**3GPP TSG- S4 Meeting #117e *S4-220147***

**, 17th February – 23rd February 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **Psuedo CHANGE REQUEST** |
|  |
|  | **26.804** | **CR** | **<CR#>** | **rev** | **<Rev#>** | **Current version:** | **<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 |  |

|  |
| --- |
|  |
| ***Title:***  | [FS\_5GMS\_EXT] Corrections and Conclusions for Traffic Identification KI |
|  |  |
| ***Source to WG:*** | S4 |
| ***Source to TSG:*** | Ericsson LM |
|  |  |
| ***Work item code:*** | FS-5GMS\_EXT |  | ***Date:*** | <Res\_date> |
|  |  |  |  |  |
| ***Category:*** | **<Cat>** |  | ***Release:*** | <Release> |
|  | *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:*** | Some aspects of the PFD description was wrong. The conclusion was missing. |
|  |  |
| ***Summary of change:*** | This contribution provides a first conclusion for the Traffic Identification Key aspect. The contribution also corrects some details around PFD management. |
|  |  |
| ***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:*** |  |

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

## 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. The increased usage of transport encryption (e.g. HTTPS) increases the difficulty of detecting the packets for certain application flows. Existing detection methods, such as using “significant parts of the URL to be matched” (contained in a Packet Flow Description, see below), are impractical for HTTPS traffic, since the URL is carried in the encrypted payload.

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.

Note that the TS 23.50x specifications use different terminology from the TS 29.xxx specifications. Furthermore, TS 23.503 [41] uses slightly different terms than TS 23.501 [23] and TS 23.502 [24]. The two common terms are defined in TS 23.503:

**- Packet flow:** A specific user data flow from and/or to the UE.

**- Service data flow**: An aggregate set of packet flows carried through the UPF that matches a service data flow template.

The terms *traffic detection* [23] and *application detection* [23] refer to the process of finding matching service data flows among all packet flows. This logic is defined in TS 23.503 as an *application detection filter*.

The procedures in TS 23.502 use the term *flow description*, which is only a subset of an *IP Packet Filter Set* (as defined in TS 23.501).

Figure 5.3.1-1 depicts the chain of functions (taken from TS 29.244 [26], Figure 5.2.1-1) within an UPF.



Figure 5.3.1-1: Packet processing flow in the UP function (Figure 5.2.1-1 from TS 29.244 [26])

The steps are as follows:

1. The UPF always first looks up the Packet Forwarding Control Protocol (PFCP) session context to which a packet belongs. The PFCP session context is an individual PDU session or a standalone PFCP session not tied to any PDU session.

2. Then there are so-called Packet Detection Rules (PDR), which implement traffic detection of the service data flows with respect to different conditions.

NOTE: A PDR is direction specific. Thus, an Uplink (UL) PDR and a Downlink (DL) PDR are needed to detect a bidirectional Service Data Flow.

3. 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).

NOTE: 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 Templates, which contain one or more Service Data Flow (SDF) Filters or an Application Identifier. An Application Identifier refers to one or more Packet Flow Descriptions (PFDs).

A Service Data Flow (SDF) Filter contains for IP PDU Sessions a single IP Packet filter, i.e. any combination of

- Source/destination IP address or IPv6 prefix.

- Source / destination port number.

- Protocol ID of the protocol above IP/Next header type.

- Type of Service (TOS) (IPv4) or Traffic class (IPv6) and Mask.

- Flow Label (IPv6).

- Security parameter index.

- Packet Filter direction.

A PFD includes a PFD ID; and one or more of the following:

- 3-tuple(s) comprising 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 criterion and information about applicable protocol(s).

The application detection filter can be configured in the SMF and the SMF then provides it in the Service Data Flow Template to the UPF. Alternatively, the Service Data Flow Template for traffic handling in the UPF is received from the dynamic PCC Rule.

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

The operator is able to configure pre-defined PCC Rules in the SMF or dynamic PCC Rules in the PCF. A PCC rule includes either a list of Service Data Flow filters or an application identifier for Service Data Flow detection. The PCC rule further includes charging control information, i.e. charging key and optionally a Sponsor identifier or an ASP identifier or both.

