sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

Ath10k Candela Technologies CT 10.4 Firmware

The CT 10.4 firmware is a modified version of the official firmware from Qualcom-Atheros based on the 10.4 code. It should support all features available in the upstream 10.4 firmware as well as additional features. The firmware is compiled for different target NICs/chipsets, be sure to get the one that works for your particular NIC!

Want to help fund new ath10k CT firmware features with modest contributions? See the ath10k kickstarter page.

This is 'wave-2' firmware, and is known to support at least these NICS:

- WLP1200 heat-sink pcie -> mini-pcie adapter
  The CUS239 related boards require extra cooling. The WLP1200 works well for this, but may be hard to find in smaller quantities and/or short lead times.
- Zcomax AC-924 / CUS239 with QCA9984
  NOTES: Requires external 2-amp 5v power supply (and ground) on the 5v solder point when used in x86 (and probably other platforms that do not have special built-in 5v power on the pcie-bus.) We had success using the 5v pin on an SATA/floppy power header, connected with 18 gauge wire so it can carry the desired power. Also may require heat-sink or other active cooling to keep the board from over-heating.
- Compex WLE1216V5-23 / CUS239 - with QCA9984
  NOTES: Requires external 2-amp 5v power supply (and ground) on the 5v loop connector when used in x86 (and probably other platforms that do not have special built-in 5v power on the pcie-bus.) We had success using the 5v pin on an SATA/floppy power header, connected with 18 gauge wire so it can carry the desired power. Also may require heat-sink or other active cooling to keep the board from over-heating.
- Compex WLE650V5-18 - with QCA9888
  This is a 2x2 MU-MIMO capable NIC. It is similar to the 9984 except that it is only 2x2. It uses the **9888** firmware images. It does not require extra cooling or external power. Early versions of this NIC with similar model number had the QCA9886 chipset, but new ones only use the QCA9888 chipset it seems.
- WLE1200v5-22 / CUS239 with QCA9980 (EOL)
  NOTES: Requires external 2-amp 5v power supply (and ground) on the 5v loop connector when used in x86 (and probably other platforms that do not have special built-in 5v power on the pcie-bus.) We had success using the 5v pin on an SATA/floppy power header, connected with 18 gauge wire so it can carry the desired power. Also may require heat-sink or other active cooling to keep the board from over-heating.
- WLE1216V5-20 5Ghz with QCA9984
  This card does not need external power, but it still runs pretty hot. You will likely need some active air flow to keep it under 80 deg C (as reported by the NIC itself). We are not sure what is the maximum operational temperature, so maybe above 80 deg C is fine. This board uses a unique BMI-id, and your board-2.bin file may not have the right entries. If that is the case, then you can try this board-2-ct.bin. It would normally be placed at: `/usr/lib/firmware/ath10k/QCA9984/hw1.0/board-2.bin`.
- WLE1216V2-20 2.4Ghz with QCA9984
  This card does not need external power, but it still runs pretty hot. You will likely need some active air flow to keep it under 80 deg C (as reported by the NIC itself). We are not sure what is the maximum operational temperature, so maybe above 80 deg C is fine. This board uses a unique BMI-id, and your board-2.bin file may not have the right entries. If that is the case, then you can try this board-2-ct.bin. It would normally be placed at: `/usr/lib/firmware/ath10k/QCA9984/hw1.0/board-2.bin`.

To use this firwmare, download one of the firmware images and rename it firmware-5.bin. The command below should work on most systems:

```
cp firmware-5-ct-full-community.bin /lib/firmware/ath10k/QCA99X0/hw2.0/firmware-5.bin
```

Get the **board.bin** file from the official firmware site, for example, 9980:

```
# ls -l /usr/lib/firmware/ath10k/QCA99X0/hw2.0/
lrwxrwxrwx 1 root root     37 Jan 15 17:07 board.bin -> boardData_AR900B_CUS239_5G_v2_001.bin
-rw-rw-r-- 1  500  500  12064 Oct 13 17:26 boardData_AR900B_CUS239_5G_v2_001.bin
-rw-rw-r-- 1  500  500  12064 Oct 13 17:26 boardData_AR900B_CUS260_2G_v2_002.bin
-rw-r--r-- 1 root root 523924 Jan 22 12:43 firmware-5.bin
```

Or, **board-2.bin** for 9984 or 9888:

```
[root@ath-9984 ~]# ls -l /lib/firmware/ath10k/QCA9984/hw1.0/
total 1200
-rw-rw-r-- 1  500  500  12144 Jun  2 15:56 board-2.bin
-rw-r--r-- 1 root root 589204 Jul 15 10:30 firmware-5.bin
-rw-rw-r-- 1  500  500 591308 Jun  2 15:56 firmware-5.bin_10.4-3.2-00072
-rw-rw-r-- 1  500  500  30479 Jun  2 15:56 notice.txt_10.4-3.2-00072
```

Then, reboot or reload the ath10k_pci driver to start using the new firmware. Look in the kernel logs (or dmesg) to make

sure the firmware version contains '-ct', such as: `10.4.3-ct-xtH-007-a5ece62`

For more advanced configuration options, see below.

There are two types of CT firmware: **The community version supports all features EXCEPT connecting multiple vifs to the same AP when using encryption.** The community version may be used for any purpose allowed by the official firmware from Qualcom-Atheros, including commercial applications. See below for firmware images compiled for more specific purposes. If using ath10k-ct driver (which is suggested), then the suggested firmware variant is: **firmware-5-ct-htt-mgt-community**.
firmware-5-ct-full-community.bin (latest) 9980 | 9984 | 4019 | 9888/9886.

The non-commercial firmware from Candela Technologies does support multiple station vifs connecting to a single AP (really, it supports rx-software-crypt, which is the enabling feature). The non-commercial firmware is NOT freely available. It is restricted to non-commerical use unless you arrange a commercial-use license with Candela Technologies. Contact sales@candelatech.com for additional information on this topic.

Any and all bug reports involving this firmware (and the modified kernels from Candela Technologies) should be sent to support@candelatech.com. Qualcom-Atheros is not responsible for the changes made to the modified firmware and should not be bothered with bug reports relating to it. Reports of success are welcome as well! To submit a useful bug report, please include kernel logs, especially any firmware crash logs. These crash logs are often chunks of ascii hex. Candela has tools that can usually decode these, but due to NDA issues, these tools may not be shared with the general public. Candela engineers will attempt to decode any reported crashes and provide help as possible. Note that unless you have a contract with Candela that provides otherwise, any help with bugs may be slow or even not much actual help at all. Please also report the kernel version and any other details about how the problem was triggered.

