batman-adv - Bug #143

kernel warning stack trace(s) followed by spontaneous reboot

01/23/2011 04:40 AM - Anonymous

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marek Lindner	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2011.2.0		

Description

I have seen this same warning several times, captured on a serial port attached to a soekris net4826, running r24954 OpenWrt with r1902 + some fragmentation patches. The device has vis_mode server turned on. The first time the same stack trace was emitted 90-some times in a row before the device rebooted itself:

```
------------[ cut here ]------------
WARNING: at lib/kref.c:34 kref_get+0x18/0x30()
Modules linked in: scx200_wdt ath_pci ath_hal(P) leds_net48xx scx200_gpio batman_adv nf_nat_tftp n
f_conntrack_tftp nf_nat_irc nf_conntrack_irc nf_nat_ftp nf_conntrack_ftp ipt_MASQUERADE iptable_na
t
 nf_nat xt_NOTRACK iptable_raw xt_state nf_conntrack_ipv4 nf_defrag_ipv4 nf_conntrack ipt_REJECT x
t_TCPMSS ipt_LOG xt_comment xt_multiport xt_mac xt_limit iptable_mangle iptable_filter ip_tables x
t
_tcpudp x_tables nsc_gpio natsemi ipv6
Pid: 322, comm: kworker/u:2 Tainted: P        W   2.6.37 #4
Call Trace:
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c1026a97>] ? warn_slowpath_common+0x87/0xb0
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c1026adb>] ? warn_slowpath_null+0x1b/0x20
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c4bc1a8f>] ? receive_client_update_packet+0x46f/0x730 [batman_adv]
 [<c1035ec5>] ? process_one_work+0x155/0x250
 [<c4bc16f0>] ? receive_client_update_packet+0xd0/0x730 [batman_adv]
 [<c1036e74>] ? worker_thread+0x124/0x200
 [<c1036d50>] ? worker_thread+0x0/0x200
 [<c1039c6c>] ? kthread+0x6c/0x80
 [<c1039c00>] ? kthread+0x0/0x80
 [<c1002e36>] ? kernel_thread_helper+0x6/0x30
---[ end trace 98aa451a0a91a4e2 ]---
```

The second time, several of these same stack traces were followed by a panic:

```
------------[ cut here ]------------
Kernel BUG at c107be6e [verbose debug info unavailable]
invalid opcode: 0000 [#1]
last sysfs file: /sys/devices/virtual/net/bat0/mesh/vis_mode
Modules linked in: scx200_wdt ath_pci ath_hal(P) leds_net48xx scx200_gpio batman_adv nf_nat_tftp n
f_conntrack_tftp nf_nat_irc nf_conntrack_irc nf_nat_ftp nf_conntrack_ftp ipt_MASQUERADE iptable_na
t nf_nat xt_NOTRACK iptable_raw xt_state nf_conntrack_ipv4 nf_defrag_ipv4 nf_conntrack ipt_REJECT
xt_TCPMSS ipt_LOG xt_comment xt_multiport xt_mac xt_limit iptable_mangle iptable_filter ip_tables
xt_tcpudp x_tables nsc_gpio natsemi ipv6

Pid: 322, comm: kworker/u:2 Tainted: P        W   2.6.37 #4 /
EIP: 0060:[<c107be6e>] EFLAGS: 00010246 CPU: 0
EIP is at kfree+0x4e/0xb0
EAX: 40000000 EBX: c3f80000 ECX: 00000000 EDX: c3fcc560
ESI: c262b000 EDI: 00000000 EBP: c2da32e0 ESP: c3809e3c
 DS: 007b ES: 007b FS: 0000 GS: 0000 SS: 0068
Process kworker/u:2 (pid: 322, ti=c3808000 task=c3853980 task.ti=c391e000)
```

```
Stack:
 c262b040 c2d74a80 c3809ef4 00000000 c11f62d8 c2d74a80 c4cfd5b6 00000000
 c2d74a80 c4d02bb1 00000080 00000031 ef462c9f 00000014 c2459000 c2d74a80
 00000000 c2da0000 00000001 c121f1d0 c1358e20 c2e449c0 c1358e40 c11fd156
Call Trace:
 [<c11f62d8>] ? +kfree_skb+0x8/0x80
 [<c4cfd5b6>] ? ieee80211_dev_kfree_skb+0x46/0x60 [ath_pci]
 [<c4d02bb1>] ? ieee80211_input+0x1211/0x1240 [ath_pci]
 [<c121f1d0>] ? ip_rcv+0x0/0x2a0
 [<c11fd156>] ? +netif_receive_skb+0x446/0x480
 [<c107c0c4>] ? +slab_alloc+0x74/0x1e0
 [<c4cfd5b6>] ? ieee80211_dev_kfree_skb+0x46/0x60 [ath_pci]
 [<c11f8000>] ? skb_shift+0xf0/0x360
 [<c11f6fd9>] ? dev_alloc_skb+0x19/0x30
 [<c11f6fd9>] ? dev_alloc_skb+0x19/0x30
 [<c4d02cb8>] ? ieee80211_input_all+0xd8/0x120 [ath_pci]
 [<c4cf7824>] ? ath_sysctl_register+0x8b34/0x8ed0 [ath_pci]
 [<c102f7e2>] ? run_timer_softirq+0xf2/0x180
 [<c1200520>] ? net_rx_action+0x50/0x110
 [<c102aff9>] ? +do_softirq+0x69/0x100
 [<c102af90>] ? +do_softirq+0x0/0x100
 <IRQ>
 [<c102b265>] ? local_bh_enable+0x65/0x80
 [<c4bc1a94>] ? receive_client_update_packet+0x474/0x730 [batman_adv]
 [<c1035ec5>] ? process_one_work+0x155/0x250
 [<c4bc16f0>] ? receive_client_update_packet+0xd0/0x730 [batman_adv]
 [<c1036e74>] ? worker_thread+0x124/0x200
 [<c1036d50>] ? worker_thread+0x0/0x200
 [<c1039c6c>] ? kthread+0x6c/0x80
 [<c1039c00>] ? kthread+0x0/0x80
 [<c1002e36>] ? kernel_thread_helper+0x6/0x30
Code: 00 00 40 c1 ea 0c c1 e2 05 01 da 8b 02 25 00 80 00 00 66 85 c0 74 06 8b 52 0c 8d 76 00 8b 02
 84 c0 78 22 f7 02 00 c0 00 00 75 04 <0f> 0b eb fe 8b 5c 24 04 89 d0 8b 74 24 08 8b 7c 24 0c 83 c4
 10
EIP: [<c107be6e>] kfree+0x4e/0xb0 SS:ESP 0068:c3809e3c
---[ end trace 98aa451a0a91a4e3 ]---
Kernel panic - not syncing: Fatal exception in interrupt
```

