BG96 Network Searching Scheme Introduction

LTE Module Series

Rev. BG96_Network_Searching_Schemem_Introduction_V1.2

Date: 2018-04-16

Status: Preliminary

Our aim is to provide customers with timely and comprehensive service. For any assistance, please contact our company headquarters:

Quectel Wireless Solutions Co., Ltd.
7th Floor, Hongye Building, No.1801 Hongmei Road, Xuhui District, Shanghai 200233, China
Tel: +86 21 5108 6236
Email: info@quectel.com

Or our local office. For more information, please visit:
http://quectel.com/support/sales.htm

For technical support, or to report documentation errors, please visit:
http://quectel.com/support/technical.htm
Or email to: support@quectel.com

GENERAL NOTES

QUECTEL OFFERS THE INFORMATION AS A SERVICE TO ITS CUSTOMERS. THE INFORMATION PROVIDED IS BASED UPON CUSTOMERS' REQUIREMENTS. QUECTEL MAKES EVERY EFFORT TO ENSURE THE QUALITY OF THE INFORMATION IT MAKES AVAILABLE. QUECTEL DOES NOT MAKE ANY WARRANTY AS TO THE INFORMATION CONTAINED HEREIN, AND DOES NOT ACCEPT ANY LIABILITY FOR ANY INJURY, LOSS OR DAMAGE OF ANY KIND INCURRED BY USE OF OR RELIANCE UPON THE INFORMATION. ALL INFORMATION SUPPLIED HEREIN IS SUBJECT TO CHANGE WITHOUT PRIOR NOTICE.

COPYRIGHT

About the Document

History

Revision	Date	Author	Description
1.0	2017-10-18	Walker HAN	Initial
1.1	2018-01-10	Hyman DING	Updated the description of Chapter 1.1
1.2	2018-04-15	Elvis SUN Hyman DING	Add More details about the network searching scheme and it should be read in its entirety

Contents

1 Introduction

This document introduces the supported RATs (Radio Access Technologies) and frequency bands of BG96 module, and also describes its network searching scheme through illustrating related AT commands and network searching/registration procedure. In addition, the document also describes some problems observed in the process of searching the network, and gives corresponding solutions.

2 Supported RAT(s) and Band(s)

Quectel BG96 module supports three RATs: LTE Cat M1, LTE Cat NB1 and EGPRS. The default RATs are LTE Cat M1 and EGPRS. And the searching sequence is: LTE Cat M1 → EGPRS. If the three RATs need to be supported synchronously or other RAT combinations are needed, then please configure through AT commands. The details of the AT commands are provided in ***Chapter 5***.

The following table lists the supported frequency bands of BG96.

Table 1: Frequency Bands of BG96 Module

RAT	Frequency Band
LTE Cat M1	LTE-FDD: B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B26/B28 LTE-TDD: B39
LTE Cat NB1	LTE-FDD: B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B26/B28
EGPRS	GSM850, EGSM900, DCS1800, PCS1900

3 Network Searching/Registration Procedure

The network searching/registration procedure of BG96 is illustrated below:

1. **UE initialization**

   Including (U)SIM card recognition and reading of NV related to network searching.

2. **PLMN/RAT selection**

   Set the network searching sequence and the network mode to be searched according to network searching related NV and related SIM EF files. And the PLMN selection include automatic and manual modes.

3. **ARFCN scan**

   LTE EARFCN/UARFCN scan includes mode scan and band scan steps.
   EGPRS ARFCN scan mainly refers to power scan.

4. **Acquisition**

   Refer to cell recognition and downlink synchronization.

5. **System information analyze**

   Refer to system information reading.

6. **Cell selection**

   If the acquired band satisfies the signal strength requirement of UE, then go to the next step (cell camp) directly. Otherwise continue band scan.

7. **Cell camping**

   Cell camping is started after successful cell selection.

8. **Attach request/location update request**

   After cell camped, the UE will send the attach request/location update request.

9. **Random access**

UE performs uplink synchronization (random access) after sending attach request/location update request.

10. RRC connection request

11. Network sends attach accept/location update accept

4 Process Affect Registration Speed

4.1. PLMN/RAT Selection Procedure

This chapter describes the steps involved in PLMN/RAT selection for BG96 targets. Figure 1-1 outlines the overall process of PLMN/RAT selection for Automatic mode of network operation. From the below figure, the PLMN/RAT selection process was determined not only by module but also by some files in the SIM card. However, in Qualcomm's platform, The SIM card has a higher priority.

