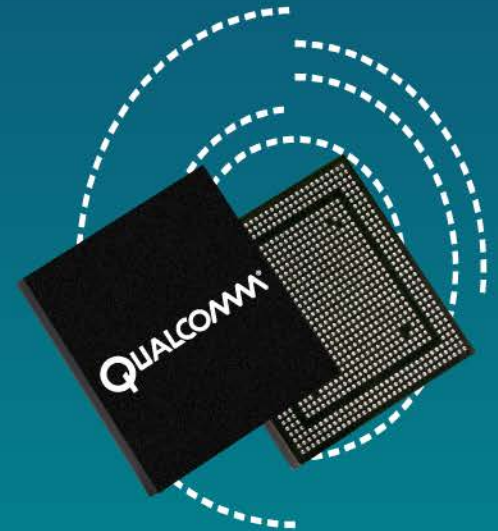


QUALCOMM®
zhangnan@hipad.com

LTE Cell Selection, Registration, and TAU Overview

80-N9811-1 C



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 websites to: DocCtrlAgent@qualcomm.com.

Restricted Distribution: Not to be distributed to anyone who is not an employee of either Qualcomm or its subsidiaries without the express approval of Qualcomm's Configuration Management.

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.

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.

This document contains confidential and proprietary information and must be shredded when discarded.

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.

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.

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

© 2012, 2014 Qualcomm Technologies, Inc.
All rights reserved.

Revision History

Revision	Date	Description
A	Feb 2012	Initial release
B	May 2012	Revised slides 7, 10, 21, 49; added slides 11 to 17 and 45 to 48
C	May 2014	Revised slides 8 and 24

Contents

- LTE Cell Selection
- Registration
- Tracking Area Update
- References
- Questions?

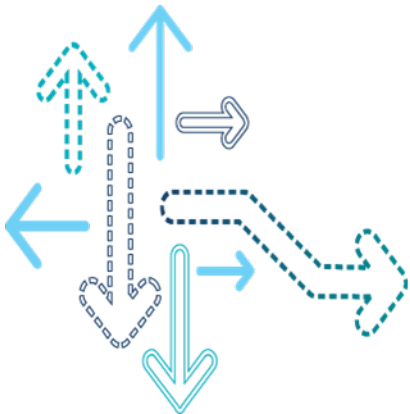
QUALCOMM®
zhangnan@hipad.com

Objectives

- At the end of this presentation, you will:
 - Be familiar with the LTE cell selection, registration, TAU procedure
 - Understand message exchange between various layers of the LTE Protocol stack

QUALCOMM
zhangnan@hipad.com

LTE Cell Selection



What Happens at UE Powerup

- The acquisition process begins when the UE powers up and NAS sends a Service Request indication to RRC by including the Requested PLMN values.
- RRC then executes a Cell Search Procedure to acquire and camp on a cell.
- Based on the scan results, RRC returns an RRC_SERVICE_IND to NAS. This can indicate full service (normal operation), limited service (emergency calls only), or no service.
- If camping was successful, RRC moves to IDLE_CAMPED.
- NAS then initiates the Attach procedure, which prompts RRC to request MAC to start the RACH procedure.

Cell Selection Procedure

- Search for PLMNs requested by NAS
- Scan all RF channels in the E-UTRA bands to find PLMNs (UE may optimize this search by using stored information in acquisition database)
- Search for the strongest cell and read the system information to determine the PLMN
- Confirm that cell access restrictions do not prohibit camping on the cell
- Confirm that cell selection criteria are fulfilled on the cell

Cell Selection Procedure Introduction

- Using the cell selection procedure, the UE shall select a suitable cell based on Idle mode measurements and cell selection criteria.
- There are two types of cell selection:
 - Initial cell selection
 - UE scans all RF channels in the E-UTRA bands according to its capabilities
 - Stored cell selection
 - UE scans all RF channels as stored in its acquisition database

Reasons for Cell Selection

- When is cell selection triggered
- Cell selection is triggered in the following scenarios:
 - Service Request from NAS
 - State Transition (connected to Idle)
 - Inter-frequency Redirection
 - Out of Service Indication from ML1 (Idle mode)
 - Radio Link Failure (Connected mode)
 - Inter-RAT Reselection/Redirection to LTE (from WCDMA, GSM, 1X)

Terminology

- PLMN – Public Land Mobile Network
- RPLMN – Last Registered PLMN
- HPLMN – Home PLMN
- EHPLMN – Equivalent HPLMN
- VPLMN – Visitor PLMN
- PPLMN – Preferred PLMN
- OPLMN – Operator Preferred PLMN
- UPLMN – User Preferred PLMN
- FPLMN – Forbidden PLMN

EF, NV, and EFS Items

- EFs used by the UE are:
 - EFIMSI – IMSI
 - EFPLMNwAcT – User-controlled PLMN selector with Access Technology
 - EFHPPLMN – Higher-priority PLMN search period
 - EFFPLMN – Forbidden PLMNs
 - EFLOCI – Location information
 - EFOPLMNwACT – Operator-controlled PLMN selector with Access Technology
 - EFHPLMNwAcT – Home HPLMN selector with Access Technology
 - EFEHPLMN – Equivalent HPLMN
 - EFLRPLMNSI – Last RPLMN selection indication
 - EFPSLOCI – Packet-switched location information
 - EFEPSLOCI – EPS location information

Note: For further details, see [Q2].

EF, NV, and EFS Items (cont.)

