

# Congestión STP, IMSIMGR sobre las aletas del estado, y del link SCTP en SGSN debido a HLR MAP\_RESET

## Contenido

[Introducción](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[El link STP recibe demasiado tráfico](#)

[IMSIMGR adentro advierten el estado](#)

[Error HLR](#)

[Recomendaciones](#)

[Flujo de tráfico](#)

[Activadores para la alarma congestionada M3UA en SGSN](#)

## Introducción

Este documento describe un problema que se encuentre en el General Packet Radio Service de la porción (GPRS) que soporta el nodo (SGSN) del router agregado las Cisco 5000 Series de los servicios (ASR). Algunas soluciones alternativas posibles para este problema también se describen.

## Antecedentes

Este encadenamiento de los eventos específico en el ASR SGSN se describe en este documento:

1. **De nov el 21, 6:25:** Un MAP\_RESET fue enviado por el registro de ubicación casera (HLR).
2. **De nov el 21, 8:13:** Una alarma de la congestión se aumenta para la punta de transferencia de señal 2 (STP-2).
3. **De nov el 21, 8:23:** Una alarma de la congestión se aumenta para STP-1 y STP-2.
4. **De nov el 21, 8:48:** El administrador internacional de la identidad del suscriptor móvil (IMSIMGR) se traslada al estado del *cuidado*.
5. **De nov el 21, 10:07:** Los links reajustaron de STP-2 hacia el SGSN.

6. **De nov el 21, 10:15:** La mejora se observa en el stats de la actualización de la ubicación SGSN (LU).
7. **De nov el 21, 10:30 del del â de 10:00:** Las estadísticas comienzan a mejorar en 10:00.
8. **De nov el 21, 11:15:** Una disminución se observa en el stats SGSN LU.
9. **De nov el 21, 11:41:** El equipo STP señala a eso el código del link de señalización (SLC)-1 de STP-2 no recibe el tráfico, se reajusta el SLC, y las devoluciones del tráfico a normal.
10. **De nov el 21, 11:42:** Una alarma de la congestión se aumenta en SGSN para SLC-1 del STP.
11. **De nov el 21, 12:00 PM:** Después de que se reajuste SLC-3, los stats GPRS LU mejoran.

## Problema

Cuando el HLR recibe el mensaje MAP\_RESET, fija un indicador para una actualización de la ubicación GPRS (GLU). Cuando el equipo del usuario (UE) envía sus primeros paquetes del uplink, el SGSN envía un mensaje GLU al HLR.

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

Tal y como se muestra en de la salida de ejemplo, hay 950,000 contextos del protocolo de datos del embalador (PDP) presentes en el SGSN, y la tentativa de UEs de hojear con él pues el día progresa.

Cuando se reciben los primeros paquetes del uplink, el SGSN acciona un mensaje GLU. Puesto que hay cientos de miles UEs, el STP no puede manejar la cantidad de tráfico se genera que y se traslada a un estado de congestión perenne.

Los mensajes se hacen cola en el SGSN, y un *descanso máximo de la retransmisión* ocurre. Puesto que todos los mensajes GLU no pasan del SGSN al HLR, el SGSN se fuerza a separar a los suscriptores móviles y a pedir que reatan. Todos los suscriptores separados entonces intentan asociar, que causa una oleada súbita en el número de peticiones entrantes de la conexión. Puesto que la protección de la sobrecarga de red es aplicada, la mayor parte de las tentativas de asociar son rechazado debido a la congestión y fuerzan a los suscriptores móviles a hacer una nueva tentativa.

Mientras que este encadenamiento de los eventos revela, produce las influencias de conexión en cascada. Muchos envían los mensajes de la información de autenticación (SAI), los mensajes GLU, y los mensajes MAP-IMEI\_CHECK se pegan en la cola SGSN o se caen. Por este motivo, todos los links STP-1 y STP-2 alcanzan a un estado de congestión. Cada STP tiene cuatro links de señalización, pero en este escenario, los primeros tres links de STP-2 no se recuperan para muy de largo.

Aquí están las alarmas de la congestión, en las cuales usted puede ver que todos los links STP se trasladan al estado de congestión en 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 se muestra, solamente el proceso de servidor de peer (PSP) 4 fue borrado, y el resto todavía está en el estado de congestión:

```
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
```

## Solución

Esta sección describe cómo resolver problemas el problema que se describe en la sección anterior.

