batman-adv - Bug #417

BLA, crash: null pointer dereference in batadv_bla_loopdetect_report()->batadv_bit_get_packet()

08/27/2020 10:07 AM - Linus Lüssing

Status:	New	**Start date:**	08/27/2020
Priority:	Normal	**Due date:**	
Assignee:	batman-adv developers	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Version:

```
$ batctl -v
batctl 2020.2-openwrt-1 [batman-adv: 2020.2-openwrt-1]
```

Setup:

8 nodes, 3 of those interconnected on the LAN with BLA. Two of the three LAN devices crashed after about 15 hours with the following trace:

```
Time: 1598432655.394152
Modules:        pppoe@bf627000+5000     ppp_async@bf61e000+5000 batman_adv@bf5e6000+2c000       at
h10k_pci@bf5d5000+b000        ath10k_core@bf55b000+67000      ath@bf552000+6000       pppox@bf54a0
00+4000     ppp_generic@bf53d000+8000       nft_set_rbtree@bf535000+4000    nft_set_hash@bf52b000+
6000      nft_reject_ipv6@bf523000+4000 nft_reject_ipv4@bf51b000+4000   nft_reject_inet@bf513000+4
000   nft_reject_bridge@bf50b000+4000 nft_reject@bf504000+4000        nft_redir@bf4fd000+4000 nft_
quota@bf4f5000+4000 nft_numgen@bf4ed000+4000        nft_meta_bridge@bf4e5000+4000   nft_meta@bf4dd
000+4000  nft_log@bf4d5000+4000   nft_limit@bf4cd000+4000       nft_fwd_netdev@bf4c5000+4000    nf
t_exthdr@bf4bd000+4000        nft_dup_netdev@bf4b5000+4000    nft_ct@bf4ad000+4000    nft_counter@
bf4a5000+4000       nft_chain_route_ipv6@bf49d000+4000      nft_chain_route_ipv4@bf495000+4000
  nf_tables_netdev@bf48d000+4000  nf_tables_ipv6@bf485000+4000    nf_tables_ipv4@bf47d000+4000  nf
_tables_inet@bf475000+4000    nf_tables_bridge@bf46d000+4000  nf_tables@bf453000+14000        mac8
0211@bf3ae000+7e000 iptable_nat@bf3a6000+4000       ipt_REJECT@bf39e000+4000        ipt_MASQUERADE
@bf396000+4000    cfg80211@bf345000+44000 xt_time@bf33d000+4000   xt_tcpudp@bf335000+4000 xt_tcpms
s@bf32d000+4000       xt_statistic@bf325000+4000      xt_state@bf31d000+4000  xt_nat@bf315000+4000
    xt_multiport@bf30d000+4000      xt_mark@bf305000+4000   xt_mac@bf2fd000+4000    xt_limit@bf2f5
000+4000  xt_length@bf2ed000+4000 xt_hl@bf2e5000+4000     xt_ecn@bf2dd000+4000    xt_dscp@bf2d5000
+4000   xt_conntrack@bf2cd000+4000    xt_comment@bf2c5000+4000        xt_TCPMSS@bf2bd000+4000 xt_R
EDIRECT@bf2b5000+4000       xt_LOG@bf2ad000+4000    xt_HL@bf2a5000+4000     xt_FLOWOFFLOAD@bf29d00
0+4000    xt_DSCP@bf295000+4000   xt_CLASSIFY@bf28d000+4000       slhc@bf286000+4000      openvswi
tch@bf265000+1a000      nfnetlink@bf25c000+4000       nf_reject_ipv4@bf255000+4000    nf_nat_redir
ect@bf24e000+4000   nf_nat_masquerade_ipv6@bf247000+4000    nf_nat_masquerade_ipv4@bf240000+4000
  nf_conntrack_ipv6@bf238000+4000 nf_nat_ipv6@bf230000+4000       nf_conntrack_ipv4@bf228000+4000
nf_nat_ipv4@bf220000+4000       nf_nat@bf215000+6000    nf_log_ipv4@bf20d000+4000     nf_flow_tabl
e_hw@bf205000+4000  nf_flow_table@bf1fa000+6000     nf_dup_netdev@bf1f3000+4000     nf_defrag_ipv6
