无线路由器
安全设置

实用技巧

二零一三年十月三十一日

前 言

使用路由器有很多方便之处，同时电脑经过路由器连到互联网，也可认为是多了一道屏障，但是使用路由器也要注意一些安全设置。

美国印第安纳大学计算机科学系的研究员发布了一个报告，指出黑客有可能连接与改变无线路由器的配置。他们描述了嵌入在网页的 JavaScript 可能被用来以管理员的帐户登录路由器，并更改其 DNS 设置，使路由器被用作见不得人的勾当的跳板，范围可以从病毒感染到基于网络钓鱼的身份盗窃。报告指出这个攻击可以运行于多数路由器，不论什么品牌或型号的路由器。

但是值的注意的是，**黑客只有在目标路由器的默认用户名与密码不变的情况下才能实施攻击**。换句话说，用户只要在攻击之前简单的修改一下他们的用户名和密码就能得到保护——因此看似很小很易被忽视的设置却可能对安全有深远的影响。本文将介绍如何修改这些设置以提高路由器的安全。

说明：

1. 标题后标注（必选）的建议修改，标注（可选）的可自行选择是否修改；可选项标识【有利】的指按此项修改后在安全或其它方面的有利之处。【不利】指按本文修改后带来的不方便之处。

2. 设置路由器的 WEB 界面大同小异，有些新款的路由器设置相对便捷些，大家可领会教程的重点根据实际情况设置即可。

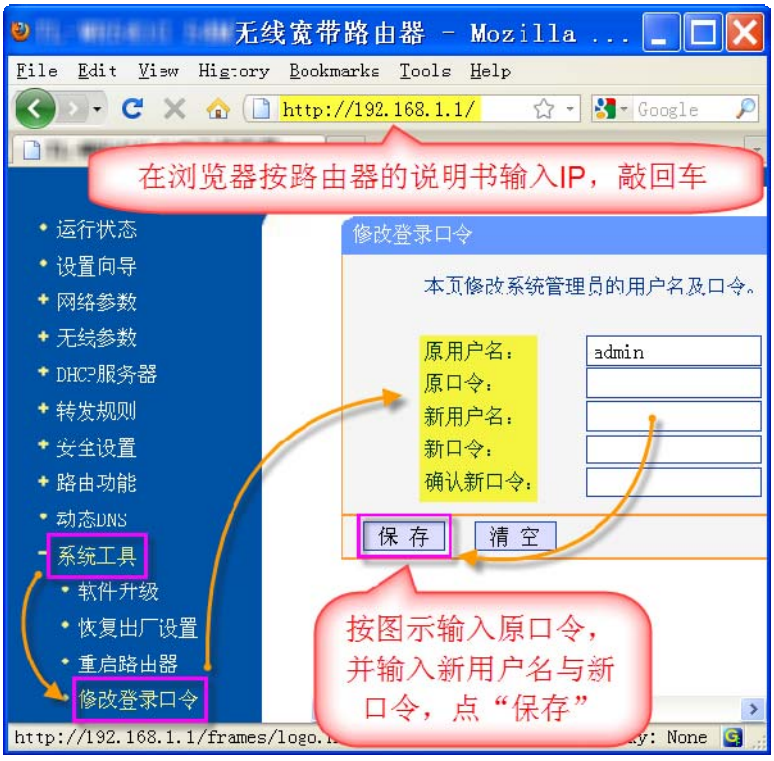
3. 有线路由器、3G 路由器亦可按此文修改，当然没有的功能无需设置。

4. **安全提示**：按照本方案進行设置后无线路由器的安全度将大大提升，但是毕竟无线路由器是有可能被外来黑客破解的。因此建议无线路由器用于普通用途，再串联一个有线路由器与重要电脑连接；详细设置方法可参考禁书网的路由器串联方案。

一、更改用户名、密码（必选）

使黑客不能利用默认用户名密码轻易修改或利用你的路由器。但用户需记住新的用户名与密码。如果忘记，可以在通电时长按路由器恢复键恢复默认设置，恢复后需从新按本文修改所有设置。

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。在**系统工具－修改登录口令**，输入**原用户名**与**原口令**，再输入**新用户名**与**新口令**和**确认新口令**，点**保存**：