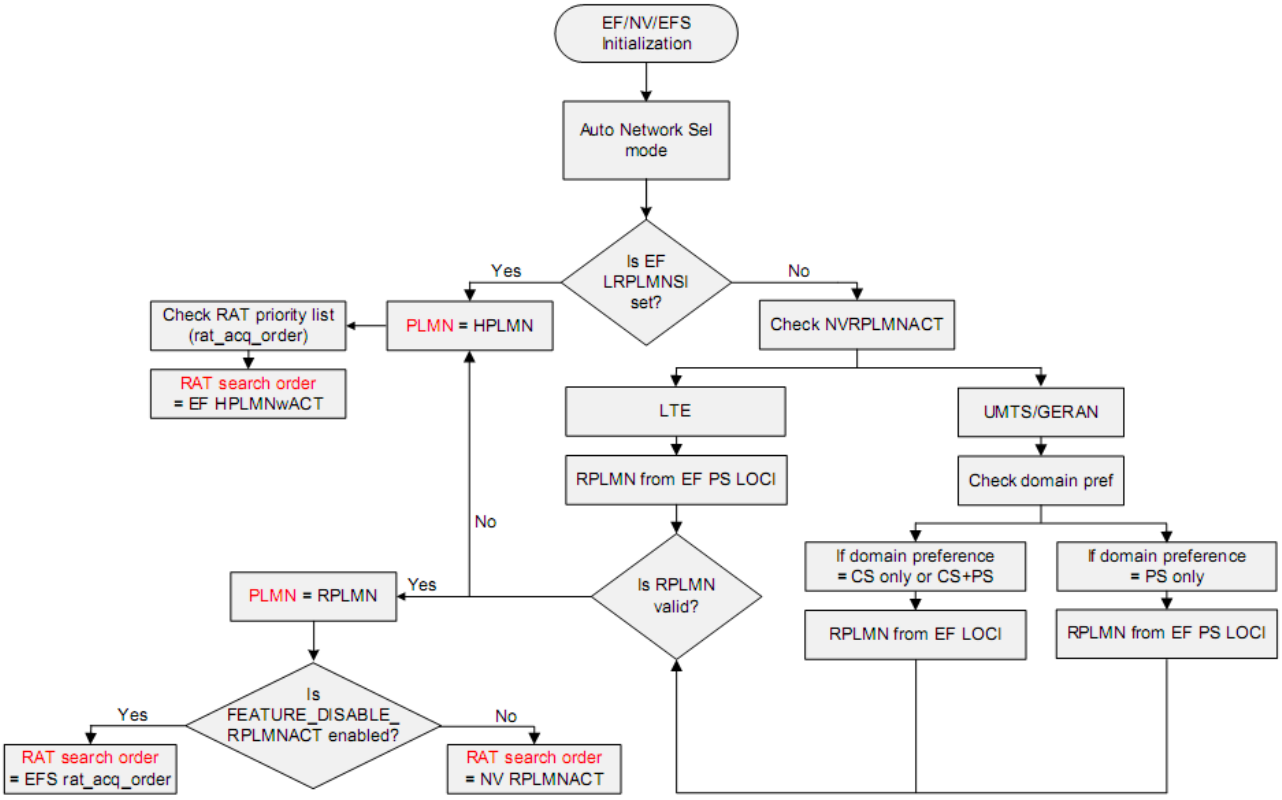


Figure 1-1 PLMN/RAT selection procedure

4.2. ARFCN Scan(Frequency Scan)

This chapter describes the effect of the ARFCN scan process on the speed of network registration. LTE EARFCN/UARFCN scan includes mode scan and band scan steps. When the module shuts down normally, it will store this time network registration information (e.g. EARFCN, PCI and so on). The next time module power on for network registration, UE will try to acquire the current network information using the stored network information. This process we called it **system scan**. This will speed up the network registration process. If the network information acquisition failed in system scan, UE will attempt all

frequency it supports. This process we called it band scan.
According to our statistics, all frequency scans under the RAT of EGPRS and LTE Cat M1 take about tens of seconds. But under LTE Cat NB1, due to the characteristics of NB1 network (especially the feature for weak signals). It will take a long time for frequency scan. **Table 2** shows our one test process, which displays the frequency scan time required in each band.

