

# Congestão STP, IMSIMGR sobre aletas do estado, e do link SCTP em SGSN devido a HLR MAP\_RESET

## Índice

[Introdução](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[O link STP recebe demasiado tráfego](#)

[IMSIMGR advertem dentro o estado](#)

[Falha HLR](#)

[Recomendações](#)

[Fluxo de tráfego](#)

[Disparadores para o alarme congestionado M3UA em SGSN](#)

## Introdução

Este documento descreve um problema que seja encontrado no nó de apoio do General Packet Radio Service do serviço (GPRS) (SGSN) do roteador agregado Cisco 5000 Series dos serviços (ASR). Algumas alternativas possíveis para esta edição são descritas igualmente.

## Informações de Apoio

Esta corrente de eventos específica no ASR SGSN é descrita neste documento:

1. **novembro 20, 6:25 AM:** Um MAP\_RESET foi enviado pelo registro de lugar home (HLR).
2. **novembro 20, 8:13 AM:** Um alarme da congestão é levantado para o ponto de transferência 2 do sinal (STP-2).
3. **novembro 20, 8:23 AM:** Um alarme da congestão é levantado para STP-1 e STP-2.
4. **novembro 20, 8:48 AM:** O gerente internacional da identidade do assinante de celular (IMSIMGR) move-se no estado da *advertência*.
5. **novembro 20, 10:07 AM:** Os links restauraram de STP-2 para o SGSN.

6. **novembro 20, 10:15 AM:** A melhoria é observada no stats da atualização do lugar SGSN (LU).
7. **novembro 20, 10:30 AM do do â de 10:00:** As estatísticas começam a melhorar em 10:00 am.
8. **novembro 20, 11:15 AM:** Uma diminuição é observada no stats SGSN LU.
9. **novembro 20, 11:41 AM:** A equipe STP relata a isso o código do link de sinalização (SLC)-1 de STP-2 não recebe o tráfego, o SLC é restaurado, e retornos do tráfego ao normal.
10. **novembro 20, 11:42 AM:** Um alarme da congestão é levantado em SGSN para SLC-1 do STP.
11. **novembro 20, 12:00 PM:** Depois que SLC-3 é restaurado, os stats GPRS LU melhoram.

## Problema

Quando o HLR recebe a mensagem MAP\_RESET, ajusta uma bandeira para uma atualização do lugar GPRS (GLU). Quando o equipamento de usuário (UE) envia seus primeiros pacotes do uplink, o SGSN envia uma mensagem GLU ao HLR.

```
At 7 AM SGSN , Nov 21st 2014 had
***** show subscriber summary *****
Total Subscribers: 2386266
Active: 2386266
sgsn-pdp-type-ipv4: 942114
```

Segundo as indicações das saídas de exemplo, há 950,000 contextos do protocolo dos dados do empacotador (PDP) atuais no SGSN, e a tentativa de UEs consultar com ele porque o dia progride.

Quando os primeiros pacotes do uplink são recebidos, o SGSN provoca uma mensagem GLU. Desde que há umas centenas de milhares de UEs, o STP não pode segurar a quantidade de tráfego que é gerada e move-se em um estado de congestionamento constante.

As mensagens são enfileiradas no SGSN, e um *intervalo máximo da retransmissão* ocorre. Desde que todas as mensagens GLU não passam do SGSN ao HLR, o SGSN é forçado a destacar os assinantes de celular e a pedir que reatam. Todos os assinantes destacados tentam então anexar, que causa um impulso repentino no número de pedidos de entrada do acessório. Desde que a proteção da sobrecarga de rede é aplicada, a maioria das tentativas de anexar são rejeitado devido à congestão e os assinantes de celular são forçados a fazer uma tentativa nova.

Enquanto esta corrente de eventos se desdobra, produz influências de conexão em cascata. Muitos enviam mensagens da informação da autenticação (SAI), mensagens GLU, e as mensagens MAP-IMEI\_CHECK são coladas na fila SGSN ou deixadas cair. Por este motivo, todos os links STP-1 e STP-2 alcançam um estado de congestionamento. Cada STP tem quatro circuitos de sinalização, mas nesta encenação, os primeiros três links de STP-2 não recuperam para muito por muito tempo.

