CISCODAI防ARP攻击思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_CISCODAI_E9_98_c101_644081.htm 配置局域网的安全特性，防止地址乱配，ARP攻击等弊病！ 1、启用DHCP SNOOPING 全局命令：ip dhcp snooping vlan 10,20,30 no ip dhcp snooping information option ip dhcp snooping database flash:dhcpsnooping.text //将snooping表保存到单独文档中，防止掉电后消失。 ip dhcp snooping 接口命令: ip dhcp snooping trust //将连接DHCP服务器的端口设置为Trust，其余unTrust（默认） 2、启用DAI 防止ARP欺骗和中间人攻击！通过手工配置或者DHCP监听snooping，交换机将能够确定正确的端口。如果ARP应答和snooping不匹配，那么它将被丢弃，并且记录违规行为。违规端口将进入err-disabled状态，攻击者也就不能继续对网络进行进一步的破坏了！ 全局命令 ip arp inspection vlan 30 接口命令（交换机之间链路配置DAI信任端口，用户端口则在默认的非信任端口）：ip arp inspection trust ip arp inspection limit rate 100 3、启用IPSG 前提是启用IP DHCP SNOOPING，能够获得有效的源端口信息。cisco认证网，加入收藏IPSG是一种类似于uRPF（单播反向路径检测）的二层接口特性，uRPF可以检测第三层或路由接口。 接口命令：switchport mode acc switchport port-security ip verify source vlan dhcp-snooping port-security 4、关于几个静态IP的解决办法 可通过ip dhcp snooping binding 1.1.1 vlan 1 1.1.1.1 interface gi0/8 通过arp access-list添加静态主机: arp access-list static-arp permit ip host 192.168.1.1 mac host 0000.0000.0003 ip arp inspection filter

static-arp vlan 30 DHCP 中绑定固定IP： ip dhcp pool test host 192.168.1.18 255.255.255.0 （分给用户的IP） client-identifier 0101.0bf5.395e.55（用户端mac） client-name test 开展及总结：思科交换机在全局配置模式下开启IP DHCP SNOOPING后，所有端口默认处于DHCP SNOOPING UNTRUSTED模式下，但DHCP SNOOPING INFORMATION OPTION功能默认是开启的，此时DHCP报文在到达一个SNOOPING UNTRUSTED端口时将被丢弃。因此，必须在4506配置IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED命令（默认关闭），以允许4506从DHCP SNOOPING UNTRUSTED端口接收带有OPTION 82的DHCP REQUEST报文。建议在交换机上关闭DHCP INFORMATION OPTION，即全局配置模式下NO IP DHCP SNOOPING INFORMATION OPTION。 1、对于允许手工配置IP地址等参数的客户端，可以手工添加绑定条目到DHCP SNOOPING BINDING数据库中。ip dhcp snooping binding 00d0.2bd0.d80a vlan 100 222.25.77.100 interface gig1/1 expiry 600表示手工添加一条MAC地址为00d0.2bd0.d80a，IP地址为222.25.77.100，接入端口为GIG1/1，租期时间为600秒的绑定条目。 2、IPSG即IP SOURCE GUARD是在DHCP SNOOPING功能的基础上，形成IP SOURCE BINDING表，只作用在二层端口上。启用IPSG的端口，会检查接收到所有IP包，只转发与此绑定表的条目相符合的IP包。默认IPSG只以源IP地址为条件过滤IP包，如果加上以源MAC地址为条件过滤的话，必须开启DHCP SNOOPING INFORMAITON OPTION 82功能。 3、DAI即DYNAMIC ARP INSPECTION也是以DHCP SNOOPING BINDING DATABASE

为基础的，也区分为信任和非信任端口，DAI只检测非信任端口的ARP包，可以截取、记录和丢弃与SNOOPING BINDING中IP地址到MAC地址映射关系条目不符的ARP包。如果不使用DHCP SNOOPING，则需要手工配置ARP ACL。