

ASR, серии 5000: trap-сообщения "BGPPeerSessionDown" в меньше, чем период таймера ожидания после сломанного события подключения происходят

Содержание

[Введение](#)

[Проблема](#)

[Решение](#)

[Вопрос](#)

[Ответ](#)

[Дополнительные сведения](#)

Введение

Этот документ объясняет синхронизацию, включенную, когда узел Протокола BGP отмечен с trap-сообщением BGPPeerSessionDown относительно синхронизации события, которое инициировало его. Время, которое требуется для узла, который будет отмечен, является значением меньше, чем время таймера ожидания. Об этой отдельной проблеме сообщили относительно Маршрутизатора агрегации (ASR) Cisco 5000, но одинаково применится к ASR 5500.

Проблема

В данном случае был prumgr process restart на Карте коммутации пакетов (PSC) Демультимплексора 1 на ASR 5000 из-за Микро проблемы Механизма, которая не является, что редкий из переходной проблемы (нет никакой потребности в 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

Технический сканер перехватывает его хорошо:

%%%%%%%%%% 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)

Эти Перехваты простого протокола управления сетью (SNMP) указывают на 10 вторых окон, по которым выключились все Одноранговые соединения по протоколу BGP на шлюзе предприятия:

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

BGP управляется на PSC 1 Демультимплексора, который в этом случае является картой,

которая имела проблему. Это поэтому не неожиданно для BGP для потери работоспособности. Кроме того, так как это было активным Предать восстановление сеанса шасси земле (ICSR) - шасси технологии, был переключатель Сервисного протокола резервирования (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
```

Решение

Вопрос

Если бы инцидент был в 13:51:45 на trap-сообщения/журналы, то он, как ожидали бы, для узлов не выключится только, чем период времени таймера ожидания BGP?

Ответ

Параметры настройки BGP для всех этих узлов совпадают с этим:

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

В то время как настроено в течение 60 секунд, согласование с узлом соблюдает минимальное значение, которое составляет 30 секунд:

```
***** 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
```

Как может узлы, которые выключаются между 13:52:00 и 13:52:10 быть объясненными, когда событие было в 13:51:45?

Ответ - то, что возможно, что подключение поставилось под угрозу в результате проблемы Модуля сетевого процессора (NPU), прежде чем был отображен первый журнал. Например, сделайте предположение 5 секунд в 13:51:40. Каждая пара Однорангового соединения по протоколу BGP передает/получает пакеты Кеераливе каждые 10 секунд, каждого на их собственном "цикле". Пары однорангового соединения по протоколу BGP все не синхронизируются друг другу относительно интервалов проверки активности, хотя каждая пара действительно имеет то же значение 10 секунд. Можно предположить, что в любые 10 вторых интервалов времени, все узлы передали пакеты Кеераливе, так как интервал проверки активности составляет 10 секунд. Если подключение сломалось в 13:51:40, то все одноранговые пары передали свои последние пакеты Кеераливе когда-то между 13:51:30 и 13:51:40 на основе того, чем их циклы были (помните, что каждая пара не связана друг с другом к любой другой паре). В этом случае, без дальнейших пакетов Кеераливе, полученных после на этот раз диапазон, это означает, что 30-секундное истечение произошло бы в диапазоне 13:52:00 - 13:52:10, который является точно, когда были отмечены все узлы.

Короче говоря, после момента времени, что подключение сломано (в состоянии ли это быть

определенным или не является другим вопросом), BGP, как ожидали бы, будет отмечен некоторое время между интервалом времени удержания и интервалом времени удержания минус согласованный интервал проверки активности. В этом случае это было бы между 20 и 30 секундами.

Дополнительные сведения

- [Руководство по системному администрированию ASR5000 - Cisco Systems](#)
- [Cisco Systems – техническая поддержка и документация](#)