**3GPP TSG-WG SA2 Meeting #141E e-meeting *S2-200xxxx***

**(revision of S2-200xxxx)**

**Source: Huawei, HiSilicon**

**Title: KI #2, Solution #8 - Solution update**

**Document for: Approval**

**Agenda Item: 8.6**

**Work Item / Release: ATSSS / Rel-17**

*Abstract: This paper updates Solution 8 to resolve the Editor’s Notes.*

# Introduction/Discussion

This paper updates Solution 8 to resolve the Editor’s Notes. Addtionally, in the non-transparent QUIC proxy solution, the SOCKv5 protocol is replaced by the MASQUE protocol and is described in an independent subclause. See some reasoning to remove the following ENs:

Editor's note: It is to be decided whether the QUIC proxy functionality should be updated as UDP proxy functionality or others.

The QUIC proxy described in this solution is comparable to MPTCP proxy defined in Rel-16, both of which run the QUIC or MPTCP between the UE and UPF. Therefore, we believe the solution is a QUIC proxy functionality, rather than UDP proxy. The corresponding EN is removed.

Editor's note: It is FFS if and how UDP fragmentation can be supported.

The UDP fragmentation can be avoided by restricting the maximum QUIC packet size on QUIC protocol level. The corresponding EN is removed.

Editor's note: The impact from operating the QUIC protocol over two different accesses is FFS.

How QUIC protocol runs over two accesses especially regarding the impact on lost and congestion control are added and the EN is removed.

Editor's note: The impact on UE and UPF is FFS.

The impact on UE and UPF is updated and the EN is removed.

The SOCKv5 for UDP is mainly applied to send the remote Server IP address and UDP port to the Proxy by using an additional header in every user packet. The MASQUE protocol can also satisfy this requirement via HTTP message, without the addition on the packet header. Therefore, in order to avoid waste of transmission resources, it is proposed to replace SOCKv5 by MASQUE, and the corresponding ENs regarding SOCKv5 are removed.

# 2. Text Proposal

It is proposed to capture the following changes in the TR 23.700.

\* \* \* \* First change \* \* \* \*

## 6.8 Solution #8: Proposed solution based on QUIC

### 6.8.1 Introduction

This solution addresses KI#2 on Additional Steering Functionalities.

This solution allows transport of the IP/UDP based application traffic by using QUIC protocol via multiple paths. It addresses two cases:

1) the QUIC functionality is supported by the UE, and with the QUIC proxy functionality enabled in the UPF, the QUIC connection can be established between the UE and UPF;

2) the QUIC functionality is implemented by the application layer between the UE and the application server.

As the QUIC connection cannot detect multiple paths, the Rel-16 ATSSS-LL, which supports four steering modes, Priority-based mode, Load-balancing mode, Smallest Delay mode and Active-standby mode, is still needed to perform traffic steering, switching, and splitting, Therefore, this solution proposes to apply a combination of QUIC functionality and ATSSS-LL functionality as a new steering method enabling UDP flows to use multiple paths, addressing the KI#8 on additional steering methods.

### 6.8.2 High-level Description

The QUIC functionality in the UE applies the QUIC protocol defined by IETF draft-ietf-quic-transport-27: "QUIC: A UDP-Based Multiplexed and Secure Transport". Additionally, the unreliable packet transported is also applied, the QUIC extensions are defined in draft-ietf-quic-datagram: "An Unreliable Datagram Extension to QUIC". It may be implemented by the operating system or by the application layer. This QUIC functionality in the UE will communicate with the QUIC Proxy functionality in the UPF or QUIC functionality in the remote server. The solution details for each case are described as below.

**QUIC connection between the UE and the UPF:**

The QUIC connection is established between the UE and the UPF per IP flow. This case is applicable to the UDP (without QUIC) based applications.

The QUIC functionality in the UE obtain the application data (i.e. UDP payload) and put it into QUIC datagram as unreliable QUIC transport is applied. Then after the QUIC header is added, the QUIC packet is encapsulated with a UDP header. The UDP fragmentation can be avoided by restricting the maximum QUIC packet size.

NOTE 1: ECN can be supported. For transparent proxy mode, the IP/UDP headers of the original packet are transported between UE and UPF without any change. For non-transparent proxy mode, all the IP/UDP headers of the original packet are transported unchanged except the source IP address and port for downlink packet and destination IP address and port for uplink packet.

The following Figure 6.8.2.-1 shows the QUIC functionality in the UE model and its relationship with the other functionalities.



