Policy and User Plane Management

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI

Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Added support for prioritization of packets to support dedicated UE services such as PTT service.	2024.01.1
• Added support for GBR bearer creation without PCF interaction for 4G and 5G. • Added the N7 optimization support. • Added support for optional PCF or PCRF configuration for local policy configuration.	2023.04.0
Added support for the following features: • QoS group of ruledefs over N7 • IPv6 support for N3 interface on UPF	2023.01.0
Added support for SMF— • to allocate UPFs with unique IP pools • to select the UPF based on PDN type	2022.04.0
Introduced support for Diff-Serv-Code-Point (DSCP) or Type of Service (ToS) QoS functions during interaction with PCF.	2021.02.3.t3
Introduced support for the following features: • Usage Monitoring over PCF • N4 QoS Mismatch Correction • Dynamic QoS Flow-based Application Detection and Control • IP Threshold-based UPF Selection	2021.02.3
Introduced support for non-standard QCI for dynamic PCC and session rules	2021.02.2

Revision Details	Release
Introduced support for the following features: • Bit rate mapping • UPF Selection based on Slice and Location • UP Optimization	2021.02.0
Introduced support for the following: • Co-located UPF Selection • Enhanced Limits for Maximum Groups in Bandwidth Policy Configuration • Handling Session Report Rejection Procedure • New Format of Outer Header information element (IE)	2021.01.0
Introduced support for the following: • UPF node selection based on DNN and PDU Session type • Modification of authorized default QoS • Additional session report and UPF node report request	2020.03.0
First introduced.	Pre-2020.02.0

Feature Description

Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

The SMF is one of the control plane NFs that provide the Session Management service in the 5G core network. The SMF manages the PDU session lifecycle through the following session management procedures:

- PDU Session Establishment
- PDU Session Modification
- PDU Session Release

This chapter describes the policy and user plane management features.

- Policy Management—Policy Control Function (PCF) or the local configuration controls the policies managed on SMF. The PCF sends Policy and Charging Control (PCC) rules along with the applicable

QoS and charging information to the SMF. The SMF uses this information to define QoS flows and apply QoS enforcement (via User Plane Function (UPF) and charging towards Charging Function (CHF). The PCC rules can be configured locally as well. The locally configured policy rules are labelled as static or predefined rules.

- User Plane Management—The user plane management on SMF includes selection of UPF and maintaining per session and node level user plane data. The SMF performs Path management of the UPF nodes. At a per session level, SMF publishes the Packet Detection Rules (PDRs), QoS Enforcement Rules (QERs), Forwarding Action Rules (FARs), and Usage Reporting Rules (URRs) to the UPF. Then, the SMF enforces the policy rules received from PCF or configured locally.

QoS Management on SMF

Feature Description

The primary functionality of the SMF is to manage the flow-based QoS model. SMF interacts with the Unified Data Management (UDM) and Policy Control Function (PCF) to get the subscribed and authorized QoS parameters for GBR and non-GBR flows and passes on the relevant information to UE (NAS), gNB (NGAP), and UPF (PFCP) so that all nodes on the network provide the desired QoS to the PDU session.

Use Cases

This section describes the various use case scenarios that can lead to creation, modification, and deletion of QoS-Profile and the corresponding actions taken.

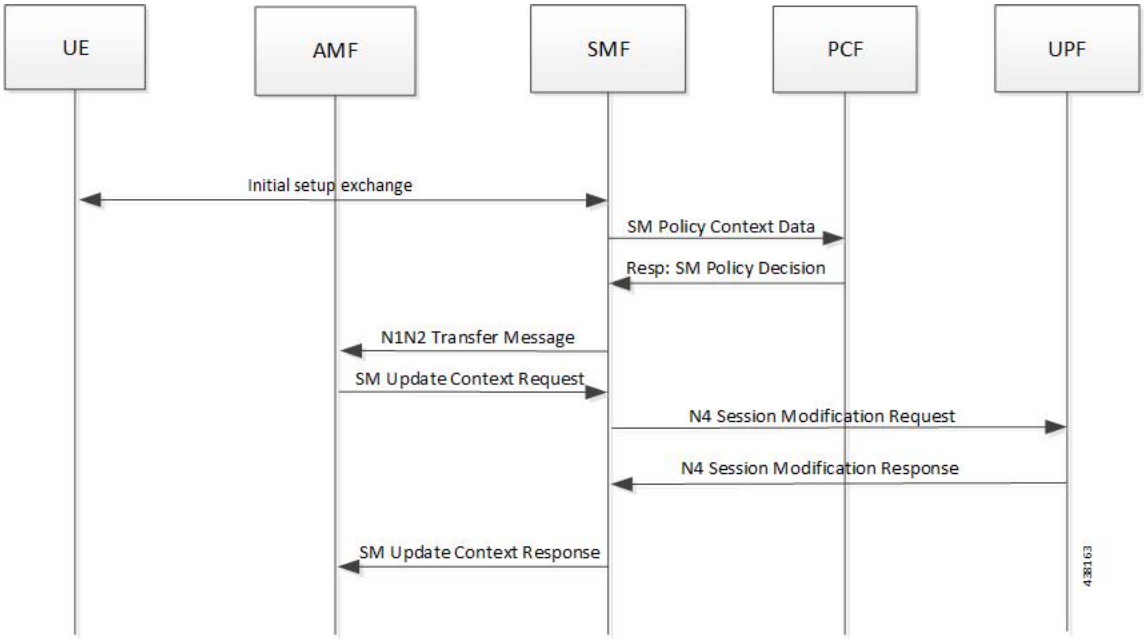
QoS-Profile associated to the PDU Context will be modified in the following scenarios:

- Response from PCF for SMPolicyContextData
- Update Notify from PCF
- Update response from PCF on behalf of Update request sent initially from SMF
- Update request from SMF will be triggered in the following cases:
  - UE triggered modify request
  - AN triggered modify request
  - UDM triggered modify request

Setup Creation

The following figure illustrates the setup creation call flow.

Figure 1: Setup Creation Call Flow


UE
AMF
SMF
PCF
UPF
Initial setup exchange
SM Policy Context Data
Resp: SM Policy Decision
N1N2 Transfer Message
SM Update Context Request
N4 Session Modification Request
N4 Session Modification Response
SM Update Context Response
438163

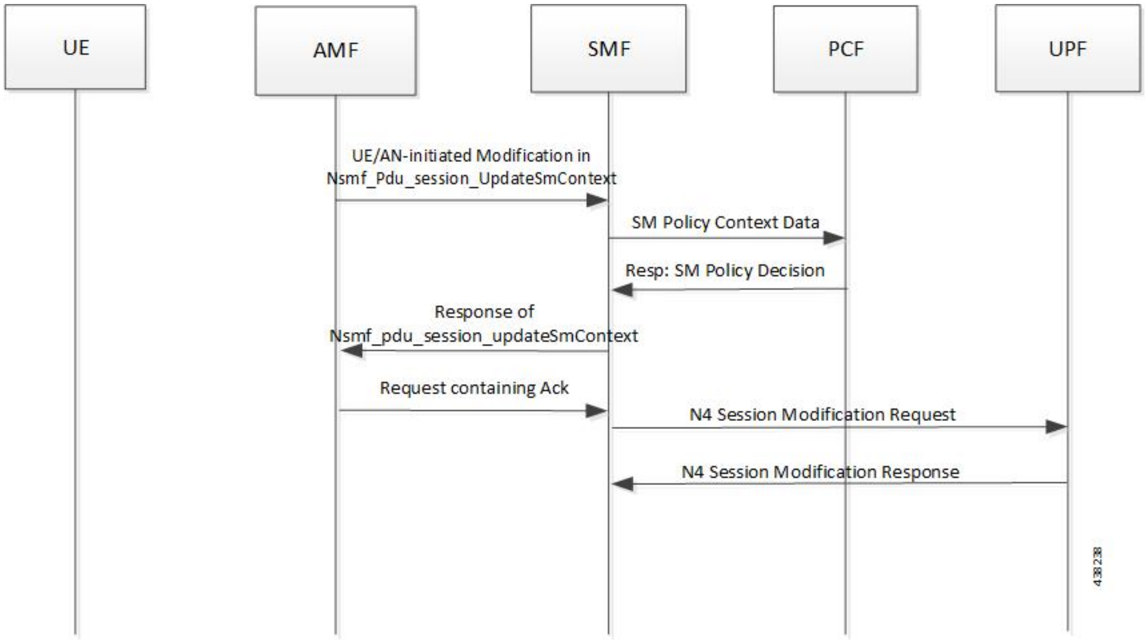
Based on the content received in SM Policy Decision, SMF pushes the following towards various interfaces.

- UPF:
  - Set of PDR derived from PCC rules
  - Set of QER derived from QoS flows which in turn are derived from QosDescription/QosCharacteristics from PCF
  - One extra QER derived from SessRules
- N1:
  - Set of QoS rules derived from QosFlows
  - Each QosRule has its associated packet filter
- N2:
  - Set of QoS Flow information

UE/AN-initiated Modification

The following figure illustrates the UE/AN-initiated modification call flow.

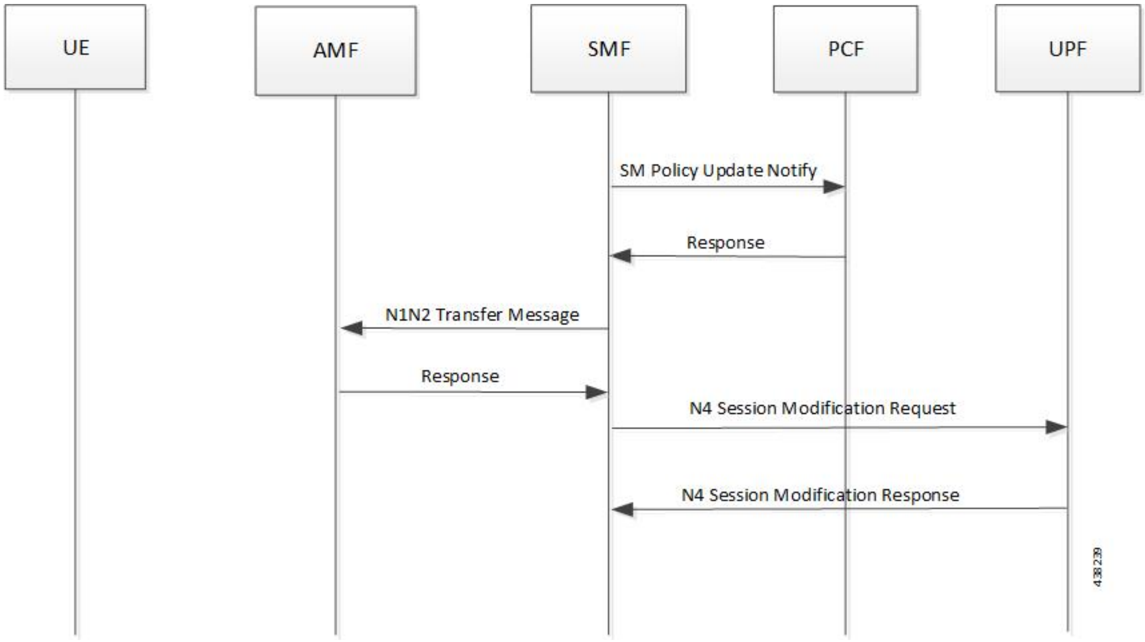
Figure 2: UE/AN-initiated Modification Call Flow


UE
AMF
SMF
PCF
UPF
UE/AN-initiated Modification in Nsmf_Pdu_session_UpdateSmContext
SM Policy Context Data
Resp: SM Policy Decision
Response of Nsmf_pdu_session_updateSmContext
Request containing Ack
N4 Session Modification Request
N4 Session Modification Response
438238

UDM/PCF-initiated Modify

The following figure illustrates the UDM/PCF-initiated Modify call flow.

Figure 3: UDM/PCF-initiated Modify



- N1:
  - PDU Session Modification command will be triggered from SMF. It can change Session-AMBR and QoS rules.

    - PDU Session Modification Request will be triggered from UE. It can change the QoS rules and maximum number of support-ed packet filters.

      In either case, the QoS rule change can happen from the following:

        - Packet filter add/delete/replace
        - Rule Precedence of QoS Rule
        - QoS Parameter – 5QI/MBR/GBR

- N2:

    - PDU Session Resource Modify Request will be triggered from SMF. It can change the existing QoS flow that is installed or delete the QoS flow already installed. If the Modify request is received, the parameters - ARP, GBR/MBR, Priority level, and so on, can change.

    - PDU Session Resource Notify will be triggered from AN. This happens when certain flow is to be released, not fulfilled any-more and fulfilled again.

Subscribed QoS

The UDM NF maintains the subscribed QoS for the UE in the Session Management Subscription Data. During the PDU setup procedure, the SMF posts an HTTP2 GET request (see *3GPP TS 29.503*) for a resource URI "/{supi}/sm-data" to fetch the Session Management Subscription Data. The subscription data has a set of DNN configurations, one for each DNN which the subscriber is allowed to access. Each DNN configuration consists of the following parameters:

- sessionAMBR: The maximum aggregated uplink and downlink bit rates to be shared across all non-GBR QoS flows in each PDU session.

- 5gQosProfile: The default 5G QoS Indicator (5QI) and default ARP values are provided to the SMF in the Session Management Subscription Data in this attribute of the DNN configuration.

The SMF saves the subscribed QoS parameters and sends this across to the PCF during the SM Policy Association Establishment procedure.

QoS Negotiation

The SMF negotiates the QoS with the PCF by initiating a Policy Association Establishment procedure as defined in *3GPP TS 23.502, section 4.16.4*. The sessionAMBR and 5gQosProfile parameters that are received from subscription are included in the Npcf_SMPolicyControl_Create request to PCF. The response from PCF may contain the following:

- Session Rules—A session rule consists of policy information elements that are associated with the PDU session. The QoS related information is Authorized session AMBR and Authorized default QoS.

    - Policy Charging and Control (PCC) Rules—The PCC rule includes the FlowDescription, FlowDirection, and RefQosData parameters among other information. There could be one or more PCC rules in the response from PCF.

        - FlowDescription—This parameter contains packet filters for IP flows. For IP PDU Session Type, the Packet Filter Set supports packet filtering based on at least 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) / Traffic class (IPv6) and mask

    - Flow Label (IPv6)

    - Security parameter index

  - FlowDirection—This parameter indicates the direction of data traffic on which the rule has to be applied. This could be UPLINK, DOWNLINK, or BIDIRECTIONAL.
  - RefQosData—This parameter refers to the QoS description to be applied to this PCC Rule. This matches the QosId of at least one of the QoS Description entries in the response from PCF.

- QoS Characteristics—The QoS characteristics include the following parameters:
  - Resource Type (GBR, Delay critical GBR, or non-GBR)
  - Priority Level
  - Packet Delay Budget
  - Packet Error Rate
  - Averaging Window
  - Maximum Data Burst Volume (for the Delay-critical GBR resource type only)

  This attribute in the response from PCF is meant to be used only for non-standard 5QI values. For standard 5QI values, the characteristics are already defined in *3GPP TS 23.501, section 5.7.4*.

- QoS Description—The QoS Description parameter consists of the following:
  - 5QI – Standard or non-standard from the QoS Characteristics attribute
  - Uplink and Downlink GBR
  - Uplink and Downlink MBR
  - Maximum Packet Loss Rate
  - QosId – Referenced in PCC rules
  - Default QoS Indication

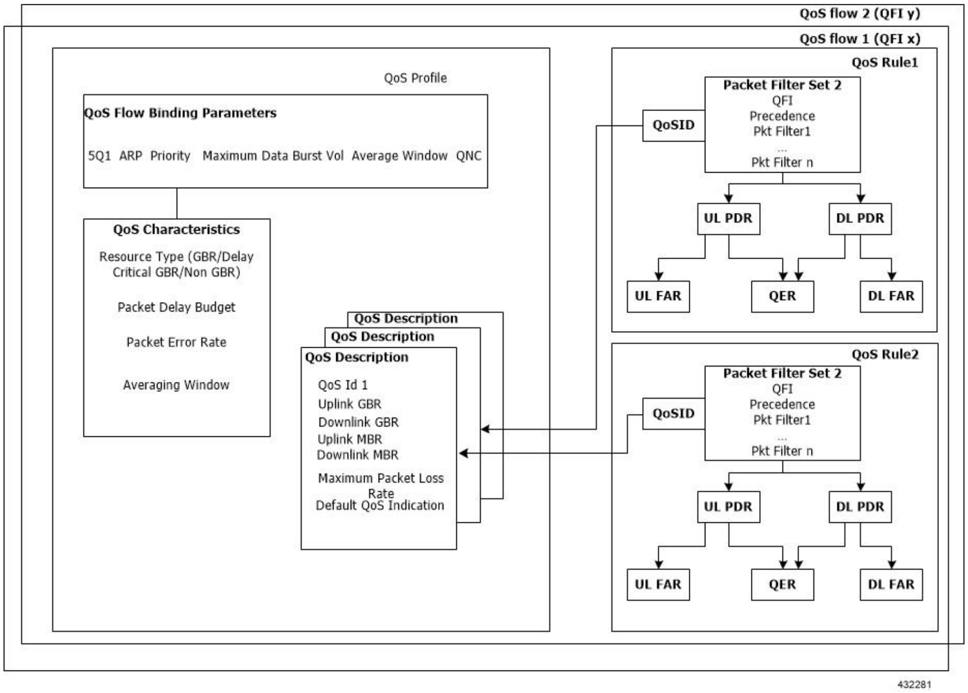
  There could be more than one QoS Description attribute in the response from PCF.

