**3GPP TSG-RAN WG2 Meeting #121bis-e R2-2304256**

**Online, 17th – 26th April, 2023**

**Agenda item: 7.6.2.2**

**Source: MediaTek Inc.**

**Title: [AT121bis-e][104][IoT NTN Enh] GNSS operation enhancements (Mediatek)**

**Document for: Discussion and Decision**

# 1 Introduction

This document is aimed at discussing on the open issues, related to GNSS operation enhancement of IoT-NTN and identify potential agreements for possible convergence.

* [[AT121bis-e][104][IoT NTN Enh] GNSS operation enhancements (Mediatek)

Initial scope: Discuss the proposals in the submitted contributions in AI 7.6.2.2

Initial intended outcome: Summary of the offline discussion with e.g.:

* List of proposals for agreement (if any)
* List of proposals that require online discussions
* List of proposals that should not be pursued (if any)

Deadline for companies' feedback: Wednesday 2023-04-19 18:00 UTC

Deadline for rapporteur's summary (in R2-2304244): Wednesday 2023-04-19 20:00 UTC

Updated scope: Discuss the remaining proposals from R2-2304244

Updated intended outcome: Summary of the offline discussion with e.g.:

* List of proposals for agreement (if any)
* List of proposals that require online discussions
* List of proposals that should not be pursued (if any)

Deadline for companies' feedback: Tuesday 2023-04-25 02:00 UTC

Deadline for rapporteur's summary (in R2-2304256): Tuesday 2023-04-25 04:00 UTC

Proposals marked "for agreement" in R2-2304256 not challenged until Tuesday 2023-04-25 20:00 UTC will be declared as agreed via email by the session chair (for the rest the discussion might continue online in the Wednesday CB session).

# 2 Contact

|  |  |
| --- | --- |
| Company | Delegate Contact |
| MediaTek | Abhishek Roy (Abhishek.Roy@mediatek.com) |
| OPPO | Haitao Li (lihaitao@oppo.com) |
| Intel | Tangxun (xun.tang@intel.com) |
| Nokia | Ping Yuan (Ping.1.Yuan@nokia-sbell.com) |
| Samsung | Jonas Sedin (j.sedin@samsung.com) |
| Xiaomi | Xiaowei jiang(jiangxiaowei@xiaomi.com) |
| Apple | Yuqin Chen (yuqin\_chen@apple.com) |
| Google | Ming-Hung Tao (mhtao@google.com) |
| Qualcomm | Bharat Shrestha (bshrestha@qti.qualcomm.com) |
| NEC | Yuhua chen (Yuhua.chen@emea.nec.com) |
| ZTE | Lu Ting (lu.ting@zte.com.cn) |
| Lenovo | Xu Min (xumin13@lenovo.com) |
| Huawei, HiSilicon | Xubin (xubin10@huawei.com) |
| Turkcell | Izzet Sağlam (izzet.saglam@turkcell.com.tr) |
| CATT | Xiangdong Zhang(zhangxiangdong@catt.cn) |
| CAICT | Sidong Li(lisidong@caict.ac.cn) |
| InterDigital | Brian Martin (brian.martin@interdigital.com) |
| CMCC | Jiayao Tan (tanjiayao@chinamobile.com) |
| Ericson | robert.s.karlsson@ericsson.com |
| Sequans | Olivier Marco (omarco@sequans.com) |

# 3 Discussion – second round

## 3.1 UE reporting GNSS position fix time duration in RRC connected state

Proposal 3 (16/19): RAN2 will wait for further progress in RAN1 about UE’s reporting of GNSS position fix time duration in RRC connected state.

* ZTE thinks we should decide. QC agrees. Ericsson agrees
* Further discuss if we can take an Agreement/Working Assumption that the UE does not need to report GNSS position fix time duration in RRC connected state as this value doesn’t change and then send LS to RAN1 to check this

**Question 1: Do companies agree that we can take an Agreement/Working Assumption that the UE does not need to report GNSS position fix time duration in RRC connected state *as this value doesn’t change*?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT | Disagree with comments | We prefer to have a conclusion in RAN2 for progress, but we don’t think RAN2 can conclude that “as this value doesn’t change”. So we suggest the following working assumption:**Working Assumption: The UE does not need to report GNSS position fix time duration in RRC connected state *with the assumption that ~~as~~ this value doesn’t change. This can be revised based on RAN1 further input if necessary.*** |
| OPPO | Agree | All in all, this is a working assumption and we can check with RAN1 whether they agree. |
| Apple | Agree |  |
| CMCC | Agree with comments | We are fine with the rewording provided by CATT. |
| ZTE | Agree | We are also fine with the rewording provided by CATT. |
| Google | Agree with comments | We are fine with CATT’s rewording. |
| Lenovo | Agree with comments | We prefer to use CATT’s rewording. |
| Xiaomi | Agree with comments | We are ok to have WA in RAN2 and further check in RAN1 |
| Huawei, HiSilicon | Agree with comments | OK to use CATT’s rewording. |
| InterDigital | Agree with comments | If we are anyway checking or waiting for RAN1 then maybe no need to make any assumption yet, but no strong view. |
| Nokia | Disagree  | For now, we don’t agree the GNSS fix time value doesn’t change during the RRC Connected state. In our understanding, if the UE starts moving or the (GNSS) propagation conditions changed a lot (e.g, shadowed when UE moves from outdoor to indoor), GNSS position fix time duration will be changed during the RRC connected state.For the sake of progress, if we want to take the assumption as proposed by CATT, we think it is mandatory to confirm with RAN1 in the LS for further discussion. |
| MediaTek | Agree | Fine with CATT’s comments |
| Ericsson | Disagree | Fix duration may change during the connection. There is no harm for UE to report this each time the UE achieve a GNSS position fix – this shall anyway not happen often and it informs the eNB that the UE has acquired a new GNSS position! Further, RAN1 are not dine discussing this yet. |
| Qualcomm | Agree | Also ok with CATT’s suggestion. GNSS fix duration should not be changing much such that we need to introduce a mechanism to update during connected mode. |
| NEC | Agree  | Also fine with the CATT version  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Question 2: If Q1 was agreed, do companies agree to send LS to RAN1 to check that UE does not need to report GNSS position fix time duration in RRC connected state?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT |  | With the updated version of the working assumption, we can just wait for RAN1 agreements.  |
| OPPO | Agree  |  |
| Apple | Agree |  |
| CMCC | Agree |  |
| ZTE | No need | Agree with CATT. |
| Google | Agree |  |
| Lenovo | Agree |  |
| Xiaomi | Agree |  |
| Huawei, HiSilicon | Agree |  |
| InterDigital | Agree |  |
| Nokia | Disagree | As indicated in Q1, we think RAN2 should ask RAN1 to confirm. |
| MediaTek | Disagree | Since RAN1 is discussing this issue, RAN2 can wait for RAN1 agreement. |
| Ericsson | Disagree | No LS needed if UE reports each time it achieves a GNSS position fix – which is anyway a rare event.  |
| Qualcomm | No need | Agree with CATT |
| NEC | Agree  | Agree to Send LS to check  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

## 3.2 Leaving RRC Connected State

Proposal 4 (15/19): UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has initiated a new measurement

* Continue offline

**Question 3: Do companies agree that UE can stay in RRC\_CONNECTED state when current GNS position becoming out-of-date if the UE has initiated a new measurement?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT | Agree with comments | “**if the UE has initiated a new measurement**”, the UE of course should stay in RRC\_CONNECTED, because the UE has traffic requirement to keep connection, otherwise, the UE need not to initiate the new measurement. But we think, more interesting question is, how to deal with the indication of the **current GNS position becoming out-of-date, if UE initiates a new measurement.** And we think that, if the UE initiates a new measurement, before the current GNSS position becoming out-of-state, the UE should ignore the indication of current GNS position becoming out-of-date.  |
| OPPO | Agree with comments  | In any case, if UE has initiated a new measurement, it should be kept in RRC\_CONNECTED, which is the whole pint for Rel-18 GNSS enhancements. Then whether current GNSS position will become out-of-date during GNSS measurement depends on how we will capture in the spec, e.g. UE should stop the GNSS validity timer during new GNSS measurement, or UE simply ignores the GNSS validity timer’s expiry during GNSS measurement. |
| Apple | Agree | In addition to this agreement, RAN2 should also discuss the question whether UE should stop validity duration timer once GNSS measurement is initiated. RRC state switch can be determined uniquely by validity timer expiry. |
| CMCC | Agree with comments | Share similar view as OPPO. |
| ZTE | Agree with comments | We have similar view as CATT and OPPO on this aspect, e.g., in any case, if UE has initiated a new GNSS measurement, it should be kept in RRC\_CONNECTED, which is the main intention for Rel-18 GNSS enhancements. RAN2 can mainly confirm this understanding, that’s enough.Moreover, in our assumption, UE only needs to start new GNSS measurement upon the expiration of previous GNSS validity timer. So we think it’s no need to discuss the case that current GNSS position becoming out-of-date after the UE has initiated a new measurement.We see such case in Q3 is an exceptional case that only exist in the solution based on the explicit trigger from eNB as explained below:* In this solution, UE starts GNSS measurement only when it receives an explicit trigger from eNB, and, upon receiving a trigger, the UE must start GNSS measurement. Therefore, if this trigger comes earlier, UE needs to deal with the exceptional case that a new measurement is started but the previous GNSS validity timer is still running (to stop or ignore the previous timer may be needed). Furthermore, if the trigger comes too early, whether UE should start the GNSS measurement or not is also a question (skip scheme may be needed).
* Another exceptional case is this trigger comes later, e.g., later than the expiration of GNSS validity timer. Then upon expiration of GNSS validity timer, whether UE should autonomously start the GNSS measurement or not is also a question.
 |
| Google | Agree with comments | We think such a principle is applicable even if UE has started/entered a measurement gap but has not yet conducted the measurement. Therefore, we suggest to reword the question/proposal as “UE can stay in RRC\_CONNECTED state when current GNS position becoming out-of-date if the UE has **started/entered a measurement gap**”  |
| Lenovo | Agree | We can agree on this firstly, and discuss the following issues as identified by companies. |
| Xiaomi | Agree | There is no such GNSS validity timer, as GNSS out of date indication is from GNSS module according to current spec:5.3.3.21 UE actions upon indication of out-of-date GNSS positionUpon indication that the GNSS position has become out-of-date while in RRC\_CONNECTED, the UE shall:1> perform the actions upon leaving RRC\_CONNECTED as specified in 5.3.12, with release cause 'other'. |
| Huawei, HiSilicon | Agree with comments | We still think this can be left to proper NW implementation to make sure UE can finish the GNSS measurement before the GNSS position is out of date.But we can go with majority for the sake of progress. |
| InterDigital | Agree with comments | Agree with Huawei.  |
| Nokia | Agree with revision. | We agree with the proposal in principle. However, we believe the new GNSS measurement performed by UE should be started before the validity duration expiry or upon the expiry of the validity duration. Otherwise, it will bring extra complexity for the design since it is not clear whether UE is allowed to perform UL transmission during the period in between the timer expiry and the start of measurement gap for GNSS measurement.Therefore, we agree with Google for the rewording:“UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has **started/entered a measurement gap**” |
| MediaTek | Agree |  |
| Ericsson | Agree with comment | The details may need to be FFS. Seeing the divergent views, it is better to wait some further progress in RAN1 on gaps and measurements, and if UE is allowed to transmit in UL after validityDuration or not…  |
| Qualcomm | Agree |  |
| NEC | Agree  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

## 3.3 Remaining validity duration or whole validity duration

Proposal 5 (16/19 GNSS validity duration UE reported after GNSS measurement is the remaining validity duration

* VC assumes the intended proposal was something like:

Proposal 5 (16/20) “GNSS validity duration UE reported after GNSS measurement is the remaining validity duration”

* ZTE has strong concerns on this as this would cause additional signalling: the UE would have to send this every time. HW agrees. Samsung does not see this problem: there is no need to report every time
* Continue offline

Regarding ZTE’s concerns, rapporteur understands that the whole validity duration does not change frequently, so that UE can send the validity duration only when the value changes. Apparently ZTE assumes that the remaining validity duration will change frequently, UE would have to send it very time. However, rapporteur doesn't think so, as the value UE reported is an enumeration value, it is not very accurate. So UE can keep the value same as the last reported one, even if there is some fluctuate caused by UL transmission. Note that, the space between the values in that enumeration is large enough to accommodate the UL transmission fluctuation and other delay if any.

