

# **BG95&BG77&BG600L Series** Network Searching Scheme Introduction

**LPWA Module Series** 

Version: 2.0

Date: 2022-04-24

Status: Released







At Quectel, our aim is to provide timely and comprehensive services to our customers. If you require any assistance, please contact our headquarters:

#### **Quectel Wireless Solutions Co., Ltd.**

Building 5, Shanghai Business Park Phase III (Area B), No.1016 Tianlin Road, Minhang District, Shanghai 200233, China Tel: +86 21 5108 6236 Email: info@guectel.com

**Or our local offices. For more information, please visit:** http://www.guectel.com/support/sales.htm.

For technical support, or to report documentation errors, please visit: <u>http://www.quectel.com/support/technical.htm</u>. Or email us at: <u>support@quectel.com</u>.

# **Legal Notices**

We offer information as a service to you. The provided information is based on your requirements and we make every effort to ensure its quality. You agree that you are responsible for using independent analysis and evaluation in designing intended products, and we provide reference designs for illustrative purposes only. Before using any hardware, software or service guided by this document, please read this notice carefully. Even though we employ commercially reasonable efforts to provide the best possible experience, you hereby acknowledge and agree that this document and related services hereunder are provided to you on an "as available" basis. We may revise or restate this document from time to time at our sole discretion without any prior notice to you.

# **Use and Disclosure Restrictions**

# License Agreements

Documents and information provided by us shall be kept confidential, unless specific permission is granted. They shall not be accessed or used for any purpose except as expressly provided herein.

# Copyright

Our and third-party products hereunder may contain copyrighted material. Such copyrighted material shall not be copied, reproduced, distributed, merged, published, translated, or modified without prior written consent. We and the third party have exclusive rights over copyrighted material. No license shall be granted or conveyed under any patents, copyrights, trademarks, or service mark rights. To avoid ambiguities, purchasing in any form cannot be deemed as granting a license other than the normal non-exclusive, royalty-free license to use the material. We reserve the right to take legal action for noncompliance with abovementioned requirements, unauthorized use, or other illegal or malicious use of the material.



# Trademarks

Except as otherwise set forth herein, nothing in this document shall be construed as conferring any rights to use any trademark, trade name or name, abbreviation, or counterfeit product thereof owned by Quectel or any third party in advertising, publicity, or other aspects.

# **Third-Party Rights**

This document may refer to hardware, software and/or documentation owned by one or more third parties ("third-party materials"). Use of such third-party materials shall be governed by all restrictions and obligations applicable thereto.

We make no warranty or representation, either express or implied, regarding the third-party materials, including but not limited to any implied or statutory, warranties of merchantability or fitness for a particular purpose, quiet enjoyment, system integration, information accuracy, and non-infringement of any third-party intellectual property rights with regard to the licensed technology or use thereof. Nothing herein constitutes a representation or warranty by us to either develop, enhance, modify, distribute, market, sell, offer for sale, or otherwise maintain production of any our products or any other hardware, software, device, tool, information, or product. We moreover disclaim any and all warranties arising from the course of dealing or usage of trade.

# **Privacy Policy**

To implement module functionality, certain device data are uploaded to Quectel's or third-party's servers, including carriers, chipset suppliers or customer-designated servers. Quectel, strictly abiding by the relevant laws and regulations, shall retain, use, disclose or otherwise process relevant data for the purpose of performing the service only or as permitted by applicable laws. Before data interaction with third parties, please be informed of their privacy and data security policy.

# Disclaimer

- a) We acknowledge no liability for any injury or damage arising from the reliance upon the information.
- b) We shall bear no liability resulting from any inaccuracies or omissions, or from the use of the information contained herein.
- c) While we have made every effort to ensure that the functions and features under development are free from errors, it is possible that they could contain errors, inaccuracies, and omissions. Unless otherwise provided by valid agreement, we make no warranties of any kind, either implied or express, and exclude all liability for any loss or damage suffered in connection with the use of features and functions under development, to the maximum extent permitted by law, regardless of whether such loss or damage may have been foreseeable.
- d) We are not responsible for the accessibility, safety, accuracy, availability, legality, or completeness of information, advertising, commercial offers, products, services, and materials on third-party websites and third-party resources.

Copyright © Quectel Wireless Solutions Co., Ltd. 2022. All rights reserved.

# **About the Document**

# **Revision History**

Revision	Date	Author	Description		
1.0	2020-01-13	Elvis SUN	Initial		
2.0	2022-04-24	Forest WANG	<ol> <li>Added the applicable module BG600L-M3.</li> <li>Updated the frequency bands of BG95 series and BG77: deleted the eMTC band B14 and NB-IoT B26 (Chapters 2.1 and 2.2).</li> <li>Updated the RAT/PLMN selection procedure figure (Figure 2).</li> <li>Updated notes of network searching AT commands (Chapter 5).</li> <li>Updated the default setting of <mode> in AT+QCFG="iotopmode" (Chapter 5.3).</mode></li> <li>Added some typical problems and corresponding cause analysis (Chapters 7.3, 7.4 and 7.5).</li> <li>Added the FAQ chapter (Chapter 8).</li> </ol>		



# Contents

Abo	About the Document				
Cor	Contents 4				
Tab	Table Index				
Fig	ure Index	6			
1	Introduction				
	1.1. Applicable Modules	7			
2	Supported RATs and Bands	8			
	2.1. Supported RATs and Bands of BG95 Series	8			
	2.2. Supported RATs and Bands of BG77	8			
	2.3. Supported RATs and Bands of BG600L-M3	9			
3	Network Searching/Registration Processes 1	0			
4	Factors Influencing Network Registration Speed1	3			
	4.1. RAT/PLMN Selection 1	3			
	4.2. LTE EARFCN Scan 1	4			
5	Network Searching Related AT Commands1	6			
	5.1. AT+QCFG="nwscanseq" Configure RAT Searching Sequence 1	6			
	5.2. AT+QCFG="nwscanmode" Configure RAT(s) to be Searched for 1	7			
	5.3. AT+QCFG="iotopmode" Configure Network Category to be Searched for under LTE RAT 1	8			
	5.4. AT+QCFG="band" Configure Frequency Band 1	9			
6	Solutions to Speed up Network Searching 2	23			
	6.1. Overview of NB-IoT Network Searching Time	23			
	6.2. Solutions to Speed up Network Searching	24			
	6.2.1. Disable NB-IoT and Enable Required RAT(s) 2	24			
	6.2.2. Enable NB-IoT Bands Supported by Current Operator Only	24			
7	Typical Problems and Root Cause Analysis	26			
	7.1. Network Searching Sequence Determined by (U)SIM Card Files	26			
	7.2. Network Searching Sequence Determined by RPLMN/RPLMNACT Stored on Module Flash2	27			
	7.3. Long Network Registration Time in Roaming State	28			
	7.4. Network Registration Request Rejected by Network	30			
	7.5. Long Network Registration Time if AT Commands are Executed Frequently	34			
8	FAQ	35			
9	Summary of CME ERROR Codes	37			
10	Appendix References	39			



# **Table Index**

Table 1: Applicable Modules	7
Table 2: Frequency Bands of BG95 Series Module	8
Table 3: Frequency Bands of BG77 Module	9
Table 4: Frequency Bands of BG600L-M3 Module	9
Table 5: Network Searching Time of NB-IoT Bands with Different SNR	. 14
Table 6: eMTC/NB-IoT Band Deployment over the World (For Reference Only)	. 15
Table 7: Solutions to Speed up Network Searching (Disable NB-IoT)	. 24
Table 8: Solutions to Speed up Network Searching (Enable NB-IoT Bands Supported)	. 24
Table 9: Related Documents	. 39
Table 10: Terms and Abbreviations	. 39



# **Figure Index**

Figure 1: Network Searching and Registration Process	. 10
Figure 2: RAT/PLMN Selection	. 13
Figure 3: RAT Searching Sequence Determined by (U)SIM Card Files	. 26
Figure 4: RAT Searching Sequence Determined by RPLMN/RPLMNACT Stored on Module Flash	. 27
Figure 5: Behaviour of the Module if (U)SIM is Card in Roaming State	. 28
Figure 6: GMM Cause Information Element	. 31
Figure 7: EMM Cause Information Element	. 32
Figure 8: Module Received Reject Cause Code	. 33
Figure 9: Module Initiated T3247 Timer and Tried to Register Another Available Network	. 33
Figure 10: Restore the Network Information	. 35

# **1** Introduction

This document outlines the supported RATs and frequency bands of Quectel BG95 series, BG77 and BG600L-M3 modules, and describes the network searching scheme by illustrating network searching/registration processes and related AT commands to help users understand the network searching mechanism of the modules.

Furthermore, the document describes some problems observed in the process of network searching, and provides the corresponding root cause analysis.