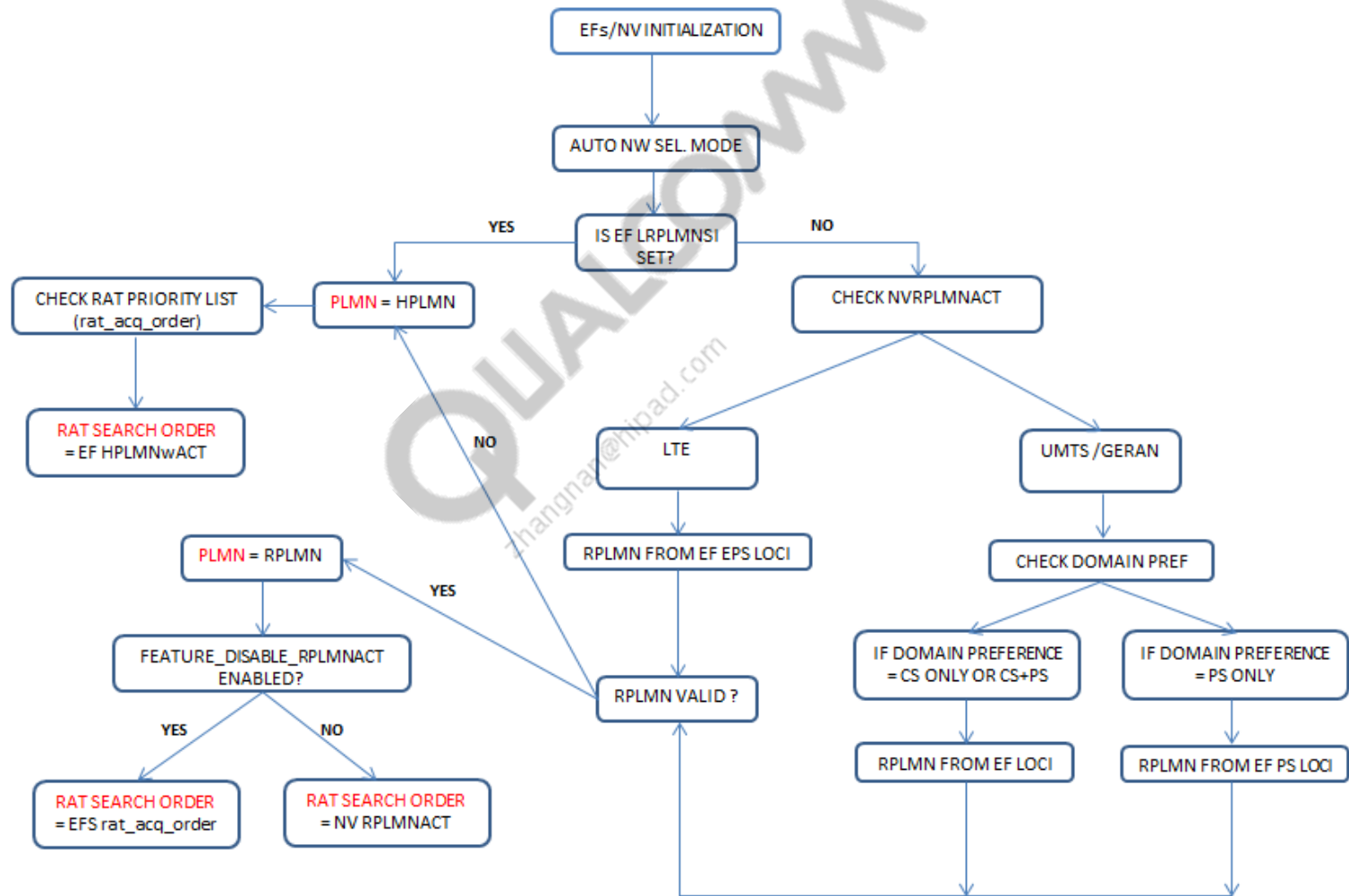
- NVs used by the UE are:
 - NV 1190 NV_RPLMNACT_I – Stores the last RPLMN RAT information
 - NV 850 NV_SERVICE_DOMAIN_PREF_I – Determines the service preference for the device
 - NV 849 NV_NET_SEL_MODE_PREF_I – Determines the network mode of operation for the device
- EFS items
 - RAT Priority List (/sd/rat_acq_order) – Determines the RAT priority list for PLMN selection

Note: For further details, see [Q2].

NW Selection Modes

- NV_NET_SEL_MODE_PREF_I is used to configure the network selection mode for the UE as either Automatic or Manual. Based on this configuration, NAS runs different PLMN selection algorithms to acquire service on a network.
 - Automatic
 - Manual
 - Limited

PLMN/RAT Selection Flow



Log Analysis – PLMN/RAT Selection

\\ EF_RPLMNSI is not set

18:58:22.390	reg_sim.c	5976	H	LRPLMNSI is - 0
18:58:22.799	reg_nv.c	821	H	Read RPLMNACT 64 0
18:58:24.064	cmregprx.c	1751	H	Send SERVICE_REQ

\\ Mode set to automatic

18:58:24.064	cmregprx.c	1767	H	net_sel_mode 2
18:58:24.064	cmregprx.c	1770	H	srv_domain 2
18:58:24.068	reg_state.c	3843	H	CM_SERVICE_REQ

\\ RAT priority list has only LTE

18:58:24.070	reg_state.c	874	H	Rat priority list num_items = 1
18:58:24.070	reg_state.c	880	H	sys_mode = 9
				bst_rat_acq_required = 1
				bst_band_cap = 0x1000

\\ Reading the RPLMN from NV

18:58:44.536	reg_nv.c	462	H	Read RPLMNACT 64 0 from cache
--------------	----------	-----	---	-------------------------------

Log Analysis – PLMN/RAT Selection (cont.)

\\ HPLMN information

18:58:44.536	reg_sim.c	2269	H	HPLMN(001- 01)
--------------	-----------	------	---	----------------

\\ Automatic service request sent

18:58:44.634	reg_state.c	1193	H	CM_SERVICE_REQ – AUTOMATIC
--------------	-------------	------	---	-------------------------------

\\ Last RPLMN RAT is LTE

18:58:44.634	reg_sim.c	3149	H	LAST RPLMN RAT LTE
18:58:44.635	reg_sim.c	2758	H	EPS RPLMN(1-1)

\\ EMM Received the REG request

18:58:44.635	reg_send.c	1121	H	MMR_REG_REQ PLMN(1-1) RAT(LTE)
18:58:44.636	emm_reg_handler.c	619	H	EMM: Received MMR_REG_REQ

\\ RRC layer obtained the service request from NAS

18:58:44.636	lte_rrc_csp.c	5603	H	CSP: Processing service request
18:58:44.638	emm_rrc_if.c	370	H	EMM: Sent LTE_RRC_SERVICE_REQ

Frequency Scan

- Using Frequency Scan, the UE selects the frequency/EARFCN for camping.
 - There are two types of frequency scan:
 - System scan, also known as List Frequency scan (similar to Acq DB scan)
 - Upper layers shall provide list of EARFCNs, requested bandwidth, and Duplex mode to L1
 - Band scan, also known as Full Frequency scan
 - Upper layers shall provide band index and the allowed set of bandwidths to L1

Log Analysis – System Scan

//Automatic service Request

11458 76:00:16:20.595reg_state.c1171HCM_SERVICE_REQ –AUTOMATIC
11491 89:00:16:20.600emm_reg_handler.c475HEMM: Received MMR_REG_REQ

//NAS sends service request to AS

11494 81:00:16:20.600emm_rrc_if.c310HEMM: Sent LTE_RRC_SERVICE_REQ

//RRC sends LTE_CPHY_START_REQ to ML1

11537 81:00:16:20.603lte_ml1_mgr_stm.c6923MLTE_CPHY_START_REQ

//LTE AS is initialized

11675 97:00:16:20.620lte_ml1_mgr_cphy_cnf_handlers.c976MLTE_CPHY_START_CNF
Status: 0
11680 89:00:16:20.620lte_ml1_mgr_stm.c12645LL1M: INACTIVE STATE ENTER

//ML1 initiates System Scan request

11704 153:00:16:20.620lte_ml1_sm_main.c1118HSM: Sys Scan Req module 1 num_sys 1
min_sys 0 early_abort 0 sys[0] band 13 earfcn 5230 bw 50

//RF tune request

11705 113:00:16:20.620lte_ml1_sm_main.c641HSM: RX cfg req freq 5230 BW 50 cell_id
65535

Log Analysis – Band Scan

//Acquisition database search (System Scan) is exhausted. No system found

11497 89:00:47:21.166lte_rrc_csp.c3603HCSP: All entries tried in acq list

11498 81:00:47:21.166lte_rrc_csp.c9373HCSP: Exhausted acquisition list

//Initiate Band Scan

11506 89:00:47:21.166lte_rrc_csp.c2191XCSP: Sending 1 bands in band scan

11507 81:00:47:21.166lte_rrc_csp.c2210XCSP: Sent Band Scan Request

11520 105:00:47:21.175rtr8600_lte.c866HRF LTE RX is tuned to band 13 and frequency 5230