Candela offers paid support options, please contact sales@candelatech.com if you have interest.

See the bottom of this page for some common crash signatures.

CT 10.4 Firmware Differences from Official QCA Firmware

The ath10k 10.4 firmware from Candela is based on the 10.4.3.3-25 firmware from QCA, but has some added features and fixes (and probably a few added bugs). Some notable differences are listed below. Most of these require the kernel modifications in the 4.4 or later Candela Linux kernels, but the firmware images should work on un-modified kernels for the standard features.

Most of the 10.1 CT features have now been ported to 10.4.

- Optimized tx-credits handling. Host driver can configure maximum tx-credits and firmware will return credits immediately so less flush-mgmt hacks are needed on host.
- Supports reporting tx-rate to the sending stack.
- Supports configuring the firmware tx-buffer count below 1024 (diet variants only, since they compile out the descriptor-management code that likes to assert when too few tx-descriptors are configured.)
- Supports rx-software-crypt (non-commercial version only, unless you purchase commercial license.). This enables having multiple station VIFs connect to the same AP. Decrypt is done on CPU, so it is relatively slow, especially on slower CPUs.
- Support IBSS (ADHOC) mode.
- Optimized firmware memory usage to be more stable in strange configurations.
- Lots of bug fixes and hardening related to memory usage issues.
- Fix 802.11r (fast roaming) in station mode.
- Supports up to 36 station VIFS (64 with 9984 and 9888).

Known CT 10.4 Firmware/Kernel Bugs

- See the ath10k bugs page to view or report bugs.

To take advantage of all of the CT firmware features, please consider using one of these kernels at https://github.com/greearb.

The CT firmware has a separate release number appended to the end of the version string. If the binaries do not yet exist, then the features that define them have not yet been implemented.

Ath10k CT 10.4.3 Beta 13

- This is code is not being changed much, and should be considered for stable use now.

See BETA release notes for details.

firmware-5-ct-full-community.bin 9980 | 9984 | 4019 | 9888
No CT-HTT-MGT feature, no upstream features compiled out (no diet), available for commercial and non-commercial use at no charge. This firmware should be a drop-in replacement for stock QCA firmware.

firmware-5-ct-community.bin 9980 | 9984 | 4019 | 9888
No CT-HTT-MGT feature. Swbmiss, beacon filtering, roaming code, descriptor-mgt is compiled out.

firmware-5-ct-non-commercial-full.bin 9980 | 9984 | 4019 | 9888
No CT-HTT-MGT feature, no upstream features compiled out (no diet), supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

These htt-mgt firmwares require a driver patch. See release notes.

firmware-5-ct-full-htt-mgt-community.bin 9980 | 9984 | 4019 | 9888

Has CT-HTT-MGT feature, no upstream features compiled out (no diet), available for commercial and non-commercial use at no charge.

firmware-5-ct-htt-mgt-community.bin 9980 | 9984 | 4019 | 9888

Has CT-HTT-MGT feature. This is a diet build with un-needed features compiled out. This is the suggested variant to use if you are unsure.

firmware-5-ct-htt-mgt-community-qcache.bin 9980 | 9984 | 4019 | 9888

Has CT-HTT-MGT feature. This is a diet build with un-needed features compiled out. This build enables qcache swap-firmware-memory-to-host feature, like upstream QCA firmware. This may allow more stations to associate. It may work around some strange bugs reported by one user, but in general it needs more testing. It received more testing around Octobe 6, 2020, and serious bugs were found as soon as it started swapping memory to host. This qcache support is NOT ready for general use at this time. --Ben

firmware-5-ct-non-commercial-full-htt-mgt.bin 9980 | 9984 | 4019 | 9888

Has CT-HTT-MGT feature, no upstream features compiled out (no diet), supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

Ath10k CT 10.4 Release 13

- Dec 13 2018: Fix ct-sta mode, it was not installing bcast keys properly. The symptom was MMIC failures among other things.
- Dec 17 2018: The TSF is only allocated when a vdev goes UP, not started. But the beacon code was testing for 'STARTED'. This lets the beacon code hit an assert where tsf-id is not assigned for an AP. Fix this by checking for UP in most code.
- Dec 17 2018: Attempt to fix live-lock related to cleaning up cached pfsched commands. This hopefully resolves problems with an earlier patch I made in this area to work around a different problem.
- Dec 19 2018: Add check for null tid/peer/vdev in tx stat code. This could cause crashes because a peer can be deleted with pending frames in the tx queues, so the tx complete callbacks happen after peer object is gone.
- Jan 2, 2019: Rebase patches to make 9980 bisectable.
- Jan 2, 2019: Fix scheduling related assert when wal-peer is deleted with pending tx buffers (bug 54, and others)
- Jan 7, 2019: Fix specifying retransmits for AMPDU frames. It was previously ignored since it is a 'software' retransmit instead of a hardware retransmit.
- Jan 9 2019: Fix potential way to get zero rates selected (and then assert)
- Jan 18 2019: pfsched has specific work-around to just return if we find invalid flags AND if we are in an out-of-order situation. Maybe this is last of the pfsched related issues (bug 54 and similar).
- Jan 24 2019: The rcSibUpdate method can be called concurrently with IRQ tx-completion callback, and that could potentially allow the tx-completion callback to see invalid state and assert or otherwise mess up the rate-ctrl logic. So, disable IRQs in rcSibUpdate to prevent this. Related to bug 58.
- Jan 28 2019: Ensure that cached config is applied to ratectrl objects when fetched from the cache. This should fix part of bug 58.
- Jan 28 2019: Ensure that ratectrl objects from cachemgr are always initialized. This fixes another part of bug 58.
- Jan 30 2019: Better use of temporary rate-ctrl object. Make sure it is initialized, simplify code path. This finishes up porting forward similar changes I made for wave-1 firmware long ago, and fixes another potential way to hit bug-58 issues.
- Jan 30 2019: Cachemgr did not have a callback for when memory was logically freed. This means that peers could keep stale references to rate-ctrl objects that were in process of being DMA'd into to load a different peer's rate-ctrl state. This was causing the bugcheck logic to fail early and often, and I suspect it might be a root cause of bug 58 as well. The fix is to add a callback and set any 'deleted' memory references to NULL so that we cannot access it accidentally. Thanks to excellent logs and patience from the bug-58 reporter!
- Feb 8, 2019: Fix rate-ctrl assert related to bad logic that tried to guess that lower bandwidth probes were automatically successful if higher was. The NSS mismatch that can happen here caused the assert. Just comment out the offending code (per comment from original QCA code). This is bug 69.
- Feb 10, 2019: Fix bssid mis-alignment that broke 4-addr vlan mode (bug 67). Original buggy commit was commit 2bf89e70ecd1eaf8d1c70df7d32f99d1e1c47fe3 dev-ds: Better packing of wal_vdev struct.
- Feb 27. 2019: Support up to 32 AP vdevs. Previous to this, stack would be corrupted if you went past 16 AP vdevs.
- Feb 28, 2019: Support beacon-tx-wmi callback message. This lets driver properly clean up beacon buffers. In wave-1, this could crash the entire OS, but I didn't see the same crashes in wave-2, so maybe it is fixed in some other way. Add the feature regardless as it seems proper.
- March 6, 2019: Fix tx-status in case of NO-ACK. Previously random garbage was returned. It is mostly a reporting issue as far as the host is concerned.
- March 12, 2019: Fix crash when tearing down VI TID when pending frames exist. Could reproduce this

