pfSense - Bug #11021

ral(4) driver kernel panics in arm64

10/30/2020 06:17 PM - Steve Wheeler

Status:	Resolved	**Start date:**	10/30/2020
Priority:	Normal	**Due date:**	
Assignee:	Steve Wheeler	**% Done:**	0%
Category:	Wireless	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Plus Target Version:		**Affected Version:**	2.5.0
Release Notes:	Default	**Affected Architecture:**	arm64

Description

Testing with an RT2700e card:

```
[2.5.0-DEVELOPMENT][root@2100-2.stevew.lan]/root: pciconf -lv
ral0@pci0:0:0:0:        class=0x028000 card=0x27901814 chip=0x07811814 rev=0x00 hdr=0x00
    vendor     = 'Ralink corp.'
    device     = 'RT2790 Wireless 802.11n 1T/2R PCIe'
    class      = network
```

The driver attaches and the card can be assigned:

```
[2.5.0-DEVELOPMENT][root@2100-2.stevew.lan]/root: ifconfig ral0_wlan0
ral0_wlan0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:15:af:cb:93:c5
        groups: wlan
        ssid "" channel 1 (2412 MHz 11b)
        regdomain FCC country US authmode OPEN privacy OFF txpower 30
        scanvalid 60 wme dtimperiod 1 -dfs bintval 0
        parent interface: ral0
        media: IEEE 802.11 Wireless Ethernet autoselect <hostap> (autoselect <hostap>)
        status: no carrier
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

However trying to bring the interface up causes a kernel panics:

```
[2.5.0-DEVELOPMENT][root@2100-2.stevew.lan]/root: ifconfig ral0_wlan0 up
Fatal data abort:
  x0:                0
  x1: ffff0000403d0000
  x2:             1800
  x3:                0
  x4:              200
  x5: ffff0000403e4960
  x6:                0
  x7: ffff000061bc4cb0
  x8: ffff000001e0f4e8
  x9:                0
 x10:          9d89d88
 x11: ffff00000092e620
```

```
 x12: ffff000000949174
 x13:                0
 x14:             2814
 x15:             2af8
 x16:             27ce
 x17:                0
 x18: ffff0000403e4a20
 x19: ffff000041b86000
 x20:               64
 x21: ffff000041b901d3
 x22: ffff000041b8c858
 x23: ffff000041b8cad0
 x24: ffff000041b8cad8
 x25: ffff000041b90132
 x26: ffff000000aafd64
 x27:              3e7
 x28:                0
 x29: ffff0000403e4a20
  sp: ffff0000403e4a20
  lr: ffff0000002c5380
 elr:                0
spsr:         20000345
 far:                0
 esr:         86000005
panic: vm_fault failed: 0
cpuid = 0
time = 1604094260
KDB: stack backtrace:
#0 0xffff0000005abfec at kdb_backtrace+0x60
#1 0xffff000000562454 at vpanic+0x18c
#2 0xffff0000005622c4 at panic+0x44
#3 0xffff000000964d14 at data_abort+0x1dc
#4 0xffff000000964a34 at do_el1h_sync+0x128
#5 0xffff00000094c874 at handle_el1h_sync+0x74
#6 0xffff0000002c537c at rt2860_init_locked+0xc78
#7 0xffff0000002c1fc0 at rt2860_parent+0xc8
#8 0xffff0000005be300 at taskqueue_run_locked+0x138
#9 0xffff0000005bf874 at taskqueue_thread_loop+0xd0
#10 0xffff000000523ee8 a◆TIM-1.0
```

Tested hostap and infrastructure mode in:

```
2.5.0-DEVELOPMENT (arm64)
built on Fri Oct 30 12:54:36 EDT 2020
FreeBSD 12.2-STABLE
```

History

#1 - 11/09/2020 05:47 AM - Renato Botelho

- Status changed from New to Feedback

- Assignee set to Renato Botelho

- Target version set to 2.5.0

I've merged recent stable/12 which contains a fix for that. Please test it again on when a new round of snapshots is ready

#2 - 11/09/2020 01:42 PM - Steve Wheeler

- Status changed from Feedback to Confirmed

Tested:

```
2.5.0-DEVELOPMENT (arm64)
built on Mon Nov 09 06:54:43 EST 2020
FreeBSD 12.2-STABLE
```

Still appears to panic in the same way:

```
[2.5.0-DEVELOPMENT][root@2100-2.stevew.lan]/root: sysctl debug.trace_on_panic=1
debug.trace_on_panic: 0 -> 1
[2.5.0-DEVELOPMENT][root@2100-2.stevew.lan]/root: ifconfig ral0_wlan0
ral0_wlan0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:15:af:cb:93:c5
        groups: wlan
        ssid "" channel 1 (2412 MHz 11b)
        regdomain FCC country US authmode OPEN privacy OFF txpower 30
        scanvalid 60 wme dtimperiod 1 -dfs bintval 0
        parent interface: ral0
        media: IEEE 802.11 Wireless Ethernet autoselect <hostap> (autoselect <hostap>)
        status: no carrier
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
[2.5.0-DEVELOPMENT][root@2100-2.stevew.lan]/root: ifconfig ral0_wlan0 up
Fatal data abort:
  x0:                0
  x1: ffff0000403cc000
  x2: ffff0000403cd800
  x3:                0
  x4:              200
  x5: ffff0000403e0960
  x6:                0
  x7:               11
  x8: ffff000001e21408
  x9: ffff000000952650
 x10:          9d89d88
 x11: ffff0000009340e4
 x12: ffff000000952820
 x13:                0
 x14:             2847
 x15:         ffffffff
 x16:             27d0
 x17:                0
 x18: ffff0000403e09e0
 x19:              200
 x20:                0
 x21: ffff0000403cc000
 x22:                0
 x23: ffff0000403cd800
 x24: ffff000041b8cad8
 x25: ffff000041b90132
 x26: ffff000000ac089c
 x27:              3e7
 x28:                0
 x29: ffff0000403e09e0
  sp: ffff0000403e09e0
  lr: ffff000000952690
 elr: ffff000000952820
spsr:         20000345
 far: fffe000080799800
 esr:         96000044
panic: vm_fault failed: ffff000000952820
cpuid = 0
time = 1604944942
KDB: stack backtrace:
#0 0xffff0000005b169c at kdb_backtrace+0x60
#1 0xffff000000567994 at vpanic+0x18c
#2 0xffff000000567804 at panic+0x44
#3 0xffff00000096e854 at data_abort+0x1dc
#4 0xffff00000096e574 at do_el1h_sync+0x128
#5 0xffff000000956074 at handle_el1h_sync+0x74
#6 0xffff00000095268c at generic_bs_sr_4+0x3c
```

```
#7 0xffff0000002c5784 at rt2860_init_locked+0xc78
#8 0xffff0000002c23c8 at rt2860_parent+0xc8
#9 0xffff0000005c39b0 at taskqueue_run_locked+0x138
#10 0xffff0000005c4f24 at taskqueue_thread_loop+0xd0
#11 0xffff000000529428 ◆TIM-1.0
```

#3 - 11/12/2020 11:40 AM - Renato Botelho

- Status changed from Confirmed to Feedback

- Assignee changed from Renato Botelho to Steve Wheeler

A new fix was committed by bz@ and imported to our tree. Next round of snapshots will have it

#4 - 11/12/2020 06:44 PM - Steve Wheeler

Testing:

```
2.5.0-DEVELOPMENT (arm64)
built on Thu Nov 12 12:57:06 EST 2020
FreeBSD 12.2-STABLE
```

The system no longer panics when the interface is brought UP. It can now be configured from the GUI. However it throws errors and I cannot actually connect to it:

```
ral0: need multicast update callback
ral0: can't map mbuf (error 27)
ral0: can't map mbuf (error 27)
ral0: can't map mbuf (error 27)
ral0: device timeout
```

#5 - 11/17/2020 06:12 PM - Steve Wheeler

- Status changed from Feedback to Resolved

The kernel panic here is resolved.

We can open a new bug report if this affects more than just my card.