Initial Acquisition

- The acquisition process on a carrier frequency consists of three parts:
 - PSS detection
 - 5 ms frame timing
 - Acquire physical layer identity (3 candidates)
 - SSS detection
 - 10 ms frame timing synchronization (SSS1 in subframe 0 and SSS2 in subframe 5)
 - Cell ID Group detection (168 candidates)
 - PBCH detection
 - MIB acquisition
 - Transmitted 4 OFDM symbols in subframe0
 - TTI is 40 ms
 - SFN, PHICH information, system bandwidth
- With acquiring PSS/SSS/MIB, UE can obtain Reference Signal (RS) position, which is based on Cell ID, and read to all scheduled SIBs in DL-SCH

Log Analysis – Cell Selection

//Service Request from NAS

00:00:15.734 modem/lte/RRC/src/lte_rrc_csp.c 03975 CSP: Processing service request
00:01:19.598 modem/lte/ML1/manager/src/lte_ml1_mgr_stm.c 05999
LTE_CPHY_START_REQ
00:01:19.599 modem/lte/ML1/manager/src/lte_ml1_mgr_stm.c 04450
LTE_CPHY_START_CNFFStatus: 0

//ACQ DB is empty

00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 02646 CSP: Zero entries in acquisition list

//Band scan

00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 05001 CSP: Starting Band Scan on Mode Change Cnf
00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 01478 CSP: Sent Band Scan Request
00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 05011 CSP: Processing next band
00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 05907 CSP: Band scan returned 1 candidate

//Band Scan results

00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 05914 CSP: Preparing acq list from band scan
00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 00873 CSP: Initing acq list
00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 05967 CSP: Acq list has 1 entry
00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 01254 CSP: Roaming restriction is allow none

Log Analysis – Cell Selection (cont.)

//ACQ Request to Layer1

00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 01521 CSP: Acq requested on earfcn 5230

00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 01539 CSP: Sent Acquisition Request

00:01:19.599 modem/lte/RRC/src/lte_rrc_csp.c 05973 CSP: Started Acquisition

00:01:19.599 modem/lte/ML1/manager/src/lte_ml1_mgr_stm.c 05669
LTE_CPHY_ACQ_REQTrans id 2

//PSS/SSS detection

00:01:19.599 modem/lte/ML1/search/src/lte_ml1_sm_deact.c 00195 LTE ML1
SEARCHER received LTE_ML1_SM_STM_ACQ_STAGE1_REQ in
LTE_ML1_SM_DEACT_STATE

00:01:19.599 modem/lte/ML1/search/src/lte_ml1_sm_acq.c 02124 Received Acq Req
from L1M in Deact Mode

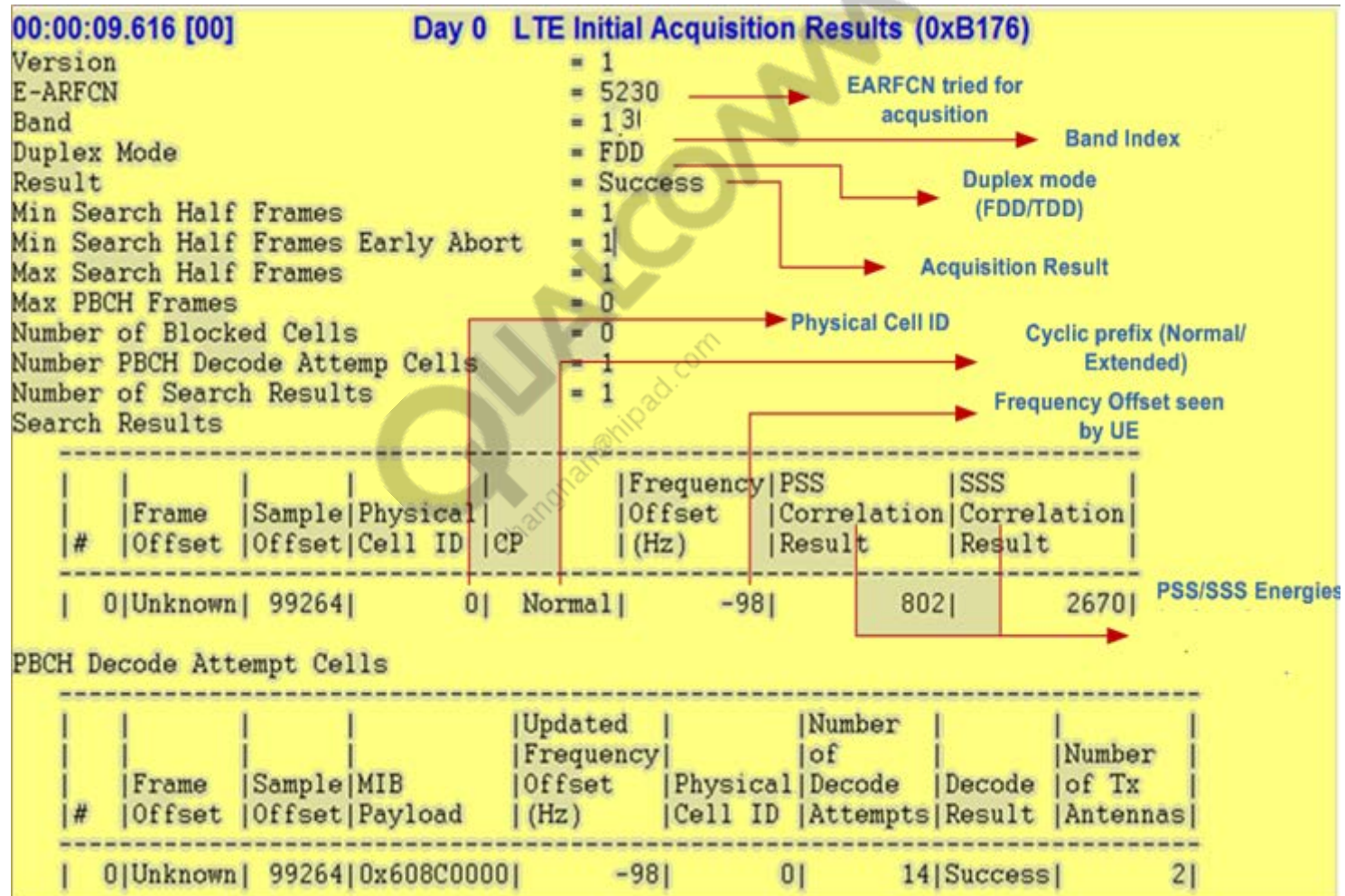
00:01:19.600 modem/lte/ML1/search/src/lte_ml1_sm_acq.c 00348 LTE ML1 SEARCHER
Acquisition Algo init done

00:01:19.612modem/lte/ML1/search/src/lte_ml1_sm_acq.c 00995 LTE ML1 SEARCHER
received LTE_ML1_SM_STM_SEARCH_RSP in LTE_ML1_SM_ACQ_DETECT_STATE
state

//Found a cell

00:01:19.612modem/lte/ML1/search/src/lte_ml1_sm_acq.c 01022 SM: Init Acq Cnf; num
cells: 1

Acquisition Log Packet



Log Analysis – Cell Selection

//PBCH decode request

00:01:19.611modem/lte/ML1/search/src/lte_ml1_sm_sd_if.c 00542 SM:

pBCH_DEC_REQ:

00:01:19.611modem/lte/ML1/search/src/lte_ml1_sm_sd_if.c 00553 SM: Sent Initial PBCH Decode Req;

//UE camped on cell

18:13:56.603 [58]lte_rrc_csp.c5510XCSP: Acq succeeded on physical cell ID 1 on earfcn 5230

//Command to start reading SIBs on the serving cell

18:13:56.603 [58]lte_rrc_sib.c4045HReceived get_sibs_reqwith phy_cell_id = 1, freq = 5230, cause = 0, proc_id = 0

18:13:56.603 [58]lte_rrc_sib.c541HSent cphy_sib_sched_req for phy_cell_id = 1 freq = 5230

//Received MIB

18:13:56.603 [58]lte_rrc_sib.c4844MMIB received for phy_cell_id = 1 & freq = 5230 at SFN 80

//SIB schedule request to acquire SIBs

18:13:56.603 [58]lte_rrc_sib.c541HSent cphy_sib_sched_req for phy_cell_id = 1 freq = 5230

Log Analysis – Cell Selection (cont.)

