BG96&BG95&BG77&BG600L Series Network Application Note

LPWA Module Series

Version: 1.0

Date: 2024-04-30

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@quectel.com

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

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

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.

About the Document

Revision History

Version	Date	Author	Description
-	2024-04-30	Linkin WANG	Creation of the document
1.0	2024-04-30	Linkin WANG	First official release

Contents

Table Index

Figure Index

1 Introduction

This document describes the network registration process of Quectel BG96, BG95 series, BG77 and BG600L-M3 modules.

1.1. Applicable Modules

Table 1: Applicable Modules

Module Family	Module
-	BG96
-	BG95 Series
-	BG77
-	BG600L-M3

NOTE

For details about the AT commands mentioned in this document, please refer to *document [1]*, *[2]* and *[3]* for BG95 series, BG77 and BG600L-M3 modules, and *document [4]* and *[5]* for BG96 module.
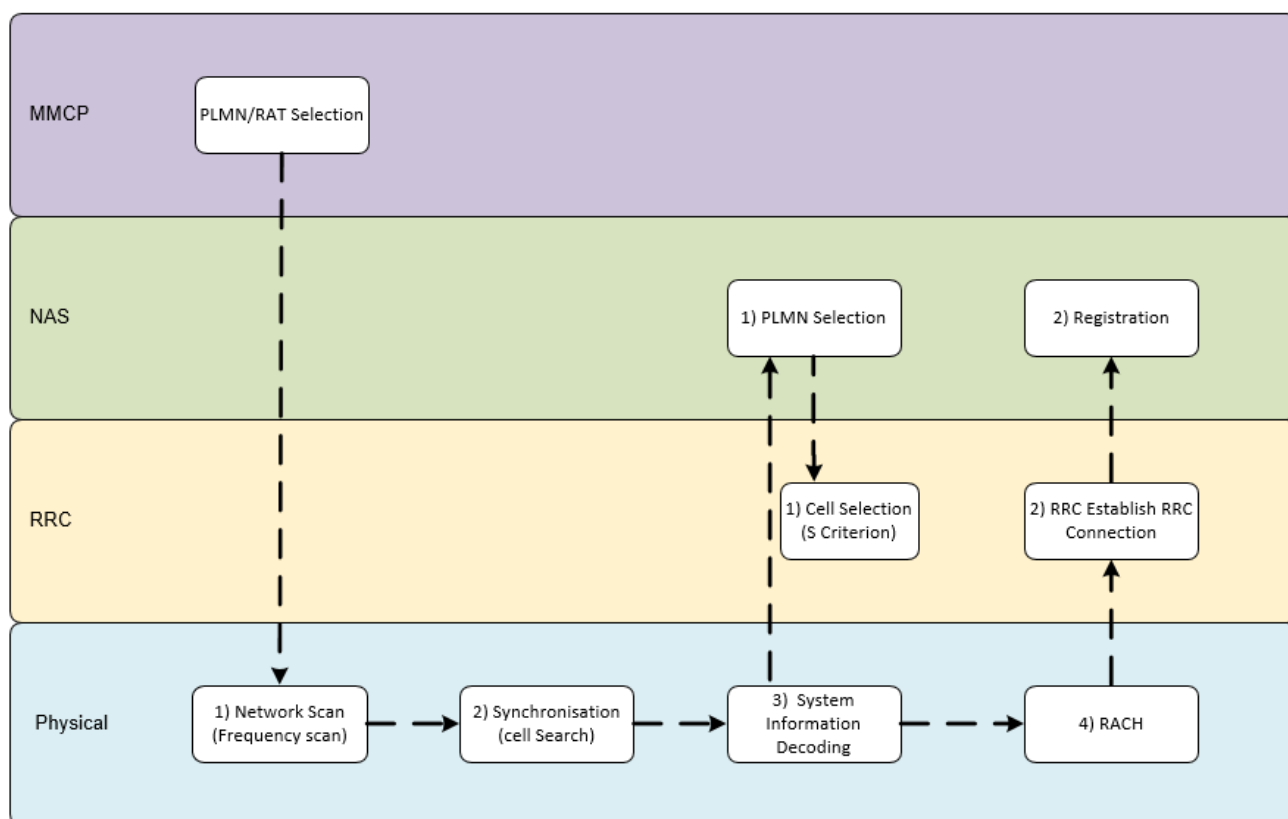
2 Network Registration Overview

Figure 1: Network Registration Overview

3 UE Initialization

UE initializes the (U)SIM files and NV files after powering up.

The (U)SIM information contains the following items (please refer to *3GPP TS 31.102* for more details) used to prioritize the PLMN.

1. *EFHPLMNwAcT*: HPLMN selector with access technology, indicating the priority of the Home PLMN and the Home PLMN access system. The file type is defined in the figure below.

EF_HPLMNwAcT (HPLMN selector with Access Technology)

Identifier: '6F62'	Structure: Transparent	Optional
SFI: '13'		
File size: 5n (n ≥ 1) bytes	Update activity: low	

Access Conditions:
READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length	
1 to 3	1st PLMN (highest priority)	M	3 bytes	MCC+MNC
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes	
6 to 8	2nd PLMN	O	3 bytes	
9 to 10	2nd PLMN Access Technology Identifier	O	2 bytes	
⋮	⋮			
(5n-4) to (5n-2)	nth PLMN (lowest priority)	O	3 bytes	
(5n-1) to 5n	nth PLMN Access Technology Identifier	O	2 bytes	

- PLMN

Contents:
Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

Coding:
according to TS 24.008 [47].

- Access Technology:

Contents: The Access Technology of the HPLMN that the ME will assume when searching for the HPLMN, in priority order. The first Access Technology in the list has the highest priority.

