QUECTEL
Build a Smarter World

QUECTEL
MASTER
CLASSES

How to address low power app implementation in NB-IoT and LTE-M

January 2021

QUECTEL
Build a Smarter World

Communication process overview

Issues & solutions during cell search

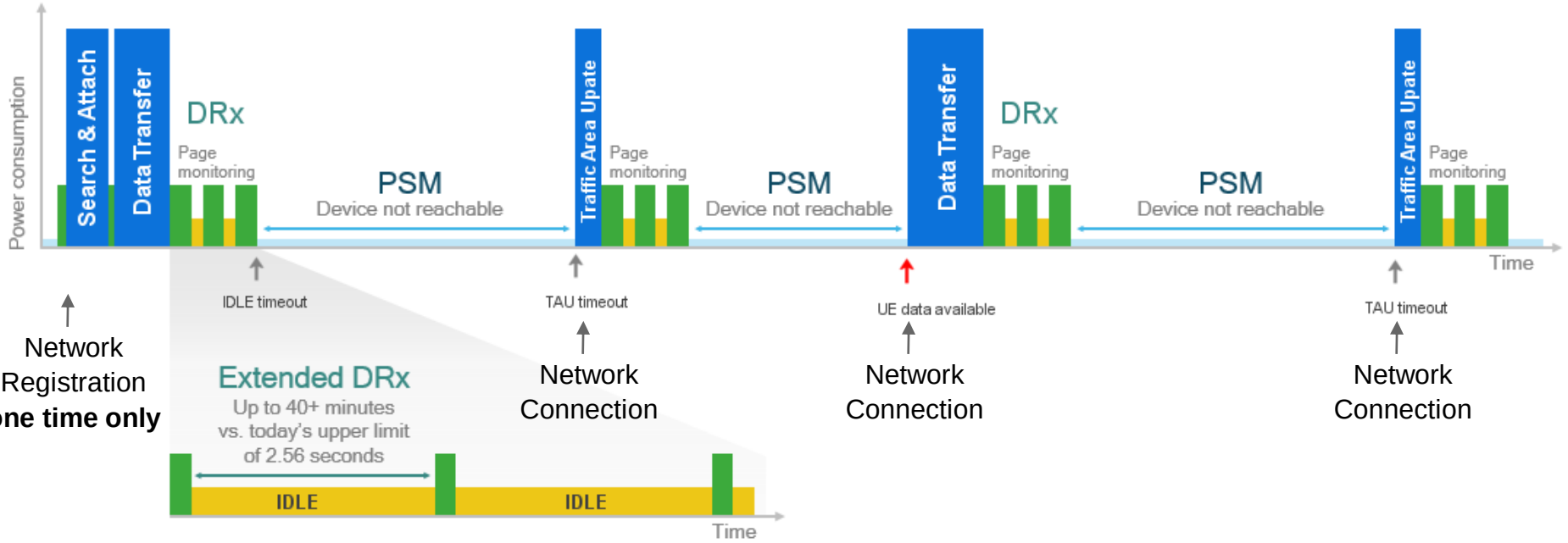
How to handle attach reject

How to skip inactive time

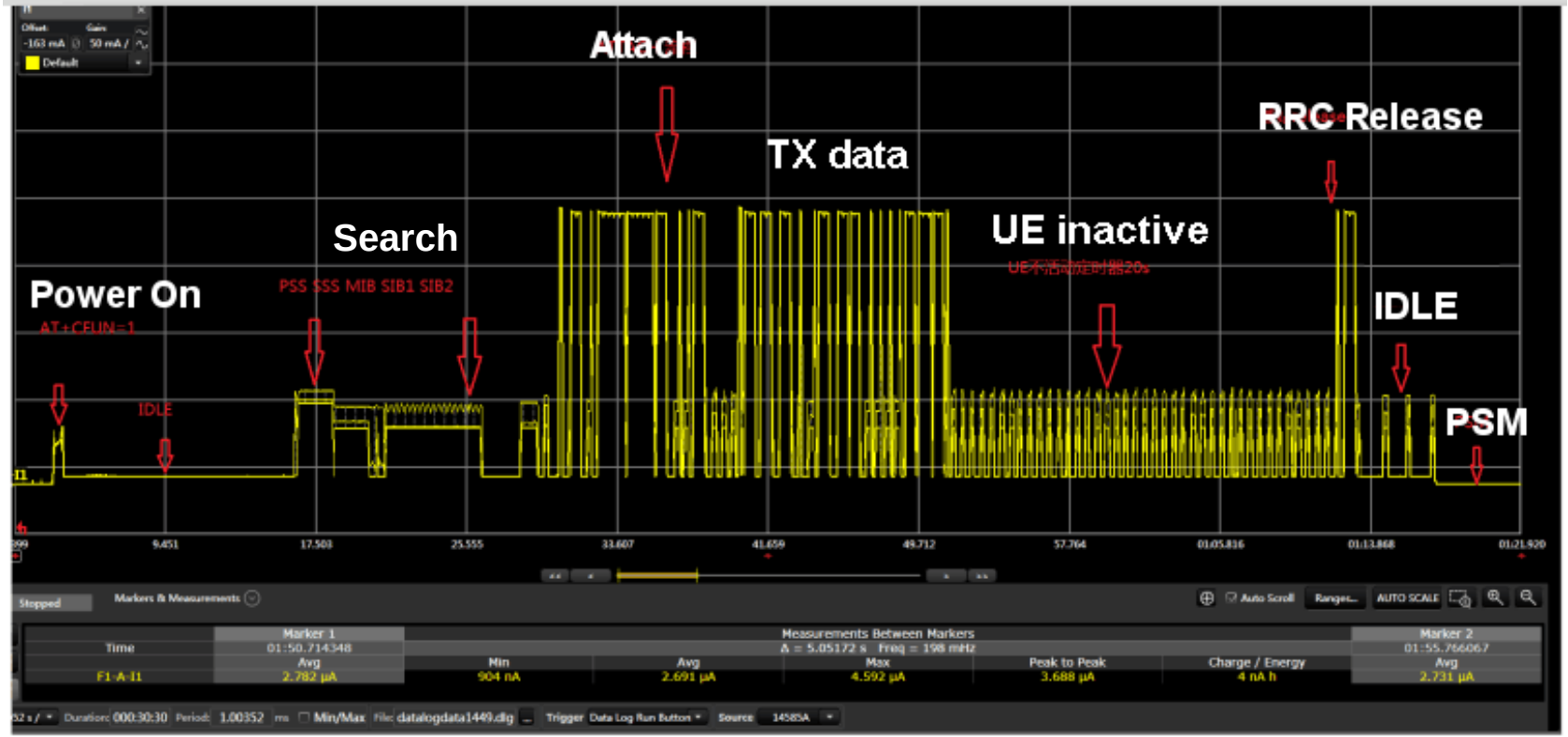
Optimize high level app for low power

QUECTEL MASTER CLASSES

Ideal communication process in NB-IoT



Real communication process in NB-IoT



QUECTEL
Build a Smarter World

Communication process overview

Issues & solutions during cell search

How to handle attach reject

How to skip inactive time

Optimize high level app for low power

QUECTEL MASTER CLASSES

Network searching/registration process

including USIM card recognition and reading of NV parameters related to network searching