//Acquisition complete

00:01:19.698modem/lte/ML1/manager/src/lte_ml1_mgr_stm.c 05913
LTE_CPHY_ACQ_CNFStatus: 0 Trans id: 2

00:01:19.698modem/lte/ML1/manager/src/lte_ml1_mgr_stm.c 05916
LTE_CPHY_ACQ_CNF cell ID: 1, cp: 0

//Issue SIB decode request

00:01:19.699modem/lte/RRC/src/lte_rrc_sib.c 00555 Sent cphy_sib_sched_req for
phy_cell_id = 1 freq = 5230; curr_mask = 0x3 next_mask = 0x0 mod_bnd = 65535

00:01:19.699modem/lte/ML1/manager/src/lte_ml1_mgr_stm.c 07022
L1M:LTE_CPHY_SIB_SCHED_REQ

//SIB decoding

00:01:19.707modem/lte/RRC/src/lte_rrc_sib.c 04952 MAC_DL_DATA (SIB1 or SI
message) received for phy_cell_id = 1 & freq = 5230 at SFN 80

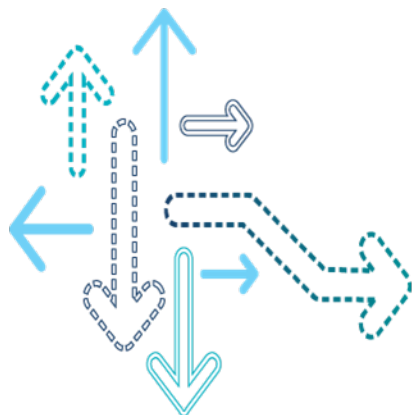
//Mandatory SIBs received. RRC issues cell select request

00:01:19.906modem/lte/ML1/manager/src/lte_ml1_mgr_stm.c 07239 L1M:
LTE_CPHY_CELL_SELECT_REQ

//Service indication to NAS

00:01:19.920 modem/lte/RRC/src/lte_rrc_csp.c 01773 CSP: Sent NAS Service Ind

Registration



RACH Outline

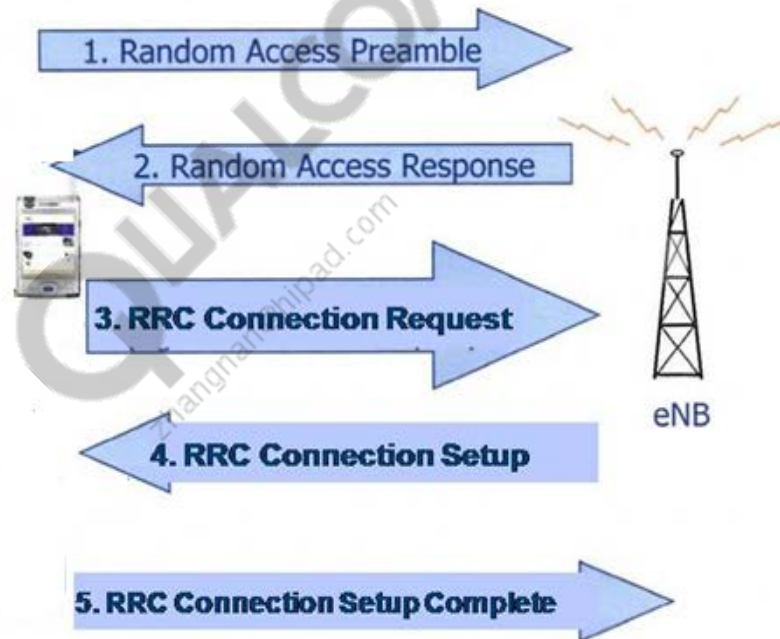
- Why/when to RACH
 - Initial access to the network
 - UL data
 - DL data when out of sync
 - No dedicated resources
 - Handover
 - Radio link failure

QUALCOMM
zhangnan@hipad.com

Contention vs Non Contention-Based RACH Comparison

- Contention-based RA
 - Initiated by UE
 - Initiated by transmitting a random preamble
 - Uses common preambles
- Non contention-based RA
 - Initiated by eNB
 - Initiated with transmission of an RA preamble assignment
 - Uses dedicated preambles

Random Access Procedure (Contention-Based)



Random Access Procedure (Contention-Based) (cont.)

- Message 1 – Random access preamble on PRACH
- Message 2 – Random access response on DL-SCH
- Message 3 – Sent on UL-SCH - Contain the RRC message
- Message 4 – Contention resolution performed

Preamble – msg1 (ML1 MSG1 Report)

Filtered View:[16]

Type	Name	Timestamp	Summary
LOG	LTE ML1 Random Access Request (MSG1) Report	00:02:27.938	Length: 0020
LOG	LTE ML1 Random Access Response (MSG2) Report	00:02:27.953	Length: 0012
LOG	LTE ML1 UE Identification Message (MSG3) Report	00:02:27.953	Length: 0012
LOG	LTE ML1 Contention Resolution Message (MSG4) Report	00:02:27.969	Length: 0008

Results

1969 Dec 31 16:00:00.000 [FF] 0xB167 LTE Random Access Request (MSG1) Report

Version = 1

Preamble Sequence = 0

Physical Root Index = 670

Cyclic shift = 0

PRACH Tx Power = 38 dBm

Beta PRACH = -49 dBm

PRACH Frequency Offset = 22

Preamble Format = 0

PRACH Timing SFN = 993

PRACH Timing Sub-fn = 8

PRACH Window Start SFN = 994

PRACH Window Start Sub-fn = 1

PRACH Window End SFN = 995

PRACH Window End Sub-fn = 1

RA RNTI = 9

Subframe number

RA-RNTI=Sub FN+1

RAR – msg2 (ML1 MSG2 Report)

Filtered View:[16]			
Type	Name	Timestamp	Summary
LOG	LTE ML1 Random Access Request (MSG1) Report	00:02:27.938	Length: 0020
LOG	LTE ML1 Random Access Response (MSG2) Report	00:02:27.953	Length: 0012
LOG	LTE ML1 UE Identification Message (MSG3) Report	00:02:27.953	Length: 0012
LOG	LTE ML1 Contention Resolution Message (MSG4) Report	00:02:27.969	Length: 0008

Results	
1969 Dec 31 16:00:00.000 [FF] 0xB168 LTE Random Access Response (MSG2) Report	
Version	= 1
SFN	= 994
Sub-fn	= 6
Timing Advance	= 1
Timing Advance Included	= Included
RACH Procedure Type	= Contention Based
RACH Procedure Mode	= Initial Access
RNTI Type	= TEMP_C_RNTI
RNTI Value	= 10

RRC Connection Request – msg3 (QXDM Log)

The screenshot shows the QXDM Item View window. The top pane lists log items, and the bottom pane shows the decoded results of the selected item.