**Question 4: Do companies agree that GNSS validity duration UE reported after GNSS measurement is the remaining validity duration?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT | Agree | The UE may finish the GNSS measurement at time T1, but it may report it at time T2. The network may know the report time T2, but the network cannot always know the time T1. But the UE has counter the GNSS validity duration from T1. So the remaining validity duration should be reported considering the gap between T1 and T2.  |
| OPPO | Agree  |  |
| Apple | Agree | Our understanding is in order for network and UE to have the same understanding about the ending point of validity duration, the starting point and the duration should be known at network side.If UE reports remaining time duration, the starting point is the transmission/reception time. The minor mismatch due to re-transmission can be ignored.Else if UE reports whole time duration, according to ZTE, the starting point of validity duration is the ending point of fix time duration. Their reasoning is anyway the validity duration is not that concise, it would be fine for UE to delay its starting point of validity duration timer a bit to the ending point of fix time duration. Our understanding is this is too coarse as UE may finish its GNSS measurement at any time point inside fixe time duration.And, for validity time duration, we think it can vary from time to time depending on factors like UE movement speed, its location, etc. Thus, we prefer UE to report it as remaining time every time UE finishes its GNSS measurement. |
| CMCC | Agree | Agree with rapporteur. |
| ZTE | Disagree | We disagree with rapporteur and think something is mixed up. The main difference between reporting whole validity duration and reporting remaining validity duration is not whether the value changes frequently, but whether the eNB needs to be aware of the starting point of new GNSS validity duration (as explained by Apple).For remaining validity duration:* If UE is allowed to report remaining validity duration, which means eNB doesn’t care about the starting point of new GNSS validity duration, **eNB would just start the GNSS validity timer on its side when receiving the UE report, with the length of GNSS remaining time.** In this scheme, after each time GNSS reacquisition, eNB has no any assumption on when to start the GNSS validity timer on its side and how long the time length should be. Therefore, it’s mandatory for UE to report the remaining time every time UE finishes its GNSS measurement, regardless of whether the remaining time is changed compared with last time GNSS reacquisition (is it any strange to say a remaining time keeps unchanged since it’s a dynamic time concept?)

For whole validity duration:* We suggest that UE can report the whole validity duration only once (can update later via UL MAC CE if it changes). The related assumption is that, UE and eNB would autonomously starts the new GNSS validity timer on their own sides on **the common time point** with the same timer length (the whole validity duration). As mentioned during first round discussion by some companies, **the common time point could be the end of the GNSS position fix duration timer** (it’s common understanding that GNSS position fix duration is the gap in which UE performs GNSS reacquisition).
* We tend to agree with Apple that it may be possible that the UE finish its GNSS measurement at a time point earlier than the end of GNSS position fix duration. But based on the understanding of the concept of GNSS position fix duration and also the reason why we introduce it, we assume this would be the rare case and the earlier amount will be relatively small. So it’s still reasonable for UE to start the new GNSS validity timerat the end of the GNSS position fix duration timer (e.g., a bit later than the end of GNSS reacquisition).
* We disagree with CATT‘s concern about T1/T2. As mentioned above, it doesn’t matter as eNB doesn’t rely on the UE report to start the time in its own side.
 |
| Google | Agree | To align with the Rel-17 UE behaviour. |
| Lenovo | Agree | Reporting the remaining duration is sufficient. UE can subtract the duration between T1 and T2 in the reported value. |
| Xiaomi | Agree |  |
| Huawei, HiSilicon | Disagree | Please take the following into consideration:1. As Rapp mentions, the reported value should be rather coarse.
2. The GNSS validity duration should be much longer than the GNSS measurement gap.

In this case, there is no problem if the ending of the gap is regarded as the starting point of the reported GNSS validity duration. The benefit would be UE doesn’t need to report this unless the GNSS validity duration changes.   |
| InterDigital | Agree | Same as R17. |
| Nokia | Agree | Agree with CATT and Apple. We don’t think NW can always assume the validity duration timer will be started the end of the GNSS measurement gap. As discussed in RAN1, UE may also perform the GNSS acquisition in C-DRX inactive time. In this case, the UE anyway need to report the start point when the timer is to be started. However, reporting the whole validity duration will bring extra signalling in Uu interface. |
| MediaTek | Agree | For network-triggered GNSS measurement, the network can know when the GNSS measurement starts, but when the GNSS measurement ends depends on UE implementation and UE’s current state.For UE autonomously triggered GNSS measurement (e.g., UE autonomously triggers in DRX inactive state), it is possible that the network does not know when the GNSS measurement starts or even when it ends.As it is a coarse measurement, for the remaining validity duration, the network can assume the validity duration starts when the UE sends the validity duration. |
| Ericsson | Agree | Reuse the R17 validityDuration RRC report.  |
| Qualcomm | Agree | There is no need to introduce two different reporting, existing one with remaining and new one with whole validity duration. |
| NEC | Disagree  | We agree with ZTE and Huawei’s analysis. different from initial access case, where the GNSS measurement may be much earlier than msg5 transmission time point, It is rare that UE willfinish GNSS measurement much earlier than the end of the measurement gap (which is configured according to UE reported fix duration).if we try to find a compromise way, suggest to have following wording : **GNSS validity duration UE reported after GNSS measurement is the validity duration from the end of the measurement gap.**Autonomously triggered GNSS measurement is not yet agreed , but if it is introduced, we will be fine to compromise at that time if remaining validity duration report is much better |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

## 3.4 UE report the GNSS validity duration by using a MAC CE

Proposal 6 (17/20): UE will report the GNSS validity duration by using a MAC CE.

* QC and MTK think that RRC does not work for NB-IoT NTN
* Continue offline

Rapporteur understands that for NB-IoT Control Plane solution, there is no AS security. The RRC signalling is also not protected, just like the MAC CE. Based on this understanding, rapporteur would like to ask companies the following question:

**Question 5a): Do companies agree that RRC signalling does not work for NB-IoT NTN (CP Solution)?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT |  | We prefer MAC CE solution for GNSS validity duration, but CP solution in NB-IoT is used for early data transmission, which means one-short data transmission, maybe we need not consider this scenario?  |
| OPPO | Agree | We do not agree to CATT’s comment that CP solution is for early data transmission which is used for RRC\_IDLE mode data transmission. From the very beginning, CP solution is one of the data transmission solutions for RRC\_CONNECTED state. |
| Apple | Agree | For control plane solution, we also agree with rapporteur that there is no security protection to MSG3/MSG5. |
| CMCC | Agree |  |
| ZTE | See comments | We agree with OPPO that RRC signaling is still feasible for UE to report something to NW during PRACH procedure or after entering RRC\_CONNECTED. But we agree with Rapp that security concern is same to RRC and MAC CE for UE with CP solution. So using MAC CE for UE report is fine to us. |
| Google | Disagree | Even if RRC is not security protected, using the RRC signalling is still feasible and has some merits such allowing a unified and simpler framework in dealing with the GNSS validity duration report and the corresponding RRC state transition.  |
| Lenovo |  | Do we need to agree on this? Outcome of Q5b is sufficient. |
| Xiaomi | Agree | We agree that for control plane solution there is no security protection for RRC message. |
| Huawei, HiSilicon | Agree | No security issue for this MAC CE. What is the issue even if this is exposed? |
| InterDigital | See comments | RRC Reconfiguration is not supported in NB-IoT and neither is measurement report. However “RRC Signalling does not work” is the wrong statement. |
| Nokia |  | Agree with InterDigital. |
| MediaTek | Agree | Please note that CP solution is not just used for EDT. The CP solution is basic solution that is widely used since Rel-13. RRC signalling is not supported for NB-IoT CP solution. |
| Ericsson | Disagree | First, our impression is that the NB-IoT CP solution is mainly for short data transmissions and thus need not to be optimized for – even though NB-IoT CP solution may be used in other cases too, that is not a major use case. Second, if there is one case where security is difficult or impossible – there is no need to make all other cases with AS security non-secure. We can use the unsecure RRC report in NB-IoT CP solution and use the secure RRC solution in all other cases…  |
| Qualcomm | Agree | For NB-IoT CP solution, only SIB1bis is used.There is no existing RRC message to carry such information between UE and eNB for NB-IoT CP solution in SRB1bis.Involving RRC incurs delay. |
| NEC |  | Agree with Lenovo and InterDigital, we can discussion Q5b directly, with this point in mind |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

**Question 5b): If the answer to Q 5a) is YES (i.e.,** **RRC signalling does not work for NB-IoT NTN), do companies agree that UE will report the GNSS validity duration by using a MAC CE?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT | Agree |  |
| OPPO | Agree |  |
| Apple | Agree | Let’s think about how to address MAC CE security issue in next release. |
| CMCC | Agree |  |
| ZTE | Agree | We disagree RRC signaling does not work.But we agree security concern is same to RRC and MAC CE for UE with CP solution. So using MAC CE for UE report is fine to us. |
| Lenovo | Agree |  |
| Xiaomi | Agree |  |
| Huawei, HiSilicon | Agree |  |
| InterDigital | Agree | Well the answer to 5a is no, but we anyway agree with MAC CE.  |
| Nokia |  | OK for the proposal to move forward. |
| MediaTek | Agree |  |
| Ericsson | Disagree | RRC works also for NB-IoT NTN, and can be used.  |
| Qualcomm | Agree | There is no SRB1bis RRC message to carry such info. |
| NEC | Agree  | Agree with ZTE. and there is less security issue with GNSS validity duration report comparing GNSS fix gap configuration. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

**Question 5c): If the answer to Q5 is NO (i.e., RRC signalling can work for NB-IoT NTN), companies are requested to select between MAC CE and RRC signalling for reporting GNSS Validity Duration?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT | MAC CE |  |
| Google |  | Slightly prefer the RRC signalling. |
| Ericsson | RRC | There is already the RRC gnss-validityDuration report in R17 and this gnss position fix duration can also be an RRC report sent at the same time. All the state transition that will be required if GNSS position fix can not be obtained will need to be described in RRC – we prefer to only model this in RRC.  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

## 3.5 Multiple attempts of GNSS measurement

Proposal 8 (15/19): RAN2 will not discuss allowing multiple attempts of GNSS measurement.