# 1.1. Applicable Modules

### **Table 1: Applicable Modules**

Module Series	Model	Description
	BG95-M1	Cat M1 only
	BG95-M2	Cat M1/Cat NB2
	BG95-M3	Cat M1/Cat NB2/EGPRS
BG95	BG95-M4	Cat M1/Cat NB2, 450 MHz Supported
	BG95-M5	Cat M1/Cat NB2/EGPRS, Power Class 3
	BG95-M6	Cat M1/Cat NB2, Power Class 3
	BG95-MF	Cat M1/Cat NB2, Wi-Fi Positioning
BG77	BG77	Cat M1/Cat NB2
BG600L	BG600L-M3	Cat M1/Cat NB2/EGPRS

# **2** Supported RATs and Bands

# 2.1. Supported RATs and Bands of BG95 Series

Quectel BG95 series module supports three RATs: eMTC, NB-IoT and EGPRS.

- Default RATs: eMTC, NB-IoT and EGPRS
- Default searching sequence:  $eMTC \rightarrow NB-loT \rightarrow EGPRS$
- If the three RATs need to be supported synchronously or other searching sequences are needed, set the relevant configuration values via AT commands. The details of AT commands are provided in *Chapter 5*.

The following table lists the supported frequency bands of BG95 series module.

### Table 2: Frequency Bands of BG95 Series Module

RAT	Frequency Band
eMTC	B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B26/B27/B28/B31/B66/B72/B73/B85
NB-IoT	B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B28/B31/B66/B71/B72/B73/B85
EGPRS	GSM850, EGSM900, DCS1800, PCS1900

NOTE

Quectel BG95 series includes multiple models with different RATs and frequency bands. For detailed information, see *document [1]*.

# 2.2. Supported RATs and Bands of BG77

Quectel BG77 module supports two RATs: eMTC and NB-IoT.



- Default RATs: eMTC and NB-IoT
- Default searching sequence:  $eMTC \rightarrow NB-IoT$
- If the two RATs need to be supported synchronously or other searching sequences are needed, set the relevant configuration values via AT commands. The details of AT commands are provided in *Chapter 5*.

The following table lists the supported frequency bands of BG77.

#### Table 3: Frequency Bands of BG77 Module

RAT	Frequency Band
eMTC	B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B26/B27/B28/B66/B85*
NB-IoT	B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B28/B66/B71/B85*

# 2.3. Supported RATs and Bands of BG600L-M3

Quectel BG600L-M3 module supports three RATs: eMTC, NB-IoT and EGPRS.

- Default RATs: eMTC, NB-IoT and EGPRS
- Default searching sequence:  $eMTC \rightarrow NB-IoT \rightarrow EGPRS$
- If the three RATs need to be supported synchronously or other searching sequences are needed, set the relevant configuration values via AT commands. The details of AT commands are provided in *Chapter 5*.

The following table lists the supported frequency bands of BG600L-M3 module.

### Table 4: Frequency Bands of BG600L-M3 Module

RAT	Frequency Band
eMTC	B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B26/B27/B28/B66/B85
NB-IoT	B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B28/B66/B71/B85
EGPRS	GSM850, EGSM900, DCS1800, PCS1900

# **3** Network Searching/Registration Processes

The network searching/registration processes of BG95 series, BG77 and BG600L-M3 modules are illustrated below:

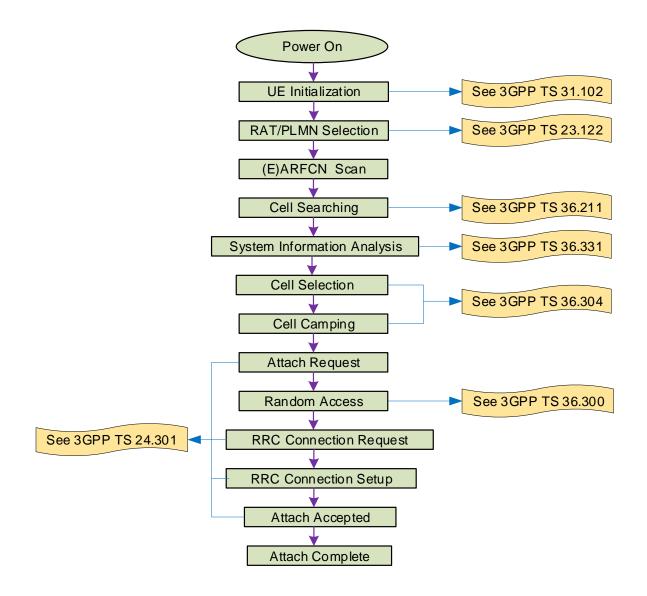


Figure 1: Network Searching and Registration Process



#### 1. UE Initialization

UE initialization includes (U)SIM card recognition and reading of NVM related to network searching.

#### 2. RAT/PLMM Selection

- Set the RAT searching sequence and the RAT(s) allowed to be searched according to network searching related NVM and related (U)SIM EF files.
- PLMN selection can be performed in either automatic or manual modes.
- For more information, see *Chapter 4.1*.

#### 3. (E)ARFCN Scan

- LTE EARFCN scan includes system scan and band scan.
- EGPRS ARFCN scan refers to power scan.
- For more information, see *Chapter 4.2*.

#### 4. Cell Searching

Cell searching refers to cell recognition and downlink synchronization.

#### 5. System Information Analysis

This step includes reading and analyzing MIB and SIB information. For detailed definition of system information, see *3GPP TS 36.331 [5.2]*.

- MIB information: the number of antennas, downlink bandwidth, cell ID and registered (E)ARFCN.
- SIB information: PLMN, cell ID, etc.

#### 6. Cell Selection

If the acquired band satisfies the signal strength requirement of UE, the UE will perform the next step (cell camping), otherwise it will continue (E)ARFCN scanning.

#### 7. Cell Camping

Cell camping is started after successful cell selection.

#### 8. Attach Request/Location Update Request

After the cell is 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. RRC Connection Setup



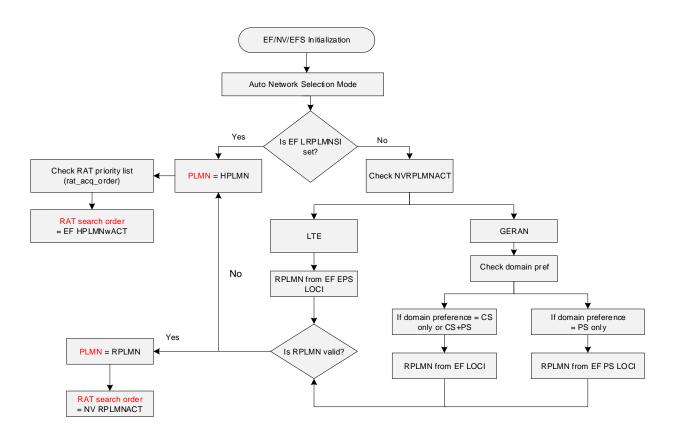
12. Attach Accepted/Location Updating Accepted

# **4** Factors Influencing Network Registration Speed

Network registration speed is affected by RAT/PLMN selection and LTE EARFCN scan. The details about the two processes are provided below.

# 4.1. RAT/PLMN Selection

This chapter describes the steps involved in RAT/PLMN selection. The following figure illustrates the overall processes of RAT/PLMN selection in automatic mode. As shown below, the search order during RAT/PLMN selection is determined not only by the module settings but also by some files on the (U)SIM card. By default, the files on the (U)SIM card have a higher priority.





# 4.2. LTE EARFCN Scan

This chapter describes the effect of LTE EARFCN scan on the speed of network registration.

LTE EARFCN scan includes system scan and band scan. When the module shuts down, it will store the current network registration information (e.g., EARFCN, PCI and so on). When the module powers on next time for network registration, UE will try to acquire the stored network registration information. This procedure is called system scan. This procedure will speed up the network registration process. If the network information acquisition failed in system scan, UE will attempt to scan all supported bands, which process constitutes the band scan.

According to statistics, the scan for all bands under eMTC and EGPRS takes about tens of seconds. However, EARFCN scan will take longer under NB-IoT, due to the characteristics of NB-IoT network (especially the weak signal feature). The following table shows the test results of some of the NB-IoT bands, which displays the EARFCN scan time required in each band.

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

#### Table 5: Network Searching Time of NB-IoT Bands with Different SNR

As BG95 series, BG77 and BG600L-M3 modules support dozens of bands under NB-IoT, it is recommended to enable only the bands supported by the service operator.

