batman-adv - Bug #294

batman-adv panic on brcm47xx with ethernet + wifi in bat0

08/26/2016 01:01 PM - Russell Senior

Status:	Rejected	**Start date:**	08/26/2016
Priority:	Normal	**Due date:**	
Assignee:	Russell Senior	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

I have a small mesh, consisting of 9 netgear wgt634u and three ubiquiti bullet m5's. Two of the three bullet m5's run batman-adv over ethernet to an ethernet port (vlan 2) on two corresponding netgear wgt634u's. The wgt634u's all mesh on an adhoc wifi interface, and provide an ap on the same radio. I have noticed instability on the two wgt634u's that run batman-adv over their ethernet interfaces. The observable symptom is that the device hangs, isn't pingable, doesn't pass traffic. A power cycle fixes it. The panics seem more frequent on the wgt634u that seems to get more traffic. Today I rigged up a raspberry pi to capture serial console traffic from the most problematic device and managed to capture an oops. Because these two wgt634u's send data over ethernet, and the ethernet MTU is 1500, packets going over ethernet are often fragmented.

The devices are all running recent LEDE-Project firmware, with batman-adv 2016.2 release 2. Most of the devices are running lede-1365-g27f47f6, the wgt634u where I captured the oops is lede-1439-g6fdc527 (kernel v4.1.20).

The network config looks like this:

```
config interface 'loopback'
    option ifname 'lo'
    option proto 'static'
    option ipaddr '127.0.0.1'
    option netmask '255.0.0.0'

config interface 'pub'
    option type 'bridge'
    option proto 'static'
    option ip6assign '60'
    option ifname 'eth0.1 bat0'
    option ipaddr '10.11.80.11'
    option netmask '255.255.252.0'
    option gateway '10.11.80.1'
    option dns '10.11.80.1'

config switch
    option name 'switch0'
    option reset '1'
    option enable_vlan '1'

config switch_vlan
    option device 'switch0'
    option vlan '1'
    option ports '0 1 2 3 5t'

config switch_vlan
    option device 'switch0'
    option vlan '2'
    option ports '4 5t'

config interface 'mesh'
    option mtu '1532'
    option proto 'batadv'
    option mesh 'bat0'

config interface 'meshwire'
    option proto 'batadv'
    option mesh 'bat0'
```

```
    option ifname 'eth0.2'
```

The batman-adv config is minimal, just turning of bridge loop avoidance:

```
config mesh 'bat0'
    option bridge_loop_avoidance '0'
```

The wireless config is as follows:

```
config wifi-device 'radio0'
    option type 'mac80211'
    option hwmode '11g'
    option path 'pci0000:00/0000:00:01.0'
    option disabled '0'
    option channel '6'

config wifi-iface
    option device 'radio0'
    option ifname 'mesh0'
    option network 'mesh'
    option mode 'adhoc'
    option ssid 'ptp-mesh'
    option encryption 'none'

config wifi-iface
    option device 'radio0'
    option ifname 'wlan0'
    option network 'pub'
    option mode 'ap'
    option ssid 'www.personaltelco.net/mesh1'
    option encryption 'none'
```

The neighbor table looks like this:

```
# batctl n
[B.A.T.M.A.N. adv 2016.2, MainIF/MAC: eth0.2/00:0f:b5:0f:2b:cb (bat0 BATMAN_IV)]
           IF        Neighbor      last-seen
       eth0.2   morrison-roof_eth0    0.690s
        mesh0         mesh8_mesh0    0.310s
        mesh0    jerry-mesh_mesh0    0.740s
        mesh0         mesh7_mesh0    7.670s
        mesh0     pete-mesh_mesh0    0.980s
        mesh0      pam-mesh_mesh0    1.690s
        mesh0   michael-mesh_mesh0    1.110s
        mesh0   howard-mesh_mesh0    0.460s
```

