S5100-EI系列交换机VLAN下发ACL功能的配置

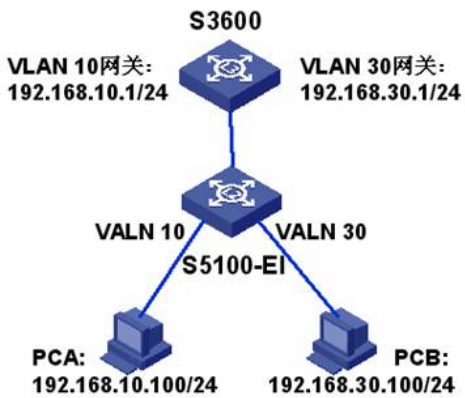
岳斌 2007-11-27 发表

S5100-EI系列交换机VLAN下发ACL功能的配置

一、 组网需求：

在H3C S5100-EI交换机分别创建VLAN 10和VLAN 30，将两个VLAN的网关设置在上连的S3600交换机上，在S5100-EI的VLAN 30上下发ACL，使VLAN 30内的PC只能ping通VLAN 10内PC，而不能进行其他操作，如FTP、Telnet等。

二、 组网图：



三、 配置步骤：

以下配置应用版本为：Version 3.10, Release 2200P02。

1、S5100-EI设备上的配置：

（1）创建VLAN 10和VLAN 30，并将端口GigabitEthernet1/0/1加入到VLAN 10中，将端口GigabitEthernet1/0/3加入到VLAN 30中。

[S51EI]vlan 10

[S51EI-vlan10]port GigabitEthernet1/0/1

[S51EI]vlan 30

[S51EI-vlan10]port GigabitEthernet1/0/3

（2）设置上连到S3600设备的端口为Trunk口，并允许VLAN 10和VLAN 30通过。

[S51EI]interface GigabitEthernet

1/0/16

[S51EI-GigabitEthernet1/0/16]port link-type

trunk

[S51EI-GigabitEthernet1/0/16]port trunk permit vlan 10 30

（3）创建ACL 3030。

[S51EI]acl number 3030

[S51EI-acl-adv-3030]rule 2 permit ICMP destination 192.168.10.0 0.0.0.255

//该rule的作用是考虑到icmp request报文进入access口是入方向的

[S51EI-acl-adv-3030] rule 3 permit icmp destination 192.168.30.0 0.0.0.255

//该rule的作用是考虑到icmp reply报文返回时对于trunk口是入方向的

[S51EI-acl-adv-3030]rule 4 deny IP

（4）在VLAN 30上下发ACL 3030。

[S51EI] packet-filter vlan 30 inbound ip-group 3030

2、S3600设备上的配置：

（1）创建VLAN 10和VLAN 30，并设置虚接口IP地址。

[S3600]vlan

10

[S3600]vlan 30

[S3600]int Vlan-interface 10

[S3600-Vlan-interface10] ip address 192.168.10.1 255.255.255.0

[S3600]int Vlan-interface 30

[S3600-Vlan-interface30] ip address 192.168.30.1 255.255.255.0

（2）设置下行到S5100EI设备的端口为Trunk口，并允许VLAN 10和VLAN 30通过。

[S3600]int Ethernet 1/0/1

[S3600-Ethernet1/0/1]port link-type trunk

[S3600-Ethernet1/0/1]port trunk permit vlan 10 30

四、 配置关键点：

基于VLAN下发ACL时，在考虑access口的同时，还要针对trunk口进行相应的配置。
而基于端口下发ACL只需考虑access口的icmp request入方向，对于icmp reply报文，端口出方向ACL不生效，因此在端口上下发的ACL如下配置即可。

```
[S51EI]acl number 3030
[S51EI-acl-adv-3030]rule 2 permit ICMP destination 192.168.10.0 0.0.0.255
[S51EI-acl-adv-3030]rule 4 deny IP
[S51EI]int GigabitEthernet1/0/3
[S51EI-GigabitEthernet1/0/3] packet-filter inbound ip-group 3030
```