Qualcomm Technologies International, Ltd.

# QCC512x and QCC302x/3x Series ROMs

## Release Note

80-CG310-1 Rev. AT

December 23, 2019

**For additional information or to submit technical questions, go to: https://createpoint.qti.qualcomm.com**

# Revision history

| Revision | Date | Description |
|---|---|---|
| AA | 14 June 2018 | Combined release note following from 80-CF568-1 and 80-CF840-1 for 512x and 3026 respectively and adding support for other 302x and 303x series parts. Alternative document number CS-00410777-RN |
| AB | 20 June 2018 | Added update CUR-5817 for PUYA Flash parts |
| AC | 24 July 2018 | Updated System Manager and Bluetooth patches available, including specific Bluetooth patch for QCC5120 on 124pin VFBGA.<br>Updates to list of known issues in Bluetooth Subsystem and System Manager, particularly note important issues CUR-5873 and B-272247 |
| AD | 31 August 2018 | Update of all patches corresponding to ADK 6.3.0.150 |
| AE | 03 September 2018 | Updated to refer to ADK 6.3.0.154 + added CUR-5931 |
| AF | 20 December 2018 | Update of all patches corresponding to ADK 6.3.1 ES release |
| AG | 17 January 2019 | Added missing QCC5120 from Section 6.1. |
| AH | 12 March 2019 | Updated to refer to ADK 6.3.1 production release |
| AJ | 02 April 219 | Updated to refer to ADK 6.3.2 production release |
| AK | 09 July 2019 | Updated to refer to ADK 6.4.0.34 production release |
| AL | 15 August 2019 | Updates for ADK6.4.0.43 production release |
| AM | 02 September 2019 | Removed Winbond 128JW from QSPI flash support table |
| AN | 03 October 2019 | Added Winbond W25Q128JW back in QSPI flash support table with footnote. Added B-283592 for information. |
| AP | 13 December 2019 | Updated for ADK 6.4 build 6.4.2.26 |
| AR | 18 December 2019 | Removed Table 9-2 present in previous issue, as information is now documented in the ADK Source Code release notes. |
| AT | 20 December 2019 | Removed F25M32B from list of support flash devices |

## SOFTWARE RELEASE DISCLAIMER

THIS RELEASE IS PROVIDED "AS IS" AND QUALCOMM TECHNOLOGIES INTERNATIONAL, LTD. (“QTIL”) CAUTIONS YOU TO DETERMINE FOR YOURSELF THE SUITABILITY OF USING THIS RELEASE. TO THE FULLEST EXTENT PERMITTED BY LAW, QTIL DISCLAIMS AND EXCLUDES ALL WARRANTIES, REPRESENTATIONS, CONDITIONS AND OTHER TERMS OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THE RELEASE. FOR ALL APPLICALE TERMS, INCLUDING LIMITS ON LIABILITY, YOU ARE REFERRED TO QTIL’S STANDARD TERMS OF SUPPLY, LICENSE AGREEMENT OR OTHER AGREEMENT BETWEEN YOU AND QTIL OR QTIL’S AFFILIATE UNDER WHICH THIS RELEASE IS SUPPLIED.

# Contents

# Tables

# 1 Introduction

This document describes the ROM firmware for the QCC512x, QCC302x, and QCC303x family of devices. Table 1-1 shows the devices covered by this release note.

**Table 1-1 Devices released**

| Device | Description |
|---|---|
| QCC5120 | QCC5120 Bluetooth Audio SoC in 124 pin VFBGA |
| QCC5121 | QCC5121 Bluetooth Audio SoC in 81 pin WLCSP |
| QCC5124 | QCC5124 Bluetooth Audio SoC in 90 pin VFBGA |
| QCC5125 | QCC5125 Value Flash Bluetooth Audio SoC in 90 pin VFBGA |
| QCC3020 | QCC3020 Bluetooth Audio SoC for Mono Earbud in 90 pin VFBGA |
| QCC3021 | QCC3021 Bluetooth aptX Audio SoC for Stereo Speakers in 80 pin QFN |
| QCC3024 | QCC3024 Bluetooth Audio SoC for Stereo Headset in 90 pin VFBGA |
| QCC3026 | QCC3026 Bluetooth Audio SoC for Mono Earbuds in 81 pin WLCSP |
| QCC3031 | QCC3031 Bluetooth aptX Audio SoC for Stereo Speakers in 80 pin QFN |
| QCC3034 | QCC3034 Bluetooth Qualcomm® aptX™ Audio SoC for Stereo Headset in 90 pin VFBGA |

## 1.1 Device specific image files

Table 1-2 lists the ROM patch images that need to be used with QCC512x and QCC302x/3x devices for correct operation.

**NOTE:** (1) Device specific image files (sometimes referred to as patch bundles) are delivered as part of ADK_QCC512x.WIN.6.4 build 6.4.2.26 available on CreatePoint.

(2) QCC5126 and QCC5127 are not covered by this release note.

### Table 1-2 Patch image files

| Subsystem | Patch Image | Unpatched Build ID | Version | 81 pin WLCSP | 90 pin VFBGA | 124 pin VFBGA | 80 pin QFN |
|---|---|---|---|---|---|---|---|
| | | | | QCC5121<br>QCC3026 | QCC5124<br>QCC5125<br>QCC3020<br>QCC3024<br>QCC3034 | QCC5120 | QCC3021<br>QCC3031 |
| **System/Boot Manager Subsystem** | `subsys0_patch0_fw0000503.hcf`<br>`subsys6_patch0_fw0000503.hcf` | 1283<br>(0x503) | v39 | 1669 | | | |
| **Bluetooth Controller Subsystem** | `subsys1_patch0_fw000033EF.hcf` | 13295<br>(0x33ef) | v88 | 14513 | 14512 | 14514 | 14515 |
| **Qualcomm® Kymera™ Audio Subsystem** | `subsys3_patch0_fw000012B2.hcf` | 4786<br>(0x12b2) | V78 | 8939 | | | |

**NOTE:** (1) The Unpatched Build ID is the ID reported when the revision of the patch is missing or incorrectly installed otherwise the version shown on the right is reported.

(2) For the Bluetooth controller, the ID is accessible through the HCI command `Read_Local_Version_Information`. If the patch is incorrectly installed, a build ID of `0x33ef` (13295) is reported.

(3) For the System/Boot manager, the Build ID can be read using PyDbg tools.

# 2 Functionality

The QCC512x and QCC302x/3x family of devices are designed to support the following applications:

- Earbuds
- Wired/wireless stereo headsets/headphones
- Wireless speakers
- USB to Bluetooth dongle with aptX HD

## 2.1 Definitions

Table 2-1 describes status definitions that apply to functionality described in this document.

**Table 2-1 Feature status definitions**

| Status | Definition |
|---|---|
| YES | The feature is available |
| NO | The feature is not available |
| License Key | The feature is available but must be enabled through installation of a license key on the product. |
| Enabled | The feature is available and is enabled without requiring a license key. |

**NOTE:** License terms and conditions are applicable to available and enabled features. For example, aptX.

# 2.2 Supported functionality

**Table 2-2 Functional overview**

| | QCC5120 | QCC5121 | QCC5124 | QCC5125 | QCC3020 | QCC3021 | QCC3024 | QCC3026 | QCC3031 | QCC3034 |
|---|---|---|---|---|---|---|---|---|---|---|
| Bluetooth | 5.0 | 5.0 | 5.0 | 5.0 | 5.0 | 5.0 | 5.0 | 5.0 | 5.0 | 5.0 |
| Application CPU | 80 MHz | 80 MHz | 80 MHz | 32 MHz | 32 MHz | 32 MHz | 32 MHz | 32 MHz | 32 MHz | 32 MHz |
| DSP | 2x120 MHz | 2x120 MHz | 2x120 MHz | 1x120 MHz | 1x120 MHz | 1x120 MHz | 1x120 MHz | 1x120 MHz | 1x120 MHz | 1x120 MHz |
| DAC Configuration | Stereo/ mono | Stereo/ mono | Stereo/ mono | Stereo/ mono | Mono | Stereo/ mono | Stereo/ mono | Mono | Stereo/ mono | Stereo/ mono |
| DSP Programmable | Yes | Yes | Yes | Yes | No | No | No | No | No | No |
| DSP Configurable | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| aptX Classic (Decode) | License Key | License Key | License Key | License Key | License Key | No | No | License Key | Enabled | Enabled |
| aptX LL (Decode) | License Key | License Key | License Key | License Key | No [1] | No | No | No [1] | License Key | License Key |
| aptX HD (Decode) | License Key | License Key | License Key | License Key | No [1] | No | No | No [1] | Enabled | Enabled |
| aptX Mono (Decode) | License Key | License Key | License Key | License Key | Enabled | No | No | Enabled | Enabled | Enabled |
| ANC | License Key | License Key | License Key | License Key | No | No | No | No | No | No |
| Qualcomm® cVc™ 1 Mic Headset | License Key | License Key | License Key | License Key | Enabled | No | Enabled | Enabled | No | Enabled |
| cVc 2 Mic Headset | License Key | License Key | License Key | License Key | Enabled | No | Enabled | Enabled | No | Enabled |
| cVc 1 Mic Speaker | License Key | License Key | License Key | License Key | No | Enabled | No | No | Enabled | No |
| cVc 2 Mic Speaker | License Key | License Key | License Key | License Key | No | License Key | No | No | License Key | No |

**NOTE:** (1) The evaluation license has these features enabled however, AptX-HD and AptX-LL are not supported with TWS. aptX and aptX-HD are bundled under License Key Feature LK-VAM-APTX-CLHD, however only AptX is supported with TWS.

(2) For further details of each part, see the corresponding *Data Sheet*.

# 3 Kymera audio subsystem functionality

## 3.1 Significant changes in this ADK

| ID | Description |
|---|---|
| B-284662 | From ADK 6.4, Voice Assistant (VA) is not supported on QCC512x/QCC302x/3x chips (ROM 2.0) devices (devices covered by this release note).<br>Patches related to VA have been removed to create more usable program memory space. |
| B-284500 | From ADK 6.4, PSRAM is not supported on QCC512x/QCC302x/3x chips (ROM 2.0) devices (devices covered by this release note).<br>Patches related to PSRAM have been removed to create more usable program memory space. |

## 3.2 Audio subsystem capabilities

QCC512x and QCC302x/3x devices include audio capabilities implemented in ROM firmware, which can be extended dynamically by additional downloadable capabilities provided with, or developed using, an ADK.

**Table 3-1 QCC512x Audio Capabilities implemented in ROM**

| Capability Name | Capability ID | Description |
|---|---|---|
| AAC_DECODER | 0x18 | The AAC decoder takes an encoded stream containing AAC data and decodes it into audio frames. |
| AEC_REFERENCE | 0x43 | The AEC Reference capability overrides the real endpoints connected to it to provide the synchronization and latency control Key for the proper operation of an acoustic echo canceller. |
| APTX_CLASSIC_DECODER | 0x19 | The Qualcomm® aptX audio decoders take an encoded stream containing aptX data and decode it into audio frames. |
| APTX_CLASSIC_MONO_DECODER | 0xa9 | A version of the APTX_CLASSIC_DECODER that operates on a mono data stream |
| APTX_CLASSIC_MONO_DECODER_NO_AUTOSYNC | 0xab | A variant of APTX_CLASSIC_MONO_DECODER with no auto synchronization. |
| APTX_LOW_LATENCY_DECODER | 0x3d | The aptX audio decoders take an encoded stream containing aptX low latency data and decode it into audio frames. |

| Capability Name | Capability ID | Description |
|---|---|---|
| APTXHD_DECODER | 0x9e | The aptX audio decoders take an encoded stream containing aptX-HD data and decode it into audio frames. |
| BASIC_PASS | 0x1 | Basic Pass-through capability takes a stream input and passes it on to a stream output of the same number of channels. |
| CELT_DECODER | 0x9d | The CELT decoder takes an encoded stream containing CELT data and decodes it into audio frames. |
| CELT_ENCODER | 0x9c | The CELT encoder takes a stream of up to 2 PCM channels and encodes them into frames of CELT codec. |
| CHANNEL_MIXER | 0x97 | The Channel Mixer capability mixes different input channels corresponding to a single stream to generate different output channels corresponding to a single stream. The channel mixer can be used as an up mixer, a down mixer, and a normal mixer. |
| COMPANDER | 0x92 | The goal of Dynamic Range Control (DRC) is to control the dynamic range of the input signals through application of a time varying gain coefficient. Two common applications of the DRC are compression and expansion. The term Compander is often used when these two DRC applications are employed together. |
| CVC_RECEIVE_FE | 0x1b | cVc Receive Frequency Extension version. |
| CVC_RECEIVE_NB | 0x1d | cVc Receive applies the processing from the cVc algorithms including Automatic Gain Control (AGC) Parametric Equalization (PEQ) Adaptive Equalization (AE) Noise Reduction (OMS) High Frequency Extension and Emphasis. |
| CVC_RECEIVE_WB | 0x1f | cVc Receive WideBand version. |
| CVCHS1MIC_SEND_NB | 0x23 | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 1 mic Headset NarrowBand. |
| CVCHS1MIC_SEND_WB | 0x24 | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 1 mic Headset WideBand. |
| CVCHS2MIC_BINAURAL_SEND_NB | 0x27 | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 2 mic Headset Mono NB. |
| CVCHS2MIC_BINAURAL_SEND_WB | 0x28 | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 2 mic Headset Mono WB. |

| Capability Name | Capability ID | Description |
|---|---|---|
| CVCHS2MIC_MONO_SEND_NB | 0x25 | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 2 mic Headset Mono NB. |
| CVCHS2MIC_MONO_SEND_WB | 0x26 | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 2 mic Headset Mono WB. |
| CVCSPKR1MIC_SEND_NB | 0x29 | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 1 mic speaker NB. |
| CVCSPKR1MIC_SEND_WB | 0x2a | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 1 mic speaker WB. |
| CVCSPKR2MIC_SEND_NB | 0x2d | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 2 mic speaker Mono NB. |
| CVCSPKR2MIC_SEND_WB | 0x2e | The cVc send applies the processing from the cVc algorithms: AGC, PEQ, Noise dependent voice control (NDVC), Adaptive Echo Cancellation (AEC), Beamforming, Noise Reduction. 2 mic speaker Mono WB. |
| DBE | 0x2f | Qualcomm® meloD™ audio processing bass provides a technique for Dynamic Bass Enhancement (DBE) that simultaneously compensates for the high-pass characteristic of speakers and compresses the low frequencies. |
| DBE_FULLBAND | 0x90 | This DBE option allows the module to process a full-band audio signal, as part of a full-band processing audio chain. |
| DBE_FULLBAND_BASSOUT | 0x91 | This DBE option allows the module to process a full-band audio input signal but produce a bass-only output signal. |
| IIR_RESAMPLER | 0x94 | The IIR Resampler capability takes a set of connected channels and performs sample rate conversion between a specified input rate and output rate. |
| MIXER | 0xa | The Mixer capability allows you to mix up to 3 input streams into 1 output stream. Each input stream can have a different number of channels. |
| PEQ | 0x49 | The PEQ capability wraps the functionality of a 10-band parametric equalizer for use in the Kymera framework. |

