DragonFlyBSD - Bug #2891

Kernel panic in IEEE802.11 related code

02/20/2016 09:13 PM - shamaz

Status:	New	**Start date:**	02/20/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Hello I am using DragonflyBSD 4.2 (but kernel panics on DragonFlyBSD 4.4 in the same situation too) with Atheros (if_ath) Wi-Fi adapter.

I have kernel panic after the following commands are executed:
ifconfig wlan0 create wlandev ath0 wlanmode ahdemo
ifconfig wlan0 up
ifconfig wlan0 list scan
ifconfig wlan0 ssid a channel 4

There is no panic if commands are reordered:

ifconfig wlan0 create wlandev ath0 wlanmode ahdemo
ifconfig wlan0 ssid a channel 1
ifconfig wlan0 up

Last kernel messages are:

```
wlan0: ieee80211_init
wlan0: start running, 1 vaps running
wlan0: ieee80211_new_state_locked: SCAN -> SCAN (nrunning 0 nscanning 0)
wlan0: ieee80211_new_state_locked: SCAN -> SCAN (nrunning 0 nscanning 0)
wlan0:  macaddr          bssid         chan  rssi  rate flag  wep  essid
- ec:22:80:cc:a1:ac ec:22:80:cc:a1:ac   11    37  54M   ess! wep! "nbn71"
- 10:fe:ed:5e:63:59 10:fe:ed:5e:63:59   11    31  54M   ess! wep!
"TP-LINK_2.4GHz_5E6359"
- 20:4e:7f:74:fa:06 20:4e:7f:74:fa:06    1    31  54M   ess! wep!
"Kristina"
- ee:43:f6:ce:ab:f8 ee:43:f6:ce:ab:f8    1    17  54M   ess! wep!
"Keenetic-1161"
- 00:22:b0:90:7b:0d 00:22:b0:90:7b:0d    2     3! 54M   ess! wep! "dysha"
- ec:22:80:cd:2f:4e ec:22:80:cd:2f:4e    2     3!  6M!  ess! wep! "nbn89"
- 00:24:01:f6:b5:7c 00:24:01:f6:b5:7c    3     6! 54M   ess! wep! "home"
- 90:f6:52:52:50:4a 90:f6:52:52:50:4a    5    16  54M   ess! wep! "ANN"
^ 04:8d:38:bc:b8:6b 04:8d:38:bc:b8:6b    6    26  54M   ess! wep! "netis
2.4G"
- d8:fe:e3:f9:3b:95 d8:fe:e3:f9:3b:95    9    30  54M   ess! wep! "kadet"
- 54:04:a6:bb:ee:0c 54:04:a6:bb:ee:0c   12    12  11M   ess! wep!
"Glorfindeil"
- 60:e3:27:d2:8a:88 60:e3:27:d2:8a:88    7    10  54M   ess! wep!
"BOBAHbICH"
^ 2c:ab:25:ff:46:86 2c:ab:25:ff:46:86    3     1! 54M   ess! wep!
"SmileNet153203102013"
- e0:cb:4e:ee:29:e4 e0:cb:4e:ee:29:e4   12     6! 11M   ess! wep!
"ASUS9571"
wlan0: ieee80211_create_ibss: creating IBSS on channel 1
wlan0: ieee80211_alloc_node 0xffffffe073280000<cc:af:78:58:73:a2> in
station table
I am in node_set_chan! Setting ni->ni_chan to 0xffffffe04e1cd6a4
wlan0: ieee80211_new_state_locked: SCAN -> RUN (nrunning 0 nscanning 0)
wlan0: scan_task: done, [ticks 64005, dwell min 100 scanend 2147545069]
wlan0: notify scan done
wlan0: ieee80211_newstate_cb: SCAN -> INIT arg -1
```

wlan0: adhoc_newstate: SCAN -> INIT (-1)
wlan0: node_reclaim: remove 0xffffffe073280000<cc:af:78:58:73:a2> from
station table, refcnt 2
wlan0: ieee80211_alloc_node 0xffffffe0730d2000<cc:af:78:58:73:a2> in
station table
wlan0: ieee80211_newstate_cb: INIT -> RUN arg -1
wlan0: adhoc_newstate: INIT -> RUN (-1)
wlan0: adhoc_newstate: unexpected state transition INIT -> RUN