The oops is as follows:

```
[13900.016381] Unhandled kernel unaligned access[#1]:
[13900.021285] CPU: 0 PID: 8 Comm: kworker/u2:1 Not tainted 4.1.20 #0
[13900.027740] Workqueue: phy0 ieee80211_ibss_leave [mac80211]
[13900.033427] task: 81841550 ti: 81880000 task.ti: 81880000
[13900.038875] $ 0   : 00000000 1000b800 00000001 00200000
[13900.044336] $ 4   : 4a86b583 00010000 00000000 00000000
[13900.049787] $ 8   : 041a6e1f 815d6e54 819c1289 5a16f70e
```

```
[13900.055258] $12   : 193d1c2a 00000fb5 00000000 fde176f8
[13900.060710] $16   : 816b3560 00000001 816b3588 81a99320
[13900.066179] $20   : 81bf7320 818819b8 8169dcd4 80cc18c4
[13900.071639] $24   : 00000000 8001ea88
[13900.077074] $28   : 81880000 818818e0 00000000 801d85bc
[13900.082546] Hi    : 00000004
[13900.085491] Lo    : 0037eeda
[13900.088496] epc   : 8007842c put_page+0x0/0x4c
[13900.093064] ra    : 801d85bc skb_release_data+0xa8/0x10c
[13900.098434] Status: 1000b803 KERNEL EXL IE
[13900.102773] Cause : 00800010
[13900.105719] BadVA : 4a86b583
[13900.108674] PrId  : 00029007 (Broadcom BMIPS3300)
[13900.113424] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_n
ull leds_gpio ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd
 aead crc32c_generic crypto_hash
[13900.134142] Process kworker/u2:1 (pid: 8, threadinfo=81880000, task=81841550, tls=00000000)
[13900.142524] Stack : 00000020 00000000 801db418 801dabec 81bb4000 81a99320 00000000 00100100
          00200200 801d8648 00000000 00000001 81bf7320 801db498 80d75500 81b49a74
          0000000a 81a374a0 81bf7320 80cc1850 80cc1800 81bf7320 00000000 00000564
          00000001 81b49ec4 80360000 81bb8800 81bf7320 81bb4400 81bb4000 00000000
          80c8985c 0000009c 81bb8800 81bb4000 81bb4400 80cc1800 8169dcde 00000000
          ...
[13900.179481] Call Trace:
[13900.182065] [<8007842c>] put_page+0x0/0x4c
[13900.186289] [<801d85bc>] skb_release_data+0xa8/0x10c
[13900.191375] [<801d8648>] __kfree_skb+0x28/0xb4
[13900.196032] [<81b49a74>] batadv_dat_drop_broadcast_packet+0x10c/0x138 [batman_adv]
[13900.203827] [<81b49ec4>] batadv_frag_skb_buffer+0x394/0x3d8 [batman_adv]
[13900.210757] [<81b54144>] batadv_recv_frag_packet+0x244/0x2c4 [batman_adv]
[13900.217773] [<81b4e518>] batadv_batman_skb_recv+0x180/0x1f4 [batman_adv]
[13900.224673] [<801e7168>] __netif_receive_skb_core+0x620/0x6e0
[13900.230548] [<801e7ddc>] netif_receive_skb_internal+0x60/0x70
[13900.236426] [<801c0ff0>] b44_poll+0x384/0x44c
[13900.240917] [<801e81c0>] net_rx_action+0x124/0x2f0
[13900.245875] [<80024fa4>] __do_softirq+0x184/0x2b0
[13900.250735] [<80025198>] do_softirq+0x48/0x68
[13900.255247] [<80025248>] __local_bh_enable_ip+0x90/0xb0
[13900.260793] [<80c12084>] ieee80211_get_vht_mask_from_cap+0x1900/0x1b8c [mac80211]
[13900.268516]
[13900.270075]
Code: 00003021  0801e0bc  24a57840 <8c820000> 3042c000  10400003  00801821  0801df83  00000000
[13900.280781] ---[ end trace af00a3cf0771ea56 ]---
[13900.294268] Kernel panic - not syncing: Fatal exception in interrupt
[13900.306101] Rebooting in 3 seconds..
}}}
```

History

#1 - 08/26/2016 02:20 PM - Sven Eckelmann

- Assignee set to Russell Senior

Can you recompile the kernel module with

```
EXTRA_CFLAGS="$(PKG_EXTRA_CFLAGS) -fno-inline -O1 -fno-optimize-sibling-calls" \
```

in https://github.com/openwrt-routing/packages/blob/master/batman-adv/Makefile (instead of the EXTRA_CFLAGS="$(PKG_EXTRA_CFLAGS)" \). Then please install this module and try to generate a new backtrace (which hopefully should be a lot more readable).

Btw. the b44 driver had such problems in the past. Not sure if this is still the case or if this is a valid batman-adv bug.

#2 - 08/26/2016 05:39 PM - Russell Senior

I have rebuilt and reflashed with the EXTRA_CFLAGS change requested, waiting for another panic.

