libosmo-sccp + libosmo-sigtran - Bug #3921

high local reference numbers get cut off

04/12/2019 01:23 PM - osmith

Status:	New	**Start date:**	04/12/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

Neels discovered, that when setting a high local reference number, such as 0x80000000, it will get cut off. The other end will reply "Cannot find connection for local reference 0", and abort the connection.

https://lists.osmocom.org/pipermail/openbsc/2019-April/012886.html

I was able to reproduce the issue, and saw in wireshark, what's going on: when the number is transmitted over the network, it isn't stored with 4 octets (uint32_t), as we do in the code, but with 3 octets instead. IT-U Q.713 confirms, that the destination local reference and source local reference get stored with 3 octets (e.g. in Table 4/Q.713 Message type: Connection confirm, and also in similar tables above and below).

Note that we currently have the local reference, which gets transmitted over the wire, mixed with an only locally used conn_id, and we are trying to separate the two in #3871.