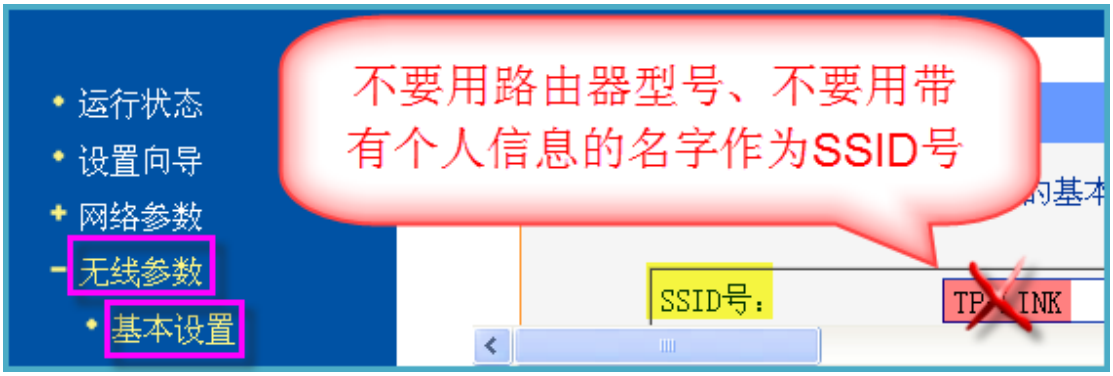


二、更改默认的 SSID 名称（必选）

更改后不易被黑客猜出路由器型号。但注意不要修改成带有个人信息的 SSID 名称。

许多用户会保留默认的无线 SSID，这个名称通常会显示出设备的生产厂商，也使被推断出其它信息成为可能。创建一个不同的 SSID，且一定避免使用任何家庭名称或地址等带有个人信息的 SSID。

♦ 在**无线参数－基本设置－SSID 号**修改，点**保存**：



说明：如果使用中文 SSID 可能更安全，因为目前一些破解软件不支持中文编码。但是有些手机与电脑不能识别中文 SSID 从而无法连接上网。因此请自行决定 SSID 名称是否使用中文。

注意：有些无线路由器只有无线功能、没有有线连接功能的，如果尝试修改 SSID 为中文，之前先更改无线参数为“允许 SSID 广播”，否则查找不到 SSID 则无法连接与修改、只能恢复出厂设置了。

三、避免使用远程管理（必选）

修改 WEB 管理端口，将使黑客妄图修改路由器的设置难上加难。但需记住此端口号，且需要在浏览器正确输入方可進入路由器设置界面。如果忘记，需通电长按路由器恢复键恢复，恢复后需按本文从新修改所有设置。

多数路由器允许你从你的网络之外登录与管理设备，但如果不是必要你应该避免使用此功能。**远端 WEB 管理 IP 地址**设置不同的 IP 代表不同的含义：

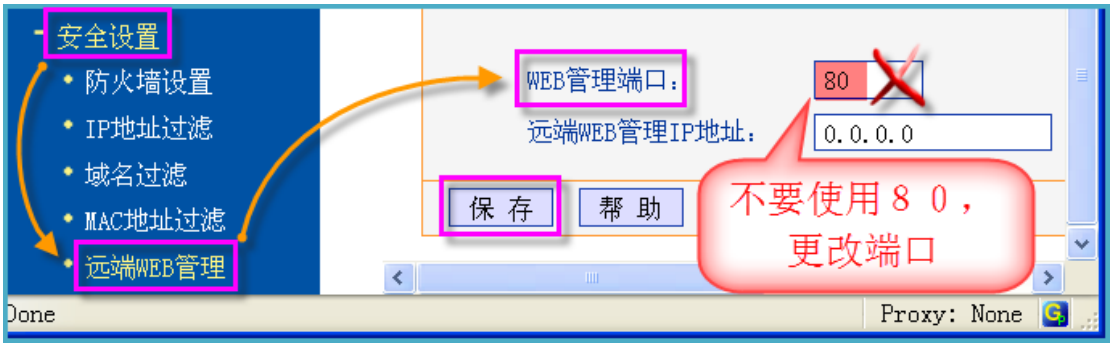
(1)通常默认设置为 0.0.0.0 即没有电脑可以使用远端 WEB 管理（推荐设置）；

