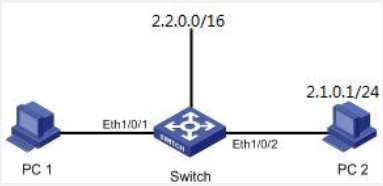
S3600交换机配置ACL后出现异常的分析处理

ACL 郭智科 2012-06-08 发表

S3600交换机配置ACL后出现异常的分析处理

一、 组网：



二、 问题描述：

某局点S3600以太网交换机需要新增加一台接入电脑2.1.0.1，但是需要控制这台电脑的访问权限，只允许其可以对2.2.0.0/16网段的访问。现场工程师小G充分了解用户需求后，决定使用交换机ACL流量过滤功能，在接入电脑所在的物理端口下下发ACL来控制数据的访问。小G在S3600交换机上进行了如下配置：

acl number 3002

rule 1 deny ip source 2.1.0.0 0.0.255.255

rule 10 permit ip source 2.1.0.0 0.0.255.255 destination 2.2.0.0 0.0.255.255

interface Ethernet1/0/2

packet-filter inbound ip-group 3002 rule 1

packet-filter inbound ip-group 3002 rule 10

当小G完成配置后发现，接入电脑并不能正常访问允许的2.2.0.0/16网段。经过流量统计和镜像抓包分析发现，数据流量最终在S3600交换机接入端口给丢掉了。于是小G再次对设备配置进行检查，发现设备之前还存在如下配置：

acl number 3001

rule 10 deny ip source 1.1.0.0 0.0.255.255 destination 1.2.0.0 0.0.255.255

interface Ethernet1/0/1

packet-filter inbound ip-group 3001 rule 10

新接入电脑2.1.0.1访问2.2.0.0/16网段的数据流量满足ACL 3002的rule 10，数据流所对应的动作为permit，那么交换机连接电脑的端口应该允许该数据流通过，为什么端口会将数据流量丢弃呢?

三、 过程分析：

1. S3600交换机ACL实现机制

S3600交换机芯片的QACL资源是每个block共享的，每个block称为PIC，8个FE口为1个EPIC，1个GE口为1个GPIC。在芯片内部有mask表和rule表，对于流限速和流统计有对应的meter表和counter表。每个EPIC有16个mask表项，256个rule表项，63个meter表项，32个counter表项。每个GPIC有16个mask表项，128个rule表项，63个meter表项，32个counter表项。

1.1 硬件ACL资源

对于S3600系列交换机来说，除了系统内部会占用一定数量的ACL资源外，一般给用户可配置的rule数目为每个EPIC 160条，每个GPIC 80条，mask数目为9条。S3600支持匹配报文前80字节的连续4字节的32个字节（可以把前面80个字节分成20段，每段4字节，但每次匹配的只能是其中的8段；实际上在分割这20段的时候还可以更灵活一点，就是每一段的起点可以使任意的偶数字节（当然这个数肯定低于76），如可以是0开始，也可以是2开始）。

1.2 MASK资源分配机制

该设备在进行硬件ACL下发时，首先会查看当前下发规则的mask是否已经存在，如果存在的话，就复用该mask；如果不存在的话，系统从第0个mask开始（以递增的方式）查找当前可用的mask空间，找到第一个可用的mask空间后，就分配该mask给配置的规则使用。当然，删除硬件ACL规则时，只有该规则对应的mask空间没有其他规则复用，才会释放该mask资源。这方面S3600-EI和S3600-SI版本存在的区别为：在EI版本上，为保证堆叠情况下OSPF功能可用，第15个mask被系统固定占用，用户不能使用

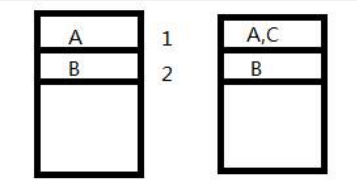
，而SI版本则没有该限制。

1.3 规则优先级

规则优先级问题是当一个报文符合多个规则，且这些规则对应的动作有冲突时才存在的，如果动作不冲突是不存在优先级问题的。当有冲突发生时，对应mask大的规则优先级高，而按照前面MASK资源分配机制所述，我们实现的配置是mask从低往高占用的，因此也可以笼统的说3600交换机后配置的规则优先级高，先生效。

2. 问题分析结果

根据3600交换机目前ACL的实现机制得知，相同的block中　QACL资源是共享的，所以在同一个block里，用户下发的ACL会存在mask资源复用的情况。如果用户后下发的配置规则复用了之前生效的配置规则占用的mask资源的话，就可能会出现优先级不可预期的情况。客户现场出现的问题正是如此，具体分析如下：



回顾工程师小G的配置过程，现场设备在成功下发了两条ACL--ACL 3001 的rule 10和ACL 3002的rule 1之后，它们将分别占用系统MASK资源1和2。当ACL 3002的rule 10被下发时，发现该规则使用的mask和ACL 3001中rule 10使用的mask完全一样，则复用该mask资源，也就是说ACL 3002的rule 10使用的系统mask资源是1。因此，当接入电脑2.1.0.1访问2.2.0.0/16网段的数据流进入E1/0/2端口时，数据流同时符合ACL 3002 rule 1和rule 10的流量定义，两个规则的动作存在冲突，将执行mask大的规则对应的动作--deny，所以数据流最终拒绝掉了，这样就可以解释现场出现的问题了。问题原因分析清楚后，我们来看一下该问题的解决方案。

四、 解决方法：

既然引起问题的原因是因为出现了mask资源复用的情况，那么我们见招拆招，为了避免mask资源复用的情况出现，可以从两个方向解决该类问题：

1. 将共用mask的端口挪到不同的block中，使其不再共享相同mask表项

S3600交换机每8个百兆口（如1-8，9-16以此类推）属于一个block，只有它们才会共享mask和rule资源，那么我们可以更改配置，使共用mask的端口挪到不同的block里解决该问题，比如使用e1/0/9替代e1/0/2。e1/0/9和e1/0/1属于不同的block，不存在资源共享的情况，这样就从根本上解决了该问题。

2. 拆分共用mask资源的rule规则，使其不再共享相同mask表项

就现场的问题来说，我们可以将其中一条rule进行拆分，这样不仅效果相同，同时也避免了公用mask资源的情况发生。比如下面的acl num 3003就是对acl num 3002进行拆分的结果，也可以解决现场的问题：

acl number 3003

rule 1 deny ip source 2.1.0.0 0.0.255.255

rule 2 permit ip source 2.1.0.0 0.0.255.255 destination 2.2.0.0 0.0.127.255

rule 3 permit ip source 2.1.0.0 0.0.255.255 destination 2.2.128.0 0.0.127.255