Band	DL Freq. (MHz)	Applicability as per 3GPP TS36.1.0.1	U.S.	China	The Middle East	Japan	Korea	Europe	Australia
B1	2100	eMTC/NB-IoT		•		•			
B2	1900	eMTC/NB-IoT	•						
B3	1800	eMTC/NB-IoT		•	•		-	•	•
B4	1700	eMTC	•						
B5	850	eMTC/NB-IoT		•			-		
B8	900	eMTC/NB-IoT		•	•	•		•	
B12	700	eMTC/NB-IoT	•						
B13	700	eMTC/NB-IoT	•						
B18	800	eMTC/NB-IoT				•			
B19	800	eMTC/NB-IoT				•			
B20	800	eMTC/NB-IoT						•	
B26	850	eMTC/NB-IoT		•					
B28	700	eMTC/NB-IoT			•				•

### Table 6: eMTC/NB-IoT Band Deployment over the World (For Reference Only)

# **5** Network Searching Related AT Commands

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

# 5.1. AT+QCFG="nwscanseq" Configure RAT Searching Sequence

AT+QCFG="nwscanseq" Configu	re RAT Searching Sequence
Write Command AT+QCFG="nwscanseq"[, <scanseq>[, <effect>]]</effect></scanseq>	Response If the optional parameters are omitted, query the current setting. +QCFG: "nwscanseq", <scanseq></scanseq>
	ок
	If any of the optional parameters is specified, configure the RAT searching sequence. OK
	If there is an error related to ME functionality: +CME ERROR: <err></err>
	If there is any other error: ERROR
Maximum Response Time	300 ms
Characteristics	<effect> determines when the command will take effect. The configurations will be saved automatically.</effect>

This Write Command configures the searching sequence of RATs or queries the current setting.



<scanseq></scanseq>	Integer type. RAT searching sequence.
	(e.g.: 020301 stands for eMTC $\rightarrow$ NB-IoT $\rightarrow$ GSM)
	<u>00</u> Automatic (eMTC $\rightarrow$ NB-IoT $\rightarrow$ GSM)
	01 GSM
	02 eMTC
	03 NB-IoT
<effect></effect>	Integer type. When to take effect.
	0 Take effect after UE reboots
	<u>1</u> Take effect immediately
<err></err>	Integer type. Error code. See Chapter 9 for details.

# NOTE

- 1. This command is invalid on BG95-M1 module.
- 2. GSM RAT (**<scanseq>**=01) is valid only on BG95-M3, BG95-M5 and BG600L-M3 modules.
- 3. NB-IoT is disabled by default.
- 4. Don't repeatedly select one RAT while specifying **<scanseq>** (for example "020202"), to prevent unexpected situations.

# 5.2. AT+QCFG="nwscanmode" Configure RAT(s) to be Searched for

This Write Command configures the RAT(s) to be searched for or queries the current setting

AT+QCFG="nwscanmode" Configure RAT(s) to be Searched for		
Write Command AT+QCFG="nwscanmode"[, <scan_mo de&gt;[,<effect>]]</effect></scan_mo 	Response If the optional parameters are omitted, query the current setting. +QCFG: "nwscanmode", <scan_mode></scan_mode>	
	ОК	
	If any of the optional parameters is specified, configure the RAT(s) to be searched for: <b>OK</b>	
	If there is an error related to ME functionality: +CME ERROR: <err></err>	
	If there is any other error:	



	ERROR
Maximum Response Time	300 ms
Characteristics	<effect> determines when the command will take effect. The configurations will be saved automatically.</effect>

<scan_mode></scan_mode>	Integer type. RAT(s) to be searched for.
	0 Automatic (GSM and LTE)
	1 GSM only
	3 LTE only
<effect></effect>	Integer type. When to take effect.
	0 Take effect after UE reboots
	1 Take effect immediately
<err></err>	Integer type. Error code. See <i>Chapter 9</i> for details.

NOTE

This command is valid only on BG95-M3, BG95-M5 and BG600L-M3 modules.

# 5.3. AT+QCFG="iotopmode" Configure Network Category to be

# Searched for under LTE RAT

This Write Command configures the network category to be searched for under LTE RAT or queries the current setting.

AT+QCFG="iotopmode" Configu LTE RAT	ire Network Category to be Searched for under	
Write Command	Response	
AT+QCFG="iotopmode"[, <mode>[,<eff ect&gt;]]</eff </mode>	If the optional parameters are omitted, query the current setting. +QCFG: "iotopmode", <mode></mode>	
	ОК	
	If any of the optional parameters is specified, configure the network category to be searched for under LTE RAT: <b>OK</b>	

	If there is an error related to ME functionality: +CME ERROR: <err></err>
	If there is any other error: ERROR
Maximum Response Time	300 ms
Characteristics	<effect> determines when the command will take effect. The configurations will be saved automatically.</effect>

<mode></mode>	Integer type. Network category to be searched for under LTE RAT.		
	0 eMTC		
	1 NB-IoT		
	2 eMTC and NB-IoT		
<effect></effect>	Integer type. When to take effect.		
	0 Take effect after UE reboots		
	<u>1</u> Take effect immediately		
<err></err>	Integer type. Error code. See Chapter 9 for details.		

NOTE

This command is invalid on BG95-M1 module.

# 5.4. AT+QCFG="band" Configure Frequency Band

This Write Command configures the frequency bands to be searched for or queries the current setting.

AT+QCFG="band" Configure Frequency Band			
Write Command	Response		
AT+QCFG="band"[, <gsm_bandval>,</gsm_bandval>	If the optional parameters are omitted, query the current		
<emtc_bandval>,<nb-lot_bandval>[</nb-lot_bandval></emtc_bandval>	setting.		
, <effect>]]</effect>	+QCFG: "band", <gsm_bandval>,<emtc_bandval>,<nb-i< th=""></nb-i<></emtc_bandval></gsm_bandval>		
	oT_bandval>		
	OK		
	If any of the optional parameters is specified, configure the		

	frequency bands to be searched for. OK
	If there is an error related to ME functionality: +CME ERROR: <err></err>
	If there is any other error: ERROR
Maximum Response Time	300 ms
Characteristics	<effect> determines when the command will take effect. The configurations will be saved automatically.</effect>

<gsm_bandval></gsm_bandval>	A hexadeci	mal value that specifies the GSM frequenc	v band (e.g.: 0xa =
		(00) + 0x8(PCS1900)). If it is set to 0, it means	
	frequency ba		
	0	No change	
	0x1	EGSM900	
	0x2	DCS1800	
	0x4	GSM850	
	0x8	PCS1900	
	<u>0xF</u>	All of the supported bands above	
<emtc_bandval></emtc_bandval>			/ band (e.g.: 0x15 =
	0x1(LTE B1	) + 0x4(LTE B3) + 0x10(LTE B5)). If it is set	to 0, it means not to
	change the eMTC frequency band.		
	0		No change
	0x1 (BAND_	PREF_LTE_BAND1)	LTE B1
	0x2 (BAND_	PREF_LTE_BAND2)	LTE B2
	0x4 (BAND_	PREF_LTE_BAND3)	LTE B3
	0x8 (BAND_	PREF_LTE_BAND4)	LTE B4
	0x10 (BAND	PREF_LTE_BAND5)	LTE B5
	0x80 (BAND	PREF_LTE_BAND8)	LTE B8
	0x800 (BAN	D_PREF_LTE_BAND12)	LTE B12
	0x1000 (BAI	ND_PREF_LTE_BAND13)	LTE B13
	0x20000 (BA	AND_PREF_LTE_BAND18)	LTE B18
	0x40000 (BA	AND_PREF_LTE_BAND19)	LTE B19
	0x80000 (BA	AND_PREF_LTE_BAND20)	LTE B20
	0x1000000 (	(BAND_PREF_LTE_BAND25)	LTE B25
	0x2000000 (	(BAND_PREF_LTE_BAND26)	LTE B26
	0x4000000 (	(BAND_PREF_LTE_BAND27)	LTE B27
	0x8000000 (	(BAND_PREF_LTE_BAND28)	LTE B28
	0x4000000	(BAND_PREF_LTE_BAND31)	LTE B31



	0x20000000000000000 (BAND_PREF_LTE_BAND66)	LTE B66
	0x800000000000000000000000000000000000	LTE B72
	0x100000000000000000000000000000000000	LTE B73
	0x100000000000000000000000000000000000	LTE B85
<nb-iot_bandval></nb-iot_bandval>	A hexadecimal value that specifies the NB-IoT frequency	
	0x1(LTE B1) + 0x4(LTE B3) + 0x10(LTE B5)). If it is set to 0, it	means not to change
	the NB-IoT frequency band.	
	0	No change
	0x1 (BAND_PREF_LTE_BAND1)	LTE B1
	0x2 (BAND_PREF_LTE_BAND2)	LTE B2
	0x4 (BAND_PREF_LTE_BAND3)	LTE B3
	0x8 (BAND_PREF_LTE_BAND4)	LTE B4
	0x10 (BAND_PREF_LTE_BAND5)	LTE B5
	0x80 (BAND_PREF_LTE_BAND8)	LTE B8
	0x800 (BAND_PREF_LTE_BAND12)	LTE B12
	0x1000 (BAND_PREF_LTE_BAND13)	LTE B13
	0x20000 (BAND_PREF_LTE_BAND18)	LTE B18
	0x40000 (BAND_PREF_LTE_BAND19)	LTE B19
	0x80000 (BAND_PREF_LTE_BAND20)	LTE B20
	0x1000000 (BAND_PREF_LTE_BAND25)	LTE B25
	0x8000000 (BAND_PREF_LTE_BAND28)	LTE B28
	0x40000000 (BAND_PREF_LTE_BAND31)	LTE B31
	0x20000000000000000 (BAND_PREF_LTE_BAND66)	LTE B66
	0x40000000000000000000000 (BAND_PREF_LTE_BAND71)	LTE B71
	0x800000000000000000000000000000000000	LTE B72
	0x100000000000000000 (BAND_PREF_LTE_BAND73)	LTE B73
	0x100000000000000000000000000000000000	LTE B85
<effect></effect>	Integer type. When to take effect.	
	0 Take effect after UE reboots	
	<u>1</u> Take effect immediately	
<err></err>	Integer type. Error code. See Chapter 9 for details.	

