OsmoSGSN - Bug #3689

Support Cisco GGSN (Cisco 7200 with IOS 12.4.x)

11/12/2018 11:39 PM - roox

Status:	New	**Start date:**	11/12/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

I just managed to connect osmo-sgsn (2G) to an old real world GGSN implementation from Cisco (IOS 12.4 on 7200er routers).
The cool thing is that you can emulate the MIPS based hardware from these cisco routers via dynamips on commodity intel hardware :-)
I had to remove some GTP IEs the osmo-sgsn had sent that prevented the GTP tunnel to properly come up.

This GGSN implementation on the 7200 (at least with the tested IOS Version 12.4(20)T5) seems to support

- GPRS only via GTPv0 and UMTS via GTPv1
- GPRS up to Release 6.0
- explicit GPRS Release 4.0 (via: gprs compliance 3gpp ggsn r4.0)

Here is some more information about this cisco IOS based GGSN:

Cisco GGSN Release 6.0 Configuration Guide, Cisco IOS Release 12.4(2)XB8
https://www.cisco.com/c/en/us/td/docs/ios/12_4/12_4x/12_42xb/ggsn6_0/cfg/ggsn60_c/ggsnover.html
Cisco GGSN Release 6.0 Command Reference, Cisco IOS Release 12.4(2)XB8
https://www.cisco.com/c/en/us/td/docs/ios/12_4/12_4x/12_42xb/ggsn6_0/cmd/ggsn60_r.html
Release Notes for Cisco GGSN Release 6.0 on the Cisco MWAM, Cisco IOS Software Release 12.4 XB
https://www.cisco.com/c/en/us/td/docs/ios/12_4/12_4x/release/notes/rnMWAMxb.html#wp268022%0A

I've attached a patch with the following GTP IEs patched out that allowed me to connect to the Cisco GGSN.

3GPP 29.060 (GPRS)
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1595#

```
#define GTPIE_RAT_TYPE      151 /* Radio Access Technology Type */  ->> TS 29.060 7.7.50
#define GTPIE_USER_LOC      152 /* User Location Information  */    ->> TS 29.060 7.7.51
#define GTPIE_MS_TZ         153 /* MS Time Zone */                  ->> TS 29.060 7.7.52
#define GTPIE_IMEI_SV       154 /* IMEI Software Version */         ->> TS 29.060 7.7.53
```

Up to GPRS release 9 all these IEs are marked as optional.
From GPRS Release 10 on the IE for IMEI_SV is marked as conditional the others remain optional.

I've also attached debug logs, pcap traces and the osmo-sgsn.cfg

The IOS debug logs were created with the following debug options enabled

```
  debug gprs gtp events
  debug gprs gtp messages
  debug gprs gtp packets
  debug gprs gtp parsing
```

Dynamips parameters (bridge fa1/0 to eth0 on my host)

```
sudo dynamips -p 1:PA-FE-TX -s 1:0:gen_eth:eth0 --idle-pc=0x6155a540 c7200-adventerprisek9_mw-mz.124-20.T5.bin
```

History

#1 - 04/09/2019 11:21 AM - laforge

Interesting test / report, I unfortuantely didn't see it until today by accident :/

I think it's actually the Cisco side that's broken if it doesn't accept "optional" IEs but refuses to ignore them?

If we need to work around such issues, the only realistic option I can see is that we have a vty configuration item which allows the user to specify the 3GPP release of the GGSN. This way we can then decide to suppress some of those later IEs on older releases.

Maybe there's also some version information visible in the GTP from the GGSN? I don't recall that part of the GTP specs off my head.

Files

cisco-ios-debug-logs-br0ken.txt	10.1 KB	11/12/2018	roox
cisco-ios-debug-logs-OK.txt	46.2 KB	11/12/2018	roox
cisco-ios-ggsn-config.txt	2.73 KB	11/12/2018	roox
osmo-sgsn-debug-logs-br0ken.txt	28.5 KB	11/12/2018	roox
osmo-sgsn-debug-logs-OK.txt	33.3 KB	11/12/2018	roox
cisco-ios-ggsn-config.txt	2.73 KB	11/12/2018	roox
osmo-sgsn.cfg	658 Bytes	11/12/2018	roox
osmo-sgsn-cisco-7200-ggsn-br0ken.pcap	704 Bytes	11/12/2018	roox
osmo-sgsn-cisco-7200-ggsn-OK.pcap	13.8 KB	11/12/2018	roox
osmo-sgsn-do-not-send-problematic-gtp-ies.patch	3.06 KB	11/12/2018	roox