(2)如果设置成一个具体的 IP 就只允许这个 IP 可以远程管理该路由器；

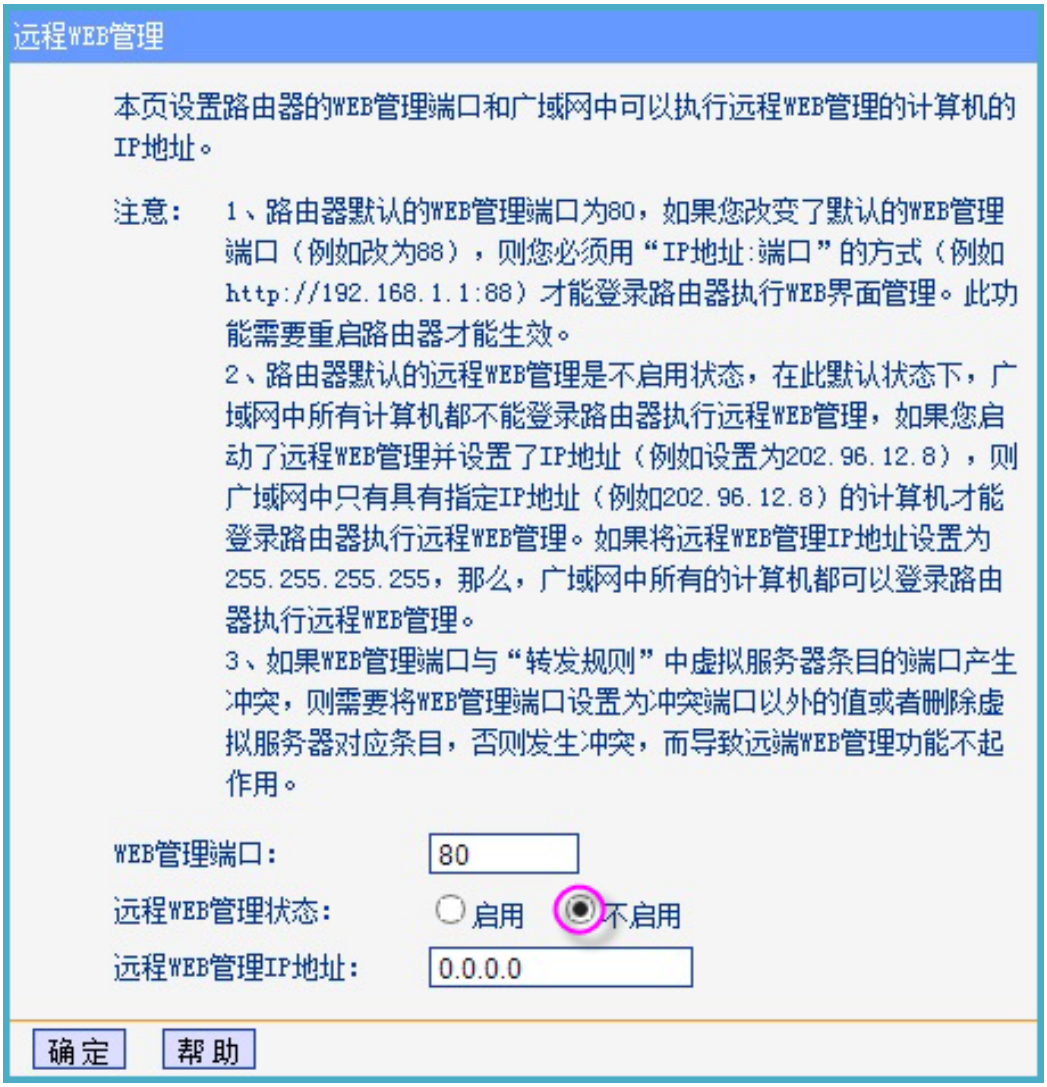
(3)如果是 255.255.255.255 就是所有 IP 均可远程管理。

重要提示： WEB 管理端口建议修改，比如修改为 100,在浏览器设置路由器时要输入：http://192.168.1.1:100 敲回车，这点很重要，避免未经授权的人任意修改路由器设置。如果忘了加端口就无法進入路由器设置界面。如果使用默认端口 80,设置时在浏览器只输入 IP 无需加端口号。

♦ 在**安全设置－远端 WEB 管理－WEB 管理端口**，修改端口号，点**保存**：



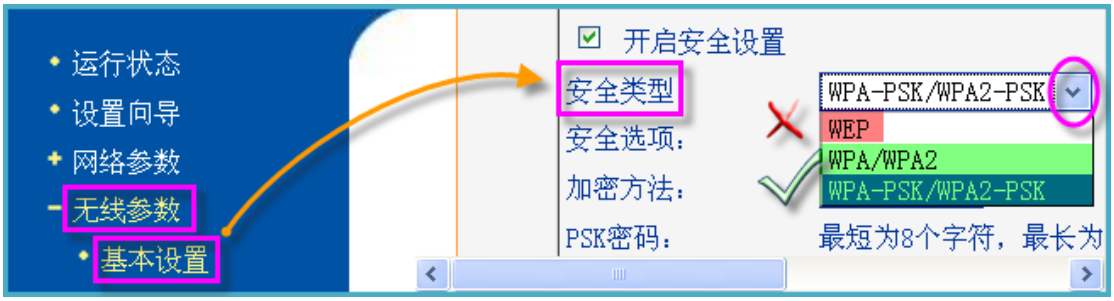
说明：有的路由器直接有是否打开**远端 WEB 管理**的选项,一定选择**禁用**或**不启用**，有关说明请看图示：