# NOTE

- 1. For the specific bands supported by each model, see corresponding specifications of the modules.
  - **<GSM\_bandval>** is valid only on BG95-M3, BG95-M5 and BG600L-M3 modules.
  - **<NB-loT\_bandval>** is invalid on BG95-M1 module.
  - LTE B31/B72/B73 is valid on BG95-M4 module only.
- 2. The value setting of **<eMTC\_bandval>** when all eMTC bands are intended to be searched for:
  - 0x10018200000004F0E189F for BG95-M4
  - 0x100002000000000000F0E189F for BG77, BG600L-M3 and other BG95 series modules
- 3. The value setting of **<NB-IoT\_bandval>** when all NB-IoT bands are intended to be searched for:
  - 0x1001820000000490E189F for BG95-M4

• 0x1000420000000000E189F for BG77, BG600L-M3 and other BG95 series modules

# 6 Solutions to Speed up Network Searching

# 6.1. Overview of NB-IoT Network Searching Time

As per 3GPP specifications, NB-IoT is expected to be deployed in a much lower coverage area. Expected Maximum Coupling Loss for NB-IoT is 164 dB, whereas it is only around 155 dB for eMTC. This pushes the device to accommodate more SNR range to detect a possible NB-IoT cell deployment. In addition, eMTC has a 1.4 MHz bandwidth, whereas NB-IoT has a 200 KHz bandwidth. This means NB-IoT has much more candidates to scan and detect in a given LTE deployed area, which leads to much longer searching time for NB-IoT than eMTC.

BG95 series, BG77 and BG600L-M3 modules divide the search process into three levels according to NB-IoT signal characteristics:

- Frequency scan level 0 (SNR level 0): SNR value > 0 dB. This takes only few milliseconds for each raster.
- Frequency scan level 1 (SNR level 1): SNR value ranges from 0 to -9 dB. This takes about 100 msec for each raster.
- Frequency scan level 2 (SNR level 2): typical SNR value is about -12 dB. This takes about 400 to 500 msec for each raster.

According to the test results in *Table 5*, NB-IoT network was searched for a long period of time. This, coupled with the dozens of bands supported by the modules, makes the total network searching time very long.

- Under SNR level 0, searching the network takes only tens of seconds.
- Under SNR level 1, the time for network searching is five to six times as long as the time for searching under SNR level 0.
- Under SNR level 2, the time for network searching is ten to fifteen times as long as the time for searching under SNR level 0.

To avoid the long network searching time, either of the following solutions should be used to optimize the network searching scheme of modules.

# 6.2. Solutions to Speed up Network Searching

# 6.2.1. Disable NB-IoT and Enable Required RAT(s)

Network searching can be sped up by disabling NB-IoT and enabling only the required RAT(s).

# Table 7: Solutions to Speed up Network Searching (Disable NB-IoT)

Solutions		Related AT Commands
Disable NB-IoT		Default configuration
Enable Required RAT(s)	Enable EGPRS only	AT+QCFG="nwscanmode",1
	Enable eMTC only	AT+QCFG="iotopmode",0 AT+QCFG="nwscanmode",3
	Enable eMTC and EGPRS both	AT+QCFG="iotopmode",0 AT+QCFG="nwscanmode",0

# 6.2.2. Enable NB-IoT Bands Supported by Current Operator Only

When NB-IoT is necessary, it is recommended to enable only the bands supported by the current service operator.

Table 8: Solutions to	Speed up Network Searc	hing (Enable NB-IoT	Bands Supported)

Regions	Solutions	Related AT Commands
		AT+QCFG="band",F,180A,180A
	Enable the three RATs	AT+QCFG="iotopmode",2
U.S	synchronously.	AT+QCFG="nwscanseq",020301
0.5	Set B2, B4, B12 and B13 as the	AT+QCFG="nwscanmode",0
	bands to be searched.	AT+QCFG="nwscanmode",3 (set only when EGPRS is
		not needed)
		AT+QCFG="band",F,80084,80084
	Enable the three RATs	AT+QCFG="iotopmode",2
Europo	synchronously.	AT+QCFG="nwscanseq",020301
Europe	Set B3, B8 and B20 as the	AT+QCFG="nwscanmode",0
	bands to be searched.	AT+QCFG="nwscanmode",3 (set only when EGPRS is
		not needed)
	Enable the three RATs	AT+QCFG="band",F,14,14
Korea	synchronously.	AT+QCFG="iotopmode",2
	Set B3 and B5 as the bands to	AT+QCFG="nwscanseq",020301



	be searched.	AT+QCFG="nwscanmode",0
		AT+QCFG="nwscanmode",3 (set only when EGPRS is
		not needed)
		AT+QCFG="band",F,8000004,8000004
	Enable the three RATs	AT+QCFG="iotopmode",2
Australia	synchronously.	AT+QCFG="nwscanseq",020301
Australia	Set B3 and B28 as the bands to	AT+QCFG="nwscanmode",0
	be searched.	AT+QCFG="nwscanmode",3 (set only when EGPRS is
		not needed)
		AT+QCFG="band",F,8000084,8000084
The	Enable the three RATs	AT+QCFG="iotopmode",2
Middle	synchronously.	AT+QCFG="nwscanseq",020301
East	Set B3, B5 and B28 as the	AT+QCFG="nwscanmode",0
Lasi	bands to be searched.	AT+QCFG="nwscanmode",3 (set only when EGPRS is
		not needed)
		AT+QCFG="band",F,60081,60081
	Enable the three RATs	AT+QCFG="iotopmode",2
lonon	synchronously.	AT+QCFG="nwscanseq",020301
Japan	Set B1, B8, B18 and B19 as the	AT+QCFG="nwscanmode",0
	bands to be searched.	AT+QCFG="nwscanmode",3 (set only when EGPRS is
		not needed)
		AT+QCFG="band",F,2000095,2000095
	Enable the three RATs	AT+QCFG="iotopmode",2
China	synchronously.	AT+QCFG="nwscanseq",020301
Unina	Set B1, B3, B5, B8 and B26 as	AT+QCFG="nwscanmode",0
	the bands to be searched.	AT+QCFG="nwscanmode",3 (set only when EGPRS is
		not needed)

# 7 Typical Problems and Root Cause Analysis

This chapter describes some typical problems and corresponding root cause analysis.

# 7.1. Network Searching Sequence Determined by (U)SIM Card Files

#### **Problem Description:**

The RAT searching sequence does not comply with the setting of AT+QCFG="nwscanseq".

#### **Root Cause Analysis:**

The sequence is determined by some files in (U)SIM card, as illustrated in the example below.

