In Milenage auth, it is highly desirable that osmo-hlr guarantees use of distinct INDs for CS and PS domains. If an MSC and SGSN attached at the same time use the same IND bucket to generate Milenage SQN, that collision would rapidly waste SQNs and load osmo-hlr with requesting new auth tuples on each CS/PS Complete-Layer3.

Currently, osmo-msc does not indicate the CN domain in the GSUP SendAuthInfo Request, which is so far also not required nor evaluated. The CN-Domain is only sent for the UpdateLocation Request that usually follows after the SendAuthInfo Request.

In order for osmo-hlr to be able to 100% guarantee distinct INDs for CS and PS, osmo-msc should set CN-Domain = CS in all SendAuthInfo Requests.

(Since officially the CN-Domain defaults to PS, osmo-sgsn doesn't necessarily need to send a CN Domain.)

**Related issues:**

Related to Distributed GSM - Bug #4319: determine auc_3g_ind from actual source_name of a request... In Progress 12/12/2019

**History**

**#1 - 12/12/2019 12:28 AM - neels**
- Description updated

**#2 - 12/12/2019 01:11 AM - neels**
- Status changed from New to In Progress
- % Done changed from 0 to 90

https://gerrit.osmocom.org/c/osmo-msc/+/16559

**#3 - 12/12/2019 07:42 AM - laforge**

while at it, it might also make sense to ensure that for now all LTE requests end up in yet another bucket. You can identify those based on the "current network type" GSPUP IE, like done in osmo-hlr Change-Id lc766bc40f6126bb479bd0a05b0e96bec3e240008

It might also make sense to always put them in the "PS" bucket, as I don't think we would expect the same subscriber to attach to both 2G/3G PS and 4G PS at the same time. But you would expect a lot of changes between those two/three, so separate buckets should make sense.

**#4 - 12/12/2019 03:08 PM - neels**
- Related to Bug #4319: determine auc_3g_ind from actual source_name of a request, not from the GSUP client conn added

**#5 - 12/12/2019 09:08 PM - neels**

On Thu, Dec 12, 2019 at 07:42:24AM +0000, laforge [REDMINE] wrote:

while at it, it might also make sense to ensure that for now all LTE requests end up in yet another bucket.

Opening up another IND pool immediately means halving the number of sites we can service before re-using INDs on a given pool. So if we currently avoid collisions for IND_bitlen == 5 meaning 16 sites guaranteed without collisions, if we add a distinct 4G bucket, we now are left with 8: 8xCS, 8xPS, 8x4G and
further 8 are practically unused from binary bit logic.

If at all possible I would try to stick with just the two pools we have, CS and PS.

You can identify those based on the "current network type" GSPUP IE, like done in osmo-hlr Change-Id lc766bc40f6126bb479bd0a05b0e96bec3e240008

So you are saying identifying 4G pools should happen on the osmo-hlr side? Don't they already show up as PS anyway? (omitting the cn_domain defaults to PS)

It might also make sense to always put them in the "PS" bucket, as I don't think we would expect the same subscriber to attach to both 2G/3G PS and 4G PS at the same time.

Would be very favorable to do that, if it is not a big concern.

would expect a lot of changes between those two/three, so separate buckets should make sense.

(not sure what this last line means: rather separate 4G pool, or also use PS pool?)

#6 - 12/13/2019 08:40 AM - laforge

Hi Neels,

On Thu, Dec 12, 2019 at 09:08:56PM +0000, neels [REDMINE] wrote:

On Thu, Dec 12, 2019 at 07:42:24AM +0000, laforge [REDMINE] wrote:

while at it, it might also make sense to ensure that for now all LTE requests end up in yet another bucket.

Opening up another IND pool immediately means halving the number of sites we can service before re-using INDs on a given pool. So if we currently avoid collisions for IND_bitlen == 5 meaning 16 sites guaranteed without collisions, if we add a distinct 4G bucket, we now are left with 8: 8xCS, 8xPS, 8x4G and further 8 are practically unused from binary bit logic.

not sure I'm following here why three would be 8 unused ones? Isn't that merely a question as to what algorithm you use to ditribute among those 32 buckets?

If at all possible I would try to stick with just the two pools we have, CS and PS.

