OsmoGGSN (former OpenGGSN) - Bug #5097

osmo-ggsn segv when using static prefix apn

03/26/2021 09:15 PM - roh

Status:	Resolved	**Start date:**	03/26/2021
Priority:	Normal	**Due date:**	
Assignee:	laforge	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

just tried to use the static prefix on a custom apn, and it segfaultet on me a few seconds after startup.

am i missing some important config bits? anyhow - it should not segfault

```
ggsn ggsn0
 gtp state-dir /tmp
 gtp bind-ip 10.23.24.2
 apn foo
  gtpu-mode tun
  tun-device tun7
  type-support v4
  ip prefix static 10.101.1.0/24
  ip dns 0 8.8.8.8
  ip dns 1 8.8.4.4
  ip ifconfig 10.101.1.0/24
  no shutdown
 apn internet
  gtpu-mode tun
  tun-device tun4
  type-support v4
  ip prefix dynamic 176.16.222.0/24
  ip dns 0 8.8.4.4
  ip dns 1 8.8.8.8
  ip ifconfig 176.16.222.0/24
  no shutdown
 apn inet6
  gtpu-mode tun
  tun-device tun6
  type-support v6
  ipv6 prefix dynamic 2001:780:44:2000:0:0:0:0/56
  ipv6 dns 0 2001:4860:4860::8888
  ipv6 dns 1 2001:4860:4860::8844
  ipv6 ifconfig 2001:780:44:2000:0:0:0:0/56
  no shutdown
 apn inet46
  gtpu-mode tun
  tun-device tun46
  type-support v4v6
  ip prefix dynamic 176.16.46.0/24
  ip dns 0 8.8.4.4
  ip dns 1 8.8.8.8
  ip ifconfig 176.16.46.0/24
  ipv6 prefix dynamic 2001:780:44:2100:0:0:0:0/56
  ipv6 dns 0 2001:4860:4860::8888
  ipv6 dns 1 2001:4860:4860::8844
  ipv6 ifconfig 2001:780:44:2100:0:0:0:0/56
  no shutdown
 default-apn internet
 no shutdown ggsn

Starting program: /usr/bin/osmo-ggsn -c /etc/osmocom/osmo-ggsn.cfg
```

```
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/libthread_db.so.1".
<0002> ../../git/ggsn/ggsn.c:186 APN(foo): Starting
<0002> ../../git/ggsn/ggsn.c:189 APN(foo): Opening TUN device tun7
<0002> ../../git/ggsn/ggsn.c:194 APN(foo): Opened TUN device tun7
<0002> ../../git/ggsn/ggsn.c:236 APN(foo): Setting tun IP address 10.101.1.0/24
<0002> ../../git/ggsn/ggsn.c:325 APN(foo): Successfully started
<0002> ../../git/ggsn/ggsn.c:186 APN(internet): Starting
<0002> ../../git/ggsn/ggsn.c:189 APN(internet): Opening TUN device tun4
<0002> ../../git/ggsn/ggsn.c:194 APN(internet): Opened TUN device tun4
<0002> ../../git/ggsn/ggsn.c:236 APN(internet): Setting tun IP address 176.16.222.0/24
<0002> ../../git/ggsn/ggsn.c:294 APN(internet): Creating IPv4 pool 176.16.222.0/24
<0002> ../../git/ggsn/ggsn.c:168 APN(internet): Blacklist tun IP 176.16.222.0/24
<0002> ../../git/ggsn/ggsn.c:325 APN(internet): Successfully started
<0002> ../../git/ggsn/ggsn.c:186 APN(inet6): Starting
<0002> ../../git/ggsn/ggsn.c:189 APN(inet6): Opening TUN device tun6
<0002> ../../git/ggsn/ggsn.c:194 APN(inet6): Opened TUN device tun6
<0002> ../../git/ggsn/ggsn.c:248 APN(inet6): Setting tun IPv6 address 2001:780:44:2000::/56
<0002> ../../git/ggsn/ggsn.c:311 APN(inet6): Creating IPv6 pool 2001:780:44:2000::/56
<0002> ../../git/ggsn/ggsn.c:168 APN(inet6): Blacklist tun IP 2001:780:44:2000::/56
