**3GPP TSG-RAN** **WG2 Meeting #118-e R2-200xxxx**

**Electronic, 9 – 20 May 2022**

**Agenda Item: 6.21.2**

**Source: Huawei, HiSilicon**

**Title: Summary of [AT118-e][082][TEI17] RRC Segmentation capability for UE capability report**

**Document for: Discussion and decision**

# Introduction

This document summarizes the following offline discussion for TEI17 UE capability reporting.

* [AT118-e][082][TEI17] RRC Segmentation capability for UE capability report (Huawei)

 Scope: allow time and discussion to check. Collect comments on the CR solution(s)

 Intended outcome: Report

 Deadline: CB W2 Friday (CRs by post meeting disc)

# Contact from companies

|  |  |
| --- | --- |
| Company | Email |
| Apple | naveen.palle@apple.com |
| Huawei, HiSilicon | zhaoyang@huawei.com |
| Vodafone | chris.pudney@vodafone.com |
| Intel | Sudeep.k.palat@intel.com |
| Qualcomm Incorporated | mkitazoe@qti.qualcomm.com |
| Nokia | amaanat.ali@nokia.com |
| BT | salva.diazsendra@bt.com |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Discussion

## Background

The below document was discussed online and only one company raised concern.

**RACS segmentation capability ind**

[R2-2205519](file:///C%3A%5CUsers%5Cmtk65284%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2_RL2%5CTSGR2_118-e%5CDocs%5CR2-2205519.zip) Indication of RRC Segmentation capability for UE capability report Huawei, HiSilicon, Apple, BT, CATT, CMCC, China Unicom, Ericsson, LG Electronics, Nokia, Nokia Shanghai Bell, NTT DOCOMO INC., Qualcomm Incorporated, Vodafone, ZTE Corporation, Sanechips discussion Rel-17 TEI17

R2-2206349 Indication of RRC Segmentation capability for UE capability report Huawei, HiSilicon, BT, CATT, CMCC, China Unicom, Ericsson, LG Electronics, Nokia, Nokia Shanghai Bell, NTT DOCOMO INC., Qualcomm Incorporated, Vodafone, ZTE Corporation, Sanechips discussion Rel-17 TEI17

DISCUSSION

* Intel think this should additionally be in the UE capability, to support inter-node messages.
* Apple think this is only needed at registration time, can always get UE capabilities and UE can respond back, so this is not needed. Apple has concerns on security. Apple think inter-node message is an issue.
* Huawei think that this is just one bit, and the full cap container is fully protected. Think we have already agreed to not forward early capabilities are not forwarded to core network. Agree that this should also be a normal UE capability.
* Apple think the network can try in any case. Huawei think that by understanding this earlier there can be a onestep UE cap inquiry. Apple think that the network can send two filters and the UE would use the one that can be supported.
* QC understand similar to Huawei. Don’t understand Apple reasoning.
* Chair: there is support for P1, only Apple is objecting. Can allow some time to check, will CB.

## Discussion

In case not yet all the companies read the paper, it is kindly remind that in R2-2206349 observation 2 and proposal 1 have explained the reason why this indication is useful. Here is a short summary of the paper:

In current spec the RRC segmentation function for UE capability report is enabled by the network blindly by including “*rrc-SegAllowed*” in the UE capability enquiry message without knowing whether the UE supports RRC segmentation or not. If this “*rrc-SegAllowed*” is received, The UE will perform segmentation only in case the UE supports RRC segmentation and the encoded UE capability message is larger than the maximum supported size of a PDCP SDU.

However, the network doesn't know whether the UE supports RRC segmentation or not before capability enquiry and thus it would be difficult for the network to decide whether to use multiple UE capability enquiry procedures for different RATs to avoid potential size problem. This can be avoided for segmentation capable UE if the support of RRC segmentation can be known by the network before capability enquiry procedure.

This cannot be done by UE capability reporting as usually the network doesn’t have the UE capability before capability enquiry except capability re-enquiry due to filter mismatch. Therefore, include this capability in msg5（RRC setup complete）is a more beneficial way to solve this issue.

