

Congestionamento de STP, IMSIMGR sobre estado e Flaps de enlace de SCTP em SGSN devido a HLR MAP_RESET

Contents

[Introdução](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[O enlace STP recebe muito tráfego](#)

[IMSIMGR em Estado de Aviso](#)

[Falha de HLR](#)

[Recomendações](#)

[Fluxo de tráfego](#)

[Disparadores para Alarme Congestionado M3UA em SGSN](#)

Introdução

Este documento descreve um problema que é encontrado no nó de suporte (SGSN) do Service General Packet Radio Service (GPRS) do Cisco 5000 Series Aggregated Services Router (ASR). Algumas soluções possíveis para esse problema também são descritas.

Informações de Apoio

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

1. 21 de novembro, 6:25 AM: um MAP_RESET foi enviado pelo Home Location Register (HLR).
2. 21 de novembro, 8:13 AM: Um alarme de congestionamento é acionado para o Ponto de Transferência de Sinal 2 (STP-2).
3. 21 de novembro, 8:23 AM: Um alarme de congestionamento é acionado para STP-1 e STP-2.
4. 21 de novembro, 8:48 AM: O International Mobile Subscriber Identity Manager (IMSIMGR) entra no estado de aviso.
5. 21 de novembro, 10:07 AM: Os links são redefinidos do STP-2 para o SGSN.

6. 21 de novembro, 10:15 AM: Melhorias são observadas nas estatísticas da SGSN Location Update (LU).
7. 21 de novembro, 10:00 â 10:30 AM: As estatísticas começam a melhorar às 10:00 am.
8. 21 de novembro, 11:15 AM : Um declínio é observado nas estatísticas SGSN LU.
9. 21 de novembro, 11:41 AM: A equipe de STP relata que o Signaling Link Code (SLC)-1 de STP-2 não recebe tráfego, o SLC é redefinido e o tráfego retorna ao normal.
10. 21 de novembro, 11:42 AM: Um alarme de congestionamento é acionado em SGSN para SLC-1 do STP.
11. 21 de novembro, 12:00 PM: Depois que o SLC-3 é redefinido, as estatísticas da LU GPRS melhoram.

Problema

Quando o HLR recebe a mensagem MAP_RESET, ele define um flag para uma GLU (GPRS Location Update - Atualização de Local GPRS). Quando o equipamento de usuário (UE) envia seus primeiros pacotes de 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
```

Como mostrado na saída do exemplo, há 950.000 contextos de Packer Data Protocol (PDP) presentes no SGSN, e os UEs tentam navegar por eles à medida que o dia avança.

Quando os primeiros pacotes de uplink são recebidos, o SGSN dispara uma mensagem GLU. Como há centenas de milhares de UEs, o STP não pode lidar com a quantidade de tráfego que é gerada e entra em um estado de congestionamento perene.

As mensagens são enfileiradas no SGSN e um tempo limite máximo de retransmissão ocorre. Como todas as mensagens GLU não passam do SGSN para o HLR, o SGSN é forçado a desconectar os assinantes móveis e solicitar que eles se reconectem. Todos os assinantes desconectados tentam anexar-se, o que causa um aumento repentino no número de solicitações de anexo de entrada. Como a proteção contra sobrecarga de rede é aplicada, a maioria das tentativas de conexão é rejeitada devido ao congestionamento e os assinantes móveis são forçados a fazer uma nova tentativa.

À medida que esta cadeia de eventos se desenrola, produz efeitos em cascata. Muitas

mensagens Send Authentication Information (SAI), mensagens GLU e mensagens MAP-IMEI_CHECK ficam presas na fila SGSN ou são descartadas. Por esse motivo, todos os links STP-1 e STP-2 atingem um estado de congestionamento. Cada STP tem quatro links de sinalização, mas nesse cenário, os três primeiros links do STP-2 não se recuperam por muito tempo.

Aqui estão os alarmes de congestionamento, nos quais você pode ver que todos os links STP se movem para o estado de congestionamento no 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, apenas o PSP (Peer Server Process) 4 foi limpo e o restante ainda está no estado de congestionamento:

<#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
```

Solução

Esta seção descreve como solucionar o problema descrito na seção anterior.

O enlace STP recebe muito tráfego

Conforme descrito na seção anterior, um link específico no STP recebe uma grande quantidade de tráfego. Você pode ver que os três primeiros links no STP-2 entram no estado de congestionamento e nunca são recuperados, portanto, apenas um link está disponível e o alarme de congestionamento é cancelado no SLC-3 (ou peer-server-2-peer-server-process-4).

