综合辅导：防止VLAN间的ARP攻击 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/240/2021_2022__E7_BB_BC_E5_90_88_E8_BE_85_E5_c101_240545.htm 针对目前出现的流行ARP欺骗攻击行为，提出Cisco的解决方案。 但是，我实验下来，这个能够防止攻击核心层Gateway，但是不能很有效的防止各VLAN间的攻击，防止VLAN间的攻击，我认为用VLAN内的VACL防止比较好，安全性能才能提高。 由于公司交换设备用的是OMNI 但是安全方面应该也有相关设置作简单演示，不去深入 100 3/12 default inactive 利用无用端口演示下6602-SHA-15F> port-security 3/12 enable6602-SHA-15F> port-security 3/12 maximum 106602-SHA-15F> port-security 3/12 violation ? ^ SHUTDOWN RESTRICT CISCO具体方案： 在全部是Cisco交换网络里，可以通过帮定每台设备的ip和mac地址可以解决。但是这样做比较麻烦，可以用思科 Dynamic ARP Inspection 机制解决。 （*注释：用port-security，必定是access口） 防范方法 ： 思科 Dynamic ARP Inspection （DAI）在交换机上提供IP地址和MAC地址的绑定， 并动态建立绑定关系。DAI 以 DHCP Snooping绑定表为基础，对于没有使用DHCP的服务器个别机器可以采用静态添加ARP access-list实现。DAI配置针对VLAN，对于同一VLAN内的接口可以开启DAI也可以关闭。通过DAI可以控制某个端口的ARP请求报文数量。所以，我认为，通过这样的配置，可以解决ARP攻击问题，更好的提高网络安全性和稳定性。 配置： IOS 全局命令：ip dhcp snooping vlan 100,200 ,300,400no ip dhcp snooping information option ip dhcp snooping ip arp inspection vlan 100,200

,300,400ip arp inspection log-buffer entries 1024 ip arp inspection log-buffer logs 1024 interval 10 IOS 接口命令：ip dhcp snooping trust ip arp inspection trust ip arp inspection limit rate 15 对于没有使用 DHCP 设备可以采用下面办法：arp access-list static-arp permit ip host 202.65.3.42 mac host 0012.3F82.1B22ip arp inspection filter static-arp vlan 201 配置DAI后的效果： 由于 DAI检查 DHCP snooping绑定表中的IP和MAC对应关系，无法实施中间人攻击，攻击工具失效。下表为实施中间人攻击是交换机的警告：3w0d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa5/16, vlan 1.([000b.db1d.6ccd/192.168.1.200/0000.0000.0000/192.168.1.2 由于对 ARP请求报文做了速度限制，客户端无法进行认为或者病毒进行的IP扫描、探测等行为，如果发生这些行为，交换机马上报警或直接切断扫描机器。如下表所示：3w0d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 184 milliseconds on Fa5/30. ******报警 3w0d: %PM-4-ERR_DISABLE: arp-inspection error detected on Fa5/30, putting Fa5/ 30 in err-disable state ******切断端口 4500-1#sh int f 5/30 FastEthernet5/30 is down, line protocol is down (err-disabled) Hardware is Fast Ethernet Port , address is 0002.b90e .3f 4d (bia 0002.b90e .3f 4d) MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255 4500-1# 用户获取 IP 地址后，用户不能修改IP或MAC，如果用户同时修改IP和MAC必须是网络内部合法的IP和MAC才可，对于这种修改可以使用下面讲到的 IP Source Guard技术来防范。下表为手动指定IP的报警：3w0d:

%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa5/30, vlan 1.([000d.6078.2d95/192.168.1.100/0000.0000.0000/192.168.1.100/01:52:28 UTC Fri Dec 29 2000]) DAI支持的平台是3560以上吧，IP Source Guard 只有4500以上才能执行貌似。 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