**Proposal 1: include the indication of supporting UL RRC segmentation in RRC setup complete message for NR and LTE.**

**Q1: Do companies agree Proposal 1?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| Apple | We would like to get company views… for us this indication is not needed (so our resp is NO as of now). | As mentioned online and in the email, this has a few issues for which we would like views from companies:1. It is very easy to fake a MCG5 with false information that can lead to the NW incorrectly assuming wrong capability from the UE on it’s UL seg support. And the same functionality can be achieved by the NW providing two filters to the UE, a legacy one that UEs which support UL seg can ignore, and a new filter given with NCE (either R16 or R17 in UE capability enquiry) that is meant to be used by the UEs which support this feature.
2. If we agree to this CR, then the NW has to still deal with R16 (in the field) UEs which have not implemented this CR. So if the NW gets a “no UL seg support’ in MSG5 from these UEs, do the NW consider that these UE do not support UL seg? In our view, the existing Rel-16 functionality anyway can blindly as for UL seg, so this CR does not solve this issue, with or without early implementation.
 |
| Huawei, HiSilicon | Yes | To respond to Apple:1. Please note that we already agreed the below before “The network should retrieve UE capabilities only after AS security activation. Network does not forward UE capabilities that were retrieved before AS security activation to the CN.” This means capability indicator is allowed before AS security is allowed, but simply in this case this would not be forwarded to the CN. We understand anyway this bit does not need to be forwarded to the CN directly from MSG5, and this is not the only bit in MSG5 to indicate potential support of some features, thus we don’t see any problem.

We do not understand why two filters solve the problem. As long as the network does not know this in advance, the network has to set the filter in a conservative way to fit the UE capability size, thus maybe only few RATs would be requested and the network has to again re-enquire the capability. While getting this indicator in advance, the NW can enquire all the capabilities at the same time. [Apple] Two filter approach is similar to what we already do in Rel-16. In Rel-16, the NW asks the UE to segment (without knowing whether the UE supports or not, until after UE responds with UE cap). We can continue this approach where NW can provide a legacy part in UE capability enquiry and a new part. This new part would be the one which NW intends the UE use if the UE supports UL seg. All of this without NW knowing if the UE supports UL seg or not.For eg: the new part an contain request for all RAT containers, and/or an expanded set of filters. This approach helps, as there is no dependency from the UE. The NW can use the same UE capability enquiry msg to all UEs, and only UEs which support respond to the new filter. And so this approach is also useful for handling Rel-16 UEs (no dependency on whether UE implemented or not).1. This is like all other optimizations, new features can only be applicable to UEs supporting this. For UEs who supported such indicator (regardless which release), the benefits can be achieved. TEI means small enhancements, which in our understanding is to address such optimizations.

