
高通CNSS技术期刊

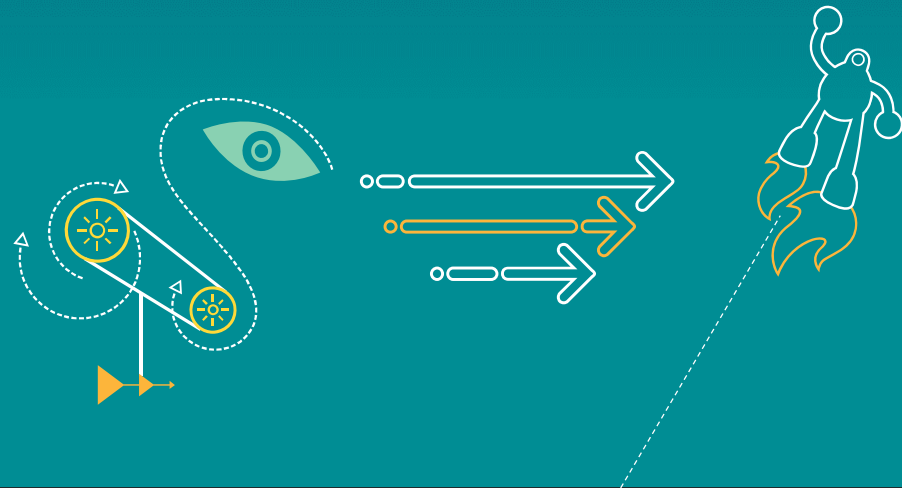
2014/12



Qualcomm Technologies, Inc.

Confidential and Proprietary – Qualcomm Technologies, Inc.

机密和专有信息——高通技术股份有限公司



Confidential and Proprietary – Qualcomm Technologies, Inc.

Confidential and Proprietary – Qualcomm Technologies, Inc.

NO PUBLIC DISCLOSURE PERMITTED: Please report postings of this document on public servers or web sites to: DocCtrlAgent@qualcomm.com. **禁止公开：**如在公共服务器或网站上发现本文档，请报告至：DocCtrlAgent@qualcomm.com.

Restricted Distribution: Not to be distributed to anyone who is not an employee of either Qualcomm or its affiliated without the express approval of Qualcomm's Configuration Management. **限制分发：**未经高通配置管理部门的明示批准，不得发布给任何非高通或高通附属及关联公司员工的人。 Not to be used, copied, reproduced, or modified in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm Technologies, Inc. 未经高通技术股份有限公司明示的书面允许，不得使用、复印、复制、或修改全部或部分文档，不得以任何形式向他人透露其内容。

The user of this documentation acknowledges and agrees that any Chinese text and/or translation herein shall be for reference purposes only and that in the event of any conflict between the English text and/or version and the Chinese text and/or version, the English text and/or version shall be controlling. 本文档的用户知悉并同意中文文本和/或翻译仅供参考之目的，如英文文本和/或版本和中文文本和/或版本之间存在冲突，以英文文本和/或版本为准。

This document contains confidential and proprietary information and must be shredded when discarded. 未经高通明示的书面允许，不得使用、复印、复制全部或部分文档，不得以任何形式向他人透露其内容。本文档含有高通机密和专有信息，丢弃时必须粉碎销毁。

Qualcomm reserves the right to make changes to the product(s) or information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. 高通保留未经通知即修改本文档中提及的产品或信息的权利。本公司对使用或应用本文档所产生的直接或间接损失概不负责。本文档中的信息为基于现状所提供，使用风险由用户自行承担。

Qualcomm is a trademark of QUALCOMM Incorporated, registered in the United States and other countries. All QUALCOMM Incorporated trademarks are used with permission. Other product and brand names may be trademarks or registered trademarks of their respective owners. Qualcomm是高通公司在美国及其它国家注册的商标。所有高通公司的商标皆获得使用许可。其它产品和品牌名称可能为其各自所有者的商标或注册商标。

This technical data may be subject to U.S. and international export, re-export, or transfer ("export") laws. Diversion contrary to U.S. and international law is strictly prohibited. 本文档及所含技术资料可能受美国和国际出口、再出口或转移出口法律的 限制。严禁违反或偏离美国和国际的相关法律。

Qualcomm Technologies, Inc. 5775 Morehouse Drive San Diego, CA 92121 U.S.A.
高通技术股份有限公司，美国加利福尼亚州圣地亚哥市莫豪斯路 5775 号，邮编 92121