四、使用 WPA 加密而不要使用 WEP（必选）

加大黑客破解难度。

- 在**无线参数－基本设置－安全类型**，如图选择（不选 WEP，选择 WPA 开头的均可）：

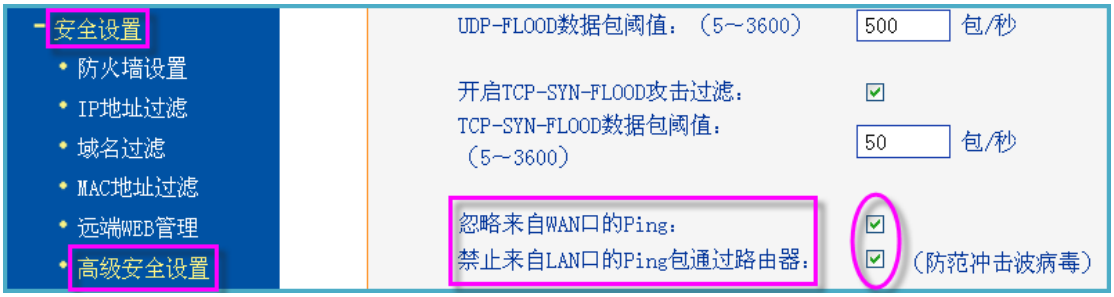


五、关闭 Ping 响应（必选）

设置此项使路由器起到防火墙的作用。

Ping 响应的设置允许你的路由器响应于由互联网发出的 Ping 命令。它默认是关闭的，但是你应该确认一下是否如此，因为它可能背叛你现存的网络给潜在的黑客，这将给进一步的被探测发出一个危险的邀请。

♦ 在**安全设置－高级安全设置**，勾选**忽略来自 WAN 口的 Ping** 和**禁止来自 LAN 口的 Ping 包通过路由器**：



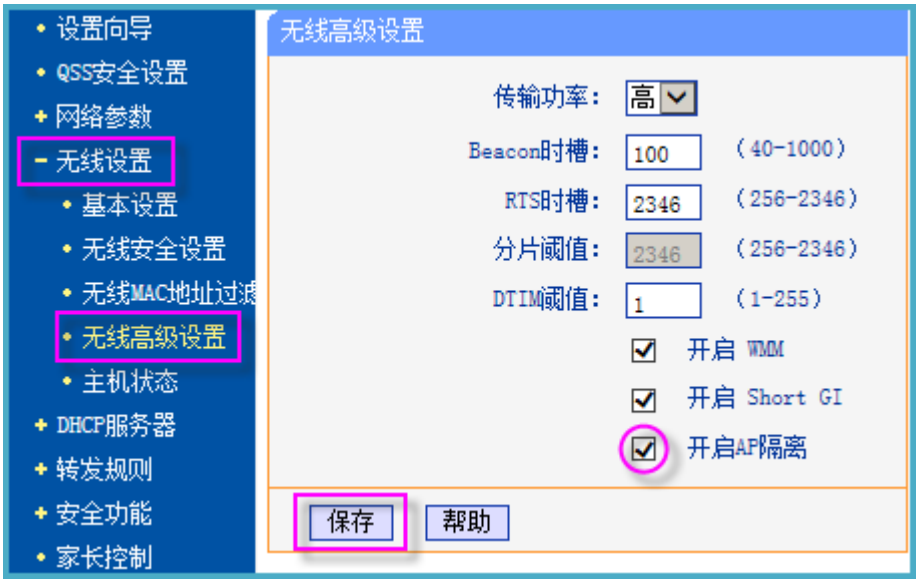
六、开启 AP 隔离（必选）

说明：新款无线路由器往往有是否开启 AP 隔离的选项，无此选项的路由器请忽略。

连接于同一个路由器的不同设备处于同一个局域网，可以互相访问；如果其它设备安装了流氓软件或木马，同时上网的重要电脑则有安全隐患。开启路由器 AP 隔离功能、设置防火墙、使用路由器串联方案、或者重要电脑与其他上网设备不同时上网，可以避免这种问题。

AP 是(Wireless) Access Point 的缩写，一般翻译为“(无线）访问节点”。 如果开启 AP 隔离，那么关联到本路由器的无线客户端之间无法互相访问。

