整机隔离方案

——

虚拟机仅主机(Host-Only)模式

安全上网的方法

完整版

二零一三年八月三日

前　言 4
- 整机隔离方案网络结构示意图 4
- 适用范围 4
- 名词解释 5

核心设置介绍 5
一、　在主机中的设置 7
（一）　Host-only 网卡的设置（仅主机网络） 7
- 虚拟机软件是 VirtualBox（如果是 VMware 请看后续部份） 7
- 虚拟机软件是 VMware（如果是 VirtualBox 请看前一部份） 11

（二）　主机参数设置 16
A. 运行“设置.bat” 16
B. 检查与手动禁用 Server、Task Scheduler、Remote Registry 服务 23
C. 手动设置部份 24
（１）去掉勾选 Microsoft 网络客户端 25
（２）卸载 Microsoft 网络的文件和打印机共享 26
（３）禁用 NetBios 27
（４）本地连接网卡设置固定 IP 29
（５）检查设置 32

（三）　主机破网软件的设置 33
- 自由门/逍遥游 33
- 无界浏览 35
- TorManager2.7 36

（四）　主机防火墙设置 38
A. 主机 IPSEC（必设置） 38
B. WIN7 自带防火墙（建议禁用） 42
C. 第三方防火墙的设置（必选 ZA 或 COMODO 之一） 43

二、　在虚拟机中的设置 48
（一）　VirtualBox 和 VMware 虚拟机里设置方法相同 48
A. 运行“设置.bat” 49
B. 虚拟机手动设置部份 52

（二）　虚拟机里上网程序的设置 52
- IE 浏览器 53
- Firefox(火狐) 55

（三）　虚拟机内防火墙设置 58
A. 虚拟机 IPSEC（必设置） 58
B. 第三方防火墙的设置（必选 ZA 或 COMODO 之一） 58

三、　联网测试 58
（一）　先查看主机的真实 IP 58
（二）　再到虚拟机里查看使用代理后的 IP 59

四、　安全事项必读 60
五、　附加功能：不隐藏 IP 登陆国内网站 60

附 录 63
1) 设置.bat （适用于 WINXP/WIN7） 63
2) 开启 SERVER 服务 69
3) WIN7 防火墙.bat （适用于 WIN7） 70
4) IP Routing Enabled 启用原因和停止方法 72
5) 主机“手动设置部份”恢复的方法 76
6) 无线路由器安全设置实用技巧（节选） 81
7) 受限帐户基础 82
8) TorManager2.7 管理器 83
9) 加密盘 TrueCrypt 的说明 83
10) 虚拟机 VirtualBox 的说明 83
11) 虚拟机 VMware 的说明 84
12) 防火墙软件 COMODO，ZoneAlarm 的相关教程 84
结 语 85

前　言

本方案可以将虚拟机与主机进行有效的隔离，防止主机的物理信息被窃取带来的安全隐患；同时只有通过匿名代理的通道才能访问网络，避免网络上的误操作带来的风险。

本设计方案采用虚拟机的仅主机(Host-only)模式；其它虚拟机网络模式不适合本方案。

● 整机隔离方案网络结构示意图

● 适用范围

- 一般用户的安全上网：能避免因各种误操作带来的风险；
- 测试运行不安全的软件；

说明：完整版提供了一些思路，而不是标准；还需要使用者逐步应用与发展。本教程适用于WINXP与WIN7，相同之处按WINXP界面显示；WIN7 与WINXP操作不同之处会单独说明或图示。如果主机操作系统设置为受限帐户或受限运行的状态将更安全，设置方法请参考受限帐户基础。

注意：　在熟练运用此方案前不要直接用于网络讲真相；网络讲真相还需要有配套方案，具体请到禁书网交流。

● 名词解释

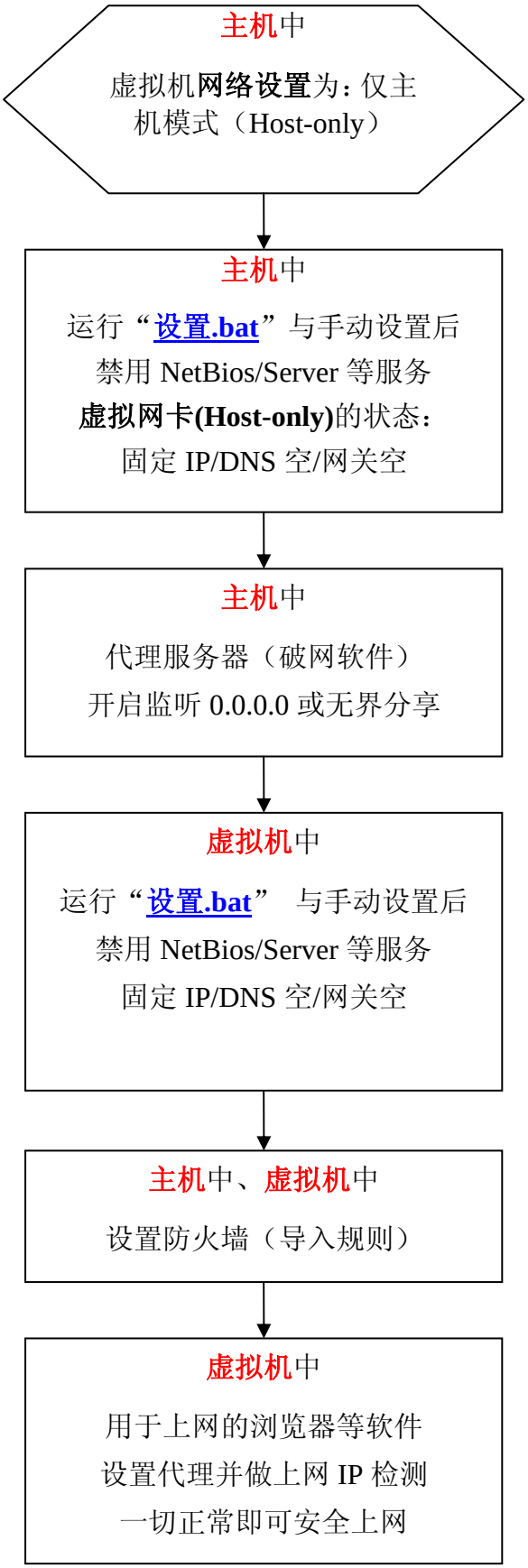
- ✧ **仅主机(Host-only)**：虚拟机有多种联网方式，如 NAT，Bridge 等；我们这里选择了 Host-only 方式，字面意思是指与主机共享的一个私有网络；
- ✧ **主机**：本地实体计算机，或称本机；也是仅主机(Host-only)联网方式中的主机；
- ✧ **主机网卡**：本地实体计算机用于本地连接的网卡；
- ✧ **主机虚拟网卡**：本地实体计算机上，在安装了虚拟机程序后产生的虚拟网卡；在本教程中特指(Host-only)虚拟网卡（除此之外可能有 NAT、Bridge 网卡等，需卸载）；
- ✧ **虚拟机**：安装 VirtualBox 或 VMware 虚拟机软件及操作系统，登录虚拟操作系统后的虚拟计算机；在本方案中，设置完备后我们将在虚拟机中上网，可与主机隔离；
- ✧ **虚拟机网卡**：登录虚拟机后，虚拟机中用于本地连接的网卡；
- ✧ **仅主机(Host-only)模式**：特指本教程中介绍的上网模式。也就是说，设置主机虚拟网卡【这里特指(Host-only)虚拟网卡】的 IP；除主机本地连接网卡外，主机虚拟网卡(Host-only)与虚拟机内本地连接网卡均不设置网关与 DNS；同时在主机与虚拟机中停用 NetBios、Server、Task Scheduler 和 Remote Registry 服务；之后设置虚拟机中浏览器或软件的代理 IP 为主机虚拟网卡(Host-only)的 IP，并设置与破网软件对应的端口；然后即可在虚拟机中安全上网。

（返回前言）（返回核心设置介绍）

核心设置介绍

分六步骤：

- ➢ 主机中启动虚拟机软件，将建立的虚拟机的网络模式设置为仅主机 (Host-only)方式；
- ➢ 主机中对主机虚拟网卡【仅主机 (Host-only)网卡】设置为固定IP（与虚拟机本地连接在同一网段），DNS为空，网关为空，同时主机上禁用NetBios、Server、Task Scheduler和Remote Registry服务；由“设置.bat”（附录 1）脚本与手动设置完成；
- ➢ 主机中架设代理服务器，开启侦听 0.0.0.0（自由门系列软件或 Tor）或 “无界分享”；
- ➢ 虚拟机内网卡（虚拟机本地连接）设置为固定IP【与仅主机 (Host-only)网卡在同一网段】，DNS为空，网关为空，同时虚拟机上禁用NetBios、Server、Task Scheduler和Remote Registry服务；由“设置.bat”脚本与手动设置完成；
- ➢ 主机与虚拟机中设置防火墙并导入提供的规则，此规则将迫使虚拟机只能通过仅主机(Host-only)网卡及代理服务器上网；
- ➢ 虚拟机中的浏览器或其它软件设置代理——即代理 IP 为主机虚拟网卡【仅主机(Host-only)网卡】设置的固定 IP，代理端口与主机中破网软件（代理服务器）的端口对应——完成后即可上网测试。


主机中
虚拟机网络设置为：仅主机模式（Host-only）
主机中
运行“设置.bat”与手动设置后
禁用 NetBios/Server 等服务
虚拟网卡(Host-only)的状态：
固定 IP/DNS 空/网关空
主机中
代理服务器（破网软件）
开启监听 0.0.0.0 或无界分享
虚拟机中
运行“设置.bat” 与手动设置后
禁用 NetBios/Server 等服务
固定 IP/DNS 空/网关空
主机中、虚拟机中
设置防火墙（导入规则）
虚拟机中
用于上网的浏览器等软件
设置代理并做上网 IP 检测
一切正常即可安全上网

一、在主机中的设置

（一）Host-only 网卡的设置（仅主机网络）

说明：使用不同的虚拟机可以选择对应的教程部份，但由于篇幅一些重要提示可能没有重复出现在不同的虚拟机说明中，因此建议所有红色字体部份都浏览一下，无关的可跳过。

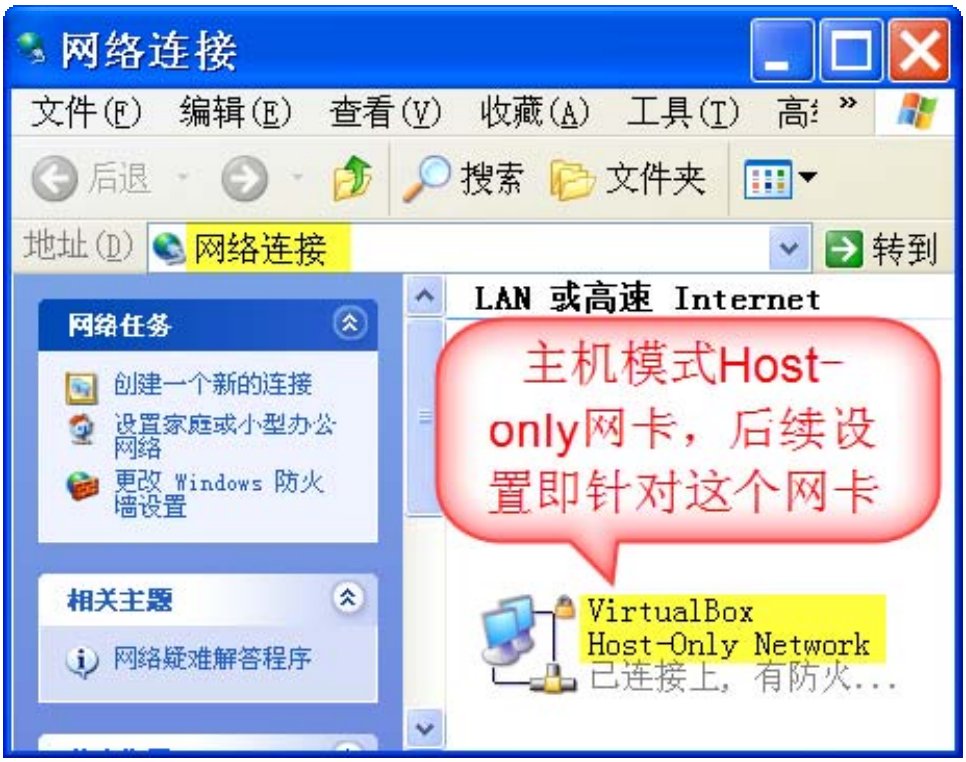
➢ 虚拟机软件是VirtualBox（如果是VMware请看后续部份）

注意：VirtualBox 与 VMware 虚拟机软件任选一款即可，无需两个都安装；VMware 软件请点击上面超链接“如果是 Vmware 请看后续部份”跳转到相关内容（即按住 CTRL 并在该文字上单击鼠标）。

A. VirtualBox 的网卡识别

1. VirtualBox 安装完毕后，在**网络连接**会出现 VirtualBox Host-only Network，这就是 VirtualBox 的 Host-only 网卡，仅主机模式的设置就针对这个网卡：

注意：建议安装虚拟机时不要勾选安装Bridge网络，如果已经安装且安装了网卡，可按后续方法卸载。



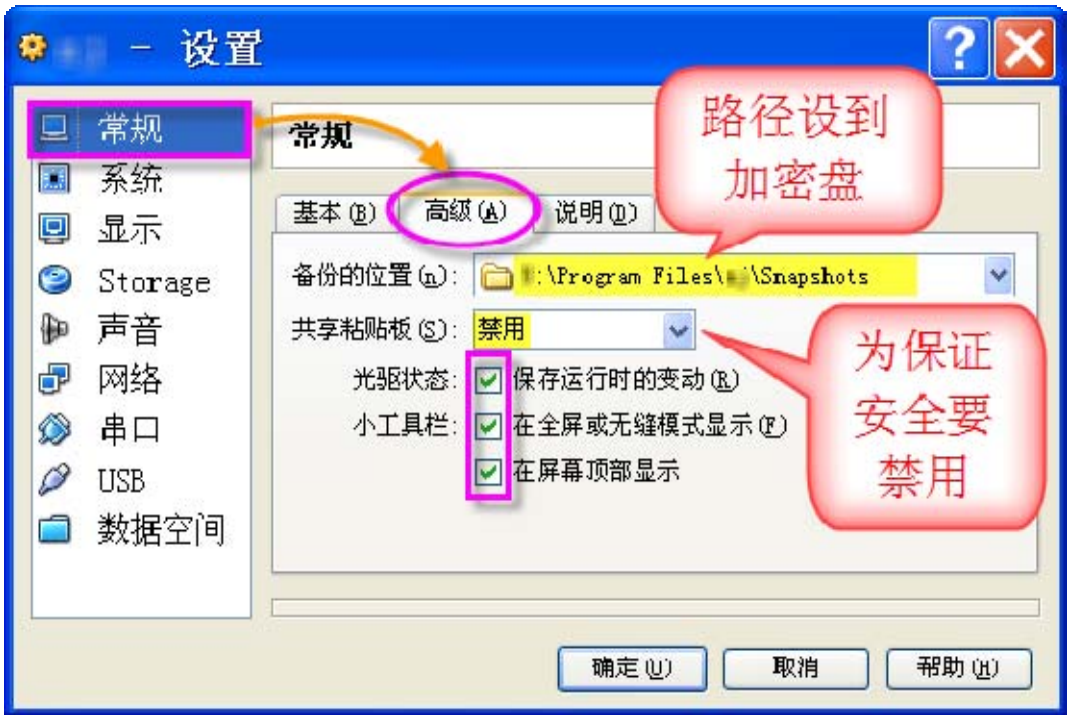
B. Host-Only 网络模式设置

1. 如果虚拟机之前已设置好，只设置网络部份可点击**网络**进行设置。

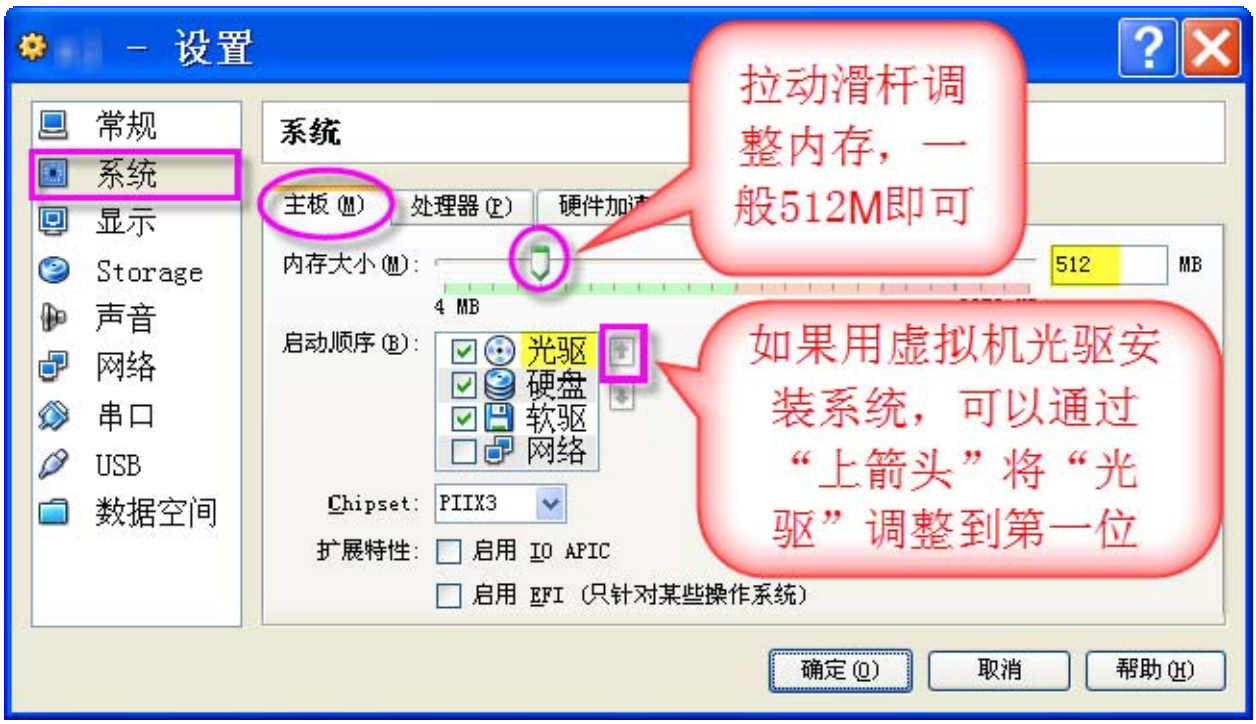
说明：由于以前使用的虚拟机与仅主机模式大不相同，且以前使用的虚拟机带有其特征；为了保证安全，建议全新建立虚拟机或从一个纯净的虚拟机克隆（有不同的 UUID 等）。

2. **全新设置**：安装虚拟机后全新设置，以下图示未涉及的部份，按其原本默认的设置即可。在虚拟机关闭状态下，选中虚拟机，点**设置**：

3. 在**常规 → 高级**，**备份的位置**选择加密盘的盘符（可与虚拟机在同一个加密盘）；**共享粘贴板**选择**禁用**，这样使用起来稍有不便，但可以避免一些恶意拷屏软件等；图示三个选项全勾选（这三个勾选不涉及安全问题，可依个人习惯更改）：



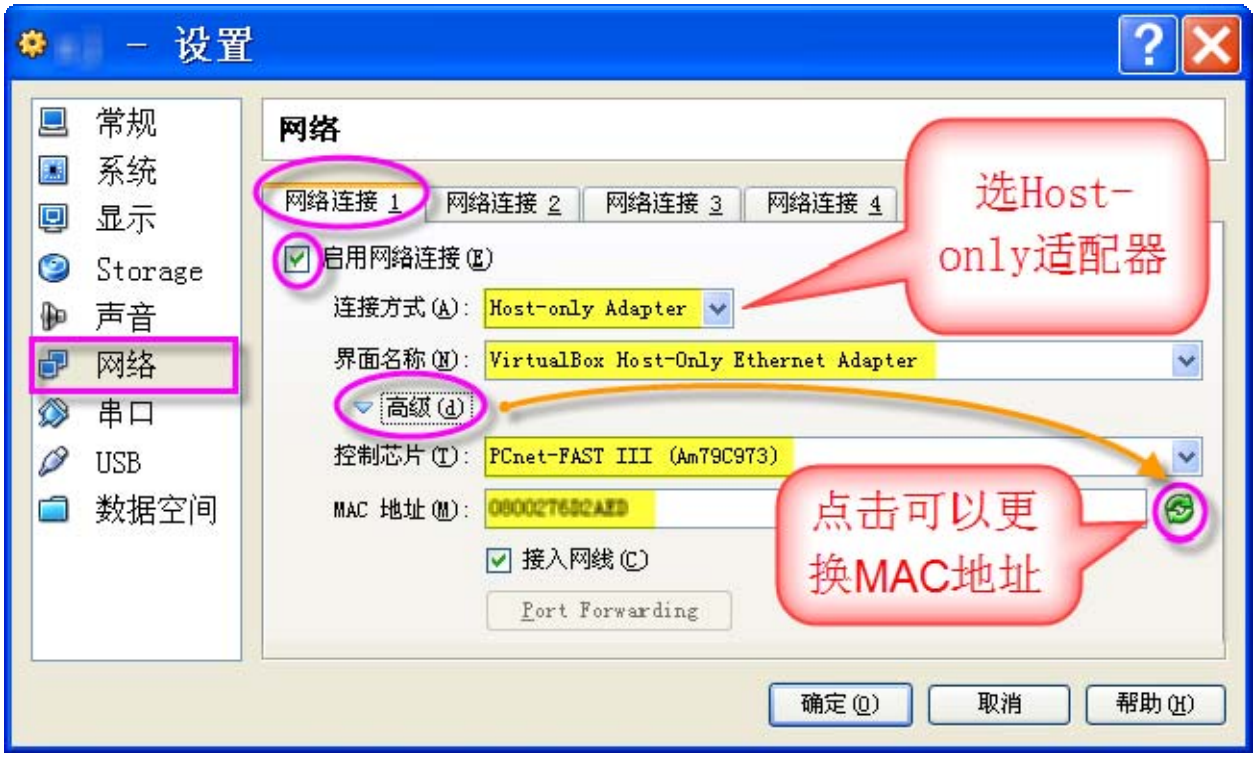
4. 在**系统 → 主板**，调整内存大小，一般 512M 即可；如果是新虚拟机需安装 Windows 系统（WINXP 使用起来较方便，当然 WIN7 亦可），可将**光驱**调整到第一**启动顺序**：



5. 在**显示 → 显卡**调整显存大小（可调到主机显存数值的一半）：

6. 在**网络 → 网络连接 1**，勾选**启用网络连接**，**连接方式**选 Host-only Adapter（仅主机适配器），**界面名称**选默认选项；点**高级**可以选择**控制芯片**并可更新 **MAC 地址**。

说明： MAC 地址是否虚拟机的特征之一尚无定论，请大家测试并到禁书网反馈。



7. **注意**：为了保证安全，建议虚拟机里不存敏感资料（虚拟机也建立在加密盘中），关联另外一个加密盘存储资料；这样操作后，只有当虚拟机的加密盘与另一个存储资料的加密盘同时打开、且盘符关联正确才能正常运行。**当然如果只是上网浏览可不必如此设置。**

   关联另一个加密盘的方法：在**数据空间**：（1）点**添加**图标，（2）选择已连接到主机的加密盘符，（3）勾选 Auto-mount（自动关联），点两个**确定**；

   到这里 VirtualBox 整个虚拟机设置就完成了：

➢ 虚拟机软件是VMware（如果是VirtualBox请看前一部份）

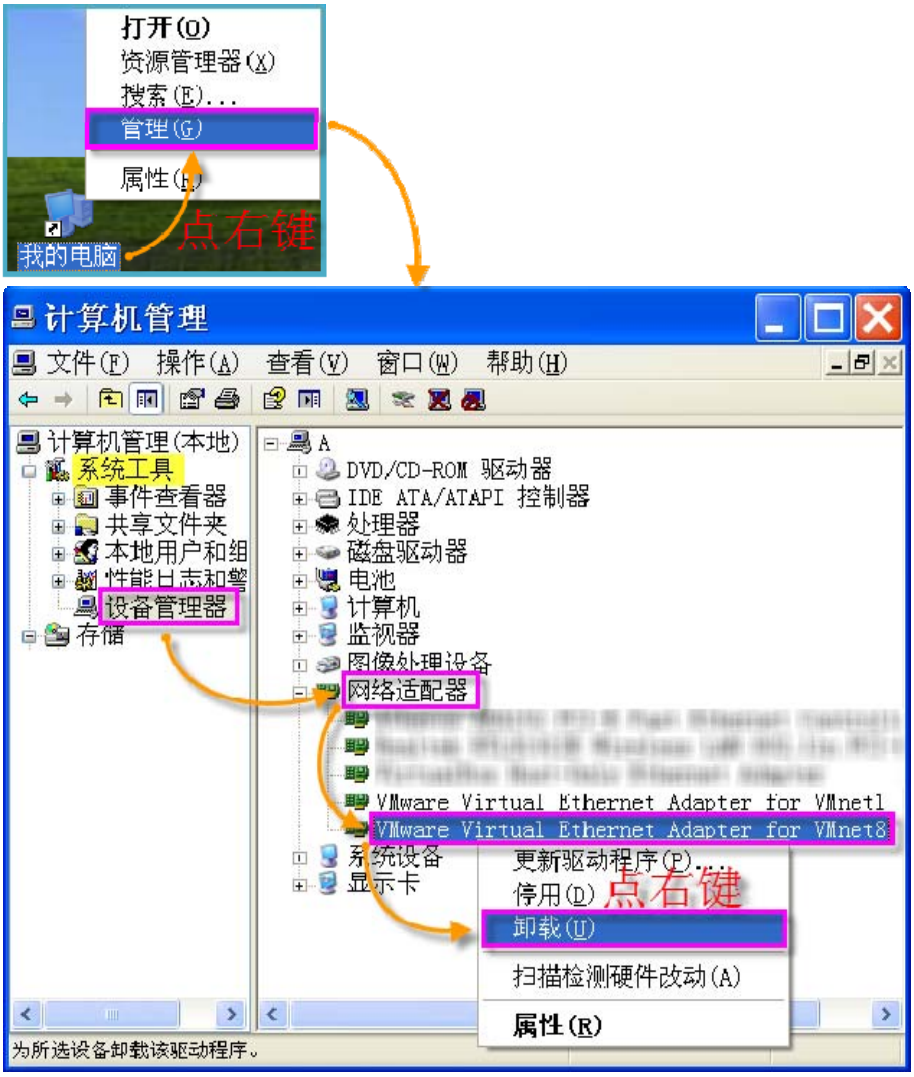
A. VMware 网卡识别与卸载 NAT 网卡

1. VMware 安装后会在网络连接中出现两个网卡：

   VMware Network Adapter VMnet1（VMware 仅主机模式网卡）
   VMware Network Adapter VMnet8（NAT 网卡，为避免漏洞必须卸载）：

注意：本方案中防火墙对 Host-only 网卡有特别的限定，其它网卡在导入的防火墙规则中未涉及，这样就会有漏洞。因此主机中除 Host-only 与本地连接网卡外应卸载所有其它网卡。如果准备使用本方案，需改变过去使用 NAT 或其它方式上网的习惯，按要求卸载 NAT 等其它网卡。另外，可建立多个虚拟机用于不同的用途。

2. 卸载其它网卡。在**我的电脑**点右键 → **管理** → **设备管理器** → **网络适配器** → **VMware Virtual Ethernet Adapter for VMnet8**，点右键 → 点**卸载**。同理，如果安装了微软的 Bridge（桥接）网卡（用于 VirtualBox），也可选中点右键、点**卸载**。



