TorManager2.7

使用帮助

二零一二年十一月三日

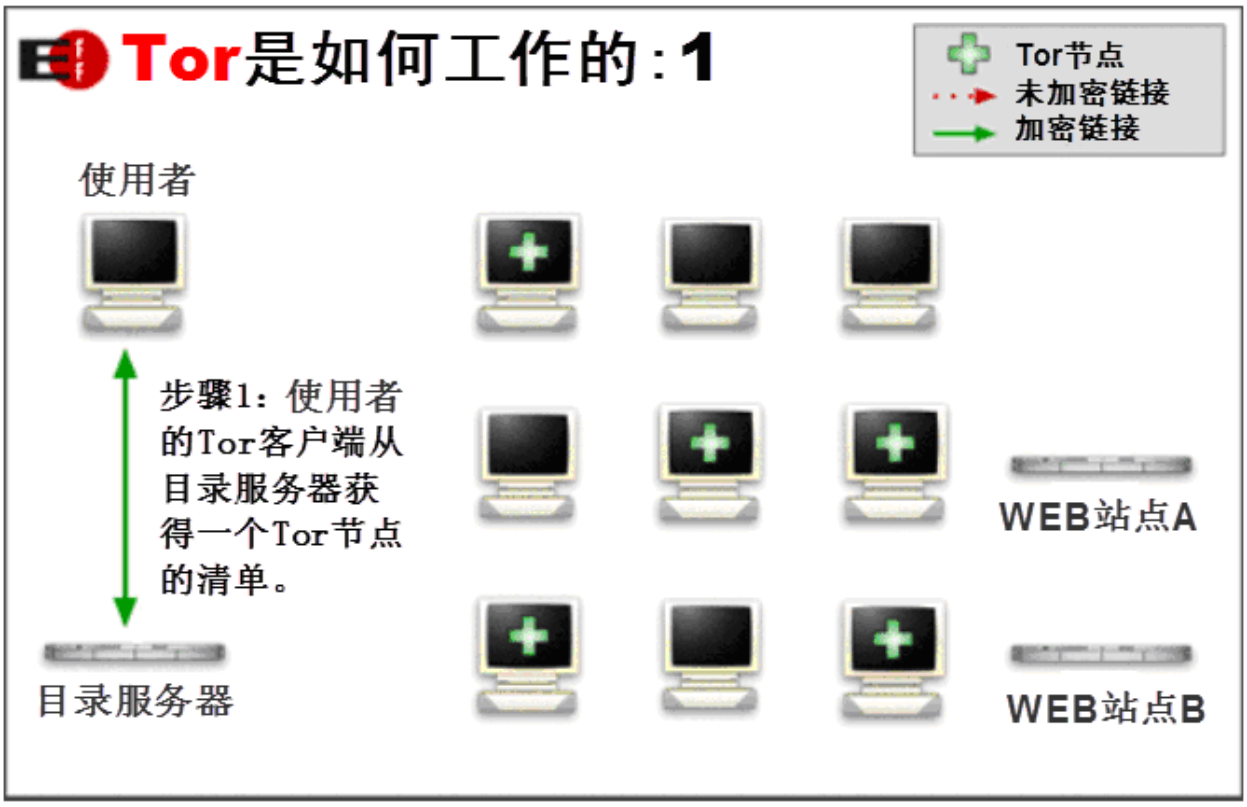
目　录

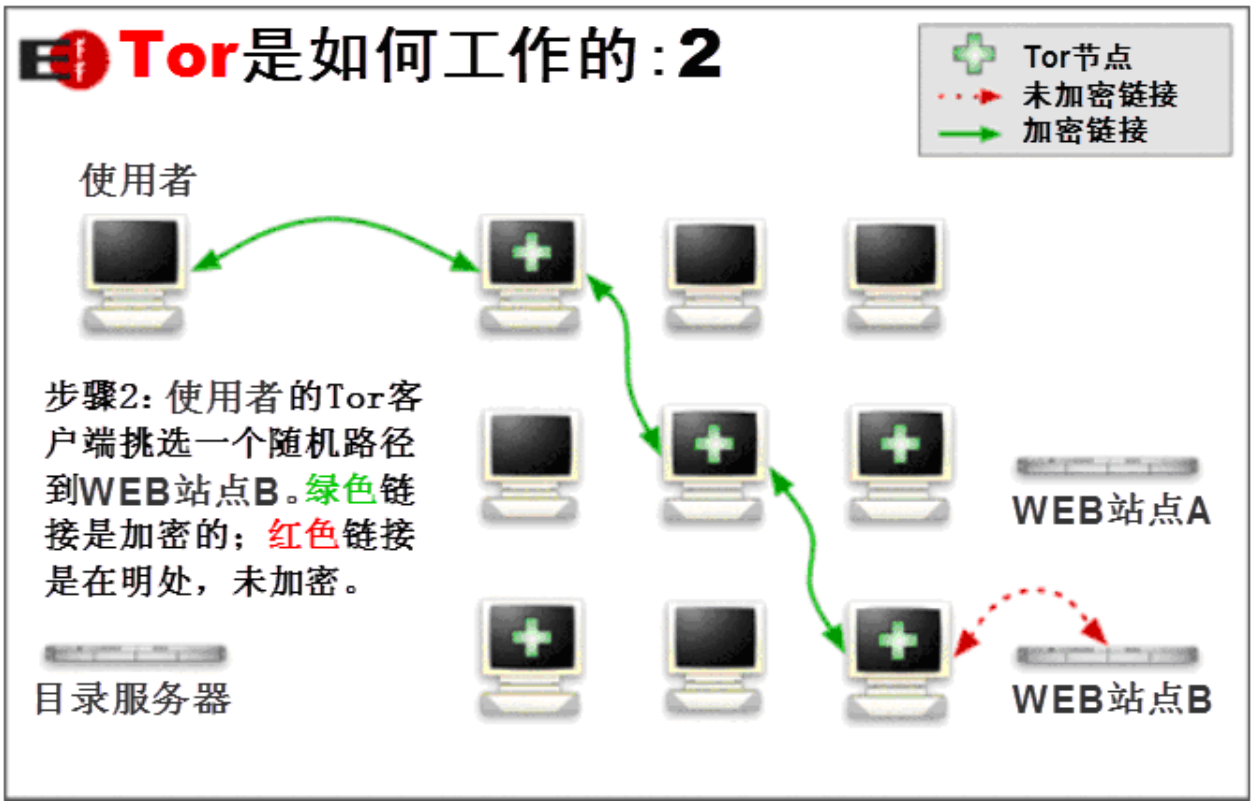
Tor 简介

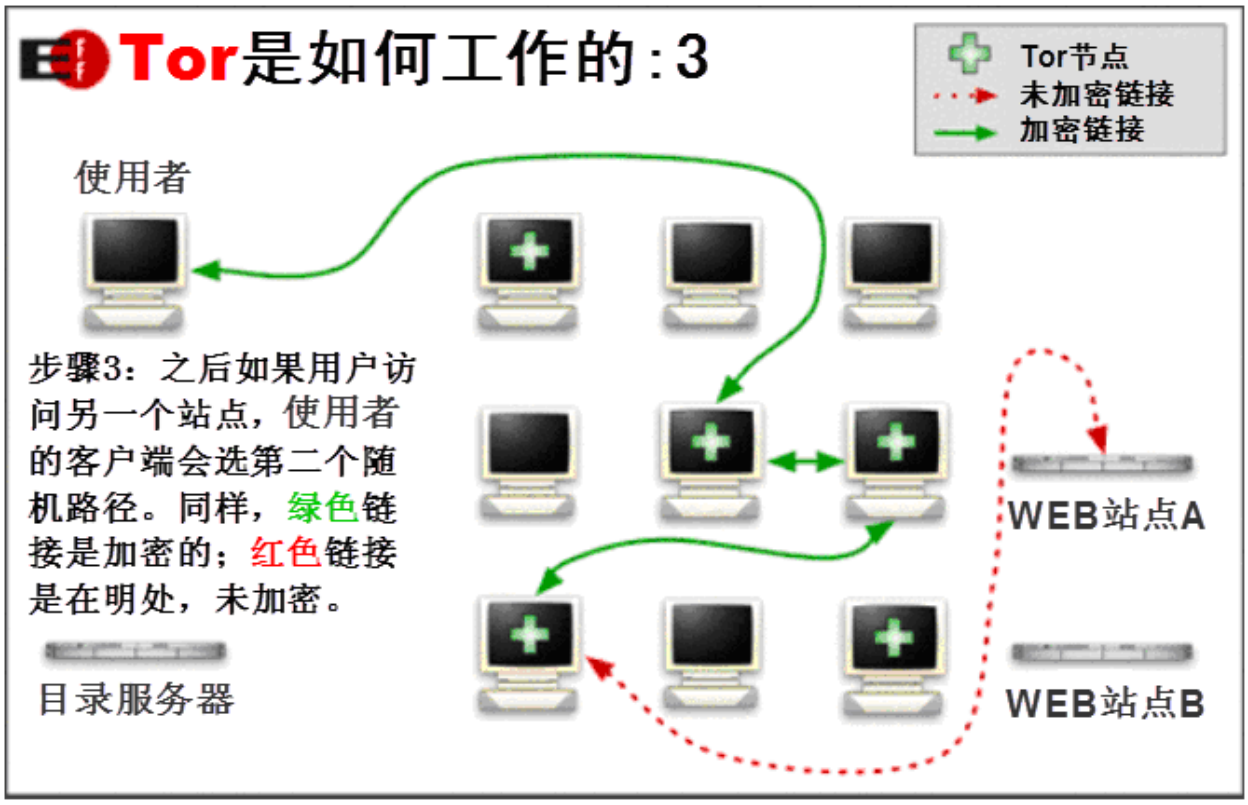
Tor 的全称是“The Onion Router”。它针对现阶段大量存在的流量过滤、嗅探分析等工具，在 JAP 之类软件基础上改进的，支持 Socks5，并且支持动态代理链（通过 Tor 访问一个地址时，所经过的节点在 Tor 节点群中随机挑选，动态变化，由于兼顾速度与安全性，节点数目通常为 2-5 个），因此难于追踪，有效地保证了安全性。另一方面，Tor 的分布式服务器可以自动获取，因此省却了搜寻代理服务器的烦琐。

官方站点（请用破网软件登录）：https://www.torproject.org/

一、 Tor 工作原理图







注意：从 Tor 工作原理图可知，入口节点可知用户的 IP，增加前置代理可避免此问题；同时为避免出口是恶意节点，登录的站点要采取 https 加密的形式，避免帐号、内容等泄密。
（返回Tor节点说明）（返回不能取消前置代理说明）（返回Tor用途 1）

二、Tor 对隐私保护的局限与对策

1) Tor 仅仅保护那些配置过将数据通过 Tor 传输的应用程序——它不会奇迹般的在你安装后就匿名所有通讯。**对策：需要确定哪些程序配置 Tor 代理，如浏览器或其它上网软件将代理服务器设置成 Tor 的相关参数即可。**

2) 浏览器插件，如 Java、Flash、ActiveX、RealPlayer、Quicktime、Adobe's PDF 插件和其它：它们可能导致泄露你的 IP 地址。另外像 Google 工具条这样的扩展会查询有关你访问站点的信息：它们可能绕过 Tor 而泄露敏感信息。 **对策：禁用一些插件；不要在线打开由 Tor 下载的文件等。**

3) 谨防 Cookies：如果你曾在未使用 Tor 的情况下浏览了某个站点，这个站点给你设置了一个 Cookie，那么，即使你又开始使用 Tor，那个 cookie 仍能用来确认你的身份。**对策：使用无影无踪等擦除软件清除使用痕迹。**

4) Tor 匿名通信的来源，并加密你和 Tor 网络以及 Tor 网络中的所有数据，但是它不能加密 Tor 网络与通信目的地之间的数据。如果你正在传输敏感信息，你应该像平时在令人担心的互联网上一样谨小慎微——使用 HTTPS 或其他端到端的加密与认证手段。**对策：使用 SSL 加密。**

5) 尽管 Tor 阻挡了在本地网络上想要发现或影响你的通信目的地的攻击者，它也使新的攻击成为可能：恶意的或配置错误的 Tor 出口节点会将错误的页面发送给你，甚至，将伪装成受信区域的、嵌入的 Java 小程序发送给你。当打开通过 Tor 下载的文件或应用程序时请格外小心，除非你已经验证了其完整性。**对策：不要对额外的东西感兴趣；验证下载的文件。**

6) Tor 使用者比较少。**对策：养成良好的上网习惯，做好防护措施。比如不用相同的系统访问敏感站点与普通站点、防火墙的设置、虚拟机快照恢复等。**

禁书网 大陆直连 https://goo.gl/C6xxGf 看 禁书禁闻禁文禁网禁片禁歌禁曲

三、国内访问现状

目前国内 Tor 是被封锁的，不能直接访问，必须通过前置代理的方式才能访问。也就是在主机与 Tor 之间由其它代理服务器连接。

这些代理的来源主要有（代理设置方法将在后续介绍）：

1) 自由门，逍遥游，无界浏览：

2) 动网通中直接提供的一些普通代理：

3) 异次元搜索一些免费提供的代理的站点。为了避免大家都使用同一搜索代理，建议可以其它普通搜索方式在找一些可用的代理。

四、Tor 的一些用途

1) 辅助破网，就是自由门、无界等主流破网软件都失效的情况下，临时用Tor破网访问海外正义网站，这个时候因为自由门、无界都失效了，无法作为前置代理来引导Tor，需要寻找海外普通的代理来作前置代理，比如从异次元代理、动网通中寻找，访问的时候必须采用SSL加密方式访问，也就是https。平时应该以自由门、无界等破网软件为主。[注意安全说明]。

2) 用来访问一些海外网站（有可能是被封锁的，或者不确定是否被封锁），比如有些网站我们需要用高度匿名安全代理来访问，但该网站又限制自由门、无界的 ip，这时可以用 Tor。

3) 用于访问国内网站，避免使用自由门、无界等破网软件时的“回墙” 现象（即只能从国内突破网络封锁，但不能回访国内网站）。但是仅仅使用Tor无法确保安全，需要其它配套的安全解决方案，比如：《整机隔离 之 虚拟机仅主机(Host-Only)方案》，链接如下：http://www.bannedbook.org/forum23/topic3136.html

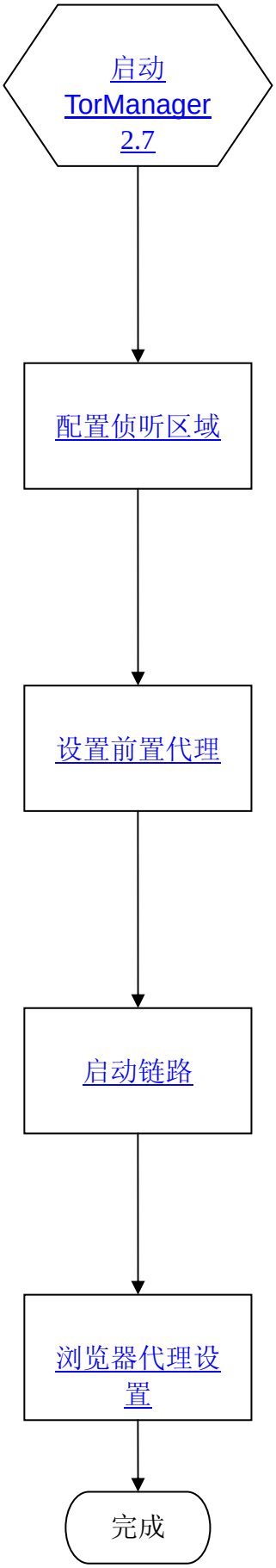
（返回目录）

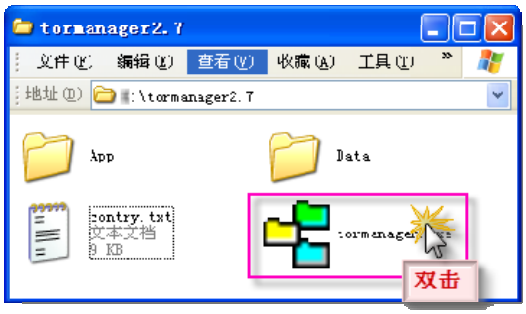
TorManager2.7 的使用方法

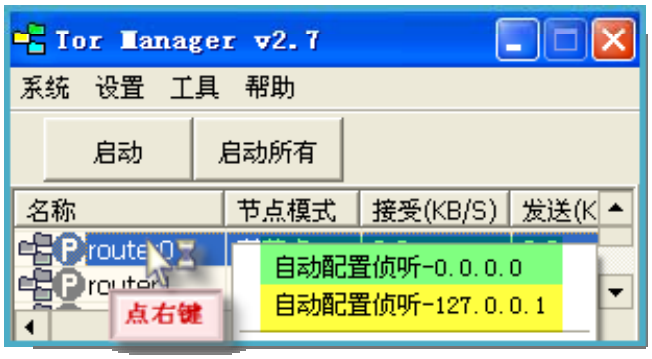
一、TorManager2.7 下载地址及简易使用图解

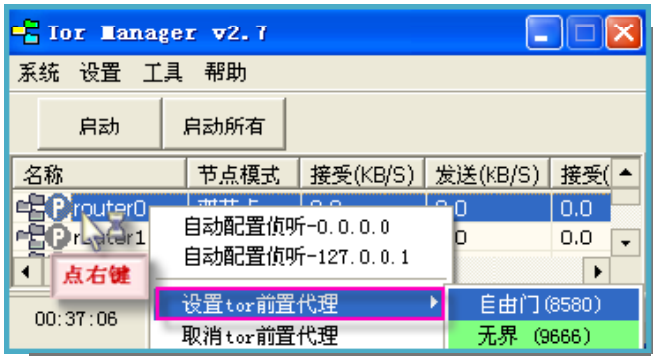
http://www.bannedbook.org/forum23/topic3150.html