<0002> ../../git/ggsn/ggsn.c:325 APN(inet6): Successfully started
<0002> ../../git/ggsn/ggsn.c:186 APN(inet46): Starting
<0002> ../../git/ggsn/ggsn.c:189 APN(inet46): Opening TUN device tun46
<0002> ../../git/ggsn/ggsn.c:194 APN(inet46): Opened TUN device tun46
<0002> ../../git/ggsn/ggsn.c:236 APN(inet46): Setting tun IP address 176.16.46.0/24
<0002> ../../git/ggsn/ggsn.c:248 APN(inet46): Setting tun IPv6 address 2001:780:44:2100::/56
<0002> ../../git/ggsn/ggsn.c:294 APN(inet46): Creating IPv4 pool 176.16.46.0/24
<0002> ../../git/ggsn/ggsn.c:168 APN(inet46): Blacklist tun IP 176.16.46.0/24
<0002> ../../git/ggsn/ggsn.c:311 APN(inet46): Creating IPv6 pool 2001:780:44:2100::/56
<0002> ../../git/ggsn/ggsn.c:168 APN(inet46): Blacklist tun IP 2001:780:44:2100::/56
<0002> ../../git/ggsn/ggsn.c:325 APN(inet46): Successfully started
<0002> ../../git/ggsn/ggsn.c:794 GGSN(ggsn0): Starting GGSN
<000d> ../../git/gtp/gtp.c:902 GTP: gtp_newgsn() started at 10.23.24.2
<0002> ../../git/ggsn/ggsn.c:830 GGSN(ggsn0): Successfully started
<0005> ../../../git/src/vty/telnet_interface.c:104 Available via telnet 127.0.0.1 4260
<000c> ../../../git/src/ctrl/control_if.c:911 CTRL at 127.0.0.1 4257

Program received signal SIGSEGV, Segmentation fault.
ippool_newip (this=0x0, member=0xbfffc524, addr=0xbfffc538, statip=0) at /usr/src/debug/osmo-ggsn/
1.6.0+gitrAUTOINC+2154607fb0-r2.18.0/git/lib/ippool.c:422
422    /usr/src/debug/osmo-ggsn/1.6.0+gitrAUTOINC+2154607fb0-r2.18.0/git/lib/ippool.c: No such fil
e or directory.
(gdb) bt
#0  ippool_newip (this=0x0, member=0xbfffc524, addr=0xbfffc538, statip=0)
    at /usr/src/debug/osmo-ggsn/1.6.0+gitrAUTOINC+2154607fb0-r2.18.0/git/lib/ippool.c:422
#1  0x0804cd42 in create_context_ind (pdp=0xb7afa040) at /usr/src/debug/osmo-ggsn/1.6.0+gitrAUTOIN
C+2154607fb0-r2.18.0/git/ggsn/ggsn.c:500
#2  0xb7fecd4d in gtp_create_pdp_ind (gsn=0xb7afa008, version=1, peer=0xbfffda7c, fd=10, pack=0xbf
ffda8c, len=149)
    at /usr/src/debug/osmo-ggsn/1.6.0+gitrAUTOINC+2154607fb0-r2.18.0/git/gtp/gtp.c:1758
#3  0xb7fee699 in gtp_decaps1c (gsn=0xb7afa008) at /usr/src/debug/osmo-ggsn/1.6.0+gitrAUTOINC+2154
607fb0-r2.18.0/git/gtp/gtp.c:3163
#4  0xb7f1c3d5 in osmo_fd_disp_fds (_eset=<optimized out>, _wset=<optimized out>, _rset=<optimized
 out>)
    at /usr/src/debug/libosmocore/1.4.2+gitrAUTOINC+34b328b6d0-r2.18.0/git/src/select.c:227
#5  _osmo_select_main (polling=polling@entry=0) at /usr/src/debug/libosmocore/1.4.2+gitrAUTOINC+34
b328b6d0-r2.18.0/git/src/select.c:265
#6  0xb7f1ca0a in osmo_select_main (polling=0) at /usr/src/debug/libosmocore/1.4.2+gitrAUTOINC+34b
328b6d0-r2.18.0/git/src/select.c:274
#7  0x08049f48 in main (argc=<optimized out>, argv=<optimized out>) at /usr/src/debug/osmo-ggsn/1.
6.0+gitrAUTOINC+2154607fb0-r2.18.0/git/ggsn/ggsn_main.c:201
(gdb) quit
```

this is with the packages from 201705 on a apu (3g starter kit setup)
osmo-ggsn 1.6.0+gitr0+2154607fb0-r2.18.0.1

