batman-adv - Bug #139

skb_over_panic

09/29/2010 12:13 PM - Anonymous

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marek Lindner	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2010.2.0		

Description

batman-adv rv1815

By running the trunk rv1815, I found that there skb_over_panic issue happens. It looks that when the aggregate packet length reach "537", skb_put will be failed with skb_over_panic.

Is anyone have any idea about this? How can I prevent this error happens?

Please let me know if any further information is needed. Thanks in advance.

System: mips
OS: Linux

Log with Debug level 3 "batctl ll 3"

```
[       901] Forwarding packet (originator 873e1856, seqno 6760, TQ 7, TTL 48, IDF on) on interfac
e ad120 [00:1a:dd:b1:6c:32]
[       901] Received BATMAN packet via NB: 87311058, IF: ad120 [00:1a:dd:b1:6c:32] (from OG: 8731
1068, via prev OG: 8731106e, seqno 6760, tq 235, TTL 48, V 12, IDF 1)
[       901] bidirectional: orig = 871c1300        neigh = 871c1380        => own_bcast =  0, real
 recv = 64, local tq:   0, asym_penalty: 255, total tq:   0
[       901] Drop packet: not received via bidirectional link
[       901] Received BATMAN packet via NB: 87337058, IF: ad120 [00:1a:dd:b1:6c:32] (from OG: 8733
7068, via prev OG: 8733706e, seqno 6760, tq 235, TTL 48, V 12, IDF 1)
[       901] bidirectional: orig = 871c1300        neigh = 871c1d80        => own_bcast =  0, real
 recv = 64, local tq:   0, asym_penalty: 255, total tq:   0
[       901] Drop packet: not received via bidirectional link
[       901] Received BATMAN packet via NB: 8731f058, IF: ad120 [00:1a:dd:b1:6c:32] (from OG: 8731
f068, via prev OG: 8731f06e, seqno 4574, tq 255, TTL 50, V 12, IDF 0)
[       901] updating last_seqno: old 4573, new 4574
[       901] bidirectional: orig = 871c1380        neigh = 871c1380        => own_bcast =  0, real
 recv = 64, local tq:   0, asym_penalty: 255, total tq:   0
[       901] Forwarding packet: tq_orig: 0, tq_avg: 12, tq_forw: 0, ttl_orig: 49, ttl_forw: 49
[       901] new_aggregated_packet:140 -- b4 skb_put, len=42
[       901] Forwarding packet: rebroadcast neighbor packet with direct link flag
[       901] Received BATMAN packet via NB: 87323058, IF: ad120 [00:1a:dd:b1:6c:32] (from OG: 8732
3068, via prev OG: 8732306e, seqno 4574, tq 227, TTL 48, V 12, IDF 1)
[       901] bidirectional: orig = 871c1380        neigh = 871c1300        => own_bcast =  0, real
 recv = 13, local tq:   0, asym_penalty: 126, total tq:   0
[       901] Drop packet: not received via bidirectional link
[       901] Received BATMAN packet via NB: 87322058, IF: ad120 [00:1a:dd:b1:6c:32] (from OG: 8732
2068, via prev OG: 8732206e, seqno 4574, tq 245, TTL 49, V 12, IDF 1)
[       901] bidirectional: orig = 871c1380        neigh = 871c1400        => own_bcast =  0, real
 recv = 64, local tq:   0, asym_penalty: 255, total tq:   0
[       901] Drop packet: not received via bidirectional link
[       901] Forwarding packet (originator 8729b056, seqno 4574, TQ 0, TTL 49, IDF on) on interfac
e ad120 [00:1a:dd:b1:6c:32]
[       901] Received BATMAN packet via NB: 87339058, IF: ad120 [00:1a:dd:b1:6c:32] (from OG: 8733
9068, via prev OG: 8733906e, seqno 4574, tq 245, TTL 49, V 12, IDF 1)
[       901] bidirectional: orig = 871c1380        neigh = 871c1d80        => own_bcast =  0, real
 recv = 64, local tq:   0, asym_penalty: 255, total tq:   0
[       901] Drop packet: not received via bidirectional link
