# This document is to collect companies' views on "how to deal with the case that UE don't use DNS configuration from MNO"

* Please select one answer or add other berief answer to the "Answer" cell. If you have no strong view, please keep the "Answer" cell empty.
* If necessary, you can provide details in the comments cell.

1. 5GC sends a DNS server(e.g. EASDF) to UE via PDU session procedure.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q#** | **Question** | **Company name** | **Answer** | **Comments** |
| Q1.1 | whether SMF shall be able to inform UE that the DNS configuration provided by the 5GC is for edge services? | AT&T | * *yes but only one (Q1.1 or Q1.2) is needed – not much difference between the two* | Simply informing lower layers in UE is useless unless UE has ability to expose this information to HLOS and apps residing on UE |
|  |  | NTT DOCOMO | * *Yes* |  |
|  |  | Qualcomm | * *Yes* |  |
|  |  | Nokia | no | If the UE is not using the DNS server indicated by the 5GC, why would it obey to an extra information related to the DNS server indicated by the 5GC |
|  |  | Sony | * *Yes* |  |
|  |  | Vodafone | * *Maybe yes* | Agree with AT&T view. If the information stays at the lower layer, it is somehow useless, \*unless\* further actions are applicable at that lower layer. |
|  |  | Charter | * *Yes* |  |
|  |  | Futurewei | * *No* | The UE is aware of PDU sessions that relate to edge service and should have its own mechanism to prevent overwriting. |
|  |  | vivo | * *No* | The DNS configuration in UE OS has very low probability to be changed by user or application. Also, UE has its own strategy to decide which DNS used or not. So, this indication is useless. |
|  |  | Verizon | * *Yes* | Even if the SMF informs the UE, there needs to be a mechanism where the HLOS maps the specific DNS configuration changes only to the EDGE specific App. IF the DNS configuration change is done via the PCO, the PDU sessions may carry multiple QoS Flows from different Apps, these changes disrupt the other flows. |
|  |  | Apple | * *Yes* | Providing this information to the UE helps UE OS/user to make informed choices.  Additionally, provisioning information about support of DNS over HTTPS would be beneficial for the UE. |
|  |  | China Mobile | * *Yes* |  |
| Q1.2 | whether SMF shall be able to inform UE should not bypass the DNS configuration provided by the 5GC? | AT&T | * *yes but only one (Q1.1 or Q1.2) is needed – not much difference between the two* | Simply informing lower layers in UE is useless unless UE has ability to expose this information to HLOS and apps residing on UE |
|  |  | NTT DOCOMO | * *no* | Sending the information to the UE should be associated to EC features in the 5GS. The MNO should not simply “lock” the DNS configuration without indicating the reason. |
|  |  | Qualcomm | * *yes* | An indication to the UE lower layers should be provided so that, based on implementation, the UE may be able to enforce the DNS configuration provided by the 5GC |
|  |  | Nokia | * no | If the UE is not using the DNS server indicated by the 5GC, why would it obey to an extra information related to the DNS server indicated by the 5GC |
|  |  | Sony | * *no* | It is sufficient to support Q1.1 |
|  |  | Vodafone | * *not really needed, Q1.1 should be sufficient* | If UE is informed that the DNS is for EC services, this should be enough. |
|  |  | Charter | * *Yes* |  |
|  |  | Futurewei | * *No* |  |
|  |  | vivo | * *No* | Whether and how the UE or application bypass the DNS configuration is totally the UE internal behavior and application’s strategy. |
|  |  | Verizon | * *Yes* | Even if the SMF informs the UE, there needs to be a mechanism where the HLOS maps the specific DNS configuration changes only to the EDGE specific App. IF the DNS configuration change is done via the PCO, the PDU sessions may carry multiple QoS Flows from different Apps, these changes disrupt the other .flows |
|  |  | Apple | * *No* | No, the option should be left to the UE OS / Application/user. |
|  |  | China Mobile | * *Yes* | The PDU session can be established for specific URSP(which may be intent for Edge Computing applications), so in this case enforcing UE to use the DNS configuration from 5GC is OK. |