Figure 2: EFHPLMNwAcT File Type

2. *EFOPLMNwAcT*: Operator-controlled PLMN selector with access technology, listing preferred PLMNs and supported access modes determined by the operator.

3. *EFPLMNwAcT*: User-controlled PLMN selector with access technology, indicating user-determined preferred PLMNs and supported access system list.

4. *EFFPLMN*: Forbidden PLMNs, indicating PLMNs where UE will not attempt automatic access.

5. *EFEHPLMN*: Equivalent HPLMN.

6. *EFLRPLMNSI*: The last RPLMN selection after bootup. 1 indicates HPLMN and 0(default) indicates RPLMN. The file type is defined in the figure below.

EF_{LRPLMNSI} (Last RPLMN Selection Indication)

Identifier: '6FDC'		Structure: transparent		Optional
File size: 1 byte		Update activity: low		

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Last RPLMN Selection Indication	M	1 byte

- Last RPLMN Selection Indication:
  Contents:
  Last RPLMN Selection Indication
Coding:
- '00' - The UE shall attempt registration on the last RPLMN at switch-on or recovery from out-of-coverage as described in TS 23.122 [31]
- '01' - The UE shall attempt registration either on the HPLMN or the last RPLMN at switch-on or recovery from out-of-coverage as described in TS 23.122 [31]
- All other values are RFU

Figure 3: EFLRPLMNSI File Type

7. *EFPSLOCI*: Saves the previous P-TMSI, TAI (RPLMN+TAC) and other LTE registration information (2G PS registration information).

8. *EFEPSLOCI*: Saves the previous GUTI, TAI (RPLMN+TAC) and other LTE registration information (LTE PS registration information).

9. *EFLOCI*: Saves the previous TMSI and LAI (RPLMN+LAC) registration information. (2G CS registration information).

4 PLMN/RAT Selection

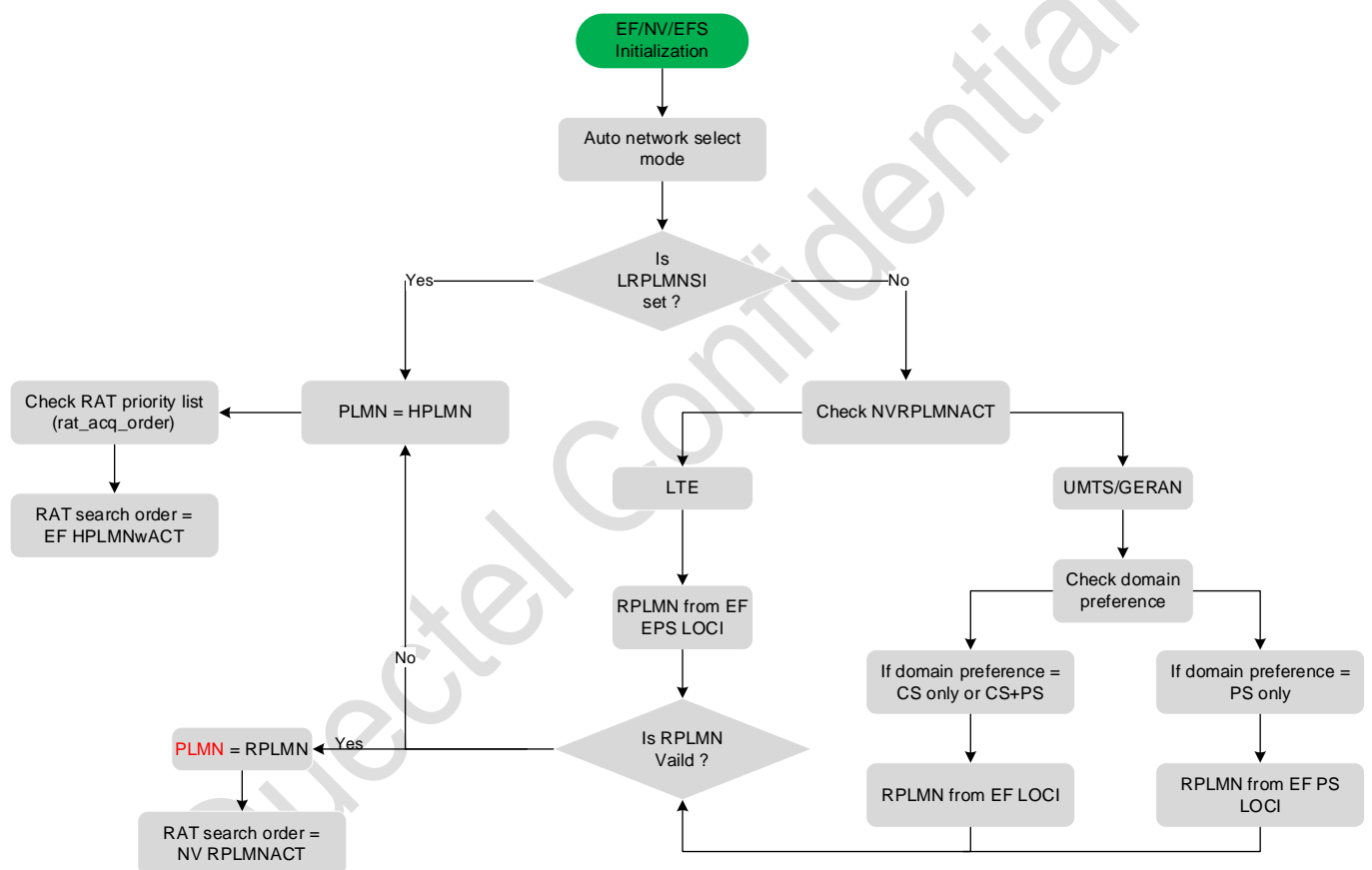## 4.1. PLMN/RAT Selection Overview

Figure 4: PLMN/RAT Selection Overview

4.2. Automatic Selection Mode

The sequence for PLMN selection during search is determined by the module settings (NV parameters) and files in the (U)SIM card, which have higher priority.