```

```
skb_over_panic: text:87389b44 len:534 put:534 head:873e1c00 data:873e1c4e tail:0x873e1e64 end:0x87
3e1e60 dev:<NULL>
Kernel bug detected[#1]:
Cpu 0
$ 0   : 00000000 80330000 00000077 00000001
$ 4   : 802f5520 80330000 00000001 803453d4
$ 8   : 802f0000 00003117 80330000 80330000
$12   : 80330000 00000000 00000000 00008000
$16   : 873e1c4e 87246380 00000001 000001fe
$20   : 00000216 87246380 00000001 00016097
$24   : 00000001 8700e0cc
$28   : 870f8000 870f9e18 87b1d500 801f1088
Hi    : 000000e2
Lo    : 196e8000
epc   : 801f1088 skb_over_panic+0x54/0x60
    Tainted: P
ra    : 801f1088 skb_over_panic+0x54/0x60
Status: 1000d403    KERNEL EXL IE
Cause : 10800024
[[PrId]]  : 00019374 (MIPS 24Kc)
Modules linked in: batman_adv ebt_mark_m ebt_mark ebt_vlan ebt_snat ebt_redirect ebt_log ebt_ip eb
t_dnat ebt_arpreply ebt_arp ebtable_nat ebtable_filter ebtable_broute ebtables wlan_acl wlan_ccmp
wlan_xauth wlan_tkip wlan_wep ath_pci ath_rate_atheros(P) ath_hal(P) wlan_scan_ap wlan_scan_sta wl
an gpioctrl
Process bat_events (pid: 3135, threadinfo=870f8000, task=879aafa8, tls=00000000)
Stack : 00800400 87389b44 00000216 00000216 873e1c00 873e1c4e 873e1e64 873e1e60
        802c42d0 87246380 801f1190 878014e0 8729b000 87246380 00000001 000001fe
        87376400 87389b44 8732e600 8732e580 8738ddb8 0000008c 00000216 87246000
        8729b000 00000000 8729b000 87b1d500 87246380 000001fe 00000216 00000001
        87246380 87246000 87390000 873821bc 801f9f58 801f9ed0 87381f88 872dd3d0
        ...
Call Trace:
[<801f1088>] skb_over_panic+0x54/0x60
[<801f1190>] skb_put+0x48/0x5c
[<87389b44>] add_bat_packet_to_list+0x338/0x4e8 [batman_adv]
[<873821bc>] schedule_own_packet+0x188/0x1b4 [batman_adv]
[<87382b50>] send_outstanding_bat_packet+0x36c/0x3c8 [batman_adv]
[<8009dd88>] run_workqueue+0xb4/0x14c
[<8009dee4>] worker_thread+0xc4/0xe4
[<800a17e4>] kthread+0x58/0x98
[<8006bf94>] kernel_thread_helper+0x10/0x18

Code: 24846870  0c02375b  afa90020 <0200000d> 0807c423  00000000  27bdffd0  afbf0028  8c870098
[       901] new_aggregated_packet:140 -- b4 skb_put, len=534
[       901] Received BATMAN packet via NB: 871e8058, IF: ad120 [00:1a:dd:b1:6c:3panic log area no
t empty, skipped writing this panic
2] (from OG: 871Fatal exception: panic in 5 seconds
e8068, via prev OG: 871e806e, seqno 5536, tq 255, TTL 50, V 12, IDF 0)
[       901] updating last_seqno: old 5535, new 5536
[       901] bidirectional: orig = 871c1400        neigh = 871c1400        => own_bcast =  0, real
 recv = 64, local tq:   0, asym_penalty: 255, total tq:   0
[       901] Forwarding packet: tq_orig: 0, tq_avg: 11, tq_forw: 0, ttl_orig: 49, ttl_forw: 49
[       901] new_aggregated_packet:140 -- b4 skb_put, len=36
[       901] Forwarding packet: rebroadcast neighbor packet with direct link flag
[       901] Received BATMAN packet via NB: 8733d058, IF: ad120 [00:1a:dd:b1:6c:32] (from OG: 8733
d068, via prev OG: 8733d06e, seqno 5536, tq 245, TTL 49, V 12, IDF 1)
[       901] bidirectional: orig = 871c1400        neigh = 871c1380        => own_bcast =  0, real
 recv = 64, local tq:   0, asym_penalty: 255, total tq:   0
[       901] Drop packet: not received via bidirectional link
[       901] Received BATMAN packet via NB: 872e7058, IF: ad120 [00:1a:dd:b1:6c:32] (from OG: 872e
7068, via prev OG: 872e706e, seqno 6971, tq 255, TTL 50, V 12, IDF 0)
[       901] updating last_seqno: old 6970, new 6971
[       901] bidirectional: orig = 871c1d80        neig
```

