STP-Überlastung, IMSIMGR Over State und SCTP Link Flaps in SGSN aufgrund von HLR MAP_RESET

Inhalt

Einführung

Dieses Dokument beschreibt ein Problem, das beim Serving General Packet Radio Service (GPRS) Support Node (SGSN) des Cisco Aggregated Services Router (ASR) der Serie 5000 auftritt. Einige mögliche Problemumgehungen werden ebenfalls beschrieben.

Hintergrundinformationen

Diese Ereigniskette für den ASR SGSN wird in diesem Dokument beschrieben:

1. **21. November, 06:25 Uhr**: Eine MAP_RESET wurde vom Home Location Register (HLR) gesendet.

2. **21. November, 08:13 Uhr**: Für Signal Transfer Point 2 (STP-2) wird ein Überlastungsalarm ausgelöst.

3. **21. November, 08:23 Uhr**: Für STP-1 und STP-2 wird ein Überlastungsalarm ausgelöst.

4. **21. November, 08:48 Uhr**: Der International Mobile Subscriber Identity Manager (IMSIMGR) wechselt in den *Warn*-Status.

5. **21. November, 10:07 Uhr**: Die Verbindungen werden von STP-2 zum SGSN zurückgesetzt.

6. **21. November, 10:15 Uhr**: Eine Verbesserung wird in den Statistiken von SGSN Location Update (LU) beobachtet.

7. **21. November, 10:00 10:30 Uhr**: Die Statistiken beginnen um 10.00 Uhr zu verbessern.

8. **21.11.15 Uhr**: Ein Rückgang ist in den SGSN LU-Statistiken zu beobachten.

9. **21. November, 11:41 Uhr**: Das STP-Team berichtet, dass Signaling Link Code (SLC)-1 von STP-2 keinen Datenverkehr empfängt, das SLC zurückgesetzt wird und der Datenverkehr wieder auf den Normalzustand zurückgesetzt wird.

10. **21. November, 11:42 Uhr**: Für SLC-1 des STP wird auf dem SGSN ein Überlastungsalarm ausgelöst.

11. **21.11.2012:00 Uhr**: Nach dem Zurücksetzen von SLC-3 verbessern die GPRS LU-Statistiken.

Problem

Wenn der HLR die MAP_RESET-Nachricht empfängt, legt er ein Flag für ein GPRS Location Update (GLU) fest. Wenn die Benutzergeräte (UE) ihre ersten Uplink-Pakete senden, sendet das SGSN eine GLU-Nachricht an das HLR.

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

Wie in der Beispielausgabe gezeigt, befinden sich im SGSN 950.000 PDP-Kontexte (Packer Data Protocol), und die UEs versuchen, diese im Laufe des Tages durchzusehen.

Wenn die ersten Uplink-Pakete empfangen werden, löst das SGSN eine GLU-Nachricht aus. Da es Hunderttausende von UEs gibt, kann das STP die Menge des generierten Datenverkehrs nicht verarbeiten und gelangt in einen permanenten Überlastungszustand.

Meldungen werden im SGSN in die Warteschlange gestellt, und es tritt *eine maximale Zeitüberschreitung bei der erneuten Übertragung* auf. Da nicht alle GLU-Nachrichten vom SGSN an das HLR weitergeleitet werden, ist das SGSN gezwungen, die mobilen Teilnehmer zu trennen und die erneute Verbindung anzufordern. Alle abgerufenen Teilnehmer versuchen dann, eine Verbindung herzustellen, was zu einem plötzlichen Anstieg der Anzahl eingehender Anhangsanträge führt. Da der Schutz vor Netzwerküberlastungen angewendet wird, werden die meisten Verbindungsversuche aufgrund von Überlastungen abgelehnt, und die mobilen Teilnehmer sind gezwungen, einen neuen Versuch zu unternehmen.

Während sich diese Ereigniskette entfaltet, erzeugt sie kaskadierende Auswirkungen. Viele SAI-Nachrichten (Send Authentication Information), GLU-Nachrichten und MAP-IMEI_CHECK-Nachrichten sind in der SGSN-Warteschlange stecken oder fallen gelassen. Aus diesem Grund erreichen alle STP-1- und STP-2-Verbindungen einen Überlastungszustand. Jedes STP verfügt

über vier Signalisierungsverbindungen. In diesem Szenario werden die ersten drei Verbindungen von STP-2 jedoch nicht sehr lange wiederhergestellt.

