batman-adv - Bug #215

Kernel panic on v2015.0.0

05/27/2015 09:09 PM - Ryan Thompson

Status:	Closed	**Start date:**	05/27/2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2015.1		

Description

Updated from v2014.1.0 to fix this issue:

#183
https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/message/DVLB4P6W2KCLEGIDGXUJS4S22Q5DPW6T/

Now we get this kernel panic after setting up two adhoc networks (on phy0 and phy1), add them to bat0, and have them attempt to join IBSS networks on different frequencies. The kernel panic always happens, but it takes 30+ minutes to happen.

```
[ 3122.581410] Unable to handle kernel NULL pointer dereference at virtual address 00000020
[ 3122.581442] pgd = 80204000
[ 3122.588647] [00000020] *pgd=00000000
[ 3122.594538] Internal error: Oops: 17 [#1] PREEMPT SMP ARM
[ 3122.594725] Modules linked in: ath3k pppoe ppp_async l2tp_ppp iptable_nat ath9k(O) pppox ppp_ge
neric nf_nat_ipv4 nf_conntrack_ipv4 mmc_spi ipt_MASQUERADE ath9k_htc(O) ath9k_common(O) xt_time xt
_tcpudp xt_state xt_quota xt_pkttype xt_physdev xt_owner xt_nat xt_multiport xt_mark xt_mac xt_lim
it xt_conntrack xt_comment xt_addrtype xt_TCPMSS xt_REDIRECT xt_LOG xt_CT vhci_hcd(C) usbip_host(C
) usbip_core(C) ums_usbat ums_sddr55 ums_sddr09 ums_karma ums_jumpshot ums_isd200 ums_freecom ums_
datafab ums_cypress ums_alauda spi_gpio_old spi_bitbang slhc rfcomm qca_nss_gmac qca_nss_drv of_mm
c_spi nf_nat_irc nf_nat_ftp nf_nat nf_defrag_ipv4 nf_conntrack_irc nf_conntrack_ftp lib80211_crypt
_wep(O) lib80211_crypt_ccmp(O) lib80211(O) iptable_raw iptable_mangle iptable_filter ipt_REJECT ip
_tables hidp hid_generic hci_uart crc7 crc_itu_t crc_ccitt cdc_wdm btusb bnep bluetooth ath9k_hw(O
) 6lowpan_iphc sg hid evdev ath10k_pci(O) ath10k_core(O) ath(O) mac80211(O) cfg80211(O) compat(O)
ledtrig_usbdev ledtrig_oneshot xt_LED ledtrig_netdev ledtrig_morse ledtrig_heartbeat ledtrig_gpio
batman_adv(O) qca_ssdk(O) ip6t_REJECT ip6table_raw ip6table_mangle ip6table_filter ip6_tables x_ta
bles nf_conntrack_ipv6 nf_defrag_ipv6 msdos loop vfat fat ntfs hfsplus hfs configfs cifs rfkill 80
21q mrp garp pcbc cryptosoft cryptodev ocf md4 ecb arc4 usb_storage dwc2_platform dwc2 ohci_hcd le
dtrig_timer sd_mod
[ 3122.720678] CPU: 0 PID: 2413 Comm: kworker/u4:0 Tainted: G        WC O 3.14.0 #25
[ 3122.720978] Workqueue: bat_events batadv_send_outstanding_bat_ogm_packet [batman_adv]
[ 3122.735865] task: 9b57f480 ti: 95c22000 task.ti: 95c22000
[ 3122.736239] PC is at batadv_softif_vlan_free_ref+0x10/0xc8 [batman_adv]
[ 3122.741620] LR is at batadv_tt_orig_list_entry_free_rcu+0x2ec/0xb38 [batman_adv]
[ 3122.748030] pc : [<7f48a6e0>]    lr : [<7f48c714>]    psr: 60000013
[ 3122.748030] sp : 95c23e20  ip : 0000000c  fp : 00000000