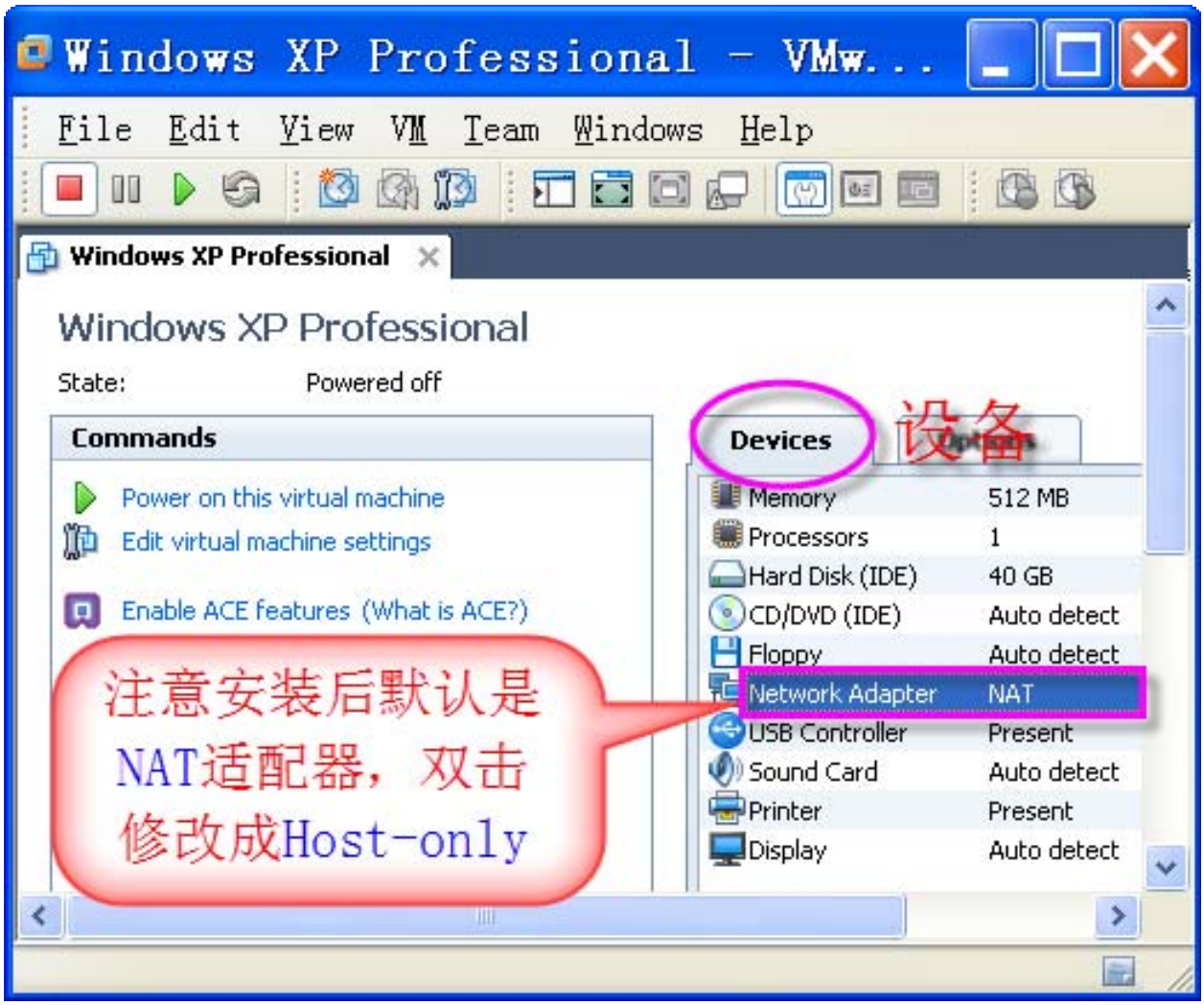
3. 点**确定**即卸载网卡完成：

（返回VirtualBox的网卡识别）

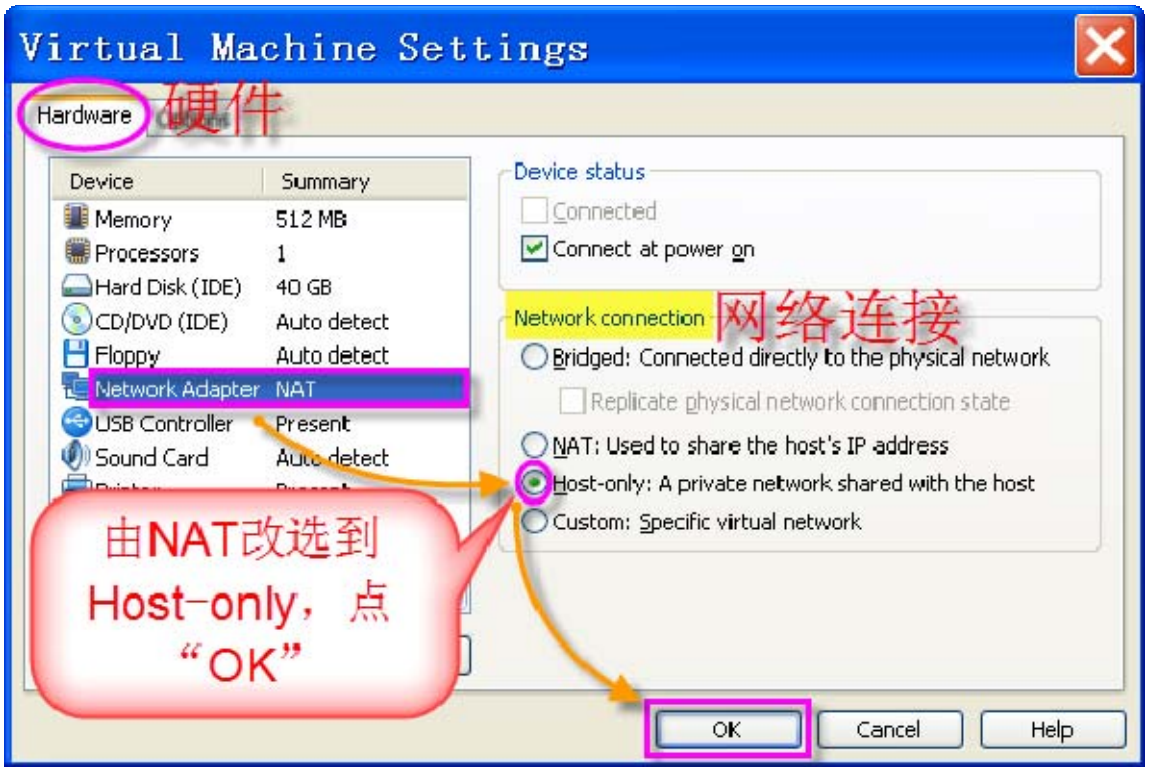
B. VMware Host-Only 网络模式设置

1. 启动 VMware 软件，打开一个已建立的虚拟机，在 **Devices**（设备）双击 **Network Adapter NAT**（网络适配器 NAT），准备修改成 Host-only。

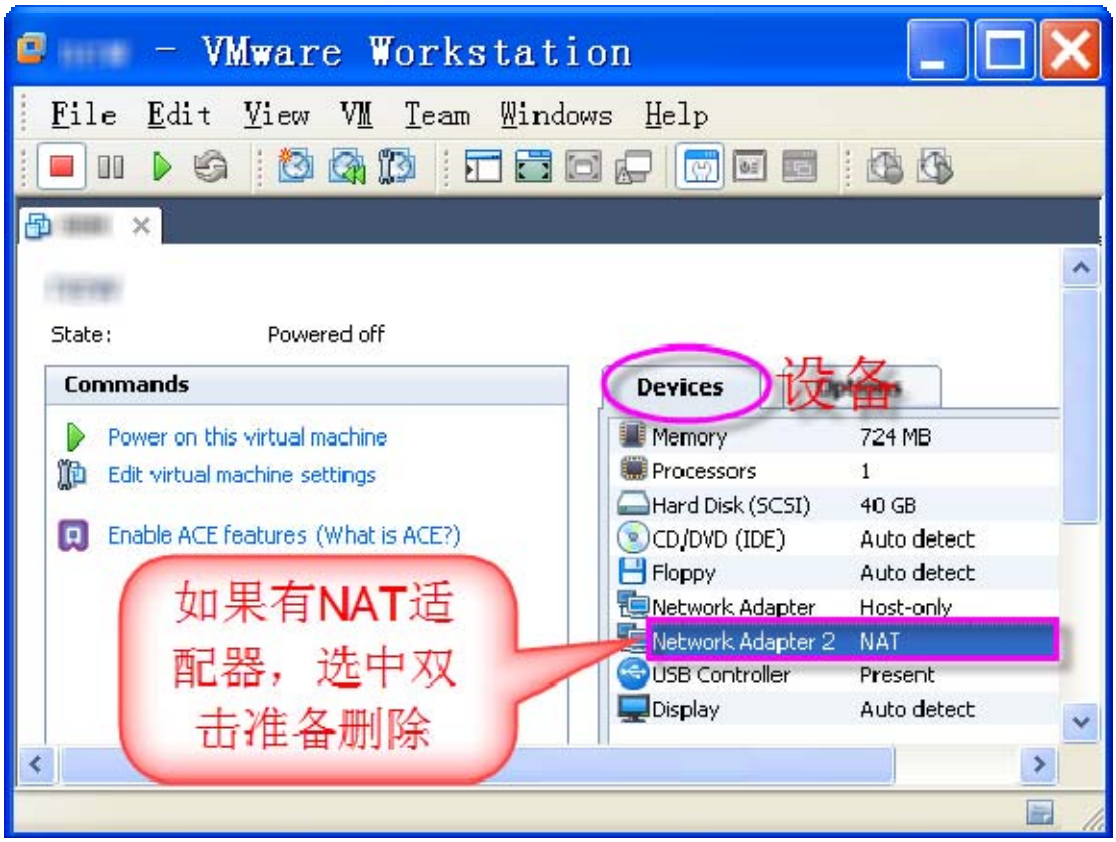
说明：由于以前使用的虚拟机模式与仅主机模式大不相同，且以前使用的虚拟机带有其特征；为了保证安全，建议全新建立虚拟机或从一个纯净的虚拟机克隆。



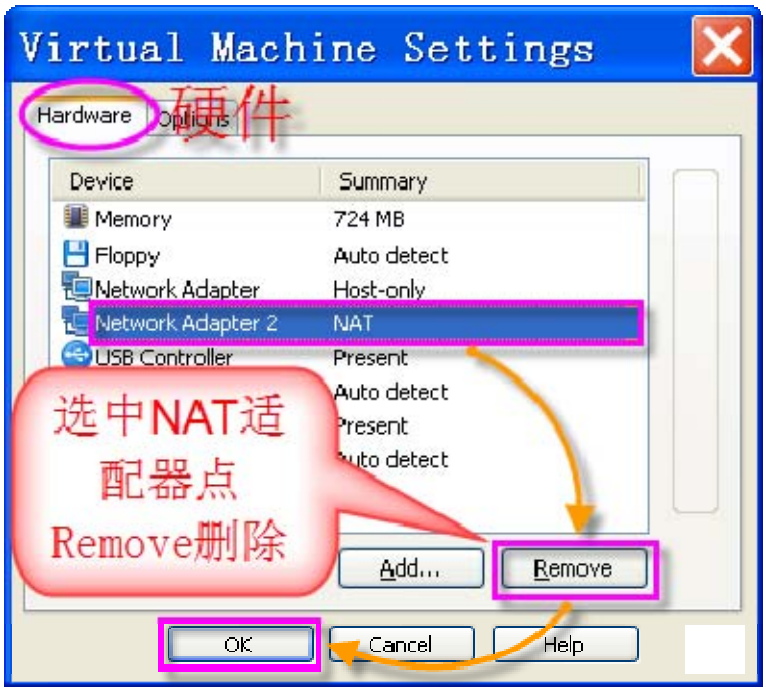
2. 在 **Hardware**（硬件），双击 **Network Adapter NAT**（网络适配器 NAT），在右侧 Network Connection（网络连接），由原来的 NAT 选项，更改成 Host-only，点 **OK**：



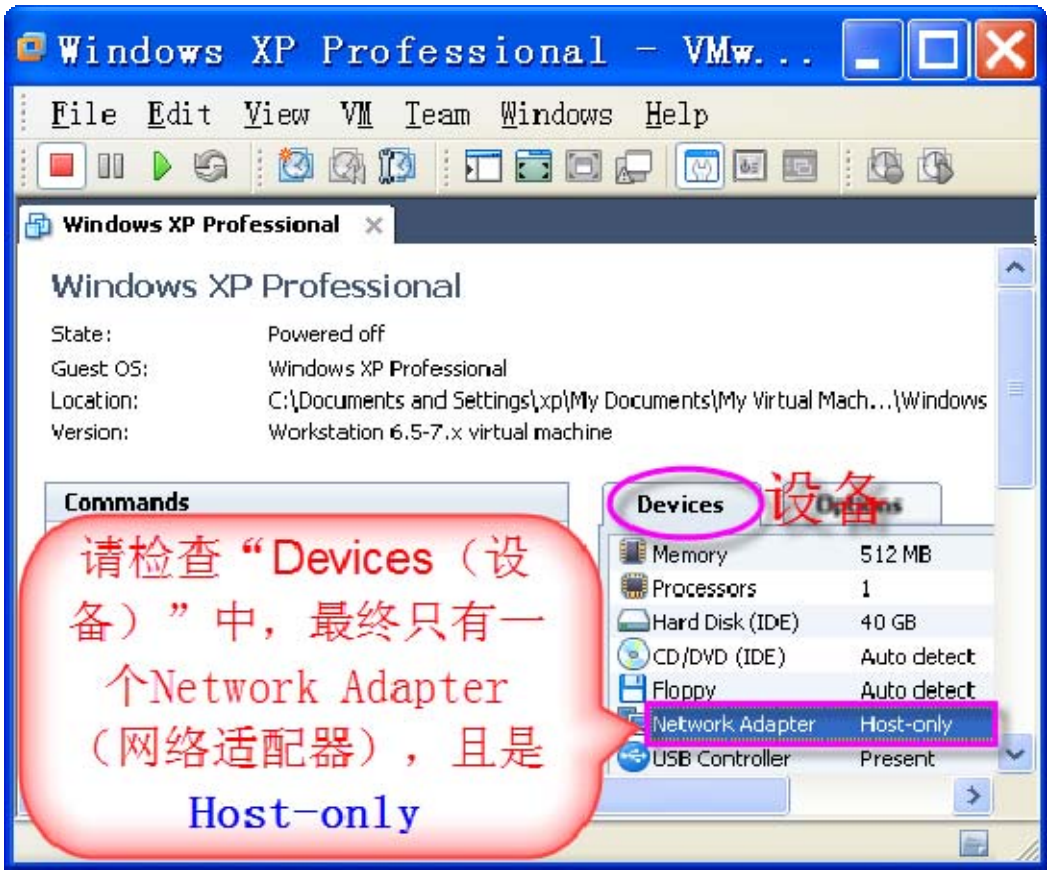
3. 如果虚拟机原来同时设置了 NAT 与 Host-only 适配器，要把 NAT 删除（很重要，否则虚拟机网络走 NAT 可能会造成 IP 泄露等）。方法是双击 Network Adapter(2) NAT：



4. 点击 Network Adapter(2) NAT，点 **Remove**（移除），点 **OK**：



5. 请注意最后查看 Devices（设备）中： Network Adapter（网络适配器）只有 Host-only 才行：



（二）主机参数设置

说明：

（1） **主机本地连接网卡需手动设置固定 IP，建议 DNS 服务器设置成国外的。**

（2） **主机上将主机虚拟网卡 (Host-only)网卡设置为固定IP，DNS为空，网关为空，同时主机上禁用NetBios、Server、Task Scheduler和Remote Registry服务。WINXP 直接运行“设置.bat”脚本加上手动设置来完成； WIN7 需以管理员身份运行 “设置.bat”， 即在本文件上点击鼠标右键选择“以管理员身份运行”，再加上手动设置；如果没有此脚本可以切换到附录中制作“设置.bat”。**

（3） **运行完成后，需从启计算机生效，然后对设置后的参数进行确认。主要确认 Host-only 网卡 DNS 为空，网关为空，Server、Task Scheduler、Remote Registry 服务和 NetBios（手动设置）禁用。如果没有设置成功，请联系禁书网来解决。**

（4） **IP 段分配要求：主机虚拟网卡(Host-Only)与虚拟机内网卡为同一个网段；同时跟主机其它网卡不在同一个网段。**本教程虚拟网卡网段以 192.168.188.*为例，因此主机本地连接网卡和所有其它网卡 IP 就一定不能是 192.168.188.*;不是特殊原因其它网卡必须卸载。

（5） 所有导入规则均按以下 IP 为例，如需修改请参考“FHQ_X.doc”(防火墙设置方法教程)，X 代表序列号，表示不同的版本，直接下载本站最新附件即可。

如果 VirtualBox 与 VMware 任使用一种，Host-only 网卡 IP 可以均设为 192.168.188.1，可以有 5 个虚拟机同时上网，虚拟机本地连接网卡 IP 可以是 192.168.188.2～192.168.188.6。

以下两条一般用户可跳过不看：

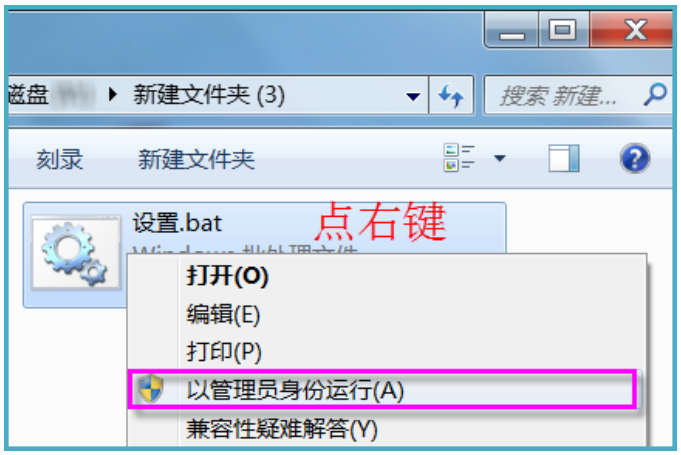
1) 如果 VirtualBox 与 VMware **两种**虚拟机都使用，且不是**两种**虚拟机同时上网，可以将上网的虚拟机的 Host-only 网卡 IP 设成 192.168.188.1，另一个改成比如：192.168.200.1；等下次用另一个虚拟机上网时再对换；这样无需修改防火墙。

2) 如果 VirtualBox 与 VMware **两种**虚拟机需同时上网，则需要修改防火墙：将所有 Host-only 的 IP 由 192.168.188.1 改成 IP 范围“192.168.188.1～192.168.188.2”，所有虚拟机网卡 IP 范围改成 192.168.188.3～192.168.188.6（可以有 4 个虚拟机同时上网）。当然虚拟机中浏览器或软件上网设置代理时要选相应的 Host-only 网卡的 IP。

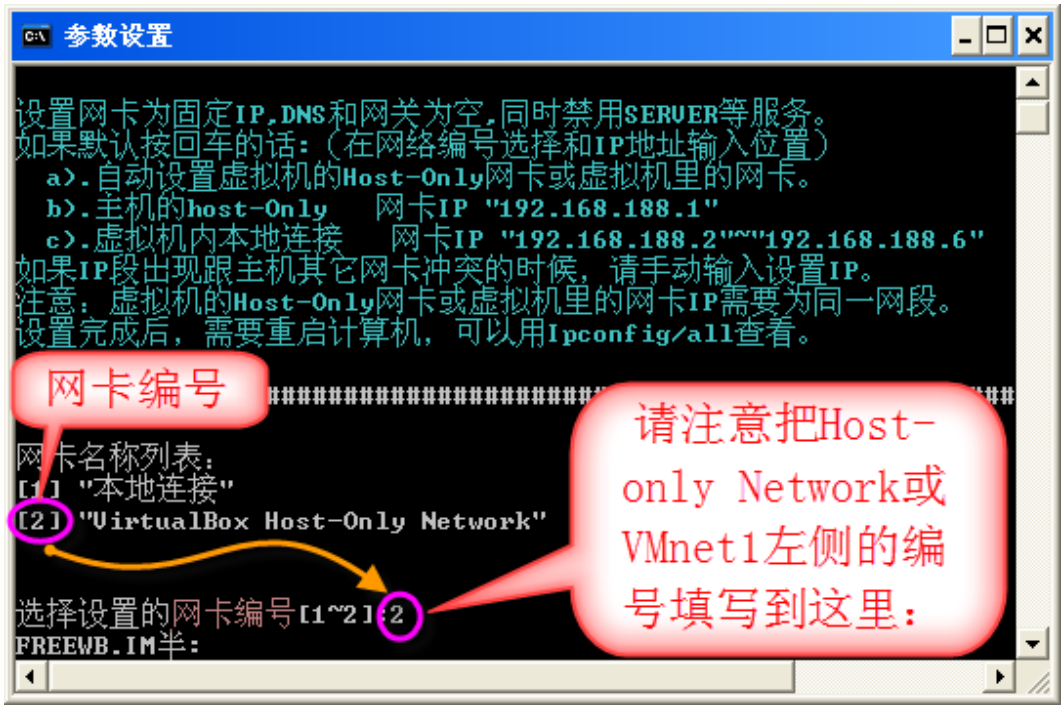
A. 运行“设置.bat”

1. **设置方法**：如果是WINXP系统，请直接在主机中运行“**设置.bat**”：

2. **如果是 WIN7 系统，需以管理员身份运行 “设置.bat”；即在本文件上点击鼠标右键选择“以管理员身份运行”：**



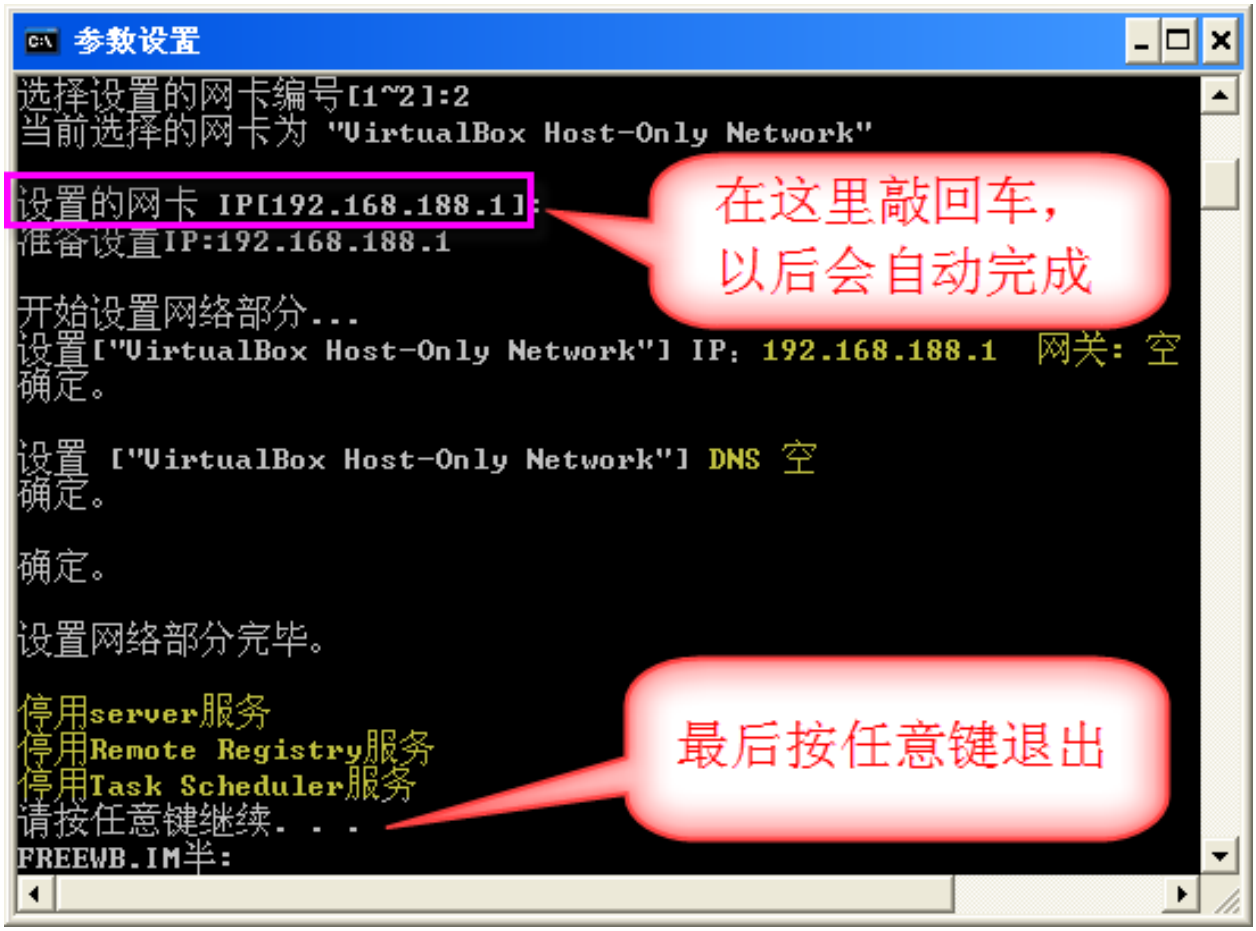
3. 请参考下图**参数设置**中浅兰色字体的设置说明。查看 VirtualBox Host-only Network（VirtualBox），或 VMware Network Adapter VMnet1（VMware）左侧对应的数字，填写到**选择设置的网卡编号**后，回车。



注意：设置时以实际 VirtualBox Host-only Network 或 VMware Network Adapter VMnet1 左侧的编号为准，不要直接把图示的编号填入。

4. 出现**设置的网卡 IP** 时，直接回车则按默认 IP 设置；或手动输入 IP 后回车。

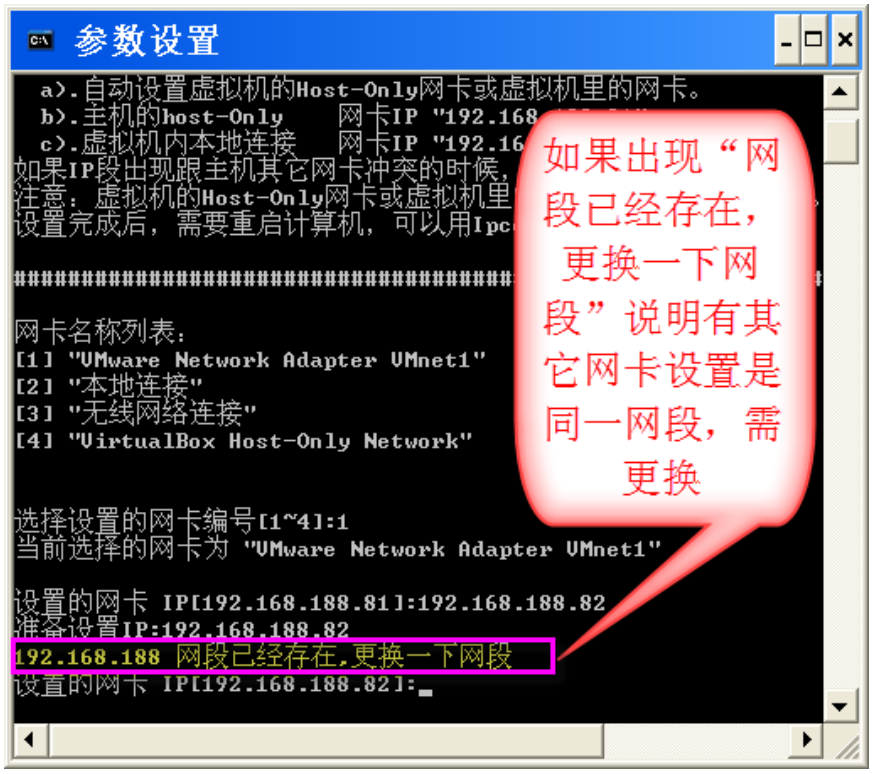
注意：一般无需手动修改 IP，如果特殊情况需要，所有的防火墙均需相应修改，否则将无法上网。