内容

- 三个AP连接兼容性问题patch
- CR#757941导致WAPI连接失败问题
- 5G AP扫描显示慢问题
- 关于unstripped wlan.ko
- Android L 64位上两个字长引起的问题
- QCA61x4A WLAN 软件模块 (常用)
- QCA61x4A WLAN 工具
- 由于未签名导致WLAN驱动加载错误的解决方法
- 提交各种“Problem Area”的蓝牙问题时的检查清单
- MSM(Bluedroid)平台的QCA61x4蓝牙驱动
- MSM+QCA61x4(Bluedroid)蓝牙启动步骤
- MSM+QCA61x4(Bluedroid)蓝牙启动的代码执行顺序
- 中国电信PLTS测试常见问题
- 如何允许手机在打紧急电话时仍能正常GPS定位？
- 文档发布及更新

三个AP连接兼容性问题patch

- CR#590602, AP不支持RRM

<https://www.codeaurora.org/cgit/quic/la/platform/vendor/qcom-opensource/wlan/prima/commit/CORE/MAC/src/pe/lim/limProcessMlmRspMessages.c?h=caf-wlan/master&id=fa1d2bb1c4fbd373bb088b566173d855c002f7ff>

- CR#686472, AP不支持short preamble

<https://www.codeaurora.org/cgit/quic/la/platform/vendor/qcom-opensource/wlan/prima/commit/CORE/MAC/src/pe/lim/limProcessMlmRspMessages.c?h=caf-wlan/master&id=c949a8b3b0120783e9d7132cd5b0d0688739d4ea>

- CR#763969 , CCX roaming时AP拒绝连接fix

<https://www.codeaurora.org/cgit/external/wlan/prima/commit/?id=4f06a7911bd3d0100fe708b841735e2527f0db8e>

CR#757941导致WAPI连接失败问题

• CR#770318

```
@@ -1765,7 +1765,11 @@ tAniBool limEncTypeMatched(tpAniSirGlobal pMac, tpSchBeaconStruct pBeacon,
    if ( (pBeacon->capabilityInfo.privacy == 1) && (pBeacon->wpaPresent == 0) &&
        (pBeacon->rsnPresent == 0) &&
        ( (pSession->encryptType == eSIR_ED_WEP40) ||
-         (pSession->encryptType == eSIR_ED_WEP104)))
+         (pSession->encryptType == eSIR_ED_WEP104)
+ #ifdef FEATURE_WLAN_WAPI
+     || (pSession->encryptType == eSIR_ED_WPI)
+ #endif
+     ))
    return eSIR_TRUE;

/* WPA OR RSN*/
```

5G AP扫描显示慢问题

- 关掉下面WCNSS_qcom_cfg.ini中配置项，设置
gInitialScanSkipDFSCCh=0

关于unstripped wlan.ko

- 请大家做版本时保留vmlinux, pronto.elf 以及未strip的wlan.ko
- 编译出该文件位置
 - A-family:
out\target\product\msm8xxx\obj\vendor\qcom\proprietary\wlan\prima\CORE\HDD\src\prima_wlan.ko
 - B-family:
out\target\product\msm8xxx\obj\vendor\qcom\opensource\wlan\prima\pronto_wlan.ko
- 没strip过的wlan.ko, 文件大小应该超过30M
- 参考solution: <https://qualcomm-cdmatech-support.my.salesforce.com/501300000013LYx?srPos=0&srKp=501>

Android L 64位上两个字长引起的问题

- CR#744932, QRCT写Nv.bin失败

vendor/qcom-proprietary/ship/wlan/utils/asf/inc/aniTypes.h

```
--- typedef unsigned long tANI_U32;
```

```
--- typedef signed long tANI_S32
```

```
+++typedef unsigned int tANI_U32;
```

```
+++ typedef signed int tANI_S32
```

- CR#640894 , get_sta_mac_list命令导致hostapd 异常

softap/sdk/qsap_api.h

```
--- typedef unsigned long int u32;
```

```
---- typedef signed long int s32;
```

```
+++ typedef unsigned int u32;
```

```
+++ typedef signed int s32;
```


QCA61x4A WLAN 软件模块（常用）

| 名称 | 默认路径 | 描述 |
|--------------------|-----------------------------|------------|
| qca_cld_wlan.ko | /system/lib/modules/qca_cld | WLAN驱动 |
| WCNSS_qcom_cfg.ini | /system/etc/wifi | WLAN配置文件 |
| wlan_mac.bin | /persist | WLAN软件MAC |
| bdwlan30.bin | /firmware/image | WLAN校准文件 |
| qwlan30.bin | /firmware/image | WLAN固件 |
| utf30.bin | /firmware/image | WLAN测试模式固件 |

注释:

所有WLAN固件可以被下载到下列目录用于临时调试目的

/system/etc/firmware

例如：下列命令可以替换WLAN所用的校准文件

adb remount

adb push bdwlan30.bin /system/etc/firmware/

QCA61x4A WLAN 工具

| 名称 | 源代码 | 描述 |
|------------|--|--------------|
| ftmdaemon | vendor/qcom/proprietary/ftm | FTM命令处理程序 |
| iwpriv | 开源代码 | WEXT调试工具 |
| iw | 开源代码 | CFG80211调试工具 |
| cnss_diag | vendor/qcom/opensource/wlan/qcacld-2.0/tools/fwdebuglog/ | WLAN固件日志调试工具 |
| pktlogconf | vendor/qcom/opensource/wlan/qcacld-2.0/tools/pktlog/ | WLAN固件封包调试工具 |