* Xiaomi thinks this depend on how we configure the measurement gap
* Continue offline

**Question 6: Do companies agree that RAN2 does not need to discuss allowing multiple attempts of GNSS measurement?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT | Disagree | It means the UE has the requirement to stay RRC\_CONNECTED that the UE initiates the GNSS measurement during the connection state. Otherwise, the UE can go to IDLE after the GNSS position becoming out-of-state. That is the pre-condition. Of course, the UE can go to IDLE if the UE cannot get GNSS position successfully after one attempt of GNSS measurement. But, what the UE behaviour after enter into IDLE? The UE has also to perform GNSS measurement, and try to establish RRC connection after a successful GNSS measurement. So, we think it is better to let UE try another one or several attempts before enter into IDLE. |
| OPPO | Agree | We do not see any benefit of network configuring a measurement gap whose length is multiple of UE’s GNSS position fix time duration, as the failure rate would be the same for the multiple attempts within the same gap. |
| Apple | Agree | I guess the case is about network configuring both MAC CE based and UE autonomous based GNSS measurement (but not one single long gap where UE can perform GNSS meas for multiple times).If our understanding is correct, we agree UE do not need to wait for multiple attempts before entering RRC idle. Our view is as long as the first GNSS measurement fails, UE considers validity duration timer is expired, which then triggers RRC state transition.  |
| CMCC | Agree | Share similar view as Apple. |
| ZTE | Agree | We are still not so clear about the intention of multiple attempts of GNSS measurement. We prefer a simple UE process, e.g., if UE fails to reacquire GNSS at the end of the GNSS position fix time duration, UE can go to idle state. |
| Google | Agree |  |
| Lenovo | Agree |  |
| Xiaomi | Disagree | As long as UE is still in inside the measurement gap, it is up to UE implementation how many attempts to try the GNSS measurement.We only need to say that after the measurement gap, if UE still cannot acquires GNSS, UE goes to idle mode. |
| Huawei, HiSilicon | Agree | The normal case should be that the measurement gap can only cover one GNSS measurement. |
| InterDigital | Agree | Agree with Huawei |
| Nokia | Agree |  |
| MediaTek | Agree | It is possible that a moving UE cannot obtain the GNSS signal temporarily.If UE fails to get the GNSS measurement during the network-triggered measurement gap and if the GNSS validity duration has not expired yet, it will help to keep the connection longer if UE is allowed to try another attempt at GNSS measurement, e.g., UE autonomously trigger GNSS measurement when the validity duration expires. |
| Ericsson | Agree |  |
| Qualcomm | Agree | UE will try to fix until the end of measurement gap, so we are not clear on what it means multiple try.At the end of measurement gap, if GNSS is not fixed, we can define behavior, may be UE goes to IDLE. |
| NEC  | agree |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

## 3.6 Security concern

Proposal 9 (15/19): There is no need to send LS to RAN1/SA3 for RAN2’s security concern about using MAC CE for aperiodic triggering.

* Continue offline

**Question 7: Do companies agree that there is no need to send LS to RAN1/SA3 for RAN2’s security concern about using MAC CE for aperiodic triggering?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT |  | Ok to confirm with SA3. |
| OPPO | Agree | No LS is needed. In the past, we don’t check with SA3 for every new MAC CE. |
| Apple | See comments | We have talked about many cases related to MAC CE security. In general, we are fine to check with SA3 but we also need to take into account the reality that control plane solution for NB-IoT does not have AS security as well.  |
| CMCC | Agree |  |
| ZTE | Agree | We already have several DL MAC CEs. |
| Google | See comments | We’re fine to check with SA3 regarding the security concern.  |
| Lenovo | Agree | Security concern can be triggered by SA3 if there is any. |
| Xiaomi | Agree |  |
| Huawei, HiSilicon | See comments | If the LS is not sent, we should confirm from RAN2 point of view there is no security concern with this MAC CE to avoid further discussion over again. Otherwise, it is better to check with SA3. |
| InterDigital | Agree | Many things are reported and controlled using MAC CE. As long as no permanent identities are exposed then there is no security concern. |
| Nokia | Agree |  |
| MediaTek | Agree | No LS to SA3 is needed. We don’t need SA3 to point out that MAC CE is not protected by the security.No LS to RAN1, as RAN1 already be aware of RAN2’s concern, and apparently RAN1 is not going to reopen their discussion. |
| Ericsson | Disagree | We shall check with SA3 cc RAN,1 if is fine to allow a threat of making UEs disappear to go measure GNSS. Note that it is much easier to achieve power advantage for an attacker on the ground when the transmissions are from a satellite compared to a terrestrial network.  |
| Qualcomm | Agree | We see no concern in this scenario. As network will configure UE whether it should expect such MAC CE for trigger or not.And obviously UE can decide when likely to receive this trigger. |
| NEC | Disagree  | It is better to check with SA3 since this MAC CE will stop UE monitoring scheduling and transmission for very long period of time |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

## 3.7 UE autonomously reacquire GNSS during the inactive state of C-DRX

Proposal 10 (17/19): RAN2 will postpone the discussion of UE autonomously reacquire GNSS during inactive state of C-DRX until there is some more progress in RAN1.

* Continue offline

**Question 8: Do companies agree that RAN2 will postpone the discussion of UE autonomously reacquire GNSS during inactive state of C-DRX until there is some more progress in RAN1?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT | Yes |  |
| OPPO | Agree  |  |
| Apple | Agree |  |
| CMCC | Agree |  |
| ZTE | See comments | We are fine to postpone the discussion. But we think it’s clear this issue is mainly in the RAN2 scope. We don’t think it’s reasonable to wait RAN1 to make decision on this aspect. |
| Google | Disagree | We don’t expect there will be significant progress in RAN1, as this issue is more within RAN2’s scope. If we postpone, then when can we resume the discussion if RAN1 eventually does not have any progress?  |
| Lenovo | Agree |  |
| Xiaomi | Agree | RAN1 is already going to send LS to us regarding this aspect. We can discuss when receiving the LS. |
| Huawei, HiSilicon | See comments | RAN1 already agreed the UE is not forbidden to re-acquire GNSS position fix during inactive state of Connected DRX and the details are up to RAN2. So we don’t need to discuss this proposal anymore and can discuss the details directly in next meeting (seems no time for this in this meeting). |
| InterDigital |  | We are fine to postpone until the next meeting. We assume that if the UE completes a measurement autonomously, then UE reports a new validity duration MAC CE to the eNB. |
| Nokia | Agree | Agree with Xiaomi and Huawei. |
| MediaTek | Agree |  |
| Ericsson | Agree |  |
| Qualcomm | See comments | We also think RAN2 can handle this issue. |
| NEC |  | Fine with Huawei’s proposal to continue discussing the issue next meeting based on further progress or LS from RAN1. No need to discuss this proposal anymore |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

## 3.8 Conflict between reading SIB31 in connected and GNSS measurement

Proposal 12 (16/19): RAN2 will use “Option 2: Postpone reading SIB31 until GNSS measurement is completed” to resolve the conflict between reading SIB31 in connected and GNSS measurement.

* Continue offline

**Question 9: Do companies agree that RAN2 will use “Option 2: Postpone reading SIB31 until GNSS measurement is completed” to resolve the conflict between reading SIB31 in connected and GNSS measurement.?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| CATT | Yes |  |
| OPPO | Agree  |  |
| Apple | Agree |  |
| CMCC | Agree |  |
| ZTE | Agree |  |
| Google | Agree |  |
| Lenovo | Agree with comments | We may need to further discuss how to handle the case wherein T318 expires during GNSS measurement (i.e., UE enters IDLE upon T318 expiring). From our understanding it could be:* For Q3 “UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has initiated a new measurement” is agreed, and thus UE stays in CONNECTED even upon T318 expiring.
* Specify that UE stays in CONNECTED upon T318 expiring if UE has initiated a GNSS measurement.
 |
| Xiaomi | Agree |  |
| Huawei, HiSilicon | Agree |  |
| InterDigital | Agree with comments | Maybe it is better to leave to UE implementation to some extent e.g. “UE may postpone” because UE may also be able to complete both. |
| Nokia | Agree with revision. | It is unclear in the proposal on the “conflict”, we prefer to make it explicitly described.**RAN2 will use “Option 2: Postpone reading SIB31 until GNSS measurement is completed” ~~to resolve the conflict between reading SIB31 in connected and GNSS measurement~~ if the UE cannot complete the SIB31 reading before the start of GNSS MG.** |
| MediaTek | Agree |  |
| Ericsson | Partly agree | We agree with Nokia formulation besides we need to provide for the case the UE can read SIB31 and acquire GNSS at the same time. Something like **For a UEs that cannot read system information and acquire GNSS position at the same time, the UE may Postpone reading SIB31 until GNSS measurement is completed” ~~to resolve the conflict between reading SIB31 in connected and GNSS measurement~~ if the UE cannot complete the SIB31 reading before the start of GNSS MG.** |
| Qualcomm | Agree |  |
| NEC | Agree  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Rapporteur Summary**

# 4 Conclusion – second round

# 5 Discussion – first round

In R-18 IoT-NTN Work Item Description (WID), further enhancement to GNSS operation has been proposed, as mentioned in table below:

Table 1: GNSS operation enhancement in R-18 IoT-NTN WID

|  |
| --- |
| 4.1.1 IoT-NTN Performance Enhancements in Rel-18 to address remaining issues from Rel-17This work considers Rel-17 IoT-NTN as baseline as well as Rel-17 NR-NTN outcome and the further IoT-NTN performance enhancements objectives are listed below:- Study and specify needed improved GNSS operations for a new position fix for UE pre-compensation during long connection times and for reduced power consumption. Simultaneous GNSS and NTN NB-IoT/eMTC operation is not assumed. [RAN1, RAN2]* *NOTE: The need for RAN4 Core requirements for this objective will be identified after the conclusion on the need for improvements.*
 |

Based on these WID objectives, several companies have provided contributions in RAN2-121bis-e. These contributions are categorized into different categories for possible discussion and agreements:

## 5.1 GNSS position fix time duration

* **RRCReestablishmentComplete and RRCConnectionReconfigurationComplete messages.**

In last RAN2 meeting, an open issue was left as:

|  |
| --- |
| For UE to report GNSS position fix time duration for measurement during the initial access, at least the following Msg5 message can be used:  RRCConnectionSetupComplete, RRCConnectionSetupComplete-NB,  RRCConnectionResumeComplete, RRCConnectionResumeComplete-NB, FFS for RRCreestablishmentComplete and RRCConnectionReconfigurationComplete. FS for Msg3 |