#3 - 08/26/2016 09:42 PM - Russell Senior

Oops'd twice this time, in quick succession, here's both:

```
[  416.609285] ------------[ cut here ]------------
[  416.614269] WARNING: CPU: 0 PID: 842 at net/core/dev.c:2359 skb_warn_bad_offload+0xc0/0xe8()
[  416.623086] : caps=(0x0000000000006200, 0x0000000000000000) len=54 data_len=0 gso_size=5774 gso_type=28513
ip_summed=0
[  416.634007] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_generic cry
pto_hash
[  416.655239] CPU: 0 PID: 842 Comm: kworker/u2:2 Not tainted 4.1.20 #0
[  416.661861] Workqueue: phy0 ieee80211_ibss_leave [mac80211]
[  416.667736] Stack : 80da2400 8035a460 802a422c 80047eb8 80cbc2c0 8035e3a3 80306f84 0000034a
          80318150 81ad762c 80da2400 800464bc 802a422c 80047eb8 80365fe4 80360000
          00000003 81ad762c 8030a634 80036654 802a422c 81ad7664 00000000 00000000
          00000000 00000000 80c13e5c 8183f200 81994500 30796870 00000000 00000000
          00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
          ...
[  416.705738] Call Trace:
[  416.708341] [<800149e8>] show_stack+0x50/0x84
[  416.713082] [<80022858>] warn_slowpath_common+0xa0/0xd0
[  416.718453] [<800228b4>] warn_slowpath_fmt+0x2c/0x38
[  416.723818] [<801e585c>] skb_warn_bad_offload+0xc0/0xe8
[  416.729183] [<801e9d2c>] __skb_gso_segment+0x50/0xf8
[  416.734512] [<801ea0c4>] validate_xmit_skb.isra.31.part.32+0xe4/0x2c8
[  416.741087] [<801ea920>] __dev_queue_xmit+0x338/0x488
[  416.746580] [<802a2914>] br_dev_queue_push_xmit+0x48/0x5c
[  416.752190] [<802a41f4>] br_handle_frame_finish+0x518/0x550
[  416.758091] [<802a44a8>] br_handle_frame+0x27c/0x2b4
[  416.763363] [<801e6ee0>] __netif_receive_skb_core+0x398/0x6e0
[  416.769242] [<801e7ddc>] netif_receive_skb_internal+0x60/0x70
[  416.775566] [<80c1f098>] ieee80211_attach_ack_skb+0xfe8/0x18b4 [mac80211]
[  416.782764]
[  416.784364] ---[ end trace a124c1fa35030a9f ]---
[  416.789234] CPU 0 Unable to handle kernel paging request at virtual address 6eb398ec, epc == 8007842c, ra =
= 801d85bc
[  416.800165] Oops[#1]:
[  416.802563] CPU: 0 PID: 842 Comm: kworker/u2:2 Tainted: G        W       4.1.20 #0
[  416.810391] Workqueue: phy0 ieee80211_ibss_leave [mac80211]
[  416.816083] task: 80cbc048 ti: 81ad6000 task.ti: 81ad6000
[  416.821530] $ 0   : 00000000 1000b800 00000001 00200000
[  416.826999] $ 4   : 6eb398ec 00010000 00006200 00000000
[  416.832460] $ 8   : 0000002d 35336166 61303330 5d206639
[  416.837922] $12   : 00000000 03bf0000 00000000 bc000000
[  416.843391] $16   : 80d2c100 00000001 80d2c128 80dcac20
[  416.848861] $20   : 00000000 80360000 80da2400 8035a460
[  416.854329] $24   : 00000003 801858ac
[  416.859763] $28   : 81ad6000 81ad7720 802a422c 801d85bc
[  416.865236] Hi    : 00000000
[  416.868181] Lo    : 00000000
[  416.871188] epc   : 8007842c put_page+0x0/0x4c
[  416.875753] ra    : 801d85bc skb_release_data+0xa8/0x10c
[  416.881123] Status: 1000b803 KERNEL EXL IE
[  416.885463] Cause : 00800008
[  416.888401] BadVA : 6eb398ec
[  416.891356] PrId  : 00029007 (Broadcom BMIPS3300)
[  416.896106] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_generic cry
pto_hash
[  416.916835] Process kworker/u2:2 (pid: 842, threadinfo=81ad6000, task=80cbc048, tls=00000000)
[  416.925386] Stack : 00000000 80360000 80da2400 8035a460 802a422c 80dcac20 ffffffea 00000000
          80d5a200 801d8648 0000000e 8035b528 80dcac20 00000000 80dcac20 801ea0dc
          ff4c382f 00000060 8035da40 00000141 00000001 80942c20 80d52000 80360000
          80dcac20 80d52000 80d5a200 81aa8000 80360000 801ea920 ffffffff 80360000
          00000141 81ad77b4 81a9e0c8 8003cc78 00000000 fffffff4 00000001 80dcac20
          ...
[  416.962507] Call Trace:
[  416.965087] [<8007842c>] put_page+0x0/0x4c
[  416.969306] [<801d85bc>] skb_release_data+0xa8/0x10c
[  416.974389] [<801d8648>] __kfree_skb+0x28/0xb4
```

```
[  416.978974] [<801ea0dc>] validate_xmit_skb.isra.31.part.32+0xfc/0x2c8
[  416.985539] [<801ea920>] __dev_queue_xmit+0x338/0x488
[  416.990757] [<802a2914>] br_dev_queue_push_xmit+0x48/0x5c
[  416.996275] [<802a41f4>] br_handle_frame_finish+0x518/0x550
[  417.001956] [<802a44a8>] br_handle_frame+0x27c/0x2b4
[  417.007044] [<801e6ee0>] __netif_receive_skb_core+0x398/0x6e0
[  417.012905] [<801e7ddc>] netif_receive_skb_internal+0x60/0x70
[  417.018965] [<80c1f098>] ieee80211_attach_ack_skb+0xfe8/0x18b4 [mac80211]
[  417.025996]
[  417.027553]
Code: 00003021  0801e0bc  24a57840 <8c820000> 3042c000  10400003  00801821  0801df83  00000000
[  417.038258] ---[ end trace a124c1fa35030aa0 ]---
[  417.051960] Kernel panic - not syncing: Fatal exception in interrupt
[  417.064164] Rebooting in 3 seconds..^@^@
```