二、简要流程图


启动 TorManager 2.7
配置侦听区域
设置前置代理
启动链路
浏览器代理设置
完成


tormanager2.7
App
Data
双击


Tor Manager v2.7
系统 设置 工具 帮助
启动
启动所有
名称
节点模式
接受(KB/S)
自动配置侦听-0.0.0.0
自动配置侦听-127.0.0.1
点右键


Tor Manager v2.7
系统 设置 工具 帮助
启动
启动所有
名称
节点模式
接受(KB/S)
发送(KB/S)
自动配置侦听-0.0.0.0
自动配置侦听-127.0.0.1
点右键
设置tor前置代理
取消tor前置代理
00:37:06


Tor Manager v2.7
系统 设置 工具 帮助
启动
启动所有
名称
节点模式
点击


书签(B) 工具(T) 帮助(H)
Tor2.7 Router0
http://www.google.com/
Gmail 更多
Google
简体中文

（返回目录）

三、设置 TorManager2.7

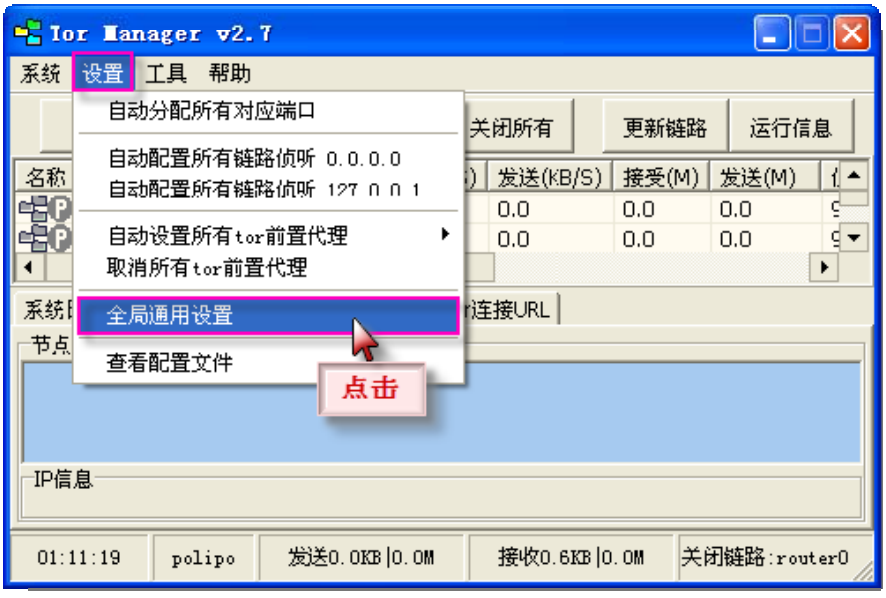
1 启动 TorManager2.7

首先将下载的压缩文件解压到文件夹中，然后双击 **tormanager.exe** 启动 TorManager2.7：

（返回目录）（返回简要流程图）

2 增加链路

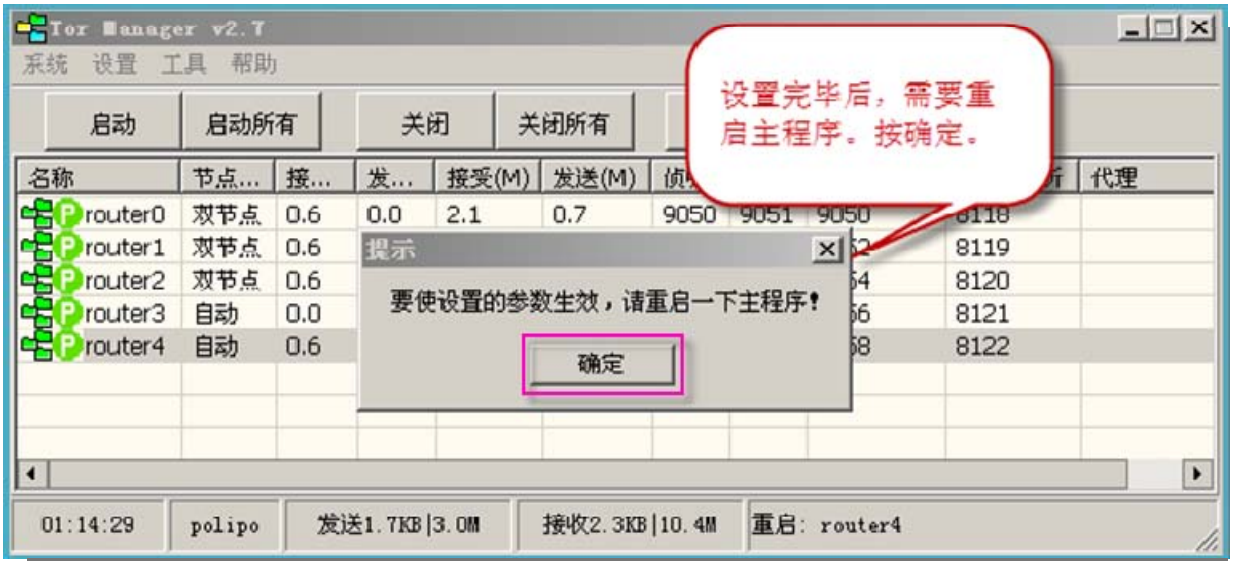
2.1 TorManager2.7 默认的是两个链路，因为不同的链路有不同的监听端口，这样可以利用不同的链路作不同的浏览器或软件的代理。在**设置 － 全局通用设置**可增加链路：



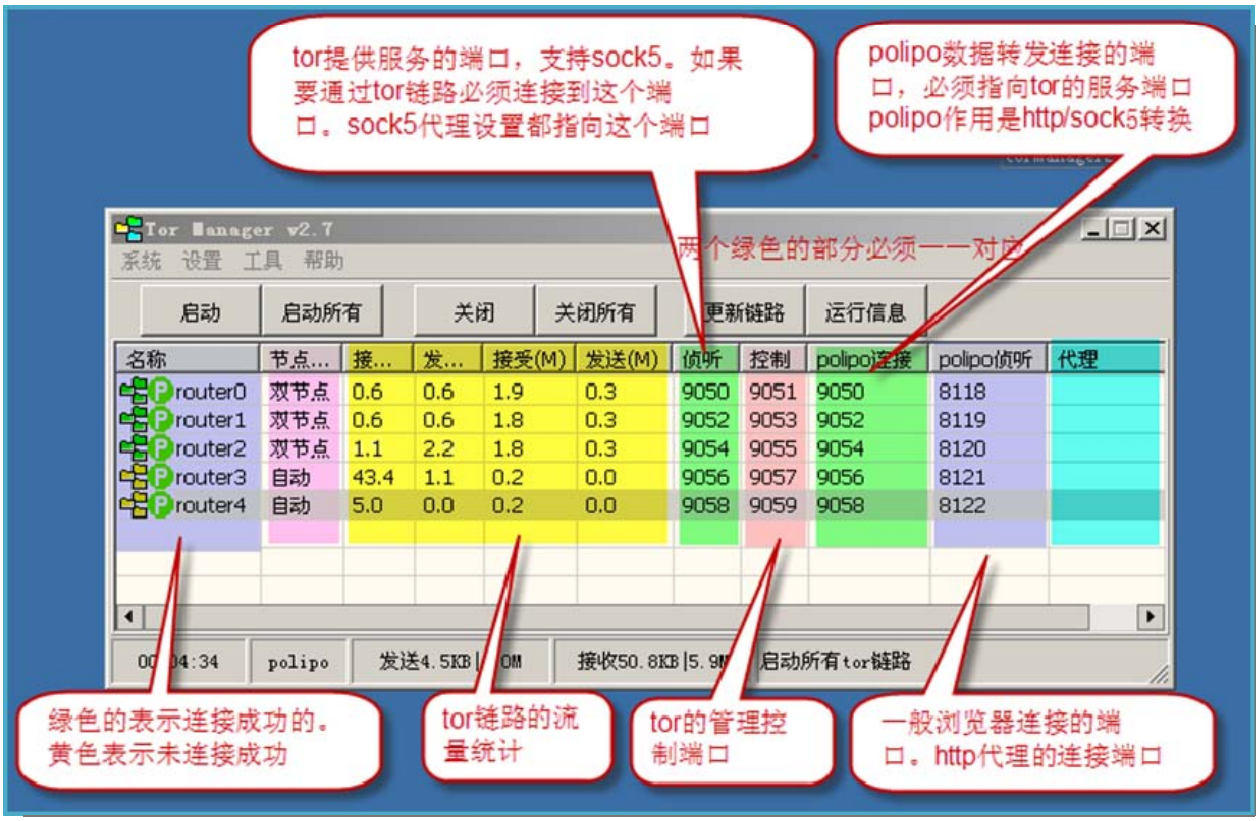
2.2 点击**代理组合个数**旁的小箭头，选择需求的链路数即可，其余默认，点**确定**。

说明：代理组合个数是指同时工作的链路的数量。可以根据需要选择**启动所有**。每个组合出的代理链路分别有一个不同的端口，可以分配给不同的程序做代理使用。

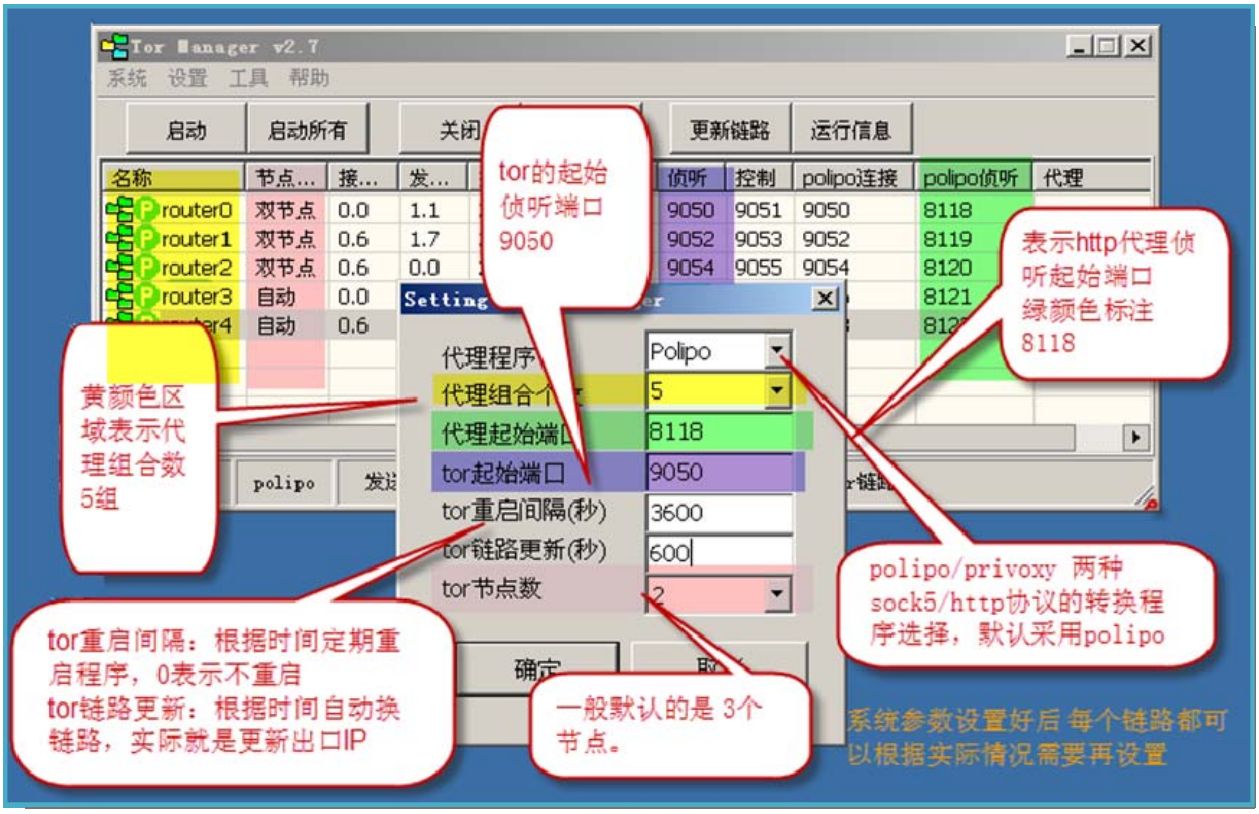
2.3 设置完成后点**确定**，点标题栏中**系统 — 退出**，再从新启动 **tormanager.exe**：



2.4 从新启动后如下图，以下是一些对应项目的说明：



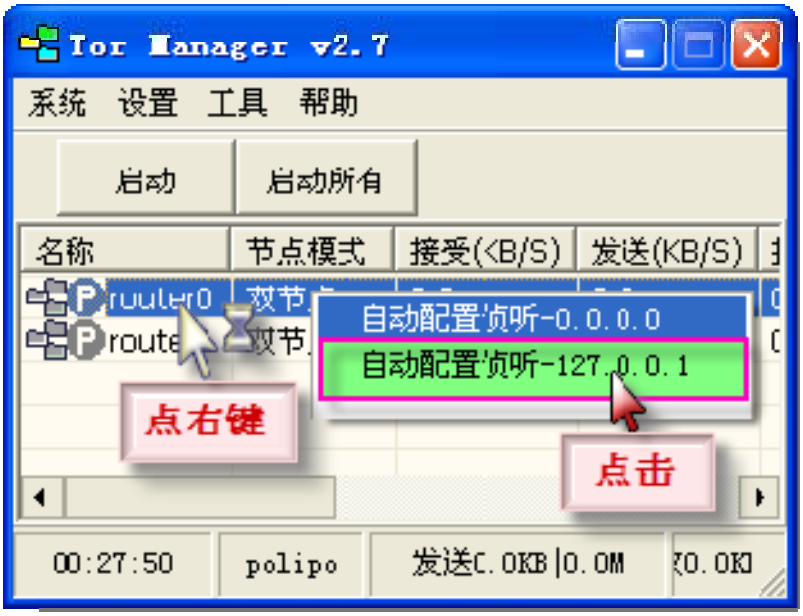
2.5 全局设置与设置完成后的对应关系与说明：



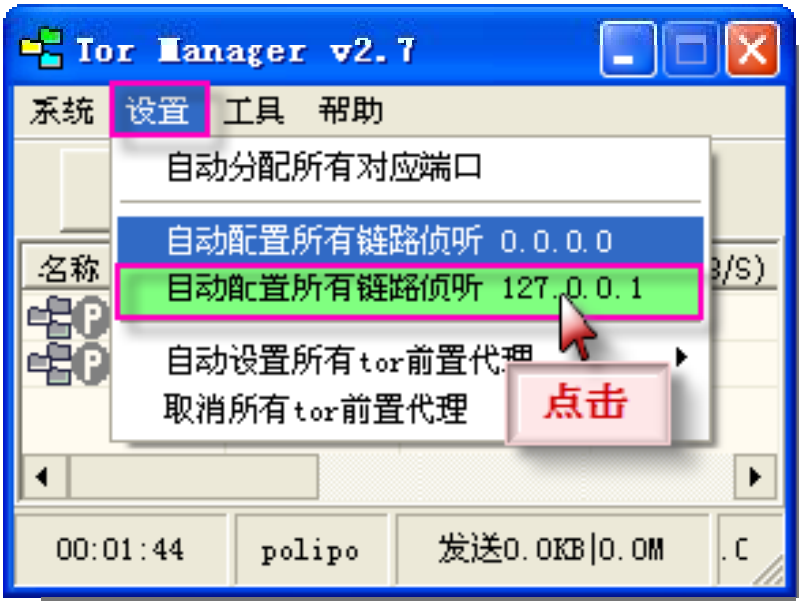
（返回目录）

3 配置侦听区域

3.1 如果只用 Tor 代理主机上的浏览器或软件，选择链路点右键，选**自动配置侦听－127.0.0.1**；如果 Tor 同时代理主机与虚拟机，则选**自动配置侦听－0.0.0.0**。
提示：通常无需设置，默认就是 127.0.0.1，即代理主机。



