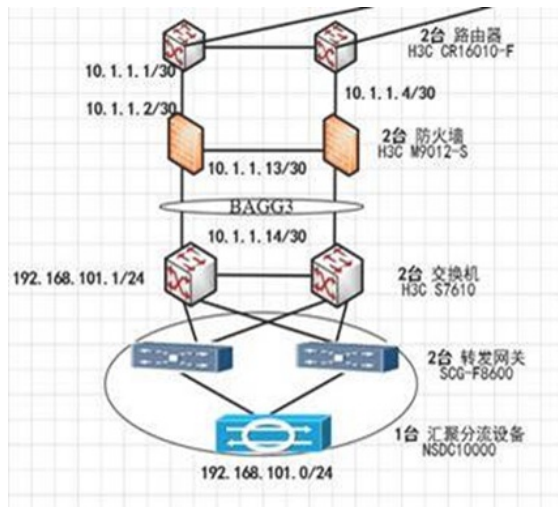


知 某局点M9000流量转发异常

IRF NAT 流量统计 刘文霖 2020-08-31 发表

组网及说明



问题描述

固定地址ping公网丢包，防火墙做的1对1nat，异常的地址存在规律，如下地址：192.168.101.102，192.168.101.106，192.168.101.110，192.168.101.114

过程分析

首先先确定是nat异常还是不过nat就有问题，于是使用这几个地址直接ping内网接口，发现也出现丢包现象，于是不用考虑nat，先排查内网问题，此时配置了一个手动备份组，或者undo nat static-load-balance enable问题解决了。

备份组一般对于对于公网地址不够，转换有问题导致，需要多个公网地址，同时一般触发限制大部分是不通，丢包不太正常，而且现在上联接口1/0/2/1nat做的都是静态的，应该不受公网地址限制才对，同时这个命令也只是取消负载，本身也没用问题，同时ping内网也丢包的话跟公网地址就没关系了，于是取消备份组进一步分析。

丢包问题，先做流统

Ping测试结果，只有三个包通了。

```
[zc@NFV-D-XNSC-01A-3111-0X05-S-SRV01 ~]$ ping -c 100 -I 192.168.101.102 10.1.1.1
1
PING 10.1.1.1 (10.1.1.1) from 192.168.101.102 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=50 ttl=253 time=0.266 ms
64 bytes from 10.1.1.1: icmp_seq=52 ttl=253 time=0.235 ms
64 bytes from 10.1.1.1: icmp_seq=60 ttl=253 time=0.237 ms

--- 10.1.1.1 ping statistics ---
100 packets transmitted, 3 received, 97% packet loss, time 99006ms
rtt min/avg/max/mdev = 0.235/0.246/0.266/0.014 ms
[zc@NFV-D-XNSC-01A-3111-0X05-S-SRV01 ~]$
```

查看流统结果：

从防火墙下联口收到了100个包

```
<SCCD-PC-CMNET-FW11-M9012-S> display qos policy interface Route-Aggregation 30
```

Interface: Route-Aggregation30

Direction: Inbound

Type : Enhancement

Policy: s_to_c

Classifier: default-class

Operator: AND

Rule(s):

If-match any

Behavior: be

-none-

Classifier: s_to_c

Operator: AND

Rule(s) :
If-match acl 3002
Behavior: accounting
Accounting enable:
100 (Packets), 0 (Bytes)

上联接口只发出去了17个包

```
Interface: HundredGigE1/0/2/1
Direction: Outbound
Type : Enhancement
Policy: s_to_c
Classifier: default-class
Operator: AND
Rule(s) :
If-match any
Behavior: be
-none-
Classifier: s_to_c
Operator: AND
Rule(s) :
If-match acl 3002
Behavior: accounting
Accounting enable:
17 (Packets)
```