@bf1eb000+4000    nf_defrag_ipv4@bf1e3000+4000    nf_conntrack_rtcache@bf1db000+4000      nf_connt
rack@bf1c2000+11000     libcrc32c@bf1ba000+4000 iptable_mangle@bf1b2000+4000    iptable_filter@bf1
aa000+4000  ipt_ECN@bf1a2000+4000   ip_tables@bf198000+6000 crc_ccitt@bf191000+4000 compat@bf18800
0+5000    ledtrig_usbport@bf180000+4000   nf_log_ipv6@bf178000+4000       nf_log_common@bf170000+4
000     ip6table_mangle@bf168000+4000   ip6table_filter@bf160000+4000   ip6_tables@bf156000+6000
      ip6t_REJECT@bf14e000+4000     x_tables@bf143000+6000  nf_reject_ipv6@bf13c000+4000    mpls_i
ptunnel@bf134000+4000     mpls_router@bf128000+7000       mpls_gso@bf120000+4000  leds_gpio@bf1180
00+4000 xhci_plat_hcd@bf10f000+4000     xhci_pci@bf106000+4000  xhci_hcd@bf0e7000+18000 dwc3@bf0db
000+7000      dwc3_of_simple@bf0d3000+4000 ohci_platform@bf0ca000+4000      ohci_hcd@bf0bd000+8000
  phy_qcom_dwc3@bf0b5000+4000     ahci@bf0ab000+6000      ehci_platform@bf0a2000+4000     sd_mod@b
f094000+9000    ahci_platform@bf08c000+4000     libahci_platform@bf085000+4000  libahci@bf07a000+7
000   libata@bf046000+27000   scsi_mod@bf020000+1a000 ehci_hcd@bf010000+b000        gpio_button_ho
tplug@bf008000+4000       crc32c_generic@bf000000+4000
<3>[   21.105247] ath10k_pci 0002:01:00.0: DANGER! You're overriding EEPROM-defined regulatory dom
```

```
ain
<3>[   21.105294] ath10k_pci 0002:01:00.0: from: 0x0 to 0x348 (svc-ready-work)
<3>[   21.112758] ath10k_pci 0002:01:00.0: Your card was not certified to operate in the domain yo
u chose.
<3>[   21.119792] ath10k_pci 0002:01:00.0: This might result in a violation of your local regulato
ry rules.
<3>[   21.128906] ath10k_pci 0002:01:00.0: Do not ever do this unless you really know what you are
 doing!
<4>[   21.139581] ath10k_pci 0002:01:00.0: 10.4 wmi init: vdevs: 8  peers: 180  tid: 450
<6>[   21.146922] ath10k_pci 0002:01:00.0: using 7 firmware rate-ctrl objects
<4>[   21.154531] ath10k_pci 0002:01:00.0: msdu-desc: 2200  skid: 360
<6>[   21.237597] ath10k_pci 0002:01:00.0: wmi print 'P 180/180 V 8 K 540 PH 556 T 656  msdu-desc:
 2200  sw-crypt: 0 ct-sta: 0'
<6>[   21.238894] ath10k_pci 0002:01:00.0: wmi print 'free: 11368 iram: 8424 sram: 512'
<6>[   21.405609] ath10k_pci 0002:01:00.0: htt-ver 2.2 wmi-op 6 htt-op 4 cal pre-cal-file max-sta
180 raw 0 hwcrypto 1
<7>[   21.626332] ath: EEPROM regdomain: 0x8348
<7>[   21.626345] ath: EEPROM indicates we should expect a country code
<7>[   21.626364] ath: doing EEPROM country->regdmn map search
<7>[   21.626377] ath: country maps to regdmn code: 0x3a
<7>[   21.626391] ath: Country alpha2 being used: US
<7>[   21.626401] ath: Regpair used: 0x3a
<6>[   21.638889] batman_adv: B.A.T.M.A.N. advanced 2020.2-openwrt-1 (compatibility version 15) lo
aded
<14>[   21.641464] kmodloader: done loading kernel modules from /etc/modules.d/*
