OsmoSTP - Bug #4234

osmo-stp segfaults if IPA client connects to AS with routing-key != 0

10/18/2019 09:35 PM - laforge

Status:	Resolved		**Start date:**	10/18/2019
Priority:	High		**Due date:**	
Assignee:	laforge		**% Done:**	100%
Category:				
Target version:				
Spec Reference:				

Description

When using something like this

```
as mahlzeit ipa
 routing-key 1005 5
```

and then connecting an IPA client, we crash in ipa_asp_fsm_wait_id_ack2() which contains an OSMO_ASSERT(as). The assert fails as we look-up the assert with a static routing-context of '0' (IPA doesn't allow us to transport a routing context in the message), which fails.

This is similar to [#4233](#4233)

The proper solution is probably to prevent the user from ever configuring a non-zero routing context for IPA AS.

Related issues:

Has duplicate OsmoSTP - Bug #4233: osmo-stp segfaults if IPA client with unkn...	**Closed**	**10/18/2019**

History

#1 - 10/20/2019 04:53 PM - laforge

- Status changed from New to In Progress

- % Done changed from 0 to 50

With the below patch, VTY now only permits routing-context 0 for IPA peers
https://gerrit.osmocom.org/c/libosmo-sccp/+/15815

#2 - 10/20/2019 04:57 PM - laforge

https://gerrit.osmocom.org/c/libosmo-sccp/+/15816 adds some related comments to the code.

#3 - 10/20/2019 04:58 PM - laforge

- Has duplicate Bug #4233: osmo-stp segfaults if IPA client with unknown unit_name attaches added

#4 - 10/22/2019 07:54 PM - laforge

- Status changed from In Progress to Resolved

- % Done changed from 50 to 100

patch merged