技术经验：反向访问控制列表 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__E6_8A_80_E6_9C_AF_E7_BB_8F_E9_c101_644687.htm 有5个VLAN,分别为管理(63)、办公(48)、业务(49)、财务(50)、家庭(51)。 要求:管理可以访问其它,而其它不能访问管理,并且其它VLAN之间不能互相访问！ 其它的应用不受影响，例如通过上连进行INTERNET的访问 方法一: 只在管理VLAN的接口上配置,其它VLAN接口不用配置。 在入方向放置ref lect ip access-list extended infilter permit ip any any reflect cciepass ! 在出方向放置evaluate ip access-list extended outfilter evaluate cciepass deny ip 10.54.48.0 0.0.0.255 any deny ip 10.54.49.0.0.0.0.255 any deny ip 10.54.50.0 0.0.0.255 any deny ip 10.54.51.0 0.0.0.255 any permit ip any any 应用到管理接口 int vlan 63 ip access-group infilter in ip access-group outfilter out 方法二：在管理VLAN接口上不放置任何访问列表，而是在其它VLAN接口都放。 以办公VLAN为例： 在出方向放置reflect ip access-list extended outfilter permit ip any any reflect cciepass ! 在入方向放置evaluate ip access-list extended infilter deny ip 10.54.48.0 0.0.0.255 10.54.49.0 0.0.0.255 deny ip 10.54.48.0 0.0.0.255 10.54.50.0 0.0.0.255 deny ip 10.54.48.0 0.0.0.255 10.54.51.0 0.0.0.255 deny ip 10.54.48.0 0.0.0.255 10.54.63.0 0.0.0.255 evaluate cciepass permit ip any any ! 应用到办公VLAN接口： int vlan 48 ip access-group infilter in ip access-group outfilter out 总结： 1）Reflect放置在允许的方向上（可进可出） 2）放在管理VLAN上配置简单，但是不如放在所有其它VLAN上直接。 3）如果在内网口上放置: 在入上设置Reflect 如果在外网

口上放置: 在出口上放置Reflect LAN WAN - inbound outbound
4）reflect不对本地路由器上的数据包跟踪,所以对待进入的数据包时注意,要允许一些数据流进入 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