The module should select the last registered PLMN (LRPLMN) or an EHPLMN (if available) using all access technologies that the MS is capable of. According to **chapter 4.4.3.1** of *3GPP 23.122 [1]*, if there is no LRPLMN, or if the registration is not possible due to the PLMN being unavailable or registration failure at switch on or recovery from lack of coverage, the UE should attempt to register on other available networks across all available modes, and select networks based on the following order:

a) The HPLMN (if the EHPLMN list is absent or empty) or the highest-priority available EHPLMN (if the EHPLMN list is present);
b) Each PLMN/access technology combination in the "user-controlled PLMN selector with access technology" data file in the (U)SIM file (in priority order);
c) Each PLMN/access technology combination in the "operator-controlled PLMN selector with access technology" data file in the (U)SIM file (in priority order) or stored in the ME (in priority order);
d) Other PLMN/access technology combinations with received high quality signals in random order;
e) Other PLMN/access technology combinations in descending order of signal quality.

4.3. Manual Selection Mode

In manual selection mode, the UE will list all PLMNs, including unavailable PLMNs for users to choose for registration. For more details, please refer to **Chapter 4.4.3.1.2** of *3GPP TS 23.122.*

4.4. Roaming Service

If the UE is located on VPLMN service, it periodically attempts to obtain service on its HPLMN (if the EHPLMN list is absent or empty) or one of its EHPLMNs (if the EHPLMN list is present), or a higher-priority PLMN/access technology combinations listed in "user-controlled PLMN selector" or "operator-controlled PLMN selector" by scanning in accordance with the requirements defined in the Automatic Network Selection Mode in **Chapter 4.4.3.1.1** of *3GPP TS 23.122*.

If the UE has a stored "Equivalent PLMNs" list, it will only select a PLMN if it has a higher priority than those of the same country as the current serving PLMN stored in the "Equivalent PLMNs" list.

Thus, there exists an HPLMN search timer to periodically search for the HPLMN when the UE is located on VPLMN service. Additionally, commands are available to disable the HPLMN search timer to prevent the UE from searching for the HPLMN.

The value of the HPLMN search timer is saved in the (U)SIM file and currently cannot be changed by the UE via AT commands. For more details, please refer to FAQs in *Chapter 8*.

Moreover, commands such as **AT+QCFG** and **AT+COPS=?** can trigger HPLMN search when the UE is located on VPLMN service and it is recommended to reset or execute **AT+CFUN=0/AT+CFUN=1** after sending these commands. It is suggested to perform these commands after RF is turned off (that is, **AT+CFUN=0**), and these commands will be saved to the NV, eliminating the need to execute them every cycle in your MCU code.
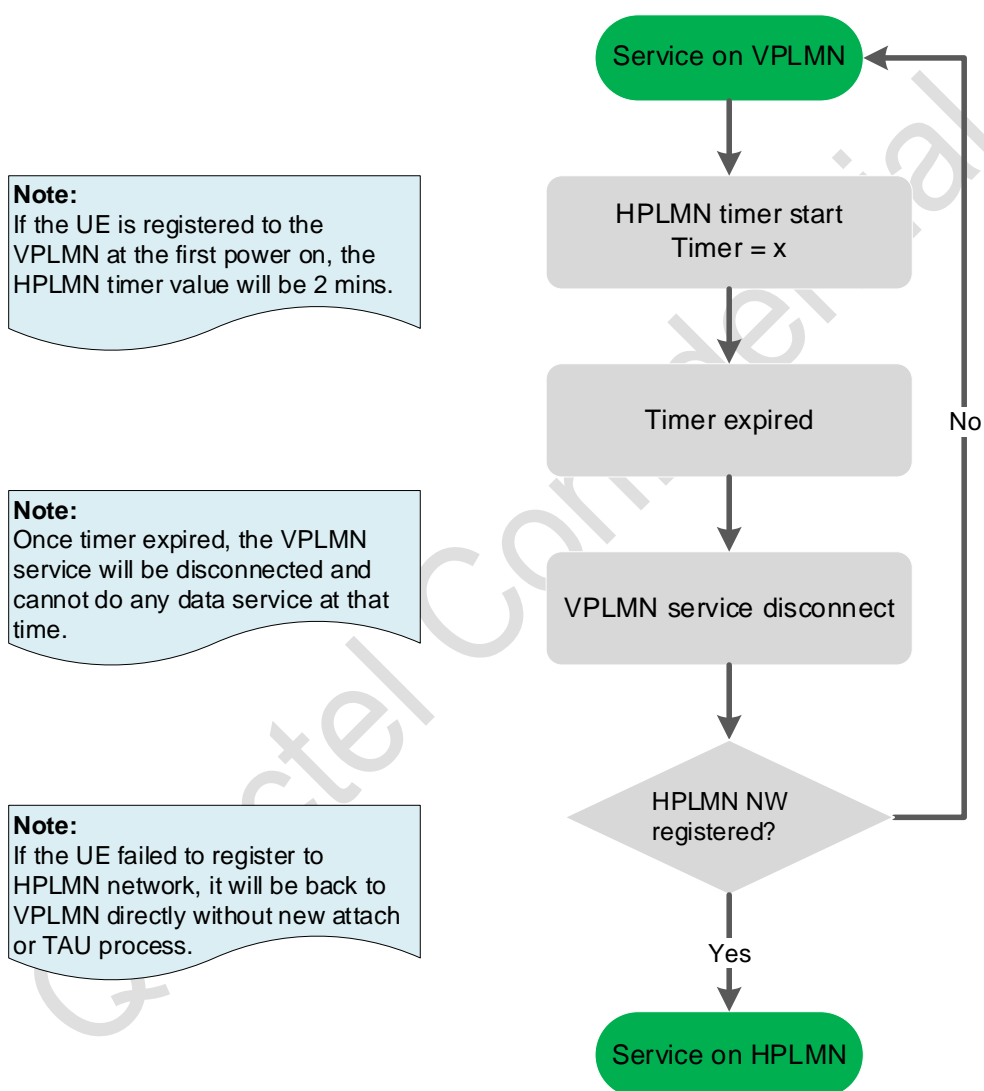