Estão aqui os alarmes da congestão, em que você pode ver que todos os links STP se movem no estado de congestionamento em STP-2:

```
Fri Nov 21 08:13:14 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-1 (point-code-782)
congested congLevel-1
Fri Nov 21 08:13:14 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-2 (point-code-782)
congested congLevel-1
Fri Nov 21 08:13:14 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-3 (point-code-782)
congested congLevel-1
Fri Nov 21 08:13:29 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 08:18:48 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 08:20:00 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 08:22:52 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 08:22:55 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 08:23:22 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 08:26:33 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 08:28:06 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 08:28:45 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
Fri Nov 21 09:27:27 2014 Internal trap notification 1074 (M3UAPSPCongested)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congested congLevel-1
```

Como mostrado, somente o processo de servidor de peer (PSP) 4 foi cancelado, e o resto está ainda no estado de congestionamento:

```
Fri Nov 21 08:18:47 2014 Internal trap notification 1075 (M3UAPSPCongestionCleared)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congestion cleared congLevel-0
```

## Solução

Esta seção descreve como pesquisar defeitos a edição que é descrita na seção anterior.

### O link STP recebe demasiado tráfego

Como descrito na seção anterior, um enlace particular no STP recebe uma grande quantidade de

tráfego. Você pode ver que os primeiros três links em STP-2 se movem no estado de congestionamento e nunca se recuperam, tão somente um link está disponível e o alarme da congestão é cancelado em SLC-3 (ou em peer-server-2-peer-server-process-4).

Conforme o mecanismo do compartilhamento de carga SGSN, deve enviar os pacotes da camada de adaptação de usuário do nível 3 do message transfer part (MTP) (MTP3) (M3UA) igualmente em todos os quatro links. Contudo, das armadilhas do protocolo de mensagem da rede simples (SNMP), os primeiros três links STP-2 são congestionados perennally, assim que significa que todo o tráfego está distribuído ao link SLC-3 (o único link disponível STP para distribuir o tráfego). Isto explica porque a distribuição de tráfego é enviesada entre os links STP-2.

Nas situações de congestionamento, uns ou vários links firmam entre congestionado e estados não-congestionados, tão somente os links disponíveis compartilham do tráfego. Por este motivo, há mais utilização em um dos links. Isto exige um link restaurar a fim recuperar os links.

A saída seguinte mostra as estatísticas do nível M3UA e destaca estatísticas. As estatísticas importantes a considerar são o exemplo 4 STP-2 PSP, onde o tráfego anormal pode ser considerado:

```
Fri Nov 21 08:18:47 2014 Internal trap notification 1075 (M3UAPSPCongestionCleared)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congestion cleared congLevel-0
```

Estão aqui os dados STP:

```
Fri Nov 21 08:18:47 2014 Internal trap notification 1075 (M3UAPSPCongestionCleared)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congestion cleared congLevel-0
```

Esta saída mostra que destaca por segundo na altura da edição:

```
Fri Nov 21 08:18:47 2014 Internal trap notification 1075 (M3UAPSPCongestionCleared)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congestion cleared congLevel-0
```

Esta saída mostra os diplomatas por segundo, conforme WEM:

```
Fri Nov 21 08:18:47 2014 Internal trap notification 1075 (M3UAPSPCongestionCleared)
ss7-routing-domain-1 peer-server-2 peer-server-process-4 (point-code-782)
congestion cleared congLevel-0
```

## IMSIMGR advertem dentro o estado

Cada anexo provisório novo da identidade do assinante de celular do atendimento IMSI/Packet (P-TMSI) e a distribuição do pedido da atualização da área (RAU) devem ser processados pelo IMSIMGR.

Com uma observação conservadora, o sistema recebe um valor de pico de 6,850 pedidos do anexo 2-G por segundo e ao redor 5,313 pedidos do anexo 3-G por segundo. O valor máximo que você pode ajustar para a proteção da sobrecarga de rede é 5,000 pedidos do anexo por segundo. A fim manter o IMSIMGR em um estado operável, o sistema não pode segurar tais um grande número atendimentos do UEs.