while doing rmmod when VI traffic was flowing and PMF was enabled but broken. Bad luck could rarely cause it to happen in more normal config too.

- March 12, 2019: Support offloading decrypt of PMF blockack frames to the host. This lets us do blockack with PMF and rx-sw-crypt. Normal hwcrypt scenarios would not need this.
- March 22, 2019: Re-work problematic patch that attempted to fix transmit on non-QOS tids. It appears buggy in several ways, hopefully improved now. This was introduced last fall. See github bug 78.
- March 28, 2019: Fix off-channel scanning while associated in proxy-station mode.
- March 29, 2019: Fix sometimes sending mgt frames on wrong tid when using htt-mgt. This bug has been around since I first enabled htt-mgt mode.
- April 8, 2019: When setting keys, if high bit of high value of key_rsc_counter is set to 0x1, then the lower 48 bits will be used as the PN value. By default, PN is set to 1 each time the key is set.
- April 8, 2019: Pack PN into un-used 'excretries' aka 'num_pkt_loss_excess_retry' high 16 bits. This lets us report peer PN, but **only** if driver has previously set a PN when setting key. This is done so that we know the driver is recent enough to deal with the PN stat reporting.
- April 16, 2019: Support specifying tx rate on a per-beacon packet. See ath10k_wmi_op_gen_beacon_dma and ath10k_convert_hw_rate_to_rate_info for API details. Driver needs additional work to actually enable this feature currently.
- April 30, 2019 Compile out tx-prefetch caching logic. It is full of tricky bugs that cause tx hangs. I fixed at least one, but more remain and I have wasted too much time on this already.
- May 9, 2019 Start rate-ctrl at mcs-3 instead of mcs-5. This significantly helps DHCP happen quickly, probably because the initial rate being too high would take a while to ramp down, especially since there are few packets sent by the time DHCP needs to start. This bug was triggered by me decreasing retries of 0x1e (upstream default) to 0x4. But, I think it is better to start with lower initial MCS instead of always having a very high retry count.
- May 15, 2019 Fix problem where rate-ctrl sometimes used rix of 0x0.
- May 15, 2019 Allow raw-tx of encrypted frame. Requires a patch to the driver to use raw mode when skb has WEP flag enabled AND skb is flagged to not be encrypted. Lightly tested.
- May 16, 2019 Fix tx-hang that happened when rate-ctrl chose an OFDM rate for 20Mhz and sent that as AMPDU. To fix, limit to (V)HT rates if peer is (V)HT. It seems that MCS0 (V)HT20 should have as good of a chance of being detected as CCK or OFDM.
- June 6, 2019 Disable TX-BFEE, TX-BFER for IBSS connections. I suspect this is part of the tx-hang issue seen with IBSS between two 9984 radios.
- June 12, 2019 Fix rx-rate reporting in 'fw_stats' logic. This was at least partly due to regressions I had added earlier when working on some multi-vdev enhancements.
- June 12, 2019 Fix case where extd peer-stats were not always populated. The stats gathering code did not handle error conditions well.
- June 24, 2019 Start rate-ctrl at minimal values to help DHCP work better for far-away peers.
- July 24, 2019 Fix old regression that made /a (and probably /b/g) perform poorly, at least on diet-compiled images.
- Aug 8, 2019 Improve a/b/g rate-ctrl by damping the PER swings caused by the all-or-nothing logic of transmitting non-block-ack frames one at a time.
- October 9, 2019: Fix rate-ctrl issue with 160Mhz. See bug https://github.com/greearb/ath10k-ct/issues/94 Thanks to swg0101 for doing detailed debugging to narrow down this issue.
- October 15, 2019: Only send beacon tx completion events if we can detect CT driver is being used (based on ATH10k_USE_TXCOMPL_TXRATE2 | ATH10k_USE_TXCOMPL_TXRATE1 flags being set). This should help CT firmware work better on stock driver.
- October 31, 2019: Compile out peer-ratecode-list-event. ath10k driver ignores the event.
- November 1, 2019: Fix rate-ctrl related crash when nss and other things were changed while station stays associated. See bug: https://github.com/greearb/ath10k-ct/issues/96
- December 6, 2019: Fix 160Mhz problem caused by logic that did not take into account the fact that 160Mhz has only 1/2 of the NSS of lower bandwidths in the rate table.
- December 13, 2019: Fix case where transmit power was at least sometimes not set properly. Bug was caused by bad patch merging it seems.
- Jan 16, 2020: Fix crash that is probably related to AP rekey problem.
- Jan 27, 2020: Fix rate-ctrl problem that broke xbox communication in some cases. Big thanks to Neil Aspinall for prompt and persistent bisecting!
- April 24, 2020: Fix tids > 425, which caused pool to overflow uint16 bounds checks. Change bounds check to 32-bit numbers.
- April 24, 2020: Tweak RAM usage so that 9888 diet + htt build can support 200 stations and 8 vdevs.
- April 24, 2020: Tweak RAM usage so that 4019 diet + htt build can support 164 stations and 8 vdevs.
- June 30, 2020: Enable building with qcache peer swapping enabled. Upstream QCA uses this option, though I had previously disabled it. Now images supporting this can be built again.
- October 5, 2020: Fix some qcache mode bugs related to regression I had done some years ago. (comparing mac-addr in AST lookup, etc). More qcache bugs remain.
- Fall of 2020: Improved compiler options to build smaller sized binaries.