Figure 6.8.2-1: QUIC Functionality in the UE

As shown in the above Figure 6.8.2-1, the application data is encapsulated by the QUIC functionality and then transported to the ATSSS-LL functionality. The ATSSS-LL functionality decides on the path for transport of the QUIC packet based on the link performance measurement of PMF. But different from the R16 ATSSS solution, in which the ATSSS-LL could only split a SDF per traffic on both accesses, the ATSSS-LL functionality can split a traffic per packet on both accesses with combination of QUIC functionality, to take advantage of both access resource to raise bandwidth, since the QUIC functionality supports the packet reordering with the sequence number included in the QUIC header. Especially, compared with TCP, the QUIC ACK frame contains one or more ACK ranges. Each ACK range could identify acknowledged packets and also contain additional ranges of packets which are alternately not acknowledged (Gap). With such enhancement, the QUIC protocol can solve the packet disordering issue received from lower layer, e.g. ATSSS-LL.

The traffic steering, switching or splitting is performed by the ATSSS-LL functionality, so there is no need to allocate the link-specific IP address for the UE as MPTCP functionality. Therefore, only one UE IP address of the MA PDU session is applied.

NOTE 2: The QUIC congestion control mechanism can be able to handle the packets in a single QUIC Connection transported via different paths, which can be different in packet delay, jitter, loss ratio etc, since this is the normal case over the Internet. For example, the different packets transported over the internet between the Client and the Server may be routed via different intermediate nodes. This is similar for this QUIC based solution for ATSSS where the packets go via different paths, i.e. 3GPP and non 3GPP accesses, between the UE and the UPF.

NOTE 3: When the path performance, e.g. the RTT, is quite different over 3GPP and non 3GPP accesses, the convergent bandwidth if applying packet splitting via two paths may not be higher than packet transport via only single path with higher performance, due to the impact of packet delay over the poor quality path, no matter which splitting method is applied, including MPTCP. This can be alleviated by implemention in the UE and the UPF or by enforcing some specific steering modes, to avoid packet splitting in case there is a big difference of the performance, e.g. RTT, between the two accesses.

NOTE 4: QUIC loss detection and congestion control as defined in IETF: “draft-ietf-quic-recovery” and ATSSS-LL with ePMF can work together to achieve the similar congestion control as MP-QUIC as defined in the MP-QUIC draft, i.e. QUIC performs the packet reordering and controls the sending window, and ATSSS-LL takes responsibility to select the access/path based on the link status reported by ePMF for each access. The upper QUIC protocol sees one link over two paths, and a single buffer memory is shared by both paths to perform packet reordering. If a packet is lost over one path/access (e.g. 3GPP access, due to congestion), the QUIC congestion controller will limit the overall transmission rate, whatever there is congestion or not over the other path. Actually, it is the same for MPTCP and MP-QUIC to couple the two paths for congestion control, as described in the MPQUIC draft: “*the windows of the different sending uniflows MUST be coupled together [RFC6356]*”. The RFC 6356 defines “Coupled Congestion Control for Multipath Transport Protocols”.The QUIC proxy functionality is enabled in the UPF, and it can be transparent QUIC proxy, or non-transparent QUIC proxy. For both transparent and non-transparent solutions, the UE needs to enable the QUIC stack in the data path based on the QUIC steering method indication from SMF. The difference is that for transparent QUIC proxy, the traffic packets transported in the QUIC connection are encapsulated with the remote Server IP address, while for non-transparent QUIC proxy, the traffic packets transported in the QUIC connection are encapsulated with the QUIC proxy IP address. The protocol stack for both transparent and non-transparent QUIC proxy is as described in Figure 6.8.2-3. The transparent QUIC proxy and non-transparent QUIC proxy solutions are described separately in the following subclauses 6.8.2.1 and 6.8.2.2.

NOTE 5: In case TLS 1.3 is applied, the UE will accept the credential of UPF during QUIC connection establishment procedure for both transparent and non-transparent QUIC proxy, as the UE knows the QUIC connection is established between the UE and UPF.

NOTE 5: There is no need to support both transparent and non-transparent proxy.

#### 6.8.2.1 Transparent QUIC proxy solution

The UE and UPF establish the QUIC connection, and the UPF apply regular UDP to the remote host. The packet from the UE is encapsulated with the destination IP address of the remote server. The QUIC packet is received in the QUIC connection. The UPF removes the QUIC header and then forward it to the remote host by using UDP.

One or more QUIC connections per IP flow between the UE and the UPF may be established based on the information received in the procedure as described in clause 6.8.3. These QUIC connections can be encrypted or be NULL encryption. The following two possible solutions can be considered to support the NULL encryption QUIC connection, which needs further to be studied in SA3.