Esta edição começa depois que 8 AM, quando o tamanho da fila alcança 1,500 pedidos do anexo por segundo:

```
network-overload-protection sgsn-new-connections-per-second 500 action  
reject-with-cause congestion queue-size 1500 wait-time 5
```

Desde que há aproximadamente 12,000 pedidos do anexo por segundo, quase 9,000 atendimentos são processados pelo IMSIMGR e rejeitados. Isto faz com que o processamento de CPU IMSIMGR alcance um estado alto.

Se o SGSN recebe mais do que o número configurado de pedidos do anexo num segundo, a seguir os pedidos estão protegidos na fila de passeio e deixados cair somente quando os excessos de buffer devido a um anexo de entrada alto avaliam. As mensagens na fila estão processadas de acordo com um first in, processo do first-out (FIFO, primeiro a entrar, primeiro a sair) (FIFO) até que elas a idade-para fora em que a vida enfileirada da mensagem cruza o tempo de espera configurado.

Quando você escolhe as opções da rejeição ou da gota baseadas em sua preferência, Cisco recomenda que você usa um código de causa da rejeição a fim indicar a congestão na rede, que permite que você compreenda as condições de rede antes que você tente um procedimento do uplink.

## Falha HLR

Conforme a ó especificação técnica do projeto da parceria da geração (3GPP) (TS) 23.060, esta seção descreve o comportamento SGSN durante um reinício HLR. Sempre que o SGSN recebe uma restauração do MAPA, espera-se enviar um pedido UL para o HLR para seus assinantes.

Quando um HLR reinicia, envia uma mensagem da restauração a cada SGSN a qual ou mais de suas estações móveis (MS) são registrados. Isto faz com que o SGSN marque os contextos móveis relevantes do Gerenciamento como inválidos se uma associação SGSN-à-móvel do registro do lugar do centro de interruptor (MSC) /Visiting (VLR) existe. Depois que recibo do primeiro quadro válido do Logical Link Control (LLC) (para o modo A/Gb) ou depois que o recibo do primeiro pacote ou uplink válido do usuário do protocolo de tunelamento GPRS (GPT-U) que sinalizam a mensagem (para o modo lu) de uma estação móvel marcada, o SGSN executa um UL ao HLR como no pedido do anexo ou nos procedimentos de distribuição inter-SGSN da atualização da área (RA). Também, se a bandeira do alerta NON-GPRS (NGAF) é ajustada, o procedimento na cláusula do *alerta NON-GPRS* é seguido. O procedimento UL e o procedimento para o MSC/VLR puderam ser atrasados pelo SGSN para uma configuração máxima do operador, dependente do uso dos recursos naquele tempo a fim evitar a elevação que sinaliza a carga.

**Note:** O backup periódico dos dados HLR ao armazenamento permanente é imperativo, como descrito em TS 23.007 [5].

## Recomendações

Cisco recomenda que você termina estas etapas a fim resolver esta edição:

1. Aumente o número de novas conexões por segundo. Isto pode ser calculado com base no número médio de pedidos do anexo.
2. Aumente o Transactions Per Second (TP) no link STP a um valor ideal.
3. Mude o valor do padrão **SCTP-RTO-MAX** de 600 ( $600 \times 100 = 60,000$ ) a 5 (Senhora  $5 \times 100$ ). Por exemplo, para dois STP com 4,000 TP, você pode apoiar até 1,000 pedidos do anexo por segundo do SGSN.

**Note:** Cada pedido do anexo conduz a quatro transações para o STP, assim que significa que 1,000 pedidos do anexo conduzem por segundo a 4,000 TP.

Idealmente, cada STP tem quatro links de modo que 125 pedidos do anexo possam ser processados pelo link STP. Isto é distribuído igualmente através de todos os links STP. Contudo, se um dos links vai para baixo, muitas tentativas da reconexão são consideradas, a fila torna-se completamente, e os descartes de pacote de informação ocorrem. Se mais links vão para baixo, a seguir o tráfego está distribuído desigualmente.

