batman-adv - Bug #422

General protection fault in batadv_orig_router_get

04/20/2021 11:49 AM - Linus Lüssing

Status:	New	**Start date:**	04/20/2021
Priority:	Normal	**Due date:**	
Assignee:	batman-adv developers	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

In a VM with kvm and a 5.11.9 kernel and a recent batman-adv from the master branch I get a general protection fault when putting the VM host to sleep and waking it up again later. The VM guest runs a few mesh instances (here bat1 to bat8).

Looks like some race condition where the orig node is deleted due to timeout but there is still an OGM in the queue from this node for further processing. Without putting a node in stand-by this seems unlikely to happen as when a node timeouts then there typically will be no OGM in the queue.

```
[308421.793525] batman_adv: bat3: IGMP Querier disappeared - multicast optimizations disabled
[308421.795414] batman_adv: bat3: MLD Querier disappeared - multicast optimizations disabled
[308421.801542] batman_adv: bat6: IGMP Querier disappeared - multicast optimizations disabled
[308421.802905] batman_adv: bat6: MLD Querier disappeared - multicast optimizations disabled
[308421.804257] batman_adv: bat5: IGMP Querier disappeared - multicast optimizations disabled
[308421.805761] batman_adv: bat5: MLD Querier disappeared - multicast optimizations disabled
[308421.813031] batman_adv: bat4: IGMP Querier disappeared - multicast optimizations disabled
[308421.814303] batman_adv: bat4: MLD Querier disappeared - multicast optimizations disabled
[308421.815716] batman_adv: bat2: IGMP Querier disappeared - multicast optimizations disabled
[308421.816779] batman_adv: bat2: MLD Querier disappeared - multicast optimizations disabled
[308421.819384] batman_adv: bat8: IGMP Querier disappeared - multicast optimizations disabled
[308421.820670] batman_adv: bat8: MLD Querier disappeared - multicast optimizations disabled
[308421.821942] batman_adv: bat7: IGMP Querier disappeared - multicast optimizations disabled
[308421.823706] batman_adv: bat7: MLD Querier disappeared - multicast optimizations disabled
[308422.813967] general protection fault, probably for non-canonical address 0x6b6b6b6b6b6b6b6b: 0
000 [#1] SMP PTI
[308422.816150] CPU: 0 PID: 12563 Comm: kworker/u2:1 Tainted: G           OE     5.11.9 #41
[308422.818045] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-1 04/01/2014
[308422.819949] Workqueue: bat_events batadv_iv_send_outstanding_bat_ogm_packet [batman_adv]
[308422.821797] RIP: 0010:batadv_orig_router_get+0x10/0x70 [batman_adv]
[308422.823032] Code: 03 00 00 00 4c 89 c7 e9 de d9 0d ea 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 0
0 0f 1f 44 00 00 41 54 48 8b 47 08 48 85 c0 74 0e <48> 39 70 10 74 16 48 8b 00 48 85 c0 75 f2 45 3
1 e4 e8 0a f2 d9
[308422.826658] RSP: 0018:ffffa0d140003d50 EFLAGS: 00010202
[308422.827700] RAX: 6b6b6b6b6b6b6b6b RBX: ffff90a4c7b2104e RCX: 000000000000000b
[308422.829049] RDX: 000000000000000a RSI: 0000000000000000 RDI: ffff90a4c4e68400
[308422.830400] RBP: ffff90a4c0763bd8 R08: ffff90a4c008e8c0 R09: 00000000000002c0
[308422.831759] R10: ffff90a4c7b21000 R11: 0000000000000001 R12: ffff90a4c008e878