3.2 如果想将所有链路均设成相同的侦听区域，则在**设置**中选择**自动配置侦听－127.0.0.1** 或**自动配置侦听－0.0.0.0**：



（返回目录）（返回简要流程图）

4 设置前置代理

由于 Tor 被封锁，通常需要设置前置代理才能联网，而且使用安全的前置代理可以对进入 Tor 链路的用户数据也起到保护作用。以下列举几种设置前置代理的方法：

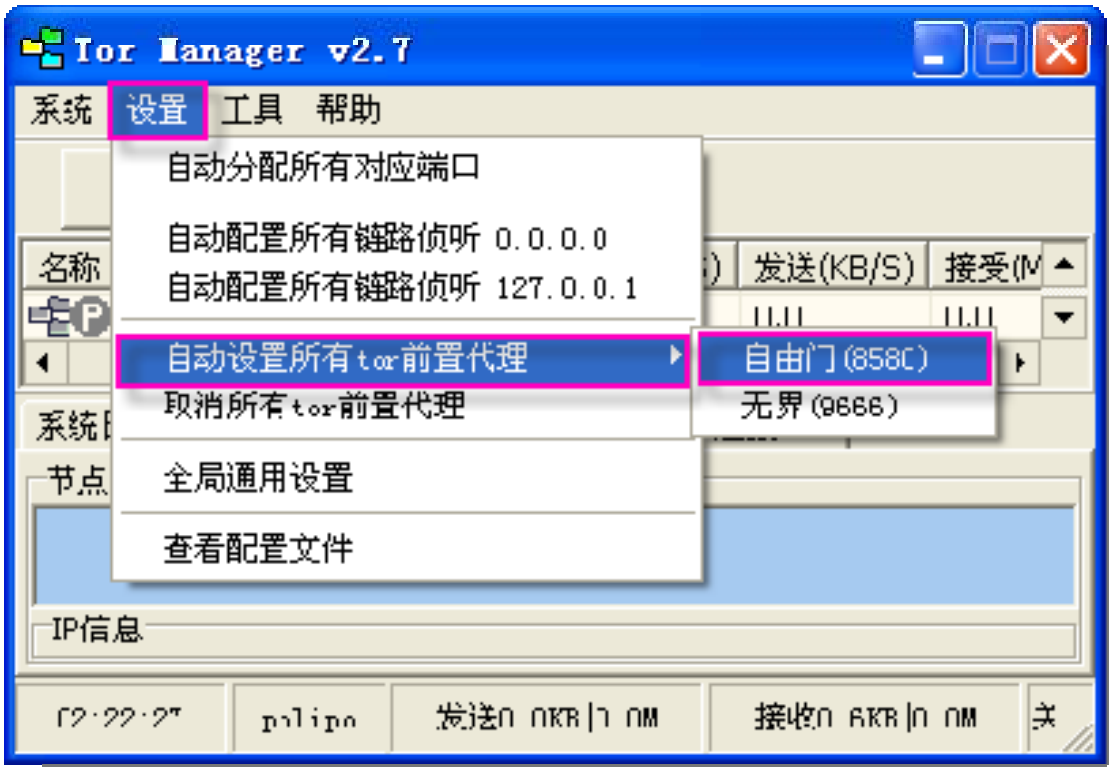
重要说明：

- Tor 的一个潜在隐患是陷阱节点，陷阱节点在中间时不起作用，因为 Tor 网络中流动的是加密数据。但陷阱节点在入口或出口处时会有隐患。为防止陷阱节点在入口处带来的不安全因素，前置代理一定使用软件内置的代理（自由门、无界等）。

4.1 使用 TorManager2.7 内置的两种前置代理：

自由门（8580）：适用软件：自由门、逍遥游。
无界（9666）：适用软件：无界浏览。

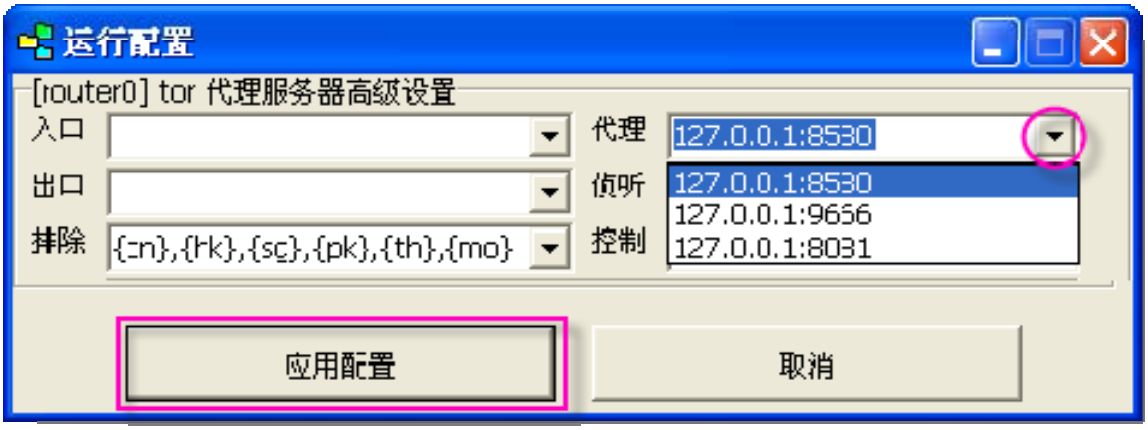
4.1.1 如果所有链路设置成相同的前置代理，可在标题栏**设置 — 自动设置所有 tor 前置代理 — 选自由门（8580）或无界（9666）**：



4.1.2 如果对一个链路设置前置代理，可以点选该链路、点右键，选**设置 tor 前置代理 — 自由门（8580）**或**无界（9666）**：

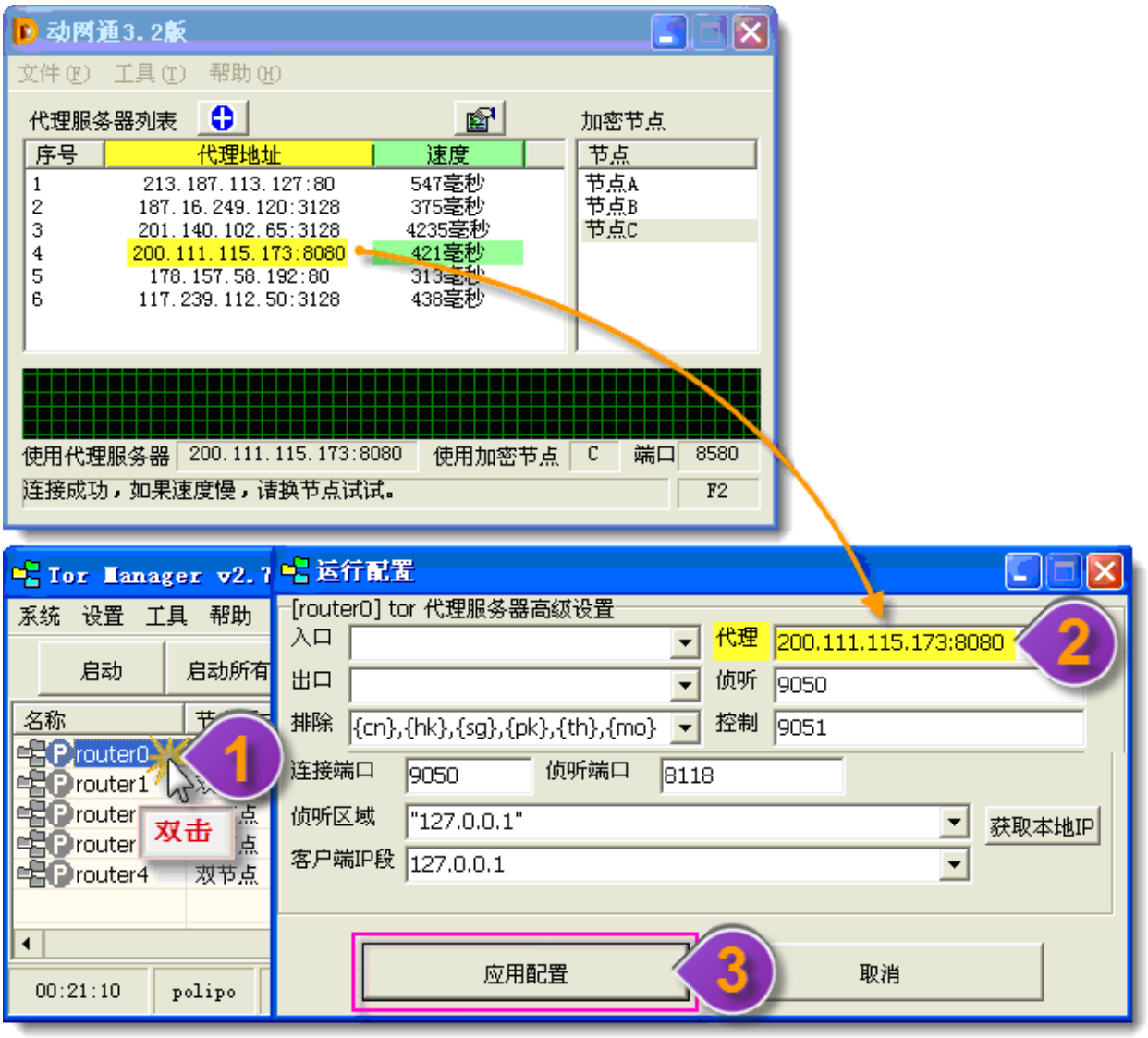
4.2 **方法二**：手动设置前置代理

4.2.1 双击一条链路后在**代理**位置点小箭头会有三个选项，如果是用**自由门、逍遥游**破网软件作代理，选第一行；用**无界浏览**作代理，选第二行；用**花园软件**作代理，选第三行。如果有其它代理按此类似格式手动填写即可。



4.2.2 有时**自由门**、**无界**破网困难，可利用**动网通**页面上显示的代理作为 TorManager2.7 的前置代理。先启动**动网通**；联通后，将页面显示的代理输入到图示位置：

（1） 双击一条链路；
（2） 选择一个动网通的**代理地址**填写到 TorManager2.7 **代理**的位置。**注**：可以参考动网通上的**速度**，不过速度快的做代理不一定就快，可多试几个；
（3） 点**应用配置**即可。



提示：

（1） **利用动网通的代理 IP 做 Tor 的前置代理目前是个非常有效、简单的方法，但是由于动网通利用的是公共资源，安全性不如自由门、无界浏览软件；**
（2） 同理，可用异次元代理作为 Tor 的前置代理；也可找一些免费或少量费用的海外 SSH 代理来做 Tor 的前置代理。

注意：以上两种方法由于代理服务器的安全未知，只能用于一般破网，更重要的工作最好用自由门、无界做前置代理。

4.2.3 **说明：**

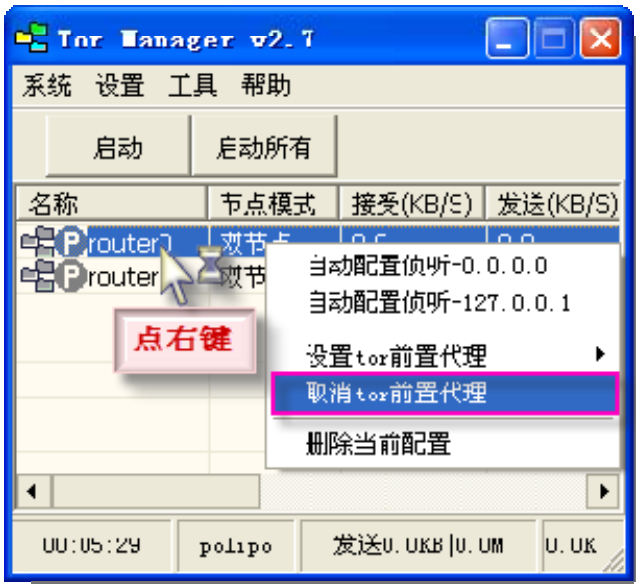
a. 选用前置代理的话，请先运行该代理软件。比如先运行自由门软件联网成功后，按以上设置自由门做**代理**，再启动 TorManager2.7 的链路；

b. 一般Tor的节点数选 3 才起到链路内部节点变换作用。现在大陆Tor不经代理无法直接联网，如果使用自由门、无界浏览做前置代理，有安全的加密保护可选**双节点**；**注意：如果使用其它前置代理，比如海外社会资源SSH代理，要选“自动”；且该服务器知道使用者的真实IP，需谨慎使用。请参考Tor原理说明。**