QoS Flow Management

The information, that is received from PCF in the Npcf_SMPolicyControl_Create response, is used to create and update QoS Flows in the SMF. Each QoS flow has a unique QoS Flow ID (QFI) and one or more PCC rules map to a single QoS flow.

The following figure illustrates how to manage the QoS information at the SMF.

Figure 4: QoS Information Management at SMF



Each QoS Flow in SMF is a combination of three sets of information:

- QoS profile: A QoS profile stores all QoS attributes for a particular QoS Flow.
  - Some QoS parameters known as the QoS flow binding parameters make a unique combination for one QoS Flow of one PDU Session. This means that, for a PDU session, each unique combination of these parameters represents a separate QoS Flow. These parameters are – 5QI, ARP, Priority, Maximum Data Burst Volume, Average Window and QNC.
  - If the 5QI for the QoS profile of a QoS Flow is non-standard, some additional QoS characteristics, such as Resource Type, Packet Delay Budget, Packet Error rate, and Averaging Window are also saved in the QoS profile.
  - The QoS profile also maintains multiple QoS Descriptions, each with a unique QoSId for a specific PDU session. Each QoS Description contains the uplink and downlink GBR, uplink and downlink MBR, maximum packet loss rate and default QoS indication.
- QoS Rules: A QoS rule is a collection of packet filters that associates with a particular QoS Description in the QoS profile of the QoS flow. The packet filters directly map to the flow descriptions received in the PCC rules in the Npcf_SMPolicyControl_Create response from PCF. The QoS rules have a reference to the QoSId of the QoS Descriptions that the rules associate with.
- PDRs: Each QoS rule maps to two Packet Detection Rules (PDR) to be sent to the UPF. One PDR is for uplink direction and the other PDR is for downlink direction. The Service Data Flow (SDF) filters in the Packet Detection Information (PDI) attribute within the PDRs map the packet filters of the QoS rule. Each PDR then maps to a Forwarding Action Rule (FAR), which determines the forwarding action for the packets matching the SDF filters. Each PDR is also associated to a QoS Enforcement Rule (QER) which carries the QoS information and it maps to the QoS description associated with the QoS rule.

QoS Communication on 3GPP Interfaces

The negotiated QoS mainly needs to be communicated to the UE (N1 interface using NAS protocol), gNB (N2 interface using NGAP protocol), and UPF (N4 interface using PFCP protocol).

- N1 Interface: On the N1 interface, the session management messages are exchanged between UE and SMF through AMF. The NAS messages are encoded into an N1 container and sent to SMF or received from SMF.
  - All the negotiated/authorized QoS related information that needs to be sent out to the UE are found in the Authorized QoS rules and Session-AMBR attributes of the PDU SESSION ESTABLISHMENT ACCEPT message in an N1 container, during the PDU session establishment (see *3GPP TS 24.501, section 8.3.2*).
  - The PDU SESSION MODIFICATION REQUEST message from UE contains the Requested QoS Rules during the UE initiated QoS modification.
  - The Authorized QoS rules and Session-AMBR attributes are also present in the PDU SESSION MODIFICATION COMMAND message sent from SMF to UE during the PCF/SMF initiated QoS modification.
  - The format of the QoS Rule NAS attribute is defined in *3GPP TS 24.501, section 9.10.4.9*. This attribute mainly consists of the packet filter list, QFI, and QoS parameters on a per QoS rule basis. This information is available in the QoS rule within the QoS flow.
- N2 Interface: On the N2 interface, SMF sends an N2 container to the gNB through AMF. The N2 container is ASN.1 encoded data and consists of specific information elements of NGAP messages. All the QoS related information to gNB is encoded and sent/received in N2 containers to/from SMF. The NGAP IEs and the corresponding NGAP messages that will finally carry the IE from AMF to gNB are listed in *3GPP TS 29.502, section 6.1.6.4.3*.
  - During the PDU session setup, the SMF sends N1N2MessageTransfer to AMF with the N2 container in the PDU Session Re-source Setup Request Transfer IE. This IE contains PDU Session Aggregate Maximum Bit Rate and QoS Flow Setup Request List. The QoS Flow Setup Request List contains QoS Flow Level QoS Parameters (GBR flow information, 5QI, and so on). These are defined in *3GPP TS 38.413, section 9.3.1*.
  - Similar information (QoS Flow Level QoS Parameters) is also sent by SMF in the PDU Session Resource Modify Request Transfer IE in an N2 container during the PCF/SMF initiated QoS Modification procedure.

    The information required to create the N2 container in SMF is present in the QoS profile of a QoS flow as described in the previous section.
- N4 Interface: On the N4 interface, the SMF sends the QoS information in the form of Packet Detection Rule (PDR), Forwarding Action Rule (FAR), and QoS Enforcement Rule (QER).
  - The PDR contains the SDF filters in the PDI IE. These SDF filters are the packet filters set in the QoS Rule of a QoS flow.
  - The QER contains the QoS parameters as per the QoS Description to which the QoS rule is associated.

    The contents of PDR, FAR, and QER are defined in *3GPP TS 29.244*.

QoS Modification

QoS modification may result in one of the following scenarios:

- QoS Flow Addition: Whenever a negotiated QoS is received from PCF either as part of UE initiated modification or PCF initiated QoS modification, the SMF extracts the received QoS Flow Binding Parameters (5QI, ARP, Priority, Max Data Burst Volume, QNC). If there is no QoS Flow with the received combination of the flow binding parameters, SMF adds a new QoS flow and the received PCC rules will be mapped against the new QoS flow. As a result, the new QoS flow rules/QoS descriptions/PDR/QER are created and the corresponding interfaces (N1, N2, and N4) are updated by creating new flows.
- QoS Flow Modification: Whenever a negotiated QoS is received from PCF either as part of UE initiated modification or PCF initiated QoS modification, the SMF extracts the received QoS Flow Binding Parameters (5QI, ARP, Priority, Maximum Data Burst Volume, QNC). If there exists a QoS flow with the same combination of binding parameters, the QoS profile, QoS rules, PDR, and QER for that QoS flow are updated on N1, N2 and N4 interfaces.

Qos Capability Support for PCF and SMF Interaction

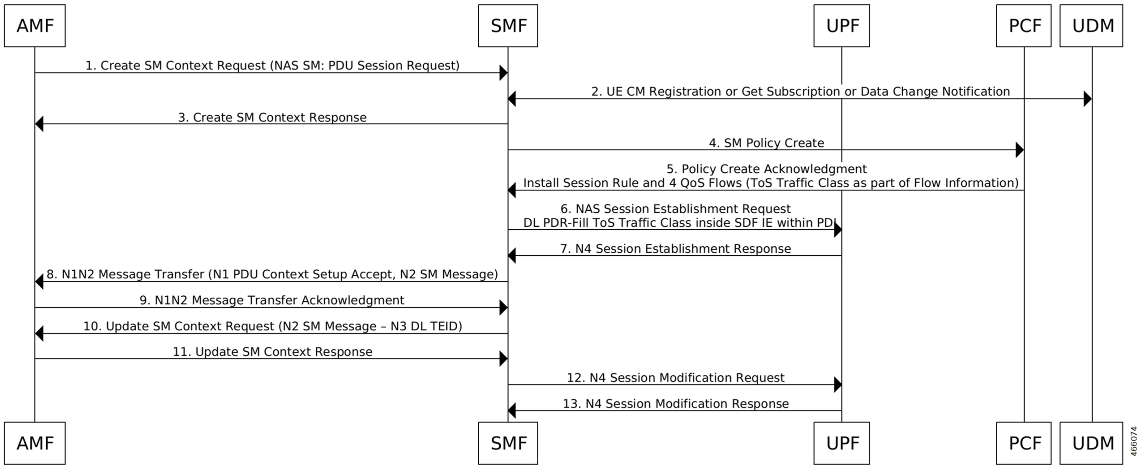
SMF supports Diff-Serv-Code-Point (DSCP) or Type of Service (ToS) QoS functions during interaction with PCF. Traffic defined at SMF can be prioritized based on the `tosTrafficClass` value that SMF receives from PCF. Using the ToS values provided, UPF performs DSCP packet match in the downlink direction and UE performs DSCP packet match in the uplink direction. This feature allows packet matching using ToS values, even if no `FlowDescription` values exist.

The following functions enable this feature:

- PCF sends `tosTrafficClass` IE which is part of `FlowInformation` within the PCC rule from PCF. SMF decodes it and stores it as part of the respective QoS Flow.
- SMF populates the `tosTrafficClass` IE value received from PCF in the `tosTrafficClass` inside SDF IE within PDI while creating the downlink PDR.
- Support for `tosTrafficClass` toward UE.

The following call flow describes the flow from PCF to SMF to support `tosTrafficClass` IE:

*Figure 5: Call Flow to Support **tosTrafficClass** IE*


AMF
SMF
UPF
PCF
UDM
1. Create SM Context Request (NAS SM: PDU Session Request)
2. UE CM Registration or Get Subscription or Data Change Notification
3. Create SM Context Response
4. SM Policy Create
5. Policy Create Acknowledgment
Install Session Rule and 4 QoS Flows (ToS Traffic Class as part of Flow Information)
6. NAS Session Establishment Request
DL PDR-Fill ToS Traffic Class inside SDF IE within PDI
7. N4 Session Establishment Response
8. N1N2 Message Transfer (N1 PDU Context Setup Accept, N2 SM Message)
9. N1N2 Message Transfer Acknowledgment
10. Update SM Context Request (N2 SM Message – N3 DL TEID)
11. Update SM Context Response
12. N4 Session Modification Request
13. N4 Session Modification Response
AMF
SMF
UPF
PCF
UDM
466074

- You can deploy basic PCF which supports minimal functionality. The PCF need not support northbound interfaces and installs dedicated flows which are based on local configuration.
- UE only creates a single session (default bearer) to support data, voice, and video. PCF triggers four flows during PDU session creation, one each for voice, video, data, and network management.
- PCF based on local configuration sends four PCC rules each with `FlowInformation` carrying `tosTrafficClass` IE in the N7 create response.
- SMF supports flow creation for PCC rules mapped with `FlowInformation` having only `tosTrafficClass` and no `FlowDescription`.
- PCF may include `FlowDescription` within `FlowInformation` with filters, such as `permit in IP from any to any` or `permit out IP from any to any`.
- PCF includes QoS Data in `smPolicyDecision` for each of the pcc rules indicating the associated QCI. SMF creates QoS Flow for each of the QCI.
- SMF includes `tosTrafficClass` inside SDF IE in the downlink PDR in `N4SessionEstablishmentReq` to UPF while installing the rules from PCF with mapped `tosTrafficClass`.
- SMF sends the N1 PDU establishment response to PCF. This response includes details, such as QoS rules containing packet filters that are configured with type of service or traffic class type, based on the information that is received from PCF. If the SMF doesn't receive the flow direction from PCF, packet filter direction is populated as `bidirectional` and packet filter component type identifier is populated as `Type of service` or `Traffic class type`.

Note `FlowDirection` is an optional parameter and its default value is **`bidirectional`**.

Bit Rate Mapping Support

Feature Description

Bit Rate Mapping support for 5G Core Network

The SMF receives QoS values for uplink and downlink traffic in bits per seconds (bps) from PCF.

If an interface other than GTPv2 interface sends Access Point Name Aggregate Maximum Bit Rate (APN-AMBR), the SMF converts the received value to kilobits per seconds (kbps). This conversion results in truncation of fractional value to the nearest integer (floor value), and hence the loss of information.

To minimize the bandwidth loss, the CLI command **bitrates rounded-up** is introduced to control the rounding off of the fractional QoS value to ceiling value or floor value. This behavior is in compliance with the 3GPP 29.274 specification, version 12. If the CLI command is enabled within **profile network-element pcf** configuration, the SMF sends the ceiling value over N1, N4, S5, or S8 interface.

In roaming scenarios, when the SMF acts as hSMF and the Bit Rate Mapping Support feature is enabled, then the hSMF sends the rounded-up bit rates in qosFlowDescription over N16 and N4.

When the SMF acts as vSMF and this feature is enabled, vSMF forwards the qosFlowDescription as received over N16 interface and rounds up the Session-AMBR value before sending over N1 and N4 interfaces.

Note vSMF does not communicate with PCF. In order to support this feature, vSMF must have network-element-profiles pcf configured with the feature enabled.

Note The **bitrates rounded-up** CLI command is applicable to both roaming and non-roaming scenarios.

By default, the SMF rounds off the bit rate to the floor value during conversion.

This feature impacts the following procedures:

- 5G session establishment
- 4G session establishment with dedicated bearer
- WiFi call establishment
- Handover scenarios
  - NR to Wi-Fi
  - Wi-Fi to NR
  - Wi-Fi to 4G
  - 4G to Wi-Fi
  - 4G to NR
  - NR to 4G
- PDU session establishment with different Data Network Names (DNNs)

Important If the PCF responds with a bit rate greater than 4.2 Gbps, then the SMF limits the bit rate to 4.2 Gbps only when the Dual Connectivity New Radio (DCNR) is disabled for a 4G-capable UE.

How it Works

This feature works only when the **bitrates rounded-up** CLI command is enabled within **profile network-element pcf** configuration. Upon enabling this feature, the SMF rounds off the QoS value upwards.

For example, if the SMF receives a bit rate of 123,456 bps over N7 interface, it converts the 123,456 bps to 123 kbps and loses the fractional value. With this feature enabled, the SMF converts 123,456 bps to 124 kbps.

Standards Compliance

The Bit Rate Mapping feature complies with the following standard:

- *3GPP TS 29.274, Release 12 – 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3*

Configuring Bit Rate Mapping

To enable the Bit Rate Mapping feature, use the following sample configuration.

```
config
  profile network-element pcf profile_name
    bitrates rounded-up
    exit
```

NOTES:

- **profile network-element pcf** *profile_name*: Specify a profile name for the PCF.
- **bitrates rounded-up**: Configure this keyword to round off the fractional QoS value to the ceiling value. The SMF sends the ceiling value over the intended network interface.

  By default, the SMF rounds off the bit rate to the floor value during conversion.

Verifying the Feature Configuration

Use the following command to verify the status of Bit Rate Mapping feature.

```
show full-configuration profile network-element pcf
```

If the bit rate round up is enabled within the PCF profile, then the **bitrates round-up** string is displayed. Otherwise, the string does not appear.

The following configuration is a sample output of this show command:

```
show full-configuration profile network-element pcf
profile network-element pcf pcf1
nf-client-profile PP1
failure-handling-profile FH1
query-params [ dnn ]
rulebase-prefix cbn#
predefined-rule-prefix crn#
bitrates rounded-up
exit
```

Bitrate Mapping across Diameter Interfaces

The SMF receives QoS values for uplink and downlink traffic in bits per seconds (bps) from PCRF.

If an APN-AMBR for uplink and the APN-AMBR for downlink are received from an interface other than the GTPv2 interface, the SMF converts the APN-AMBR for uplink and the downlink values in bits per second to kilobits per second. If this conversion results in fractions, then the value of APN-AMBR for uplink and the APN-AMBR for downlink gets rounded upwards.

By default, if the configuration isn’t configured, the SMF rounds off the bit rate to the CEIL value during conversion.

This feature impacts the following procedures:

- 4G session establishment
- Default bearer update over RAR/CCA-U

Configuring Bit Rate Mapping with Diameter Interfaces

To enable Bitrate mapping across Diameter and GTPv2 interfaces, use the following sample configuration.

Note Use the same configuration for dedicated bearer bitrates conversion such as MBR/GBR/APN-AMBR.

```
config
   profile network-element pcrf profile_name
      bitrates rounded-down
      diameter-client-profile Diameter Client_Profile Name
      subscription-idsubscription-id
      exit
```

NOTES:

- **profile network-element pcrf** *profile_name*: Specify a profile name for the PCRF.
- **bitrates rounded-down**: Configures bitrates round down. The SMF sends the Floor value over the intended network interface.

  By default, the SMF rounds off the bit rate to the CEIL value during conversion and the bitrates are rounded-up.

Handling of Authorized QoS for Default Bearer

Feature Description

The CHF server interacts with PCF to report the user quota exhaustion. Then, the PCF initiates a policy update request towards SMF to modify the authorized default Quality of Service (QoS) of a session rule. The QoS can be QoS Class Identifier (QCI) or 5G QoS Indicator (5QI), session Aggregate Maximum Bit Rate (AMBR), or both QCI/5QI and session AMBR.

Whenever the quota of user exhausts, this QoS modification results in downgrading:

- the DSCP marking of the data packets for the session
- the AMBR of the session

When you replenish the quota, the PCF reverts to the previous authorized QoS for the default bearer.

Be aware of the following changes whenever the QCI/5QI changes for the default flow or bearer.

- The QCI/5QI information is updated in the Event Data Record (EDR) generated for that session. Then, the SMF sends the updated bearer level information over Packet Forwarding Control Protocol (PFCP) message to support the EDR functionality.
- DSCP marking for the data packets is updated for all Packet Detection Rules (PDRs) pertaining to the default bearer or flow.
- Any QCI information sent in LI packets are updated.

