一、我的路由器仲了 ARP 病毒那我那样搞好?

如果对 ARP 病毒攻击进行防制的话我们必须得做路由器方面和客户端双方的设置才保证问题的最终解决。所以我们选择路由器的话最好看看路由器是否带有防制 ARP 病毒攻击的功能，Qno 侠诺产品正好提供了这样的功能，相比其他产品操作简单易学。下面具体谈谈 Qno 侠诺路由器产品是如何设置防止 ARP 病毒攻击的。

1、激活防止 ARP 病毒攻击：

输入路由器 IP 地址登陆路由器的 Web 管理页面，进入“防火墙配置”的“基本页面”，再在右边找到“防止 ARP 病毒攻击”在这一行的“激活”前面做点选，再在页面最下点击“确认”。

中文路由器 Web 管理页面

2、在路由器端绑定用户 IP/MAC 地址：

进入“DHCP 功能”的“DHCP 配置”，在这个页面的右下可以看到一个“IP 与 MAC 绑定”你可以在此添加 IP 与 MAC 绑定，输入相关参数，在“激活”上点“√”选再“添加到对应列表”，重复操作添加内网里的其他 IP 与 MAC 的绑定，再点页面最下的“确定”。　　当添加了对应列表之后，其对应的信息就会在下面的白色框里显示出来。不过建议不采用此方法，这样操作需要查询网络内所有主机 IP/MAC 地址工作量繁重，还有一种方法来绑定 IP 与 MAC，操作会相对容易，可以减少大量的工作量，节约大量时间，下面就会讲到。

进入“DHCP 功能”的“DHCP 配置”找到 IP 与 MAC 绑定右边有一个“显示新加入的 IP 地址”点击进入。

点击之后会弹出 IP 与 MAC 绑定列表对话框，此对话框里会显示网内未做绑定的 pc 的 IP 与 MAC 地址对应情况，输入计算机“名称”和“激活”上“√”选，再在右上角点确定。
此时你所绑定的选项就会出现在 IP 与 MAC 绑定列表框里，再点击“确认/Apply”绑完成。

3、对每台 pc 上绑定网关的 IP 和其 MAC 地址

进行这样的操作主要防止 ARP 欺骗网关 IP 和其 MAC 地址首先在路由器端查找网关 IP 与 MAC 地址，

然后在每台 PC 机上开始/运行 cmd 进入 dos 操作，输入 arp　-s　192.168.1.1　0-0e-2e-5b-42-03，Enter 后完成 pc01 的绑定。

针对网络内的其他主机用同样的方法输入相应的主机 IP 以及 MAC 地址完成 IP 与 MAC 绑定。但是此动作，如果重起了电脑，作用就会消失，所以可以把此命令做成一个批处理文件，放在操作系统的启动里面，批处理文件可以这样写：

```
@echo off
arp -d
arp -s 路由器 LAN IP　路由器 LAN MAC
```

对于已经中了 arp 攻击的内网，要找到攻击源。方法：在 PC 上不了网或者 ping 丢包的时候，在 DOS 下打 arp -a 命令，看显示的网关的 MAC 地址是否和路由器真实的 MAC 相同。如果不是，则查找这个 MAC 地址所对应的 PC，这台 PC 就是攻击源。

其他的路由器用户的解决方案也是要在路由器和 PC 机端进行双向绑定 IP 地址与 MAC 地址来完成相应防制工作的，但在路由器端和 PC 端对 IP 地址与 MAC 地址的绑定比较复杂，需要查找每台 PC 机的 IP 地址与 MAC 加大了工作量，操作过程中还容易出错。

以上方法基本可以解决 ARP 病毒攻击对网络造成相关问题，以上方法也经过多个用户以

及网吧实验，都达到了用户预期的效果。QNO 侠诺产品的解决方法操作比较容易学习，而且不必要查找整个网络的 IP/MAC 地址，就可以在路由器端进行绑定，安全可靠。

二、在家用路由器怎么防止 ARP 病毒攻击

不要把你的网络安全信任关系建立在 IP 基础上或 MAC 基础上。设置静态的 MAC-->IP 对应表，不要让主机刷新你设定好的转换表。 除非必要，否则停止 ARP 使用，把 ARP 做为永久条目保存在对应表中。使用 ARP 服务器。确保这台 ARP 服务器不被黑。使用"proxy"代理 IP 传输。 使用硬件屏蔽主机。 定期用响应的 IP 包中获得一个 rarp 请求，检查 ARP 响应的真实性。 定期轮询，检查主机上的 ARP 缓存。 使用防火墙连续监控网络。〇解决方案 建议采用双向绑定解决和防止 ARP 欺骗。在电脑上绑定路由器的 IP 和 MAC 地址首先，获得路由器的内网的 MAC 地址（例如 HiPER 网关地址 192.168.16.254 的 MAC 地址为 0022aa0022aa 局域网端口 MAC 地址>）。编写一个批处理文件 rarp.bat 内容如下：@echo off arp -d arp -s 192.168.16.254 00-22-aa-00-22-aa 将网关 IP 和 MAC 更改为您自己的网关 IP 和 MAC 即可，让这个文件开机运行(拖到“开始-程序-启动”)。

三、网关欺骗 arp 攻击，高分给解决方案

防护 arp 攻击软件最终版-Antiarp 安全软件

使用方法：

1、填入网关 IP 地址，点击〔获取网关地址〕将会显示出网关的 MAC 地址。点击[自动防护]即可保护当前网卡与该网关的通信不会被第三方监听。注意：如出现 ARP 欺骗提示，这说明攻击者发送了 ARP 欺骗数据包来获取网卡的数据包，如果您想追踪攻击来源请记住攻击者的 MAC 地址，利用 MAC 地址扫描器可以找出 IP 对应的 MAC 地址.

2、IP 地址冲突

如频繁的出现 IP 地址冲突，这说明攻击者频繁发送 ARP 欺骗数据包，才会出现 IP 冲突的警告，利用 Anti ARP Sniffer 可以防止此类攻击。

3、您需要知道冲突的 MAC 地址，Windows 会记录这些错误。查看具体方法如下：

右击[我的电脑]--[管理]--点击[事件查看器]--点击[系统]--查看来源为[TcpIP]---双击事件可以看到显示地址发生冲突，并记录了该 MAC 地址，请复制该 MAC 地址并填入 Anti ARP Sniffer 的本地 MAC 地址输入框中(请注意将:转换为-)，输入完成之后点击[防护地址冲突]，为了使 MAC 地址生效请禁用本地网卡然后再启用网卡，在 CMD 命令行中输入 Ipconfig /all，查看当前 MAC 地址是否与本地 MAC 地址输入框中的 MAC 地址相符，如果更改失败请与我联系。如果成功将不再会显示地址冲突。

注意:如果您想恢复默认 MAC 地址,请点击[恢复默认],为了使 MAC 地址生效请禁用本地网卡然后再启用网卡。