c. 本软件有**取消tor前置代理**的选项，**注意：为了安全，不要取消前置代理。**

d. Tor 经常成功运行的话，以后就更容易连接。

禁书网 大陆直连 https://goo.gl/C6xxGf 看 禁书禁闻禁文禁网禁片禁歌禁曲



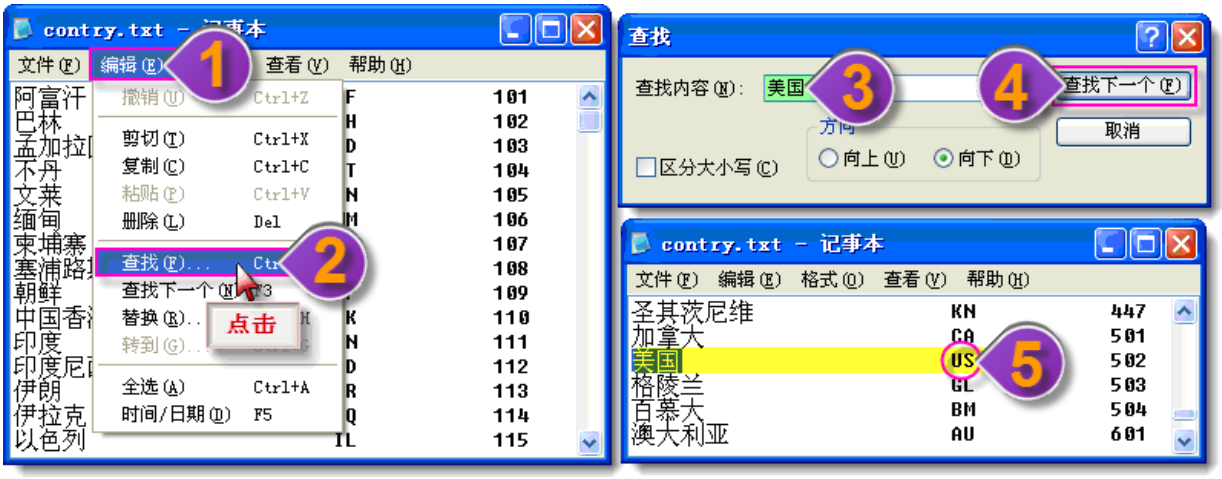
（返回目录）（返回简要流程图）

5 按国别设置出口

5.1 **国别代码**可在**工具** — **国别代码**中查询：

5.2 **国别代码**文件自动打开后：

（1）点**编辑**；（2）点**查找**；（3）输入查找内容，比如美国；（4）点**查找下一个**；（5）对应美国的 **US** 即为**国别代码**：



5.3 双击一个链路，在**出口**处按图示方式将**国别代码**用{}括起来，多个**国别代码**用半角逗号（,）隔开；设置完成后点**应用配置**：

（返回目录）（返回简要流程图）

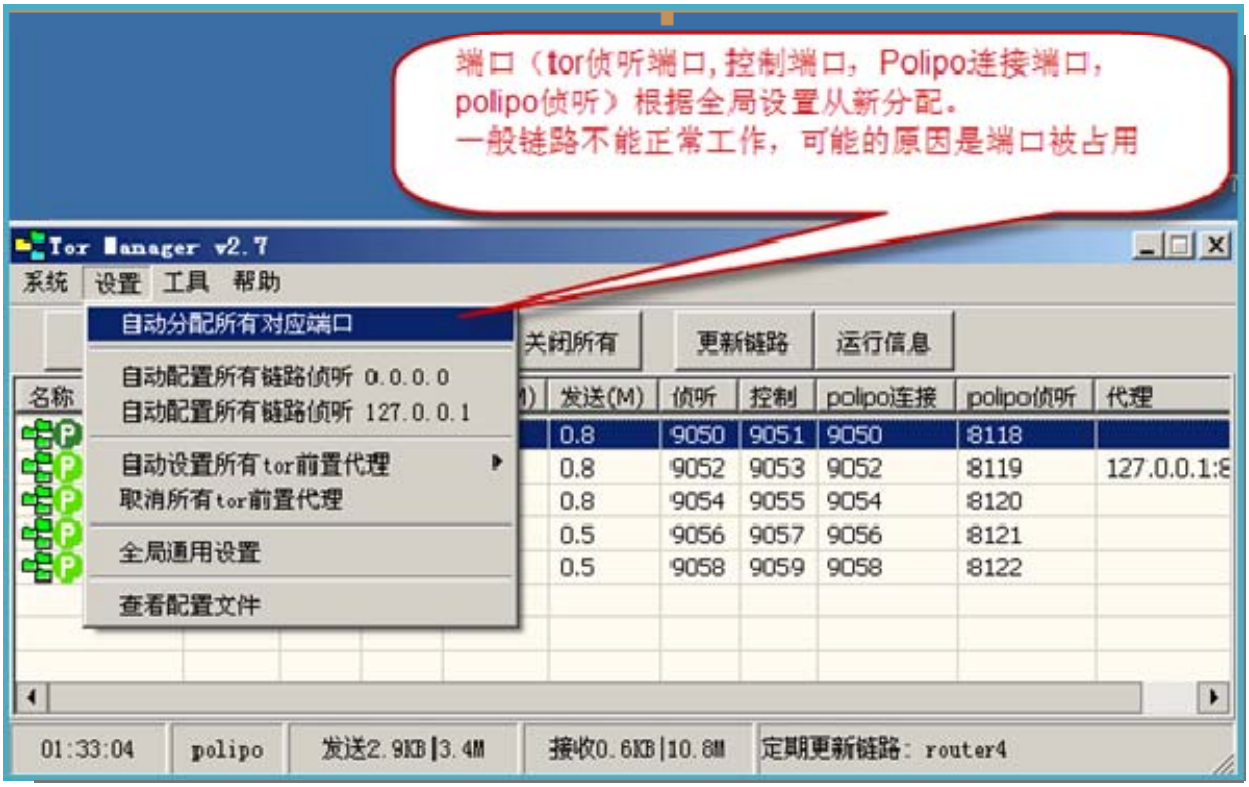
6 启动链路

6.1 前置代理与监听区域设置好之后，可以启动链路了：

（1） 点击一条链路，比如 router0；
（2） 点击**启动**；
（3） 再点击**运行信息**；
（4） 点 **Tor 日志**页签；
（5） 看到有类似 Bootstrapped 10%~20%这样的数字一直增长；
（6） 直到出现 **Bootstrapped 100%：Done** 说明链路已启动；
（7） 此时观察链路的标识为全绿色，说明可以通过此链路作代理上网了：

（返回目录）（返回简要流程图）

7 自动分配所有对应端口



（返回目录）（返回简要流程图）

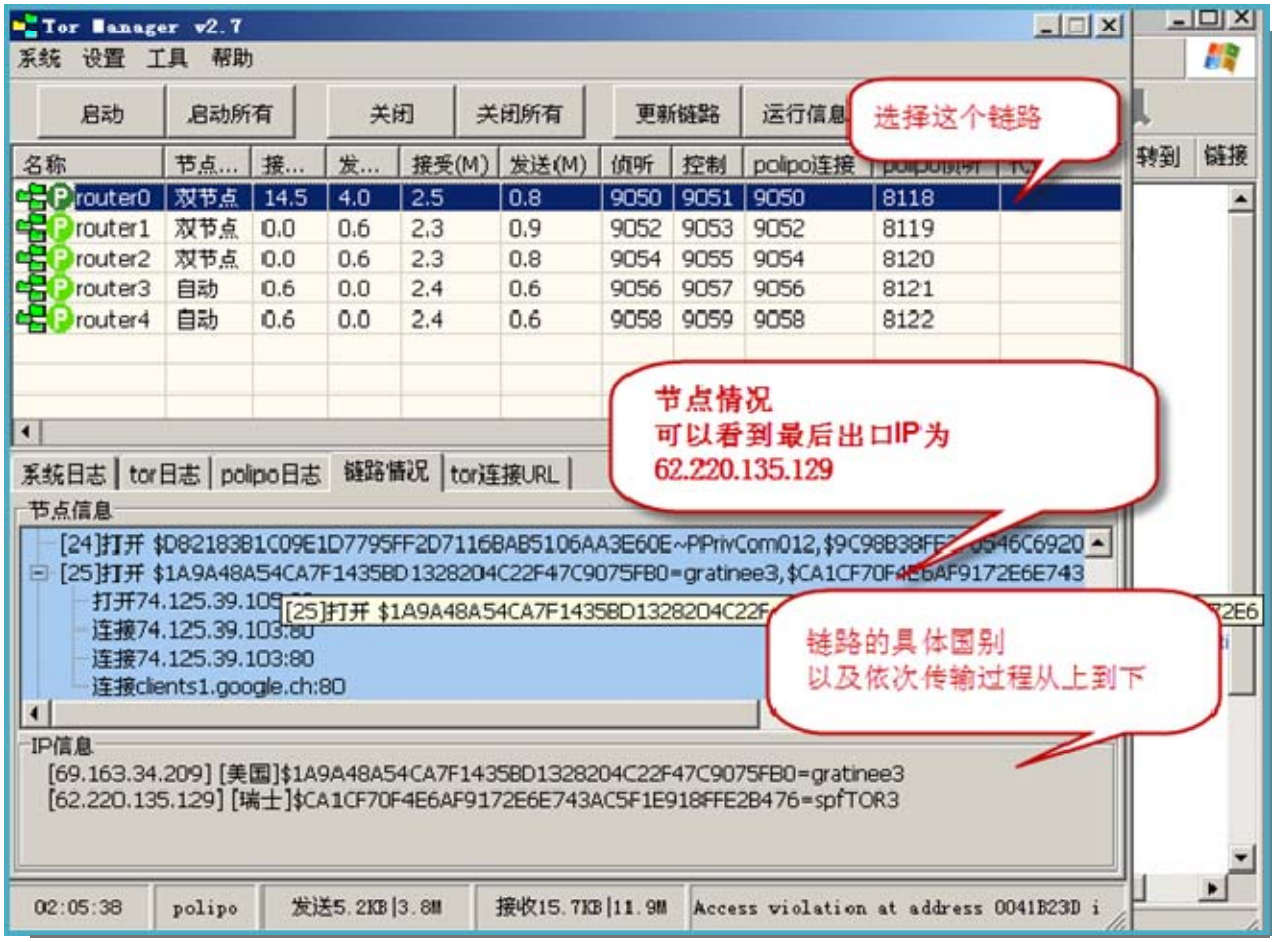
8 部份运行信息说明

8.1 系统日志：

8.2 Tor 日志：


Tor Manager v2.7
系统 设置 工具 帮助
启动
启动所有
关闭
关闭所有
更新链路
运行信息
名称
节点...
接受(M)
发送(M)
侦听
控制
polipo连接
polipo侦听
3. 启动
2关闭
1选择这个线路
router2 双节点 0.0 0.6 2.3 0.8 9054 9055 9054 8120
router3 自动 0.6 0.0 2.4 0.6 9056 9057 9056 8121
router4 自动 0.6 0.0 2.4 0.6 9058 9059 9058 8122
系统日志
tor日志
polipo日志
链路情况
tor连接URL
tor的输出日志。有可能看不到。
操作步骤： 根据上面1，2，3步骤。
双击情况日志
Nov 08 15:31:43.171 [notice] We now have enough directory information to build circuits.
Nov 08 15:31:43.171 [notice] Bootstrapped 80%: Connecting to the Tor network.
Nov 08 15:31:43.171 [notice] New control connection opened.
Nov 08 15:31:45.171 [notice] Bootstrapped 85%: Finishing handshake with first hop.
02:09:57
polipo
发送1.7KB|3.8M
接收1.7KB|11.9M
启动链路: router0

8.3 链路情况：


Tor Manager v2.7
系统 设置 工具 帮助
启动 启动所有 关闭 关闭所有 更新链路 运行信息
选择这个链路
名称 节点... 接... 发... 接受(M) 发送(M) 侦听 控制 polipo连接
router0 双节点 14.5 4.0 2.5 0.8 9050 9051 9050 8118
router1 双节点 0.0 0.6 2.3 0.9 9052 9053 9052 8119
router2 双节点 0.0 0.6 2.3 0.8 9054 9055 9054 8120
router3 自动 0.6 0.0 2.4 0.6 9056 9057 9056 8121
router4 自动 0.6 0.0 2.4 0.6 9058 9059 9058 8122
节点情况
可以看到最后出口IP为
62.220.135.129
系统日志 tor日志 polipo日志 链路情况 tor连接URL
节点信息
[24]打开 $D82183B1C09E1D7795FF2D7116BAB5106AA3E60E~PPrivCom012,$9C98B38FF
[25]打开 $1A9A48A54CA7F1435BD1328204C22F47C9075FB0=gratinee3,$CA1CF70F4E6AF9172E6E743
打开74.125.39.105
连接74.125.39.103:80
连接74.125.39.103:80
连接clients1.google.ch:80
链路的具体国别
以及依次传输过程从上到下
IP信息
[69.163.34.209] [美国]$1A9A48A54CA7F1435BD1328204C22F47C9075FB0=gratinee3
[62.220.135.129] [瑞士]$CA1CF70F4E6AF9172E6E743AC5F1E918FFE2B476=spfTOR3
02:05:38 polipo 发送5.2KB|3.8M 接收15.7KB|11.9M Access violation at address 0041B23D i
转到 链接