#4 - 08/26/2016 09:55 PM - Russell Senior

Also, this one:

```
[  747.768349] CPU 0 Unable to handle kernel paging request at virtual address 00000004, epc == 801433f4, ra =
= 80144770
[  747.779026] Oops[#1]:
[  747.781401] CPU: 0 PID: 6 Comm: kworker/u2:0 Not tainted 4.1.20 #0
[  747.787849] Workqueue: phy0 ieee80211_ibss_leave [mac80211]
[  747.793538] task: 8182f028 ti: 8183c000 task.ti: 8183c000
[  747.798986] $ 0   : 00000000 10003800 81821e20 00000000
[  747.804439] $ 4   : 8035d410 8035d254 00000000 00000000
[  747.809899] $ 8   : fffffffc 00000000 1b294900 1b294900
[  747.815361] $12   : 000000ae 000135f6 00000000 0000000f
[  747.820813] $16   : 8035d410 8035d254 000000ae 00000003
[  747.826265] $20   : 8035d210 00000000 00000001 000000ae
[  747.831726] $24   : 00000000 8001ea88
[  747.837160] $28   : 8183c000 8183d658 1a9117a1 80144770
[  747.842633] Hi    : 00000000
[  747.845577] Lo    : 000135f6
[  747.848595] epc   : 801433f4 rb_insert_color+0x2c/0x14c
[  747.853954] ra    : 80144770 timerqueue_add+0xbc/0x114
[  747.859150] Status: 10003802 KERNEL EXL
[  747.863205] Cause : 00800008
[  747.866149] BadVA : 00000004
[  747.869097] PrId  : 00029007 (Broadcom BMIPS3300)
[  747.873847] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_ge
neric crypto_hash
[  747.894565] Process kworker/u2:0 (pid: 6, threadinfo=8183c000, task=8182f028, tls=00000000)
[  747.902946] Stack : 000000ae 00000003 8035d210 00000000 8035d410 8035d248 000000ae 800505b0
          00000000 80361ce8 ffffffff 80360000 80360000 8035d210 1a9117a1 80050b24
          00000000 81bf31a0 1000b801 803e0000 81a39600 1a9117a1 000000ae 7fffffff
          80360000 80360000 80360000 80360000 ffffffff 7fffffff 1a9117a1 000000ae
          00000000 00000007 00000000 80361ce8 00000000 8102f9a0 8030a7d8 8030a800
          ...
[  747.939938] Call Trace:
[  747.942528] [<801433f4>] rb_insert_color+0x2c/0x14c
[  747.947560] [<80144770>] timerqueue_add+0xbc/0x114
[  747.952512] [<800505b0>] __run_hrtimer.isra.3+0x7c/0xf8
[  747.957893] [<80050b24>] hrtimer_interrupt+0x168/0x324
[  747.963192] [<8001760c>] c0_compare_interrupt+0x74/0x9c
[  747.968540] [<80049174>] handle_irq_event_percpu+0x64/0x188
[  747.974231] [<8004bfbc>] handle_percpu_irq+0x54/0x84
[  747.979359] [<80048aec>] generic_handle_irq+0x2c/0x40
```

```
[  747.984551] [<80011e10>] do_IRQ+0x1c/0x2c
[  747.988684] [<8000acbc>] plat_irq_dispatch+0x40/0x17c
[  747.993848] [<80001048>] ret_from_irq+0x0/0x4
[  747.998333] [<800056b0>] __copy_user_common+0x248/0x2d8
[  748.003696] [<801d8adc>] skb_copy_ubufs+0xec/0x1f8
[  748.008617] [<801e7178>] __netif_receive_skb_core+0x630/0x6e0
[  748.014488] [<801e7ddc>] netif_receive_skb_internal+0x60/0x70
[  748.020363] [<801c0ff0>] b44_poll+0x384/0x44c
[  748.024847] [<801e81c0>] net_rx_action+0x124/0x2f0
[  748.029797] [<80024fa4>] __do_softirq+0x184/0x2b0
[  748.034648] [<80025198>] do_softirq+0x48/0x68
[  748.039159] [<80025248>] __local_bh_enable_ip+0x90/0xb0
[  748.044617] [<81b090c8>] cfg80211_get_bss+0xaa8/0xc98 [cfg80211]
[  748.050775]
[  748.052331]
Code: 30660001  14c00047  00000000 <8c660004> 10460016  00000000  10c00005  00000000  8cc70000
[  748.062779] ---[ end trace f808cc0c2b50a418 ]---
[  748.075998] Kernel panic - not syncing: Fatal exception in interrupt
[  748.087889] Rebooting in 3 seconds..^@
```

#5 - 08/26/2016 10:09 PM - Sven Eckelmann

Ok, these look like the b44 problems which can be found in the OpenWrt forums/mailing lists/tickets - even without batman-adv

#6 - 08/28/2016 05:00 AM - Russell Senior

```
[58709.642612] CPU 0 Unable to handle kernel paging request at virtual address 0e28e4c4, epc == 8007842c, ra =
= 801d85bc
[58709.653550] Oops[#1]:
[58709.655943] CPU: 0 PID: 6 Comm: kworker/u2:0 Not tainted 4.1.20 #0
[58709.662296] Workqueue: bat_events batadv_send_outstanding_bat_ogm_packet [batman_adv]
[58709.670231] task: 8182f028 ti: 8183c000 task.ti: 8183c000
[58709.675678] $ 0   : 00000000 1000b800 00000001 00200000
[58709.681148] $ 4   : 0e28e4c4 00010000 005920d9 ffffffff
[58709.686616] $ 8   : 00000000 00000000 00000000 00600543
[58709.692070] $12   : 00000008 0000707f 00000000 00000000
[58709.697522] $16   : 80afe8c0 00000001 80afe8e8 81a900e0
[58709.702992] $20   : 803b5dcc 00000002 00000008 0000000a
[58709.708443] $24   : 00000000 8001ea88
[58709.713878] $28   : 8183c000 8183dca0 00000101 801d85bc
[58709.719349] Hi    : 00000001
[58709.722294] Lo    : 00000001
[58709.725303] epc   : 8007842c put_page+0x0/0x4c
[58709.729866] ra    : 801d85bc skb_release_data+0xa8/0x10c
[58709.735236] Status: 1000b803 KERNEL EXL IE
[58709.739576] Cause : 00800008
[58709.742522] BadVA : 0e28e4c4
[58709.745478] PrId  : 00029007 (Broadcom BMIPS3300)
[58709.750227] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_ge
neric crypto_hash
[58709.770952] Process kworker/u2:0 (pid: 6, threadinfo=8183c000, task=8182f028, tls=00000000)
[58709.779334] Stack : 00000000 81be0c94 00d20fc0 4817008c ff070000 81a900e0 81a900e0 803314fc
```

```
          80f8ee60 801d8648 80360000 8035dfe0 814fa860 803314fc 8035dfe0 801e6838
          8183dce0 8183dce0 00000009 00000002 803b5dd0 00000001 803b5dd4 00000013
          803b0000 80024fa4 8035d1a0 8030ce94 1000b801 00000000 80cc4000 80cc50f0
          00000000 04208060 005920d9 80360000 80310000 803b5dcc 8035d1a0 8030ce94
          ...
[58709.816283] Call Trace:
[58709.818863] [<8007842c>] put_page+0x0/0x4c
[58709.823092] [<801d85bc>] skb_release_data+0xa8/0x10c
[58709.828176] [<801d8648>] __kfree_skb+0x28/0xb4
[58709.832747] [<801e6838>] net_tx_action+0xd8/0x140
[58709.837607] [<80024fa4>] __do_softirq+0x184/0x2b0
[58709.842459] [<80025198>] do_softirq+0x48/0x68
[58709.846971] [<80025248>] __local_bh_enable_ip+0x90/0xb0
[58709.852384] [<81b00da4>] 0x81b00da4
[58709.855998]
[58709.857561]
Code: 00003021  0801e0bc  24a57840 <8c820000> 3042c000  10400003  00801821  0801df83  00000000
[58709.868242] ---[ end trace a124c1fa35030a9f ]---
[58709.881448] Kernel panic - not syncing: Fatal exception in interrupt
[58709.893085] Rebooting in 3 seconds..^@^@
```