♦ 在**无线设置－无线高级设置**，勾选**开启 AP 隔离**，点**保存**：

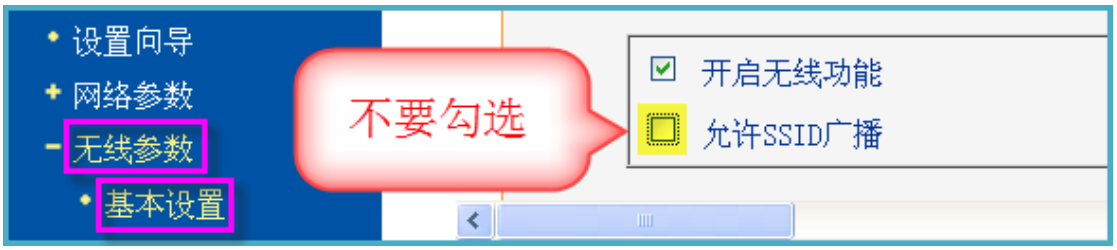


七、关闭 SSID 广播（可选）

【有利】不易被黑客轻易搜索到。
【不利】当设备需无线连接路由器时，该路由器 SSID 不会显示在设备的 WIFI 可选项里，需手动用 SSID 名称搜索，输入密码连接后，以后联网设备打开 WIFI 后无需再搜索、可以自动连接了；笔记本电脑无线网络**属性－连接**勾选“即使网络未广播其名称也连接（SSID)”。如果偶尔出现没有自动连接 SSID，需再次手动搜索。

SSID 广播使你很容易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。最好只有你知道你自己的 SSID，而不让黑客轻易搜索到。

- 在**无线参数－基本设置**去掉**允许 SSID 广播**的勾选：



八、降低无线功率（可选）

没必要购买太大功率的路由器。有的路由器可以调节功率，你可以调小路由器的无线发射功率以使信号在你的住宅或办公室范围内。可能会有一些误差，但要尽量减少跑到街上或邻居院子的信号。

九、消除或减少 DHCP 的使用（可选）

【有利】禁用 DHCP 可减少一个未经授权的设备轻易得到 IP 的机率，也就是减少黑客设备加入你的局域网的可能性。

【不利】需知道路由器的 IP 范围，然后在电脑或上网设备上手动填写静态 IP。比如是 192.168.1.x，或是 192.168.100.x 等。

DHCP 的自动分配 IP 提供了极大的方便，特别是当你有许多设备去管理的时候，**但是请记住**：DHCP 很高兴分配一个 IP 给任何提出请求的系统。如果你只有很少的设备，关掉 DHCP 而设置静态 IP，这将加大非授权用户从你的网络得到一个有效地址的难度。**注意**：这样设置后所有设备需手动设置不同的静态 IP，如果设备比较多建议使用以下第九条的方法：

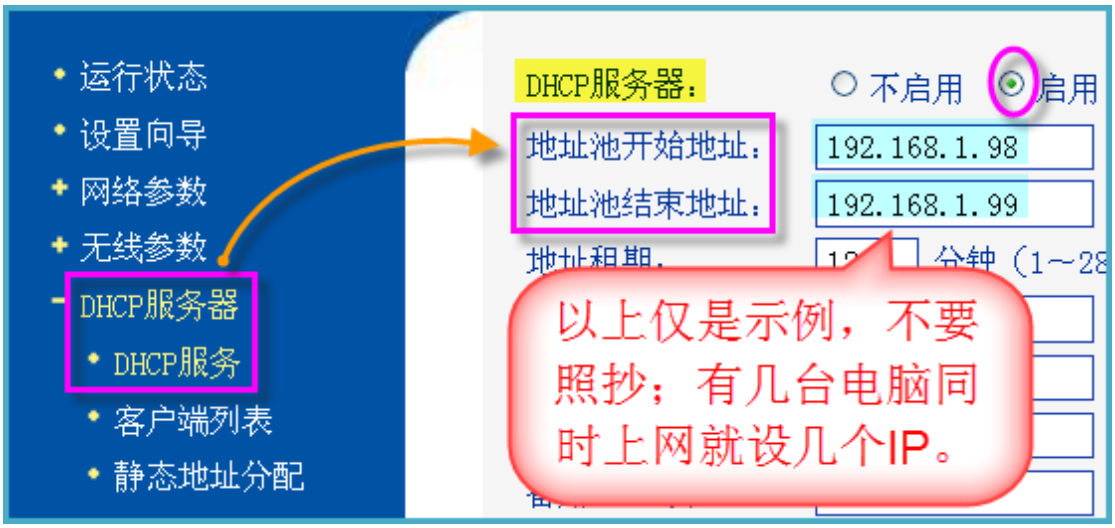
♦ 在 DHCP 服务器－DHCP 服务－DHCP 服务器点选**不启用**，点**保存**：

十、保持打开 DHCP，但减少地址池的大小(可选)

