局域网内 IP 地址防盗技术研究

Research Technology to Prevent for Embezzling IP Address in LAN

吴军强 （嘉兴学院 数学与信息工程学院 浙江嘉兴 314001）

摘 要: 本文首先介绍了 IP 地址盗用的概念及常用的 IP 地址盗用方法，然后主要分析了目前常用的 IP 地址防盗技术的工作原理和缺点，最后结合笔者的实际应用给出了一种既操作简单，又管理方便的防盗方法。该方法能快速地解决局域网环境中 IP 地址盗用问题。

关键词: IP 地址 MAC 地址 IP 地址盗用 防盗技术

1 引言

IP 地址盗用是指在局域网中，盗用者将本机的 IP 地址修改为本子网内的另外一个合法用户的 IP 地址或未分配的 IP 地址，然后利用该 IP 地址去访问网络，以达到非法使用网络资源或隐藏身份从事非法活动的行为。这样，一切基于该 IP 地址的控制或计费都会发生错误，从而影响合法用户的网络的正常使用，侵害了网络正常用户的合法权益，给网络带来了巨大的安全隐患和管理难度。

Internet 是建立在 TCP/IP 协议上的互联网络。在 TCP/IP 网络环境下，每个主机都分配了一个 IP 地址。IP 地址是标识主机的一种逻辑地址，用户可以任意设置和修改。如有两台或多台主机 IP 地址相同，则两台或多台主机将相互报警，且无法上网，造成网络混乱。另外，当局域网中的主机 A 处于关机状态时，主机 B 就可以使用 A 的 IP 地址登录并进行各种 Internet 访问。当局域网内几百台、甚至上千台主机同时上网时，如何防止 IP 地址盗就显得非常重要，是维护网络正常运转的必要技术手段。

2 IP 地址盗用的常用方法

IP 地址的盗用方法多种多样，常用的主要有以下几种[1]。

2.1 静态修改 IP 地址配置

对于任何一个 TCP/IP 实现来说，IP 地址是用户配置的必选项。如果用户在配置 TCP/IP 选项时，使用的不是管理员分配的 IP 地址，就形成了 IP 地址的盗用。由于 IP 地址是一个逻辑地址，因此无法限制用户对于 IP 地址的静态修改，但如果使用 DHCP 服务器动态分配 IP 地址，又会给管理带来很多其它问题。

2.2 同时修改 MAC 地址和 IP 地址

MAC 地址是设备的硬件地址，对于以太网来说，即俗称的网卡地址。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，固化在网卡上，一般不能随意改动。但是，一些兼容网卡的 MAC 地址却可以使用配置程序修改。

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 电子欺骗就是通过伪造 IP 地址的方法，使某台主机能够伪装成另外一台主机与其它的机器进行通信。IP 电子欺骗通常需要使用 SOCKET 编程，发送带有假冒的源 IP 地址的 IP 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。

3 常用 IP 地址防盗技术分析

针对 IP 地址盗用现象，现在比较流行的防范技术

主要是依据 TCP/IP 的层次结构原理，在不同的层次采用不同的方法来防止 IP 地址的盗用。常用的防范技术主要有划分 VLAN、IP – MAC 地址捆绑技术、代理服务器技术、IP – MAC – USER 认证授权技术等[1] [2]。

3.1 静态路由技术

根据接入互联网的 IP 地址管理是通过 IP 地址分配和路由器的配置来实现的原理，可以通过设置路由器的静态 ARP 表，解决 IP 地址和 MAC 地址的绑定，保证合法 IP 地址的惟一性。这样就解决了同网段的 IP 地址盗用问题。因为在一个网段内的网络寻址不是依靠 IP 而是 MAC 地址。因此在网段的路由器上有 IP 和 MAC 的动态对应表，这是由 ARP 协议生成并维护的。配置路由器时，可以指定静态的 ARP 表，路由器会根据静态的 ARP 表检查数据包，如果不能对应，则不进行处理。

3.2 交换机控制技术

尽管采取了 IP 地址与 MAC 地址的绑定措施，但在 WINDOWS 操作系统的‘控制面板\网络\网卡\属性\高级\Network Address\设置’中，用户可以随意修改主机的 MAC 地址。这样就可以同时盗用合法用户的 IP 及 MAC 地址。这样静态路由技术就不能解决问题了。采用交换机的 VLAN 虚拟子网技术和交换机端口绑定技术可解决问题。

