路由器与交换机安全策略示例思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/629/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E4_c101_629019.htm 百考试题Cisco站整理： 作为管理员需要为单位所有的网络设备机制定一套基本的安全配置策略是极为重要的。为此，将某单位内部路由器和交换机的安全策略拿来与大家共享： 路由器安全策略示例： 1. 路由器上不得配置用户账户。 2. 路由器上的enable password命令必须以一种安全的加密形式保存。 3. 禁止IP的直接广播。 4. 路由器应当阻止源地址为非法地址的数据包。 5. 在本单位的业务需要增长时，添加相应的访问规则。 6. 路由器应当放置在安全的位置，对其物理访问仅限于所授权的个人。 7. 每一台路由器都必须清楚地标识下面的声明：“ 注意：禁止对该网络设备的非授权访问。您必须在获得明确许可的情况下才能访问或配置该设备。在此设备上执行的所有活动必须加以记录，对该策略的违反将受到纪律处分，并有可能被诉诸于法律。 ”每一台网络交换机必须满足以下的配置标准： 1. 交换机上不得配置用户账户。 2. 交换机上的enable password命令必须以一种安全的加密形式保存。 3. 如果交换机的MAC水平的地址能够锁定，就应当启用此功能。 4. 如果在一个端口上出现新的或未注册的MAC地址，就应当禁用此端口。 5. 如果断开链接后又重新建立链接，就应当生成一个SNMP trap. 6. 交换机应当放置在安全的位置，对其物理访问仅限于所授权的个人。 7. 交换机应当禁用任何Web 服务器软件，如果需要这种软件来维护交换机的话，应当启动服务器来配置交换机，然后再禁用它。对管理员功能的所有访问

控制都应当启用。 8. 每一台交换机都必须清楚地标识下面的声明：“ 注意：禁止对该网络设备的非授权访问。您必须在获得明确许可的情况下才能访问或配置该设备。在此设备上执行的所有活动必须加以记录，对该策略的违反将受到纪律处分，并有可能被诉诸于法律。 ”这些安全要求未必适合你单位的情况，仅供参考。 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