- Rulebase change and Ruledef activation or deactivation work as expected along with 5QI change and session AMBR change.
- Any modified QoS is sent in Charging Data Request (Update) message to the CHF. Also, change in QCI/5QI in the authorized QoS is treated as a QoS change trigger for charging and CDR-U is sent.

How it Works

This section provides detailed changes in SMF to support change of QCI/5QI value in authorized QoS once the PDU session is established.

Default-Bearer QoS Handling for 4G and WiFi Sessions

The following procedure explains how the SMF handles the modification of authorized default QoS in 4G and WiFi sessions.

1. The SMF receives SmPolicyUpdateNotify from PCF with changed QCI/5QI in AuthorizedDefaultQoS and/or a different session AMBR value.
2. The SMF initiates Update Bearer Request towards S-GW for the default bearer.
    a. In the Update Bearer Request, Bearer Context IE is included for the default bearer and the corresponding Bearer QoS is updated with the changed QCI value.
    b. For the 4G session, the extended Protocol Configuration Options (ePCO), if supported, is included in the Update Bearer Request message. The ePCO includes 5G Authorized QoS Flow Information with updated QCI value for the default flow when the interworking (IWF) is enabled for the session. Otherwise, PCO IE is sent with the same details.
    c. For the WiFi session, Additional Protocol Configuration Options (APCO) is included in the Update Bearer Request message. The APCO contains 5G Authorized QoS Flow Information with updated QCI value for the default flow.
3. The SMF accepts the Update Bearer Response from S-GW.
4. On the N4 interface, the following changes are done:
    a. New instance of the BearerLvlInfo IE is included with the changed QCI value for default bearer tunnel.
    b. Update PDR is sent for all PDRs which are a part of default flow to reflect the association with the new BearerLvlInfo IE.
    c. FAR associated with all PDRs in the default flow is updated with the new DSCP marking value if the 5QI-DSCP mapping configuration has a different value for the changed 5QI.

Default-Bearer QoS Handling for 5G Sessions

The following procedure explains how the SMF handles the modification of authorized QoS for the default bearer in a 5G session.

1. The SMF receives SmPolicyUpdateNotify from PCF with changed 5QI in AuthorizedDefaultQoS and/or a different session AMBR value.

2. The SMF initiates N1N2MessageTransfer procedure with AMF to send N1 PDU Session Modification Command and N2 PDU Session Resource Modify Request Transfer IE in this message.
    a. In the N1 message, the default QoS flow is modified in Authorized QoS Flow Description IE to update the 5QI value.
    b. In the N1 message, the Mapped EPS Bearer Context IE is modified to update the QCI of the default bearer.
    c. In the N2 message, the QoS flow level QoS parameter for the default flow is modified to update the 5QI value.
3. The SMF accepts the SMContextUpdate Request from AMF with the responses for the N1 and N2 requests sent in N1N2Message Transfer message.
4. On the N4 interface, the following changes are done:
    a. New instance of the BearerLvlInfo IE is included with the changed 5QI to QFI mapping.
    b. Update PDR is sent for all PDRs which are a part of default flow to reflect the association with the new BearerLvlInfo IE.
    c. Forwarding Action Rule (FAR) associated with all PDRs in the default flow is updated with the new DSCP marking value if the 5QI-DSCP mapping configuration has a different value for the changed 5QI.

Default-Bearer QoS Handling During WiFi Handovers

The following procedure explains how the SMF handles the modification of authorized default QoS during WiFi handover and other handovers.

1. The SMF sends SMPolicy Update Request to the PCF at the end of each handover procedure. For example, when the PCF arms different policy triggers, the SMF sends SMPolicy Update Request to the PCF. The response from PCF contains the changed QCI in Session Rule (Authorized Default QoS). The SMF initiates the modification procedure towards RAN/UE, and communicates the same information on N1, N2, N4, and S5 interfaces.
2. For all handovers (excluding WiFi-NR/EPS and NR/EPS-WiFi), the SMF sends SMPolicy Update Request to the PCF indicating the RAT type change. The response from PCF contains the changed QCI in Session Rule (Authorized Default QoS). The SMF initiates the modification procedure towards RAN/UE, and communicates the same information on N1, N2, N4, and S5 interfaces.

The handovers involving WiFi are different from the other handovers. The SMF triggers SMPolicy Update Request towards PCF during the handover and not after the handover. For the handovers involving WiFi, the target RAN installs the flows and bearers as new instead of an update. The SMF sends the latest QCI received in the response from PCF while installing the default flow and bearer during the handover.

Default-Bearer QoS Modification During Failure Handling

For a 5G session, the modification of QCI/5QI typically does not fail on the N1 or N2 interface as the default flow is a non-GBR flow and no resource reservation is required for the QCI/5QI modification. However, if the modification procedure fails due to no N1 or N2 responses from AMF, the modification is rolled back and the session continues with the old QCI/5QI and session AMBR values. If the N2 rejects the flow modification, the session is deleted as it cannot remain without the default flow.

For a 4G session, the Update Bearer response does not fail for default bearer modification. However, if the Update bearer Response is missing or if it fails, the modification is rolled back and the session continues with the old 5QI and session AMBR values.

For both 4G and 5G sessions, if the N4 update fails or the response is not received, then the SMF takes the action according to the UPF failure handling template configuration. For 4G and WiFi sessions, if there is a failure on the N4 interface, another Update Bearer Request is sent with the old 5QI and AMBR values to S-GW and ePDG respectively.

The failure handling mechanism remains the same for the PCF-initiated modification procedure.

Limitations

The Authorized QoS Handling for Default Bearer feature has the following limitations:

- The combination of QoS flow binding parameters, such as 5QI and ARP, for the authorized QoS never remains the same as that of a dedicated bearer or flow. That is, change in QCI/5QI should not result in the default flow having the binding parameters similar to another flow.
- The SMF does not support changes to all the binding parameters except Allocation and Retention Priority (ARP) and the QCI/5QI (with or without session AMBR) in the Session Rules.
- When the QCI/5QI changes, the existing default bearer flow is modified toward N1, N2, and N4 interfaces. In this case, the SMF does not delete the existing flow instead of creating a new flow.

Authorized QoS Handling OAM Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The SMF maintains the label "SESSRULE_CHANGE" to indicate any changes to the AMBR value, QCI/5QI value, or a combination of both AMBR and QCI/5QI values.

GBR Bearer Creation Based on Local Policy

Feature Description

In cases where a minimum bit-rate guarantee is required, GBR bearers are needed to be created. With the N7 interface, the GBR bearers are created upon receiving the request from the PCF. However, in the absence of PCF, the GBR bearers can be created right after the session creation using the local policy configured in the SMF.

SMF allows creating GBR bearers based on local policies in 4G and 5G RATs.

How It Works

In this approach, there are two bearers created:

1. **Default Non-GBR Bearer**: The default non-GBR bearer/flow is created based on the QoS received from UDM or local configuration in case of New Radio (NR) and the QoS received from MME is used in case of EUTRA.
2. **Dedicated GBR Bearer**: Dedicated GBR flows/bearers are additionally created based on local policy configuration.

Creating Default Non-GBR Bearer and Dedicated GBR Bearer Without PCF

For creating the default bearer/flow, the negotiated QoS profile is chosen.

- For 4G sessions, if N7 interaction is disabled, MME provided QoS is used.
- For 5G sessions, if N7 and N10 interaction is disabled, the locally defined QoS profile, which is associated to the DNN profile is used.

For creating Dedicated Bearer/Flow without PCF intervention, event management policies are required. The association of event management policies with the DNN profile takes place with the help of a configuration. Whenever an event is triggered, the event management policy associated to that DNN is executed. Each event policy configured under the event management policies are executed in a sequence of priority, until a match is found based on event and rule.

The new configuration allows define the event management policies. Multiple priority-based event handling policies can be configured under the event management policy. Each of the event policies configured are executed in the order of priority till a match is found based on event and rule.

In case of NR, the dedicated and default flow parameters are sent to the UE in N1 PDU Session Establishment Accept and to the gNB in N2 Setup Request. In case of E-UTRA, the Default Bearer creation is done as part of the Create Session Response and a GBR Dedicated Bearer is created by triggering a Create Bearer Request (CBR) immediately after sending the Create Session Response. This is similar to the piggy-backed CBR triggered by PCF, which is already supported in SMF.

Note This feature does not supports the real piggybacked-CBR, where CBR and CSR response are sent in the same message.

5G Attach with Dedicated GBR Bearer Creation

The following call flow displays the process of 5G attach with Dedicated GBR Bearer creation:

Figure 6: Call Flow for 5G Attach with Dedicated GBR Bearer Creation (Without PCF Interaction)

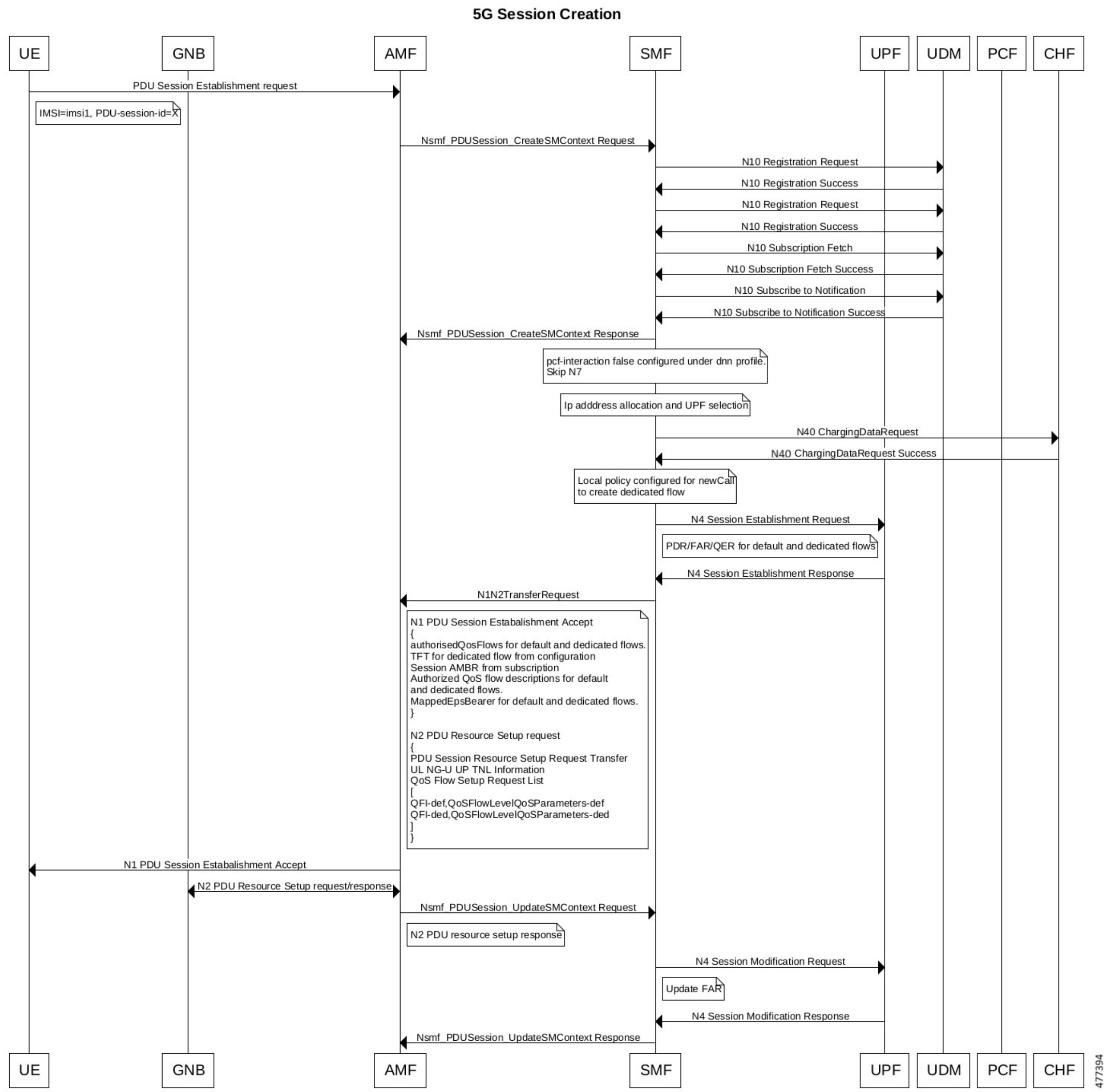

5G Session Creation
UE
GNB
AMF
SMF
UPF
UDM
PCF
CHF
PDU Session Establishment request
IMSI=imsi1, PDU-session-id=X
Nsmf_PDUSession_CreateSMContext Request
N10 Registration Request
N10 Registration Success
N10 Registration Request
N10 Registration Success
N10 Subscription Fetch
N10 Subscription Fetch Success
N10 Subscribe to Notification
N10 Subscribe to Notification Success
Nsmf_PDUSession_CreateSMContext Response
pcf-interaction false configured under dnn profile.
Skip N7
Ip adddress allocation and UPF selection
N40 ChargingDataRequest
N40 ChargingDataRequest Success
Local policy configured for newCall
to create dedicated flow
N4 Session Establishment Request
PDR/FAR/QER for default and dedicated flows
N4 Session Establishment Response
N1N2TransferRequest
N1 PDU Session Estabalishment Accept
{
authorisedQosFlows for default and dedicated flows.
TFT for dedicated flow from configuration
Session AMBR from subscription
Authorized QoS flow descriptions for default
and dedicated flows.
MappedEpsBearer for default and dedicated flows.
}
N2 PDU Resource Setup request
{
PDU Session Resource Setup Request Transfer
UL NG-U UP TNL Information
QoS Flow Setup Request List
[
QFI-def,QoSFlowLevelQoSParameters-def
QFI-ded,QoSFlowLevelQoSParameters-ded
]
}
N1 PDU Session Estabalishment Accept
N2 PDU Resource Setup request/response
Nsmf_PDUSession_UpdateSMContext Request
N2 PDU resource setup response
N4 Session Modification Request
Update FAR
N4 Session Modification Response
Nsmf_PDUSession_UpdateSMContext Response
UE
GNB
AMF
SMF
UPF
UDM
PCF
CHF
477394

Table 3: Call Flow Description for 5G Attach with Dedicated GBR Bearer Creation (Without PCF Interaction)

Step	Description
1.	The UE initiates the PDU Session Establishment procedure by sending a NAS message to the AMF, containing a PDU Session Establishment Request within the N1 SM container. The PDU Session Establishment Request includes a PDU session ID and IMSI.
2.	If the AMF does not have an association with an SMF for the PDU Session ID provided by the UE, the AMF invokes the Nsmf_PDUSession_CreateSMContext Request. The AMF forwards the PDU Session ID together with the N1 SM container containing the PDU Session Establishment Request received from the UE.

Step	Description
3.	SMF sends the N10 Registration Request to the UDM. Then, UDM sends the N10 Registration Response to the SMF.
4.	SMF sends the N10 Subscription Fetch Request to the UDM. Then, UDM sends the N10 Subscription Fetch Response to the SMF.
5.	SMF sends the N10 Subscribe to Notification Request to the UDM. Then, UDM sends the N10 Subscribe to Notification Success Response to the SMF.
6.	If the SMF is able to process the PDU Session Establishment Request, the SMF creates an SM context. Then, SMF sends the Nsmf PDU Session CreateSMContext Response to the AMF. If the PCF is not deployed, hence **pcf-interaction false** has to be configured on the SMF. Hence, SMF applies the local configuration to perform the mapping of PCC rules and 5G QoS parameters. At this stage, the SMF also selects one or more UPFs.
7.	(Optional) The SMF sends a charging data request over the N40 interface to the CHF. Then, the CHF responds back to the SMF with N40 ChargingDataRequest Success response.
8.	At this stage, the local policy is used to configure a new call to create a dedicated flow. If the predefined rules are mapped to a dedicated flow/bearer, SMF sends the N4 Session Establishment Request to the UPF. SMF also sends Create PDR/FAR/QER/URR Request for both default and dedicated flows to the UPF.
9.	The UPF responds to SMF with the N4 Session Establishment Response.
10.	SMF sends the NamfCommunication N1N2 Message Transfer request to AMF. This message contains N1 PDU Session Establishment Accept with authorized QoS Flows for both default and dedicated flows, TFT for dedicated bearer from configuration, Session AMBR from subscription, Authorized QoS flow descriptions for default and dedicated flows, and Mapped EPS bearers for default and dedicated flows. The NamfCommunication N1N2 Message Transfer request also contains N2 PDU Resource Setup Request containing PDU Session Resource Setup Request Transfer, UL NG-U UP TNL Information, and QoS Flow Setup Request List.
11.	The N1 PDU Session Establishment Accept is sent from AMF to the UE.
12.	The N2 PDU Resource Setup Request is sent from the AMF to the gNB. In response, the gNB sends the N2 PDU Resource Setup Response to the AMF.
13.	AMF sends the Nsmf PDU Session UpdateSMContext Request (N2 PDU Resource Setup Response) to SMF. This message contains N2 PDU Resource Setup Request.
14.	SMF sends the N4 Session Modification Request to UPF. This request is to update FAR with GNB tunnel information.
15.	UPF sends the N4 Session Modification Response to SMF.
16.	SMF sends the Nsmf PDU Session UpdateSMContext Response to AMF.

