网络中心动员大会

1. **招新内容:**

**招新时间和内容:**

根据对应的时间节点从3月18日开始

3月25日安排笔试工作；到时候安排勤助提前一天将要用到的试题打印出来，提前申请图书馆609课室，多打印三四份，然后在考试当天有二至四位勤助来负责分发试卷和收取试卷，考试前十五分钟提醒结束时间，每场建议时间两小时内，允许提前交卷。（注意时间安排：上午十点一批，下午两点有一批），预估六位勤助人员左右

3月26日-28日各位值班组长负责打分。

4月2日面试工作；提前将找出勤助人员来负责该事务，提前申请图书馆609作为面试场地，

每场会议至少一个提问人员与一个记录人员，可以三十到四十分钟一批同学（面试同学为4-5人），再询问完一批同学到下一批同学来前可以预留出10分钟间隔，将同学的回答记录到一个共享文档中（提前创建），不用特别着急；然后可以上午、下午各进行二到三批，会议数量到时根据面试人数进行商定。（若线下那么可以考虑将课室腾一下，放置两个面试场地，不用开启会议）

提问的问题提前告知各位负责面试提问的勤助同学，各位勤助需要注意时间，面试分为问答题，抢答题等类型问答题控制在20分钟，抢答题10分钟左右（待定）；预估十位勤助人员左右

4月3日-6日，确认进阶名单，各位参与笔试和面试的勤助同学相互交流，给出进阶名单；

4月7日-22日第一次阶段培训+考核，提前发送培训文档给各位进阶的同学；

4月23日考察机试内容，提前一天将机试试题打印，然后让同学们到达609进行机试考试，提前准备好插排和让同学携带充电器。24-25日进行机试成绩打分和筛选进入下一阶段培训+考核（可以考虑是否第一次考核加入制作水晶头，注：提前一天申请609课室和所需工具，要工具包提前收集。）

预估六位勤助人员左右

4月26日-5月13日，发送文档让同学们学习，提前一天申请609课室和所需工具，要工具包提前收集。5月14日第二次培训+考核水晶头必做（模块选择是否考核），以及故障检测。预估六位勤助人员左右

5月7-9日最终筛选入职人员，综合给出具体评价。

5月10日，招新总结，文件打包保存留给下一届参考。

5月10-19日，入职后第一次培训，每一次内容需考核大部分，考核模块制作（必做，水晶头如果不熟练可再次制作）对对应的文档内知识进行讲解。

5月19日-6月3日，入职后第二次培训，对对应的文档内知识进行讲解。（模块和水晶头如果不熟练可再次制作）

**在确定入职人员后可以考虑带他们做单，参观弱电井可以添加到机试后或第一次培训+考核时一同进行，可以选择到T1、T2、T3去查看。**

**二、培训内容:**

目前各位勤助的都较为不错，在平时处理事件的过程中都已经比较熟练了，都能够完美应对。

因此我们这次培训的话主要是偏向理论方面，主要是对一些我们日常可能会见到的理论进行一些讲解介绍。

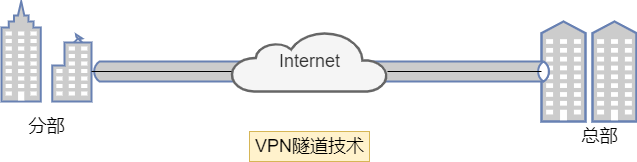
**培训案例:**

1. 在日常维修时，时常会遇到用户反映连接有线网络时锐捷客户端提示故障:“请不要开启远程vpn为别人提供代理”:

首先我们先来了解vpn的基础知识:

**VPN的概念:**

虚拟专用网（Virtual Private Network，VPN）是利用Internet等公共网络的基础设施，通过隧道技术，为用户提供的与专用网络具有相同通信功能的安全数据通道。其中，**“虚拟”**是指用户不需要建立各自专用的物理线路，而是利用Internet等公共网络资源和设备建立一条逻辑上的专用数据通道，并实现与专用数据通道相同的通信功能。**“专用网络”**是指虚拟出来的网络并非任何连接在公共网络上的用户都能使用，只有经过授权的用户才可以使用。该通道内传输的数据经过加密和认证，可保证传输内容的完整性和机密性。