See Release notes for details.

firmware-5-ct-full-community-13.bin 9980 | 9984 | 4019 | 9888

No CT-HTT-MGT feature, no upstream features compiled out (no diet), available for commercial and non-commercial use at no charge.

firmware-5-ct-community-13.bin 9980 | 9984 | 4019 | 9888

No CT-HTT-MGT feature, some un-used and/or useless upstream features compiled out (diet), available for commercial and non-commercial use at no charge.

firmware-5-ct-non-commercial-13.bin 9980 | 9984 | 4019 | 9888

No CT-HTT-MGT feature, swbmiss, beacon filtering, roaming code, descriptor-mgt compiled out, supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

firmware-5-ct-non-commercial-full-13.bin 9980 | 9984 | 4019 | 9888

No CT-HTT-MGT feature, no upstream features compiled out (no diet), supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

These htt-mgt firmwares require a driver patch. See release notes.

firmware-5-ct-htt-mgt-community-13.bin 9980 | 9984 | 4019 | 9888

If unsure, this is the suggested firmware to use.
Has CT-HTT-MGT feature, features not in upstream driver are compiled out (diet mode).
Available for commercial and non-commercial use at no charge.

firmware-5-ct-full-htt-mgt-community-13.bin 9980 | 9984 | 4019 | 9888

Has CT-HTT-MGT feature, no upstream features compiled out (no diet), available for commercial and non-commercial use at no charge.

firmware-5-ct-non-commercial-htt-mgt-13.bin 9980 | 9984 | 4019 | 9888

Has CT-HTT-MGT feature, swbmiss, beacon filtering, roaming code, descriptor-mgt compiled out, supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

firmware-5-ct-non-commercial-full-htt-mgt-13.bin 9980 | 9984 | 4019 | 9888

Has CT-HTT-MGT feature, no upstream features compiled out (no diet), supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

Ath10k CT 10.4 Release 10

- Fix an assert related to tx scheduling. This hopefully fixes what appears to be a regression that I added some time back.
- Other stability improvements, including regression fixes from some tricky bugs introduced in earlier releases.
- Allow compiling for IPQ4019 chipset.
- Firmware will now send txbf frames to the host (driver) if the TXBF (0xF00000001) set-special feature is enabled, or when the radio is in monitor mode. But, if the frame is consumed by the txbf_cv logic, then the pkt cannot be delivered to the host in this manner. Instead, a WMI event will be sent and host can find the txbf_cv data in shared mmory. See ath10k_wmi_event_txbf_cv_mesg() in ath10k-ct driver.
- Support rx-all-mgt option. When enabled, the firmware will deliver all management frames that it can to the host. No RX filters are changed when this option is enabled.
- Fix at least some problems with sending tx-beamforming frames to SU-MIMO peers. Looks like this was a regression in my code.
- Fix a crash in rate-ctrl due to nss mismatch. This was something I introduced while trying to fix other bugs in rate-ctrl some time back.
- Attempt to fix a sw-peer-key object leak in IBSS mode. The peer key code is very complex, and shares some pointers as union members. I think I fixed at least some of the issues, but would not be surprised if more exist.
- Improve ath10k user guide to document CT firmware features: https://www.candelatech.com/ath10k-ug.php
- Add ct-special option to configure the txbf sounding time. See ath10k-ug.php
- Fix crashes related to deleting peers while they are in power-save mode. Reported by LEDE user on r7800 with 9984 NIC.
- Make rate-ctrl txbf probe work better. If enabled, the rate-ctrl logic will periodically send out probes at an NSS that can to txbf. Previously, txbf probes would not reliably happen if both AP and peer had the same nss (ie, 2x2 talking to 2x2). To enable this feature, you need to enable the fwtest-cmdid number 20.
- Report rx-timeout error counters. These were previously un-reported, though the field existed in the wmi struct already.
- txbf: Ignore frames not destined for us. If NIC is in promisc mode, it could acquire and process NDPA frames that were not destined for it. Check the dest-MAC and ignore frames not for us (pass them up the stack for monitor mode instead of save them in the peer's rate-ctrl logic.)
- Add custom-stats support, for rx-reorder-stats. Similar to what I did for wave-1.
- Disable AMSDU for IBSS. This now matches what I did for peregrine. It seems to work better this way, though I did not debug it in detail.

- Enable the set-special command to re-enable AMSDU for IBSS if user wants to experiment.
- Fix bug where dbglog did not disable IRQs, so if you made dbglog messages from the IRQ handler, it could cause corruption that could crash the firmware and/or corrupt the log message buffers.
- Don't assert if there are no buffer descriptors for RX of non-data frame.
- Retry any stuck block-ack sessions every 20 seconds instead of just disabling BA for ever when we get too many failures.
- Fix SGI flag when reporting tx-rate info. The flag moved since wave-1 days, and I did not notice that when I ported my changes forward to wave-2.
- Allow disabling special CCA handling for IBSS txqs. Earlier testing indicated this might improve throughput in some testing on 9984 chips in IBSS mode, but subsequent testing looks about the same without it. Since I do not really understand what this setting exists for, leave it at upstream defaults. A new set-special API command (0x12) can be used to enable this hack for testing. Setting 0x1 bit disables special CCA handling for non-beacon IBSS txqs, setting 0x2 bit disables it for beacon queues as well.
- When calculating the rx-address filter (affects ACK & BLOCK-ACK, among other things), to not add in monitor interfaces if other interfaces are up. There is no need for a monitor device to ACK frames.
- Fix key leak in monitor mode.