Type	Name	Timestamp	Summary
MSG	LTE RRC/CEP	00:01:21.533	modem/lte/RRC/src/lte_r
LOG	LTE RRC OTA Message	00:01:21.533	OTA message Log Packet
MSG	LTE MACCTRL/High	00:01:21.533	modem/lte/L2/mac/src/lte
MSG	LTE RRC/CEP	00:01:21.533	modem/lte/RRC/src/lte_r
MSG	LTE RRC/CTRL	00:01:21.533	modem/lte/RRC/src/lte_r
MSG	LTE MACUL/Rach	00:01:21.533	modem/lte/L2/mac/src/lte
MSG	LTE MACUL/Rach	00:01:21.533	modem/lte/L2/mac/src/lte

Results

```
OTA msg Log Packet
RB ID: 0
Phy cell id: 0
Freq: 2100
SFN: 0
Sub Frame Number: 0
PDU num: 6
Encoded msg length: 6
Decoded msg:
value UL-CCCH-Message ::=
{
  message c1 : rrcConnectionRequest :
  {
    criticalExtensions rrcConnectionRequest-r8 :
    {
      ue-Identity randomValue : '00101100 11010100 10110110 00000101 011 ...'B,
      establishmentCause mo-Signalling,
      spare '0'B
    }
  }
}
```

RRC Connection Setup – msg4

Type	Name	Timestamp	Summary
LOG	LTE RRC OTA Message	00:01:21.763	OTA message Log Packet
MSG	LTE ML1/High	00:01:21.763	modem/lte/ML1/dlm/src/

Results

```
Phy cell id: 0
Freq: 2100
SFN: 346
Sub Frame Number: 1
PDU num: 4
Encoded msg length: 22
Decoded msg:
value DL-CCCH-Message ::=
{
  message c1 : rrcConnectionSetup :
  {
    rrc-TransactionIdentifier 0,
    criticalExtensions c1 : rrcConnectionSetup-r8 :
    {
      radioResourceConfigDedicated
      {
        srb-ToAddModList
        {
          {
            srb-Identity 1,
            rlc-Config explicitValue : am :
            {
              ul-AM-RLC
              {
                t-PollRetransmit ms45,
                pollPDU pInfinity,
                pollByte kBinfinity,
                maxRetxThreshold t4
              },
              dl-AM-RLC
              {
                t-Reordering ms35,
                t-StatusProhibit ms0
              }
            },
            logicalChannelConfig explicitValue :
            {
              ul-SpecificParameters
              {
                priority 1,
                prioritisedBitRate infinity,
                bucketSizeDuration ms50,
                logicalChannelGroup 0
              }
            }
          }
        }
      },
      mac-MainConfig explicitValue :
```

RRCConnection setup is TM

SRB 1 LCID = Default =1

RRC Connection Setup Complete QXDM Log

Item View

Type	Name	Timestamp	Summary
LOG	LTE RRC OTA Message	00:01:21.770	OTA message Log Packet
MSG	LTE ML1/Low	00:01:21.770	modem/lte/ML1/schdlr/s

Results

OTA msg Log Packet

RB ID: 1

Phy cell id: 0

Freq: 2100

SFN: 0

Sub Frame Number: 0

PDU num: 7

Encoded msg length: 48

Decoded msg:

value UL-DCCH-Message ::=

```
{  
  message c1 : rrcConnectionSetupComplete :  
  {  
    rrc-TransactionIdentifier 0,  
    criticalExtensions c1 : rrcConnectionSetupComplete-r8 :  
    {  
      selectedPLMN-Identity 1,  
      dedicatedInfoNAS '0741710809101010325476980480800000 ...'H  
    }  
  }  
}
```

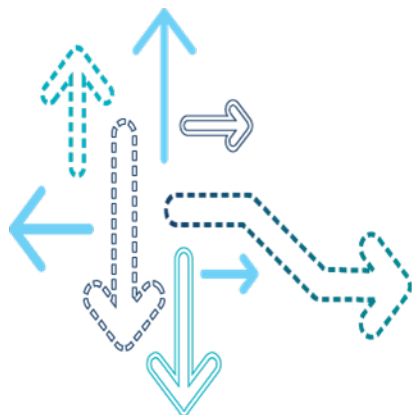
Bits

8	7	6	5	4	3	2	1	
0	1	0	0	0	0	0	1	41 Attach request
0	1	0	0	0	0	1	0	42 Attach accept
0	1	0	0	0	0	1	1	43 Attach complete
0	1	0	0	0	1	0	0	44 Attach reject
0	1	0	0	0	1	0	1	45 Detach request
0	1	0	0	0	1	1	0	46 Detach accept
0	1	0	0	1	0	0	0	48 Tracking area update request
0	1	0	0	1	0	0	1	49 Tracking area update accept
0	1	0	0	1	0	1	0	4A Tracking area update complete
0	1	0	0	1	0	1	1	4B Tracking area update reject

24.301 Table 9.8.1

Attach Request is piggy backed

Tracking Area Update



Tracking Area Update

- Purpose

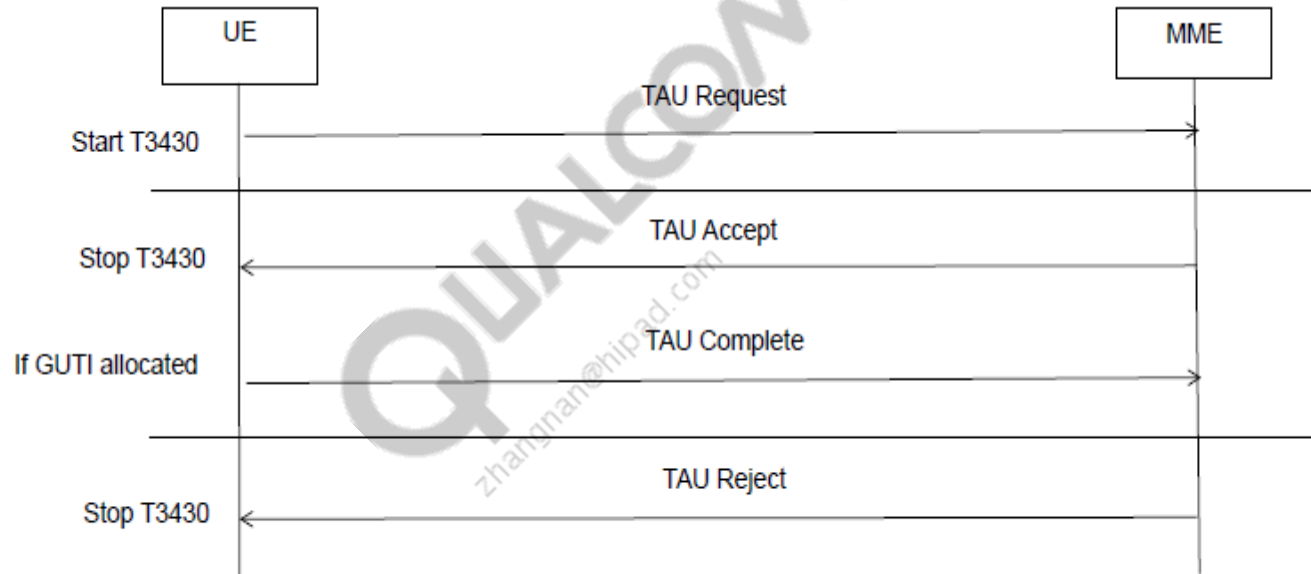
- Used by the UE for a variety of reasons, primarily to update the network with the tracking area the UE is currently in
- Trigger
 - Update registration of actual TA of a UE (Normal TAU)
 - Update registration of actual TA for a UE in CS/PS mode (Combined TAU)
 - Periodic TAU to notify UE availability to the network
 - At inter-system change from UMTS/GSM/CDMA to LTE
 - Update UE-specific parameters/capabilities in the network
 - At recovery from errors
 - Indicate that UE entered S1 (LTE) mode after CSFB
- Types of TAU
 - Normal
 - Combined
 - Periodic