Contributions in [1], [2], [3], [4], [9], [10], [11], [12], [15], [16] have mentioned about whether to report GNSS position fix time duration in RRCReestablishmentComplete(-NB) and RRCConnectionReconfigurationComplete messages. The 8 companies think it needs to be reported and 4 companies think it is not needed. Based on these contributions the rapporteur would like to ask the following question:

**Question 1: Do companies agree that UE should report the GNSS position fix duration in RRCReestablishmentComplete(-NB) and RRCConnectionReconfigurationComplete messages?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Disagree | UE has reported the GNSS position fix duration during initial access and that will be stored as UE’s context in network side and that is sufficient for network to know for connected mode UE.  |
| Intel | Disagree | Agree with Oppo’s view |
| Nokia | Agree | In Rel-17, GNSS validity duration was agreed to be reported in RRCReestablishmentComplete(-NB) and RRCConnectionReconfigurationComplete messages. We don’t see motivation to differentiate the behaviour for GNSS position fix duration hence introduce more complexity. Furthermore, we think the GNSS position fix time duration maybe dynamically changed during the long connection if the UE starts moving or the (GNSS) propagation conditions changed a lot (e.g, shadowed). It is not reasonable to add a dynamic changed parameter as part of UE context (for inter-node information exchange). |
| Samsung | Disagree | We think it can be reported via UEInformationRequest/Response as it is not crucial.  |
| Xiaomi | Disagree | New eNB can retrive this information from old eNB. |
| Apple | Agree | We don’t understand the argument from companies saying that fix duration is already stored as UE’s context. Please note that in last meeting we agreed that fix duration will be carried in RRCResumeComplete message, where the UE context is also available at network side.  |
| Google | Agree | Same view as Apple that as we already agreed to carry the fix duration in the RRCResumeComplete message, the same information should be also carried during the re-establishment and HO procedure.  |
| Qualcomm | See comments | It should be sufficient to clarify that source transfers this info to target eNB when transferring UE’s current context.If not, better to agree this. |
| NEC  | Disagree  | We have similar view as others that it can be part of UE context.On the other hand, this is relevant to Q3 whether the fix duration can be changed during the connection time especially during handover. We are fine to go with majority view |
| ZTE | Agree with comments | To answer Apple’s question:For IoT NTN, UE needs to (re)acquire the GNSS position before establishing the connection to avoid interruption during the connection. This is also applicable to the case that a UE in idle/inactive resumes RRC connection. So it’s easy to have agreement on *RRCConnectionResumeComplete* for UE to report the latest value*.* However, RRC re-establishment and handover (only for eMTC) are different cases. Firstly, this is the common understanding that the target eNB also needs to know the GNSS position fix duration. Secondly, we assume UE would not re-acquire the GNSS position before it connects to the target eNB as this would cause additional (long) service interruption time, so GNSS position fix duration could keep unchanged. Since source eNB also has the same value as UE of the GNSS position fix duration, either way is feasible, e.g., to let UE to report this GNSS position fix duration to target eNB (Alt1), or to let target eNB acquires this value from source eNB via UE context retrieval procedure (Alt2).But we understand that, even we go for the UE context retrieval procedure (Alt2), this GNSS position fix duration value is not carried in UE context naturally. It should be firstly introduced into the AS configuration elements in the *HandoverPreparationInformation* message (see ***RRC Context*** -> ***UE Context Information*** IE in ***RETRIEVE UE CONTEXT RESPONSE*** in TS 36.423).In a summary, we are fine with either way: to include GNSS position fix duration in ***HandoverPreparationInformation*** message, or in ***RRCReestablishmentComplete(-NB)*** and ***RRCConnectionReconfigurationComplete*** messages. |
| Lenovo | See comments | Firstly we need to confirm whether the duration may be changed or not after the first report. If no, then either Alt.1 (UE report) or Alt.2 (context retrieval) mentioned by ZTE is OK; If yes, only Alt.1 can work. |
| Huawei, HiSilicon | Disagree | The GNSS position fix duration doesn’t change frequently. Note that apart from the HO case, during reestablishment, the UE may still stay in the same gNB. So it is better not let UE report every time when HO or RLF happens. |
| Turkcell | Disagree | It can be part of UE context.  |
| CATT | Disagree | If GNSS position fix time duration for measurement will not change during the UE RRC\_CONNECTED, we see reason to report it via *RRCreestablishmentComplete* and *RRCConnectionReconfigurationComplete* message.We can at least have a working assumption now, and can revise this if RAN1 have further agreement on whether GNSS position fix time duration for measurement will not change during the UE RRC\_CONNECTED. |
| MediaTek | Disagree | The network should be able to know the reported GNSS position fix time duration, it is not necessary to report the GNSS position fix time duration in RRCConnectionReestablishmentComplete(-NB) and RRCConnectionReconfigurationComplete. |
| CAICT | Disagree | Same view as CAICT. If GNSS position fix time duration will not change, it is no need to be reported via *RRCreestablishmentComplete* and *RRCConnectionReconfigurationComplete* message. |
| InterDigital | Agree | Agree with Nokia comments. Simpler to be consistent with R17. |
| CMCC | Agree | Share similar view with ZTE. |
| Ericsson | Agree | Agree with ZTE, it is much simpler to not require the transfer of this in UE context between eNBs.  |
| Sequans | Agree | Ideally, part of UE context + allow UE to signal a different value if required. |

**Rapporteur Summary**

8 out of 20 companies agree that UE should report GNSS position fix duration in RRCReestablishmentComplete(-NB) and RRCConnectionReconfigurationComplete messages. 2 more companies have not explicitly agreed, but their opinions are similar to agreeing to the question. 10 companies disagree that it is not needed as the GNSS position fix duration will not change and the network will know it anyway. As the companies are split almost evenly, the rapporteur suggests to make this issue for further discussion.

**Proposal 1: RAN2 will discuss if UE should report the GNSS position fix duration in RRCReestablishmentComplete(-NB) and RRCConnectionReconfigurationComplete messages.**

* **Msg3**

In last RAN2 meeting, an open issue was left as:

|  |
| --- |
| For UE to report GNSS position fix time duration for measurement during the initial access, at least the following Msg5 message can be used:  RRCConnectionSetupComplete, RRCConnectionSetupComplete-NB,  RRCConnectionResumeComplete, RRCConnectionResumeComplete-NB, FFS for RRCreestablishmentComplete and RRCConnectionReconfigurationComplete. FS for Msg3 |

Contributions in [1], [4], [14] tender to no need to for UE to provide GNSS position fix time duration in Msg3.

Contribution [16] thinks it may be beneficial in some cases to already transmit the GNSS assistance information in Msg3, in case there is sufficient UL grant available.

Based on these contributions the rapporteur would like to ask the following question:

**Question 2: Do companies agree that it is no need for UE to provide GNSS position fix time duration in Msg3?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Agree | It is not urgent to provide it in Msg3 as normally NW will use it after Msg5. Plus, Msg3 has a size limitation. |
| Intel | Agree |  |
| Nokia | Agree |  |
| Samsung | Agree | There is no motivation to have it in Msg3. And no need to overload msg3 and make scheduling more difficult.  |
| Xiaomi | Agree |  |
| Apple | Agree |  |
| Google  | Agree |  |
| Qualcomm | Agree |  |
| NEC  | Agree  |  |
| ZTE | Agree | Msg3 is very critical for successful RA procedure and its size should be kept as small as possible. |
| Lenovo | Agree |  |
| Huawei, HiSilicon | Agree |  |
| Turkcell | Agree |  |
| CATT | Agree |  |
| MediaTek | Agree |  |
| CAICT | Agree |  |
| InterDigital | Agree |  |
| CMCC | Agree |  |
| Ericsson | Agree |  |
| Sequans | Agree |  |

**Rapporteur Summary**

All the 20 companies have agreed that there is no need for UE to provide GNSS position fix time duration in Msg3. Hence, based on the unanimous consensus the rapporteur proposes the following proposal:

**Proposal 2 (20/20): There is no need for UE to provide GNSS position fix time duration in Msg3.**

* **Report of GNSS position fix time duration in connected mode**

This issue was discussed in the last RAN2 meeting and was postponed. Contribution [3] and [8] think GNSS fix time duration report is not needed during RRC connection. Contribution [10] thinks we can wait for RAN1’s progress. Contributions [12],[14] think UE reports GNSS fix time duration UEInformationRequest /UEInformationResponse which imply it can be reported in RRC connected. Since this issue is still open in RAN1, rapporteur suggest we wait for the progress in RAN1.

**Question 3: Do companies agree that we wait for the progress in RAN1 about UE report GNSS position fix time duration in RRC connected?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Agree with comments | We can wait for RAN1, but this is only about whether GNSS position fix time will change in RRC connected and whether reporting GNSS position fix time is triggered by its change. This should be decoupled with Q1 as the two RRC messages in Q1 are also related to RRC connected mode. |
| Intel | Agree |  |
| Nokia | Agree |  |
| Samsung | Disagree | We do not think that we need to leave this to RAN1.  |
| Xiaomi | Agree |  |
| Apple | Agree | It’s OK to wait for RAN1 progress. In general, we feel fix duration would not be changed during the RRC connection thus there is no need to have additional report in RRC connected state. |
| Google | Agree |  |
| NEC | Agree  | We are fine to wait |
| ZTE | Disagree | RAN1 has discussed this issue for several meetings. According to the RAN1 latest agreement “*UE reports* ***only one*** *GNSS position fix time duration for GNSS measurement at least when moving to RRC connected state”*, we understand RAN1 has achieved kind of common understanding that GNSS position fix time duration can be stable and there is no need for UE to re-report/update this value in connected mode, e.g., during the same connection. So it seems waiting doesn’t help. For moving forward, we suggest RAN2 to confirm that it’s no need for UE to report GNSS position fix time duration connected mode. |
| Lenovo | Agree |  |
| Huawei, HiSilicon | Agree | To our understanding, RAN1’s agreement mentioned by ZTE doesn’t exclude the report of GNSS position fix time duration in connected mode. The intention was to not let UE report more than one durations at one time when moving to RRC connected state. In this sense, it is still open in RAN1 and we should wait. |
| Turkcell | Agree |  |
| CATT | Agree with comments | Have the same view with OPPO. We also agree with ZTE to push progress, maybe RAN2 can have the following working assumption firstly:***RAN2 assumes that connected UE will not report GNSS position fix time duration.*** |
| MediaTek | Agree | Agree with Huawei |
| CAICT | Agree |  |
| InterDigital | Agree |  |
| CMCC | Agree |  |
| Ericsson | Disagree | We think is up to RAN2 to decide when this report will be needed. We propose **Proposal 3:** **Introduce a new RRC parameter gnss-fixDuration for reporting “GNSS position fix time duration for measurement”. The report gnss-fixDuration is triggered to be reported in the same places where gnss-validityDuration is triggered today.**  Regarding RAN1 agreement “*UE reports* ***only one*** *GNSS position fix time duration for GNSS measurement at least when moving to RRC connected state*”, the “***only one***” part is because RAN1 discussed if UE could report a number of values at the same time (for example one each for cold, warm, and hot start). Thus, not related to how often positionFixDuration would be reported. For validityDuration, the value reported by a UE will always be an estimation because the UE do not always know how much/fast it will be moving in the future (and if movement compensation is possible without acquiring new GNSS position fix). The state of the GNSS receiver may change during a connection, thus if UE anyway need to send the validityDuration we think the UE can send the positionFixDuration too.  |
| Sequans | Agree |  |

**Rapporteur Summary**

16 out of 19 companies agree that RAN2 needs to wait for the progress in RAN1 about UE report GNSS position fix time duration in RRC connected. 3 companies (Samsung, ZTE and Ericsson) do not agree to this. ZTE has mentioned that according to RAN1 agreement UE reports only one GNSS position fix time duration for GNSS measurement at least when moving to RRC connected state. However, as pointed out by Huawei and MediaTek, the RAN1 agreement was not for connected mode. Based on the wide majority, and since RAN1 has been working for quite some time, the rapporteur believes it is better to wait for RAN1. Hence, the rapporteur makes the following proposal:

**Proposal 3 (16/19): RAN2 will wait for further progress in RAN1 about UE’s reporting of GNSS position fix time duration in RRC connected state.**

## 5.2 Leaving RRC Connected State

In last RAN2 meeting an open issue was left as:

|  |
| --- |
| 2.FFS whether the UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has initiated a new measurement |

Contributions in [3], [5],[7], [10], [14] thinks UE can stay in RRC connected mode, Contribution [11] think we should wait for RAN1 conclusion on the mechanisms to allow UL transmission after original GNSS validity duration expires without GNSS re-acquisition.