2. If a UE bypasses the DNS server configured by SMF (i.e. the HLOS DNS setting is changed), then:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q#** | **Question** | **Company name** | **Answer** | **Comments** |
| Q2 | shall UE detect the bypassing? | AT&T | * *yes, if UE has the capability?* | “no” acceptable if functionality in comments of Q1.1 and Q1.2 can somehow be specified or enforced in the UE. |
|  |  | NTT DOCOMO | * *yes, if OS/App can use the information* | This could be considered, but the consequent action should be to notify the user or app that this may result in degraded performance. |
|  |  | Qualcomm | * *yes, if UE has the capability* |  |
|  |  | Nokia | *NO* | MUCH better to have network detection (this works on any UE) and then no need for UE to inform 5GC of the bypassing |
|  |  | Sony | * *No, as long as Q1.1 is supported* | An Edge aware application in the UE need to use the expected DNS configuration |
|  |  | Vodafone | * *Yes, if the UE has the capability* | The important point here is \*how\* the lower layer in the UE is to detect it |
|  |  | Charter | * *NO* | Network should detect and mitigate |
|  |  | Futurewei | * *No* | If DNS configuration is bypassed, the user is consciously making such changes and that it may not get optimal service. |
|  |  | vivo | * *No* | The UE has no authority to detect or modify the applications’ packets. This detection and hijack have serious legal and privacy issues. The UE does not accept this risk. |
|  |  | Verizon | * *yes, shall if UE has the capability* | For UE to detect the bypassing, and inform 5GC would need NAS signaling changes with heavy dependency on the HLOS. |
|  |  | Apple | * *No* | No. UE cannot be expected to detect such actions. |
|  |  | China Mobile | * *Yes* |  |
| Q2.1 | If yes to Q2, shall UE inform 5GC of the bypassing? | AT&T | * *yes, if UE has the capability?* | “no” acceptable if functionality in comments of Q1.1 and Q1.2 can somehow be specified or enforced in the UE. |
|  |  | NTT DOCOMO | * *no* | It should be handled in the UE. |
|  |  | Qualcomm | * *yes, if UE has the capability* |  |
|  |  | Nokia | * *NO* | MUCH better to have network detection (this works on any UE) and then no need for UE to inform 5GC of the bypassing |
|  |  | Vodafone | * *yes, definitely* | The network shall take actions and manage the implications, e.g. at SLA, charging, anchoring, etc. |
|  |  | Charter | * *Yes* |  |
|  |  | Futurewei | * *No* |  |
|  |  | vivo | * *No* | The UE has no authority to detect or modify the applications’ packets. This detection and hijack have serious legal and privacy issues. The UE does not accept this risk |
|  |  | Verizon | * *yes, if UE has the capability* | For UE to detect the bypassing, and inform 5GC would need NAS signaling changes with heavy dependency on the HLOS. |
|  |  | Apple | * *No* |  |
|  |  | China Mobile | * *Yes* |  |
| Q2.2 | If yes to Q2, shall UE redirect the DNS query to the DNS server configured by MNO (e.g. EASDF)? | AT&T | * *yes, if UE has the capability?* | “no” acceptable if functionality in comments of Q1.1 and Q1.2 can somehow be specified or enforced in the UE. |
|  |  | NTT DOCOMO | * *no* |  |
|  |  | Qualcomm | * *yes, if UE has the capability* |  |
|  |  | Nokia | * no | The network can take more elaborate decisions such as sending the DNS request to the DNS server selected by the UE Appp/HLOS via the EASDF. UE redirecting to EASDF loses the UE willingness to use a specific DNS server |
|  |  | Vodafone | * *yes, if UE has the capability; network should be informed of detection and possible redirection redirection* | The network should be notified that the UE redirection can be applied; UE shall not take any action by itself. |
|  |  | Charter | * *Yes IF UE has capability* | Preferably network should detect and mitigate |
|  |  | Futurewei | * *No* |  |
|  |  | vivo | * *No* | The UE has no authority to detect or modify the applications’ packets. This detection and hijack have serious legal and privacy issues. The UE does not accept this risk. |
|  |  | Verizon | * *yes, if UE has the capability* | For UE to detect the bypassing, and inform 5GC would need NAS signaling changes with heavy dependency on the HLOS. |
|  |  | Apple | * *No* | Redirecting DNS queries in this manner goes against the privacy and security offered to the user. |
|  |  | China Mobile | * *yes, if UE has the capability. And whether this can be used also depends on agreement between operators and 3rd parties (who own the application).* |  |