<6>[   24.336245] Atheros 8031 ethernet gpio-0:00: attached PHY driver [Atheros 8031 ethernet] (mi
i_bus:phy_addr=gpio-0:00, irq=POLL)
<6>[   24.337418] dwmac1000: Master AXI performs any burst length
<6>[   24.346656] ipq806x-gmac-dwmac 37600000.ethernet eth1: IEEE 1588-2008 Advanced Timestamp sup
ported
<6>[   24.352226] ipq806x-gmac-dwmac 37600000.ethernet eth1: registered PTP clock
<6>[   24.365549] br-lan: port 1(eth1) entered blocking state
<6>[   24.367972] br-lan: port 1(eth1) entered disabled state
<6>[   24.374348] IPv6: ADDRCONF(NETDEV_UP): br-lan: link is not ready
<6>[   24.506123] Atheros 8031 ethernet gpio-0:01: attached PHY driver [Atheros 8031 ethernet] (mi
i_bus:phy_addr=gpio-0:01, irq=POLL)
<6>[   24.513244] dwmac1000: Master AXI performs any burst length
<6>[   24.516426] ipq806x-gmac-dwmac 37400000.ethernet eth0: IEEE 1588-2008 Advanced Timestamp sup
ported
<6>[   24.522078] ipq806x-gmac-dwmac 37400000.ethernet eth0: registered PTP clock
<6>[   24.534347] br-wan: port 1(eth0) entered blocking state
<6>[   24.537849] br-wan: port 1(eth0) entered disabled state
<6>[   24.544469] br-wan: port 1(eth0) entered blocking state
<6>[   24.548271] br-wan: port 1(eth0) entered forwarding state
<6>[   24.751737] 8021q: adding VLAN 0 to HW filter on device bat0
<6>[   24.752006] br-lan: port 2(bat0) entered blocking state
<6>[   24.756560] br-lan: port 2(bat0) entered disabled state
<6>[   24.761574] device bat0 entered promiscuous mode
<6>[   24.766771] device eth1 entered promiscuous mode
<6>[   24.771559] br-lan: port 2(bat0) entered blocking state
<6>[   24.776138] br-lan: port 2(bat0) entered forwarding state
<6>[   24.798361] IPv6: ADDRCONF(NETDEV_CHANGE): br-lan: link becomes ready
<6>[   25.263219] batman_adv: bat0: No IGMP Querier present - multicast optimizations disabled
<6>[   25.263251] batman_adv: bat0: No MLD Querier present - multicast optimizations disabled
<6>[   25.382134] br-wan: port 1(eth0) entered disabled state
<6>[   27.516892] ipq806x-gmac-dwmac 37600000.ethernet eth1: Link is Up - 1Gbps/Full - flow contro
l rx/tx
<4>[   31.710745] ath10k_pci 0002:01:00.0: 10.4 wmi init: vdevs: 8  peers: 180  tid: 450
<6>[   31.710774] ath10k_pci 0002:01:00.0: using 7 firmware rate-ctrl objects
<4>[   31.717361] ath10k_pci 0002:01:00.0: msdu-desc: 2200  skid: 360
<6>[   31.800345] ath10k_pci 0002:01:00.0: wmi print 'P 180/180 V 8 K 540 PH 556 T 656  msdu-desc:
 2200  sw-crypt: 0 ct-sta: 0'
<6>[   31.801611] ath10k_pci 0002:01:00.0: wmi print 'free: 11368 iram: 8424 sram: 512'
<4>[   32.193725] ath10k_pci 0002:01:00.0: Firmware lacks feature flag indicating a retry limit of
 > 2 is OK, requested limit: 4
<6>[   32.193942] IPv6: ADDRCONF(NETDEV_UP): client1: link is not ready
<6>[   32.208336] br-lan: port 1(eth1) entered blocking state
```

```
<6>[   32.209836] br-lan: port 1(eth1) entered forwarding state
<6>[   32.237464] br-lan: port 3(client1) entered blocking state
