Congestión STP, estado de exceso IMSIMGR y inestabilidad de enlace SCTP en SGSN debido a HLR MAP_RESET

Contenido

Introducción

Este documento describe un problema que se encuentra en el nodo de soporte de Serving General Packet Radio Service (GPRS) (SGSN) del Cisco 5000 Series Aggregated Services Router (ASR). También se describen algunas posibles soluciones para este problema.

Antecedentes

Esta cadena específica de eventos en ASR SGSN se describe en este documento:

1. 21 de noviembre, 6:25 AM: El Registro de Ubicación de Casa (HLR) envió un MAP_RESET.

2. 21 de noviembre, 8:13 AM: Se activa una alarma de congestión para el punto 2 de transferencia de señal (STP-2).

3. 21 de noviembre, 8:23 AM: Se activa una alarma de congestión para STP-1 y STP-2.

4. 21 de noviembre, 8:48 a.m: el administrador de identidad de suscriptor móvil internacional (IMSIMGR) pasa al estado warn.

5. 21 de noviembre, 10:07 AM: Los links se reinician desde el STP-2 hacia el SGSN.

6. 21 de noviembre, 10:15 AM: Se observa una mejora en las estadísticas de actualización de ubicación de SGSN (LU).

7. 21 de noviembre, 10:00 â 10:30: Las estadísticas comienzan a mejorar a las 10:00 am.

8. 21 de noviembre, 11:15 AM : Se observa una disminución en las estadísticas de LU de SGSN.

9. 21 de noviembre, 11:41 AM: El equipo STP informa que el Signaling Link Code (SLC)-1 de STP-2 no recibe tráfico, el SLC se reinicia y el tráfico vuelve a la normalidad.

10. 21 de noviembre, 11:42 AM: Se activa una alarma de congestión en SGSN para SLC-1 del STP.

11. 21 de noviembre, 12:00 PM: Después de reiniciar SLC-3, las estadísticas de GPRS LU mejoran.

Problema

Cuando el ELO recibe el mensaje MAP_RESET, establece un indicador para una actualización de ubicación GPRS (GLU). Cuando el equipo de usuario (UE) envía sus primeros paquetes de enlace ascendente, el SGSN envía un mensaje GLU al ELO.

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

Como se muestra en el ejemplo de salida, hay 950 000 contextos de protocolo de datos de empaquetador (PDP) presentes en el SGSN y los UE intentan examinarlos a medida que avanza el día.

Cuando se reciben los primeros paquetes de link ascendente, el SGSN activa un mensaje GLU. Dado que hay cientos de miles de UE, el STP no puede manejar la cantidad de tráfico que se genera y se mueve a un estado de congestión perenne.

Los mensajes se ponen en cola en el SGSN y se produce un tiempo de espera de retransmisión máximo. Dado que todos los mensajes GLU no pasan del SGSN al HLR, el SGSN se ve obligado a desconectar a los suscriptores móviles y solicitar que se vuelvan a conectar. A continuación, todos los suscriptores desconectados intentan conectarse, lo que provoca un aumento repentino en el número de solicitudes de conexión entrantes. Dado que se aplica la protección contra sobrecarga de red, la mayoría de los intentos de conexión se rechazan debido a la congestión y los suscriptores móviles se ven obligados a realizar un nuevo intento.

A medida que se desarrolla esta cadena de eventos, produce efectos en cascada. Muchos

mensajes de información de autenticación de envío (SAI), mensajes GLU y mensajes MAP-IMEI_CHECK se atascan en la cola SGSN o se descartan. Por esta razón, todos los links STP-1 y STP-2 alcanzan un estado de congestión. Cada STP tiene cuatro links de señalización, pero en este escenario, los tres primeros links de STP-2 no se recuperan durante mucho tiempo.

Estas son las alarmas de congestión, en las que puede ver que todos los links STP pasan 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, sólo se borró el proceso de servidor par (PSP) 4 y el resto sigue en estado de congestión:

