

问题描述

MSR路由器怎么限制特定用户上网?

解决方法

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, 所以通过包过滤防火墙限制不能有效防范, 最合适的做法是限制MAC地址, 在本例中可以实现图中这三个终端只能访问内网10.1.1.0/24网段, 而不能访问外网。

```
<H3C>system-view
[H3C]acl number 3000
[H3C-acl-adv-3000]rule permit ip destination 10.1.1.0 0.0.0.255 //配置终端可以访问的内网网段
[H3C-acl-adv-3000]quit
[H3C]traffic classifier gw //定义gw分类规则, 匹配acl3000
[H3C-classifier-gw]if-match acl 3000
[H3C-classifier-gw]quit
[H3C]traffic classifier mac operator or //定义mac分类规则, 匹配3个源地址, 匹配操作符为“逻辑或”
[H3C-classifier-mac]if-match source-mac 0015-c50d-1111
[H3C-classifier-mac]if-match source-mac 0015-c50d-2222
[H3C-classifier-mac]if-match source-mac 0015-c50d-3333
[H3C-classifier-mac]quit
[H3C]traffic behavior permit
[H3C-behavior-permit]filter permit //定义流行为permit
[H3C-behavior-permit]quit
[H3C]traffic behavior deny
[H3C-behavior-deny]filter deny //定义流行为deny
[H3C-behavior-deny]quit
[H3C]qos policy 123 //定义qos策略123
[H3C-qospolicy-123]classifier gw behavior permit //优先将分类gw与流动作permit绑定
[H3C-qospolicy-123]classifier mac behavior deny //然后将分类mac与流动作deny绑定
[H3C-qospolicy-123]quit
[H3C]interface Vlan-interface 1
[H3C-Vlan-interface1]qos apply policy 123 inbound //将qos策略应用在内网网关接口的入方向
[H3C-Vlan-interface1]quit
```