<6>[   32.237491] br-lan: port 3(client1) entered disabled state
<6>[   32.242616] device client1 entered promiscuous mode
<6>[   32.394857] br-wan: port 1(eth0) entered disabled state
<6>[   32.457821] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
<6>[   32.762860] ath10k_pci 0002:01:00.0: NOTE:  Firmware DBGLOG output disabled in debug_mask: 0
x10000000
<6>[   32.770474] IPv6: ADDRCONF(NETDEV_CHANGE): client1: link becomes ready
<6>[   32.771583] br-lan: port 3(client1) entered blocking state
<6>[   32.777580] br-lan: port 3(client1) entered forwarding state
<6>[   32.886573] Atheros 8031 ethernet gpio-0:01: attached PHY driver [Atheros 8031 ethernet] (mi
i_bus:phy_addr=gpio-0:01, irq=POLL)
<6>[   32.893172] dwmac1000: Master AXI performs any burst length
<6>[   32.897375] ipq806x-gmac-dwmac 37400000.ethernet eth0: IEEE 1588-2008 Advanced Timestamp sup
ported
<6>[   32.902530] ipq806x-gmac-dwmac 37400000.ethernet eth0: registered PTP clock
<6>[   32.916682] br-wan: port 1(eth0) entered blocking state
<6>[   32.918477] br-wan: port 1(eth0) entered disabled state
<6>[   32.928463] IPv6: ADDRCONF(NETDEV_UP): br-wan: link is not ready
<4>[   38.723594] ath10k_pci 0001:01:00.0: 10.4 wmi init: vdevs: 8  peers: 180  tid: 450
<6>[   38.723623] ath10k_pci 0001:01:00.0: using 7 firmware rate-ctrl objects
<4>[   38.731093] ath10k_pci 0001:01:00.0: msdu-desc: 2200  skid: 360
<6>[   38.811599] ath10k_pci 0001:01:00.0: wmi print 'P 180/180 V 8 K 540 PH 556 T 656  msdu-desc:
 2200  sw-crypt: 0 ct-sta: 0'
<6>[   38.812877] ath10k_pci 0001:01:00.0: wmi print 'free: 11368 iram: 8424 sram: 512'
<4>[   39.201170] ath10k_pci 0001:01:00.0: Firmware lacks feature flag indicating a retry limit of
 > 2 is OK, requested limit: 4
<6>[   39.201339] IPv6: ADDRCONF(NETDEV_UP): client0: link is not ready
<6>[   39.216274] br-lan: port 4(client0) entered blocking state
<6>[   39.217340] br-lan: port 4(client0) entered disabled state
<6>[   39.222873] device client0 entered promiscuous mode
<6>[   39.528761] IPv6: ADDRCONF(NETDEV_CHANGE): client0: link becomes ready
<6>[   39.529012] br-lan: port 4(client0) entered blocking state
<6>[   39.534302] br-lan: port 4(client0) entered forwarding state
<6>[   40.691860] IPv6: ADDRCONF(NETDEV_UP): mesh0: link is not ready
<6>[   40.731037] IPv6: ADDRCONF(NETDEV_UP): mesh1: link is not ready
<6>[   40.823371] ath10k_pci 0001:01:00.0: mac flush null vif, drop 0 queues 0xffff
<6>[   40.898665] ath10k_pci 0002:01:00.0: mac flush null vif, drop 0 queues 0xffff
<6>[   41.760998] br-lan: port 4(client0) entered disabled state
<6>[   41.762528] br-lan: port 3(client1) entered disabled state
<6>[   44.641968] br-lan: port 3(client1) entered blocking state
<6>[   44.642010] br-lan: port 3(client1) entered forwarding state
<6>[   44.649723] batman_adv: bat0: Adding interface: mesh1
<6>[   44.652216] batman_adv: bat0: Interface activated: mesh1