Table 2: Network Searching time under Cat.NB1 with different SNR in each band

Band	Band Width	Searching time with SNR 0	Searching time with SNR 1	Searching time with SNR 2
B1	60M	25	139	313
B2	60M	26	132	310
B3	75M	32	164	386
B4	45M	20	104	229
B5	25M	11	69	132
B8	35M	15	77	185
B12	17M	7	38	90
B13	10M	4	21	49
B18	15M	7	36	78
B19	15M	6	39	77
B20	40M	13	67	157
B25	65M	15	86	183
B28	45M	20	104	238

For BG96 support 13 bands under LTE Cat NB1. We recommend that customers only enable the bands which their service operator used.

Table 3: 15 LTE bands required to address global market with multi-mode Cat.M1 and Cat.NB1 solution (for reference)

Band	DL freq. (MHz)	Applicability as per 3GPP TS36.1.0.1	U.S	China	Middle East	Japan	Korea	Europe	Australia
B1	2100	Cat.M1, NB1		■		■			
B2	1900	Cat.M1, NB1	■						
B3	1800	Cat.M1, NB1		■	■		■	■	■
B4	1700	Cat.M1	■						
B5	850	Cat.M1, NB1		■			■		
B8	900	Cat.M1, NB1		■	■	■		■	
B12/B17	700	Cat.M1, NB1	■						
B13	700	Cat.M1, NB1	■						
B18	800	Cat.M1, NB1				■			
B19	800	Cat.M1, NB1				■			
B20	800	Cat.M1, NB1						■	
B26	850	Cat.M1, NB1		■					
B28	700	Cat.M1, NB1			■				■
B39	1900	Cat.M1		■					

5 Network Searching Related AT Commands

In order to optimize network searching/registration time, related AT commands can be used to set the network searching sequence, network mode to be searched, network category to be searched under LTE network mode, and preferred frequency bands to be searched.

5.1. AT+QCFG="nwscanseq" Network Searching Sequence Configuration

The command specifies the sequence of searching network. If **<effect>** is omitted, the configuration will take effect immediately.

AT+QCFG="nwscanseq" Network Searching Sequence Configuration	
Write Command **AT+QCFG="nwscanseq"[,<scanseq>[,<effect>]]**	Response If **<scanseq>** and **<effect>** are both omitted, return the current configuration: **+QCFG: "nwscanseq",<scanseq>** **OK** If **<scanseq>** and **<effect>** are not omitted, configure the network searching sequence: **OK** **ERROR** If there is an error related to ME functionality: **+CME ERROR: <err>**
Maximum Response Time	300ms

NOTE

This command not supported on **BG96-M** product.

Parameter

<scanseq>	Number format. Network search sequence. (e.g.: 020301 stands for LTE Cat M1 → LTE Cat NB1 → GSM) 00 Automatic (LTE Cat M1 → LTE Cat NB1 → GSM) 01 GSM 02 LTE Cat M1 03 LTE Cat NB1
<effect>	Number format. When to take effect. 0 Take effect after UE reboots 1 Take effect immediately

5.2. AT+QCFG="nwscanmode" Network Search Mode Configuration

The command specifies the network mode to be searched. If **<effect>** is omitted, the configuration will take effect immediately.

AT+QCFG="nwscanmode" Network Search Mode Configuration	
Write Command **AT+QCFG="nwscanmode"[,<scanmode>[,<effect>]]**	Response If **<scanmode>** and **<effect>** are both omitted, return the current configuration: **+QCFG: "nwscanmode",<scanmode>** **OK** If **<scanmode>** and **<effect>** are not omitted, configure the network mode to be searched: **OK** **ERROR** If there is an error related to ME functionality: **+CME ERROR: <err>**
Maximum Response Time	300ms

Parameter

<scanmode>	Number format. Network mode to be searched. 0 Automatic 1 GSM only

	3 LTE only
<effect>	Number format. When to take effect. 0 Take effect after UE reboots 1 Take effect immediately

NOTE

This command not supported on **BG96-M** product.

5.3. AT+QCFG="iotopmode" LTE Network Search Mode Configuration

The command specifies the network category to be searched under LTE network mode. If **<effect>** is omitted, the configuration will take effect immediately.