Ath10k CT 10.4 Release 9

- Build images for the 9888 chipset.
- Fix channel parsing for vht160 mode. Should be compatible with the way ath10k wants to do it, and hopefully doesn't break whatever driver wants to do it the new and weird way.
- Disable WAR that ignored the driver setting opmode to 80Mhz on a NIC that supports 160Mhz. This WAR broke the ability for a station to configure itself to only 80Mhz on these chips.
- Port forward rate-ctrl change from 10.1 CT firmware that will cache tx-status if the rate-ctrl object is not currently swapped in from the host memory. This keeps the rate-ctrl logic from getting stuck at low rates when using 30+ stations and fast UDP download to all of them. This is implemented a bit differently from 10.1, hopefully better. Might can backport that some day if desired.
- Use the patch-allocram for 9888 target. This should save a bit of RAM, and gives good debugging hooks in case we need to go exploring.
- Let driver configure larger max-amsdu (up to 31 is allowed). This improves tx rate somewhat when packets are small.
- Probe requests logic had an un-initialized variable that could cause them to be sent at invalid tx rates. This was introduced by me some time ago. It is now fixed.
- Allow compiling with gcc 4.7 and fix the many compile warnings it found. Most were probably not serious, but a few, especially for the 9888 target, might have caused buffer overflows and such.
- Backport latest 3.4.71 firmware to this code base.
- Compile out COEX code in diet builds in order to save memory.
- Backport latest 3.4.82 firmware to this code base.
- Fix some type-safety issues in WDS logic. Might fix WDS mode in CT firmware.
- Comment out a line of code in wlan_vdev.c that came in with 3.4.71 and made multiple vdev performance with 9888 (at least) work poorly.
- Modify firmware to not ask for txq prefetch for self-peers. It is useless, at best, since the driver has no idea about self-peers since the AST-add event is not sent to the driver, and thus will not be able to fetch anything.
- The firmware tries to cache rate-ctrl objects in the host (driver) memory. But, with lots of active stations, this appears to cause constant cache swapping and in the end, rate-ctrl fails to work well at all. CT Firmware has lots of RAM savings, especially when using fewer than 64 vdevs, so allow users to configure more than the default of in-ram rate-ctrl objects. As long as firmware RAM is available, allocating as many rate-ctrl objects as possible (up to number of peers) is probably a good idea. Setting value to 0 means use firmware defaults.
- Fix channel reservation logic. This has been broken for a long time in CT firmware, at least when using multiple station vdevs. Somehow, it mostly worked before, but the bug became appearant lately. Tracked it down and fixed it I did.
- Fix key-setting bug that broke sending the EAPOL 2/4 in some cases. This was a bug I introduced some time back while trying to fix .11r and simplify the key handling logic. (Patch to wpa_supplicant fixed the race with sending the 4/4 and setting the key...un-patched supplicant will still have this race and the 4-way auth will not work as reliably.)
- Increase amount of active-tids that can be scheduled. This fixes a tx-stall seen with many station vdevs.
- Fix bug in upstream code that would cause the maximum peer to never be scheduled for tx.
- Fix crash when some rate indices had zero available rates. This was seen when specifying that a station should only transmit on VHT-MCS 31 when peer was only a 3x3. Probably other ways of getting zero ratesets would also trigger this.
- Inspect beacons, and wake a station vdev if we detect the AID in the beacon TIM IE. This fixes the case where you ping from AP to a power-save station and the station takes 10+ seconds to respond.
- Fix 802.11s mesh interfaces, specifically beaconing was broken. And, there was a crash related to mesh when a monitor interface was the last vdev in the firmware. That is fixed as well.

- Add wmi message to allow host to inspect txbf-cv data. Disabled by default, use the set-special API to enable. See 4.9 ath10k-ct driver for syntax.
- Fix problem with mesh where ARPs could not be sent. This was due to the firmware tx-scheduler having boundary-condition errors when there was only peer-0 wanting to transmit. Possibly peer-0 would always have issues and it was only detected in the mesh test case?

Ath10k CT 10.4.3 Release 8

- Backport 10.4.3.3.92 changes from upstream.
- Optimize for memory, especially the DIET (trimmed) builds. qboost and RTT are disabled in diet builds now. Neither seem that useful for normal wifi work, and qboost is not used by the ath10k driver at present anyway.
- Consolidate and re-work block-ack to not need a timer per session. Instead use one timer and walk all sessions at expiry. Saves a nice bit of RAM, and is cleaner fix for a previously worked-around use-after-free timer crash bug, but hard to test properly. Please report any BA issues.
- Diet build now supports 64-vdevs (128 sta, etc) on 9984 and 9886 hardware, 9980 supports 48 vdevs.
- Enable 160Mhz capability flag. Haven't actually tried to see if it can actually function at 160Mhz bandwith.
- Allow compiling for 9886/9888 chipset. This NIC seems to work pretty well so far, tested on a 9886 NIC from Compex.
- Auto-calculate the 'base' MAC address. This lets us create vdevs with a MAC address range differing from the 'real' MAC of the radio and still keep a tight BSSID-Filter mask.
- Fix assert related to prefetch-sched logic when completion comes in after peer object was deleted and then quickly re-used.
- set-special: Some: Many of the set-special options are not supported by 10.4 firmware. Setting THRESH62, NOISE_FLR_THRESH, MAX_TXPOWER, and MAX_PER_THR should work in previous releases.
  STA_TXBW_MASK, RIFS_ENABLE is not supported.
  PDEV_XRETRY_TH is not supported (or needed).
  WMI_WD is not supported (WMI WD is not enabled in 10.4 firmware)
- Fix some crashes related to tx-callbacks in the firmware when deleting peer (and tid) objects.

Ath10k CT 10.4.3 Release 7

- Fix regression that broke mu-mimo, among other things. MU-MIMO does not work with rxsw-crypt enabled, however.
- Fix htt-mgt-tx for 4.5 and higher kernels. Problem was that mgt tid and non-pause tids were being converted to non-qos tid, which means that mgt frames were going onto the air with 10 bytes of junk on the end.

