

OsmoMSC - Bug #2669

osm-msc doesn't clean up BSC state

11/20/2017 07:13 PM - laforge

Status:	New	Start date:	11/20/2017
Priority:	Low	Due date:	
Assignee:	osmith	% Done:	0%
Category:	A interface (general)	Spec Reference:	
Target version:			
Resolution:			
Description			
<p>If a BSC has ever sent a BSSMAP RESET to OsmoMSC we acknowledge this with a RESET-ACK. But then it appears we keep its state indefinitely and want to perform a MSC-originated RESET procedure in return. If the BSC never gets back, this process appears to continue indefinitely.</p> <p>This is bad, as it means that anyone ever sending/spoofing a single "BSSMAP RESET" to OsmoMSC will be able to turn it into an "amplification attack" with OsmoMSC sending BSSMAP RESET in return.</p> <p>In order to avoid this, we should probably do both of:</p> <ul style="list-style-type: none">• stop re-transmitting the BSSMAP RESET after some point and simply forget about the BSCs• introduce a "locked down" mode in which we don't accept BSSMAP from any random source out there, but only explicitly configured BSCs (in the VTY)			

History

#1 - 12/23/2017 05:45 PM - laforge

- Category set to A interface (AoIP)

#2 - 12/23/2017 05:47 PM - laforge

- Category changed from A interface (AoIP) to A interface (general)

#3 - 04/03/2018 04:41 PM - dexter

See also [#2397](#) As soon as we start collecting LACs we can also collect information about when the BSC appeared first and when the last activity was. This allows us to perform a regular garbage collection.

#4 - 04/09/2018 08:18 PM - dexter

Another idea: Once we can maintain the lists using the VTY, we could also have an VTY option that disables the BSC-Auto-Learning completely if necessary.

#5 - 09/30/2018 11:37 AM - laforge

- Assignee changed from dexter to osmith