Note:
If the UE is registered to the VPLMN at the first power on, the HPLMN timer value will be 2 mins.

Note:
Once timer expired, the VPLMN service will be disconnected and cannot do any data service at that time.

Note:
If the UE failed to register to HPLMN network, it will be back to VPLMN directly without new attach or TAU process.

Figure 5: Roaming Service

4.5. RAT Selection

When considering the RAT selection, it's important to be aware of the SIM card RAT order. Typically, the SIM card has no RAT order configuration but not for all SIM provider. For example, some providers define an initial RAT priority in their SIM configurations (LTE>NB-IoT>GSM), and this priority takes precedence over configurations set via **AT+QCFG="nwscanseq"**.

Thus, when a SIM card RAT order is configured, RAT selection follows the SIM configuration rather than AT commands. This function can be disabled through AT command, please refer to FAQs in *Chapter 8* for details.
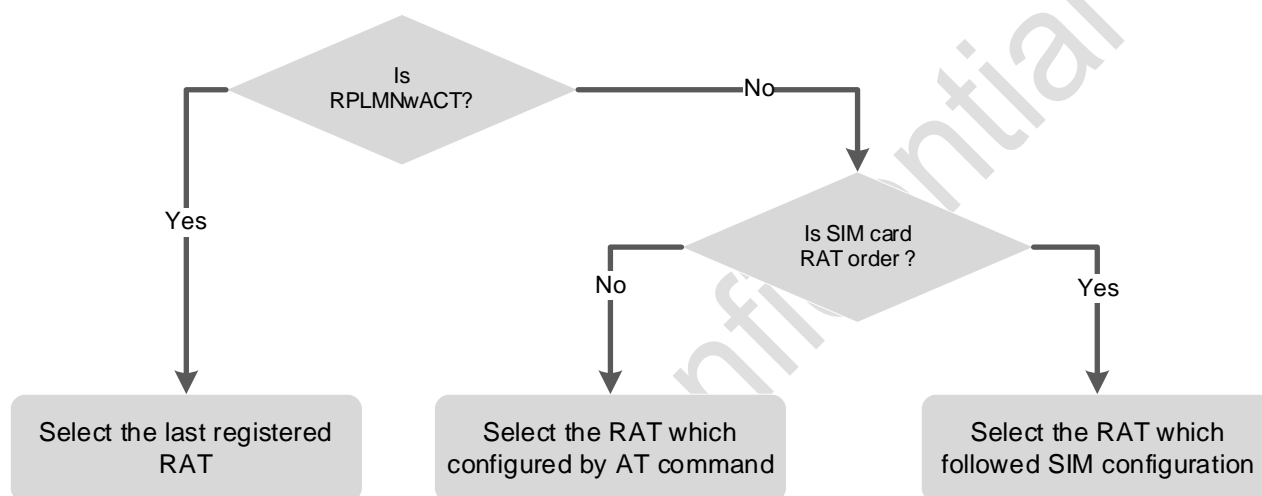
Figure 6: RAT Selection

a) Upon module bootup, the UE reads SIM/NV files to select the last registered RAT.
b) If there is no RPLMNwACT and SIM card RAT order existed and enabled, the UE will select the RAT saved in the SIM configuration.
c) If the SIM card RAT order is disabled, the UE will select the RAT configured by AT command.
d) If a suitable frequency cannot be found in the higher RAT, the UE will switch to the secondary RAT until a suitable frequency is found.
e) If the UE registers on a network that is not the highest priority RAT network, an IRAT timer starts, with a default value of 60 minutes. Once the timer expires, the UE attempts to re-search the network on the highest priority RAT. (The IRAT timer duration can be configured using a command, see FAQs in *Chapter 8* for details)

NOTE

RPLMNwACT refers to the last registered RAT, saved in NV. For information on when RPLMNwACT is saved to NV, please refer to FAQs in *Chapter 8*.

---

5 Frequency Scan

There are two modes for frequency scanning: system scan and band scan.