**El link STP recibe demasiado tráfico**

Según lo descrito en la sección anterior, un link determinado en el STP recibe una gran cantidad de tráfico. Usted puede ver que los primeros tres links en STP-2 se trasladan al estado de congestión y nunca se recuperan, tan solamente un link está disponible y la alarma de la congestión se borra en SLC-3 (o peer-server-2-peer-server-process-4).

Según el mecanismo de la carga a compartir SGSN, debe enviar los paquetes de la Capa de adaptación del usuario del nivel 3 de la parte de transferencia de mensaje (MTP) (MTP3) (M3UA) igualmente en los cuatro links. Sin embargo, de los desvíos del (SNMP) del protocolo de mensaje de la red simple, los primeros tres links STP-2 perenne se congestionan, así que significa que todo el tráfico está ruteado al link SLC-3 (el único link disponible STP para rutear el tráfico). Esto explica porqué la distribución del tráfico se sesga entre los links STP-2.

En las situaciones de congestión, uno o más links conectan entre congestionado y los estados no congestionados, tan solamente los links disponibles comparten el tráfico. Por este motivo, hay más utilización en uno de los links. Esto requiere un link reajustar para recuperar los links.

La salida siguiente muestra las estadísticas del nivel M3UA y separa las estadísticas. Las estadísticas importantes a considerar son el caso 4 STP-2 PSP, donde el tráfico anormal puede 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
```

Aquí están los datos 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 salida muestra que separa por segundo a la hora del problema:

```
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 salida muestra a los attaches por segundo, según 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 adentro advierten el estado

Cada nueva fijación temporal de la identidad del suscriptor móvil de la llamada IMSI/Packet (P-TMSI) y rutear la petición de la actualización del área (RAU) se deben procesar por el IMSIMGR.

Con una observación conservadora, el sistema recibe un valor pico de 6,850 peticiones de la fijación 2-G por segundo y alrededor 5,313 peticiones de la fijación 3-G por segundo. El valor máximo que usted puede fijar para la protección de la sobrecarga de red es 5,000 peticiones de la fijación por segundo. Para mantener el IMSIMGR un estado operable, el sistema no puede manejar tales un gran número de llamadas del UEs.

Este problema comienza después de que 8, cuando el tamaño de la cola alcanza 1,500 peticiones de la fijación por segundo:

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

Puesto que hay aproximadamente 12,000 peticiones de la fijación por segundo, casi 9,000 llamadas son procesadas por el IMSIMGR y rechazadas. Esto hace el IMSIMGR procesamiento de la CPU alcanzar un alto estado.

Si el SGSN recibe más que el número configurado de peticiones de la fijación en las segundas, después las peticiones están mitigadas en la cola de establecimiento del paso y caídas solamente cuando los desbordamientos de búfer debido a una alta fijación entrante valoran. Los mensajes en la cola se procesan de acuerdo con un primero en entrar, proceso del primero en salir ((Primero en Entrar, Primero en Salir FIFO)) hasta que ellos la edad-hacia fuera en que el curso de la vida hecho cola del mensaje cruza el tiempo de espera configurado.

Cuando usted elige las opciones del rechazo o del descenso basadas en su preferencia, Cisco recomienda que usted utiliza un código de la causa del rechazo para indicar la congestión en la red, que permite que usted entienda a los estados de la red antes de que usted intente un procedimiento del uplink.

## Error HLR

Según la especificación técnica del proyecto de la sociedad de la 3ra generación (3GPP) (TS) 23.060, esta sección describe el comportamiento SGSN durante un reinicio HLR. Siempre que el SGSN reciba una restauración del MAPA, se espera que envíe una petición UL hacia el HLR para sus suscriptores.

Cuando un HLR recomienza, envía un mensaje de la restauración a cada SGSN a cuál o más de sus estaciones móviles (MS) se registran. Esto hace el SGSN marcar los contextos móviles relevantes de la Administración como inválidos si existe una asociación SGSN-a-móvil del registro de la ubicación del centro de transferencia (MSC) /Visiting (VLR). Después de que el recibo del primer bastidor válido del Logical Link Control (LLC) (para el modo A/Gb) o después del recibo del primer paquete válido o del uplink del usuario del Tunneling Protocol GPRS (GPT-U) que señala el mensaje (para el modo lu) de una estación móvil marcada, el SGSN realice un UL al HLR como en la petición de la fijación o los procedimientos interes-SGSN de la actualización del área que rutean (RA). También, si se fija el indicador de la alerta NON-GPRS (NGAF), el procedimiento en la cláusula de la *alerta NON-GPRS* se sigue. El procedimiento UL y el procedimiento hacia el MSC/VLR se pudieron retrasar por el SGSN para una configuración máxima del operador, dependiente sobre el uso de los recursos en aquel momento para evitar el alto que señalaba la carga.