<#root>

```
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

En esta sección se describe cómo solucionar el problema descrito en la sección anterior.

El link STP recibe demasiado tráfico

Como se describió en la sección anterior, un link particular en el STP recibe una gran cantidad de tráfico. Puede ver que los primeros tres links en STP-2 pasan al estado de congestión y nunca se recuperan, por lo que sólo hay un link disponible y la alarma de congestión se borra en SLC-3 (o peer-server-2-peer-server-process-4).

Según el mecanismo de distribución de carga SGSN, debe enviar los paquetes de Capa de adaptación del usuario (M3UA) de nivel 3 (MTP3) de la parte de transferencia de mensajes (MTP) por igual en los cuatro links. Sin embargo, a partir de las trampas del Protocolo simple de mensajes de red (SNMP), los primeros tres links STP-2 están congestionados permanentemente, lo que significa que todo el tráfico se enruta al link SLC-3 (el único link STP disponible para rutear el tráfico). Esto explica por qué la distribución del tráfico está sesgada entre los links STP-2.

En situaciones de congestión, uno o más links alternan entre estados congestionados y no congestionados, de modo que sólo los links disponibles comparten el tráfico. Por esta razón, hay más utilización en uno de los links. Esto requiere un restablecimiento del link para recuperar los links.

El siguiente resultado muestra las estadísticas de nivel M3UA y las estadísticas de desconexión. Las estadísticas importantes a considerar son la instancia 4 de PSP STP-2, donde se puede ver tráfico anormal:

Time	#1:ss7rd-m3ua-psp-data-tx	#2:ss7rd-m3ua-psp-error-tx	#3:ss7rd-m3ua-psp-data-rx
21-11-14 7:30	37409	0	37942
21-11-14 8:00	43677	0	43866
21-11-14 8:30	190414	0	71844
21-11-14 9:00	547418	0	104135
21-11-14 9:30	536019	0	102477
21-11-14 10:00	376797	0	132227
21-11-14 10:30	100394	0	97302
21-11-14 11:00	119652	0	114809
21-11-14 11:30	107073	0	95354

Estos son los datos STP:

DATE	TIME	LSN	LOC	SLC	LINK	TX %	RX %
11/21/2014	9:00 sgsncisco	5216	3	A	IPVL	11.26	62.07
11/21/2014	9:00 sgsncisco	5213	0	A1	IPVL	11.29	4.86
11/21/2014	9:00 sgsncisco	5214	1	A1	IPVL	11.27	4.85
11/21/2014	9:00 sgsncisco	5215	2	A	IPVL	11.23	4.7

Este resultado muestra las separaciones por segundo en el momento del problema:

Time	#13:2G-ms-init-detach	#14:2G-nw-init-detach
21-11-14 6:30	136465	7400
21-11-14 7:00	149241	9557
21-11-14 7:30	165788	12630
21-11-14 8:00	179311	16963
21-11-14 8:30	125564	44759
21-11-14 9:00	112461	95299
21-11-14 9:30	240341	112461
21-11-14 10:00	288014	116298
21-11-14 10:30	203261	123300
21-11-14 11:00	67788	122945

Este resultado muestra las conexiones por segundo, según WEM:

Time	#3:2G-total-attach-req-all	Request/Second
21-11-14 8:00	738279	205.078
21-11-14 9:00	14053511	3903.753
21-11-14 10:00	24395071	6776.409
21-11-14 11:00	24663454	6850.959
21-11-14 12:00	17360687	4822.413

IMSIMGR en estado de advertencia

El IMSIMGR debe procesar cada nueva solicitud de conexión de identidad de suscriptor móvil temporal de paquetes/IMSI de llamada (P-TMSI) y de actualización de área de enrutamiento (RAU).

Con una observación conservadora, el sistema recibe un valor máximo de 6850 solicitudes de adhesión de 2 G por segundo y alrededor de 5313 solicitudes de adhesión de 3 G por segundo. El valor máximo que puede establecer para la protección contra sobrecarga de red es de 5000 solicitudes de conexión por segundo. Para mantener el IMSIMGR en un estado operable, el sistema no puede manejar un número tan grande de llamadas desde los UE.

Este problema comienza después de las 8 AM, cuando el tamaño de la cola alcanza las 1500 solicitudes de adhesión por segundo:

<#root>

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

Dado que hay aproximadamente 12.000 solicitudes de adhesión por segundo, el IMSIMGR procesa y rechaza casi 9.000 llamadas. Esto hace que el procesamiento de la CPU IMSIMGR alcance un estado alto.

Si el SGSN recibe más del número configurado de solicitudes de adición en un segundo, las solicitudes se almacenan en la cola de espaciado y solo se descartan cuando el búfer se desborda debido a una alta velocidad de adición entrante. Los mensajes en la cola se procesan de acuerdo con un proceso FIFO (First-In, First-Out) hasta que caducan cuando la duración del mensaje en cola cruza el tiempo de espera configurado.

Cuando elige las opciones de rechazo o descarte según sus preferencias, Cisco recomienda que utilice un código de causa de rechazo para indicar la congestión en la red, lo que le permite comprender las condiciones de la red antes de intentar un procedimiento de enlace ascendente.

Falla HLR

Según la especificación técnica (TS) 23.060 del proyecto de asociación de 3ª generación (3GPP), esta sección describe el comportamiento de SGSN durante un reinicio de HLR. Siempre que el SGSN recibe un reinicio de MAP, se espera que envíe una solicitud de UL hacia el HLR para sus suscriptores.