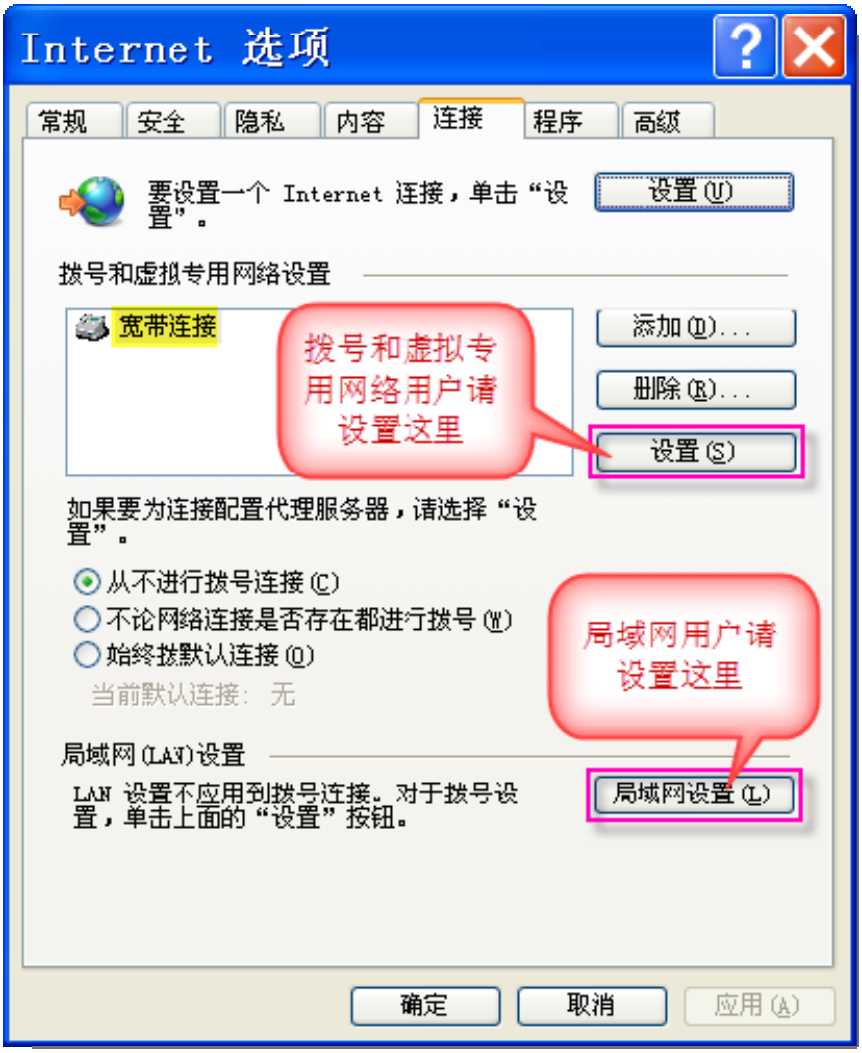
8.4 Tor 连接 URL：

（返回目录）（返回简要流程图）

四、浏览器代理服务器的设置与上网

1 IE 的代理服务器设置

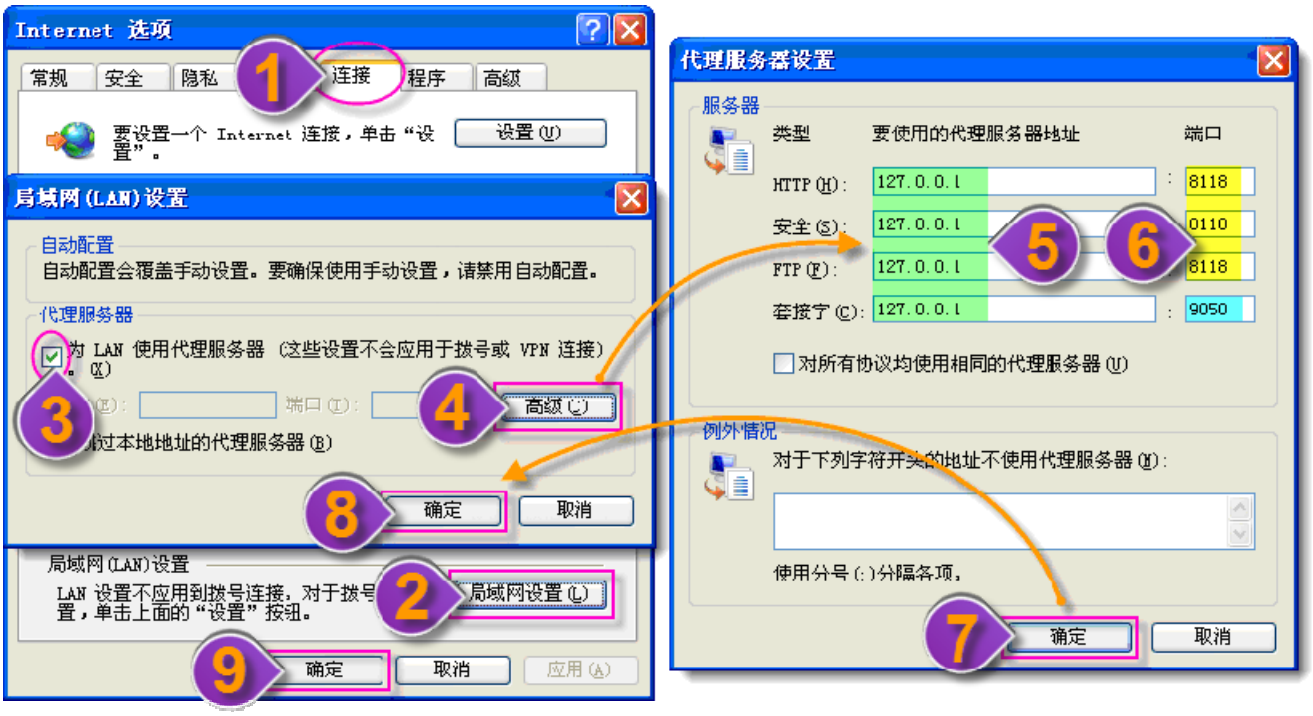
说明：不同网络用户在 IE 设置的位置不同，以下将详述两种设置方法：



1.1 局域网或经路由器网络的代理服务器设置

在 IE 的**工具** — **Internet 选项**中：

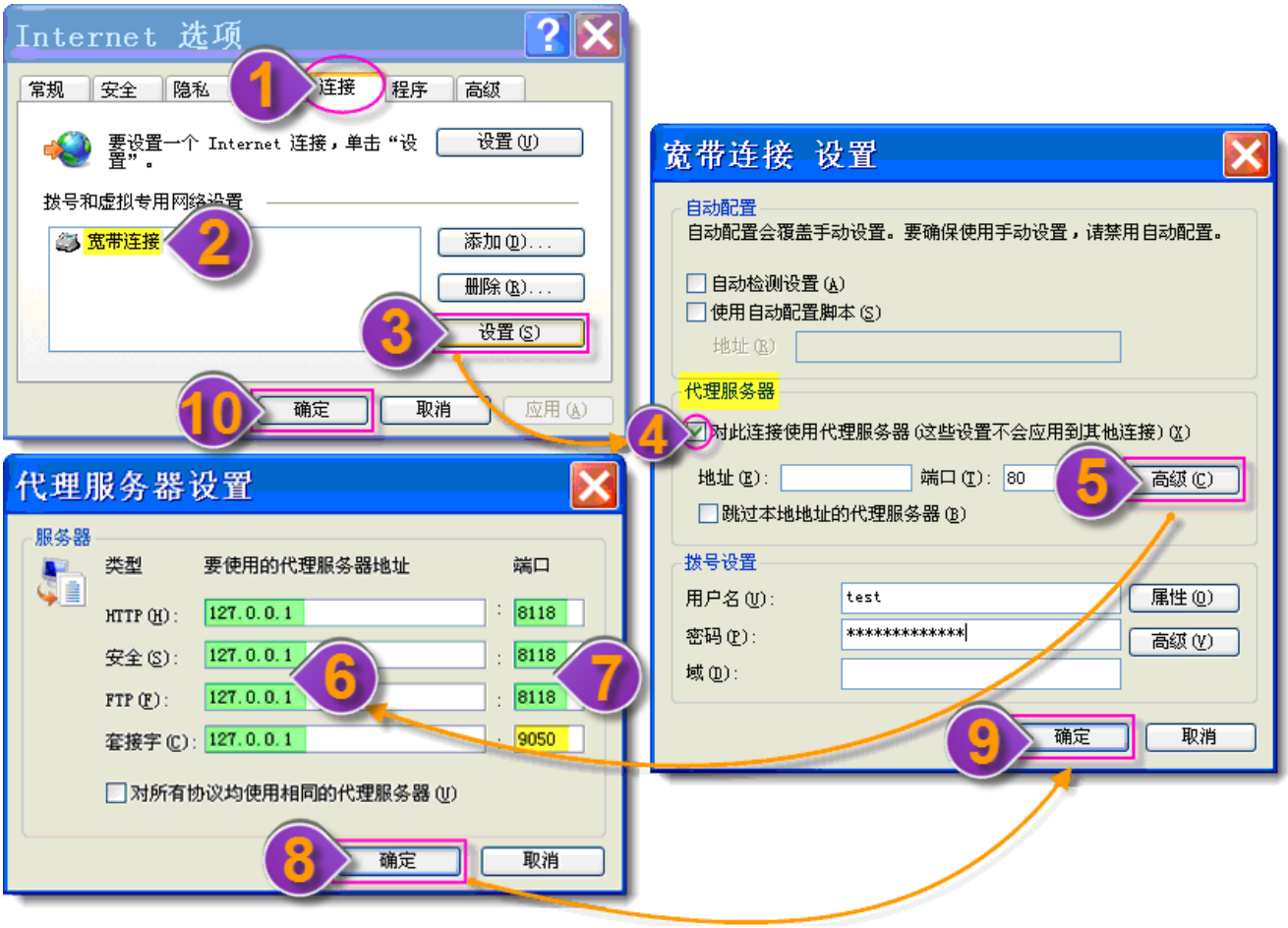
（1）点**连接**页签；
（2）点**局域网设置**；
（3）勾选**为 LAN 使用代理服务器**；
（4）点**高级**；
（5）**代理服务器地址**均填写 127.0.0.1；
（6）**端口**需与链路 polipo 代理服务器侦听端口相同，通常是 8118/8119 递增；套接字与 Tor 代理服务器侦听端口对应，通常是 9050/9052 双数递增。
（7）点**确定**；
（8）点**确定**；
（9）点**确定**；



1.2 拨号或虚拟专用网络的代理服务器设置

在 IE 的**工具** — **Internet 选项**中：

（1）点**连接**页签；
（2）点选一个拨号链接，这里以名为“宽带连接”的为例；
（3）点**设置**；
（4）勾选**对此连接使用代理服务器**；
（5）点**高级**；
（6）**要使用的代理服务器地址**均填写 127.0.0.1；
（7）**端口**需与链路 polipo 代理服务器侦听端口相同，通常是 8118/8119 递增；套接字与 Tor 代理服务器侦听端口对应，通常是 9050/9052 双数递增。
（8）点**确定**；
（9）点**确定**；
（10）点**确定**：



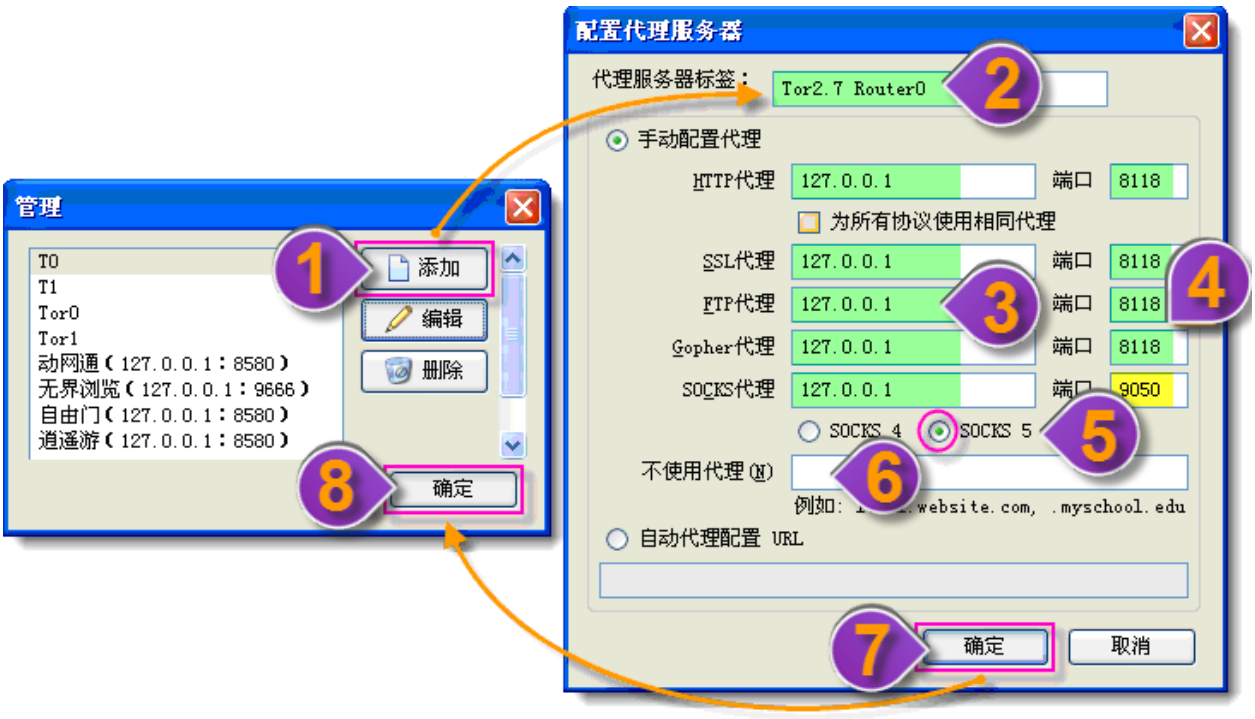
（返回目录）（返回简要流程图）

2 火狐(Firefox)的代理服务器设置

推荐使用FirefoxPortableESR 10.0.5 便携中文版，因为它可以很方便的更改代理服务器，下载地址：http://www.bannedbook.org/forum23/topic2390.html

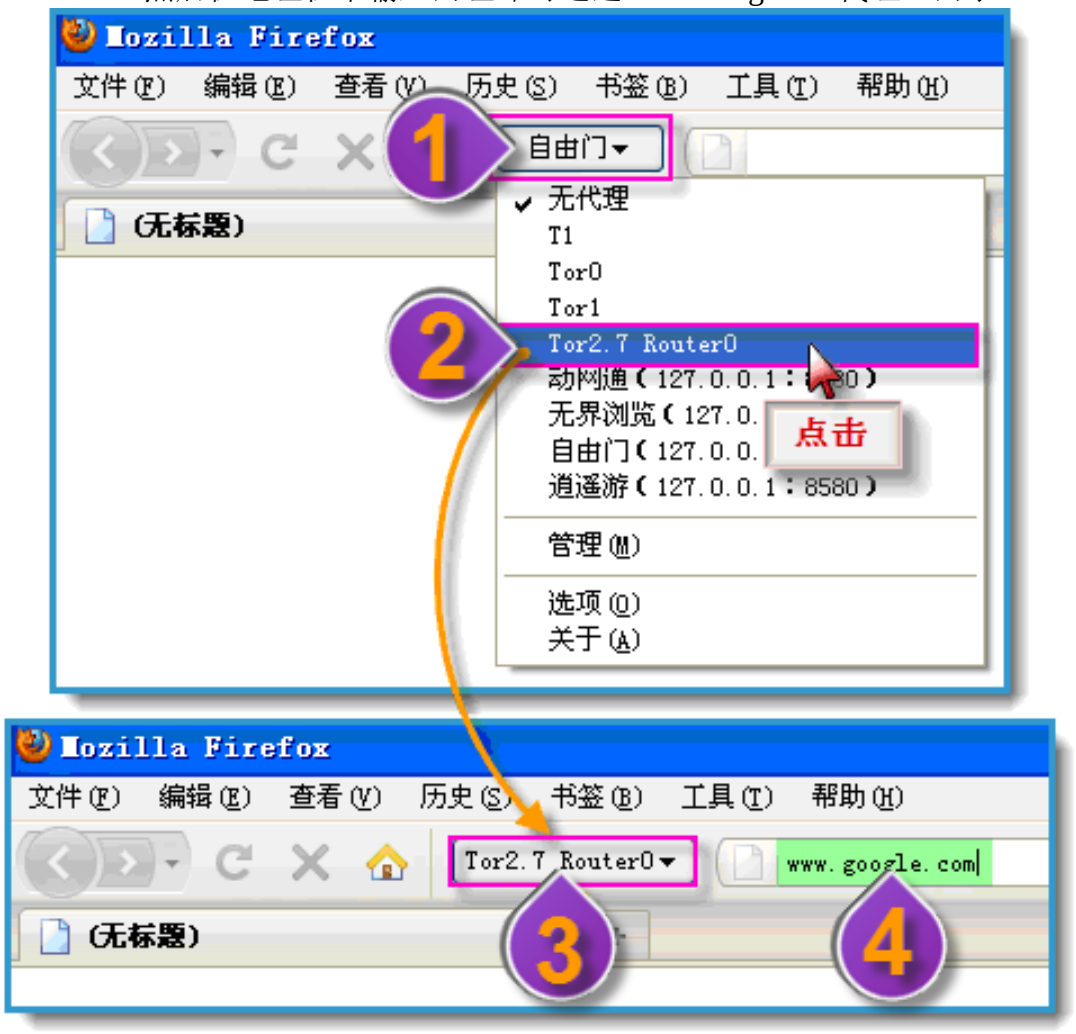
2.1 下面以 FirefoxPortableESR 10.0.5 便携中文版为例创建一个新的快捷代理。点**自由门**，在下拉菜单中点击**管理**：

（1） 点**添加**；
（2） 在**代理服务器标签**中写个易于记忆的名称（注意符号需用全角才能写上）；
（3） **手动配置代理**中的所有**代理**均填写 127.0.0.1；
（4） **端口**：除 SOCKS 代理的端口是 9050/9052 等按不同链路双数递增，其余代理端口是 8118/8119 按不同链路递增；
（5） 点选 **SOCKS5**；
（6） **不使用代理**清空；
（7） 点**确定**；
（8） 点**确定**：



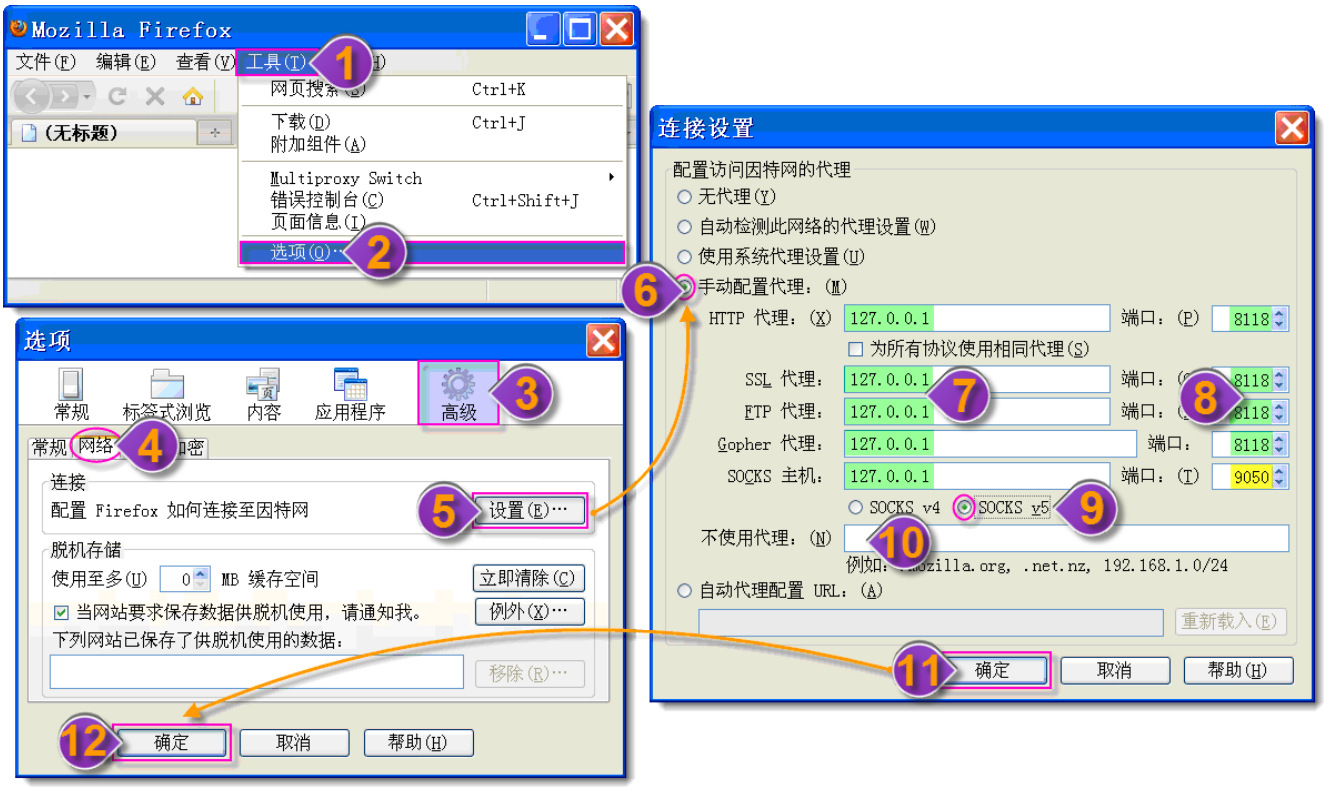
2.2 以上设置完成后：

（1）点开**自由门**；
（2）在下拉菜单找到刚才添加的代理 Tor2.7 Router0 点击；
（3）出现 Tor2.7 Router0 的标识，说明将由其代理上网；
（4） 然后在地址栏中输入网址即可通过 TorManager2.7 代理上网了：



