防范私自修改IP地址的三种方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E9_98_B2_E8_8C_83_E7_A7_81_E8_c101_142650.htm 我们单位所在局域网有100多台计算机，为了区分不同用户分配更详细的访问权限，我们采用的是设置固定IP的方法，而不是自动获取IP地址，再就是我们还要有一部分要连到互联网上。这样就要设两个子网如内网我们设为192.168.0.1网段，能连外网的我们设为192.168.1.1网段。在实际使用中遇到了经常有用户为了上网私自修改IP地址，从而造成网络冲突的问题。表现如下：因为我们的计算机都是使用Windows XP系统的可以设两个以上的IP所以用户可以私自设置上两个网段的IP地址这样第一可以联入单位的局域网也可以连到因特网，这是公司不允许的。公司经理要求马上解决这个问题，要不然这个月的奖金就没了。 下面是我解决的过程和自己的一些心得，希望能给要解决这样问题的一些提示。 方法一，IP与MAC地址的绑定加上路由器的MAC过滤功能(我用的是TP-LINK路由器) 使用ARP -s 192.168.1.2 00-AO-43-E0-6A-84的命令，这样就将静态IP地址192.168.1.2与网卡地址为00-AO-43-E0-6A-84的计算机绑定在一起了，使别人就不能使用这个IP地址了。再进入路由器的MAC过滤功能选中只允许下列MAC的网卡地址连入外网把00-AO-43-E0-6A-84填入即可。 可是上面提到的方法虽然可以在一定程度上解决非法用户网络接入的问题和网络冲突的问题，但用户还是可以通过修改注册表，下载专用修改MAC小工具等方法，轻松更改了本机的MAC地址，甚至将本机的MAC地址和IP地址改得和上面能上网的机器一模一样

。非法用户又可以非法使用网络了。并且我用的路由器MAC过滤功能只能填入16个MAC(我不是说TP-LINK的东东不好，只是我们用的那个价格太低了)。 方法二，交换机的MAC地址与端口绑定 我可以将交换机的MAC地址与端口绑定后，非法用户擅自改动本机网卡的MAC地址，该机器的网络访问将因其MAC地址被交换机认定为非法而无法实现。这样他们想改也不敢了。 登录进入交换机(我单位用的是CISCO交换机，我想别的品牌的交换机也差不多)，输入管理口令进入配置模式: 敲入命令：(config)#mac_address_table permanent [MAC地址] [以太网端口号] 这样逐一地将每个端口与相应的计算机MAC地址进行绑定，保存退出后就彻底阻止了用户的非法修改。 方法三，防火墙与代理服务器 我个人感觉使用防火墙与代理服务器相结合，更能较好地解决IP地址盗用问题：防火墙用来隔离内部网络和外部网络，用户访问外部网络通过代理服务器进行。使用这样的办法是将IP防盗放到应用层来解决，变IP管理为用户身份和口令的管理，因为用户对于网络的使用归根结底是要使用网络进入因特网。这样实现的好处是，盗用IP地址只能在子网内使用，失去盗用的意义.合法用户可以选择任意一台IP主机使用，通过代理服务器访问外部网络资源，而无权用户即使盗用IP，也没有身份和密码，不能使用外部网络。 使用防火墙和代理服务器的缺点也是明显的，由于使用代理服务器访问外部网络对用户不是透明的，增加了用户西作的麻烦.另外，对于大数量的用户群来说，用户管理也是一个问题。 