

## Re: Hard(?) lock when reassociating ath with wpa\_supplicant on RELENG\_7

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/stable/2008-07/msg00159.html>

---

- *From:* "Alexandre \"Sunny\" Kovalenko" <[alex.kovalenko@xxxxxxxxxxx](mailto:alex.kovalenko@xxxxxxxxxxx)>
  - *Date:* Fri, 11 Jul 2008 21:07:26 -0400
- 

On Fri, 2008-05-16 at 12:23 -0400, Sam Leffler wrote:

Alexandre "Sunny" Kovalenko wrote:

On Mon, 2008-05-12 at 19:33 -0700, Sam Leffler wrote:

Alexandre "Sunny" Kovalenko wrote:

I seem to be able to lock my machine by going into wpa\_cli and asking it to 'reassoc'. The reason for question mark after "hard" is that debug information (caused by wlandebug and athdebug) is being printed on the console. The only way to get machine's attention is to hold power button for 8 seconds.

So this is just livelock due to console debug msgs.

I am not sure, I have parsed this well enough, so I will try to clarify: machine becomes unresponsive *\*without\** any debugging turned on, to an extent that pressing the power button twice *\*does not\** generate ACPI console message (something to the tune of "going into S5 already -- gimme a break"). If I turn ath debugging on, I do see those messages, and only them, scrolling on the console.

Guess I misunderstood you.

I have finally got enough time and equipment to investigate this further. Here are some conclusions:

-- at this point (RELENG\_7 as of July 9th around 15:30 EST) it is indeed a livelock.

-- all system does, is executing ath\_intr (if\_ath.c) in the tight loop

Re: Hard(?) lock when reassociating ath with wpa\_supplicant on RELENG\_7

with the same status --- 0x1000 AKA HAL\_INT\_MIB. In order to eliminate possibility that I have caused livelock with the debug messages, I have put conditional panic() into ath\_intr, as soon as sc->sc\_stats.ast\_mib reaches 10,000. Without any kind of the debug messages, it will be triggered within 40-60 seconds after starting of wpa\_supplicant.

--- I suspect that comment below, might not hold true on my equipment

```
if (status & HAL_INT_MIB) {
sc->sc_stats.ast_mib++;
/*
 * Disable interrupts until we service the MIB
 * interrupt; otherwise it will continue to fire.
 */
ath_hal_intrset(ah, 0);
/*
 * Let the hal handle the event. We assume it will <=====
 * clear whatever condition caused the interrupt. <=====
 */
ath_hal_mibevent(ah, &sc->sc_halstats);
ath_hal_intrset(ah, sc->sc_imask);
}
```

My hardware is:

```
ath_hal: 0.9.20.3 (AR5210, AR5211, AR5212, RF5111, RF5112, RF2413,
RF5413)
ath0: <Atheros 5212> mem 0xedf00000-0xedf0ffff irq 17 at device 0.0 on
pci3
ath0: [ITHREAD]
ath0: using obsoleted if_watchdog interface
ath0: Ethernet address: 00:16:cf:26:2f:3f
ath0: mac 10.3 phy 6.1 radio 10.2
```

My wpa\_supplicant.conf is:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=wheel
eapol_version=2
```

```
network={
ssid="XXXXXXXXXXXX"
scan_ssid=1
priority=1
proto=WPA
pairwise=TKIP
group=TKIP
key_mgmt=WPA-PSK
psk="xxxxxxxxxxxxxxxxxxxxxxxx"
}
```

Access point is Netgear WNDR3300-1B with 11N and 11G SSID set up to different values. Only 11G SSID is configured in wpa\_supplicant.conf. In the test setup, AP is with 10' (3m) from the laptop.

Re: Hard(?) lock when reassociating ath with wpa\_supplicant on RELENG\_7

Re: Hard(?) lock when reassociating ath with wpa\_supplicant on RELENG\_7

AP is successfully used by handful of Windows clients (including this same laptop) and iBook G4.

Neither wpa\_supplicant with '-d -d' nor wlandebug 0xFFFFFFFF show anything but normal scan.

athdebug 0xFFFFFFFF loops with ath\_intr: status 0x1000 until I power down my laptop.

I would appreciate any suggestion on what I can investigate further --- at this point I have comfortable console setup and should be able to field requests for further information much better.

--

Alexandre "Sunny" Kovalenko ( ;5:A0=4@ >20;5=:>)

---

freebsd-stable@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-stable>

To unsubscribe, send any mail to "freebsd-stable-unsubscribe@xxxxxxxxxxx"