Based on the majority view, rapporteur would like to ask the following question:

**Question 4: Do companies agree that UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has initiated a new measurement?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO |  | Maybe we should first discuss whether to stop the current GNSS valid timer if the UE has initiated a new measurement since anyway UE will have a new GNSS valid timer to start after GNSS measurement. Then we don’t need to consider the case of current GNSS validity timer’s expiry during GNSS measurement. |
| Intel | Agree | It’s unnecessary to let UE go to Idle if the GNSS coordinates can be acquired soon. |
| Nokia | Agree the revised the proposal. | We think the new GNSS measurement performed by UE should be started no later than the validity duration expiry or upon the expiry of the validity duration. Otherwise, it is not clear whether UE is allowed to perform UL transmission during the period in between the timer expiry and the start of measurement gap for GNSS measurement. So, we proposed as below:* *UE can stay in RRCCONNECTED state when current GNSS position becoming out-of-date if a new GNSS measurement* ***is performing*** *by the UE or* ***is to be performed*** *by the UE upon the validity duration expiry.*

On the new mechanism to allow UL transmission after original GNSS validity duration expires **without GNSS re-acquisition**, it is a different issue. We can wait for RAN1 progress. |
| Samsung | Agree | To OPPO: The GNSS validity duration is not really defined as a timer. And we think that it will be more complicated to define a stop and then a start. We have spec text on how this can be solved in R2-2304017. We are not sure with the clarification by Nokia. We think that if the GNSS validity is out-of-date and UE has not started a measurement, then it should go to idle mode as legacy. It needs to be started before the GNSS validity is out-of-date and the text seem to imply that it is about to be started. Agree with the clarification by Nokia, but we think that the agreement should be:**Proposal 4: UE can stay in RRC\_CONNECTED state when current GNSS position is out-of-date if the UE has initiated a new measurement before the GNSS becomes outdated according to GNSS validity duration.**  |
| Xiaomi |  | Agree with the intention, perhaps we need to wait for RAN1 to determine when to start the GNSS measurement. |
| Apple | Agree | We actually shared the same understanding in our contribution [9].Our preference is to handle the RRC state switching by a simple “validity duration timer expiry”. That is why we proposed when UE starts GNSS measurement, UE stops the validity duration timer (no expiry) which leads to the same outcome “UE stay in RRC connected state”.In short, we also agree with OPPO that we should discuss how to handle the validity duration timer when UE initiates the GNSS measurement. |
| Google | Agree in general | We agree in general but think it is not very clear what does the condition “if the UE has initiated a new measurement” mean. To avoid the confusion, we suggest re-wording the proposal as “**UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has ~~initiated a new measurement~~ entered/started a measurement gap**” |
| Qualcomm | Agree |  |
| NEC | Agree |  |
| ZTE | Yes with comments | Firstly, we also have sympathy with OPPO’s comments (not clearly understand the Samsung’s response) and agree it’s reasonable to let UE stop the current GNSS valid timer (if running) when UE initiates a new GNSS measurement. Then we don’t need to consider the case of current GNSS validity timer’s expiry during GNSS reacquisition.Secondly, our basic assumption is that, new GNSS measurement should be performed **upon** the expiry of the validity duration. This can help avoid unnecessary GNSS reacquisition, and also ensure each reacquired GNSS would be used for as long as possible. Furthermore, upon the expiry of the validity duration, even UE stop the UL/DL transmission and begin to reacquire GNSS, we assume UE is still in connected mode. In normal case (except C-DRX case), we cannot see any necessity that UE starts the new GNSS measurement **earlier than** the validity duration expiry. We disagree with above Apple’s comment that “validity duration timer expiry” should be the trigger of RRC state switching. In R17, just for avoiding possible complicated discussion on GNSS reacquisition process in connected mode, RAN2 agree to let the UE go back to idle state to reacquire GNSS. But this does not mean that the UE must go back to idle upon the expiry of the GNSS validity timer. We understand RAN1 also has no such assumption.Moreover, as we assume UE should start the new GNSS measurement upon the expiry of the validity duration, we think, normally, there is no such case that UE starts the new GNSS measurement **after** the expiry of the validity duration.We know RAN1 is discussing the possibility to allow UL transmission after original GNSS validity duration expires without GNSS reacquisition for some duration, e.g., at least when frequency error is within frequency error requirements. From RAN2 perspective, we suggest to keep consistent UE behaviour, e.g., stop UL transmission and begin to reacquire GNSS upon GNSS validity duration expires. An equivalent way to facilitate RAN1’s intention is to let eNB extend the current GNSS validity duration for the UE. That would result in longer interval between two times successive GNSS reacquisitions. |
| Lenovo | Agree |  |
| Huawei, HiSilicon | Disagree | In general, we think proper NW implementation can ensure this case doesn’t happen as the NW knows when the UE’s GNSS validity duration will expire. By implementation the NW can even trigger the UE to perform and finish GNSS measurement a little ahead of expiry. In other words, this a corner case, and there is no big issue if UE follows legacy Rel-17 behavior. |
| Turkcell |  | We can wait for the progress of RAN1.  |
| CATT | Agree with comments | We think that if the UE has initiated a new GNSS measurement before the current GNSS position becoming our-of-date, the validity evaluation of the current GNSS position should be ignored or stopped, i.e. RRC layer will ignore the indication from GNSS module. That is, the case described by the proposal should not happen.  |
| MediaTek | Agree | UE should be able to stay in connected mode when current GNSS position becoming out-of-date. Network can adjust the UE UL TA via Timing Advance Command MAC CE, so that the UL transmission can last longer even when the GNSS position has become out-of-date and the GNSS measurement has not initiated.GNSS validity duration extension is under discussion in RAN1, we are fine to wait for the progress of RAN1. |
| CAICT | Agree |  |
| InterDigital | maybe | Agree with Huawei in general. NW should initiate a new measurement in good time, so there’s no need to specify error handling for this case.However, we don’t have a strong concern if the majority of companies want to optimise.  |
| CMCC | Agree |  |
| Ericsson | Agree with comment | The details may need to be FFS. However, seeing the divergent views, it is better to wait some further progress in RAN1 on gaps and measurements, and if UE is allowed to transmit in UL after validityDuration or not…  |
| Sequans | Agree |  |

**Rapporteur Summary**

15 companies agree that UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has initiated a new measurement. 2 companies (Huawei and Interdigital) have disagreed as they think proper network implementation can take care of this problem. 2 companies (Turkcell and Interdigital) prefer to wait for more progress in RAN1. Ericsson (although agreeing to it) has also commented to wait for RAN1. Oppo mentions to first discuss whether to stop the current GNSS valid timer if the UE has initiated a new measurement, as the UE will anyway have a new GNSS valid timer to start after GNSS measurement. As there is some majority, the rapporteur suggests the following proposal:

**Proposal 4 (15/19): UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has initiated a new measurement**

**3.3 GNSS validity duration report**

* **Remaining validity duration or whole validity duration**

In last RAN2 meeting an open issue was left as:

|  |
| --- |
| 4.UE reports GNSS validity duration after GNSS measurement. FFS whether the UE reports every time or only if the validity duration changes. FFS if the duration is the remaining validity duration or the whole duration |

Contributions in [1], [2], [3], [5], [7],[9],[10],[11],[14],[15], [16] think the duration should be remaining validity duration while the contributions in [4],[8],[13] think the duration can be the whole duration.

Based on the majority view, rapporteur would like to ask the following question:

**Question 5: Do companies agree that the GNSS validity duration UE reported after GNSS measurement is the remaining validity duration?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Agree | Only remaining valid duration is useful for network to schedule the right timing of GNSS measurement gap. |
| Intel | **Agree** |  |
| Nokia | Agree | Following Rel-17 principle is fine. |
| Samsung | Agree | Same as Rel-17.  |
| Xiaomi | Agree |  |
| Apple | Agree | It has to be the remaining validity duration. Otherwise, network would need to know the starting point of “whole validity duration”. |
| Google | Agree | To align the Rel-17 UE behaviour. |
| Qualcomm | Agree |  |
| NEC | Disagreed | Report the whole GNSS validity duration could be enough and simple, and the start time of the whole validity duration could be the end of GNSS measurement gap triggered by gNBReport remaining validity duration does not really bring any gain regarding signalling overhead . moreover, most likely the remaining validity duration is equal to the whole validity duration if the MAC CE will be sent immediately after GNSS measurement. Finally, it will bring up issue of determining the start point of the remaining validity duration, considering possible retransmission.  |
| ZTE | Disagree | We think the reason for “reporting remaining validity duration” during initial access is no longer applicable to the connected mode case. In that initial access case it’s true that the eNB cannot know when the UE finished the latest GNSS measurement and started the related timer. In connected mode, if the UE always starts the GNSS measurement upon the expiration of GNSS validity duration timer, and the GNSS measurement can be finished at the end of the GNSS position fix time duration (implicit gap) and the new timer is also started, the eNB and the UE can always keep consistent understanding on the GNSS status. Sowe disagree with some concern that, if reporting “whole validity duration”, “*network would need to know the starting point of “whole validity duration”*”. The start point could be the time point of “expiration of last GNSS validity duration timer + GNSS position fix time duration”.By this way, UE does not need to report the remaining GNSS validity duration every time and the eNB also does not need to trigger UE to perform GNSS measurement every time before the GNSS validity duration timer close to timeout. Both UL and DL signalling overhead can be reduced. The only thing needed is to occasionally update the GNSS validity duration, which we assume is also rare case. |
| Lenovo | Agree | Same as Rel-17. |
| Huawei, HiSilicon | Disagree | Similar view with NEC that the start point of the validation duration should be the end of measurement GAP. It is much simpler and signalling-saving to report the whole validation duration only when it changes. |
| Turkcell | Disagree | The whole GNSS validity duration is enough for the sake of simplicity.  |
| CATT | Agree | Same as Rel-17. We cannot assume there is no delay for UE reporting GNSS validity duration (the UE may has no UL grant in time). And maybe we cannot assume the GNSS measurement duration is applied from the end of the GNSS measurement gap too, for we have the case that the UE can perform GNSS measurement automatously when no receiving eNB triggering, maybe without a measurement gap, and the eNB has no idea when the UE has finished the GNSS measurement. |
| MediaTek | Agree |  |
| CAICT | Agree |  |
| InterDigital | Agree | When the validity duration is reported after completing measurement then “whole” and “remaining” are actually the same thing, assuming the report is done within a few seconds, given that the smallest value is 10s. |
| CMCC | Agree |  |
| Ericsson | Agree |  |
| Sequans | Agree | Aligned with R17, anyway the granularity of this is very coarse. |

**Rapporteur Summary**

16 out of 20 companies agree that GNSS validity duration UE reported after GNSS measurement is the remaining validity duration. 4 companies are against this and suggests the UE to include the entire validity duration. While reporting the remaining duration is in line with Rel-17 agreements, the companies against it feel remaining validity duration report will need the “start point” of GNSS validity (end of measurement GAP). Based on the majority and in compliance with Rel-17 the rapporteur makes the following proposal:

**Proposal 5 (16/19):** **GNSS validity duration UE reported after GNSS measurement is the remaining validity duration.**

* **GNSS validity report (MAC CE or RRC signalling)**

RAN1 has agreed that the GNSS validity report is via UL MAC CE.