5. 如果出现“**网段已经存在，更换一下网段**”，说明主机中有网卡与此网段冲突。此提醒是为了保证 Host-only 网段的唯一性，避免与其它网卡（比如本地连接）网段重复带来不安全隐患，或不能正常上网——因为防火墙对 Host-only 网段 IP 的权限是有特别设置的。

特别提醒：1. 如果网卡是禁用状态，即使在相同网段也没有提示，因此凡禁用网卡要手动去**网络连接** → 选中**禁用**网卡点右键，点**属性** → **Internet 协议（TCP/IP）** → **属性**中查看 IP 是否在 192.168.188.x 网段，是的话手动修改 IP 到其它网段。以免**启用**后与 Host-only 在同一网段。

2. 运行“设置.bat”并从启计算机后一定要按步骤 7 查看主机 Host-only 网卡的 IP 是否 192.168.188.1；或选中 Host-only 网卡，点右键点**状态**，在**支持**页签查看，如果 **IP 地址**并非 192.168.188.1，要从新运行“设置.bat”；由此引申提醒：虚拟机浏览器上网时防火墙不弹出要经过代理上网的提示（指未将允许操作记忆的情况），说明代理有问题。要查看 Host-only 网卡 IP 是否 192.168.188.1、破网软件是否打开侦听 0.0.0.0、虚拟机内网卡是否 192.168.188.2 以及虚拟机浏览器是否选择了正确的代理及端口。

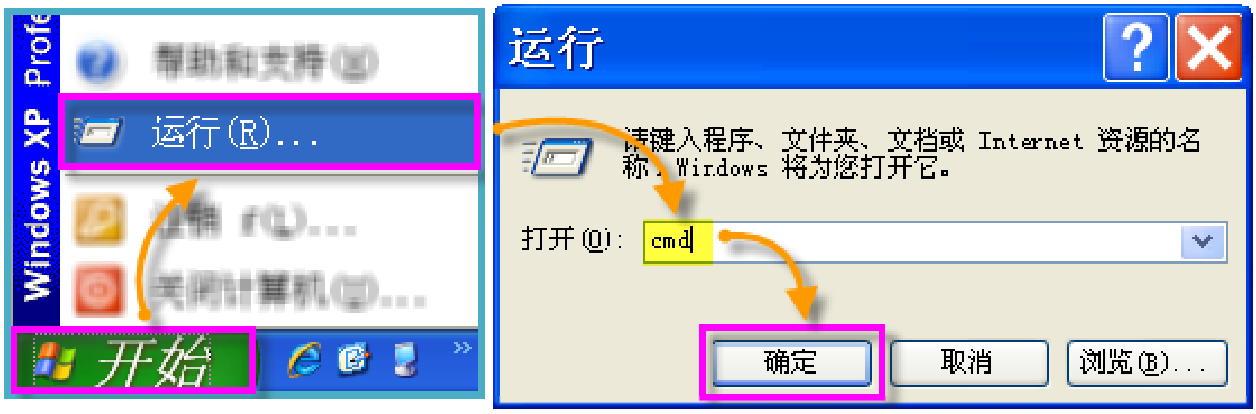


6. 还有一种可能是同时安装了两种虚拟机软件，之前设置了另一个虚拟机的网卡、造成网段重复，这时可以到之前设置的虚拟机 Host-only 网卡的 Internet 协议（TCP/IP）中手动修改到另一网段，需要用时再修改回来。这样可免去修改防火墙规则。

注意：修改时尽量与 188 外观差异大些，比如 200；否则如以下 189 与 188 很类似，有时上不了网不易发现问题。

7. 设置完毕需从新启动计算机；启动后需核查设置是否正确。

检测方法：计算机从启后，在**开始 → 运行**中输入 cmd，点**确定**：



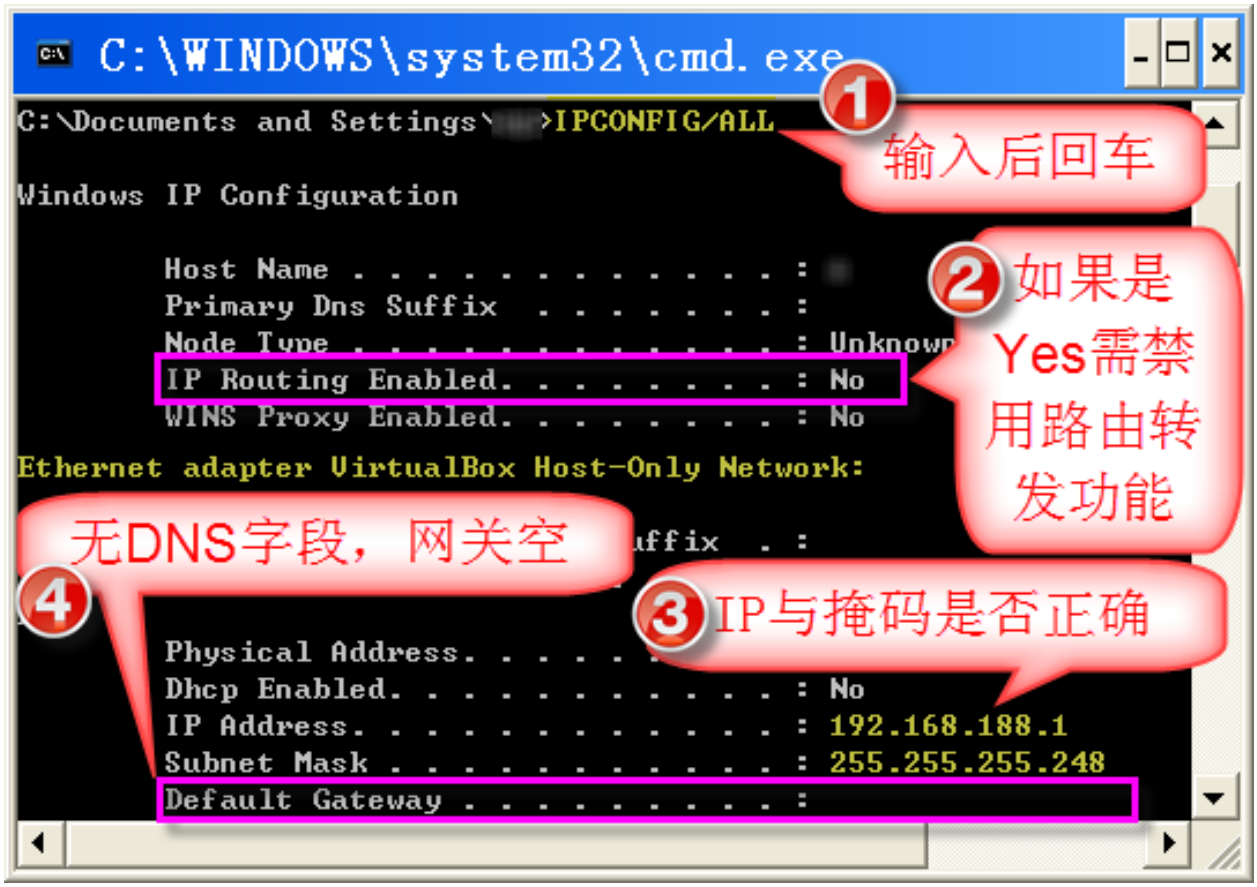
8. 在出现的 DOS 窗口中输入或查看以下几项内容：

（1） 输入 **ipconfig/all**，敲回车。

（2） **IP Routing Enabled**：正常是No。如果IP Routing Enabled显示是Yes的话，具有路由转发能力，将有安全隐患；必须经过设置后再检测显示为No才可以。请参考附录《IP Routing Enabled 启用原因和停止方法》；

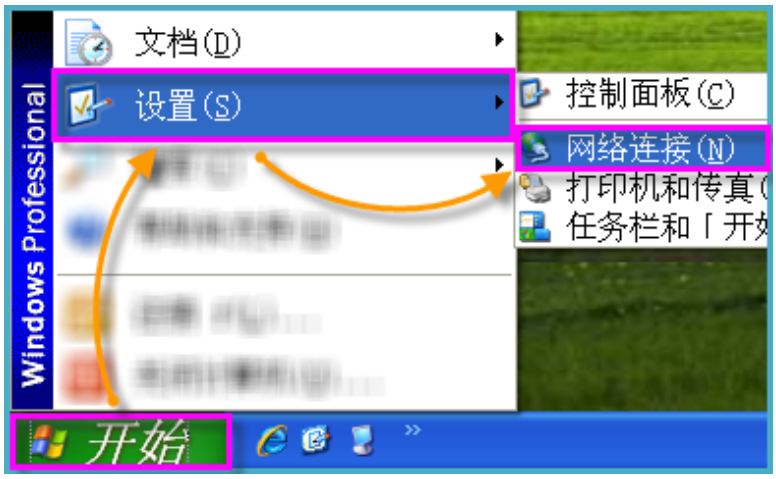
（3） **Host-only 网卡 IP** 地址是否设置正确；

（4） **Default Gateway** 是否为空；无 **DNS Server** 字段（特指 Host-only 网卡无此字段，而连网状态下**本地连接是**有 DNS Server 的）：

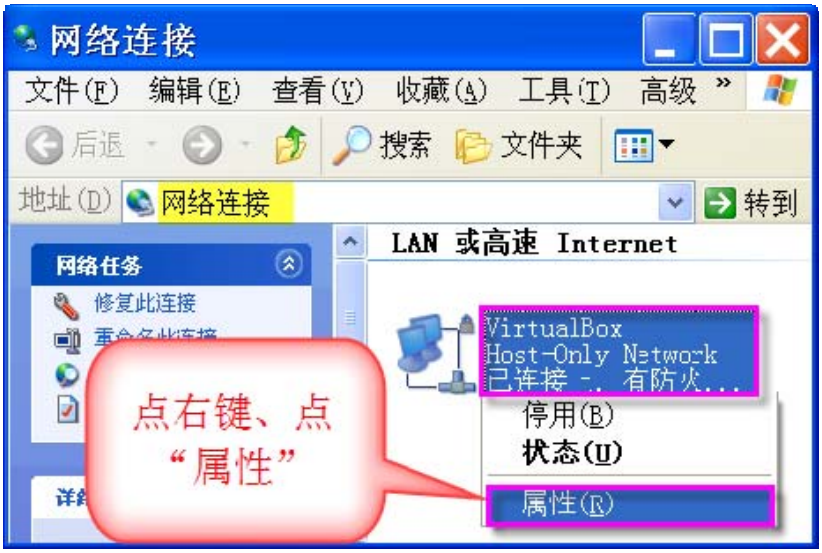


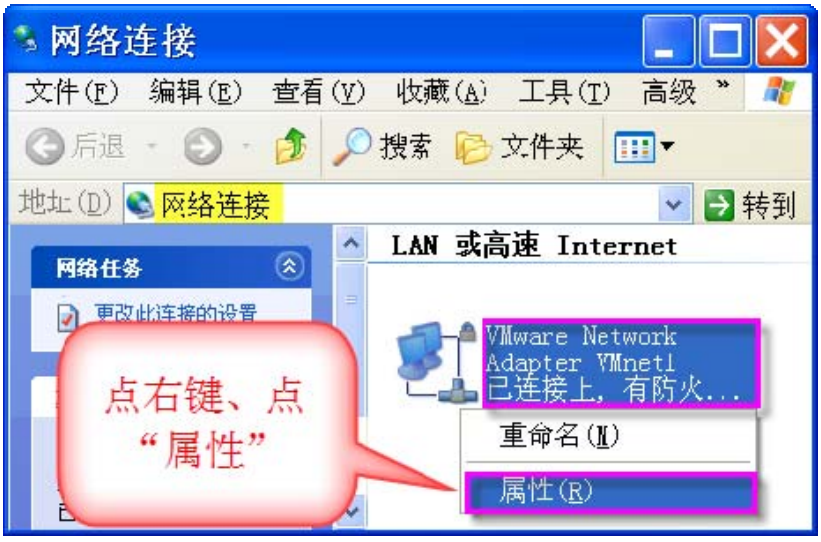
9. 其中的网关、DNS 部分也可通过 VirtualBox Host-only Network（或 VMware Network Adapter VMnet1）网卡的 Internet 协议（TCP/IP）的**属性**中查看。

步骤如下：在**开始 → 设置 → 网络连接：**



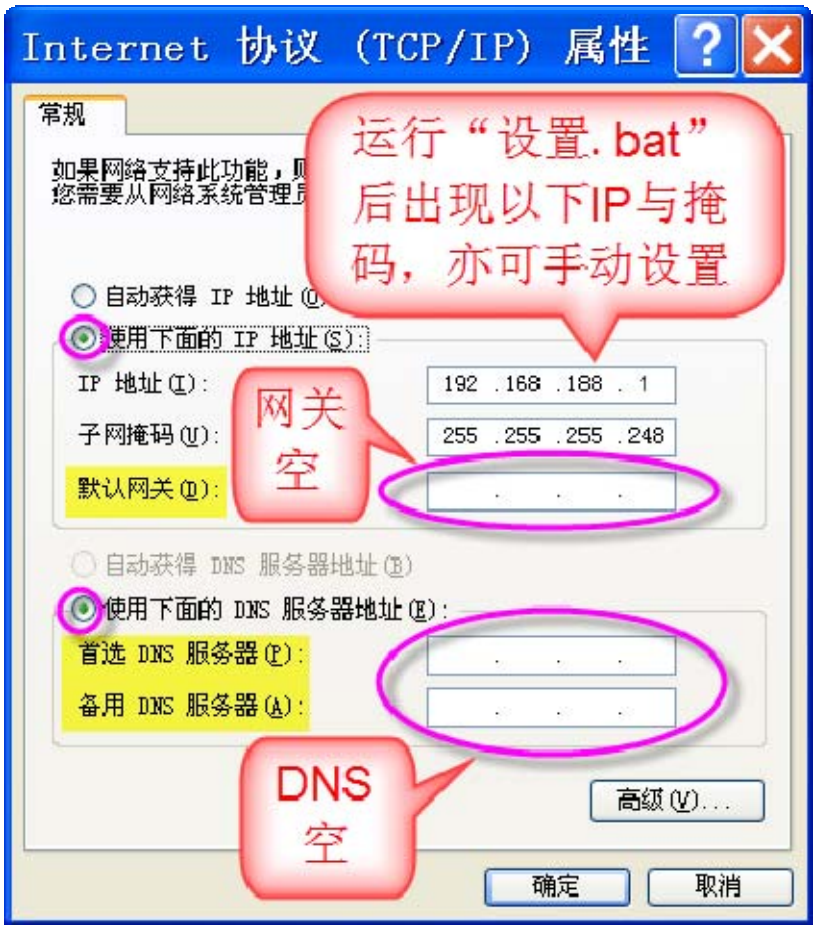
10. 选中 **VirtualBox Host-only Network**（或 **VMware Network Adapter VMnet1**）点右键 → **属性：**





11. 在**常规** → **Internet 协议（TCP/IP）** → **属性**：

12. 查看是否**默认网关**空，**DNS 服务器**空；非空则手动清空，手动设置 IP 亦可在这里修改：



注意：查看实时 IP 的方法：在电脑右下角**本地连接**图标点右键，点**状态**，在**支持**页签，点**详细信息**，这时看到的是实时 IP。有时忘记从启电脑会出现以下“详细信息”中的 IP 与设置的不同，因而不能正常上网。这时需从新运行“设置.bat”并从启计算机。

B. 检查与手动禁用 Server、Task Scheduler、Remote Registry 服务

1. 在**我的电脑**点右键，点**管理**：

2. 查看这三项服务是否**状态**均为空白，**启动类型**均为“已禁用”，如果不是需手动禁用；如果没有 SERVER 服务则无需设置：

3. 分别选中这三项中的一项，点右键点**属性**：

4. 在**启动类型**点右侧小箭头，选中**已禁用**，点**应用－停止－确定**；全部完成后从启计算机再次查看状态直至三项全部禁用：

C. 手动设置部份

重要说明：强烈建议一般用户完成这四个手动设置，将有利的保护安全。

高级用户可参考以下不同情况的对应设置办法：

◆ 如果需要在公共网络环境自动获取 IP，可跳过**手动设置部份**不设。

说明：如果能够知道公共网络的 IP 段，比如 192.168.0.x，可在完成“手动设置部份”的前提下手动设置固定 IP 上网；当然 IP 有可能冲突，可多尝试几个 IP，直至可联网。

◆ 如果需要共享文件或打印机，不要设置**手动设置部份**，主机需同时开启SERVER服务，

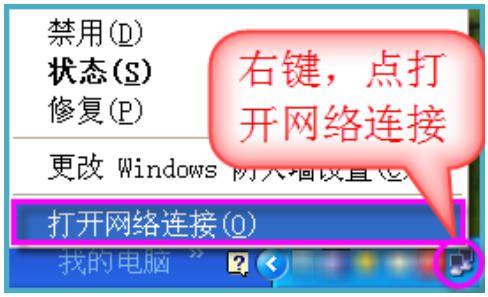
并修改开启文件与打印机共享的IPSEC设置，以及修改开启文件与打印机共享的COMODO设置和修改ZA设置；

重要提示：强烈建议禁用共享；如果实在需要共享最好不用实施本方案的电脑；如果必须用本电脑共享，有很大潜在隐患，请自行取舍。

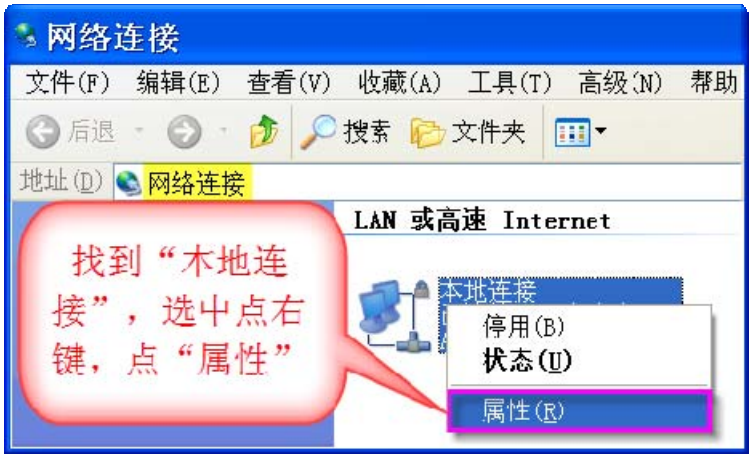
◆ 如果完成**手动设置部份**后，在某些情况又需在公共网络环境自动获取IP，或需共享文件或打印机，可按主机“手动设置部份”恢复的方法分别开启相关禁用的设置。

（1）去掉勾选 Microsoft 网络客户端

1. 在电脑右下角**本地连接**图标点右键，点**打开网络连接**：

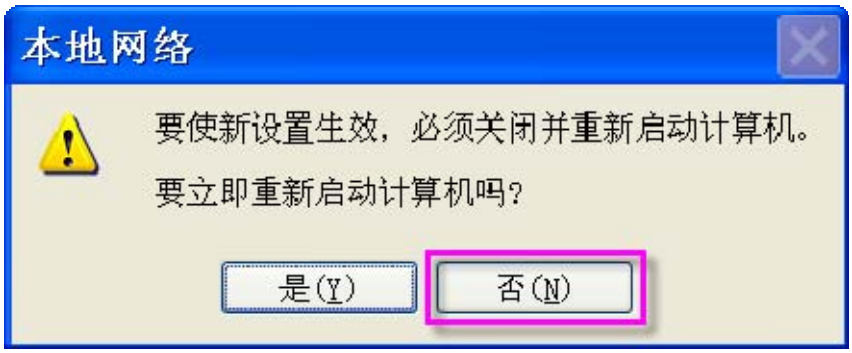


2. 在**本地连接**点右键，点**属性**：



3. 在**常规**页签，去掉 Microsoft 网络客户端的勾选：

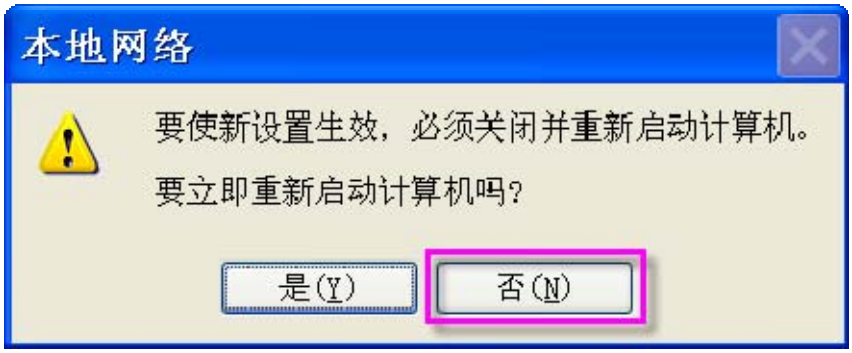
4. 如果提示是否启动计算机，选**否**（后续几项设置完成后一同从新启动计算机）：



（2）卸载 Microsoft 网络的文件和打印机共享

1. 同上在**本地连接**的**常规**页签，选中 **Microsoft 网络的文件和打印机共享**，点**卸载**：

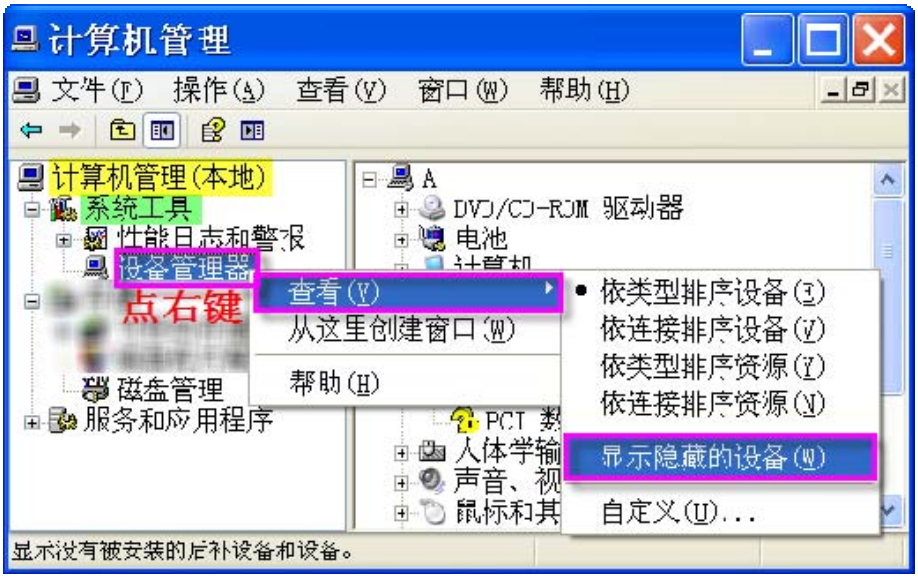
2. 提示是否启动计算机，选**否**（后续几项设置完成后一同从新启动计算机）：



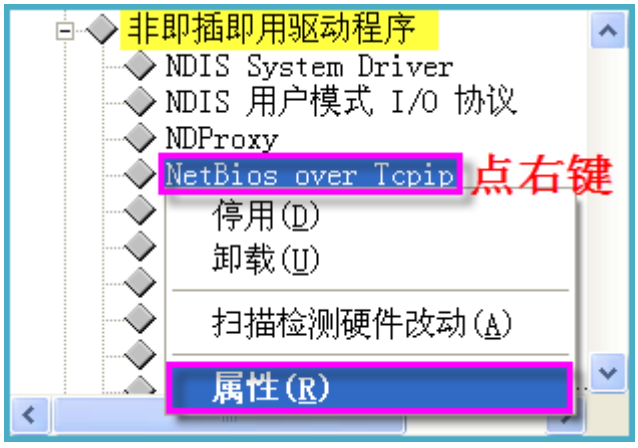
（3）禁用 NetBios

1. 在**我的电脑**点右键，点**管理**：

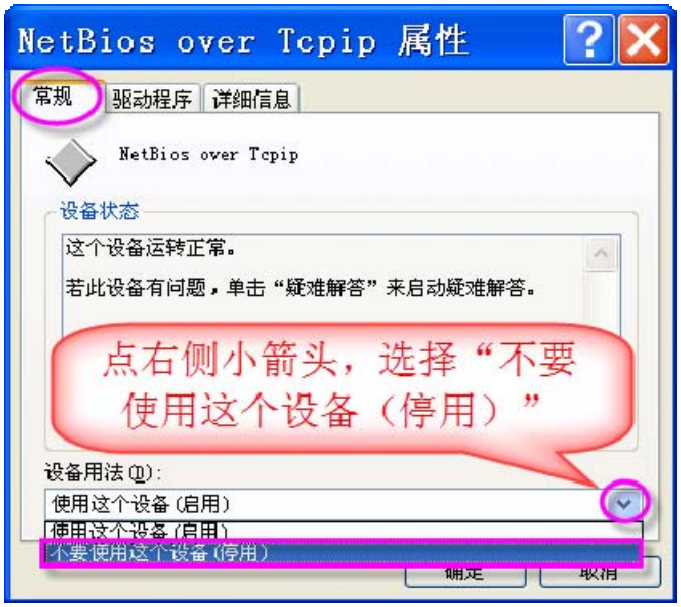
2. 在**设备管理器**点右键，点**查看**，点**显示隐藏的设备**：



3. 在**非即插即用驱动程序**中，找到 NetBios over Tcpip，点右键，点**属性**：



4. 在**常规**页签，点**设备用法**右侧小箭头，选择**不要使用这个设备（停用）**：

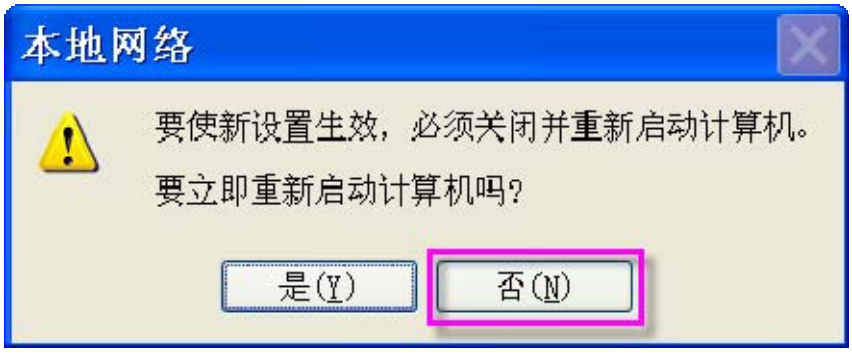


5. 在**驱动程序**页签，（1）在**类型**点右侧小箭头，选择**已停用**，（2）在**当前状态**点**停止**，（3）最后点**确定**：

6. 出现以下提示点**确定**，只要设置完成从启计算机后查看确实已停用即可：

7. 选**否（N）**。等最后一步设置完成后再从新启动计算机。

注意：如果是虚拟机内的手动设置部份，到这里已完成，可从新启动虚拟机。

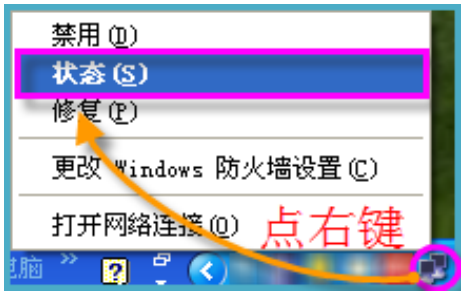


（返回虚拟机手动设置部份）

（4）本地连接网卡设置固定 IP

说明：NetBIOS 一般是给局域网用户提供消息通信及资源共享服务的。禁用后，一些局域网的功能可能不能正常使用，比如主机不能自动获取网络 IP，表现为网卡图标为搜索状态（  ），因此需要我们设置固定 IP。对拨号上网用户可以在本地连接网卡上设置任意 IP。对局域网用户（比如使用家用无线路由器的用户）需要设置固定的网段 IP，网关，DNS，否则用户不能正常上网，请按以下方法设置。