Im Folgenden sehen Sie die Überlastungswarnungen, bei denen alle STP-Verbindungen in den Überlastungszustand auf STP-2 verschoben werden:

```
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
```

Wie gezeigt wurde nur der Peer-Server-Prozess (PSP) **4** gelöscht, und die restlichen Vorgänge befinden sich noch im Überlastungszustand:

```
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
```

Lösung

In diesem Abschnitt wird beschrieben, wie Sie das im vorherigen Abschnitt beschriebene Problem beheben.

STP-Verbindung empfängt zu viel Datenverkehr

Wie im vorherigen Abschnitt beschrieben, empfängt eine bestimmte Verbindung im STP eine große Menge an Datenverkehr. Sie sehen, dass die ersten drei Verbindungen in STP-2 in den Überlastungszustand wechseln und sich nie wiederherstellen. Daher ist nur eine Verbindung verfügbar, und der Überlastungsalarm wird auf SLC-3 (oder Peer-Server-2-Peer-Server-process-4) gelöscht.

Gemäß dem SGSN-Lastverteilungsmechanismus müssen die M3UA-Pakete (Message Transfer Part, MTP) Level 3 (MTP3) User Adaptation Layer (M3UA) (Message Transfer Part) auf allen vier Verbindungen gleich gesendet werden. Von den SNMP-Traps (Simple Network Message Protocol) werden die ersten drei STP-2-Verbindungen jedoch permanent überlastet, d. h. der gesamte Datenverkehr wird an die SLC-3-Verbindung weitergeleitet (die einzige verfügbare STP-Verbindung, die für die Weiterleitung des Datenverkehrs verfügbar ist). Dies erklärt, warum die Datenverkehrsverteilung zwischen den STP-2-Verbindungen verzerrt ist.

In Überlastungssituationen können eine oder mehrere Verbindungen zwischen überlasteten und nicht überlasteten Zuständen hin- und herschalten, sodass nur die verfügbaren Verbindungen den Datenverkehr gemeinsam nutzen. Aus diesem Grund wird in einem der Links mehr genutzt. Dies erfordert ein Zurücksetzen der Verbindung, um die Links wiederherzustellen.

Die nächste Ausgabe zeigt die M3UA-Level-Statistiken und Trennstatistiken. Wichtige Statistiken sind die Instanz **4** des STP-2-PSP, bei der anormaler Datenverkehr sichtbar ist:

```
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
```

Die STP-Daten sind wie folgt:

```
   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
```

Diese Ausgabe zeigt die Entfernungen pro Sekunde zum Zeitpunkt des Problems an:

```
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
```

Diese Ausgabe zeigt die Anhänge pro Sekunde gemäß 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 im Warn-Zustand

Jeder neue Anruf IMSI/Packet Temporary Mobile Subscriber Identity (P-TMSI) Attach and Routing Area Update (RAU)-Anfrage muss vom IMSIMGR verarbeitet werden.

Bei konservativer Betrachtung erhält das System einen Spitzenwert von 6.850 2-G-Attach-Anfragen pro Sekunde und etwa 5.313 3-G-Attach-Anfragen pro Sekunde. Der maximale Wert, den Sie für den Schutz vor Netzwerküberlastungen festlegen können, beträgt 5.000 Attach-Anfragen pro Sekunde. Um den IMSIMGR in einem betriebsfähigen Zustand zu halten, kann das System eine so große Anzahl von Anrufen von den UEs nicht verarbeiten.

Dieses Problem beginnt nach 8 Uhr, wenn die Warteschlangengröße 1.500 Anforderungen pro Sekunde zum Anhängen erreicht:

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

Da pro Sekunde ca. 12.000 Attach-Anfragen vorliegen, werden fast 9.000 Anrufe vom IMSIMGR verarbeitet und abgelehnt. Dadurch erreicht die IMSIMGR-CPU-Verarbeitung einen hohen Status.

