OsmoSGSN - Bug #1947

GPRS Attach reject for Apple/Android mobile

02/09/2017 03:31 PM - sergio292

Status:	New	**Start date:**	02/09/2017
Priority:	Normal	**Due date:**	
Assignee:	laforge	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

I try to deploy network with OsmoSGSN + IP.Access BS model 139. When I make GPRS Attach on Android it fail with cause *GMM Cause: MS identity cannot be derived by the network (9)*. Same time Nokia E52 work fine.
From traces (attached) I see that android didn't respond to Identity request. I propose that Android didn't understand any of MS Radio Capability parameters sent in Identity request.

History

#1 - 02/13/2017 08:52 PM - laforge

- Assignee deleted (Osmocom CNI Developers)

sergio292 wrote:

> From traces (attached) I see that android didn't respond to Identity request. I propose that Android didn't understand any of MS Radio Capability parameters sent in Identity request.

Unfortunately your trace only shows a very short

Do you have any specific reason to say so? Did you verify that they are different from what the MS sends to the network as part of the "Attach Request" Layer3 Message ("MS Network Capability IE")?

Do you have a access to DIAG/QXDM on the phoen side? Do you have a OsmocomBB-phone that you can use with gprsdecode to see what actually happens on the radio interface? or a different BTS for comparison?

#2 - 04/12/2017 02:56 PM - afinello

I'm struggling with the same issue on similar setup (OsmoSGSN + ip.access 165)

I'm unable to make GPRS working and get the following logs from the osmo-sgsn:

```
<0011> gprs_bssgp.c:379 BSSGP TLLI=0x7f4bf450 Rx UPLINK-UNITDATA
<0012> gprs_llc.c:522 LLC RX: unknown TLLI 0x7f4bf450, creating LLME on the fly
<0012> gprs_llc_parse.c:82 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS=0x6c2c55 CMD=UI DATA
<0002> gprs_gmm.c:1243 MM(---/ffffffff) -> GMM ATTACH REQUEST MI(--my-phone-IMEI-here--) type="GPRS attach"
<0002> gprs_gmm.c:225 MM(--my-phone-IMEI-here--/fc50ce8e) Starting MM timer 3370 while old timer 3370 pending
<0002> gprs_gmm.c:548 MM(--my-phone-IMEI-here--/fc50ce8e) <- GPRS IDENTITY REQUEST: mi_type=IMEI
<0011> gprs_bssgp.c:506 BSSGP BVCI=2 TLLI=7f4bf450 Rx LLC DISCARDED
...
<0002> gprs_gmm.c:2141 MM(--my-phone-IMEI-here--/fc50ce8e) T3370 expired >= 5 times
<0002> gprs_gmm.c:481 MM(--my-phone-IMEI-here--/fc50ce8e) <- GPRS ATTACH REJECT: MS identity cannot be derived
 by the network
<0002> gprs_gmm.c:305 MM(--my-phone-IMEI-here--/fc50ce8e) Cleaning MM context due to GPRS ATTACH REJECT (T3370
)
```

This happens with all kind of devices (iPhone, Android, 3G-modem in 2G mode)

From the OsmoSGSN tty stats I see that all LLCs are discarded

```
NSEI   101, BVCI     2, RA-ID: 1-1-1-0, CID: 0, STATE: UNBLOCKED
 BSSGP Peer Statistics:
  Packets at BSSGP Level ( In):       40 (0/s 14/m 26/h 0/d)
  Packets at BSSGP Level (Out):       25 (0/s 10/m 15/h 0/d)
  Bytes at BSSGP Level   ( In):     1469 (0/s 550/m 919/h 0/d)
  Bytes at BSSGP Level   (Out):     1432 (0/s 621/m 811/h 0/d)
```

```
  BVC Blocking count:        0 (0/s 0/m 0/h 0/d)
  BVC LLC Discarded count:       22 (0/s 8/m 14/h 0/d)
  BVC Status count:        0 (0/s 0/m 0/h 0/d)
FC-BVC(bucket_max: 64000oct, leak_rate: 60000oct/s, cur_tokens: 0oct, max_q_d: 30, cur_q_d: 0)
NSEI   101, BVCI     0, RA-ID: 0-0-0-0, CID: 0, STATE: UNBLOCKED
 BSSGP Peer Statistics:
  Packets at BSSGP Level ( In):        0 (0/s 0/m 0/h 0/d)
  Packets at BSSGP Level (Out):        0 (0/s 0/m 0/h 0/d)
  Bytes at BSSGP Level   ( In):        0 (0/s 0/m 0/h 0/d)
  Bytes at BSSGP Level   (Out):        0 (0/s 0/m 0/h 0/d)
  BVC Blocking count:        0 (0/s 0/m 0/h 0/d)
  BVC LLC Discarded count:        0 (0/s 0/m 0/h 0/d)
  BVC Status count:        0 (0/s 0/m 0/h 0/d)
FC-BVC(bucket_max: 100000oct, leak_rate: 262144oct/s, cur_tokens: 0oct, max_q_d: 30, cur_q_d: 0)
```