2.3 Firefox 的直接设置代理服务器的方法

（1） 在**工具**；
（2） 点**选项**；
（3） 点**高级**；
（4） 选择**网络**页签；
（5） 点**设置**；
（6） 点选**手动配置代理**；
（7） 所有**代理**均填写 127.0.0.1；
（8） **端口**：除 SOCKS 代理的端口是 9050/9052 等按不同链路双数递增，其余代理端口是 8118/8119 按不同链路递增；
（9） 点选 **SOCKS5**；
（10） **不使用代理**清空；
（11） 点**确定**；
（12） 点**确定**：



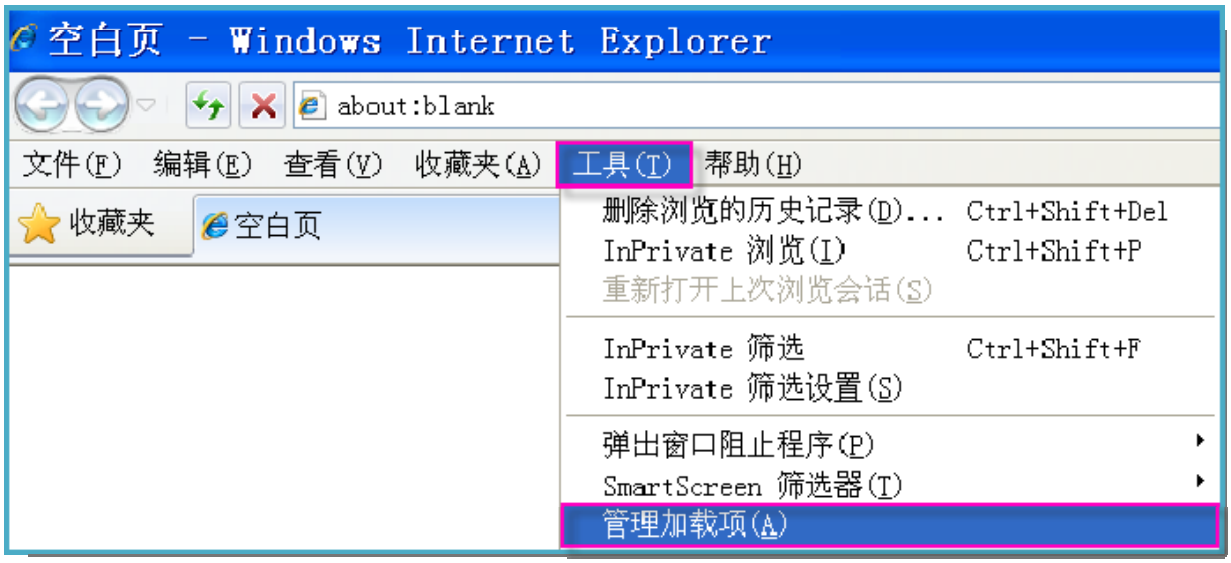
3 使用安全问题

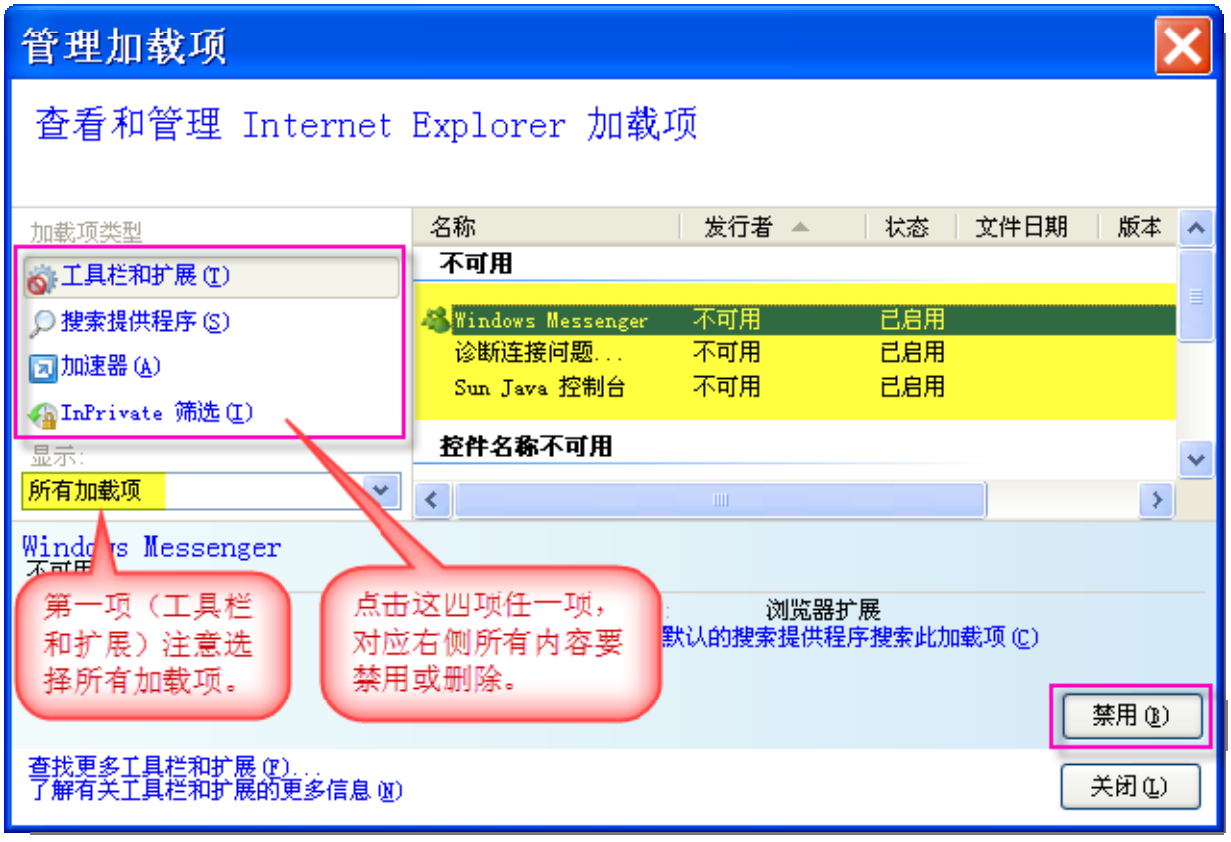
鉴于 Tor 安全的局限性，尽可能较少启用浏览器插件，并在使用浏览器前后清除现有 cookies。

IE 浏览器 cookies 和浏览痕迹建议使用无影无踪软件擦除。
Firefox 浏览器可以设置关闭时，自动删除 cookies,并删除浏览痕迹。

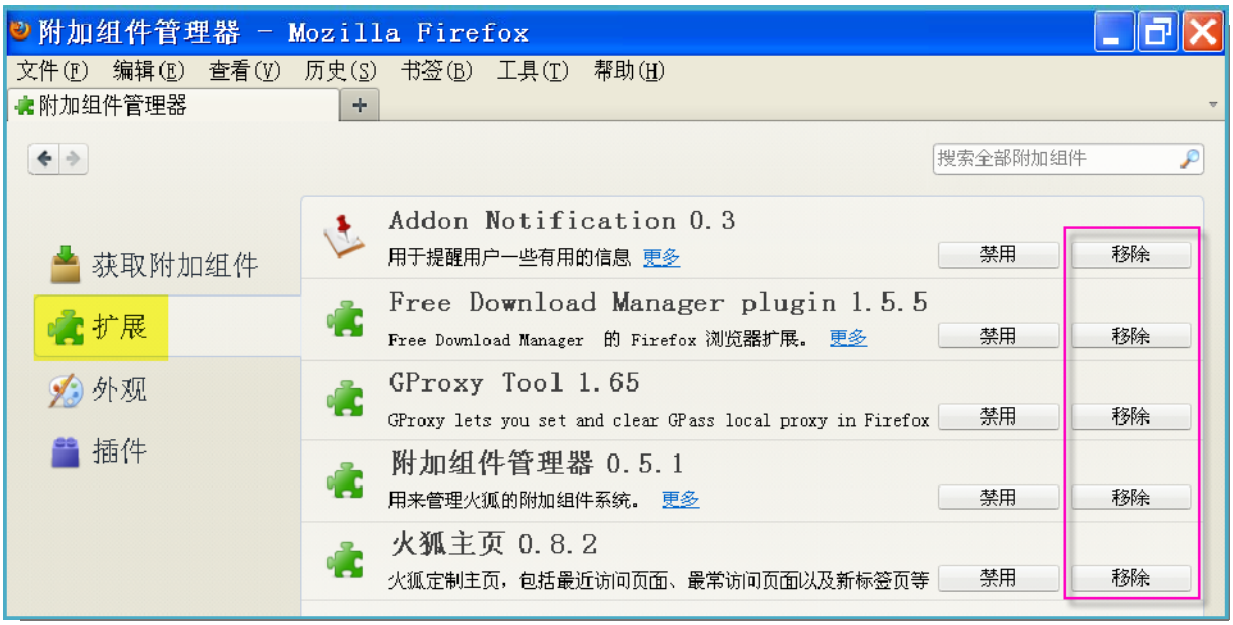
以下说明浏览器插件的处理方法：

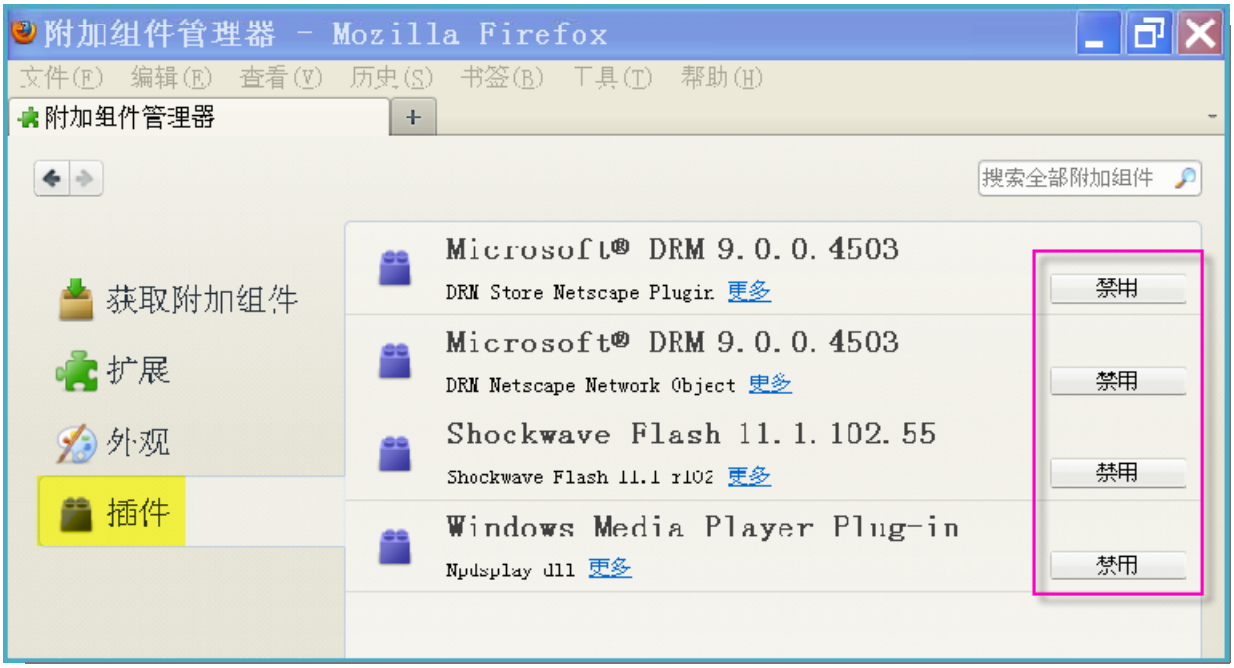
- **IE** ：在**工具** — **管理加载项**中，分别点左侧四个项目，把右侧出现的所有项，除必须使用的外，均禁用或删除。





- **Firefox**（火狐）：在**工具** — **附加组件**中，除了保留必须使用的外，将其余所有**扩展**移除，将所有**插件**禁用。



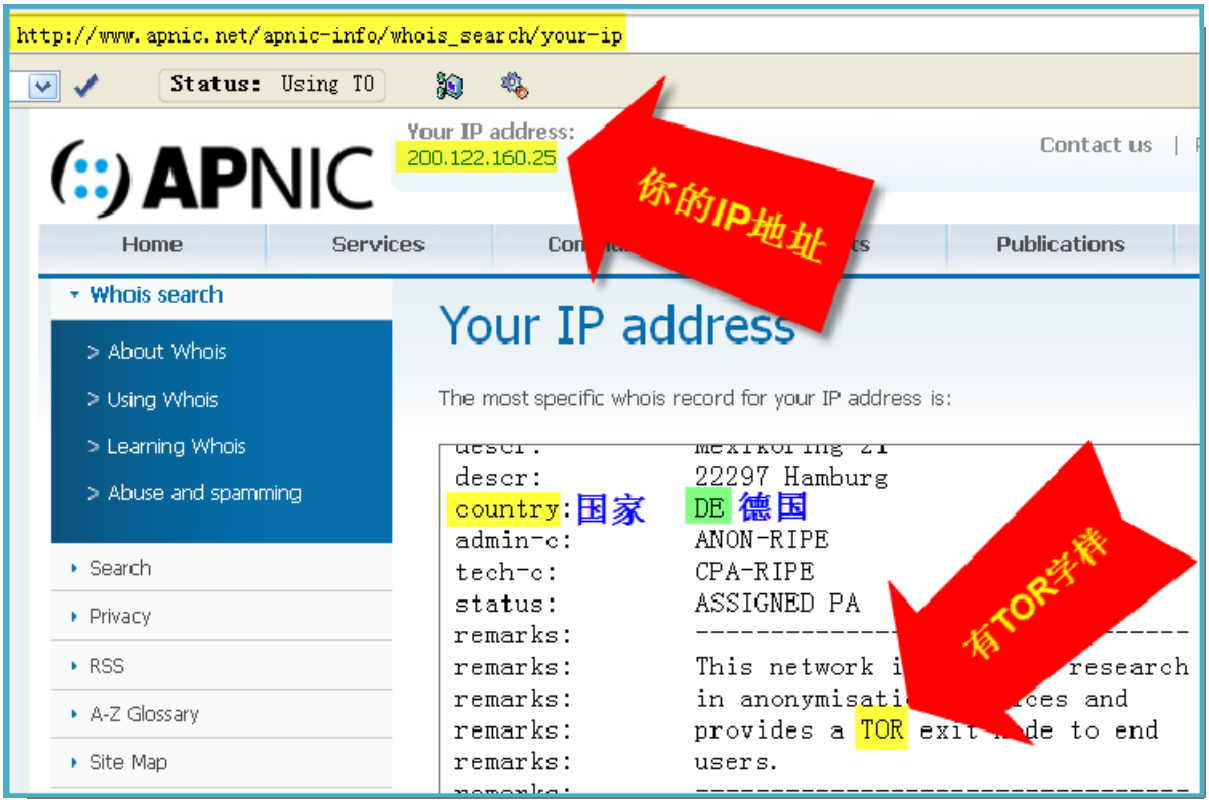


4 上网 IP 检测

上网前一般先确定是否使用了 tor 链路(tor 链路是匿名的),建议用海外的站点来检测。

第一步 在浏览器地址栏输入 http://apnic.net/apnic-info/whois_search/your-ip 回车：

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 DE 代表德国。说明此时的 IP 显示是来自德国，而非本地 IP；同时因使用 Tor 作为代理软件，通常会看到有 TOR 字样：