determined by module NV setting and files in USIM, which have higher priority

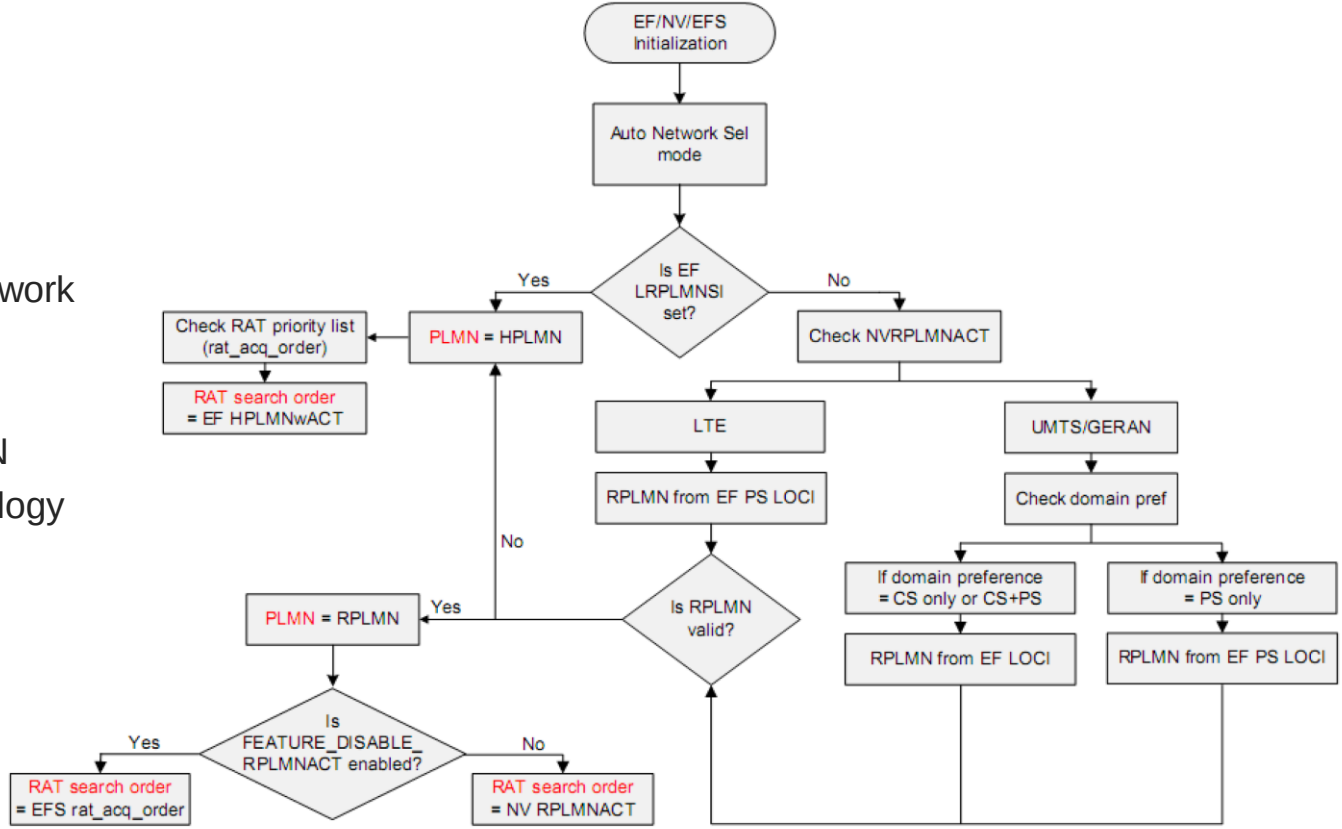
scan all supported bands to find suitable cell to camp on

if access criteria is met, UE will initiate an attach procedure and will not continue to search for other frequencies or bands

RAT/PLMN selection procedure

- NV is file on module
- EF(S) is file on SIM

- **H**omePLMN is the network derived from IMSI
- **R**egistered PLMN
- **L**ast **R**egistered PLMN
- **R**adio **A**ccess **T**echnology
- **AC**cess **T**echnology
  GPRS / NB / LTE-M / ...



LRPLMN & multi-mode modules

Once in a network, always in that network, until it’s lost

- Once the module successfully registers in a network, information about it is saved for future use (**LRPLMN**)
- The saved information will be the first one used for later registration attempts
- Principle is to get the module to a known working network as quickly as possible, to save energy – even if it’s not the highest priority one
- The only workaround to switch is to void LRPLMN

The LRPLMN effect in action

From fresh start: 3min30s

```
[2020-08-20_10:40:22:260]OK
[2020-08-20_10:40:23:923]AT+cereg=2
[2020-08-20_10:40:23:923]OK
[2020-08-20_10:40:24:468]at+creg=2
[2020-08-20_10:40:24:468]OK
[2020-08-20_10:40:26:532]at+cfun=1
[2020-08-20_10:40:26:883]OK
[2020-08-20_10:40:27:322]
[2020-08-20_10:40:27:322]+CPIN: READY

[2020-08-20_10:40:27:322]+QUSIM: 1

[2020-08-20_10:40:27:322]+CREG: 2

[2020-08-20_10:40:27:322]+CEREG: 2
[2020-08-20_10:40:27:459]
[2020-08-20_10:40:27:459]+QIND: SMS DONE
[2020-08-20_10:43:58:152]
[2020-08-20_10:43:58:152]+CREG: 5,"3887","8185C82", 8

[2020-08-20_10:43:58:152]+CEREG: 5,"3887","8185C82",8
[2020-08-20_10:44:25:586]at+qnwinfo
[2020-08-20_10:44:25:586]+QNWINFO: "eMTC","23410","LTE BAND 20",6400

[2020-08-20_10:44:25:602]OK
```

After next power on: 3s

```
[2020-08-20_10:46:08:329]+CEREG: 0
[2020-08-20_10:46:08:589]
[2020-08-20_10:46:11:126]RDY

[2020-08-20_10:46:11:126]+CFUN: 1
[2020-08-20_10:46:11:548]
[2020-08-20_10:46:11:548]+CPIN: READY

[2020-08-20_10:46:11:548]+QUSIM: 1
[2020-08-20_10:46:11:701]AT+cereg=2
[2020-08-20_10:46:11:701]OK
[2020-08-20_10:46:11:768]
[2020-08-20_10:46:11:768]+QIND: SMS DONE
[2020-08-20_10:46:12:241]at+creg=2
[2020-08-20_10:46:12:241]OK
[2020-08-20_10:46:13:967]
[2020-08-20_10:46:13:967]APP RDY
[2020-08-20_10:46:14:392]
[2020-08-20_10:46:14:392]+CREG: 5,"3887","8185C82", 8

[2020-08-20_10:46:14:392]+CEREG: 5,"3887","8185C82",8
[2020-08-20_10:46:17:818]at+qnwinfo
[2020-08-20_10:46:17:818]+QNWINFO: "eMTC","23410","LTE BAND 20",6400

[2020-08-20_10:46:17:834]OK
```

Tips & Tricks - NVLRPLMNACT

NVLRPLMNACT value is stored in NVRAM at detach

NVLRPLMNACT = GSM / LTE-M / NBIoT / not stored

- save state with AT+CFUN=0
- be careful with resets & power cuts

NVLRPLMNACT is erased by AT+QCFG=”nwscanseq”,...

- setting band scan sequence will also wipe LRPLMN info
- this will cause a full scan and registration in later power ups

The Roaming SIM misconceptions (I)

I configured the module with CatM/NB/2G sequence but it always registers to 2G! It's not working!

- What does the SIM say?
- What's inside the EHPLMN, UPLMN and OPLMN lists?
- What about the the stored LRPLMN info?

The Roaming SIM misconceptions (I)

4.4.3.1.1 Automatic Network Selection Mode Procedure

The MS selects and attempts registration on other PLMN/access technology combinations, if available and allowable, in the following order:

i) either the HPLMN (if the EHPLMN list is not present or is empty) or the highest priority EHPLMN that is available (if the EHPLMN list is present) ;

ii) each PLMN/access technology combination in the "User Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iii) each PLMN/access technology combination in the "Operator Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iv) other PLMN/access technology combinations with received high quality signal in random order;

v) other PLMN/access technology combinations in order of decreasing signal quality.

Source:
3GPP 23.122

Roaming SIMs will never find a HPLMN, so (ii) or (iii) applies.

The 2G PLMN may have higher priority

The Roaming SIM misconceptions (I)

QUECTEL Build a Smarter World

4.4.3.1.1 Automatic Network Selection Mode Procedure

The MS selects and attempts registration on other PLMN/access technology combinations, if available and allowable, in the following order:

i) either the HPLMN (if the EHPLMN list is not present or is empty) or the highest priority EHPLMN that is available (if the EHPLMN list is present) ;

ii) each PLMN/access technology combination in the "User Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iii) each PLMN/access technology combination in the "Operator Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iv) other PLMN/access technology combinations with received high quality signal in random order;

v) other PLMN/access technology combinations in order of decreasing signal quality.

Source: **3GPP 23.122**

Roaming SIMs never find a HPLMN and many have the lists empty. So (iv) applies

The Roaming SIM misconceptions (II)

Why is the module choosing a network with a signal of -90dB, instead of another one of -80dB ?

- What does the SIM say?
- What's inside the EHPLMN, UPLMN and OPLMN lists?
- What about the the stored LRPLMN info?