De acordo com o mecanismo de compartilhamento de carga SGSN, ele deve enviar os pacotes MTP Nível 3 (MTP3) User Adaptation Layer (M3UA) igualmente em todos os quatro enlaces. No entanto, a partir das interceptações do Protocolo de Mensagem de Rede Simples (SNMP - Simple Network Message Protocol), os três primeiros enlaces do STP-2 estão congestionados permanentemente, o que significa que todo o tráfego é roteado para o enlace do SLC-3 (o único enlace do STP disponível para rotear o tráfego). Isso explica por que a distribuição de tráfego é distorcida entre os links STP-2.

Em situações de congestionamento, um ou mais links alternam entre estados congestionados e não congestionados, de modo que apenas os links disponíveis compartilham o tráfego. Por esse motivo, há mais utilização em um dos links. Isso exige uma redefinição de link para recuperar os links.

A próxima saída mostra as estatísticas do nível M3UA e as estatísticas de desanexação. As estatísticas importantes a serem consideradas são a instância 4 do STP-2 PSP, onde o tráfego anormal pode ser visto:

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

Aqui estão os dados do 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

Esta saída mostra as desconexões por segundo no momento do 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

Esta saída mostra as conexões por segundo, de acordo com o 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 em Estado de Aviso

Cada nova solicitação de IMSI/Packet Temporary Mobile Subscriber Identity (P-TMSI) e Routing Area Update (RAU) de chamada deve ser processada pelo IMSIMGR.

Com uma observação conservadora, o sistema recebe um valor de pico de 6.850 solicitações de conexão 2-G por segundo e cerca de 5.313 solicitações de conexão 3-G por segundo. O valor máximo que você pode definir para a proteção contra sobrecarga de rede é de 5.000 solicitações anexadas por segundo. Para manter o IMSIMGR em um estado operável, o sistema não pode lidar com um número tão grande de chamadas dos UEs.

Esse problema começa após as 8 da manhã, quando o tamanho da fila atinge 1.500 solicitações de anexo por segundo:

<#root>

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

Como há aproximadamente 12.000 solicitações de conexão por segundo, quase 9.000 chamadas são processadas pelo IMSIMGR e rejeitadas. Isso faz com que o processamento da CPU do IMSIMGR atinja um estado alto.

Se o SGSN receber mais do que o número configurado de solicitações de anexação em um segundo, as solicitações serão armazenadas em buffer na fila de ritmo e só serão descartadas quando o buffer estourar devido a uma alta taxa de anexação de entrada. As mensagens na fila são processadas de acordo com um processo First-In, First-Out (FIFO) até expirarem quando o tempo de vida da mensagem na fila ultrapassar o tempo de espera configurado.

Quando você escolhe as opções de rejeição ou eliminação com base em sua preferência, a Cisco recomenda que você use um código de causa de rejeição para indicar o congestionamento na rede, o que permite que você compreenda as condições da rede antes de tentar um procedimento de uplink.

Falha de HLR

De acordo com a Especificação Técnica (TS) 23.060 do 3rd Generation Partnership Project (3GPP), esta seção descreve o comportamento da SGSN durante uma reinicialização do HLR. Sempre que o SGSN recebe uma reinicialização de MAP, espera-se enviar uma solicitação de UL para o HLR para seus assinantes.

Quando um HLR é reiniciado, ele envia uma mensagem de redefinição para cada SGSN ao qual uma ou mais de suas estações móveis (MSs) estão registradas. Isso faz com que o SGSN marque os contextos relevantes de Gerenciamento Móvel como inválidos se existir uma associação SGSN-para-Centro de Switching Móvel (MSC)/Registro de Localização Visitante (VLR). Após o recebimento do primeiro quadro válido de Controle Lógico de Enlace (LLC - Logical Link Control) (para o modo A/Gb) ou após o recebimento do primeiro pacote GPRS Tunneling Protocol User (GTP-U - GPRS Tunneling Protocol User) válido ou mensagem de sinalização de uplink (para o modo lu) de uma estação móvel marcada, o SGSN executa um UL para o HLR, como nos procedimentos de solicitação de conexão ou de atualização da área de roteamento (RA - Routing Area) inter-SGSN. Além disso, se o Non-GPRS Alert Flag (NGAF) for definido, o procedimento na cláusula Non-GPRS Alert será seguido. O procedimento UL e o procedimento para a MSC/VLR podem ser atrasados pela SGSN para uma configuração máxima do operador, dependendo da utilização de recursos nessa altura, a fim de evitar uma carga de sinalização elevada.