  This same bug might have make APs using this firmware not be able to associate with /a/b/g stations as well, but not certain of that.
- Fix memory corruption relating to passing the wrong value to methods taking void pointers as context. While fixing this, convert several classes of void pointers into typed pointers so that the compiler can catch stupid mistakes. This was in core code, so both 9980 and 9984 will benefit.
- Fix memory corruption in iq-cal logic for 9984 (and probably 9888 if I compile for that) chipsets. Basic problem was poor code quality causing buffer overflow in a structure located in SRAM storage.
- Return stats when no vdevs are active. Seems this was a regression added to the upstream firmware at some point.
- Allow compiling out the peer-caching (swap to host) logic. It breaks use-case of having multiple STA vdevs connected to one AP, and I suspect it might be cause of instability in many station load test case.
- Merge in upstream 10.4.3.3-25 code.
- Fix, or at least work-around asserts in rate-ctrl code with TCP download test.
- Lots more tweaks to rate-ctrl logic.
- Fix regression bug with htt-mgt and OPEN APs.

Ath10k CT 10.4.3 Release 6

- Fix regression bug that broke encryption.
- Tested with 36 station vdevs.
- Disable WMI keepalive timer. It was not actually working properly and was crashing due to calling a function-pointer that was NULL. Can properly re-enable it later if it turns out wave-2 firmware/hardware actually has WMI hang issues.
- Ensure key event is sent on error when AST is full. Saves 3-second timeout under RTNL lock in the driver in cases where not enough AST entries are allocated.
- Pull in changes from the CNSS.BL.3.0.2-00068-S-1 release.
- Fix NPE crash when removing vdev. Looks like frame completion logic was trying to access a just-freed peer object, and so it crashed. So, protect against NULL pointers in this case.
- Fix several crashes related to removing peers, especially when deleting a partially created peer.
- Fix more asserts related to running out of peer-key objects and similar.

Ath10k CT 10.4.3 Release 5

- Fix AP mode. I had introduced a regression in the rx-filter concurrency logic in Release 4. In addition, there were some other bugs in AP mode when using htt-mgt that are resolved.
- Ensure mgt frames use proper management rate in htt-mgt mode. This significantly improves the ability to associate. This had not worked properly since the introduction of htt-mgt logic. Images compiled without htt-mgt would not have had this bug.
- Support CT Ratemask feature (ability to disable any rate or set of rates).
- These firmware images all have memory poisoning debugging enabled...I will need to remove that in future builds, and that will probably improve performance.

Ath10k CT 10.4.3 Release 4

- 10.4 is now mostly feature-compatible with older 10.1 CT firmware.
- Fix IBSS + STA concurrent use. It mostly worked, but needed to remove some asserts that seemed overly restrictive. (NOTE: Still see issues with IBSS + other vdev combinations, IBSS works best by itself currently.)
- Fix ANQP queries to APs with which the station is not currently connected. The station will now use the bss-peer if actual peer is unknown. This changes some behaviour for how mgt frames to unknown peers is handled. This appears good for ANQP/GAS, but possibly there are other test cases where the old logic was needed?
- Return temperature for the 4 ADC units in the register-dump stats.
- Fix TID mapping: When host requests one of the special TIDS, such as HTT_DATA_TX_EXT_TID_NON_QOS_MCAST_BCAST, then the firmware should NOT attempt to re-map this to AC/TID. Instead, pass it unchanged into the lower code.
  This lets null-func packets go out as truly non-qos frames instead of turning them into QoS best-effort frames and then letting block-ack work (or not, or at least not fast enough, in my testing).
  May require host patch to set the TID to HTT_DATA_TX_EXT_TID_NON_QOS_MCAST_BCAST as needed to make good use of this firmware.
  This change only affects station mode.
- Allow over-riding thresh62_ext. The other 'special' cmd IDs involving CTS timing have not been implemented yet.
- Enable CT Management-over-HTT firmware variants. These are *NOT* compatible with stock drivers. Stock 10.4 has somewhat similar HTT mgt API already, so this is mostly to be compatible with earlier firmware and to make sure all frames go through the same code path instead of using the MGT specific packet-transmit API that stock firmware uses.
- Allow monitor mode to receive 'Association Request', block-ack action frames, nodata frames, TYPE-CTL frames. Previously, these were not delivered to the WMI interface, and the kernel driver is configured to drop mgmt frames in the normal RX htt datapath, so host never saw them.
  This makes sniffing with ath10k a lot more useful. When no monitor devices are active, the firmware reverts to the previous behaviour. I guess the idea is that this is an optimization and keeps some un-needed frames off the host.
- Enable setting noise-floor-threshold and min-cca-power. If set, this will over ride the defaults, including eeprom (though firmware ignores these settings in the eeprom anyway.) Don't mess with this unless you understand the consequences. But, if set properly, noise-floor-threshold tweaking may fix ETSI CCA adapatibility test failures.
- Allow disabling firmware-added legacy, HT and VHT related IEs in probe requests. The host can do a better job of adding these, and this keeps there from being duplicated IEs in probe requests. Requires kernel patch to take advantage of these new features. NOTE: Flags values changed from 10.1 FW since 10.4 stole the bits I was using.
- Ensure that off-channel packets sent on 5Ghz band do not use CCK encoding rates (which are only valid on 2.4Ghz band). This fixes at least one problem with ANQP queries to APs on the 5Ghz band.
- vdev-up logic was resetting the mcast/bcast and non-data rate-ctrl codes to default values. This over-rode any settings that the driver may have previously set, breaking the driver's ability to properly specify rates.
  So, a check has been added so that if the driver has set the mcast rate before the vdev-up command happens, then the mcast, bcast, and non-date rate control settings are not modified. It is assumed that if the driver is setting mcast rate, then it is also setting the rest. The Candela kernel driver patches do this at least.
  In additiona, add the off-channel fixup logic for mcast/bcast frames as well, just in case those can be sent as off-channel frames.
- Allow setting a global maximum tx-power. This is to allow a user to be as sure as possible that the hardware will never transmit above thsi power level. See CT kernels for a patch that enables setting this value.
- Allow tuning the g_rc_rate_max_per_thr value. This rate-ctrl tunable defaults to 50, and some reports indicate that setting this to a higher value (70, for instance), may make performance better in a crouded RF environment.
- Remove EAPOL M1, M4 snooping. This logic attempted to stop any DATA frames from being transmitted until the M4 was successfully sent (for STA, IBSS), and until the M1 had been sent for AP mode.
  This was breaking 802.11r roaming because the 4-way is only done at the initial connection, not on subsequent roams.