Associated revisions

Revision ecef920b - 03/27/2021 06:00 PM - laforge

ggsn: Reject PDP CTX ACT for static IP addresses

We don't implement handling of static IP addresses for now,
let's properly reject those rather than allocating a dynamic address
anyway.

Change-Id: Iac8868438655fe4e5e07d167d7dbd6273dbb7678
Related: OS#5097

Revision 5379273e - 03/27/2021 06:03 PM - laforge

vty: Inform user that static IP addresses are not supported

Currently, osmo-ggsn doesn't implement PDP contexts with static IP
addresses. The code for specifying ranges that can be used for
static IPs was always present even from OpenGGSN days, but we never
really treated them. Let's not raise the impression we do by
warning accordingly if the user configures them.

Change-Id: I7787dae037c46c0c5052aa6dd000be330984f144
Related: OS#5097

Revision 7ef6d101 - 04/01/2021 07:27 PM - laforge

ggsn: Fix TC_pdp4_act_deact_with_single_dns()

In TC_pdp4_act_deact_with_single_dns we activate, deactivate and then
re-activate a PDP context. Hoewver, we re-use the same variable and
don't reset the state in between. This results in the second PDP CTX
activation to include an end-user-address (static IP allocation), which
OsmoGGSN doesn't implement.

Before osmo-ggsn Change-Id Iac8868438655fe4e5e07d167d7dbd6273dbb7678,
the test passed as osmo-ggsn simply ignored the requested static address.
After that change, we reject static addresses and hence the test starts
to fail.

Change-Id: I1b1869bc2cee39c8fddd8fa63f48bdaa6a65e462
Related: OS#5097

History

#1 - 03/27/2021 05:50 PM - laforge

On Fri, Mar 26, 2021 at 09:15:37PM +0000, roh [REDMINE] wrote:

> just tried to use the static prefix on a custom apn, and it segfaultet on me a few seconds after startup.
> am i missing some important config bits? anyhow - it should not segfault

I am wondering why static can be selected at all, and how that would work.

Static IPs in 3GPP networks usually mean tha

a) the HLR stores a static IP address for each (subscriber, APN)
b) the GGSN talks to the HLR to obtain that subscription information

AFAICT, we have neither of the above, so it's not surprising that it fails.

As stated, the bit question is why one can configure it in the VTY...

#2 - 03/27/2021 05:51 PM - laforge

ok, so it's s lightly different than I recalled.

3GPP specs:

- HLR must store the static IP address per (subscriber, apn)
- HLR provides this information during "insert subscriber data"
  from HLR -> SGSN
- SGSN must include the "PDP Address" field in the "End User Address IE"
  during the PDP CTX ACT REQ from SGSN to GGSN.

Looking at osmocom:

- osmo-hlr cannot store static IPs per (apn, subscriber)
- GSUP doesn't have related IEs
- libosmocore gsup code doesn't represent this in 'osmo_gsup_pdp_info'
- osmo-sgsn consequently doesn't handle it nor sends it to GGSN
- osmo-ggsn doesn't handle this in create_context_ind()

So what we should ASAP do (in the GGSN):

- remove the VTY configuration for static IP pools
- reject any PDP CTX ACT REQ for static IPs

#3 - 03/27/2021 06:15 PM - laforge

- https://gerrit.osmocom.org/c/osmo-ggsn/+/23516 ggsn: Reject PDP CTX ACT for static IP addresses [NEW]
- https://gerrit.osmocom.org/c/osmo-ggsn/+/23517 vty: Inform user that static IP addresses are not supported [NEW]

#4 - 03/30/2021 01:58 PM - roh

just tested a build with these and it rejects the static config fine without crashes (exits properly)

#5 - 04/11/2021 09:31 PM - laforge

- Status changed from New to Resolved

- Assignee set to laforge

- % Done changed from 0 to 100