4G Attach with Dedicated GBR Bearer Creation

The process of 4G attach with the Dedicated GBR Bearer creation follows the given steps:

Figure 7: Call Flow for 4G Attach with Dedicated GBR Bearer Creation

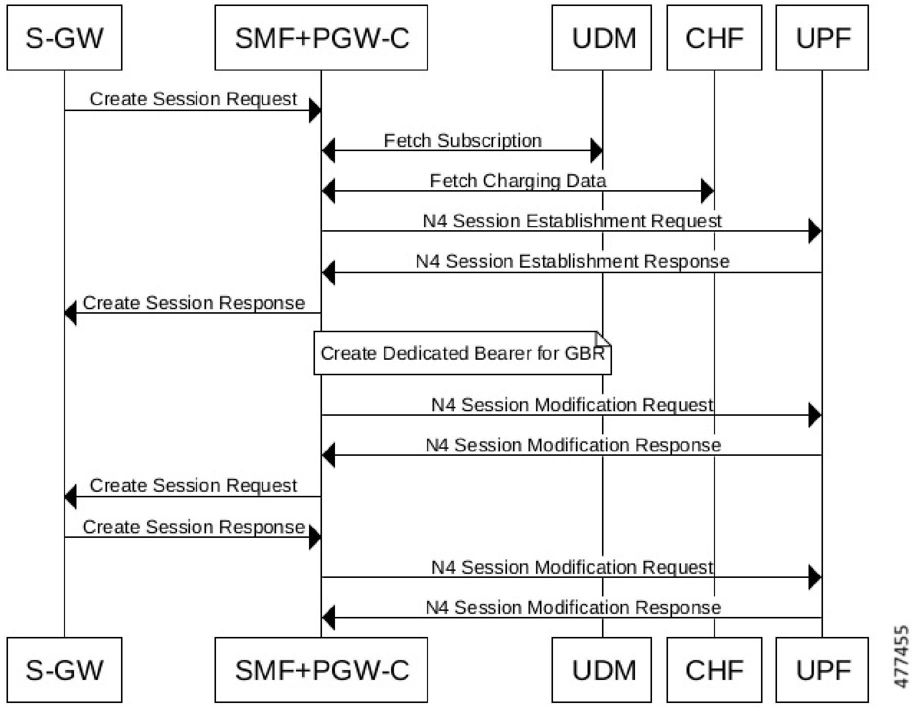

S-GW
SMF+PGW-C
UDM
CHF
UPF
Create Session Request
Fetch Subscription
Fetch Charging Data
N4 Session Establishment Request
N4 Session Establishment Response
Create Session Response
Create Dedicated Bearer for GBR
N4 Session Modification Request
N4 Session Modification Response
Create Session Request
Create Session Response
N4 Session Modification Request
N4 Session Modification Response
S-GW
SMF+PGW-C
UDM
CHF
UPF
477455

Table 4: Call Flow Description for 4G Attach with Dedicated GBR Bearer Creation

Step	Description
1.	S-GW sends the Create Session Request to SMF.
2.	SMF sends the Subscription Fetch Request to the UDM. Then, UDM sends the Subscription Fetch Response to SMF.
3.	SMF sends the Charging Data Request to CHF. Then, CHF sends the N40 Charging Data Response to the SMF.
4.	SMF sends the N4 Session Establishment Request to UPF.
5.	After the creation of the tunnel, UPF sends the N4 Session Establishment Response to SMF.
6.	SMF sends the Create Session Response to S-GW. This response includes the 4G default bearer tunnel information.
7.	Dedicated GBR bearer creation is initiated based on local policy configuration. At this stage, SMF sends the N4 Session Modification Request to the UPF. This message includes a request for creating a dedicated GBR bearer.

Step	Description
8.	UPF sends the N4 Session Modification Response to the SMF.
9.	SMF sends the Create Bearer Request to S-GW. This request includes information on the bearer context list, which contains information about QOS, TFTs, and UPF FTEIDs.
10.	SGW sends the Create Bearer Response to SMF. The response includes details on request accepted or request accepted partially and bearer contexts.
11.	SMF sends the N4 Session Modification Request to UPF. This request is to update FAR with SGW-U tunnel information for each bearer
12.	UPF responds with N4 Session Modification Response to the SMF and the bearer is established on SMF.

Limitations

Following are the known limitations of this feature:

- This feature supports 4G calls without PCF and not without PCRF.

Configuration for Creating Default Non-GBR Bearer and Dedicated GBR Bearer without PCF

To create Default Non-GBR and Dedicated GBR bearers, the following step-wise configuration is required:

1. Associate QoS profile and event management policy to the DNN profile. A new CLI is introduced for this configuration.
2. Create QoS configuration for the default flow/bearer. This is an existing configuration. For more details, refer to Configuring QoS Parameters.
3. Add an event management configuration by defining the priority, the event to be executed, the rules, and the actions to be performed, if there is a rule match.
4. Add rule definition policies by specifying the conditions for rules.
5. Add action definition policies, the action will be to activate the rulebase to create GBR bearer/flow.
6. Configure rulebase, pre-defined rules, and charging-action. This is an existing configuration. For more details, refer to Configuring ACS Rulebase in ACS Configuration Mode.
7. Configure QoS for each of the dedicated bearer/flow QCI/ARP. This is an existing configuration. For more details, refer to Configuring Bandwidth ID.

Configuration for Associating QoS Profile and Event Management Policy to the DNN Profile

Associating the QoS profile and event management policy to the DNN profile can be done through following configuration:

```
config
  profile dnn dnn_profile_name
    qos-profile qos_profile_name
    eventmgmt-policy eventmgmt_policy_name
    exit
```

NOTES:

- **eventmgmt-policy** *eventmgmt_policy_name*—This CLI allows configuring priority-based event handling associated to a DNN. Each of the event policy configured under **eventmgmt-policy** are executed in the order of priority till a match is found based on event and rule.
- **qos-profile** *qos_profile_name*—This CLI allows associating the QoS profile and the event management policy to the DNN profile. This QoS profile will be used to read QoS values for 5G default flow, if the UDM does not provide it.

Configuration for Adding Event Management Policy

Adding an event management policy happens through the following configuration:

```
config
  policy eventmgmt policy_eventmgmt_name
    priority  event_priority [ event event_name ] ruledef ruledef_name actiondef
 actiondef_name
    exit
```

NOTES:

- **eventmgmt** *policy_eventmgmt_name*—This CLI allows configuring the event management policies and defining the attributes.
- **priority** *event_priority*—Allows defining the priority of a particular event management policy.
- **event** *event_name*—This is an optional CLI that defines an event for which a particular action is to be performed. It supports only **new-call** as the event name. For semantic and syntactic error handling scenarios, it supports **cbr-resp** as the event name.

  If the **event** is not configured, **actiondef** is executed for all the defined events if there is a rule match.
- **ruledef** *ruledef_name*—Defines a rule for a local policy that when matched an action is performed.
- **actiondef** *actiondef_name*—Configures the action name to be executed.

Configuration for Adding Rule Definition Policies

The following configuration allows adding rule definition policies:

```
config
  policy rulemgmt policy_rulemgmt_name
    ruledef rule_def condition condition_string
    exit
```

- **rulemgmt** *policy_rulemgmt_name*—Defines a rule to be added in the policies.
- **ruledef** *rule_def*—Configures a rule attribute. A ruledef is declared when the conditions match.

- **condition** *condition_string*—Defines the use cases for a rule. It only supports **any** and **cause matches "cause"** conditions.

Configuration for Adding Action Definition Policies

The following configuration adds action definition policies:

```
config
  policy actionmgmt policy_actionmgmt_name
    actiondef actiondef_name
      priority priority_number action action_name [ attributes { rulebase
rulebase_name [ rules rules_name ] } ]
      exit
```

NOTES:

- **actionmgmt** *policy_actionmgmt_name*—Configures the action to be executed.
- **actiondef** *actiondef_name*—Defines the action attributes to be executed. Currently, it supports only **activate-rulebase** as the action.

  In the semantic and syntactic error handling, the actions differ while the UE is in the 4G or 5G RAT.
- **priority** *priority_number*—Defines the priority in which the actions are to be executed.
- **action** *action_name*—Defines the actions associated with an actiondef in the order of priority. In case of GBR creation failure, SMF supports **release-session** action.
- **attributes** —Defines the attributes of a particular action. This is an optional command.
- **rulebase** *rulebase_name*—Defines a collection of protocol rules to match a flow and associated actions to be taken for matching the flow.
- **rules** *rules_name*—Defines a list of rules to be executed.

Note The existing configurations of charging action, bandwidth policy, and packet filter are used to configure QoS parameters of each rule.

Configuration Example

Following is the sample configuration for associating QoS profile and event management policy to the DNN profile:

```
config
profile dnn dnnprof-data
qos-profile qos camera_profile
eventmgmt-policy emp
end
```

Following sample configuration adds the event management policy:

```
policy eventmgmt emp
 priority 1 event new-call ruledef rd1 actiondef ad1
end
```

Following is the sample configuration for adding the **any** and **cause matches “cause”** rule definition policies:

```
policy rulemgmt rm1
  ruledef rd1
    condition “any”
    end
```

```
policy rulemgmt rm1
ruledef rd1
condition cause matches [ 83 ] source ue
```

Following is the sample configuration for adding action definition policies:

```
policy actionmgmt am1
  actiondef ad1
    priority 1 action activate-rulebase  attributes rulebase rb1 rules [r1,r2]
    exit
end
active-charging service olympics
rulebase rb1
bandwidth default-policy bw_policy1
action priority 1 dynamic-only ruledef r1 charging-action ca1
action priority 2 dynamic-only ruledef r2 charging-action ca2
exit

charging-action ca1
allocation-retention-priority 1
qos-class-identifier 6
tft packet-filter tft1
flow limit-for-bandwidth id 1
end

packet-filter tft1
direction bi-directional
ip protocol 6
ip remote-port range start 1002 end 1005
end

active-charging service acs1
bandwidth-policy bw_policy1
flow limit-for-bandwidth id 1 group-id 1
group-id 1 direction uplink peak-data-rate 1000000000 peak-burst-size 100 violate-action
discard committed-data-rate 1000 committed-burst-size 100 exceed-action discard
group-id 1 direction downlink peak-data-rate 2000000000 peak-burst-size 100 violate-action
 discard committed-data-rate 1000 committed-burst-size 100 exceed-action discard
```

For handling the case where dedicated bearer creation fails, it is recommended to have the following configuration:

```
policy eventmgmt emp
  priority 2 event cb-resp ruledef rd3 actiondef ad3
      exit

policy rulemgmt rm1
      ruledef rd3
               condition cause matches “cause”
            exit
     exit

policy actionmgmt am1
      actiondef ad3
priority 1 action release-session
            exit
exit
```

OAM Support

This section discusses the metrics and statistics supported in this feature.

Metrics

As part of this feature the following label is added in the **smf_service_stats**:

- **policy_status**: This metric is associated with the configured local policy.

SMF-triggered Metadata for EDR Generation on UPF

The SMF provides the following metadata to the User Plane Function (UPF) to enable EDR generation.

- Called-Station-ID: Specifies the DNN for the session
- Calling-Station-ID: Specifies the MSISDN of the UE
- RAT Type: RAT type for the current session (NR or EUTRAN)
- ULI: User location for the current session

The UPF receives preceding data in the "Subscriber Parameters" IE in the PFCP Session Establishment Request message. The RAT type and ULI can change during the lifetime of session (for events, such as 5G to 4G handover). The UPF receives the changed values of these parameters in the PFCP Session Modification Request message.

Note

- All the parameters are always sent from the SMF to the UPF irrespective of EDR configuration being available. These parameters ensure that any change in configuration after the session creation is immediately applied on the UPF.
- The SMF supports EDR related configurations. However, the SMF does not require these configurations for its functionality. These configurations are sent to the UPF.

For more information on the UPF EDRs, see the *UCC 5G UPF Configuration and Administration Guide*.

Dynamic Configuration Update

Feature Description

The SMF allows you to dynamically change the configuration of SMF profile and SMF service profile.

It is mandatory to perform following maintenance operational procedure for changes to certain SMF profile or service profile configuration parameters. This maintenance operational procedure operation helps to keep the SMF system in maintenance mode so that it doesn't impact the system by rejecting the new sessions. Also, this maintenance procedure provides flexibility to operators to clear the subscribers manually by executing **clear subscriber all** command.

The SMF updates configuration parameters change to NRF by sending "NFUPdate" using PUT Method.

How it Works

This section describes the maintenance operational procedure and how dynamic change in configuration works for the supported SMF configurations.

Maintenance Operational Procedure

For a change in the configuration parameters that require mandatory operational maintenance, perform the following steps:

1. Shutdown (offline) SMF by executing **mode offline** CLI command under SMF profile.

   The SMF sends NFUpdate with Method PUT and NFStatus as "UNDISCOVERABLE".

Note During the online to offline transition period, the SMF does not accept any new request.

2. Clean up the sessions using **clear subscriber sess all** CLI command.
3. Change the configurations and remove **mode offline** CLI command.

   SMF sends NFUpdate with Method PUT and NFStatus as "Registered".

SMF Profile and SMF Service Profile

The following table describes how dynamic change in configuration works for the supported SMF configurations.

Table 5: Dynamic Change in SMF Profile and SMF Service Profile

Configuration parameters	Dynamic Change	Impact on Existing Sessions	NRF Update	Maintenance Operational Procedure
locality	Allowed	Sessions will start using the newer values.	Not Required	Required
node-id	Not applicable	No impact	Not applicable	Not applicable
fqdn	Allowed	SMF always fetches the latest FQDN value for sessions while interacting with UDM.	Required	Required
allowed-nssai	Allowed	Sessions will start using the newer values.	Required	Required
plmn-id	Allowed	Sessions will start using the newer values.	Required	Required

Configuration parameters	Dynamic Change	Impact on Existing Sessions	NRF Update	Maintenance Operational Procedure
service name, schema, service-id, version	Allowed	Sessions will start using the newer values.	Required	Required
http-endpoint	Allowed	Sessions will start using the newer values.	Required	Required
icmpv6-profile	Allowed	Sessions will start using the newer values.	Not required	Not required
compliance-profile	Allowed	SMF might perform parse-failure because of incompatibility issues between SMF and other NFs for various SBI interfaces.	Not required	Not required
access-profile	Allowed	Sessions will start using the newer values.	Not required	Not required
subscriber-policy	Allowed	Sessions will start using the newer values.	Not required	Not required

Configuring Dynamic Configuration Change Support

To enable the offline mode of operation under SMF profile, use the following sample configuration.

```
config
  profile smf profile_name
    mode offline
    exit
```

NOTES:

- **mode**: Specify the mode of operation.

- **offline**: Specify the mode is offline and new sessions are rejected.

Verifying Dynamic Configuration Change Support Configuration

Use the **show running-config profile smf** CLI command to verify if the feature is enabled. When enabled, the following field will be displayed as part of the show command output:

- mode offline

Dynamic PCC Rules Enforcement

Feature Description

SMF uses either the Policy and Charging Control (PCC) rules from Policy Control Function (PCF) or the locally configured policy rules to control the policy management. The PCF sends the PCC rules along with the applicable QoS and charging information to the SMF. The SMF uses this information to define the QoS flows and apply the QoS enforcement (via UPF) and charging towards CHF.

The PCC rules can be configured locally as well. The locally configured policy rules are labelled as static or predefined rules.

The following sections provide information on the features that are implemented for the dynamic policy management.

Supported Features Negotiation

The SMF and the PCF negotiate the supported features during Policy Context Creation and during PDU session establishment. Based on the negotiated features, the PCF provides the relevant information.

The following table lists the features that can be negotiated as defined in the 3GPP specification 29.512.

Table 6: Supported Negotiated Features

Feature Number	Feature Name	Description
1	TSC	This feature indicates support for traffic steering control in the (S)Gi-LAN or routing of the user traffic to a local Data Network identified by the DNAI per Application Function (AF) request. If the SMF supports this feature, the PCF performs the functions as described in 3GPP specification 29.512, subclause 4.2.6.2.20.
2	ResShare	This feature indicates the support of service data flows that share resources. If the SMF supports this feature, the PCF performs the functions as described in 3GPP specification 29.512, subclause 4.2.7.4.
4	ADC	This feature indicates the support of application detection and control.
6	NetLoc	This feature indicates the support of the Access Network Information Reporting for 5GS.
7	RAN-NAS-Cause	This feature indicates the support for the detailed release cause code information from the access network.
8	EPSFallbackReport	Indicates EPS Fallback has occurred and resource corresponding to rules in rule report were setup successfully post EPS Fallback. SMF performs the function as described in 3GPP Specification Release 16.10.0, 23.502/29.512.

The SMF sends supportedFeatures attribute in the Npcf_SMPolicyControl_Create message, and further includes a bitmap representing the supported features. The PCF also sends the supportedFeatures attribute in the response message. The response should either match or be a subset of the request.

The string contains a bitmask indicating supported features in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents the support of the features as described in the preceding table. The most significant character representing the highest-numbered features appears first in the string, and the character representing features 1–4 appears last in the string. The list of features and their numbering (starting with 1) are defined separately for each API.

Provisioning and Management of Session AMBR and Default QoS

For the N4 interface, the SMF sends the QoS information in the form of:

- Packet Detection Rule (PDR)
- Forwarding Action Rule (FAR)
- QoS Enforcement Rule (QER)

The SessionAMBR includes the maximum aggregated uplink and downlink bit rates to be shared across all non-GBR QoS flows in each PDU session. The SMF sends the session level QER for non-GBR flows along with existing QER to the UPF.