| Capability Name | Capability ID | Description |
|---|---|---|
| RINGTONE_GENERATOR | 0x37 | The Ringtone Generator capability generates ringtones using music Notes in the range of C0 to B9 and a tempo. |
| RTP_DECODE | 0x98 | RTP Decode capability is used to either generate TTP timestamps for outgoing data, to indicate when the encoded audio should be played, or to remove the RTP headers from an incoming A2DP stream. |
| SBC_DECODER | 0x16 | The SBC decoder takes an encoded stream containing SBC data and decodes it into audio frames. |
| SBC_ENCODER | 0x14 | The SBC encoder takes a stream of up to 2 PCM channels and encodes them into frames of SBC codec. |
| SCO_RCV | 0x4 | The SCO Receive capability handles the reception of narrowband audio over a SCO connection. It has one input and one output terminal. |
| SCO_SEND | 0x3 | The SCO Send capability handles the sending of narrowband audio over a SCO connection. It has one input and one output terminal. |
| SOURCE_SYNC | 0x99 | A Source Sync capability's primary task is to ensure that data flow out of all its outputs (source terminals) is synchronized and continues when data at its inputs (sink terminals) is absent or late. |
| SPDIF_DECODE | 0x36 | The S/PDIF Decode capability is used to handle the reception of audio from one or two input S/PDIF Rx endpoints. |
| SPLITTER | 0x13 | The Splitter capability allows you to split a stream into two separate streams that are both duplicates of the original input. |
| TTP_PASS | 0x3c | TTP (Time to Play) Pass-through capability takes a set of audio inputs, generates TTP timestamps for it and pass it on to the outputs. |
| USB_AUDIO_RX | 0x9a | The USB Audio Rx capability handles the reception and routing of USB Audio received from a USB host, where the Capability input is always connected to a USB Audio Rx endpoint. |
| USB_AUDIO_TX | 0x9b | The USB Audio Tx handles USB Audio that is to be transmitted to a USB host, where the capability output is always connected to a USB Audio Tx endpoint, and routing USB Audio Tx can only be done using this Operator. |
| VOL_CTRL_VOL | 0x48 | The Volume and Auxiliary Audio Mix capability provides volume related processing for up to 8 channels. It also provides support for the mixing of up to 8 transient auxiliary audio channels. |
| VSE | 0x4a | The Virtual Stereo Enhancement (VSE) goal is to provide the listener with the impression that the sound comes from the widely spaced virtual loudspeakers instead of the closely spaced real physical speakers. |

| Capability Name | Capability ID | Description |
|---|---|---|
| WBS_DEC | 0x6 | The Wideband Speech Decode capability handles reception and decoding of audio from an eSCO connection. It has one input and one output terminal. |
| WBS_ENC | 0x5 | The Wideband Speech Encode capability handles encoding and sending of wideband 16 kHz audio over an eSCO connection. It has one input and one output terminal. |
| XOVER | 0x33 | The Crossover capability wraps the functionality of a 2-band or 3-band crossover (using Capability ID) for use in the Kymera framework. The filtering core consists of IIR filters configured in second order sections (biquads). |

# 4 Bluetooth controller subsystem functionality

The software was written against the *Bluetooth Core Specification, v5.1*. This release provides the following Bluetooth features:

## 4.1 Bluetooth BR/EDR functionality

- Support for Basic Rate and Enhanced Data Rate Bluetooth links
- BR/EDR Secure Connections
- Support for eSCO audio (depends also on Audio Subsystem)
- Support for AFH channel classification
- Connectionless Slave Broadcast
- Support for shallow sleep power saving
- Support for deep sleep power saving

## 4.2 Bluetooth Low Energy functionality

- Support for Bluetooth Low Energy links
- Secure Connections – Link Layer Ping Mechanism
- Secure Connections – HCI Cryptographic Function Access
- Dual Mode Topology
- Link Layer Topology
- Low Duty Cycle Directed Advertising
- Faster non-connectable advertising rates
- Data Length Extension
- Channel Selection Algorithm #2
- 2 Mbps PHY

## 4.3 Other functionality

- Support for the QTIL proprietary radiotest mode for continuous wave and packet tests.
- Support for tunneling of ACCMDs (which allow the host to communicate with and command the Audio subsystem) using the Bluetooth host interface
- Support for the downloading of files using the System Manager for ROM patching and for PS Key configuration.
- Off-chip host is supported over BCSP or H4 Bluetooth host transports for Bluetooth qualification.

## 4.4 Functional restrictions

This Bluetooth Subsystem release has the following limitations:

- This release does not provide any support for SCO over HCI (SCO goes directly to the audio subsystem);
- The H4 transport “sync loss recovery” mechanism, available as mandated by the Bluetooth specification, is not suitable for use in a production environment to deal with a host delivering unreliable data.
- HCI Remote Loopback is not supported; HCI Local Loopback mode does not support Host Controller to Host flow control.
- The BTSS does not support warm reset (bcset warm_reset).
- Qualcomm has identified that careful selection of the Broadcast Audio feature’s CSB Interval (CSBI) is important if undue impacts upon other concurrent Bluetooth activities are to be avoided. Selection of CSBI = 22 slots and 2-DH5 packets in the VM Application has been verified by Qualcomm as providing a good balance of performance. As part of its commitment to ongoing development and product improvement, additional advice may be provided in the future regarding the impact of other values of CSB Interval.
- Customers should be aware that if 5-slot A2DP packets are in use with a CSB Interval of less than 20 slots, this may negatively impact A2DP reception.
- The success rate of Page and Page Scan activities is significantly reduced when Broadcast Audio and A2DP audio are simultaneously active, due to the inherent time-division nature of Bluetooth. These effects can be mitigated by increasing the duration for which Paging or Page Scanning is performed. There may be some reduction in the success rate of Page Scan and Inquiry Scan for values of CSB interval like 8, 16 or 32 which are divisors of 2048 or 4096.
- The Bluetooth firmware will permit the creation of a Connectionless Slave Broadcast (CSB) link in situations where existing (e)SCO links leave insufficient remaining airtime for CSB traffic to be scheduled.
  - In these situations, the Bluetooth firmware will correctly prioritise (e)SCO traffic to safeguard (e)SCO audio quality.
  - Ultimately, the CSB link may subsequently disconnect due to link starvation.
- Internal performance comparisons have identified that this Bluetooth firmware exhibits reduced page scan performance in use cases where the device is also using a high proportion of the available bandwidth for data transfer, impacting the likelihood of the device being located in any given page operation.
  - Available data suggests that under test conditions, a page operation to this device succeeds in ≥ 90% of cases within 5.12 seconds and 99% of cases within 10.24 seconds.

  - This issue is likely to manifest itself in use cases as an increased proportion of connection attempts exhibiting an increased connection time.

- Any attenuation value used in a basic rate power table entry must be present in an enhanced data rate entry, or the device emits a hardware error `invalid_edr_powertable_attenuation`, and radio calibration is incomplete.

# 5 System Manager

## 5.1 Significant System Manager changes in this ADK

The following tables gives a list of System Manager changes compared with patches from previous ADKs, see also section 8.3 and section 9.3.

**Table 5-1 Significant changes to the System Manager**

| Reference ID | Change area | Description |
|---|---|---|
| CUR-6553 | | Power optimisation for dormant mode when entering dormant after the last deep sleep used accurate timing. |
| CUR-6564 | | Charging in external mode (ie with an external transistor) could give charge currents significantly higher than requested on some parts.<br><br>This patch adjusts the trim used to improve the accuracy of the charging current when in external mode.<br><br>Updates to a previous patch (CUR-6371) in order to support new production hardware. |
| CUR-6493 | | The XtalPowerModeStateSettings System Manager configuration key has been removed.<br>This key was not intended to be used. Any customers who were using it should seek assistance from Qualcomm. |
| CUR-6591, CUR-6506 | | Updates to the System Manager configuration key documentation. |
| CUR-6568 | | The value of the system manager configuration key DSULPTimeConversionFactor has been updated to represent 96ppm to better match the bulk of crystals supported. This key does not need to be further changed when recommended crystals are used. Seek advice from Qualcomm before changing this key. |

# 6 Supported QSPI devices

## 6.1 QSPI Flash Support

Table 6-1 lists the Q-SPI Flash devices supported on the Apps SQIF interface.

**Table 6-1 QSPI Flash devices supported/tested and clocked at 32 MHz**

| Manufacturer | Part Number | Size (Mbytes) |
|---|---|---|
| Adesto | AT25SL321 (1) (2) | 4 MB |
| Adesto | AT25SL641 (1) (2) | 8 MB |
| Adesto | AT25SL128A (1) (2) | 16 MB |
| Cypress (Spansion) | S25FS064S (2) | 8 MB |
| Cypress (Spansion) | S25FS128S (2) | 16 MB |
| ESMT (EON) | EN25S80B(2S) (1) | 1 MB |
| ESMT (EON) | EN25S16B(2S) (1) | 2 MB |
| ESMT (EON) | EN25S32A(2S) (1) (2) | 4 MB |
| ESMT (EON) | EN25S64A(2SC) (1) (2) | 8 MB |
| Fidelix | F25M64C (1) (2) | 8 MB |
| Fidelix | F25M4AA (1) (2) | 16 MB |
| Fidelix | F25M4AB (1) | 16 MB |
| GigaDevice | GD25LE80C (1) | 1 MB |
| GigaDevice | GD25LQ80C (1) (2) | 1 MB |
| GigaDevice | GD25LE16C (2) | 2 MB |
| GigaDevice | GD25LQ16C | 2 MB |
| GigaDevice | GD25LE32D | 4 MB |
| GigaDevice | GD25LE32E (2) | 4 MB |
| GigaDevice | GD25LQ32C (2) | 4 MB |
| GigaDevice | GD25LQ32D (2) | 4 MB |
| GigaDevice | GD25LQ64C (2) | 8 MB |
| GigaDevice | GD25LE64C (2) | 8 MB |
| GigaDevice | GD25LQ128D (2) | 16 MB |
| GigaDevice | GD25LE128D | 16 MB |
| ISSI | IS25WP080D (1) | 1 MB |
| ISSI | IS25WP016D (1) (2) | 2 MB |
| ISSI | IS25WP032D (1) (2) | 4 MB |
| ISSI | IS25WP064A (1) (2) | 8 MB |

| Manufacturer | Part Number | Size (Mbytes) |
|---|---|---|
| Macronix | MX25U8035E [1] [2] | 1 MB |
| Macronix | MX25U8035F [1] | 1 MB |
| Macronix | MX25U1635E [1] | 2 MB |
| Macronix | MX25U1633F [1] [2] | 2 MB |
| Macronix | MX25U1635F [1] [2] | 2 MB |
| Macronix | MX25U3235E [1] | 4 MB |
| Macronix | MX25U3232F [1] [2] | 4 MB |
| Macronix | MX25U3235F [1] [2] | 4 MB |
| Macronix | MX25U6432F [1] [2] | 8 MB |
| Macronix | MX25U6435F [1] | 8 MB |
| Macronix | MX25U12832F [1] [2] | 16 MB |
| Macronix | MX25U12835F [1] | 16 MB |
| Macronix | MX25U12843G [1] [2] | 16 MB |
| Puya | P25Q80L [1] | 1 MB |
| Puya | P25Q80LE [1] | 1 MB |
| Puya | P25Q16L [1] | 2 MB |
| Puya | P25Q32L [1] | 4 MB |
| Puya | P25Q64L [1] | 8 MB |
| Winbond | W25Q80EW [1] | 1 MB |
| Winbond | W25Q16FW [1] [2] | 2 MB |
| Winbond | W25Q32FW [1] [2] | 4 MB |
| Winbond | W25Q64FW [1] | 8 MB |
| Winbond | W25Q128FW [1] | 16 MB |
| Winbond | W25Q32JW [1] | 4 MB |
| Winbond | W25Q64JW [1] | 8 MB |
| Winbond | W25Q128JWxIQ [1] [2] [3] | 16 MB |
| XMC | XM25QU64A [1] | 8 MB |

**NOTE:** [1] Parts require MIB keys to operate correctly. Example MIB files are to be found in the ADK under the directory **/qspi_config/**

[2] Parts have been tested by Qualcomm. Other parts may be used but the customer is advised to test them thoroughly before selection.

[3] Winbond W25Q128JW parts with pre-release date codes (prior to 1933) are not supported.

**Table 6-2 QSPI Flash devices supported/tested and clocked at 80 MHz**

| Manufacturer | Part Number | Size (Mbytes) |
|---|---|---|
| ISSI | IS25WP128F (1) (2) | 16 MB |
| Micron | MT25QU128ABA | 16 MB |

## 6.1.1 QE Quad Enable bit

Many QSPI devices require a Non-Volatile Quad Enable bit to be set. This NV QE bit can be set using the Qualcomm® BlueSuite™ nvscmd tool.

## 6.1.2 Resume/suspend MIB settings

The P0 application processor needs to be able to suspend programming and erase operations to allow it to avoid blocking while these operations complete. Only QSPI devices supporting suspend and resume operations can be used.

The P0 application has defaults for these commands:

- Program or Erase Suspend `0x75`.
- Erase or Program Resume `0x7a`.

**NOTE:** The P0 application is delivered with ADK releases

These values are suitable for devices from a wide range of manufacturers. For devices that implement different commands for these the MIB Key `SiflashSuspendResumeCommands` is provided in the Application subsystem MIB.

This is the case with the ESMT, Macronix and XMC devices. devices as shown in Table 6-3, which require the following to be set `SiflashSuspendResumeCommands = 0xb030b030`.

**Table 6-3 – Non-default suspend/resume settings**

| Device | MIB Setting |
|---|---|
| EN25SxxX | `SiflashSuspendResumeCommands = 0xb030b030` |
| MX25Uxx35X | `SiflashSuspendResumeCommands = 0xb030b030` |
| XM25QU64A | `SiflashSuspendResumeCommands = 0xb030b030` |

## 6.1.3 4Kbyte Sector support

Enhancement CUR-6169 allows the Q-SPI Flash to be arranged in 4Kbyte sectors from the previous 64Kbyte sectors. This benefits flash utilization when a small flash devices are selected.