AT+QCFG="iotopmode" LTE Network Search Mode Configuration	
Write Command **AT+QCFG="iotopmode"[,<mode>[,<effect>]]**	Response If **<mode>** and **<effect>** are both omitted, return the current configuration: **+QCFG: "iotopmode",<mode>** **OK** If **<mode>** and **<effect>** are not omitted, configure the network category to be searched under LTE network mode: **OK** **ERROR** If there is an error related to ME functionality: **+CME ERROR: <err>**
Maximum Response Time	300ms

Parameter

<mode>	Number format. Network category to be searched under LTE network mode. 0 LTE Cat M1 1 LTE Cat NB1 2 LTE Cat M1 and LTE Cat NB1
<effect>	Number format. When to take effect. 0 Take effect after UE reboots 1 Take effect immediately

NOTE

This command not supported on **BG96-M** product.

5.4. AT+QCFG="band" Band Configuration

The command specifies the preferred frequency bands to be searched of UE. If **<effect>** is omitted, the configuration will take effect immediately.

AT+QCFG="band" Band Configuration	
Write Command **AT+QCFG="band"[,<gsmbandval>,<catm1bandval>,<catnb1bandval>[,<effect>]]**	Response If all configuration parameters and **<effect>** are omitted (that is, only execute **AT+QCFG="band"**), return current configuration: **+QCFG: "band",<gsmbandval>,<catm1bandval>,<catnb1bandval>** **OK** If configuration parameters are all entered, configure the preferred frequency bands to be searched: **OK** **ERROR** If there is an error related to ME functionality : **+CME ERROR: <err>**
Maximum Response Time	300ms

Parameter

<gsmbandval>	A hexadecimal value that specifies the GSM frequency band. If it is set to 0, it means not to change GSM frequency band. (eg.: a=2(GSM1800)+ 8(GSM1900)) 00000000 No change 00000001 GSM 900MHz 00000002 GSM 1800MHz 00000004 GSM 850MHz 00000008 GSM 1900MHz 0000000F Any frequency band
<catm1bandval>	A hexadecimal value that specifies the LTE Cat M1 frequency band. If it is set to 0

	or 0x40000000, it means not to change the frequency band. (eg.: 0x15=0x1(LTE B1)+0x4(LTE B3)+0x10(LTE B5))
	0x1 (CM_BAND_PREF_LTE_EUTRAN_BAND1) LTE B1
	0x2 (CM_BAND_PREF_LTE_EUTRAN_BAND2) LTE B2
	0x4 (CM_BAND_PREF_LTE_EUTRAN_BAND3) LTE B3
	0x8 (CM_BAND_PREF_LTE_EUTRAN_BAND4) LTE B4
	0x10 (CM_BAND_PREF_LTE_EUTRAN_BAND5) LTE B5
	0x80 (CM_BAND_PREF_LTE_EUTRAN_BAND8) LTE B8
	0x800(CM_BAND_PREF_LTE_EUTRAN_BAND12) LTE B12
	0x1000 (CM_BAND_PREF_LTE_EUTRAN_BAND13) LTE B13
	0x20000 (CM_BAND_PREF_LTE_EUTRAN_BAND18) LTE B18
	0x40000(CM_BAND_PREF_LTE_EUTRAN_BAND19) LTE B19
	0x80000 (CM_BAND_PREF_LTE_EUTRAN_BAND20) LTE B20
	0x2000000 (CM_BAND_PREF_LTE_EUTRAN_BAND26) LTE B26
	0x8000000(CM_BAND_PREF_LTE_EUTRAN_BAND28) LTE B28
	0x4000000000(CM_BAND_PREF_LTE_EUTRAN_BAND39) LTE B39
	0x400A0E189F (CM_BAND_PREF_ANY) Any frequency band
<catnb1bandval>	A hexadecimal value that specifies the LTE Cat NB1 frequency band. If it is set to 0 or 0x40000000, it means not to change the frequency band.
	0x1 (CM_BAND_PREF_LTE_EUTRAN_BAND1) LTE B1
	0x2 (CM_BAND_PREF_LTE_EUTRAN_BAND2) LTE B2
	0x4 (CM_BAND_PREF_LTE_EUTRAN_BAND3) LTE B3
	0x8 (CM_BAND_PREF_LTE_EUTRAN_BAND4) LTE B4
	0x10 (CM_BAND_PREF_LTE_EUTRAN_BAND5) LTE B5
	0x80 (CM_BAND_PREF_LTE_EUTRAN_BAND8) LTE B8
	0x800(CM_BAND_PREF_LTE_EUTRAN_BAND12) LTE B12
	0x1000 (CM_BAND_PREF_LTE_EUTRAN_BAND13) LTE B13
	0x20000 (CM_BAND_PREF_LTE_EUTRAN_BAND18) LTE B18
	0x40000(CM_BAND_PREF_LTE_EUTRAN_BAND19) LTE B19
	0x80000 (CM_BAND_PREF_LTE_EUTRAN_BAND20) LTE B20
	0x2000000 (CM_BAND_PREF_LTE_EUTRAN_BAND26) LTE B26
	0x8000000(CM_BAND_PREF_LTE_EUTRAN_BAND28) LTE B28
	0xA0E189F (CM_BAND_PREF_ANY) Any frequency band
<effect>	Number format. When to take effect.
	0 Take effect after UE reboots
	1 Take effect immediately