	NAV NEV/TIGH	
41	NAS REG/High	[ reg_send.c 2793] =REG= MMR_CLEAR_LAI_REJECT_LIST_REQ
41	NAS REG/Medium	[ reg_sim.c 7519] = REG= ENS Supported Application Flag - 0
41	NAS REG/High	[ reg_state.c 2970] =REG= CM_SERVICE_REQ - AUTOMATIC type=2
41	NAS REG/High	reg_mode_c8034] - REGUpdated_service_available_rat_to1
41	NAS REG/High	[ reg sim.c 9393] = REG= LRPLMNSI is - 1
41	NAS REG/High	[ reg_sim.c 9409] =REG= is_hplmn_has_to_b selected is - 1
41	NAS REG/High	[ reg_mode.c 8635] =REG= SET HPMLN to be given priority in OOS/Power up 1
41	NAS REG/High	[ reg_mode.c 2168] =REG= Set BST STATUS to 1 EFIrpImnsi and EFhpImnwact
41	NAS REG/High	
41	NAS REG/High	reg_sim.c 5413] = REG= FPLMN list length = 15 in (U)SIM determinded the RAT/PLMN
41	NAS REG/High	reg_sinc. 5484] =REG= Forbidden PLMN list (length = 1)
41	NAS REG/High	[ reg_sim.c 5488] = REG= # MCC-MINC
41	NAS REG/High	[ reg_nv.c 3298] =REG= reg_nv_gcf_flag value set to 0 [ reg_nv.c 1066] =REG= Read RPLMNACT 0 0 from cache
41	NAS REG/High	[ reg_nv.c 1066] = REG= Read RPLMNACT 0 0 from cache
41	NAS REG/High	[ reg_mode.c 9924] = REG= HLOS MCC reported = 0
41	NAS REG/High	[ <u>reg sim.c 21141 = REG= reg sim find plmn in fplmn counter list() returns</u> 0 for plmn 13 ∅ 14
41	NAS REG/High	[ reg_sim.c 3575] =REG= HPLMN RAT Search Order is num_of_rats; 3
41	NAS REG/High	[ reg_sim.c 3598] =REG= RAT 0: LTE
41	NAS REG/High	[ reg_sim.c 3595] =REG= RAT 1: LTE
41	NAS REG/High	[ reg_sim.c 3581] = REG= RAT 2: GSM
41	NAS REG/High	[ reg_sim.c 4355] =REG= LAST RPLMN RAT UNDEFINED
41	NAS REG/High	[ reg_sim.c 2114] =REG= reg_sim_find_plmn_in_fplmn_counter_list() returns 0 for plmn 13 0 14
41	NAS REG/High	[ reg_sim.c 2114] =REG= reg_sim_find_plmn_in_fplmn_counter_list() returns 0 for plmn 13 0 14
41	NAS REG/High	[ reg_sim.c 2114] =REG= reg_sim_find_pImn_in_fpImn_counter_list() returns 0 for folmn 13 0 14
41	NAS REG/High	[ reg_nv.c 441] = REG = REG DB search for mcc 0x0
41	NAS REG/High	[ reg_nv.c 441] =REG= REG DB search for mcc 0x0
41	NAS REG/High	[ reg_nv.c 441] = REG = REG DB search for mcc 0x0
41	NAS REG/High	[ reg_nv.c 441] =REG= REG DB search for mcc 0x0
41	NAS REG/High	[ reg_nv.c 441] = REG = REG DB search for mcc 0x0
41	NAS REG/High	[ reg_send.c 206] =REG= MCC 0x310 for rat 12 does not have bands engoled
41	NAS REG/High	[ reg_send.c 1558] =REG= grat_scan_status: 0
41	NAS REG/High	<u>req mode.c 9692] =REG= TRM timeout set to 0xffffffff secs</u>
41	NAS REG/High	[ req_send.c 1731] =REG= MMR_REG_REQ_PLMN(310-410)_RAT(LTE_M1)_
41	NAS REG/High	[ reg_timers.c 1781] =REG= Cleared UPDATE LTE CAP Timer
141	NAS_REG/High	freq state registering c 2801 - REG - REG STATE REGISTERING

Figure 3: RAT Searching Sequence Determined by (U)SIM Card Files

# 7.2. Network Searching Sequence Determined by RPLMN/RPLMNACT

# Stored on Module Flash

#### **Problem Description:**

The RAT searching sequence does not comply with the setting of AT+QCFG="nwscanseq".

#### **Root Cause Analysis:**

In the example shown below, EF<sub>LRPLMNSI</sub> (0x6FDC, this file is optional in 3GPP protocol) does not exist on the (U)SIM card. The module thus searches RPLMN/RPLMNACT stored inside.

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 [ req_sim.c 8282] = REG= # MCC-MNC
NAS REG/High [ req_sim.c 8303] = REG= 0 460- 00
NAS REG/High [ req_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 [ req_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 NAS REG/High Read RPLMNACT from reg_sim.c 3833] = REG= CS RPLMN(460-0) NAS REG/High Read RPLMNACT from reg_sim.c 2551] = REG= NV Read status = 0 NV support extended fplmn_icc = 1
NAS REG/High module reg_nv.c 1066] =REG= Read RPLMNACT 0 128 from cache
NAS REG/High
NAS REG/High [ req_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 $\text{REG/High}$ [ reg rin c 2028] = $\text{REG}$ [MS[1] = 0x06
NAS REG/HIGN [ FEG_STATE.C 3420] = REG= CM_SERVICE_REQ - IVIAINUAL_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 5223] = REG = # MCC-MNC
NAS $REG/High$ [reg sim.c 554] = $REG = 0.460 - 01$
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 LAST RPLMN RAT (s reg nv.c 3298) = REG= reg nv gct flag value set to 0 NAS REG/High LAST RPLMN RAT (s reg_sim.c 4365) = REG= LAST RPLMN RAT GSM
NAS REG/High GSM,LAST rplmn is 46000 im.c 2114] =REG= reg_sim_find_plmn_in_fplmn_counter_list() returns 0 for plmn 64 f0 0 NAS REG/High GSM,LAST rplmn is 46000 im.c 2114] =REG= reg_sim_find_plmn_in_fplmn_counter_list() returns 0 for plmn 64 f0 0
NAS KE0/High [ reg_sim_c 2114] =REG= reg_sim_ind_pimin_in_pimin_counter_list() returns 0 for pimin 64 f0 0 NAS REG/High [ reg_sim_c 2114] =REG= reg_sim_find_pimin_in_fpimin_counter_list() returns 0 for pimin 64 f0 0
NAS REG/High [ reg_sim_c 2114] =REG= REG DB search for mcc 0x0
NAS REG/High [ reg_nv.c 441] = REG= REG DB search for mice 0x0
NAS REG/High [ reg_nv.c 441] = REG= REG DB search for micc 0x0 NAS REG/High [ reg_nv.c 441] = REG= REG DB search for micc 0x0
NAS REG/High module request plmp/r#g_nv.c 441] =REG= REG DB search for mcc 0x0
NAS REG/High module request plmn/rate_nv.c 441] = REG= REG DB search for mcc 0x0 NAS REG/High module request plmn/rate_nv.c 441] = REG= REG DB search for mcc 0x0
NAS REG/High is 46000/gsm [ 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_send.c     1718]     =REG=     MMR_REG_REQ_PLMN(460-0)     RAT(GSM)       NAS     REG/High     [     reg_timers.c     1781]     =REG=     Cleared     UPDATE     LTE     CAP
NAS KEU/HIGN [ reg_timers.c 1/8]] = KEG = Cleared UPDATE LTE CAP TIMER

Figure 4: RAT Searching Sequence Determined by RPLMN/RPLMNACT Stored on Module Flash

# 7.3. Long Network Registration Time in Roaming State

### **Problem Description:**

When the module is in roaming state, the network registration time becomes longer, especially when the module powers on for the first time in roaming state or when the module registers to NB-IoT network.

### Roaming State Introduction:

When the PLMN of the module's registered network is not consistent with the HPLMN or EHPLMN of (U)SIM card, the module is in the roaming state. In this case, **<stat>** returned by executing **AT+CREG?/AT+CGREG?/AT+CEREG?** is **5**, which also indicates that the module is in the roaming state.

The behaviour of the module if the (U)SIM card is in roaming state is described in the figure below:

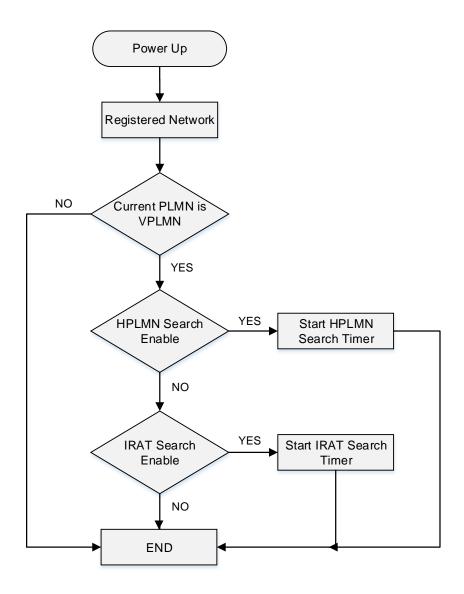


Figure 5: Behaviour of the Module if (U)SIM is Card in Roaming State



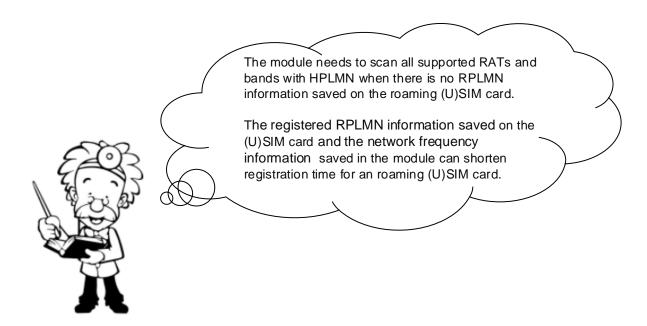
#### **Root Cause Analysis:**

When the module is powered on for the first time with a roaming (U)SIM card, there is no RPLMN information on the (U)SIM card, thus the module needs to scan for high priority PLMN (HPLMN, EHPLMN and so on). It means that the module needs to scan all supported RATs and bands to confirm whether there is any available HPLMN around the cells first. Therefore, the network registration time of the module is always longer when powering on for the first time with a roaming (U)SIM card.

