Troubleshoot Inter-PLMN Handover Failures with Intra-SGSN RAUs on the ASR5x00

TAC **Document ID: 119254**

Contributed by Karuna Jha and Azgar Shaik, Cisco TAC Engineers.
Sep 01, 2015

Contents

Introduction

This document describes a problem that is encountered on the Cisco Aggregated Services Router (ASR) 5x00 Series that acts as a Serving General Packet Radio Service (GPRS) Support Node (SGSN) after a subscriber moves from one Public land Mobile Network (PLMN) to another PLMN within the same SGSN, or between two SGSNs.

The expected behavior is that the SGSN should perform a Routing Area Update (RAU) *reject*, and that the User Equipment (UE) should perform a fresh attach in the new PLMN. However, this is not the case in some instances. A workaround to this problem is provided.

Call Flow with Configuration

Here is the call flow when a UE moves from its home PLMN to a foreign PLMN:

1. Once the call arrives at the SGSN, the SGSN checks the operator policy name against the International Mobile Subscriber Identity (IMSI):

```
sgsn-global

    imsi-range mcc xxx mnc yyy operator-policy
     <operator_policy_name>
```

2. The associated call-control profile is checked against the operator policy:

```
operator-policy name <operator_policy_name>

    associate call-control-profile
     <call_control_profile_name>

 #exit
```

3. After the call-control profile is checked, the UE behaves as per the configuration:

```
call-control-profile < call_control_profile_name>

    rau-inter-plmn restrict access-type gprs all

    rau-inter-plmn access-type gprs all failure-code 14
```

```
rau-inter-plmn restrict access-type umts all

rau-inter-plmn access-type umts all failure-code 14
```

This configuration enables or disables the restriction of all RAUs that occur between the different PLMNs. Ideally, it should be restricted so that the Mobile Station (MS) attempts a fresh *attach* in the new PLMN.

Problem

Once the inter-RAU is rejected, the MS behaves as per the failure code that is defined (you can see this in the output of the **config verbose** command).

Note: The default is *Failure Code 14*.

In this case, after the Packet Data Protocol (PDP) *reject*, the UE does not attempt a fresh *attach*:

```
Wednesday June 17 2015

INBOUND>>>>>  From sessmgr:1 gtapp_tun_fsm.c:4489 (Callid 00135958) 05:05:22:168
 Eventid:116003(3)

GTPC Rx PDU, from <>:2123 to <>:19001 (14)

TEID: 0x81F0A001, Message type: GTP_DELETE_PDP_CONTEXT_RES_MSG (0x15)

Sequence Number:: 0x4E43 (20035)

GTP HEADER FOLLOWS:

Version number: 1

Protocol type: 1 (GTP C/U)

Extended header flag: Not present

Sequence number flag: Present

NPDU number flag: Not present

Message Type: 0x15 (GTP_DELETE_PDP_CONTEXT_RES_MSG)

Message Length: 0x0006 (6)

Tunnel ID: 0x81F0A001

Sequence Number: 0x4E43 (20035)

GTP HEADER ENDS.

INFORMATION ELEMENTS FOLLOW:

Cause: 0x80 (GTP_REQUEST_ACCEPTED)

INFORMATION ELEMENTS END.

PDU HEX DUMP FOLLOWS:

0x0000   3215 0006 81f0 a001 4e43 0000 0180             2.......NC....


Wednesday June 17 2015

INBOUND>>>>>  From sessmgr:1 gbmgr_bssgp.c:60 (Callid 00135958) 05:05:22:195
```

```
 Eventid:115053(13)

===>BSSGP Message (20 Bytes)

nsei-11311  bvci-10439

Message: UL-UNITDATA

Incorrect length=19

Decode Error

0x0000   0198 53da 0114 0020 0888 0425 4014 0121        ..S........%@..!

0x0010   3c67 0e80                                      <g..

Wednesday June 17 2015

INBOUND>>>>>  From sessmgr:1 gbmgr_bssgp.c:60 (Callid 00135958) 05:05:22:195
 Eventid:115053(13)

===>BSSGP Message (20 Bytes)

nsei-11311  bvci-10439

Message: UL-UNITDATA

Incorrect length=19

Decode Error

0x0000   0198 53da 0114 0020 0888 0425 4014 0121        ..S........%@..!

0x0010   3c67 0e80                                      <g..

Wednesday June 17 2015

***CONTROL*** From sessmgr:1 sessmgr_func.c:7482 (Callid 00135958) 05:05:22:259
 Eventid:10285

CALL STATS: <>, msid <>, Call-Duration(sec): 541

input pkts: 1986                      output pkts: 2039

input bytes: 319924                   output bytes: 1126648

input bytes dropped: 0                output bytes dropped: 4266

input pkts dropped: 0                 output pkts dropped: 8

Disconnect Reason: sgsn-roaming-not-allowed

***

*** Call Finished - Waiting to trace next matching call

***
```

```
Wednesday June 17 2015

<<<<OUTBOUND  From aaaproxy:1 proxy_handler.c:1002 (Callid 00135958) 05:06:08:843
 Eventid:66001(7)

CDR Tx from <>:49999 to <>:3386 (252) PDU-dict=custom33

Message Type: GTPP_DATA_RECORD_TRANSFER_REQUEST_MSG (0xf0)


CDR ELEMENTS FOLLOW

recordType                          SGSNPDPRECORD
```

Root Cause

For Failure Code 14, the MS performs these actions:

- Deletes any Routing Area Identifier (RAI), Packet Temporary Mobile Subscriber Identity (P-TMSI), P-TMSI signature, and General Packet Radio Service (GPRS) ciphering key sequence numbers that are stored.
- Sets the GPRS update status to **GU3 ROAMING NOT ALLOWED**, resets the GPRS attach attempt counter, and changes to state **GMMDEREGISTERED**.
- Stores the PLMN identity in the *forbidden PLMNs for GPRS service* list, which is flushed by a power off/on only.