<6>[   44.658352] IPv6: ADDRCONF(NETDEV_CHANGE): mesh1: link becomes ready
<4>[   44.891497] ath10k_pci 0002:01:00.0: Invalid peer id 0 or peer stats buffer, peer: cb915000
 sta:   (null)
<6>[   47.250647] br-lan: port 4(client0) entered blocking state
<6>[   47.250682] br-lan: port 4(client0) entered forwarding state
<6>[   47.257308] batman_adv: bat0: Adding interface: mesh0
<6>[   47.260838] batman_adv: bat0: Interface activated: mesh0
<6>[   47.308240] IPv6: ADDRCONF(NETDEV_CHANGE): mesh0: link becomes ready
<4>[   75.993607] NOHZ: local_softirq_pending 08
<4>[  219.354201] NOHZ: local_softirq_pending 08
<4>[  444.633812] NOHZ: local_softirq_pending 08
<4>[  506.073732] NOHZ: local_softirq_pending 08
<4>[  526.553749] NOHZ: local_softirq_pending 08
<4>[  669.913737] NOHZ: local_softirq_pending 08
<4>[  751.833940] NOHZ: local_softirq_pending 08
<4>[  772.313676] NOHZ: local_softirq_pending 08
<4>[  792.793586] NOHZ: local_softirq_pending 08
<4>[  813.273624] NOHZ: local_softirq_pending 08
<4>[  848.273737] ath10k_pci 0002:01:00.0: peer-unmap-event: unknown peer id 8
<4>[  850.884255] ath10k_pci 0001:01:00.0: peer-unmap-event: unknown peer id 5
<1>[ 1263.833736] Unable to handle kernel NULL pointer dereference at virtual address 00000038
<1>[ 1263.833770] pgd = c0204000
```

```
<1>[ 1263.840947] [00000038] *pgd=00000000
<0>[ 1263.843483] Internal error: Oops: 17 [#1] SMP ARM
<4>[ 1263.847138] Modules linked in: pppoe ppp_async batman_adv ath10k_pci ath10k_core ath pppox p
pp_generic nft_set_rbtree nft_set_hash nft_reject_ipv6 nft_reject_ipv4 nft_reject_inet nft_reject_
bridge nft_reject nft_redir nft_quota nft_numgen nft_meta_bridge nft_meta nft_log nft_limit nft_fw
d_netdev nft_exthdr nft_dup_netdev nft_ct nft_counter nft_chain_route_ipv6 nft_chain_route_ipv4 nf
_tables_netdev nf_tables_ipv6 nf_tables_ipv4 nf_tables_inet nf_tables_bridge nf_tables mac80211 ip
table_nat ipt_REJECT ipt_MASQUERADE cfg80211 xt_time xt_tcpudp xt_tcpmss xt_statistic xt_state xt_
nat xt_multiport xt_mark xt_mac xt_limit xt_length xt_hl xt_ecn xt_dscp xt_conntrack xt_comment xt
_TCPMSS xt_REDIRECT xt_LOG xt_HL xt_FLOWOFFLOAD xt_DSCP xt_CLASSIFY slhc openvswitch nfnetlink nf_
reject_ipv4 nf_nat_redirect nf_nat_masquerade_ipv6
<4>[ 1263.901905]  nf_nat_masquerade_ipv4 nf_conntrack_ipv6 nf_nat_ipv6 nf_conntrack_ipv4 nf_nat_i
pv4 nf_nat nf_log_ipv4 nf_flow_table_hw nf_flow_table nf_dup_netdev nf_defrag_ipv6 nf_defrag_ipv4
nf_conntrack_rtcache nf_conntrack libcrc32c iptable_mangle iptable_filter ipt_ECN ip_tables crc_cc
itt compat ledtrig_usbport nf_log_ipv6 nf_log_common ip6table_mangle ip6table_filter ip6_tables ip
6t_REJECT x_tables nf_reject_ipv6 mpls_iptunnel mpls_router mpls_gso leds_gpio xhci_plat_hcd xhci_
pci xhci_hcd dwc3 dwc3_of_simple ohci_platform ohci_hcd phy_qcom_dwc3 ahci ehci_platform sd_mod ah
ci_platform libahci_platform libahci libata scsi_mod ehci_hcd gpio_button_hotplug crc32c_generic
