**3GPP TSG-SA4 Meeting #113e *S4-210522***

 **Electronic Meeting, Telco, Apr 04-14, 2021**

|  |
| --- |
| *CR-Form-v12.0* |
| **Pseudo CHANGE REQUEST** |
|  |
|  | **26.804** | **CR** | **<CR#>** | **rev** | **-** | **Current version:** | **0.0.1** |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | [FS\_5GMS-EXT] Key Topic Traffic Identification using ToS IP Header Field |
|  |  |
| ***Source to WG:*** | Ericsson LM |
| ***Source to TSG:*** | SA4 |
|  |  |
| ***Work item code:*** | FS\_5GMS-EXT |  | ***Date:*** | 2021-03-31 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | The study item description identifes the key topic “Traffic Identification”. The 5G System supports different methods for traffic identification, including using some IP header fields like ToS (or DSCP) or Flow Label (IPv6 only). |
|  |  |
| ***Summary of change:*** | The text fully describes the UPF traffic identification chain, incl Packet Detection, etc.  |
|  |  |
| ***Consequences if not approved:*** | Key topic only partially addressed |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
| ***56***  |  |
| ***This CR's revision history:*** |  |

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

[4] 3GPP TS 26.512: "5G Media Streaming (5GMS); Protocols".

[5] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[6] 3GPP TS 29.551: “5G System; Packet Flow Description Management Service; Stage 3"

**===== CHANGE =====**

# 4 Introduction to 5G Media Streaming

## 4.1 Introduction

## 4.2 Collaboration Scenarios

## 4.3 Architectures

## 4.4 Summary of Stage-3 enablers

**===== CHANGE =====**

# 5 Key Topics

## 5.1 Introduction

## 5.3 Traffic Identification

### 5.3.1 Description

For different features within the 5G Media Streaming Architecture, it is necessary for the 5G System to identify the traffic flows. Multimedia streaming applications might not be able to uniquely identify the 5-Tuple of the streaming session, since the 5-Tuples are often changing. This is due to factors such as load balancing, CDN distribution, multiple concurrent requests for different types of resources, etc. This study will address how to properly configure the 5G System to enable efficient detection of application flows (service data flows) e.g. for event reporting, and QoS profile usage, etc.

Figure 5.3.1-1 depicts the chain of functions (taken from TS 29.244, Figure 5.2.1-1) within an UPF for incoming IP packets (from DN side). The UPF always first looks up the PFCP session to which a packet belongs. The PFCP session is similar to a PDU session. Then there are so-called Packet Detection Rules (PDR), which implement traffic identification with respect to different conditions.



Figure 5.3.1-1: Packet processing flow in the UP function (Figure 5.2.1-1 from TS 29.244)

Based on the PDR result, the next rules are executed, namely Multi-Access Rule (MAR), Forward Action Rule (FAR), QoS Enforcement Rule (QER), and Usage Reporting Rule (URR).

Only the Forward Action Rule (FAR) is mandatory. The QoS Enforcement Rule (QER) is only present for QoS Flows. The Usage Reporting Rule (URR) is only available when traffic volume measurements (e.g. for charging) are needed.

The Packet Detection Rule (PDR) is based on Service Data Flow (SDF) Filters or Application Identifiers. An Application Identifier refers to one or more Packet Flow Descriptions (PFD).

A Service Data Flow (SDF) Filter contains a single IP Packet filter, i.e. a Flow Description (5-Tuple), and/or a ToS Traffic Class and/or a Security Parameter Index and/or a Flow Label.

The Management of Packet Flow Descriptions enables the UPF to perform accurate application detection when PFD(s) are provided by an ASP and then to apply enforcement actions as instructed in the PCC Rule.

The operator is able to configure pre-defined PCC Rules in the SMF or dynamic PCC Rules in the PCF that include at least an application identifier for service data flow detection, charging control information, i.e. charging key and optionally the Sponsor identifier or the A SP identifier or both. Depending on the service level agreements between the operator and the Application Server Provider, it may be possible for the ASP to provide individual PFDs or the full set of PFDs for each application identifier maintained by the ASP to the SMF via the PFD Management service in the NEF (PFDF). The PFDs become part of the application detection filters in the SMF/UPF and therefore are used as part of the logic to detect traffic generated by an application. The ASP may remove or modify some or all of the PFDs which have been provided previously for one or more application identifiers. The SMF may report the application stop to the PCF for a application instance identifier as defined in clause 5.8.2.8.4 of TS 23.501 [5] if the removed/modified PFD in SMF/UPF results in that the stop of the application instance is not being able to be detected.

The ASP manages (provision, update, delete) the PFDs through the NEF (PFDF). The PFD(s) are transferred to the SMF through the NEF (PFDF). The PFDF is a logical functionality in the NEF which receives PFD(s) from the ASP through the NEF, stores the PFD(s) in the UDR and provides the PFD(s) to the SMF(s) either on the request from ASP PFD management through NEF (PFDF) (push mode) or on the request from SMF (pull mode). The PFDF functionality is a service provided by the NEF.

The ASP may provide/update/remove PFDs with an allowed delay to the NEF (PFDF). Upon reception of the request from the ASP, the NEF (PFDF) shall check if the ASP is authorized to provide/update/remove those PFD(s) and request the allowed delay. The NEF (PFDF) may be configured with a minimum allowed delay based on SLA to authorize the allowed delay provided by the ASP. When ASP and requested allowed delay are successfully authorized, the NEF (PFDF) shall translate each external Application Identifier to the corresponding Application Identifier known in the core network. The NEF (PFDF) stores the PDF(s) into the UDR.

The Application identifier is an index to a set of application detection rules configured in UPF. It is an identifier that can be mapped to a specific application traffic detection rule

The procedure is depicted by the following diagram:



The PFD (Packet Flow Description) is a set of information enabling the detection of application traffic.