If the host/driver allows data frames before encryption keys are set, then possibly this opens up a race where un-encrypted frames could hit the air. Linux, at least, will not send in-appropriate send frames to an un-authorized peer, so my change should be safe on Linux. Possibly other OS's might have issues.

- Compile out some tx-descriptor debugging in the hot path. I have never seen this code find any bugs, so I'm assuming it is not needed.
- Add 'no-beacon-miss-ct' feature flag for 'diet' builds. This lets the host know that beacon-miss is not enabled so it can let mac80211 handle the beacon miss.
- When a user used a scan request that needed more than 5 buffers (many bssids, for instance) the scan logic ran out of local mgt buffers and then just failed to send more frames. Instead, use it's (now fixed) delay-time logic to wait a bit and send the rest of the frames 5ms or so later.
- Fix use-after free with the 'ps_timer'. This caused us to crash after deleting a vdev (and after first creating several vdevs, which makes ps_timer start to run).
- Support advanced pool-mgr memory poisoning and timer debugging. This will likely be compiled into specific images since it bloats the code and uses too much CPU cycles for normal production use.
- Fix using DBGLOG logic from IRQ and timer context.
- Optimize timer usage in vdevs by using a single timer and checking all vdevs 10 times per second. This saves quite a bit of RAM, and should not cause any significant degradation of timer-related services & features.
- Debug and work-around appearant 'va_arg' bug in the firmware. Was more of a bother than anything, probably it does not cause any real harm except to confuse debugging efforts.
- Support up to 36 station vdevs (more testing is needed of course, but I could associate this many in a quick test.)
- Fix IBSS mode when using wave-2 mu-mimo adapter on both sides.

Ath10k CT 10.4.3 Release 3

- Remove asserts that are no longer needed now than we can properly crash on bad memory access.
- Support rx-software-crypt (needed for multiple STA vdevs connected to same AP with encryption)
- Fix some use-after-free bugs and read-of-uninitialized-memory bugs in tx-scheduler logic, tx-descriptors, and resource-mgr logic.
- Make it harder to crash blockack logic.
- Optimize RAM, IRAM, and SRAM usage so that we can support 32+ vdevs.
- Support register-dump debugfs API from 10.1 CT firmware.
- Allow flushing all vdev, peers, tids with one WMI command.
- Allow not reserving channel on vdev start to improve connection time.
- Add no-bmiss-ct feature flag to let driver know firmware does not support beacon-miss.
- Fix crash I introduced earlier related to htt-tx status.
- Verify IBSS/ADHOC works. Tested bi-directional between another Peregrine ath10k and got about 150Mbps UDP traffic in each direction, so it seems stable. Still need to test wave2 <-> wave2 IBSS, possibly AMSDU bug exists in wave2 (it did in the older AR988X chips)
- More concurrency cleanup so we have the bulk of the rx-filter configuration in a single place.

Ath10k CT 10.4.3 Release 2

- Fix problem where the NIC would hang instead of quickly crash if the firmware accessed bad memory (ie, read from a NULL pointer). I also fixed the decode tool to provide useful backtraces in this case, and made the dbglog buffers readable after a crash.
- Rebase against upstream version CNSS.BL.3.0.2-00056-S-1
- The diet build now disables SWBMISS code, verbose debugging (including pktlog). With this disabled, PRINTF logic in firmware can now be enabled, but it did not help so far with the NULL dereference problem.
- Fix some issues with 'make clean' type logic so that we can easily script builds.
- Enable tx-rate reporting. This requires kernel driver patches.
- Do not hard-code the vdev count to 17 (or 8, depending). Instead, just use the value the host requests.
- Ensure 'key-add' WMI command always gets an answer, even if the operation failed. Without this patch, the host may wait up to 3 seconds and then timeout if key-add fails. With driver patches, the key-add failure can be noticed as well.
- Add ability to read crash registers and debug-logs using the 'pingpong' method. This often works in case of bad CE/AXI related crash. Requires driver patches.
- Significant re-write of the concurrency logic in order to handle various vdev better.
- Support multiple station vdevs attaching to the same AP peer. Good for testing, probably not very useful for anything else.

Ath10k CT 10.4 Release 1

- Mostly stock upstream firmware, with a few WMI credits patches.

- Support WMI-NOP keep-alive timer (requires patched Candela 4.4 kernel).

CT Ath10k Advanced configuration

The CT kernel 4.4 and later supports advanced per-NIC configuration options that over-ride and/or take the place of configuration that was previously done with ath10k module options (or hard-coded into the driver). This is done with a text file created by the user and placed into the firmware directory. This works with at least 10.1 and 10.4 CT ath10k firmware.

You can find the name of the file that the NIC will use by looking in ath10k debugfs. The first two entries show current config, and the 'fwcfg' entry shows the text file that it will use (prefixed by: /lib/firmware/ath10k):

```
[root@ath10k lanforge]# cat /debug/ieee80211/wiphy3/ath10k/firmware_info
directory: ath10k/QCA99X0/hw2.0
firmware:  firmware-5.bin
fwcfg: fwcfg-pci-0000:05:00.0.txt
```

The file name cooresponds to the bus ID:

```
[root@ath10k lanforge]# lspci|grep Qual
03:00.0 Network controller: Qualcomm Atheros AR93xx Wireless Network Adapter (rev 01)
04:00.0 Network controller: Qualcomm Atheros QCA986x/988x 802.11ac Wireless Network Adapter
05:00.0 Network controller: Qualcomm Atheros Device 0040
```

Example for one of my systems configured for many station vdevs:

```
[root@ath10k lanforge]# ls -l /lib/firmware/ath10k/
total 16
-rw-r--r--  1 root root  323 Apr  1 10:22 fwcfg-pci-0000:05:00.0.txt
drwxr-xr-x  3 root root 4096 Feb 23 15:37 QCA988X
drwxr-xr-x  3 root root 4096 Oct 13 17:29 QCA99X0

[root@ath10k lanforge]# cat /lib/firmware/ath10k/fwcfg-pci-0000\:05\:00.0.txt
# Created by LANforge.  LANforge will over-write this file
# unless you add the string LEAVE-ME-Be  (with last E also capitalized)

vdevs = 64
peers = 128
active_peers = 128
stations = 128
rate_ctrl_objs = 7
# Do not change regdom unless you understand the consequences.  You
# might make your device violate FCC and related regulatory requirements.
# The value is the ISO country-code, for instance 840 for USA.
regdom = 840
fwname = firmware-5-htt-mgt.bin
fwver = 5
nohwcrypt = 1
tx_desc = 1024
#max_nss = 3
tids = 256
skid_limit = 360
max_amsdus = 3
# Needed for some early WLE1216V5-20
#bname = WLE1216V5-2-board.bin
```

