Congestione STP, sovraccarico di stato di IMSIMGR e flap del collegamento SCTP in SGSN a causa di MAP_RESET dell'RLN

Sommario

Introduzione

Questo documento descrive un problema riscontrato nel GPRS (General Packet Radio Service) che supporta il nodo (SGSN) di Cisco serie 5000 Aggregated Services Router (ASR). Vengono inoltre descritte alcune possibili soluzioni per questo problema.

Premesse

Questa catena di eventi specifica sull'SGSN ASR è descritta nel presente documento:

1. 21 nov, 6:25 AM: Un MAP_RESET è stato inviato dall'RLN (Home Location Register).
2. 21 nov, 8:13 AM: Segnale di trasferimento 2 (STP-2) in congestione.
3. 21 nov, 8:23 AM: Viene emesso un allarme congestione per STP-1 e STP-2.
4. 21 novembre, 8:48 AM: International Mobile Subscriber Identity Manager (IMSIMGR) passa nello stato di avviso.
5. 21 nov, 10:07 AM: I collegamenti vengono ripristinati da STP-2 verso SGSN.
6. 21 nov, 10:15 AM: si osserva un miglioramento negli stati di SGSN Location Update (LU).
7. 21 novembre, 10:00 â 10:30 AM: Le statistiche iniziano a migliorare alle 10:00 AM.

8. 21 nov, 11:15 AM : Si osserva un declino nelle statistiche LU SGSN.

9. 21 nov, 11:41 AM: Il team STP segnala che Signaling Link Code (SLC)-1 di STP-2 non riceve traffico, che SLC viene reimpostato e che il traffico torna alla normalità.

10. 21 nov, 11:42 AM: SGSN emette un allarme di congestione per la SLC-1 del STP.

11. 21 nov, 12:00: Dopo il reset di SLC-3, lo stato di GPRS LU migliora.

Problema

Quando l'RLN riceve il messaggio MAP_RESET, imposta un flag per un aggiornamento della posizione GPRS (GLU). Quando l'apparecchiatura utente (UE) invia i primi pacchetti uplink, il SGSN invia un messaggio GLU all'RLN.

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

Come mostrato nell'output dell'esempio, il protocollo SGSN contiene 950.000 contesti PDP (Packer Data Protocol). L'utente tenterà di spostarsi da un contesto all'altro durante il giorno.

Quando si ricevono i primi pacchetti uplink, il SGSN attiva un messaggio GLU. Essendo centinaia di migliaia gli utenti, l'STP non può gestire la quantità di traffico che viene generata e si porta in uno stato di congestione permanente.

I messaggi vengono accodati al SGSN e si verifica un timeout massimo di ritrasmissione. Poiché tutti i messaggi GLU non passano dalla SGSN alla RLN, la SGSN è costretta a scollegare gli abbonati della telefonia mobile e a richiederne il ricollegamento. Tutti gli abbonati scollegati tentano quindi di connettersi, causando un aumento improvviso del numero di richieste di allegati in ingresso. Poiché viene applicata la protezione da sovraccarico di rete, la maggior parte dei tentativi di connessione viene rifiutata a causa di congestione e gli abbonati mobili sono costretti a effettuare un nuovo tentativo.

Man mano che la catena di eventi si sviluppa, produce effetti a catena. Molti messaggi SAI (Send Authentication Information), GLU e MAP-IMEI_CHECK sono bloccati nella coda SGSN o eliminati. Per questo motivo, tutti i collegamenti STP-1 e STP-2 raggiungono uno stato di congestione. Ogni STP ha quattro collegamenti di segnalazione, ma in questo scenario, i primi tre collegamenti di STP-2 non si ripristinano per molto tempo.

Di seguito sono riportati gli allarmi di congestione, in cui è possibile vedere che tutti i collegamenti

STP passano nello stato di congestione su 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
```

Come mostrato, solo il processo Peer Server (PSP) 4 è stato cancellato e gli altri sono ancora in stato di congestione:

<#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
```

Soluzione

Questa sezione descrive come risolvere il problema descritto nella sezione precedente.

Il collegamento STP riceve un volume di traffico eccessivo

Come descritto nella sezione precedente, un particolare collegamento nell'STP riceve una grande quantità di traffico. Come si può notare, i primi tre collegamenti dell'STP-2 entrano nello stato di congestione e non vengono mai ripristinati, quindi solo un collegamento è disponibile e l'allarme di congestione viene cancellato sull'SLC-3 (o peer-server-2-peer-server-process-4).