A new MIB key (QSPIFRAMLUTSectorEraseOverride) has been introduced. CUR-6186 changes the precompiled `System Manager layer1.hcf` file to set this key to use 4 KB sector sizes. Set this MIB key to 0 in a higher-level config file to override the default and use 64 KB sectors as previously.

# 7 Bluetooth and regulatory status

Sections 7.1 and 7.2 describe regulatory compliance applicable to the QCC512x and QCC302x/3x range of devices.

## 7.1 Radio certification

QCC5120, QCC5121, QCC5124, QCC5125, QCC3020, QCC3021, QCC3024, QCC3026, QCC3031 and QCC3034 have been validated to comply with the following specifications:

- FCC 47CFR 15.247 and IC RSS-247
- Japanese Radio Law - Ordinance concerning Technical Regulations Conformity Certification, and so on, of Specified Radio Equipment: Article 2 The specified radio equipment in Article 38-2, Paragraph 1, Part 19
- ETSI ETS 300-328 (2016-11) compliance:

  The Bluetooth AFH DAA algorithm has been updated to be complaint to the ETSI ETS 300-328 specification where the firmware meets the following limits.

  - 3.85 s to respond to an interference event on a particular channel or group of channels. This means that the firmware maps out an interferer within 3.85 s of it appearing, in the worst case.
  - Once mapped out, channels stay mapped out for a minimum of 14.8 seconds before being brought back into service.

## 7.2 Bluetooth qualification

The QCC5120, QCC5121, QCC5124, QCC5125, QCC3020, QCC3021, QCC3024, QCC3026, QCC3031 and QCC3034 Bluetooth controllers with patch are compliant to the Bluetooth 5.1 specification and will appear under Bluetooth qualification listings:

- Controller Listing: D043815 (https://launchstudio.bluetooth.com/ListingDetails/88811)
- Component Listing: D041992 (https://launchstudio.bluetooth.com/ListingDetails/85302)

# 8 Known issues

QCC521x, QCC302x, and QCC303x devices have a number of known issues that are listed in Sections 8.1 to 8.3, which cover the:

- Kymera audio subsystem
- Bluetooth controller subsystem
- System/boot Manager

## 8.1 Audio subsystem known issues

**Table 8-1 Audio subsystem known issues**

| ID | Description |
|---|---|
| B-233123 | If the CELT frame size set in a `CELT_DECODER` operator with the `CELT_ENC_ID_SET_ENCODING_PARAM` message does not match the frame size of the received stream; the audio subsystem can crash. |
| B-240484 | Setting the CodecOutputDisableTimeout MIB key to a nonzero value can lead to clicks on the headphone (LP) DACs when the audio subsystem is shut down (`OperatorFrameworkEnable(0)`). This MIB key should be left at its default value of zero. |
| B-243983 | If a COMPANDER or DBE operator on one audio processor is connected to an operator on the other processor, or such an operator on the second core is connected directly to a stream endpoint, the audio subsystem can crash. |
| B-244575 | Audio subsystem does not support more than 10 stereo stream connections (or 16 mono stream connections) between the first core and second core operators. Attempts to create further connections fail with `STREAM_CONNECT_RESP` status `CMD_FAILED`. |
| B-250530 | Ringtone capability may not run properly at sample rates greater than 8 kHz |
| B-253463 | Connecting a ringtone generator to an IIR resampler causes `FAULT_AUDIO_SUPPLIED_BUFFER_TOO_SMALL`, audio fault 0x005d in most cases. In this case this is not an indication of an actual problem, the buffer in question is large enough for the purpose. |
| B-255258 | The mode of cVc send headset variants cannot be changed (from apps) after the operator has started |
| B-250793 | Running `RTP_DECODE and AAC_DECODE` capabilities of the music graph on different processors can cause an audio subsystem panic.. |
| B-255676 | If the System Manager (curator) MIB key is set to boot AudioSS at a lower clock than the application configured active clock, it does not retain the booted clock after exiting AOV LP mode unless the active clock has been configured the same as the audioSS boot clock. |
| B-258636 | If the CELT Encoder capability is used with a frame length that is an odd number of octets, encoded frame contents are truncated.<br><br>This does not affect the CELT encoder's uses for broadcast audio. |

| ID | Description |
|---|---|
| B-261207 | When using the low-power voice graph in the Sink application as Bluetooth Slave using NB SCO packet type =EV4 with Tesco=12 and Wesco=6, periodic high THD audio may be observed rarely. |
| B-263288 | Using Invert the low frequency band functionality of crossover causes all bands of crossover output to be inverted.<br><br>Workaround is to Invert only a single band of crossover, use Invert the high frequency band" instead along with the appropriate crossover parameters. |
| B-263882 | At the point volume reaches its limits a beep is generated. In the broadcast scenario, the beep may be elongated on the sender with gaps and there may be distortion on the BA receiver. |
| B-269361 | Broadcast audio exhibits slightly higher THD of about 1% than other nonbroadcast audio use cases. |
| B-269687 | There is a high USB send path delay while using cVc in wired mode. This occurs when the audio output is I2S or DAC and the sampling rate in the receive path is configured at 48 KHz or 44.1 KHz. This problem manifests itself as audio glitches if cVc is used with USB Audio. |
| B-270058 | Small audio pops may be heard during voice prompt playback, for example at turn on and off. |
| B-270119 | If more than one phone is paired when using Broadcast Audio, glitches may be heard in the broadcast receiver. |
| B-271865 | Using the second audio core introduces processing overhead on the primary and secondary audio cores. This is due to Inter-Processor Communication (IPC) between the two cores.<br>Graphs with particularly high IPC overhead are graphs with only basic passthrough operators; For example, with a BASIC_PASS operator on P1:<br><br>`ADC L ----> \|  BASIC_PASS  \| ---> DAC L`<br>`ADC R ----> \|  (running on P1)  \| ---> DAC R`<br><br>You usually want to run an operator on the second core only if the amount of processing that this operator performs is significantly more than the IPC overhead.<br>You can minimize IPC overhead by synchronizing audio endpoints. This reduces kick propagation across cores.<br>The number of operators on the secondary does not significantly impact the primary core overhead.<br>Provided the endpoints are synchronised, stereo processing is not expected to add much IPC overhead, compared to mono. |
| B-277786/ B-279375 | Auxiliary input to Volume control may not be mixed with the main input. This may manifest as voice prompts not being played out completely. |
| B-281613 | Running sbc_decoder.cfg.json test on KSE config under ADK 6.3.x hangs. |
| B-283551 | When encoding 0dB signals some 3rd party AAC encoder implementations may produce encoded data which causes saturation to occur at the output of the AAC decoder. This results in audio distortion in the PCM output signal of an AAC decoding chain. |
| B-284716 | It is possible for I2S1 and I2S0 outputs to be out of sync by one sample in scenarios where I2S is also used as an input. |
| B-285356 | The Audio build system does not support more than one prebuilt libraries to be imported to the bundle. |
| B-286713 | A2DP audio streaming with AAC may cause temporary left to right earbud synchronisation issues. |

| ID | Description |
|---|---|
| B-286720 | ADK6.3.1 Long term A2DP streaming with iphones occasionally causes the slave earbud to lose audio. |
| B-279631 | If you reconnect a group of synchronised audio streams to an already running operator, start with the head of sync group, other wise audio streams might not start flowing. |
| B-285256 | Two source files in the same library but different paths cannot have the same file name. If they do, the build system fails. |

# 8.2 Bluetooth controller known issues

Table 8-2 lists the issues known to be present in this release.

**Table 8-2 Bluetooth controller known issues**

| ID | Description |
|---|---|
| B-54012 | When Bluetooth device is master of a link and it initiates a disconnect procedure during Authentication, Bluetooth device can fail to send an Authentication Complete event to its host. |
| B-66906 | When Bluetooth device is responding to Secure Simple Pairing and the local host initiates a disconnect procedure, Bluetooth device can fail to send a Simple Pairing Complete event to its host. |
| B-67171 | If the device is connected to multiple peers and two SCO or eSCO negotiations are initiated simultaneously (by the device, by the remote peers or a mix) then problems can occur. The problems can occur on connection or disconnection of the SCO link.<br><br>Typical symptoms are:<br><br>Receiving a disconnection complete event with the reason code of "unspecified error" immediately after the connection complete event when bringing up an SCO link;<br>Seeing `LMP_not_accepted remove_(e)SCO_link_req invalid_lmp_parameters` sent over the air when the (e)SCO link disconnection is attempted.<br>or<br>If running upper layers on chip, the firmware may terminate with `PANIC_STREAM_GONE_MISSING`. |
| B-81479 | Problems may be encountered if the device is asked to pair with multiple remote devices simultaneously.<br><br>The most common symptom is to get hardware error 0x4c (`FAULT_LM_SPURIOUS_TIMEOUT`). It is believed that other symptoms may be possible.<br><br>As a workaround, where possible, the application should avoid multiple simultaneous pairings. This situation is quite rare in practice. |

| | |
|---|---|
| B-170083 | PSKEY_LC_MAX_TX_POWER and BCCMDVARID_MAX_TX_POWER are supposed to limit the maximum power ever transmitted by the Bluetooth radio.<br><br>These limits are not being applied to Bluetooth Low Energy links.<br><br>Normally, this is not a problem as the PS Key defaults to +20 dBm and the default Bluetooth Low Energy power (which is controlled by PSKEY_BLE_DEFAULT_TX_POWER) is not allowed to exceed +10 dBm.<br><br>However, if either the PS Key or BCCMD are lowered below the Bluetooth Low Energy power then the Bluetooth Low Energy power is not being clipped. This could cause regulatory failures in jurisdictions where the maximum transmit power of devices is limited. The PS Key setting is unlikely to be an issue in practice as such problems would be detected before devices were released.<br><br>A workaround is to set the Bluetooth Low Energy default power explicitly whenever the maximum device power is set let below the current default power.<br><br>**NOTE:** As documented in the BCCMD documentation, changing the maximum transmit power has no effect on links that are already running. It affects only new links. |
| B-255586 | In rare circumstances when ACL data is being received simultaneously from multiple remote devices and an ACL link is disconnected then the device can become unresponsive.<br><br>The underlying cause is a race in the firmware when switching from sending the host an ACL packet received from one remote device to sending the host an ACL packet received from another remote device and having a link disconnect during the switch.<br><br>The scenario is unusual, and the race is extremely narrow. It has been found in Qualcomm internal testing. This problem has never been reported from the field despite having been present for over a decade.<br><br>Two possible signatures of this failure are the panic codes `PANIC_HOSTIO_OUT_OF_ORDER_CLEAR` and `PANIC_HOSTIO_DATA_OUT_BUFFER_ERROR`.<br><br>This issue has been previously reported as TF-14837 or TF-16907 on some release notes. |
| B-257839 | Altering the length of PSKEY_AM_PRE_EMPHASIS_COEFFS from 3 coefficients when using the 2nd FIR tap filter degrades the ACP and DEVM performance of the radio. |
| B-265027 | When slave of Bluetooth link that has an eSCO using a multi-slot packet type (EV4, EV5, 2-EV5 or 3-EV5) with a short packet length, say 80 octets or less, it is possible that audio frames will be dropped causing intermittent or periodic audio drop out or audio glitches.<br><br>Using single slot packet types avoids this problem. All of the HFP safe settings use single slot packets so HFP use cases will not be affected by this issue. |
| B-265512 | If Remote Loopback Mode is enabled and there is an eSCO connection with multi-slot packets enabled, then a NULL packet may be sent in every second eSCO reserved slot. |

| | |
|---|---|
| B-278496 | If the device is slave of an eSCO but master of multiple Bluetooth Low Energy links with connection intervals that are a multiple of the eSCO interval and automatic PHY updates and data length extensions are enabled, audio glitches may be heard.<br><br>This situation can be improved in the following ways:<br><br>First by disabling auto PHY which is achieved by setting PSKEY_LE_PHY_POLICY to 0.<br><br>Second by modifying the connection interval of the Bluetooth Low Energy links such that they aren't all multiples of the eSCO interval.<br><br>Third by turning off data length extensions for the Bluetooth Low Energy links. |
| B-283004 | The "Enhanced Setup Synchronous Connection Command" and the "Enhanced Accept Synchronous Connection Request Command", when asked for an input or output data path of "HCI" should send "`UNSUPPORTED FEATURE OR PARAMETER VALUE`" (`0x11`) not `INVALID HCI COMMAND PARAMETERS` (`0x12`).<br><br>This may fail Qualification Test LMP/LIH/BV-136 on a later TS. |
| B-283592 | The radio calibration that corrects for non-linearity between amplitude and phase modulation paths is designed to function correctly when the radio is presented with a 50 Ohm load. If this is not so - for example, if no antenna is present - then the calibration may fail. If the calibration fails, compensation will not be applied and, that may result in degraded DEVM. If this happens, the calibration will signal the same to the upper layers by emitting a fault over HCI, with code 0x9a (FAULT_AM_PM_PHASE_UNACCEPTABLY_LARGE). |
| TF-1936 | Bluetooth low energy connections may occasionally fail to establish by timing out 6 events after connection creation. QTIL believes this problem is likely to occur in ~0.002% of connection attempts.<br><br>After a connection fails to establish, subsequent attempts to establish a connection are possible without any need for a reset (warm or cold). Given the low frequency of occurrence, such attempts are likely to succeed so the failure does not appear to have a major impact on the user experience. |
| TF-3196 | On rare occasions when slave of an €SCO link creation of a BLE connection may fail. |
| TF-5701 | Putting a link into sniff and enabling sniff subrating may occasionally cause the link to be dropped. |
| TF-6451 | In a complex scatternet use case where the device is:<br><br>▪ Slave of a BR/EDR link to a remote device with (e)SCO (the failure has been observed only with eSCO, ev3, T=6 but links with other parameters may be affected)<br>▪ Master of an Bluetooth Low Energy link to a second device with connection interval of 48.<br>▪ Page scanning<br>▪ Advertising<br>▪ When a third device establishes a BR/EDR link, there may be a transient impact to (e)SCO audio quality to the first device. After the connection is established, (e)SCO audio quality returns to normal. |
| TF-7696 | In some scenarios where the device is the master of a Bluetooth Low Energy link to a remote peer and the slave of two other ACL/eSCO links with TeSCO=6 and WeSCO=2 to separate remote peers, loss of eSCO packets can occur, adversely impacting audio quality. |

