H3C S9500交换机VLAN-ACL配置

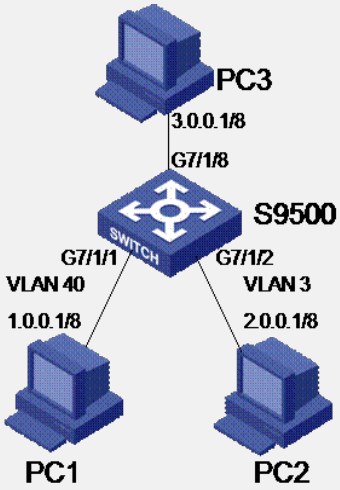
刘志伟　2006-12-03 发表

H3C S9500交换机VLAN-ACL配置

一、组网需求：

　将端口GigabitEthernet7/1/1和GigabitEthernet7/1/2每天8：00～18：00转发的报文下一跳地址都定义为3.0.0.1。

二、组网图：



三、配置步骤：

软件版本：S9500交换机全系列软件版本

硬件版本：S9500交换机全系列硬件版本

定义时间段

定义8:00～18:00时间段。

<S9500> system-view

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

[S9500] time-range test 8:00 to 18:00 daily

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。

[S9500] acl number 2000

定义报文的流分类规则，允许指定时间段内的报文通过。

[S9500-acl-basic-2000] rule 0 permit source any time-range Test

[S9500-acl-basic-2000] quit

对VLAN 2配置报文重定向

将VLAN 2内的端口转发的报文下一跳都定义为3.0.0.1。

[S9500] vlan 2

[S9500-vlan2] traffic-redirect inbound ip-group 2000 rule 0 next-hop 3.0.0.1

查看配置结果

查看VLAN 2内的端口（GigabitEthernet7/1/1和GigabitEthernet7/1/2）是否已同步了VLAN-ACL。

[S9500-vlan2] display vlan-acl-member-ports vlan 2

Vlan-acl member port(s):

　　GigabitEthernet7/1/1　　GigabitEthernet7/1/2

四、配置关键点：

1.流模板的注意事项

？(1)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；

？(2)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；

？(3)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；

？(4)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。
7．若VLAN下发ACL规则时，属于此VLAN的某端口所在单板不在位，则单板在位以后，此端口不能同步ACL规则。如果想同步ACL规则，可以通过配置命令port can-access vlan-acl来实现。