

## 知 配置IPv4路由策略对IPv6路由造成的影响

路由策略

IPv6

IPv4

zhiliao\_mglxRe

2021-09-14 发表

### 组网及说明

evpn组网（虽然本案例与evpn关系不大）

leaf——spine——防火墙

#### 问题描述

现场发现leaf设备下的vpn-teacher中的下挂终端都无法正常上网，经过检查，发现vpn-teacher中ipv6路由表项不正常，并没有从spine设备中传递过来，于是尝试着在spine设备中写了一条ipv6静态，发现一样没有通过bgp同步到leaf设备下，而且仅有该vpn实例下的ipv6表项不正常

## 过程分析

经过检查，发现与其他的vpn实例相比，该vpn-teacher实例视图下引用了一条路由策略ap1，如果不出意外，它应该就是罪魁祸首，如下：

```
ip vpn-instance vpn-teacher
route-distinguisher 1:6
import route-policy ap1
```

该路由策略ap1规则如下：

```
ip prefix-list 66 index 50 permit 172.18.0.0 18 less-equal 32 (注意，此处地址前缀列表66只匹配了ipv4的路由)
```

```
#
```

```
route-policy ap1 deny node 10
```

```
if-match ip address prefix-list 66
```

```
#
```

```
route-policy ap1 permit node 20 (注意，这里是空节点，默认放通所有路由)
```

理论而言，该路由策略ap1应该起到这样的作用：node10节点过滤掉一部分指定的ipv4路由，但我还有一个node20空节点，没有写任何的if-match匹配规则，因此默认匹配所有路由，其余没被node10过滤的ipv4路由，与所有的ipv6路由全部都可以通过node20空节点，这样就可以达成完美的过滤效果。

实际上呢？

配置手册里有这样一句话：

如果一个节点中if-match子句只指定了IPv6 ACL，没有指定IPv4 ACL，所有的IPv4路由信息都会匹配这个节点。如果一个节点中if-match子句只指定IPv4 ACL，没有指定IPv6 ACL，所有的IPv6路由信息都会匹配这个节点。

如上的话可以这样理解：

我写的路由策略ap1，实际上无法起到正常的过滤作用，因为在node10中，不止对应的ipv4路由，其他所有的ipv6路由也会默认匹配过来，然后被deny干掉，就没有机会去通过node20的空节点了。最终结果就是：匹配规则中的ipv4路由，以及所有的ipv6路由全都被干掉了，只有那些没在匹配规则中的ipv4路由幸运逃生。

现场的现象完全吻合这一点。

但是呢，手册中的话说得不够明确，不能百分之百确定是这个意思，为了确认现场问题是否真的是这个原因导致的，我做了一个简单的实验探究了下：

设备用的是6520x，我们称其为a设备，写了条静态的ipv6路由，这里为了排除是bgp的影响，改为使用ospfv3向一台下联设备b建立邻居，同时在ospfv3 1中配置import-route static route-policy aaa，将那条静态ipv6路由发布给下联邻居b（前提是那条静态路由能够通过路由策略aaa的考验呵呵），具体的路由策略aaa写法与前文实际案例一模一样，都是过滤ipv4的规则，理论上不该影响到ipv6的路由。

现象：确实有影响，下联邻居b完全看不到这条路由。

于是我把node20的那个空节点修改了下，加了匹配规则，让它匹配ipv6的路由，并且放通，但下联邻居b还是看不到这条ipv6的路由，因此可以确定，这条ipv6路由在node10阶段就已经被干掉了，因此我进入node10，在下面添加了一条另外的if-match匹配规则，匹配ipv6的lu"you（一个node节点里可以有n多个if-match匹配规则），并且动作改为permit放通，再去设备b上检查时，发现这条路由出现了！通过ospfv3传递过来了！

#### 解决方法

对于路由策略而言，只写ipv4的规则，亦或者只写ipv6的规则，实际上都会对另外的类型造成影响，所以说，如果组网中既有ipv4路由，也有ipv6的路由，两种路由都在路径上传递，想让路由策略起到相应的作用，请在节点中写两条if-match，分别把ipv4和ipv6的规则都匹配上。