3.2.1 VLAN 划分法

采用交换机的 VLAN 虚拟子网技术，可控制一段 IP 地址在某一 VLAN 中使用，而在其他 VLAN 中无效。在不同 VLAN 之间采用具有三层交换功能的交换机，既能保证交换式网络的速度，又可以有效的进行网络隔离控制。这种方法可防止不同 VLAN 之间的 IP 地址盗用，但在同一 VLAN 的有效 IP 范围内，仍然会出现 IP 盗用。

3.2.2 交换机端口绑定法

交换机端口绑定法要求网络中的交换机要具有可管理功能。在可管理的交换机中都有端口 – 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的访问将被拒绝。

3.3 路由器隔离技术

检测和保护网络免受 IP 电子欺骗的最好办法是安装过滤路由器。对于来自网络外部的 IP 电子欺骗，阻止的方法很简单，在局域网对外的路由器上加一个限制条件，只要在路由器上设置不允许声称来自内部的网络的外来包通过就行了。

这种技术能够较好地解决 IP 地址的盗用问题，但对非法用户成对修改 IP – MAC 地址的 IP 地址盗用无能为力。

3.4 防火墙与代理服务器技术

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。利用防火墙与代理服务器相结合的技术，通过身份认证取得访问网络的权限才能够访问外部网络。使用这样的办法是将 IP 防盗放到应用层来解决，将 IP 地址的管理转换成对用户及口令的管理。

这种技术可以很好解决盗用者访问外部网，对于同时盗用 IP 地址和 MAC 地址的盗用行为有一定的作用。但对于非法用户盗用内部网合法用户 IP 地址无能为力，并且由于使用代理服务器访问外部网络很容易产生瓶颈问题，在一定程度上会影响用户访问网络的速度。

3.5 ARP 伪装防盗技术

ARP 伪装防盗技术采用纯软件的解决办法，在每个子网内安装一个 IP 防盗用软件系统，并建立子网内合法用户的 IP 地址 – MAC 地址 – IP 开关状态标志，由 IP 防盗用软件根据子网的 IP – MAC 地址库实现 IP 地址与主机 MAC 地址的绑定，任一子网内的主机只有使用在 IP – MAC 地址库中登记的且与其 MAC 地址对应的 IP 地址，才能进行正常的网络通信，从而在整个局域网实现 IP 防盗用。

这种技术对成对修改 IP – MAC 地址和动态修改 IP 地址的 IP 地址盗用方式进行一定的防范。但每个子网都要安装 IP 防盗用软件系统，给网络管理员的维护工作带来了不便。

3.6 透明网关过滤技术

透明网关过滤技术是一种结合静态路由和防火墙的优点，使用 IP – MAC – USER 模型来进行授权验证，以实现防止 IP 地址盗用。其工作原理是：实现一个透明网关，该网关跨接在内部网络和外部网络之间，对于内部主机访问外部网络，在使用 ARP 获取外部主机或路由器地址时，验证其 IP – MAC 地址对，不匹配的非法主机不能获得 ARP 应答信息，因而不能继续和外部

网络通讯,对于外部主机访问内部网络,则采用静态路由,使 IP – MAC 地址对不匹配的内部主机接收不到正确的 IP 包。另外,为了防止 IP – MAC 地址成对修改的情况,在外部 IP 包经过透明网关时,如果其源地址为国外主机,则还要检测其目的主机是否有用户注册,若没有用户注册,则其 IP 包被丢弃;有用户注册则 IP 包被转发进去,同时将 IP 流量记入该用户的账上。这样,即使用户成对修改了 IP – MAC 地址,如果没有合法的用户注册,它仍不能访问外部网络,盗用 IP 地址失去意义。

这种技术的缺点是不能实现定位和反向追踪盗用行为,即无法获知盗用者。

3.7 动态配置 MAC 地址技术

动态配置 MAC 地址技术的工作原理是:设计一个 C/S 程序,合法用户都有一个用户名和密码,用户的机器运行客户端程序,局域网的服务器运行服务器端程序。客户端在用户关机前,向服务器申请修改客户端的 MAC 地址,服务器收到申请后,随机动态配置一个 MAC 地址给该客户端,该 MAC 地址不会与在数据库中的整个内部网络其他 MAC 地址冲突,客户端在收到服务器返回的 MAC 地址后,对本机 MAC 地址做出修改,然后正常关机。用户可以在客户端软件中保存用户名和密码,这样全部动态配置和认证过程可以在用户正常使用网络的同时,由软件自动在后台进行,对用户使用网络不会有干扰和影响。用户在每次开机连入网络时,都使用不同的 MAC 地址,当用户在使用网络时,盗用者即使通过某些手段获取该用户的 IP – MAC 地址对,也无法盗用,因为网络系统会发生地址冲突,而当该用户下一次开机时,会使用新申请的 MAC 地址进入网络,这样盗用者将始终无法盗用 IP – MAC 地址对。

