S5560S-52P-SI 调用PBR后业务转发卡顿

策略路由 **许鹏鹏** 2021-08-28 发表

组网及说明

不涉及

问题描述

客户在interface vlan接口下调用pbr后发现上网卡顿严重

过程分析

卡顿的时候查看设备CPU很高，持续了50%以上，继而发现设备收到大量http报文冲击了CPU，怀疑配置PBR后报文软转了。

==========debug rxtx softcar show slot 1==========

ID Type RcvPps Rcv_All DisPkt_All Pps Dyn Swi Hash Am APps

63 HTTP/HTTPS 1000 2205530 22859 500 S On SMAC 8 512

看现场配置当前已经调用的pbr如下：

```
interface Vlan-interface20
ip address 20.1.1.1 255.255.255.0
ip policy-based-route vlan20
#


interface Vlan-interface40
ip address 40.1.1.1 255.255.255.0
ip policy-based-route vlan40
#

interface Vlan-interface90
ip address 90.1.1.1 255.255.255.0
ip policy-based-route vlan90
#
interface Vlan-interface100
ip address 100.1.1.1 255.255.255.0
ip policy-based-route vlan100
#

policy-based-route vlan20 permit node 10
if-match acl 3004
#
policy-based-route vlan20 permit node 24
if-match acl 2004
apply next-hop 10.10.20.1
#


policy-based-route vlan40 permit node 10
if-match acl 3009
#
policy-based-route vlan40 permit node 29
if-match acl 2009
apply next-hop 10.10.40.1
#

policy-based-route vlan90 permit node 10
if-match acl 3002
#
policy-based-route vlan90 permit node 22
if-match acl 2002
apply next-hop 10.10.90.1
#

policy-based-route vlan100 permit node 20
if-match acl 2100
apply next-hop 10.10.100.1
```

详细的acl如下：

```
acl basic 2004
rule 0 permit source 10.20.4.0 0.0.0.255
#
```

acl basic 2002
rule 0 permit source 10.20.2.0 0.0.0.255
#

解决方法

建议精简2009rule规则，控制在16条以内，可以合并规则，如acl 3009，6条规则可以合并成一条
rule 0 permit source 10.20.9.0 0.0.0.255
rule 0 permit ip source 10.20.9.0 0.0.0.255 destination 10.20.2.0 0.0.15.255
#

acl basic 2100
rule 0 permit source 66.66.100.0 0.0.0.255
#

acl advanced 3002
rule 0 permit ip source 10.20.2.0 0.0.0.255 destination 10.20.3.0 0.0.0.255
rule 5 permit ip source 10.20.2.0 0.0.0.255 destination 10.20.4.0 0.0.0.255
rule 10 permit ip source 10.20.2.0 0.0.0.255 destination 10.20.5.0 0.0.0.255
rule 15 permit ip source 10.20.2.0 0.0.0.255 destination 10.20.6.0 0.0.0.255
rule 20 permit ip source 10.20.2.0 0.0.0.255 destination 10.20.7.0 0.0.0.255
rule 25 permit ip source 10.20.2.0 0.0.0.255 destination 10.20.8.0 0.0.0.255
rule 30 permit ip source 10.20.2.0 0.0.0.255 destination 10.20.9.0 0.0.0.255
#

acl advanced 3004
rule 0 permit ip source 10.20.4.0 0.0.0.255 destination 10.20.2.0 0.0.0.255
rule 5 permit ip source 10.20.4.0 0.0.0.255 destination 10.20.3.0 0.0.0.255
rule 10 permit ip source 10.20.4.0 0.0.0.255 destination 10.20.5.0 0.0.0.255
rule 15 permit ip source 10.20.4.0 0.0.0.255 destination 10.20.6.0 0.0.0.255
rule 20 permit ip source 10.20.4.0 0.0.0.255 destination 10.20.7.0 0.0.0.255
rule 25 permit ip source 10.20.4.0 0.0.0.255 destination 10.20.8.0 0.0.0.255
rule 30 permit ip source 10.20.4.0 0.0.0.255 destination 10.20.9.0 0.0.0.255
#

acl advanced 3009
rule 0 permit ip source 10.20.9.0 0.0.0.255 destination 10.20.2.0 0.0.0.255
rule 5 permit ip source 10.20.9.0 0.0.0.255 destination 10.20.3.0 0.0.0.255
rule 10 permit ip source 10.20.9.0 0.0.0.255 destination 10.20.4.0 0.0.0.255
rule 15 permit ip source 10.20.9.0 0.0.0.255 destination 10.20.5.0 0.0.0.255
rule 20 permit ip source 10.20.9.0 0.0.0.255 destination 10.20.6.0 0.0.0.255
rule 25 permit ip source 10.20.9.0 0.0.0.255 destination 10.20.7.0 0.0.0.255
rule 30 permit ip source 10.20.9.0 0.0.0.255 destination 10.20.8.0 0.0.0.255
#
这款设备最多支持下发16个PBR node资源，一个node里默认按照一个acl rule计算，如果有多个rule，则需要翻倍计算，比如下面目前应用的4个pbr，共7个node，一个配置了25个rule，则占用了25个node资源了，超规格了，超规格之后报文查路由表软转，导致上网卡顿