S3610/55510系列交换机硬件ACL实现机制说明

岳斌 2009-12-30 发表

1、硬件ACL资源

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，S3610可以支持2048条，S5510支持4096条。

（2）扩展型的ACL为48bytes，S3610可以支持1024条，S5510支持2048条。

（3）FE端口最多256条，GE端口最多512条，一个vlan上最多512条。

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。

下发到VLAN上的ACL规则是扩展型的，而且，一旦配置了VLAN上的规则，所有端口的标准型的规则都要被修改为扩展型的，而且，之后再下发ACL，都会被设置为扩展型的。

系统内部的一些功能模块需要使用ACL，如集群协议、802.1x、Voice VLAN、端口隔离、DHCP snooping、ARP Detection、MFF、Smart-Link、EAD、灵活QinQ、MAC+IP端口绑定等等，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，如端口隔离下发的ACL失败，就会导致本机的ARP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。IPv6协议模块也要使用一些ACL的资源。

3、规则优先级（端口>VLAN>全局）

报文首先查找端口上的ACL规则，如果匹配，则执行相应的动作而不再继续查找VLAN上的规则。如果没有匹配，则继续查找VLAN上的规则，最后查找全局的规则。

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，端口上策略的优先级最高，端口car次之，Smart-Link 、802.1x协议的ACL、集群协议、ARP Detetion、DHCP snooping、Voice VLAN、EAD、端口隔离、MFF高优先级规则、802.1x服务器下发的ACL、MAC+IP端口绑定（IP check）、灵活QinQ与MFF低优先级规则。

报文是按照顺序查找规则，一旦命中了第一条与之匹配的规则，便不再继续查找。因此就会有一些情况下发现端口上的某个功能模块不起作用了，这时就需要检查一下报文是否匹配了其它的规则。