Tracking Area Update (cont.)

- UE actions on receiving TAU Accept
 - Update – GUTI, TAI list, Update Status, EPLMN list
 - Send TAU Complete, if needed
- UE actions when TAU Reject is received
 - Behavior shall depend on reject cause received
 - If combined update is successful for EPS services only, MM LOCI shall be updated and appropriate state will be entered for follow-up actions
 - If UE is configured to support UMTS/GSM, MM and GMM parameters shall be updated as if this reject cause is received on UMTS/GSM

Tracking Area Update (cont.)

- Call flows



Tracking Area Update (cont.)

2011 Dec 29 18:58:24.395 [00] 0xB0C0 LTE RRC OTA Packet -- BCCH_DL_SCH

Radio Bearer ID = 0, Physical Cell ID = 1

Freq = 5230

SysFrameNum = 212, SubFrameNum = 5

PDU Number = BCCH_DL_SCH Message, Msg Length = 17

message c1 : systemInformationBlockType1 :

```
{
  cellAccessRelatedInfo
  plmn-Identity
    {
      mcc
      {
        0,
        0,
        1
      },
      mnc
      {
        0,
        1
      }
    },
  cellReservedForOperatorUse notReserved
}
},
trackingAreaCode '00000000 00000001'B,
```

Tracking Area Update (cont.)

// Upon cell selection, EMM receives a service indication from RRC –TAI of the current cell not part of existing TAI List

emm_esm_handler.c295HEMM: Sent ATTACH_COMPLETE

emm_esm_handler.c297HEMM: Set state 3 (REGISTERED)

emm_esm_handler.c297HEMM: Set substate 0 (NORMAL SERVICE)

emm_rrc_handler.c931HEMM: Received new RRC Service Indication

emm_rrc_handler.c582HEMM: TAI is not part of the existing TAI list. Start TAU

// RRC connection established successfully and UE gets the TAU ACCEPT from network

emm_update_lib.c2714HEMM: T3430 has been started

emm_connection_handler.c370HEMM: Start RRC connection establishment

emm_rrc_if.c491HEMM: Sent LTE_RRC_CONN_EST_REQ

emm_update_lib.c2737HEMM: Set state 4 (EMM_TRACKING_AREA_UPDATING_INITIATED)

emm_connection_handler.c819HEMM: Received LTE_RRC_CONN_EST_CNF

emm_connection_handler.c592HEMM – RRC connection has been established successfully

emm_update_lib.c2912HEMM – Received TAU Accept message

Tracking Area Update (cont.)

//EMM sends service indication to REG and responds with a TAU complete to the network

emm_update_lib.c2914HEMM: T3430 has been stopped

emm_sim_handler.c524HEMM: Set EPS update status to 0

emm_reg_handler.c1039HEMM sent MMR_SERVICE_IND

emm_update_lib.c3077HEMM: Send TAU COMPLETE message to NW

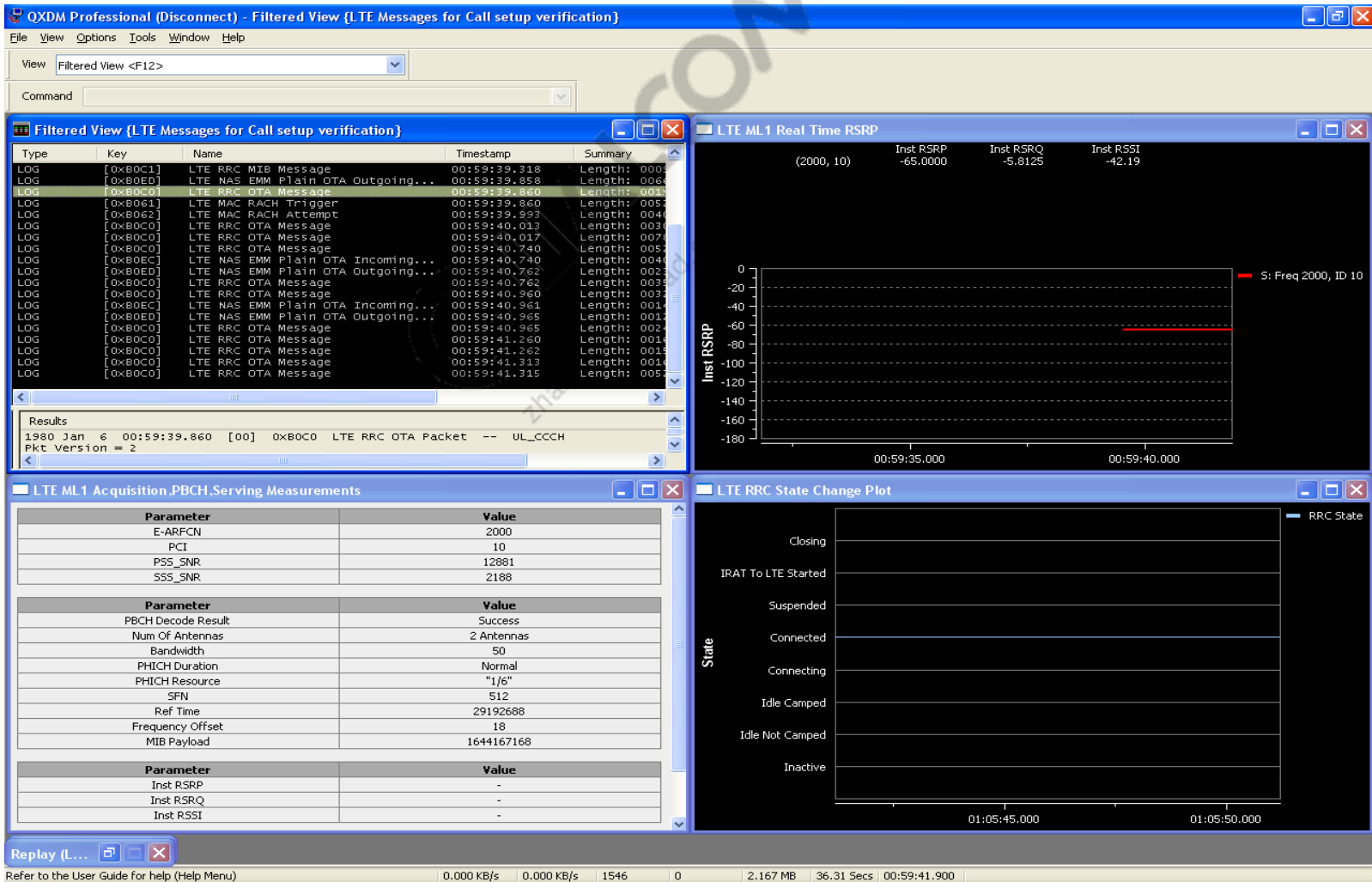
emm_rrc_if.c544HEMM: Sent LTE_RRC_UL_DATA_REQ

