OsmoHNBGW - Bug #2776

osmo-hnbgw seems to never discard RUA<->SUA mappings

12/21/2017 03:45 AM - neels

Status:	Resolved	**Start date:**	12/21/2017
Priority:	High	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

attach a subscriber, and on the hnbgw vty, 'show hnb all'. This will show the hNodeB and two mappings for the subscriber, one for IuCS and one for IuPS.

```
HNB 192.168.0.15:61809 "000295-0000154153@ap.ipaccess.com"
    MCC 901 MNC 70 LAC 24358 RAC 22 SAC 65535 CID 1048575 HNBAP ID 0 RUA ID 0
    IuCS 25->1004 (RUA->SUA) state=1
    IuPS 25->1005 (RUA->SUA) state=1
```

Put the phone in flight mode, the mappings remain. Re-attach the phone, two more mappings show up, and so on.

The mappings remain even after the log shows numerous

```
osmo-iuh/src/context_map.c:143 Running context mapper garbage collection
```

Make sure that this gets cleaned up at some point. I would expect at least after a UE Detach, the mappings should go away. I'd expect also right after a conn is closed, so that they are discarded e.g. when a Location Updating is done.

History

#1 - 12/21/2017 03:46 AM - neels

- Priority changed from Normal to High

#2 - 12/21/2017 03:48 AM - neels

hmm, there aren't necessarily new mappings created for each flight mode and back... maybe I got the semantics wrong. Still seems to me that the mappings stay around for too long...

#3 - 12/24/2017 08:46 PM - neels

- Status changed from New to In Progress

- % Done changed from 0 to 70

indeed there is a context_map_deactivate() function, which only gets called when the entire hnb context gets torn down.

When to remove context maps? There is a RUA id-Disconnect class of messages, which coincides with an Iu-Release. It makes sense to invalidate a mapping at that point. OsmoHNBGW code already has some state for a mapping by which a discarded mapping remains reserved for two more garbage collector runs, after which it will be discarded.

Found another bug in the garbage collector: must use llist_for_each_entry_*safe* when discarding entries.

#4 - 12/24/2017 09:14 PM - neels

a quite interesting question is: this context map maps RUA Context-IDs to SUA Context IDs (?) but we're not using SUA anymore. In immediate consequence, it maps RUA Context-IDs to prim->*.conn_id, but I'm having trouble to find any place where this prim conn_id is even used in the current M3UA stack when composing RANAP towards the CN. It seems that there must be some mapping in order for connection-ful messages to receive their responses back to RUA with the correct RUA Context-ID, but I can't find the prim conn_id sent up to RANAP anywhere. Could it be that the entire context_map mechanism in osmo-hnbgw is already superseded by some libosmo-sigtran feature?? Still looking...

#5 - 12/24/2017 09:34 PM - laforge

komm doch mal in IRC oder Jabber :P

#6 - 12/24/2017 09:47 PM - neels

It is a bit confusing, but I found the locally created context ID in the SCCP Source Local Reference, where it belongs.

The confusing part is: we created e.g. the local reference id 1002 (decimal), and in the wireshark trace, I get 0xea0300. This looks like a completely unrelated ID, until I observe that hex(1002) = 0x03ea. It seems that either the wireshark dissector for SCCP is a bit crude, or that we encode the reference in the "wrong" byte order. As long as the references go back and forth in the same byte order, there isn't really a "wrong" byte order, yet this made it quite challenging to understand what was going on in the network trace.

#7 - 12/24/2017 09:54 PM - laforge

each SCCP connection is identified (to the SCCP user, such as the hnb-gw) by a connection ID.

Compare the situation with a TCP Socket and think of it something like a socket file descriptor, which has only significance between the "socket provider" (kernel) and the "socket user" (your application program).

The source/destination local references are just present on the wire. Their only requirement is to be unique. There is **no** defined mapping between the locally-significant connection_id and the protocol-layer source/remote references!

#8 - 12/24/2017 11:52 PM - neels

- % Done changed from 70 to 100

https://gerrit.osmocom.org/5574
https://gerrit.osmocom.org/5575

Related to above discussion: no longer showing the individual context maps on VTY output, rather show overall counts, with
https://gerrit.osmocom.org/5573

#9 - 12/24/2017 11:53 PM - neels

- Assignee set to neels

#10 - 01/07/2018 07:00 PM - neels

- Status changed from In Progress to Resolved