路由器访问控制的安全配置实用配置 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/252/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E8_c101_252876.htm 路由器的访问控制是比较重要的安全措施，但是目前由于需求不明确，可以考虑暂时不实施。作为建议提供。 1 建议不要远程访问路由器。即使需要远程访问路由器，建议使用访问控制列表和高强度的密码控制。 2 严格控制CON端口的访问。 配合使用访问控制列表控制对CON口的访问。 如：Router(Config)#Access-list 1 permit 192.168.0.1 Router(Config)#line con 0 Router(Config-line)#Transport input none Router(Config-line)#Login local Router(Config-line)#Exec-timeoute 5 0 Router(Config-line)#access-class 1 in Router(Config-line)#end 同时给CON口设置高强度的密码。 3 如果不使用AUX端口，则禁止这个端口。默认是未被启用。禁止如： Router(Config)#line aux 0 Router(Config-line)#transport input none Router(Config-line)#no exec 4 建议采用权限分级策略。如：Router(Config)#username test privilege 10 xxxx Router(Config)#privilege EXEC level 10 telnet Router(Config)#privilege EXEC level 10 show ip access-list 5 为特权模式的进入设置强壮的密码。不要采用enable password设置密码。而要采用enable secret命令设置。并且要启用Service password-encryption。 Router（config）#service password-encryption Router（config）#enable secret 6 控制对VTY的访问。如果不需要远程访问则禁止它。如果需要则

一定要设置强壮的密码。由于VTY在网络的传输过程中为加密，所以需要对其进行严格的控制。如：设置强壮的密码；控制连接的并发数目；采用访问列表严格控制访问的地址；可以采用AAA设置用户的访问控制等 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