The Roaming SIM misconceptions (II)

QUECTEL Build a Smarter World

4.4.3.1.1 Automatic Network Selection Mode Procedure

The MS selects and attempts registration on other PLMN/access technology combinations, if available and allowable, in the following order:

i) either the HPLMN (if the EHPLMN list is not present or is empty) or the highest priority EHPLMN that is available (if the EHPLMN list is present) ;

ii) each PLMN/access technology combination in the "User Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iii) each PLMN/access technology combination in the "Operator Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iv) other PLMN/access technology combinations with received high quality signal in random order;

v) other PLMN/access technology combinations in order of decreasing signal quality.

Source: **3GPP 23.122**

High quality signal: The high quality signal limit is used in the PLMN selection procedure. It is defined in the appropriate AS specification: 3GPP TS 43.022 [35] for the GSM radio access technology, 3GPP TS 25.304 [32] for the UMTS radio access technology (FDD or TDD mode), 3GPP TS 36.304 [43] for the E-UTRAN radio access technology. For 3GPP2 access technologies the high quality signal limit is defined in 3GPP2 C.S0011 [4] and in 3GPP2 C.S0033 [46] for cdma2000® HRPD. A mobile station attempting to find a ce… IoT (see 3GPP TS 43.064 [55]) does not use high quality signal classification in the PLMN selection procedure.

3GPP 36.304

5.1.2 Support for PLMN selection

5.1.2.1 General

On request of the NAS the AS shall perform a search for available PLMNs and report them to NAS.

5.1.2.2 E-UTRA and NB-IoT case

The UE shall scan all RF channels in the E-UTRA bands according to its capabilities to find available PLMNs. On each carrier, the UE shall search for the strongest cell and read its system information, in order to find out which PLMN(s) the cell belongs to. If the UE can read one or several PLMN identities in the strongest cell, each found PLMN (see the PLMN reading in TS 36.331 [3]) shall be reported to the NAS as a high quality PLMN (but without the RSRP value), provided that the following high quality criterion is fulfilled:

1. For an E-UTRAN and NB-IoT cell, the measured RSRP value shall be greater than or equal to -110 dBm.

Tips&Tricks - Disable SIM effect

Enable/Disable RAT search order stored in SIM

- AT+QCFG="simeffect",0 // disable SIM search order
  AT+CFUN=1,1 // reboot to take effect

Network searching/registration process

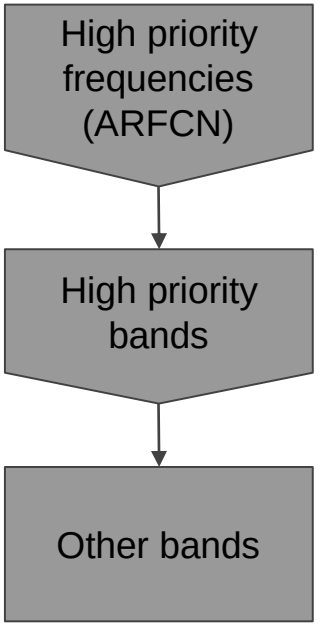
including USIM card recognition and reading of NV parameters related to network searching

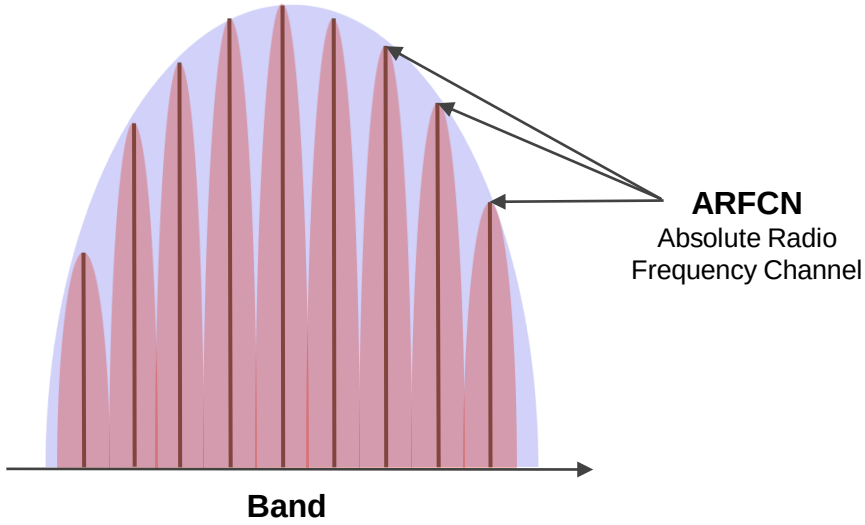
determined by module NV setting and files in USIM, which have higher priority

scan all supported bands to find suitable cell to camp on

if access criteria is met, UE will initiate an attach procedure and will not continue to search for other frequencies or bands

Frequency scan





$$\frac{16 \text{ bands}}{200 \text{ Khz}} \times 3 \text{ CE levels}$$

Network searching time

Band	Time in CE 0 [s]	Time in CE 1 [s]	Time in CE 2 [s]
2	36	180	432
3	45	225	540
4	27	135	324
...			
8	21	105	252
20	18	90	216
...			

Solutions to speed up NW searching

- **Reduce number of bands to search**

  AT+QBAND=**3**,3,8,20 //enable B3/B8/B20 only (Europe, all operators)
  AT+QBAND=**2**,8,20 //enable B8/B20 only (Vodafone in Europe only)

- **Lock to specific frequency channel**

  AT+QLOCKF=1,2175,2 //lock to EARCFN 2175

Solutions to speed up NW searching

- **Enable required RAT(s) only**

```
AT+QCFG="iotopmode",0                  // enable LTE-M only
AT+QCFG="nwscanmode",3

AT+QCFG="iotopmode",0                  // enable LTE-M + EGPRS
AT+QCFG="nwscanmode",0

AT+QCFG="band",F,80084,80084           // enable LTE-M + NBIoT on B3/B8/B20 only
AT+QCFG="iotopmode",2
AT+QCFG="nwscanseq",020301
AT+QCFG="nwscanmode",3
```

Solutions to speed up NW searching

- **Execute special commands only once, in CFUN=0, because each will trigger a new scan, even if you set same value. There will be a registration after it**

AT+CFUN=0	**// turn off radio**
AT+QCFG=”iotopmode", ...	// setup configuration as required
AT+QCFG=”nwscanseq”, ...	
AT+QCFG=”band”,...	
AT+QCFG=”servicedomain”,...	
AT+QCFG=”nwscanmode”, ...	
AT+CFUN=1,1	**// turn on radio and reset module to take effect**

Tips&Tricks - Registration URCs

- **When testing/debugging, enable the registration URCs**

```
[2020-08-20_11:33:47:584]at+qnwinfo
[2020-08-20_11:33:47:584]+QNWINFO: "eMTC","23410","LTE BAND 20",6400

[2020-08-20_11:33:47:584]OK
[2020-08-20_13:34:01:813]at+creg=2
[2020-08-20_13:34:01:813]OK
[2020-08-20_13:34:06:708]AT+cereg=2
[2020-08-20_13:34:06:708]OK
[2020-08-20_13:34:11:634]at+cgreg=2
[2020-08-20_13:34:11:634]OK
[2020-08-20_13:34:18:720]at+qurccfg="urcport","uart1"
[2020-08-20_13:34:18:720]OK
[2020-08-20_13:34:50:438]at+qcfg="iotopmode",2
[2020-08-20_13:34:50:454]OK
[2020-08-20_13:35:05:955]
[2020-08-20_13:35:05:955]+CREG: 2

[2020-08-20_13:35:05:955]+CEREG: 2
[2020-08-20_13:36:26:578]at+qnwinfo
[2020-08-20_13:36:26:578]+QNWINFO: No Service

[2020-08-20_13:36:26:578]OK
```