【有利】可减少其它未经授权的设备轻易得到 IP 的机率，也就是减少黑客设备加入你的局域网的可能性。
【不利】地址池设的太大起不到作用；设的小的话，如果同时上网的设备突然增加又会有设备上不了网。这时需手动修改本项，以满足更多的 IP 需求。

多数路由器设置了几乎所有可用的地址－－超过 250 个－－到地址池，这远远超出了实际需求并且留下了许多给未经授权用户。限制 DHCP 可用地址的数量可以使你使用 DHCP，同时又可阻止无线闯入者得到可用地址。地址池前三位参考路由器说明，第四位可选择 2～254；设同时上网的设备数即可，比如共有 5 个设备，但最多 3 个同时上网，设 3 个地址即可：比如 192.168.1.2～192.168.1.4。

♦ 在 DHCP 服务器－DHCP 服务－DHCP 服务器点选**启用**，按以上说明分别设置**地址池开始地址**与**地址池结束地址**：



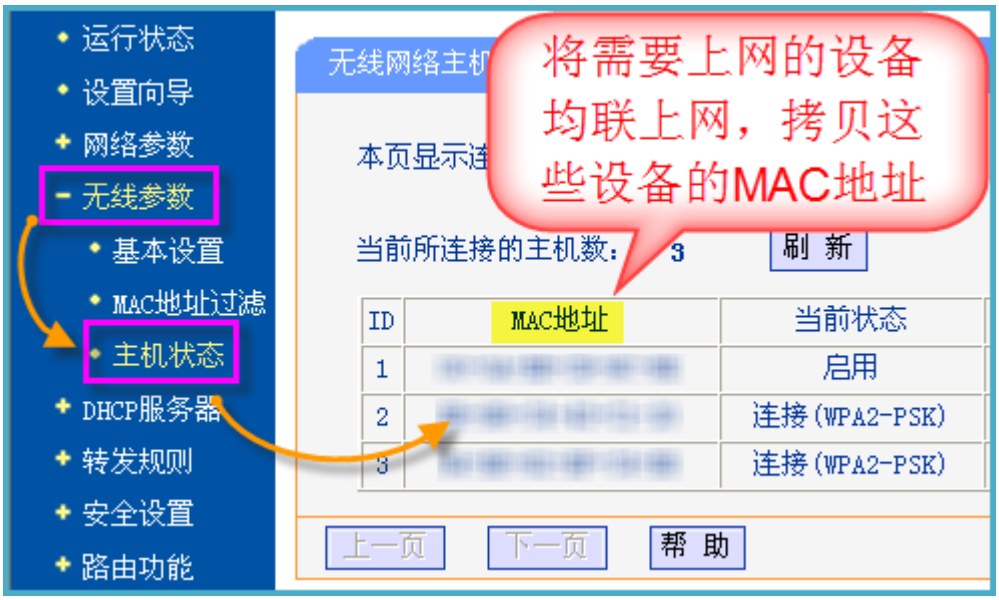
十一、打开 MAC 过滤（可选）

【有利】设置 MAC 过滤后，可以大大减少一般黑客修改路由器设置的可能；而且可以防止蹭网。

【不利】必需预先加入所有需要上网设备的 MAC，如果有新设备需要**无线联网**，需将其 MAC 加入到路由器 MAC 过滤中（新设备通过无线路由器用网线有线联网不需要设置，因为有线联网用的是路由器自身的 MAC，已经加入过滤中了）。

虽然它代替不了无线加密，但 MAC 过滤是一个好的补充，只有那些对应 MAC 地址的设备具备上网的通道。有的路由器可以让你很容易的添加关联的设备到过滤清单，而避免查找每个设备 MAC 地址的麻烦。或者用以下方法查到上网设备的 MAC 后，手动添加。MAC 过滤有两部份可设置，第一部份在**无线参数－MAC 地址过滤**，第二部份在**安全设置－MAC 地址过滤**。按第一部份设置即可，第二部份选看。