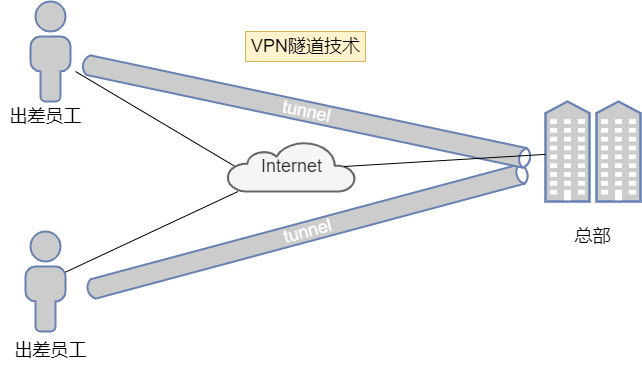


**根据组网方式进行划分:**

（1）远程访问VPN

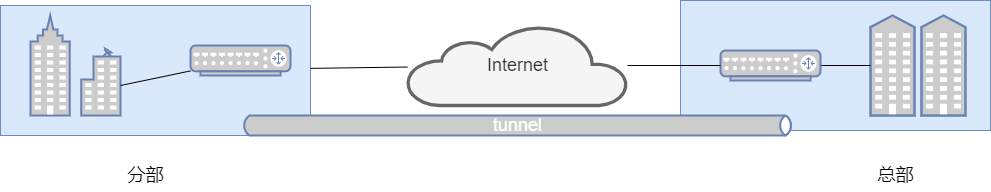
这种方式适用于出差员工拨号接入VPN的方式，员工可以在只要有Internet的地方都可以通过VPN接入访问内网资源。