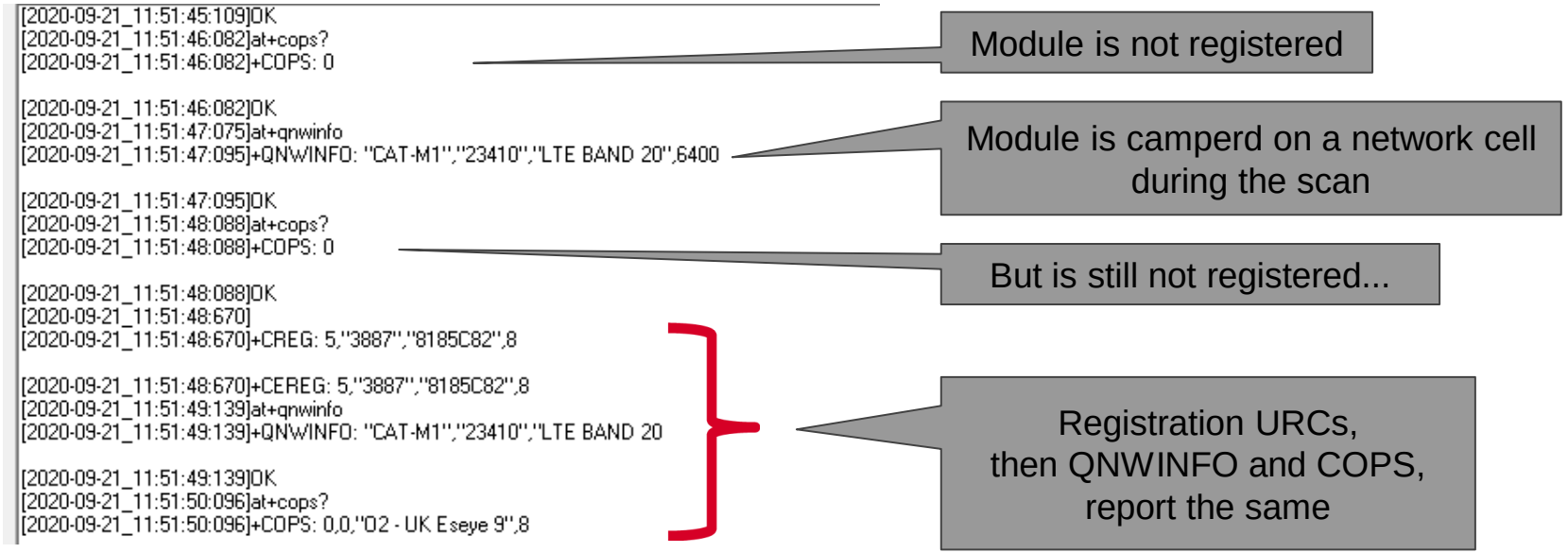
URCs enabled
URC port configured

"Innocent" command

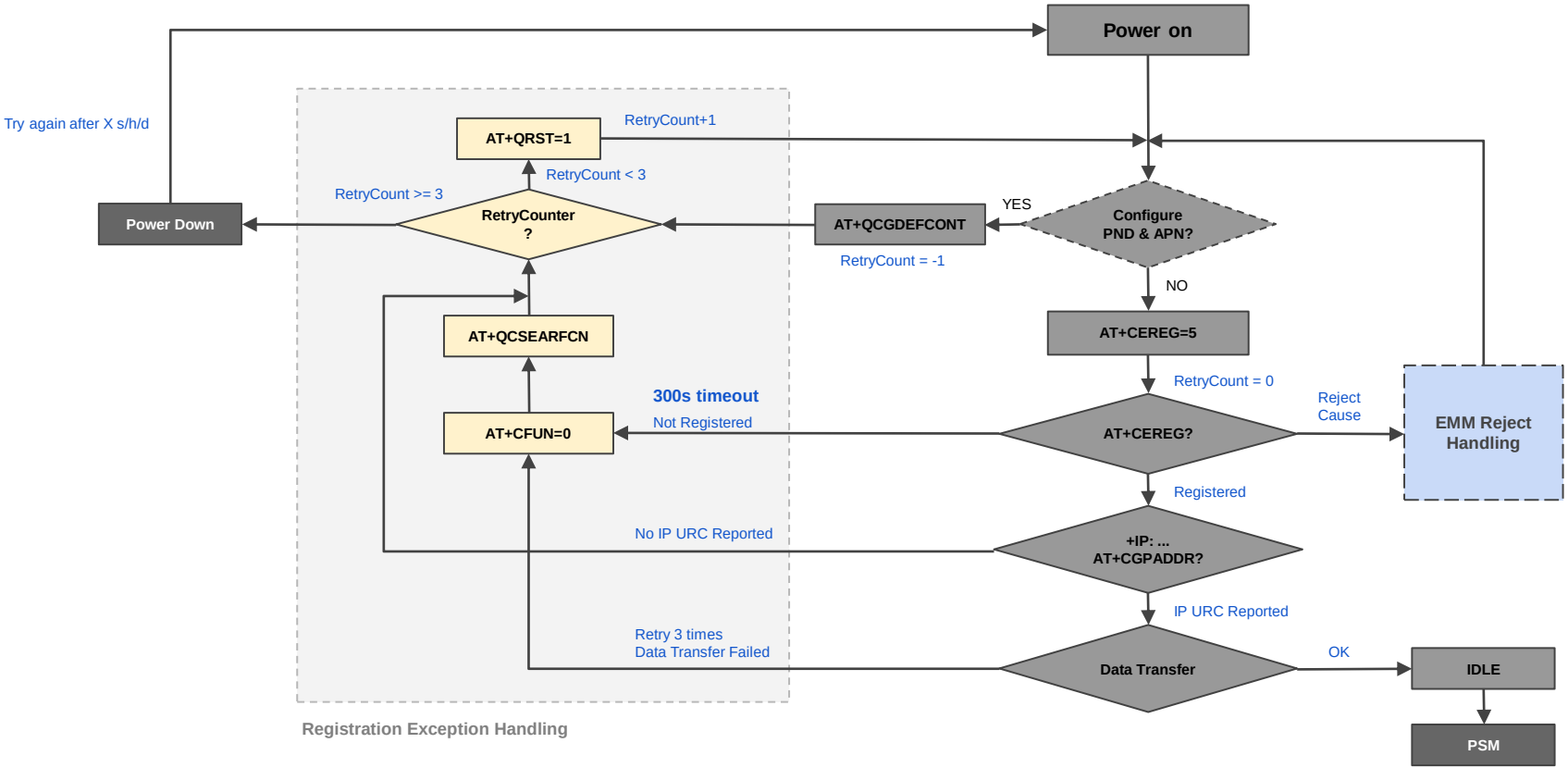
Completely unexpected
side effect!

Tips & Tricks - QNWINFO vs COPS

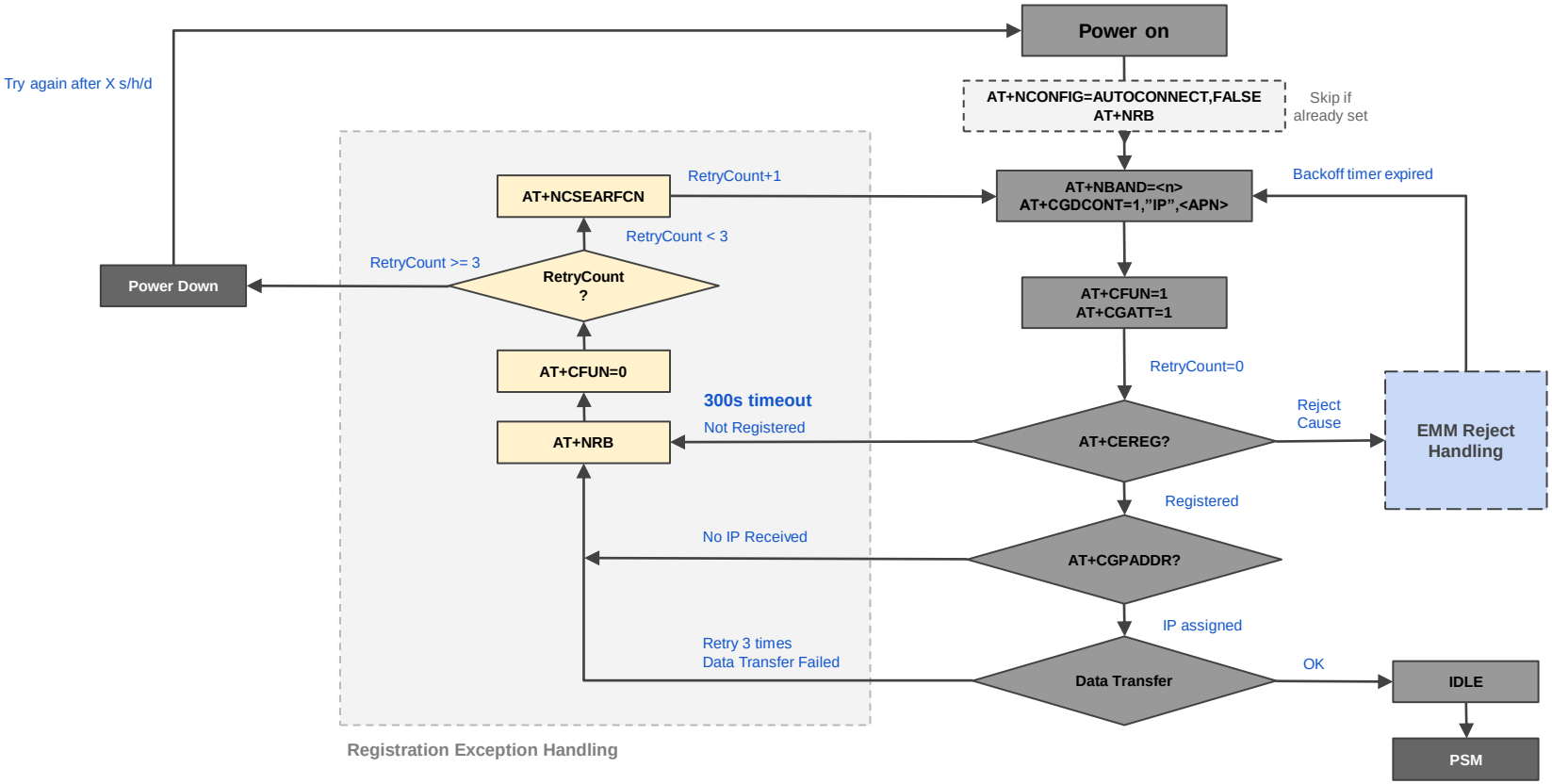
- AT+COPS? returns network where module is **registered**
- AT+QNWINFO returns network where module is **camped**



