VPN连接前后的路由表变化情况来找出问题的症结所在。大家可以边根据我的说明边进行实际操作，这样在需要使用VPN远程访问的时候会留下更深刻的印象。在VPN没有连接之前，输入route?print命令，出现当前的路由表项，然后连接上VPN，再次运行 route?print命令，比较前后两次命令的区别。可以看到，在命令行窗口中连接后多出了几条路由，比较重要的有两条路由在出现的结果 ActiveRoutes下的第三行和第十行分别有一条（我称为 route1
）0.0.0.0???0.0.0.0???150.0.1.226??150.0.1.226????1；另一条（我称为 route2
）218.70.201.62??255.255.255.255??150.0.1.43??150.0.1.41??20，注意，各位网友的路由中部分IP也可能会略有不同。 这里route1的150.0.1.226是VPN客户端从VPN服务器上获得的IP地址，而route2的150.0.1.41是客户机网卡的IP，218.70.201.62是VPN服务器的公网IP。你们还可以看出，最右侧一列原来的路由metric值已经增加了，而且高于新的路由route1的metric值，这样原来的路由就失效了，现在起作用的是route1，它的metric值更低。那么到目前为止到Internet的访问就已经使用了新的路由route1，这条路由把数据包交给VPN的计划程序端口，然后VPN 端口的数据再发送到远方的VPN服务器（route2），这个过程后会引起不能访问Internet上的站点，这就是前

面所说的VPN连接后不能访问外网的原因。（二）如何实现对VPN数据包的封装加密并安全传输的过程 现在我们来看一下VPN客户端的路由决策及数据包封装的过程。众所周知，VPN虚拟接口就是一个虚拟的点对点链路接口，当VPN虚拟接口收到数据包时，它把从网络层得到的数据包封装成PPP点对点数据帧并进行加密等操作，然后把它送到网关，这里的网关正是VPN客户端自己，所以这个被封装的 PPP点对点数据帧又被返回给本机再次处理，这次处理其实就是再次封装的过程。 那为什么要再次封装？由于第一次封装的帧只能通过虚拟的VPN接口，如果要把数据通过实际的接口进行传输，还必须在实际的链路层上进行再次封装才行。而在最终封装成链路层数据帧之前，需要对第一次封装成的PPP数据帧进行其他的多级封装。因为规范中是不能直接把PPP帧封装在另一个链路层帧中的，需要在它们之间添加一些报头，最简单的PPTP封装就是在PPP帧前添加了一个GRE头和IP头。 在封装到网络层比如IP报头的时候，这里需要进行一次路由决策，这是由于数据包要明确地发送到远方的VPN服务器，它将寻找一条到达远方VPN 服务器的路由。在VPN连接建立时就同时创建一条到达VPN服务器的路由（route2），再次封装成PPTP格式或L2TP格式的IP数据包交给这条路由指定的接口进行处理。如果是以太网接口，这个数据包就加上以太网报头；如果是点对点，就加上点对点链路报头，发送到物理网络上。在此处，route2指定的接口是150.0.1.41，即是网卡接口，所以它将加上以太网帧头，然后发送到物理网络上去。 (三)对于使用VPN不能访问外网的解决方案 上面的三段我只想说明一点：使用VPN连接，必须让通过VPN连接传输的数据

包先到达VPN虚拟接口进行处理，如果绕过了VPN虚拟接口不处理的话，由于这个VPN连接的数据包没有经过加密措施就直接发送到了Internet上，那么你的VPN安全就根本没有保证。 现在我们来看一下，在VPN连接后此时VPN客户端的路由表。默认路由没有变，添加了一条VPN端口IP对应的分类网络路由条目
：150.0.0.0????255.255.0.0???150.0.1.226???150.0.1.226????1。假设现在通过VPN 连接访问远程公司内网的192.168.0.0/24子网，根据上面的路由表，匹配的路由只有第一条默认路由。默认VPN路由设置是通过本地网卡到达网关后直接发送到192.168.0.0/24去的，因为Internet上的路由器不会转发到达私有网络的数据包，这样就可以达到外界不能访问公司内网、保证内网安全的目的。因此选中了“ 在远程网络上使用默认网关 ”选项，采用了默认路由，就不会出现前面所说的路由问题和安全问题。 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