Keywords for Log Analysis

- Use the following key words for analysis
 - LTE_CPHY_, acq req, acq cnf, cell id, pbch_dec, MIB cell, service ind, barred, CSP, Phy_cell_Id, Plain OTA, RRC OTA, TAU COMPLETE, acq succ, EMM:,mmr_service_ind, TAU accept

LTE Cell Selection, Registration, and TAU – QXDM Dashboard

- QXDM window showing the filtered view, ML1 acquisition, PBCH serving measurements, ML1 Real time RSRP, RRC state change plot



LTE Cell Selection, Registration, and TAU – Configuring the Filtered View-OTA Messages

- This window shows which RRC\NAS OTA messages that must be enabled to see the messages in filtered view

The screenshot displays the QXDM Professional (Disconnect) - Filtered View [LTE Messages for Call setup verification] window. The main pane shows a list of filtered messages with columns for Type, Key, Name, Timestamp, and Summary. A dialog box titled "Item List Config" is open, showing the configuration for filtering messages. The "Filter/Register On Target For Items" checkbox is checked. The "Item Types" list on the left includes "Log Packets (OTA)" which is checked. The "RRC Layer" section on the right lists various RRC messages, with "LTE RRC MIB Message" and "LTE RRC OTT Message" circled in red. The "NAS Layer" section lists various NAS messages, with "LTE NAS ESM Plain OTA Incoming Message" and "LTE NAS ESM Plain OTA Outgoing Message" circled in red. The bottom of the window shows a graph of "Inst RSRP" over time, with a legend indicating different frequencies and IDs.

QXDM Professional (Disconnect) - Filtered View [LTE Messages for Call setup verification]

View: Filtered View <F12>

Command:

Filtered View [LTE Messages for Call setup verification]

Type	Key	Name	Timestamp	Summary
LOG	[0xB0C0]	LTE RRC OTA Message	13:59:10.100	Length: 008
LOG	[0xB0C0]	LTE RRC OTA Message	13:59:10.278	Length: 005
LOG	[0xB0EC]	LTE NAS EMM Plain OTA Incoming...	13:59:10.980	Length: 004
LOG	[0xB0E0]	LTE NAS EMM Plain OTA Outgoing...	13:59:11.010	Length: 002
LOG	[0xB0C0]	LTE RRC OTA Message	13:59:11.011	Length: 003
LOG	[0xB0C0]	LTE RRC OTA Message	13:59:11.212	Length: 003
LOG	[0xB0C0]	LTE NAS EMM Plain OTA Inc...		
LOG	[0xB0C0]	LTE NAS EMM Plain OTA Out...		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0E2]	LTE NAS ESM Plain OTA Inc...		
LOG	[0xB0E2]	LTE NAS ESM Plain OTA Out...		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0EC]	LTE NAS EMM Plain OTA Inc...		
LOG	[0xB0E2]	LTE NAS ESM Plain OTA Inc...		
LOG	[0xB0E0]	LTE NAS EMM Plain OTA Out...		
LOG	[0xB0C0]	LTE RRC OTA Message		
LOG	[0xB0C0]	LTE RRC OTA Message		

Item List Config

Item Types

- ☐ DIAG Malformed Packets
- ☐ DIAG Requests
- ☐ DIAG Responses
- ☐ Event Reports
- ☐ GPS Reports
- ☒ Log Packets
- ☐ Log Packets (OTA)
- ☐ Message Packets
- ☐ Strings
- ☐ Subsystem Dispatch Requests
- ☐ Subsystem Dispatch Responses

Filter/Register On Target For Items

RRC Layer

- ☒ [0xB0C0] LTE RRC OTA Message
- ☒ [0xB0C1] LTE RRC MIB Message
- ☒ [0xB0C2] LTE RRC OTT Message
- ☐ [0xB0C3] Internal - LTE PLMN Search Request
- ☐ [0xB0C4] Internal - LTE PLMN Search Response
- ☐ [0xB0C5] Internal - LTE RRC Partial PLMN Search
- ☐ [0xB0C6] LTE RRC eMBMS Bearer List Info

NAS Layer

- ☐ [0xB0E0] LTE NAS ESM Security Protected OTA
- ☐ [0xB0E1] LTE NAS ESM Security Protected OTA
- ☒ [0xB0E2] LTE NAS ESM Plain OTA Incoming Message
- ☒ [0xB0E3] LTE NAS ESM Plain OTA Outgoing Message
- ☐ [0xB0E4] LTE NAS ESM Bearer Context State
- ☐ [0xB0E5] LTE NAS ESM Bearer Context Info
- ☐ [0xB0E6] LTE NAS ESM Procedure State
- ☐ [0xB0E7] LTE NAS ESM Security Protected OTA
- ☐ [0xB0E8] LTE NAS ESM Security Protected OTA
- ☒ [0xB0EC] LTE NAS EMM Plain OTA Incoming Message
- ☒ [0xB0ED] LTE NAS EMM Plain OTA Outgoing Message

Delayed Subsystem Responses Only ☐ Accept Unknowns ☒

SD Logging: [v]

OK Cancel

LTE ML1 Real Time RSRP

	Inst RSRP	Inst RSRQ
(2000, 10)	-68.4375	-4.1875
(2000, 314)	-155.3750	-30.0000
(2000, 433)	-155.3750	-30.0000
(2000, 193)	-155.3750	-30.0000
(2000, 22)	-155.3750	-30.0000
(2000, 79)	-155.3750	-30.0000