[Apple] As mentioned earlier, with current CR, the NW still had to follow legacy methods because there can be Rel-16 UEs which did not implement this CR BUT still support UL seg. Our proposals is simpler (we assume) to the NW in these situations.The main concern that is relevant here is we do not want the NW assume that UE does NOT support UL seg, if the UE did not set this bit in MSG5. With our proposal, there is no assumption needed at the NW at all (this is another issue along with the security issue). |
| Vodafone | Yes, BUT… | The Apple proposal does have some advantages:The UE RAC should only ever be sent by the UE on very rare occasions. For a R16 UE that supports RACS the UE RAC is only sent at the first ever power on in a PLMN. For a UE that doesn’t support RACS, it is about once every power on. Hence adding extra signalling for message 5 in every RRC connection setup seems quite an overhead (especially as this ‘support bit’ is sent after indications of support/non-support for many non-essential features). This extra message 5 signaling is a particular issue for LTE message 5 as the LTE Service Request procedure was heavily optimised (e.g. 16 bit rather than 32 bit NAS integrity check) to keep message 5 small (and, I think, of predictable size). Also, in LTE there are many releases of optional features that have to be shown as absent before the UE can signal that Segmentation is supported.\*\*\*\*\*An alternative is to clearly link the ‘optional’ presence of this parameter in message 5 so that it is sent only when the UE is performing a NAS mobility procedure (e.g. an Attach). |
| Intel | Yes | This could be useful though as Apple mentioned there may be UEs that may not support this in Rel-16 will require networks to implement with and without this feature.Response to VF: Agree that LTE Service request is very optimised and including this can potentially increase the IDLE to CONNECTED transition time that was a key KPI for LTE when Service request was initially designed. But for Service request, the network already has the full UE capability and this bit is not needed. Hence one solution is to include this bit only for NAS registration messages – that is, when selected PLMN/AMF are included.For NR/5GS, CT1 has not optimised the service request (we do not seem to care about the IDLE/CONNECTED delay) – so we could include this bit always or follow the above approach suggested for LTE.Regarding man in the middle attack, if the bit is also included in the UE capability itself, the network will know about the true UE capability at least when it retrieves the actual UE capability (over a secure link). Hence the consequences of the risk does not seem to be severe. |
| Qualcomm Incorporated | Yes | Agree with Intel on security. |
| Nokia | Yes | Agree with Intel on the security aspect, the impact is just transient.  |
| BT | Yes | About security concerns, a fake MSG5 can force the network to apply segmentation but the important bit here is that this fake capability will not be forwarded as the network has to wait until the connection is secured to forward any UE capability. As pointed by Huawei and Intel, we don’t observe a risk here. Similar security questions were asked to SA3 in RedCap WI as the RedCap needs to do early indication of 1Rx and/or 2Rx support in MSG3. The conclusion was that there is no risk, and we observe the same situation here.We are fine to follow LTE approach also for NR/5GS and include this bit only for NAS registration messages as proposed by Vodafone and Intel.  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**If proposal 1 is agreeable, the subsequent discussion is how to support it in case of handover.**

Generally it is also beneficial for the target RAN node to be aware about whether the UE supports segmentation: if the RAN node wants to re-enquire the capability, the filtering can be set appropriately after knowing whether UE supports it. In the original paper, it is proposed to include it in the AS-Context. During the online discussion, there were also comments raised on whether in the UE capability container needs to include this indication. This may be useful that once the capability is stored in the CN, the RAN node can retrieve this information from the CN.

**Proposal 2a: whether the UE supports UL segmentation is also indicated in AS-Context.**

**Proposal 2b: whether the UE supports UL segmentation is also indicated in UE capability container.**

**Q2: If companies agree P1, do companies have preference of 2a or 2b?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| Apple | No to 2a.No strong view on 2b, but we can accept if companies think this is useful (atleast for us this info is stale, as the NW now already has the UE capability) | We are wondering why would a RAN node need this UL seg support info outside of UE capability) in AS-context. If it meant for handover, the source node should have already gotten the UE cap and should be able to provide this info to the target via existing spec interfaces.Prop 2a results in a separate UL-seg info tied to the UE (via C-RTNI?) and another (legacy) UE capability container, so we have two set of UE info being exchanged, and we are very hesitantly of such procedures. In our view, this whole UL seg at MSG5 (if it is to exist) should be at the first transaction when the UE tries to RACH to the NW, where the NW does not have any UE context, only to be use by the gNB for preparation of UE capability enquiry procedure. This information should not be persistent, and should not be tagged to the UE and exchanged across nodes. |
| Huawei, HiSilicon |  | With the condition that MSG5 indicates the support, in the initial UE capability enquiry, the NW can get this information and then make suitable filtering. After that, whether to use Proposal 2a or 2b seems no big difference, we are open to discuss which way is better. |
| Vodafone | 2b | How does R16 RRC segmentation work for large RRCReconfigurationCommands if the RRC segmentation capability is not in the R16 UE Radio Access Capabilities? |
| Intel | 2b | If it is included in the UE capability, it will get transferred over network interfaces and IDLE/CONNECTED transitions without any additional specification work. Further, it will also be transferred across network nodes that do not support this additional indication in the AS context (this indication will be dropped by these nodes in 2a). |
| Qualcomm Incorporated | 2b | We think UE capability should be declared by the UE on top of Mag5 indication (this provides some security protection as discussed in Q1), and then the option 2b is natural option where the information provided with security protection is forwarded across nodes.  |
| Nokia |  | Agree that the indication from UE is the one which helps the network, after that phase the 2a and 2b are just ways for network to remember this to be passed on to the next node |
| BT | 2b | Agree with QC |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**About Early implementation**

