**3GPP TSG- Meeting #125S4-231359**

**, Sweden, August. – 25. August 2023**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **0052** | **rev** |  | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | [5GMS\_Pro\_Ph2] Traffic Identification |
|  |  |
| ***Source to WG:*** | Ericsson LM |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | 5GMS\_Pro\_Ph2 |  | ***Date:*** | 26.7.2023 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | This CR collects the changes to TS 26.512, due to Objective #5 “Extensions to 5GMS protocols to support traffic identification based on the conclusions in TR 26.804, clause 6.3.”The CR may be updated and extended during several meetings. |
|  |  |
| ***Summary of change:*** |  |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\* Short Introduction \*\*\*\*

This CR starts collecting the changes related to 5GMS\_Pro\_Ph2, Objective #5 “Extensions to 5GMS protocols to support traffic identification based on the conclusions in TR 26.804, clause 6.3.”.

TR 26.804, Clause 6.3 (Conclusion Summary) is



The conclusions of the Traffic Identification Key Topic (Key Topic #3) from TR 26.804 is



**Proposal**

Annex X should be ammended with an informative Annex about usage of DSCP / ToS for traffic Identification. The following additions are described

- The plan is to re-use material from TR 26.804, Clause 5.3, specifically the description of DiffServ, the implications on the deployment scenario and some sequence charts.

- TS 26.512 already contains support for ToS as traffic separation and the informative usage text should be based on the existing functionality

1. The Service Access Information: This information element is used to inform the MSH about the “how to access the media streaming service”. The Dynamic Policy Confoguration (Clause 11.2.3) contains the property sdfMethods which is a list of recommended service data flow descriptions to be used for identifying the traffic. The 5GMS AF may add TYPE\_OF\_SERVICE\_MARKING to the list.

2. When activating a Dynamic Policy (M5 API access), the MSH provide one or more serviceDataFlowDescriptions to the 5GMS AF. The *serviceDataFlowDescription* property can be of type IpPacketFilterSet (Clause 6.4.3.1), allowing the definition of a source or destination IP addresses, a type of service value, a direction value and other parameters. Thus, when activating a Dyanmic Policy, the MSH may select an TOS value to be used for the communication between the 5GMS Client and the 5GMS AS.

\*\*\*\* First Change \*\*\*\*

Annex X (informative):
Usage of ToS/DSCP for traffic identification

# X.1 General

< Give a overview of the purpose and the assumptions.>

# X.2 Differentiated Services/ToS-enabled Collaboration Scenarios

Differentiated Services (DS) [76, 77] is a scalable scheme for managing application traffic by classifying the traffic into a set of coarse-grained traffic classes. A Differentiated Service (DS) domain is a continuous set of DS-capable routers, which are operated with a common set of configurations. Each IP packet in a DS domain is marked and conditioned according to its traffic class. A 6-bit DS Code Point (DSCP) of the 8-bit differentiated services field (DS field) is used for marking. The DS field replaces the ToS field in the IPv4 packet headers and the Traffic Class field in the IPv6 header.

End host systems may mark IP packets with a specific DSCP value prior to transmission. DS-enabled routers treat the packet according to the DSCP value when performing routing operations on it. Border gateway routers typically mark packets with a DSCP value based on some traffic policy, overriding any value set by hosts.

NOTE: Usage of Differentiated Services across administrative borders is technically possible. The preservation of the DSCP field by networks between the MNO network and the external Data Networks hosting the 5GMS functions is assumed to be governed by an SLA and by transport-level arrangements that are outside 3GPP scope. When the DSCP field is used only for traffic identification, preservation of the DSCP field could be achieved by using a tunnelling solution.

The RFCs defining Differentiated Services recommend a set of Per-Hop Behaviors (PHB), namely:

- Default Forwarding (DF) PHB, defined in section 4.1 of RFC 2474 [76], is used for traffic without special treatment.

- Class Selector PHB, defined in section 4.2.2.2 of RFC 2474 [76] is used for maintaining backwards compatibility with the IP precedence field of ToS.

- Expedited Forwarding (EF) PHB, defined by RFC 3246 [78], is dedicated to low loss or low latency traffic.

- Assured Forwarding (AF) PHB, defined by RFC 2597 [79], offers different levels of forwarding assurances.

