

知 6520X-30QC-EI cannot successfully configure policy routing

Switches 龚训杰 2020-12-11 Published

Network Topology

NULL

Problem Description

When configuring PBR on the int vsi interface, it prompts that the operation is not supported

```
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]int vsi
[SH-5F-CORE-S6520X-1]int Vsi-interface 2502
[SH-5F-CORE-S6520X-1-Vsi-interface2502]
[SH-5F-CORE-S6520X-1-Vsi-interface2502]int Vsi-interface 3502
[SH-5F-CORE-S6520X-1-Vsi-interface3502]
[SH-5F-CORE-S6520X-1-Vsi-interface3502]dis this
#
interface Vsi-interface3502
 ip binding vpn-instance vpn-default
 ip address 10.3.32.1 255.255.255.0
 mac-address 0000-0000-0001
 local-proxy-arp enable
 dhcp select relay proxy
 dhcp relay information circuit-id vxlan-port
 dhcp relay information enable
 dhcp relay server-address 10.3.255.253
 dhcp relay source-address interface Vsi-interface4094
 dhcp relay request-from-tunnel discard
 distributed-gateway local
#
return
[SH-5F-CORE-S6520X-1-Vsi-interface3502]
[SH-5F-CORE-S6520X-1-Vsi-interface3502]ip po
[SH-5F-CORE-S6520X-1-Vsi-interface3502]ip policy-based-route 1 ?
<cr>

[SH-5F-CORE-S6520X-1-Vsi-interface3502]ip policy-based-route 1
The operation is not supported.
[SH-5F-CORE-S6520X-1-Vsi-interface3502]ip policy-based-route 1
The operation is not supported.
[SH-5F-CORE-S6520X-1-Vsi-interface3502]
```

```
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]
[SH-5F-CORE-S6520X-1]int vsi
[SH-5F-CORE-S6520X-1]int Vsi-interface 2502
[SH-5F-CORE-S6520X-1-Vsi-interface2502]
[SH-5F-CORE-S6520X-1-Vsi-interface2502]int Vsi-interface 3502
[SH-5F-CORE-S6520X-1-Vsi-interface3502]
[SH-5F-CORE-S6520X-1-Vsi-interface3502]dis this
#
interface Vsi-interface3502
 ip binding vpn-instance vpn-default
 ip address 10.3.32.1 255.255.255.0
 mac-address 0000-0000-0001
 local-proxy-arp enable
 dhcp select relay proxy
 dhcp relay information circuit-id vxlan-port
 dhcp relay information enable
 dhcp relay server-address 10.3.255.253
 dhcp relay source-address interface Vsi-interface4094
 dhcp relay request-from-tunnel discard
 distributed-gateway local
#
return
[SH-5F-CORE-S6520X-1-Vsi-interface3502]
[SH-5F-CORE-S6520X-1-Vsi-interface3502]ip po
[SH-5F-CORE-S6520X-1-Vsi-interface3502]ip policy-based-route 1 ?
<cr>

[SH-5F-CORE-S6520X-1-Vsi-interface3502]ip policy-based-route 1
The operation is not supported.
[SH-5F-CORE-S6520X-1-Vsi-interface3502]ip policy-based-route 1
The operation is not supported.
[SH-5F-CORE-S6520X-1-Vsi-interface3502]
```

Process Analysis

This is because the VPN is specified in the ACL rule called by PBR. The underlying hardware of the device chip does not support ACL matching vpn, so if PBR calls this ACL, an error will be reported. Even if the matching VPN is not written in the rule, the traffic of source 10.3.32.3 can be matched (the current chip's underlying hardware does not support ACL matching VPN). The disadvantage is that in environments such as MPLS, if multiple VPNs use the same network segment, At this time, the ACL will match all VPNs that exist in the network segment, and it cannot exactly match the network segment

in a specific VPN).

The reason why the rule binding VPN can be configured is because ACL can also be used for software platform functions, such as ssh server acl 3010. In addition, as long as the ACL application that will deliver the underlying hardware has this restriction, such as QOS. This restriction exists whether it is applied to the int vlan port or the int vsi port.

The test is as follows:

```
[2034-S6520X-EI]acl advanced 3010
[2034-S6520X-EI-acl-ipv4-adv-3010] rule 10 permit ip vpn-instance vpn-default source 10.3.32.3 0
[2034-S6520X-EI-acl-ipv4-adv-3010]quit
[2034-S6520X-EI]policy-based-route 1 permit node 1
[2034-S6520X-EI-pbr-1-1] if-match acl 3010
[2034-S6520X-EI-pbr-1-1] apply next-hop vpn-instance vpn-default 172.31.2.9
[2034-S6520X-EI-pbr-1-1]#
[2034-S6520X-EI-pbr-1-1]quit
[2034-S6520X-EI]int Vsi-interface 3503
[2034-S6520X-EI-Vsi-interface3503]dis th
#
interface Vsi-interface3503
description jituan_caiwu
ip binding vpn-instance lan
ip address 10.88.136.1 255.255.254.0
#
return
[2034-S6520X-EI-Vsi-interface3503]ip policy-based-route 1 ?
<cr>
[2034-S6520X-EI-Vsi-interface3503]ip policy-based-route 1
```

The operation is not supported.

When applying QOS based on this ACL flow system, the following error will be reported.

```
[2034-S6520X-EI-Ten-GigabitEthernet1/0/1]qos apply policy p1 inbound
[2034-S6520X-EI-Ten-GigabitEthernet1/0/1]%Jun 24 04:28:49:568 2013 2034-S6520X-EI QOS/4/QO
S_POLICY_APPLYIF_CBFAIL: Failed to apply classifier-behavior c1 in policy p1 to the inbound
direction of interface Ten-GigabitEthernet1/0/1. In a classifier with AND operator, you cannot configur
e multiple ACL match rules.
```

```
[2034-S6520X-EI-Ten-GigabitEthernet1/0/1]qos apply policy p1 out
[2034-S6520X-EI-Ten-GigabitEthernet1/0/1]qos apply policy p1 outbound
[2034-S6520X-EI-Ten-GigabitEthernet1/0/1]%Jun 24 04:29:26:010 2013 2034-S6520X-EI QOS/4/QO
S_POLICY_APPLYIF_CBFAIL: Failed to apply classifier-behavior c1 in policy p1 to the outbound dire
ction of interface Ten-GigabitEthernet1/0/1. In a classifier with AND operator, you cannot configure m
ultiple ACL match rules
```

Solution

Cancel the vpn binding in the rule, and then it can be delivered successfully.

```
acl advanced 3010
rule 10 permit ip source 10.3.32.3 0
#
#
policy-based-route 1 permit node 1
if-match acl 3010
apply next-hop vpn-instance vpn-default 172.31.2.9
#
[2034-S6520X-EI]int Vsi-interface 3503
[2034-S6520X-EI-Vsi-interface3503]dis th
#
interface Vsi-interface3503
description jituan_caiwu
ip binding vpn-instance lan
ip address 10.88.136.1 255.255.254.0

[2034-S6520X-EI-Vsi-interface3503]ip policy-based-route 1
[2034-S6520X-EI-Vsi-interface3503]dis th
#
interface Vsi-interface3503
```

```
description jituan_caiwu
ip binding vpn-instance lan
ip address 10.88.136.1 255.255.254.0
ip policy-based-route 1
#
```