The application identifier references one or more PFDs, which are managed using the PFD Management API. Depending on the service level agreements between the operator and the Application Server Provider, it may be possible for the ASP to provide to the SMF individual PFDs or the full set of PFDs for each application identifier maintained by the ASP via the PFD Management service in the NEF (PFDF). The PFDs become part of the application detection filters in the SMF/UPF and are thereafter 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 an 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 would result in an inability to detect traffic for that application instance.

The ASP manages (i.e. provisions, updates, deletes) 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). Finally, 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) checks 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 both the requesting ASP and the requested allowed delay are successfully authorized, the NEF (PFDF) translates 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 simply an index to a set of application detection rules configured in the UPF. It is an identifier that can be mapped to a specific application traffic detection rule.

The procedure is depicted Figure 5.3.1‑2 below:



Figure 5.3.1‑2:

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 a PFD ID is included in the PFD are described in TS 29.551 [6]. There may be different PFD types associated with an Application Identifier.

### 5.3.2 Collaboration Scenarios

#### 5.3.2.1 General Collaboration Scenarios

The 5GMSd Application Provider negotiates with the MNO an SLA to provide differentiated treatment, including network QoS and charging for its 5GMSd-Aware Application. The Application Provider provides the necessary information to the MNO to detect the traffic, to ensure its correct and exclusive identification. The MNO detects 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 external Data Network (Figure 5.9.2‑1) or via a 5GMSd AF in the trusted Data Network (Figure 5.9.2‑2).



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.

#### 5.3.2.2 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.

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 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 [15], 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 5.3.2.2-1 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 5.3.2.2-1: 5GMS deployment within a DS domain

Figure 5.3.2.2-2 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 5.3.2.2-1: 5GMS deployment within a DS domain

### 5.3.3 Deployment Architectures

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



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

The Service Data Flow Templates support multiple different combinations to define parameters for traffic detection. This clause describes the common parameter combinations to detect specifically media streaming application traffic.

The Service Data Flow Template can take the form of either Service Data Flow filters (i.e. IP Packet Filter Sets) or an Application Id referencing Packet Flow Descriptions (PFDs).

An IP Packet Filter Set can contain different combinations of parameter values. Unspecified parameter values in the IP Packet Filter Sets are used to match any value of the corresponding information in the header of an IP packet. Common IP Packet Filter Set combinations are:

- 5-Tuple: The source and destination IP addresses, source and destination port numbers (potentially expressed as a small range of values) and the Protocol ID. This method of traffic detection is further described in clause 5.3.4.2 below.

- ToS: The source IP address and the Type of Service (ToS). This method of traffic detection is further described in clause 5.3.4.3 below.

NOTE: The Type of Service field is used here to map an application data flow to a specific PCC rule.

A Packet Flow Description (PFD) can contain different parameters. Common parameters are:

- Domain Name: The Internet domain name of an application server. This method of traffic detection is not described further in the present document.

#### 5.3.4.2 Usage of 5-tuples for Traffic Identification

The application detection filters in the UPF can be configured based on a pre-configured PCC rule (i.e. in the SMF and provided to the UPF) or a dynamic PCC rule (i.e. provided by the PCF) By interacting with the PCF (possibly via the NEF) the 5GMS AF is able to provision, update and remove a dynamic PCC rule which contains Service Data Flow description parameters for traffic handling and traffic detection in the UPF.

When using 5-tuples for traffic detection, the following fields of the IP Packet Filter Set are used:

- Source/destination IP address or IPv6 prefix.

- Source/destination port number.

- Protocol identifier of the protocol above IP/Next header type.

- Packet Filter direction (uplink or downlink).

NOTE: These fields are encoded in the Flow Description field, defined in clause 5.3.8 of TS 29.514 [28].

As shown in figure 5.3.4.2-1 (below), the 5GMSd AF in the external DN can send a request using Nnef\_AFsessionWithQos API to provision, update or remove a request to reserve resources for a specific application/flow with specific flow descriptions. After the AF request authorization, the NEF interacts with the PCF, providing the flow description together with the QoS reference, the optional other parameters like Alternative Service Requirements, period of time or traffic volume, etc.



Figure 5.3.4.2-1:Flow description usage for traffic flow identification

If the request is authorised, the PCF determines the required QoS parameters based on the information provided by NEF/AF. After the Nnef\_AFsessionWithQoS\_Create Procedure, a transaction identifier is allocated by the NEF to identify this AF Session. Then the 5GMSd AF can subsequently invoke the Nnef\_AFsessionWithQoS\_Update API with this transaction identifier to update the flow description.

