arptables 来防止 ARPRequest 获得

一般欺骗机器通过 ARPRequest 获得网关的 MAC ,然后同样方法获得你服务器的 MAC 进行双向欺骗，然后 sniffer 密码，挂马之类。

国内几乎所有的 IDC 都是几百服务器公用一个网关的。然后上百个服务器总有几个有漏洞的，然后你就被 ARP 欺骗挂马或者抓密码了

下面介绍的是 Linux 利用 arptables 来防止 ARPRequest 获得你的 MAC。这样攻击者会认为你的服务器是不存在的（本来很复杂的，需要 patch 编译内核什么的，上周才发现还有一个 arptables，免编译内核，现在把方法写一下）

```
Debian/Ubuntu: （runassudo）CentOS/RHAS 叫 arptables_jf

Quote:

apt-getinstallarptables

arptables-AINPUT--src-mac!网关 MAC-jDROP

arptables-AINPUT-s!网关 IP-jDROP
```

如果你有本网的内网机器要互联，可以

Quote:

```
arptables-IINPUT--src-mac 你的其他服务器 MACACCEPT
```

如果你的 MAC 已经被欺骗机器拿到，那只能 ifconfigethxhwetherMAC 来修改了

有一定的危险性，请酌情测试，你也可以疯狂刷新网关+本机 ARP 绑定，看具体需要

还要注意这个时候不要发出 ARPRequest 到除网关以外的其他 IP ,其后果可能是被其他机器拿到 MAC