最常见的就是SSL VPN、L2TP VPN。



（2）站点到站点的VPN

这种方式适用于企业两个局域网互通的情况。例如企业的分部访问总部。最常见的就是MPLS VPN、IPSEC VPN。



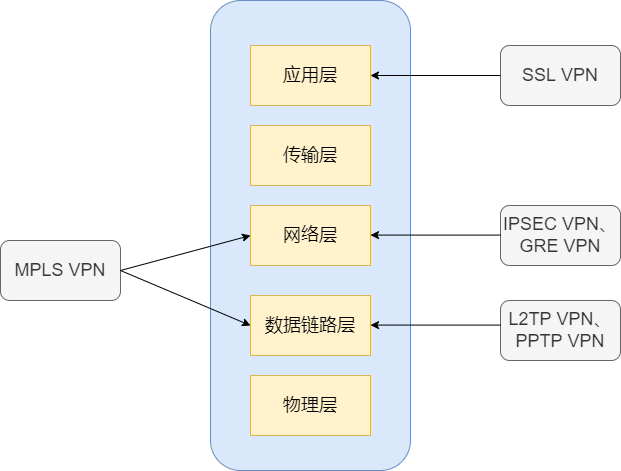
**根据工作网络层次进行划分:**

VPN可以按照工作层次进行划分：

（1）应用层：SSL VPN

（2）网络层：IPSEC VPN 、GRE VPN

（3）数据链路层：L2TP VPN、PPTP VPN

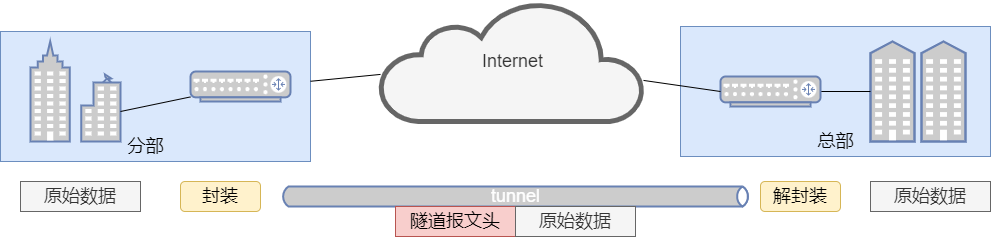


**VPN关键技术:**

1、**隧道技术**

VPN技术的基本原理其实就是用的隧道技术，就类似于火车的轨道、地铁的轨道一样，从A站点到B站点都是直通的，不会堵车。对于乘客而言，就是专车。

隧道技术其实就是对传输的报文进行封装，利用公网的建立专用的数据传输通道，从而完成数据的安全可靠性传输；



可以看到原始报文在隧道的一端进行封装，封装后的数据在公网上传输，在隧道另一端进行解封装，从而实现了数据的安全传输。

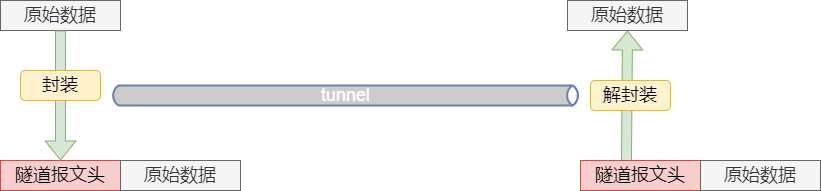
PPTP、L2TP、IPSec、GRE和GTP这些VPN技术被广泛应用。现有两种类型隧道协议：一种是二层隧道协议，用于传输二层网络协议，主要用于构建Access VPN和Extranet VPN，另一种是三层隧道协议，用于传输三层网络协议，主要应用于构建Intranet VPN和Extranet VPN；L2TP和IPSec配合使用是目前性能最好，应用最广泛的一种。

**Access VPN(远程接入VPN，Client-LAN类型)**：它提供了一种安全的远程访问手段，使用公网作为骨干网在设备之间传输VPN数据流量。例如，出差在外的员工，有远程办公需要的分支机构，都可以利用这种类型的VPN，实现对企业内部网络资源进行安全的远程访问。

**Intranet VPN(内联网VPN，LAN-LAN类型）：**为了在不同局域网之间建立安全的数据传输通道，例如在企业内部各分支机构之间或者企业与其合作者之间的网络进行互联，可以采用LAN-LAN类型的VPN。而采用LAN-LAN类型的VPN，可以利用基本的Internet和Intranet网络建立起全球范围内物理的连接，再利用VPN的隧道协议实现安全保密需要，就可以满足公司总部与分支机构以及合作企业间的安全网络连接。

**Extranet VPN(外联网VPN，ExtranetVPN类型)：**即与合作伙伴企业网构成Extranet，将一个公司与另一个公司的资源进行连接，这和第一种VPN类似。

隧道协议通过在隧道的一端给数据加上隧道协议头，即进行封装，使这些被封装的数据能都在某网络中传输，并且在隧道的另一端去掉该数据携带的隧道协议头，即进行解封装。

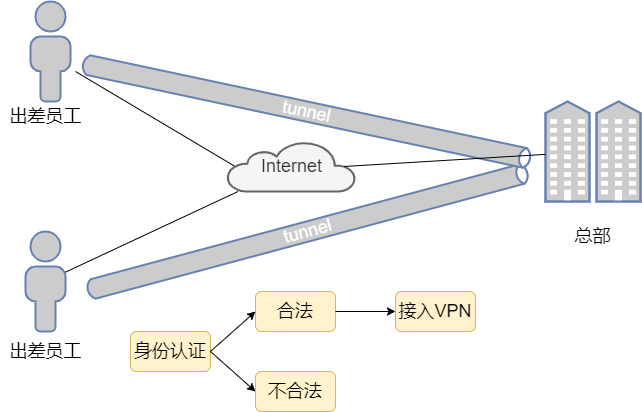


报文在隧道中传输前后都要通过封装和解封装两个过程。

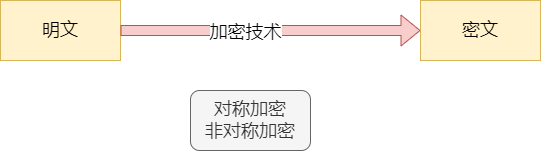
2、身份认证、数据加密、数据验证

身份认证、数据加密、数据验证可以有效保证VPN网络和数据的安全性。

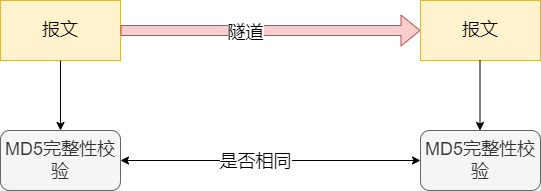
身份认证：VPN网关对接入VPN的用户进行身份认证，保证接入的用户都是合法用户。