If the above proposals are agreeable, the release to support this can be discussed. RACS are introduced in Rel-16 and proponents see benefits to introduce since Rel-16, however from some previous offline discussion there were also concerns raised that this might be too late for Rel-16. Therefore to change Rel-17 with early implementation from Rel-16 could be a compromised way forward. The options can be summarized as below.

Option 1: only change Rel-17

Option 2: change Rel-17 with early implementation to Rel-16

Option 3: change both Rel-16 and Rel-17

**Q3: please companies provide your preferred option.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option** | **Comments** |
| Apple | We are ok with any release, as we would like to progress, but as mentioned in the resp to Q1 with point #2, we are not sure if this helps, as there are already UEs with Rel-16 which will not be implementing this. The comment is posted again for convenience. | If we agree to this CR, then the NW has to still deal with R16 (in the field) UEs which have not implemented this CR. So if the NW gets a “no UL seg support’ in MSG5 from these UEs, do the NW consider that these UE do not support UL seg? In our view, the existing Rel-16 functionality anyway can blindly as for UL seg, so this CR does not solve this issue, with or without early implementation. |
| Huawei, HiSilicon | Either way is fine. | Please see our response in Q1, we do not understand Apple’s comment on legacy UEs. If MSG5 does not indicate the support, the network of course would use previous way to deal with it. For any optimizations, we only address UEs who supporting this new addition, not mentioning this is anyway a UE-specific enhancement.Slight preference of option 2, as we understand if some R16 UEs are willing to support so, option 2 provides this possibility.  |
| Vodafone | Option 2 if possible | This feature is most useful for UEs (in networks) that do NOT support RACS. Without RACS, it is useful once every UE power cycle.With RACS it is useful once per PLMN that the UE visits.(in response to Apple, the network needs to be able to cope with R15 UEs, so it does not matter if some R16 UEs don’t support this.) |
| Intel | Option 2 or 3 is fine | Even with option 3, networks will have to handle UE implementations that do not support this feature. As this feature is optional, we do not see a big difference between option 2 and option 3 in reality (other than in terms of specification work). |
| Qualcomm Incorporated | Option 2 or 3 |  |
| Nokia | Option 2 or 3, or even make this mandatory could be another option? | One could also think of making this mandatory from Rel-16 as this is useful feature? |
| BT | Option 3 or | We are fine to accept option 2 or mandatory from Rel-17. We understand that there are Rel-16 UEs on field but we will have a clean start in Rel-17 so it should not be a problem to make it mandatory as suggested by Nokia. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Q4: please companies provide comments on CR details. [To be discussed once Q1-Q3 are concluded]**

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Apple | **We also would like to confirm that the intention from the proponents of the CR, is that this is ‘optional’ capability, and the UEs which actually support UL seg, do NOT need to mandatorily set this field.**  |
| Huawei, HiSilicon | Yes, this is optional as we showed in the TP. |
| Apple2 | Our intent is to raise the issues that we perceive this CR brings, to the attention of companies. If companies think there are minor issues, then we would not persist with strong objections, in the interest of progress. To us, we cannot accept P2a (inter-node in AS-config) and we think it’s better to add a UE capability field inside the capability (P2b). Even though we are fully sure how useful this capability is, we are ok to have this added – the NW would atleast know that UE does support UL seg, once it reads the UE capability.  |
| Vodafone | Would be good to clearly link the optional use of this parameter to only the RRC connection Setups used by NAS procedures (e.g. Attach) that can trigger UE RAC retrieval. |
| Nokia | Okay for the field to be optional BUT UEs that support UL segmentation are required to set the field, correct? So this is like a IOT bit? We are fine to have it like this.Of course as Apple mentioned if the UE doesn’t support this then it is not required to set the bit. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Conclusion