Fatal trap 12: page fault while in kernel mode
cpuid = 3; lapic->id = 03000000
fault virtual address = 0xffff
fault code = supervisor read data, page not present
instruction pointer = 0x8:0xffffffff806ea42c
stack pointer = 0x10:0xffffffe04e6ab868
frame pointer = 0x10:0xffffffe04e6ab8c0
code segment = base 0x0, limit 0xfffff, type 0x1b
= DPL 0, pres 1, long 0, def32 0, gran 1
processor eflags = interrupt enabled, resume, IOPL = 0
current process = Idle
current thread = pri 12
kernel: type 12 trap, code=0

This is a cut from kgdb session:

(kgdb) bt
#0 _get_mycpu () at ./machine/thread.h:69
#1 md_dumpsys (di=di@entry=0xffffffff8151f760 <dumper>) at
/usr/src/sys/platform/pc64/x86_64/dump_machdep.c:265
#2 0xffffffff805f0627 in dumpsys () at
/usr/src/sys/kern/kern_shutdown.c:915
#3 0xffffffff802c0152 in db_fncall (dummy1=<optimized out>,
dummy2=<optimized out>, dummy3=<optimized out>,
dummy4=<optimized out>) at /usr/src/sys/ddb/db_command.c:539
#4 0xffffffff802c059b in db_command (aux_cmd_tablep_end=<optimized out>,
aux_cmd_tablep=<optimized out>,
cmd_table=<optimized out>, last_cmdp=0xffffffff80f71450
<db_last_command>) at /usr/src/sys/ddb/db_command.c:401
#5 db_command_loop () at /usr/src/sys/ddb/db_command.c:467
#6 0xffffffff802c3179 in db_trap (type=type@entry=12, code=code@entry=0)
at /usr/src/sys/ddb/db_trap.c:71
#7 0xffffffff809e0625 in kdb_trap (type=type@entry=12, code=code@entry=0,
regs=regs@entry=0xffffffe04e6ab798)
at /usr/src/sys/platform/pc64/x86_64/db_interface.c:175
#8 0xffffffff809e623a in trap_fatal (frame=frame@entry=0xffffffe04e6ab798,
eva=<optimized out>)
at /usr/src/sys/platform/pc64/x86_64/trap.c:1035
#9 0xffffffff809e6462 in trap_pfault (frame=frame@entry=0xffffffe04e6ab798,
usermode=usermode@entry=0)
at /usr/src/sys/platform/pc64/x86_64/trap.c:940
#10 0xffffffff809e6c8f in trap (frame=0xffffffe04e6ab798) at
/usr/src/sys/platform/pc64/x86_64/trap.c:618
#11 0xffffffff809d017f in calltrap () at
/usr/src/sys/platform/pc64/x86_64/exception.S:188
#12 0xffffffff806ea42c in ieee80211_getcapinfo
(vap=vap@entry=0xffffffe03dc66d00,
chan=0xffff)
at /usr/src/sys/netproto/802_11/wlan/ieee80211_output.c:2231
#13 0xffffffff806ea4db in ieee80211_beacon_construct
(m=m@entry=0xffffffe07319b200,
frm=0xffffffe0731be162 "",
bo=bo@entry=0xffffffe03dc676e8, ni=ni@entry=0xffffffe0730d2000)
at /usr/src/sys/netproto/802_11/wlan/ieee80211_output.c:2966
#14 0xffffffff806ebad1 in ieee80211_beacon_alloc
(ni=ni@entry=0xffffffe0730d2000,
bo=bo@entry=0xffffffe03dc676e8)
at /usr/src/sys/netproto/802_11/wlan/ieee80211_output.c:3167

