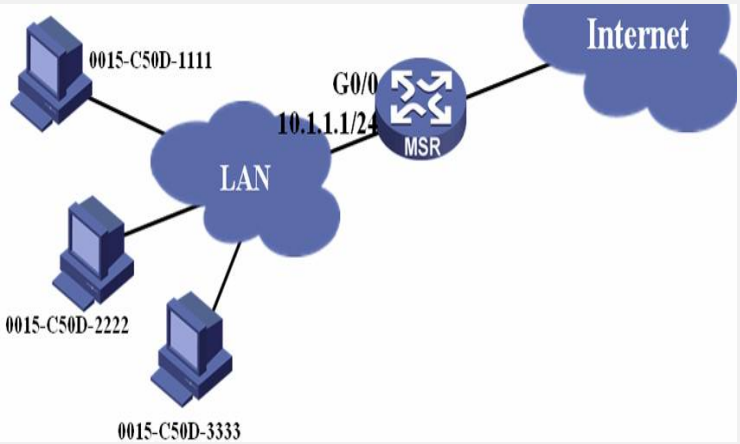
MSR系列路由器限制某个源MAC只允许访问网关不允许访问外网功能的配置

丘子隽 2007-08-24 发表

MSR系列路由器
限制某个源MAC只允许访问网关不允许访问外网功能的配置

关键字：MSR; MQC; 过滤; MAC

一、**组网需求**：
MSR作为LAN网关，要限制某些主机上网，但是由于这些主机可以变换IP地址，所以通过防火墙限制不能有效防范，最合适的做法是限制MAC地址，在本例中可以实现限制某些MAC访问互联网，但是可以访问网关。
设备清单：MSR系列路由器1台
二、组网图：



三、配置步骤：
适用设备和版本：MSR系列、Version 5.20, Release 1206后所有版本。

MSR配置

```
#
//定义gw分类规则，匹配acl3000
traffic classifier gw operator and
 if-match acl 3000
//定义mac分类规则，匹配3个源地址，匹配操作符为“逻辑或”
traffic classifier mac operator or
 if-match source-mac 0015-c50d-1111
 if-match source-mac 0015-c50d-2222
 if-match source-mac 0015-c50d-3333
#
//定义流行为permit
traffic behavior permit
 //允许通过
 filter permit
//定义流行为deny
traffic behavior deny
 //拒绝并丢弃
 filter deny
#
//定义qos策略myqos
qos policy myqos
 //将gw流和permit绑定
 classifier gw behavior permit
 //将mac流和deny绑定
 classifier mac behavior deny
#
//acl 3000匹配目的地址10.1.1.1/32，即网关地址
acl number 3000
 rule 0 permit ip destination 10.1.1.1 0
#
//连接内网的接口G0/0
interface GigabitEthernet0/0
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 //接口入方向应用myqos策略
 qos apply policy myqos inbound
#
```

四、**配置关键点**：
1) 注意不能使用ACL4000~4999匹配源MAC地址，因为3层接口只能在桥组模式下支

> 持该ACL，所以必须使用if-match source-mac来匹配源MAC，并通过修改匹配操作符“or”来匹配多个MAC地址；
> 2) 在QoS策略中需要注意配置顺序，先允许访问网关，再过滤MAC源地址，表示访问网关全部允许，因为到该接口的流量除了访问网关就是访问互联网，因此可以过滤掉访问互联网的流量中某个源MAC，实现该功能。