Notes:

如果上述工具默认没有被编译，可以至源代码目录使用mm -B命令编译

由于未签名导致WLAN驱动加载错误的解决方法

如果使用默认的内核，未经签名的模块无法被插入到内核

```
insmod: init_module 'system/lib/modules/wlan.ko' failed (Required key not available)
```

- 为了方便调试内核模块，可以关闭内核配置项中的 `CONFIG_MODULE_SIG`

```
.config - Linux/arm64 3.10.49 Kernel Configuration
> Enable loadable module support qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
lqqqqqqqqqqqqqqqqqqqqq Enable loadable module support qqqqqqqqqqqqqqqqqqqqqk
x Arrow keys navigate the menu. <Enter> selects submenus --->. x
x Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, x
x <M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> x
x for Search. Legend: [*] built-in [ ] excluded <M> module < > x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x --- Enable loadable module support x x
x x [ ] Forced module loading x x
x x [*] Module unloading x x
x x [*] Forced module unloading x x
x x [*] Module versioning support x x
x x [ ] Source checksum for all modules x x
x x [ ] Module signature verification x x
x x x x x x
```

提交各种“Problem Area”的蓝牙问题时的检查清单
请参考如下各种“Problem Area”对应的Solution

- Bluetooth/A2DP Profile - 00029052
- Bluetooth/Controller/Firmware - 00029053
- Bluetooth/HFP/HSP Profiles - 00029055
- Bluetooth/Low Energy (LE) - 00029056
- Bluetooth/OBEX Profiles - 00029057
- Bluetooth/Other Profiles - 00029058
- Bluetooth/IOT(Interoperability) - 00029059
- Bluetooth/Qualification - 00029061

MSM(Bluedroid)平台的QCA61x4蓝牙驱动

- 代码路径
 - \hardware\qcom\bt\libbt-vendor\src
- bt_vendor_qcom.c
 - HAL file of QCOM BT user space driver
- hci_uart.c
 - UART driver
- hw_rome.c
 - QCA61x4 driver

MSM+QCA61x4(Bluetooth)蓝牙启动步骤

- 协议栈初始化
- QCA61x4上电
- 打开串口
- 读取NV
 - 从NV文件读取蓝牙地址
- 初始化QCA61x4
 - 读取ROME版本号
 - 下载RamPatch和NVM
 - 打开Controller日志
 - HCI Reset
- Start HCI filter
- Connect to local socket

MSM+QCA61x4(Bluedroid)蓝牙启动的代码执行顺序

中国电信PLTS测试常见问题

- (一) PLTS首先提示“The Mobile did not report a valid BASE_ID”，一段时间后显示“Unable to establish data call or socket connection with the mobile. The current results for this call will be discarded and a new call will be established”，最终测试失败。

失败原因和解决方法请参考solution 00029977。

- (二) 第三方测试PLTS抛出异常“time out while waiting for AirAccess C2K to return to the Paging Channel Processing state”

异常原因和解决方法请参考solution 00030029。

中国电信PLTS测试常见问题（续）

（三）第三方测试手机发送拒绝短信PLTS无法接收。

原因：PLTS不支持在专用信道上接收短信。

解决方案：设置NV 4228 = 1，在接入信道上发送拒绝短信

（四）TC-LBS-07011 GPS Sensitivity Test (MS-Based) - User Plane-SubCase1 (MSB Tracking)测试过程中无法搜到卫星或搜到不足4颗卫星数量

原因：测试过程中使用的是中国电信USIM卡，手机会根据国家给出一个参考位置，这个位置与测试case给的基于基站的参考位置存在冲突。

解决方案：NV3520 = 0，禁止使用国家码提供参考位置

如何允许手机在打紧急电话时仍能正常GPS定位？

在北美，控制层A-GPS被用来在紧急电话时提供用户位置。因此，紧急电话发起时，手机将低优先级的GPS定位中断，以对GPS引擎进行预热，准备接收来自网络的NI请求。紧急电话结束后，原有的GPS定位可以继续。

如果客户手机销售市场非北美国家，那么可以通过设置NV来禁止这个特性，这样，紧急电话不会对GPS定位产生任何影响。

```
GNSS_NV_EFS_SM_E911_CONFIG(NV 72533) = 1
NV_AAGPS_EMERGENCY_SERVICES_SPPRT_I (NV
01930) = 2
```

文档发布及更新

- 80-NR168-1 Linux LA CCX Application Notes
- 80-Y8698-5 WLAN MAC ADDRESS SPOOFING