<4>[ 1263.961027] CPU: 0 PID: 2470 Comm: kworker/u4:2 Not tainted 4.14.187 #0
<4>[ 1263.983254] Hardware name: Generic DT based system
<4>[ 1263.989826] Workqueue: bat_events batadv_bla_periodic_work [batman_adv]
<4>[ 1263.994629] task: cbcbed00 task.stack: ca46e000
<4>[ 1264.001153] PC is at batadv_bit_get_packet+0xc4/0xf4 [batman_adv]
<4>[ 1264.005669] LR is at batadv_bit_get_packet+0xb8/0xf4 [batman_adv]
<4>[ 1264.011901] pc : [<bf5ebe30>]    lr : [<bf5ebe24>]    psr: 60000013
<4>[ 1264.017976] sp : ca46fec0  ip : 000000c8  fp : cd804200
<4>[ 1264.024050] r10: ccd38000  r9 : 00000007  r8 : 00000000
<4>[ 1264.029260] r7 : cb8a64c0  r6 : cb90e300  r5 : cc6f7e8c  r4 : 00000000
<4>[ 1264.034471] r3 : 00000038  r2 : 00000002  r1 : 00000000  r0 : cc6f7e8c
<4>[ 1264.041069] Flags: nZCv  IRQs on  FIQs on  Mode SVC_32  ISA ARM  Segment none
<4>[ 1264.047578] Control: 10c5787d  Table: 4dd7406a  DAC: 00000051
<0>[ 1264.054784] Process kworker/u4:2 (pid: 2470, stack limit = 0xca46e210)
<0>[ 1264.060513] Stack: (0xca46fec0 to 0xca470000)
<0>[ 1264.066960] fec0: cc6f7e80 cb90e300 cb90e300 bf5ecbf4 cb95c0c0 00000200 c0b02d00 00000007
<0>[ 1264.071393] fee0: cb8a678c cb8a669c cb90e300 cb8a64c0 cb8a669c 00000000 00000000 00000080
<0>[ 1264.079554] ff00: cd804200 bf5ecd70 cb8a677c cb8a677c 60000013 cb8a669c cb93b080 cd804200
<0>[ 1264.087713] ff20: cbd6c600 00000000 00000000 00000080 cd804200 c0337120 cd804218 ffffe000
<0>[ 1264.095873] ff40: cb93b080 cd804200 cb93b098 cd804218 ffffe000 c0b02d00 00000088 c033761c
<0>[ 1264.104032] ff60: cc72febc ccdd6400 ca46e000 c8fe6880 cc72febc ccdd641c cb93b080 c03372d8
<0>[ 1264.112192] ff80: 00000000 c033d2bc 00000000 c8fe6880 c033d174 00000000 00000000 00000000
<0>[ 1264.120351] ffa0: 00000000 00000000 00000000 c0307d28 00000000 00000000 00000000 00000000
<0>[ 1264.128511] ffc0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
<0>[ 1264.136670] ffe0: 00000000 00000000 00000000 00000000 00000013 00000000 00000000 00000000
<4>[ 1264.144917] [<bf5ebe30>] (batadv_bit_get_packet [batman_adv]) from [<bf5ecbf4>] (batadv_bla_
loopdetect_report+0xa48/0xb44 [batman_adv])
<4>[ 1264.153012] [<bf5ecbf4>] (batadv_bla_loopdetect_report [batman_adv]) from [<bf5ecd70>] (bata
dv_bla_periodic_work+0x80/0xb04 [batman_adv])
<4>[ 1264.164984] [<bf5ecd70>] (batadv_bla_periodic_work [batman_adv]) from [<c0337120>] (process_
one_work+0x28c/0x444)
<4>[ 1264.177456] [<c0337120>] (process_one_work) from [<c033761c>] (worker_thread+0x344/0x58c)
<4>[ 1264.187695] [<c033761c>] (worker_thread) from [<c033d2bc>] (kthread+0x148/0x150)
<4>[ 1264.195860] [<c033d2bc>] (kthread) from [<c0307d28>] (ret_from_fork+0x14/0x2c)
<0>[ 1264.203329] Code: eb4724e3 e5944008 e2843038 f593f000 (e1932f9f)
<4>[ 1264.210463] ---[ end trace 54361f4755dee328 ]---

==========================%
```

History

#1 - 08/27/2020 10:13 AM - Linus Lüssing

- Description updated