CCNA中文笔记第9章:AccessLists PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022_CCNA_E4_B8_AD_E6_96_87_c101_142035.htm Chapter9 Managing Traffic with Access ListsIntroduction to Access Lists 访问列表(access list,ACL)的主要作用是过滤你不想要的数据包.设置ACL的一些规则: 1.按顺序的比较,先比较第一行,再比较第二行..直到最后1行 2.从第一行起,直到找到1个符合条件的行.符合以后,其余的行就不再继续比较下去 3.默认在每个ACL中最后1行为隐含的拒绝(deny),如果之前没找到1条许可(permit)语句,意味着包将被丢弃.所以每个ACL必须至少要有1行permit语句,除非你想想所有数据包丢弃 2种主要的访问列表: 1.标准访问列表(standard access lists):只使用源IP地址来做过滤决定 2.扩展访问列表(extended access lists):它比较源IP地址和目标IP地址,层3的协议字段,层4端口号来做过滤决定 利用ACL来过滤,必须把ACL应用到需要过滤的那个router的接口上,否则ACL是不会起到过滤作用的.而且你还要定义过滤的方向,比如是是想过滤从Internet到你企业网的数据包呢还是想过滤从企业网传出到Internet的数据包呢?方向分为下面2种: 1.inbound ACL:先处理,再路由 2.outbound ACL:先路由,再处理 一些设置ACL的要点: 1.每个接口,每个方向,每种协议,你只能设置1个ACL 2.组织好你的ACL的顺序,比如测试性的最好放在ACL的最顶部 3.你不可能从ACL从除去1行,除去1行意味你将除去整个ACL,命名访问列表(named access lists)例外(稍后介绍命名访问列表) 4.默认ACL结尾语句是deny any,所以你要记住的是在ACL里至少要有1条permit语句 5.记得创建了ACL后要把它应用在需要过滤

的接口上 6.ACL是用于过滤经过router的数据包,它并不会过滤router本身所产生的数据包 7.尽可能的把IP标准ACL放置在离目标地址近的地方.尽可能的把IP扩展ACL放置在离源地址近的地方 Standard Access Lists 介绍ACL设置之前先介绍下通配符掩码(wildcard masking).它是由0和255的4个8位位组组成的.0代表必须精确匹配,255代表随意,比如:172.16.30.0 0.0.0.255,这个告诉router前3位的8位位组必须精确匹配,后1位8位位组的值可以为任意值.如果你想指定172.16.8.0到172.16.15.0,则通配符掩码为0.0.7.255(15-8=7) 配置IP标准ACL,在特权模式下使用access-lists [范围数字] [permit/deny] [any/host]命令.范围数字为1到99和1300到1999.permit/deny分别为允许和拒绝.any为任何主机,host为具体某个主机(需要跟上IP地址)或某1段 我们来看1个设置IP标准ACL的实例: 