

思科认证辅导:深度剖析VPN访问外网不畅Cisco认证考试 PDF
转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/584/2021_2022__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_584401.htm 2009年下半年全国

计算机等级考试你准备好了没?考计算机等级考试的朋友,2009年下半年全国计算机等级考试时间是2009年9月19日至23日。

更多优质资料尽在百考试题论坛 百考试题在线题库 在局域网

组网规模相对较大的单位，单位员工时常会选用VPN方式来访问内部网络。借助VPN网络连接，单位员工可以十分轻松地摆脱地理位置的限制，随心所欲地在Internet网络的任何位置都能访问到单位内部网络。相比普通拨号网络连接服务

，VPN网络连接服务具有被更多上网用户认可的优势，目前在使用过程中正在慢慢取代普通的拨号网络连接服务。不过在实际使用VPN网络的时候，当单位员工成功建立VPN连接后，尽管能够顺畅地访问单位的内部网络资源，不过此时员工的本地工作站却不能访问Internet网络了，这是什么原因呢?

现在，本文就对这种故障现象进行详细剖析，希望大家能从中获得收获! 初探VPN工作站访问外网不畅 众所周知，VPN

工作站是利用Internet网络连接单位内部网络VPN服务器的，那么为什么上网用户在成功创建了VPN网络连接后，反而不能顺畅访问Internet网络中的内容呢?发生了这种故障现象时，

很多熟悉网络知识的朋友都知道这种现象可能是由路由参数设置不当引起的，所以在解决这种故障现象时，许多人都会打开VPN网络连接的属性设置界面，进入其中的高级TCP/IP

设置页面，再将“在远程网络上使用默认网关”项目取消选中(如图1所示)，来实现访问Internet网络的目的。从表面上来

看这种解决故障的方法是切实可行的，上网用户会认为解决了一个路由故障，事实上简单地取消选中“在远程网络上使用默认网关”项目容易造成新的路由故障，甚至还可能威胁到单位内部网络的运行安全性。我们不妨扪心自想一下，当初使用VPN网络连接访问单位内部网络的目标是为了保障局域网网络的安全运行，结果却可能由于VPN网络连接影响了整个单位网络的运行安全性，那么这样就有点得不偿失了。如此说来难道我们就不能找出更好的办法，让VPN工作站既能正常访问单位内部网络，又能顺畅访问Internet网络了吗？在回答这个问题之前，我们认为有必要先来探究一下VPN工作站的路由寻径情况。既然VPN访问外网不畅的原因是由路由引起的，现在不妨仔细检查一下VPN网络连接成功前后，VPN工作站的本地路由表发生了什么变化，之后根据具体的变化情况来看寻找网络故障的原因所在。当VPN工作站没有建立VPN网络连接时，我们可以在本地系统依次单击“开始”/“运行”命令，在弹出的系统运行文本框中输入字符串命令“cmd”，单击回车键后，将系统状态切换到DOS命令行状态。在DOS命令行提示符下输入字符串命令“route print”，单击回车键后，我们将看到如图2所示的结果界面。接着，在VPN工作站中建立好VPN网络连接后，再次进入到DOS命令行状态，并在该状态下执行字符串命令“route print”，随后我们又将看到一个与图2界面不同的结果。仔细对比这两个结果画面，我们可以非常清楚地看到，在建立VPN网络连接后本地工作站的路由表内容发生了明显变化，变化较大的就是本地VPN工作站访问Internet网络的路径会优先选用VPN的计划程序端口，之后上网请求信息会通过VPN端口将数据信