Contributions in [2], [3], [5], [8],[9],[10],[15], [16] think GNSS validity duration is reported by UE via MAC CE.

Contribution in [12] think GNSS validity should be reported via UEInformationResponse and UEInformationResponse-NB.

Based on the majority view, rapporteur would like to ask the following question:

**Question 6: Do companies agree that the** **GNSS validity duration should be reported via MAC CE?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Agree |  |
| Intel | Agree |  |
| Nokia |  | We can accept majority view (via MAC CE). |
| Samsung | Disagree | We do not think that these procedures should be in MAC at all. The reasons are: * The GNSS out-of-date handling is specified in RRC in Rel-17
* The GNSS position fix time we have agreed to report in RRC messages
* If we have UE-triggered GNSS measurements, these are likely triggered in RRC based on RRC configuration

Furthermore, in question Q4, we are discussing how to deal with the GNSS measurement related to current RRC procedures. In Q11 we are discussing connection between RLF and GNSS measurements and in Q12 we are discussing problems related to another RRC procedure. Do we really want to specify indications in-between MAC and RRC in these cases just because RAN1 made an uninformed decision?Our proposal is: **Proposal 6: GNSS measurements are triggered in RRC using an RRC command and GNSS validity duration reported via RRC.**  |
| Xiaomi | Agree |  |
| Apple | Agree |  |
| Google |  | We have similar view as Samsung that it would be simpler if RRC is the only layer involved (since it is relevant to the RRC state transition).  |
| Qualcomm | Agree | UE knows when to perform GNSS measurement. If this is received and GNSS validation is sufficiently long, UE does not have to trigger measurement.It continues UL/DL activities and could just inform network new validity duration.So there is really no security issue disrupting communication. |
| NEC | Agree  |  |
| ZTE | Agree | MAC CE may cause less signalling overhead. |
| Lenovo | Agree |  |
| Huawei, HiSilicon | Agree | There seems no security issue with this UL MAC CE. No strong motivation to reverse RAN1 agreement in this case. |
| Turkcell | Agree |  |
| CATT | Agree | Have the same view with Huawei.  |
| MediaTek | Agree |  |
| CAICT | Agree |  |
| InterDigital | Agree |  |
| CMCC | Agree |  |
| Ericsson | Disagree. | We need to ask RAN1 in an LS about the reasons why RAN1 have decided on the type of signalling to use which is normally a RAN2 issue. What are the requirements for security and delay of triggering and reporting of GNSS position fix? Using an MAC CE to trigger GNSS measurements is a major security risk, as an attacker may make UEs disappear, and is unreliable and therefore risk the UE not doing GNSS measurements that eNB has requested.We already have a defined way to report validityDuration in RRC, and all handling of timers and RRC state changes are described in RRC, thus it is a major redesign if this needs to be done in MAC instead. |
| Sequans | Agree |  |

**Rapporteur Summary**

16 out of 20 companies agree that GNSS validity duration should be reported via MAC CE. One company is okay to go with the majority. 3 companies disagree to this. While Samsung and Google believe that GNSS out-of-date handling is specified in RRC and hence RRC should be used to report GNSS validity duration, Ericsson has raised security concerns for using MAC CE, prefers to send an LS to RAN1 for this and wants to use RRC signalling. Based on the majority, the rapporteur suggests the following proposal:

**Proposal 6 (17/20): UE will report the GNSS validity duration by using a MAC CE.**

* **Report GNSS validity duration (every time vs. only if the validity duration changes)**

In last RAN2 meeting an open issue was left as:

|  |
| --- |
| 4.UE reports GNSS validity duration after GNSS measurement. FFS whether the UE reports every time or only if the validity duration changes. FFS if the duration is the remaining validity duration or the whole duration |

Contributions in [1], [2], [9],[14], [15],[16] think the UE always report the GNSS validity duration after GNSS measurement. Contributions in [3], [8], [10], [11] think the UE should report only if the validity duration changes.

Based on the majority, rapporteur would like to ask the following question:

**Question 7: Do companies agree that the UE always report the GNSS validity duration after GNSS measurement?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Agree |  |
| Intel | Disagree | Optimization is needed to save UE power if the GNSS validity duration doesn’t change all the time. |
| Nokia | Disagree | If the GNSS validity duration is not changed at all, repeat the same reporting is a waste of UE’s power consumption. |
| Samsung | Agree | We do not see any need of having optimizations here. Power saving is a bad argument – the power consumption due to performing a GNSS measurement will be several magnitudes larger compared to sending the report. This just makes the procedures more complicated for very weak reasons.  |
| Xiaomi | Agree | Given that UE anyway needs to tell network that it has come back from GNSS measurement, UE can use this as the indication. |
| Apple | Agree | This is the simplest way to align the new validity duration span. |
| Google | Agree | This would serve as an acknowledgement mechanism.  |
| Qualcomm | Agree | This is simplest and works as ack to network. |
| NEC | Disagree | We think it is good to avoid unnecessarily repetition of the same GNSS validity duration report after each GNSS measurement |
| ZTE | Disagree | Signalling overhead would be a reasonable argument to disagree reporting the GNSS validity duration after every time GNSS reacquisition.Furthermore:* Firstly, as mentioned in Q5, we don’t think eNB cannot know the starting point of “whole validity duration”. It could be the time point of “expiration of last GNSS validity duration timer + GNSS position fix time duration”.
* Secondly, some companies think the whole during is not appropriate since at least 1/2 UE-eNB RTT should be reduced when the eNB receives it. For strict alignment, it’s easy to understand no matter “whole validity duration” or “remaining validity duration” is reported, the1/2 UE-eNB RTT should be [subtract](https://dict.cn/subtract)ed from the reported value.
* Thirdly, RAN1 give no agreement that UE needs to send an explicit report to tell network that it has finished GNSS reacquisition. Another option given by RAN1 is that the reception of any UL transmission from the UE at eNB after the GNSS measurement.
 |
| Lenovo | See comments | Firstly we need to confirm whether the duration is fixed for any measurement. If yes, then report after measurement is not needed; If no, report after measurement is needed. |
| Huawei, HiSilicon | Disagree | Same comment with Q5:It is much simpler and signalling-saving to report the whole validation duration only when it changes. |
| Turkcell | Disagree | It can trigger unnecessary UE power consumption and signaling overhead.  |
| CATT | Agree | We think remaining validity duration will be reported in Q5, and the remaining validity duration can be different every time the UE report it. And maybe in some case, the report of remaining validity duration can be seen as an indication that the UE has finished the GNSS measurement, which is under discussion in RAN1. |
| MediaTek | Disagree | UE always report the GNSS validity duration is simplest way, but not power consumption optimized. And with UL transmission being the most power consumed action, it is worthy to be optimized. |
| InterDigital | Disagree | There are 2 issues here1. Whether UE needs to explicitly inform the network of a successful measurement. We think it does.
2. Whether validity time is reported only when it changes. We think it can be reported only when it changes. The change can happen after successful measurement (compared to previous measurement) or it could happen before expiry if the conditions change, in which case UE would trigger a new MAC CE with a new validity time without necessarily having performed a new measurement. In addition, uf UE is able to obtain a new GNSS fix without a gap then the new validity duration should be reported. In case MAC CE is used to inform the network of successful measurement then it may be short version if the validity time can be omitted. If successful measurement is implicit (E.g. reception of any UL transmission) then we can avoid sending the report altogether if the value is the same as the last reported value.
 |
| CMCC | See comments | Firstly, we would like to clarify our proposal means additional enhancement is needed if the UE only reports GNSS validity duration when it changes, e.g. an explicit indication is introduced to indicate the successful GNSS measurement. Anyway, we understand that the UE will report something about the successful GNSS measurement, implicitly or explicitly. Therefore, we think signaling is unavoidable. UE always reporting the GNSS validity duration is the simplest way, we are ok with it. |
| Ericsson | Agree | The UE may update its mobility state estimation, and thus it may change the validityDuration. After a GNSS measurement, it is good for eNB to get the UEs current estimate of validityDuration as well as the current UEs estimation of the positionFixDuration.  |
| Sequans | Agree with comment | We think the question is more if UE has to ack the successful measurement – which seems preferable.If yes it may be ok to always report (anyway no much saving in using some delta signaling).If not, would be better to avoid reporting if it has not changed. |

**Rapporteur Summary**

9 companies agree that UE always report the GNSS validity duration after GNSS measurement. 8 companies disagree, as this will involve signalling overhead and incur excessive power consumption in UE. 2 companies have raised the need for further clarifications and discussions. As the companies’ opinion are almost evenly split, the rapporteur suggests deferring this issue for further discussion.

**Proposal 7: RAN2 will further discuss if the UE will always report the GNSS validity duration after GNSS measurement.**

* **One or more attempts of GNSS measurement**

Contributions in [5], [7],[9] think when UE failed to obtain GNSS fix during the GNSS measurement gap, UE moves to idle. Contributions in [2], [3], if UE failed on getting GNSS fix, and there is another configuration that allows UE can do GNSS measurement again, UE can try another attempts of GNSS measurement.

