**【问题】导入QCN后online设备，设备Crash的问题**

|  |  |
| --- | --- |
| **创建时间：** | *2017/9/7 11:22* |
| **作者：** | *习凡* |

问题的现象：

     使用QRCT工具，将xml源文件制作成QCN；之后使用QPST工具将制作好的QCN文件restore到设备。通过QXDM/QRCT工具，将device从FTM模式，切换为online模式（QXDM：mode ftm/mode online）；切换完成后，设备Crash。

LOG及问题原因的分析：

     设备Crash后，抓取dump信息；通过Qualcomm的QCAP解出f3log，log信息如下：

Coredump:

rfgsm\_core\_rx.c:2755   rfgsm\_core\_rx() rfgsm\_core\_set\_gain failed for sub 0 and PRx dev 0 rx\_lvl\_dbm

F3 Software:

======================================================================

00:03:38.830:                   rfgsm\_nv\_cmn.c:2009     arfcn index is out of range: 255

00:03:38.830:                  rfgsm\_core\_rx.c:2008     rfgsm\_core\_calc\_gain()arfcn index is out of range: 255

00:03:38.830:        qpRegistrationMonitor.cpp:1012     sendMafMessage

00:03:38.885:                  rfgsm\_core\_rx.c:2755     rfgsm\_core\_rx() rfgsm\_core\_set\_gain failed for sub 0 and PRx dev 0 rx\_lvl\_dbm

     通过f3log，可以初步的分析出是由于GSM在calculate gain range时，获取的arfcn\_index超过范围导致的。



解决的方法：

    导致device Crash的代码，在路径/mdm9640-le-3-0\_amss\_standard\_oem.git/modem\_proc/rftech\_gsm/rf/core/src/rfgsm\_core\_rx.c

    Line: 1972 ~ 1974

      /\* Get the closest channel that was calibrated \*/

      /\* @TODO possible enhancement caching of single or multiple channels circular buffer...?? \*/

      arfcn\_index =  rfgsm\_nv\_get\_closest\_arfcn\_index(rfgsm\_rx\_nv\_tbl, arfcn\_discontinuity);

    Line: 1997 ~ 2013

      /\* Avoid KW warning \*/

      if (arfcn\_index < RFCOM\_GSM\_NUM\_RX\_CAL\_CHAN)

      {

        /\* Get the switchpoints from NV \*/

        actual\_switch\_1\_2 = rx\_sw\_pt\_ptr->rx\_switch\_1\_2\_dBm[arfcn\_index];

        actual\_switch\_2\_3 = rx\_sw\_pt\_ptr->rx\_switch\_2\_3\_dBm[arfcn\_index];

        actual\_switch\_3\_4 = rx\_sw\_pt\_ptr->rx\_switch\_3\_4\_dBm[arfcn\_index];

        actual\_switch\_4\_5 = rx\_sw\_pt\_ptr->rx\_switch\_4\_5\_dBm[arfcn\_index];

      }

      else

      {

        MSG\_1(MSG\_SSID\_RF, MSG\_LEGACY\_ERROR, "rfgsm\_core\_calc\_gain()arfcn index is out of range: %d", arfcn\_index);

        if ( ftm\_gsm\_rx\_device\_is\_ftm\_state( rfm\_dev ) == FALSE )

        {

          return FALSE;

        }

  }

**修改点，/mdm9640-le-3-0\_amss\_standard\_oem.git/modem\_proc/rftech\_gsm/rf/core/src/rfgsm\_nv\_cmn.c文件下的函数：**

    uint8 **rfgsm\_nv\_get\_closest\_arfcn\_index**( rfgsm\_nv\_band\_rx\_data\_type \*rfgsm\_rx\_nv\_tbl, uint16 arfcn);

    Line: 2005 ~ 2012

        arfcn\_index = arfcn\_index - 1;

        if (arfcn\_index > rfgsm\_rx\_nv\_tbl->rx\_cal\_nv\_data.rx\_cal\_chan\_size)

        {

          MSG\_1(MSG\_SSID\_RF, MSG\_LEGACY\_ERROR, " arfcn index is out of range: %d",arfcn\_index);

          arfcn\_index = rfgsm\_rx\_nv\_tbl->rx\_cal\_nv\_data.rx\_cal\_chan\_size - 1;

          +++return 0;

    }