Alternatively, the 5GMSd AF in the trusted DN can directly send a request using Npcf\_PolicyAuthorization API to provision, update and remove a request to reserve resources for a specific application/flow with specific flow descriptions.

Then the PCF initiates the PDU Session modification procedure to provide the updated PCC rule to the SMF and the SMF updates the PDRs in the UPF for the application/traffic identification and policy handling.

However, when a new TCP connection is opened and the old one is closed, the 5-tuple in the Flow Description needs to be changed. (This may be from the consequence of factors such as load balancing, multiple concurrent requests for different types of resources, use of a shared TCP connection pool, etc.) In such cases, the 5GMSd AF can invoke the NEF/PCF-related APIs with new flow description to update the PDRs installed in UPF to follow the changed transport layer 5-tuples for application/flow identification.

#### 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, meaning, only the Type of Service field is used within a SDF Filter. The Type of Service (ToS) is an 8-bit field within the IP header (both IPv4 and IPv6) that can be used to convey a 6-bit DS Code Point (DSCP) value as described in clause 5.3.2.2, and for ECN marking [30]. Here, and in the candidate solution presented in clause 5.3.6, only the leading 6 bits are considered 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.



Figure 5.3.4.3-1: ToS usage within an 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 5). 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).

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

2: The 5GMSd AF uses the Policy Authorization Service API and triggers a PCC rule activation. The 5GMSd AF provides the UE IP address, an IP Packet Filter Set with the ToS value and the UE IP address of the requesting UE and QoS parameters.

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

4: The SMF uses the PDU Session Modification procedure to add/modify a QoS Rule in the UE SDAP entity.

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, the UPF starts taking actions on the detected traffic.

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

NOTE 1: The ToS Value is not immediately provided to the Media Session Handler to prevent race conditions.

7: 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.

8: 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 in the PCC Rule.

NOTE 2: The PCC Rule is scoped by the PDU Session, so the treatment of the ToS field value by the UPF is limited to the requesting UE. The UPF first looks up the relevant PDRs for a PDU session based on the incoming GTP Tunnel Id.

The UPF also needs 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 3: This solution may not work for cases where traffic crosses 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.

NOTE 4: The connection handshake of other transport protocols may be more difficult to detect.

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 5: This is similar to solution A above.

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

The following are simplified call flows for the realization of the traffic identification leveraging Packet Flow Descriptions (PFDs).

In the first call flow (Figure 5.3.4.4‑1) the provisioning step is described, in which one or more PFDs for the traffic identification of a single application are provisioned. The provisioned PFDs for the application are identified by the Application Identifier.



Figure 5.3.4.4-1: PFD Provisioning using the PFD Management API (simplified)

In the second call flow (Figure 5.3.4.4‑2) the on-demand usage of a set of PFDs for an application is described.



Figure 5.3.4.4-2: PFD usage within an application detection filter (simplified)

Here, the 5GMSd AF resides within the Trusted Data Network and interacts directly with the PCF. When activating an QoS flow, the 5GMSd AF provides to the PCF the Application Identifer for detecting the 5G Media Streaming traffic together with the UE IP address and other policy information.

When the 5GMSd AF resides in an external Data Network, the 5GMSd AF instead uses the equivalent NEF API (such as the Nnef\_AFsessionWithQoS or Nnef\_ChargeableParty service APIs) and provides the (external) Application Identifier, referencing one or more PFDs, to the NEF.

The 5GMSd AF can update the PFDs during an ongoing media streaming session. When updating, the 5GMS AF uses the NEF PFD management APIs. The system then automatically updates the Packet Detection Rules in the UPF used for traffic detection.

### 5.3.5 Potential open issues

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

The following open issues have been identified:

1. The Npcf\_PolicyAuthorization API as defined in TS 23.502 [24] only supports usage of a flow description or an application identifier. The flow description is not further defined in TS 23.501 or TS 23.502. In Stage 3 specifications, a flow description represents only a 5-tuple. Other information elements of the Service Data Flow Filter are not supported.

2. The Nnef\_ChargeableParty and Nnef\_AFsessionWithQOS APIs supports usage of a flow description or an Application Identifier for referencing one or more PFDs. The flow description is not further defined in TS 23.501 or TS 23.502. Other information elements of the Service Data Flow Filter are not supported.