History

#1 - 01/26/2011 06:25 PM - Anonymous

[Ignore the broadcom trace above, that was a different problem]

With r1902 + magic-next.patch (getting me to the current next as of 2011-01-25), I got the following trace (several of these before a spontaneous reboot) after about 14.5 hours of uptime:

```
------------[ cut here ]------------
WARNING: at lib/kref.c:34 kref_get+0x18/0x30()
Modules linked in: scx200_wdt ath_pci ath_hal(P) leds_net48xx scx200_gpio batman_adv nf_nat_tftp nf_conntrack_
tftp nf_nat_irc nf_conntrack_irc nf_nat_ftp nf_conntrack_ftp ipt_MASQUERADE iptable_nat
 nf_nat xt_NOTRACK iptable_raw xt_state nf_conntrack_ipv4 nf_defrag_ipv4 nf_conntrack ipt_REJECT xt_TCPMSS ipt
_LOG xt_comment xt_multiport xt_mac xt_limit iptable_mangle iptable_filter ip_tables xt
_tcpudp x_tables nsc_gpio natsemi ipv6
Pid: 322, comm: kworker/u:2 Tainted: P            2.6.37 #1
Call Trace:
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c1026a97>] ? warn_slowpath_common+0x87/0xb0
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c1026adb>] ? warn_slowpath_null+0x1b/0x20
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c57aea9f>] ? send_vis_packets+0x39f/0x660 [batman_adv]
 [<c1035ec5>] ? process_one_work+0x155/0x250
 [<c57ae700>] ? send_vis_packets+0x0/0x660 [batman_adv]
 [<c1036e74>] ? worker_thread+0x124/0x200
 [<c1036d50>] ? worker_thread+0x0/0x200
 [<c1039c6c>] ? kthread+0x6c/0x80
 [<c1039c00>] ? kthread+0x0/0x80
 [<c1002e36>] ? kernel_thread_helper+0x6/0x30
---[ end trace 26da713fde6cc87b ]---
```

note that this one appears in send_vis_packets rather than receive_client_update_packet.

#2 - 01/27/2011 11:12 PM - Anonymous

I tried compiling the batman-adv.ko module with EXTRA_CFLAGS="-O0 -fno-inline -DCONFIG_BATMAN_ADV_DEBUG -DREVISION_VERSION=\\\"$(PKG_REV)\\\"" (the .ko got bigger, about 2MB on x86). Got this trace:

```
------------[ cut here ]------------
WARNING: at lib/kref.c:34 kref_get+0x18/0x30()
Modules linked in: scx200_wdt ath_pci ath_hal(P) leds_net48xx scx200_gpio batman_adv nf_nat_tftp nf_conntrack_
tftp nf_nat_irc nf_conntrack_irc nf_nat_ftp nf_conntrack_ftp ipt_MASQUERADE iptable_nat
Pid: 7, comm: kworker/u:1 Tainted: P            2.6.37 #1
Call Trace:
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c1026a97>] ? warn_slowpath_common+0x87/0xb0
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c1026adb>] ? warn_slowpath_null+0x1b/0x20
 [<c1120be8>] ? kref_get+0x18/0x30
 [<c54f9050>] ? send_vis_packets+0xa5/0x153 [batman_adv]
 [<c1035ec5>] ? process_one_work+0x155/0x250
 [<c54f8fab>] ? send_vis_packets+0x0/0x153 [batman_adv]
 [<c1036e74>] ? worker_thread+0x124/0x200
 [<c1036d50>] ? worker_thread+0x0/0x200
 [<c1039c6c>] ? kthread+0x6c/0x80
 [<c1039c00>] ? kthread+0x0/0x80
 [<c1002e36>] ? kernel_thread_helper+0x6/0x30
---[ end trace 71ab3cb3e2c490f8 ]---
```

#3 - 05/15/2011 11:47 AM - Anonymous

- % Done changed from 0 to 100

- Assignee changed from Anonymous to Marek Lindner

I think that it was fixed in commit:818b0cd8aa5523356385be4b508126121af6ef78

#4 - 05/23/2011 10:20 PM - Anonymous

- Status changed from New to Resolved

#5 - 07/10/2011 03:11 PM - Marek Lindner

- Status changed from Resolved to Closed

#6 - 02/11/2017 09:35 AM - Sven Eckelmann

- Target version set to 2011.2.0