息转发到远程VPN服务器中，这个寻找路径的过程自然不会成功访问到Internet网络中的内容，而只能访问到单位内部网络的内容，这也是前面所说的VPN工作站建立VPN网络连接后不能顺畅访问Internet网络的原因。揭密数据在VPN通道传输过程为了更好地解决VPN访问外网不畅的故障现象，我们还有必要来了解一下上网数据信息在VPN网络连接通道中的传输过程。我们知道，VPN网络连接接口其实就是一个点对点方式的虚拟链路接口，当VPN网络连接接口收到网络访问包时，该连接接口就会把从网络层获取得来的数据信息包封装成PPP点对点格式的数据帧，同时对该数据帧进行安全加密操作，之后再吧安全封装好的数据帧信息传输到指定的网关那里，这里所提到的网关其实就是VPN工作站自己，因此这个被安全封装的上网数据信息帧又被重新返回给本地工作站再次进行处理，这次处理操作实际上就是再次对上网数据信息帧进行封装的过程。那么VPN工作站为什么需要重复对上网数据信息帧进行封装呢?这是因为第一次进行安全封装的数据帧往往只能通过虚拟的VPN网络连接接口进行传输，要想将上网数据信息通过实际的网络连接接口进行传输，还需要在实际的网络链路层中重新进行一次安全封装操作才行。而在最终封装成符合网络链路层传输要求的数据帧之前，往往要对第一次封装过的上网数据信息帧进行其他的多级封装，这是由于按照规定是无法直接把PPP点对点格式的数据帧封装在另一个链路层数据帧中的，这需要在PPP点对点格式的数据帧之前添加一些报头，例如最简单的是添加一个GRE报头和IP报头。当上网数据信息帧被封装到符合网络层传输要求时，比方说在封装到IP报头的时候，还需要在这个过程中进

行一次路由指定，这是因为上网数据信息包必须要明确地发送到目标远程VPN服务器那里，上网数据信息包需要在这里寻找到一条能够到达目标远程VPN服务器的路由，之后上网数据信息就在目标路由的指定下将数据送到特定的网络接口进行处理。应对VPN访问外网不畅的方案 通过上面的分析，我们不难看出，使用VPN网络连接访问单位内部网络时，一定要让通过VPN网络连接传输的数据信息包先到达VPN网络虚拟连接接口进行处理，倘若没有经过虚拟VPN网络连接接口处理的话，那么通过VPN网络连接出去的数据信息包就没有经过安全加密环节，这些的数据信息在互联网通道中传输时，自然就会影响到单位内部网络的安全性。当我们在VPN网络连接属性设置界面中将“在远程网络上使用默认网关”项目取消选中时，尽管远程局域网网络能通过互联网通道到达目标网站内容，可是这个访问过程没有通过虚拟VPN网络连接端口进行传输，那样一来上网信息就没有经过安全加密处理，这样的话上网信息的安全性就无法得到保证，很显然这并不是VPN网络访问真正想要实现的目的，所以简单地将“在远程网络上使用默认网关”项目取消选中显然是不可取的。退一步来说，即使我们将远程局域网的内网IP地址分配给VPN工作站，一旦将“在远程网络上使用默认网关”项目的选中状态取消，同样也会出现路由寻径问题，因为此时所有发送到本地工作子网中的数据信息包都将被自动路由到远程局域网网络中。为了有效防止VPN工作站出现这种路由寻径错误，我们可以尝试为VPN工作站分配一个特殊的IP地址，确保该地址不能与VPN工作站所处的本地工作子网地址范围相同，不过要与远程局域网工作子网地址范围相同。但是