From what I understand at this point, I don't think this is an option for mixed 2G/3G <-> 4G deployments, unless you want to re-sync all the time.

You can identify those based on the "current network type" GSPUP IE, like done in osmo-hlr Change-Id lc766bc40f6126bb479bd0a05b0e96bec3e240008

So you are saying identifying 4G pools should happen on the osmo-hlr side?

On which side would it ever happen, of not by the HLR (based on GSPU+IPA) who is generating the auth tuple? How would you do the CS/PS distinction, if not by the HLR (based on GSUP+IPA)

Don't they already show up as PS anyway? (omitting the cn_domain defaults to PS)

yes.

would expect a lot of changes between those two/three, so separate buckets should make sense.

(not sure what this last line means: rather separate 4G pool, or also use PS pool?)
It is a clear statement for separate 4G IND buckets. You have two entities requesting auth vectors as subscribers move between 2/3G and 4G coverage:

a) the MME for subscribers requiring 4G authentication
b) the SGSN for subscribers requiring 2G/3G authentication

As there's no passing of tuples between those two elements, there should be separate IND buckets to avoid re-sync at all times.

This is applicable to "normal" networks, as well as to D-GSM use cases at e.g. Rhizomatica once they add 4G support.

Please note that in at least some SIM card OS / USIM applications you can actually disable SQN validation at all. That may be one option for some operators where replay protection and inherent security implications is not a main concern. I wouldn't recommend it, but it's just one variable to take into consideration. I would also typically favor any kind of D-GSM solution that works with a "typical" USIM, i.e. one that has IND=5 and SQN checks active. This is the only way one can ensure any future interoperability with inbound roaming from other operators. Sure, for your own non-subscribes in the home network you could "optimize" with different settings, but the fall-back for "typical" USIM should exist, within the related limitations.

#7 - 12/13/2019 12:37 PM - neels

On Fri, Dec 13, 2019 at 08:40:24AM +0000, laforge [REDMINE] wrote:

As there's no passing of tuples between those two elements, there should be separate IND buckets to avoid re-sync at all times.

Taking it from the top:

We do need some way or other of getting adjacent sites into distinct IND pools, all of:
- CS and PS of the same site
- 4G and 23G of the same site
- physically adjacent separate sites.

By now I think my bit shifting idea is not a good one at all, because it addresses only one of the above points. We need a solution for all of them.

Easiest would be to delegate that to humans: add VTY commands and describe in the manual how to administer >32 VLRs properly, "done".

If it were automatic, idea is to count resyncs seen per VLR. That isn't all that trivial, because changing the IND for a site could cause a series of resyncs itself, so the algorithm needs to account for not retriggering itself.

Another idea for a heuristic:

From LU, record the moves from prev VLR -> current VLR, as a global counter per site. Thus we know which sites are most adjacent (by usage patterns). Count concurrent CS vlr and PS vlr as adjacent, maybe with a factor of 10. Also determine the average/median IND_bitlen from the subscriber DB, then work with the IND table, such that within that IND_bitlen there are no collisions between adjacent vlrs.

(The counters could be very slowly degrading moving-average to phase out legacy relations automatically after say a month)

Going back again, is all that really worth it? Usually if an MSC and SGSN are at the same site, when the first subscriber shows up on them, both of them will be added to the VLR->IND table one right after the other. What are the chances of exactly 31 other VLRs being registered between an MSC and SGSN that belong together? So I hardly expect any collisions in the inherent usual assignments anyway. I think I should drop the CS/PS bit shifting again and shouldn't keep spending time on this aspect right now, just add a simple incrementing IND and leave it up to the admin to take care about having more than 32 VLRs, and if we still need to, add a heuristic sort of like I invented above, but later.

Then we don't even need to indicate CS in the SendAuthInfo Request at all...

Sure, for your own non-subscribes in the home network you could "optimize" with different settings, but the fall-back for "typical" USIM should exist, within the related limitations.
yes, my aim ATM is to find a way that works well with 32 IND pools for all scenarios.

#8 - 05/10/2020 09:46 PM - neels
- Status changed from In Progress to Resolved
- % Done changed from 90 to 100

merged https://gerrit.osmocom.org/c/osmo-msc/+/16559