FreeBSD: 802.11 status

Adrian Chadd <adrian@freebsd.org>

(**This is 100% me and 0% my current employer**.)

What's been happening

- wiki.freebsd.org
  - Now sports a "WiFi" page, with the beginnings of documentation
    - I could do with more help documenting things here
  - ath(4) and ath_hal(4) documentation project
    - Lists all (as far as I know) supported MAC and radio chips
    - Beginning of HAL and hardware documentation
      - Based on what's already in the driver
      - .. no, this isn't from Atheros or any datasheets
      - .. you'd be surprised what you can glean just from the driver.

What's been happening (ctd)

- net80211
  - 802.11n negotiation updates to spec - bschmidt@
  - general locking fixes - adrian@
  - 802.11n HT channel width change - adrian@
  - 802.11s updates from draft to spec - monthadar@
  - 802.11n TX/RX aggregation debugging - adrian@, bschmidt@
  - DFS AP/STA fixes - adrian@
  - Wifi simulator (wtap) - monthadar@

What's been happening (ctd)

- iwn(4) - bschmidt@
  - Updated to support current generation(s) of Intel 802.11n NICs
  - Actively finding/fixing 802.11n issues, especially around TX aggregation and rate handling
- bwn(4)
  - Some bug fixes
  - .. lacking chipset support updates and general debugging
  - .. ie, lacking a maintainer
- mwl(4)
  - Works fine if TX aggregation is disabled
  - (debugging in progress)

What's been happening (ctd)

- ral(4) - bschmidt@, ray@
  - bschmidt@, ray@ and the community have been working on updating the rt support from OpenBSD
  - Focusing on basic NIC support, then extend with 802.11n support

What's been happening (ctd)

- ath(4) - adrian@
  - 802.11n features - sponsored by **HobNob, Inc.**
    - TX/RX aggregation, BAR handling, software queues/retries, channel width change support
  - Chipset support
    - Fixed AR9280, AR9285 support
    - Implemented AR9287 support
    - General radio/baseband calibration fixes
  - Driver support
    - Fixed _lots_ of concurrency related issues
      - Eg - concurrent TX, RX and reset/channel change
  - Rate control support
    - .. very basic 802.11n awareness, "good enough"

What's missing for 802.11n?

- net80211
  - 802.11n negotiation fixes are in 9.x
  - No plans to backport to 8.x
- iwn(4)
  - It works - just use it
  - bschmidt actively ports fixes back to 9.x
- mwl(4)
  - It works - disable TX aggregation for now (-ampdutx)
- ath(4) - HEAD only! (No 11n support on < 10-HEAD)
  - It works - don't use bgscan (-bgscan), don't scan during live traffic, broken AP mode power save support

Current issues (net80211)

- There's a lack of locking in net80211
  - Too many thread contexts:
    - various user processes -> ioctl()
    - net80211 taskqueue
    - swi callout()
    - driver taskqueue
    - driver interrupt handler
    - various user processes -> tx() -> vap_start()
  - Lots of "state" checking occurs whilst holding no node or com lock
    - They're only held when manipulating lists, not always when checking state
  - Reentrant paths
    - RX completion -> net80211 -> IP -> TX frame

Current issues (net80211) (ctd)

- ieee80211_node handling
  - A previous commit changed the refcount semantics
    - Before: last refcount owned by the node list, would be purged by decrementing the refcount to 1, then garbage collecting it and freeing it by decrementing refcount to 0
    - Now: last refcount orphans the node and frees it
      - Thread A: dec's ref to 0, frees
      - Thread B: inc's ref, but thread A has already freed it, so it increments a now-freed node and returns t
- Atomic operations do not always replace locks!

Current issues (net80211) (ctd)

- ieee80211_sta_join1()
  - It just replaces iv->iv_bss
  - Drivers may be using it
  - Combined with the above refcounting issue, stale nodes can be referenced
    - .. or, as I've occasionally seen, partially setup nodes!
  - This requires some (better) locking!

Current issues (ctd)

- Drivers have the same problem
  - Concurrent channel change/reset, ioctl, TX, RX
  - ath(4) solves it via "pretend" states, serialising concurrent TX, RX, reset, etc
- Drivers can't hold locks during RX or TX completion
  - iwn(4) just drops the IWN_LOCK() before calling ieee80211_input(), then reacquires it again
  - This all requires much more thought to solve!
    - Perhaps batch RX and TX completion and separate "drain hardware queue" and "handle mbufs", rather than complete packet-at-a-time

What's next?

- power save handling support - AP
  - Requires driver and net80211 support
  - PS-POLL - send _one_ frame at a time to the driver
  - .. if the driver has a queue of frames, drain those first
  - .. then drain the net80211 power save queue frames
- Migrate (more) TX aggregation support into net80211
- Plan out better net80211/driver locking
  - Linux solution - "grab mac80211 lock before entering tx/rx handling"
  - Simple, but scalable for 802.11n/802.11ac?

What's next? (adrian)

- I'm next going to work on:
  - Fix/improve net80211/ath locking, especially in the TX aggregation path
  - Work with bschmidt@ to improve AP power save support in net80211
  - .. then improve the power save support in ath(4)
  - Fix scan/bgscan, so 802.11n traffic isn't simply dropped (which causes 802.11n sessions to hang)
  - Add some better diagnostic tools for net80211/ath(4) - to log TX/RX path decisions (to debug traffic stalls)
  - Upcoming chipset support
    - AR93xx, AR94xx, AR95xx HAL from Atheros
  - (Lots) more documentation and tutorials!

The future ?

- Improved regulatory support
  - Per-country entries, rather than "regulatory domain"
- DFS / radar support
  - mwl(4) supports it in firmware
  - ath(4) supports it in software - requires a radar pattern matcher driver (sys/dev/ath/ath_dfs/)
  - .. already prototyped and tested, works well, but requires regulatory testing before it can be used
  - net80211 DFS support works well, both AP/STA
  - per-packet TPC, dynamic power control
- 802.11ac support?
  - .. it's rapidly approaching, it should be thought about!

What we're lacking!

- Developers!
- Drivers, ported from *BSD/Linux!
  - Various USB/PCI NICs, including:
    - ath(4) USB NICs (AR9170), (AR7010, AR9287)
- Maintainers for:
  - mwl(4) / bwn(4) / bwi(4)
  - an(4) - doesn't use net80211, may be deprecated
  - wi(4) - needs updates from OpenBSD to work on all NICs
    - .. but only if you care
  - .. and anything not ath(4) (adrian@), iwn(4) (bschmidt@) and ral (bschmidt@, ray@)

What we're lacking! (ctd)

- More regression testing!
  - monthadar@ and adrian@ are working on it
  - Thank god for wtap(4)
- 802.11n aware rate control
  - Multi-rate retry
  - Handling various 802.11n options
- 802.11n >2 stream support
  - No 3-stream devices are yet supported
  - It's likely that the AR93xx/AR94xx chips will be the first supported 3 stream devices
- uAPSD power save support
- Station-side power save (sleep, frame queuing) support

Thankyou!

- Adrian Chadd <adrian@freebsd.org>
- freebsd-wireless@freebsd.org
- http://wiki.freebsd.org/WiFi/
- http://wiki.freebsd.org/dev/ath(4)
- http://wiki.freebsd.org/dev/ath_hal(4)