 互联网充满着各种安全威胁,其中之一就是IP地址欺骗。IP欺骗技术就是伪造某台主机的IP地址的技术。通过IP地址的伪装使得某台主机能够伪装另外的一台主机，而这台主机往往具有某种特权或者被另外的主机所信任。在一次典型的地址欺骗尝试中，攻击者只是简单地伪装源数据包使其看起来是内自于内部网络。下面谈一下怎样利用思科IOS防止你公司的网络遭到这种攻击。 互联网操作系统（IOS）是思科特有的核心软件数据包，主要在思科路由器和交换机上实现，特别是可用它配置Cisco路由器硬件，令其将信息从一个网络路由或桥接至另一个网络。可以毫不客气地说，I0S是思科路由器产品的动力之源。那么怎样利用思科IOS防止IP欺骗呢？ 阻止IP地址 防止IP欺骗的第一步就是阻止能造成风险的IP地址。虽然攻击者可以欺骗任何IP地址，最常被欺骗的IP地址是私有IP地址（请参考RFC1918）和其它类型的共享/特别的IP地址。 例如，笔者就阻止如下的IP地址（后面紧跟着其子网掩码）从Internet访问本机： 10.0.0.0（255.0.0.0） 172.16.0.0（255.240.0.0） 192.168.0.0（255.255.0.0） 127.0.0.0（255.0.0.0） 224.0.0.0（224.0.0.0） 169.254.0.0（255.255.0.0） 以上所列示的是私有的在互联网上不可路由的IP地址，抑或是用于其它目的的IP地址，因此不应出现在互联网上。如果来自互联网的通信以其中某个IP地址为源地址，必定是欺骗性的通信。 此外，其它常被欺骗的IP地址是那些你的组织使用的任何内部IP地址

。如果你正使用全部的私有IP地址，那你的范围就应该属于以上所列示的IP地址。然而，如果你正使用自己的公有IP地址范围，你就应该将其加入到以上列表中。 实施访问控制列表(ACL) 最简单的防止欺骗的方法就是对所有的互联网通信使用一个进入过滤器。进入过滤器会丢弃源地址为以上所列地址的任何数据包。换句话说，就是创建一个ACL（access control list），使之丢弃所有进入的网络的源地址为上述列表中IP地址的数据包。 下面是一个配置的例子： Router# conf tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# ip access-list ext ingress-antispoofRouter(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 anyRouter(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any Router(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 any Router(config-ext-nacl)# deny ip 127.0.0.0 0.255.255.255 anyRouter(config-ext-nacl)# deny ip 224.0.0.0 31.255.255.255 anyRouter(config-ext-nacl)# deny ip 169.254.0.0 0.0.255.255 any Router(config-ext-nacl)# permit ip any any Router(config-ext-nacl)# exitRouter(config)#int s0/0Router(config-if)#ip access-group ingress-antispoof in互联网服务供应商（ISP）必须在其网络中使用这样的过滤，这一点是在RFC 2267中定义的。注意此ACL操作中包含“ permit ip any any ”。在现实世界中，你可能会在路由器中有一个正式的防火墙，用以保护内部LAN。 当然，你可以将此方法用于过滤所有进入本机所在子网的、来自网络内部其它子网的数据包，以确保不在某子网内的任何人不会将欺骗性的数据通信传到其它网络。你也可以实施一个“ 转出ACL ”来防止内

部网络从其它网络实施IP地址欺骗。不过，请记住，这仅是你全局网络安全策略的一个局部而已。 使用反向路径转发(IP验证) 另一个保护网络免受IP地址欺骗的方法是反向路径转发（RPF），即IP验证。在思科的IOS中，用于反向路径转发（RPF）的命令是以“ ip verify ”开始的。 RPF在工作起来就象一个反垃圾邮件解决方案的部分功能一样，该功能部分收到进入的电子邮件消息，找到源电子邮件的源地址，然后到发送服务器上执行一个检查操作，确定发送者是否真的存在于发送消息的服务器上。如果发送者不存在，服务器就丢弃此电子邮件消息，因为它极有可能是一个垃圾邮件。 RPF对数据包作出相似的操作。它取出所收到的来自互联网的某个数据包的源地址，查看在路由器的路由表中是否存在一个路由可以应答此数据包。如果路由表中没有路由来作为返回给源IP地址的数据包的应答，那么就是有人发送了欺骗性数据包，路由器就丢弃这个数据包。 下面展示怎样在路由器中配置反向地址转发： Router(config)# ip cefRouter(config)# int serial0/0Router(config-if)# ip verify unicast reverse-path保护私有网络免受攻击者的侵害是极端重要的。我们在这里介绍的三个方法将对你保护网络免受IP地址欺骗起到重要的作用。