

关于在聚合子接口下做镜像只能镜像出方向流量的经验案例

郭子威 2018-01-28 发表

客户将SR6616-X设备上的GigabitEthernet1/7/0/2和GigabitEthernet1/7/0/3两个接口加入聚合组，并在两个接口下输入mirroring-group 1 mirroring-port both做镜像，但是镜像后用wireshark抓包软件所抓出来的报文中只看到了一个方向的数据流量：只有出反向的报文没有进方向的报文。客户原配置如下：

```
#
interface Route-Aggregation2
description to chukou-yidong
service chassis 1 slot 7
ip address x.x.x.x 255.255.255.224
#
interface GigabitEthernet1/7/0/1
port link-mode route
combo enable copper
mirroring-group 1 monitor-port
#
interface GigabitEthernet1/7/0/2
port link-mode route
combo enable copper
mirroring-group 1 mirroring-port both
port link-aggregation group 2
#
interface GigabitEthernet1/7/0/3
port link-mode route
combo enable copper
mirroring-group 1 mirroring-port both
port link-aggregation group 2
```

718	17:37:10.182310	183.203.31.98	49.159.139.105	UDP	100	UDP	7710-7903 Len=58
719	17:37:10.182311	183.203.31.98	117.28.236.188	UDP	100	UDP	7334-7273 Len=58
720	17:37:10.134423	183.203.31.98	219.158.36.218	TCP	74	TCP	Echo (ping) request id=0x04cf, seq=47974/26299,
721	17:37:10.150768	183.203.31.98	223.5.5.5	DNS	73	UDP	Standard query 0xbcf92 A www.baidu.com
722	17:37:10.153065	183.203.31.98	39.67.17.146	UDP	100	UDP	7711-26693 Len=58
723	17:37:10.153112	183.203.31.98	183.63.206.204	UDP	100	UDP	7712-12993 Len=58
724	17:37:10.153130	183.203.31.98	60.191.11.202	UDP	100	UDP	7713-6662 Len=58
725	17:37:10.153343	183.203.31.98	39.67.17.146	UDP	100	UDP	7711-26693 Len=58
726	17:37:10.153346	183.203.31.98	183.238.99.233	UDP	100	UDP	7340-7382 Len=58
727	17:37:10.153347	183.203.31.98	101.191.1.14	UDP	100	UDP	7714-8188 Len=58
728	17:37:10.153347	183.203.31.98	113.106.5.105	UDP	100	UDP	7715-8023 Len=58
729	17:37:10.153487	183.203.31.98	125.111.160.18	UDP	100	UDP	7716-44717 Len=58
730	17:37:10.153489	183.203.31.98	124.236.133.116	UDP	100	UDP	7717-5834 Len=58
731	17:37:10.153489	183.203.31.98	114.88.15.88	UDP	100	UDP	7356-7273 Len=58
732	17:37:10.153588	183.203.31.98	123.57.159.181	UDP	100	UDP	7283-7273 Len=58
733	17:37:10.189538	183.203.31.98	118.190.175.178	UDP	100	UDP	7285-7517 Len=58
734	17:37:10.200755	183.203.31.98	60.191.37.136	TCP	189	TCP	17045-8888 [PSH, ACK] Seq=102295 Ack=29957 Win=58
735	17:37:10.203907	183.203.31.98	123.139.89.210	UDP	100	UDP	7718-8176 Len=58
736	17:37:10.254640	183.203.31.98	221.221.179.11	UDP	100	UDP	7392-8149 Len=58
737	17:37:10.254642	183.203.31.98	114.223.97.254	UDP	100	UDP	7704-7870 Len=58
738	17:37:10.254644	183.203.31.98	112.85.255.251	UDP	100	UDP	7719-7274 Len=58
739	17:37:10.254700	183.203.31.98	124.65.129.74	UDP	100	UDP	7720-32656 Len=58
740	17:37:10.254819	183.203.31.98	124.166.172.204	UDP	100	UDP	7300-7772 Len=58
741	17:37:10.279688	183.203.31.100	171.120.229.194	TCP	124	TCP	8547-10806 [PSH, ACK] Seq=3500 Ack=900 Win=62864
742	17:37:10.283100	183.203.31.100	171.120.229.194	TCP	60	TCP	8547-10806 [ACK] Seq=3570 Ack=978 Win=62786 Len=0
743	17:37:10.290307	183.203.31.98	86.15.56.194	UDP	60	UDP	7721-50845 Len=2
744	17:37:10.399389	183.203.31.98	60.25.11.172	UDP	60	UDP	7722-4170 Len=2
745	17:37:10.399421	183.203.31.98	211.212.247.131	UDP	60	UDP	7723-4803 Len=2
746	17:37:10.399442	183.203.31.98	58.223.151.33	UDP	60	UDP	7724-16179 Len=2
747	17:37:10.399458	183.203.31.98	121.229.151.195	UDP	60	UDP	7725-5158 Len=2
748	17:37:10.399505	183.203.31.98	59.41.44.192	UDP	60	UDP	7726-6651 Len=2
749	17:37:10.399520	183.203.31.98	218.20.36.129	UDP	60	UDP	7727-4670 Len=2
750	17:37:10.399573	183.203.31.98	83.5.252.29	eDonkey	60	UDP	Kademlia UDP: KADEMLIA2_BOOTSTRAP_REQ

原因是镜像配置在了聚合组的子接口上了，将子接口上镜像的命令undo掉后，在聚合组上配置镜像的命令，即可在抓包中看到正常的报文交互过程

将聚合组子接口的镜像命令undo掉，将镜像的命令配置在聚合组下即可。修改后的配置如下：

```
#
interface Route-Aggregation2
description to chukou-yidong
service chassis 1 slot 7
ip address x.x.x.x 255.255.255.224
mirroring-group 1 mirroring-port both
#
interface GigabitEthernet1/7/0/1
port link-mode route
combo enable copper
mirroring-group 1 monitor-port
#
interface GigabitEthernet1/7/0/2
port link-mode route
combo enable copper
port link-aggregation group 2
#
interface GigabitEthernet1/7/0/3
```

```
port link-mode route
combo enable copper
port link-aggregation group 2
#
```

给聚合组全部的子接口做镜像的时候，在聚合组下面配置镜像端口，不要在聚合组子接口下配置，否则镜像后抓到的文件可能会存在只有一个方向的报文。