Due to the NB-IoT network characteristics (200 kHz bandwidth), network scanning is much slower (For more details, see *Chapter 6.1*).

For non-initial network registration, the last registered RPLMN information is saved on the (U)SIM card and the last registered network frequency information is saved in the module. It means that the module can find the target network as fast as possible. Therefore, the network registration time of the module is faster for non-initial network registration of a roaming (U)SIM card.

According to 3GPP specification (*3GPP TS 23.122 subclause 4.4.3.3*), the module should attempt to access the HPLMN, EHPLMN or another high priority PLMN (hereinafter referred to as "HPLMN search") with HPLMN search timer when the module is in the roaming state. For BG95 series, BG77 or BG600L-M3 module, when the module is locked to one RAT, HPLMN search process is imperceptible for users, and the ongoing operation will not be affected.



#### **Recommendation:**

- Lock as few as possible RATs and bands to shorten the network searching time.
- Use normal power-down methods (such as executing AT+QPOWD=1, see *document [2]* for details) to power off the module, to make sure the network registration information is saved on the (U)SIM card and the module flash. It is not recommended to disconnect the power supply of the module directly.

# 7.4. Network Registration Request Rejected by Network

### **Problem Description:**

The module's network registration request was rejected.

### **Reject Cause Information Element Introduction:**

The purpose of the reject cause information element is to indicate the reason why a GMM/EMM request from the UE was rejected by the network. The GMM cause information element is defined in *3GPP TS 24.008*, and the EMM cause information element is defined in *3GPP 24.301*. The reject cause is a type 3 information element with the length of 2 octets (see *Figure 6* for GMM cause value and *Figure 7* for EMM cause value).

When the module receives a reject cause code, it means that the module has searched the network, but the registration request was rejected by the network. The network searching sequence of the module complies with the 3GPP specification when the module receives a reject cause code, and the module will always try to search for available networks even if it receives a reject cause code from a certain network.



B	7	6	5	4	3	2	1	
)	0	0	0	0	0	1	0	IMSI unknown in HLR
)	0	0	0	0	0	1	1	Illegal MS
)	0		_	0			1	IMEI not accepted
	0	0	0	0	1	1	0	Illegal ME
	0	0	0	0	1	1	1	GPRS services not allowed
)	0	0	0	1	0	0	0	GPRS services and non-GPRS services not allowed
)	0	0	0	1	0	0	1	MS identity cannot be derived by the network
)	0	0	0	1	0	1	0	Implicitly detached
)	0	0	0	1	0	1	1	PLMN not allowed
)	0	_	0	1	1	0	0	Location Area not allowed
	0	0	_		1	_	1	Roaming not allowed in this location area
	0	0	_	1	1	1	0	GPRS services not allowed in this PLMN
	0	0	-	1	1	1	1	No Suitable Cells In Location Area
	0	0	1		0	0	0	MSC temporarily not reachable
	0	0	1	0	0	0	1 0	Network failure
	0	0	1	-	1	0	1	MAC failure Svnch failure
	0	-	1		1	1	ò	Congestion
	ŏ	0	1	_	1	1	1	GSM authentication unacceptable
	ŏ	ŏ	1	-	ò		1	Not authorized for this CSG
	ŏ	ŏ	1		1		ò	SMS provided via GPRS in this routing area
	ŏ	1	ò		ò	~	ŏ	No PDP context activated
	õ		1		õ	_	ŏ	}
	-		t	0	-	-	-	} retry upon entry into a new cell
)	0	1	1	1	1	1	1	}
	1	0	1	1	1	1	1	Semantically incorrect message
	1	1	0	0	0	0	0	Invalid mandatory information
	1	1	_	_	0	0	1	Message type non-existent or not implemented
	1	1	0	0	0	1	0	Message type not compatible with the protocol
	1	1	0	0	0	1	1	state Information element non-existent or not
			U	0	U		1.1	implemented
	1	1	0	0	1	0	0	Conditional IE error
	1	1	ŏ	ŏ	1	ŏ	1	Message not compatible with the protocol state
	1	1		1			1	Protocol error, unspecified
								e mobile station shall be treated as 0110 1111, "Proto

### Table 10.5.147/3GPP TS 24.008: GMM cause information element

Figure 6: GMM Cause Information Element

The listed reject cause values are defined in annex G.

NOTE:





Bit	-	-	-		_	_		
8 0	7 0	6 0	5 0			2	1 0	IMSI unknown in HSS
0	0	-	-	0	-	1	1	Illegal UE
0	ő		-	ő	-		1	IMEI not accepted
0	0				1	1	ò	Illegal ME
õ	ŏ	ŏ	-		÷	÷	1	EPS services not allowed
ŏ	ŏ	-	ŏ	1	ò	ò	ò	EPS services and non-EPS services not allowed
0	ŏ	ŏ	ŏ	÷	-	ŏ	1	UE identity cannot be derived by the network
ŏ	ŏ	ŏ	ŏ	÷	ŏ	ĭ	ò	Implicitly detached
ŏ	ŏ	ŏ	ŏ	÷	ŏ	÷	1	PLMN not allowed
õ	ŏ	-	ŏ	÷	1	ò	ò	Tracking Area not allowed
õ	õ	õ	õ	1	1	õ	1	Roaming not allowed in this tracking area
õ	ŏ	ŏ	ŏ	1	1	1	ó	EPS services not allowed in this PLMN
0	0	0	0	1	1	1	1	No Suitable Cells In tracking area
0	0	0	1	0	0	0	0	MSC temporarily not reachable
0	0	0	1	0	0	0	1	Network failure
0	0	0	1	0	0	1	0	CS domain not available
0	0	0	1	0	0	1	1	ESM failure
0	0	0	1	0	1	0	0	MAC failure
0	0	0	1	0	1	0	1	Synch failure
0	0	0	1	0	1	1	0	Congestion
0	0	0	1	0	1	1	1	UE security capabilities mismatch
0	0	0	1	1		-	0	Security mode rejected, unspecified
0	0	0	1	1	-	0	1	Not authorized for this CSG
0	0	0	1	1	-	1	0	Non-EPS authentication unacceptable
0	0	1	0	0	0	1	1	Requested service option not authorized in this PLMN
0	0	1	0	0	1	1	1	CS service temporarily not available
0	0	1	0	1	0	0	0	No EPS bearer context activated
0	0	1	0	1	0	1	0	Severe network failure
0	1	-	1			1		Semantically incorrect message
0	1	1	-	0	-	-	-	Invalid mandatory information
0	1	1	-				1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	-		1	0	1	Message not compatible with the protocol state
0	1	1	0	1	1	1	1	Protocol error, unspecified
err	or, I	uns	pec	ified	1". A	١ny		mobile station shall be treated as 0110 1111, "protoco lue received by the network shall be treated as 0110

Figure 7: EMM Cause Information Element

# Example Analysis:

When the module receives a reject cause code from the network, it means that the module has searched the network and initiated an attach request.

Then the module starts the T3247 timer, which is a random value ranging from 30 minutes to 60 minutes. After the timer expires, the module initiates network registration again on the PLMN, as illustrated in the figure below.