The SMF receives sessionRule from PCF in SmPolicyDecision during PDU session creation. The sessionRule consists of authSessAmbr and authDefQos. The authorized AMBR consists of the Uplink (UL) and Downlink (DL) MBR at a session level and authDefQos contains the 5Qi, ARP, and other QoS binding parameters for the default QoS flow.

The SMF performs the following actions:

- Any PCC rules received from the PCF that have an associated QoS Desc with the same binding parameters as received in authDefQos are tagged with the default QoS flow.
- On the N4 interface, the UL and DL Packet Detection Rules (PDRs) are created for each PCC rule that is associated with the default QoS flow. For session AMBR enforcement, the SMF creates a QoS Enforcement Rule (QER) with appropriate AMBR and associates it with all PDRs for non-GBR rules.
- On the N1 interface, the "QoS Flow Description" attribute in the PDU SESSION ESTABLISHMENT ACCEPT message contains the QFI and MFBR and 5Qi values. The Session AMBR is also sent in this message.
- On the N2 interface, the PDU Session Resource Setup Transfer Request IE contains the AMBR and the "QoS flow level QoS parameters" (5Qi, ARP, and so on) and QFI.
- The SMF supports the UDM-initiated Session AMBR modification. In this case:
  - The SMF sends Npcf_SMPolicyControl_Update to the PCF along with the new subscribed session AMBR within the "subsSessAmbr" attribute and the SE_AMBR_CH policy control request trigger within the "repPolicyCtrlReqTriggers". On receiving the change of session AMBR, the PCF provisions the new authorized session AMBR to the SMF in the response.
  - Update the QERs on N4 interface for Session AMBR enforcement.
  - Initiate N1N2MessageTransfer towards the AMF with Sess AMBR in PDU SESSION MODIFICATION COMMAND message in N1 interface and PDU Session Resource Modify Request transfer IE in N2 container having the new AMBR.

Provisioning of Policy Revalidation Time

Feature Description

The PCF instructs the SMF to trigger PCF interaction to request PCC rule from the PCF if not provided yet. The PCF performs this operation by providing revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute in SmPolicyDecision. The PCF can change the revalidation time by including a new value for the "revalidationTime" attribute. The PCF can also disable the revalidation function by removing RE_TIMEOUT policy control request trigger if it has been provided.

If the SMF receives the existing revalidation time or the new revalidation time, the SMF stores the received value and starts the timer based on it. Then, the SMF sends the PCC rule request before the indicated revalidation time. If the RE_TIMEOUT policy control request trigger is removed, the SMF stops the timer for revalidation.

Note When the RE_TIMEOUT is removed, the revalidation time value previously provided to the SMF is no longer applicable.

How it Works

Revalidation time is a string of the format "date-time" as defined in OpenAPI specification. The SMF, on receiving the revalidation time in "revalidationTime" attribute and RE_TIMEOUT trigger in "policyCtrlReqTriggers" attribute, starts a timer for the difference duration (revalidationTime – currentTime – 5 seconds buffer). Once the timer expires, the SMF initiates the PCF interaction to request PCC rules.

Standard Compliance

The Policy Revalidation Time feature complies with *3GPP TS 29.512, v15.2.0*.

Provisioning and Management of Additional QoS Flows

The PCF can create, modify, or delete multiple GBR and non-GBR PCC rules.

The following scenarios are possible:

1. Multiple non-GBR and GBR PCC rules are activated during PDU session establishment. In this case:

   a. The SMF creates the QoS flow according to the QoS flow binding principle as described in the QoS Management section.

   b. On the N4 interface, the UL and DL PDRs are created for each PCC rule that is associated with all the flows. For flow-level QoS enforcement, the SMF creates QERs with the MFBR and GFBR (for GBR flows) values and associates it with each PDR of a flow.

   c. On the N1 interface, the "QoS Flow Description" attribute in the PDU SESSION ESTABLISHMENT ACCEPT message contains the QFI and MFBR, GFBR, and 5Qi values. The packet filters associated with each QoS rule are sent on the N1 interface in the "Authorized QoS Rules" attribute.

   d. Different types of packet filters are supported on both the N4 and the N1 interfaces. This list includes:

```
Packet filter component type identifier
Bits
8 7 6 5 4 3 2 1
```

```
0 0 0 0 0 0 0 1 Match-all type
0 0 0 1 0 0 0 0 IPv4 remote address type
0 0 0 1 0 0 0 1 IPv4 local address type
0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type
0 0 1 0 0 0 1 1 IPv6 local address/prefix length type
0 0 1 1 0 0 0 0 Protocol identifier/Next header type
0 1 0 0 0 0 0 0 Single local port type
0 1 0 0 0 0 0 1 Local port range type
0 1 0 1 0 0 0 0 Single remote port type
0 1 0 1 0 0 0 1 Remote port range type
```

e. On the N2 interface, the PDU Session Resource Setup Transfer Request IE contains the "QoS flow level QoS parameters" (5Qi, ARP, and so on) and QFIs for each of the flows. The "GBR QoS Flow Information" field of the IE contains the MFBR and GFBR of the GBR flows.

2. Modification of PCC rules after PDU session establishment. In this case, the following scenarios are observed:

a. Modification, addition, and removal of packet filters of one or more PCC rules:

1. In this case, the SDF filters of the PDR on the N4 interface are changed by invoking N4 session modification.

2. The SMF initiates N1N2MessageTransfer towards the AMF with "Authorized QoS Rules" attribute in PDU SESSION MODIFICATION COMMAND message in N1 interface. The rule operation code in this attribute is one of the following:

```
0 1 1 Modify existing QoS rule and add packet filters
1 0 0 Modify existing QoS rule and replace all packet filters
1 0 1 Modify existing QoS rule and delete packet filter
```

b. Change in QoS associated with one or more PCC rules:

1. The SMF performs QoS flow binding evaluation which in turn results in the following operations:

1. Addition of a new QoS flow results in change of QFI on the N4 interface for some of the PDRs.

2. Movement of a PCC rule from one QoS flow to another QoS flow. In this case, the PDR/QER of impacted PCC rules are modified to update the QFI.

3. Removal of a QoS flow when the last PCC rule in that flow is moved to a different QoS flow. In this case, the PDR/QER of impacted PCC rules are modified to update the QFI.

2. In the preceding cases, on the N1 interface the Authorized QoS Rules and Authorized QoS Descriptors are sent with the operation code as one of the following:

```
0 0 1 Create new QoS flow description
0 1 0 Delete existing QoS flow description
0 1 1 Modify existing QoS flow description
```

3. On the N2 interface, QoS Flow Level QoS parameters of the PDU Session Resource Modify Request transfer IE carry the modified GFBR, MFBR, 5Qi and so on. For any flow removal, the QoS Flow to re-lease List is included in this IE.

c. PCC rule removal:

1. In this case, the SMF removes all the PDRs associated with a QoS flow on the N4 interface.

2. On the N1 interface, the Authorized QoS Rules and Authorized QoS Descriptors are sent with the operation code as one of the following:

```
0 1 0 Delete existing QoS flow description
```

3. On the N2 interface, the PDU Session Resource Modify Request transfer IE carries the QoS Flow to release List.

QoS enforcement

The SMF enforces QoS at PCC rule (SDF) level, QoS flow level, and session level by creating one QER:

- per PCC rule level to enforce MBR/GBR as per the associated QoS Desc supplied by PCF and associated to the given PCC rule.
- at QoS flow level which has aggregated MBR/GBR of all the PCC rules associated with a QFI.
- at session level to enforce the Session AMBR for all non-GBR QoS flows.

Once these QERs are created, the SMF associates:

- the session level QER to all PDRs belonging to the non-GBR QoS category.
- the SDF level QER to each individual PCC rule.

For any QoS modification including movement of the PCC rules from one flow to another and QoS modification within flow, the SMF modifies the GFBR/MFBR (or Session AMBR) and updates the QERs accordingly on the N4 interface.

Default Qos flow indication

Table 7: Feature history

Feature name	Release information	Description
Default QoS flow indication support	2026.01.0	This feature binds a dynamic PCC rule to the default bearer, when the SMF receives **defQosFlowIndication IE** as **true**.

SMF binds the dynamic PCC rule to the deafult bearer, whenever the SMF receives the **defQosFlowIndication IE** set as **true** from the PCF.

When defQosFlowIndication IE is set, the rule does not fail even if the SMF does not receove the 5Qi and other QoS values.

Policy Control Request Triggers

The PCF provides one or more policy control request trigger(s) by including the triggers in the "policyCtrlReqTriggers" attribute(s) in the SmPolicyDecision data structure.

During the lifetime of the PDU session, the PCF updates or removes the policy control request triggers. To update the trigger, the PCF provides a new complete list of applicable policy control request triggers by including the trigger(s) in the "policyCtrlReqTriggers" attribute.

The PCF removes all previously provided triggers by providing a "policyCtrlReqTriggers" attribute set to NULL value. Upon reception of a policy control request trigger with this value, the SMF does not inform PCF of any trigger except for those triggers that are always reported and does not require provisioning from the PCF.

Whenever the PCF provisions the trigger, unless otherwise specified in the trigger's value definition, the SMF sends the corresponding currently applicable values (for example, access type, RAT type, user location information, and so on) to the PCF within the UeCampingRep data structure in the response of the HTTP POST message. In this case, the "repPolicyCtrlReqTriggers" attribute is not included.

The list of supported triggers is as follows:

Trigger	Description
RES_MO_RE	A request for resource modification has been received by the SMF. This is a mandatory trigger. **Note** This request is sent from SMF to PCF when UE/AMF requested QoS modification is triggered.
UE_IP_CH	UE IP address change. This is a mandatory trigger.
DEF_QOS_CH	Default QoS Change. This is a mandatory trigger.
SE_AMBR_CH	Session AMBR Change. This is a mandatory trigger.
SAREA_CH	Location Change about the Serving Area in N11 update.
SCNN_CH	Location Change about the Serving CN node. See the following section for details on how the SMF supports this trigger during the different handover scenarios.
RE_TIMEOUT	Indicates that the SMF has generated the request because there has been a PCC revalidation timeout (that is, Enforced PCC rule request as defined in Table 6.1.3.5.-1 of *3GPP TS 29.503*).
EPS_FALLBACK	Indicates that SMF supports EPS Fallback Report functionality for pccRules for which the EPS_FALLBACK trigger was sent by PCF.

Support SCNN_CH Trigger in Handovers

The SMF supports the serving network change trigger in the following handovers:

- **Inter AMF Handover**: If the "SCNN_CH" is provisioned, when the SMF detects a change of serving Network Function (for example, the AMF), the SMF includes the "SCNN_CH" within the "repPolicyCtrlReqTriggers" attribute and the current serving Network Function in the "servNfId" attribute. When the serving Network Function is an AMF, the SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **5G to 4G handover**: When the UE handed over from the 5GS to EPC/E-UTRAN, the SMF includes, if the "SCNN_CH" policy control request trigger is provisioned and met, the "servNfId" attribute including the S-GW identification within the "anGwAddr" attribute.
- **4G to 5G handover**: The SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.

- **WiFi to 5G handover**: The SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **5G to WiFi handover**: When the UE handed over from the 5GS to EPC non-3GPP access, the SMF includes, if the "SCNN_CH" policy control request trigger is provisioned and met, the ePDG identification within the "anGwAddr" attribute included in the "servNfId" attribute.

Gating Control

Feature Description

Gating control is the capability to block or allow IP packets belonging to a certain IP flow, based on the decisions by the PCF. The PCF could, for example, make gating decisions based on session events (start and stop of service) reported by the AF.

The AF instructs the PCF to temporarily block the user traffic corresponding to a specific PCC rule on uplink or downlink direction, or both the directions.

To enable the PCF gating control decisions, the AF reports session events (for example, session termination, modification) to the PCF. For example, session termination, in gating control, triggers the blocking of packets or "closing the gate".

Note Gating Control applies only for service data flows of IP type.

How it Works

The Gating Control feature works in the following manner:

1. PCF sends flowStatus attribute in TrafficControlData referenced by the PCC rule. The value of this attribute is set to "enabled", "disabled", "enable_uplink", or "enable_downlink" based on the PCF decision.
2. On receiving this attribute, the SMF instructs the UPF to open or close the GATE for the UL or DL Packet Detection Rule (PDR), or both UL and DL PDRs for the associated PCC rule. The Gate Status Information Element (IE) in Create QoS Enhancement Rule (QER) or Update QER associated with the PDR is set to OPEN or CLOSED.
3. If there is any subsequent change, the PCF triggers a N4 modification request to change the GATE status.

Standards Compliance

The Gating Control feature complies with the following standards:

- *3GPP TS 29.512, version 15.2.0*

How it Works

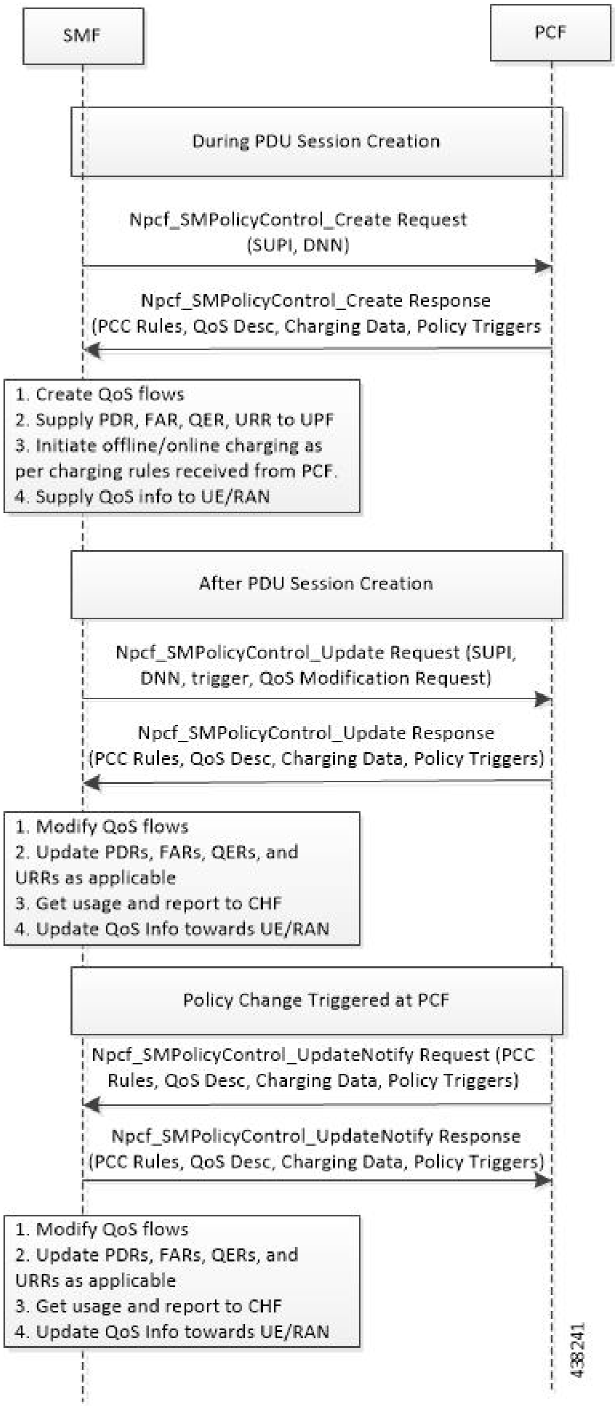
The SMF requests the policy information from PCF. The PCF in turn provides the policy rules during and after PDU session creation to enable the dynamic policy application. Dynamic policy management involves the following operations:

- Policy Context Creation: This operation is performed at the time of PDU session create and the PCF sends the PCC rules and the associated QoS, Charging and other policy data in the response message.

- Policy Context Update: For any RAN-initiated or UE-initiated policy updates and for notification of trigger events, the SMF initiates a policy context update. In response, the PCF sends the changed policy data that impacts the QoS and charging.
- Policy Context Update Notification: During the lifecycle of a PDU session, the PCF can initiate a policy update based on interaction with the AF or local configuration changes at PCF. The SMF handles the updated policy rules when received in a notification from the PCF.
- Policy Context Delete: At the end of a PDU session, the SMF terminates the Policy Context with PCF.

The following figure illustrates the dynamic policy management procedure for a PDU session.

Figure 8: Dynamic Policy Management Call Flow


SMF
PCF
During PDU Session Creation
Npcf_SMPolicyControl_Create Request (SUPI, DNN)
Npcf_SMPolicyControl_Create Response (PCC Rules, QoS Desc, Charging Data, Policy Triggers
1. Create QoS flows
2. Supply PDR, FAR, QER, URR to UPF
3. Initiate offline/online charging as per charging rules received from PCF.
4. Supply QoS info to UE/RAN
After PDU Session Creation
Npcf_SMPolicyControl_Update Request (SUPI, DNN, trigger, QoS Modification Request)
Npcf_SMPolicyControl_Update Response (PCC Rules, QoS Desc, Charging Data, Policy Triggers)
1. Modify QoS flows
2. Update PDRs, FARs, QERs, and URRs as applicable
3. Get usage and report to CHF
4. Update QoS Info towards UE/RAN
Policy Change Triggered at PCF
Npcf_SMPolicyControl_UpdateNotify Request (PCC Rules, QoS Desc, Charging Data, Policy Triggers)
Npcf_SMPolicyControl_UpdateNotify Response (PCC Rules, QoS Desc, Charging Data, Policy Triggers)
1. Modify QoS flows
2. Update PDRs, FARs, QERs, and URRs as applicable
3. Get usage and report to CHF
4. Update QoS Info towards UE/RAN
438241

Standards Compliance

The Dynamic PCC Rules Enforcement feature complies with the following standard:

- *3GPP TS 29.512 Version 15.4.0 – 5G; 5G System; Session Management Policy Control Service; Stage 3*

Limitations

The Dynamic PCC Rules Enforcement feature has the following limitations:

- SMF supports only the following combination of operations:
  - Creation of new PCC Rule with new QoS descriptor to create new QoS Flow
  - Addition of new PCC Rule to an existing QoS Flow
  - Removal of PCC rule
  - Updating of GBR/MBR parameters associated with the rule
  - Session AMBR Changes

Configuring the Dynamic PCC Rules Enforcement Feature

This section describes how to configure the Dynamic PCC Rules Enforcement feature.