5.1. System Scan

UE will start with system scan. A system scan involves the UE scanning historical frequencies saved in NV files, with a maximum of 10 frequencies saved. Additionally, **AT+QNWCFG="acqdb"** is supported to query historical frequencies.
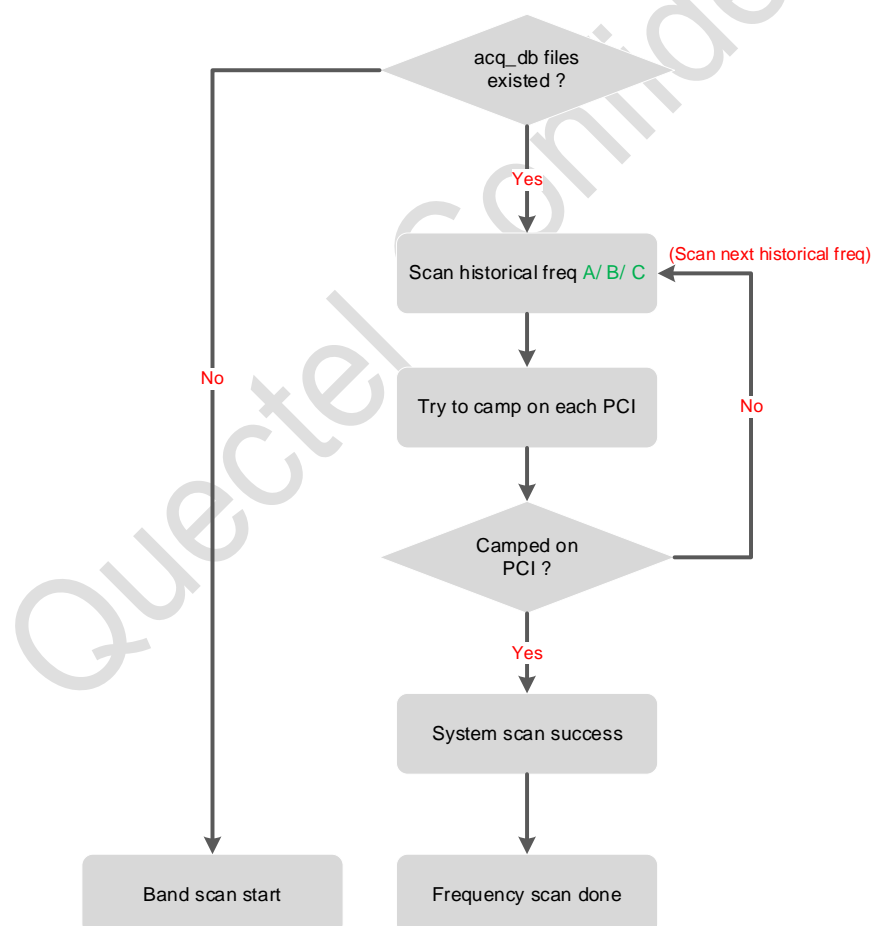

Figure 7: System Scan

5.2. Band Scan

When the system scan is finished and no available frequency is acquired, the UE starts a band scan. In the band scan, the UE lists all supported bands (generally starting from Band 1) and scans frequencies on each band (each band lists no more than 30 frequencies, ordered by RSSI from high to low). The band scan continues until a suitable frequency is found, at which point it stops.
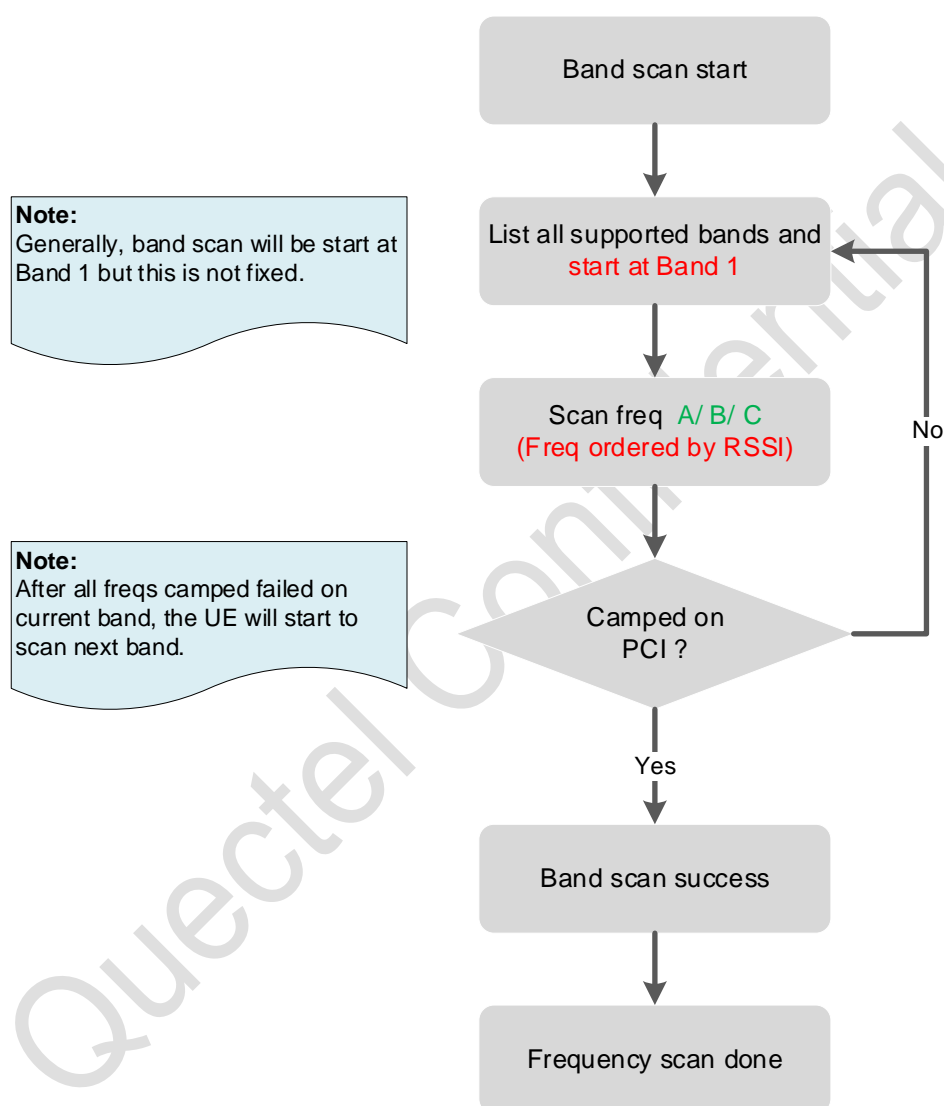

