OsmoHNBGW - Bug #2638

segfault during IuCS connect request

11/14/2017 11:55 AM - neels

Status:	Closed	**Start date:**	11/14/2017
Priority:	Urgent	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

using current master of osmo-hnbgw, I get a segfault consistently:

```
<0000> ../../../src/osmo-iuh/src/context_map.c:85 Creating new Mapping RUA CTX 0x555555850bd0/23 <
-> SCU Conn ID 0x55555584ecc0/1000

Program received signal SIGSEGV, Segmentation fault.
strlen () at ../sysdeps/x86_64/strlen.S:106
106    ../sysdeps/x86_64/strlen.S: No such file or directory.
(gdb) bt
#0  strlen () at ../sysdeps/x86_64/strlen.S:106
#1  0x00007ffff67cad78 in _IO_vfprintf_internal (s=s@entry=0x7fffffffcb60, format=<optimized out>,

    format@entry=0x5555555936f0 "rua_to_scu() %s to %s, rua_ctx_id %u scu_conn_id %u\n", ap=ap@ent
ry=0x7fffffffdda0)
    at vfprintf.c:1637
```

Details follow...

Related issues:

Related to Cellular Network Infrastructure - Bug #2330: add --enable-sanitize...	**Closed**	**06/18/2017**
Related to Cellular Network Infrastructure - Feature #2618: write Osmocom Net...	**Closed**	**11/07/2017**