3. The Npcf\_PolicyAuthorization API Stage 3 as defined in TS 29.514 [42], only supports a flow description and a ToS value. However, it is not possible to define whether the ToS value should be used in uplink traffic detection or downlink traffic detection.

4. The Nnef\_AFsessionWithQOS and Nnef\_ChargeableParty stage 3 APIs, as defined in TS 29.522 [43], only supports a Packet Flow Description (through the FlowInfo Type) or an Application Identifier for referencing one or more PFDs. Other information elements of the Service Data Flow Filter (like a ToS value) are not supported. Note, the FlowInfo Type from TS 29.122 [44] is different from the FlowInformation Type in TS 29.512 [45].

### 5.3.6 Candidate Solutions

#### 5.3.6.1 Overview

This section gives an overview of the different candidate solutions for application traffic flow identification within a PDU Session beyond providing (non-wildcarded) 5-tuples. Solutions fall into one of the following two categories:

- *Charging separation-only:* Only the application detection filters in the UPF are provisioned with either IP Packet Filter Set (PFS) or PFD parameters,

- *QoS separation:* The application detection filters in the UE and in the UPF are provisioned with either IP Packet Filter Set or PFD parameters in order to mark packets with the appropriate QFI inside the 5G System.

NOTE 1: Both types of solution may also be used for traffic policing.

NOTE 2: In context of the following candidate solutions to the Traffic Identification key issue, only the leading 6 bits of the Type of Service (ToS) field are considered. In case of Differentiated Services [D], these bits convey the DS field, as described in clause 5.3.2.2.

#### 5.3.6.2 Candidate IP-PFS Solution 1: Using IP ToS marking for downlink-only QoS flow mapping

This candidate solution focuses on a scenario where only downlink traffic needs to be mapped to a specific QoS Flow and handled differently by the 5G System. Related uplink traffic is handled using default QoS.

Editor’s Note: Such a solution is counterproductive for TCP- and QUIC-based transports, i.e. protocols depending on acknowledgements. Such solutions can make sense for RTP/UDP based flows, such as in Media Production.

#### 5.3.6.3 Candidate IP-PFS Solution 2: Using IP ToS marking for uplink-only QoS flow mapping

This candidate solution focuses on a scenario where only uplink traffic needs to be mapped to a specific QoS Flow and handled differently by the 5G System. Related downlink traffic is handled using default QoS.

Editor’s Note: Such a solution is counterproductive for TCP- and QUIC-based transports, i.e. protocols depending on acknowledgements. Such solutions can make sense for RTP/UDP based flows, such as in Media Production.

#### 5.3.6.4 Candidate IP-PFS Solution 3a: Using IP ToS marking for bi-directional QoS flow mapping, initiated by downlink traffic

This candidate solution focuses on a scenario where both downlink and uplink traffic for a particular application flow within a PDU Session shared by several different application flows (from the same or different UE applications) needs to be mapped to a specific QoS Flow and handled differently by the 5G System. The UPF is provisioned with a QoS Rule before the 5GMS-related application flow establishment. The UE QoS rule indicates the usage of reflective QoS. In this candidate solution, the 5GMS AF initiates the QoS Flow establishment by using specific ToS values in the downlink traffic.



Figure 5.3.6.4-1:

Assumptions:

- A PCC rule for the UE is activate in the 5G System. The PCC rule contains a Service Data Flow Filter with a ToS value and the UE IP address.

- Reflective QoS is enabled for the PDU Session in question (used here in step 3).

Steps:

Provisioning: The 5GMS System is provisioned for Dynamic Policy usage as defined in clause 5.7.2 of TS 26.501 [15]. As a result, various functions of the 5G System are provisioned for QoS usage as follows:

1. The 5GMS Client has received Service Access Information (through M6 or M5), providing the information needed to use the Dynamic Policy Invocation API. Here, the sdfMethod indicates the usage of ToS. The 5GMS Client has activated a Dynamic Policy as described in clause 5.7 of TS 26.501 [15].

2. The 5GMS AF has provisioned the information for a Dynamic PCC rule with the PCF (possibly through NEF).

3. The PCF has authorized the request and created a PCC rule. The PCF has sent the PCC rule to the SMF, which has forwarded the QoS rule to the UE (indicating “reflective QoS” here) and to the UPF.