Figure 8: Band Scan

5.3. Out of Service (OOS)

After scanning all frequencies supported by RATs but no available frequency is discovered, the UE will enter OOS status. Simultaneously, the UE will start a timer to initiate a periodic frequency scan, during timer's lifetime UE do not scan. Please see the figure below:
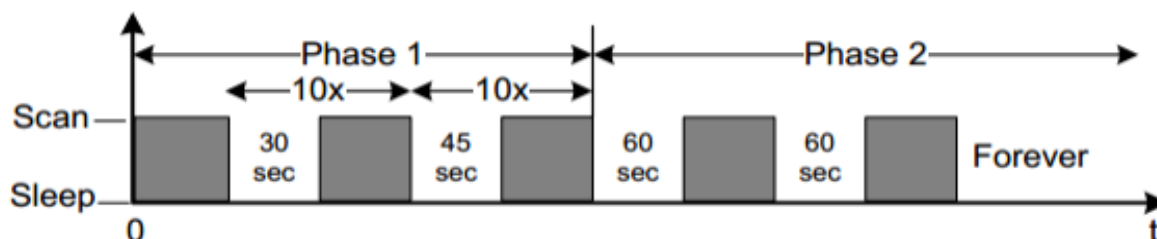

Figure 9: OOS Scan

Phase 1:
a) Timer lifetime set at 30 seconds
   1) Attempt to acquire full service on the GSM and LTE acquisition list.
   2) Go back to step a) and repeat 10 times.
b) Timer lifetime set at 45 seconds
   1) Attempt to acquire full service on the GSM and LTE acquisition list.
   2) Go back to step b) and repeat 10 times.

Phase 2:
c) Timer lifetime set at 60 seconds
   1) Attempt to acquire full service on the GSM and LTE acquisition list.
   2) Go back to step c) and repeat continuously until a service is found.

NOTE

For BG95 series module, the step a) of phase 1 should be repeated 20 times.

6 Cell Selection

6.1. Cell Searching

LTE cell search is actually PSS (Primary Synchronization Signal) and SSS (Secondary Synchronization Signal) synchronization, enabling UE cell identification and downlink synchronization. In this way, the UE can receive the MIB and SIB messages broadcasted by the cell, stay at the cell and use various services provided by the network.

The cell searching process is as follows:

1. The UE performs a cell search and selects the most suitable cell for camping. The selection is based on the synchronization signal PSS/SSS sent by the eNodeB (cell) every 5 milliseconds. Through PSS/SSS, the UE achieves time and frequency synchronization with the cell, and obtains the PCI of the cell.

2. After determining the communication cell, the UE needs to obtain cell information for proper operation. The cell continuously sends system information (MIB/SIB) related to itself, and the UE will obtain the information when needed.
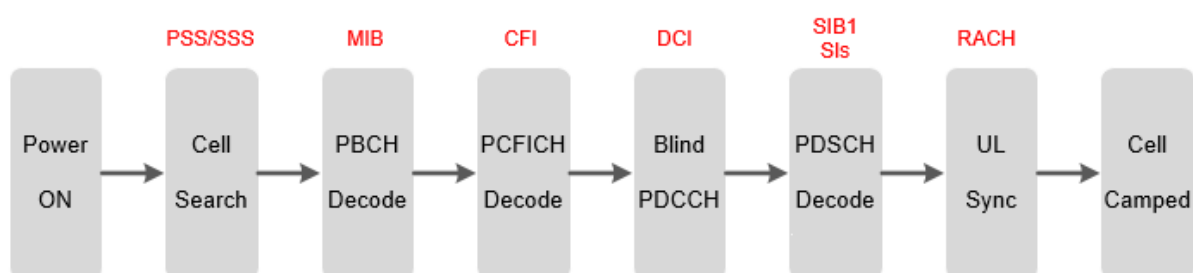

Figure 10: Cell Searching

The purpose of cell searching:

a) Detect physical cell ID.
   1) Obtain the cell ID through PSS and SSS detection.
b) Achieve time/frequency synchronization.
   1) 10-millisecond frame synchronization;
   2) Synchronization with eNodeB carrier frequency.
c) Detect the number of transmit antennas used by eNodeB.
d) Decode MIB.
   1) Obtain SFN;
   2) Obtain downlink bandwidth;
   3) Obtain PHICH configuration information
e) Read PDSCH and decode SIB message.

6.2. SIB/MIB Decoding

System message parsing primarily involves reading MIB (Master Information Block) and SIB (System Information Block) messages. For detailed definitions, please refer to **Chapter 5.2** of *3GPP TS 36.331*.

The MIB message contains information such as the number of antennas, downlink bandwidth, cell ID, frequency.

