MSR-G2路由器下发二层ACL的经验案例

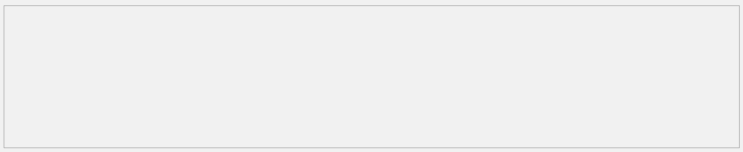
马文斌 2013-10-23 发表

MSR-G2路由器下发二层ACL的经验案例

一、 组网：

公司只允许源MAC地址为000f-e2e5-0b70的PC机上公网，携带其他源MAC地址的报文一律不允许通过。

PC连接RTA的Interface Vlan 1接口，RTA的G0/1接口连接公网。



使用版本：R0007P03

二、 问题描述：

使用CBQ方法下发：

使用CBQ的方法来调用二层ACL，然后通过在接口上下发qos策略，但是下发后却发现策略不生效，无法限制目标流量。

使用防火墙包过滤方法下发：

MSR-G2（V7设备）在接口上没有像V5设备中的firewall ethernet-frame-filter *INTEGER<4000-4999>* {inbound|outbound}这条命令，应该如何下发?

三、 过程分析：

使用CBQ方法下发：

在流分类（traffic classifier）中调用二层ACL，然后在动作中设置相应的permit/deny动作，但是CBQ方式虽然可以在接口下发，但是却无法生效，原因为CBQ方法无法直接调用二层ACL，导致流量无法匹配到相应的ACL，所以配置不生效。

使用包过滤防火墙方法下发：

V7设备中的包过滤防火墙和V5设备命令有所区别，在V7设备中，下发包过滤防火墙命令变为：packet-filter *acl-number* {inbound|outbound}。

四、 解决方法：

使用CBQ方法下发

遇到如上组网方式，需要在路由器的interface vlan-interface接口上做MAC地址过滤，可以使用CBQ的方法，而且必须使用如下配置：

[H3C]traffic classifier 1

[H3C-classifier-1]if-match source-mac 0001-0001-0001

因为CBQ方式无法直接调用二层ACL，所以匹配流中不能匹配二层ACL，只能够使用如上方式，在匹配流中直接调用MAC地址，这样就可以起到限制MAC地址的效果了。

完整配置：

[H3C]traffic classifier 1

[H3C-classifier-1]if-match source-mac 0001-0001-0001

[H3C-classifier-1]quit

[H3C]traffic behavior 1

[H3C-behavior-1]filter deny

[H3C-behavior-1]quit

[H3C]qos policy 1

[H3C-qospolicy-1]classifier 1 behavior 1

[H3C-qospolicy-1]qu

[H3C]interface vlan-interface 1

[H3C-Vlan-interface1]qos apply policy 1 inbound

使用包过滤防火墙方法下发：

可直接在interface vlan-interface接口下使用packet-filter命令下发二层ACl，这样是可以生效的。

包过滤防火墙工作原理：

ACL中匹配规则为permit时，如果匹配了ACL中的规则，那么直接通过；如果流量不匹配ACL中的规则，那么执行防火墙的默认动作。

ACL中匹配规则为deny是，如果匹配了ACL中的规则，那么报文直接丢弃；如果流量不匹配ACL中的规则，那么执行防火墙的默认动作。