#7 - 08/28/2016 08:41 AM - Sven Eckelmann

Did you try to contact the b44/LEDE/OpenWrt developers regarding your latest backtraces?

#8 - 08/28/2016 03:01 PM - Russell Senior

Sven Eckelmann wrote:

> Ok, these look like the b44 problems which can be found in the OpenWrt forums/mailing lists/tickets - even without batman-adv

Can you point me at one of these? My searches have been thus far unfruitful. Thanks!

#9 - 08/28/2016 03:24 PM - Sven Eckelmann

Just did a quick search for Broadcom "b44" "Unable to handle kernel paging request at" site:openwrt.org and this came up:

- https://lists.openwrt.org/pipermail/openwrt-devel/2014-July/026788.html * https://dev.openwrt.org/ticket/11091 * https://dev.openwrt.org/ticket/7552#comment:63

Maybe there are more relevant ones but I only did a quick search for things which are not yet closed/solved.

#10 - 08/28/2016 10:30 PM - Russell Senior

```
[51385.521222] Unhandled kernel unaligned access[#1]:
[51385.526133] CPU: 0 PID: 826 Comm: hostapd Not tainted 4.1.20 #0
[51385.532132] task: 8188d088 ti: 80dc6000 task.ti: 80dc6000
[51385.537579] $ 0   : 00000000 1000b800 00000001 00200000
[51385.543049] $ 4   : 14a1fd2b 00010000 00000001 deadbef5
[51385.548518] $ 8   : 80d7d900 48c6b143 81962308 058057d4
[51385.553988] $12   : deadbef5 00000fb5 00007eba fb655fdc
[51385.559456] $16   : 80f4c640 00000001 80f4c668 80d5a020
[51385.564926] $20   : 80f451a0 80e7a8f0 80dc785c 8035a460
[51385.570395] $24   : 00000000 8001ea88
[51385.575838] $28   : 80dc6000 80dc7788 00000000 801d85bc
[51385.581312] Hi    : 00000004
[51385.584256] Lo    : 0037eeda
[51385.587273] epc   : 8007842c put_page+0x0/0x4c
[51385.591834] ra    : 801d85bc skb_release_data+0xa8/0x10c
[51385.597206] Status: 1000b803 KERNEL EXL IE
[51385.601546] Cause : 00800010
[51385.604490] BadVA : 14a1fd2b
[51385.607447] PrId  : 00029007 (Broadcom BMIPS3300)
[51385.612197] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_generic cry
pto_hash
[51385.632925] Process hostapd (pid: 826, threadinfo=80dc6000, task=8188d088, tls=77857e50)
[51385.641054] Stack : 0000bf31 800736f0 80361ce8 00010220 00000020 80d5a020 00000000 00200200
          00100100 801d8648 815fa872 81b9c580 80da89e0 815fa872 80dd3300 81b8b654
          80da89e0 815fa872 80da89e0 815fa872 80d56000 80d69e94 00003fba 80d69e94
          80d69e00 81b8b6ac 00000040 0000000a 80da89e0 80dc7898 0000ba3f 81ac1280
          00000002 81b8b77c 8035a460 81b974fc 80dc785c 81b8bb98 0000000a 80dc7898
          ...
[51385.678201] Call Trace:
[51385.680788] [<8007842c>] put_page+0x0/0x4c
[51385.685017] [<801d85bc>] skb_release_data+0xa8/0x10c
[51385.690103] [<801d8648>] __kfree_skb+0x28/0xb4
[51385.694762] [<81b8b654>] batadv_dat_drop_broadcast_packet+0x14c/0x7a4 [batman_adv]
[51385.702563] [<81b8b6ac>] batadv_dat_drop_broadcast_packet+0x1a4/0x7a4 [batman_adv]
[51385.710363] [<81b974fc>] batadv_recv_unicast_packet+0x308/0x3cc [batman_adv]
[51385.717647] [<81b8bd6c>] batadv_frag_skb_buffer+0x24/0x68 [batman_adv]
[51385.724413] [<81b979e4>] batadv_recv_frag_packet+0x280/0x2fc [batman_adv]
[51385.731436] [<81b91090>] batadv_batman_skb_recv+0x164/0x214 [batman_adv]
[51385.738332] [<801e7168>] __netif_receive_skb_core+0x620/0x6e0
[51385.744206] [<801e7ddc>] netif_receive_skb_internal+0x60/0x70
[51385.750083] [<801c0ff0>] b44_poll+0x384/0x44c
[51385.754575] [<801e81c0>] net_rx_action+0x124/0x2f0
[51385.759534] [<80024fa4>] __do_softirq+0x184/0x2b0
[51385.764392] [<80025198>] do_softirq+0x48/0x68
[51385.768905] [<80025248>] __local_bh_enable_ip+0x90/0xb0
[51385.774288] [<8029ce6c>] packet_poll+0xfc/0x114
[51385.778968] [<801d0904>] sock_poll+0xfc/0x11c
[51385.783468] [<800b2e30>] do_select+0x2dc/0x5a8
[51385.788046] [<800b32c0>] core_sys_select+0x1c4/0x314
[51385.793141] [<800b34dc>] SyS_select+0xcc/0x108
[51385.797717] [<800033c8>] handle_sys+0x128/0x14c
[51385.802330]
[51385.803881]
Code: 00003021  0801e0bc  24a57840 <8c820000> 3042c000  10400003  00801821  0801df83  00000000
[51385.814571] ---[ end trace 014d0b7d6b98ab3a ]---
[51385.828193] Kernel panic - not syncing: Fatal exception in interrupt
[51385.840123] Rebooting in 3 seconds..
```