Wenn das SGSN in einer Sekunde mehr als die konfigurierte Anzahl von Anfügeanforderungen empfängt, werden die Anforderungen in der Warteschlange für das Pacing gepuffert und nur dann verworfen, wenn der Puffer aufgrund einer hohen Attach-Rate überlaufen wird. Nachrichten in der Warteschlange werden gemäß einem First-In, First-Out (FIFO)-Prozess verarbeitet, bis sie verfallen, wenn die Lebensdauer der in der Warteschlange angezeigten Nachrichten die konfigurierte Wartezeit überschreitet.

Wenn Sie die Ablehnungs- oder Drop-Optionen basierend auf Ihrer Präferenz auswählen, empfiehlt Cisco, einen Ursachencode für Ablehnungen zu verwenden, um eine Netzwerküberlastung anzuzeigen. Auf diese Weise können Sie die Netzwerkbedingungen verstehen, bevor Sie einen Uplink-Vorgang versuchen.

HLR-Fehler

Gemäß 3GPP (3rd Generation Partnership Project) Technical Specification (TS) 23.060 beschreibt dieser Abschnitt das SGSN-Verhalten während eines HLR-Neustarts. Wenn das SGSN eine MAP-Zurücksetzung erhält, wird erwartet, dass es eine UL-Anfrage an das HLR für seine Teilnehmer sendet.

Beim Neustart eines HLR wird jedem SGSN, an den eine oder mehrere seiner mobilen Stationen (MSs) registriert sind, eine Reset-Nachricht gesendet. Dadurch wird der SGSN dazu veranlasst,

die relevanten Mobile Management-Kontexte als ungültig zu kennzeichnen, wenn eine Zuordnung von SGSN zu Mobile Switching Center (MSC)/Visiting Location Register (VLR) besteht. Nach Erhalt des ersten gültigen LLC-Frames (für den A/Gb-Modus) oder nach Erhalt des ersten gültigen GPRS Tunneling Protocol User (GPT-U)-Pakets oder der Uplink-Signalisierungsmeldung (für den Iu-Modus) von einer markierten mobilen Station führt der SGSN eine UL für das HLR durch, wie in der Anforderung zur Ergänzung oder in der RR-Aktualisierung (Inter-SGSGSN Routing Area, RA). Wenn außerdem das Nicht-GPRS-Warnungs-Flag (NGAF) festgelegt ist, wird das Verfahren in der *Nicht-GPRS-Warnungs*-Klausel befolgt. Das UL-Verfahren und das Verfahren zum MSC/VLR können vom SGSN für eine maximale Operatorkonfiguration verzögert werden, abhängig von der Nutzung der Ressourcen zu diesem Zeitpunkt, um eine hohe Signalisierungslast zu vermeiden.

> **Hinweis**: Die regelmäßige Sicherung der HLR-Daten auf nichtflüchtigen Speichern ist obligatorisch, wie in TS 23.007 beschrieben [5].

Empfehlungen

Cisco empfiehlt, die folgenden Schritte auszuführen, um dieses Problem zu beheben:

1. Erhöhen Sie die Anzahl neuer Verbindungen pro Sekunde. Dies kann auf Basis der durchschnittlichen Anzahl von Attach Requests berechnet werden.

2. Erhöhen Sie die Anzahl der Transaktionen pro Sekunde (TPS) in der STP-Verbindung auf einen idealen Wert.

3. Ändern Sie den Standardwert **SCTP-RTO-MAX** von 600 (600*100 = 60.000) in 5 (5*100 ms). Beispielsweise können Sie bei zwei STPs mit 4.000 TPS vom SGSN bis zu 1.000 Attach Requests pro Sekunde unterstützen.

   Hinweis: Jede Anforderung zum Anhängen führt zu vier Transaktionen zum STP, was bedeutet, dass 1.000 Attach Requests pro Sekunde zu 4.000 TPS führen.