Based on the contributions, rapporteur would like to ask the following question:

**Question 8: Do companies agree to allow multiple attempts of GNSS measurement when it is possible?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Disagree | If GNSS measurement during gap fails, then we don’t see any better chance to succeed using UE autonomous measurement supposing that GNSS coverage remains the same. In our understanding, UE autonomous GNSS measurement is only useful when UE has not received/tried the gap-based measurement requested by the network and GNSS validity timer expires. |
| Intel | Disagree | We prefer “UE moves to idle” in this case. |
| Nokia | Disagree | Similar view as OPPO. |
| Samsung | Disagree | Will be very complicated for the network to handle UEs if they can stay in connected and come back after several GNSS measurement attempts.  |
| Xiaomi | See comments | It depends on the measurement gap configured for the GNSS measurement. If the gap length is multiple of the time required for one GNSS measurement, UE can try multiple time for GNSS measurement.  |
| Apple | See comments | This is an interesting question. The assumption of the question is UE gets both the MAC CE indicated GNSS measurement gap and autonomous GNSS measurement configuration (which I suppose is based on RRC message). Basically, we prefer a simple handling that UE should go to idle if the first GNSS measurement fails. But we see this is somehow relevant to the validity duration handling, e.g, whether the validity duration timer should keep running during GNSS measurement. Probably we can discuss that first. |
| Google | Disagree | This seem to complicate the UE and NW too much. |
| Qualcomm | Disagree |  |
| NEC | Disagree  | It is not clear what “another configuration that allows UE can do GNSS measurement again” means  |
| ZTE | Disagree | We think “UE moves to idle” is a suitable process for this R18 exceptional case “UE fails to reacquire GNSS during connected mode”. Multiple attempts would not give help.We understand this issue is independent of the previous discussion, e.g., it doesn’t matter how the UE is triggered to initiate GNSS reacquisition. |
| Lenovo | Disagree | Seems impossible considering the length of GNSS measurement, and also introduces complexity. |
| Huawei, HiSilicon | Disagree | We see no big issue without this enhancement. |
| Turkcell | Disagree |  |
| CATT | Agree (the proponent) | Firstly, the UE is required (based on traffic requirement) to stay RRC\_CONNECTED state if the connected UE has triggered GNSS measurement, and if the has not finish GNSS position successfully during the configured gap, and the UE go to IDLE, then the UE will also have to continue to try GNSS measurement, and try to establish RRC connection, again.To the question of OPPO that, “UE autonomous GNSS measurement is only useful when UE has not received/tried the gap-based measurement requested by the network and GNSS validity timer expires”, RAN1 has no agreement that, if the UE cannot finish GNSS measurement during the configured gap, the UE will perform GNSS measurement autonomously. Further clarification to the question of NEC: “another configuration that allows UE can do GNSS measurement again” means that, the network can configure UE to try another one or more attempts if the UE has not finish GNSS measurement successfully during the configured gap.  |
| MediaTek | Agree | When UE is on the move, the GNSS measurement may not always be successful due to moving indoors or being under the bridge. Allowing the UE to have a second chance to acquire GNSS position will reduce the unexpected connection failures. |
| InterDigital | Disagree | We assume most of the time the gap will be sufficient, and we already have failure condition that UE moves to Idle. |
| CMCC | Disagree | We prefer that the UE moves to idle state if it fails to obtain GNSS fix during the GNSS measurement gap. |
| Ericsson | Not for RAN2 to decide. | Likely RAN1 will decide on these issues when discussing measurement gaps and timers after validityDuration with possible allowed uplink transmissions. Therefore, we need to wait on RAN1 progress. |
| Sequans | Disagree | Maybe moving to idle is simpler in that case. |

**Rapporteur Summary**

14 companies disagree to allow the UE making multiple attempts of GNSS measurement when it is possible. Only 2 companies, the proponent CATT and MediaTek agree to the proposal. 2 other companies (Apple and Xiaomi) mention that it depends on measurement gap configuration and validity timer duration. One company (Ericsson) has mentioned that it is better to leave it to RAN1. Hence, based on the majority, the rapporteur suggests the following proposal:

 **Proposal 8 (15/19): RAN2 will not discuss allowing multiple attempts of GNSS measurement.**

## 5.4 GNSS Measurement trigger

* **eNB aperiodcally trigger via MAC CE or RRC signalling**

RAN1 has agreement that the eNB aperiodcally trigger is via MAC CE. But in the last RAN2 meeting, companies have security concern on MAC CE, as it is not protected by AS security. if an attacker sends this triggering MAC CE – the UE would stop communicating and disappear from the network’s point of view.

Contributions in [2], [3], [9], [10] think eNB aperiodcally trigger is via MAC CE. Contributions in [12],[14] think it is via RRC signalling. Contribution in [8] thinks it can be RRC signalling, or DCI based.

Since RAN1 has made agreement on MAC CE, and RAN2 has divergence on this issue, rapporteur would like to ask the following question:

**Question 9: Do companies agree to send LS to RAN1 for RAN2’s security concern?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Disagree | We don’t see any security issue here, similar as other MAC CEs. Also RAN1 is not in the position to discuss/resolve security issues. |
| Intel | Disagree | If there is security concern, we could consult SA3 and CC RAN1. |
| Nokia | Disagree |  |
| Samsung | Disagree | No need for this. There are several other cases where using MAC CE causes a UE to go off for a long time as explained by some companies in the last meeting. We think that MAC CE is highly unsuitable for many other reasons.  |
| Xiaomi | Disagree | We don’t see any security issue. |
| Apple | Disagree | Though we also share the understanding that MAC CE is less secure than RRC message, it is hard to say what is the real issue here. Please note that there are several MAC CE commands introduced in Rel-18 features, e.g. for MIMO management. The situation is same here. For the security protection on the MAC CE, if needed, we can have a general enhancement for all the MAC CE commands in R19. |
| Google | No strong view |  |
| Qualcomm | Disagree |  |
| NEC | see comment | We cannot ask RAN1 if there is security concern, we agree this question is to SA3 instead.but we could inform the possible security concern of MAC CE/DCI comparing with RRC signalling. Moreover, it would be good to check why MAC CE is chosen instead of DCI if security is not a concern. in our view, DCI seems better than MAC CE if we the gap start time is refer to the receiving timing of the trigger |
| ZTE | Disagree with comments | From RAN2 perspective, we don’t think security issue to be the main factor to consider in choosing RRC or MAC CE.As we assume eNB don’t need to trigger UE every time the GNSS validity duration timer approaches expiration and such trigger can be just for enabling the function of GNSS reacquisition during connected mode in UE, we think RRC, e.g., Msg4, could be another feasible alternative. We are open to discuss. |
| Lenovo | Disagree |  |
| Huawei, HiSilicon | See comments | We are fine to send an LS to SA3 (cc RAN1). If there is security concern, we can solve it now because MAC CE is not the only way to serve the purpose. It is not good to disregart this concern and then afterwards we try to fix this again. |
| Turkcell |  | No strong opinion. We’re ok with the majority’s view.  |
| CATT | Disagree | If necessary, LS to SA3 can be used. But we can have the working assumption based on the RAN1 agreement.  |
| MediaTek | Disagree |  |
| InterDigital | Disagree | We have many operations and UL reports using MAC CE. The main security concern would be if any permanent identity and associated measurement (e.g. PCI + RSRP) is revealed but it is not. |
| CMCC | Disagree | We don’t see any security issue here. |
| Ericsson | Agree | RAN1 have not sent an LS to ask RAN2 to take their agreements into account. It may be that they have considered the security issues and signalling delay, but that is hard to know from the agreement alone. The LS from RAN2 may be sent to SA3 for the security questions, and to RAN1 for questions on the delays. The observation that there are other MAC CEs that can be used for an attacker is not an argument for introducing new MAC CEs with security issues. For the vulnerability of MAC CEs we recommend an internet search on LTE forged attack and read the first article <https://dl.acm.org/doi/full/10.1145/3534124> “Also RAN1 is not in the position to discuss/resolve security issues.” RAN1 is also not in the position to select the RAN2 signalling options.  |
| Sequans | Disagree |  |

**Rapporteur Summary**

14 companies believe there is no need to send an LS to RAN1/SA3 regarding the security concerns. Once company has no strong view and one company is okay to go with the majority. 3 companies, (the proponent Ericsson, NEC and Huawei) are in favour of sending the LS. As the majority is in favour of not sending any LS, the rapporteur suggests the following proposal:

**Proposal 9 (15/19): There is no need to send LS to RAN1/SA3 for RAN2’s security concern about using MAC CE for aperiodic triggering.**

* **UE autonomously trigger GNSS measurement in C-DRX inactive time**

Contribution in [4],[7] support UE autonomously reacquire GNSS during inactive state of C-DRX. Contribution in [11] thinks the discussion should be postponed for RAN1’s progress.

Since this topic was discussed in RAN1, rapporteur would like to ask the following question:

**Question 10: Do companies agree to postpone the discussion of UE autonomously reacquire GNSS during inactive state of C-DRX in RAN2?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Comments** |
| OPPO | Agree  |  |
| Intel | Agree |  |
| Nokia | Agree | From our point of view, RAN2 should prioritize the discussion on the basic functions of GNSS operation for long data connections (e.g. aperiodical triggered GNSS MG and autonomous GNSS MG). Based on that, RAN2 can further discuss whether the UE can reacquire the GNSS position fix outside the Connected DRX Active Time. |
| Samsung | Agree |  |
| Xiaomi | Agree |  |
| Apple | Agree |  |
| Google |  | We don’t think RAN1 will have much progress on this issue and also think this issue is more relevant to RAN2. But we are okay to follow the majority.  |
| Qualcomm | See comments | This is up to UE. If UE thinks it can fix the GNSS while being in DRX sleep, i.e., DRX cycle is long like 2.56s and 2 s is enough, it can do so without network knowledge.But agree UE can still send the new validity duration to network. |
| NEC  | Agree  |  |
| ZTE | Disagree | The general GNSS reacquisition upon expiration of GNSS validity duration would inevitably cause service transmission interruption. Meanwhile, it's easy to understand that GNSS reacquisition during inactive state of C-DRX can reduce such service transmission interruption as no DL/UL will be scheduled during inactive state of C-DRX. Therefore, we support to study this feature. We are considering not only the ideal case where the expiration of GNSS validity duration timer is just within the inactive state of C-DRX and the time length of inactive state is also long enough for UE to complete the GNSS reacquisition (as mentioned by QC), but also the possibility to allow UE to deliberately stop GNSS validity duration timer and start GNSS reacquisition early, e.g., during inactive state of C-DRX.As there would be some procedure-related issues, we think they are more suitable to be discussed in RAN2. |
| Lenovo | Agree |  |
| Huawei, HiSilicon | Agree |  |
| Turkcell | Agree |  |
| CATT | Agree |  |
| MediaTek | Agree |  |
| InterDigital | Agree | In general agree with QC, but OK to wait. |
| CMCC | Agree |  |
| Ericsson | Agree |  |
| Sequans | Agree |  |

**Rapporteur Summary**

16 companies agree to postpone the discussion of UE autonomously reacquire GNSS during inactive state of C-DRX in RAN2, as this is under discussion in RAN1. One company (Google) is okay to go with the majority. Only ZTE prefers to discuss this, and Qualcomm thinks this is up to UE. Hence, based on the wide majority the rapporteur suggests the following proposal:

**Proposal 10 (17/19): RAN2 will postpone the discussion of UE autonomously reacquire GNSS during inactive state of C-DRX until there is some more progress in RAN1.**

## 5.5 Other

* **Conflict between RLF and GNSS measurement**

During the long duration of GNSS measurement, the supervision of DL channel is still running, it will probably lead to a radio link failure as the UE has to suspend the DL receiving during the GNSS measurement. To address this issue, contributions in [1] and [5] thinks the UE suspends RLM and RLF monitoring when new GNSS measurement is triggered. Contribution in [4] if the out-of-sync evaluation period is shorter or equal than the GNSS position fix time duration, UE can firstly trigger RLF and reacquires GNSS position fix during RLF procedure. Contribution in [6] provides options: (1) suspend RLM; (2) configure a longer T310 to cover GNSS measurement gap; (3) suspend RRC reestablishment until the end of the gap.