Please tell me if you need some kind of logs or captures to be attached

#3 - 04/13/2017 02:56 PM - afinello

In case if anyone interested - the issue is related to malformed PDU message in gprs_bssgp.c (libosmocore) in the following function

```
int bssgp_tx_dl_ud(struct msgb *msg, uint16_t pdu_lifetime, struct bssgp_dl_ud_par *dup)
```

We should remove the following parts of the request (they are from GPRS Attach Request, but not from GPRS Identity Request):
IMSI (why do we add IMSI data when we are asking for that in this message?)
DRX parameters
MS Radio Access Capability

And then add missing Alignment octets (some BTSes are sensible to the data alignment depending on the firmware version)

After this fix - the attach procedure is working as expected.

#4 - 07/10/2017 10:27 PM - laforge

- Assignee set to laforge

#5 - 07/10/2017 10:33 PM - laforge

Sorry for the late response.

afinello wrote:

> In case if anyone interested - the issue is related to malformed PDU message in gprs_bssgp.c (libosmocore) in the following function

can you please provide a PCAP file of the malformed (and a non-malformed, if you have) message, so we can compare?

> We should remove the following parts of the request (they are from GPRS Attach Request, but not from GPRS Identity Request):
> IMSI (why do we add IMSI data when we are asking for that in this message?)

3GPP TS 48.018 Section 6.1 states:

```
The SGSN shall include the IMSI in the PDU. As an exception, the SGSN may omit the IMSI in the PDU if the mobi
le
 station identified by the TLLI is in MM non-DRX mode period (i.e. during a GMM procedure for GPRS attach or
 routing area updating defined in 3GPP TS 24.008) and the SGSN does not have a valid IMSI.
```

So we **shall** include the IMSI, and we only **may** omit it. Including it in every PDU is thus the intended behavior as per the spec. Which part of which specification makes you assume that including the IMSI in BSSGP DL-USERDATA is creating a malformed packet?

> DRX parameters

3GPP TS 48.018 Section 6.1 states:

```
If the SGSN has valid DRX Parameters for a TLLI, then the SGSN shall include them in the PDU. Nevertheless, th
e
 SGSN can omit the DRX Parameters if the MS identified with the TLLI is in MM non-DRX mode period to speed up
 the transmission of the LLC-PDU on the radio interface. The SGSN shall not send a DL-UNITDATA PDU without the
 DRX Parameters IE if the MS identified with the TLLI is not in MM non-DRX mode period.
```

So once again we **shall** include them, but only **may** omit them. Again, nothing wrong with the current behavior, as far as I can see?

> MS Radio Access Capability

3GPP TS 48.018 Section 6.1 states:

```
If there is valid MS Radio Access Capability information known by the SGSN for the associated MS, the SGSN sha
ll include it in the DL-UNITDATA PDU. Otherwise, MS Radio Access Capability shall not be present;
```

Once again we **shall** include the RA Capability.

> And then add missing Alignment octets (some BTSes are sensible to the data alignment depending on the firmware version)

This indeed is a bug. Can you please provide a pcap file or hexdump of messages that are missing alignment octets?

> After this fix - the attach procedure is working as expected.

This sounds like you made it work. However, I couldn't see any related patches in gerrit or attached to that ticket. Please share your fixes, this is a collaborative development effort!

#6 - 04/13/2019 11:21 AM - laforge

Dear @afinello, it seemed like you fixed a problem two years ago, but we still haven't been able to fix the official osmocom code as you never provided the related patch. It would be great if everyone could benefit from your fix. thsanks!

Files

GPRS_Attach_fail.pcapng	23.6 KB	02/09/2017	sergio292