[308422.833103] R13: ffff90a4c7b21040 R14: 0000000000000000 R15: 0000000000000001
[308422.834425] FS:  0000000000000000(0000) GS:ffff90a4cde00000(0000) knlGS:0000000000000000
[308422.835926] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[308422.836984] CR2: 00007ffced2d6000 CR3: 0000000009cde000 CR4: 00000000000006f0
[308422.838301] Call Trace:
[308422.838789]  <IRQ>
[308422.839318]  batadv_iv_ogm_process_per_outif+0x261/0xff0 [batman_adv]
[308422.840332]  ? enqueue_entity+0x163/0x760
[308422.841867]  batadv_iv_ogm_receive+0x26a/0x4a0 [batman_adv]
[308422.842560]  batadv_batman_skb_recv+0x117/0x1d0 [batman_adv]
[308422.843357]  __netif_receive_skb_one_core+0x8e/0xa0
[308422.844492]  process_backlog+0x96/0x160
[308422.845036]  net_rx_action+0x146/0x430
[308422.845594]  __do_softirq+0xc5/0x275
[308422.846510]  asm_call_irq_on_stack+0x12/0x20
[308422.847059]  </IRQ>
[308422.847348]  do_softirq_own_stack+0x37/0x40
```

```
[308422.848588]  do_softirq+0x5e/0x70
[308422.849420]  __local_bh_enable_ip+0x4b/0x50
[308422.850164]  __dev_queue_xmit+0x376/0x8b0
[308422.850989]  batadv_send_skb_packet+0xcc/0xf0 [batman_adv]
[308422.851950]  batadv_iv_send_outstanding_bat_ogm_packet+0x18d/0x1b0 [batman_adv]
[308422.853154]  process_one_work+0x1ec/0x380
[308422.853946]  worker_thread+0x53/0x3e0
[308422.854566]  ? process_one_work+0x380/0x380
[308422.855276]  kthread+0x11b/0x140
[308422.855827]  ? __kthread_bind_mask+0x60/0x60
[308422.856577]  ret_from_fork+0x22/0x30
[308422.857199] Modules linked in: batman_adv(OE) bridge(OE) veth(E) dummy(E) libcrc32c(E) crc32c_
generic(E) crc32_generic(E) crc16(E) mac80211(E) cfg80211(E) rfkill(E) libarc4(E) stp(E) llc(E) rp
csec_gss_krb5(E)
[308422.867669] ---[ end trace 3d57397987128d5a ]---
[308422.868423] RIP: 0010:batadv_orig_router_get+0x10/0x70 [batman_adv]
[308422.869429] Code: 03 00 00 00 4c 89 c7 e9 de d9 0d ea 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 0
0 0f 1f 44 00 00 41 54 48 8b 47 08 48 85 c0 74 0e <48> 39 70 10 74 16 48 8b 00 48 85 c0 75 f2 45 3
1 e4 e8 0a f2 d9
[308422.872321] RSP: 0018:ffffa0d140003d50 EFLAGS: 00010202
[308422.873143] RAX: 6b6b6b6b6b6b6b6b RBX: ffff90a4c7b2104e RCX: 000000000000000b
[308422.874270] RDX: 000000000000000a RSI: 0000000000000000 RDI: ffff90a4c4e68400
[308422.875433] RBP: ffff90a4c0763bd8 R08: ffff90a4c008e8c0 R09: 00000000000002c0
[308422.876548] R10: ffff90a4c7b21000 R11: 0000000000000001 R12: ffff90a4c008e878
[308422.877735] R13: ffff90a4c7b21040 R14: 0000000000000000 R15: 0000000000000001
[308422.878778] FS:  0000000000000000(0000) GS:ffff90a4cde00000(0000) knlGS:0000000000000000
[308422.880257] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[308422.881197] CR2: 00007ffced2d6000 CR3: 0000000009cde000 CR4: 00000000000006f0
[308422.882512] Kernel panic - not syncing: Fatal exception in interrupt
[308422.884049] Kernel Offset: 0x29600000 from 0xffffffff81000000 (relocation range: 0xffffffff800
00000-0xffffffffbfffffff)
[308422.886580] ---[ end Kernel panic - not syncing: Fatal exception in interrupt ]---
```

History

#1 - 04/20/2021 11:49 AM - Linus Lüssing

- Description updated

#2 - 04/20/2021 11:50 AM - Linus Lüssing

- Description updated