| | |
|---|---|
| | These configurations are not fully supported owing to the inherent costs of servicing three separate clock domains and must be considered a "best endeavours" basis.<br><br>Use cases should not design-in this combination of link parameters and topology if robust operation is required. |
| TF-8757 | In some complex topologies it is possible for ACL data to flow unevenly as the Bluetooth baseband switches between piconets. The more complex the topology the more uneven the data flow can become.<br><br>For use cases where data needs to be delivered by a deadline this can cause problems, for example it may cause glitches in A2DP use cases if the data is delayed long enough for the receiver's buffer to drain. The smaller the buffer the more likely this is to occur.<br><br>During Qualcomm's internal baseband testing; simulating an A2DP link with one device maintaining a second idle ACL link while being master of five Bluetooth low energy links, some with low (around 10 ms) connection intervals, data was occasionally delayed for more than 65ms.<br><br>Real world A2DP devices tend not to have such complex scenarios and tend to use significantly larger receive buffers.<br><br>This problem has not been seen in system level testing which runs more common topologies and buffer sizes. |
| TF-9647 | Internal development testing has identified that there are occasional isolated failures of a test case when the use of an illegal reason for link disconnection is detected by a test script.<br><br>The test forces one side of a link to enable encryption on an Bluetooth Low Energy link whilst keeping the other side unencrypted. A packet is sent unencrypted but received encrypted. The test is to ensure that the system detects the problem and disconnects the link.<br><br>In about 1% of cases, the unencrypted packet appears to be a packet that would force the link to be disconnected. This includes the packet appearing to be a `TERMINATE_IND` or packet initiating a transaction that uses an instant but the instant is in the past.<br><br>In these cases, the code path that disconnects the link due to the packet contents disconnects the link before the code path that disconnects the link due to an invalid MIC.<br><br>The same code path race could cause an genuine attack on an encrypted link to be misreported as some other reason in a small fraction of cases. The link is always disconnected so the attacker cannot inject data onto the link.<br><br>The overall result is that the link is always safely disconnected but in these 1% of cases the reason for the disconnection is incorrect. Commonly it's Instant Passed (`0x28`) less commonly it can be an arbitrary value (except `0x00` Success and `0x08` Connection Timeout which are both trapped by the firmware and rewritten to `0x1f` Unspecified Error). |

| | |
|---|---|
| | **NOTE:** The disconnection event is unusual for having two status/reason/error codes in it. One is the status indicating whether the disconnection was successful. This is always Success (`0x00`) indicating the link has now been dropped. The other is the reason for the disconnection. It's only this latter reason code that may be corrupted.<br><br>Hosts worried about attacks should always be able to deal with arbitrary reason codes in a disconnection complete event as on an unencrypted link, or even an encrypted link without man-in-the-middle protection, an attacker on the other side could always have sent an arbitrary reason code.<br><br>On previous release notes this issue may have been reported as a Known Issue because of concerns that the invalid reason code was due to memory corruption which could have had far larger impacts. Investigation has shown that this is not the case and so this is now being reported as an issue that has been addressed (by the investigation and this report of the investigation's findings). |
| TF-10766 | Internal testing has identified that there are piconet topologies where the Bluetooth firmware fails to correctly schedule (e)SCO reserved slots when they clash with other activities.<br>Impact within a given use case is dependent on the probability of a failure to schedule a particular set of reserved (e)SCO slots and a lack of successful retransmission.<br>Although in testing the failure showed rarely and normally caused a drop of only a small number of (e)SCO packets, very occasionally larger number of packets were dropped, sometimes exceeding 1% which would lead to degraded audio. |
| TF-11036 | In complex scenarios, where connection formation is not expected to be completely reliable, the probability of forming a connection when the device is page scanning is lower than it should be. |
| TF-12534 | The audio quality of Connectionless Slave Broadcast may degrade in challenging RF environments where minimal numbers of RF channels remain viable. Consequently, it is not currently possible to validate that Connectionless Slave Broadcast is at CS quality purely through subsystem-level testing of the Bluetooth Subsystem. |
| TF-12987 | Internal performance comparisons have identified that this Bluetooth firmware exhibits reduced page scan performance in use cases where the device is also using a high proportion of the available bandwidth for data transfer, impacting the likelihood of the device being located in any given page operation.<br><br>Available data suggests that under test conditions, a page operation to this device will succeed in ≥90% of cases within 5.12 seconds and 99% of cases within 10.24 seconds.<br><br>This issue is likely to manifest itself in use cases as an increased proportion of connection attempts exhibiting an increased connection time. |
| TF-13040 | Internal testing has identified that in Bluetooth Low Energy scatternet scenarios where the Bluetooth firmware is servicing multiple clock domains, where the local device is functioning as Bluetooth Low Energy slave for more than one of those domains, and there are multiple, relatively short-interval (up to a connection interval of 24) Bluetooth Low Energy links which are continually made and broken, one of the slave links may be dropped.<br>Applications should anticipate the possibility of unexpected Bluetooth Low Energy link failure in complex use cases, and respond accordingly. |

| | |
|---|---|
| TF-13219 | The Bluetooth firmware will permit the creation of a Connectionless Slave Broadcast (CSB) link in situations where existing (e)SCO links leave insufficient remaining airtime for CSB traffic to be scheduled.<br><br>In these situations, the Bluetooth firmware will correctly prioritise (e)SCO traffic to safeguard (e)SCO audio quality.<br><br>Ultimately, the CSB link may subsequently disconnect due to link starvation. |
| TF-14291 | Data transfer rates may be 1% lower than would typically be expected for production devices. This data transfer rate reduction was observed with 3DH5 packets in use over the air interface. |
| TF-15086 | In a scatternet scenario where the local device is slave of a T=12 eSCO link, master of an ACL to a second device and master of multiple Bluetooth Low Energy links to additional devices, occasional LE link failure has been observed.<br>Not all Bluetooth Low Energy links are affected by this failure mode. Bluetooth Low Energy link failure has been correlated with the creation of the eSCO link.<br>Available test data suggests that the observed failure rate for affected Bluetooth Low Energy links is around 2%. |
| TF-15643 | The device could exhibit reduced page scan performance when it is simultaneously performing undirected advertising. |
| TF-16442 | On rare occasions, a Bluetooth Low Energy disconnect may complete with the reason code `connection_timeout`.<br><br>Ultimately the link still disconnects but the host doesn't receive the notification until after the connection timeout period. |
| TF-16837 | On rare occasions, Bluetooth Low Energy links may be dropped. |
| TF-17241 | If the device is slave to a BR/EDR link in sniff and, a slave or master of a Bluetooth Low Energy link with a connection interval that's a multiple of the sniff period, the Bluetooth Low Energy link may be dropped.<br><br>Attempting to perform a connection update on the Bluetooth Low Energy link may also cause the link to be dropped. |
| TF-17820 | A Bluetooth low energy Link may be dropped in the following scenario:<br><br>A piconet where the device is master of an (e)SCO and a Bluetooth low energy link using data length extensions where the connection interval of the Bluetooth low energy link is a multiple of the (e)SCO interval.<br><br>To reduce the likelihood of link loss in this scenario QTIL recommended that the connection timeout of the Bluetooth low energy link is at least six connection intervals. |
| TF-17874 | Switching a Bluetooth low energy link from 1 Mbps to 2 Mbps increases the likelihood of transmitting or receiving packets with checksum errors.<br><br>Packets containing these errors will then be retransmitted so no data will be lost. This could marginally lower the data transfer rate.<br><br>If too many packet errors are detected in a short space of time and dependent on the setting of the PHY policy and switch points in PSKEY_LE_PHY_POLICY and PSKEY_LE_PHY_POLICY_SWITCH_POINTS respectively it could cause the controller to autonomously switch the link's PHY down to 1 mbps. |

| | |
|---|---|
| TF-17962 | When slave of a Bluetooth link with a short interval eSCO (T=6) and master to multiple Bluetooth low energy links whose connection intervals are multiples of the eSCO interval, audio glitches may occur.<br><br>Extending the eSCO interval (if possible) or adjusting the Bluetooth Low Energy link connection intervals such that they are not all multiples of the eSCO interval should nullify or minimize any audio glitches. |
| TF-17982 | Interoperability testing has revealed a number of issues with BR/EDR Secure Connections encryption with a range of devices, typically, mobile phones, from multiple manufacturers that are already deployed in the field.<br><br>Although the issues have different underlying causes the net result is that the BR/EDR link is dropped (usually for security reasons).<br><br>The link is most likely to be dropped with high volumes of inbound data such as when operating as an A2DP sink. In some testing the link was typically dropped after about half an hour of streaming. This can give a poor user experience. There is some evidence that some of the failure modes are more likely to be encountered in noisier environments or when the third party device is performing coexistence with co-located Wi-Fi.<br><br>If BR/EDR Secure Connections encryption is not an absolute requirement of the use case then Qualcomm are currently recommending that BR/EDR Secure Connections be left turned off in the application. This will cause the system to use the legacy E0 encryption.<br><br>If BR/EDR Secure Connections encryption is an absolute requirement then customers are advised to test extensively with the mobile phones with which they intend to operate and, if necessary, advise end users of potential interoperability issues if they use untested phones.<br><br>Qualcomm do not recommend that devices try to determine automatically whether to use BR/EDR Secure Connections. If BR/EDR Secure Connections encryption was a security requirement then the device would become vulnerable to a downgrade attack. In contrast, if legacy encryption is acceptable from a security perspective then using it all the time avoids the user experience problems.<br><br>**NOTE:** These issues do not affect Bluetooth Low Energy secure connections. |
| TF-18072 | When the device is busy performing a Link Manager Protocol procedure on BR/EDR link encrypted using Secure Connections, it can occasionally generate spurious Authenticated Payload Timeout events.<br><br>This can be worked around by increasing the value of PSKEY_SC_PING_TIME_ADJUST which will increase the lead time used by the controller to decide how far ahead of the Authenticated Payload Timeout it should initiate a ping procedure. |
| TF-18099 | When master of one Bluetooth low energy link, and slave to another Bluetooth Low Energy link whose connection interval is a multiple of the master link, it's possible that the slave link may get dropped.<br><br>This can be avoided by using connection intervals that are not multiples of each other. |

| | |
|---|---|
| TF-18496 | Using a Bluetooth Low Energy link with a long effective connection interval (either due to a large connection interval or large connection latency), commands that use an 'instant' will take a long time to complete. During this time the device will not be able to initiate or respond to other link layer commands.<br><br>Commands that use an instant will take affect 6 connection intervals after being issued.<br><br>For example, a Bluetooth low energy link with `connection_interval` of 14 slot pairs and `connection_latency` of 499 could take up to 52.4 s to complete if the slave device uses the full latency on each connection interval.<br><br>During that time commands such as `le_start_encryption` or `le_read_remote_features` are buffered and are not issued or responded to until after the instant has passed. |

# 8.3 System and boot manager known issues

Table 8-3 lists the issues known to be present in this release.

**Table 8-3 System Manager known issues**

| ID | Description |
|---|---|
| CUR-6139 | In the system message `MessageSubsystemVersionInfo` delivered to the application when a subsystem starts, in the case of the audio subsystem (`ss_id == 3`), only the lower 16 bits of the `fw_rom_version` identify the audio firmware version; the upper 16 bits contain unwanted data (although it is expected to be constant for a given audio firmware version). |
| CUR-6244 | Upon insertion of some VOOC/Dash USB chargers, such as the VIVO V2323A-CN, the System Manager will report several faults for a minute. This is not known to cause any issues with charging or the general device. |
| CUR-6586 | If the System Manager configuration key ResetOnChargerAttach is set to true, the device will also reset if the charger type changes while attached e.g. A wall charger enumerates late and becomes a SDP. |

# 9 Resolved issues

Sections 9.1 to 9.3 list the resolved issues in the Audio, Bluetooth, and System Manager ROMs between this release and previous releases. Table 9-1 summarizes the ADK version numbers for reference.

**Table 9-1 ADK Version number summary**

| ADK Release Containing ROM Patches | Audio Version/Build Numbers | Bluetooth Version /Build Numbers | System Manager Version/Build Numbers |
|---|---|---|---|
| ADK_QCC512x.WIN.6.4.2.26 | v79/8988 | V88/14512/3/4/5 | V39/1669 |
| ADK_QCC512x.WIN.6.4.0.43 | v64/7992 | v83/14444/5/6/7 | v36/1607 |
| ADK_QCC512x.WIN.6.4.0.34 | v58/7603 | v75/14363/4/5/6 | v35/1584 |
| ADK_QCC512x.WIN.6.3.2.24 | v48/6519 | v68/14100/1/2/3 | v33/1549 |
| ADK_QCC512x.WIN.6.3.1.31 | v40/5862 | v68/14100/1/2/3 | v26/1502 |
| ADK_QCC512x.WIN.6.3.1.26 | v40/5862 | v68/14100/1/2/3 | v25/1488 |
| ADK_QCC512x.WIN.6.3.0.154 | v26/5360 | v61/13942/3/4/5 | v21/1458 |
| ADK_QCC512x.WIN.6.2.84 | v20/5163 | v54/13835,13836 | v18/1424 |
| ADK_QCC512x.WIN.6.2.77 | v20/5163 | v51/13804,13805 | v16/1413 |
| ADK_QCC512x.WIN.6.2.50 | v14/5064 | v41/13715,13716 | v12/1368 |