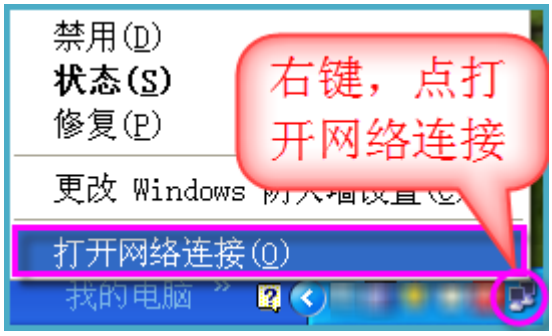
1. 先记录“原始状态”（**本地连接**现在的状态），以便下一步手动设置 IP。在电脑右下角**本地连接**图标点右键，点**状态**：



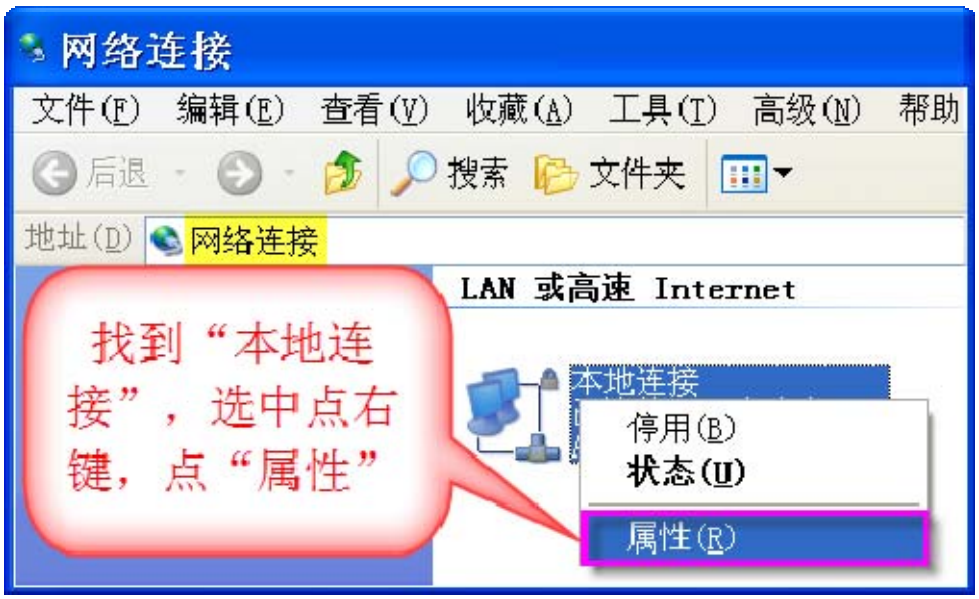
2. 在**支持**页签，点**详细信息**：

3. 记录以下高亮部份信息：

4. 然后到电脑右下角**本地连接**图标点右键，点**打开网络连接**：

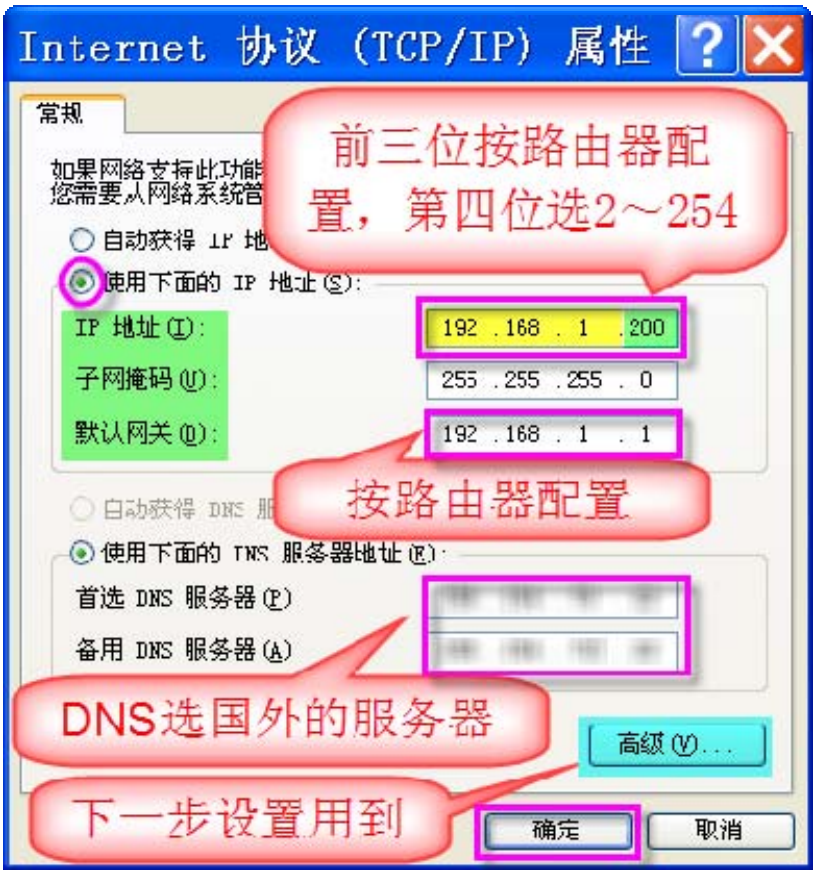


5. 选中**本地连接**，点右键，点**属性**：



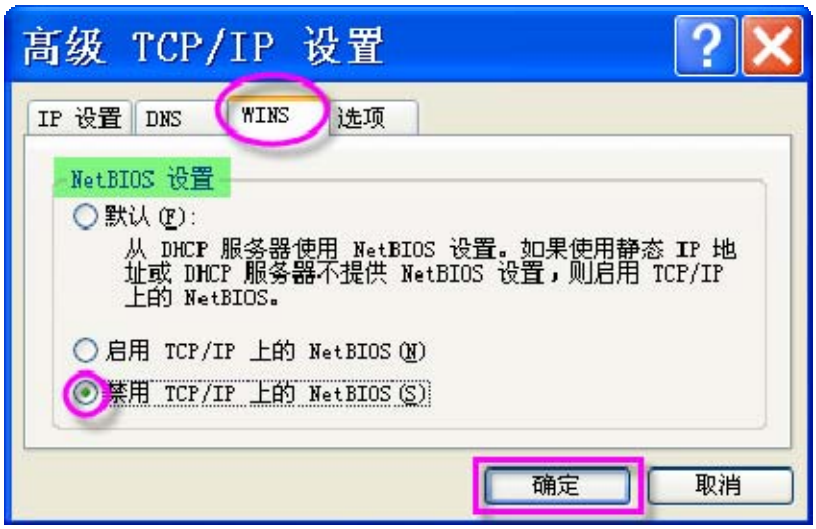
6. 在**常规**页签，选中 Internet 协议（TCP/IP），点**属性**：

7. 点选**使用下面的 IP 地址**；将刚才记录的“原始状态”，填写到对应的项目中。**IP 地址**可用“原始状态”记录的，也可前三位相同，最后一位在 2~254 中任选一位：**子网掩码**默认；**默认网关**如果使用路由器的话，一般是 192.168.0.1 或 192.168.1.1，具体请参考路由器说明书。**使用下面的 DNS 服务器地址**，这里无需选用国外 DNS 服务器，因可能影响速度，且 DNS 特殊可能成为特征，因此设置与**默认网关**一致即可；或按“原始记录”填写。

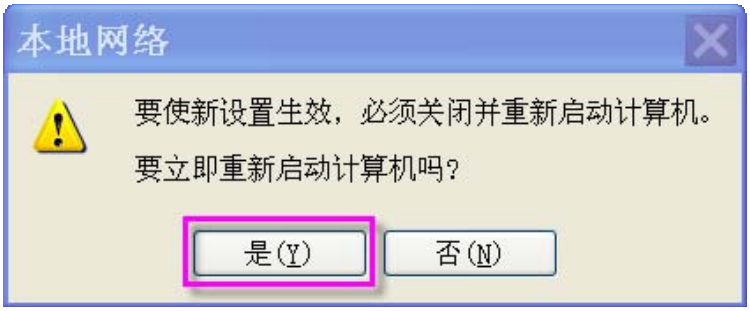


注意：这样设置以后，每次插上网线，网卡图标还会显示搜索状态；过几秒后拔下网线从新插上即可。之后如果还是长时间显示搜索状态，可右键点**禁用**后，再**启用**本地连接。如果插拔网线不方便，可不用理会，不影响上网。

8. 以下步骤不是必须的，但为了双重保险亦可手动设置：在以上图示中点**高级**，在 WINS 页签，NetBIOS **设置**点选成**禁用** TCP/IP **上的** NetBIOS(S)，点**确定**，再点**确定**，最后点**关闭**：



9. 如果出现以下提示，点**是（Y）**；如果没有出现提示，请自行从新启动计算机。以上四个手动设置就完成了。



（5）检查设置

说明：从新启动计算机后请查看是否设置成功。如果设置后主机或虚拟机没有做相应备份，主机恢复系统或虚拟机恢复快照后，要注意从新设置。

1. 在电脑右下角**本地连接**图标点右键，点**打开网络连接**；在**本地连接**点右键，点**属性**，在**常规**页签查看 **Microsoft 网络客户端**没有勾选，没有 **Microsoft 网络的文件和打印机共享**即可，点**取消**：

2. 在**我的电脑**点右键，点**管理**，找到**设备管理器**点右键 → **查看** → **显示隐藏的设备**，在**非即插即用驱动程序**，找到 **NetBios over Tcpip**，左侧有 X 说明已禁用：

（返回虚拟机手动设置）

（三）主机破网软件的设置

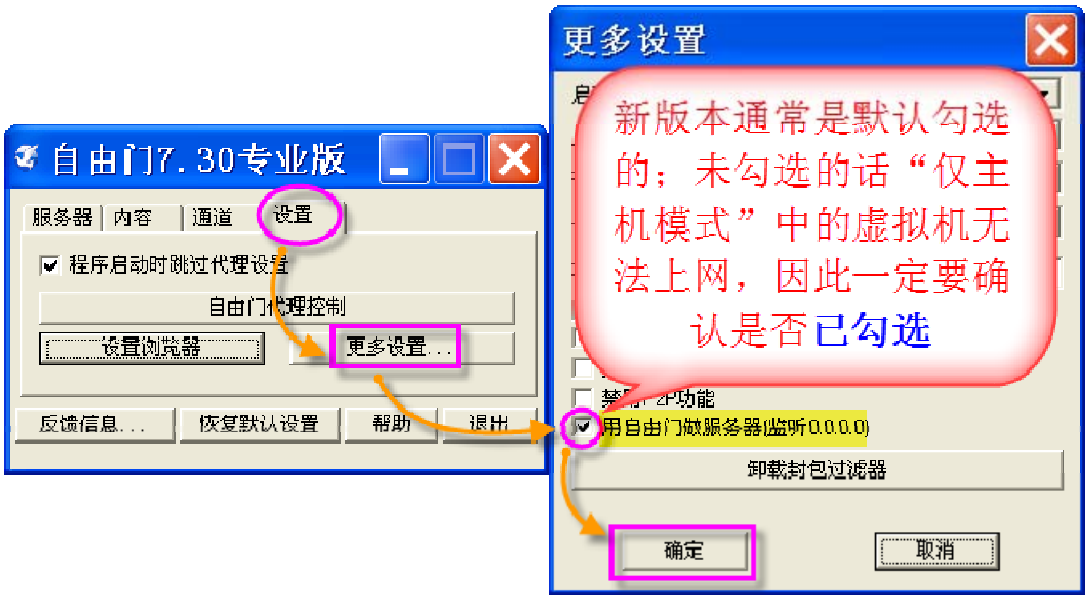
主要的破网软件有：**自由门/逍遥游/无界/TorManager2.7** 等。

➢ 自由门/逍遥游

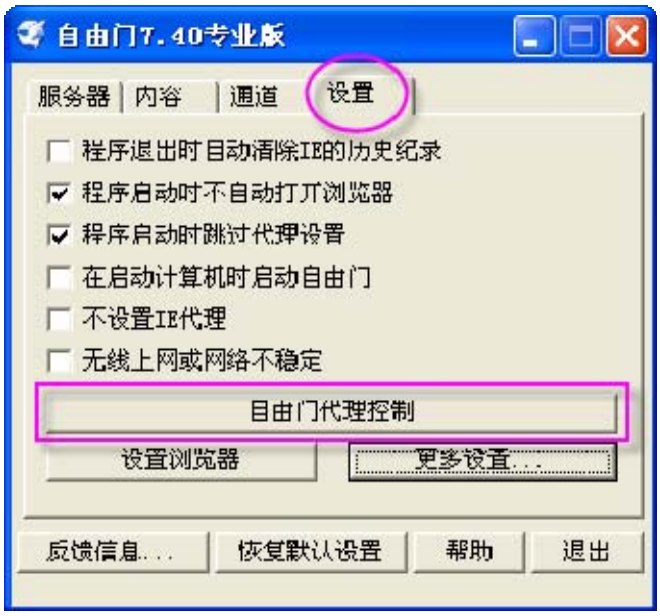
侦听 IP：0.0.0.0　　**端口**：8580/8581

1. **侦听区域设置**：自由门/逍遥游的设置方法相似。在**设置** → **更多设置** → 勾选**用自由门（逍遥游）做服务器（监听 0.0.0.0）** → **确定**。

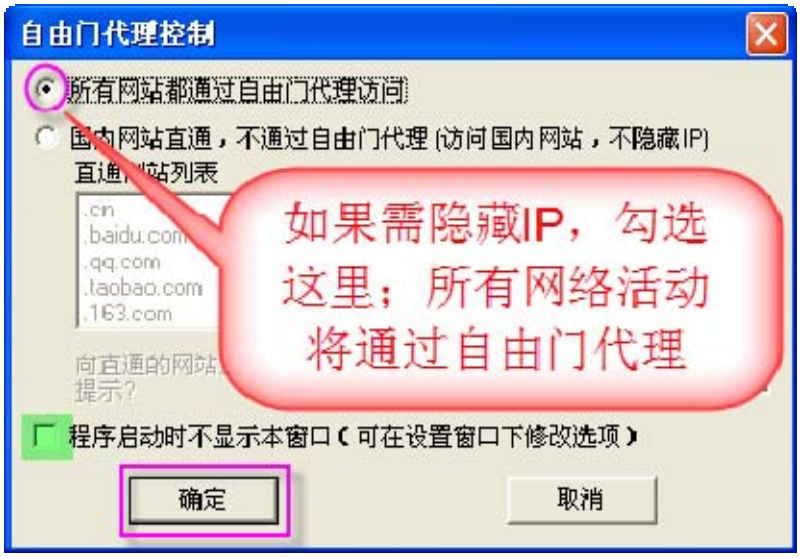
重要提示：如果这里没有设置**监听 0.0.0.0**，虚拟机无法上网。



2. 提示：以下设置涉及安全问题，请一定要确认设置正确。在初次使用自由门时会弹出设置，或在**设置－自由门代理控制**（如果**逍遥游代理控制**可用，设置方法相同）：



3. 勾选**所有网站都通过自由门代理访问。重要提示**：如果勾选了**国内网站直通，不通过自由门代理（访问国内网站，不隐藏 IP）**的功能后，登陆**直通网站列表**中的网站时是以真实 IP 登陆的；为了不出现暴露真实 IP 的情况，启动自由门后要在**自由门代理控制**的设置中勾选**所有网站都通过自由门代理访问**；为了避免无意中使用了“国内网站直通”功能，不要勾选下方的**程序启动时不显示本窗口**，这样每次上网前确认一下。最后点**确定**。

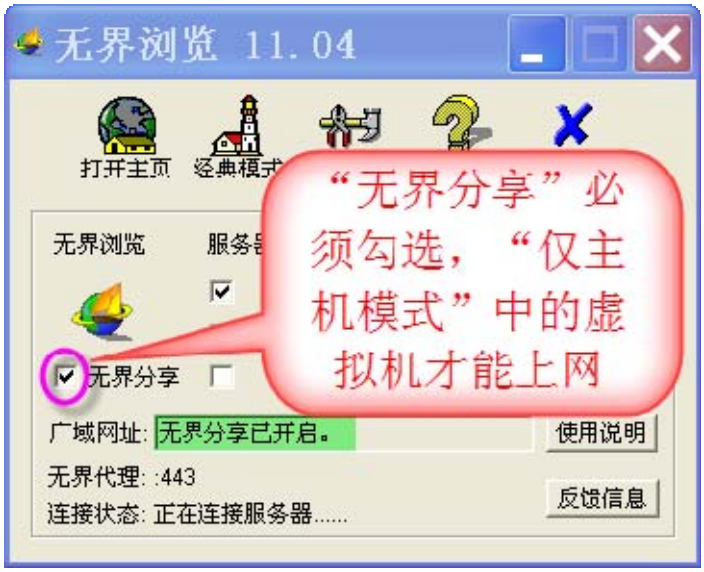


4. 那么在整机隔离方案下如何短时间上普通网站、或运行非安全软件呢？请参考：附加功能：不隐藏IP登陆国内网站

➢ 无界浏览

侦听 IP：0.0.0.0　　**端口**：443

设置方法：勾选**无界分享**（只有高版本才有此功能，请选择 11.03 以上版本），无界代理变成以 **443** 为端口的代理；此时可以侦听 0.0.0.0：
注意：端口 9666 只能代理本地（主机浏览器与软件等）上网，无法代理本方案中的虚拟机上网；因此必须按以上方法设置后才有效。



➢ TorManager2.7

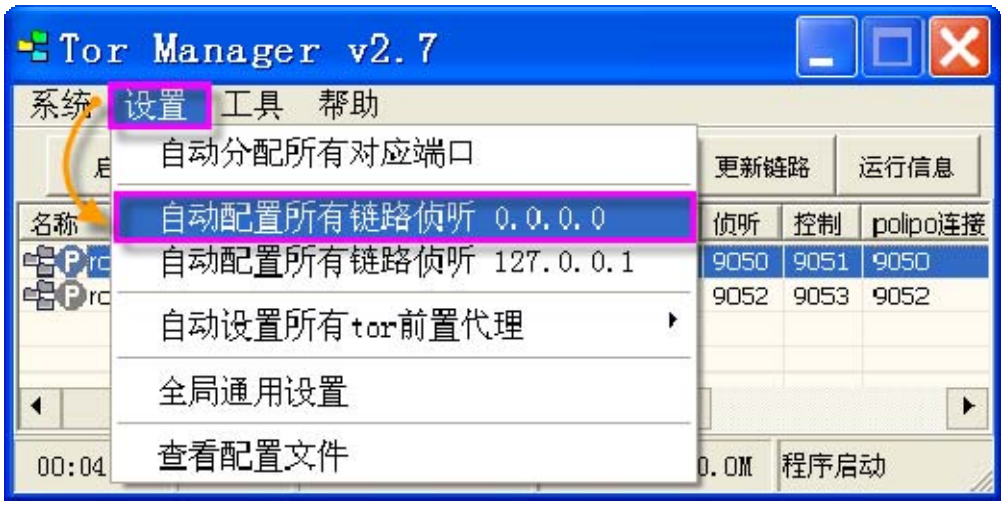
侦听 IP：0.0.0.0（或 Host-only 网卡 IP）　两类端口：**http(https)**：8118；　**Socks5**：　9050

注意：使用 TorManager2.7 时，为防止 Tor 的一些恶意节点，必须使用自由门、无界浏览做前置代理；只有在自由门、无界浏览失效的情况下，可以用普通的代理作为 TorManager2.7 前置代理，但只能用于临时的翻墙、访问海外网站，不能用于重要工作。

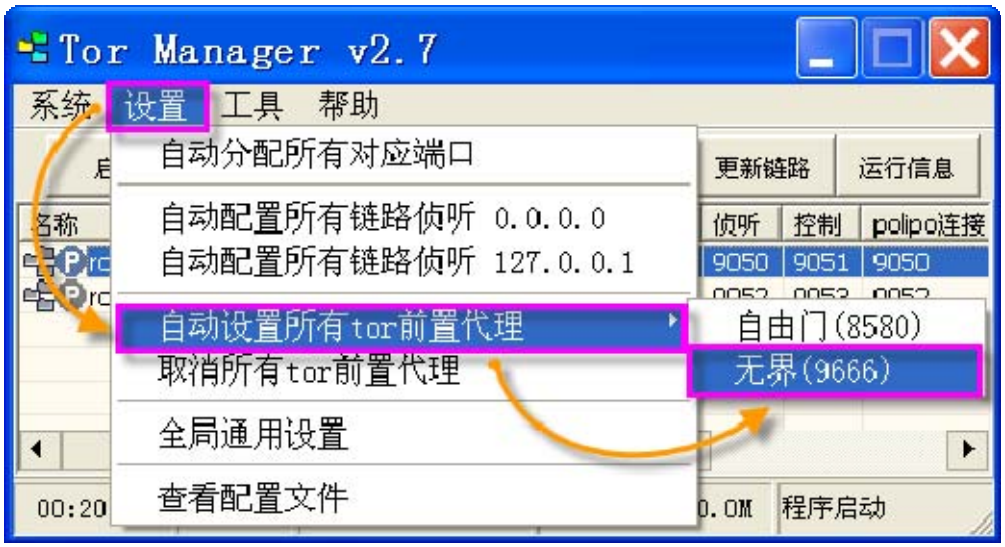
说明：自由门/无界浏览当用于 Tor 的前置代理时：自由门不要设置“侦听 0.0.0.0”；无界不要勾选“无界分享”，此时无界浏览的端口是 9666 而不是 443。

Tor 与其它破网软件不同之处是可以变换出口的 IP，可访问国内网站。

1. **步骤**：启动 tormanager.exe 后，在**设置**选**自动配置所有链路侦听 0.0.0.0**：



2. 在**设置**，选**自动设置所有 Tor 前置代理**，根据实际选用的破网软件选择**自由门（8580）**或**无界（9666）**；



3. 以上两项也可以通过双击链路按图示手动设置，这样只设置了一条链路。其中的**侦听 9050**(socks5) 为 tor 侦听的端口，**侦听端口** 8118（http/https）为 polipo 侦听的端口，这些都是默认设置好的无需改动；以下内容需设置：

（1） 在**代理**点击右侧小箭头选择不同的前置代理：有三个选项，根据使用的破网软件的对应端口选择；亦可手动修改（比如运行**动网通**，把动网通上显示的**代理服务器**及**端口**用相同形式填写到这里 xx.xx.xx.xx:yyyy）；

（2） 两个**侦听区域**均选择 Host-only 网卡 IP；（如果 Tor 同时代理本地网络与虚拟机，两处均改成 0.0.0.0）

（3） **客户端 IP 段**填写虚拟机本地连接网卡的 IP。图示目前的设置显示 Tor 只侦听 Host-only 网卡 IP，不代理主机本地网络；如果同时代理主机本地网络，可加上 127.0.0.1 并用半角逗号,隔开，如：192.168.188.2,127.0.0.1：

说明：本地侦听 0.0.0.0 启用，如果被防火墙禁止，需对防火墙進行确认，允许侦听端口。如果虚拟机上的程序不能连接到网络，请检查是否这个原因造成的。

（四）主机防火墙设置

A. 主机 IPSEC（必设置）

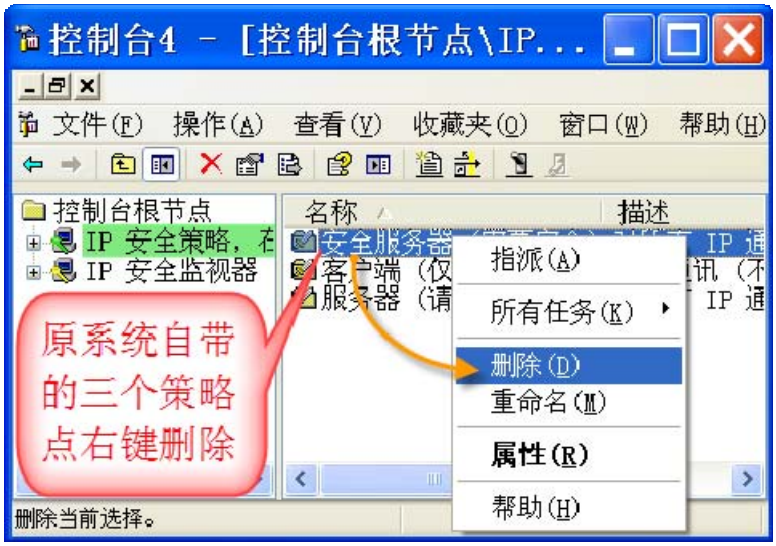
说明：导入“IPSEC_ZHUJI_X.ipsec”；导入的策略是按本教程默认 IP 设置的，通常无需修改，如需更改请参考教程《FHQ_X. doc》；以上 X 指不同的版本，用从本站下载的同名最新版本即可。

导入方法一：WINXP/WIN7 系统**开始 → 设置 → 控制面板 → 管理工具 → 本地安全策略 → IP 安全策略、在本地计算机**；

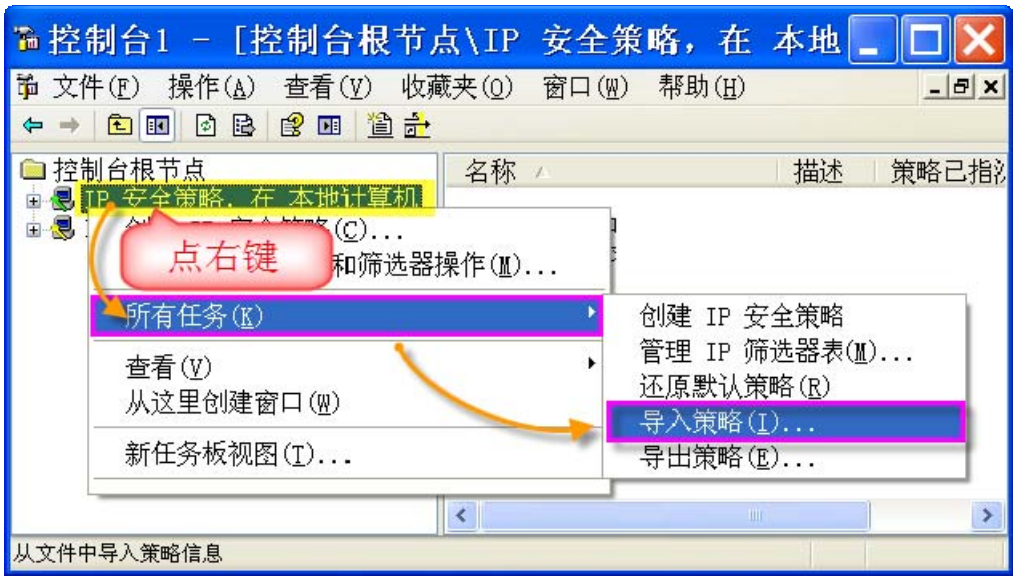
导入方法二：WINXP/WIN7 系统**开始 → 运行**输入“secpol.msc”点**确定**，在 **IP 安全策略、在本地计算机**；

导入方法三：建立**控制台**，详细请参考《防火墙设置方法》（FHQ_X.doc）。
（返回开启文件与打印机共享的IPSEC设置）

1. 删除系统自带的三个策略，这是为了后续删除一些无关的规则（避免无意中使用错误规则带来隐患）。如果系统中没有自带策略则无需删除：



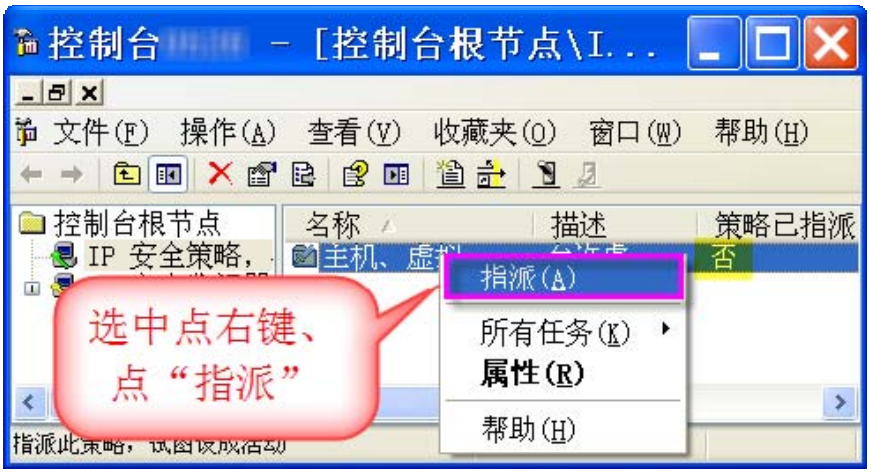
2. 在 **IP 安全策略、在本地计算机**点右键 → **所有任务** → **导入策略**：