**Note:** El respaldo periódico de los datos HLR al almacenamiento permanente es obligatorio, según lo descrito en TS 23.007 [5].

## Recomendaciones

Cisco recomienda que usted completa estos pasos para resolver este problema:

1. Aumente el número de nuevas conexiones por segundo. Esto se puede calcular sobre la base del número medio de peticiones de la fijación.
2. Aumente el Transactions Per Second (TP) en el link STP a un valor ideal.
3. Cambie el valor del valor por defecto **SCTP-RTO-MAX** de 600 ( $600 \cdot 100 = 60,000$ ) a 5 (el ms  $5 \cdot 100$ ). Por ejemplo, para dos STP con 4,000 TP, usted puede soportar hasta 1,000 peticiones de la fijación por segundo del SGSN.

**Note:** Cada petición de la fijación da lugar a cuatro transacciones hacia el STP, así que significa que 1,000 peticiones de la fijación por segundo dan lugar a 4,000 TP.

Idealmente, cada STP tiene cuatro links para poder procesar 125 peticiones de la fijación por el link STP. Esto se distribuye igualmente a través de todos los links STP. Sin embargo, si va uno de los links abajo, se consideran muchas tentativas de la reconexión, la cola se convierte por completo, y los descartes de paquetes ocurren. Si van más links abajo, después el tráfico se distribuye irregularmente.

## Flujo de tráfico

El tráfico UE no sigue una moda Lineal. Ocurre generalmente en una explosión y con muchas tentativas de la reconexión. El SGSN envía el tráfico en los conjuntos al STP. En aquel momento, las cantidades del tráfico exceden los TP configurados en el STP. Esto hace algunos links en el STP comenzar a hacer publicidad del tamaño de la ventana bajo si procesan ya más llamadas, y el SGSN comienza a hacer cola los pedazos de los datos SCTP se hacen cola que. Entonces espera el temporizador RTO MAX para expirar.

Si el STP envía periódicamente un buen tamaño de la ventana de divulgación, después usted debe poder enviar más pedazos de los datos SCTP si el valor **SCTP\_RTO\_MAX** se reduce a cinco segundos o menos. La cola se borra más rápidamente y una alarma de la congestión M3UA no se acciona. Además, usted no debe ver el indicador de control del flujo interno accionado por el SCTP para controlar el flujo de paquetes.

El SGSN envía solamente los paquetes en la cantidad que el STP puede validar, que se basa en el tamaño de la ventana de divulgación. Si usted aumenta los TP por el STP conecta, ayuda a evitar la congestión STP y reduce el temporizador **SCTP\_RTO\_MAX**.

## Activadores para la alarma congestionada M3UA en SGSN

Si el tamaño de la ventana de divulgación en el mensaje del acuse de recibo selectivo del Stream Control Transmission Protocol (SCTP) (SACO) está cercano a cero (o a cero), después el SGSN aumenta una alarma M3UA para indicar que los mensajes no se deben enviar para ese punto final del par. Esto hace el link agitar o trasladarse a un estado de congestión. Puesto que el SGSN envía un tamaño de la ventana más alto, usted continúa recibiendo los datos M3UA de los nodos del peer, y esos paquetes se pudieron caer en la fila de procesos en espera si el código de punto del par nunca sale del estado de congestión.

Aquí tiene un ejemplo:

1. El SCTP envía una indicación del comienzo del control de flujo al M3UA.
2. El M3UA fija el indicador activo de la congestión para la asociación y comienza a sondear el SCTP periódicamente sobre su estatus del control de flujo.
3. Mientras que una asociación está en el control de flujo, hace cola los pedidos de datos futuros para esa asociación hasta que el QUEUE\_SIZE haya alcanzado 8,000. En ese momento, los mensajes futuros para la asociación se desechan.
4. Si el STP envía un tamaño de la ventana de divulgación apropiado, después el M3UA intenta vaciar los mensajes se hacen cola que hasta que alcancen 5,000. El temporizador RTO también desempeña un papel en esto.

Los Mensajes SCTP se hacen cola solamente para esas asociaciones donde el indicador de control de flujo llega a ser **verdad**, y los procesos SGSN entonces de acuerdo con la respuesta 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 se muestra, la razón detrás de la congestión es que el número total de pedazos salientes excede el límite 5,000 ( $8050+143=8193$ ) y golpea el 60-segundo temporizador máximo RTO, que da lugar a los pedidos de datos desechados SCTP. También, hay un temporizador más alto RTO.