**NOTE:** Changes with a strike through (~~thus~~) indicate changes subsequently removed or replaced.

# 9.1 Audio subsystem resolved issues

**Table 9-2 Audio subsystem issues resolved between v64 and release v78**

| ID | Description |
|---|---|
| B-247915 | Audio graphs using IIR resampler could suddenly start experiencing unrecoverable high-pitch buzz at the output. The buzz could be very loud in some circumstances but it also can be very quiet. |
| B-254207 | In some cases Time-to-Play (TTP) playback could become choppy due to inaccurate TTP info generated by a TTP_PASS operator. This was not observed to affect standard A2DP or HFP use cases; it could affect wired input at very low sample rates like 8 kHz. |
| B-255939 | A threading issue causes the SBC encoder to crash if its input is attached to a task running at a higher priority. |
| B-276322 | Audio graphs using IIR resampler could suddenly start experiencing unrecoverable high-pitch buzz at the output. The buzz could be very loud in some circumstances but it also could be very quiet. |
| B-285729 | Internal DAC channels might have spurious tonal noise that might be noticeable when their input is silent or very quiet. This happens only if DACs have configured HW DC offset (using efuse or MIB key) for avoiding pop and clicks. |
| B-288687 | Addition of Opus-CELT encoder downloadable capability supporting 16kbps voice encoding. |
| B-288826 | Graphs using CVC + AEC_REFERENCE for echo cancellation might experience noticeably high echo in SEND path once every few hours for a short period of time (a few seconds).<br>The problem has been observed only in narrow-band graphs however it's a generic issue and happening in other configurations cannot be ruled out. |
| B-290955 | The Packet Loss Concealment(PLC) algorithm used for Wide Band Speech eSCO links can fail to conceal corrupt packets smoothly and instead introduce discontinuities into the output. These may be heard as sharp glitches. |
| B-291552 | There is a possibility of memory corruption in audio subsystem if a digital or analogue microphone is connected/disconnected while another microphone is being used for standalone ANC or hardware sidetone. The corruption will cause audio to crash with a panic, but the type of panic can vary. |
| B-291735 | A left/right channel phase offset is seen at the DAC output after enabling a stream. |
| B-291965 | File Manager causes a panic if two files are loaded in the Audio RAM and the file loaded last is removed. |
| B-292167 | There is possibility of cVc microphone inputs are sampled of sync when ANC is enabled. This problem does not happen in first call. |
| B-292915 | Update timestamp handling for aptX adaptive streams from AOSP / Generic devices. Improves long term stability |
| B-293609 | Added support for HFP voice graphs to handle unaligned WBS frames. This support is often required for WBS SCO connections to PCs. |

| ID | Description |
|---|---|
| B-294040 | Graphs with timed-playback enabled might see sudden change in the latency, the amount of change can be up to 2ms and it will take several seconds for that that change to gradually disappear. The sudden change is mostly triggered by jittery delivery to the graph.<br>One consequence of this bug is a potential short-term out of sync issue between left and right channels in synchronized devices.<br>This has only been seen with graphs using AEC_REFERENCE for timed playing back, however it occuriing in other timed playback modules cannot be ruled out.<br>This bug only affects a workaround that addresses the cases where AEC_REFERENCE is used for timed playback. |

### Table 9-3 Audio subsystem issues resolved between v63 and release v64

| ID | Description |
|---|---|
| | None (The patch reports a different build number but has no other changes) |

### Table 9-4 Audio subsystem issues resolved between v58 and release v63

| ID | Description |
|---|---|
| B-288663 | Enabling Audio chain(Prompt/music/voice) while standalone ANC is ON cause audible pop along with drop in output of the ANC path. |
| B-288486 | In the QCC512x Sink Application when ANC is enabled in standalone mode or when music is being streamed an audible pop is heard. However when ANC is enabled during a call no audible pop is heard. |
| B-287934 | CMC should be disabled by default. |
| B-288191 | ADK6.x Long term A2DP streaming with an iPhone using the AAC codec occasionally causes the slave earbud to lose audio. |
| B-288199 | In music streaming cases using the AAC codec, a temporary disruption to the Bluetooth link could result in playback timing problems, most noticeable in TWS systems where there could be a significant synchronisation error. |
| B-287526 | When encoding 0dB signals some 3rd party AAC encoder implementations may produce encoded data which causes saturation to occur at the output of the AAC decoder. This results in audio distortion in the PCM output signal of an AAC decoding chain. |
| B-284133 | If the audio thread offload feature is enabled using the MIB key, OperatorFrameworkEnable(SECOND_PROCESSOR_ON/OFF) trap returns failure.<br><br>Also selecting a non-zero processor ID for the CreateOperatorEx() trap / `CREATE_OPERATOR_EX` ACCMD does not allow the operator instance to use the offload feature even if is supported by the capability. |

### Table 9-5 Audio subsystem issues resolved between v48 and release v58

| ID | Description |
|---|---|
| B-281613 | Running sbc_decoder.cfg.json test on KSE config under ADK 6.3.x hangs. |
| B-281647 | Support for building download_async_wbs capability from the MDE on ADK 6.3.x is not available. |
| B-281706 | DC remove cbops operator does not converge to zero and so may have a residual DC offset. |
| B-283159 | The Q format of the filter coefficients used in ANC hardware needs to match how QACT interprets it |

| ID | Description |
|---|---|
| B-284002 | KCSMaker fails when the nth argument passed to a C function is a variable and n >=5. |
| B-284168 | KCSMaker throws an error when including a non-private library (`.a`) in **lib_release** or when calling into libc functions (such as `vsnprintf`). Example: `"Exception: Error returned: 1, file: C:\<WORKSPACE_PATH>\audio\kalimba\kymera\lib_release\debugobj\<OBJ_FILE>.o"` |
| B-284942 | Having a group of `const` variables in the code can generate an "Unexpected symbol name" error in KCSMaker |
| B-285079 | Building private libraries with KCSMaker might fail with error: "Exception: Unexpected symbol name: loop0 from KCSMaker" |
| B-285325 | Downloadable AEC reference build fails trying to include `patch_ids.h` file |
| B-286967 | This bug fix a QACT issue concerning maximum value allowed for AEC tail length parameter (`AEC_FILTER_LENGTH`). |
| B-284500 | Remove Audio SS external PSRAM access functionality from the patch bundle for QCC3020/21/24/26/31/34 and QCC5120/21/24/25 |
| B-284662 | Remove voice activation (i.e. the ability to respond to a wake up word) functionality from the patch bundle for QCC3020/21/24/26/31/34 and QCC5120/21/24/25 to reduce the size of the patch bundle. |

### Table 9-6 Audio subsystem issues resolved between v40 and release v48

| ID | Description |
|---|---|
| B-280810 | Added new MIB key RelaxMallocStrictness.<br><br>▪ 0: Default. No fallback for MALLOC_PREFERENCE_DM2 and MALLOC_PREFERENCE_DM1. Memory allocation mechanism attempts to allocate evenly between DM1 and DM2 (called load balancing) for MALLOC_PREFERENCE_NONE option.<br>▪ 1: Load balancing enabled for MALLOC_PREFERENCE_NONE option. Failure to allocate from the requested region for MALLOC_PREFERENCE_DM1 or MALLOC_PREFERENCE_DM2 option will fall back to the other region.<br>▪ 2: DM1 as the preferred region for MALLOC_PREFERENCE_NONE option with no load balancing. Failure to allocate from the requested region for MALLOC_PREFERENCE_DM1 or MALLOC_PREFERENCE_DM2 option will fall back to the other region.<br>▪ 3: DM2 as the preferred region for MALLOC_PREFERENCE_NONE option with no load balancing. Failure to allocate from the requested region for MALLOC_PREFERENCE_DM1 or MALLOC_PREFERENCE_DM2 option will fall back to the other region.<br><br>Default value 0 is the setting used until the introduction of this new MIB key. |
| B-281102 | When using TWS with A2DP SBC input, the audio subsystem could occasionally fail with `PANIC_HYDRA_ASSERTION_FAILED` when the data flow was disturbed (observed when the relay link dropped, maybe also possible in other scenarios). |
| B-281303 | The QCC302x/QCC512x DAC operating in class D mode may produce periodic noise which might be audible in quiet conditions when sensitive speakers are used. |

| ID | Description |
|---|---|
| B-281840 | Adds additional MIB keys for Class D Amplifier configuration.<br>"Codec0OutClsDAmpDitherEnable" enables whitening of tonal noise in the audio band with a small SNR degradation.<br>"Codec0OutClsDAmpControlMode" enables a reduction of pop/clicks while turning on the Class D DAC with a small increase in power consumption.<br>By default, both MIB values are set to true.<br>Enable new DAC initialization sequence to improve pop & click performance. |
| B-281062 | Reduction in pop seen when ANC is in standalone mode. |
| B-281102 | Stall A2DP endpoint earlier to avoid out-of-memory situations. |
| B-274900 | A new feature has been added to allow some capabilities to "offload" their processing to the second DSP core, without much of the overhead involved in normal dual-core operation. This is only available on devices where the second core is available. This can be used to have more MIPs available while keeping memory foot print low. The audio graphs are constructed as if they are running on one core. Use of this feature may increase the latency of the audio graph.<br>A new ThreadOffload MIB is used to enable the feature. |
| B-281112 | OperatorFrameworkPreserve has no effect if only endoints are specified. |
| B-282056 | Repeated destroying of certain operators such as TTP-passthrough, RTP-decode, USB Rx, and AEC_REFERENCE may result in audio drop-outs at the beginning of the stream. |
| B-280703 | DC remove cbops operator does not converge to zero and so may have a residual DC offset. |

### Table 9-7 Audio subsystem issues resolved between v26 and v40

| ID | Description |
|---|---|
| ~~B-270530~~ | ~~QVA leaks memory every time it's issued a start message~~ |
| ~~B-272245~~ | ~~Stack overflow in QVA may occur caused because of large automatic variable~~ |
| B-272938 | Re-order Kalimba assembly instructions to avoid hardware ISA bug:<br><br>This bug affects ASHIFT instruction immediately following RMACB with optional add, where the shift operand register is the same as the destination register of the optional add. For example:<br><br>MACB = rMACB + r0*r5, r0 = r2-rMAC;<br>r0 = r0 ASHIFT -1; // r0 is invalid<br><br>This issue may be worked around by inserting a NOP (or other unaffected instruction) between the rMACB MAC and the ASHIFT instruction, as follows:<br><br>MACB = rMACB + r0*r5, r0 = r2-rMAC;<br>NOP;<br>r0 = r0 ASHIFT -1; // r0 is invalid |
| B-274395 | Enable the Audio Thread offload support which enables the capabilities to selectively offload some work to the audio second core. This is enabled only when the audio dual core support is disabled on QCC512x using coreEnable MIB key. |
| B-274629 | File manager can allocate files to external SRAM. |
| B-276126 | A panic (`0x19`) occurs when attempting to set the Source Sync capability from persistent storage (PS). |

| ID | Description |
|---|---|
| B-276156 | A new API is provided to access data on an external SRAM chip. The access mode supported are circular or random, read and write. |
| B-276163 | Internal code relocation in preparation for development of a new feature, the `EXT_BUFFER`. None of the initial source code was reaching the customers and it still doesn't after the changes in this bug. The `cbuffer_ex` API should look the same externally. |
| B-276392 | Removed `PANIC_AUDIO_TIMER_TOO_OLD` |
| B-276431 | The Application can set new `OP_CLIENT_PROMOTE_PARAM` system key to promote an operator to an operator client by delegating a set of operators to it.<br>Call with no delegated parameters to cancel the promotion. |
| B-276432 | Delegated operators will have their unsolicited messages re-routed by the adaptor to the operator client owner. |
| B-276439 | Update the AOV client to work with the va graph manager |
| B-276718 | Using `AEC_REFERENCE` in a graph that speaker input or microphone output is originating/terminating from/to an audio type Source/Sink could cause firmware to panic with `PANIC_AUDIO_LIBRARY_ERROR`.<br><br>The effect is less likely to be observed with locally clocked back end (I2S master or internal codecs for example) there is higher chance for this to happen if backend is slave I2S and or if speaker path of `AEC_REFERENCE` is connected/disconnected while the operator is running. |
| B-276903 | The file manager (used with AOV) cannot handle odd-sized files. |
| B-277154 | Capability command handlers (start, stop, reset, and so on) no longer need to set the relevant response ID (although continuing to do so is harmless provided the correct ID is used). |
| B-277310 | Added support to enable, disable and clock control for SRAM. |
| B-278123 | The Framework enables the VA Graph Manager to specify any of the supported clock values as a custom clock to dynamically accommodate for VA graph MIPS needs. |
| B-278248 | Add support for new trap APIs `OperatorFrameworkDelegateMultiple` and OperatorFrameworkPreserve. |
| B-278249 | Fix a bug in the trigger notification message from low power. |
| B-278309 | Access functions to read/write PIOs allocated to the Audio subsystem (using curator's PioSubsystemAllocationElements MIB key) are missing |
| B-278443 | Stopping and starting an operator without being disconnected from an audio endpoint can leak memory. |
| B-278509 | Wrong patch version is reported from the audio second core. |
| B-278908 | Deprecate AEC REFERENCE capability and replace it with downloadable_aec_reference capability on ADK 6.3.1. |
| B-279001 | DSP will fail a request to set the deprecated `trigger_mode` argument in `AudioDspClockConfigure()` , and always return 0 in the corresponding argument of `AudioDspGetClock()`. |
| B-279589 | AAC and cVc running together need a bigger block of memory. |
| B-279787 | Loading and unloading downloadable capabilities in different order could corrupt the free pm heap management. |
| B-280031 | Update a DSP parameter check to accept updated `OperatorFrameworkTriggerType` values. |

| ID | Description |
|---|---|
| B-250509 / B-267795 / B-272934 | The AEC_REFERENCE capability does not currently work correctly if its speaker and microphone connections are clocked unequally (for instance, if the microphone input is analog but the speaker output is an I2S connection where DUT is the slave device). If it is used in a cVc graph, echo cancellation is not expected to work correctly in this situation. |

### Table 9-8 Audio subsystem issues resolved between v20 and release v26

| ID | Description |
|---|---|
| B-247915 | Audio graphs using IIR resampler could suddenly start experiencing unrecoverable loud high-pitch buzz at the output. The effect has been observed only in 1:2 resampling ratio but occurring in other cases cannot be ruled out. |
| B-254049 | Increase the maximum space available for a single downloadable capability on QCC521x/QCC302x/QCC303x. |
| B-254049 | Increase the maximum space available for a single downloadable capability on QCC521x/QCC302x/QCC303x. |
| B-255955 | Using the aptX mono decoder without a valid licence key could lead to a strange behaviour - instead of generating a stream of silence as expected, the decode chain is likely to fail with `PANIC_HYDRA_ASSERTION_FAILED`. |
| B-256224 | Microphone inputs can join and leave `AEC_REFERENCE` operator while the operator is running. However, a microphone source that has been disconnected from a running `AEC_REFERENCE` operator will fail to close later (`SourceClose()` will fail).<br><br>Typical uses of the `AEC_REFERENCE` operator (such as in the supplied sink application) are not affected, as typically the operator is stopped before any inputs are disconnected. |
| B-264983 | The profiler from ACAT doesn't advertise the correct CPU speed on QCC512x/QCC302x/QCC303x. |
| B-266595 | Setting time-to-play filter parameters or startup time with the `OPMSG_COMMON_SET_TTP_PARAMS` message could cause the TTP sample rate to be corrupted, resulting in jittery or stalled playback. |
| B-267382 | Digital mic performance may degrade on QCC512x/QCC302x/QCC303x at low frequencies (that is, digital mic is clocked at 2 MHz or below). |
| B-268422 | Audio graphs using the Timestamped source (apps-to-audio direction) endpoint, TWS slave, broadcast receiver and so forth, could incorrectly keep some data buffered at that endpoint instead of propagating it along the graph, leading to an increase in end to end latency. |
| B-268728 | Disabling the default audio endpoint signal processing in an audio graph is not possible on ADK 6.1/ADK 6.2.<br><br>This requires support for a new config key (`STREAM_AUDIO_DISABLE_ENDPOINT_PROCESSING`) for the `StreamConfigure()` trap with values:<br>0: Remove all endpoint signal processing<br>1: Remove DC filter from audio endpoint signal processing<br><br>**NOTE:** The stream configure command with the above key should be called before connecting the endpoint with any operator. |
| B-269795 | `CVC_SEND` patch may adversely affects the quality of receive path in wired voice graphs. It may also cause pops and glitches in send path. Wireless CVC (SCO NB and WB) use cases are not expected to be affected. |

| ID | Description |
|---|---|
| B-271565 | Running USB Receive Audio could exhaust available memory in use cases involving high amount of internal buffering like broadcast audio use case. |
| B-271767 | Support a new private lib template for third party security on QCC512x. |
| B-271726 | An error response to an operator message by an audio second core operator with no parameters results the application to panic. |
| B-272337 | Free up some unused memory adjacent to the share heap in single core configurations and add it to the shared heap. |
| B-272657 | Audio graphs using IIR resampler could suddenly start experiencing unrecoverable loud high-pitch buzz at the output. The effect has been observed only in 1:2 resampling ratio but occurring in other cases cannot be ruled out. |
| B-273500 | In audio graphs containing a splitter operator, it was possible for uneven data flow (as seen with A2DP inputs) to provoke a state of very bad audio, with short bursts of the wanted output between regular large gaps.<br>This has only been observed in the Broadcaster graph but is theoretically possible in other use cases (although expected to be much less likely in normal A2DP or TWS master scenarios) |
| B-273838 | An externally clocked stream passing through a Source Sync operator could over time cause the stall detection threshold of the operator to drift from its intended level. If the external clock was slower than the local clock, this could eventually cause false stall detection, and likely glitchy or distorted audio.<br>Also:<br>Depending on the type of input streams and on the timing of first the data from those streams arriving at the inputs of a Source Sync operator, the operator could subsequently be susceptible to false detection and handling of stalls. |