Thus, with the use of Failure Code 14, the MS never attempts the fresh attach, and the UE is not able to browse in the new PLMN until the device is restarted.

Solution

In order to workaround this issue, you can change Failure Code 14 to either 9 or 10.

For Failure Code 9 (*MS identity cannot be derived by the network*) the MS performs these actions:

- Sets the GPRS update status to **GU2 NOT UPDATED** and enters the state **GMM-DEREGISTERED**.
- Deletes any P-TMSI, P-TMSI signature, RAI, and GPRS ciphering key sequence numbers.
- Automatically initiates the GPRS attach procedure. If *S1* mode is supported in the UE, the UE handles the EPS Mobility Management (EMM) parameters EMM state, Evolved Packet System (EPS) update status, Globally Unique Temporary UE Identity (GUTI), last visited registered Tracking Area Identity (TAI), and TAI list and key set identifier (KSI).

For Failure Code 10 (*Implicitly detached*), the MS performs these actions:

- Changes the state to **GMM-DEREGISTERED.NORMAL-SERVICE**.
- Performs a new attach procedure.

- Activates the PDP context(s) in order to replace any previously active PDP contexts.
- Performs the procedures that are needed in order to activate any previously active multicast service(s). If *S1* mode is supported in the UE, the UE handles the EMM state for the case when the TAU procedure is rejected with this cause value.

When either Failure Code 9 or 10 is used, after a move to the new PLMN and after the PDP is deleted, the MS attempts a fresh attach and is able to browse:

```
Wednesday June 17 2015

INBOUND>>>>>  From sessmgr:16 gtapp_tun_fsm.c:4489 (Callid 048dbde2) 19:03:02:682
 Eventid:116003(3)

GTPC Rx PDU, from <>.55:2123 to<>:19016 (14)

TEID: 0x83108010, Message type: GTP_DELETE_PDP_CONTEXT_RES_MSG (0x15)

Sequence Number:: 0x2E96 (11926)

GTP HEADER FOLLOWS:

Version number: 1

Protocol type: 1 (GTP C/U)

Extended header flag: Not present

Sequence number flag: Present

NPDU number flag: Not present

Message Type: 0x15 (GTP_DELETE_PDP_CONTEXT_RES_MSG)

Message Length: 0x0006 (6)

Tunnel ID: 0x83108010

Sequence Number: 0x2E96 (11926)

GTP HEADER ENDS.

INFORMATION ELEMENTS FOLLOW:

Cause: 0x80 (GTP_REQUEST_ACCEPTED)

INFORMATION ELEMENTS END.

PDU HEX DUMP FOLLOWS:

0x0000   3215 0006 8310 8010 2e96 0000 0180            2.............


Wednesday June 17 2015

***CONTROL*** From sessmgr:16 sessmgr_func.c:7482 (Callid 048dbde2) 19:03:02:745
 Eventid:10285

CALL STATS: <>, msid <>, Call-Duration(sec): 899

input pkts: 6490                      output pkts: 6021

input bytes: 844122                   output bytes: 3710188
```

input bytes dropped: 0 output bytes dropped: 8361

input pkts dropped: 0 output pkts dropped: 31

Disconnect Reason: sgsn-roaming-not-allowed

Wednesday June 17 2015

INBOUND>>>>> From sessmgr:16 gbmgr_bssgp.c:60 (Callid 77359e2d) 19:03:02:813
Eventid:115053(13)

===>BSSGP Message (79 Bytes)

nsei-1001 bvci-10243

Message: UL-UNITDATA

TLLI(Current)

TLLI Value: 0x953ce010 (Foreign TLLI)

QOS Profile

Peak Bitrate provided by NW : 5242 (in 0.1 kbps)

Precedence : Radio Priority 1

A-Bit : Radio interface uses RLC/MAC-ARQ functionality

T-Bit : The Sdu Contains Signalling

C/R-Bit : The Sdu does not contain a LLC ACK or SACK Command/response frame type

Peak Bit Rate Granularity : 0.1 kbps increments

Cell Identifier

Length: 8

MCC digit 1 : 4

MCC digit 2 : 0

MCC digit 3 : 5

MNC digit 1 : 0

MNC digit 2 : 3

MNC digit 3 : 1

LAC : 0x17d5

RAC : 0x3d

CI : 10813

Alignment Octets

Length: 0

LLC-PDU

```
Length: 57

===> Logical Link Control (LLC) (0x39) (57 bytes)

Address Field :

0... ....         Protocol Discriminator : LLC

.0.. .... Command / Response : Command (MS to SGSN)

..00 .... Spare : 0

.... 0001 SAPI : GPRS Mobility Management

Control Field :

.... Unconfirmed Information Format (UI)

...0 0... Spare : 0

N(U) : 0 (0x000)

.... ..0. Encryption Mode bit : Non-ciphered information

.... ...1 Protected Mode bit : Protected information

Information Field :

===>GPRS Mobility/Session Management Message (51 Bytes)

Protocol Discriminator : GMM message

0000 .... : Skip Indicator : (0)

.... 1000 : Protocol Discriminator : (8)

Message Type: 0x1 (1)

Message : Attach Request
```