During media plane usage:

4. The 5GMS Client initiates connection establishment by sending a TCP SYN packet. The packet is forwarded by the UE SDAP entity (Layer 2) and the UPF to the 5GMS AS.

5. The 5GMS AS looks up the ToS policy, including the ToS value for this UE/network. Details are out of scope for 3GPP.

NOTE: The 5GMS AS may also wait until the first HTTP request message is received to determine the purpose of the request. A 5GMS Client may use the TCP connection for subsequent HTTP transactions (persistent TCP connection).

6. The 5GMS AS sends a TCP SYN–ACK to the UE to continue the TCP connection establishment handshake. The 5GMS AS sets the TOS field value. The packet reaches the UPF on its path to the UE.

7. The UPF detects a PDR match for the UE. Here, the PDR for the UE IP address contains the ToS value. (The PDR was provided to the UPF in an earlier step as described in clause 5.3.4.3.)

8. The UPF encapsulates the downlink IP packet inside an N3 packet. The UPF sets the QFI value in the N3 packet header.

9. The UPF sends the N3 packet to the RAN and the RAN marks the QFI value in the SDAP layer, sending the packet to the UE.

10. The UE SDAP entity (Layer 2) detects a new QFI.

11. Reflective QoS is activated for the PDU Session and the UE creates a “UE-derived QoS Rule” as defined in TS 23.501 [23], clause 5.7.5.2.

12. The UE SDAP entity (Layer 2) forwards the TCP SYN/ACK to the 5GMS Client.

13. The 5GMS Client send the TCP ACK to complete the TCP connection handshake. (This packet does not need to be marked with a specific ToS value by the 5GMS Client.

14. The UE SDAP entity (Layer 2) detects a PDR match for the UE. Here, the PDR is the 5-tuple as stored in the UE-derived QoS rule.

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

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

Discussion:

- The 5GMS AS needs to determine whether QoS should be used for this session and which ToS value to use.

- The Npcf\_PolicyAuthorization API allows a ToS value to be provisioned (without a direction indication), but the Nnef\_AFsessionWithQOS API does not support provisioning of a ToS value.

- The uplink traffic is not marked with a ToS field.

#### 5.3.6.5 Candidate IP-PFS Solution 3b: Using IP ToS marking for bi-directional QoS flow mapping, initiated by downlink traffic

This candidate solution focuses on a scenario where both downlink and uplink traffic for a particular application flow within a PDU Session shared by several different application flows (from the same or different UE applications) needs to be mapped to a specific QoS Flow and handled differently by the 5G System. In this candidate solution, the 5GMS AF initiates the QoS Flow establishment by using specific ToS values in the downlink traffic.

The difference between this and Solution 3a is that the UE receives a QoS rule containing an uplink Packet Filter with ToS.



Figure 5.3.6.5-1:

Assumptions:

- A PCC rule for the UE is activate in the 5G System. The PCC rule contains a Service Data Flow Filter with a ToS value and the UE IP address.

Steps:

Provisioning: The 5GMS System is provisioned for Dynamic Policy usage as defined in clause 5.7.2 of TS 26.501 [15]. As result, various functions of the 5G System are provisioned for QoS usage as follows:

1. The 5GMS Client has received Service Access Information (through M6 or M5), providing the information needed to use the Dynamic Policy Invokation API. Here, the sdfMethod indicates the usage of ToS. The 5GMS Client has activated a Dynamic Policy as described in clause 5.7 of TS 26.501 [15].

2. The 5GMS AF has provisioned the information for a Dynamic PCC rule with the PCF (possibly through NEF).

3. The PCF has authorized the request and created a PCC rule. The PCF has sent the PCC rule to the SMF, which has forwarded the QoS rule to the UE and to the UPF. The QoS Rule for the UE contains the ToS value.

During media plane usage:

4. The 5GMS Client initiates connection establishment by sending a TCP SYN packet. The packet is forwarded by the UE SDAP entity (Layer 2) and the UPF to the 5GMS AS.

5. The 5GMS AS looks up the ToS policy, including the ToS value for this UE/network.

NOTE: The 5GMS AS may also wait until the first HTTP request message is received to determine the purpose of the request. A 5GMS Client may use the TCP connection for subsequent HTTP transactions (persistent TCP connection).

