MAC_CAM攻击的防范思科认证 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_MAC_CAM_E6_94_BB_c101_644149.htm 1.1MAC/CAM攻击的原理和危害 交换机主动学习客户端的 MAC 地址，并建立和维护端口和 MAC 地址的对应表以此建立交换路径，这个表就是通常我们所说的 CAM 表。 CAM 表的大小是固定的，不同的交换机的 CAM 表大小不同。 MAC/CAM 攻击是指利用工具产生欺骗 MAC，快速填满 CAM 表，交换机 CAM 表被填满后，交换机以广播方式处理通过交换机的报文，这时攻击者可以利用各种嗅探攻击获取网络信息。 CAM 表满了后，流量以洪泛方式发送到所有接口，也就代表 TRUNK 接口上的流量也会发给所有接口和邻接交换机，会造成交换机负载过大，网络缓慢和丢包甚至瘫痪。 1.2典型的病毒利用MAC/CAM攻击案例 曾经对网络照成非常大威胁的 SQL 蠕虫病毒就利用组播目标地址，构造假目标 MAC 来填满交换机 CAM 表。 1.3使用 Port Security feature 防范MAC/CAM攻击 思科 Port Security feature 可以防止 MAC 和 MAC/CAM 攻击。通过配置 Port Security 可以控制： 端口上最大可以通过的 MAC 地址数量 端口上学习或通过哪些 MAC 地址 对于超过规定数量的 MAC 处理进行违背处理 端口上学习或通过哪些 MAC 地址，可以通过静态手工定义，也可以在交换机自动学习。交换机动态学习端口 MAC，直到指定的 MAC 地址数量，交换机关机后重新学习。目前较新的技术是 Sticky Port Security，交换机将学到的 mac 地址写到端口配置中，交换机重启后配置仍然存在。 对于超过规定数量的 MAC 处理进行处理一般有三种方式

（针对交换机型号会有所不同）： Shutdown 。这种方式保护能力最强，但是对于一些情况可能会为管理带来麻烦，如某台设备中了病毒，病毒间断性伪造源 MAC 在网络中发送报文。 Protect 。丢弃非法流量，不报警。 Restrict 。丢弃非法流量，报警，对比上面会是交换机 CPU 利用率上升但是不影响交换机的正常使用。推荐使用这种方式。 1.4配置 port-security 配置选项： Switch(config-if)# switchport port-security ? aging Port-security aging commands mac-address Secure mac address maximum Max secure addresses violation Security violation mode 配置 port-security 最大 mac 数目，违背处理方式，恢复方法 Cat4507(config)#int fastEthernet 3/48 Cat4507 (config-if)#switchport port-security Cat4507 (config-if)#switchport port-security maximum 2 Cat4507 (config-if)#switchport port-security violation shutdown Cat4507 (config)#errdisable recovery cause psecure-violation Cat4507 (config)#errdisable recovery interval 30 通过配置 sticky port-security学得的MAC interface FastEthernet3/29 switchport mode access switchport port-security switchport port-security maximum 5 switchport port-security mac-address sticky switchport port-security mac-address sticky 000b.db1d.6ccd switchport port-security mac-address sticky 000b.db1d.6cce switchport port-security mac-address sticky 000d.6078.2d95 switchport port-security mac-address sticky 000e.848e.ea01 编辑特别推荐: 成本速度成关键解析 四种宽带接入技术 常用TCP端口作用及其操作建议 统一通信将成为IP语音未来发展趋势 提高企业网络可靠性的捷径 防御攻击策略之保持领先黑客一步 网络安全八个潜规则