- Solution 1: TLS 1.3 can be extended to support the NULL encryption algorithm.

- Solution 2: The TLS layer is taken as optional for QUIC protocol, as the TLS authentication and encryption can be skipped when it is applied between the UE and UPF.

If the radio level security is enabled, it is proposed to use the NULL encrypted QUIC connection.

Regarding the QUIC connection establishment procedure, the version information, transport parameters of the QUIC protocol applied by the QUIC proxy can be sent to UE in QUIC connection establishment procedure via user plane, as defined in IETF draft-ietf-quic-transport [6]. Alternatively, the QUIC proxy information can also be sent to UE via NAS message in order to achieve 0-RTT QUIC connection establishment. In the QUIC proxy side, it will identify the QUIC traffic based on the packet filter and QUIC method indication from SMF via N4 rule and forward these packets to the target server after removing QUIC header..

For the QoS control, there is no impact on the transparent QUIC solution as the QUIC packet IP/UDP header is the original IP/UDP header..

The protocol stack is defined in Figure 6.8.2-3, taking untrusted non 3GPP access as an example:



Figure 6.8.2-3: Protocol stack of QUIC

NOTE 1: The Protocol stack in the UPF towards the server is based on UDP protocol, i.e. the application data is encapsulated with UDP header.

#### 6.8.2.2 Non-Transparent QUIC proxy solution

Similar as MPTCP solution in R16, the network needs to send the QUIC proxy information to the UE, i.e. the QUIC functionality IP address and the port number. The UE will use this QUIC IP address as the destination IP address to encapsulate the user data and when receiving the uplink packet the UPF replaces it with the remote server IP address. The following IETF protocol is needed in this non-transparent QUIC solution to transport the IP address of the remote server to the UPF:

- IETF draft-ietf-masque-connect-udp: "The CONNECT-UDP HTTP Method". The call follow is the same as Solution 13 as defined in subclause 6.13.3.2, with the following difference:

1) There is no need to notify the UPF about the QoS flow ID in the HTTP message, since the QUIC connection is established for the IP flows which need to perform traffic splitting per packet, rather than for the QoS flows.

2) Usage of Datagram-Flow-Id to identify the IP flow is optional, since the QUIC connection is established per single IP flow and the HTTP message is also transported with this QUIC connection.

NOTE 1: The SOCKSv5 protocol can also be applied to support the QUIC proxy between the UE and UPF.

The QUIC connections between the UE and UPF per IP flow can be encrypted or be NULL encrypted as described in subclasue 6.8.2.1.

The QUIC connection establishment procedure is the same as transparent QUIC proxy solution as described in subclasue 6.8.2.1, with an addition that the QUIC proxy needs to replace the target IP address with the remote Server IP address and UDP port number.

For the QoS control, similar mechanism is applied as defined in R16 MPTCP solution, i.e. both the QoS rule and N4 rules are provided for the original IP packets instead of the QUIC packet IP/UDP header information.

### 6.8.3 Procedure

For the first case, i.e. QUIC connection is between the UE and the UPF, the signalling flow for a MA PDU Session establishment when the UE is not roaming, or when the UE is roaming and the PDU Session Anchor (PSA) is located in the VPLMN, is described as below.



Figure 6.8.3-1: QUIC based MA PDU Session establishment procedure

- In step 1, the UE provides a "MA PDU Request" indication in UL NAS Transport message and an ATSSS Capability indicating support of "QUIC Capability" in PDU Session Establishment Request message.

- In step 2, if the AMF supports MA PDU sessions, then the AMF selects an SMF, which supports MA PDU sessions, and forwards the MA PDU Session Establishment Request to the SMF.

- In step 3, if the MA PDU session is allowed and dynamic PCC is to be used for the MA PDU Session, the SMF sends an "MA PDU Request" indication and the ATSSS Capability of MA PDU Session to the PCF in the SM Policy Control Create message and. The ATSSS Capability includes the QUIC functionality.

The PCF provides ATSSS Steering policy if the MA PDU session is allowed. The PCF provides PCC rules for the MA PDU session, i.e. PCC rules that include ATSSS policy control information, which includes the QUIC functionality and ATSSS-LL functionality indication if both QUIC functionality and ATSSS-LL functionality are supported. Additionally, the PCC rules may also indicate on whether the encryption of the QUIC connection is needed or not based on operator policy and subscription data or access type for this MA PDU session.

- In step 4, the SMF establishes the user-plane resources over the 3GPP access and/or non-3GPP.

