S5120系列交换机硬件ACL实现机制说明

岳斌 2009-12-30 发表

一、S5120-SI系列交换机

1、硬件ACL资源

S5120-SI仅支持按照端口下发，规则仅对ingress的报文生效，硬件单个芯片可以最多下发512条ACL。对用户ACL配置，S5120-SI支持64条，3Com S2900系列则无限制，除系统占用的ACL资源，剩下其它都可以被用户使用。

ACL的规则因为支持的长度不同在芯片内部分为标准型和扩展型，对用户不可见。

（1）标准型的ACL为24bytes的长度，可以支持1024条标准的ACL规则。

（2）扩展型的ACL为48bytes的长度，可以支持512条扩展型的ACL规则。

2、资源分配机制

ACL规则是标准型还是扩展型，必须在一个端口上保持一致。例如，在一个端口上开始下发的规则是标准型，但是后来下发的一条规则是扩展型，那么这个端口上前面的标准型的规则也会被修改为扩展型，并且该端口上以后再下发规则，都会被设置为扩展型的，直到该端口上的规则被全部删除，才可能再下发标准型的规则。

一个端口上的规则类型，不会影响其它端口的规则类型。比如，端口1上的规则都是扩展型的，而端口2的规则可以都是标准型的。

系统内部的一些功能模块需要使用ACL，如LACP、桥MAC、集群协议、LLDP、DLDP、DHCP snooping等等，一旦使能这些模块，就要占用一些ACL资源。

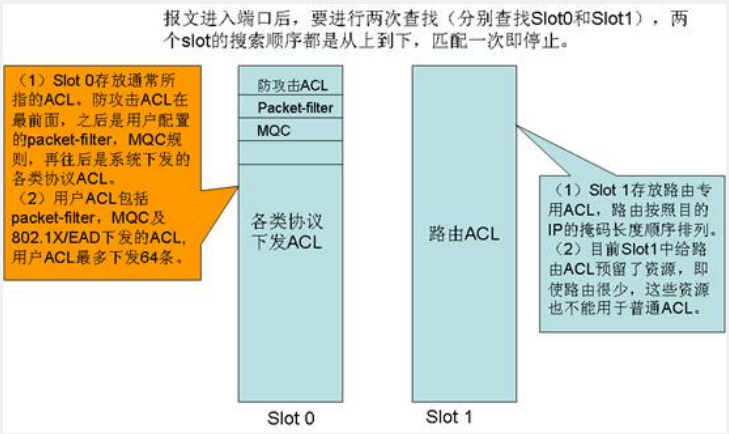
802.1x模块也可以通过服务器下发一些配置好的ACL，也会占用系统的ACL资源。

因此，有时候在端口上或整机上用户配置ACL，会发现达不到规格，原因就是被一些功能模块使用了。或者用户配置了大量的ACL，系统内部模块下发ACL会出现资源不足而失败，导致功能不可用或有缺陷，如LLDP下发的ACL失败，就会导致报文无法上CPU，802.1x通过服务器下发的ACL因资源不足会导致用户无法上线等。

3、规则优先级

端口上的ACL的匹配顺序首先是按照模块之间的优先级来匹配。例如，端口上防攻击的规则优先级最高，之后是用户配置的packet filter，MQC策略，然后是端口car， ARP Detetion、DHCP snooping、Smart-Link 、LACP协议、STP协议、GVRP、MFF高优先级规则、MFF低优先级规则、802.1x服务器下发的ACL、MAC+IP端口绑定（IP check）、集群协议、桥MAC、回环检测、CDP、LLDP、DLDP，最后是MAC+IP端口绑定（IP check）的缺省规则。注意，不是所有以上协议都被支持，但是支持的协议中，都是按照这个顺序进行匹配。

报文查找了流程如下图所示。



二、S5120-EI系列交换机

1、硬件ACL资源

S5120-EI中各类规则存在于一个全局TCAM表中，分为16个slice（每个slice有128个entry），每个slice在匹配过程中只能生成一个动作，最终动作由16个slice中最高优先级slice动作指定。

（1）单个slice匹配能力不足时，可以使用奇偶数slice进行double匹配

（2）每种匹配组合对相同slice（double）内所有entry生效

（3）每个slice（double）内仅能按照index从小到大命中一条entry

（4）可以命中不同slice（double）内的不同entry

（5）出现冲突动作时，以slice index大的entry为准

报文匹配流程与S5500系列交换机一样。

2、规则优先级（端口>VLAN>全局）

由于系统中各类规则匹配优先级不同，定义顺序如下图。

说明：

（1）同颜色规则类型可共用slice，就是可存在覆盖关系；不同颜色规则类型不存在覆盖关系。

（2）相同类型内部按照先下发先生效排序。

（3）不同端口下发相同内容POLICY，可以共享一条硬件ENTRY资源，带有CAR、ACCOUNT动作的POLICY除外。