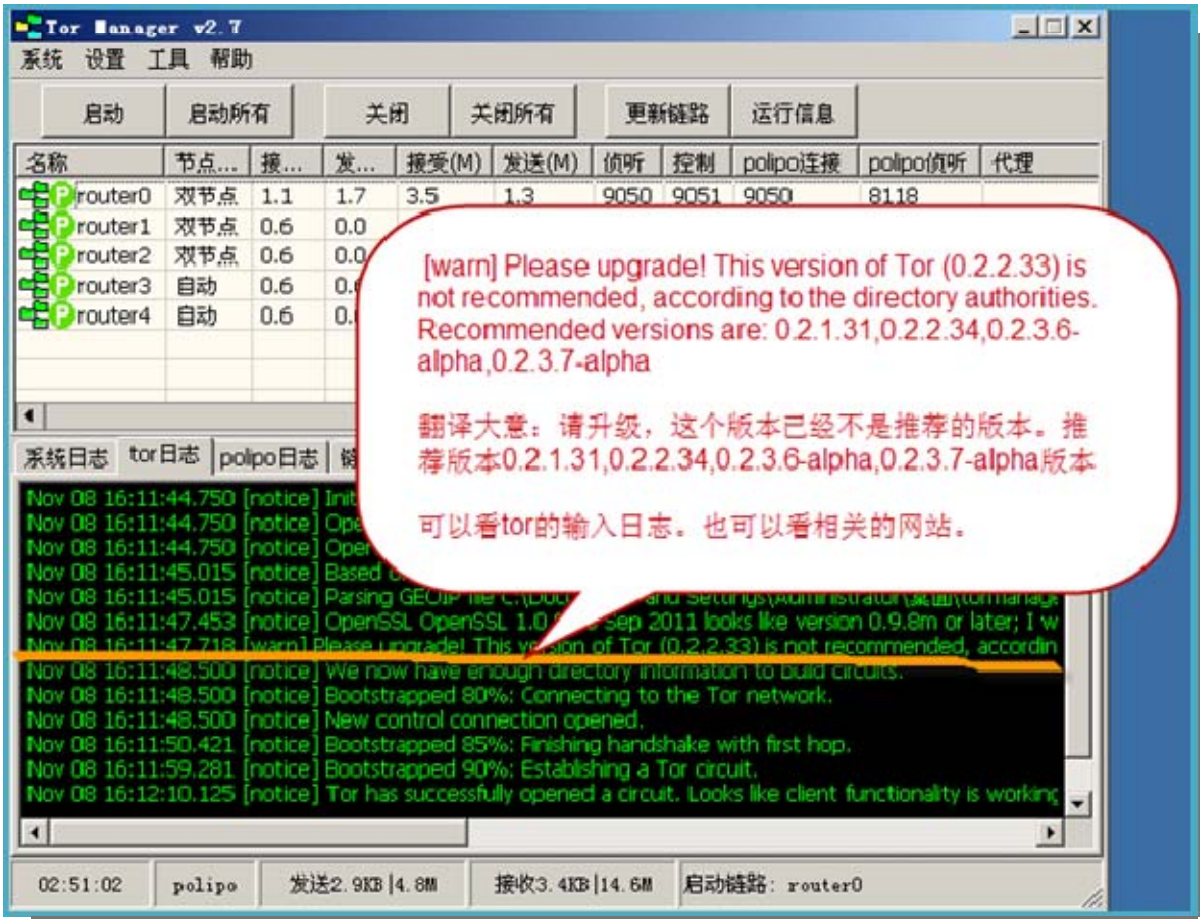
第二步 如果以上检测是海外地址，再登录以下链接检查是否经过 Tor：
https://check.torproject.org/?lang=zh_CN
出现绿色洋葱头说明目前在使用 Tor 作代理；未使用 Tor 会出现个红叉；两种情况均会显示目前检测到的 IP，粉框中是目前显示的代理 IP：

（返回目录）（返回简要流程图）

五、TorManager2.7 的更新

1 TorManager2.7 需更新的提示

如果在 tor 日志中出现以下提示，说明需更新 TorManager2.7 的文件；亦可去官网去查看是否有新版本：



说明：polipo 和 privoxy 是较有名的 http/sock5 转换软件。tor 已经把 polipo 作为内置专门协议转换软件，也就是有 tor 一般就有 polipo。根据用户自己的习惯选择使用。

内置的 privoxy 和论坛 TORPlusBundle 组合包里的同一组件一样，是采用官方版本。privoxy 可以到官方网站(www.privoxy.org)破网下载，只需更新主程序即可。不更新不影响使用，privoxy 在 tor 管理器中仅仅起到转发数据的作用。

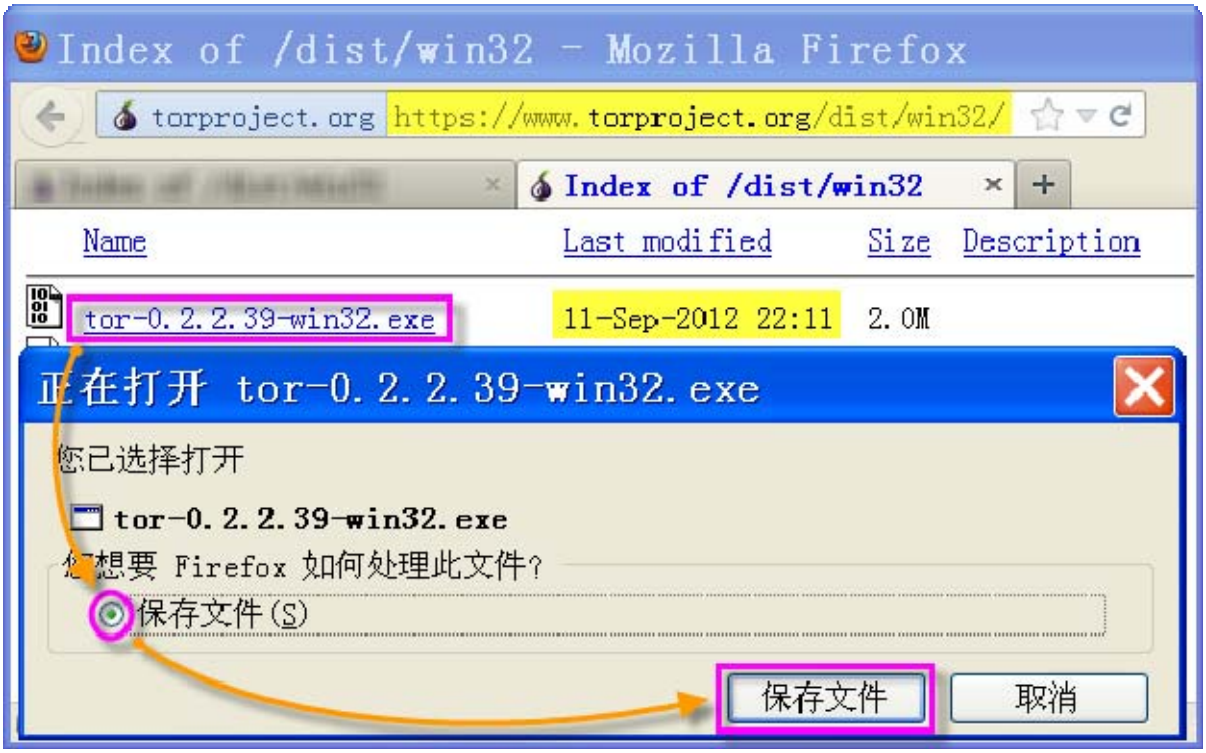
polipo 在官方版本的基础上去除了其本身做代理的功能，保障在虚拟机中或同一地点的其它机台用 Tor 管理器作服务器时使用 polipo 组件不会泄露真实 IP。因此，Tor 管理器的 polipo 不可更新。

Tor 管理器和论坛 TORPlusBundle 组合包的区别：前者使用官方 Tor，后者使用根据 Tor 的源代码修改后的 Tor。Tor 管理器可以随官方 Tor 更新，建议用户及时更新 Tor。下面介绍更新步骤。

2 从 Tor 官网下载更新与安装

2.1 下载

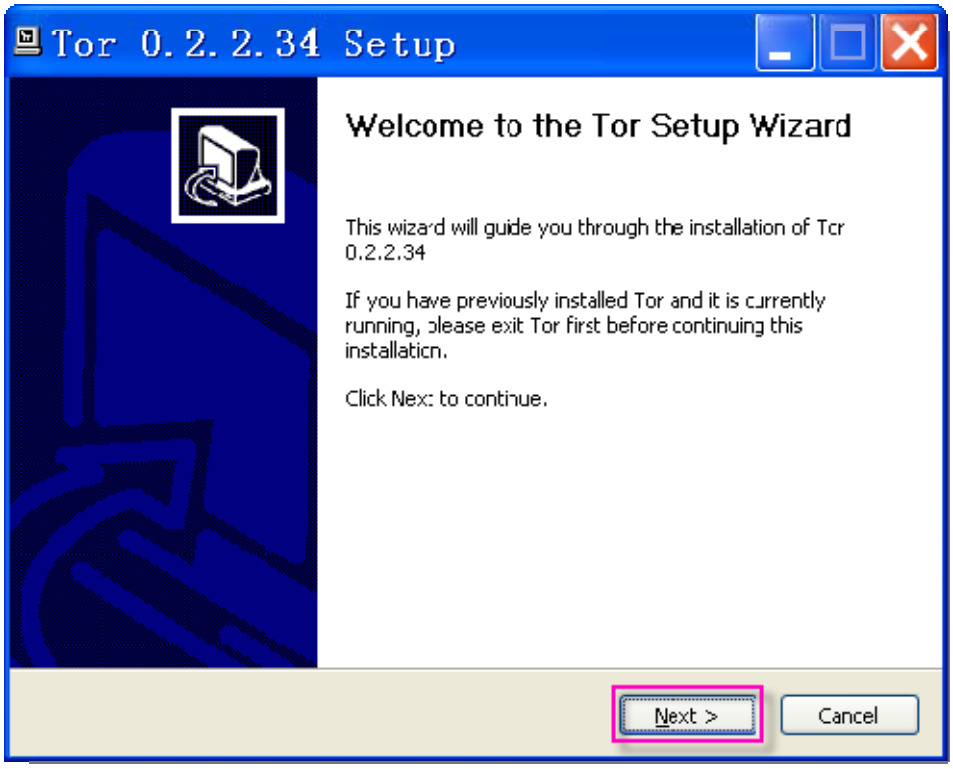
（1） 通过代理登录：**https://torproject.org/dist/win32/**
（2） 查看时间点击最新更新的 **tor-xxxxx-win32.exe** 文件；
（3） 点**保存文件**：



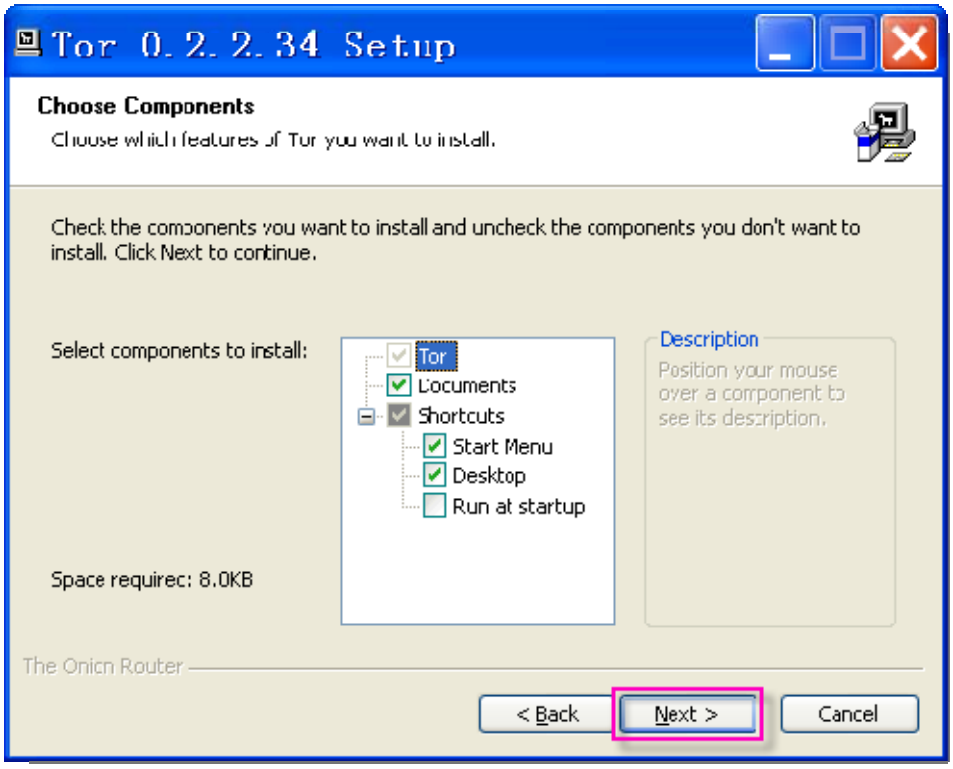
2.2 双击最新下载的文件。**注意**：（1）以下安装 Tor 步骤最好在虚拟机中进行；提取相应文件存盘后，可恢复虚拟机备份；如果是在主机安装，之后按教程卸载。（2）以下图片为示例，实际以双击的文件以下载的最新版本为准：