6 Solutions for Speed up Network Searching

As per 3GPP spec, Cat.NB1 is expected to be deployed in much lower coverage area. Expected Minimum Coupling Loss for NB is 164dB whereas for Cat.M1 it is only around 155dB. This pushes device to accommodate more SNR range to detect a possible NB cell deployment. And Cat.M1 has a bandwidth of 1.4 MHz, whereas Cat.NB1 has a 200 KHz bandwidth. This means NB has much more candidates to scan and detect in a given LTE deployed area. Which lead to Cat.NB1 searching time is a lot longer than Cat.M1.

Qualcomm MDM9206 platform divided the search process into three stages for Cat.NB1 signal characteristics:

- Frequency **scan level 0(SNR 0)** – Used for good SNR levels; detects strong cells first and takes the shortest time to acquire cells.
- Frequency **scan level 1(SNR 1)** – Used for medium SNR levels.
- Frequency **scan level 2(SNR 2)** – Used for poor SNR levels.

As the test result of the **table 2**, we can see that for SNR 0, module will only take tens of seconds to searching the network, for SNR 1, it takes five to six times the time of the SNR 0 and for SNR 2 it takes ten to fifteen times of the SNR 0. That will spend long time for searching the Cat.NB1 network. And due to our BG96 is a global project which support more than 13 FDD bands, the total time of the searching is huge.

In order to avoid the long searching period, it is recommended that the customers use the following solution to optimize the searching strategy of the BG96 module.

Solution A: Disable the NB1 RAT supported and only enable the required RAT(s).

- Enable GPRS only:
  AT+QCFG="nwscanmode",1
- Enable Cat.M1 only:
  AT+QCFG="iotopmode",0
  AT+QCFG="nwscanmode",3
- Enable GPRS and Cat.M1 both:
  AT+QCFG="iotopmode",0
  AT+QCFG="nwscanmode",0

Solution B: Need support Cat.NB1. It is recommended only enable the band supported which their currently service operator provided.

- For **U.S** region, enable the 3 RATs at the same time and set the band supported for B2, B4, B12 and

B13:
AT+QCFG="band",F,180A,180A
AT+QCFG="iotopmode",2
AT+QCFG="nwscanseq",020301
AT+QCFG="nwscanmode",0
If no need to support GPRS, please set with
AT+QCFG="nwscanmode",3

- For **Europe** region, enable the 3 RATs at the same time and set the band supported for B3, B8 and B20:
  AT+QCFG="band",F,80084,80084
  AT+QCFG="iotopmode",2
  AT+QCFG="nwscanseq",020301
  AT+QCFG="nwscanmode",0
  If no need to support GPRS, please set with
  AT+QCFG="nwscanmode",3

- For **Korea** region, enable the 3 RATs at the same time and set the band supported for B3 and B5:
  AT+QCFG="band",F,14,14
  AT+QCFG="iotopmode",2
  AT+QCFG="nwscanseq",020301
  AT+QCFG="nwscanmode",0
  If no need to support GPRS, please set with
  AT+QCFG="nwscanmode",3

- For **Australia** region, enable the 3 RATs at the same time and set the band supported for B3 and B28:
  AT+QCFG=”band”,F,8000004,8000004
  AT+QCFG=”iotopmode”,2
  AT+QCFG=”nwscanseq”,020301
  AT+QCFG="nwscanmode",0
  If no need to support GPRS, please set with
  AT+QCFG="nwscanmode",3

- For **Middle East** region, enable the 3 RATs at the same time and set the band supported for B3, B8 and B28:
  AT+QCFG="band",F,8000084,8000084
  AT+QCFG="iotopmode",2
  AT+QCFG="nwscanseq",020301
  AT+QCFG="nwscanmode",0
  If no need to support GPRS, please set with
  AT+QCFG="nwscanmode",3