6. The 5GMS AS sends a TCP SYN–ACK to the UE to continue the TCP connection establishment handshake. The 5GMS AS sets the ToS field value. The packet reaches the UPF on its path to the UE.

7. The UPF detects a PDR match for the UE. Here, the PDR for the UE IP address contains the ToS value. (The PDR was provided to the UPF in an earlier step as described in clause 5.3.4.3.)

8. The UPF encapsulates the downlink IP packet inside an N3 packet. The UPF sets the QFI value in the N3 packet header.

9. The UPF sends the N3 packet to the RAN and the RAN marks the QFI value in the SDAP layer, sending the packet to the UE.

10. The UE SDAP entity (Layer 2) forwards the TCP SYN–ACK to the 5GMS Client.

11. The 5GMS Client send the TCP ACK to complete the TCP connection handshake. (This packet does not need to be marked with a specific ToS value by the 5GMS Client.

12. The UE detects a QoS Rule match for the UE. Here, the IP Packet Filter contains only the ToS value.

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

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

Discussion:

- The 5GMS AS needs to determine whether QoS should be used for this session and which ToS value to use.

- The Npcf\_PolicyAuthorization API allows a ToS value to be provisioned (without a direction indication), but the Nnef\_AFsessionWithQOS API does not support provisioning of a ToS value.

#### 5.3.6.6 Candidate IP-PFS Solution 4a: Using ToS marking for bi-directional QoS flow mapping, initiated by uplink traffic

This candidate solution 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 separated by the 5G System. In this candidate solution, the 5GMS Client initiates the QoS Flow establishment by using specific ToS values in the uplink traffic. Here, the reception of the ToS-marked IP Packet in the UPF triggers the creation of a new QoS rule in the UPF, similar to reflective QoS principles.

NOTE: Creation of a new QoS rule derived from an IP packet is defined as “UE-derived QoS rule” creation in clause 5.3.4 (Reflective QoS) of TS 23.501 [15].



Figure 5.3.6.6-1:

Assumptions:

- A PCC rule for the UE is activate in the 5G System. The PCC rule contains a Service Data Flow Filter with a ToS value and the UE IP address.

- Reflective QoS is enabled for the PDU Session in question.

Steps:

Provisioning: The 5GMS System is provisioned for Dynamic Policy usage as defined in clause 5.7.2 of TS 26.501 [15]. As result, various functions of the 5G System are provisioned for QoS usage as follows:

1. The 5GMS Client has received Service Access Information (through M6 or M5), providing the information needed to use the Dynamic Policy Invokation API. Here, the *sdfMethod* indicates the usage of ToS. The 5GMS Client has activated a Dynamic Policy as described in clause 5.7 of TS 26.501 [15].

2. The 5GMS AF has provisioned the information for a Dynamic PCC rule with the PCF (possibly through NEF).

3. The PCF has authorized the request and created a PCC rule. The PCF has sent the PCC rule to the SMF, which has forwarded the QoS rule to the UE and to the UPF.

During media plane usage

4. The 5GMS Client initiates connection establishment by sending a TCP SYN packet. The packet is forwarded by the UE SDAP entity (Layer 2) and the UPF. The 5GMS Client has set a ToS value in the TCP SYN packet, as provided by the 5GMS AF in an earlier step (see clause 5.3.4.3).

5. The UPF detects a PDR match for the UE. Here, the PDR for the PDU Session (e.g. identified by the TEID) contains the ToS value. (The PDR was provided to the UPF in an earlier step as described in Clause 5.3.4.3.)

6. The UPF creates a “UPF derived QoS Rule”, similar to the “UE derived QoS Rule” (see TS 23.501 [15], clause 5.7.5.2). The UPF derives the IP Packet Filter set (similar to the derivation in the “UE derived QoS rule”) by taking the IP addresses, protocol identifier and port numbers into the IP Packet Filter Set.

7. The UPF forwards the TCP SYN packet to the 5GMS AS.

8. The 5GMS AS replies with a TCP SYN–ACK packet to continue the TCP connection establishment handshake.

9. The UPF detects a PDR match for the UE. Here, the PDR for the UE contains the 5-tuple of the TCP connection.

10. The UPF encapsulates the downlink IP packet into an N3 packet. The UPF sets the QFI value in the N3 packet header.

11. The UPF sends the N3 packet to the UE via the RAN.

12. The UE SDAP entity (Layer 2) detects a new QFI value.

13. Since Reflective QoS is activated for the PDU Session, the UE creates a “UE-derived QoS Rule” as defined in TS 23.501 [23], clause 5.7.5.2.