History

#1 - 11/14/2017 12:00 PM - neels

```
===== asn1c =====
1b38a280d97c9c3b705d1e3d9f62ba5c4468c3dd

===== libasn1c =====
0a433101824b510f1e480c6365e401bd7d7fcd82

===== libosmo-abis =====
323d39d784417b5582098d6a27b24f94bb2e1d12

===== libosmo-netif =====
bea215a565390009ddc79b830db334fa33cc7b3a

===== libosmo-sccp =====
b393b3f4cc8a83e1e58c44187a383050378d860f

===== libosmocore =====
e08da9757099af3d275c122c9379d46a037eb309

===== libsmpp34 =====
0f760a64769c63e267532080f476f63a42eda339

===== osmo-bsc =====
4a3b044ad71535d7849bd1e7a507e4ae7a672490

===== osmo-bts =====
25647562968ac6985e3999f4e71bbfd7751d6715
```

```
===== osmo-ggsn =====
afd76a731fbb03c39e78309baf52829901a0ac66

===== osmo-hlr =====
8db490695d2bc9c08199c4073b01d79f72158c85

===== osmo-iuh =====
9420ef8d2929165cf500ad33aa61915ca5cd33c8

===== osmo-mgw =====
333f8f24a4ed07444b65faf1289707b45308cf84

===== osmo-msc =====
c698ab9a823855e67f1247b0d1503519bfe877b3

===== osmo-sgsn =====
b10a2947d511e5637ea8d4fc990efb06fb48b061

===== osmo-trx =====
1468a5c3dc4c193422d0ccbe5e09e423395bbec5

<0001> ../../../src/osmo-iuh/src/hnbgw_hnbap.c:386 HNB-REGISTER-REQ from 000295-0000152614@ap.ipaccess.com
<0000> ../../../src/osmo-iuh/src/context_map.c:143 Running context mapper garbage collection
<0000> ../../../src/osmo-iuh/src/context_map.c:143 Running context mapper garbage collection
<0000> ../../../src/osmo-iuh/src/context_map.c:143 Running context mapper garbage collection
<0000> ../../../src/osmo-iuh/src/context_map.c:143 Running context mapper garbage collection
<0001> hnbap_decoder.c:759 Decoding message UERegisterRequestIEs (hnbap_decoder.c:759)
<0001> ../../../src/osmo-iuh/src/hnbgw_hnbap.c:436 UE-REGISTER-REQ ID_type=1 imsi=901700000014701 cause=1
<0001> ../../../src/osmo-iuh/src/hnbgw.c:166 created UE context: id 0x17, imsi 901700000014701, tmsi 0x0
<0000> rua_decoder.c:21 Decoding message RUA_ConnectIEs (rua_decoder.c:21)
<0002> ../../../src/osmo-iuh/src/hnbgw_rua.c:345 RUA IuCS Connect.req(ctx=0x17, normal)
<0000> ../../../src/osmo-iuh/src/context_map.c:85 Creating new Mapping RUA CTX 0x555555850bd0/23 <-> SCU Conn
ID 0x55555584ecc0/1000

Program received signal SIGSEGV, Segmentation fault.
strlen () at ../sysdeps/x86_64/strlen.S:106
106    ../sysdeps/x86_64/strlen.S: No such file or directory.
(gdb) bt
#0  strlen () at ../sysdeps/x86_64/strlen.S:106
#1  0x00007ffff67cad78 in _IO_vfprintf_internal (s=s@entry=0x7fffffffcb60, format=<optimized out>,
    format@entry=0x5555555936f0 "rua_to_scu() %s to %s, rua_ctx_id %u scu_conn_id %u\n", ap=ap@entry=0x7ffffff
fdda0)
    at vfprintf.c:1637
#2  0x00007ffff67f1e59 in _IO_vsnprintf (string=0x7fffffffcd61 "rua_to_scu() IuCS to ", maxlen=<optimized out>
,
    format=0x5555555936f0 "rua_to_scu() %s to %s, rua_ctx_id %u scu_conn_id %u\n", args=0x7fffffffdda0) at vsn
printf.c:114
#3  0x00007ffff798f6e8 in _output (target=0x5555557d48a0, subsys=2, level=1,
    file=0x555555593630 "../../../src/osmo-iuh/src/hnbgw_rua.c", line=220, cont=0,
    format=0x5555555936f0 "rua_to_scu() %s to %s, rua_ctx_id %u scu_conn_id %u\n", ap=0x7fffffffdda0)
    at ../../../src/libosmocore/src/logging.c:364
#4  0x00007ffff798fa71 in osmo_vlogp (subsys=2, level=1, file=0x555555593630 "../../../src/osmo-iuh/src/hnbgw_
rua.c", line=220,
    cont=0, format=0x5555555936f0 "rua_to_scu() %s to %s, rua_ctx_id %u scu_conn_id %u\n", ap=0x7fffffffde18)
    at ../../../src/libosmocore/src/logging.c:464
#5  0x00007ffff798fc36 in logp2 (subsys=2, level=1, file=0x555555593630 "../../../src/osmo-iuh/src/hnbgw_rua.c
", line=220, cont=0,
    format=0x5555555936f0 "rua_to_scu() %s to %s, rua_ctx_id %u scu_conn_id %u\n") at ../../../src/libosmocore
/src/logging.c:497
#6  0x0000555555578fe7 in rua_to_scu (hnb=0x555555850bd0, cN_DomainIndicator=0, type=OSMO_SCU_PRIM_N_CONNECT,
context_id=23, cause=0,
    data=0x555555852150 "", len=78) at ../../../src/osmo-iuh/src/hnbgw_rua.c:217
#7  0x0000555555579530 in rua_rx_init_connect (msg=0x555555850d80, in=0x7fffffffe208) at ../../../src/osmo-iuh
/src/hnbgw_rua.c:347
#8  0x000055555557992a in rua_rx_initiating_msg (msg=0x555555850d80, imsg=0x7fffffffe1f8) at ../../../src/osmo
-iuh/src/hnbgw_rua.c:466
#9  0x0000555555579b3d in _hnbgw_rua_rx (msg=0x555555850d80, pdu=0x7fffffffe1f0) at ../../../src/osmo-iuh/src/
hnbgw_rua.c:517
#10 0x0000555555579ce2 in hnbgw_rua_rx (hnb=0x555555850bd0, msg=0x555555850d80) at ../../../src/osmo-iuh/src/h
nbgw_rua.c:549
#11 0x000055555557651e in hnb_read_cb (conn=0x55555584f040) at ../../../src/osmo-iuh/src/hnbgw.c:220
#12 0x00007ffff70d55c5 in osmo_stream_srv_read (conn=0x55555584f040) at ../../../src/libosmo-netif/src/stream.
c:784
#13 0x00007ffff70d57db in osmo_stream_srv_cb (ofd=0x55555584f048, what=1) at ../../../src/libosmo-netif/src/st
ream.c:835
```

```
#14 0x00007ffff7986df1 in osmo_fd_disp_fds (_rset=0x7fffffffe4b0, _wset=0x7fffffffe430, _eset=0x7fffffffe3b0)
    at ../../../src/libosmocore/src/select.c:216
#15 0x00007ffff7986f61 in osmo_select_main (polling=0) at ../../../src/libosmocore/src/select.c:256
#16 0x0000555555576f29 in main (argc=1, argv=0x7fffffffe668) at ../../../src/osmo-iuh/src/hnbgw.c:534
(gdb) frame 6
#6  0x0000555555578fe7 in rua_to_scu (hnb=0x555555850bd0, cN_DomainIndicator=0, type=OSMO_SCU_PRIM_N_CONNECT,
context_id=23, cause=0,
    data=0x555555852150 "", len=78) at ../../../src/osmo-iuh/src/hnbgw_rua.c:217
217         DEBUGP(DRUA, "rua_to_scu() %s to %s, rua_ctx_id %u scu_conn_id %u\n",
(gdb) l
212         osmo_prim_init(&prim->oph, SCCP_SAP_USER, type, PRIM_OP_REQUEST, msg);
213
214         map = context_map_alloc_by_hnb(hnb, context_id, is_ps, cn);
215         OSMO_ASSERT(map);
216
217         DEBUGP(DRUA, "rua_to_scu() %s to %s, rua_ctx_id %u scu_conn_id %u\n",
218                cn_domain_indicator_to_str(cN_DomainIndicator),
219                osmo_sccp_addr_dump(remote_addr),
220                map->rua_ctx_id, map->scu_conn_id);
221
(gdb) p cn_domain_indicator_to_str(cN_DomainIndicator)
$1 = 0x5555555935ea "IuCS"
(gdb) p osmo_sccp_addr_dump(remote_addr)
$2 = 0x7ffff751c780 <buf> "RI=2,PC=185,SSN=142,GTI=0"
(gdb) p map->rua_ctx_id
$3 = 23
(gdb) p map->scu_conn_id
$4 = 1000
(gdb)
```