Configuring the Dynamic PCC Rules Enforcement feature involves the following steps:

1. Creating QoS Profile, on page 39
2. Configuring QoS Parameters, on page 39
3. Defining QoS Profile in DNN Profile Configuration, on page 40

Creating QoS Profile

To create an instance of a quality of service (QoS) profile, use the following sample configuration.

```
config
  profile qos qos_profile_name
  exit
```

NOTES:

- **qos** *qos_profile_name*: Create a quality of service profile and provide access to the QoS Profile Configuration mode to configure the QoS parameters. *qos_profile_name* must be an alphanumeric string uniquely identifying the QoS profile.

Configuring QoS Parameters

To configure the QoS parameters, use the following sample configuration.

```
config
  profile qos qos_profile_name
    ambr { ul uplink_ambr | dl downlink_ambr }
    arp { preempt-cap preemption_capability |
    preempt-vuln preemption_vulnerability |
    priority-level priority_level }
    max data-burst burst_volume
    priority qos_priority
    qi5 5qi_value
    exit
```

NOTES:

- **ambr { ul** *uplink_ambr* **| dl** *downlink_ambr* **}**: Define the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber to network) and the downlink (network to subscriber) traffic.
- **arp preempt-cap** *preemption_capability*: Specify the preemption capability flag. The options are:
    - MAY_PREEMPT—Bearer may be preempted
    - NOT_PREEMPT—Bearer cannot be preempted
- **arp preempt-vuln** *preemption_vulnerability*: Specify the preemption vulnerability flag. The options are:
    - PREEMPTABLE—Bearer may be preempted
    - NOT_PREEMPTABLE—Bearer cannot be preempted
- **arp priority-level** *priority_level*: Define the Allocation and Retention Priority (ARP) for the service data. The default value of *priority_level* is 8.
- **max data-burst** *burst_volume*: Define the maximum data burst volume. *burst_volume* must be an integer in the range of 1–4095.
- **priority** *qos_priority*: Specify the 5QI priority level. *qos_priority* must be an integer in the range of 1–127.
- **qi5** *5qi_value*: Specify the 5G QoS Identifier (5QI) for the authorized QoS parameters. *5qi_value* must be an integer in the range of 0–255.

Defining QoS Profile in DNN Profile Configuration

To configure the QoS profile in the existing DNN profile, use the following sample configuration.

```
config
  profile dnn dnn_profile_name
    qos-profile qos_profile_name
    exit
```

NOTES:

- **qos-profile** *qos_profile_name*: Define the locally configured default QoS profile. This profile is configured under the existing DNN Profile configuration. *qos_profile_name* must be the name of the configured QoS profile.

Verifying the Dynamic PCC Rules Enforcement Feature Configuration

This section describes how to verify the Dynamic PCC Rules Enforcement feature configuration.

Use the following show command to verify the feature configuration details.

show full-configuration

The following is an example of this show command output.

```
show full-configuration
profile dnn dnn1
qos-profile qos1
!
profile qos qos1
ambr ul 1024
ambr dl 1024
qi5 128
arp priority-level 8
arp preempt-cap NOT_PREEMPT
arp preempt-vuln NOT_PREEMPTABLE
priority 9
max data-burst 2048
exit
```

Controlling PCF and SMF Interaction

PCF and SMF interaction for subscriber calls is enabled by default. To disable the PCF interaction with SMF, use the following sample configuration:

```
config
   profile dnn dnn_profile_name
      pcf-interaction { false | true }
      end
```

NOTES:

- **profile dnn** *dnn_profile_name*: Specify the DNN profile name. *dnn_profile_name* must be an alphanumeric string.
- **pcf-interaction { false | true }**: Disable or enable the interaction with PCF.
  - **false**: SMF does not interact with PCF.
  - **true**: SMF interacts with PCF wherever applicable as part of all call flows. This is the default configuration.

Note The **pcf-interaction { false | true }** CLI command will be deprecated in the future releases.

Configuration Example

The following is an example configuration.

```
config
profile dnn intershat1
pcf-interaction false
end
```

Configuration Verification

Check the **pcf-interaction** configuration to determine if PCF interaction with SMF is enabled or disabled. To verify the configuration, use the following command at the Exec mode:

```
show running-config profile dnn intershat1
```

You can also verify the feature configuration using the following show command at the Global Configuration mode.

```
show full-configuration profile dnn intershat1
```

The following is an example output of the **show running-config profile dnn intershat1** command.

```
[smf] smf# show running-config profile dnn intershat1
profile dnn intershat1
 dns primary ipv4 209.165.200.239
 dns primary ipv6 fd01:976a::9
 dns secondary ipv6 fd01:976a:c002:1:fd95:6218:825e:f867
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:48
 pcscf-profile    PCSCF_Prof_2
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat1
 pcf-interaction  false
exit
```

The following is an example output of the **show full-configuration profile dnn intershat1** command.

```
[smf] smf(config)# show full-configuration profile dnn intershat1
profile dnn intershat1
 dns primary ipv4 209.165.200.239
 dns primary ipv6 fd01:976a::9
 dns secondary ipv6 fd01:976a:c002:1:fd95:6218:825e:f867
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:48
 pcscf-profile    PCSCF_Prof_2
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat1
 pcf-interaction  false
exit
```

In the preceding examples, **pcf-interaction false** is displayed, indicating that SMF does not interact with PCF.

Handling Traffic Flow for Dedicated UE Services

Table 8: Feature History

Feature Name	Release Information	Description
Handling Traffic Flow for Dedicated UE Services	2024.01.2	This feature allows specific UEs, like PTTs, to connect on the 5G RAT using specific TFTs. To enable this functionality, PCF sets the value of the **PacketFilterUsage** IE attribute to **true** in the dynamic PCC rule. This rule causes the SMF to only send the PCC Rule TFTs instead of the IP "Any-Any". This feature is only applicable for default flow. **Default Setting:** Enabled - Always-on

Feature Description

When a specific UE with a limited-service accessibility (such as a PTT device) attaches to the 5G RAT, the PCF sends dynamic PCC rules associated with a default flow to the SMF. If PCF sends a **PacketFilterUsage** IE with value set to **true** in the dynamic PCC rule and if the PCC rule is associated to the default flow, SMF adds the QoS rule with the flow information and sends the TFT (Traffic Flow Template) to the UE.

If the **packetFilterUsage** IE is set to false, SMF adds the QoS rule with "**Any-Any**" filter and sends it to the UE. The packet filter "**Any-Any**" is a default filter that allows the UEs to communicate with any IP and avail any service. The purpose of this feature is to enable the prioritization of packets to support dedicated UE services such as PTT service.

This feature is supported only for dynamic rules and not for static or predefined rules. This feature is also not applicable for dedicated bearer.

Note As there is no impact on the N4 interface, all the rules and filters are sent to UPF as received from the PCF.

How It Works

Sending the TFT parameters associated to the default flow toward the UE happens through the following steps:

1. **PCC Rule Identification**: The following two conditions are used for identifying the PCC rule associated with the default flow:

    - If a PCC rule is associated to the QoS Data with the same binding parameters (5QI, arp) as the authDefQos (authDefQos contains the 5QI, ARP, and other QoS binding parameters for the default QoS flow) parameter.

    Note For the PCC rules associated with default flow, only the **authDefQos** parameter is considered and all other QoS parameters are ignored.

    - If a PCC rule received from the PCF has **defQosFlowIndication** IE set to **true**.

2. **TFT Update**: SMF sends the corresponding TFT parameters to the UE based on the following conditions:

Conditions	Expected Behavior	Comments
PCC rules with **packetFilterUsage IE** set to **true**.	TFT associated to that PCC rule is sent to UE over the N1 interface.	
PCC rules with **packetFilterUsage IE** set to **false**.	"**Any-Any**" TFT is sent to the UE.	
Existing TFT with "**Any-Any**" filter + new rules with **packetFilterUsage** IE set to **true**.	SMF updates TFT with the new packet filter received from PCF.	Old QoS rule is deleted and new QoS rule is created toward UE.
Last rule with TFT **packetFilterUsage** = **true** is deleted.	SMF pushes updates TFT by deleting the current rule and adding a new rule with "**Any-Any**" filter.	
Multiple PCC rules for default flow with **packetFilterUsage**=**true**.	SMF randomly selects only one of the rules with **packetFilterUsage** IE as **true**.	SMF rejects all other rules with **packetFilterUsage** IE as **true**.
SMF is already having a PCC rule with **packetFilterUsage**=**true** and PCF sends a new rule with **packetFilterUsage**=**true**.	SMF rejects the new rule.	

Note

- SMF sends only one QoS rule for default flow with DQR (Default QoS Rule)=1 and packet filter as "**Any-Any**" or specific TFT over the N1 interface. The SMF does not send or add up the bit rates in QoS description of the PCC Rules in FBR IE. The MBR in UE should be derived from session AMBR.
- SMF does not send a CREATE_QER for the PCC rules QoS description over the N4 interface. The QER IDs in the PDRs for the PCC rules are set to the Session Rules QER IDs. SMF includes an additional QER in the PDR of the PCC rule, which contains only the gate status as enabled or disabled. The QER does not contain any MBR information.

Standards Compliance

This feature complies with the *3GPP TS 29.512 version 15.6.0; Session Management Policy Control Service; Stage 3* standard.

N7 Optimization

Table 9: Feature History

Feature Name	Release Information	Description
Minimizing SMF and PCF interactions on the N7 interface	2023.04	For the N7 optimization support, the SMF skips the N7 Update message by sending the UE IP address in the N7 Create message.

Feature Description

For the N7 optimization support, the SMF skips the N7 Update message by sending the UE IP address in the N7 Create message. After you enable this feature through the CLI command, the SMF allocates the IP address and performs the UPF selection before starting interaction with the PCF. If you have configured the SMF to select an alternate UPF that needs IP reallocation, then during the N4 failure, the SMF sends an N7 Update message after the N4 Success message to indicate the new IP address.

How it Works

Call Flows

This section describes the call flows that are associated with this feature.

- 5G Session Creation with N7 Optimization Call Flow, on page 45
- 5G Session Creation During N4 Session Establishment Failure with N7 Optimization Call Flow, on page 47

5G Session Creation with N7 Optimization Call Flow

The following call flow depicts the 5G session creation call flow with the N7 optimization enabled.

Figure 9: 5G Session Creation with N7 Optimization Call Flow

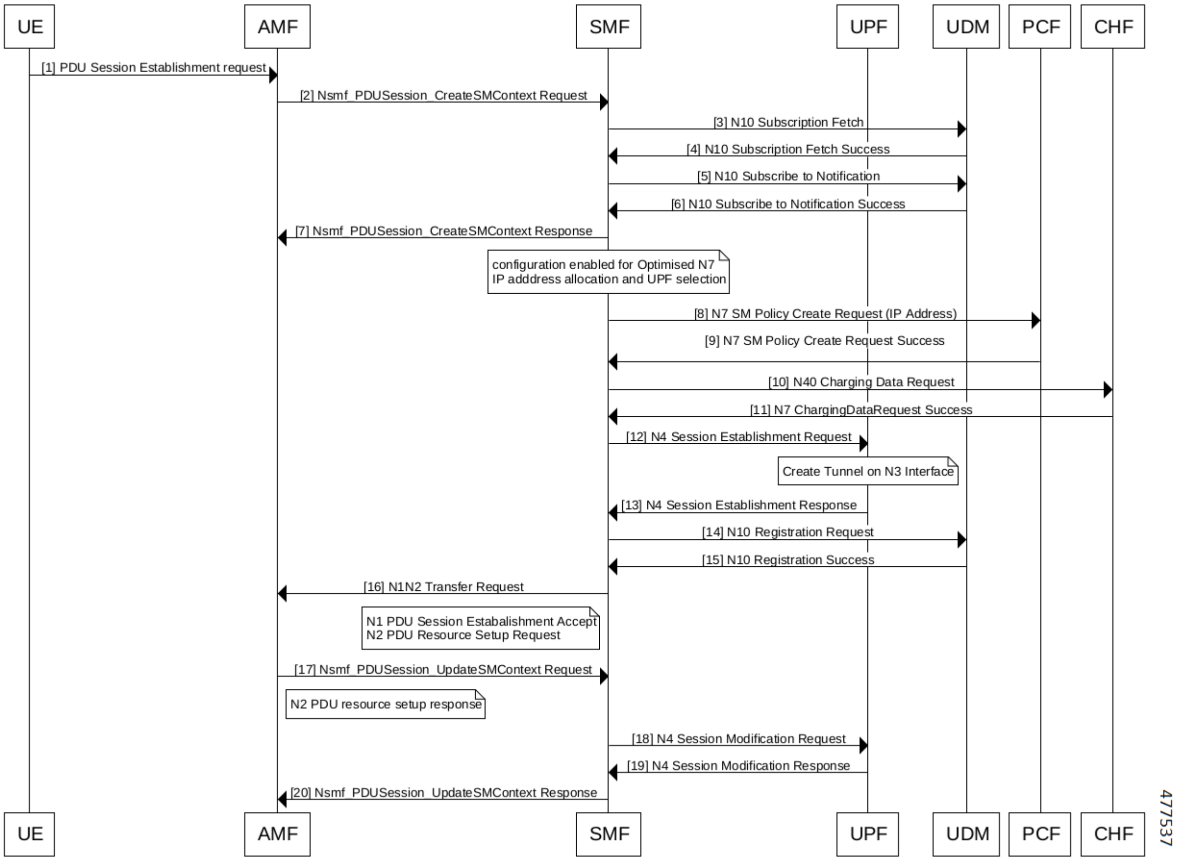

UE
AMF
SMF
UPF
UDM
PCF
CHF
[1] PDU Session Establishment request
[2] Nsmf_PDUSession_CreateSMContext Request
[3] N10 Subscription Fetch
[4] N10 Subscription Fetch Success
[5] N10 Subscribe to Notification
[6] N10 Subscribe to Notification Success
[7] Nsmf_PDUSession_CreateSMContext Response
configuration enabled for Optimised N7
IP adddress allocation and UPF selection
[8] N7 SM Policy Create Request (IP Address)
[9] N7 SM Policy Create Request Success
[10] N40 Charging Data Request
[11] N7 ChargingDataRequest Success
[12] N4 Session Establishment Request
Create Tunnel on N3 Interface
[13] N4 Session Establishment Response
[14] N10 Registration Request
[15] N10 Registration Success
[16] N1N2 Transfer Request
N1 PDU Session Estabalishment Accept
N2 PDU Resource Setup Request
[17] Nsmf_PDUSession_UpdateSMContext Request
N2 PDU resource setup response
[18] N4 Session Modification Request
[19] N4 Session Modification Response
[20] Nsmf_PDUSession_UpdateSMContext Response
UE
AMF
SMF
UPF
UDM
PCF
CHF
477537

Table 10: Call Flow Description for 5G Session Creation with N7 Optimization

Step	Description
1	UE sends the PDU Session Establishment Request message to AMF.
2	AMF sends the Nsmf_PDUSession_CreateSMContext Request message to SMF.
3	SMF sends the N10 Subscription Fetch request to UDM.
4	UDM sends the N10 Subscription Fetch Success response to SMF.
5	SMF sends the N10 Subscribe to Notification message to UDM.
6	UDM sends the N10 Subscribe to Notification Success response to SMF.
7	SMF sends the Nsmf_PDUSession_CreateSMContext Response to AMF.
8	On SMF, the configuration is enabled for the optimised N7 IP adddress allocation and UPF selection. SMF sends the N7 SM Policy Create Request message along with the IP Address to PCF.
9	PCF sends the N7 SM Policy Create Request Success response to SMF.

Step	Description
10	SMF sends the N40 Charging Data Request message to CHF.
11	CHF sends the N7 Charging Data Request Success response to SMF.
12	SMF sends the N4 Session Establishment Request to UPF.
13	A tunnel is created on the N3 interface. Then, UPF sends the N4 Session Establishment Response to SMF.
14	SMF sends the N10 Registration Request message to UDM.
15	UDM sends the N10 Registration Success response to SMF.
16	SMF sends the N1N2 Transfer Request message to AMF.
17	The N1 PDU Session Establishment request is accepted and the N2 PDU Resource Setup Request is sent. AMF sends the Nsmf_PDUSession_UpdateSMContext Request message to SMF.
18	AMF sends the N2 PDU resource setup response. SMF sends the N4 Session Modification Request message to UPF.
19	UPF sends the N4 Session Modification Response to SMF.
20	SMF sends the Nsmf_PDUSession_UpdateSMContext Response to AMF.