- For **Japan** region, enable the 3 RATs at the same time and set the band supported for B1, B8, B18

and B19:
AT+QCFG="band",F,60081,60081
AT+QCFG="iotopmode",2
AT+QCFG="nwscanseq",020301
AT+QCFG="nwscanmode",0
If no need to support GPRS, please set with
AT+QCFG="nwscanmode",3

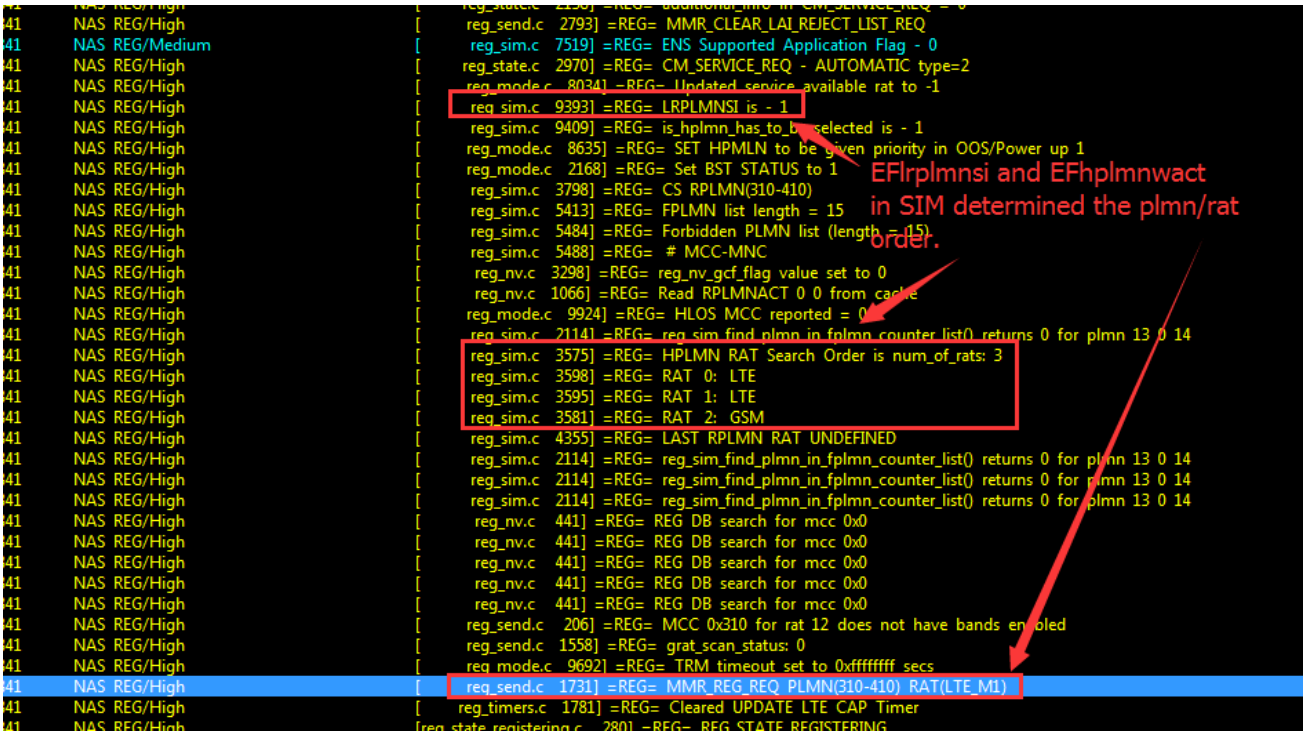
- For **China** region, enable the 3 RATs at the same time and set the band supported for B1, B3, B5, B8, B26 for Cat.M1 and Cat.NB1, B39 for Cat.M1 only:
  AT+QCFG="band",F,4002000095,2000095
  AT+QCFG="iotopmode",2
  AT+QCFG="nwscanseq",020301
  AT+QCFG="nwscanmode",0
  If no need to support GPRS, please set with
  AT+QCFG="nwscanmode",3

7 Typical Customer Problems and Analysis

Here share some typical customer questions and analysis.