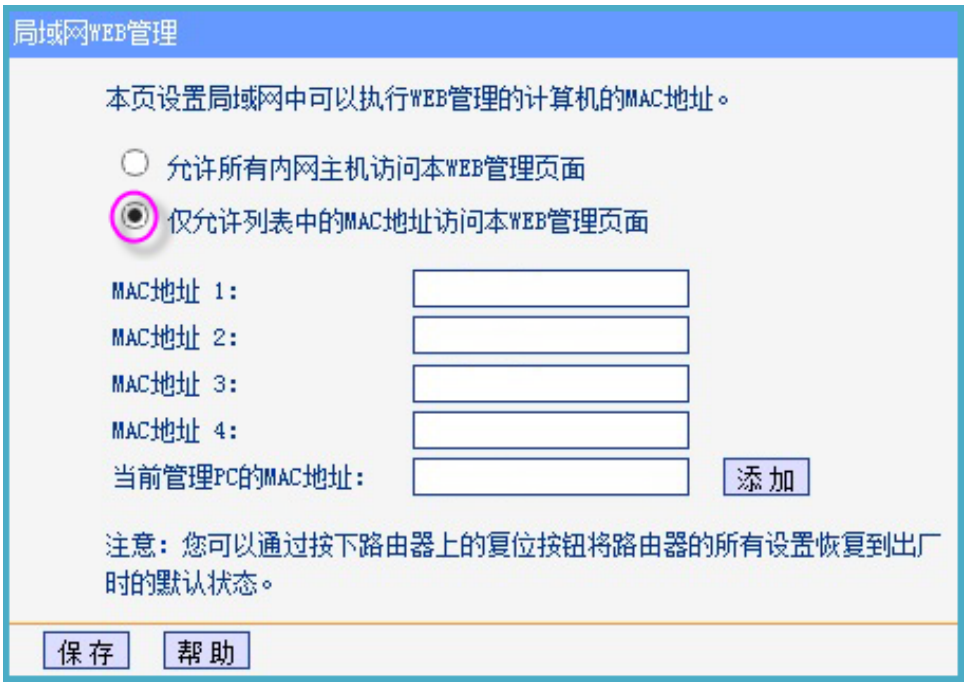
1. 打开所有需连接此路由器的设备并联网，在**无线参数－主机状态**会看到所有连到此路由器的设备，分别拷贝这些 **MAC 地址**：



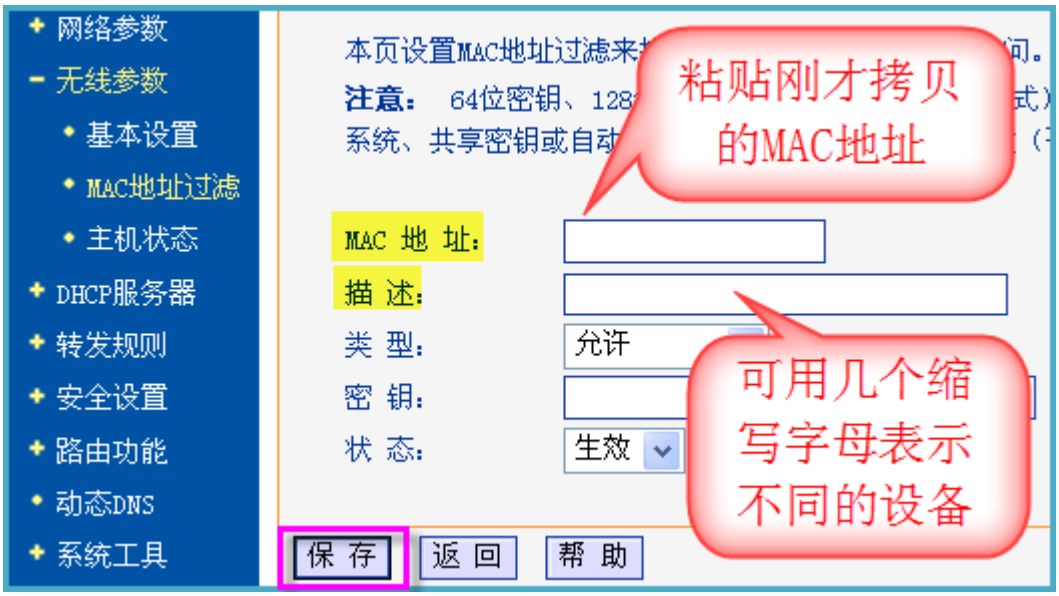
2. 在**无线参数－MAC 地址过滤**点**添加新条目**（添加方法请看下一条）；添加所有上网设备后点选**禁止列表中生效规则之外的 MAC 地址访问本无线网络**；再点**开启过滤**，使 **MAC 地址过滤功能**成“已开启”状态。

说明：（1）这里的 MAC 地址是限定可以连接到此无线路由器的设备，这些设备可以用浏览器登录（比如 http://192.168.1.1）来设置路由器。这项限定很重要，避免外来的设备随意更改路由器设置。

（2）新款的路由器有更方便的选择，比如可以直接选择“仅允许列表中的 MAC 地址访问本 WEB 管理页面”，点选此选项后，只有在这里设置 MAC 的电脑或设备才可以登录 WEB 修改路由器的设置：



3. 点**添加新条目**后，把拷贝的内容粘贴到 **MAC 地址**；**描述**可用字母表示不同的设备（但尽量不要让人一看就知道是什么设备）、亦可留空，点**保存**：



