校园网络中 IP 地址盗用与防范技术

The Technology To Prevent For Embezzling IP Address In Campus Network

王 智 （新疆石河子工程技术学校 新疆石河子 832000）

摘要：在校园网络中若有两台主机 IP 地址相同，则两台主机相互报警，造成网络混乱。因此，IP 地址盗用成了网管员最头疼的问题。当几百台、甚至上千台主机同时上网，如何控制 IP 地址盗用？

关键词：IP 地址 MAC 地址 路由器 防火墙

1 引言

随着 Internet 网络的普及与发展，大中专院校都已组建自己的校园网络，采用专线方式或光纤接入互联网。校园网络管理部门在规划自己的内部网段时，为用户分配并制定了相应的网络 IP 地址资源，以保证通信数据的正常传输。网络管理员在配置 IP 地址资源时，应满足下面两个方面要求，第一，分配的地址应在规划的子网网段范围内；第二，分配的 IP 地址对任何联网的主机必须是惟一的。在校园网络中若有两台主机的 IP 地址相同，则两台主机将相互报警，且无法上网，造成网络混乱。在校园网络上任何用户使用未经授权的 IP 地址称为 IP 地址盗用，因此，IP 地址盗用成了网管人员最头疼的问题。当几百台、甚至上千台主机同时上网，如何防止 IP 地址盗用问题，是维护网络正常运行的必要技术手段。

在实际运行中，网络管理员负责管理用户 IP 地址的分配，通过正确地注册后才认为是合法用户。但在校园网络上使用未经授权的 IP 地址，将在校园网络运行时可产生以下结果：第一、非法的 IP 地址；即 IP 地址不在规划的校园网络范围之内，第二、重复的 IP 地址；与已经分配且正在校园网络内运行的合法的 IP 地址发生资源冲突，使合法用户无法上网；第三、盗用合法用户的 IP 地址；如果不对网络采取各种防范措施，将影响网络的正常运行及用户的合法权益受到侵害。

2 IP 地址盗用方法

IP 地址的盗用方法多种多样，其常用方法主要有以下几种：

2.1 静态修改 IP 地址

对于任何一个网络用户来说，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，使用的不是网络管理员分配的 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。

2.2 成对修改 MAC 地址和 IP 地址

对于静态修改 IP 地址的问题，可以采用静态路由技术加以解决，即 IP－MAC 地址绑定。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。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，那么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。

2.3 IP 电子欺骗

IP 电子欺骗就是指伪造某台主机的 IP 地址的技术。IP 欺骗通常需要用编程来实现。通过使用 SOCKET 编程，发送带有假冒的源 IP 地址的 IP 数据包。对于网络编程高手来说，绕过上层网络软件，动态修改自己的 IP 地址，达到 IP 欺骗并不是一件很困难的事。

3 防范 IP 地址盗用技术

针对 IP 盗用的问题，网络专家采用了各种防范技术，现在比较常用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。

3.1 交换机控制

解决 IP 地址盗用最有效的方法是使用交换机进行控制，即在 TCP/IP 第二层（数据链路层）进行控制。在可网络管理的交换机中都有 Prot－MAC 地址绑定功能。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访问都被拒绝。

通过交换机端口管理，可以在实际使用中迅速发现并阻断 IP 地址的盗用行为，尤其是解决了 IP－MAC 成对盗用的问题，同时也不影响网络的运行效率。

3.2 路由器隔离

采用路由器隔离的办法，主要依据是 MAC 地址作为以太网卡物理地址全球唯一不能改变，在网络层实现 IP 与相应的 MAC 地址绑定以防范 IP 地址盗用，其实现方法是通过 SNMP 协议定期扫描校园网络路由器的 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：第一、使用正确的 IP 与 MAC 地址映射覆盖非法的 IP－MAC 表项；第二、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；第三、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了静态修改 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。

3.3 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，这是一种在应用层上解决 IP 盗用的办法。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。任何上网用户需要到网络管理部门申请帐户和口令，即变 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网络的应用。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，而无帐户的用户即使盗用 IP，也没有用户名和密码，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来说，增加用户管理的难度。

4 结束语

通过以上几种方法有效地解决了校园网络 IP 地址盗用问题，但仍然有可能存在未经授权的用户使用未经授权的 IP 地址而造成 IP 冲突，侵犯合法用户的权益。尽管盗用者无法使用该 IP，但给网络带来了混乱。我们可以利用网络交换设备的网络管理功能，完善检测手段，提高网络故障的检测能力，迅速准确地定位和查找故障主机点。

随着网络设备功能的日趋完善和网络管理人员的管理水平的提高，会有更多更好的防止 IP 盗用的方法。

参考文献

1 《计算机网络技术》[M] 段博原编，科学出版社，2003.12。
2 《网络安全实用技术标准教程》[M]，李伟编，清华大学出版社，2005.7。
3 《计算机网络安全应用基础》[M]，杨富国编，清华大学出版社，2005.1。