

[组图]Configuring IP Access List PDF转换可能丢失图片或格式, 建议阅读原文

[https://www.100test.com/kao\\_ti2020/224/2021\\_2022\\_\\_3Cspan\\_clas\\_c101\\_224533.htm](https://www.100test.com/kao_ti2020/224/2021_2022__3Cspan_clas_c101_224533.htm) Pt.1 Introduction IP访问控制列表(access control list,ACL)用于过滤IP流量,其中RFC 1700定义了知名(well-known)端口号,RFC 1918定义了私有IP地址空间 Pt.2 Understanding ACL Concepts Using Masks ACL里的掩码也叫inverse mask(反掩码)或wildcard mask(通配符掩码),由32位长的2进制数字组成,4个八位位组.其中0代表必须精确匹配,1代表任意匹配(即不关心) 反掩码可以通过使用255.255.255.255减去正常的子网掩码得到,比如要决定子网掩码为255.255.255.0的IP地址172.16.1.0的反掩码:  $255.255.255.255-255.255.255.0=0.0.0.255$  即172.16.1.0的反掩码为0.0.0.255 注意: 反掩码为255.255.255.255的0.0.0.0代表any,即任意地址 反掩码为0.0.0.0的10.1.1.2代表主机地址10.1.1.2 Summarizing ACLs 下面描述的是如何汇总(summarization)一组网络地址,来达到优化ACL的目的:  
192.168.32.0/24 192.168.33.0/24 192.168.34.0/24 192.168.35.0/24  
192.168.36.0/24 192.168.37.0/24 192.168.38.0/24 192.168.39.0/24 这组IP地址的前2个和最后1个八位位组是一样的,再看第3个八位位组,把它们写成2进制的形式: 32:00 10 00 00 33:00 10 00 01 34:00 10 00 10 35:00 10 00 11 36:00 10 01 00 37:00 10 01 01 38:00 10 01 10 39:00 10 01 11 注意这组范围里的前5位都是一样的,所以这组IP地址范围可以汇总为192.168.32.0/21 255.255.248.0,那么这组IP地址范围的反掩码为 $255.255.255.255-255.255.248.0=0.0.7.255$  比如在做IP standard ACL的时候,就可以: access-list 10 permit 192.168.32.0 0.0.7.255 再来看另一组IP地范围: 192.168.146.0/24

192.168.147.0/24 192.168.148.0/24 192.168.149.0/24 照之前的方法,把第3个八位位组写成2进制形式: 146:10 01 00 10 147:10 01 00 11 148:10 01 01 00 149:10 01 01 01 是不是可以写成192.168.146.0/21呢?不是.因为采用/21的话将有8个子网将被考虑进去,如果在用ACL拒绝上述1组地址的时候,就有可能把另外4个地址给封杀掉.一定要考虑到精确匹配,上述地址就只能汇总成下面这2条地址: 对于192.168.146.x-192.168.147.x 为:192.168.146.0/23(192.168.146.0 255.255.254.0) 对于192.168.146.8-192.168.149.x为:192.168.148.0/23(192.168.148.0 255.255.254.0) 所以反掩码分别为:0.0.1.255和0.0.1.255 比如在做IP standard ACL的时候,就可以: access 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](http://www.100test.com)