Since all args to LOGP seem to be well defined, I'm not sure what's causing this.

#2 - 11/16/2017 11:28 AM - neels

- Related to Bug #2330: add --enable-sanitize configure flag to osmocom cellular network projects (osmo-{msc,bsc,sgsn} and dependencies) added

#3 - 11/16/2017 11:29 AM - neels

- Status changed from New to In Progress

#4 - 11/16/2017 11:29 AM - neels

- Assignee set to neels

#5 - 11/16/2017 11:32 AM - neels

btw, this fault seems to be triggered because my MCC+MNC LAC/RAC config in the hNodeB mismatches the CN config

#6 - 11/20/2017 12:33 PM - neels

- Related to Feature #2618: write Osmocom Network In The Box wiki page added

#7 - 11/20/2017 12:41 PM - neels

- Priority changed from Normal to Urgent

Taken a detour via --enable-sanitize builds and resolving sanitizer complaints, a test of hnbgw after this is pending.

I could move to a different machine to continue / re-install or somesuch, but instead I really would like to understand precisely what is going on here. Might ask for some assistance soon.

#8 - 11/23/2017 12:58 AM - neels

- Status changed from In Progress to Resolved

- % Done changed from 0 to 100

Various patches have been merged, and it is not clear exactly which one fixes it, but I can no longer reproduce the error (which used to trigger 100% of the time before).

#9 - 02/06/2018 08:26 AM - laforge

- Status changed from Resolved to Closed