Based on the contributions, rapporteur would like to ask the following question:

**Question 11: Which option do companies prefer to address the issue of possible RLF during the measurement gap?**

**Option 1: suspend the RLM**

**Option 2: if the out-of-sync evaluation period is shorter or equal than the GNSS position fix time duration, UE can firstly trigger RLF and reacquires GNSS position fix during RLF procedure.**

**Option 3: Network ensure the configuration of RLF detection can cover GNSS measurement gap.**

**Option 4: Keep the RLM but suspend the RRC reestablishment until the end of the gap.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comments** |
| OPPO | Option 1 | Suspending RLM is the simplest way as UE’s cellular module is suspended as well during GNSS measurement.For option 2, triggering RLF is not a good choice as gap-based GNSS measurement is intended to keep UE in connected mode without triggering RLF.For option 3, a longer T310 may delay RLF declaration and RRC re-establishment for the case when UE is not performing GNSS measurement. For option 4, UE is in fact not suffering RLF and it is just using gap to perform GNSS measurement and triggering RRC reestablishment will defeat the benefit of introducing gap-based GNSS measurement, which is supposed to keep UE in connected as much as possible. |
| Intel | Option 1 |  |
| Nokia | Option1 with comments | We tend to agree the principle that the RLM should be temporarily stopped during the gap while resume the monitoring after the gap. However, to minimize the impact to the spec (e.g., to avoid much impact on the UE behaviour in RAN4 spec), in case of there is a collision between T310 and GNSS MG, the simplest way seems to be UE extending the network configured T310 with the additional GNSS MG length to avoid any fake RLF declaration.  |
| Samsung | Option 1 |  |
| Xiaomi | Option 1 |  |
| Apple | Option 1 | Suspending RLM is the simplest way to go. |
| Google | Option 1 |  |
| Qualcomm | Option 1 |  |
| NEC | Option1 | Option2 and 4 will trigger Re-establishment unnecessarily Option3, it is not possible that a configuration will be suitable to both the time period with and without GNSS measurement gap.  |
| ZTE | Option 2 or Option 1 | It may be not always feasible to align RLF detection configuration with GNSS fix time duration (gap), so we understand anyway it’s possible for (some) UEs to encounter this situation that RLF occurs during GNSS reacquisition. Suspending RLM seems feasible but not so sure whether it would cause other issue. Fine to go with majority view now. But we assume we still can come back if new issue is identified. |
| Lenovo | Option 1 | In [6] we provide all possible options for discussion. We prefer Option 1 as it is simple to implement and can follow majority’s view. |
| Huawei, HiSilicon | Option 1 |  |
| Turkcell  | Option 1 | It’s the simplest one.  |
| CATT | Option 1 |  |
| MediaTek | Option 1 |  |
| InterDigital | Option 1 |  |
| CMCC | Option 1 |  |
| Ericsson | Option 1 |  |
| Sequans | Option 1 |  |

**Rapporteur Summary**

All 19 companies prefer “Option 1: suspend the RLM” to address the issue of possible RLF during the measurement gap. Only one company (ZTE) has included Option 2 also (besides Option 1) and is okay to go with the majority. Hence, the rapporteur suggests the following proposal based on unanimous preference.

**Proposal 11 (19/19): RAN2 selects “Option 1: Suspend the RLM” for addressing the issue of possible RLF during the measurement gap.**

* **Conflict between reading SIB31 in connected and GNSS measurement**

It is possible that T317 expired during the GNSS measurement gap. Contribution in [6] think in this case, UE should read SIB31 and postpone the GNSS measurement. Contribution in [15] think UE should perform the GNSS measurement and read SIB31 after the GNSS measurement.

Based on the contributions, rapporteur would like to ask the following question:

**Question 12: Which option do companies prefer to resolve the conflict between reading SIB31 in connected and GNSS measurement?**

**Option 1: Read SIB31 and postpone the GNSS measurement**

**Option 2: Postpone reading SIB31 until GNSS measurement**

**Option 3: Network configuration**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comments** |
| OPPO | Option 2 | Since GNSS measurement has been started, it is better not to interrupt/stop it. Plus, option 2 should be:**Option 2: Postpone reading SIB31 until GNSS measurement is done** |
| Intel | Option 2 |  |
| Nokia | FFS | If the UE can read the SIB31 before the start of MG, we wonder why the SIB31 reading or the GNSS measurement should be postponed.  |
| Samsung | Option 3 | We think that we should not complicate the T317/T318 procedures (for both network and the UE). If T318 has expired the UE goes to RLF as in Rel-17. The possible values of T317 and T318 should be able to solve this.  |
| Xiaomi | Option 2 | Agree with OPPO |
| Apple | Option 2 | UE should finish GNSS measurement before performing SIB31 acquisition. If the current GNSS info is not accurate, UE cannot acquire the SIB31 correctly since the DL propagation delay is not correct. |
| Google | Option 2  | Agree with OPPO |
| Qualcomm | Option 2 | Agree with OPPO |
| NEC | Option2 | It is normal that UE listen to NW, so GNSS measurement should be done based on the trigger. |
| ZTE | Option 2 | Option 2 seems more reasonable. But we assume we still can come back if new issue is identified. |
| Lenovo | See comments | In [6] we do not mean to postpone the GNSS measurement procedure to acquire SIB31. Our understanding is that, before a GNSS measurement start, UE may re-acquire SIB31 to ensure a valid ephemeris e.g., by implementation. Anyway, we can also accept Option 2 if it is majority’s view. |
| Huawei, HiSilicon | Option 2 |  |
| Turkcell | Option 2 | Agree with OPPO. |
| CATT | Option 2 |  |
| MediaTek | Option 2 |  |
| InterDigital | Option 2 |  |
| CMCC | See comments | We understand the UE can read SIB31 before GNSS measurement gap by UE implementation. We can also accept option 2 if it’s majority view. |
| Ericsson | FFS | Agree with Nokia.  |
| Sequans | Option 2 |  |

**Rapporteur Summary**

For resolving the conflict between reading SIB31 in connected and GNSS measurement, 14 companies agree with “Option 2: Postpone reading SIB31 until GNSS measurement”. Two companies (Lenovo and CMCC) think before a GNSS measurement start, UE may re-acquire SIB31 to ensure a valid ephemeris e.g., by implementation, but they are okay to go with the majority view. One company prefers a new Option 3: Network configuration of timers T317/T318. Two companies (Nokia and Ericsson) also believe UE can read the SIB31 before the start of MG, and hence there is no need to postpone reading of SIB31 or GNSS measurement. Based on the majority view, the rapporteur suggests the following proposal:

**Proposal 12 (16/19): RAN2 will use “Option 2: Postpone reading SIB31 until GNSS measurement is completed” to resolve the conflict between reading SIB31 in connected and GNSS measurement.**

# 6 Conclusion – first round

**Proposals with Consensus**

**Proposal 2 (20/20): There is no need for UE to provide GNSS position fix time duration in Msg3.**

**Proposal 11 (19/19): RAN2 selects “Option 1: Suspend the RLM” for addressing the issue of possible RLF during the measurement gap.**

**Proposals with Majority**

**Proposal 3 (16/19): RAN2 will wait for further progress in RAN1 about UE’s reporting of GNSS position fix time duration in RRC connected state.**

**Proposal 4 (15/19): UE can stay in RRC\_CONNECTED state when current GNSS position becoming out-of-date if the UE has initiated a new measurement**

**Proposal 5 (16/19): GNSS validity duration UE reported after GNSS measurement is the remaining validity duration.**

**Proposal 6 (17/20): UE will report the GNSS validity duration by using a MAC CE.**

**Proposal 8 (15/19): RAN2 will not discuss allowing multiple attempts of GNSS measurement.**

**Proposal 9 (15/19): There is no need to send LS to RAN1/SA3 for RAN2’s security concern about using MAC CE for aperiodic triggering.**

**Proposal 10 (17/19): RAN2 will postpone the discussion of UE autonomously reacquire GNSS during inactive state of C-DRX until there is some more progress in RAN1.**

**Proposal 12 (16/19): RAN2 will use “Option 2: Postpone reading SIB31 until GNSS measurement is completed” to resolve the conflict between reading SIB31 in connected and GNSS measurement.**

**Proposals for further discussions**

**Proposal 1: RAN2 will discuss if UE should report the GNSS position fix duration in RRCReestablishmentComplete(-NB) and RRCConnectionReconfigurationComplete messages.**

**Proposal 7: RAN2 will further discuss if the UE will always report the GNSS validity duration after GNSS measurement.**

# 7 References

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | [R2-2302543](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2302543.zip) | Discussion on GNSS operation for IoT NTN | OPPO |
| 2 | [R2-2302558](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2302558.zip) | Discussion on GNSS operation in connected mode | CATT |
| 3 | [R2-2302673](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2302673.zip) | GNSS operation enhancements | MediaTek Inc. |
| 4 | [R2-2302820](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2302820.zip) | Procedure of GNSS reacquisition | ZTE Corporation, Sanechips |
| 5 | [R2-2303044](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303044.zip) | GNSS fix in RRC\_CONNECTED | Qualcomm Incorporated |
| 6 | [R2-2303250](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303250.zip) | On GNSS position fix in RRC\_CONNECTED for IoT NTN | Lenovo |
| 7 | [R2-2303297](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303297.zip) | Discussion on the GNSS Validity Reporting in Connected State | Google Inc. |
| 8 | [R2-2303330](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303330.zip) | GNSS fix in connected mode | NEC |
| 9 | [R2-2303404](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303404.zip) | Improved GNSS Operation | Apple |
| 10 | [R2-2303518](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303518.zip) | Discussion on GNSS enhancement for IoT-NTN | CMCC |
| 11 | [R2-2303645](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303645.zip) | Discussion on enhancements on GNSS operation for IoT NTN | Nokia, Nokia Shanghai Bell |
| 12 | [R2-2303836](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303836.zip) | R18 IoT NTN GNSS operation enhancements | Ericsson |
| 13 | [R2-2303965](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2303965.zip) | Discussion on GNSS operation enhancements | Huawei, HiSilicon |
| 14 | [R2-2304017](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2304017.zip) | On improved GNSS operation for IoT NTN | Samsung R&D Institute UK |
| 15 | [R2-2304029](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2304029.zip) | Discussion on GNSS operation enhancement | Xiaomi |
| 16 | [R2-2304183](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_121bis-e/Docs/R2-2304183.zip) | GNSS acquisition and reporting for IoT NTN | InterDigital, Europe, Ltd. |