Come per il meccanismo di condivisione del carico SGSN, deve inviare i pacchetti MTP (Message Transfer Part) Level 3 (MTP3) User Adaptation Layer (M3UA) in modo uniforme su tutti e quattro i collegamenti. Tuttavia, dalle trap SNMP (Simple Network Message Protocol), i primi tre collegamenti STP-2 sono perennemente congestionati, il che significa che tutto il traffico viene instradato al collegamento SLC-3 (l'unico collegamento STP disponibile per instradare il traffico). Questo spiega perché la distribuzione del traffico è distorta tra i collegamenti STP-2.

In situazioni di congestione, uno o più collegamenti passano da uno stato congestionato a uno non congestionato e viceversa, quindi solo i collegamenti disponibili condividono il traffico. Per questo motivo, in uno dei link è presente un utilizzo maggiore. Per ripristinare i collegamenti, è necessario reimpostare il collegamento.

L'output successivo mostra le statistiche del livello M3UA e le statistiche di scollegamento. Le statistiche importanti da considerare sono l'istanza 4 di PSP STP-2, in cui è possibile rilevare traffico anomalo:

```
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
```

Di seguito sono riportati i dati 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
```

Questo output mostra i distacchi al secondo al 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
```

Questo output mostra gli attacchi al secondo, come per 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 in stato di avviso

Ogni nuova richiesta di chiamata IMSI/Packet Temporary Mobile Subscriber Identity (P-TMSI) attach and Routing Area Update (RAU) deve essere elaborata da IMSIMGR.

Con un'osservazione conservativa, il sistema riceve un valore massimo di 6.850 richieste di collegamento 2-G al secondo e circa 5.313 richieste di collegamento 3-G al secondo. Il valore massimo che è possibile impostare per la protezione da sovraccarico di rete è 5.000 richieste di collegamento al secondo. Per mantenere IMSIMGR in uno stato operativo, il sistema non è in grado di gestire un numero così elevato di chiamate provenienti dagli UE.

Questo problema inizia dopo le 8 del mattino, quando la dimensione della coda raggiunge 1.500 richieste di collegamento al secondo:

```
<#root>

network-overload-protection sgsn-new-connections-per-second 500 action
```

```
reject-with-cause congestion queue-size 1500 wait-time 5
```

Poiché vi sono circa 12.000 richieste di collegamento al secondo, quasi 9.000 chiamate vengono elaborate da IMSIMGR e rifiutate. In questo modo, l'elaborazione della CPU IMSIMGR raggiunge uno stato elevato.

Se il numero di richieste di collegamento ricevute in un secondo dal servizio SGSN è superiore al numero configurato, le richieste vengono memorizzate nel buffer nella coda di attesa e vengono eliminate solo quando il buffer esegue un overflow a causa di una frequenza di collegamento in ingresso elevata. I messaggi nella coda vengono elaborati in base a un processo FIFO (First-In, First-Out) fino al timeout quando la durata dei messaggi in coda supera il tempo di attesa configurato.

Quando si scelgono le opzioni di rifiuto o eliminazione in base alle proprie preferenze, Cisco consiglia di utilizzare un codice della causa di rifiuto per indicare la congestione nella rete, in modo da poter comprendere le condizioni di rete prima di tentare una procedura uplink.

Errore RLN

In questa sezione del progetto 3GPP (3rd Generation Partnership Project) Technical Specification (TS) 23.060 viene descritto il comportamento di SGSN durante un riavvio dell'RLN. Ogni volta che il SGSN riceve una reimpostazione della mappa, è previsto che invii una richiesta UL all'RLN per i suoi sottoscrittori.

Quando un RLN viene riavviato, invia un messaggio di ripristino a ogni SGSN al quale sono registrate una o più delle sue stazioni mobili (MS). In questo modo, il SGSN contrassegnerà i contesti di gestione mobili rilevanti come non validi se esiste un'associazione SGSN-to-Mobile Switching Center (MSC)/VLR (Visiting Location Register). Dopo aver ricevuto il primo frame LLC (Logical Link Control) valido (per la modalità A/Gb) o dopo aver ricevuto il primo pacchetto o messaggio di segnalazione uplink (per la modalità Iu) valido dell'utente GPRS Tunneling Protocol (GPT-U) da una stazione mobile contrassegnata, SGSN esegue un URL per l'RLN come nelle procedure di aggiornamento della richiesta di collegamento o dell'area di routing tra SGSN. Inoltre, se è impostato il flag di avviso non GPRS (NGAF), viene seguita la procedura descritta nella clausola di avviso non GPRS. La procedura UL e la procedura verso l'MSC/VLR possono essere ritardate dall'SGSN per una configurazione massima dell'operatore, a seconda dell'uso delle risorse in quel momento, al fine di evitare un elevato carico di segnalazione.