[ 3122.755673] r10: 9633d7b4  r9 : 9af3c6c0  r8 : 000001ed
[ 3122.766859] r7 : 00200200  r6 : 963394c0  r5 : 00000000  r4 : 00000000
[ 3122.772071] r3 : 00000020  r2 : 95c23e18  r1 : 000083eb  r0 : 00000000
[ 3122.778670] Flags: nZCv  IRQs on  FIQs on  Mode SVC_32  ISA ARM  Segment kernel
[ 3122.785180] Control: 10c5787d  Table: 5d02006a  DAC: 00000015
[ 3122.792381] Process kworker/u4:0 (pid: 2413, stack limit = 0x95c22240)
[ 3122.798286] Stack: (0x95c23e20 to 0x95c24000)
[ 3122.804714] 3e20: 00000000 95c2a480 00000000 7f48c714 00000400 00000000 00000400 9af3c6c0
[ 3122.809142] 3e40: 9334ca00 00000000 95c22000 963394c0 95c22000 7f48d648 00db2214 9b013e18
[ 3122.817303] 3e60: 00000042 96339794 963394c0 9b013e00 9334ca00 00000000 95c22000 00000000
[ 3122.825463] 3e80: 95c22000 7f49080c 00000000 9334ca20 96339000 7f478398 9dc27b80 002b13d1
[ 3122.833623] 3ea0: 00000000 00000001 7f4920b0 9b013e00 96339000 963394c0 9b013e00 9b013e18
[ 3122.841780] 3ec0: 00000000 9334ca20 96339000 96339588 9334ca00 00000000 95c22000 00000000
[ 3122.849942] 3ee0: 95c22000 7f489500 7f489424 959a4b00 9334ca20 9d404400 9cfe6c00 8023f810
[ 3122.858102] 3f00: 8096cb80 8096cb80 8097a8cc 8080f8e0 9d4fd77c 959a4b00 9d404400 9d404414
[ 3122.866263] 3f20: 959a4b18 95c22000 00000089 95c22038 95c22000 80240454 9d404400 8097a895
[ 3122.874420] 3f40: 00000000 963e0980 00000000 959a4b00 802401fc 00000000 00000000 00000000
```

```
[ 3122.882583] 3f60: 00000000 802453c0 00000000 00000000 000000f8 959a4b00 00000000 00000000
[ 3122.890740] 3f80: 95c23f80 95c23f80 00000000 00000000 95c23f90 95c23f90 95c23fac 963e0980
[ 3122.898899] 3fa0: 802452d8 00000000 00000000 80208cd8 00000000 00000000 00000000 00000000
[ 3122.907058] 3fc0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 3122.915219] 3fe0: 00000000 00000000 00000000 00000000 00000013 00000000 00000000 00000000
[ 3122.923443] [<7f48a6e0>] (batadv_softif_vlan_free_ref [batman_adv]) from [<7f48c714>] (batadv_t
t_orig_list_entry_free_rcu+0x2ec/0xb38 [batman_adv])
[ 3122.931589] [<7f48c714>] (batadv_tt_orig_list_entry_free_rcu [batman_adv]) from [<7f48d648>] (b
atadv_tt_purge+0x6e8/0x9d0 [batman_adv])
[ 3122.944605] [<7f48d648>] (batadv_tt_purge [batman_adv]) from [<7f49080c>] (batadv_tt_local_comm
it_changes+0x1c/0x28 [batman_adv])
[ 3122.956756] [<7f49080c>] (batadv_tt_local_commit_changes [batman_adv]) from [<7f478398>] (batad
v_iv_ogm_schedule+0xa8/0x12f0 [batman_adv])
[ 3122.968563] [<7f478398>] (batadv_iv_ogm_schedule [batman_adv]) from [<7f489500>] (batadv_send_o
utstanding_bat_ogm_packet+0xdc/0xf4 [batman_adv])
[ 3122.980883] [<7f489500>] (batadv_send_outstanding_bat_ogm_packet [batman_adv]) from [<8023f810>
] (process_one_work+0x210/0x354)
