batman-adv - Bug #131

"unable to handle kernel NULL pointer dereference" in send_vis_packets

09/01/2009 10:01 PM - Linus Lüssing

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marek Lindner	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.2		

Description

I got a nice backtrace of the crashing batman-adv-module. I'm using batman-adv self-compiled from the trunk rev. 1418 with the subgraph-patch with Simon's additions (mailing-list Sun Aug 30 19:55:53 UTC 2009). I was restarting tinc which is providing two interfaces for batman and then noticed, that batman still claimed those interfaces being inactive although they were up.

History

#1 - 09/02/2009 11:48 PM - Linus Lüssing

And the same problem again. What I did this time is pretty much the same as yesterday: tinc interface inside of batman-adv, then I restarted the tinc daemon while the interface was still used by batman.

#2 - 09/03/2009 12:08 AM - Linus Lüssing

Ok, it is absolutely reproduceable, here the steps I'm doing in detail:
First, starting tinc, which creates two tunnel interfaces '3micc' and '3micc-blochi'. The vis-server is on a batman-node behind '3micc'. Then I'm inserting the batman-adv-kernel module with 'insmod batman_adv.ko'. Next two steps are "echo 3micc > /proc/net/batman-adv/interfaces" and "echo 3micc-blochi > /proc/net/batman-adv/interfaces". Originators on this machine get listed from '3micc', but from '3micc-blochi' not (couldn't figure out why this is so yet). Now I'm restarting tinc with '/etc/init.d/tinc restart' and it responds with:
"Restarting tinc daemons: 3m 3micc 3micc-blochiA tincd is already running for net @3micc-blochi' with pid 3378.
3micc-maxi sellars2asta." (already something odd with 3micc-blochi???)
At that moment, I get the backtrace with dmesg. I'm also not able to stopp the tincd explicitly for 3micc-blochi with 'tincd -k -n 3micc-blochi', dmesg then gives me a lot of lines like "[889.600012] unregister_netdevice: waiting for 3micc-blochi to become free. Usage count = 1". So it looks like tincd crashes first which takes down batman-adv then.

#3 - 09/03/2009 12:16 AM - Linus Lüssing

Ok, and now run tincd in debug-mode again. It looks like it does not totally crash, but tries to close a connection... The problem also only occurs if I'm restarting really fast, so that it might not have the chance to close the connection. Though it is strange that this kills the batman-adv-module anyway.

```
/dev/net/tun is a Linux tun/tap device (tap mode)
Listening on :: port 3659
Can't bind to 0.0.0.0 port 3659/tcp: Die Adresse wird bereits verwendet
Ready
Trying to connect to blochi (188.192.189.102 port 587)
Connected to blochi (188.192.189.102 port 587)
Connection with blochi (188.192.189.102 port 587) activated
Got TERM signal
Closing connection with blochi (188.192.189.102 port 587)
Closing connection with krtek (MYSELF)
```

#4 - 09/06/2009 09:24 PM - Marek Lindner

- Status changed from New to In Progress

The patches submitted in r1425 and r1426 should fix the issues. Please close this ticket as soon as you can confirm it.

#5 - 09/07/2009 12:18 AM - Linus Lüssing

- Status changed from In Progress to Closed

Yes, thanks Marek, they did :).

#6 - 09/30/2010 12:56 AM - Anonymous

Milestone 0.2 release deleted

#7 - 03/26/2011 09:25 PM - Anonymous

- Category set to 2

#8 - 02/11/2017 09:43 AM - Sven Eckelmann

- Target version set to 0.2

Files

module-crash-01-09-09.log	2.63 KB	09/01/2009	Linus Lüssing
objdump-vis.o	37.2 KB	09/01/2009	Linus Lüssing
module-crash-02-09-09.log	2.88 KB	09/02/2009	Linus Lüssing