> Nota: il backup periodico dei dati RLN su una memoria non volatile è obbligatorio, come descritto in TS 23.007 [5].

Consigli

Cisco consiglia di completare i seguenti passaggi per risolvere il problema:

1. Aumentare il numero di nuove connessioni al secondo. Questo valore può essere calcolato

in base al numero medio di richieste di collegamento.

2. Aumentare il valore di Transazioni al secondo (TPS) nel collegamento STP a un valore ideale.

3. Modificare il valore predefinito SCTP-RTO-MAX di 600 (600*100 = 60.000) in 5 (5*100 ms). Ad esempio, per due STP con 4.000 TPS, è possibile supportare fino a 1.000 richieste di collegamento al secondo da SGSN.

Nota: ogni richiesta di collegamento genera quattro transazioni verso STP, ovvero 1.000 richieste di collegamento al secondo generano 4.000 TPS.

Idealmente, ogni STP ha quattro collegamenti in modo che possano essere elaborate 125 richieste di collegamento per ogni collegamento STP. Questa condizione viene distribuita equamente tra tutti i collegamenti STP. Tuttavia, se uno dei collegamenti non funziona, si verificano molti tentativi di riconnessione, la coda si riempie e i pacchetti vengono scartati. Se un numero maggiore di collegamenti non è disponibile, il traffico è distribuito in modo non uniforme.

Flusso traffico

Il traffico dell'UE non segue una linea lineare. Si verifica in genere in un burst e con molti tentativi di riconnessione. L'SGSN invia il traffico in bundle all'STP. In quel momento, le quantità di traffico superano i TPS configurati sull'STP. In questo modo, se alcuni collegamenti nell'STP già elaborano altre chiamate, iniziano a annunciare una finestra di dimensioni ridotte e l'SGSN inizia a mettere in coda i blocchi di dati SCTP in coda. Quindi attende la scadenza del timer RTO MAX.

Se l'STP invia periodicamente una finestra di dimensioni adeguate, dovrebbe essere possibile inviare più blocchi di dati SCTP se il valore di SCTP_RTO_MAX viene ridotto a cinque secondi o meno. La coda viene cancellata più rapidamente e non viene attivato alcun allarme di congestione M3UA. Inoltre, non deve essere visualizzato il flag di controllo del flusso interno attivato dall'SCTP per controllare il flusso del pacchetto.

Il SGSN invia i pacchetti solo nella quantità che il STP può accettare, basata sulle dimensioni della finestra annunciate. Aumentando il TPS per collegamento STP, si evita la congestione del STP e si riduce il timer SCTP_RTO_MAX.

Trigger per M3UA Congested Alarm in SGSN

Se le dimensioni della finestra annunciate nel messaggio SACK (Selective Acknowledgement) del protocollo SCTP (Stream Control Transmission Protocol) sono vicine allo zero (o allo zero), il SGSN genera un allarme M3UA per indicare che i messaggi non devono essere inviati per l'endpoint peer. In questo modo, il collegamento viene interrotto o spostato in uno stato di congestione. Poiché il SGSN invia una finestra di dimensioni maggiori, si continuano a ricevere dati M3UA dai nodi peer e tali pacchetti potrebbero essere scartati nella coda di attesa se il codice del punto peer non esce mai dallo stato di congestione.

Di seguito è riportato un esempio:

1. L'SCTP invia un'indicazione di avvio del controllo del flusso all'M3UA.

2. M3UA imposta il flag di congestione attiva per l'associazione e inizia a eseguire periodicamente il polling dell'SCTP sullo stato del controllo di flusso.

3. Quando un'associazione è nel controllo del flusso, accoda le richieste di dati future per l'associazione fino a quando QUEUE_SIZE non raggiunge 8.000. A questo punto, i messaggi futuri per l'associazione verranno ignorati.

4. Se l'STP invia una finestra annunciata di dimensioni adeguate, M3UA tenta di svuotare i messaggi in coda fino a raggiungere le 5.000. Anche il timer RTO svolge un ruolo in questo.

I messaggi SCTP vengono accodati solo per le associazioni in cui il flag di controllo del flusso diventa True e l'SGSN elabora quindi in base alla risposta 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
```

Come mostrato, la causa della congestione è che il numero totale di blocchi in uscita supera il limite di 5.000 (8050+143=8193) e raggiunge il timer massimo di RTO di 60 secondi, che determina richieste di dati SCTP scartate. Inoltre, il timer RTO è più elevato.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).