14. The UE SDAP entity (Layer 2) forwards the TCP SYN–ACK to the 5GMS Client.

15. The 5GMS Client sends the TCP ACK to complete the TCP connection handshake. (Unlike in step 4, this packet does not need to be marked with a specific ToS value by the 5GMS Client.)

16. The UE SDAP entity (Layer 2) detects a PDR match for the UE. Here, the PDR is the 5-tuple as stored in the UE derived QoS rule.

17. The UE encapsulates the IP packet into the according radio protocols, including the QFI marking.

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

Discussion:

- TS 23.501 [23] defines only a “UE-derived QoS Rule”. The concept does not exist for the UPF.

- The Npcf\_PolicyAuthorization API allows a ToS value to be provisioned (without a direction indication), but the Nnef\_AFsessionWithQOS API does not support provisioning of a ToS value.

#### 5.3.6.7 Candidate IP-PFS Solution 4b: Using ToS marking for bi-directional QoS flow mapping, initiated by uplink traffic

This candidate solution 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 separated by the 5G System. In this candidate solution, the 5GMS Client initiates the QoS Flow establishment by using specific ToS values in the uplink traffic. Here, the IP packet with the ToS value reaches the 5GMS AS and is re-used for downlink traffic.



Figure 5.3.6.7-1:

Assumptions:

- A PCC rule for the UE is activate in the 5G System. The PCC rule contains a Service Data Flow Filter with a ToS value and the UE IP address.

- Reflective QoS is enabled for the PDU Session in question.

Steps:

Provisioning: The 5GMS System is provisioned for Dynamic Policy usage as defined in clause 5.7.2 of TS 26.501 [15], Clause 5.7.2. As result, various functions of the 5G System are provisioned for QoS usage as follows:

1. The 5GMS Client has received Service Access Information (through M6 or M5), providing the information needed to use the Dynamic Policy Invokation API. Here, the sdfMethod indicates the usage of ToS. The 5GMS Client has activated a Dynamic Policy as described in clause 5.7 of TS 26.501 [15].

2. The 5GMS AF has provisioned the information for a Dynamic PCC rule with the PCF (possibly through NEF).

3. The PCF has authorized the request and created a PCC rule. The PCF has sent the PCC rule to the SMF, which has forwarded the QoS rule to the UE and to the UPF.

During Media Plane usage

4. The 5GMS Client initiates connection establishment by sending a TCP SYN packet. The packet is forwarded by the UE SDAP entity (Layer 2) and the UPF to the 5GMS AS. The 5GMS Client has set a ToS value in the TCP SYN packet, as provided by the 5GMS AF in an earlier step (see clause 5.3.4.3).

5. 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.

6. The 5GMS AS sends a TYP SYN–ACK back to the UE. The packet reaches the UPF on its path to the UE.

7. The UPF detects a PDR match for the UE. Here, the PDR for the UE IP address contains the ToS value. (The PDR was provided to the UPF in an earlier step as described in clause 5.3.4.3.)

8. The UPF encapsulates the downlink IP packet into an N3 packet. The UPF sets the QFI value in the N3 packet header.

9. The UPF sends the N3 packet to the RAN and the RAN marks the QFI value in the SDAP layer, sending the packet to the UE.

10. The UE SDAP entity (Layer 2) detects a new QFI value.

11. Since Reflective QoS is activated for the PDU Session, the UE SDAP entity (Layer 2) creates a “UE-derived QoS Rule” as defined in TS 23.501 [23], clause 5.7.5.2.

12. The UE SDAP entity (Layer 2) forwards the TCP SYN–ACK to the 5GMS Client.

13. The 5GMS Client send the TCP ACK to complete the TCP connection handshake. (Unlike in step 4, this packet does not need to be marked with a specific ToS value by the 5GMS Client.)

14. The UE SDAP entity (Layer 2) detects a PDR match for the UE. Here, the PDR is the 5-tuple as stored in the UE-derived QoS rule.

15. 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.

Discussion:

- The 5GMS AS needs to determine whether QoS should be used for this session and which ToS value to use.

- The Npcf\_PolicyAuthorization API allows a ToS value to be provisioned (without a direction indication), but the Nnef\_AFsessionWithQOS API does not support provisioning of a ToS value.