[ 3122.993965] [<8023f810>] (process_one_work) from [<80240454>] (worker_thread+0x258/0x3e0)
[ 3123.005155] [<80240454>] (worker_thread) from [<802453c0>] (kthread+0xe8/0xec)
[ 3123.013487] [<802453c0>] (kthread) from [<80208cd8>] (ret_from_fork+0x14/0x3c)
[ 3123.020602] Code: e92d4038 e1a04000 e2803020 f57ff05b (e1932f9f)
[ 3123.027897] ---[ end trace 73752ea21b0b9805 ]---
[ 3123.034021] Kernel panic - not syncing: Fatal exception in interrupt
[ 3123.038655] CPU1: stopping
[ 3123.044984] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G      D WC O 3.14.0 #25
[ 3123.047522] [<802202a4>] (unwind_backtrace) from [<8021d03c>] (show_stack+0x10/0x14)
[ 3123.054379] [<8021d03c>] (show_stack) from [<8041bb74>] (dump_stack+0x98/0xd0)
[ 3123.062359] [<8041bb74>] (dump_stack) from [<8021f544>] (handle_IPI+0xe0/0x158)
[ 3123.069389] [<8021f544>] (handle_IPI) from [<802084f8>] (gic_handle_irq+0x58/0x5c)
[ 3123.076593] [<802084f8>] (gic_handle_irq) from [<80209540>] (__irq_svc+0x40/0x70)
[ 3123.084226] Exception stack(0x9d4a5f98 to 0x9d4a5fe0)
[ 3123.091777] 5f80:                                                     ffffffed 1d2bb000
[ 3123.096817] 5fa0: 80976f00 00000000 9d4a4000 80976458 8080f3fc 9d4a4000 8097a8d1 00000001
[ 3123.104976] 5fc0: 8097a8d1 9d4a4000 00000000 9d4a5fe0 8021aa68 8021aa6c 60000013 ffffffff
[ 3123.113137] [<80209540>] (__irq_svc) from [<8021aa6c>] (arch_cpu_idle+0x34/0x50)
[ 3123.121301] [<8021aa6c>] (arch_cpu_idle) from [<80260f44>] (cpu_startup_entry+0xd4/0x124)
[ 3123.128789] [<80260f44>] (cpu_startup_entry) from [<42208584>] (0x42208584)
[ 3123.136834] Rebooting in 3 seconds..
```

History

#1 - 06/09/2015 03:29 PM - Marek Lindner

- Status changed from New to In Progress

- File 0001-batman-adv-fix-kernel-crash-due-to-missing-NULL-chec.patch added

Thanks for reporting the issue. I attached a patch which should fix it. Do you mind giving it a try ?

#2 - 06/18/2015 05:49 AM - Ryan Thompson

Marek Lindner wrote:

> Thanks for reporting the issue. I attached a patch which should fix it. Do you mind giving it a try ?

It appears to be working! No kernel panics in several hours of operation. I'll report back if we end up seeing any, but it's looking promising.

#3 - 06/18/2015 06:14 AM - Marek Lindner

Thanks for testing! I already submitted the patch for upstream inclusion.

#4 - 07/10/2015 11:19 AM - Marek Lindner

- Status changed from In Progress to Closed

#5 - 04/16/2016 11:12 PM - Sven Eckelmann

- Description updated

#6 - 02/11/2017 08:50 AM - Sven Eckelmann

- Target version set to 2015.1

#7 - 05/27/2020 10:33 PM - Sven Eckelmann

- Description updated

Files

0001-batman-adv-fix-kernel-crash-due-to-missing-NULL-chec.patch	2.54 KB	06/09/2015	Marek Lindner