#11 - 08/29/2016 07:08 AM - Russell Senior

```
[32408.475855] ------------[ cut here ]------------
[32408.480855] WARNING: CPU: 0 PID: 6 at net/core/dev.c:2359 skb_warn_bad_offload+0xc0/0xe8()
[32408.489505] : caps=(0x0000000000006200, 0x0000000000000000) len=86 data_len=0 gso_size=24576 gso_type=48128
 ip_summed=0
[32408.500528] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_ge
neric crypto_hash
[32408.521768] CPU: 0 PID: 6 Comm: kworker/u2:0 Not tainted 4.1.20 #0
[32408.528322] Workqueue: bat_events batadv_send_outstanding_bat_ogm_packet [batman_adv]
[32408.536338] Stack : 80db2c00 8035a460 802a422c 80047eb8 8182f2a0 8035e3a3 80306f84 00000006
          80318150 8183d81c 80db2c00 800464bc 802a422c 80047eb8 80365fe4 80360000
          00000003 8183d81c 8030a634 80036654 802a422c 8183d854 00000000 00000000
          00000000 00000000 81b98a80 8183f100 81998000 5f746162 6e657665 00007374
          00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
          ...
[32408.574265] Call Trace:
[32408.576874] [<800149e8>] show_stack+0x50/0x84
[32408.581620] [<80022858>] warn_slowpath_common+0xa0/0xd0
[32408.587286] [<800228b4>] warn_slowpath_fmt+0x2c/0x38
[32408.592398] [<801e585c>] skb_warn_bad_offload+0xc0/0xe8
[32408.597989] [<801e9d2c>] __skb_gso_segment+0x50/0xf8
[32408.603099] [<801ea0c4>] validate_xmit_skb.isra.31.part.32+0xe4/0x2c8
[32408.609900] [<801ea920>] __dev_queue_xmit+0x338/0x488
[32408.615212] [<802a2914>] br_dev_queue_push_xmit+0x48/0x5c
[32408.620957] [<802a41f4>] br_handle_frame_finish+0x518/0x550
[32408.626647] [<802a44a8>] br_handle_frame+0x27c/0x2b4
[32408.631961] [<801e6ee0>] __netif_receive_skb_core+0x398/0x6e0
[32408.638116] [<801e7ddc>] netif_receive_skb_internal+0x60/0x70
[32408.644192] [<80c1f098>] ieee80211_attach_ack_skb+0xfe8/0x18b4 [mac80211]
[32408.651444]
[32408.653047] ---[ end trace 1064c52c54737b51 ]---
[32408.658016] CPU 0 Unable to handle kernel paging request at virtual address 00008000, epc == 801d8738, ra =
= 801d8740
[32408.668948] Oops[#1]:
[32408.671347] CPU: 0 PID: 6 Comm: kworker/u2:0 Tainted: G        W       4.1.20 #0
[32408.678903] Workqueue: bat_events batadv_send_outstanding_bat_ogm_packet [batman_adv]
[32408.686839] task: 8182f028 ti: 8183c000 task.ti: 8183c000
[32408.692287] $ 0   : 00000000 00000001 00000000 00200000
[32408.697755] $ 4   : 00008000 00010000 00006200 00000000
[32408.703215] $ 8   : 0000002d 34356332 62373337 5d203135
[32408.708668] $12   : 00000000 03bf0000 00000000 bc000000
[32408.714139] $16   : 80a76020 00000000 80a76048 80cd6ce0
[32408.719607] $20   : 00000000 80360000 80db2c00 8035a460
[32408.725067] $24   : 00000003 801858ac
[32408.730503] $28   : 8183c000 8183d8f8 802a422c 801d8740
[32408.735968] Hi    : 00000000
[32408.738910] Lo    : 00000000
[32408.741912] epc   : 801d8738 kfree_skb_list+0x14/0x30
[32408.747071] ra    : 801d8740 kfree_skb_list+0x1c/0x30
[32408.752181] Status: 1000b803 KERNEL EXL IE
[32408.756522] Cause : 80800008
[32408.759465] BadVA : 00008000
[32408.762422] PrId  : 00029007 (Broadcom BMIPS3300)
[32408.767173] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_generic cry
pto_hash
[32408.787898] Process kworker/u2:0 (pid: 6, threadinfo=8183c000, task=8182f028, tls=00000000)
[32408.796280] Stack : 00000000 803112a8 80d64088 803379b8 80a76020 801d8600 00006200 00000000
          00000000 80360000 80db2c00 80cd6ce0 ffffffea 00000000 80da3d80 801d8648
          0000000e 8035c650 80cd6ce0 00000000 80cd6ce0 801ea0dc e0d10f3e 00001d79
          8035d410 8035d248 00000001 80cd6560 80d64000 80360000 80cd6ce0 80d64000
          80da3d80 81ac7000 80360000 801ea920 ffffffff 80360000 00000000 8183d9a4
          ...
[32408.833246] Call Trace:
[32408.835821] [<801d8738>] kfree_skb_list+0x14/0x30
[32408.840652] [<801d8600>] skb_release_data+0xec/0x10c
[32408.845732] [<801d8648>] __kfree_skb+0x28/0xb4
[32408.850321] [<801ea0dc>] validate_xmit_skb.isra.31.part.32+0xfc/0x2c8
[32408.856894] [<801ea920>] __dev_queue_xmit+0x338/0x488
[32408.862109] [<802a2914>] br_dev_queue_push_xmit+0x48/0x5c
[32408.867626] [<802a41f4>] br_handle_frame_finish+0x518/0x550
[32408.873309] [<802a44a8>] br_handle_frame+0x27c/0x2b4
```

```
[32408.878404] [<801e6ee0>] __netif_receive_skb_core+0x398/0x6e0
[32408.884276] [<801e7ddc>] netif_receive_skb_internal+0x60/0x70
[32408.890343] [<80c1f098>] ieee80211_attach_ack_skb+0xfe8/0x18b4 [mac80211]
[32408.897378]
[32408.898940]
Code: afb00010  10800005  8fbf0014 <0c0761b5> 8c900000  1000fffb  02002021  8fb00010  03e00008
[32408.909614] ---[ end trace 1064c52c54737b52 ]---
[32408.923668] Kernel panic - not syncing: Fatal exception in interrupt
[32408.936110] Rebooting in 3 seconds..
```

