Cisco交换机防止VLAN间的ARP攻击方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/287/2021_2022_Cisco_E4_BA_A4_E6_8D_c101_287836.htm 很多交换机都能够防止ARP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