，如果将VPN网络连接属性设置界面中的“在远程网络上使用默认网关”选项保持选中，我们就不能实现同时访问远程局域网和Internet网络的目的，这显然是一个两难问题，针对这种问题我们目前还没有找到一个合适的设置方法，只能在不同的工作环境中使用不同的网络设置来解决网络连接问题。由于将VPN网络连接属性设置界面中的“在远程网络上使用默认网关”项目取消选中，一定会影响远程局域网的安全运行。为此，在远程局域网对安全要求较高的情况下，我们肯定要选中“在远程网络上使用默认网关”选项。对于那些既想访问Internet网络又想访问远程局域网的朋友来说，我们不妨尝试使用HTTP代理实现访问Internet网络的目的，该功能大部分代理服务器往往是支持的。例如，要是我们希望VPN工作站能够同时访问Internet网络和远程局域网时，可以考虑在VPN服务器中安装专业的代理服务器程序，例如可以安装专业的Wingate工具程序。之后从系统的“开始”菜单中启动运行Wingate程序，打开“Users”选项设置页面，再双击“Assumed users”选项，然后单击其后界面中的“By IP Address”选项卡，在对应的选项设置页面中单击“Add”按钮，如此一来我们就能看到Location设置对话框了，在这里输入需要访问代理服务器的VPN工作站IP地址，同时将对应界面中的“Guest”项目选中，最后单击“OK”按钮，那样一来指定的VPN工作站就能通过代理服务器来访问Internet网络中的内容了。在对代理服务器系统的相关参数进行合适设置后，我们还需要对VPN工作站的IE浏览器进行设置。在设置IE浏览器的代理参数时，我们可以先运行IE浏览器程序进入IE浏览器窗口，单击该窗口菜单栏中的“工具”选项，从

下拉菜单中点选“Internet选项”菜单命令，从其后的Internet属性界面中单击“连接”标签，打开如图3所示的标签设置页面。在该标签设置页面的“局域网设置”处单击“局域网设置”按钮，进入如图4所示的代理服务器参数设置界面，之后在该页面中正确输入代理服务器的IP地址以及代理服务端口号码，通常来说默认的代理服务端口号码为“80”，最后单击“确定”按钮结束代理服务器客户端参数设置操作，如此一来VPN工作站通过VPN网络连接与远程局域网中的VPN服务器建立连接后，再通过架设在VPN服务器中的代理服务器就能实现访问Internet网络的目的了。当然，需要提醒各位注意的是，要是VPN工作站只想访问远程局域网网络，而不访问本地工作子网时，可以直接将VPN工作站的IP地址设置成与VPN服务器的IP地址位于相同的逻辑子网，此时我们就能将“在远程网络上使用默认网关”项目取消选中了。小提示在普通工作站中创建VPN连接时，我们有时会看到网络连接创建向导窗口中“使用拨号或VPN连接”选项处于灰色不可选状态，那样的话我们就无法在普通工作站中成功创建VPN网络连接了，那为什么会出这种现象呢，我们又该如何解决这样的故障现象呢？其实，引起这种网络故障的因素有很多，我们必须对此进行依次排查。首先应该检查本地工作站的系统文件有没有受到受损，倘若与VPN网络连接有关的系统文件意外受到损坏时，那就很容易出现上面的故障现象。在判断本地工作站的系统文件有没有受到损坏时，我们不妨先依次单击本地系统桌面中的“开始”、“运行”命令，在其后弹出的系统运行框中输入字符串命令“sfc /scannow”，单击“确定”按钮后，Windows系统就会自动扫描本地工作站

系统文件，遇到有系统文件被破坏时屏幕就会自动弹出提示要求我们进行恢复。要是受损的系统文件被恢复正常后，我们再将本地工作站系统重新启动一下，之后重新创建网络连接，相信此时“使用拨号或VPN连接”选项就有可能处于可选状态了。如果通过上面的操作无法让“使用拨号或VPN连接”选项的显示状态恢复正常的话，那就说明这种故障现象与系统文件无关，此时我们就需要认真检查与VPN网络连接创建操作相关的系统服务是否运行正常了，例如一旦系统服务Remote Access Connection Manager工作状态不正常时，那就有可能出现“使用拨号或VPN连接”选项显示不正常的现象了。在检查Remote Access Connection Manager系统服务工作状态是否运行正常时，可以依次单击“开始”/“程序”/“管理工具”/“服务”命令，在弹出的系统服务列表界面中双击Remote Access Connection Manager服务选项，进入目标系统服务的属性设置界面，在该属性界面的常规标签页面中，我们就能非常直观地看到该服务的工作状态是否正常了。相信经过上面的设置，多半就能解决VPN网络连接无法创建的故障现象了。特别推荐：2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 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