数据加密：将明文通过加密技术成密文，哪怕信息被获取了，也无法识别。



数据验证：通过数据验证技术验证报文的完整性和真伪进行检查，防止数据被篡改。



**VPN与代理的区别:**

1.匿名性不同

代理和 VPN 的操作非常相似。它们都位于请求的中间，都隐藏了您的 IP 地址，并且都将信息转发给您。主要区别在于 VPN 需要隧道过程，该过程建立了到您和 VPN 服务器的直接且不可穿透的连接。代理只是一个开放的端口，你可以连接，没有隧道，也不是不能通过的。

其次，代理往往是任何人都可以连接到的单个 IP 地址。如果它是公共代理服务器，那么由于没有密码和身份验证，因此很多人都可以连接到它，并且通常可以在网络上使用它。一般来说，公共代理并不安全，因此不应使用。

2.加密不同

VPN 会加密我们的流量，而代理服务器不会。 VPN 服务可保护我们免受 ISP 跟踪，政府监视和黑客攻击。 代理不是，因此我们绝不应该使用它们来处理敏感信息。

3.安全性不同

VPN 比代理更安全，更私有。从技术角度来看，它们本质上是封闭的系统，您只能在获得许可的情况下访问它们。

4.运行级别不同

VPN 在操作系统级别运行，并重定向我们所有的流量，而代理在应用程序级别运行，并且仅重定向来自特定应用程序或浏览器的流量。

5.速度不同

VPN 可能比代理慢，因为它们必须加密我们的数据。 但是，有一些方法可以改善我们的连接和浏览速度。

6.成本不同

VPN 通常是付费服务，而许多代理服务器是免费的。 我们不能信任免费服务，因为它们有局限性并倾向于挖掘我们的数据。

7.连接不同

VPN 连接更可靠，因为代理服务器连接失败的可能性更高。

**出现该问题可能原因:**

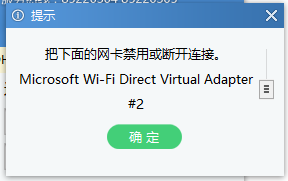
1、电脑带有[蓝牙功能](http://wenwen.soso.com/z/Search.e?sp=S%E8%93%9D%E7%89%99%E5%8A%9F%E8%83%BD&ch=w.search.yjjlink&cid=w.search.yjjlink" \t "http://www.360doc.com/content/14/0330/17/_blank)或红外功能，附近如果有蓝牙设备或[红外设备](http://wenwen.soso.com/z/Search.e?sp=S%E7%BA%A2%E5%A4%96%E8%AE%BE%E5%A4%87&ch=w.search.yjjlink&cid=w.search.yjjlink)时，就可能出现这种“传入的连接”，比如手机跟电脑连接时，可能出现这种连接。

2、有些[笔记本电脑](http://wenwen.soso.com/z/Search.e?sp=S%E7%AC%94%E8%AE%B0%E6%9C%AC%E7%94%B5%E8%84%91&ch=w.search.yjjlink&cid=w.search.yjjlink" \t "http://www.360doc.com/content/14/0330/17/_blank)的[无线网卡](http://wenwen.soso.com/z/Search.e?sp=S%E6%97%A0%E7%BA%BF%E7%BD%91%E5%8D%A1&ch=w.search.yjjlink&cid=w.search.yjjlink)可以工作在“AP模式”，这时，附近的带有无线网卡的电脑，也可能自动出现“传入的连接”。