### Table 9-9 Audio subsystem issues resolved between v14 and v20

| ID | Description |
|---|---|
| B-250756 | Enhance the CVC SEND capabilities to support a new operator message `GET_VOICE_QUALITY` for providing the audio quality on the microphone path.<br><br>The mic audio quality should be reported in a scale of 0 to 15 in the operator message response, where:<br>▪ 0 = low quality<br>▪ …<br>▪ …<br>▪ 15 = best quality |
| B-261355 | Enabling and disabling ANC while DAC is in use (for example audio streaming) may cause audio clicks at the output. The level of audio clicks while using digital mic input is smaller compared to analog mic input. |
| B-264007 | Wired or wireless cVc might experience unrecoverable latency increase in received side. For 2EV3 and similar-length SCO packets latency increase could happen once packets starts arriving late from Bluetooth. |
| B-264701 | In configurations where multiple external digital microphone devices, each with a data line, were clocked by a single clock output from the QTIL device, it was possible for the data on the channels not associated with the clock output to be misinterpreted; for instance, this could manifest as a channel swap. This was more likely to happen at higher clock rates. |
| B-265998 | Streaming audio may fail with ANC, due to inconsistencies in the configuration of the ANC hardware block. |

| ID | Description |
|---|---|
| ~~B-266178~~ | ~~The output from digital microphones (DMICs) can take a significant amount of time to settle on power-up. This can lead to undesirable pops and clicks when enabling ANC (due to the DMIC turn-on).~~ |
| B-266489 | Stream connect fails while setting up a graph that contains a timestamped source endpoint and a SCO sink endpoint. |
| B-266673 | Incorrect behavior may occur when attempting to close an endpoint with a non `audio_endpoint` type. |
| B-267185 | CVC Send capability now supports metadata, allowing it to be used in audio graphs to perform timed playback. |

# 9.2 Bluetooth controller resolved issues

**Table 9-10 Bluetooth controller resolved issues between v83 and this release v88**

| ID | Description |
|---|---|
| B-291437 | From v83 onwards, the EDR Tx configuration is incorrect in Qualcomm's proprietary Radio Test mode. This causes problems for EDR modulation while transmitting packets and will increase ACP.<br><br>This does not affect radio operation in normal mode. |
| B-289472 | Some parts show higher Bit Error Rate (BER) at -40°C for Enhanced Data Rate (EDR) packets. |
| B-288998 | When a device has an eSCO of greater than 6 slots, it may choose to do eSCO retransmissions in preference to paging or inquiring. This will typically not be a problem unless there are also other activities also taking time away from the paging or inquiring, such as short-interval Bluetooth Low Energy links, in which case it may be difficult to make additional BR/EDR links. |
| B-289886 | When in a BR/EDR link, if our peer asks the device to disconnect a SCO or eSCO link immediately after setting it up then, it is possible for us to reject the request for disconnection as we have not yet finished setting it up. In this state, the (e)SCO link remains connected on our side but the remote side will think it is disconnected. The (e)SCO link can be disconnected by our host.<br><br>This can happen only in very unusual circumstances where the remote Link Manager processes our acceptance of the (e)SCO parameters, but the remote baseband does not acknowledge the packet. Interoperability testing has shown that there is at least one third-party device that can provoke this situation reliably when playing very short tones. |

**Table 9-11 Bluetooth controller resolved issues between v75 and release v83**

| ID | Description |
|---|---|
| B-272758 | The BT Radio IP2 can be adjusted to improve Wi-Fi blocking performance. |
| B-283359 | Packets on a Bluetooth Low Energy link may be missed when operating at 2 Mbps if the inter-frame spacing (T_IFS) of the remote device approaches 145us.<br><br>Dropping such packet may lower data throughput on the link and if sufficient packets are missed may lead to the link being dropped. |

| ID | Description |
|---|---|
| B-286686 | eSCO retransmissions are assigned a lower priority than bulk ACL data to prevent the eSCO retransmissions locking out all data transfer completely. Even with just small amounts of ACL data transfer, this can lead to degraded eSCO performance in an environment with high packet loss, such as at long range or when significant interference is present. The prioritisation should be more balanced to allow more eSCO retransmissions to be used with moderate ACL transfer rates. |
| B-286687 | When a device is master of an eSCO, and it receives an eSCO packet with a CRC error in the payload, the device will unnecessarily increase the priority of polling that slave for new ACL data.<br><br>The result of this is that this polling activity might take the place of eSCO retransmit slots, reducing packet loss performance of the eSCO in a noisy environment. If there are other links present, then the device may also assign less time to communicating with those links. |

### Table 9-12 Bluetooth controller resolved issues between v68 and release v75

| ID | Description |
|---|---|
| B-281412 | Removal of Unit Keys as part of 5.1 updates.<br><br>If the host issues Read Local Supported Commands HCI command, the controller will return a Command Complete event with bit 4 of octet 6 of the Supported Commands parameter set to 1. This bit is reserved for future use and should be set to 0.<br><br>If the host issues Create New Unit Key HCI command, the controller will return a Command Complete event with the Status parameter set to Command Disallowed (0x0C) instead of Unknown HCI Command (`0x01`).<br><br>If the controller receives an LMP_unit_key from a peer during pairing, it will carry on with the procedure instead of rejecting it with Pairing With Unit Key Not Supported (0x29) error.<br><br>These are in violation of the Bluetooth 5.1 specification which has removed support for the use of unit keys for security.<br><br>In addition to the above, PSKEY_LM_USE_UNIT_KEY should never be modified from its default value of FALSE. Attempting pairing with this key set to TRUE will result in undefined behaviour. |
| B-282217 | Adjacent channel power (ACP) at +/- 3, 4 and 5 MHz was approximately 10 dB too high due to radio timing in Radio Test mode. |
| B-282695 | The device will reject HCI `LE Write Suggested Default Data Length` command if the `TxTime` parameter is over `0x848`, with error code `0x12` (Invalid HCI Command Parameters). It should accept values up to `0x4290` as valid.<br><br>This will fail Qualification Test HCI/CCO/BV-11.<br><br>**NOTE:** Although the device should accept values above `0x848`, it will not be able to usefully use these values, because BLR is not supported. |
| B-287060 | When the device has an encrypted Bluetooth Low Energy link with another device, if the peer does not support the Bluetooth Low Energy Ping Feature, the Bluetooth Low Energy Ping is now still sent. |

### Table 9-13 Bluetooth controller resolved issues between v61 and release v68

| ID | Description |
|---|---|
| TF-15788 | On rare occasions the Bluetooth Low Energy enhanced receiver test can miss a packet. |
| TF-18554 | When the A2DP sink/CSB transmitter device is also receiving an over the air update from the A2DP source using a concurrent Bluetooth smart link, A2DP audio data may underflow resulting in audio glitches. |
| B-264697 | If the host issues a Read Local OOB Extended Data HCI command before enabling Secure Connections Host Support, the Status parameter in the resulting Command Complete event will contain Unsupported Feature Or Parameter Value (0x11) error code instead of Command Disallowed (0x0C) error code. |
| B-266913 | A device will reject adding an eSCO to a link if the μ-law log synchronous data feature is disabled, even if a different air mode is requested. A device may accept adding an eSCO to a link if the μ-law log synchronous data feature is enabled, even if a different air mode is requested, which is disabled by its feature bit. |
| B-267321 | Extremely rarely, over-the-air packets can be corrupted even in clean environments. |
| B-268785 | Radio ACP is marginal on some parts. |
| B-273131 | The start of day calibration that provides the linearity correction for transmit output power can be sensitive to the presence of external RF "noise", as previously reported under B-269424. As reported there, the solution to this problem is that values of "attenuation" greater than 10 should not be used. Power tables must be designed with this restriction in mind.<br><br>By modulating the local oscillator during calibration, and taking more measurement samples, it is possible to further increase robustness to external noise. |
| B-273509 | When a device is slave to 2 active BR/EDR masters, and is also a Bluetooth Low Energy slave, the length of baseband packets that can be transmitted by both BR/EDR masters to the slave is decreased from 5 slots to 1 slot.<br><br>This will result in low data rates and might manifest to the user as breaks in the audio stream on one of the BR/EDR links even when the other links are idle. |
| B-273757 | On a Bluetooth Low Energy link, the Host has the option to allow the controller to initiate autonomous PHY update procedures. The controller initiates autonomous PHY updates until the Peer specifies it prefers different values for its transmitter PHY than the ones our Controller suggested. This will cause the autonomous PHY updates to stop after which they can never be restarted by the Host. |
| B-274033 | If an autonomous PHY Update Procedure fails to complete, subsequent PHY update requests initiated by the Host may be sent to the Peer device with values for TX PHY and RX PHY that do not match those requested by the Host.<br><br>In these cases no Bluetooth Low Energy PHY Update Complete events will be sent to the Host. |
| B-275187 | When a device in the slave role is performing a role switch initiated by its host and receives certain LMP messages from the master (`LMP_hold_req`, `LMP_hold`, or `LMP_switch_req`), then a mistake in the transaction collision resolution can result in the device being unable to send data.<br><br>This problem does not occur in the master role. |
| B-276748 | In Connectionless Slave Broadcast, a memory leak will occur if an attempt is made to reserve an LTADDR that is already in use. Each attempt to do this will leak more memory, and sufficient repetition will cause the command to return a `memory_full` error, instead of "`acl_connection_already_exists`". |

| ID | Description |
|---|---|
| B-277028 | When a collision occurs between a Connection Update Procedure and a Connection Parameters Request Procedure the Slave initiated procedure is rejected with error code “Different Transaction Collision” (0x2a) instead of “LMP Error Transaction Collision / LL Procedure Collision” (0x23). |
| B-277765 | When a Bluetooth low energy link has a short connection interval of 12 or 14 slots, and is using 2 Mb signalling in one direction and 1 Mb signalling in the other, and data length extensions is used, then the device may send LL_LENGTH_REQ or LL_LENGTH_RSP messages containing invalid MaxRxTime or MaxTxTime values. |
| B-279170 | A zero-length L2CAP start packet (such as is tested by LL/DFL/MAS/BV-01; represented over HCI as a 4-octet packet with LLID of "start") will be discarded by the firmware. Because of this, a subsequent continuation for the packet (with LLID of continuation, and beginning with the L2CAP header) will be sent over the air as a "continuation" packet, when it should be combined with the zero-length start and sent over the air as a "start" packet.<br><br>On reception of a zero-length L2CAP packet the firmware will emit a hardware error, with code 0x6d (hci_acl_packet_no_payload). Because such a packet is not useful, and should not be sent by a correctly functioning host, this error is emitted independently of the bug described here, in order to warn developers of a problem with their host. Tests that deliberately send such packets in order to test L2CAP segmentation handling by the device should ignore the hardware error. |
| B-279350 | In some scatternet situations a device might transmit longer packets than it determines is ideal for the situation. It does this without going beyond the max slots value negotiated with the peer.<br><br>One way this could be observed in practice is in asymmetrical bulk ACL data rates between a scatternet device and its peer in the presence of eSCO or a short-interval Bluetooth Low Energy link. |
| B-279419 | As a result of changes to adaptive gain control (AGC) settings under B-272599 and TF-15788, the "margin" for Bluetooth Low Energy Time Inter Frame Space (T_IFS) has been reduced by approximately 2 microseconds, especially for links at relatively high RSSI. By default, there is approximately 3 microseconds additional margin in this parameter, so devices should remain within the specification; however, it is desirable to restore the extra "margin". |