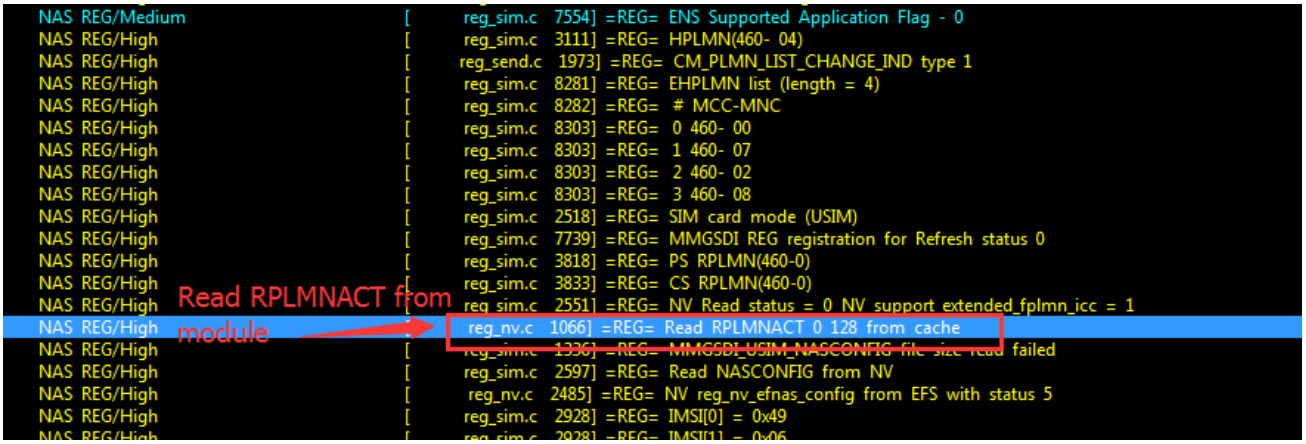
7.1. Module network searching order was determined by SIM-card file.

In this example, we can find that the rat order is not comply with the command “AT+QCFG=”nwscanseq””.