2.3 安装

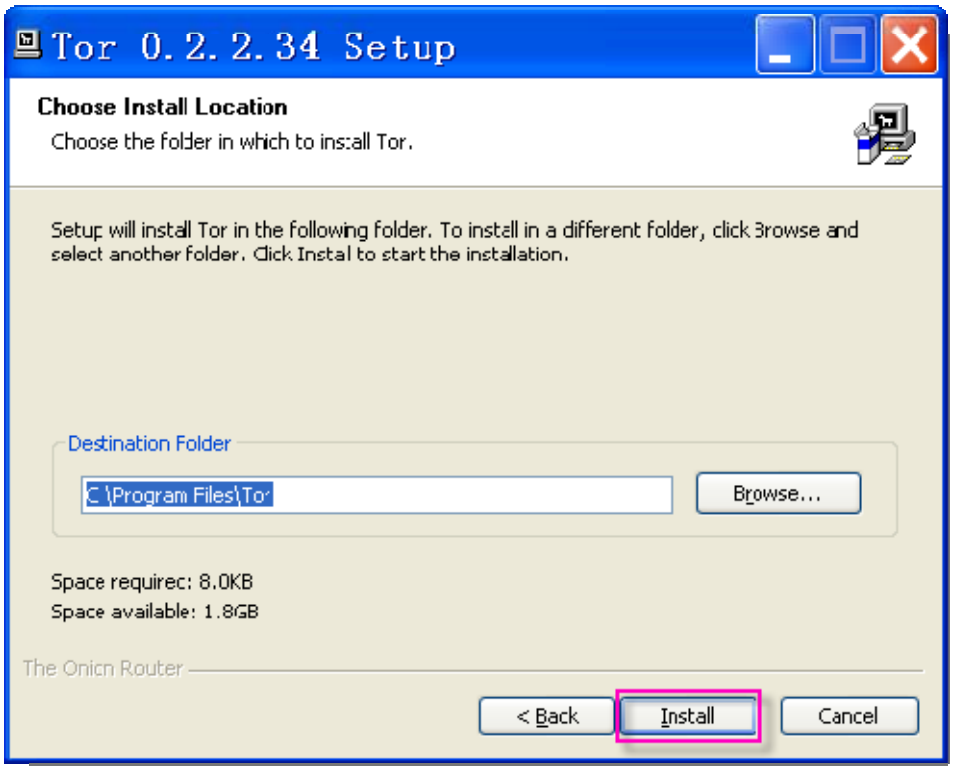
2.3.1 点 **Next**（下一步）：



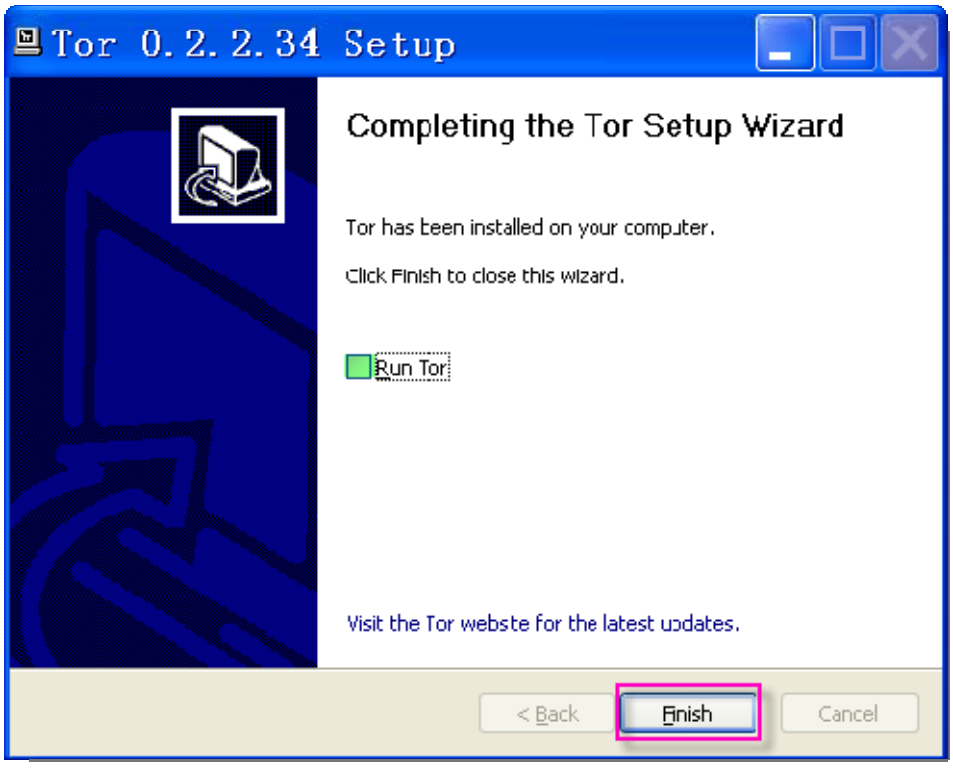
2.3.2 设置默认，点 **Next**（下一步）；



2.3.3 路径默认，点 **Install**（安装）：



2.3.4 去掉勾选，点 **Finish**（完成）：



3 提取并替换 tor.exe、tor-resolve.exe 及 geoip

3.1 提取 **tor.exe**、**tor-resolve.exe 和 geoip** 三个文件：

（1）**拷贝**下面三行斜体字内容；
（2）打开**记事本**，**粘贴**；
（3）在**文件 → 另存为**，文件名为 gettor.bat；
（4）**双击**运行 gettor.bat；
（5）之后会在当前目录出现 tor.exe、tor-resolve.exe 和 geoip 三个文件（如果在虚拟机中运行，要退出文件夹再从新打开文件夹才能看到这个三件文件）：

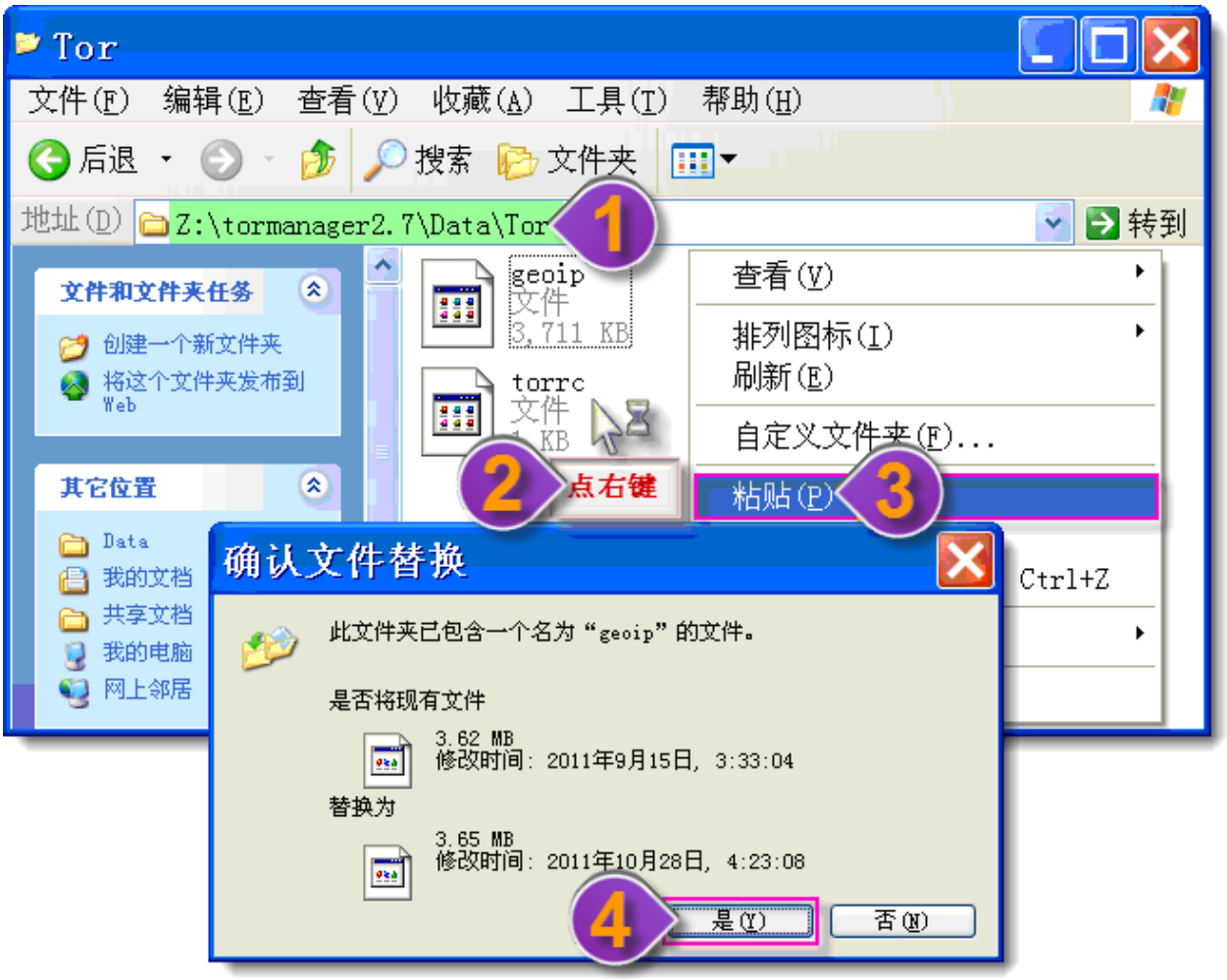
copy "%APPDATA%\Tor\geoip" geoip
copy "%ProgramFiles%\Tor\tor.exe" tor.exe
copy "%ProgramFiles%\Tor\tor-resolve.exe" tor-resolve.exe

3.2 在以上文件夹拷贝 **tor.exe**、**tor-resolve.exe**，替换 TorManager2.7 的 **tor.exe** 和 **tor-resolve.exe** 两个文件：

（1） **路径**：\tormanager2.7\App
（2） 在空白处**点右键**；（3）点**粘贴**；（4）点**是**；（5）点**是**：

3.3 在以上文件夹拷贝 **geoip**，替换 TorManager2.7 的 **geoip**

（1） **路径**：\tormanager2.7\Data\Tor
（2） 在空白处**点右键**；
（3） 点**粘贴**；（4）点**是**：



4 卸载为提取文件安装的 Tor 最新版本

（1）开始 — （2）所有程序 — （3）**Tor** — （4）**Uninstall**（卸载）

说明：如果是虚拟机可直接恢复快照。

5 单独更新 geoip

可以破网下载每月更新的 IP 库文件用批处理转换为 geoip 文件：

5.1 在以下链接下载 GeoIPCountryCSV.zip：
http://geolite.maxmind.com/download/geoip/database/GeoIPCountryCSV.zip

5.2 将下载的文件**解压缩**为 GeoIPCountryWhois.csv（**注意必须先解压缩**）。

5.3 **复制**下面的代码，打开**记事本**，**粘贴**并**另存为** geoip generater.bat：

```
@echo off
color 0a
title geoip 生成器
mode con: cols=60 lines=10
cls

echo 正在生成 geoip，请勿关闭此窗口...

if exist geoip del /a /f /q geoip
if not exist GeoIPCountryWhois.csv (
echo GeoIPCountryWhois.csv 不在当前目录!
pause
) else (
for /f "delims=, tokens=3-5" %%i in (GeoIPCountryWhois.csv) do echo %%~i,%%~j,%%~k>>geoip
)
cls

if exist geoip pause>nul|echo 已经在当前目录生成 geoip，按任意键退出.....
```

5.4 把geoip generater.bat这个文件和解压缩的GeoIPCountryWhois.csv文件放在同一个文件夹内，双击geoip generater.bat，即可生成geoip配置文件，然后拷贝geoip按以上方法替换旧文件。geoip基本每月有更新，因此可单独替换。

（返回目录）（返回简要流程图）

附 录

网络基础知识

什么是 TCP/IP 协议

TCP/IP 协议(Transmission Control Protocol/Internet Protocol)叫做传输控制/网际协议，是 Internet 国际互联网络的基础。

TCP/IP 是网络中使用的基本的通信协议。虽然从名字上看 TCP/IP 包括两个协议，传输控制协议(TCP)和网际协议(IP)，但 TCP/IP 实际上是一组协议，它包括 IP、TCP、UDP、ICMP、ARP 等，而 TCP 协议和 IP 协议是保证数据完整传输的两个基本的重要协议。通常说 TCP/IP 是 Internet 协议族，而不单单是 TCP 和 IP。

什么是 IP、TCP、ICMP、UDP

IP （Internet Protocol），网际协议；IP 是 TCP/IP 的最底层，高层协议都要转化为 IP 包，IP 包含了源地址和目的地址，路由决策也发生在 IP 层；

TCP （Transmission Control Protocol），传输控制协议，一种运行于 IP 之上的、可靠的、面向连接的传输层协议。TCP 运行在 IP 之上，是基于数据流连接和面向的协议，应用程序把数据要经过 TCP/IP 的分割成若干包，这样数据就以字节流发送和接收，到达目的地后，TCP/IP 再按顺序进行组装。TCP/IP 要保证机器与机器之间的连接的可靠性，还要有纠错。TCP 是否被选择，取决于应用程序或服务；

UDP （User Datagram Protocol） ，用户数据报协议 ，一种运行于 IP 之上的、不可靠的、无连接的传输层协议。象 TCP 一样运行在 IP 之上，是基于数据报或分组的协议，UDP/IP 可以直接发送和接收数据报文，而不必做验证，这一点与 TCP/IP 不同。

ICMP （Internet Control Message Protocol），网际控制消息协议；它包括了数据包的错误、控制等相关信息。比如 ping 命令就是利用 ICMP 来测试一个网络的连接情况的工具；

在互联网上，区分每台计算机是使用 IP 地址， IP 协议和路由就是为了将数据包(Packet)发送到正确的主机。只是确定数据包的传送路径还不够，还需要保证传输过程中，数据的完整性，所以就有了 TCP 协议。

TCP 协议提供了可靠的面向对象的数据流传输服务的规则和约定。简单的说在 TCP 模式中，对方发一个数据包给你，你要发一个确认数据包给对方。通过这种确认来提供可靠性。网络上常见的服务：WWW、FTP、SMTP 等都是 TCP 协议。

在对数据传送的稳定性不做太多要求的情况下，可以使用 UDP 协议，由于 UDP 不需要确认数据是否正确传输，更加快速。

DNS 查询、网络即时通讯(QQ)、一些 P2P 影像软件等主要使用 UDP 协议。

什么是端口(Ports)

互联网上的每台电脑都有自己的唯一 IP，信息的传递就在不同 IP 之间。

由于一台电脑要运行很多不同的程序，只有 IP 是不够的，系统不知道将这个数据包分配给哪个具体程序。

于是，为了区别不同的程序，系统就为程序分配不同的端口，数据的传输就是在两台电脑两个端口间进行。

简单的说不同的端口可以代表不同的程序，同一个程序可以使用不止一个端口。

端口的分类

通常的客户端/服务器连接有两种方式，主动连接和被动连接。对应于本机的客户端端口和服务端端口。

服务端监听端口：当本机运行某些网络服务程序或者 P2P 软件时，会开启相应的端口(Listening)，等待客户端的接入。

客户端端口：当我们的浏览器需要连接远程 WWW 服务器时，需要启用一个大于 1024 的随机端口，连接 WWW 服务器的 HTTP 端口。

通常 0-1023 端口会保留给系统服务使用，所以又叫做 Well Known Ports 公认端口。例如，80 端口分配给 WWW 服务，21 端口分配给 FTP 服务等。

本机客户端程序所启用的随机端口是在 1025-65535 之间，这些端口又叫作 Dynamic Ports 动态端口。是因为它 一般不固定分配某种服务，而是动态分配。动态分配是指当一个系统进程或应用 程序进程需要网络通信时，它向主机申请一个端口，主机从可用的端口号中分配 一个供它使用。当这个进程关闭时，同时也就释放了所占用的端口号。

通常 XP 系统的动态端口是 1025-5000，如果到了 5000，系统会返回 1025，再按顺序使用。

端口的数量

共有 65536 (2^16)个端口，0-65535

端口的安全性

经常有人说，我的机子开了 xxx 个端口，xx 端口不安全。

其实，端口是没有安全性的，真正影响安全的是端口背后的服务。

因为端口是由服务开启的，要关闭端口，就要关闭相应的服务。

所以，本机要运行什么服务，一定要使用最新、最安全的版本。至于，开启哪个端口，并不是最重要的。没有不安全的端口，只有不安全的服务(程序)。

连接的双向性和 4 个重要参数

单向的发送数据包是不可能建立一条连接。通常使用浏览器访问一个网站，是本机启用一个大于 1024 的随机端口，发送数据包到服务器的服务端口，通常是固定 80 端口。服务器再将我们需要的资料，由 80 端口，返回本机建立连接的随机端口。

于是有下面 4 个重要参数：

来源 IP (Source Address)

目的 IP (Destination Address)
来源端口 (Source Port)
目的端口 (Destination Port)

注意来源和目的是相对的，要看数据包传输的方向。

端口(开放、关闭、隐藏)

前面讲过开放(Open)的端口与本机运行的服务有关。

Windows 系统默认运行的服务会开放一些端口，要关闭这些端口，需要关闭相应的服务。最简单的方法是关闭不用的服务，并且使用工具，比如 Windows Worms Doors Cleaner。

端口关闭(Closed)，说明没有服务启用这个端口，端口没有被系统分配，一个关闭的端口当收到连接请求以后，会返回一个错误提示(通常是 ICMP "Destination Unreachable")。 例如，当你关闭 BT、eMule 等 P2P 软件以后，你的系统会大量向外发送 ICMP "Destination Unreachable" 目标不可达，表示端口已经关闭。

端口隐藏(Stealthed)，端口隐藏和端口关闭是一样的，不允许连入，只是不返回出错信息而已。

从安全上讲，端口隐藏和端口关闭，没有大的区别，都是不允许非法连入。端口隐藏的好处是不返回任何信息，使入侵者无法得知具体的端口、系统信息；另外，由于丢弃数据包这样的静默处理，可以使端口扫描一直等待结果而超时。

端口在线检测

网络扫描是有前提的，必须是外网 IP，不能通过路由器、代理服务器上网，否则结果不准确。

如果，你是 ADSL 路由器上网，想要获得正确的结果。必须：
1.断开路由器，使用拨号上网的方式，然后扫描。
2.或者，将本机 IP 加入到路由器的 DMZ，或者在路由器映射所有端口。

主要的防火墙在线检测站点：
Shields UP!
PCFlank
Nmap Online
Symentic Security Check
HackerWhacker

什么是 DNS

要找到指定的主机，我们用到 IP；要传输数据，需要 TCP、UDP、ICMP。问题是 IP 地址是很难记忆的，于是我们使用了主机域名来解决这个问题。普通用户可以通过 www.google.com 来访问网站，而不需要输入 IP 地址。

实际上，这中间有一项服务：Domain Name System (DNS)，将域名转换成 IP 地址。个人电脑必须向域名服务器(DNS：Domain Name Server)查询 IP 地址，然后浏览器才会根据返回的 IP 地址，连接相应的主机服务器。

DNS 是我们经常用到的协议，一旦在防火墙阻止，就不能正常上网了。

（返回目录）

后　记

这里只提供了 TorManager2.7 较初级的教程，更深入的 Tor 的使用还需大家继续探讨与研究。

（返回目录）