- the N4 rules derived by SMF for the MA PDU session are sent to UPF and one or two N3 UL CN tunnels info may be allocated by the SMF or by the UPF. If the ATSSS functionality for the MA PDU Session indicates "QUIC functionality and ATSSS-LL functionality", the SMF includes QUIC functionality and ATSSS-LL functionality into the N4 rule to instruct the UPF to activate the QUIC functionality and ATSSS-LL functionality for the traffic. If the QUIC connection needs encryption or NULL encryption, the SMF also indicates it to the UPF.

- In step 5, the UPF allocates QUIC functionality information if the non-transparent QUIC functionality applied for this MA PDU session in the UPF. The UPF sends QUIC functionality information to the SMF. The QUIC functionality information includes the QUIC functionality IP address and UDP port number.

- In step 6, for the MA PDU session, the SMF includes an "MA PDU session Accepted" indication and PDU Session Establishment Accept message which includes ATSSS rules for MA PDU Session and the QUIC functionality information in the Namf\_Communication\_N1N2MessageTransfer message to the AMF and the AMF marks this PDU session as MA PDU session based on the received "MA PDU session Accepted" indication, same as defined in Rel-16 specifications.

- In step 8, the UE receives a PDU Session Establishment Accept message, which indicates to the UE that the requested MA PDU session was successfully established. This message includes the ATSSS rules for the MA PDU Session, which includes steering mode, the QUIC functionality and ATSSS-LL functionality indication and encryption or NULL encryption indication for the traffic.

- After step 8 in Figure 6.8.3-1, if the SMF was informed in step 2 that the UE is registered over both accesses, then the SMF initiates the establishment of user-plane resources over non-3GPP access too as specified in TS 23.502 [4] clause 4.22.2.1.

The last step above is not executed when the UE is registered over one access only, in which case the MA PDU Session is established with user-plane resources over one access only. How user-plane resources can be added over an access of the MA PDU Session is specified in TS 23.502 [4] clause 4.22.7.

For the second case, i.e. QUIC connection between the UE and remote server, the existing procedure as specified in TS 23.502 [4] clause 4.22.2 is applied.

### 6.8.4 Impacts on services, entities, interfaces and IETF protocols

#### 6.8.4.1 Transparent QUIC proxy solution

This solution will impact the following entities in 5GS:

- SMF: Supports to select the UPF based on its QUIC and ATSSS-LL capability.

- PCF: Supports to authorize both QUIC functionality and ATSSS-LL functionality steering method for the SDF.

- UPF: Supports the QUIC proxy functionality, and establishes the QUIC connection with the UE. Adds/removes the QUIC header before forwarding the packet to the UE or the remote server over N6 interface.

- UE: Supports the QUIC functionality, and establishes the QUIC connection with the UPF per IP flow. To be more specific, for uplink traffic, the QUIC functionality in the UE obtains the application data (i.e. UDP payload) and put it into the QUIC datagram if unreliable QUIC transport is applied, and encapsulated with QUIC header. The QUIC packet is then encapsulated with an original IP/UDP header. For downlink traffic, the UE decapsulates the received QUIC packet and retrieves the QUIC payload (application data) and delivers it to the application.

- 5G-AN/ NG RAN: No impact.

This solution needs to enhance the existing SM NAS protocol, N5 and N4 interfaces, Npcf service to support this QUIC based steering functionality.

This solution has dependency on the following IETF drafts:

- IETF draft-ietf-quic-transport [6]: "QUIC: A UDP-Based Multiplexed and Secure Transport" along with the loss detection and congestion control as defined in draft-ietf-quic-recovery [7].

- IETF draft-ietf-quic-datagram [8]: "An Unreliable Datagram Extension to QUIC".

This solution may have additional impact on IETF:

- As the current QUIC connection defined by IETF shall be encrypted based on the TLS 1.3, the NULL encryption QUIC connection requires IETF support.

#### 6.8.4.2 Non-transparent QUIC proxy solution

Besides the impact listed above in subclause 6.8.4.1, there are some additional impacts on the UE and UPF to support the non-transparent QUIC proxy solution.

- UPF: Supports the MASQUE protocol, i.e. handles the HTTP message to obtain the remote Server IP address and UDP port number per IP flow. The target IP/UDP header will be replaced by the remote Server IP address and UDP port number for the UL. For the DL, the source IP address and UDP port are replaced by the ones of the QUIC proxy in the UPF.

- UE: Supports the MASQUE protocol, i.e. creates the HTTP message and sends the remote Server IP address and UDP port number to the UPF.

This solution has additional dependency on an IETF draft, apart from those listed in subclause 6.8.4.1:

- IETF draft-ietf-masque-connect-udp [19]: "The CONNECT-UDP HTTP Method".

\* \* \* \* End of changes \* \* \* \*