3.主要原因可能是电脑热点共享，被锐捷客户端检测到后进行警告。

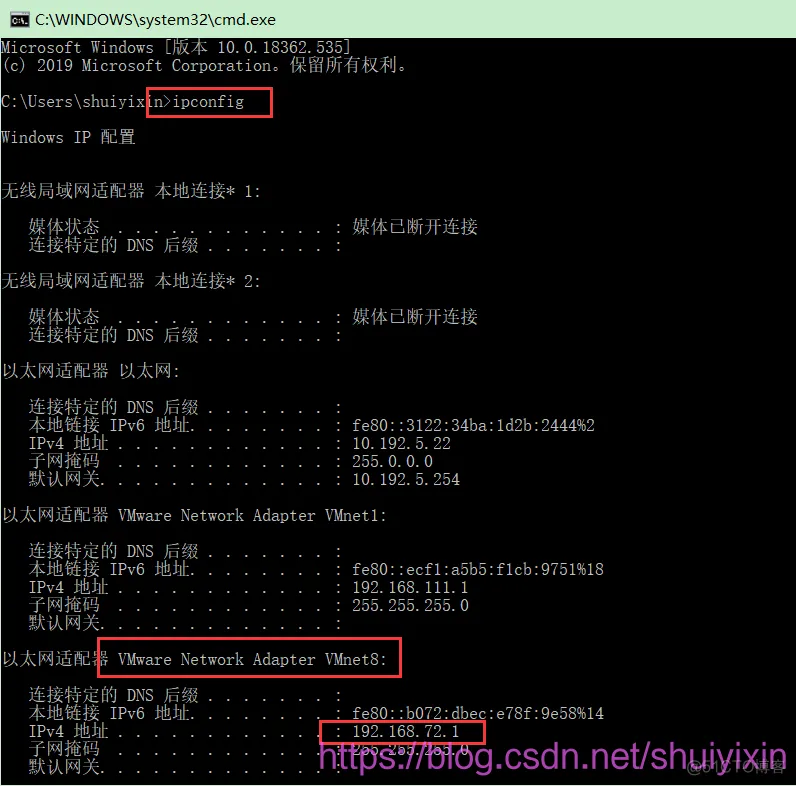
**解决方案:**

1. 删除”传入的连接”即可恢复连接，
2. 可能是其他vpn工具和WIFI共享工具，进行卸载删除后重新尝试。

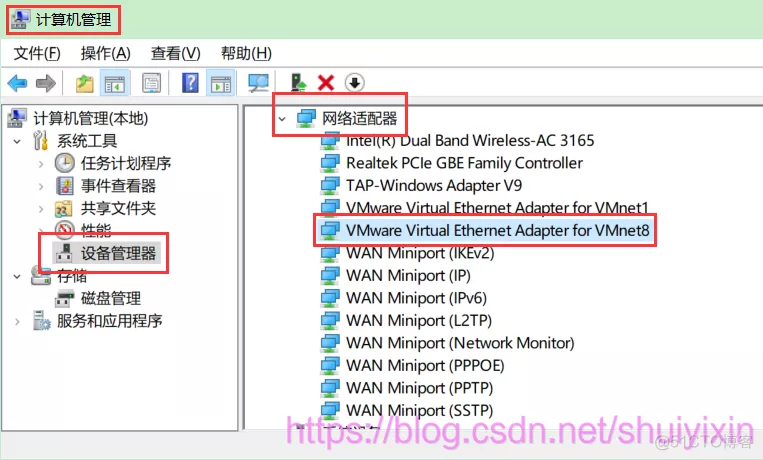


1. **遇到多网卡的问题，例如锐捷客户端提示:请将下列网卡禁用或者断开连接。**

遇到这个问题，首先我们要知道这个的网卡是哪一个，我们打开黑窗体，如果有对应ip地址用ipconfig查询：

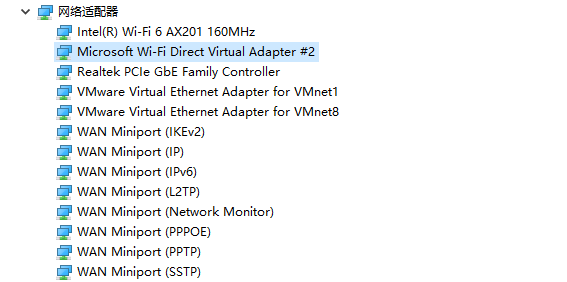


我们找到这个网卡后，打开计算机管理，进入网络适配器，右键禁用对应网卡即可：



如果没有对应的ip地址，仅有网卡名称，可以右击”我的电脑”，打开”管理”,“网络适配器”，

来寻找对应网卡，并且禁用。



1. **还有情况是虚拟机的网络设置问题，导致多网卡故障问题出现。**

在NAT模式下虚拟机连接外网，会导致一台电脑多个ip，且会被锐捷客户端检测到踢下线。

**NAT模式和桥接模式介绍:**

https://www.51cto.com/article/595506.html

一、Brigde——桥接：默认使用VMnet0

1、原理：

Bridge 桥"就是一个主机，这个机器拥有两块网卡，分别处于两个局域网中，同时在"桥"上，运行着程序，让局域网A中的所有数据包原封不动的流入B，反之亦然。这样，局域网A和B就无缝的在链路层连接起来了，在桥接时，VMWare网卡和物理网卡应该处于同一IP网段 当然要保证两个局域网没有冲突的IP.

VMWare 的桥也是同样的道理，只不过，本来作为硬件的一块网卡，现在由VMWare软件虚拟了!当采用桥接时，VMWare会虚拟一块网卡和真正的物理网卡就行桥接，这样，发到物理网卡的所有数据包就到了VMWare虚拟机，而由VMWare发出的数据包也会通过桥从物理网卡的那端发出。

所以，如果物理网卡可以上网，那么桥接的软网卡也没有问题了，这就是桥接上网的原理了。

