局域网盗用IP地址的安全问题 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/269/2021_2022__E5_B1_80_E5_9F_9F_E7_BD_91_E7_c67_269288.htm 一、IP地址盗用方法分析 IP地址的盗用方法多种多样，其常用方法主要有以下几种： 1、静态修改IP地址 对于任何一个TCP/IP实现来说，IP地址都是其用户配置的必选项。如果用户在配置TCP/IP或修改TCP/IP配置时，使用的不是授权机构分配的IP地址，就形成了IP地址盗用。由于IP地址是一个逻辑地址，是一个需要用户设置的值，因此无法限制用户对于IP地址的静态修改，除非使用DHCP服务器分配IP地址，但又会带来其它管理问题。 2、成对修改IP-MAC地址 对于静态修改IP地址的问题，现在很多单位都采用静态路由技术加以解决。针对静态路由技术，IP盗用技术又有了新的发展，即成对修改IP-MAC地址。MAC地址是设备的硬件地址，对于我们常用的以太网来说，即俗称的计算机网卡地址。每一个网卡的MAC地址在所有以太网设备中必须是唯一的，它由IEEE分配，是固化在网卡上的，一般不能随意改动。但是，现在的一些兼容网卡，其MAC地址可以使用网卡配置程序进行修改。如果将一台计算机的IP地址和MAC地址都改为另外一台合法主机的IP地址和MAC地址，那静态路由技术就无能为力了。 另外，对于那些MAC地址不能直接修改的网卡来说，用户还可以采用软件的办法来修改MAC地址，即通过修改底层网络软件达到欺骗上层网络软件的目的。 3、动态修改IP地址 对于一些黑客高手来说，直接编写程序在网络上收发数据包，绕过上层网络软件，动态修改自己的IP地址（或IP-MAC地址对），达到IP

欺骗并不是一件很困难的事。 二、防范技术研究 针对IP盗用问题，网络专家采用了各种防范技术，现在比较通常的防范技术主要是根据TCP/IP的层次结构，在不同的层次采用不同的方法来防止IP地址的盗用。 1、交换机控制 解决IP地址的最彻底的方法是使用交换机进行控制，即在TCP/IP第二层进行控制：使用交换机提供的端口的单地址工作模式，即交换机的每一个端口只允许一台主机通过该端口访问网络，任何其它地址的主机的访问被拒绝。但此方案的最大缺点在于它需要网络上全部采用交换机提供用户接入，这在交换机相对昂贵的今天不是一个能够普遍采用的解决方案。 2、路由器隔离 采用路由器隔离的办法其主要依据是MAC地址作为以太网卡地址全球唯一不能改变。其实现方法为通过SNMP协议定期扫描校园网各路由器的ARP表，获得当前IP和MAC的对照关系，和事先合法的IP和MAC地址比较，如不一致，则为非法访问。对于非法访问，有几种办法可以制止，如： a.使用正确的IP与MAC地址映射覆盖非法的IP-MAC表项； b.向非法访问的主机发送ICMP不可达的欺骗包，干扰其数据发送； c.修改路由器的存取控制列表，禁止非法访问。 路由器隔离的另外一种实现方法是使用静态ARP表，即路由器中IP与MAC地址的映射不通过ARP来获得，而采用静态设置。这样，当非法访问的IP地址和MAC地址不一致时，路由器根据正确的静态设置转发的帧就不会到达非法主机。 路由器隔离技术能够较好地解决IP地址的盗用问题，但是如果非法用户针对其理论依据进行破坏，成对修改IP-MAC地址，对这样的IP地址盗用它就无能为力了。 3、防火墙与代理服务器 使用防火墙与代理服务器相结合，也能较好地解决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应用。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，增加了用户操作的麻烦；另外，对于大数量的用户群（如高校的学生）来说，用户管理也是一个问题。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com