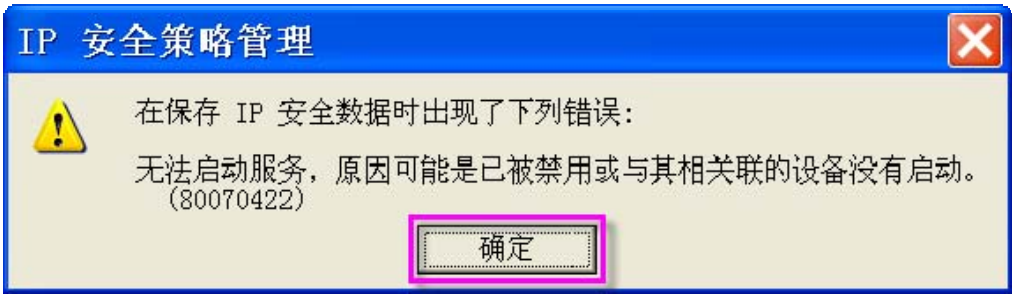
3. 找到最新下载的 IPSEC_ZHUJI_X.ipsec，点**打开**；X 代表不同的更新版本，只要下载本站最新附件即可：

➢ 指派主机策略

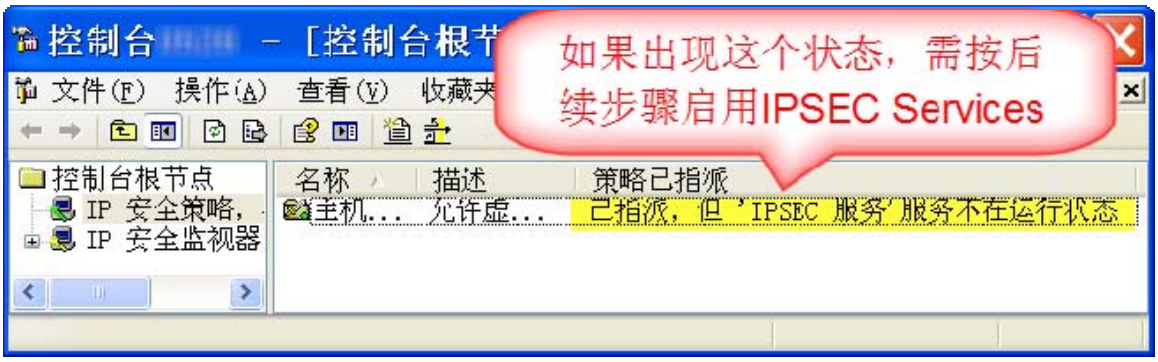
1. 选中导入的策略，点右键、点**指派**：



2. 错误提示，点**确定**：

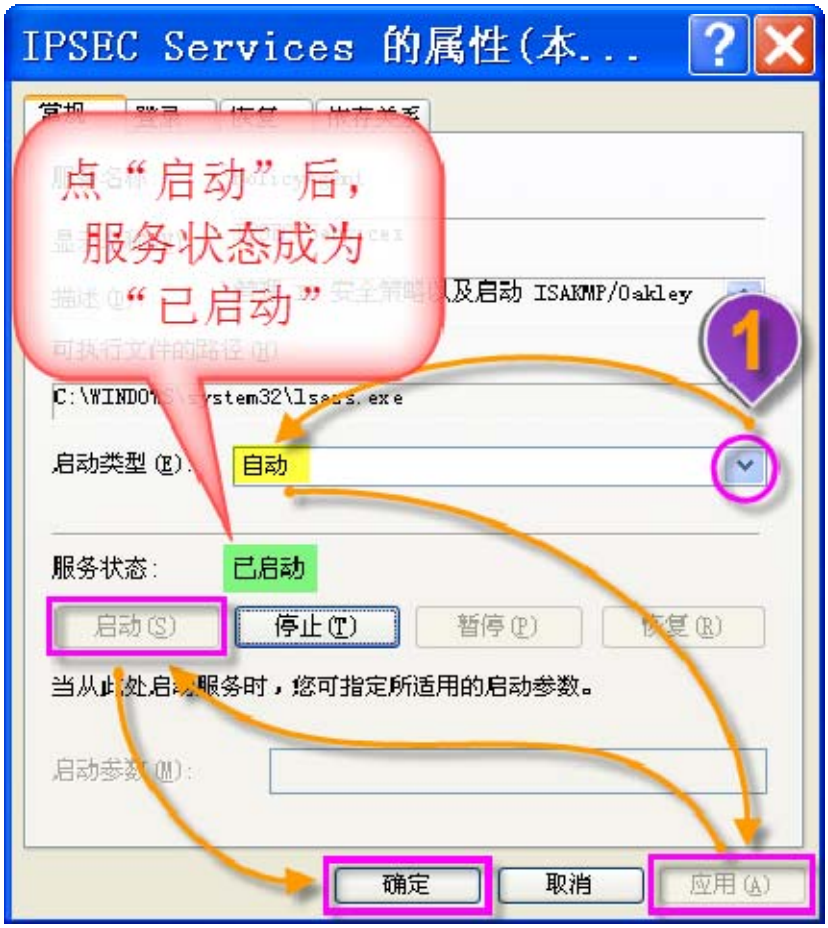


3. 如果出现以上提示，**策略已指派**的状态如下，请按后续方法解决：

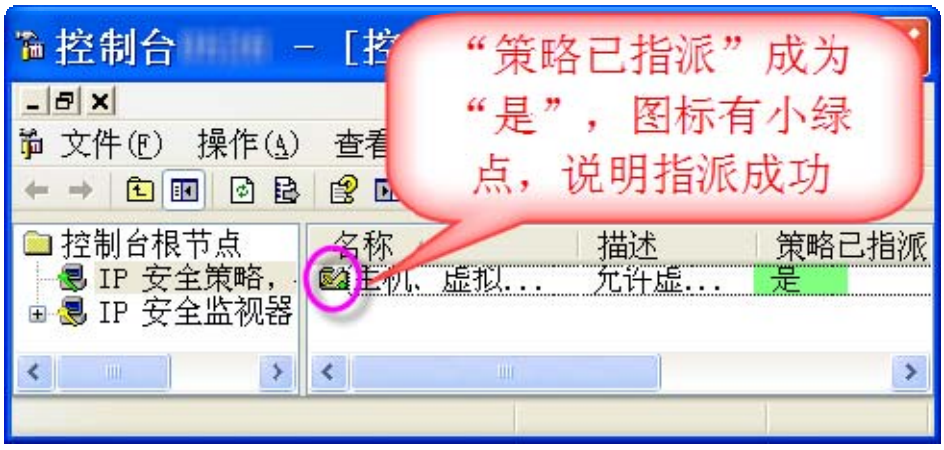


4. 在**我的电脑**点右键 → **管理** → **服务**，开启 **IPSEC Services**：

5. 在图示 **1** 的小箭头找到**自动**，然后按图示顺序点**应用** → **启动** → **确定**：



6. 正常后**策略已指派**会显示**是**，图标有绿色小点：



（返回导入方法一）（返回导入方法二）（返回虚拟机IPSEC）

➢ 开启文件与打印机共享的 IPSEC 设置

注意：如果开启文件与打印机共享，需按以下方法修改IPSEC。按导入方法一或二的路径，双击**xuniji-hostonly安全**，将导入规则中zuzhi-netbios去除勾选（不起作用），点**应用**后，点**确定**：

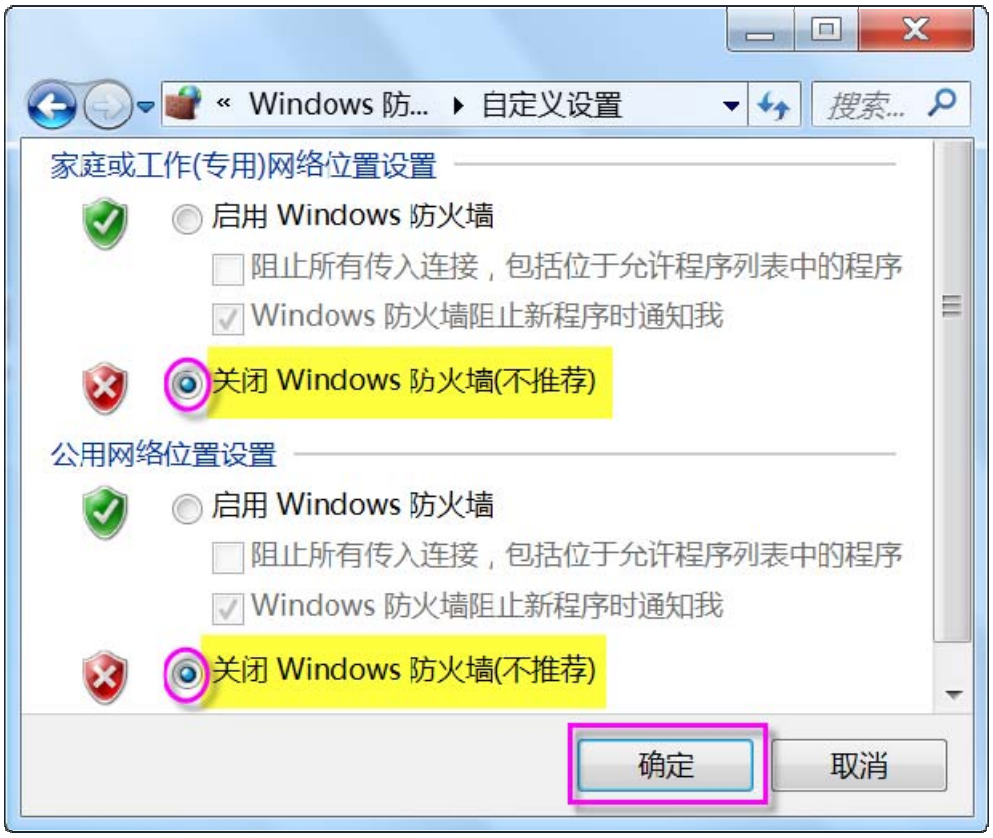
（返回手动设置部份）（返回导入方法一）（返回导入方法二）（返回虚拟机IPSEC）

B. WIN7 自带防火墙（建议禁用）

临时没有第三方防火墙，可参考WIN7 防火墙.bat的方法制作，在主机中双击运行。WIN7 自带防火墙规则在注册表中，不便于删除涉及敏感信息的条目，而整体删除规则又会清零从新配置。因此建议禁用。

1. 禁用方法：在 WIN7 开始 → 控制面板 → 系统和安全 → Windows 防火墙，点击打开或关闭 Windows 防火墙：

2. 点选两个**关闭 Windows 防火墙**，点**确定**：



（返回虚拟机第三方防火墙）

C. 第三方防火墙的设置（必选 ZA 或 COMODO 之一）

说明：1. WIN7 可选用 ZoneAlarm 9.3.014，导入规则依然使用 ZA8_ZHUJI_X.xml；论坛推荐版本 Comodo 3.14 不适用于 WIN7 64 位，但可用于 WIN7 32 位。

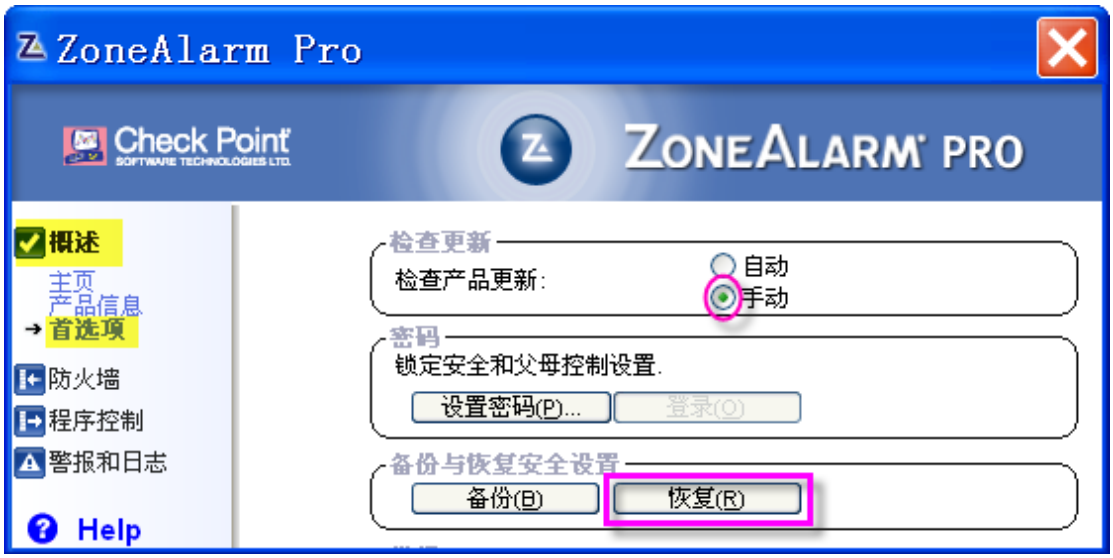
2. 防火墙出现的提示尽量不要选择“记忆”，这样不留有敏感信息，同时可以查看每一步骤是否正常运作，即下一次不弹出提示，说明某一部份设置有问题。比如代理设置有问题时，浏览器上网防火墙不会提示要通过代理上网，这时就可以去查看相应部份。

➢ ZoneAlarm的设置（如果是COMODO请看后续部份）

说明：请将 ZA8_ZHUJI_X.xml 按以下图示导入；如需修改请参考《FHQ_X.doc》（防火墙设置方法）；以上 X 指不同的版本，用从本站下载的同名最新版本即可。

A. 导入设置

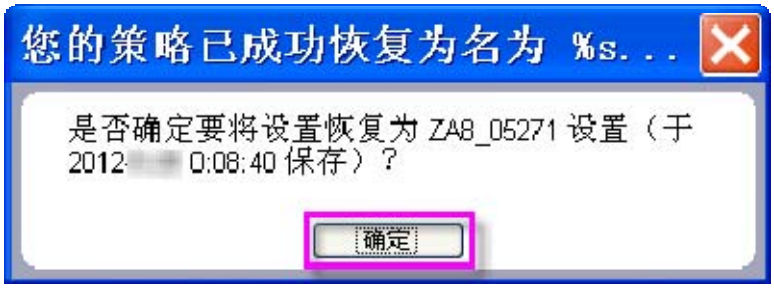
1. 在**概述 → 首选项**，先将**检查产品更新**改为**手动**，然后点**恢复**：



2. 找到下载的文件，点**打开**：

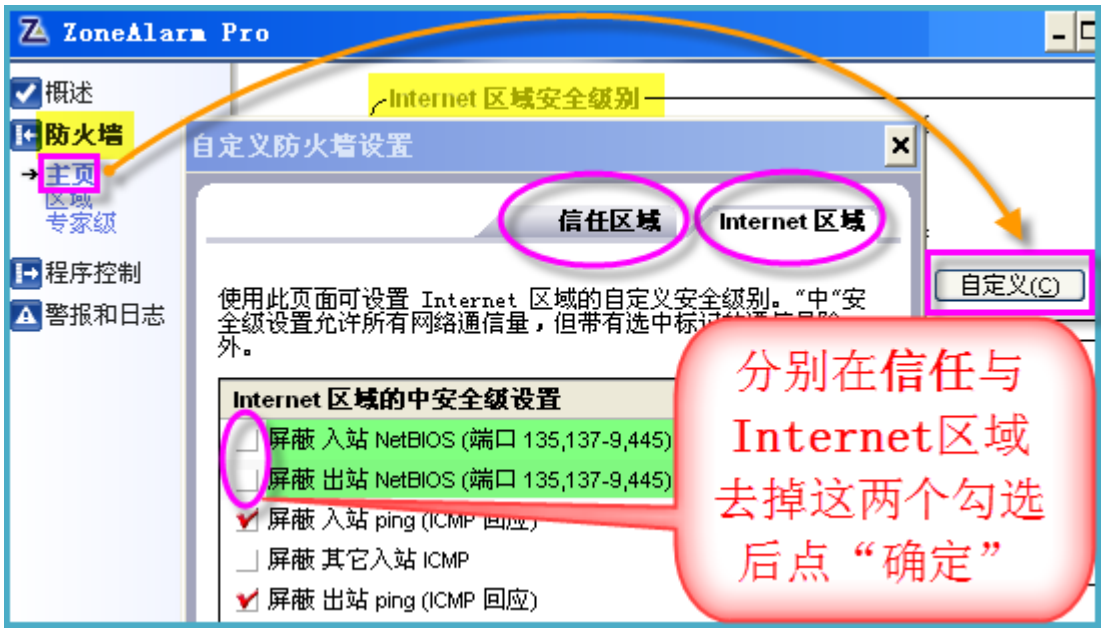
3. 点**确定**：

4. 点**确定**。**注意：**导入后第一时间**设置密码**，以保证规则不被任意修改；在**概述 → 首选项 → 设置密码**设定。详细请参考《FHQ_X.doc》相关说明。



（返回虚拟机第三方防火墙的设置）

5. 如果主机开启**文件与打印机共享**，需在 ZA **防火墙** → **主页** → **自定义** → 在**信任区域**与 **Internet 区域**分别去除图示两个勾选后点**确定**：



（返回手动设置部份）

➢ 第三方防火墙Comodo的设置（如果是ZA请看前面部份）

说明：请将 COMODO314_ZHUJI_X 按以下图示导入；如需更改请参考教程《FHQ_X.doc》；以上 X 指不同的版本，用从本站下载的同名最新版本即可。

A. 导入并激活设置

1. 在**其它**，点**管理我的配置**：

2. 点**导入**：

3. 找到下载的 COMODO314_ZHUJI_X（X 代表不同的版本，只要下载本站的同名附件即可），点**打开**：

4. 导入时会自动带入名称，也可自行修改，点**确定**：

5. 导入成功提示：

6. **关键步骤：一定要激活才起作用**：选中导入的配置名称，点**激活**，出现提示点**确定**：

7. 激活后该配置右侧有“**活动**”标识，点**关闭**：

8. **注意**：导入后第一时间添加密码，以保证规则不被任意查看与修改。详细请参考《FHQ_X.doc》相关说明。

（返回虚拟机第三方防火墙的设置）

B. 开启文件与打印机共享的 COMODO 设置（注意开启共享有风险）

1. **安全提示：为了安全，一般用户不要开启文件与打印机共享。**如需共享需去除导入规则已禁用的 System。打开 Comodo 后，在**防火墙 → 高级设置 → 网络安全规则**：

2. 在**应用程序规则**页签，选中 System，点**移除**，点**确定**：

（返回主机手动设置部份）

二、在虚拟机中的设置

（一）VirtualBox 和 VMware 虚拟机里设置方法相同

说明：虚拟机内网卡设置为固定IP，DNS为空，网关为空，同时虚拟机上禁用NetBios、Server、Remote Registr和Task Scheduler服务；可以通过“设置.bat”脚本与手动设置完成。

A. 运行“设置.bat”

- 虚拟机系统为WINXP，直接在虚拟机里运行设置.bat即可。

- 虚拟机系统为WIN7，请选中设置.bat，点右键选择以管理员身份运行；如果运行后界面一晃而过，需要将设置.bat拷贝到本地C盘下，再次按以上方法运行。

- 无论主机是 WINXP 或 WIN7，虚拟机使用 WINXP 或 WIN7 均可，无对应关系。如果没有特别的用途，建议虚拟机使用 WINXP，减少激活等不便之处。

- 虚拟机中 WINXP/WIN7 升级方法：由于虚拟机只能通过代理上网，为了减少代理流量，可以使用禁书网提供的批量更新的办法升级系统。即先按论坛提供的微软下载地址，在纯净主机上下载后，再到虚拟机用安装工具安装。相关链接如下：

◇ **微软XP,Office2003 中文版升级补丁和自动安装**

◇ **Win7_x86_x64 系统补丁、自动安装工具（9.23，加入IE9 累计安全更新）**

- 虚拟机中 Avira 小红伞可离线升级。可先下载离线升级包**下载工具 Avira Fusebundle Generator**（地址如下，英文版，无中文版），解压缩后运行 fusebundle.exe 会自动下载病毒库，当 Dos 窗口最左侧成为 100%后窗口自动消失，这时 install 文件夹中会出现 vdf_fusebundle.zip（病毒库，中英文版本通用），之后打开 Avira 小红伞到**更新－手动更新**，选中 install 文件夹中的 vdf_fusebundle.zip 即可实现离线更新病毒库。**注意**：如果更新时间与最新病毒库定义有时间差，**上次更新**处还是有叹号！，这没有关系。

http://www.avira.com/zh-cn/download?product=avira-fusebundle-generator

- 运行**设置.bat**后，请参考浅兰色字体说明；以下为设置过程：

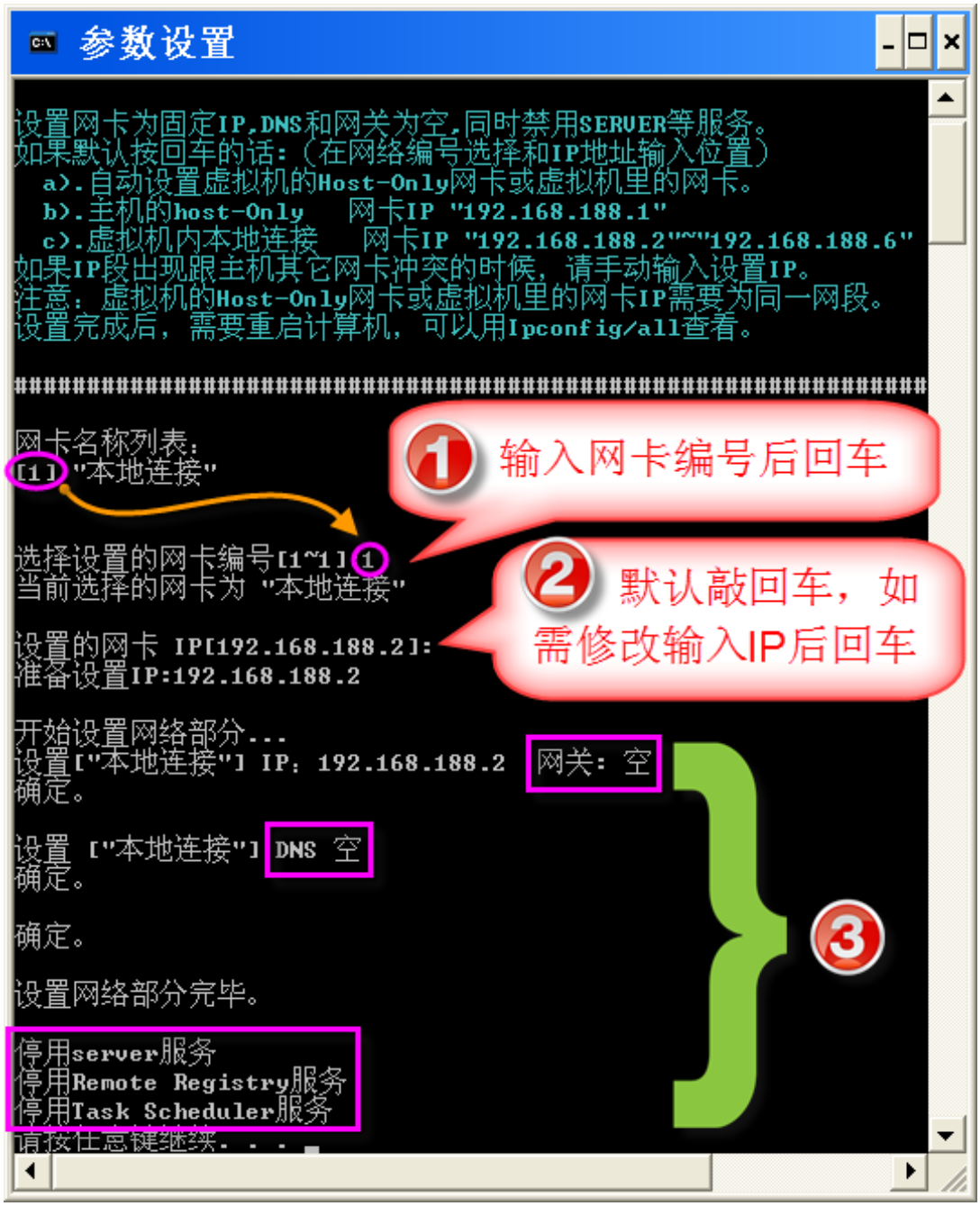
（1） 输入网卡编号后回车；

（2） 使用默认 IP 则直接回车（一般无需修改），或输入希望设置的 IP 后回车。

注意：如果使用的不是教程示例 IP，请相应修改防火墙的内容，否则将无法上网。

（3） 回车后设置将自动完成：IP 设置、网关空、DNS 空、停用 Server、Remote Registry 以及 Task Scheduler 服务等，最后按任意键退出。

（4） 注意：从启虚拟机后生效。



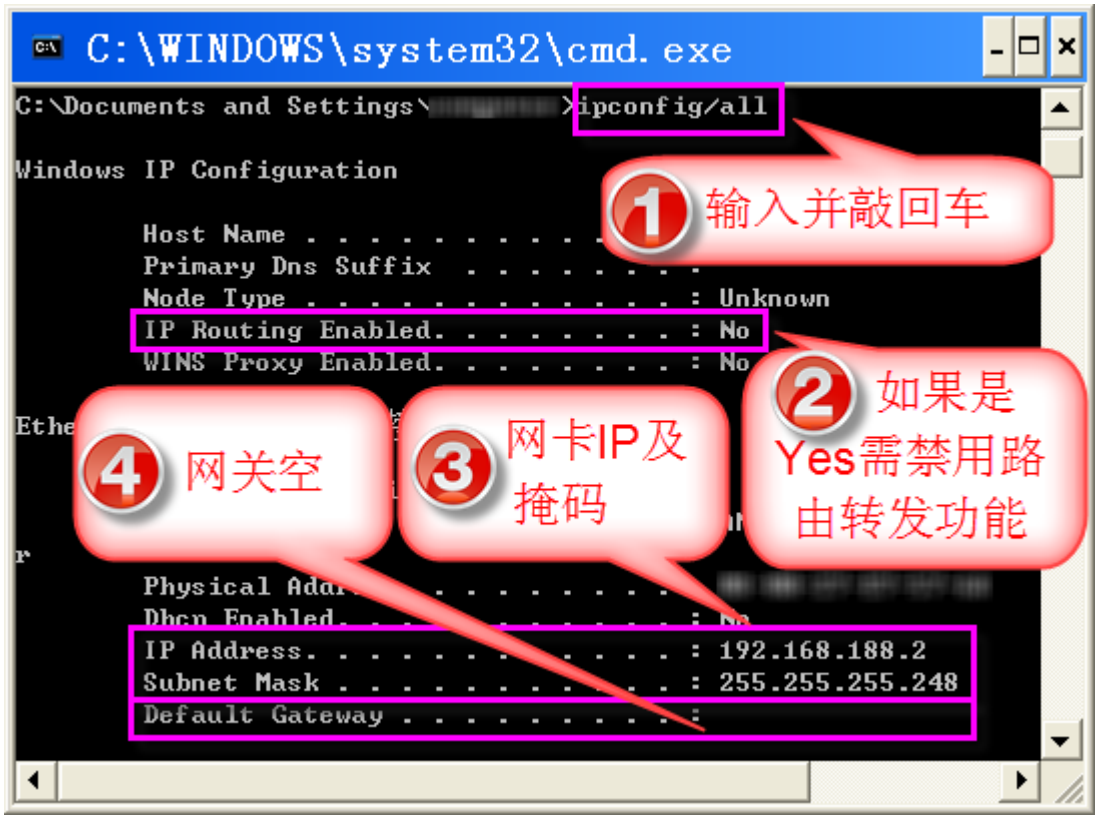
1. **检测方法**：虚拟机从启后，在虚拟系统的**开始** → **运行**中输入 **cmd**；在出现的 DOS 窗口中：