It is up to the user to configure sane values. In general, if you make changes to the defaults, and something crashes right as the firmware starts, you are probably running out of memory in the firmware or have some other invalid configuration. To see resoruce config after booting the firmware, look in dmesg or use some other way to look at kernel logs:

```
[root@ath10k lanforge]# journalctl -b 0|grep "wmi print"
Apr 01 12:08:23 ath10k.candelatech.com kernel: ath10k_pci 0000:04:00.0: wmi print 'P 129 V 8 T 411'
Apr 01 12:08:23 ath10k.candelatech.com kernel: ath10k_pci 0000:04:00.0: wmi print 'msdu-desc: 1424  sw-crypt: 1'
Apr 01 12:08:23 ath10k.candelatech.com kernel: ath10k_pci 0000:04:00.0: wmi print 'alloc rem: 24688 iram: 36596'
Apr 01 12:08:23 ath10k.candelatech.com kernel: ath10k_pci 0000:05:00.0: wmi print 'P 72/72 V 36 K 216 T 298  msdu-desc: 102
Apr 01 12:08:23 ath10k.candelatech.com kernel: ath10k_pci 0000:05:00.0: wmi print 'free: 8488 iram: 11348 sram: 9676'
Apr 01 12:10:21 ath10k.candelatech.com kernel: ath10k_pci 0000:05:00.0: wmi print 'P 72/72 V 36 K 216 T 298  msdu-desc: 102
Apr 01 12:10:21 ath10k.candelatech.com kernel: ath10k_pci 0000:05:00.0: wmi print 'free: 8488 iram: 11348 sram: 9676'
```

Some example fwcfg files.

9984 firmware, full htt-mgt build, configured as AP supporting 98 connected stations.

```
vdevs = 4
peers = 100
active_peers = 100
```

```
stations = 100
rate_ctrl_objs = 7
regdom = 840
#fwname = firmware-5-htt-mgt-b.bin
fwver = 5
nohwcrypt = 0
ct_sta_mode = 0
tx_desc = 2200
#max_nss = 3
tids = 256
skid_limit = 360
max_amsdus = 3
```

9984 firmware, trimmed htt-mgt build, configured as AP supporting 173 connected stations.

```
vdevs = 4
peers = 175
active_peers = 175
stations = 175
rate_ctrl_objs = 7
regdom = 840
#fwname = firmware-5-htt-mgt-b.bin
fwver = 5
nohwcrypt = 0
ct_sta_mode = 0
tx_desc = 2200
#max_nss = 3
tids = 400
skid_limit = 400
max_amsdus = 3
```

9984 firmware, trimmed htt-mgt build, configured as AP supporting 180 connected stations (Jun 2, 2020 and later builds).

```
vdevs = 8
peers = 180
active_peers = 180
stations = 180
rate_ctrl_objs = 7
regdom = 840
#fwname = firmware-5-htt-mgt-b.bin
fwver = 5
nohwcrypt = 0
ct_sta_mode = 0
tx_desc = 2200
#max_nss = 3
tids = 450
skid_limit = 360
max_amsdus = 3
```

4019 firmware, trimmed htt-mgt build, configured as AP supporting 162 connected stations.

```
devs = 8
peers = 147
active_peers = 147
stations = 147
rate_ctrl_objs = 7
regdom = 840
#fwname = firmware-5-htt-mgt-b.bin
fwver = 5
nohwcrypt = 0
ct_sta_mode = 0
tx_desc = 2000
#max_nss = 3
tids = 450
skid_limit = 360
max_amsdus = 3
```

9886/8 firmware, trimmed htt-mgt build, configured as AP supporting 202 connected stations.

```
# 9888 chip
vdevs = 8
peers = 202
active_peers = 202
stations = 202
rate_ctrl_objs = 7
regdom = 840
#fwname = firmware-5-htt-mgt-b.bin
```

```
fwver = 5
nohwcrypt = 0
ct_sta_mode = 0
tx_desc = 2200
#max_nss = 3
tids = 450
skid_limit = 360
max_amsdus = 3
```

9880 wave-1 firmware, optimized for lots of station vdevs. This only works on diet builds since otherwise firmware will go OOM. The 'full' builds would have to be configured for less resources.

```
vdevs = 64
peers = 128
active_peers = 128
stations = 127
rate_ctrl_objs = 8
regdom = 840
fwname = firmware-2.bin
fwver = 2
nohwcrypt = 1
ct_sta_mode = 0
tx_desc = 1496
#max_nss = 3
tids = 256
skid_limit = 360
max_amsdus = 3
allow_all_mcs = 0
```

Specific fwcfg options.

dma_burst

Some conflicting patches set dma_burst to 0 or 1 for wave-2 radios. It seems that setting to 1 fixes some systems and breaks others, and setting to 0 fixes some and breaks others. In addition, just maybe value 2 could work on wave-1 cards, though I have not tested it. As of Sept 8, 2020, the ath10k-ct 5.4 driver allows configuring the dma_burst through fwcfg so that users can experiment without editing code. Other driver versions will be updated soon after.

```
    dma_burst = 1
```

NRCC Firmware Variants

The 'nrcc' variants do not swap rate-control objects to host. This means they may be more efficient and they use less host resources, so this option may be good for low powered systems. But, they cannot be configured with as many resources (peers, vdevs, etc) in exchange. For 9887, I tested successfully with a fwcfg file that looks like this (below) for firmware firmware-2-ct-htt-mgt-nrcc-community.bin. You could tune with more peers, but watch dmesg logs for 'iram' and make sure the firmware has enough RAM. If you slowly add peers, for instance, and then it starts crashing on load, then decrease peers again until it boots properly. Or, decrease tx descriptors, or vdevs or some other resource.

```
root@LEDE:/# cat /lib/firmware/ath10k/fwcfg-pci-0000\:00\:00.0.txt
vdevs = 4
peers = 80
```

CT 10.4 Firmware Crash Signatures

None known at this time.