

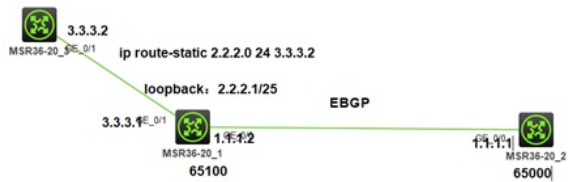
## 知 某局点通过路由策略过滤BGP路由信息不成功

域间策略/安全域 孔德飞 2022-04-24 发表

### 组网及说明

组网如下：

现场有如下需求，MSR1与MSR2建立EBGP邻居，MSR1上有2.2.2.0/24的静态路由与2.2.2.0/25的直连路由，现场想MSR1发布给MSR2的时候只发布2.2.2.0/25



告警信息

不涉及

## 问题描述

问题描述:

现场在MSR1上做如下路由策略, ACL中只写反掩码0.0.0.127对应正掩码25位

```
acl advanced 3900
```

```
rule 5 permit ip source 2.2.2.0 0.0.0.127
```

```
rule 10 deny ip
```

```
route-policy test permit node 1
```

```
if-match ip address acl 3900
```

```
route-policy test deny node 2
```

```
bgp 65100
```

```
router-id 22.22.22.22
```

```
peer 1.1.1.1 as-number 65000
```

```
#
```

```
address-family ipv4 unicast
```

```
import-route direct
```

```
import-route static
```

```
peer 1.1.1.1 enable
```

```
peer 1.1.1.1 filter-policy 3900 export
```

结果发现MSR2上还是能看到2.2.2.0/24为掩码的BGP路由

```
<H3C>dis ip routing-table
```

```
Destinations : 13    Routes : 13
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/0	Static	60	0	1.1.1.2	GE0/0
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	Direct	0	0	1.1.1.1	GE0/0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.255/32	Direct	0	0	1.1.1.1	GE0/0
<b>2.2.2.0/24</b>	<b>BGP</b>	<b>255</b>	<b>0</b>	<b>1.1.1.2</b>	<b>GE0/0</b>
2.2.2.0/25	BGP	255	0	1.1.1.2	GE0/0

## 过程分析

问题分析:

如果以2.2.2.0作为过滤条件, 那么ACL中不管是反掩码为0.0.0.255 (比较前24位) 或者0.0.0.127 (比较前25位)

2.2.2.0/24与2.2.2.0/25都能匹配上, 因为两条路由的前24位完全一致, ACL不管怎样都区分不开两者的路由, 当然无法过滤

## 解决方法

解决方案:

可以使用前缀列表+路由策略的方式过滤:

前缀列表是具体到掩码的位数的, 所以前缀列表可以由掩码的具体位数作为区分条件

**即相当于与ACL相比, 前缀列表多了一个判定条件就是掩码位数**

```
ip prefix-list test1 index 10 permit 2.2.2.0 25
```

```
route-policy test permit node 1
```

```
if-match ip address prefix-list test1
```

```
route-policy test deny node 2
```

```
bgp 65100
```

```
router-id 22.22.22.22
```

```
peer 1.1.1.1 as-number 65000
```

```
#
```

```
address-family ipv4 unicast
```

```
import-route direct
```

```
import-route static
```

```
peer 1.1.1.1 enable
```

```
peer 1.1.1.1 route-policy test export
```

**可以看到MSR2的路由表中只有2.2.2.0/25的路由**

```
<H3C>dis ip routing-table
```

```
Destinations : 12    Routes : 12
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/0	Static	60	0	1.1.1.2	GE0/0
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	Direct	0	0	1.1.1.1	GE0/0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.255/32	Direct	0	0	1.1.1.1	GE0/0
<b>2.2.2.0/25</b>	<b>BGP</b>	<b>255</b>	<b>0</b>	<b>1.1.1.2</b>	<b>GE0/0</b>
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

