Gamme 5000 ASR : Les déroutements de « BGPPeerSessionDown » en moins de la période de temporisateur d'attente après événement cassé de Connectivité se produit

Contenu

Introduction

Ce document explique la synchronisation impliquée quand un pair de Protocole BGP (Border Gateway Protocol) est identifié vers le bas par le déroutement de BGPPeerSessionDown en ce qui concerne la synchronisation de l'événement qui l'a déclenchée. Le temps où il prend pour que le pair obtienne marqué vers le bas est une valeur moins que la période du temporisateur d'attente. Cette question particulière a été signalée sur un routeur de services d'agrégation de Cisco (ASR) 5000 mais s'appliquerait également à un ASR 5500.

Problème

Dans ce cas particulier, il y avait un process restart de npumgr sur la carte de commutation par paquets de Demux (PSC) 1 sur ASR 5000 dû à la question micro d'engine, qui n'est pas celle rare d'une question passagère (il n'y a aucun besoin de RMA) :

```
2015-Jun-13+13:51:44.198 [sft 58000 info] [1/0/4255 <sft:100>
sft_monitor.c:115]
[software internal system critical-info syslog] SFT : Forced 1 times RX
packet at slot 1, cpu 0, inst 100, inflight packets 30

2015-Jun-13+13:51:45.306 [sft 58000 info] [1/0/4255 <sft:100>
sft_monitor.c:115]
[software internal system critical-info syslog] SFT : Forced 81 times RX
packet at slot 1, cpu 0, inst 100, inflight packets 110

2015-Jun-13+13:51:45.205 [sft 58000 info] [1/0/4255 <sft:100>
sft_monitor.c:115]
[software internal system critical-info syslog] SFT : Forced 71 times RX
packet at slot 1, cpu 0, inst 100, inflight packets 100
```

```
Sat Jun 13 13:51:45 2015 Internal trap notification 73 (ManagerFailure)
facility npumgr instance 1 card 1 cpu 1

2015-Jun-13+13:51:45.335 [npuctrl 16019 error] [8/0/4729 <npuctrl:0>
rl_sf_handler.c:2570] [software internal system syslog] SF CTRL:
monitoring_recovery:
Task packet test failed on failed_card 1, calling npuctrl_sf_insert_card()

2015-Jun-13+13:51:48.469 [npuctrl 16019 error] [8/0/4729 <npuctrl:0>
rl_sf_handler.c:2558] [software internal system syslog] SF CTRL:
monitoring_recovery:
too many sf insert calls on failed_card 1, cnt = 1 calling
npuctrl_restart_npumgr()

Sat Jun 13 13:51:48 2015 Internal trap notification 150 (TaskFailed)
facility npumgr instance 1 on card 1 cpu 1

2015-Jun-13+13:51:48.470 [npuctrl 16020 info] [8/0/4729 <npuctrl:0>
npuctrl_func.c:230] [software internal system critical-info syslog]
CTRL: restart npumgr instance 1

2015-Jun-13+13:51:48.547 [rct 13012 info] [8/0/4643 <rct:0> rct_task.c:323]
[software internal system critical-info syslog] Death notification of task
npumgr/1 on 1/1 sent to parent task npuctrl/0

Sat Jun 13 13:51:58 2015 Internal trap notification 1099 (ManagerRestart)
facility npumgr instance 1 card 1 cpu 1

Sat Jun 13 13:51:58 2015 Internal trap notification 151 (TaskRestart)
facility npumgr instance 1 on card 1 cpu 1

2015-Jun-13+13:51:58.376 [npuctrl 16018 info] [8/0/4729 <npuctrl:0>
npuctrl_msg.c:241] [software internal system critical-info syslog]
task facility npumgr instance 1 created
```

Le scanner d'ingénierie le capture bon :

```
%%%%%%%%%%%%% SFT : Forced X times RX packet at slot Y %%%%%%%%%%%%%
May be a case of Ucode storage corruption. Please check techzone article
2015-Jun-13+13:51:48.729 [sft 58000 info] [1/0/4255  sft_monitor.c:115]
[software internal system critical-info syslog] SFT : Forced 321 times
RX packet at slot 1, cpu 0, inst 100, inflight packets 238(Count: 33,
First seen: 2015-Jun-13+13:51:44.903,
Last seen: 2015-Jun-13+13:51:48.729)
```