#12 - 08/29/2016 08:55 AM - Sven Eckelmann

Thanks for all the backtraces. But just to clarify: this cannot be fixed in batman-adv when the bug is in b44.

#13 - 08/29/2016 07:19 PM - Russell Senior

```
[42519.105615] Data bus error, epc == 80016d28, ra == 80001020
[42519.111282] Oops[#1]:
[42519.113666] CPU: 0 PID: 6 Comm: kworker/u2:0 Not tainted 4.1.20 #0
[42519.120123] Workqueue: phy0 ieee80211_ibss_leave [mac80211]
[42519.125812] task: 8182f028 ti: 8183c000 task.ti: 8183c000
[42519.131261] $ 0   : 00000000 1000b800 00000000 8183c000
[42519.136736] $ 4   : ab5a6406 00000000 00000001 deadbef5
[42519.142206] $ 8   : 1000b801 1000001e 81962308 b4e751e1
[42519.147677] $12   : a56395a8 00000fb5 00000000 aec6d36b
[42519.153145] $16   : 8183d7f8 8c820000 ab5a6402 8007842c
[42519.158615] $20   : 00000000 801d85bc 8183d984 8035a460
[42519.164076] $24   : 00000000 8001ea88
[42519.169528] $28   : 8183c000 8183d7c8 00000000 80001020
[42519.175010] Hi    : 0000023e
[42519.177954] Lo    : 000a173a
[42519.180982] epc   : 80016d28 do_ade+0x578/0x91c
[42519.185625] ra    : 80001020 ret_from_exception+0x0/0x28
[42519.190999] Status: 1000b803 KERNEL EXL IE
[42519.195339] Cause : 0080001c
[42519.198295] PrId  : 00029007 (Broadcom BMIPS3300)
[42519.203043] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_ge
neric crypto_hash
[42519.223769] Process kworker/u2:0 (pid: 6, threadinfo=8183c000, task=8182f028, tls=00000000)
[42519.232151] Stack : 80d58620 80c97800 80bba7dc 80bba7e6 80f2b0e0 00000001 80f2b108 80cc8f20
          81af6aa0 80b91d50 8183d984 80001020 80d59400 80c97800 80d59400 80d58620
          0fb50f00 0000cb2b 00000000 80d59400 00000000 1000b800 00000001 00200000
          ab5a6402 00010000 00000001 deadbef5 80d95f80 59bc51bb 81962308 b4e751e1
          a56395a8 00000fb5 00000000 aec6d36b 80f2b0e0 00000001 80f2b108 80cc8f20
          ...
[42519.269212] Call Trace:
[42519.271813] [<80016d28>] do_ade+0x578/0x91c
[42519.276121] [<80001020>] ret_from_exception+0x0/0x28
[42519.281221] [<8007842c>] put_page+0x0/0x4c
[42519.285445] [<801d85bc>] skb_release_data+0xa8/0x10c
[42519.290530] [<801d8648>] __kfree_skb+0x28/0xb4
[42519.295190] [<81b8b654>] batadv_dat_drop_broadcast_packet+0x14c/0x7a4 [batman_adv]
[42519.302991] [<81b8b6ac>] batadv_dat_drop_broadcast_packet+0x1a4/0x7a4 [batman_adv]
[42519.310792] [<81b974fc>] batadv_recv_unicast_packet+0x308/0x3cc [batman_adv]
[42519.318074] [<81b8bd6c>] batadv_frag_skb_buffer+0x24/0x68 [batman_adv]
[42519.324841] [<81b979e4>] batadv_recv_frag_packet+0x280/0x2fc [batman_adv]
[42519.331863] [<81b91090>] batadv_batman_skb_recv+0x164/0x214 [batman_adv]
[42519.338760] [<801e7168>] __netif_receive_skb_core+0x620/0x6e0
[42519.344636] [<801e7ddc>] netif_receive_skb_internal+0x60/0x70
[42519.350511] [<801c0ff0>] b44_poll+0x384/0x44c
[42519.355005] [<801e81c0>] net_rx_action+0x124/0x2f0
[42519.359963] [<80024fa4>] __do_softirq+0x184/0x2b0
```

```
[42519.364822] [<80025198>] do_softirq+0x48/0x68
[42519.369335] [<80025248>] __local_bh_enable_ip+0x90/0xb0
[42519.374881] [<80c12084>] ieee80211_get_vht_mask_from_cap+0x1900/0x1b8c [mac80211]
[42519.382601]
[42519.384163]
Code: 00851024  144000ba  00000000 <8a560003> 9a560000  24120000  1000000b  00000000  26440002
[42519.394878] ---[ end trace 27968d5caaf56c64 ]---
[42519.408448] Kernel panic - not syncing: Fatal exception in interrupt
[42519.420336] Rebooting in 3 seconds..
```