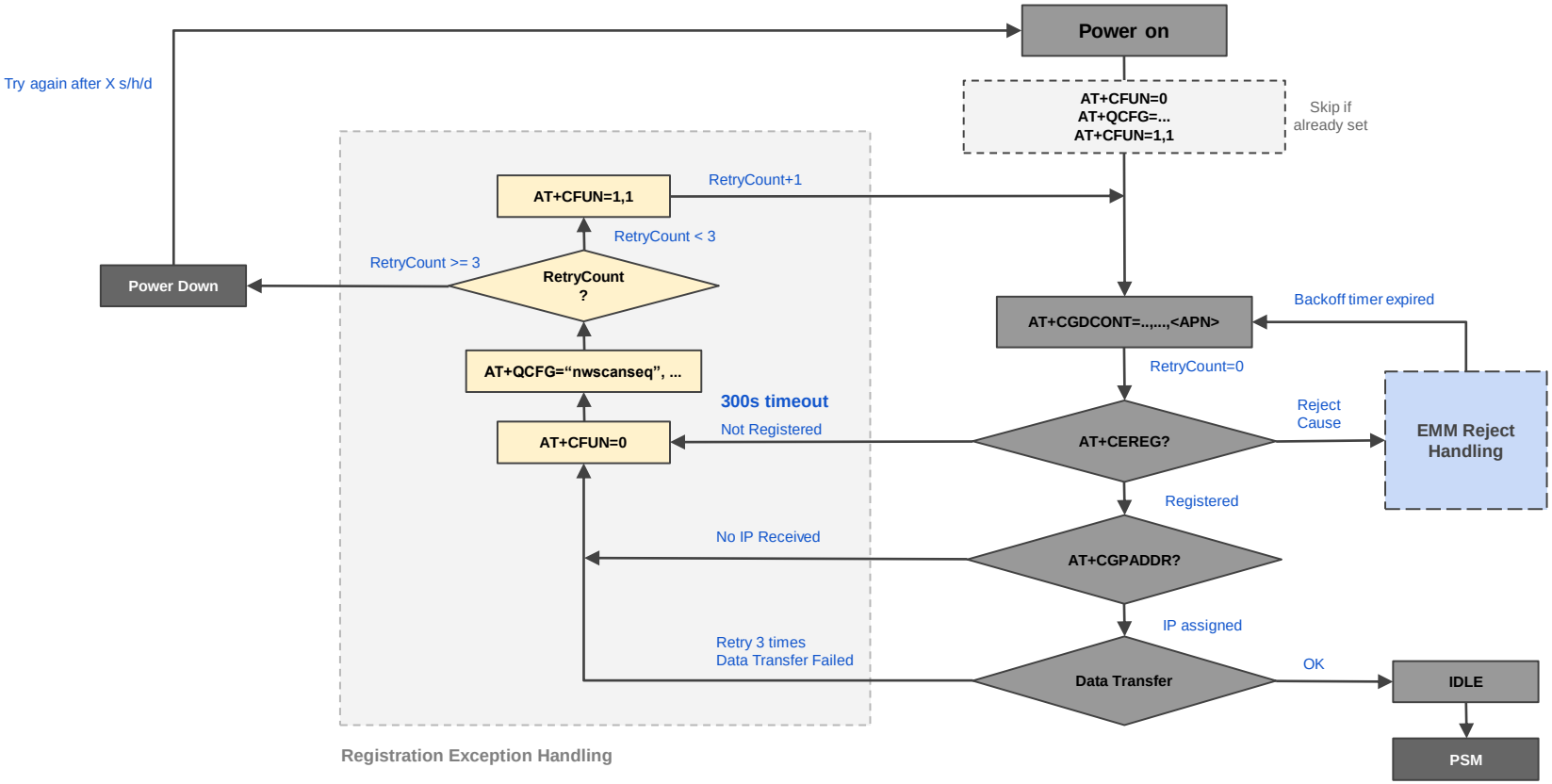
How to handle disconnects (BC66)



How to handle disconnects (BC68/95-G)



How to handle disconnects (BG77/95/96)



Registration Exception Handling

No fallback in LPWA

Why can’t the LPWA modules be like the normal 2G/3G/4G parts, that switch around RATs automatically?

- The module should be constantly scanning bands
- “Low Power” devices cannot afford such power consumption
- The 2G/3G/4G evolution was designed considering fallbacks, not the case of the LPWA networks
- Most LPWA applications work intermittently, with on/off cycles
- In LPWA applications, the signal conditions can be really extreme
- Many features (PSM/eDRX) are very network specific

Tips - The IRAT Timer

If NBIoT network is lost, module will not switch to higher priority network immediately, even if it is present. It will use IRAT timer

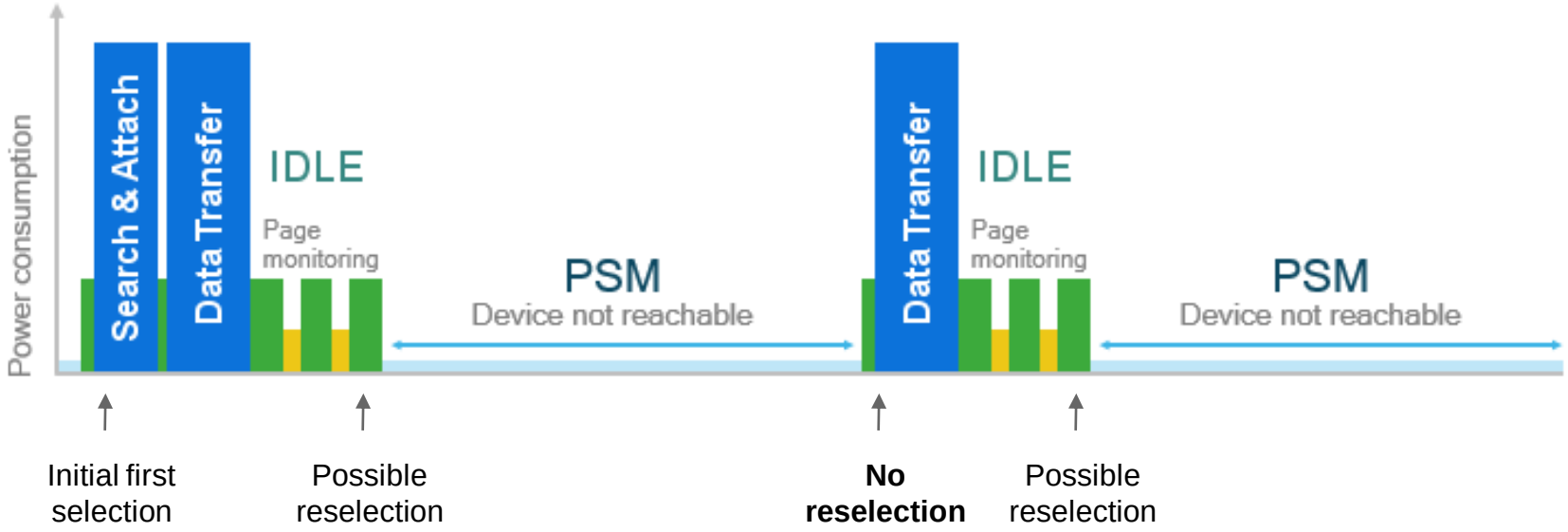
- It’s a module internal timer
- It will periodically look for a higher priority RAT (Radio Access Technology)
- RAT priority as defined by “nwscanseq”
- Default value is 60 minutes
- Some modules support to change value by AT commands