Connecting

Idle Camped

Idle Not Camped

Inactive

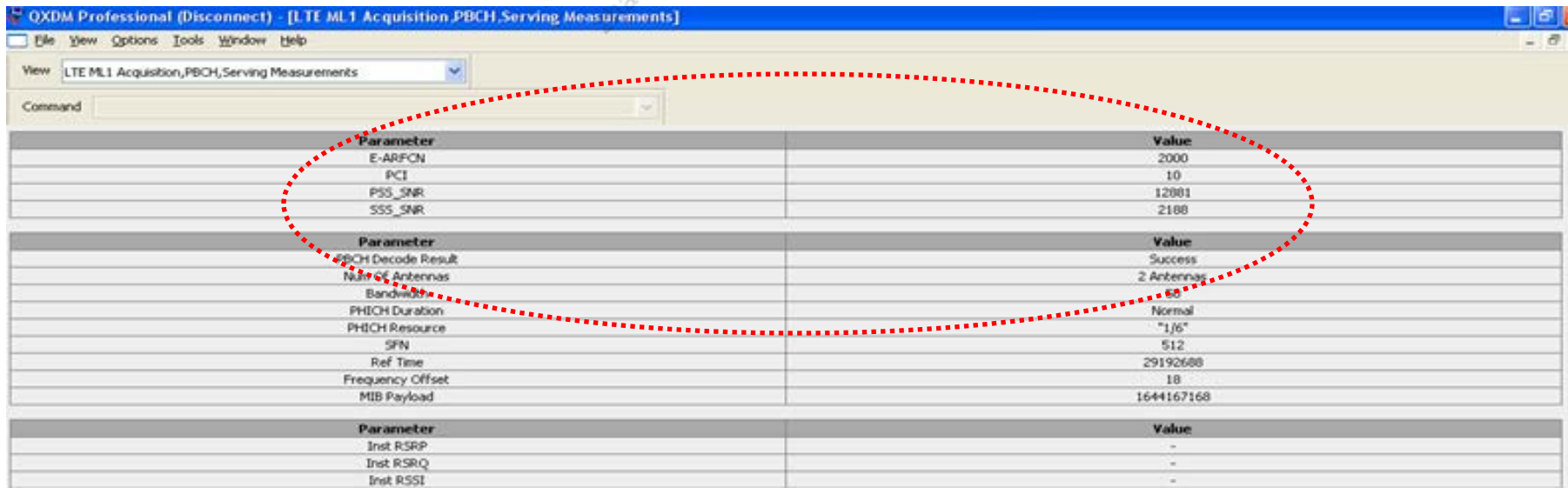
OS Cor...

Refer to the User Guide for help (Help Menu)

0.000 KB/s 0.000 KB/s 110511 0 18.132 MB 1.56 Hrs 13:59:15.553

LTE Cell Selection, Registration, and TAU – LTE ML1 Acquisition, PBCH, Serving Measurements

- This window shows:
 - EARFCN number of the cell
 - Phy_Cell_ID (PCI) of the cell
 - Bandwidth – Bandwidth of the system
 - PBCH decode result of cell whether is it successful or failure
 - PSS_SNR – $10 \log_{10}$ (Primary Synchronization Signal (PSS) Correlation result /128)
 - SSS_SNR – $10 \log_{10}$ (Secondary Synchronization Signal (SSS) correlation result /256). SSS SNR < 0 is considered as weak cell.



OXDM Professional (Disconnect) - [LTE ML1 Acquisition, PBCH, Serving Measurements]

View: LTE ML1 Acquisition, PBCH, Serving Measurements

Command:

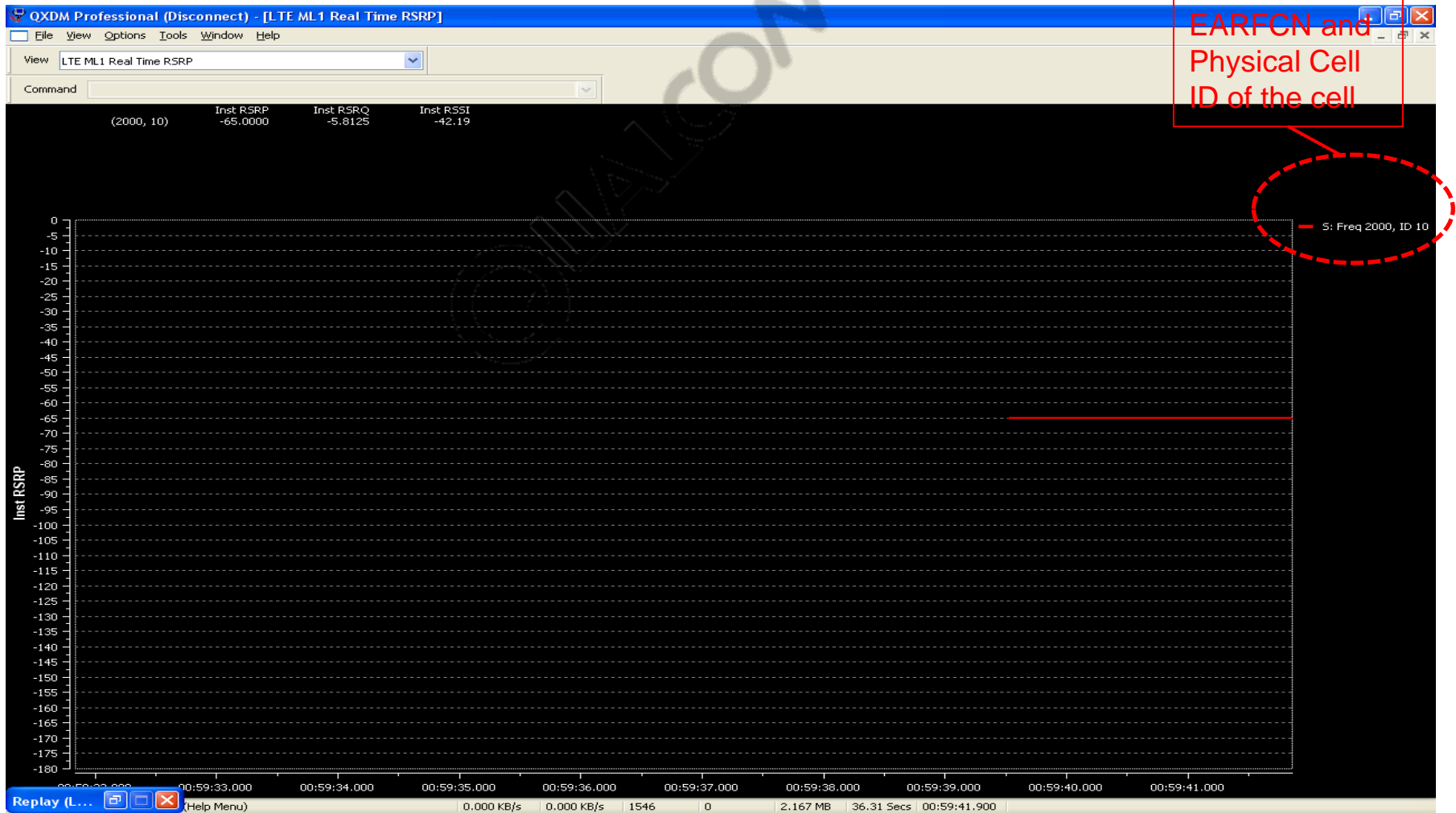
Parameter	Value
E-ARFCN	2000
PCI	10
PSS_SNR	12001
SSS_SNR	2188

Parameter	Value
PBCH Decode Result	Success
Number of Antennas	2 Antennas
Bandwidth	5 MHz
PBCH Duration	Normal
PBCH Resource	"1/6"
SFN	512
Ref Time	29192688
Frequency Offset	18
MIB Payload	1644167168

Parameter	Value
Inst RSRP	-
Inst RSRQ	-
Inst RSSI	-

LTE Cell Selection, Registration, and TAU – ML1 Real Time RSRP

- This window shows the real-time Reference Signal Received Power (RSRP) of the cell



References

Ref.	Document	
Qualcomm Technologies		
Q1	Application Note: Software Glossary for Customers	CL93-V3077-1
Q2	Application Note: PLMN/RAT Selection – GSM/WCDMA/LTE Targets	80-N9533-2



Questions?

<https://support.cdmatech.com>