#14 - 08/30/2016 02:16 AM - Russell Senior

```
[ 2588.558252] Unhandled kernel unaligned access[#1]:
[ 2588.563164] CPU: 0 PID: 811 Comm: hostapd Not tainted 4.1.20 #0
[ 2588.569162] task: 80db8a78 ti: 80d72000 task.ti: 80d72000
[ 2588.574607] $ 0   : 00000000 1000b800 00000001 00200000
[ 2588.580079] $ 4   : e51454fb 00010000 00020000 000000c3
[ 2588.585547] $ 8   : deadbef3 7c4e0000 00000005 6c604830
[ 2588.591017] $12   : ff030160 0000707f 00000000 00000000
[ 2588.596486] $16   : 81f7f4e0 00000001 81f7f508 81370620
[ 2588.601955] $20   : 00000002 00000040 81370620 80d73874
[ 2588.607416] $24   : 00000000 8001ea88
[ 2588.612851] $28   : 80d72000 80d73798 81ad0b20 801d85bc
[ 2588.618324] Hi    : 00000000
[ 2588.621267] Lo    : 00000880
[ 2588.624279] epc   : 8007842c put_page+0x0/0x4c
[ 2588.628841] ra    : 801d85bc skb_release_data+0xa8/0x10c
[ 2588.634210] Status: 1000b803 KERNEL EXL IE
[ 2588.638549] Cause : 00800010
[ 2588.641495] BadVA : e51454fb
[ 2588.644443] PrId  : 00029007 (Broadcom BMIPS3300)
[ 2588.649191] Modules linked in: ath5k mac80211 ath batman_adv libcrc32c cfg80211 compat crypto_null leds_gpi
o ehci_platform ehci_hcd gpio_button_hotplug usbcore nls_base usb_common crc16 ssb_hcd aead crc32c_ge
neric crypto_hash
[ 2588.669921] Process hostapd (pid: 811, threadinfo=80d72000, task=80db8a78, tls=77c12e50)
[ 2588.678040] Stack : 00000050 00000000 00000020 8009d8e8 81f7eb98 81370620 81f7eb80 00000050
          819d8400 801d8648 00000002 00000040 81370620 80d73874 80d738c4 80c20ae0
          80d3b800 80360000 81d72aa0 00000020 00000050 00000000 00000000 801dacdc
          00000001 80bbbce0 00000012 80c53fd4 80c60000 80c53fa0 00000040 80cb5400
          00000050 80c5402c 81370620 81d72aa0 81f7eb80 80d738c4 81370620 819d8400
          ...
[ 2588.715066] Call Trace:
[ 2588.717646] [<8007842c>] put_page+0x0/0x4c
[ 2588.721866] [<801d85bc>] skb_release_data+0xa8/0x10c
[ 2588.726951] [<801d8648>] __kfree_skb+0x28/0xb4
[ 2588.731717] [<80c20ae0>] ieee80211_sta_uapsd_trigger+0xca0/0x2df4 [mac80211]
[ 2588.739009]
[ 2588.740568]
Code: 00003021  0801e0bc  24a57840 <8c820000> 3042c000  10400003  00801821  0801df83  00000000
[ 2588.751239] ---[ end trace d2c4e43577120eb1 ]---
[ 2588.764157] Kernel panic - not syncing: Fatal exception in interrupt
[ 2588.775546] Rebooting in 3 seconds..
```

#15 - 08/30/2016 11:10 AM - Russell Senior

I managed to reproduce a panic without batman-adv, reported to LEDE Project here: https://bugs.lede-project.org/index.php?do=details&task_id=126

Sorry to bother you all.

#16 - 08/30/2016 11:22 AM - Sven Eckelmann

- Status changed from New to Rejected

Thanks for taking care of it :)