（1） 输入 **ipconfig/all**，敲回车；

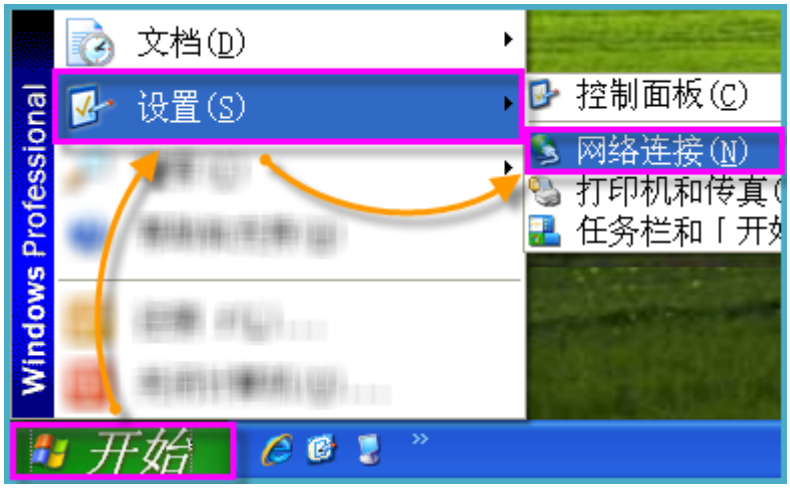
（2） IP Routing Enabled正常显示是No，如果是Yes请参考附录《IP Routing Enabled 启用原因和停止方法》，最后检测是No即可；

（3） 核查网卡 IP 与掩码是否正确：192.168.188.2/255.255.255.248。

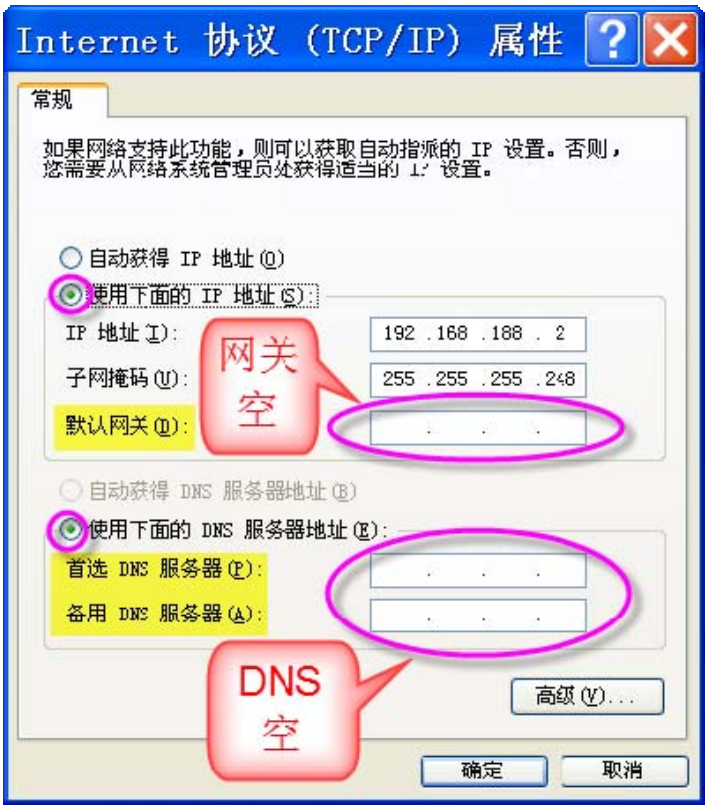
（4） Default Gateway 右侧是空，说明网关为空：



2. 其中的网关，DNS 部分也可按以下方法查看。在虚拟系统的**开始 → 设置 → 网络连接**：



3. 虚拟机中**本地连接**点右键 → **属性** → **常规** → **Internet 协议(TCP/IP)** → **属性**，按以下图示查看：



B. 虚拟机手动设置部份

1. 请按主机手动设置部份的方法设置，完成前三个设置即可，无需第四个固定IP的设置（虚拟机中**设置.bat**已完成这一步）。
2. 从新启动虚拟机后检查设置（方法同主机）。

（二） 虚拟机里上网程序的设置

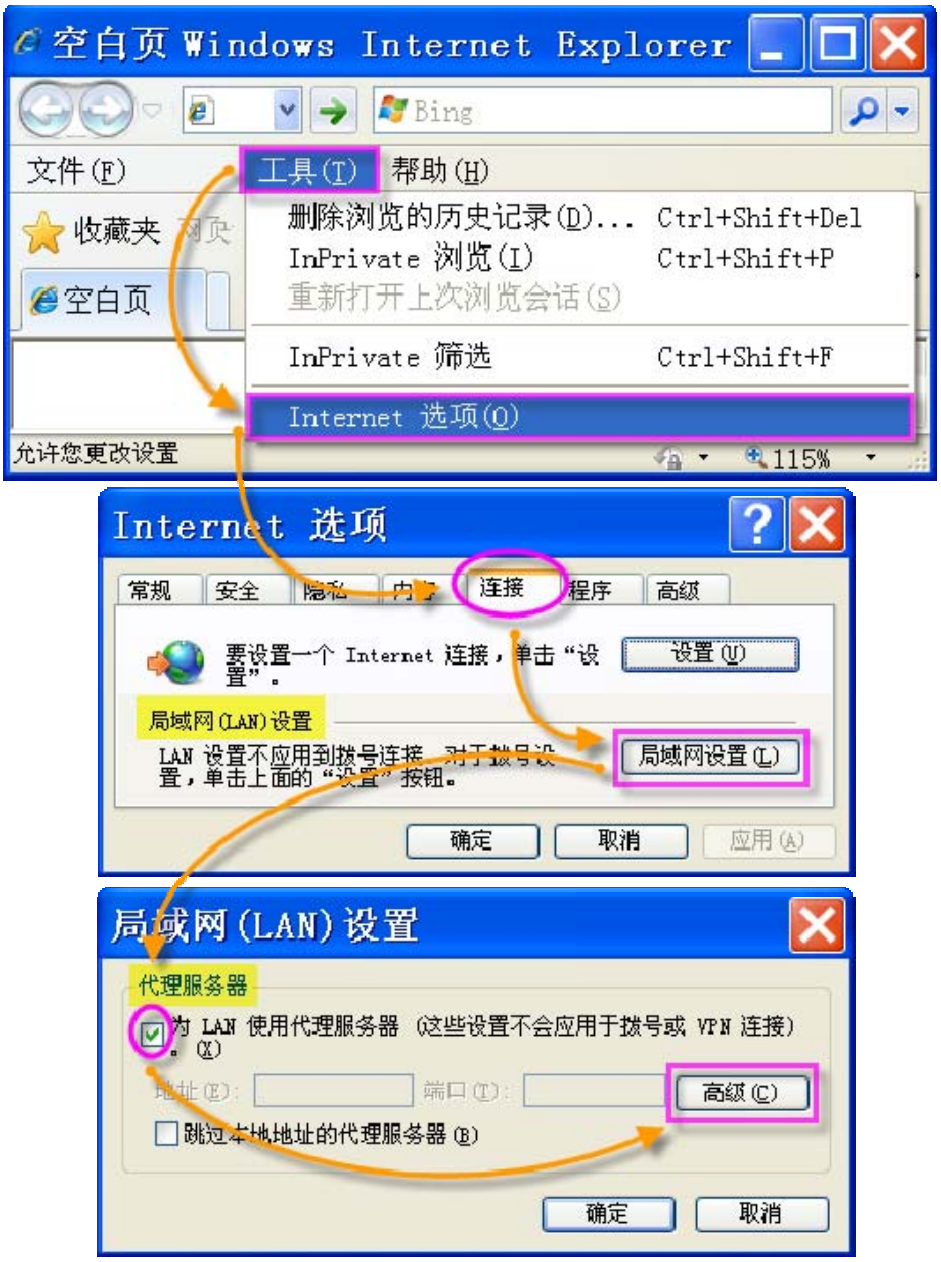
设置时只要上网程序的 IP 为仅主机（Host-Only）网卡的 IP，代理端口为主机破网软件的侦听端口即可。本教程以比较常用的 IE 浏览器和 Firefox（火狐）为例，介绍设置方法。

不同破网软件相对应的代理 IP 与端口参考设置：

VirtualBox/VMware 虚拟机内	指向主机上的 Host-Only 网卡 IP： 示例：192.168.188.1	**自由门/逍遥游端口：**8580/8581
		无界分享端口：443
		Tormanager2.7： http(s)端口： 8118/8119/8120/8121/8122 Sock5 端口： 9050/9052/9054/9056/9058

➢ IE 浏览器

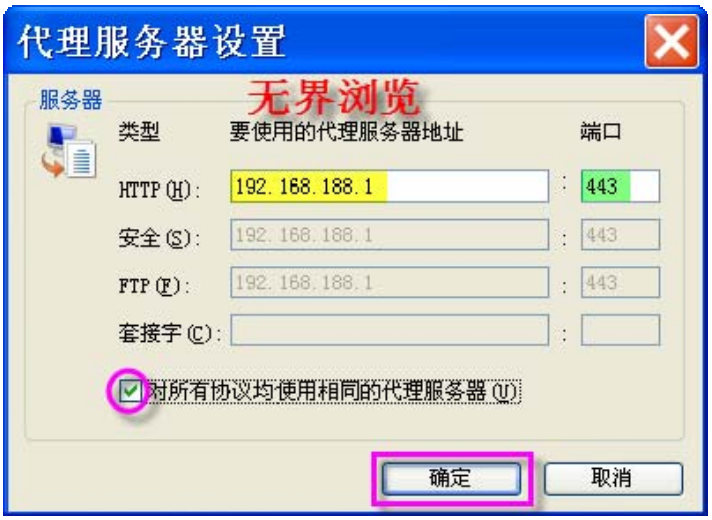
1. **IE → 工具 → Internet 选项 → 连接**页签 **→ 局域网设置 → 代理服务器**下勾选**为 LAN 使用代理服务器 → 高级：**

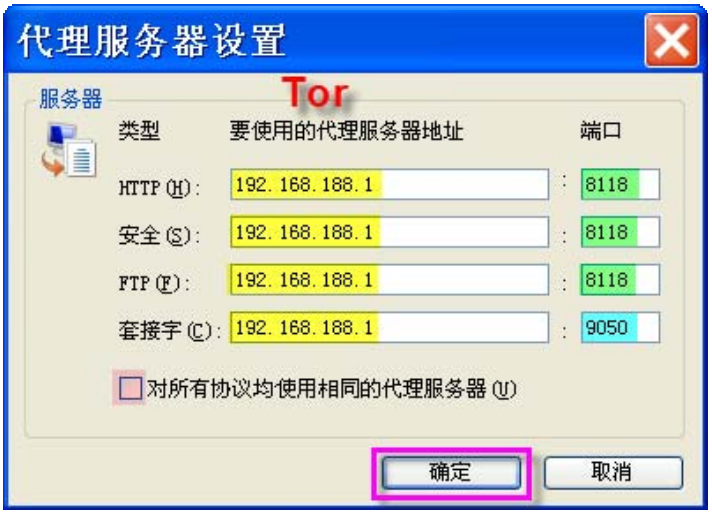


2. 由上继续，点**高级**后几种常见的设置方法：根据不同类型代理服务器（主机启用的不同的破网软件，如自由门/逍遥游/无界/Tor 等）设置。

以主机的虚拟网卡（Host-Only）IP 是 192.168.188.1 为例；如果端口相同可勾选**“对所有协议均使用相同的代理服务器”，**否则不要勾选：

破网软件	Host-only 网卡 IP	端口
自由门/逍遥游	192.168.188.1	8580/8581
无界分享	192.168.188.1	443
Tormanager2.7	192.168.188.1	http(s)：8118/8119/8120/8121/8122
		Socks：9050/9052/9054/9056/9058





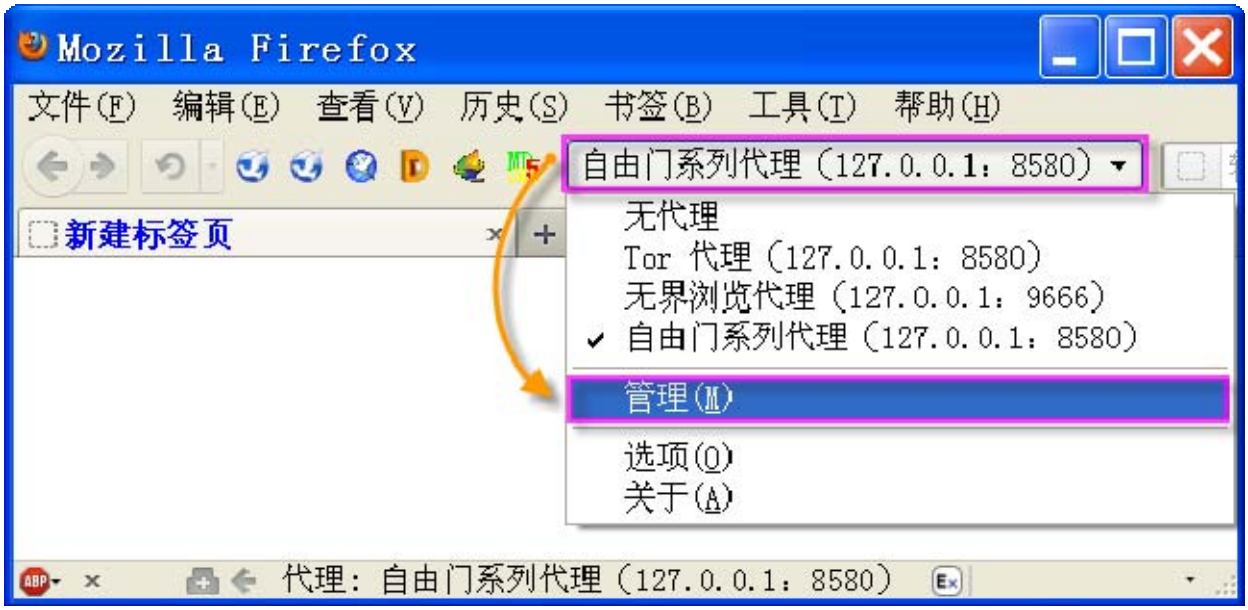
注：以上图示中标识“套接字”的在有些 IE 版本中标识为“Socks”，两者的设置方法相同的。

➢ Firefox(火狐)

以 FirefoxPortableESR10.0.4_G 为例：

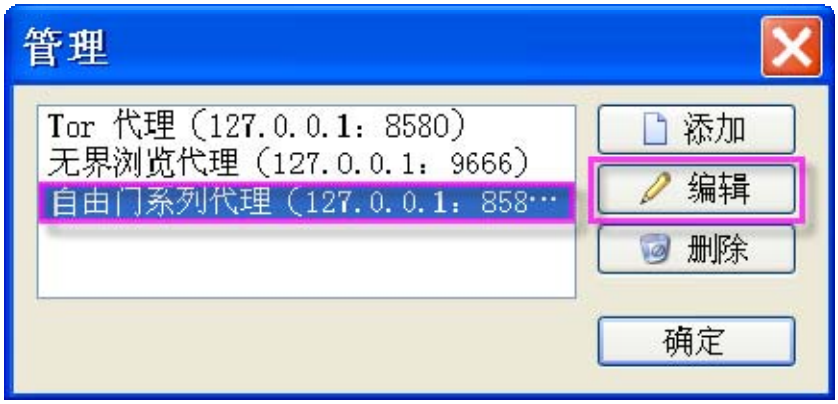
下载地址：火狐(Firefox)浏览器绿色中文便携版及使用图解

1. 因虚拟机浏览器的代理 IP 要用主机虚拟网卡 Host-only 的 IP，因此原程序自带的代理服务器设置不能直接用，需从新设置。点击**自由门系列代理**，选择**管理**：

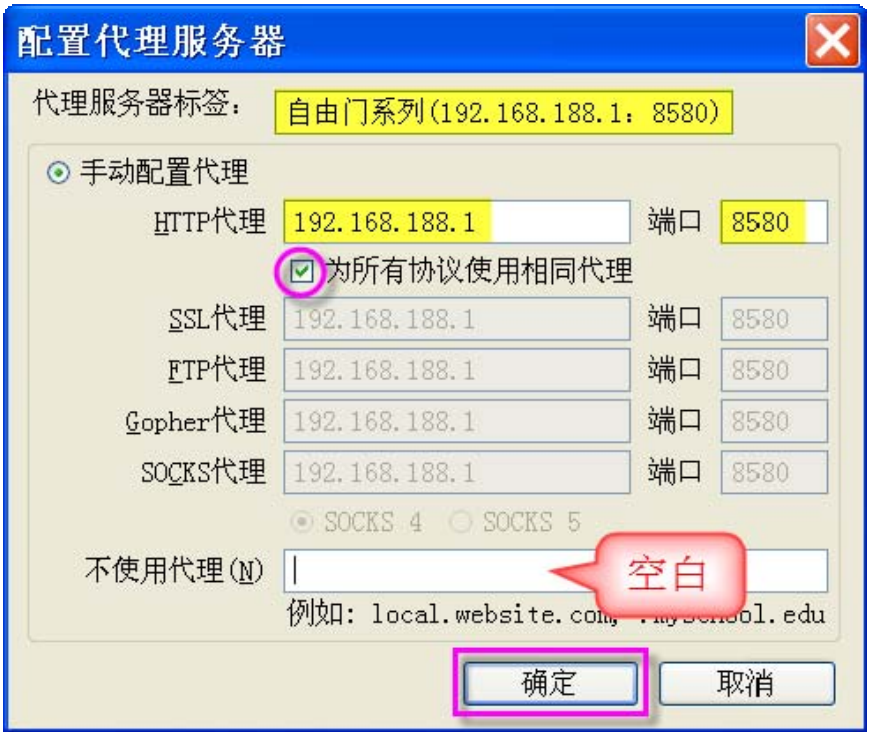


2. 顺序选中以下三个代理，点**编辑**：

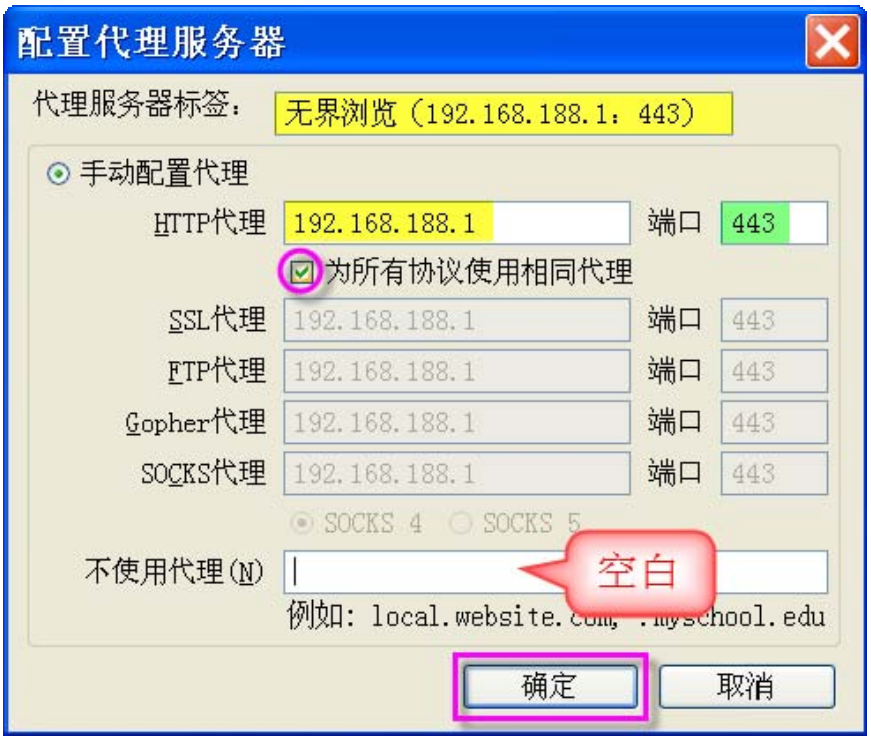
说明：完全建立新的代理，可点**添加**；再按以下方法添加新的代理设置，只是以下方法中需更改的部份，要从新填写：



3. **自由门系列代理（127.0.0.1：8580）**：更改**代理服务器标签**，把括号中的 IP 改成目前所用的 Host-only 网卡 IP，注意冒号要用全角；才能保存；**HTTP 代理**输入 Host-only 网卡 IP（192.168.188.1）；**端口**输入自由门/逍遥游端口 8580（个别时候会是 8581）；勾选**为所有协议使用相同代理**；**不使用代理**处清空；点**确定**：

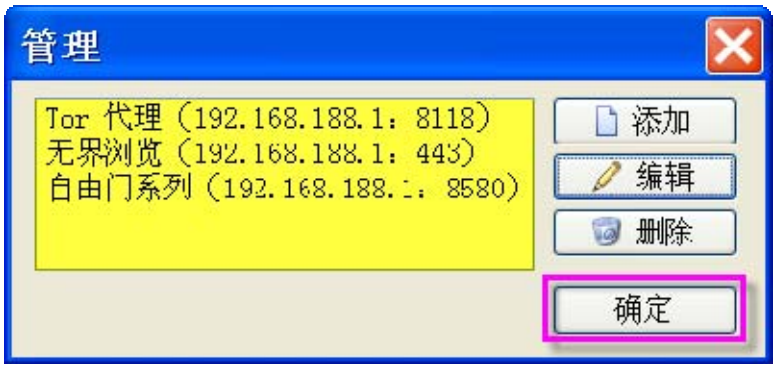


4. **无界浏览代理（127.0.0.1：9666）**：更改**代理服务器标签**，把括号中的 IP 改成 Host-only 网卡 IP；**HTTP 代理**输入目前所用的 Host-only 网卡 IP（192.168.188. 1）；**端口**输入无界分享端口 443；勾选**为所有协议使用相同代理**；**不使用代理**处清空；点**确定**：



5. **Tor 代理（127.0.0.1：8580）**：因为 Tor 可以有许多链路，不同的链路需设立不同的代理，以下可更改 Tor 为 Tor0，更多 Tor 代理设置方法类似。所有代理均设置目前所用的 Host-only 网卡 IP（192.168.188.1）；不勾选**为所有协议使用相同代理**；前四项**端口**设置 Tor 的 polipo 侦听端口 8118（建立更多 Tor 代理顺排 8119/8120/8121/8122）；**Socks 端口** 9050（建立更多 Tor 代理顺排 9052/9054/9056/9058）；勾选 **Socks5**，**不使用代理**处清空；点**确定**：

6. 设置完成后如图，点**确定**：



7. 使用哪个破网软件，就选择对应的代理；启用后在浏览器下方状态栏可看到已启用的代理；之后输入网址回车即可通过代理上网；下次启动火狐后会默认是上一次使用的代理：

（三） 虚拟机内防火墙设置

A. 虚拟机 IPSEC（必设置）

与主机IPSEC的设置方法相同，导入"IPSEC_XUNIJI_X.ipsec"。如需修改策略请参考“FHQ_X.doc”。 X指不同的数字，用从论坛下载的同名最新版本即可。

B. 第三方防火墙的设置（必选 ZA 或 COMODO 之一）

1. ZoneAlarm：请将ZA8_XUNIJI_X.xml，按照主机防火墙ZoneAlarm的设置方法导入；如需修改请参考“FHQ_X.doc”。

注意：WIN7 适用的 ZA 版本与 XP 的不同，但是可用同一导入规则。

1. **Comodo**：请将COMODO314_XUNIJI _X，按主机防火墙Comodo的设置方法导入；如需修改请参考“FHQ_X.doc”。

注意：1. 论坛推荐的 Comodo3.14 不适用于 WIN7 64 位（WIN7 32 位可用），第三方防火墙可选用 ZoneAlarm。
2. 如果已使用第三方防火墙，建议禁用WIN7 自带防火墙。

三、联网测试

联网前请检查虚拟机中上网软件是否已设置成经代理服务器上网（代理服务器指自由门/无界/Tor 等破网软件）；可检测虚拟机里上网 IP 与主机真实 IP，如果不同说明代理正常工作；如果设置不当虚拟机中软件无法正常上网。

（一） 先查看主机的真实 IP

说明：使用破网软件之前，需要在主机上查看。主机通过连接海外的 IP 检测网站获取连接的 IP。

查看时，请不要在主机上运行代理软件，因为代理软件一运行，浏览器会强制设置代理。导致查看到的是代理的 IP。

一般可以通过搜索（如: “IP”等关键字）找到排名靠前的一些海外检测站点。
比如：http://apnic.net/apnic-info/whois_search/your-ip

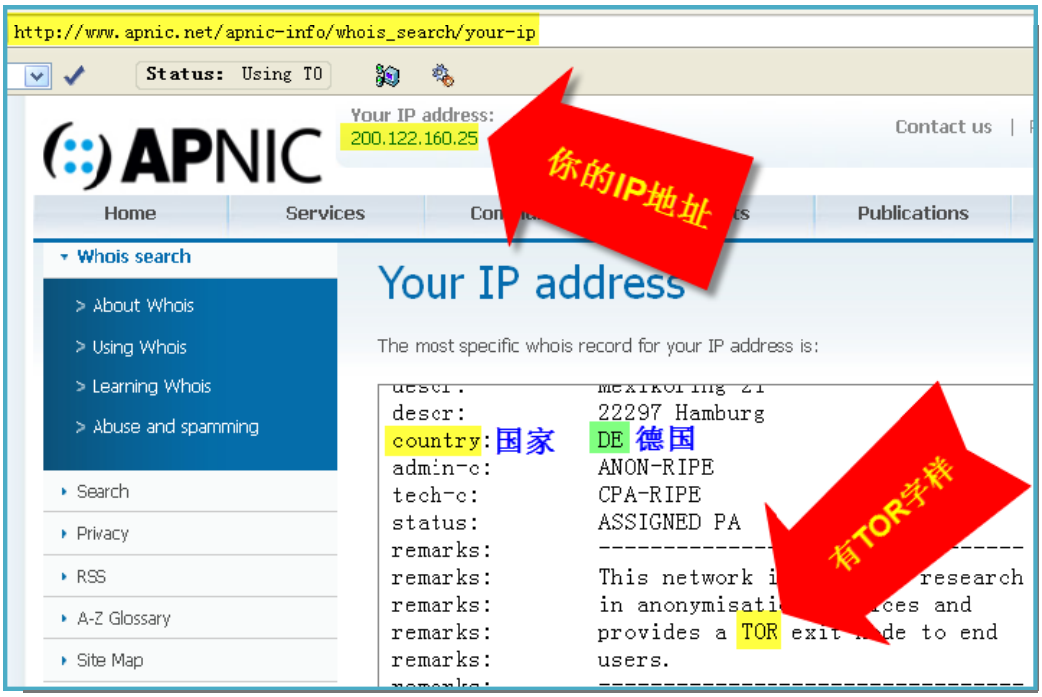
查看方法：在**主机**浏览器中输入以上网址敲回车，Your IP address 就是主机的真实 IP。

（二） 再到虚拟机里查看使用代理后的 IP

说明：虚拟机里的上网程序通过主机代理上网，此时主机需要运行代理程序（启用破网软件）。

1. 查看方法是在**虚拟机**中的浏览器登录海外检测 IP 的网站，如：
   http://apnic.net/apnic-info/whois_search/your-ip
2. 在打开的网页左上角可看到当前 IP，在网页下方可看到 **Country**（国家），右侧的 US 代表美国。说明此时的 IP 显示是来自美国，而非本地 IP：

