Cisco3550交换机MAC地址的访问控制 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/251/2021_2022_Cisco3550_E4_c101_251119.htm 在网络管理工作中，常常会碰到这样的情况：某些用户违反管理规定，私自修改自已的IP地址，以达到访问受限资源的目的。这样的行为，不但破坏了信息安全规则，还可能因为地址冲突引起网络通讯故障。 网管管理员可能会试图使用如后文所述的各种技术手段来解决这一问题，但效果不一定很理想：首先技术手段无法完全阻止这种现象的发生，其次是增加了管理的复杂性和成本。所以遏制这种现象最有效的方法是行政手段，这是技术手段所无法替代的。 在介绍这些管理手段之前我们先来看一个模拟的环境：工作站PC和SERVER连接到一台Cisco Catalyst 3550交换机上，它们分属不同的VLAN，借助3550的路由功能进行通讯（附交换机配置）：hostname Cisco3550!interface GigabitEthernet0/11 description Connect to PC!interface GigabitEthernet0/12 description Connect to SERVER switchport access vlan 2!interface Vlan1ip address 1.1.1.254 255.255.255.0!interface Vlan2 ip address 2.1.1.254 255.255.255.0 如果不需要做权限限制，只是要防止IP地址冲突的话，最佳的方案可能是使用DHCP.DHCP 服务器可以为用户设置IP 地址、子网掩码、网关、DNS等参数，使用方便，还能节省IP地址。在Cisco设备上设置DPCP可以参考：《Cisco路由器上配置DHCP全程详解 》.静态的分配和设置需要较多管理开销，如果用户不捣乱的话，由于用户名和IP地址一一对应，维护起来比较方便，以下均假设采用的是静态的管理方法。 测试1.假设VLAN1内只允许IP 1.1.1.1 访

问Server： 2.1.1.1，其它访问全部禁止。 限制方法：使用IP访问控制列表interface Vlan1ip address 1.1.1.254 255.255.255.0ip access-group 100 in! access-list 100 permit ip host 1.1.1.1 host 2.1.1.1 突破方法：非法用户将IP地址自行改为 1.1.1.1即可访问Server. 非法用户抢占地址1.1.1.1将会引起IP地址冲突问题。如果用户将IP地址设成网关的IP，还会影响到整个VLAN的通讯。通过修改Windows 设置，可以防止用户修改“ 网络 ”属性，但这一方法也很容易被突破。 测试2.在测试1的基础上加上静态ARP绑定可以防止IP地址盗用。 实现方法：在测试1配置的基础上设置arp 1.1.1.1 0001.0001.1111 ARPA 注意以下的命令是错误的，因为ARP的端口参数是三层（路由）端口而非二层（交换）端口： arp 1.1.1.1 0001.0001.1111 ARPA GigabitEthernet0/11 设置完成之后，如果非法用户把地址改为1.1.1.1，它发送到路由器的包正常，但是从目标服务器2.1.1.1返回的数据包在路由器上转发的时候，目标MAC地址将总是设为0001.0001.1111，非法用户不能接收。 类似办法：使用“ ARP SERVER ”按一定的时间间隔广播网段内所有主机的正确IP-MAC映射表 突破方法：修改MAC地址很容易，在Windows网络连接设置修改网卡的配置，在“ 高级 ”页面中找到Network Address设置为指定的值即可。 测试3.使用Port Secure 原理：如果限制了指定端口只能被特定MAC地址的机器，用户若更改了MAC地址端口将会进入不可用状态。 设置方法：interface g 0/1switchport mode access switchport port-security 设置完成之后，交换机端口上首次连接的PC的MAC地址将会记录到交换机中，成为唯一能够使用该端口的MAC地址。如果该PC更换MAC地址，默认将会使用端口

置于shutdown状态，无法与网络连通。 可以使用命令设置安全冲突的处理方法： sw port-security violation [protect | restrict | shutdown] protect 丢弃来自非法源地址的包，不告警 restrict 丢弃来自非法源地址的包，发送syslog告警 shutdown（默认）关闭端口，发送SNMP trap、Syslog 告警，除非管理员执行命令shut/no shut，否则端口一直处理down状态。 突破方法：代理服务器。用户在同一VLAN内能够对外访问的主机上安装代理服务器，通过代理访问。 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