对面也回了17个包

```
<SCCD-PC-CMNET-FW11-M9012-S>display qos policy interface HGE1/0/2/1
```

```
Interface: HundredGigE1/0/2/1
Direction: Inbound
Type : Enhancement
Policy: c_to_s
Classifier: default-class
Operator: AND
Rule(s) :
If-match any
Behavior: be
-none-
Classifier: c_to_s
Operator: AND
Rule(s) :
If-match acl 3001
Behavior: accounting
Accounting enable:
17 (Packets)
```

但最后下联口只发出了三个包，和ping测试结果一致

```
Interface: HundredGigE1/1/2/1
Direction: Outbound
Type : Enhancement
Policy: c_to_s
Classifier: default-class
Operator: AND
Rule(s) :
If-match any
Behavior: be
-none-
Classifier: c_to_s
Operator: AND
Rule(s) :
If-match acl 3001
Behavior: accounting
Accounting enable:
3 (Packets)
```

流统表明包就是丢在我们设备上了

此时查看CPU利用率

```
=====display process cpu chassis 1 slot 8 cpu 1 =====
```

CPU utilization in 5 secs: 2.4%; 1 min: 2.1%; 5 mins: 2.1%

```
463 0.0% 0.0% 0.0% [kdrvdp0]
464 0.0% 0.0% 0.0% [kdrvdp1]
.....
486 2.1% 2.0% 2.0% [kdrvdp23]// 48个转发核
100/48=2.08,也就是说达到2.08就已经把单核打满了
487 0.0% 0.0% 0.0% [kdrvdp24]
488 0.0% 0.0% 0.0% [kdrvdp25]
489 0.0% 0.0% 0.0% [kdrvdp26]
490 0.0% 0.0% 0.0% [kdrvdp27]
491 0.0% 0.0% 0.0% [kdrvdp28]
492 0.0% 0.0% 0.0% [kdrvdp29]
493 0.0% 0.0% 0.0% [kdrvdp30]
494 0.0% 0.0% 0.0% [kdrvdp31]
495 0.0% 0.0% 0.0% [kdrvdp32]
496 0.0% 0.0% 0.0% [kdrvdp33]
497 0.0% 0.0% 0.0% [kdrvdp34]
.....
506 0.0% 0.0% 0.0% [kdrvdp43]
507 0.0% 0.0% 0.0% [kdrvdp44]
508 0.0% 0.0% 0.0% [kdrvdp45]
509 0.0% 0.0% 0.0% [kdrvdp46]
510 0.0% 0.0% 0.0% [kdrvdp47]
```

可以看出出现了单核打满的情况

进到probe视图查看接口使用情况，1/0/1/13和2/0/1/23存在接口打满的情况

```
---: Not supported.
[SCCD-PC-CMNET-Fw11-M9012-S-probe]dis counters rate inbound interface
Usage: Bandwidth utilization in percentage
Interface      usage (%)  Total (pps)  Broadcast (pps)  Multicast (pps)
HGE1/0/2/1     0          374          0                 0
HGE1/0/2/2     10         4579638      0                 4579374
HGE1/1/2/1     0          477          0                 0
HGE1/1/2/2     0          403          0                 5
HGE2/0/2/1     0          259          0                 0
HGE2/0/2/2     0          434          0                 28
HGE2/1/2/1     0          425          0                 0
HGE2/1/2/2     0          391          0                 5
RAGG10         0          374          0                 0
RAGG20         0          259          0                 0
RAGG30         0          902          0                 0
XGE1/0/1/13    100        4579241      0                 4579240
XGE1/1/1/5     0          0            0                 0
XGE2/0/1/13    100        4578742      0                 4578742
XGE2/1/1/5     0          0            0                 0
```

造成slot8的cpu单核打满，上到此业务板的报文会有ping丢包情况。

Undo nat负载，或者使用手动备份组，业务上送到slot7，slot7没有单核打满的情况，所以不会丢包，从而造成了之前关闭负载和配置手动备份组能解决该问题的情况，只是流量没有到slot8了，看似解决了问题，实则是规避了。

解决方法

shutdown这两个异常接口，设备正常

后续排查接口下联设备为何上送大量报文上防火墙，调整下联设备后问题解决