2、联网方式：

这一种联网方式最简单，在局域网内，你的主机是怎么联网的，你在虚拟机里就怎么连网。把虚拟机看成局域网内的另一台电脑就行了!

提示：主机网卡处在一个可以访问Internet的局域网中，虚拟机才能通过Bridge访问Internet。

二、NAT——网络地址转换:默认使用VMnet8

1、原理：

NAT 是 Network address translate的简称。NAT技术应用在internet网关和路由器上，比如192.168.0.123这个地址要访问internet，它的数据包就要通过一个网关或者路由器，而网关或者路由器拥有一个能访问internet的ip地址，这样的网关和路由器就要在收发数据包时，对数据包的IP协议层数据进行更改(即 NAT)，以使私有网段的主机能够顺利访问internet。此技术解决了IP地址稀缺的问题。同样的私有IP可以网关NAT 上网。

VMWare的NAT上网也是同样的道理，它在主机和虚拟机之间用软件伪造出一块网卡，这块网卡和虚拟机的ip处于一个地址段。同时，在这块网卡和主机的网络接口之间进行NAT。虚拟机发出的每一块数据包都会经过虚拟网卡，然后NAT，然后由主机的接口发出。

虚拟网卡和虚拟机处于一个地址段，虚拟机和主机不同一个地址段，主机相当于虚拟机的网关，所以虚拟机能ping到主机的IP，但是主机ping不到虚拟机的IP。

2、联网方式：

方法1、动态IP地址。

主机是静态IP或动态IP，都无所谓，将虚拟机设置成使用DHCP方式上网,Windows下选择“自动获取IP“，linux下开启DHCP服务即可。(这种方法最简单，不用过多的设置，但要在VMware中进行“编辑→虚拟网络设置”，将NAT和DHCP都开启了。一般NAT默认开启，DHCP默认关闭)

方法2、静态IP地址。

如果不想使用DHCP，也可以手动设置：

IP设置与vmnet1同网段,网关设置成vmnet8的网关(在“虚拟网络设置”里的Net选项卡里能找到Gateway)通常是xxx.xxx.xxx.2。

子网掩码设置与VMnet8相同(设置好IP地址后，子网掩码自动生成)