#### 5.3.6.7 Candidate IP-PFS Solution 4c: Using ToS marking for bi-directional QoS flow mapping, initiated by uplink traffic

This candidate solution 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 separated by the 5G System. In this candidate solution, 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.



Figure 5.3.6.7-1:

Assumptions:

- A PCC rule for the UE is activate in the 5G System. The PCC rule contains a Service Data Flow Filter with a ToS value and the UE IP address.

- A QoS rule with a ToS and a QFI value for uplink traffic is provisioned.

Steps:

Provisioning: The 5GMS System is provisioned for Dynamic Policy usage as defined in clause 5.7.2 of TS 26.501 [15], Clause 5.7.2. As result, various functions of the 5G System are provisioned for QoS usage as follows:

1. The 5GMS Client has received Service Access Information (through M6 or M5), providing the information needed to use the Dynamic Policy Invokation API. Here, the sdfMethod indicates the usage of ToS. The 5GMS Client has activated a Dynamic Policy as described in clause 5.7 of TS 26.501 [15].

2. The 5GMS AF has provisioned the information for a Dynamic PCC rule with the PCF (possibly through NEF).

3. The PCF has authorized the request and created a PCC rule. The PCF has sent the PCC rule to the SMF, which has forwarded the QoS rule to the UE and to the UPF.

During Media Plane usage

4. The 5GMS Client initiates connection establishment by sending a TCP SYN packet. The 5GMS Client has set a ToS value in the TCP SYN packet, as provided by the 5GMS AF in an earlier step (see clause 5.3.4.3).

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

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

7. 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.

8. The 5GMS AS sends a TYP SYN–ACK back to the UE. The packet reaches the UPF on its path to the UE.

9. The UPF detects a PDR match for the UE. Here, the PDR for the UE IP address contains the ToS value. (The PDR was provided to the UPF in an earlier step as described in clause 5.3.4.3.)

10. The UPF encapsulates the downlink IP packet into an N3 packet. The UPF sets the QFI value in the N3 packet header.

11. The UPF sends the N3 packet to the RAN 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.

12. The 5GMS Client send the TCP ACK to complete the TCP connection handshake.

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

14. 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.

Discussion:

- The 5GMS AS needs to determine whether QoS should be used for this session and which ToS value to use.

- The Npcf\_PolicyAuthorization API allows a ToS value to be provisioned (without a direction indication), but the Nnef\_AFsessionWithQOS API does not support provisioning of a ToS value.

### 5.3.7 Conclusions

This Key Issue explored different solutions for traffic identification, so that the 5G System can detect different application flows and is enabled to apply an appropriate Policy and Charging Rules (PCC) to the associated traffic. The 5G System supports different means for direction-specific traffic detection. The use of the following traffic detection schemes is studied in detail in the context of 5G Downlink Media Streaming, e.g. assuming DASH content delivery:

- **5-tuple:** UE IP address, server IP address, protocol, UE port and server port.

- **Type of Service (ToS) field:** The ToS field is an 8-bit field within the IP header, that can be used to convey the 6-bit DSCP value. In IPv6, the Traffic Class field.

- **Packet Flow Description:** 3-tuple of Server IP address, protocol and server port.

The use of the Flow Label (IPv6 only), the security parameter index (IPsec) and the domain name (part of the Packet Flow Description) are not studied in detail. It is recommended to study IPsec and the usage of the security parameter index for traffic identification is a subsequent study.

NOTE: PFDs also support URL-based and domain name traffic detection. However, the URL is increasingly often encrypted (e.g. by the use of TLS or alternative encrypted transport) and therefore not visible to the network and domain name are also getting encrypted as encrypted forms of DNS and ECH are adopted.

Although TS 23.501 [23] defines a rich set of traffic detection schemes within the Packet Filter Set structure, only a subset of the schemes can be dynamically provisioned using APIs calls. Values for the ToS field, the Flow Label (IPv6 only), and the Security Parameter Index (IPsec only) can only be manually provisioned.

The data model of the Dynamic Policy API supports the selection of TOS, FlowLabel or Domain Names within the SdfMethod data type. However, there is no detailed definition on the usage of the feature, including the values for the ToS field. It is recommended to specify the usage of TOS and the configuration of the TOS values within a normative work item.

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