5G Session Creation During N4 Session Establishment Failure with N7 Optimization Call Flow

The following call flow depicts the 5G session creation call flow during the message failure with the N7 optimization enabled.

Figure 10: 5G Session Creation During N4 Session Establishment Failure with N7 Optimization Call Flow

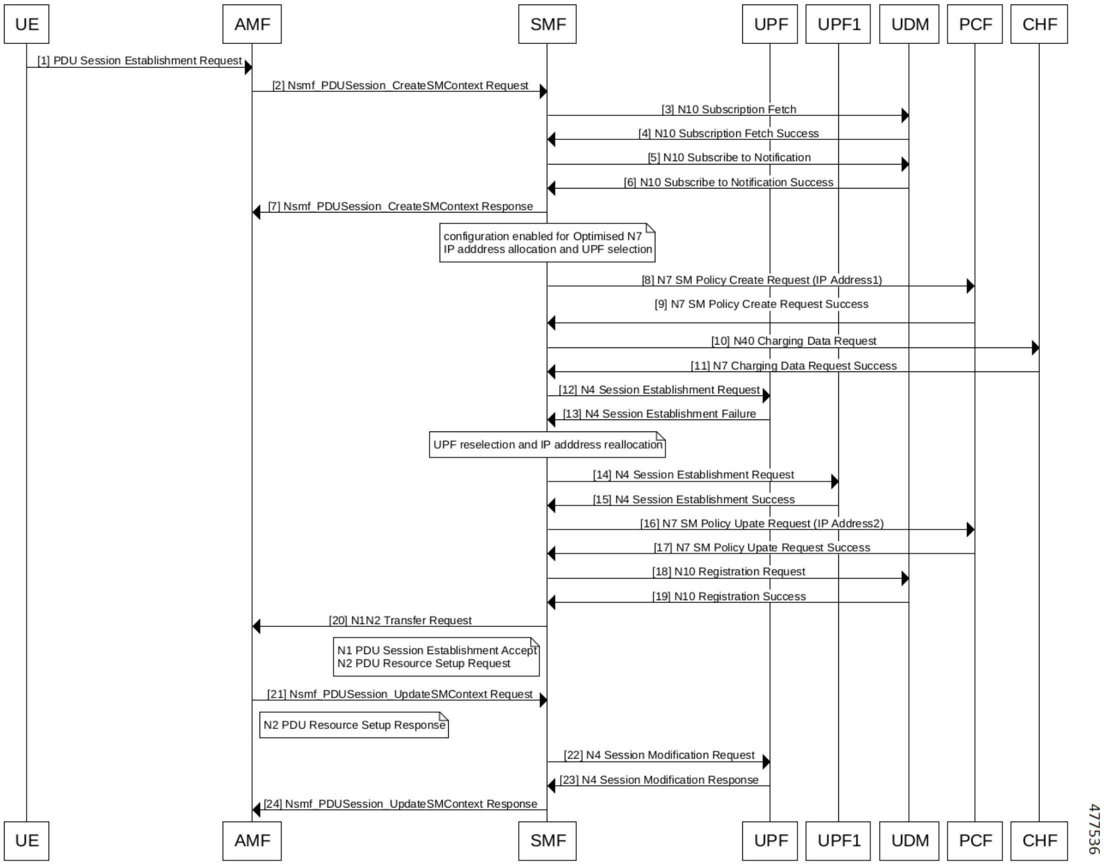

UE
AMF
SMF
UPF
UPF1
UDM
PCF
CHF
[1] PDU Session Establishment Request
[2] Nsmf_PDUSession_CreateSMContext Request
[3] N10 Subscription Fetch
[4] N10 Subscription Fetch Success
[5] N10 Subscribe to Notification
[6] N10 Subscribe to Notification Success
[7] Nsmf_PDUSession_CreateSMContext Response
configuration enabled for Optimised N7 IP adddress allocation and UPF selection
[8] N7 SM Policy Create Request (IP Address1)
[9] N7 SM Policy Create Request Success
[10] N40 Charging Data Request
[11] N7 Charging Data Request Success
[12] N4 Session Establishment Request
[13] N4 Session Establishment Failure
UPF reselection and IP adddress reallocation
[14] N4 Session Establishment Request
[15] N4 Session Establishment Success
[16] N7 SM Policy Upate Request (IP Address2)
[17] N7 SM Policy Upate Request Success
[18] N10 Registration Request
[19] N10 Registration Success
[20] N1N2 Transfer Request
N1 PDU Session Establishment Accept
N2 PDU Resource Setup Request
[21] Nsmf_PDUSession_UpdateSMContext Request
N2 PDU Resource Setup Response
[22] N4 Session Modification Request
[23] N4 Session Modification Response
[24] Nsmf_PDUSession_UpdateSMContext Response
UE
AMF
SMF
UPF
UPF1
UDM
PCF
CHF
477536

Table 11: Call Flow Description for 5G Session Creation During N4 Session Establishment Failure with N7 Optimization

Step	Description
1	UE sends the PDU Session Establishment Request message to AMF.
2	AMF sends the Nsmf_PDUSession_CreateSMContext Request message to SMF.
3	SMF sends the N10 Subscription Fetch request message to UDM.
4	UDM sends the N10 Subscription Fetch Success response to SMF.
5	SMF sends the N10 Subscribe to Notification message message to UDM.
6	UDM sends the N10 Subscribe to Notification Success response to SMF.
7	SMF sends the Nsmf_PDUSession_CreateSMContext Response to AMF.
8	On SMF, the configuration is enabled for the optimised N7 IP adddress allocation and UPF selection. SMF sends the N7 SM Policy Create Request message along with the IP Address to PCF.
9	PCF sends the N7 SM Policy Create Request Success message to SMF.

Step	Description
10	SMF sends the N40 Charging Data Request message to CHF.
11	CHF sends the N7 Charging Data Request Success message to SMF.
12	SMF sends the N4 Session Establishment Request message to UPF.
13	UPF sends the N4 Session Establishment Failure message to SMF.
14	The UPF reselection and IP adddress reallocation happens. SMF sends the N4 Session Establishment Request message to UPF1.
15	UPF1 sends the N4 Session Establishment Success message to SMF.
16	SMF sends the N7 SM Policy Upate Request, with another IP address to PCF.
17	PCF sends the N7 SM Policy Upate Request Success message to SMF.
18	SMF sends the N10 Registration Request message to UDM.
19	UDM sends the N10 Registration Success message to SMF.
20	SMF sends the N1N2 Transfer Request message to AMF.
21	The N1 PDU Session Establishment is accepted and the N2 PDU Resource Setup Request message is sent. AMF sends the Nsmf_PDUSession_UpdateSMContext Request message to SMF.
22	N2 PDU Resource Setup Response message is received. SMF sends the N4 Session Modification Request message to UPF.
23	UPF sends the N4 Session Modification Response message to SMF.
24	SMF sends the Nsmf_PDUSession_UpdateSMContext Response to AMF.

Configuring N7 Optimization

To configure the N7 optimization, use the following sample configuration:

```
config
  profile dnn dnn_profile_name
    policy [ local | optimized ]
      rat-type [ nr | wlan | eutra ]
    end
```

NOTES:

- **profile dnn** *dnn_profile_name*: Specify the DNN profile name. *dnn_profile_name* must be an alphanumeric string.
- **policy [local | optimized]**: Disable or enable the interaction with PCF.
    - **local**: SMF does not interact with UPF.

Note

- This parameter is applied only during session creation and doesn't change during handover.
- If you configure **policy local**, then the configuration of PCF or PCRF is not mandatory.

- **optimized**: SMF skips the N7 update by sending the UE IP address in N7 Create message.

Note

In case you configure both **policy local** and **policy optimized** together, then **policy local** takes the precendence.

- **rat-type [nr | wlan | eutra]**: This keyword is to reduce the number of messages being exchanged with PCF for the specified RAT type.

Note

This keyword is optional. If **rat-type** is not configured then the **policy local** or **policy optimized** is valid for all the three RAT types, which are NR, WLAN, and EUTRA.

OAM Support

Bulk Statistics Support

The SMF maintains the following metrics as part of this feature.

- smf-service-stats

  Description: This statistics includes policy_type label to indicate the number of session setup with the optimized N7.

  Labels:

  - policy_type

- Values:
  - pcf
  - pcrf
  - local_policy
  - pcf_optimized

The smf-service-stats needs to be enabled as part of granular-labels configuration. If enabled, smf-service-stats indicates the number of session setup with the optimized N7 for the policy_type label.

To enable the smf-service-stats statistics, configure the granular-labels statistics for pcf_optimized using the following:

```
infra metrics verbose application
  metrics smf_service_stats
    granular-labels [ policy_type ]
  exit
```

Dynamic QoS Flow-based Application Detection and Control

Feature Description

To support the dedicated bearer on QCI 80 (QoS Class Identifier), SMF must support application detection and control (ADC) feature.

On receiving a PCC rule for application detection and control, with an application-Id and APP_STA/APP_STO provisioned in Policy-control-request-trigger, SMF instructs the UPF to detect the application traffic. When the application traffic is identified by an application identifier received from the UPF, SMF reports the start of the application to the PCF. Then, PCF makes the policy decisions based on the information received and installs a new dedicated PCC rule with QCI 80 to SMF.

SMF supports the following functionalities:

- Enable and disable ADC from PCF.
- Report APP_START and APP_STOP to PCF based on application traffic detection at UPF.
- Mute application detection.
- Process applications START, STOP from UPF in session report and triggering APP_STA/APP_STO toward the PCF.
- Detect application for L3, L4, and L7 rules.

Dynamic QoS Flow Based Application Detection and Control is applicable to both roaming and non-roaming scenarios.

How it Works

This section describes how Dynamic QoS Flow Based Application Detection and Control feature works.

Interface Details

PCF SMF interface – PCF enables ADC at SMF

ADC related IEs from PCF to SMF:

appId: application identifier provided by PCF within PCC-Rule.

APP_STA and APP_STO: PCF provisions these triggers in Policy control request trigger.

muteNotif : Mute Notification. PCF may mute a notification about a specific detected application by including IE in "traffContDecs" and including a "refTcData" attribute referring to the Traffic Control Data decision within the PCC rule.

Example:

```
{   'sessRules': {'SessRule-1': {…}}},
    'pccRules': {
         'PccRule-1': {…},
         'crn#rda1': {'pccRuleId': 'crn#rda1', 'appId': 'x', reftcdata:”TCD-2”}},
    'qosDecs': {'QoS-1': {…}}
    'traffContDecs':{'TCD-2':{'tcId':'TCD-2','flowStatus':'DISABLED',’muteNotif‘:true}},
    ‘policyCtrlReqTriggers’:[‘PLMN_CH’,’AC_TY_CH’,’APP_STA’,’APP_STO’] }
}
```

Important Unmuting a predefined rule is not supported.

Mute function is supported only during PolicyCreate and not during PolicyUpdate.

SMF PCF -Reporting Start or Stop Trigger to PCF

SMF sends a SMPolicyControl_Update including detected application information in "appDetectionInfo" and "APP_STA" / ”APP_STO” within the "repPolicyCtrlReqTriggers" attribute.

When UPF optimization enabled, SMF does not filter APP_STA or APP_STO trigger and it sends all APP_STA or APP_STO triggered to PCF which are triggered by UPF. UPF optimization enabled by setting environment variable UPF_ADC_OPTIMIZED = true in SMF setup.

Table 12: Definition of type AppDetectioninfo

Attribute Name	Data Type	P	Cardinality	Description
appId	String	M	1	Reference to the application detection filter configured at the UPF
InstanceId	String	O	1	Identifier dynamically assigned by SMF in order to allow correlation of the application Start and Stop events to the specific service data flow description, if service data flow descriptions are deducible.
sdfDescriptions	array(flow Information)	O	1...N	Contains the deducted service data flow descriptions if they are deducible.

Limitations

The Dynamic QoS Flow Based Application Detection and Control feature has the following limitations:

- In case both ADC start or stop and non-ADC Usage-report(vol/time threshold) come from UPF in same session-report, it is not deterministic weather first ADC report or Non-ADC report is processed. When both ADC and non-ADC report come in a session-report, smf-service pod posts two internal events ADC event and non-ADC usage-report event. Infra creates two separate go-routines to process both events. But it is not deterministic which go-routine is going to be scheduled first, because of this limitation, some times Non-ADC usage-report is processed before ADC report or the other way around.

- When APP-Start and App-Stop event for two separate App-Id's are received from UPF in same session-report request, SMF informs both(Start and Stop) events in same SmPolicyUpdateReq to PCF. APP_STA and APP_STO are sent in repPolicyCtrlReqTriggers IE.\, this is a global IE. Since PCF has history of receiving APP_STA and APP_STO, it can link the APP_STO to the appId for which an APP_STA already received. APP_STA trigger is applicable to the appId for which PCF has not received a start indication.

Dynamic ADC Rules Enforcement Over Gx

Table 13: Feature History

Feature name	Release information	Description
Traffic Prioritization based on Flows of Dynamic ADC Rules	2025.01.0	SMF uses TosTrafficClass field in dynamic ADC rules from PCRF to prioritize the traffic flows associated with IoT applications during network congestion.
Modification of QCI, ARP, and Online/Offline Charging Attributes	2024.03.0	With this release, SMF supports modification of these additional AVPs included in the dynamic ADC rule: • QCI • ARP • Online • Offline These modifications allow the service providers to classify the traffic more efficiently.
Dynamic ADC Rules Over Gx Interface	2024.02.0	SMF allows the users to install, modify or remove the dynamic ADC rules. SMF forwards the new or updated rules to UPF for traffic classification. This feature allows the service providers to manage the IoT devices, such as connected cars, and charge their subscribers based on the traffic flows classified by SMF/UPF. With this traffic classification, the service providers enable service monetization. **Default Setting**: Enabled — Always-on

Feature Description

SMF supports addition, modification, and removal of dynamic ADC rules over the Gx interface. Upon receiving a new dynamic ADC rule with TDF-App-Identifier AVP (Application Id) and TosTrafficClass AVP from

PCRF, SMF processes the dynamic ADC rule and sends N4 messages to the UPF along with TDF-App-Identifier and TosTrafficClass to install the ADC rule.

The TosTrafficClass field received in a dynamic rule from PCRF supports the prioritization of traffic flow during network congestion. When the TosTrafficClass field is received by UPF, the ToS is applied in the IP Header for all the uplink and downlink packets for the flows matching the ADC Rule.

UPF matches the dynamic ADC rule with the configured TDF-App-Identifier for further processing of the dynamic ADC rules.

This feature enables the policy server to control the Rating Group and Service ID for each subscriber dynamically.

Note SMF processes the dynamic ADC rules associated with the default bearer only.

How it Works

To enable dynamic ADC rules over Gx, SMF and PCRF server exchange information about features they support using the supported feature bit over CCR-I/CCA-I messages. Thus, SMF and PCRF server negotiate the supported features that would be enabled for a session.

Upon a successful negotiation of the supported feature bit, SMF receives a dynamic ADC rule from the PCRF. SMF then initiates the installation, modification, or removal of dynamic ADC rules.

SMF supports the following operations for dynamic ADC rules over Gx interface:

- Installing dynamic ADC rules
- Modifying dynamic ADC rules
- Removing dynamic ADC rules

Installing Dynamic ADC Rule

Following call flow explains the process of installing dynamic ADC rules:

Figure 11: Dynamic ADC Rule Install Call Flow

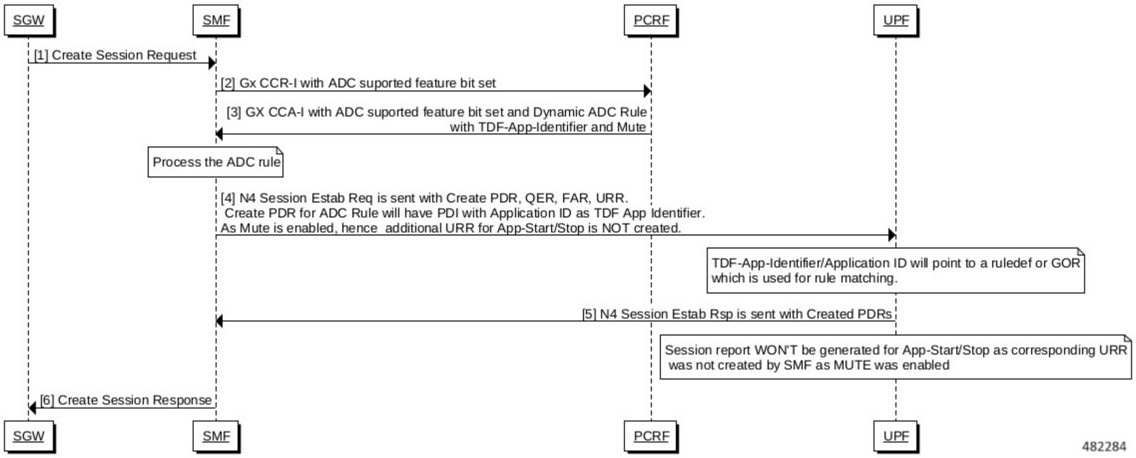

SGW
SMF
PCRF
UPF
[1] Create Session Request
[2] Gx CCR-I with ADC suported feature bit set
[3] GX CCA-I with ADC suported feature bit set and Dynamic ADC Rule with TDF-App-Identifier and Mute
Process the ADC rule
[4] N4 Session Estab Req is sent with Create PDR, QER, FAR, URR.
Create PDR for ADC Rule will have PDI with Application ID as TDF App Identifier.
As Mute is enabled, hence additional URR for App-Start/Stop is NOT created.
TDF-App-Identifier/Application ID will point to a ruledef or GOR which is used for rule matching.
[5] N4 Session Estab Rsp is sent with Created PDRs
Session report WON'T be generated for App-Start/Stop as corresponding URR was not created by SMF as MUTE was enabled
[6] Create Session Response
SGW
SMF
PCRF
UPF
482284

Table 14: Dynamic ADC Rule Install Call Flow Description

Step	Description
1.	SMF receives Create Session Request from SGW.
2.	SMF sends a CCR-I with ADC supported feature bit to PCRF. **Note** Supported Feature bit for ADC should be negotiated between PCRF and SMF.
3.	SMF receives the dynamic ADC rule with TDF-App-Identifier and Mute from PCRF through CCA-I message. The TosTrafficClass is an optional value received in CCA-I message.
4.	SMF installs the rule and sends N4 Session Establishment Request to UPF to create Packet Detection Rule (PDR), QoS Enforcement Rule (QER), Forwarding Action Rule (FAR), and Usage Reporting Rule (URR). Create PDR Request for this ADC rule contains the TDF-App-Identifier and TosTrafficClass If the TOS value received is different from the bearer level FARs created, new UL/DL FARs are created for a dynamic rule. The TOS value and the corresponding mask is populated in TRANSPORT LEVEL MARKING IE in DL FAR and in INNER PACKET MARKING IE in UL FAR respectively in N4 Establishment request. **Note** SMF supports only dynamic ADC rules with Mute AVP enabled. Hence, the additional URR is not created for APP-START and APP-STOP notifications.
5.	UPF sends a N4 Session Establishment Response with PDRs created for the ADC rule. UPF does not generate the session report for APP-START and APP-STOP, as it receives the ADC rule with Mute enabled.
6.	SMF sends the Create Session Response from SGW.