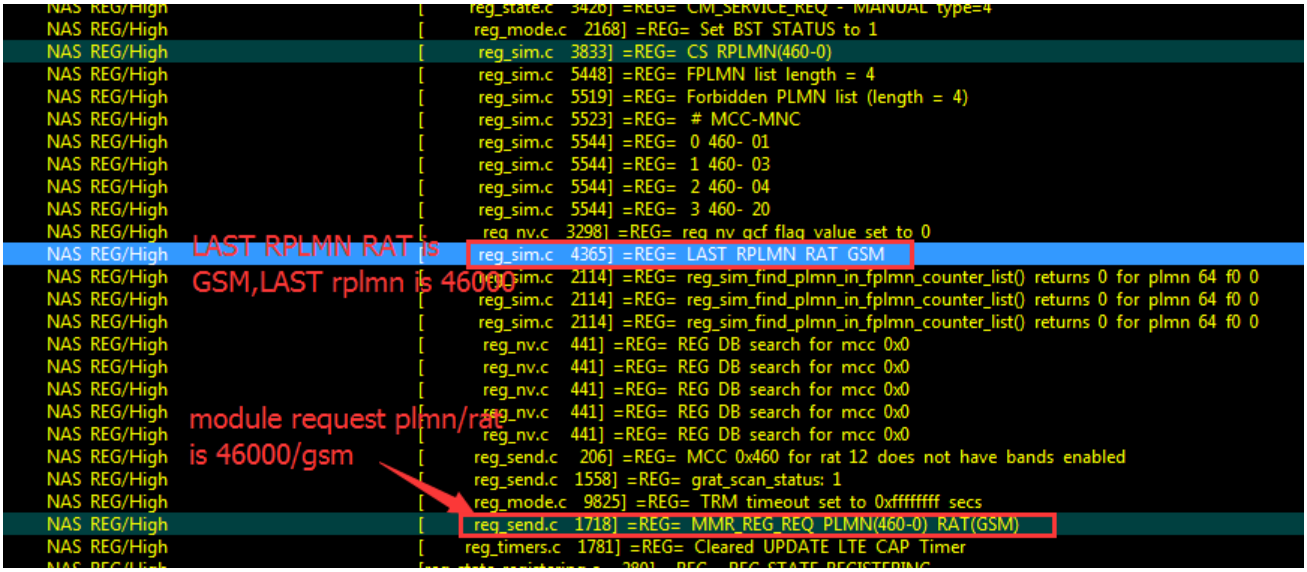


7.2. Module network searching order was determined by RPLMN/RPLMNACT stored in module.

In this example, $EF_{LRPLMNSI}$(0x6FDC, this file is optional in 3gpp protocol) is not existed in the SIM. Module will search RPLMN/RPLMNACT stored in the module.




```
NAS REG/Medium  [  reg_sim.c  7554] =REG= ENS Supported Application Flag - 0
NAS REG/High    [  reg_sim.c  3111] =REG= HPLMN(460- 04)
NAS REG/High    [  reg_send.c  1973] =REG= CM_PLMN_LIST_CHANGE_IND type 1
NAS REG/High    [  reg_sim.c  8281] =REG= EHPLMN list (length = 4)
NAS REG/High    [  reg_sim.c  8282] =REG=  # MCC-MNC
NAS REG/High    [  reg_sim.c  8303] =REG=  0 460- 00
NAS REG/High    [  reg_sim.c  8303] =REG=  1 460- 07
NAS REG/High    [  reg_sim.c  8303] =REG=  2 460- 02
NAS REG/High    [  reg_sim.c  8303] =REG=  3 460- 08
NAS REG/High    [  reg_sim.c  2518] =REG= SIM card mode (USIM)
NAS REG/High    [  reg_sim.c  7739] =REG= MMGSDI REG registration for Refresh status 0
NAS REG/High    [  reg_sim.c  3818] =REG= PS RPLMN(460-0)
NAS REG/High    [  reg_sim.c  3833] =REG= CS RPLMN(460-0)
NAS REG/High    [  reg_sim.c  2551] =REG= NV Read status = 0 NV support extended_fplmn_icc = 1
NAS REG/High    [  reg_nv.c  1066] =REG= Read RPLMNACT 0 128 from cache
NAS REG/High    [  reg_sim.c  1336] =REG= MMGSDI_USIM_NASCONFIG file size read failed
NAS REG/High    [  reg_sim.c  2597] =REG= Read NASCONFIG from NV
NAS REG/High    [  reg_nv.c  2485] =REG= NV reg_nv_efnas_config from EFS with status 5
NAS REG/High    [  reg_sim.c  2928] =REG= IMSI[0] = 0x49
```




```
NAS REG/High    [  reg_state.c  3426] =REG= CM_SERVICE_REQ - MANUAL type=4
NAS REG/High    [  reg_mode.c  2168] =REG= Set BST STATUS to 1
NAS REG/High    [  reg_sim.c  3833] =REG= CS RPLMN(460-0)
NAS REG/High    [  reg_sim.c  5448] =REG= FPLMN list length = 4
NAS REG/High    [  reg_sim.c  5519] =REG= Forbidden PLMN list (length = 4)
NAS REG/High    [  reg_sim.c  5523] =REG=  # MCC-MNC
NAS REG/High    [  reg_sim.c  5544] =REG=  0 460- 01
NAS REG/High    [  reg_sim.c  5544] =REG=  1 460- 03
NAS REG/High    [  reg_sim.c  5544] =REG=  2 460- 04
NAS REG/High    [  reg_sim.c  5544] =REG=  3 460- 20
NAS REG/High    [  reg_nv.c  3298] =REG= reg_nv_gcf_flag_value_set_to_0
NAS REG/High    [  reg_sim.c  4365] =REG= LAST RPLMN RAT GSM
NAS REG/High    [  reg_sim.c  2114] =REG= reg_sim_find_plmn_in_fplmn_counter_list() returns 0 for plmn 64 f0 0
NAS REG/High    [  reg_sim.c  2114] =REG= reg_sim_find_plmn_in_fplmn_counter_list() returns 0 for plmn 64 f0 0
NAS REG/High    [  reg_sim.c  2114] =REG= reg_sim_find_plmn_in_fplmn_counter_list() returns 0 for plmn 64 f0 0
NAS REG/High    [  reg_nv.c  441] =REG= REG DB search for mcc 0x0
NAS REG/High    [  reg_nv.c  441] =REG= REG DB search for mcc 0x0
NAS REG/High    [  reg_nv.c  441] =REG= REG DB search for mcc 0x0
NAS REG/High    [  reg_nv.c  441] =REG= REG DB search for mcc 0x0
NAS REG/High    [  reg_nv.c  441] =REG= REG DB search for mcc 0x0
NAS REG/High    [  reg_send.c  206] =REG= MCC 0x460 for rat 12 does not have bands enabled
NAS REG/High    [  reg_send.c  1558] =REG= grat_scan_status: 1
NAS REG/High    [  reg_mode.c  9825] =REG= TRM timeout set to 0xffffffff secs
NAS REG/High    [  reg_send.c  1718] =REG= MMR_REG_REQ PLMN(460-0) RAT(GSM)
NAS REG/High    [  reg_timers.c  1781] =REG= Cleared UPDATE LTE CAP Timer
```