Debug Message added:

```
Index: aggregation.c
===================================================================
--- aggregation.c    (revision 1815)
+++ aggregation.c    (working copy)
@@ -135,6 +135,9 @@

     INIT_HLIST_NODE(&forw_packet_aggr->list);

+    bat_dbg(DBG_ROUTES, bat_priv,
+            "%s:%d -- b4 skb_put, len=%d\n",
+            +func+, +LINE+, packet_len);
     skb_buff = skb_put(forw_packet_aggr->skb, packet_len);
     forw_packet_aggr->packet_len = packet_len;
     memcpy(skb_buff, packet_buff, packet_len);
@@ -169,7 +172,6 @@
               bool direct_link)
 {
     unsigned char *skb_buff;
-
     skb_buff = skb_put(forw_packet_aggr->skb, packet_len);
     memcpy(skb_buff, packet_buff, packet_len);
     forw_packet_aggr->packet_len += packet_len;
@@ -234,6 +236,9 @@
                       send_time, direct_link,
                       if_incoming, own_packet);
     } else {
+        bat_dbg(DBG_ROUTES, bat_priv,
+                "%s:%d -- b4 skb_put, len=%d\n",
+                +func+, +LINE+, packet_len);
         aggregate(forw_packet_aggr,
               packet_buff, packet_len,
               direct_link);
```

History

#1 - 09/29/2010 12:15 PM - Anonymous

The packet length causing the problem should be "534" instead of "537". Sorry for the typo.

#2 - 09/30/2010 12:52 AM - Marek Lindner

- Status changed from New to In Progress

Thanks for this detailed bug report! That does not happen every day. ;-)

From what I see I would guess that this node has 80+ locally announced mac addresses which collides with the internal packet size limit (without proper checking). Could you append the local translation table to verify this theory ?

Am I right assuming you are running the module in some kind of emulated environment ? The "ad120" interface looks a bit suspicious.

For some reason the mac addresses are not properly printed:

```
Received BATMAN packet via NB: 87337058
```

Is that a bug on our side or did you patch the code further ?

#3 - 10/04/2010 04:46 AM - Marek Lindner

Since you did not reply to mail I guess it did not reach you ?!
Here is what I wrote:

> It looks strange that the it didn't show the mac address of the packet,
> however, it seems didn't cause the issue.

No, you are right. This is not the issue but it might be another bug. Which kernel version do you use ?

> Anyway, could you point me to the location translation table you mentioning?

Check the "translation table" section:
Understand-your-batman-adv-network

> (ps. I am running the code on a embedded machine, just like OpenWRT, ad120
> is just a name I randomly pick as a ad-hoc device ;))

Ok.

> To fix the issue, I have make a quick hack to the new_aggregated_packet
> function. Since the packet_len is possible to be larger than the
> MAX_AGGREGATION_BYTES, the original skb allocation is not large enough to
> hold the whole packet! There is no checking against the packet_len and
> MAX_AGGREGATION_BYTES, too. I guess the hack could help to find a proper
> way to fix it in code :)

The code definitely lacks a check whether the packet_len is bigger than MAX_AGGREGATION_BYTES but simply increasing the packet size won't help either.

Note that such a big packet is highly unusal - the protocol needs less than 20bytes plus the announcements. So, I am wondering why the packet is growing to this size. If the additional size is coming from the local translation table, I'd suggest to limit the size of that table.

#4 - 10/18/2010 12:17 PM - Marek Lindner

- Status changed from In Progress to Closed

Fixed in r1830/r1831/r1832.

#5 - 02/11/2017 09:38 AM - Sven Eckelmann

- Target version set to 2010.2.0

- Description updated