### Table 9-14 Bluetooth controller resolved issues between v54 and release v61

| ID | Description |
|---|---|
| TF-18918 | When Slave A2DP sink and Connectionless Slave Broadcast (CSB) audio source, and when the CSB audio sink is in close proximity to the A2DP source and the A2DP sink/CSB audio source is far away, this may result in the CSB sink receiving the A2DP and CSB packets at a similar power level.<br><br>This may cause over the air interference between A2DP and CSB, resulting in audio glitches on the CSB sink.<br><br>This is not a bug in the firmware, but an intrinsic aspect of the Bluetooth design. It may be mitigated by careful choice of the erasure coding parameters used for the CSB link. |

| ID | Description |
|---|---|
| B-262602 | Radiotest commands TXDATA cannot be used with sufficient precision to design power tables.<br><br>The power control architecture differs strongly from previous chips, and the method initially chosen to transfer information from the `lvl` parameter does not allow sufficiently precise setting of the various elements, which is needed for power table design by TXDATA. It does suffice to simply cause an increase in transmit power with increasing `lvl`.<br><br>See the application note on Designing Power Tables for full details. The fundamental architecture for packet-based transmit products power in response to three elements: attenuation, magnitude and exponent. Attenuation (`atten`) is an analog component and corresponds to the number of "segments" switched off; 0 switches off none and produces most power; 15 switches off all and produces no power. Magnitude (`mag`; signed, range `7` to `-8`) and exponent (`exp`; unsigned, range `0` to `3`) act together digitally to produce power proportional to (`1 + Mag / 16) / power(2, exp`).<br><br>In brief, the fix for this problem is that the `lvl` parameter should regarded as a 16-bit word of four nybbles `0xabcd`; `a` is used as `atten`, `b` is used as `mag`, the bottom two bits of `c` as `exp` and the top two bits are reserved, the high bit of `d` is a flag that bypasses the correction for non-linearity of the analog and the bottom three bits are reserved. Reserved bits must be `0`. |
| B-263452<br>(TF-17124) | Bluetooth low energy links with short connection intervals (12 slots) performing duplex bulk data transfers and using data length extended packets can block slave BR/EDR Bluetooth links from being serviced.<br><br>This can lead to failure to create a slave BR/EDR link/LMP response timeouts when attempting LMP commands and failure to transfer ACL data on the link. |
| B-270178<br>(TF-13040) | When the device has two Bluetooth Low Energy links, one each as master and slave, and the anchor point for the link where it is slave is about 1200 us after the master link, the firmware will try to receive the remote master's transmission although it cannot accommodate all of the window widening needed by the slave link. This may cause the slave link to time out. |
| B-270224 | In a scatternet topology containing a periodic event such as eSCO or Bluetooth Low Energy with an interval less than 30 ms, as well as sending data over a BR/EDR link to another device, choosing large packet sizes for the BR/EDR link may cause degradation of the periodic event.<br><br>The observed result is loss of SCO frames, or Bluetooth Low Energy connection events. |
| B-270571 | During duplex data transfers over an Bluetooth Low Energy link with Data Length Extension Enabled, with the device as slave and with a narrow range of timing differences between the clocks of the device and its peer, the data transfer rate can be significantly lower than it should be because the device fails to schedule the Bluetooth Low Energy activity about 30% of the time. As the timings of the devices drift with respect to one another, the devices would drift in and out of this situation. |
| B-270572 | When the device is in a scatternet, with at least one link a Bluetooth Low Energy link with Data Length Extension enabled, then due to a small timing miscalculation, the data rate may be a bit low (about 6% lower than optimal) on the Bluetooth Low Energy DLE link. |

| ID | Description |
|---|---|
| B-271151 | In cases where only a single Bluetooth Low Energy link is active and then disconnected, the channel map used for that initial Bluetooth Low Energy link will be used to create a subsequent Bluetooth Low Energy connection. If a long time were to pass between these connections that channel map may have become stale.<br><br>**NOTE:** The channel map is always re-evaluated immediately following connection establishment. At this point the current channel map may be updated if the device is in the Master role, so a stale channel map will be updated within the first few connection events. |
| B-271207 | When master of encrypted Bluetooth Low Energy link, if the device asks for a re-transmission at the end of a connection event and the packet is resent at the beginning of the next connection event, the device will disconnect the link with a `MIC failure` error code. |
| B-272005 | When a device has an eSCO link and is also slave of a BR/EDR duplex bulk data transfer and sending and receiving multi-slot packets, then multi-slot bulk data retransmits sometimes get unintended priority over SCO, even if retransmits are generally working well.<br><br>This leads to loss of SCO frames. |
| B-272247 | In “radiotest” TXDATAn mode (n = 1..4), the power level may be configured either by the (1) TXDATAn command to allow precise control of the hardware registers (ATTEN, MAG and EXP) that affect output power; or it may be (2) configured by first using CFG_TX_POWER, which picks an entry from the device’s power table. See the *QCC512x Bluetooth Power Table Optimization Application Note* for further details.<br><br>In case (1) the boot-time non-linearity calibration will be re-done, for the specified value of ATTEN. This calibration will be placed into “block 0” which will be the level that the topmost (highest power) level of the power table uses, replacing the boot-time calibrated value.<br><br>If the value of ATTEN specified in (1) was different from the value that the highest power entry in the power table used, and (2) selects that level, then case (2) will use an incorrect non-linearity correction. This is likely to affect the output power, as well as more subtle aspects of the signal for EDR packets such as EVM or ACP.<br><br>Also, the ATTEN value used will be the value appropriate for BR, regardless of whether BR or EDR packets have been selected. This is unlikely to be a problem, as the ATTEN values for BR and EDR are usually the same for a given power level.<br><br>Also, if “radiotest” is used after normal operation, it is likely to produce incorrect power levels. |
| B-272599 | In the presence of modulated blockers, receiver sensitivity at mid and low powers (below -50 dBm) is less than optimal. |
| B-273509 | When the device is slave to 2 active BR/EDR masters, if it also becomes a Bluetooth Low Energy slave to one of the same 2 master devices, the length of baseband packets that can be transmitted by both BR/EDR masters to the slave is decreased from 5 slots to 1 slot.<br><br>This will result in low data rates and might manifest to the user as breaks in the audio stream on one of the BR/EDR links even when the other links are idle. |
| B-274550 | If the quality of a BR/EDR link degrades while a bidirectional ACL data transfer is in progress and the master is using multi-slot packets, ACL traffic from the slave might stall leading to various Link Manager procedure failures. |

| ID | Description |
|---|---|
| TF-18150 | If a slave device in a Bluetooth Low Energy link rejects a channel map update initiated by the master, master will carry on and apply the new channel map when the instant is reached without retrying the procedure.<br><br>Typically, a slave device is not allowed to reject a channel map update from the master as the master-initiated procedure takes precedence if there is a procedure collision. The above scenario can happen if the channel map update follows immediately after another procedure with an instant and the master and slave devices have differing interpretations of when a procedure with an instant is complete. |

### Table 9-15 Bluetooth controller resolved issues between v51 and v54

| ID | Description |
|---|---|
| B-269424 | The start of day calibration that provides the linearity correction for transmit output power can be sensitive to the presence of external RF noise. |

### Table 9-16 Bluetooth controller issues resolved between v41 and v51

| ID | Description |
|---|---|
| B-244218 | The receiver configuration, (including ADC sampling rate and the gain settings), is modified by firmware for different modes - high sensitivity mode or lower power consumption mode (see PSKEY_AGC_RSSI_THRESHOLD_BREDR and related keys). When only these settings change, without any change to RSSI measurement set up, the read RSSI can differ by about 6 dB for the same signal level at the antenna. |
| B-257197 | There can be large variations in the qualification measurement of +/-3 MHz EDR Adjacent Channel Power (ACP). These variations can be as much as 10 dB.<br><br>The boot-to-boot variation has now been reduced to 1 dB. |
| B-257676 | IP2 calibration is not functional due to missing hardware configuration. |
| B-258314 | The RSSI calculated for a link may be wrong. When the device has a single link up, the results are believed to be correct; but in more complex situations involving multiple links the RSSI for a given link may be misreported.<br><br>Since the system uses RSSI in automatic AGC switching to balance receive sensitivity and current (see PSKEY_AGC_RSSI_THRESHOLD_BREDR and related keys) the RSSI errors may adversely affect this balance. |
| B-261257 | Bluetooth Low Energy links with a connection interval that is a multiple of a SCO link 'T' value may occasionally be dropped in the presence of other periodic events. |
| B-262741 | The output transmit power may vary from part to part due to variations in the chip production process. |
| B-263106 | In very rare cases memory corruption may occur when creating a Bluetooth Low Energy connection as master. This was determined by code inspection and has not been observed in a running device. |

| ID | Description |
|---|---|
| B-263968 | If the chip is booted at a temperature below -20°C, then the boot time calibration of the radio may fail leading to poor ACP (adjacent channel power) performance and more general degraded radio transmit performance.<br><br>In a previous release, the solution given was: the problematic calibration is now done at manufacture time and the result recorded in nonvolatile memory on chip. This production line calibration is used as a fall-back if the boot temperature is too low for the boot time calibration to be trustworthy.<br><br>The temperature threshold is controlled by the new PS Key, PSKEY_AM_DELAY_TEMPERTURE_THRESHOLD, index `0x2753`. In this release, the firmware has been improved and this procedure is no longer required. For completeness, the previous solution remains available, but the control PSKEY_AM_DELAY_TEMPERATURE_THRESHOLD has been set to below the operating envelope of the device, so the previous solution is not by default invoked. |
| B-264584 | Attempting to accept an over-the-air SCO request (`LMP_SCO_LINK_REQ`) with a packet type that is for eSCO only causes the device to become unresponsive. |
| B-264896<br>(TF-18126) | When a peer device rejects a LE link layer control procedure with a `LL_REJECT_IND` PDU rather than using the extended reject PDU (`LL_REJECT_EXT_IND`) which should be supported, the control procedure times out causing the link to be terminated.<br><br>Bluetooth Low Energy devices are required to support the Extended Reject Indication feature for all link layer control procedures added to the specification after 4.2. As a result this problem can only happen with a non-spec-compliant peer device. |
| B-265044 | If a device has two Bluetooth Low Energy links up, either as master or slave, one of which is transferring data, the link that is not transferring data may fail to be scheduled and may be dropped. |
| B-265808<br>(TF-17854) | On very rare occasions HCI commands for a slave device of a Bluetooth Low Energy link can fail to complete. Once in this state, a device reset is required.<br><br>The issue occurs because the master has previously requested a Channel Map Update that has not been applied by the slave device.<br><br>This means that the issue is more prevalent in a noisy environment where the master is having to change the channel map regularly. |
| B-265165 | If a host has not initialized the random address of a Bluetooth Low Energy device and tries to enable advertising with `Own_Address_Type` parameter set to Random, the Status parameter in the resulting Command Complete event will contain Command Disallowed (`0x0c`) error code instead of Invalid HCI Command Parameters (`0x12`) error code. |
| B-265227 | Device could become unresponsive if it receives a malformed SCO or eSCO link request from a misbehaving peer device.<br><br>A reset is required when the device is in this state.<br><br>This problem was found during extensive internal testing by QTIL and has not been observed in the real world. |

| ID | Description |
|---|---|
| B-265808 | On very rare occasions HCI commands for a slave device of a Bluetooth Low Energy link can fail to complete. Once in this state, a device reset is required.<br><br>The issue occurs because the master has previously requested a Channel Map Update that has not been applied by the slave device.<br><br>This means that the issue is more prevalent in a noisy environment where the master is having to change the channel map regularly. |
| B-266315 | If a host has not initialized the random address of a Bluetooth Low Energy device and tries to enable scanning or create a link with `Own_Address_Type` parameter set to `Random`, the `Status` parameter in the resulting `Command Complete` or `Command Status` event contains `Command Disallowed` (`0x0C`) error code instead of `Invalid HCI Command Parameters` (`0x12`) error code. |
| B-266415 | One of the calibrations that is done at manufacture time, and whose result is recorded in nonvolatile memory on chip as `BT_BIST_ADC_OFFSET`, is encoded as 8-bit signed-magnitude; but the firmware interprets it as two's-complement. Therefore, negative numbers, of which perhaps 10% or less are expected, will be misinterpreted. The value of the NVM can be read post-boot from PSKEY_BT_BIST_ADC_OFFSET_GAIN, low octet (bits 0 to 7).<br><br>Typically, the true values, when negative, are small negative numbers on the order of -2; and thus when interpreted as two's complement become large negative values on the order of -126.<br><br>On parts that suffer from this, the results of internal ADC measurements will be over-corrected. This may affect some of the boot-time radio calibrations, potentially leading to poor receive sensitivity and / or moderate increases in per-part output power variation. |
| B-266493 | On rare process corners and at low temperatures, boot time radio calibrations may result in low radio output power at the highest power level, possibly resulting in the power being low enough to fail the minimum step size requirement. |
| B-266522 (TF-8704, TF-18261) | The jitter on temperature measurements reported by the firmware frequently exceeds ±5°C (the internal temperature is available from BCCMD `cached_temperature`) and may show glitches of greater than 20°C. These glitches can be large enough for the firmware to erroneously believe that the temperature has changed enough for a partial radio recalibration to be needed.<br><br>This in itself should have no harmful effects on radio performance. The recalibration is performed correctly, but a small amount of radio bandwidth may be lost while the recalibration occurs. In general, this loss is small, but can cause the firmware to close Bluetooth Low Energy connection intervals early, leading to Bluetooth Low Energy data rates significantly lower than the expected maximum. |
| B-266572 | The start of day calibration that provides the linearity correction for transmit output power output works suboptimally. This effect is most notable on VFBGA parts and particularly at cold temperatures, where it may be enough to cause the size of adjacent power steps, especially the step down from maximum, to be less than the Bluetooth specification limit of 2 dB. |
| B-266600 | When a device has multiple Bluetooth Low Energy links of which it is master, and a new (e)SCO is brought up, one or more of the Bluetooth Low Energy links may time out. |
| B-266656 | Some of the start-of-day radio calibrations are affected by the mode of the PMU/SMPS. Optimally, these calibrations should be done with the SMPS in the same mode as is used during routine radio use, although the effects of changing mode during calibration are minor. |
| B-267100 | Bluetooth Low Energy receive sensitivity may be degraded by up to approximately 3 dB on certain parts at high temperatures across a wide set of channels. |

| ID | Description |
|---|---|
| B-269370 | If the host issues `LE Set PHY`, `LE Set Default PHY`, `LE Enhanced Transmitter Test`, or `LE Enhanced Receiver Test` HCI commands with valid parameter values that are not supported by the Controller, the `Status` parameter in the resulting `Command Status or Command Complete` event will contain the `Invalid HCI Command Parameters` (`0x12`) error code, whereas it should return `Unsupported Feature or Parameter Value` (`0x11`) error code.<br>**NOTE:** If the commands are issued with PHY values that are out of range, the resulting event contains the `Invalid HCI Command Parameters` (`0x12`) error code. |

# 9.3 System and boot manager resolved issues

**Table 9-17 System and boot manager issues resolved between v36 and v39**

| BugID | Description |
|---|---|
| CUR-6553 | Power optimisation for dormant mode when entering dormant after the last deep sleep used accurate timing. |
| CUR-6564 | Charging in external mode (ie with an external transistor) could give charge currents significantly higher than requested on some parts.<br><br>This patch adjusts the trim used to improve the accuracy of the charging current when in external mode.<br><br>Updates to a previous patch (CUR-6371) in order to support new production hardware. |
| CUR-6493 | The XtalPowerModeStateSettings System Manager configuration key has been removed.<br>This key was not intended to be used. Any customers who were using it should seek assistance from Qualcomm. |
| CUR-6591<br>CUR-6506 | Updates to the System Manager configuration key documentation. |
| CUR-6568 | The value of the system manager configuration key DSULPTimeConversionFactor has been updated to represent 96ppm to better match the bulk of crystals supported. This key does not need to be further changed when recommended crystals are used. Seek advice from Qualcomm before changing this key. |

