# 5000 Series ASR: As armadilhas de “BGPPeerSessionDown” em menos do que o período de temporizador da posse após evento quebrado da Conectividade ocorrem

## Índice



## Introdução

Este documento explica o sincronismo envolvido quando um par do Border Gateway Protocol (BGP) é identificado para baixo por meio da armadilha de BGPPeerSessionDown no que diz respeito ao sincronismo do evento que o provocou. O tempo onde toma para que o par obtenha marcado para baixo é um valor menos do que a época do temporizador da posse. Esta questão particular foi relatada em um roteador dos serviços da agregação de Cisco (ASR) 5000 mas aplicar-se-ia ingualmente a um ASR 5500.

## Problema

Neste caso particular, havia um reinício do processo do npumgr no cartão do packet switching de Demux (PSC) 1 em ASR 5000 devido à micro edição do motor, que não é aquela rara de uma edição transiente (não há nenhuma necessidade para o 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
```

O varredor da engenharia captura-a boa:

```
%%%%%%%%%%%% 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)
```

Estas armadilhas de Protocolo de Gerenciamento de Rede Simples (SNMP) indicam um indicador 10 segundo sobre de que todos os bgp peer no gateway da empresa foram abaixo:

```
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
```

O BGP é controlado no PSC 1 de Demux que é neste caso o cartão que teve a edição. É consequentemente não inesperado para que o BGP vá para baixo. Adicionalmente, desde que esta era uma recuperação inter ativa da sessão do chassi (ICSR) - chassi da tecnologia, havia um switchover do protocolo de redundância do serviço (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
```

# Solução

## Pergunta

Se o incidente estava em 13:51:45 pelas armadilhas/logs, não se esperaria para que os pares vão abaixo de não mais logo do que o período de tempo do temporizador da posse BGP?

## Resposta

Os ajustes BGP para todos estes pares são os mesmos que este:

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

Quando configurada por 60 segundos, a negociação com o par honra o valor mais baixo, que é 30 segundos:

```
******** 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
```

Como podem os pares que vá para baixo entre 13:52:00 e 13:52:10 ser explicado quando o evento estava em 13:51:45?

A resposta foi que é possível que a Conectividade esteve comprometida em consequência da edição da unidade do processador de rede (NPU) antes que o primeiro log esteve indicado. Por exemplo, faça uma suposição dos segundos 5 em 13:51:40. Cada bgp peer que o par envia/recebe manutenções de atividade os segundos cada 10, cada um no seus próprios “ciclo”. Os pares do bgp peer não são toda sincronizados a um outro a propósito dos intervalos da manutenção de atividade, embora cada par tem o mesmo ajuste dos segundos 10. Você pode supor que em todo o intervalo 10 segundo do tempo, todos os pares enviaram o Keepalives desde que o intervalo keepalive é os segundos 10.  Se a Conectividade quebrou em 13:51:40, a seguir todos os pares de peer enviaram seu último Keepalives algum dia entre 13:51:30 e 13:51:40 baseados em quais seus ciclos eram (recorde que cada par é não relacionado a todos os outros pares). Neste caso, sem um Keepalives mais adicional recebido após este intervalo de tempo, significa que a segundo expiração 30 ocorreria na escala de 13:52:00 - 13:52:10, que é precisamente quando todos os pares foram marcados para baixo.

Em curto, depois que o ponto a tempo que a Conectividade é quebrada (se aquela pode ser determinado ou não é uma outra pergunta), BGP seria esperado ser marcado abaixo de alguma hora entre o intervalo de tempo de contenção e o intervalo de tempo de contenção menos o intervalo keepalive concordado. Neste caso isso realizar-se-ia entre 20 e 30 segundos.

## Informações Relacionadas

- Guia de Administração de Sistema ASR5000 - Cisco Systems
- Suporte Técnico e Documentação - Cisco Systems