## Fluxo de tráfego

O tráfego UE não segue uma forma Linear. Ocorre geralmente em uma explosão e com muitas tentativas da reconexão. O SGSN envia o tráfego nos pacotes ao STP. Naquele tempo, as quantidades do tráfego excedem os TP configurados no STP. Isto faz com que alguns links no STP comecem a anunciar o baixo tamanho de janela se já processam mais atendimentos, e o SGSN começa a enfileirar os pedaços dos dados SCTP que são enfileirados. Espera então o temporizador RTO MAX para expirar.

Se o STP envia periodicamente um bom tamanho de janela anunciado, a seguir você deve poder enviar mais pedaços dos dados SCTP se o valor **SCTP\_RTO\_MAX** é reduzido a cinco segundos ou menos. A fila é cancelada mais rapidamente e um alarme da congestão M3UA não é provocado. Adicionalmente, você não deve ver o flag de controle do fluxo interno provocado pelo SCTP a fim controlar o fluxo de pacote de informação.

O SGSN envia somente pacotes na quantidade que o STP pode aceitar, que é baseado no tamanho de janela anunciado. Se você aumenta os TP pelo STP liga, ajuda a evitar a congestão STP e reduz o temporizador SCTP\_RTO\_MAX.

## Disparadores para o alarme congestionado M3UA em SGSN

Se o tamanho de janela anunciado na mensagem do reconhecimento seletivo do Stream Control Transmission Protocol (SCTP) (SACO) é próximo a zero (ou a zero), a seguir o SGSN levanta um alarme M3UA a fim indicar que as mensagens não devem ser enviadas para esse valor-limite do par. Isto faz com que o link bata ou mova-se em um estado congestionado. Desde que o SGSN envia um tamanho de janela mais alto, você continua a receber dados M3UA dos peer node, e aqueles pacotes puderam ser deixados cair na fila de espera se o point code do par nunca sai do estado congestionado.

Aqui está um exemplo:

1. O SCTP envia uma indicação do começo do controle de fluxo ao M3UA.
2. O M3UA ajusta a bandeira ativa da congestão para a associação e começa a votar periodicamente o SCTP sobre seu estado do controle de fluxo.
3. Quando uma associação estiver no controle de fluxo, enfileira as solicitações de dados futuras para essa associação até que o QUEUE\_SIZE alcance 8,000. Nesse ponto, os mensagens futura para a associação são rejeitados.
4. Se o STP envia um tamanho de janela anunciado apropriado, a seguir o M3UA tenta esvaziar as mensagens que são enfileiradas até que alcancem 5,000. O temporizador RTO igualmente joga um papel neste.

Os Mensagens SCTP são enfileirados somente para aquelas associações onde a bandeira de controle de fluxo se torna **verdadeira**, e os processos SGSN então de acordo com a resposta STP:

```
*Peer Server Id :          2    Peer Server Process Id:          2

Association State : ESTABLISHED

Flow Control Flag : TRUE
Peer INIT Tag : 20229
SGSN INIT Tag : 3315914061
Next TSN to Assign to
Outgoing Data Chunk : 3418060778
Lowest cumulative TSN acknowledged : 3418060634
Cumulative Peer TSN arrived from peer : 103253660
Last Peer TSN sent in the SACK : 103253658
Self RWND : 1048576
Advertised RWND in received SACK : 8
Peer RWND(estimated) : 8
Retransmission counter : 0
Zero Window Probing Flag : FALSE
Last Tsn received during ZWnd Probing : 0
Bytes outstanding on all
addresses of this association : 19480
Congestion Queue Length : 143
Ordered TSN assignment Waiting QLen      :          8050
Unordered TSN assignment Waiting QLen : 0
Total number of GAP ACKs Transmitted : 279
Total number of GAP ACKs Received : 58787
```

Path No. : 1

```
Current CWND : 11840
SSThresh : 11840
Partial Bytes Acked : 0
Bytes Outstanding for this Path : 19480
Current RTO for this Path(in ms)      :          60000
```

Como mostrado, a razão atrás da congestão é que o número total de pedaços de partida excede o limite 5,000 ( $8050+143=8193$ ) e bate o 60-segundo temporizador máximo RTO, que conduz às solicitações de dados rejeitadas SCTP. Também, há um temporizador mais alto RTO.