**Table 9-18 System and boot manager issues resolved between v35 and v36**

| BugID | Description |
|---|---|
| CUR-6371 | Charging in external mode (ie with an external transistor) could give charge currents significantly higher than requested on some parts.<br><br>This patch adjusts the trim used to improve the accuracy of the external charge current. |

| BugID | Description |
|---|---|
| CUR-6297 | When the PMUForcePWM MIB key is set to TRUE on exit from deep sleep the device may transition to run from the crystal oscillator too early. Also the SMPSs are transitioned from their ultra-low-power (ULP) mode to the normal high-power (PWM) mode incorrectly.<br><br>This may result in undesired issues including small glitches on the 1v8 SMPS output on exit from deep sleep.<br><br>These effects are not present with the default setting of this MIB key (FALSE). |

### Table 9-19 System and boot manager issues resolved between v33 and v35

| ID | Description |
|---|---|
| CUR-6302 | Reduce glitches seen on the 1v8 line on deep sleep and dormant entry and exit. |
| CUR-6321 | A new system manager configuration key DeepSleepVoltageReduction is provided.<br><br>This key can be used to adjust the digital voltage used in deep sleep, but must only be set on guidance from Qualcomm. |

### Table 9-20 System and boot manager issues resolved between v26 and v33

| ID | Description |
|---|---|
| CUR-5782 | MIB documentation update only to point out that the Slew Enable control which is part of the PioPadControlElements MIB configuration key has no effect on slew and should be set to 0. |
| CUR-6214 | The device has been seen to reset at very low temperatures, typically -17C or lower, where the XTAL is used in ULP mode rather than the SOSC. This is due to a sequencing error which requires correction. The device had been observed to lose time accuracy under these circumstances |
| CUR-6216 | Some VOOC/Dash USB chargers, such as the VIVO V2323A-CN, produce non-compliant USB activity (several USB resets) on insertion and will cause the device to crash. |
| CUR-6217 | The System Manager only notifies the Application that a charger detection is pending after a debouncing period has completed. With this change, the Application will be notified as soon as a charger is detected, before debouncing. |

### Table 9-21 System and boot manager issues resolved between v25 and v26

| ID | Description |
|---|---|
| B-279198 / CUR-6096 | Occasionally it is seen that the start-up of the Application causes the debugger to disconnect when using USB Debug. The ISP network is reported to fail but reappears and the debugger can usually be reconnected afterwards. |

### Table 9-22 System and boot manager issues resolved between v21 and v25

| ID | Description |
|---|---|
| CUR-4736 | The following System Manager MIB keys have been deprecated:<br>▪ PioDrive<br>▪ PioDirection<br>▪ PioMuxSetting<br>▪ PioSubsystemAllocation<br>▪ PioPullEnable<br>▪ PioPullDirection<br>▪ PioDriveStrength<br>▪ PioPullStrength<br>▪ PioStickyEnable<br>▪ PioMuxSettingElements<br>They have superseded by the following keys. See their documentation for details.<br>▪ PioDriveElements<br>▪ PioDirectionElements<br>▪ PioSubsystemAllocationElements<br>▪ PioPadControlElements |
| CUR-5900 | The chip consumes approximately an extra 500 µA while using the internal charger with a floating data lines charger to provision for a very slow insertion into an SDP.<br><br>This does not affect DCP or proprietary chargers. |
| CUR-5946 | If running Apps or Audio under Qualcomm MDE debugger and the subsystem is paused or at a breakpoint, if the subsystem has heavy processing to perform on continuing execution then the subsystem watchdog may go off. Due to the presence of the debugger this would result in all subsystems being halted for debugger inspection or core dump, regardless of MIB keys normally used for configuring panic and watchdog handling. |
| CUR-5931 | Non USB compliant hosts, that leave the D+/D- lines floating during charger detect, are incorrectly detected as a proprietary charger and so the device does not enumerate on these hosts.<br>Google Chromebook Pixel is one example of such host and since it is used during the interop part of USB compliance testing, USB certification is impacted by this. |
| CUR-5998 | Added support for GigaDevice GD25LE128D QSPI flash devices. |

### Table 9-23 System and boot manager issues resolved between v18 and release v21

| ID | Description |
|---|---|
| CUR-5817 | PUYA has updated the configuration for Quad-SPI operation.<br><br>The new datasheets for PUYA 32 Mbit and 64 Mbit flash parts indicates the QE bit of Status Register has to be set using the `Write Status Register1` command, (31H). Previously, it was done using the `Write Status Register` command, (01H). It is understood correct operation of PUYA production parts require this change.<br><br>As a result, operation of PUYA Q-SPI flash parts with ADK 6.2-build 77 cannot be guaranteed.<br><br>QTIL is working to provide an updated configuration which is expected to be available by end of June 2018 and in ADK 6.3. Contact your QTIL representative for more details. |

| ID | Description |
|---|---|
| CUR-5847 | When a subsystem crashes due to either a watchdog timeout or a PANIC while the Qualcomm MDE debugger is attached to it then that subsystem will be halted. This is intentional as it eases debugging of the problem. However other subsystems will continue running which may complicate diagnosis of why the initial subsystem crashed.<br><br>This can be worked around by setting the "HaltAllSubsystemsOnPanic" system manager configuration key to "true".<br><br>Not setting this configuration key does not change the behavior when a debugger is not attached. |
| CUR-5863 | DCP chargers are not detected if they are attached, removed and then re-attached all within 5 seconds.<br><br>Slower rates of plug-unplug-plug cycles are not affected by this bug. Nor are scenarios where the charger is unplugged and plugged in again within 5 seconds, as long as it was initially plugged in for more than 5 seconds.<br><br>Only DCP chargers are affected.<br><br>When this happens the Application will not know that there is a charger present. It can be recovered by unplugging the charger then plugging it back in again. |
| CUR-5873 | If `EFUSE_BITFIELDS_SECURITY_ENABLE` is set to `1` (which implies a customer security key has been programmed into eFuse), QCC512x/QCC302x/3x will fail to load the Boot Manager (Janitor) patch and will instead load the out of date Boot Manager image from ROM.<br><br>The Boot Manager patches are important and so it is not recommended to set `EFUSE_BITFIELDS_SECURITY_ENABLE` to `1`, that is to encrypt the SQIF image, until a patch is available for this issue.<br><br>Example of Boot Manager patches applicable include (but is not limited to), using Bluetooth with Deep Sleep. For example, sniff or Bluetooth Low Energy and, connecting/disconnecting USB. |

### Table 9-24 System and boot manager issues resolved between v16 and v18

| ID | Description |
|---|---|
| CUR-5810 | Improve the performance of the `OperatorFrameworkEnable` trap function. This reduces the Audio subsystem start-up time. |
| CUR-5815 | If the device has previously suffered a panic or subsystem watchdog reboot, and then reset using the nvscmd within the ADK to reboot the device, for example, to restart or reflash the device, then one or more of Audio, Apps, or Bluetooth subsystems may fail to start after the reboot. |

### Table 9-25 System and boot manager issues resolved between v12 and v16

| ID | Description |
|---|---|
| CUR-5463 | The device system manager can occasionally panic after a subsystem watchdog on the Apps P0 processor.<br><br>This happens only if there is a serious execution error or incorrect configuration of the Apps P0 processor. For example, if the QPSI flash suspend/resume command configuration is incorrect.<br><br>When this happens, the device can be recovered over Transaction Bridge by doing a full chip erase for the QPSI flash. |
| CUR-5589 | An occasional spurious fault `FAULT_HYDRA_TIMED_EVENT_BAD_PARMS` (`0x105a`) may be seen. |

# A Important notes

## A.1 Securing USB Debug

With this release, QCC512x and QCC302x/3x series parts have enhanced facilities to secure USB Debug post-production.

Further, additional eFuses have been added**:** `USB_DEBUG_ALLOW` and `USB_DEBUG_MASTER DISABLE`, complementing the existing MIB **USBDebugger**.

### USB_DEBUG_ALLOW

When `USB_DEBUG_ALLOW` is set allow USB Debug to be used irrespective of MIB USBDebugger. This is useful in development to prevent USB Debug from accidentally be disabled and locking the user out.

### USB_DEBUG_MASTER_DISABLE

When `USB_DEBUG_MASTER_DISABLE` is set, it prevents the use of USB Debug irrespective of anything else including the MIB and USB_DEBUG_ALLOW. This is useful if the customer feels that USBDebugger MIB is insufficient.

BlueSuite 3.2.1 supports these new eFuse bits. See the BlueSuite 3.2.1 documentation for more details.

**CAUTION:** The USBDebugger MIB key *must* be set on devices which expose USB. If USB debug is used on the production line for programming or testing, this MIB key MUST be set in the device filesystem at the end of the production line to disable USB debug. If USB debug is not used on the production line then this MIB key MUST be set in the `curator_cfg_filestem`. Failure to set this key will mean production devices can be accessed using USB debug on any USB host with the correct drivers and key installed. This may represent a serious security risk

Once USB debug is disabled via MIB, it may be desirable to temporally enable it. The MIB USBDebugger is made dynamic to the allow the application to change it and the Apps P0 provided with the ADK provides a trap call to the App P1 application to do so. See the ADK release note and documentation for details of the trap. It is the responsibility of the application to ensure this trap is only called in limited circumstances.

## A.2 MIB setting for ULP mode

If the QCC5125, QCC5131 or QCC5134 are in use or, the device is to be used at low temperatures (typically <-35°C), it may be necessary to adjust the XTAL ULP clock compensation factor for sleep timing.

QTIL testing has shown that for a number of crystals on the market, the default value is adequate to maintain the required Bluetooth 250 ppm timing accuracy.

If adjustment is required, it may be achieved using the system manager (Curator) MIB `DSULPTimeConversionFactor`. More details on MIB settings can be found in the HTML documentation:

**C:\qtil\ADK_QCC512x_QCC302x_WIN_6.4.2.*26*\doc\subsystem_config**

# **B** Notice file

This Notice txt file contains certain notices Qualcomm Technologies International, Ltd. (“QTIL”) is required to provide with certain software components. Except where prohibited by the open source license, the content of this file is only provided solely to satisfy QTIL’s attribution and notice requirement and your use of such software components together with the QTIL software (“Software”) is subject to the terms of your separate license from QTIL. Compliance with all copyright laws and software licenses included in this file are the responsibility of the user. Except as may be granted by separate express written agreement, this file provides no license to any patents, trademarks, copyrights, or other intellectual property of QTIL or its affiliates.

Software provided with this notice is NOT A CONTRIBUTION to any open source project. If alternative licensing is available for any of the components with licenses or attributions provided below, a license choice is made for receiving such code by QTIL.



```
/* This is an independent implementation of the encryption algorithm:
/*
/* SAFER+ by Cylink
/*
/* which is a candidate algorithm in the Advanced Encryption Standard
/* programme of the US National Institute of Standards and
Technology.
/*
/* Copyright in this implementation is held by Dr B R Gladman but I
/* hereby give permission for its free direct or derivative use
subject
/* to acknowledgment of its origin and compliance with any conditions
/* that the originators of the algorithm place on its exploitation.
/*
/* Dr Brian Gladman (gladman@seven77.demon.co.uk) 14th January 1999
*/
```

```
/* Copyright (c) 2007-2008 CSIRO
Copyright (c) 2007-2009 Xiph.Org Foundation
Copyright (c) 2008 Gregory Maxwell
Written by Jean-Marc Valin and Gregory Maxwell */
/*
Redistribution and use in source and binary forms, with or without
```

```
modification, are permitted provided that the following conditions
are met:
Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
Neither the name of the Xiph.org Foundation nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*/
```

# Terms and definitions

| Term | Definition |
|---|---|
| A2DP | Advanced Audio Distribution Profile |
| ACCMD | Audio Client Command |
| ACL | Asynchronous ConnectionLess |
| ACP | Adjacent Channel Power |
| ADK | Audio Development Kit |
| AE | Adaptive Equalization |
| AEC | Adaptive Echo Cancellation |
| AFH | Adaptive Frequency Hoping |
| AGC | Automatic Gain Control |
| BCCMD | BlueCore Command |
| BCSP | BlueCore Serial Protocol |
| BR | Base Rate |
| CELT | Constrained Energy Lapped Transform (codec) |
| CSB | Connectionless Slave Broadcast |
| CSBI | CSB Interval |
| cVc | Clear Voice Capture |
| DAC | Digital-to-Analog Converter |
| DBE | Dynamic Bass Enhancement |
| DFU | Device Firmware Upgrade |
| DMIC | Digital microphone |
| DRC | Dynamic Range Control |
| EDR | Enhance Data Rate |
| eSCO | Extended SCO |
| HCI | Host Controller Interface |
| HD | High Definition |
| I2S | Inter-Integrated Circuit Sound |
| ID | Identifier |
| IIR | Infinite Impulse Response (filter) |
| LE | Bluetooth Low Energy |
| NB | NarrowBand |
| NDVC | Noise Dependent Voice Control |
| NR | Noise Reduction |
| NVM | Non Volatile Memory |
| PCM | Pulse Code Modulation |
| PDU | Protocol Data Unit (packet or message) |
| PEQ | Parametric Equalization |
| PHY | Physical (layer) |
| PMU | Power Management Unit |

| Term | Definition |
|---|---|
| PSRAM | Pseudo Static Random Access Memory |
| QSPI | Quad Serial Peripheral Interface |
| QTIL | Qualcomm Technologies International, Ltd. |
| ROM | Read Only Memory |
| RSSI | Received Signal Strength Indication |
| RTP | Real Time Protocol |
| Rx | Receive or Receiver |
| S/PDIF | Sony/Philips Digital InterFace |
| SBC | Sub-band Coding |
| SCO | Synchronous Connection-Oriented |
| SIP | System In Package |
| SMPS | Switched Mode Power Supply |
| SoC | System on Chip |
| QVA | Qualcomm Voice Activation (previously Snapdragon Voice Activation, SVA) |
| TTP | Time to Play |
| Tx | Transmit or Transmitter |
| UART | Universal Asynchronous Receiver Transmitter |
| ULP | Ultra Low Power |
| USB | Universal Serial Bus |
| VFBGA | Very Fine Ball Grid Array |
| VSE | Virtual Stereo Enhancement |
| WB | WideBand |
| Wi-Fi | Wireless Fidelity (IEEE 802.11b wireless networking) |
| WLCSP | Wafer Level Chip Scale Package |
| XTAL | Crystal |