Im Idealfall verfügt jedes STP über vier Verbindungen, sodass 125 Attach-Anfragen pro STP-Verbindung verarbeitet werden können. Diese wird gleichmäßig auf alle STP-Links verteilt. Wenn jedoch eine der Verbindungen ausfällt, werden viele Verbindungsversuche angezeigt, die Warteschlange ist voll, und es werden Paketverwerfen durchgeführt. Wenn mehr Verbindungen ausfallen, wird der Datenverkehr ungleichmäßig verteilt.

Datenverkehrsfluss

Der EU-Datenverkehr verläuft nicht linear. In der Regel tritt sie bei einem Burst und bei vielen erneuten Verbindungsversuchen auf. Das SGSN sendet Datenverkehr in Paketen an das STP. Zu diesem Zeitpunkt überschreiten die Datenverkehrsmengen die konfigurierten TPS auf dem STP. Dies veranlasst einige Links im STP, eine niedrige Fenstergröße anzukündigen, wenn sie bereits mehr Anrufe bearbeiten, und das SGSN beginnt, die in die Warteschlange gestellten SCTP-Daten-Chunks in die Warteschlange zu stellen. Anschließend wartet er auf den Ablauf des RTO MAX-Timers.

Wenn das STP regelmäßig eine gute angegebene Fenstergröße sendet, sollten Sie in der Lage sein, mehr SCTP-Daten-Chunks zu senden, wenn der Wert **SCTP_RTO_MAX** auf maximal fünf Sekunden verringert wird. Die Warteschlange wird schneller gelöscht, und ein M3UA-Überlastungsalarm wird nicht ausgelöst. Darüber hinaus sollte das vom SCTP ausgelöste Internal Flow Control-Flag nicht angezeigt werden, um den Paketfluss zu steuern.

Das SGSN sendet nur Pakete in der Menge, die das STP akzeptieren kann, und zwar entsprechend der angegebenen Fenstergröße. Wenn Sie die TPS pro STP-Verbindung erhöhen, können STP-Überlastungen vermieden und der SCTP_RTO_MAX-Timer reduziert werden.

Trigger für überlasteten M3UA-Alarm in SGSN

Wenn die angezeigte Fenstergröße in der SACK-Nachricht (Stream Control Transmission Protocol) (SCTP) Selective Acknowledgement (SACK) nahe Null (oder Null) liegt, löst das SGSN einen M3UA-Alarm aus, um anzuzeigen, dass Nachrichten für diesen Peer-Endpunkt nicht gesendet werden sollen. Dies bewirkt, dass der Link Flapping auslöst oder in einen überlasteten Zustand wechselt. Da das SGSN eine größere Fenstergröße sendet, werden weiterhin M3UA-Daten von den Peer-Knoten empfangen. Diese Pakete können in die Warteschlange fallen, wenn der Peer-Point-Code nie aus dem überlasteten Zustand kommt.

Hier ein Beispiel:

1. Das SCTP sendet eine Startanzeige für die Flusssteuerung an das M3UA.

2. Das M3UA legt das "Congestion active"-Flag für die Zuordnung fest und fängt an, das SCTP regelmäßig über den Status der Flusskontrolle abzufragen.

3. Während sich eine Zuordnung in der Flusskontrolle befindet, werden künftige Datenanforderungen für diese Zuordnung in die Warteschlange gestellt, bis QUEUE_SIZE 8.000 erreicht hat. An diesem Punkt werden zukünftige Nachrichten für die Assoziation verworfen.

4. Wenn das STP eine korrekte angegebene Fenstergröße sendet, versucht das M3UA, die in die Warteschlange gestellten Nachrichten zu leeren, bis sie 5.000 erreicht haben. Dabei spielt auch der RTO-Timer eine Rolle.

Die SCTP-Nachrichten werden nur für Zuordnungen in die Warteschlange gestellt, bei denen das Flag für die Flusskontrolle **True** wird, und das SGSN verarbeitet dann entsprechend der STP-Antwort:

```
*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
```

Wie gezeigt, liegt der Grund für die Überlastung darin, dass die Gesamtzahl ausgehender Chunks die Grenze von 5.000 überschreitet (8050+143=8193) und den maximalen RTO-Timer von 60 Sekunden erreicht, was zu verworfenen SCTP-Datenanforderungen führt. Außerdem ist der RTO-Timer höher.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.