The SIB message contains PLMN, PCI (Physical Cell ID), Q-RxlevMin (use for S criterion), etc.
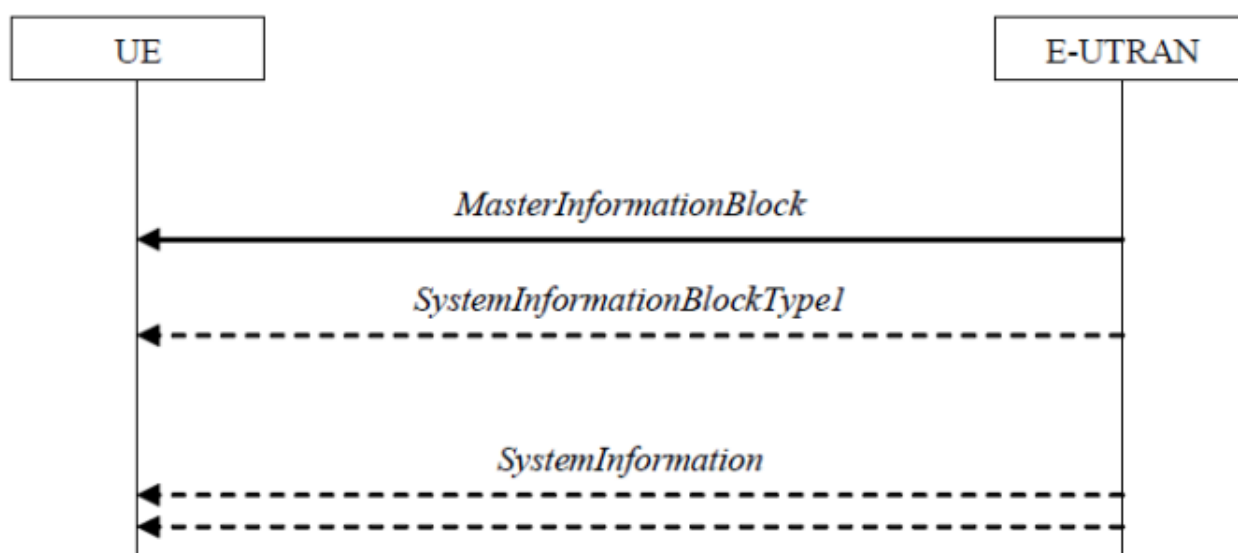

Figure 11: SIB/MIB Decoding

6.3. Cell Selection

The cell selection process involves validating the S (select) criterion. For more details, please refer to **Chapter 5.2** of *3GPP TS 36.304* (Cell selection and reselection) and **Chapter 5.2.4.6** of *3GPP TS 36.304* (Intra-frequency and equal priority inter-frequency Cell Reselection criteria).

$$Squal = Q_{qualmeas} - Qqualmin$$

$$Srxlev = Q_{rxlevmeas} - Qrxlevmin - Pcompensation$$

Where:

Squal	Cell Selection quality value, (dB) Not applicable for TDD cells or GSM cells.
Srxlev	Cell Selection RX level value (dB)
$Q_{qualmeas}$	Measured cell quality value. The quality of the received signal expressed in CPICH E_C/N_0 (dB) for FDD cells. Not applicable for TDD cells or GSM cells.
$Q_{rxlevmeas}$	Measured cell RX level value. This is received signal, CPICH RSCP for FDD cells (dBm), P-CCPCH RSCP for TDD cells (dBm) and RXLEV for GSM cells (dBm).
Qqualmin	Minimum required quality level in the cell (dB). Not applicable for TDD cells or GSM cells.
Qrxlevmin	Minimum required RX level in the cell. (dBm)
Pcompensation	Max(UE_TXPWR_MAX_RACH – P_MAX, 0) (dB)
UE_TXPWR_MAX_RACH	Maximum TX power level an UE may use when accessing the cell on RACH (read in system information), (dBm)
P_MAX	Maximum RF output power of the UE, (dBm)

Figure 12: Cell Selection S Criterion

6.4. Cell Camping

After a suitable cell is discovered and S criterion is satisfied, the UE will camp on this cell. Subsequently, it proceeds with tasks such as establishing an RRC connection and RACH. If not satisfied, the UE will try to camp on the next frequency.

7 Network Attaching

After a successful cell camping, the UE initiates an attach request at the NAS layer. And for BG96, BG95 series, BG77 and BG600L-M3 modules, the default PDP bearer is activated automatically.
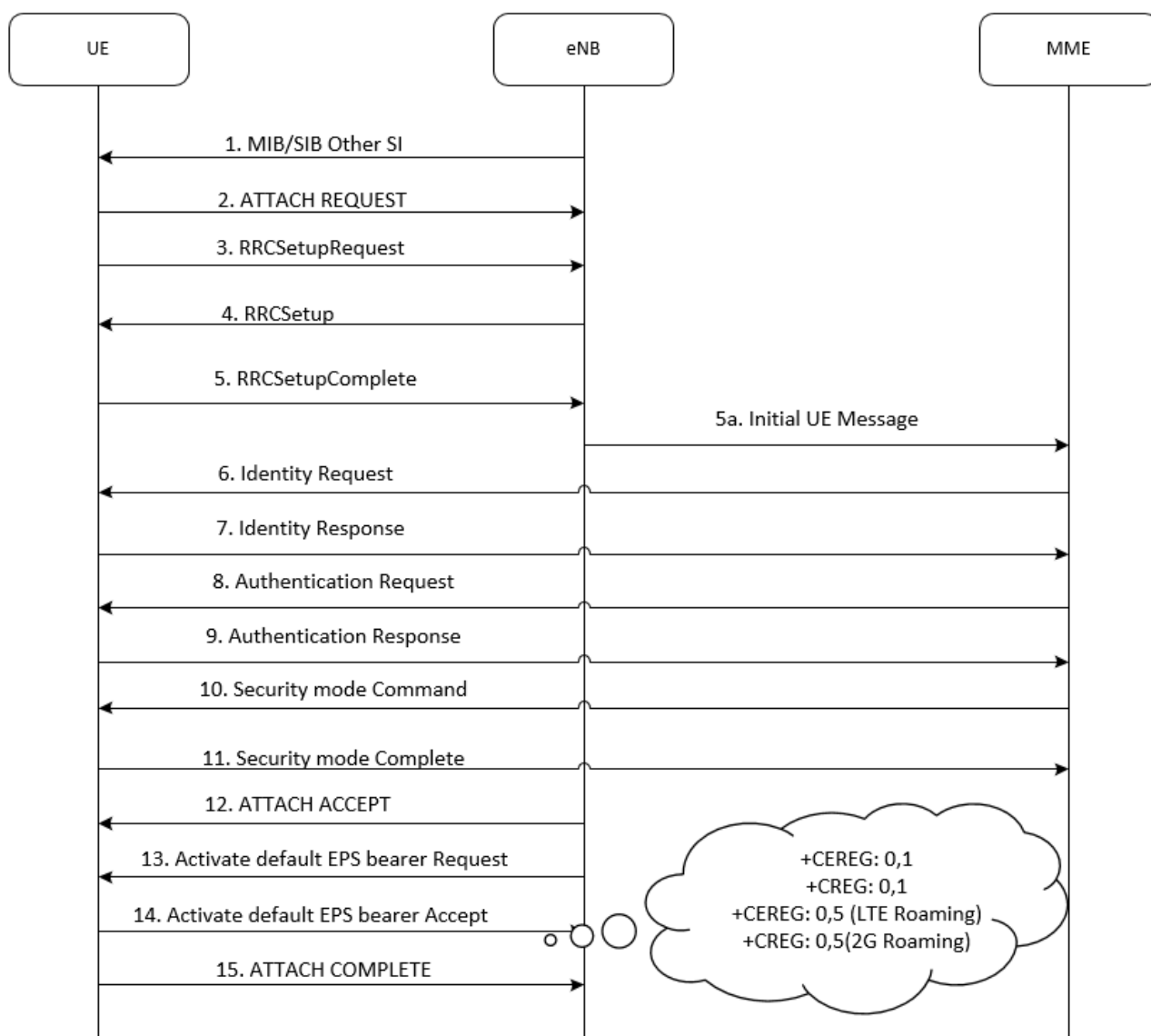