No cell reselection in NBIoT

If signal is low but cell still exists, module will not switch to a better cell when waking up from PSM, but only when in IDLE

- For cell reselection, it needs to reach the threshold
- Threshold is configured by the base station
- If the threshold is reached, module needs 15s to complete measurement of neighbouring cells and complete cell reselection
- It will not reselect the best cell, but the first cell that meets reselection criteria
- It will not reselect a better cell, even if IDLE is more than 15s, because it will not search for it if another good enough was already found

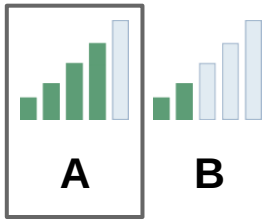
No cell reselection in NBIoT



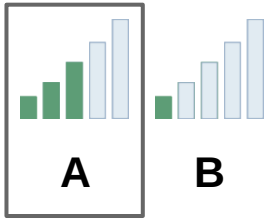
Parking sensor example

A **B**

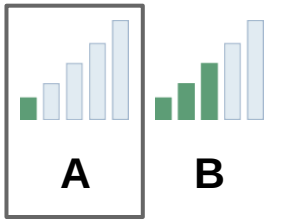
Parking sensor example



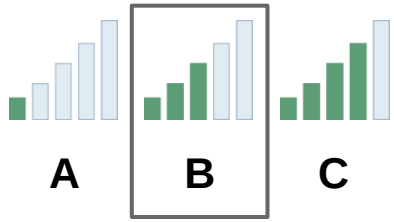
Parking sensor example



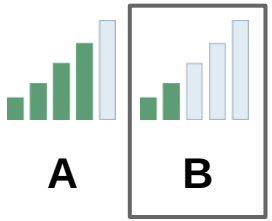
Parking sensor example



Parking sensor example



Parking sensor example



QUECTEL
Build a Smarter World

Communication process overview

Issues & solutions during cell search

How to handle attach reject

How to skip inactive time

Optimize high level app for low power

QUECTEL MASTER CLASSES

Network searching/registration process

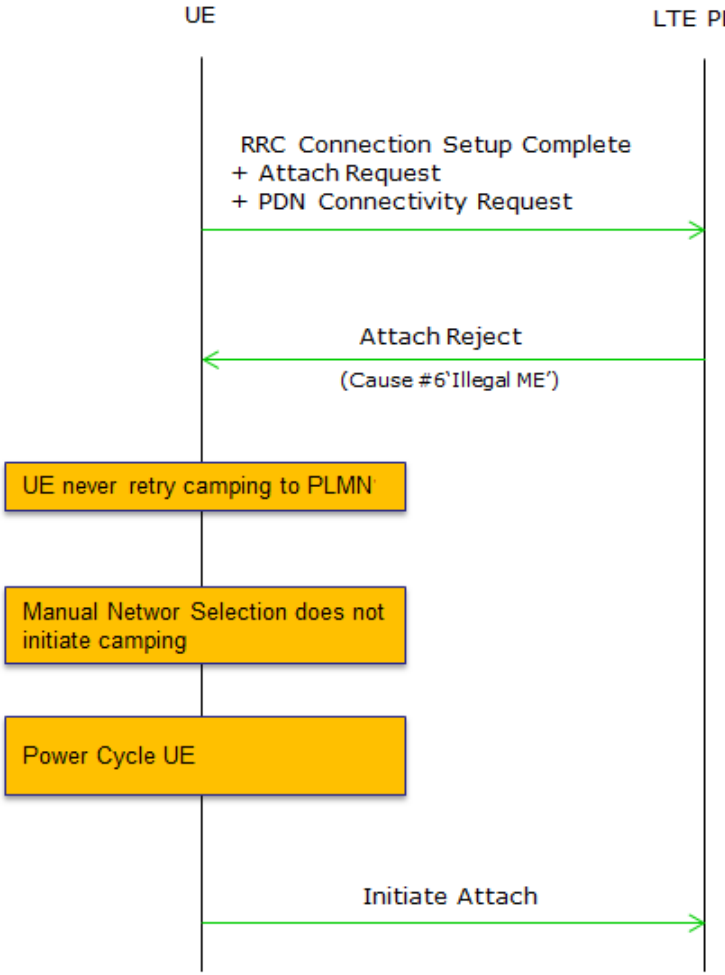
including USIM card recognition and reading of NV parameters related to network searching

determined by module NV setting and files in USIM, which have higher priority

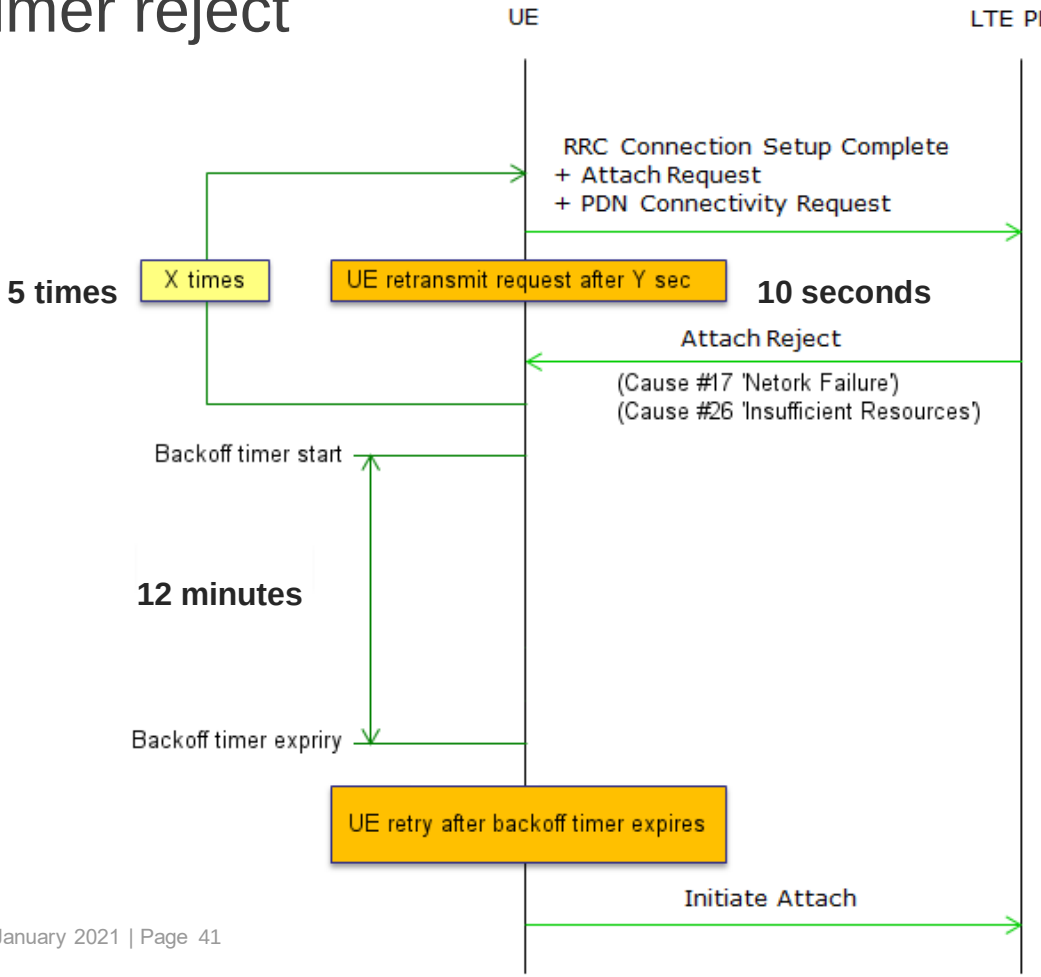
scan all supported bands to find suitable cell to camp on

if access criteria is met, UE will initiate an attach procedure and will not continue to search for other frequencies or bands

Reject cause #6



Backoff timer reject



How to detect reject cause?