Cuando se reinicia un ELO, envía un mensaje de reinicio a cada SGSN en el que se registran una o más de sus estaciones móviles (MS). Esto hace que el SGSN marque los contextos de gestión móvil relevantes como no válidos si existe una asociación entre SGSN y Mobile Switching Center (MSC)/Registro de ubicación de visita (VLR). Después de recibir la primera trama válida de Control de link lógico (LLC) (para el modo A/Gb) o después de recibir el primer paquete válido de usuario de protocolo de túnel GPRS (GPT-U) o mensaje de señalización de enlace ascendente (para el modo Iu) desde una estación móvil marcada, el SGSN realiza una URL al HLR como en los procedimientos de actualización de solicitud de conexión o de área de ruteo (RA) entre SGSN. Además, si se establece el indicador de alerta no GPRS (NGAF), se sigue el procedimiento de la cláusula Non-GPRS Alert. El procedimiento UL y el procedimiento hacia MSC/VLR podrían ser demorados por el SGSN para una configuración máxima del operador, dependiendo del uso de recursos en ese momento para evitar una carga de señalización alta.

> Nota: La copia de seguridad periódica de los datos ELO en el almacenamiento no volátil es obligatoria, como se describe en TS 23.007 [5].

Recomendaciones

Cisco recomienda que complete estos pasos para resolver este problema:

1. Aumente el número de nuevas conexiones por segundo. Esto se puede calcular en función del número medio de solicitudes de adhesión.

2. Aumente las transacciones por segundo (TPS) en el enlace STP a un valor ideal.

3. Cambie el valor SCTP-RTO-MAX predeterminado de 600 (600*100 = 60.000) a 5 (5*100 ms). Por ejemplo, para dos STP con 4.000 TPS, puede admitir hasta 1.000 solicitudes de adhesión por segundo desde el SGSN.

Nota: Cada solicitud de adición da lugar a cuatro transacciones hacia el STP, lo que significa que 1.000 solicitudes de adición por segundo dan lugar a 4.000 TPS.

Idealmente, cada STP tiene cuatro links de modo que se puedan procesar 125 solicitudes de adjuntar por link STP. Esto se distribuye equitativamente a través de todos los links STP. Sin embargo, si uno de los links deja de funcionar, se ven muchos intentos de reconexión, la cola se llena y se producen descartes de paquetes. Si se desactivan más enlaces, el tráfico se distribuye de forma desigual.

Flujo de tráfico

El tráfico de la UE no sigue una moda lineal. Suele ocurrir en una ráfaga y con muchos intentos de reconexión. El SGSN envía el tráfico en paquetes al STP. En ese momento, las cantidades de tráfico exceden el TPS configurado en el STP. Esto hace que algunos links en el STP comiencen a anunciar el tamaño bajo de la ventana si ya procesan más llamadas, y el SGSN comienza a poner en cola los fragmentos de datos SCTP que están en cola. A continuación, espera a que caduque el temporizador RTO MAX.

Si el STP envía periódicamente un buen tamaño de ventana anunciado, entonces debería poder enviar más fragmentos de datos SCTP si el valor SCTP_RTO_MAX se reduce a cinco segundos o menos. La cola se borra más rápido y no se activa una alarma de congestión M3UA. Además, no debería ver el indicador de control de flujo interno activado por SCTP para controlar el flujo de paquetes.

El SGSN sólo envía paquetes en la cantidad que el STP puede aceptar, que se basa en el tamaño de ventana anunciado. Si aumenta el TPS por link STP, ayuda a evitar la congestión STP y reduce el temporizador SCTP_RTO_MAX.

Disparadores de la alarma congestionada M3UA en SGSN

Si el tamaño de ventana anunciado en el mensaje de confirmación selectiva (SACK) del protocolo de transmisión de control de flujo (SCTP) está cerca de cero (o cero), el SGSN genera una

alarma M3UA para indicar que no se deben enviar mensajes para ese punto final del par. Esto hace que el link se inestable o se mueva a un estado congestionado. Dado que el SGSN envía un tamaño de ventana más alto, usted continúa recibiendo datos M3UA de los nodos de peer, y esos paquetes podrían ser descartados en la cola de espera si el código de punto de peer nunca sale del estado congestionado.

Aquí tiene un ejemplo:

1. El SCTP envía una indicación de inicio de control de flujo al M3UA.

2. El M3UA establece el indicador activo de congestión para la asociación y comienza a sondear el SCTP periódicamente acerca de su estado de control de flujo.

3. Mientras una asociación está en control de flujo, pone en cola futuras solicitudes de datos para esa asociación hasta que QUEUE_SIZE alcance 8.000. En ese momento, se descartan los mensajes futuros para la asociación.

4. Si el STP envía un tamaño de ventana anunciado adecuado, el M3UA intenta vaciar los mensajes que están en cola hasta que alcanza 5,000. El temporizador RTO también juega un papel en esto.

Los mensajes SCTP se ponen en cola solamente para aquellas asociaciones donde el indicador de control de flujo se convierte en True, y el SGSN luego se procesa de acuerdo con la respuesta STP:

<#root>

```
*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 fragmentos salientes excede el límite de 5.000 (8050+143=8193) y alcanza el temporizador máximo de RTO de 60 segundos, lo que resulta en solicitudes de datos SCTP descartadas. Además, hay un temporizador RTO más alto.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).