#15 0xffffffff803d6e01 in ath_beacon_alloc (sc=sc@entry=0xffffffe04de21a00,
ni=ni@entry=0xffffffe0730d2000)
at /usr/src/sys/dev/netif/ath/ath/if_ath_beacon.c:200
#16 0xffffffff803cefa3 in ath_newstate (vap=0xffffffe03dc66d00,
nstate=<optimized out>, arg=<optimized out>)
at /usr/src/sys/dev/netif/ath/ath/if_ath.c:6126
#17 0xffffffff806ed8a0 in ieee80211_newstate_cb (xvap=0xffffffe03dc66d00,
npending=<optimized out>)
at /usr/src/sys/netproto/802_11/wlan/ieee80211_proto.c:1770
#18 0xffffffff80629f05 in taskqueue_run (queue=queue@entry=0xffffffe0064efd80,
lock_held=lock_held@entry=1)
at /usr/src/sys/kern/subr_taskqueue.c:331
#19 0xffffffff8062a023 in taskqueue_thread_loop (arg=<optimized out>) at
/usr/src/sys/kern/subr_taskqueue.c:489
#20 0xffffffff80602d42 in lwkt_deschedule_self (td=<optimized out>) at
/usr/src/sys/kern/lwkt_thread.c:321
#21 0x0000000000000000 in ?? ()
(kgdb) frame 13
#13 0xffffffff806ea4db in ieee80211_beacon_construct
(m=m@entry=0xffffffe07319b200,
frm=0xffffffe0731be162 "",
bo=bo@entry=0xffffffe03dc676e8, ni=ni@entry=0xffffffe0730d2000)
at /usr/src/sys/netproto/802_11/wlan/ieee80211_output.c:2966
2966   capinfo = ieee80211_getcapinfo(vap, ni->ni_chan);
(kgdb) p ni->ni_chan
$1 = (struct ieee80211_channel *) 0xffff
(kgdb) p vap->iv_des_chan
$2 = (struct ieee80211_channel *) 0xffffffe04e1cd6a4
(kgdb) p *(vap->iv_des_chan)
$3 = {ic_flags = 66688, ic_freq = 2412, ic_ieee = 1 '\001', ic_maxregpower
= 20 '\024', ic_maxpower = 63 '?',
ic_minpower = 0 '\000', ic_state = 0 '\000', ic_extieee = 0 '\000',
ic_maxantgain = 0 '\000', ic_pad = 0 '\000',
ic_devdata = 0}
(kgdb) p vap->iv_bss->ni_chan
$4 = (struct ieee80211_channel *) 0xffff
(kgdb) p vap->iv_ic->ic_curchan
$5 = (struct ieee80211_channel *) 0xffffffe04e1cd6a4
(kgdb) p vap->iv_ic->ic_bsschan
$6 = (struct ieee80211_channel *) 0xffffffe04e1cd6a4
(kgdb) quit

As you see IEEE80211_CHAN_ANYC (0xffff) constant is being dereferenced.
I've added "I am in node_set_chan!" on entry to ieee80211_node_set_chan()
to be sure that ni->ni_chan has a real pointer to channel structure rather
than 0xffff. But later that node is freed and a new node is allocated with
ni_chan == IEEE80211_CHAN_ANYC (see last kernel messages).

Also there are strange state changes:

1) SCAN -> RUN followed by SCAN -> INIT. So where is RUN?
2) INIT -> RUN, which is "unexpected".

Please confirm this on master and/or with other drivers. Any ideas what's
going on?

Vasily

History

#1 - 05/29/2016 05:49 PM - swildner

Can you retry with master (from a snapshot for example, http://avalon.dragonflybsd.org/snapshots/x86_64/).

See if the issue still occurs, since we recently upgraded our 80211 stack.

Thanks,
Sascha