Figure 13: Network Attaching

8 FAQs

8.1. How to Disable HPLMN Search Timer?

You can use the command **AT+QNWCFG="hplmnsearch_ctrl",0** to disable the HPLMN search timer. However, it's important to note that once this function is disabled, the UE will never search for the HPLMN even when it is located within an area covered by the HPLMN.

8.2. How to Configure IRAT Timer?

You can use the command **AT+QCFG="irat/timer"[,<timer_value>[,<alignment_value>]]** to configure the IRAT timer. For more details on parameter descriptions, please refer to *document [2]*.

8.3. How to Disable SIM RAT Order?

You can use the command **AT+QCFG="simeffect",0** to disable the SIM RAT order. For more details on parameter descriptions, please refer to *document [2]*.

8.4. When is RPLMNwACT Saved?

When the UE registers to a network, the RPLMNwACT is saved when UE enters LPM, PSM, or executing **AT+CFUN=0**, **AT+CFUN=1,1**, **AT+QPOWD=1** etc. Please note that the fast power down will not save RPLMNwACT to NV.

8.5. How to Clear RPLMN/FPLMN?

1. Clear LOCI (including RPLMN) via **AT+CRSM=214,28542,0,0,11,"FFFFFFFFFFFFFFFFFFFFFF"**.
2. Clear PSLOCI (including RPLMN) via **AT+CRSM=214,28531,0,0,14,"FFFFFFFFFFFFFFFFFFFFFF**

FFFFFFFF".

3. Clear EPSLOCI (including RPLMN) via **AT+CRSM=214,28643,0,0,18,"FFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF**".

4. Clear FPLMN via **AT+CRSM=214,28539,0,0,12,"FFFFFFFFFFFFFFFFFFFFFFFF**".

9 Appendix References

Table 2: Related Documents

Document Name
[1]   Quectel_BG95&BG77&BG600L_Series_AT_Commands_Manual
[2]   Quectel_BG95&BG77&BG600L_Series_QCFG_AT_Commands_Manual
[3]   Quectel_BG95&BG77&BG600L_Series_QNWCFG_AT_Commands_Manual
[4]   Quectel_BG96_AT_Commands_Manual
[5]   Quectel_BG96_QCFG_AT_Commands_Manual

Table 3: Terms and Abbreviations

Abbreviation	Description
CS	Circuit Switched
EHPLMN	Equivalent Home Public Land Mobile Network
EPSLOCI	Evolved Packet Switched Location Information
FPLMN	Forbidden Public Land Mobile Network
GSM	Global System for Mobile Communications
HPLMN	Home Public Land Mobile Network
ID	Identifier
LOCI	Location Information
LPM	Low Power Mode
LRPLMN	Last Registered Public Land Mobile Network
LTE	Long-Term Evolution

MCC	Mobile Country Code
MCU	Mobile Control Unit
MIB	Master Information Block
NAS	Non-Access Stratum
NV	Non-Volatile
OOS	Out of Service
PCI	Physical Cell ID
PDSCH	Physical Downlink Shared Channel
PHICH	Physical Hybrid ARQ Indicator Channel
PLMN	Public Land Mobile Network
PS	Packet Switched
PSLOCI	Packet Switched Location Information
PSM	Power Saving Mode
PSS	Primary Synchronization Signal
RACH	Random Access Channel
RAT	Radio Access Technology
RF	Radio Frequency
RRC	Radio Resource Control
RSSI	Received Signal Strength Indicator
SFN	System Frame Number
SIB	System Information Block
SIM	Subscriber Identity Module
SSS	Secondary Synchronization Signal
UE	User Equipment
(U)SIM	Universal Subscriber Identity Module
VPLMN	Visited Public Land Mobile Network