The DS domain operator can also implement additional custom PHBs.

In the context of ToS-based traffic identification and separation, it is reasonable to assume the Data Network north of the UPF (N6) is DS-enabled. The 5G System is embedded in a larger DS domain, using same ToS values across multiple devices in order to provide Quality of Service Support like a DSCP-enabled link. However, it is not required to deploy DS capable routers for using in order to use the ToS field in the IP packet filter set for traffic identification.

According to clause 4.1 of TS 26.501 [2], the 5GMS functions may be deployed within the trusted Data Network or an external Data network. As noted above, DS Code Points are often reset at network domain borders, but not always. There may be deployments e.g., with localized Edge Computing or with direct peering realizations, where the DSCP values can be used up to the 5GMSd AF and/or 5GMS AS in an external Data Network. In this case, the logical DS domain is extended to include those externally-deployed 5GMS functions.

Figure X.2-1 illustrates a deployment with a DS domain between the 5G System and the 5GMS functions deployed in the external DN. (The model is also valid for deployments in which the 5GMS functions both reside in the trusted DN.)

 

Figure X.2-1: 5GMS deployment within a DS domain

Figure X.2-2 illustrates a deployment with a DS domain between the 5G System and an externally deployed 5GMSd AS. The 5GMSd AF is deployed in the trusted DN.



Figure X.2-2: 5GMS deployment within a DS domain

# X.3 Procedure for using ToS Traffic Class for traffic identification

This call flow focuses on a scenario where both downlink and uplink traffic for a particular application flow within a PDU Session shared by several application flows needs to be mapped to a specific QoS Flow and handled separately by the 5G System. In this call flow, the 5GMS Client initiates the QoS Flow establishment by using specific ToS values in the uplink traffic. A ToS-based QoS rule is already provisioned, so that the Uplink Traffic is mapped to the correct QoS Flow.

It is assumed here that the QoS flow should be used (e.g. for Premium QoS) as described in annex A.



Figure X.3-1: High-level call flow for using ToS Traffic Class for traffic identification

Prerequisites:

- It is assumed that the 5GMS System is already provisioned for Dynamic Policy usage as defined in clause 5.7.2 of TS 26.501 [2]. As result, various functions of the 5G System are provisioned for QoS usage.

The steps are as follows:

1. The 5GMS Client acquires Service Access Information (through M8+M6 or M5), providing the information needed to use the Dynamic Policy Invokation API. Here, the sdfMethod indicates the usage of ToS.

2. The 5GMS Client activates a Dynamic Policy as described in clause 5.7 of TS 26.501 [2]. The serviceDataFlowDescriptions array contains objects of data type IpPacketFilterSet, where the srcIp, toSTc, dstIP properties are present. The filter for a bi-directional Service Data Flow requires two objects, one with direction set to in and one with direction set to out.

3. As a result of the previous step, the 5GMS AF provisions the information for a Dynamic PCC rule with either the PCF or the NEF.

4. The PCF authorizes the request and creates a PCC rule. The PCF compiles and notifies the SMF about the PCC rule (containing the flow descriptions) and the QoS description, has and the SMF forwards the QoS rule to the UE and (in the form of a PDR) to the UPF. The information contains, among other things, the QFI value and the ToS value.

During a media streaming session:

5. The 5GMS Client initiates connection establishment by sending a TCP SYN packet. The ToS value in the TCP SYN packet is set by the 5GMS Client to the same value as provided to the 5GMS AF in earlier step 2.

6. The UE SDAP entity detects a matching ToS value in the uplink traffic.

7. The UE SDAP entity (Layer 2) encapsulates the IP packet into the according radio protocols, including the QFI marking.

8. The 5GMS AS reads the ToS value from the uplink packet. The 5GMS AS uses the uplink ToS value to mark all downlink packets in that TCP connection.

NOTE: When the 5G System employs an N6 NAT, the N6 NAT may set the downlink ToS value to the same value as the uplink ToS value.

9. The 5GMS AS marks its acknowledgement IP packet (conveying the TCP SYN–ACK) with the same ToS value as the incoming packet.