Туре	Time Stamp	Name	Summary	SubID Payload IW Time Stam: ProcID Source
TA LOG	00:27:25.080021	BCCH_DL_SCH / SystemInformation	Radio Bearer ID: 0, Freq: 6300, SFN: 0	0x100060006000
ITA LOG	00:27:25.525337 00:27:25.526142	BCCH_DL_SCH / SystemInformationBlockType1 BCCH DL SCH / SystemInformation	Radio Bearer ID: 0, Freq: 1850, SFN: 602 Radio Bearer ID: 0, Freq: 1850, SFN: 0	0x100041004100The module selects PLMN 46011
A LOG	00:27:25.584007	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg	✓ 0x10006c00to send attach request.
ALOG	00:27:25.585014	UL CCCH / RRCConnectionRequest	Radio Bearer ID: 0, Freq: 1850, SFN: 0	0x100027002700
TA LOG	00:27:25.648004	DL_CCCH / RRCConnectionSetup	Radio Bearer ID: 0, Freq: 1850, SFN: 614	0x10004e004e00
TA LOG	00:27:25.653008	UL_DCCH / RRCConnectionSetupComplete	Radio Bearer ID: 1, Freq: 1850, SFN: 0	0x10007300730Attach request is rejected and the re
TA LOG	00:27:25.689044	DL DCCH / DLInformationTransfer	Radio Bearer ID: 1, Freq: 1850, SFN: 618	0x100027002700
ia log		LTE NAS EMM Plain OTA Incoming Message	Attach reject Msg	A then the module second is 14, then the module second is 14.
A LOG A LOG	00:27:25.690006	DL_DCCH / RRCConnectionRelease	Radio Bearer ID: 1, Freq: 1850, SFN: 619	0x100023002300 0x10003b003b0.3247 timer and the timer value is
A LOG	00:27:25.999266 00:27:26.000008	BCCH_DL_SCH / SystemInformationBlockTypeT BCCH_DL_SCH / SystemInformation	Radio Bearer ID: U, Freq: 6300, SFN: 248 Radio Bearer ID: 0, Freq: 6300, SFN: 0	0x10005000600pandom from 30 to 60 minutes.
A LOG	00:27:26.060015	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg	
A LOG	00:27:26.061005	UL_CCCH / KKCConnectionKequest	Kadio Bearer ID: 0, Freq: 6300, SFN: 0	0x100027002700
A LOG	00:27:26.127030	DL_CCCH / RRCConnectionSetup	Radio Bearer ID: 0, Freq: 6300, SFN: 261	a topotogo I he module uses another available
A LOG	00:27:26.132044	UL_DCCH / RRCConnectionSetupComplete	Radio Bearer ID: 1, Freq: 6300, SFN: 0	0x10002a00PLMN 24601 to send attach reque
A LOG	00:27:26.184028	DL_DCCH / DLInformationTransfer	Radio Bearer ID: 1, Freq: 6300, SFN: 267	0x10002a002a00
	00:27:26.184028	LTE NAS EMM Plain OTA Incoming Message		0x100016001600.and set T3410 timer, the timer val
A LOG	00:27:26.209165	DL_DCCH / RRCConnectionRelease	Radio Bearer ID: 1, Freq: 6300, SFN: 269 Radio Bearer ID: 0, Freq: 6300, SEN: 276	0x100023002300is 10 seconds.
A LOG A LOG	00:27:36.185010			0x1000360036010 10 000011003.
A LOG	00:27:36.185010	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg	0×10005c00 0×100027002700
A LOG	00:27:36.247087	DL_CCCH / RRCConnectionSetup	Radio Bearer ID: 0, Freq: 0300, 3FN: 0 Radio Bearer ID: 0, Freq: 6300, SFN: 249	0x100027002700 0x100048004800
A LOG	00:27:36.250022	UL_DCCH / RRCConnectionSetupComplete	Radio Bearer ID: 1, Freq: 6300, SFN: 0	0x100073007300
A LOG	00:27:36.304065	DL_DCCH / DLInformationTransfer	Radio Bearer ID: 1, Freq: 6300, SFN: 255	0x10092a002a00
	00:27:36.305053	LTE NAS EMM Plain OTA Incoming Message	Attach reject Msg	
A LOG	00:27:36.330024	DL_DCCH / RRCConnectionRelease	Radio Bearer ID: 1, Freq: 6300, SFN: 257	0x100016054600 0x100023002300 If the attach request is still
A LOG	00:27:36.399152	BCCH DL SCH / SystemInformationBlockType1	Radio Bearer ID: 0. Freq: 6300. SFN: 264	0x10003b00 rejected, it will be sent again even
	00:27:46.306002	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg	<ul> <li>In the definition request to stall response to stall</li></ul>
A LOG	00:27:46.306002	UL_CCCH / RRCConnectionRequest	Radio Bearer ID: 0, Freq: 6300, SFN: 0	- <sub>0x100027002700</sub> , 10 seconds, 4 times to retry, and
A LOG A LOG	00:27:46.367057 00:27:46.370014	DL_CCCH / RRCConnectionSetup	Radio Bearer ID: 0, Freq: 6300, SFN: 237	<sup>0x100048004800</sup> 5 attempts in total.
A LOG	00:27:46.423019	UL_DCCH / RRCConnectionSetupComplete DL DCCH / DLInformationTransfer	Radio Bearer ID: 1, Freq: 6300, SFN: 0 Radio Bearer ID: 1, Freq: 6300, SFN: 243	0,1002,002,00
A LOG	00:27:46.423013	LTE NAS EMM Plain OTA Incoming Message	Attach reject Msg	0x100028002800
A LOG	00:27:46.457167	DL_DCCH / RRCConnectionRelease	Radio Bearer ID: 1, Freq: 6300, SFN: 246	0x100016001600 0y100023002300
LOG	00:27:46.519108	BCCH DL SCH / SystemInformationBlockType1	Radio Bearer ID: 0, Freq: 6300, SFN: 252	x10003b003b0
	00:27:56.425015	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg	0x10005c005c00
A LOG	00:27:56.425015	UL_CCCH / RRCConnectionRequest	Radio Bearer ID: 0, Freq: 6300, SFN: 0	0x100027002700
A LOG	00:27:56.487077	DL_CCCH / RRCConnectionSetup	Radio Bearer ID: 0, Freq: 6300, SFN: 225	0x100048004800
A LOG	00:27:56.490026	UL_DCCH / RRCConnectionSetupComplete	Radio Bearer ID: 1, Freq: 6300, SFN: 0	0x100073007300
A LOG	00:27:56.544013	DL_DCCH / DLInformationTransfer	Radio Bearer ID: 1, Freq: 6300, SFN: 231	0x10002a002a00
A LOG A LOG	00:27:56.544013 00:27:56.570086	LTE NAS EMM Plain OTA Incoming Message DL DCCH / RRCConnectionRelease	Attach reject Msg Radio Bearer ID: 1, Freq: 6300, SFN: 233	0x100016001.600 0x100023002300
A LOG A LOG	00:27:56 639208	BCCH DL_SCH / SystemInformationBlockType1	Radio Bearer ID: 1, Freq: 6300, SEN: 233 Radio Rearer ID: 0, Freq: 6300, SEN: 240	0x100023002300
LOG	00:28:06.545007	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg	0x10005c005c00
A LOG	00:28:06.545007	UL_CCCH / RRCConnectionRequest	Radio Bearer ID: 0, Freq: 6300, SFN: 0	0x100027002700
A LOG		DL_CCCH / RRCConnectionSetup	Radio Bearer ID: 0, Freq: 6300, SFN: 213	0x100048004800
	00.29.05 512047	III DCCH / PPCConnectionSetupComplete	Padio Pearer ID: 1 Freque 6200 SENI: 0	0~100072007200
00 EC 80	15 2D C7 16	14 00 00 00ì°C	re	el version major = 5 (0x5)
44 OE	10 22 07 10	D.		el_version_minor = 0 (0x0)
				ecurity_header_or_skip_ind = 0 (0x0)
				rot_disc = 7 (0x7) (EPS mobility management messages)
				sg_type = 68 (0x44) (Attach reject)
				te_emm_msg
				emm_attach_reject
				<pre>cause_value = 14 (0xe) (EPS services not allowed in this PL</pre>
				esm msg container incl = 0 $(0x0)$

# Figure 8: Module Received Reject Cause Code

00:27:25.690000	NAS MM/High NAS MM/High	[emm_utility.c 4083] = EMM= sent NW REJ EVT to GSTK [emm_undate_linc_2610] = EMM= Received attach reject is a plain msgr [mmtimets.c 395] = MM= Random timeout for TIMER T3247 - 2040/	According to 3GPP, the modul
00:27:25.690000	NAS MM/High		
00:27:25.690000	NAS MM/High NAS MM/High	[ mmtimers.c 580] =MM= Start 92, timeout 2040:0 [ emm_utility.c 12003] =EMM= emm_check_if_sec_attack_mitigation_poss [ emm_utility.c 272] =EMM= Cause - Value = 14	receiving reject cause code #1
00:27:25 600000	NAS MM/High	emm ifflific ///L-FM/K/- Laifs - Valite - I/	
Time Stamp	Name	Summary	The module tries to searc
00:27:25.693985	Data Services/High	[ ds_pdn_manager.c 1136] ds_3gpp_pdn_mgr_handle_bearer_down_ind	The module tries to searc <sup>§</sup> P <sup>bID</sup> and register another
00:27:25.693985 00:27:25.693985	Data Services/High NAS REG/High	[ds_pdn_manager.c 1136] ds_3gpp_pdn_mgr_handle_bearer_down_ind [reg_send.c 1665] =REG= grat_scan_status: 0	and register another
00:27:25.693985	Data Services/High	[ ds_pdn_manager.c 1136] ds_3gpp_pdn_mgr_handle_bearer_down_ind	
00:27:25.693985 00:27:25.693985	Data Services/High NAS REG/High	[ds_pdn_manager.c 1136] ds_3gpp_pdn_mgr_handle_bearer_down_ind [reg_send.c 1665] =REG= grat_scan_status: 0	and register another available network.
00:27:25.693985 00:27:25.693985 00:27:25.693985	Data Services/High NAS REG/High NAS MM/High	[ds_pdn_manager.c 1136] ds_3gpp_pdn_mgr_handle_bearer_down_ind [reg_send.c 1665] =REG= grat_scan_status: 0 [mmtask.c 3401] =MM= Message Set= 10 Message Id= 193	and register another available network.
00:27:25.693985 00:27:25.693985 00:27:25.693985	Data Services/High NAS REG/High NAS MM/High	[ds_pdn_manager.c 1136] ds_3gpp_pdn_mgr_handle_bearer_down_ind [reg_send.c 1665] =REG= grat_scan_status: 0 [mmtask.c 3401] =MM= Message Set= 10 Message Id= 193 [reg_send.c 1685] =REG= Scan Info New scan 1, use_timer=0, scan_t	and register another available network.
00:27:25.693985 00:27:25.693985 00:27:25.693985 00:27:25.693985 00:27:25.693985 00:27:25.693985	Data Services/High NAS REG/High NAS MM/High NAS REG/High NAS REG/High	[ds_pdn_manager.c         1136]         ds_3gpp_pdn_mgr_handle_bearer_down_ind           [reg_send.c         1665]         =REG=         grat_scan_status: 0           [mmtask.c         3401]         =MM=         Message Set=         10         Message         Id=         193           [reg_send.c         1665]         =REG=         Scan Info         New scan         1, use_timer=0, scant         reg_send.c         10486]         -REG=         TRM timewit set to 0xffffffffffffffffffffffffffffffffffff	and register another available network.
00;27:25.693985 00;27:25.693985 00;27:25.693985 00;27:25.693985 00;27:25.693985 00;27:25.693985	Data Services/High NAS REG/High NAS REG/High NAS REG/High NAS REG/High NAS REG/High	[ ds_pdn_manager.c     1136] ds_3gpp_pdn_mgr_handle_bearer_down_ind       [ reg_send.c     1665] =REG= grat_scan_status: 0       [ mmtask.c     3401] =MM= Message Set= 10 Message Id= 193       [ reg_send.c     1685] =REG= Scan Info New scan 1, use timer=0, scant       [ reg_mode_c     1486] =REG= TRM timeout set no./Kiffffff sec       [ reg_send.c     1873] =REG= MMR_REG_REQ_PLMN(246-1) RAT(LTE_M1)	and register another available network.