- **Register for URC with AT+CEREG=3 or AT+CEREG=5**

+CEREG: <stat>[,[<tac>],[<ci>],[<AcT>][,<**cause_type**>,<**reject_cause**>]] ...

<cause_type> 0 means <reject_cause> contains an EMM cause value (3GPP TS24.008 Annex G)

<reject_cause> contains the cause of the registration failure

How to know backoff timer value?

- **Query by AT+NCIDSTATUS** (BC68, BC95-G)

Response: [+NCIDSTATUS:<cid>[<**status**>,[<**backoff value**>]]

When status=3, backoff_value contains the remaining time of backoff timer T3396 in seconds.

- **Enable URC by AT+QEMMTIMER=1** (BC66, BC66-NA)

URC: +QEMMTIMER: <**backoff_timerId**>,<event>,<period>,<**remaining**>

<backoff_timerId> is 5 for T3396

<period> Timer period in milliseconds.

<remaining>Remaining time in milliseconds, till timer stops.

How to know backoff timer value?

- **Not supported yet via AT commands** (BG96/95/77/600)

Can be visible via Qualcomm debug log, but not available to user at run time.

AT query is under development.

How should app layer handle backoff?

- **Keep AT+CFUN=1** (BC68, BC95-G)

After receiving EMM reject with backoff timer, module stays in IDLE DRX 1.28s (reduced power).

- **Execute AT+CFUN=4** (BC66, BC66-NA, BG77/95/96/600)

Power consumption is lower, compared to CFUN=1.

After time value expires, switch back to AT+CFUN=1 to enable search and attach.

How should app layer handle backoff?

Do NOT take below actions:

- hardware power cut off
- software power down by AT command
- disable modem by AT+CFUN=0
- software or hardware reset

else timer will start counting again from max value.

Just keep current state until timer expires (default 12 minutes)

QUECTEL
Build a Smarter World

Communication process overview

Issues & solutions during cell search

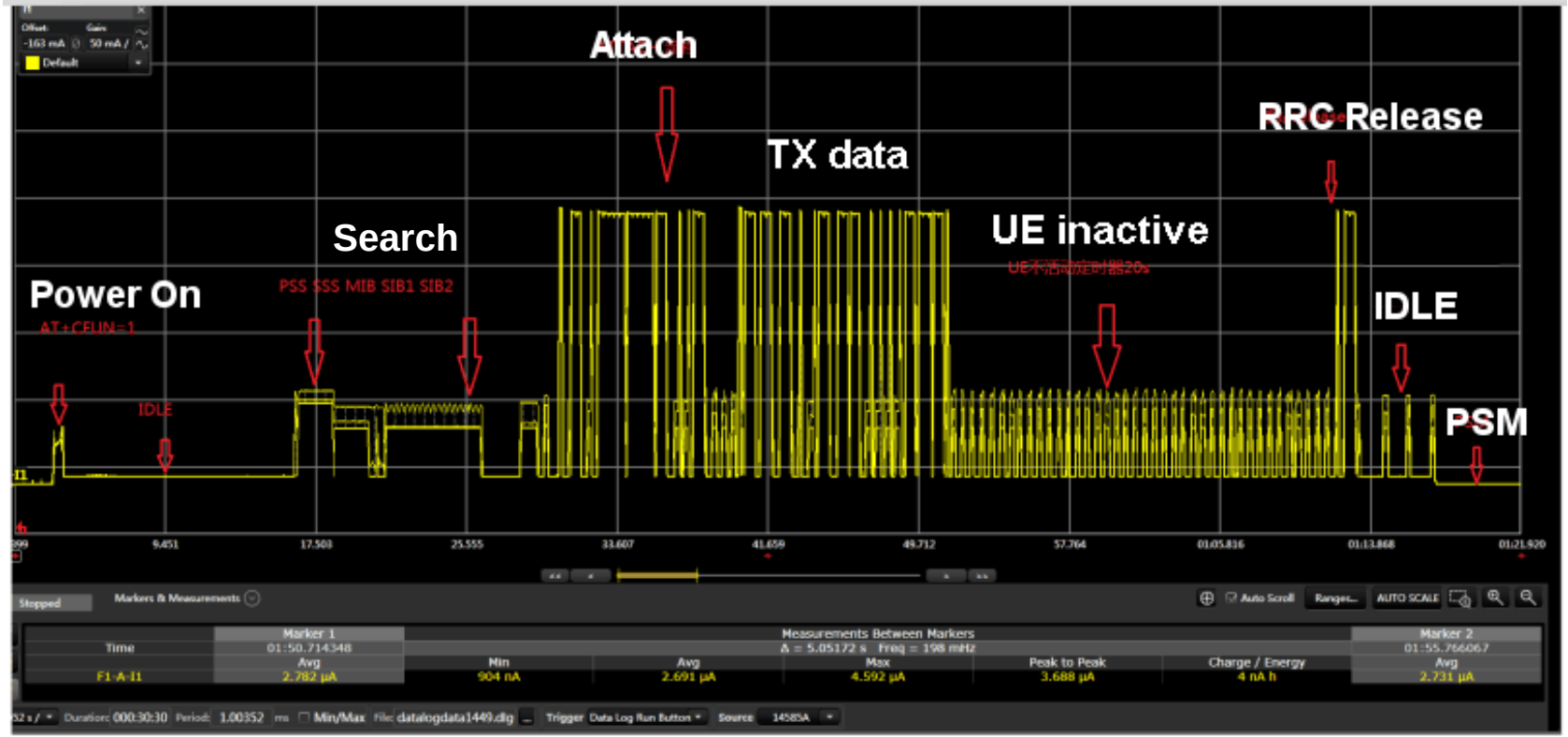
How to handle attach reject

How to skip inactive time

Optimize high level app for low power

QUECTEL MASTER CLASSES

How to skip inactive time with RAI flag



How to skip inactive time with RAI flag

AT+QNBIOTRAI=<**rai_mode**>

- 0 = No RAI information available (default)
- 1 = No further downlink (reply) data expected
- 2 = Only a single downlink (reply) data and no further uplink (request) data expected

Execute command before sending UDP data.

Applies to Mediatek based modules (BC66/66-NA)

How to skip inactive time with RAI flag

AT+QISENDEX=<connectID>,<hex_string>[,<**rai_info**>]

- 0 = No RAI information available (default)
- 1 = No further downlink (reply) data expected
- 2 = Only a single downlink (reply) data and no further uplink (request) data expected

Applies to Qualcomm based modules (BG95/96/77/600)

How to skip inactive time with RAI flag

AT+NSOSTF=<socket>,<...>,<...>,<**flag**>,<length>,<data>[,<sequence>]

- 0 = No RAI information available (default)
- 0x100 = No further downlink (reply) data expected
- 0x400 = Only a single downlink (reply) data and no further uplink (request) data expected

Applies to Neul based modules (BC68/95-G)