10. The 5GMS AS sends the TCP SYN–ACK packet back to the UE. The packet reaches the UPF on its path to the UE.

11. The UPF detects a matach for the PDR rule configured in step 4 above containing the UE's IP address and ToS value.

12. The UPF encapsulates the downlink IP packet into an GTP‑U packet, and sets the QFI value in the GTP‑U packet header.

13. The UPF sends the GTP‑U-encapsulated packet to the RAN via reference point N3 and the RAN marks the QFI value in the SDAP layer, sending the packet to the UE. The UE SDAP entity (Layer 2) forwards the TCP SYN–ACK to the 5GMS Client.

14. The 5GMS Client sends the TCP ACK (again with the ToS field set in the IP header) to complete the TCP connection handshake.

15. The UE SDAP entity (Layer 2) detects a ToS match for the UE.

16. The UE SDAP entity (Layer 2) encapsulates the IP packet into the according radio protocols, including the QFI marking.

The 5GMS Client continues to use the established TCP connection.

\*\*\*\* Next Change \*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 26.501: "5G Media Streaming (5GMS); General description and architecture".

[3] DASH Industry Forum, "Specification of Live Media Ingest",
<https://dashif-documents.azurewebsites.net/Ingest/master/DASH-IF-Ingest.pdf>

[4] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[5] Standard ECMA-262, 5.1 Edition: "ECMAScript Language Specification", June 2011.

[6] IETF RFC 6234: "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)".

[7] 3GPP TS 23.003: "Numbering, addressing and identification".

[8] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005: "Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

[9] IETF RFC 7230: "Hypertext-Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[10] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".

[11] IEEE Standard 1003.1™, Issue 7: "The Open Group Base Specifications", 2018.
<https://pubs.opengroup.org/onlinepubs/9699919799/>

[12] 3GPP TS 29.571: "Common Data Types for Service Based Interfaces; Stage 3".

[13] 3GPP TS 38.321: "NR; Medium Access Control (MAC) protocol specification".

[14] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[15] 3GPP TS 27.007: "AT Command set for User Equipment (UE)".

[16] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3", August 2018.

[17] IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures", April 2015.

[18] ISO 3166‑1: "Codes for the representation of names of countries and their subdivisions — Part 1: Country codes".

[19] ISO 3166‑2: "Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code".

[20] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.

[21] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[22] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[23] OpenAPI: "OpenAPI 3.0.0 Specification", <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.

[24] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[25] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[26] IETF RFC 7232: "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".

[27] IETF RFC 7233: "Hypertext Transfer Protocol (HTTP/1.1): Range Requests".

[28] IETF RFC 7234: "Hypertext Transfer Protocol (HTTP/1.1): Caching".

[29] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[30] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol V8rsion 1.2".

[31] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[32] ISO/IEC 23009-1: "Information technology; Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats".

[33] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[34] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[35] 3GPP TS 26.511: "5G Media Streaming (5GMS); Profiles, codecs and formats".

[36] Void.

[37] 3GPP TS 26.244: "Transparent end-to-end packet switched streaming service (PSS); 3GPP file format (3GP)".

[38] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format", December 2017.

[39] ISO 14496-12: "Information technology – Coding of audio-visual objects – Part 12: ISO base media file format".

[40] ISO 23000-19: "Information technology – Coding of audio-visual objects – Part 19: Common media application format (CMAF) for segmented media".

[41] IETF RFC 3986: "URI Generic Syntax".

[42] 3GPP TS 26.118: "Virtual Reality (VR) profiles for streaming applications".

[43] 3GPP TS 24.558: "Enabling Edge Applications; Protocol specification".

[44] 3GPP TS 29.558: "Enabling Edge Applications; Application Programming Interface (API) specification; Stage 3".

[45] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[46] 3GPP TS 29.517: "5G System; Application Function Event Exposure Service; Stage 3".

[47] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[48] 3GPP TS 26.531: "Data Collection and Reporting; General Description and Architecture".

[49] 3GPP TS 26.532: "Data Collection and Reporting; Protocols and Formats".

[50] 3GPP TS 29.522: "5G System. Network Exposure Function Northbound APIs; Stage 3".

[51] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[52] 3GPP TS 26.347: "Multimedia Broadcast/Multicast Service (MBMS); Application Programming Interface and URL".

\*\*\*\* Last Change \*\*\*\*