DNS设置与主机相同。

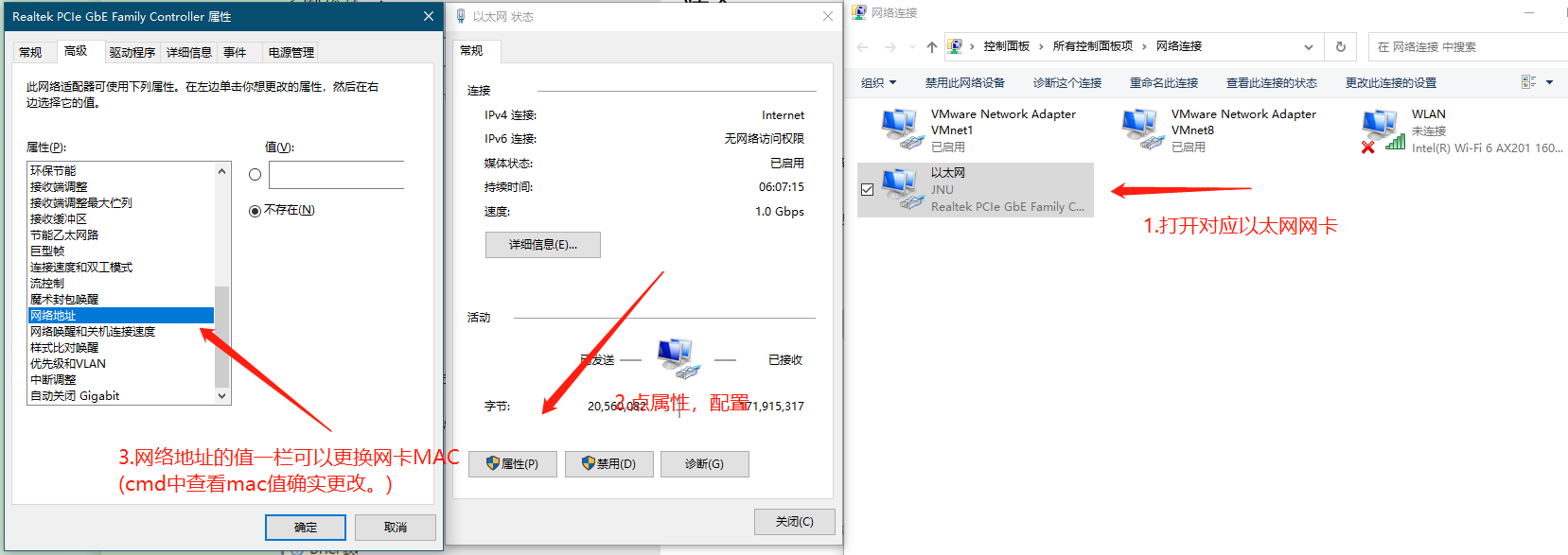
例如：主机IP是10.70.54.31,设置虚拟机IP为10.70.54.22。Netmask,Gateway,DNS都与主机相同即可实现 虚拟机 ---主机 虚拟机<---->互联网 通信。

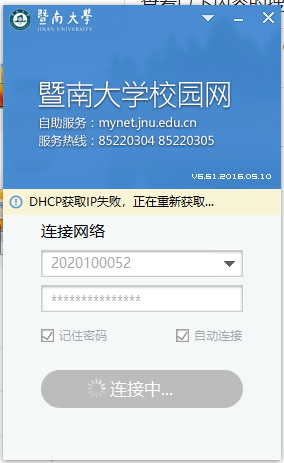
提示：使用NAT技术，主机能上网，虚拟机就可以访问Internet，但是主机不能访问虚拟机。

1. 在适配器中更换mac地址的操作:

在适配器的对应网卡中我们可以尝试更换网卡的MAC地址，但是会导致锐捷客户端无法成功认证。

修改操作:





1. **netsh winsock reset：**

其中Winsock 是一种[应用程序编程接口 (API)](https://www.howtogeek.com/343877/what-is-an-api/)，可在应用程序（如 Web 浏览器）和底层通信协议（如[TCP/IP）](https://www.howtogeek.com/751880/the-foundation-of-the-internet-tcpip-turns-40/)之间工作。如果一台机器上的Winsock协定配置有问题的话将会导致网路连线等问题，就需要用netsh winsock reset命令来重置Winsock目录借以恢复网路。这个命令可以重新初始化网路环境，以解决由于软体冲突、病毒原因造成的参数错误问题。netsh是一个能够通过命令行操作几乎所有网路相关设定的接口，比如设定IP，DNS，网卡，无线网路等，Winsock是系统内部目录，Winsock是Windows网路编程接口，winsock工作在套用层，它提供与底层传输协定无关的高层数据传输编程接口，reset是对Winsock的重置操作。当执行完winsock的命令重启计算机后，需要重新配置IP。