Each PFD may be identified by a PFD id. A PFD id is unique in the scope of a particular application identifier. Conditions for when PFD ID is included in the PFD is described in TS 29.551 [6]. There may be different PFD types associated to an application identifier.

A PFD include the following information:

- PFD id; and

- one or more of the following:

- 3-tuple(s) including protocol, server side IP address and port number;

- the significant parts of the URL to be matched, e.g. host name;

- a Domain name matching criteria and information about applicable protocol(s).

### 5.3.2 Collaboration Scenarios

The 5GMSd Application Provider concludes with the MNO an SLA to provide differentiated treatment, including QoS and charging for their application. The Application Provider provides the necessary information to the MNO to identify the traffic, to ensure correct and exclusive identification of the related traffic. The MNO identifies the traffic correctly and applies the agreed traffic treatment.

Due to privacy concerns, the content hosting is provided by the Application Provider in an external data network. However, the 5GMSd Application Provider leverages the network features either via a 5GMSd AF in the trusted data network or via a 5GMSd AF in the external data network.



Figure 5.9.2-1: Collaboration 1 (Collaboration 3 of TS 26.501)



Figure 5.9.2-2: Collaboration 2 (Collaboration 4 of TS 26.501)

In order to use flow-based network features (such as different QoS classes or different charging policies), the 5G System needs to detect the relevant traffic. The 5G System uses so-called **Packet Detection Rules** (PDRs) in the UPF to detect the traffic. The PDRs are created based on **Service Data Flow Templates**. The Service Data Flow Templates are provided by the 5GMSd AF.

### 5.3.3 Deployment Architectures

The following figure depicts a potential architecture design for the realization of traffic identification. The architecture shows the involved network functions in the traffic identification.



Figure 5.3.3-1: Relevant architecture components

### 5.3.4 Mapping to 5G Media Streaming and High-Level Call Flows

#### 5.3.4.1 General

Editor’s Note: Short introduction into the different Traffic Identification schemes

#### 5.3.4.2 Usage of Packet Flow Descriptions for Traffic Identification

The following are potential and simplified call flows for the realization of the traffic identification. In the first call flow, the provisioning step is described, in which one or more PFDs for a single application are provisioned. The provisioned PFDs for a single application are identified by the Application Identifier.



Figure 5.3.4-1: PFD Provisioning using the PFD Management API (simplified)

In the second call flow, the update procedure for the PFD to adjust to an actual session is described.



Figure 5.3.4-2: PFD usage within a application traffic detection rule (simplified)

#### 5.3.4.3 Usage of ToS Traffic Class for Traffic Identification

The following is a simplified call flow when using the ToS Traffic Class for Traffic Identification. It is assumed here that the QoS flow should be used (e.g. for Premium QoS) as described in TS 26.512, Annex A.

The ToS field is a bit field in the IP headers, which is also used for DiffServ [RFC 7657] and for ECN [RFC 3168] marking.



Figure 5.3.4.3-1: PFD usage within a application traffic detection rule (simplified)

Figure 5.3.4.3-1 depicts a call flow for ToS-based traffic detection. It is assumed here that the 5GMSd AF provides the ToS value for traffic identification in the Policy Activation response message (step 2). Another solution might be that the Media Session Handler allocates a ToS value and then provides the value to the 5GMSd AF.

The call flow works as the following steps:

1: The Media Session Handler activates a Dynamic Policy and provides the Policy Template Id with the activation request (among other parameters).

2: If the Dynamic Policy can be activated, the 5GMSd AF provides a value for the ToS field in return.

NOTE: The ToS field value is scoped with the IP address of the requesting UE.

The 5GMSd AF triggers the activation of a Dynamic PCC rule:

3: The 5GMSd AF uses the Policy Authorization Service API and triggers a PCC rule activation. The 5GMSd AF provides the ToS value together with the IP address of the requesting UE and QoS parameters.

4: As result, the PCF uses the Npcf\_SMPolicyControl APIs to provide a new PCC rule to the SMF.

5: The SMF uses the N4 interface to provide a new Packet Detection Rule (PDR) together with other rules for the UE to the UPF. Once the new rule is installed in the UPF.

6: The Media Player prepares a new TCP connection and sets the ToS value nominated by the 5GMSd AF on the TCP socket using the setsockopt() API or equivalent. As a result, all TCP packets for the flow will be marked by the UE with the ToS value.

7: The TCP Connection is established, and the traffic is marked with the ToS field. The UPF detects the traffic (by inspecting the IP header) and handles it according to the policy.

The UPF nees to detect the downlink traffic matching the uplink traffic. There are different solutions to achieve this:

A: The 5GMSd AS uses the same ToS field for downlink traffic as used for uplink traffic.

NOTE: The traffic should not cross operational domain boundaries, since the ToS header field is often reset by border IP routers.

B: The UPF captures the 5-tuple carrying a specific ToS field from the TCP SYN Packet that establishes the connection in the uplink direction. As result, the UPF automatically creates a new PDR in the opposite direction derived by inverting the address fields found in the SYN packet.

C: Often, the UEs in a PLMN are shielded from public Internet traffic by means of firewalls that employ Network Address Translation (NAT). In order to set the ToS field within the Trusted DN to an appropriate value, the N6‑NAT may set the downlink ToS to the same value as the uplink ToS.

NOTE:: This is similar to solution A above.

### 5.3.5 Potential open issues

The exact behavior and information that needs to be provided to and by the 5GMSd AF as well as the MSH need to be specified.

### 5.3.6 Candidate Solutions

Editor’s Note: Provide candidate solutions (including call flows) for each of the identified issues.