

H3C S9500交换机QoS流量监管功能的配置

一、组网需求:

流量监管 (traffic-limit) 是基于流的速率限制。它监督某一流量的速率, 如果流量超出指定的规格, 交换机就采用相应的措施, 如丢弃那些超出规格的报文或重新设置它们的服务参数。配置流量监管涉及到的主要参数有:

cir: 承诺平均速率 (单位: Kbps)

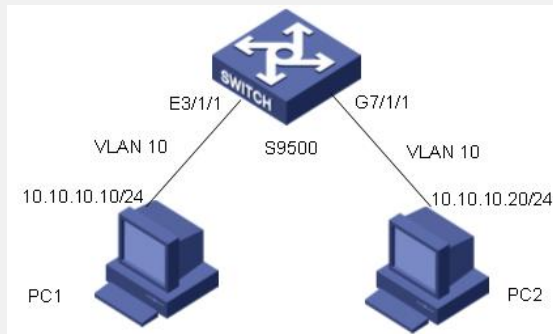
cbs: 承诺突发尺寸 (单位: byte)

ebs: 最大突发尺寸 (单位: byte)

pir: 峰值速率 (单位: Kbps)

以下组网图中, PC1连接在S9500的E3/1/1端口, IP地址为10.10.10.10, PC2连接在S9500的GE7/1/1上, IP地址为10.10.10.20, 它们都属于VLAN 10。需要利用S9500的流量监管功能, 限制端口E3/1/1和GE7/1/1进来的ICMP流量为2000kbps, 超出部分丢弃。

二、组网图:



流量监管典型组网图

三、配置步骤:

软件版本: 端口ACL, S9500交换机全系列软件版本; VLAN-ACL, S9500交换机1270及以后版本

硬件版本: S9500交换机全系列硬件版本

该组网需求可以通过VLAN-ACL或者端口ACL实现, 建议用端口ACL

配置VLAN-ACL

1) 配置vlan10及虚接口地址, 使PC1和PC2能ping通S9500

```
[S9500]vlan 10
[S9500-vlan10]port Ethernet 3/1/1
[S9500-vlan10]port GigabitEthernet 7/1/1
[S9500]interface Vlan-interface 10
[S9500-Vlan-interface10]ip address 10.10.10.1 255.255.255.0
```

2) 在交换机上配置ACL规则, 允许ICMP报文通过

```
[S9500]acl number 3000
[S9500-acl-adv-3000]rule 0 permit icmp
```

3) 在vlan 10 配置流量监管, cir为2000, cbs为200000, ebs为300000

```
[S9500]vlan 10
[S9500-vlan10]traffic-limit inbound ip-group 3000 2000 200000 300000 conform
remark-drop-priority exceed drop
```

配置端口ACL

1) 配置vlan 10及其虚接口, 使PC1和PC2能ping通S9500

```
[S9500]vlan 10
[S9500-vlan10]port Ethernet 3/1/1
[S9500-vlan10]port GigabitEthernet 7/1/1
[S9500]interface Vlan-interface 10
[S9500-Vlan-interface10]ip address 10.10.10.1 255.255.255.0
```

2) 配置ACL规则, 允许ICMP报文通过

```
[S9500]acl number 3000
[S9500-acl-adv-3000]rule 0 permit icmp
```

3) 在端口E3/1/1与GE7/1/1下配置流量监管, cir为2000, cbs为200000, ebs为300000

```
[S9500]interface Ethernet 3/1/1
[S9500-Ethernet3/1/1]traffic-limit inbound ip-group 3000 2000 200000 300000
conform remark-drop-priority exceed drop
[S9500]interface GigabitEthernet 7/1/1
[S9500-GigabitEthernet7/1/1]traffic-limit inbound ip-group 3000 2000 200000
300000 conform remark-drop-priority exceed drop
```

四、配置关键点：

1. VLAN-ACL配置注意事项

- 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) VLAN内尚无端口下发ACL规则，当在VLAN视图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；
- 5) 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；
- 6) 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）；
- 7) 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；
- 8) VLAN-ACL不能在POS口绑定的VLAN下发，即VLAN-ACL不会下发到POS口；
- 9) 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；
- 10) VLAN-ACL在XP4单板端口下实际不生效；
- 11) 配置VLAN-ACL的端口必须为以太网端口。

2. traffic-limit配置注意事项

- 1) 在参数设定时，要求 $cir \leq pir$ ， $cbs \leq ebs$ 。建议将cbs、ebs设成cir的100~150倍；
- 2) 使用限制：traffic-limit在B/DB单板上使用单速率时，实际速率是真实限制速率的2倍左右，一般情况下建议采用双速率限速功能。