S8500交换机 VLAN-ACL技术说明

罗淳榕　2006-08-07 发表

S8500 VLAN-ACL技术说明

一、简单介绍

VLAN-ACL即基于VLAN的ACL。用户通过对VLAN配置QACL动作，从而实现对VLAN内所有端口的访问控制。VLAN-ACL使用户能够更加方便地管理网络。用户只需在VLAN下配置QACL，相应的QACL动作就能同步到所有成员端口，而无需在每个成员端口上单独配置。

VLAN-ACL配置有以下限制：

（1）流模板的限制

VLAN-ACL只在采用默认流模板的端口下发，所下发的ACL规则字段只能是默认流模板规定的字段；

若VLAN内尚无端口下发ACL规则，当在VLAN视图下下发第一个规则时会检查VLAN内所有端口，只要有一个端口使用自定义流模板，则不允许下发；

若VLAN内已有部分端口下发VLAN-ACL，此时加入一个使用自定义流模板的端口，结果为：端口能加入VLAN，但不能下发VLAN-ACL；此时，再在VLAN视图下下发VLAN-ACL，原有的端口能够成功下发，但新加入的端口无法下发。当此端口删除自定义流模板时，系统会自动下发VLAN内的QACL规则到该端口；

当端口已下发有VLAN-ACL时，如果想在端口下发自定义流模板，系统会提示端口已下发有VLAN-ACL，不允许下发自定义流模板。

（2）当端口所在的VLAN和端口都下发有QACL规则时，只有端口下的QACL起作用；VLAN-ACL只有在删除端口下的QACL规则、并且删除端口下的自定义流模板之后才起作用。

（3）当VLAN内没有成员端口时，不允许下发VLAN-ACL（包括增加和删除规则）。

（4）如果两个端口的VLAN-ACL同步情况不一致，则这两个端口无法动态聚合。

（5）VLAN-ACL不能在与POS口绑定的VLAN下发，即VLAN-ACL不会下发到POS口。

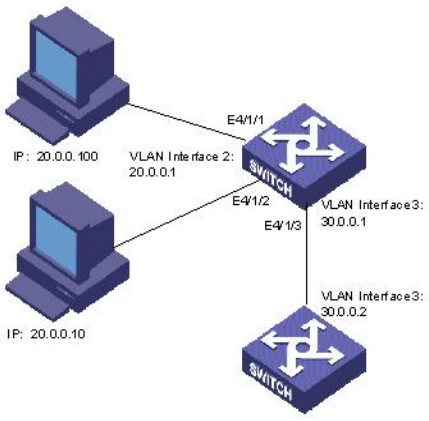
（6）混插端口所在的VLAN不允许下发VLAN-ACL；反之，下发有VLAN-ACL的VLAN不能再用于MPLS混插。

二、设备配置实例

1．组网需求

每天8：00～18：00限制转发经过端口Ethernet4/1/1和Ethernet4/1/2的报文。

2．组网图



VLAN-ACL典型组网图

2．配置步骤

(1)　定义时间段

定义8:00～18:00时间段。

<SA> system-view

System View: return to User View with Ctrl+Z.

[SA] time-range h3c 8:00 to 18:00 daily

(2)定义PC报文的流规则

进入基于数字标识的基本访问控制列表视图，用2000标识。

[SA] acl number 2000
定义报文的流分类规则，拒绝指定时间段内的任何的报文通过。
[SA-acl-basic-2000] rule 0 deny source any time-range h3c
[SA-acl-basic-2000] quit
(3)对VLAN 2配置包过滤
[SA] vlan 2
[SA-vlan2] packet-filter inbound ip-group 2000 rule 0

三、正确配置状态显示
查看VLAN 2内的端口（Ethernet4/1/1和Ethernet4/1/2）是否已同步了VLAN-ACL。
[SA-vlan2] display vlan-acl-member-ports vlan 2
Vlan-acl member port(s):
Ethernet4/1/1 Ethernet4/1/2