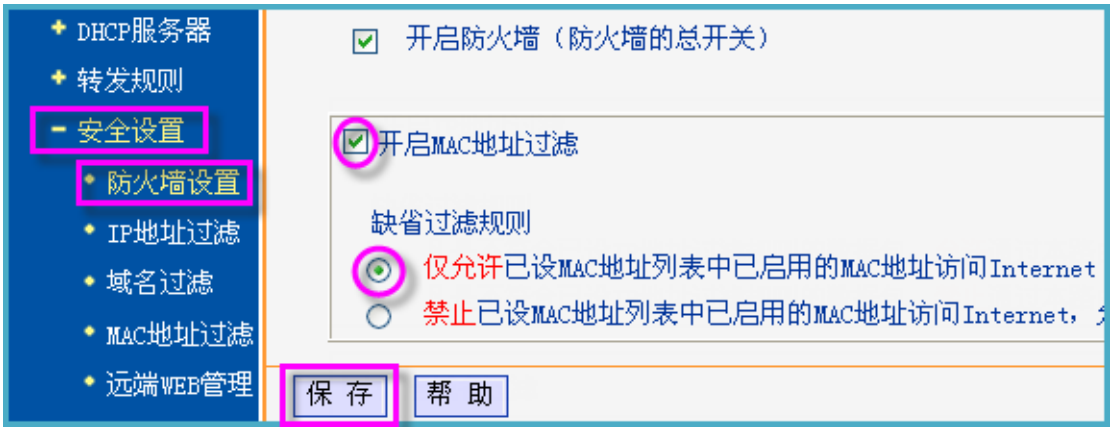
提示：一旦采用了 MAC 过滤，无论重不重要的设备包括手机的 MAC 均需设置，这样比较繁琐；如果想不设置 MAC 过滤，同时又想保护好重要电脑的安全，可参考禁书网的路由器串联方案。

说明：MAC 过滤的设置到上一步就可以了，以下非必看。以下的 MAC 过滤是限定哪些设备可以上网、或不可以上网，在这里允许上网的 MAC 也必须在**无线参数**—**MAC 地址过滤**有设定，否则上不了网。

1. 在**安全设置**—**MAC 地址过滤**点**添加新条目**：

2. 在 MAC 地址粘贴刚才拷贝的内容，**描述**可用缩写字母表示不同的设备、亦可留空；需一条一条分别粘贴后点**保存**：

3. 在**安全设置－防火墙设置**，勾选**开启 MAC 地址过滤**，点选**仅允许已设 MAC 地址列表中已启用的 MAC 地址访问 Internet**：



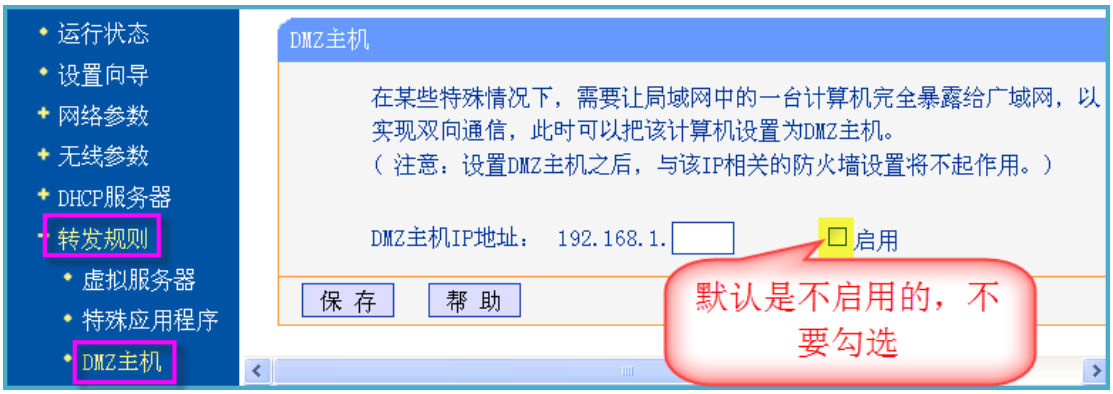
说明：如果以上设置完成后通过无线上网不稳定可到**安全设置－防火墙设置**，去掉**开启 MAC 地址过滤**的勾选。

十二、确认关掉你的 DMZ（可选）

说明：确认 DMZ 是关闭状态即可，一般用户通常用不到此项功能。

DMZ（非控制区）是一个 IP（或 IP 范围）公开到了互联网，存在安全隐患。

♦ 在**转发规则－DMZ 主机**，查看**启用**是未勾选状态：



结 语

以上简单介绍了一些常见的无线路由器的安全设置，如果在路由器的使用中发现有本文未涉及却对安全非常重要的功能或设置，欢迎到禁书网反馈。