QUECTEL
Build a Smarter World

Communication process overview

Issues & solutions during cell search

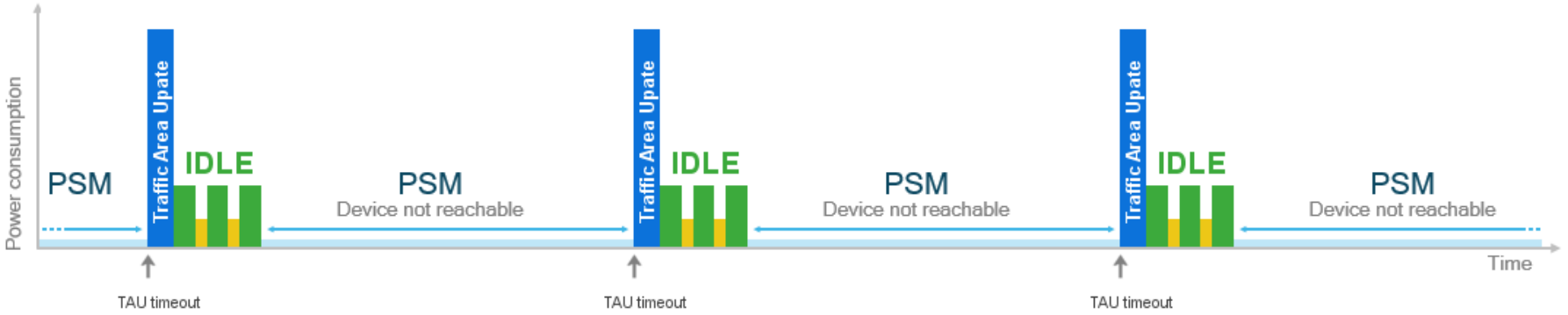
How to handle attach reject

How to skip inactive time

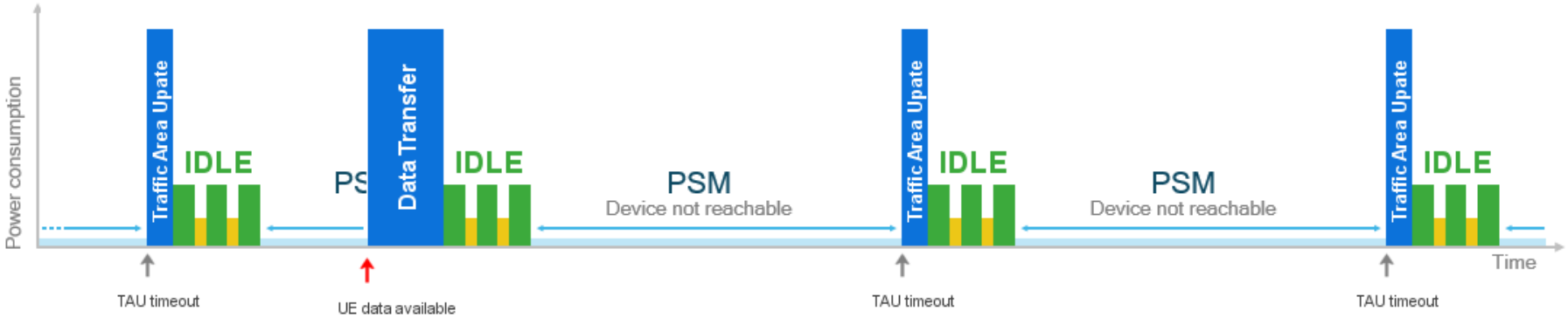
Optimize high level app for low power

QUECTEL MASTER CLASSES

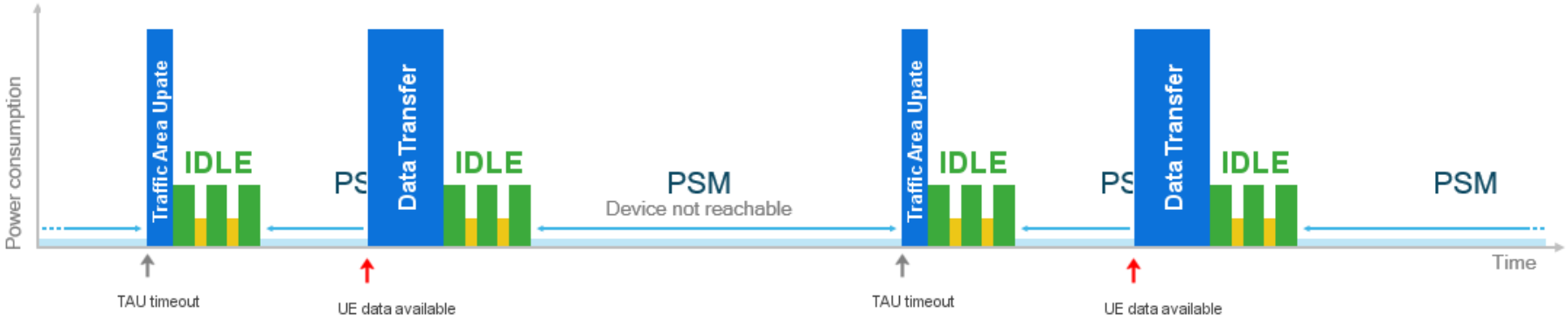
Optimize high level app for low power



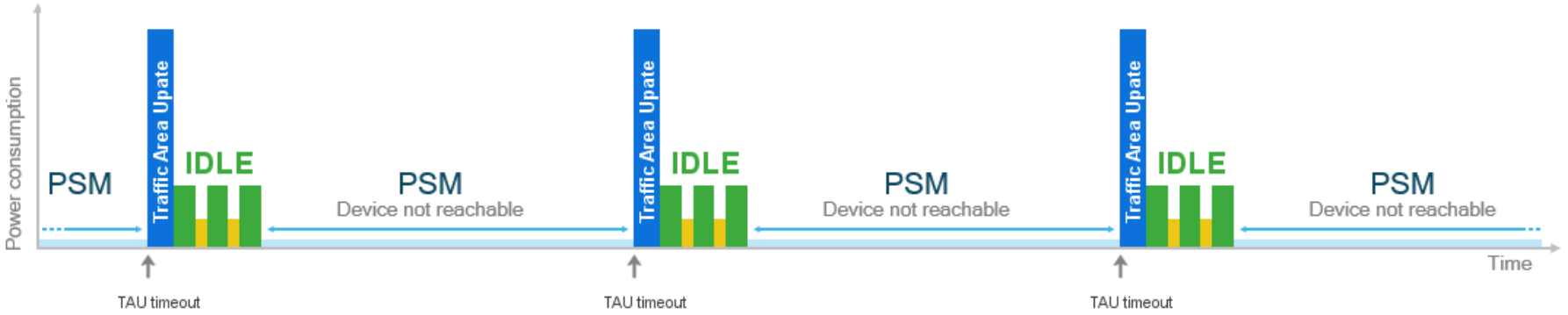
Optimize high level app for low power



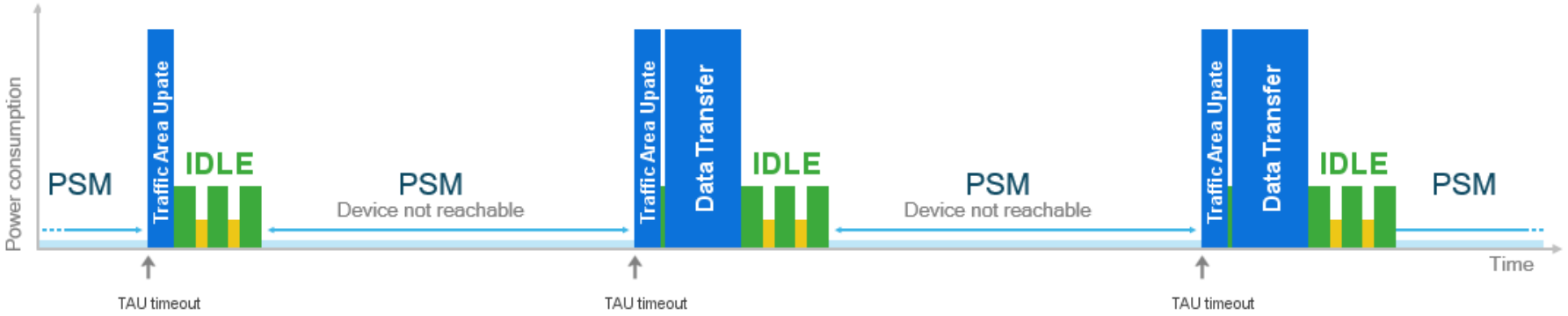
Optimize high level app for low power



Optimize high level app for low power



Optimize high level app for low power



- store data available
- wait TAU timeout URC
- send data during Traffic Area Update session

QUECTEL
Build a Smarter World

The number one cellular module vendor in the world and a leading GNSS module supplier

- **Unbeatable choice from the broadest module portfolio in the world**
- **The highest quality products for the best possible prices**
- **Superb support with the largest R&D team in the industry**
- **Continuous innovation – first to market with 5G, LPWA, CV2X, snapdragon**
- **A passionate, dedicated team of "Quectelers" ensure our customers always come first**

Thank You

www.quectel.com

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** • Technical Support: **support@quectel.com**