详细介绍Cisco交换机端口安全 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__E8_AF_A6_E7_BB_86_E4_BB_8B_E7_c101_251097.htm 在Cisco中有以下三种方案可供选择，方案1和方案2实现的功能是一样的，即在具体的交换机端口上绑定特定的主机的MAC地址（网卡硬件地址），方案3是在具体的交换机端口上同时绑定特定的主机的MAC地址（网卡硬件地址）和IP地址。 方案1基于端口的MAC地址绑定： 思科2950交换机为例，登录进入交换机，输入管理口令进入配置模式，敲入命令：Switch#config terminal ＃进入配置模式Switch(config)# Interface fastethernet 0/1 ＃进入具体端口配置模式Switch(config-if)switchport port-security mac-address MAC(主机的MAC地址) ＃配置该端口要绑定的主机的MAC地址Switch(config-if)no switchport port-security mac-address MAC(主机的MAC地址) ＃删除绑定主机的MAC地址 注意：以上命令设置交换机上某个端口绑定一个具体的MAC地址，这样只有这个主机可以使用网络，如果对该主机的网卡进行了更换或者其他PC机想通过这个端口使用网络都不可用，除非删除或修改该端口上绑定的MAC地址，才能正常使用。（以上功能适用于思科2950、3550、4500、6500系列交换机） 方案2基于MAC地址的扩展访问列表Switch(config)Mac access-list extended MAC10＃定义一个MAC地址访问控制列表并且命名该列表名为MAC10Switch(config)permit host 0009.6bc4.d4bf any＃定义MAC地址为0009.6bc4.d4bf的主机可以访问任意主机Switch(config)interface fa0/20#进入配置具体端口模

式Switch(config)mac access-group MAC10 in＃在该端口上应用名为MAC10的访问列表（即前面我们定义的访问策略）Switch(config)no mac access-list extended MAC10＃清除名为MAC10的访问列表 此功能与应用一大体相同，但它是基于端口做的MAC地址访问控制列表限制，可以限定特定源MAC地址与目的地址范围。 注意：以上功能在思科2950、3550、4500、6500系列交换机上可以实现，但是需要注意的是2950、3550需要交换机运行增强的软件镜像（Enhanced Image） 方案3IP地址的MAC地址绑定 只能将应用1或2与基于IP的访问控制列表组合来使用才能达到IP-MAC 绑定功能。Switch(config)mac access-list extended MAC10#定义一个MAC地址访问控制列表并命名为MAC10Switch(config)permit host 0009.6b4c.d4bf any#定义MAC地址为0009.6b4c.d4bf 的主机可以访问任何主机Switch(config)permit any host 0009.6b4c.d4bf#定义任何主机可以访问MAC为0009.6b4c.d4bf的主机Switch(config)ip access-list extended IP10#定义一个IP地址访问控制列表并且命名为IP10Switch(config)permit 192.168.0.1 0.0.0.0 any#定义IP地址为192.168.0.1的主机可以访问任何主机Switch(config)permit any 192.168.0.1 0.0.0.0#定义任何主机都可以访问IP地址为192.168.0.1的主机完成了这一步就可以进入端口配置模式去配置端口啦!Switch(config)int fa0/20#进入端口配置模式Switch(config-if)＃在该端口上应用名为MAC10的访问列表（即前面我们定义的访问策略）Switch(config-if)ip access-group IP10 in＃在该端口上应用名为MAC10的访问列表（IP访问控制列表哟） 下面是清除端口上的访问控制列表Switch(config-if)no mac access-group MAC10

inSwitch(config-if)no ip access-group IP10 in#取消端口的访问控制列表应用 再清除访问控制列表Switch(config)no mac access-list extended MAC10Switch(config)no access-list extended IP10#清除所定义的MAC10/IP10访问控制列表 上述所提到的应用1是基于主机MAC地址与交换机端口的绑定，方案2是基于MAC地址的访问控制列表，前两种方案所能实现的功能大体一样。如果要做到IP与MAC地址的绑定只能按照方案3来实现，可根据需求将方案1或方案2与IP访问控制列表结合起来使用以达到自己想要的效果。（以上功能在思科2950、3550、4500、6500系列交换机上可以实现，但是需要注意的是2950、3550 需要交换机运行增强的软件镜像（Enhanced Image））。 在企业实际应用中，我们还可以更灵活的使用，我们都知道访问控制（ACL）功能的强大，如果能够很好的结合交换加以运用，会有更好的效果。以上文章希望对大家有所帮助！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