3. 如果主机用 Tor 作为代理软件，查询 IP 时会显示在不同的国家，且会看到有 TOR 字样：



说明：用逍遥游/自由门做代理服务器，虚拟机检测 IP 一般是“65.49.2.X”或“65.49.68.X”；用无界浏览做代理服务器，虚拟机检测 IP 一般是“65.49.14.X”；用 Tor 做代理服务器，用以上方法可看到 IP 在不同的国家，在一些描述中会看到有“TOR”字样。

注意：如果按以上设置后，虚拟机里经海外网站测试显示的上网 IP 跟主机未使用破网软件显示的相同，或者虚拟机里显示的代理国别为中国时，请拷屏并联系禁书网来解决。因为我们采用的通常是自由门/无界/Tor 等高度加密的软件，一般显示的国别都是海外国别。

四、安全事项必读

1. 主机上需要照常安装防火墙、杀毒软件、擦除痕迹软件等；为了使用方便本方案并没有禁止主机上网，但一定要注意保持主机的纯净，这是所有安全的支点；同时把虚拟机、破网软件、重要资料放置在加密盘中；

2. 虚拟机中需要安装防火墙增加防御能力，并装杀毒软件、擦除痕迹软件等。即使虚拟机每次启动前恢复快照，但在关闭虚拟机与恢复快照前，虚拟机中的痕迹是一直保留着的，如果虚拟机意外被打开是有风险的，因此关闭虚拟机前应擦除痕迹；

3. 虚拟机要使用最新版本，以避免安全漏洞；

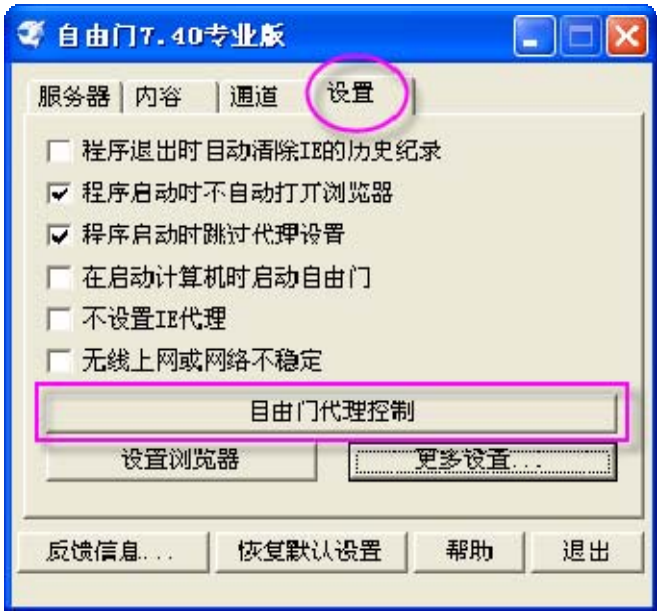
4. 虚拟机要专机专用，可建立多个虚拟机；重要虚拟机不要延用原来使用过的，要从新建立与安装系统。如果测试不安全软件的虚拟机，不要登陆敏感工作邮箱及平时用的私人邮箱，避免虚拟机中未经论证安全性的软件泄漏私人帐号和密码；但可以登录临时邮箱。

5. 建议虚拟机第一次上网前按教程设置完成，并安装所需要的软件后，建立一个虚拟机快照，每次使用后关闭虚拟机时点**控制－退出－强制退出**（勾选**恢复到当前备份 XX**）。

五、附加功能：不隐藏 IP 登陆国内网站

说明：整机隔离方案的安全基础是主机安全，因此主机不能使用国内软件及其它不安全软件、不直接登陆网站等。同时由于整机隔离方案设定的特殊的联网方式，虚拟机不通过代理是无法上网的。那么在整机隔离方案下如何短时间上普通网站、或运行非安全软件呢？这里有解决方案：建立一个全新的虚拟机，设置完备后建立快照，每次使用后关闭虚拟机时点**控制－退出－强制退出**（勾选**恢复到当前备份 XX**）；此虚拟机的网络代理设置方法、浏览器代理设置与整机隔离相同，但是破网软件目前只能使用自由门（如果逍遥游的**逍遥游代理控制**可用的话，亦可用逍遥游代理上网），具体方法如下：

1. 在自由门软件的**设置**点**自由门代理控制**：



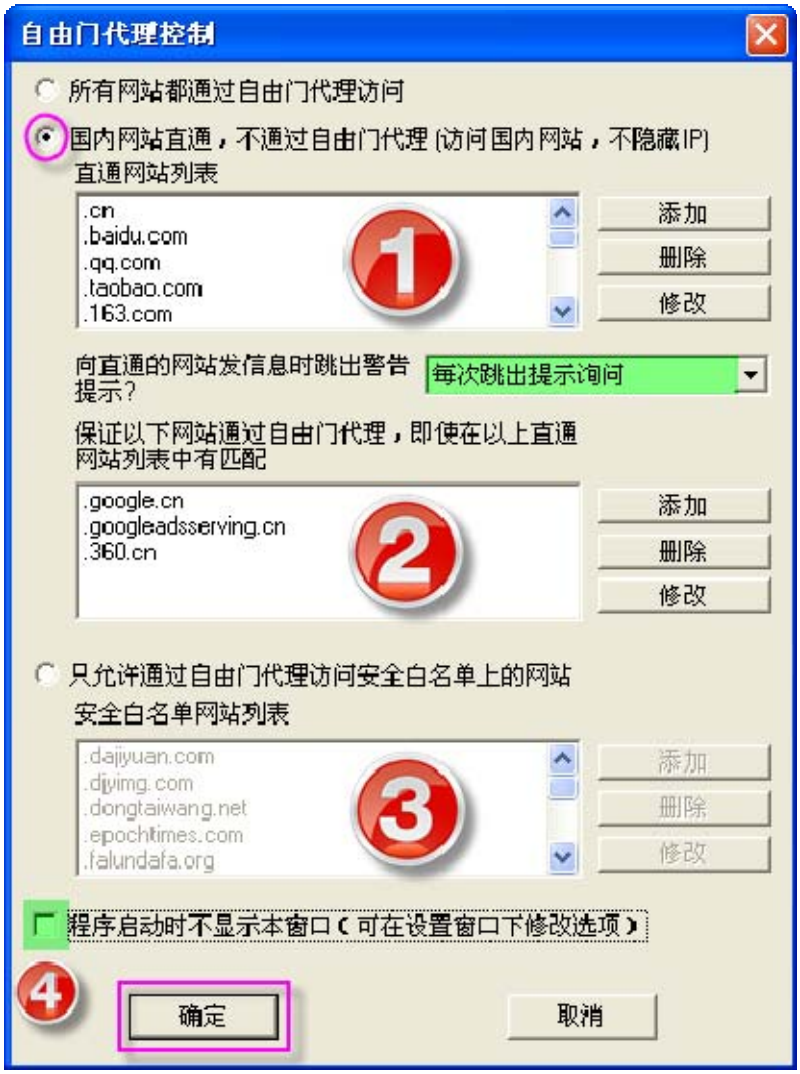
2. 勾选**国内网站直通，不通过自由门代理（访问国内网站，不隐藏 IP）。向直通的网站发信息时跳出警告提示？**选择**每次跳出提示询问**。这样设置是为了避免未经代理误连国内网站；如果确认是要连接国内网站，可在出现的提示询问上点**不再显示本窗口**（下一步有具体说明）；

①可**添加、删除、修改**“直通网站列表”；添加的关键字仿照自带列表，或在软件主界面点**帮助**查看；

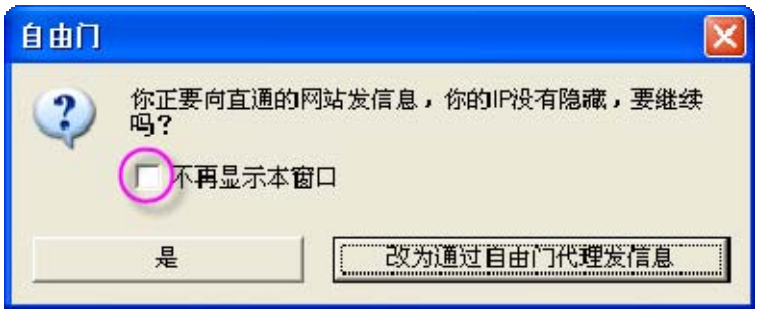
②与以上**直通网站列表**关键字相同、但又想通过自由门代理上网，可**添加**到这里，亦可**删除、修改**；

③如果只想通过代理访问白名单上的网站，可勾选**只允许通过自由门代理访问安全白名单上的网站**。可**添加、删除、修改**“安全白名单网站列表”；

④不要勾选**程序启时不显示本窗口**（通过代理和未经代理直通国内网站的两种上网方式同时存在，为了保证正确设置，每次开自由门时需从新确认），最后点**确定**：



3. 因为以上设置了向直通网站发信息时每次跳出提示询问，在每一步需发信息给网站都会跳出提示；如果你确认目前是在不隐藏 IP 登陆国内网站，点**是**；如果这段时间都不隐藏 IP 登陆国内网站，可临时勾选**不再显示本窗口**，再点**是**；如果需要经代理上网，可点**改为通过自由门代理发信息**。注意：国内网站往往在使用自由门等代理时是无法登陆的。



附 录

1) 设置.bat （适用于 WINXP/WIN7）

下载或制作“设置.bat”，用于一键设置网卡。如果没有从本站上下载“设置.bat”，可以按以下方法建立：

（1） **请拷贝以下内容：**

```
@echo off
setlocal enabledelayedexpansion
title 参数设置
echo.#########################################################################
#####
echo.
echo.设置网卡为固定 IP,DNS 和网关为空,同时禁用 SERVER 等服务。
echo.如果默认按回车的话:（在网络编号选择和 IP 地址输入位置）
echo.  a).自动设置虚拟机的 Host-Only 网卡或虚拟机里的网卡。
echo.  b).主机的 host-Only  网卡 IP "192.168.188.1"
echo.  c).虚拟机内本地连接  网卡 IP "192.168.188.2"~"192.168.188.6"
echo.如果 IP 段出现跟主机其它网卡冲突的时候，请手动输入设置 IP。
echo.注意：虚拟机的 Host-Only 网卡或虚拟机里的网卡 IP 需要为同一网段。
echo.设置完成后，需要重启计算机，可以用 Ipconfig/all 查看。
echo.
echo.#########################################################################
#####


echo.


rem 检测操作系统版本
SET sysver=""
VER|FINDSTR -I " 5.0." > nul && SET sysver=win2000
VER|FINDSTR -I " 5.1." > nul && SET sysver=winXP
VER|FINDSTR -I " 6.0." > nul && SET sysver=winVista
VER|FINDSTR -I " 6.1." > nul && SET sysver=win7

if "%sysver%"=="" (
  echo 未能自动识别出当前的操作系统版本，请按照上述说明手动进行设置
  goto :eof
) else (
```

```
  if /i "%sysver%"=="win7" (
    echo 在 win7 里需要以管理员身份运行:在本文件上点击鼠标右键选择"以管理员身份运行"
    echo.
  )
)


   :seladapter

    if /i "%sysver%"=="win7" (
        rem 关闭 ipv6 的隧道
        netsh interface teredo set state disable > nul
        netsh interface 6to4 set state disabled > nul
        netsh interface isatap set state disabled > nul

        rem 禁用 ipv6
                                                    reg             add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\
/v DisabledComponents /t REG_DWORD /d 0xffffffff /f > nul

    )
    set adapternum=0
    set selno=1
    set NetCardRefNo=0
    set NetCardName=""

    echo.网卡名称列表:

    FOR /F "tokens=2*" %%i IN ('ipconfig/all^|find "Ethernet adapter"') DO
(
      FOR /F "tokens=1* delims=:" %%a in ("%%j") do (
          set /a adapternum+=1
          echo [!adapternum!] "%%a"
          set Desp!adapternum!="%%a"
              if /i "%%a" == "VMware Network Adapter VMnet1" set
NetCardRefNo=!adapternum!
               if /i "%%a" == "VirtualBox Host-Only Network" set
NetCardRefNo=!adapternum!

        )
    )
```

```
rem 在中文版 win7 系统里，上述代码因为标识问题无法查询到适配器，改为下边的
if %adapternum% EQU 0 (
  if /i "%sysver%"=="win7" (
    FOR /F "tokens=1*" %%i IN ('ipconfig/all^|find "适配器"') DO (
      FOR /F "tokens=1* delims=:" %%a in ("%%j") do (
           set /a adapternum+=1
           echo [!adapternum!] "%%a"
           set Desp!adapternum!="%%a"
               if /i "%%a" == "VMware Network Adapter VMnet1" set
NetCardRefNo=!adapternum!
                if /i "%%a" == "VirtualBox Host-Only Network" set
NetCardRefNo=!adapternum!
        )
    )
    FOR /F "tokens=1*" %%i IN ('ipconfig/all^|find "適配器"') DO (
      FOR /F "tokens=1* delims=:" %%a in ("%%j") do (
           set /a adapternum+=1
           echo [!adapternum!] "%%a"
           set Desp!adapternum!="%%a"
               if /i "%%a" == "VMware Network Adapter VMnet1" set
NetCardRefNo=!adapternum!
                if /i "%%a" == "VirtualBox Host-Only Network" set
NetCardRefNo=!adapternum!
        )
    )
  )
)

    echo.
    echo.

    if %adapternum% EQU 0 (
        echo 未能找到网卡信息退出
        goto :eof
    )

    REM 如果没有找到默认的 Host-Only 网卡,就设置第一个网卡。
    if %NetCardRefNo% EQU 0 (set selno=1) else (set selno=%NetCardRefNo% )

    set /p selno="选择设置的网卡编号[1~%adapternum%]:"


    if %selno% GTR %adapternum% (
        echo.输入编号无效，请从新选择...
```

```
        goto :seladapter)


    if  %selno% LSS 1  (
        echo.输入编号无效，请从新选择...
        goto :seladapter)

    for /l %%i in (1 1 %adapternum%) do (
       if %%i EQU %selno% set NetCardName=!Desp%%i!
     )

    echo 当前选择的网卡为 %NetCardName%
    echo.

     REM 如果只有一个网卡设置为 "192.168.188.2" 多个网卡设置为 "192.168.188.1"
       if %adapternum% EQU 1 (set myip=192.168.188.2) else (set myip=192.168.188.1)

   :setmyip

    set mydot=.
    set myiprang=""

    set /p myip="设置的网卡 IP[%myip%]:"

    echo 准备设置 IP:%myip%


    REM 查看当前的是否存在网段

    for /f "tokens=1-3 delims=." %%i in ("%myip%") do (
      set myiprang=%%i%mydot%%%j%mydot%%%k
    )

    set findnum=0
    FOR /F "tokens=*" %%i IN ('ipconfig^|find /i "%myiprang%"') DO (
      set /a findnum+=1
    )



SET ipname=ip
if /i "%sysver%"=="win7" SET ipname=ipv4
```

```
if %findnum% GTR 1 (
  echo %myiprang% 网段已经存在,更换一下网段
  goto :setmyip
)

if %findnum% EQU 0 goto :netConfig

SET b=0
FOR /F %%i IN ('netsh interface %ipname% show address %NetCardName%^|find
"%myiprang%."') DO (
  SET b=1
)
if %b%==0 (
  echo %myiprang% 网段已经存在, 请更换一下网段
  goto :setmyip
)


   :netConfig
    echo.

echo IP 地址初始化设置...

echo  IP 地址正在从 DHCP 自动获取
netsh interface ip set address name=%NetCardName% dhcp
echo  DNS 地址正在从 DHCP 自动获取
netsh interface ip set dns name=%NetCardName% dhcp

    echo 开始设置网络部分...



echo 设置[%NetCardName%] IP: %myip%  网关: 空
netsh interface %ipname% set address name=%NetCardName% static %myip%
255.255.255.248 gateway=none


echo 设置 [%NetCardName%] DNS 空
netsh interface %ipname% set dns name=%NetCardName% source=static none
netsh interface %ipname% set wins name=%NetCardName% source=static none


    echo 设置网络部分完毕。
```

```
    echo.

    echo 停用 server 服务


SET DISABLED=0 && sc qc Browser|FINDSTR -I "DISABLED" > nul && SET DISABLED=1
if %DISABLED%==0 (
  sc config Browser start= disabled
  net stop Browser
)

SET DISABLED=0 && sc qc lanmanServer|FINDSTR -I "DISABLED" > nul && SET
DISABLED=1
if %DISABLED%==0 (
  sc config lanmanServer start= disabled
  net stop lanmanServer
)


rem 停用 2 个高风险的服务

echo 停用 Remote Registry 服务
  SET DISABLED=0 && sc qc RemoteRegistry|FINDSTR -I "DISABLED" > nul && SET
DISABLED=1
  if %DISABLED%==0 (
    sc config RemoteRegistry start= disabled
    net stop RemoteRegistry
  )

echo 停用 Task Scheduler 服务

if /i NOT "%sysver%"=="win7" (
  SET DISABLED=0 && sc qc Schedule|FINDSTR -I "DISABLED" > nul && SET
DISABLED=1

  if %DISABLED%==0 (
    sc config Schedule start= disabled
    net stop Schedule
  )
)


  :eof
  Pause
```

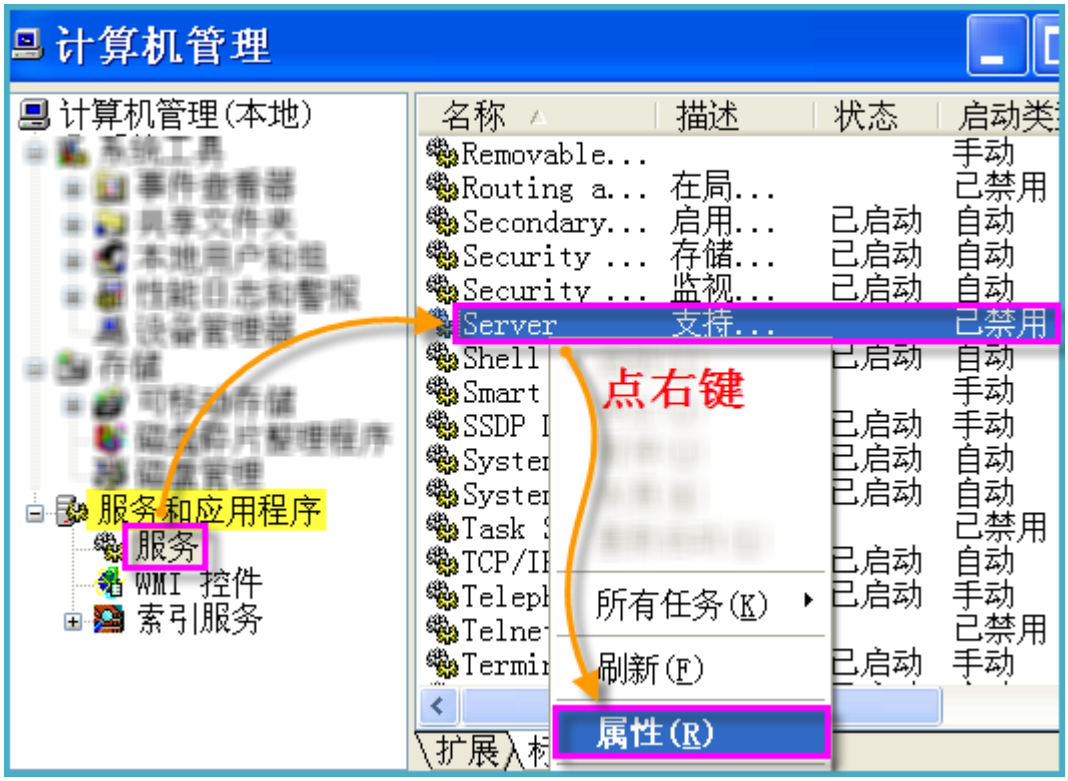
（2） 粘贴到记事本中，点击**文件 → 保存**：

（3） 文件名为：**设置.bat**（注意不能只写“设置”，这样存盘后会成为“设置.txt”），点**保存**：

（返回核心设置介绍）（返回主机参数设置）

2) 开启 SERVER 服务

（1） 在**我的电脑**，点右键选择**管理**；到**计算机管理**选择**服务和应用程序 → 服务**，在右侧栏中选中 **SERVER**，点右键点**属性**：



（2） 在**常规**页签，点**启动类型**右侧小箭头，由**已禁用**改成**自动**，点**应用**，点**启动**，最后点**确定**。如需其它设置，可完成后一并从新启动计算机。

（返回如果需要共享文件或打印机的设置）

3) WIN7 防火墙.bat （适用于 WIN7）

（1） 拷贝以下内容，粘贴到记事本，保存为“WIN7 防火墙.bat”（方法如以上“设置.bat”的制作说明）。直接在 WIN7 主机双击“WIN7 防火墙.bat”即设置了 WIN7 自带的防火墙：

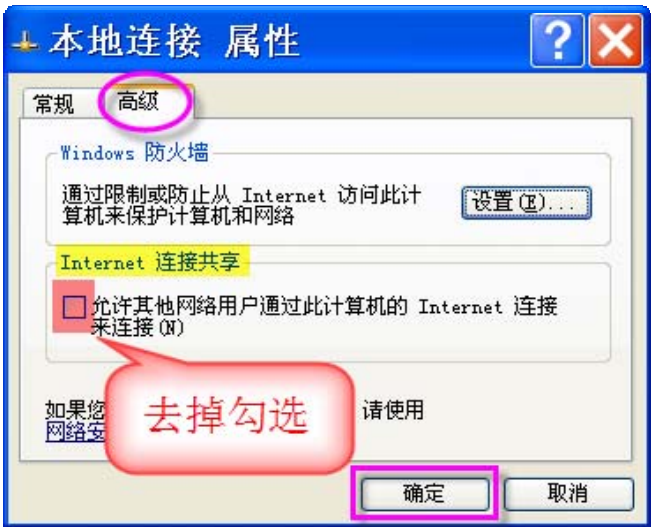
```
@echo off
setlocal enabledelayedexpansion
title Win7 防火墙设置

echo 还原 Win7 防火墙默认设置
netsh advfirewall reset

echo 打开 windows 防火墙
netsh advfirewall set allprofiles state on

echo 高级设置，入站规则
echo 许可虚拟机网段访问主机的侦听端口，其它都禁止
netsh advfirewall firewall add rule name="我的规则-允许虚拟机网段 TCP 访问主机侦听端口" dir=in action=allow description = "允许虚拟机网段 TCP 访问主机侦听端口" enable=yes localip=192.168.188.1 remoteip=192.168.188.0/29 localport=8580,443,8118,9050,8119,9052 remoteport=any protocol=tcp
netsh advfirewall firewall add rule name="我的规则-禁止虚拟机网段 TCP 访问主机非侦听端口" dir=in action=block description = "禁止虚拟机网段 TCP 访问主机非侦听端口" enable=yes localip=any remoteip=192.168.188.0/24 localport=0-442,444-8117,8120-8579,8581-9049,9051,9053-65535 remoteport=any protocol=tcp
netsh advfirewall firewall add rule name="我的规则-禁止虚拟机网段 UDP 访问主机" dir=in action=block description = "禁止虚拟机网段访问主机非侦听端口" enable=yes localip=any remoteip=192.168.188.0/24 localport=any remoteport=any protocol=udp

echo 高级设置，出站设置
echo 禁止 host-Only 虚拟网卡上程序访问子网。

netsh advfirewall firewall add rule name="我的规则-禁止 host-Only 虚拟网卡上程序访问子网" dir=out action=block description = "禁止 host-Only 虚拟网卡上程序访问子网" enable=yes localip=192.168.188.1 remoteip=LocalSubnet

echo 防火墙设置完成。
Pause
```

(返回WIN7 用自带防火墙)

4) IP Routing Enabled 启用原因和停止方法

- **原因一**：为了实现 Internet 网络共享

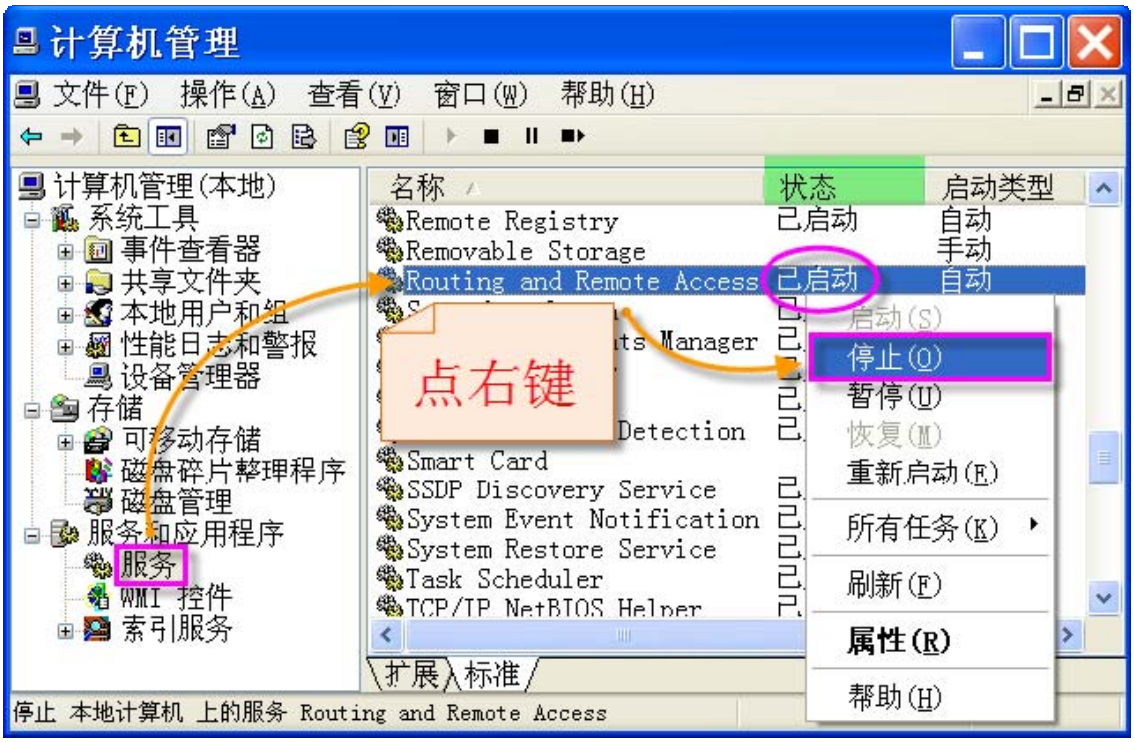
停止方法：在**主机本地连接**点右键 → **属性** → **高级**，把**允许网络其他用户通过此计算机的 Internet 连接来连接**的勾选去掉，点**确定**即可：



- **原因二**：启用了 Routing and Remote Access 服务

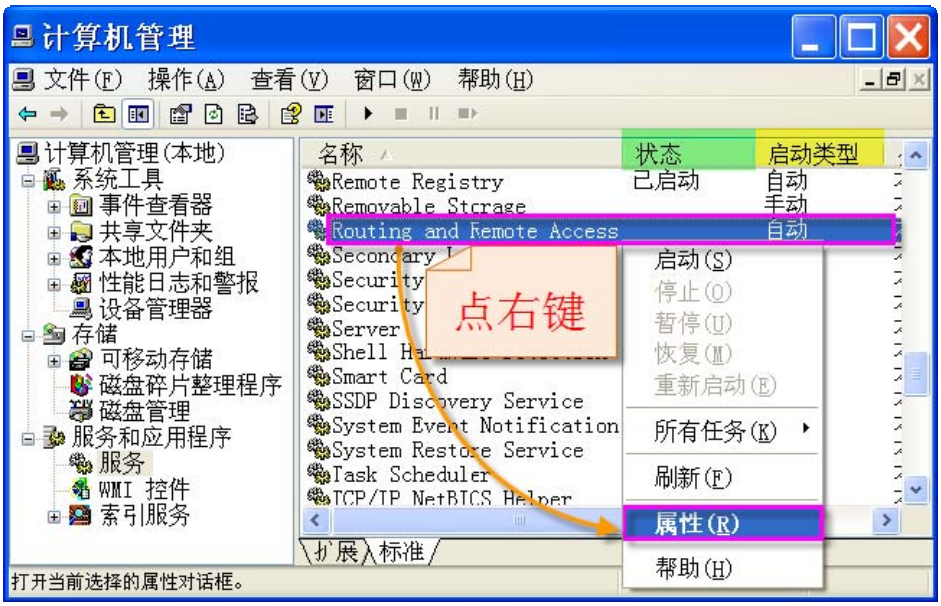
停止方法：

（1） 到**我的电脑**点右键 → **管理** → **服务和应用程序** → **服务** → 在右侧找到 **Routing and Remote Access**，如果此时状态是**已启动**，点右键，点**停止**：