Figure 9: Module Initiated T3247 Timer and Tried to Register Another Available Network

# 7.5. Long Network Registration Time if AT Commands are Executed

# Frequently

### **Problem Description:**

During the network searching progress, the network registration time becomes longer if some network-searching commands are executed frequently.

### **Root Cause Analysis:**

Executing a network-searching command (see *Chapter 5* for more information) immediately triggers a one-time network search even if network searching is already in progress. Therefore, frequent executing of network-searching commands may cause longer network registration time.

#### **Recommendation:**

Before executing any network-searching command, it is recommended to check whether the current network configuration of the module is the desired one. If it is, there is no need to reset the network configuration.

### Example

AT+QCFG="nwscanmode" +QCFG: "nwscanmode",3	<pre>//Query the current RAT(s) allowed to be searched for. //The module only searches for LTE bands.</pre>
OK AT+QCFG="nwscanmode",1 OK	//Change the network configuration if it is not the desired one.

QUECTEL



- 1. Q: How does the module search for the network in OOS (Out of Service) state?
  - A: When the module is in OOS (Out of Service) state, it will always periodically try to search for available networks, as shown in the figure below.

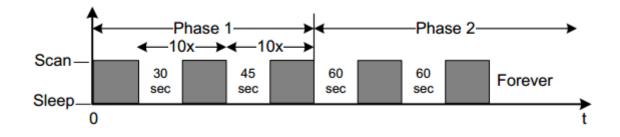


Figure 10: Restore the Network Information

### Phase 1

a) Sleep for 30 seconds

i. Attempt acquisition of full service and then limited service on the GSM and LTE acquisition list. ii. Go back to step a. and repeat 10 times.

b) Sleep for 45 seconds

i. Attempt acquisition of full service and then limited service on the GSM and LTE acquisition list.

ii. Go back to step b. and repeat 10 times.

### Phase 2

c) Sleep for 60 seconds

i. Attempt acquisition of full service and then limited service on the GSM and LTE acquisition list.

- ii. Go back to step c. and repeats continuously until a service is found.
- 2. Q: How to clear the registration information history of the module?

**A:** a) If you want to clear the historical frequency information stored in the module, you can execute the following commands:

- AT+QNVFD="/nv/item\_files/modem/geran/grr/acq\_db" under GSM.
- AT+QNVFD="/nv/reg\_files/modem/lte/rrc/csp/acq\_db" under LTE (eMTC and NB-IoT).
- AT+QNVFD="/nv/reg\_files/modem/nb1/rrc/csp/acq\_db" under NB-IoT.
- b) If you want to clear RPLMN information stored on (U)SIM card, you can execute the following commands:



# **9** Summary of CME ERROR Codes

Final result code **+CME ERROR: <err>** indicates an error related to mobile equipment or network. The operation is similar to **ERROR** result code.

<err> values are mostly used by common message commands. The following table lists most of general and GPRS related **ERROR** codes. For some GSM protocol failure causes described in GSM specifications, the corresponding **ERROR** codes are not included.

<err></err>	Meaning
0	Phone failure
1	No connection to phone
2	Phone-adaptor link reserved
3	Operation not allowed
4	Operation not supported
5	PH-SIM PIN required
6	PH-FSIM PIN required
7	PH-FSIM PUK required
10	(U)SIM not inserted
11	(U)SIM PIN required
12	(U)SIM PUK required
13	(U)SIM failure
14	(U)SIM busy
15	(U)SIM wrong

### Table 1: Summary of CME ERROR Codes

16	Incorrect password
17	(U)SIM PIN2 required
18	(U)SIM PUK2 required
20	Memory full
21	Invalid index
22	Not found
23	Memory failure
24	Text string too long
25	Invalid characters in text string
26	Dial string too long
27	Invalid characters in dial string
30	No network service
30 31	No network service Network timeout
31	Network timeout
31 32	Network timeout Network not allowed - emergency calls only
31       32       40	Network timeout Network not allowed - emergency calls only Network personalization PIN required
31       32       40       41	Network timeout         Network not allowed - emergency calls only         Network personalization PIN required         Network personalization PUK required
31       32       40       41       42	Network timeout         Network not allowed - emergency calls only         Network personalization PIN required         Network personalization PUK required         Network subset personalization PIN required
31       32       40       41       42       43	Network timeout         Network not allowed - emergency calls only         Network personalization PIN required         Network personalization PUK required         Network subset personalization PIN required         Network subset personalization PUK required
31         32         40         41         42         43         44	Network timeout         Network not allowed - emergency calls only         Network personalization PIN required         Network personalization PUK required         Network subset personalization PIN required         Network subset personalization PUK required         Service provider personalization PIN required
31         32         40         41         42         43         44         45	Network timeoutNetwork not allowed - emergency calls onlyNetwork personalization PIN requiredNetwork personalization PUK requiredNetwork subset personalization PIN requiredNetwork subset personalization PUK requiredService provider personalization PIN requiredService provider personalization PUK requiredService provider personalization PUK required



# **10** Appendix References

#### **Table 9: Related Documents**

#### **Document Name**

- [1] Quectel\_BG95\_LPWA\_Specification
- [2] Quectel\_BG95&BG77&BG600L\_Series\_AT\_Commands\_Manual
- [3] Quectel\_BG95&BG77&BG600L\_Series\_QCFG\_AT\_Commands\_Manual

#### Table 10: Terms and Abbreviations

Abbreviation	Description
(U)SIM	(Universal) Subscriber Identity Module
3GPP	3rd Generation Partnership Project
ARFCN	Absolute Radio Frequency Channel Number
CS	Circuit Switching Domain
CSG	Closed Subscriber Group
EARFCN	E-UTRA Absolute Radio Frequency Channel Number
EF	Elementary File
EFS	Encrypt File System
EGPRS	Enhanced General Packet Radio Service
EHPLMN	Equivalent Home PLMN
EMM	EPS Mobility Management
eMTC	Enhanced Machine Type Communication
EPS	Evolved Packet System

EPSLOCI	EPS Location Information
ESM	EPS Session Management
GMM	GPRS Mobility Management
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
IE	Information Element
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IRAT	Inter-RAT
LOCI	Location Information
LTE	Long Term Evolution
MAC	Medium Access Control
ME	Mobile Equipment
MIB	Master Information Block
MS	Mobile Station
MSC	Mobile Switching Center
NB-IoT	Narrow Band Internet of Things
NV	Non-volatile Flash Memory
NVM	Non-Volatile Memory
PCI	Peripheral Component Interconnect
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PS	Packet Switching Domain
PSLOCI	Packet Switch Location Information

RAT	Radio Access Technology
RPLMN	Registered Public Land Mobile Network
RRC	Radio Resource Control
SIB	System Information Block
SNR	Signal Noise Ratio
UE	User Equipment
VPLMN	Visiting Public Land Mobile Network