这种技术和透明网关过滤技术一样不能实现 IP 盗用的逆向寻踪,即无法获知盗用者。

3.8 802.1x 认证技术

近来,随着 802.1x 协议的标准化,一些 L2/L3 厂家开始推广 802.1x 认证,又称 EAPOE 认证。802.1x 协议仅仅关注端口的打开与关闭,对于合法用户(根据账号和密码)接入时,该端口打开,而对于非法用户接入或没有用户接入时,则该端口处于关闭状态。认证的结果在于端口状态的改变,而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题,是各种认证技术中最简化的实现方案。

目前,各厂商所称道 802.1x 的优势和安全性很大程度上依赖于私有拨号客户端。如果一旦客户端被破解,或者被仿造,那么很多功能将形如虚设,比如限制代理服务器的使用、绑定 IP、客户端版本的限制等。

4 用“超级网管(SuperLANadmin)”多方式防止 IP 盗用

根据笔者维护网络的经验,使用“超级网管(SuperLANadmin)”不但可以多方式有效地防止 IP 地址被盗用,而且既操作简单,又管理方便。

4.1 绑定 IP 地址与网卡 MAC 地址

在“超级网管(SuperLANadmin)”中选择要绑定的计算机,在“网络管理”中单击“MAC 绑定”即可完成单台计算机的绑定操作。也可以一次性对局域网中的某个工作组内的计算机或网内所有计算机进行 MAC 地址的绑定。

图 1 绑定 IP 地址与网卡 MAC 地址

4.2 锁定未分配的 IP 地址

虽然绑定 IP 地址与网卡 MAC 地址后,已使用的 IP 地址不会再被盗用,但是还有一些未分配的 IP 地址,可能会被盗用。单击“IP 锁定”,再单击“新增 IP 锁定段”,输入要锁定的 IP 地址段,确定后指定的 IP 地址就被锁定了。

4.3 检查并解决 IP 地址盗用

在网络的维护过程中,随时可对 IP 地址登记情况进行检查。单击“IP 盗用”,可将网内所有使用的 IP 地址及计算机与原有的保存记录进行对比,进而判断有无 IP 地址被盗用。

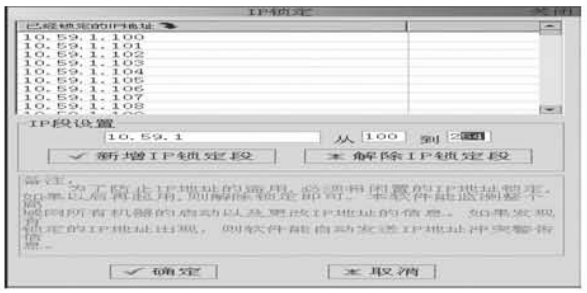

图 2　锁定未分配的 IP 地址

图 3　检查 IP 地址有无盗用

如果出现 IP 地址盗用，可以强迫其退出网络。选择盗用者主机，单击“IP 冲突”，在对话框中输入盗用者 IP 地址，选择发送 IP 冲突次数。单击“发送”后，盗用者的电脑上将显示 Windows 系统错误窗口，提示 IP 地址发生冲突，并无法再使用网络。

被盗用的 IP 地址找回后需重新登记。单击“IP 登记”，输入找回的 IP 地址和原来主机网卡的 MAC 地址，为该主机建立一个主机名，确定后即可让原来的用户重新使用该 IP 地址了。

5　结束语

IP 地址的管理是网络管理中一个重要的方面。针对 IP 地址盗用技术，我们要根据每个单位网络的具体情况而采取相应的防范措施。同时，还应加强用户的网络安全与网上职业道德教育，提高用户的网络安全意识和上网素质。

参考文献

1　翁小兰. 校园网环境下 IP 地址盗用防范技术研究[J]. 微计算机应用，2005，26(6)：684－686.

2　陈志平. 校园网络安全与防火墙技术[J]. 现代计算机，2007，(1)：47－49.