Ces déroutements de Protocole SNMP (Simple Network Management Protocol) indiquent une seconde fenêtre 10 au-dessus dont tous les pairs BGP sur la passerelle d'entreprise ont descendu :

```
Sat Jun 13 13:52:00 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS14 ipaddr 55.54.84.107

Sat Jun 13 13:52:02 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS16 ipaddr 55.54.84.123

Sat Jun 13 13:52:03 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS06 ipaddr 55.54.84.43

Sat Jun 13 13:52:04 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS04 ipaddr 55.54.84.26

Sat Jun 13 13:52:04 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS14 ipaddr 55.54.84.106
```

```
Sat Jun 13 13:52:04 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS05 ipaddr 55.54.84.35

Sat Jun 13 13:52:04 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS02 ipaddr 55.54.84.11

Sat Jun 13 13:52:04 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn EXGWin ipaddr 55.55.245.4

Sat Jun 13 13:52:05 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS16 ipaddr 55.54.84.122

Sat Jun 13 13:52:05 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS12 ipaddr 55.54.84.91

Sat Jun 13 13:52:05 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS01 ipaddr 55.54.84.3

Sat Jun 13 13:52:05 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS11 ipaddr 55.54.84.83

Sat Jun 13 13:52:05 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS15 ipaddr 55.54.84.115

Sat Jun 13 13:52:05 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS01 ipaddr 55.54.84.2

Sat Jun 13 13:52:06 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS04 ipaddr 55.54.84.27

Sat Jun 13 13:52:06 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS05 ipaddr 55.54.84.34

Sat Jun 13 13:52:06 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS11 ipaddr 55.54.84.82

Sat Jun 13 13:52:06 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS06 ipaddr 55.54.84.42

Sat Jun 13 13:52:07 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Ingress ipaddr 55.55.245.5

Sat Jun 13 13:52:07 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS03 ipaddr 55.54.84.18

Sat Jun 13 13:52:07 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS10 ipaddr 55.54.84.254

Sat Jun 13 13:52:08 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS03 ipaddr 55.54.84.19

Sat Jun 13 13:52:08 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS15 ipaddr 55.54.84.114

Sat Jun 13 13:52:09 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS02 ipaddr 55.54.84.10

Sat Jun 13 13:52:10 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS13 ipaddr 55.54.84.98

Sat Jun 13 13:52:10 2015 Internal trap notification 119 (BGPPeerSessionDown)
vpn Egress-MPLS12 ipaddr 55.54.84.90
```

Le BGP est contrôlé sur le PSC 1 de Demux qui est dans ce cas la carte qui a eu la question. Il

est donc non inattendu pour que le BGP descende. Supplémentaire, puisque c'était une reprise inter active de session de châssis (ICSR) - châssis de technologie, il y avait un basculement de Protocol de Redondance de service (SRP) :

```
[local]Enterprise_XGW> show srp call-loss statistics
Switchover-9  started at : Sat Jun 13 13:52:06 2015,  took 3 seconds to finish.
   Switchover reason : BGP failure
   Total number of active calls at switchover time : 714711
```

Solution

Question

Si l'incident était à 13:51:45 par déroutements/logs, est-ce qu'on ne s'attendrait pas à ce qu'il pour que les pairs descendent pas plus tôt que la période du temporisateur d'attente BGP ?

Réponse

Les configurations BGP pour tous ces pairs sont identiques que ceci :

```
timers bgp keepalive-interval 10 holdtime-interval 60
```

Tandis que configurée pendant 60 secondes, la négociation avec le pair honore la valeur inférieure, qui est de 30 secondes :

```
******** show ip bgp neighbors *******
Saturday June 13 14:42:38 UTC 2015
BGP neighbor is 55.55.245.4, remote AS 22394, local AS  64873, external link
 BGP version 4, remote router ID 55.54.244.197
 BGP state = Established,up for 5d04h29m
 Hold time is 30 seconds, keepalive interval is 10 seconds
 Configured Hold time is 60 seconds, keepalive interval is 10 seconds
```

Comment les pairs qu'allez vers le bas entre 13:52:00 et 13:52:10 peuvent-ils être expliqué quand l'événement était à 13:51:45 ?

La réponse est qu'il est possible que la Connectivité a été compromise en raison de la question de l'unité de processeur de réseau (NPU) avant que le premier log ait été affiché. Par exemple, faites une supposition de 5 secondes à 13:51:40. Chaque pair BGP que la paire envoie/reçoit des keeps-alive toutes les 10 secondes, chacun sur leurs propres moyens « cycle ». Les paires de pair BGP ne sont pas toutes synced à une une autre quant aux intervalles de keep-alive, bien que chaque paire ait la même configuration de 10 secondes. Vous pouvez supposer que dans n'importe quel seconde intervalle 10 de temps, tous les pairs ont envoyé le Keepalives puisque l'intervalle de keepalive est de 10 secondes. Si la Connectivité se cassait à 13:51:40, alors toutes les paires de pair ont envoyé leur dernier Keepalives un jour ou l'autre entre 13:51:30 et 13:51:40 basés sur ce qu'étaient leurs cycles (souvenez-vous chaque paire est indépendant de n'importe quelles autres paires). Dans ce cas, sans davantage de Keepalives reçu après cette plage de temps, il signifie que la seconde échéance 30 se produirait de l'ordre de 13:52:00 - 13:52:10, qui est avec précision quand tous les pairs ont été marqués vers le bas.

En bref, après qu'on s'attende à ce que le moment que la Connectivité est cassée (, que ce puisse être déterminé ou pas est une autre question), BGP soit marqué en bas d'une certaine heure entre l'intervalle de durée d'attente et l'intervalle de durée d'attente sans l'intervalle convenu de

keepalive. Dans ce cas c'aurait lieu entre 20 et 30 secondes.

Informations connexes

- Guide de l'administration système ASR5000 - Cisco Systems
- Support et documentation techniques - Cisco Systems