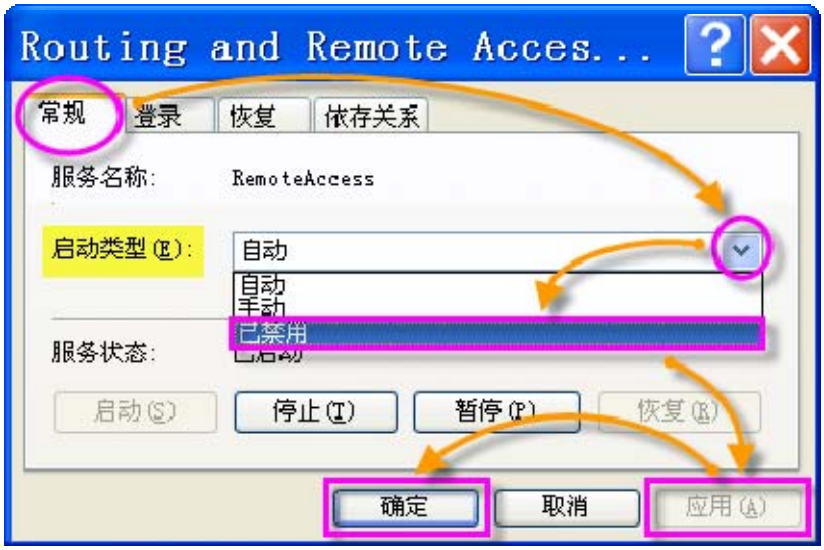


（2） 正在停止：

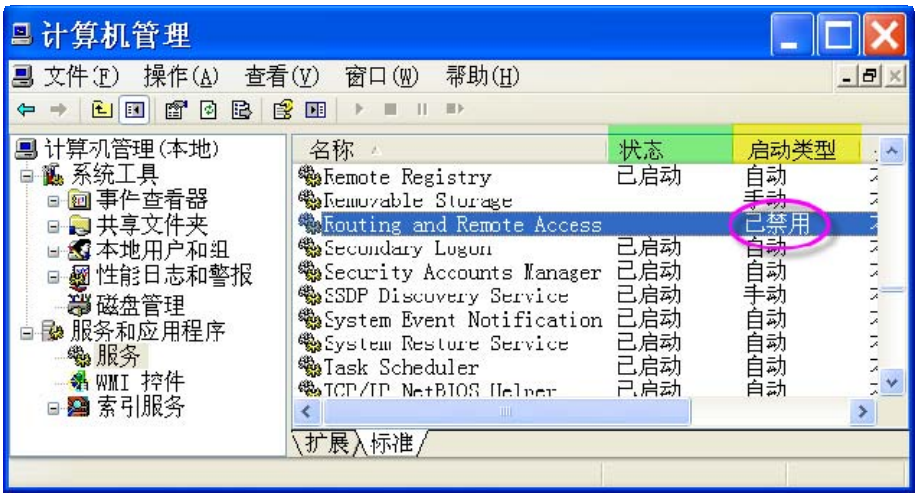
（3） 停止后 Routing and Remote Access **状态**是空白，点右键 → **属性**：



（4） 在**常规** → **启动类型**，选择**已禁用**，点**应用**，点**确定**：



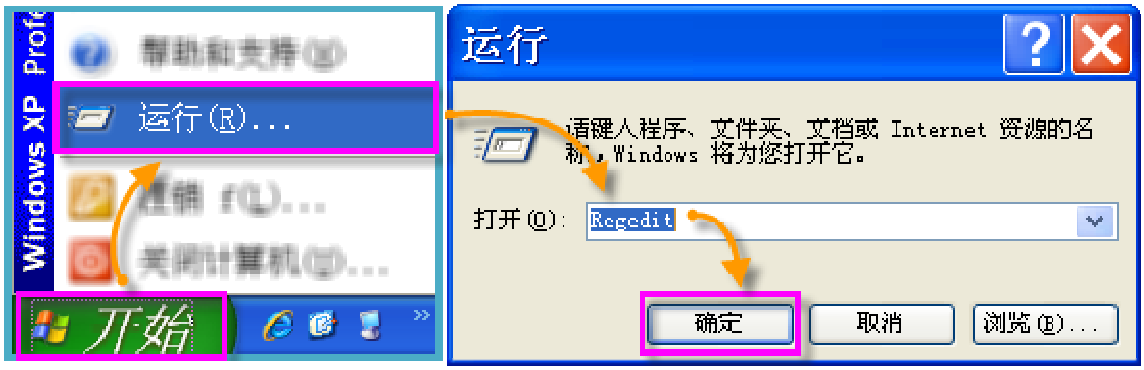
（5） 设置完成后，Routing and Remote Access **状态**空白，**启动类型**是**已禁用**：



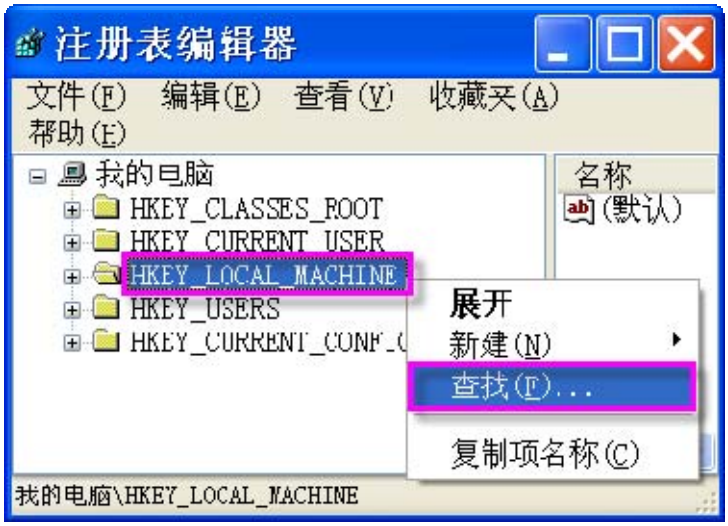
➢ **原因三**：人为强制使用启用 TCP/IP 转发

停用方法如下：

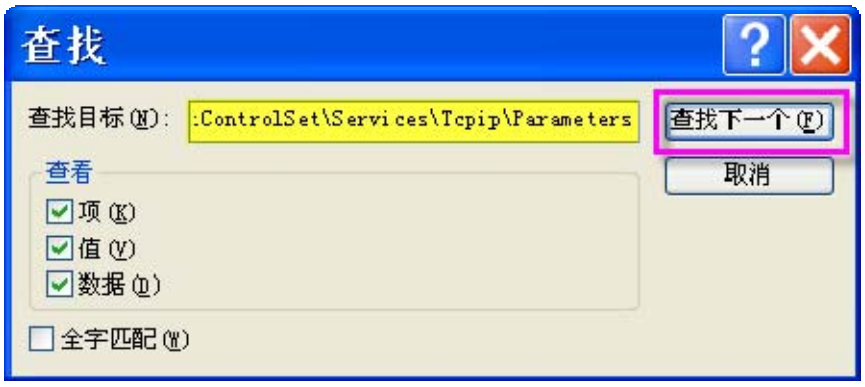
（1） 在**开始** → **运行**中输入 **Regedit** 启动**注册表编辑器** (Regedit.exe)；



（2） 在**注册表编辑器**中，找到 **HKEY_LOCAL_MACHINE** 后点右键 → **查找**，拷贝 SYSTEM\CurrentControlSet\Services\Tcpip\Parameters：

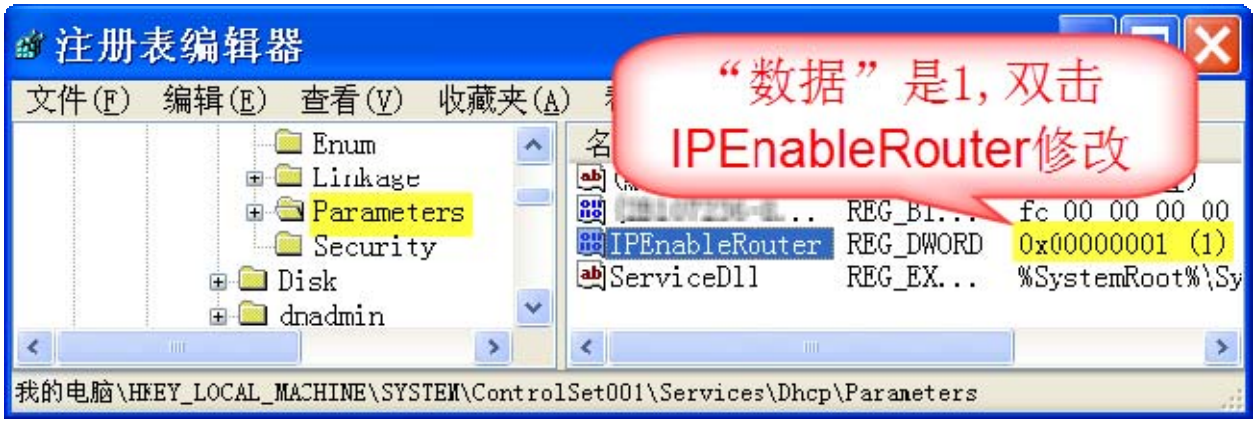


（3） 粘贴 SYSTEM\CurrentControlSet\Services\Tcpip\Parameters，点**查找下一个**：



（4） 正在查找：

（5） 找到后，选中 Parameters，看右侧是否有数值**名称**：IPEnableRouter，数值**类型**：REG_DWORD，数值**数据**：1，是的话双击 IPEnableRouter 修改：



（6） 将**数值数据**改为 0，点**确定**：

（7） 完成后**数据**为 0，点右上角 X 退出**注册表编辑器**：

注意：设置完成后，请在主机再次运行 ipconfig/all，从新检查 IP Routing Enabled 状态。如果仍然没有设置为 No，请联系禁书网来解决。

（返回主机设置步骤 8）

5) 主机“手动设置部份”恢复的方法

1. 如果需要把开启的 SERVER 服务禁用，直接运行“设置.bat”，暂不要从新启动计算机：

2. 以下步骤将勾选 **Microsoft 网络客户端**和安装 **Microsoft 网络的文件和打印机共享**。在电脑右下角选中**本地连接**图标，点右键选**打开网络连接**，选中**本地连接**，点右键点**属性**，在**常规**页签，直接勾选 **Microsoft 网络客户端**即可，如果无需安装其它部份可直接点**确定**：

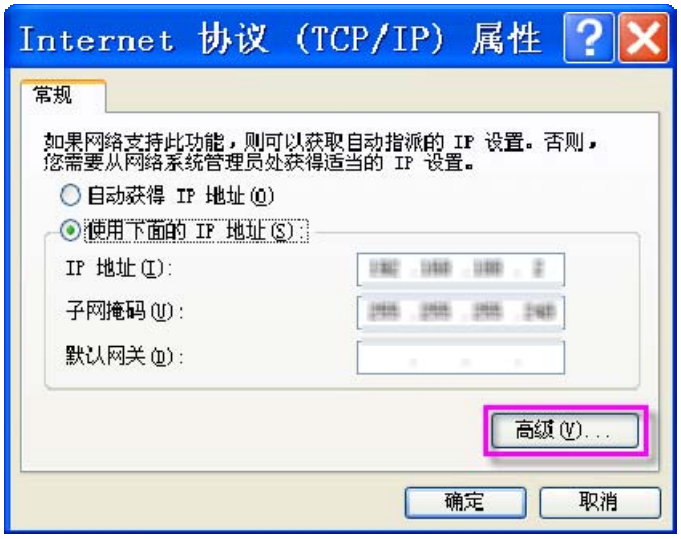
3. 如果安装 **Microsoft 网络的文件和打印机共享**，继续在此画面点**安装**：

4. 选中**服务**，点**添加**：

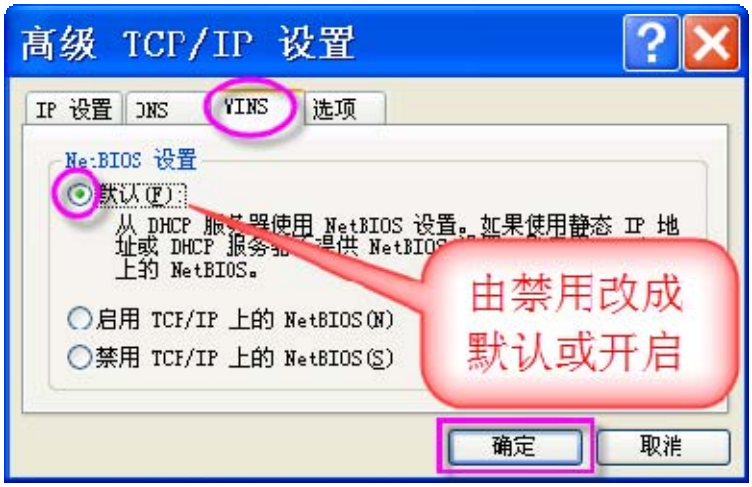
5. 在**厂商**选中 **Microsoft**，在**网络服务**选中 **Microsoft 网络的文件和打印机共享**，点**确定**：

6. 安装成功后如下图，暂不**关闭**，下一步将开启 **TCP/IP** 上的 NetBios。选中 **Internet 协议（TCP/IP）**，点**属性**：

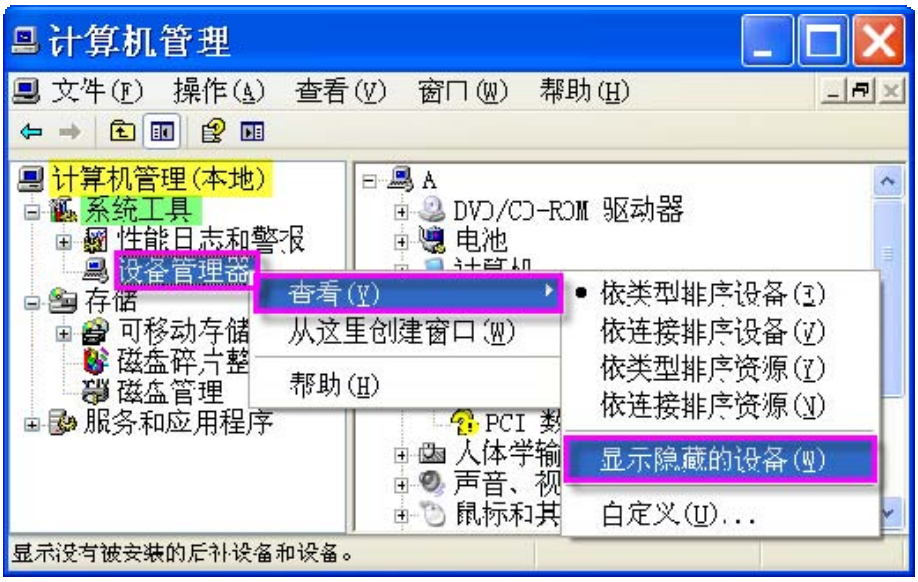
7. 点**高级**：



8. 在 **WINS** 页签，**NetBIOS 设置**中将**禁用 TCP/IP 上的 NetBIOS(S)**改为**默认**或**启用 TCP/IP 上的 NetBIOS(N)**，点**确定**，再点**确定**，点**关闭**：



9. 如果出现从启计算机提示选**否（N）**，下一步将开启**设备管理器**中的 NetBios。到**我的电脑**点右键，点**管理**，找到**设备管理器**点右键 → **查看** → **显示隐藏的设备**：

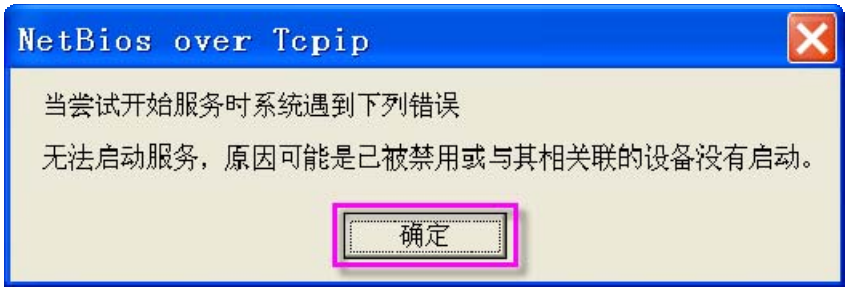


10. 在**非即插即用驱动程序**，找到 **NetBios over Tcpip**，点右键，点**属性**：

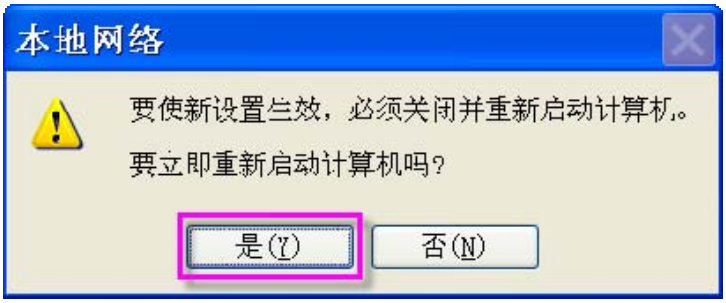
11. 在**常规**页签，在**设备用法**下点右侧小箭头，选择**使用这个设备（启用）**：

12. 在**驱动程序**页签，先将**类型**由**已禁用**，改为**自动**后点**确定**；由以上方法从新進入此界面，此时**启动**按键由灰色变为可用状态，点**启动**后，点**确定**：

13. 如果出现以下界面点**确定**；等从新启动计算机后，到此界面看确实已启动成功即可：



14. 如果出现从新启动计算机提示，点**是（Y）**；或自行从新启动计算机，主机“四个手动设置部份”的恢复就完成了。如果只需恢复其中几项，该项恢复完成后从启计算机即可：

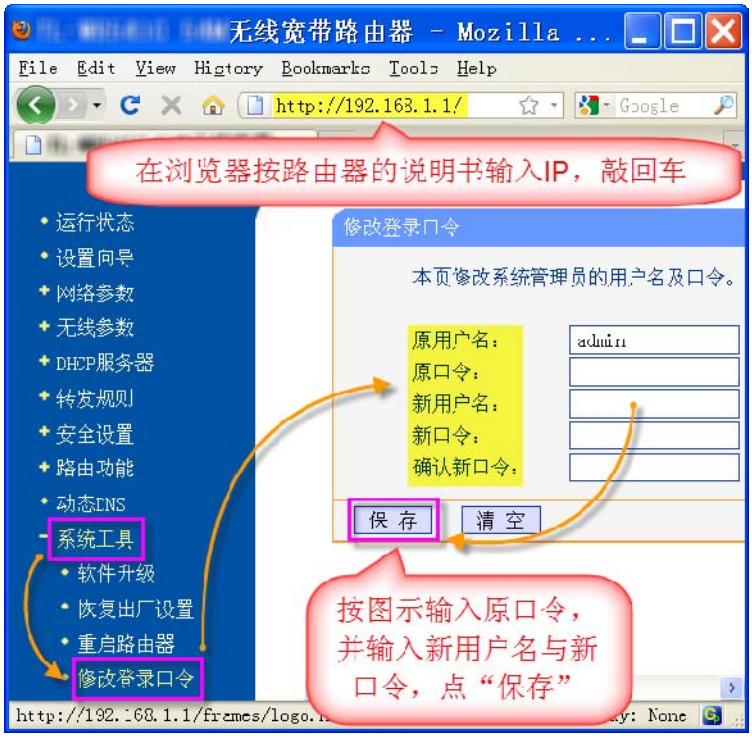


（返回手动设置部份）

6) 无线路由器安全设置实用技巧（节选）

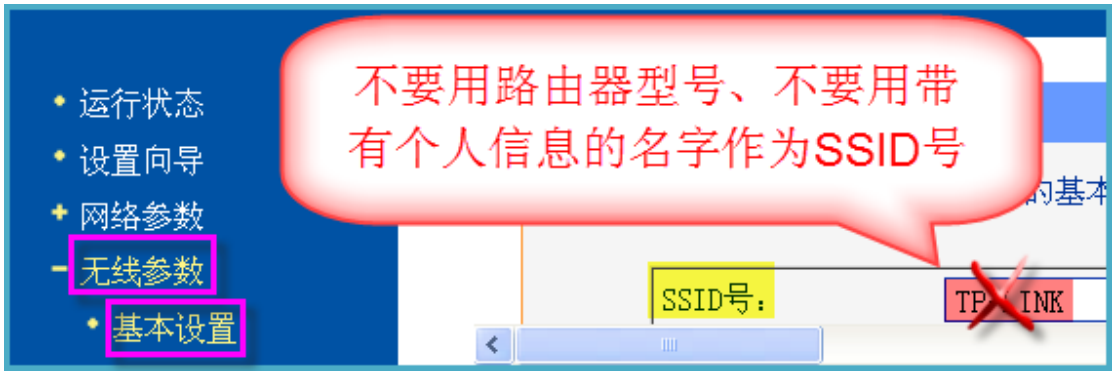
1. 更改管理员密码

如果你的路由器的密码是"password"、"admin"、"1234"，或任何其它默认值，你就正在找麻烦，所以赶紧更改它。



2. 更改默认的 SSID 名称

就象许多用户会忽略其路由器的密码一样，许多用户会保留默认的无线 SSID，这个名称总是显示出设备的生产厂商，也使推断其它信息成为可能。丢弃默认，创建一个不同的 SSID，且一定避免使用任何家庭名称或地址信息。

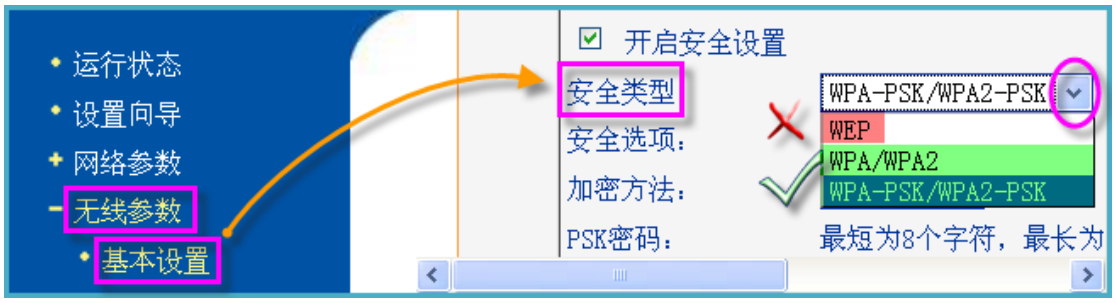


3. 关闭 SSID 广播

广播使你的 SSID 超级容易去关联新的无线设备到你的网络。但是它也广告了你的网络给任何过路者，这可不是个理想的情况。关掉这个功能不会对使用特殊软件的恶意闯入者隐藏你的网络的存在，但是知道你的网络的人越少越好。只要你知道你自己的 SSID，你配置一个新的联网设备不会有任何问题：用 SSID 号搜索到后，输入 WPA 密码即可关联。

4. 使用 WPA 加密而不要使用 WEP

底线——使用 WPA 加密你的无线网络，避免购买与使用任何强制你使用 WEP 去适应的设备。除了大大提高安全度，使用 WPA 还有个有益的用处，因为不象 WEP，你无需在 ASCII 或 HEX 中选择，并且密钥无需符合特殊的长度（比如，13 或 26 个字符为 128 位 WEP）



以上为节选，全文请参考：无线路由器安全设置实用技巧

其它相关内容请参考：

http://www.bannedbook.org/forum42/topic3148.html

《无线宽带路由器的设置兼谈网络基本常识.pdf》

《150M迷你型 3G无线路由器TL-WR703N V1_快速安装指南.pdf》

《无线宽带路由器TL-WR740N详细配置指南.pdf》

7) 受限帐户基础

受限帐户使用基础教程
http://www.bannedbook.org/forum23/topic955.html

创建《受限帐户》的详细过程
http://www.bannedbook.org/forum42/topic3149.html
（返回说明）

8) TorManager2.7 管理器

TorManager2.7 管理器
http://www.bannedbook.org/forum23/topic3150.html

9) 加密盘 TrueCrypt 的说明

可使用 8G（或更大容量）的 U 盘，制作成加密盘，把常用的敏感软件、虚拟机装在此加密盘中，需要时用 USB 与电脑连接，不使用时便于收藏。

注意：不同版本的 TrueCrypt 间不一定兼容，请保留好加密时版本的 TrueCrypt 软件；考虑到 U 盘本身与加密盘的不稳定因素，重要软件、文件、虚拟机请在另一个加密盘中备份。

请参考以下链接，或直接用以下文件名在相关论坛中搜索下载，学习了以下教程就会创建与使用 TrueCrypt 加密盘了。

TrueCrypt 简体中文安装版及绿色版

加密盘TrueCrypt录像说明

从禁书网以上链接可以下载到相关版本，有安装版与绿色版。也可以直接下载这些软件、并按教程安装即可。

官方下载链接：https://truecrypt.org/downloads

10) 虚拟机 VirtualBox 的说明

以下提供了一些 VirtualBox 有关教程的链接：

《VirtualBox 免费虚拟机使用简介（4.02 版）》：
http://www.bannedbook.org/resources/file/315

VirtualBox 录像说明 vbox.wmv：
http://www.bannedbook.org/resources/file/316

◇ 免费开源中文虚拟机软件 VirtualBox 使用图解：
http://www.bannedbook.org/forum23/topic651.html

VirtualBox 4.0.10 下载地址：
http://download.virtualbox.org/virtualbox/4.0.10/VirtualBox-4.0.10-72479-Win.exe

支持 USB2.0 扩展包下载地址：
http://download.virtualbox.org/virtualbox/4.0.10/Oracle_VM_VirtualBox_Extension_Pack-4.0.1

0-72436.vbox-extpack

11) 虚拟机 VMware 的说明

1. 《从官方VMware7.1 中快速提取制作绿色版的方法（仅下载、提取两个步骤）》
http://www.bannedbook.org/forum42/topic3152.html

说明：此链接有如何从官方下载正式版的说明，并有英文版安装教程及绿色版提取方法。

2. 《◇VMware7 中文图解说明》
http://www.bannedbook.org/forum42/topic3154.html

说明：新版因无安全汉化版，技术网站以上链接提供了对应的中文图片，其位置是对应的、可对照使用英文版。

3. 《◇VMware5 升级到VMware7 的图解》
http://www.bannedbook.org/forum42/topic3155.html

说明：7.1 以下的版本可能有安全漏洞，应尽早升级到高版本。虚拟机系统内不要安装 7.1 以下版本的 VMtools，已知安全漏洞主要是在 VMtools 中，虚拟机通过 VMtools 和主机交互。

12) 防火墙软件 COMODO，ZoneAlarm 的相关教程

《科摩多（comodo-毛豆）互联网安全套装多语言版（使用说明）》:
http://www.bannedbook.org/forum42/topic3156.html

《ZoneAlarm 8.0.298 防火墙》:
http://www.bannedbook.org/forum42/topic3157.html

帮助文件和汉化包下载 ：

下载ZoneAlarm 8.0.298 防火墙汉化版安装使用教程
http://www.bannedbook.org/forum42/topic3159.html

下载 ZoneAlarm 汉化文件（779KB）
ZoneAlarm 8.0.298 汉化安装文件.zip

结 语

以上教程中涉及的内容看起来较繁杂，但通过一段时间的演练，会逐渐领会各个环节之间的关联关系而容会贯通。

禁书网将推出多种基于本方案的软件使用教程，希望大家能很快掌握此方案，对于更自如、安全的突破封锁将大有助益。

预祝大家成功！