Nota: O backup periódico dos dados do HLR para armazenamento não volátil é obrigatório, conforme descrito na TS 23.007 [5].

Recomendações

A Cisco recomenda que você conclua estas etapas para resolver este problema:

1. Aumente o número de novas conexões por segundo. Isso pode ser calculado com base no número médio de solicitações de anexo.
2. Aumente as Transações por Segundo (TPS) no link STP para um valor ideal.
3. Altere o valor padrão SCTP-RTO-MAX de 600 ($600 \times 100 = 60.000$) para 5 (5×100 ms). Por exemplo, para dois STPs com 4.000 TPS, você pode suportar até 1.000 solicitações de anexo por segundo do SGSN.

Observação: cada solicitação de anexação resulta em quatro transações para o STP, o que significa que 1.000 solicitações de anexação por segundo resultam em 4.000 TPS.

Idealmente, cada STP tem quatro links para que 125 solicitações de anexo possam ser processadas por link STP. Isso é distribuído igualmente por todos os links STP. No entanto, se um dos links ficar inativo, muitas tentativas de reconexão serão vistas, a fila ficará cheia e ocorrerão descartes de pacotes. Se mais links ficarem inativos, o tráfego será distribuído de forma desigual.

Fluxo de tráfego

O tráfego UE não segue uma forma linear. Geralmente ocorre em uma rajada e com muitas tentativas de reconexão. O SGSN envia tráfego em pacotes para o STP. Nesse momento, as quantidades de tráfego excedem o TPS configurado no STP. Isso faz com que alguns links no STP comecem a anunciar tamanho de janela baixo se já processarem mais chamadas, e o SGSN começa a enfileirar os blocos de dados SCTP que estão enfileirados. Em seguida, ele espera até que o temporizador RTO MAX expire.

Se o STP enviar periodicamente um tamanho de janela bem anunciado, você poderá enviar mais blocos de dados SCTP se o valor de SCTP_RTO_MAX for reduzido para cinco segundos ou menos. A fila é limpa mais rapidamente e um alarme de congestionamento M3UA não é disparado. Além disso, você não deve ver o indicador de controle de fluxo interno disparado pelo SCTP para controlar o fluxo do pacote.

O SGSN envia somente pacotes na quantidade que o STP pode aceitar, que é baseada no tamanho da janela anunciada. Se você aumentar o TPS por link STP, isso ajudará a evitar o congestionamento de STP e reduzirá o temporizador SCTP_RTO_MAX.

Disparadores para Alarme Congestionado M3UA em SGSN

Se o tamanho da janela anunciada na mensagem de Confirmação Seletiva (SACK) do Protocolo de Transmissão de Controle de Fluxo (SCTP - Stream Control Transmission Protocol) estiver próximo de zero (ou zero), o SGSN acionará um alarme M3UA para indicar que as mensagens não devem ser enviadas para esse ponto final do peer. Isso faz com que o link oscile ou entre em um estado congestionado. Como o SGSN envia um tamanho de janela maior, você continua a receber dados M3UA dos nós de peer, e esses pacotes podem ser descartados na fila de espera se o código de ponto de peer nunca sair do estado congestionado.

Aqui está um exemplo:

1. O SCTP envia uma indicação de início de controle de fluxo para o M3UA.
2. O M3UA define o sinalizador de congestionamento ativo para a associação e começa a sondar o SCTP periodicamente sobre seu status de controle de fluxo.
3. Enquanto uma associação estiver no controle de fluxo, ela enfileirá futuras solicitações de dados para essa associação até que QUEUE_SIZE atinja 8.000. Nesse ponto, as mensagens futuras da associação serão descartadas.
4. Se o STP enviar um tamanho de janela anunciado adequado, o M3UA tentará esvaziar as mensagens que estão na fila até atingir 5.000. O temporizador de RTO também desempenha um papel nisso.

As mensagens SCTP são enfileiradas somente para as associações onde o indicador de controle de fluxo se torna Verdadeiro, e o SGSN então processa de acordo com a resposta 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 mostrado, o motivo por trás do congestionamento é que o número total de blocos de saída excede o limite de 5.000 ($8050+143=8193$) e atinge o temporizador máximo de RTO de 60 segundos, o que resulta em solicitações de dados SCTP descartadas. Além disso, há um temporizador de RTO mais alto.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.