3. 5GC reactions If a UE bypasses the DNS server configured by SMF:.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q#** | **Question** | **Company name** | **Answer** | **Comments** |
| Q3 | shall 5GC/UPF be able to detect the bypassing? | AT&T | * *yes* |  |
|  |  | NTT DOCOMO | * *no* | Detection can be done also out of 3GPP scope. Detection in the 5GC/UPF is needed only if 5GC corrective actions are specified as well. |
|  |  | Qualcomm | * *yes* | It should be a possibility |
|  |  | Nokia | * yes | And the network can take corrective actions even in case of encrypted DNS requests |
|  |  | Sony | * *no* | 1. Not needed as long as Q1.1 is supported to an edge aware application. 2. Detection will not help unless 5GC is able to perform correctional action on all (including encrypted) DNS request |
|  |  |  | * *Yes* | Either by itself or by notification from the UE. |
|  |  | Charter | * *Yes* |  |
|  |  | Futurewei | * *Yes* | For all DNS (encrypted and clear), header fields can be used to detect. For Do53, additional inspection is possible. |
|  |  | vivo | * *No* | This is the application’s or user’s privacy. It had better not sniff the packets. |
|  |  | Verizon | * *Yes* |  |
|  |  | Apple | * *No* | We do not encourage this approach. The Application provider, MNO, 5GC, UE, OS and the end-user are key stakeholders in providing/experiencing the edge services and any unilateral action in 5GC has an effect of upsetting the trust between them. |
|  |  | China Mobile | * *yes* | 5GC should know whether the EC configuration is used in UE side or not. |
| Q4 | shall 5GC be able to send the DNS queries via the DNS server configured by MNO (and control the EASDF to then use the DNS server selected by the UE)? | AT&T | * *yes* |  |
|  |  | NTT DOCOMO | * *no* | It does not work with encrypted DNS. And (regardless encryption), if the app does not use the MNO’s DNS address, the DNS query should just be routed to its destination. |
|  |  | Qualcomm | * *yes* | It should be a possibility |
|  |  | Nokia | * yes | It works with non encrypted DNS requests and can allow EASDF to trigger SMF actions (UL CL/BP insertion, SSC mode 2 / 3) |
|  |  | Sony | * *no* | Same as our answer on Q3 |
|  |  | Vodafone | * *maybe yes* | Not sure the question is totally clear 😊 as the DNS server configured by the MNO is the EASDF, or is this a different DNS server? And when referring to 5GC… which of the many NFs would be involved? |
|  |  | Charter | * *Yes* |  |
|  |  | Futurewei | * *Yes* | May allow additional network setup with EASDF for Do53 |
|  |  | vivo | * *No* | This will break the DNS integrity and the IP replacement is the DNS hijack. |
|  |  | Verizon | * *Yes* |  |
|  |  | Apple | * *No* |  |
|  |  | China Mobile | * *Yes* |  |
| Q5 | shall the mitigation measures (as mentioned in Q3 and Q4) done by the 5GC be specified? | AT&T | * *yes* |  |
|  |  | NTT DOCOMO | * *no* | Is there any mitigation measure (involving UP traffic impact) that would be acceptable to application providers? |
|  |  | Qualcomm | * *yes* |  |
|  |  | Nokia | * yes | there any mitigation measures that would be acceptable to application providers: UL CL/BP insertion (based on UE location) or even reaching via EADSF the DNS server selected by the UE App are actions transparent to the App (provider)  UL CL/BP insertion (based on UE location) relies on information provided by AF on target FQDN and IP addresses via Nnef-traffic-influence . In this case ( UL CL/BP insertion based on UE location) FQDN is not used but IP addresses. |
|  |  | Sony | * *no* | Same comment as NTT DOCOMO. Already today the easiest way for a large application service provider to avoid strange behavior in different networks is to add end to end encryption to avoid “optimizations” in the networks so the service is always working. |
|  |  | Vodafone | * *yes* |  |
|  |  | Charter | * *Yes* |  |
|  |  | Futurewei | * *Yes* |  |
|  |  | vivo | * *No* | Whether and how the 5GC detect or replace the applications’ packets are implementation. And this also has the problem in DNS hijack and user’s privacy. This part is not suitable for standardization. |
|  |  | Verizon | * *Yes* |  |
|  |  | Apple | * *No* | We think no network action in this regard should be specified in the TS. |
|  |  | China Mobile | * *Yes* |  |