Modifying Dynamic ADC Rule

These stages describe the process of modifying dynamic ADC rules:

Figure 12: Dynamic ADC Rule Modification Call Flow

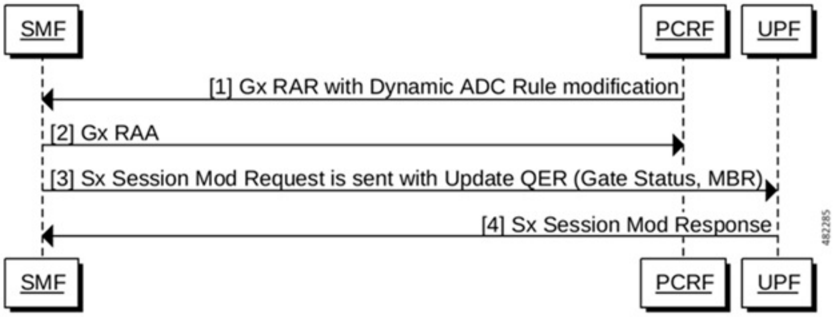

SMF
PCRF
UPF
[1] Gx RAR with Dynamic ADC Rule modification
[2] Gx RAA
[3] Sx Session Mod Request is sent with Update QER (Gate Status, MBR)
[4] Sx Session Mod Response
482285

Table 15: Dynamic ADC Rule Modification Call Flow Description

Step	Description
1.	SMF receives a Re-Authorization Request (RAR) along with the dynamic ADC Rule Modification Request from PCRF. SMF supports modifications of the following AVPs in dynamic ADC rule: • Flow-Status • Max-Requested-Bandwidth-UL • Max-Requested-Bandwidth-DL • QCI • ARP • Online • Offline **Note** You can modify the QCI and ARP of a dynamic rule only if the QCI and ARP of the default bearer are also being adjusted.
2.	SMF sends the Re-Authorization Answer (RAA) to the PCRF.
3.	SMF sends a N4 Session Modification Request with Update QER IE to the UPF. This Update QER IE includes both Gate Status IE and Maximum Bitrate (MBR) IE.
4.	UPF sends the N4 Session Modification Response to SMF.

Modification of Charging Data for an Installed Dynamic ADC Rule

SMF supports modification of the following two dynamic ADC rule charging attributes:

- **Offline**: The possible values are ENABLE_OFFLINE (1) and DISABLE_OFFLINE(0).
- **Online**: The possible values are ENABLE_ONLINE (1) and DISABLE_ONLINE(0).

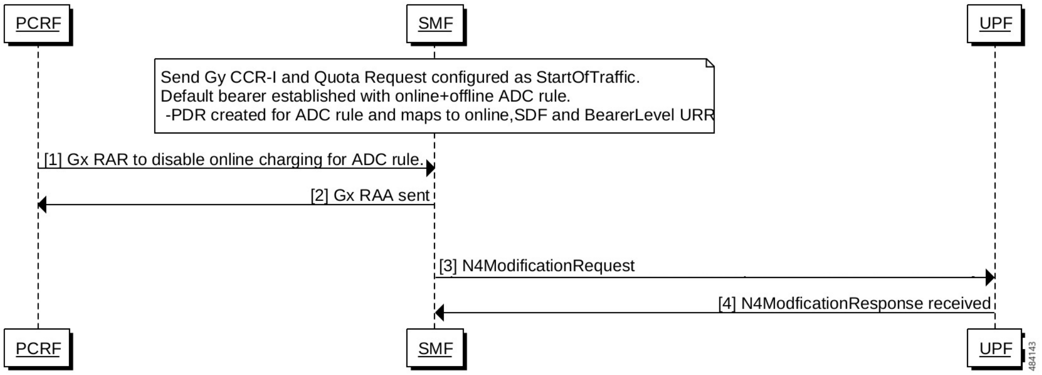
There are multiple combinations for modifying the charging attributes of a dynamic ADC rule. Two major combinations include:

- Online and Offline to Offline Only
- Offline Only to Online and Offline

Modifying Charging Attributes from Both Offline and Online to Offline Only

These stages describe the process of modifying the charging attributes from both Offline and Online to Offline only:

Figure 13: Call Flow for Charging Modification from Both Offline and Online to Offline Only


PCRF
SMF
UPF
Send Gy CCR-I and Quota Request configured as StartOfTraffic.
Default bearer established with online+offline ADC rule.
-PDR created for ADC rule and maps to online,SDF and BearerLevel URR
[1] Gx RAR to disable online charging for ADC rule.
[2] Gx RAA sent
[3] N4ModificationRequest
[4] N4ModficationResponse received
PCRF
SMF
UPF
484143

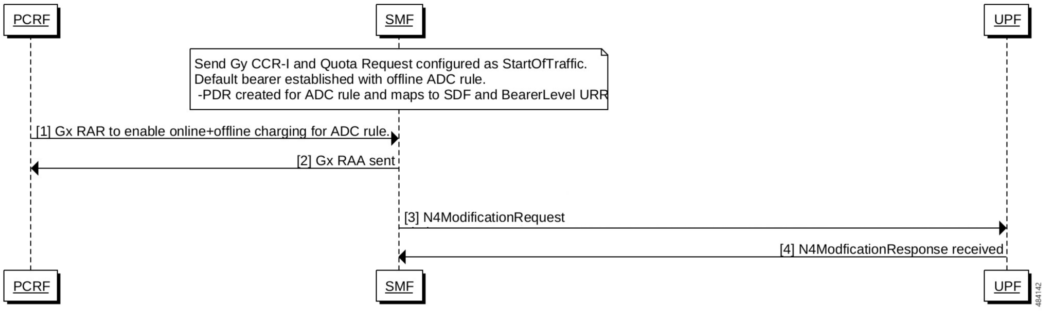
Upon successful PDN attach, the dynamic ADC rule is installed with both Online and Offline rule on the default bearer. At this time, a PDR is created and mapped to Online, Service Data Flow (SDF) level and bearer-level URR.

1. PCRF sends the Gx RAR to SMF to disable Online charging on the dynamic ADC rule. PCRF sends DISABLE_ONLINE(0) to modify the rule as Offline only.
2. The SMF sends the Gx RAA to the PCRF.
3. SMF sends an N4 Modification Request to the UPF with the following two instructions:
   a. Remove the URR associated with Online charging.
   b. Update PDR for the dynamic ADC rule to map to the SDF and bearer-level URR.
4. UPF sends the N4 Modification Response to SMF.

Modifying Charging Attributes from Offline Only to Both Offline and Online

These stages describe the process of modifying the charging attributes from Offline only to both Offline and Online:

Figure 14: Call Flow for Charging Modification from Offline Only to Both Offline and Online


PCRF
SMF
UPF
Send Gy CCR-I and Quota Request configured as StartOfTraffic.
Default bearer established with offline ADC rule.
-PDR created for ADC rule and maps to SDF and BearerLevel URR
[1] Gx RAR to enable online+offline charging for ADC rule.
[2] Gx RAA sent
[3] N4ModificationRequest
[4] N4ModficationResponse received
PCRF
SMF
UPF
484142

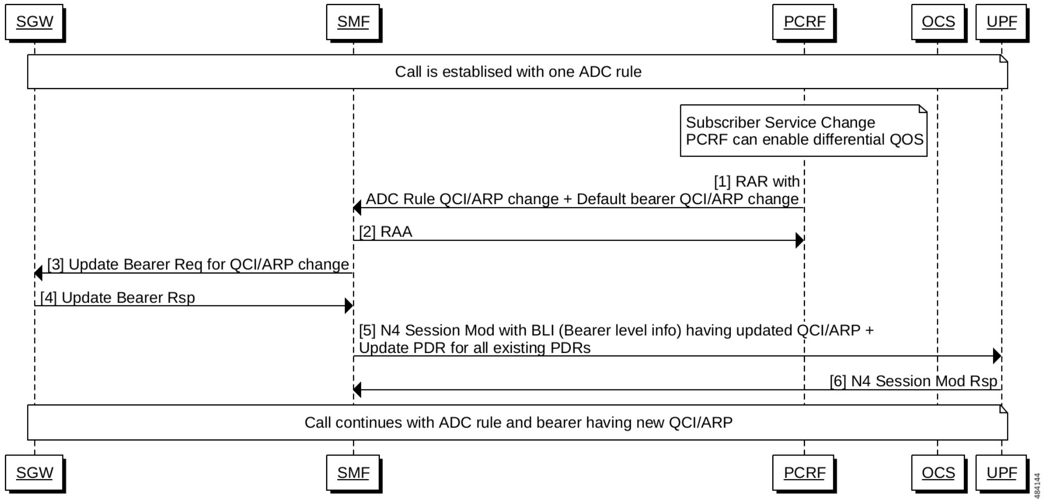
Upon successful PDN attach, the dynamic ADC rule is installed on a default bearer with offline charging enabled. At this time, a PDR is created for dynamic ADC rule and mapped to SDF URR, and Bearer-level URR.

1. PCRF sends the Gx RAR to SMF to enable both Offline and Online charging on the dynamic ADC rule. PCRF sends ENABLE_ONLINE(1) to modify rule from Offline only to both Online and Offline charging.
2. The SMF sends the Gx RAA to the PCRF.
3. SMF sends an N4 Modification Request to the UPF with the following two instructions:
   a. Create Online URR to enable Online Charging with Start of Traffic (SoT) set.
   b. Update PDR for dynamic ADC rule to map to the Online, SDF level and bearer-level URR.
4. UPF sends the N4 Modification Response to SMF.

Modifying QCI and ARP of an Installed Dynamic ADC Rule

These stages describe the process of modifying the QCI and ARP of an installed dynamic ADC rule:

Figure 15: Call Flow for Modifying QCI and ARP of an Installed Dynamic ADC Rule


SGW
SMF
PCRF
OCS
UPF
Call is establised with one ADC rule
Subscriber Service Change
PCRF can enable differential QOS
[1] RAR with
ADC Rule QCI/ARP change + Default bearer QCI/ARP change
[2] RAA
[3] Update Bearer Req for QCI/ARP change
[4] Update Bearer Rsp
[5] N4 Session Mod with BLI (Bearer level info) having updated QCI/ARP +
Update PDR for all existing PDRs
[6] N4 Session Mod Rsp
Call continues with ADC rule and bearer having new QCI/ARP
SGW
SMF
PCRF
OCS
UPF
484144

1. PCRF sends Gx RAR to SMF, containing QCI and ARP changes for the dynamic ADC rule and the default bearer.

2. SMF sends the Gx RAA to the PCRF.
3. SMF sends an Update Bearer Request to SGW to modify the QCI and ARP of the default bearer.
4. SGW sends an Update Bearer Response to SMF.
5. SMF sends an N4 Session Modification Request with the Bearer Level Information (BLI) containing the updated QCI and ARP. The N4 Session Modification Request also contains the Update PDR instruction for all the existing PDRs.
6. UPF sends the N4 Modification Response to SMF.
7. The session continues with the ADC rule and bearer having the new QCI and ARP.

Removing Dynamic ADC rules

The following call flow explains the process of removing dynamic ADC rules:

Figure 16: Dynamic ADC Rule Removal Call Flow

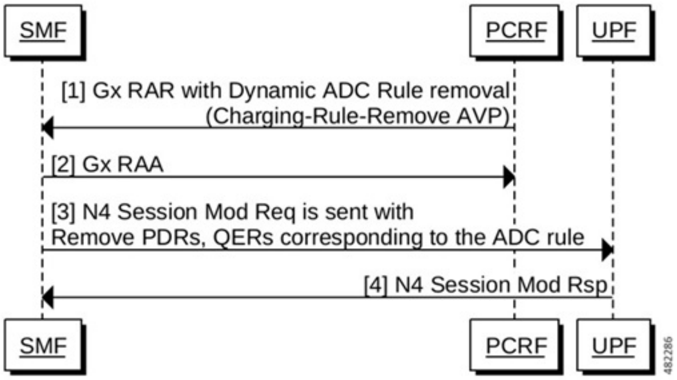

SMF
PCRF
UPF
[1] Gx RAR with Dynamic ADC Rule removal
(Charging-Rule-Remove AVP)
[2] Gx RAA
[3] N4 Session Mod Req is sent with
Remove PDRs, QERs corresponding to the ADC rule
[4] N4 Session Mod Rsp
SMF
PCRF
UPF
482286

Table 16: Dynamic ADC Rule Removal Call Flow Description

Step	Description
1.	SMF receives a Re-Authorization request (RAR) along with Charging-Rule-Remove AVP from PCRF.
2.	SMF sends the Re-Authorization Answer (RAA) to the PCRF.
3.	SMF sends a N4 Session Modification Request to the UPF with Remove PDRs and QERs and FARs corresponding to the ADC rule.
4.	UPF sends the N4 Session Modification Response to SMF.

Note REMOVE_FARs are sent only when the rule is deleted and no other rule PDRs are associated to these FARs

Limitations

Following are the known limitations of this feature:

- Currently, the ADC rule installation and modification failures are not reported to PCRF.
- The Rating-Group and Service-Identifier AVPs cannot be shared across dynamic ADC rule and static rules. However, these AVPs can be shared across multiple dynamic ADC rules.
- The name of dynamic ADC rule name cannot start with “adc” string.
- This feature only supports Dynamic ADC rules with Mute notification enabled.
- Modifying a dynamic ADC rule from a charging state (PDR mapped to Online, Offline, or both URRs) to a no-charging state (PDR mapped to no URR) is not supported.
- Gy interface failure handling is supported for modification of ADC rule from Offline-only charging to both Offline and Online charging. It is currently not supported for other types of charging modifications.
- The QCI and ARP of all dynamic ADC rules must always match the QCI and ARP of the default bearer.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

The following statistics are supported for the Dynamic ADC Rules Enforcement Over Gx feature.

- **policy_adc_total**: This metric reflects the total number of dynamic ADC rules installed. This metric is enabled at the debug level. Following new label is added in support of this feature:
  - **mute**: This label specifies if the Mute AVP is enabled for the dynamic ADC rule. The possible values of this label are 'True' and 'False'.
- **policy_dynamic_pcc_rules_total**: This metric displays the total number of dynamic rules pushed from PCF. Following are the new labels added in support of this feature:
  - **is_adc**: This label specifies if the dynamic rule is an ADC rule. The possible values of this label are 'True' and 'False'.
  - **mute**: This label specifies if the Mute AVP is enabled for the dynamic rule. The possible values of this label are 'True' and 'False'.

Show Command Output

This section describes the show command and output available to view the configuration related to the dynamic ADC rule.

show subscriber nf-service smf supi *supi_id* full

The following show subscriber command has been enhanced to display the **mute** and **appId** for ADC dynamic rule and **ToSTrafficClass** and **flowstatus** information for all dynamic rules:

```
[unknown] smf# show subscriber nf-service smf supi imsi-123456789012345 full

pccRuleId": "rd1-adc",
   "qfi": 1,
   "mbrDl": 2000,
   "mbrUl": 2000,
   "chargingInformation": {
   "chargingId": "rd1-adc",
   "meteringMethod": "Duration and Volume",
   "Type": "Offline",
   "ratingGroup": 10,
   "serviceId": "20"
  },
  "appId": "adc",
  "mute": "Required",
  "flowStatus": "Enabled (2)"
   ToSTrafficClass: 20fe
```

Monitoring Support

The following monitor subscriber command has been enhanced to show the TDF App ID, TosTraffic AVP and Mute AVP information for ADC dynamic rule for both Gx and N4 interfaces:

```
[unknown] smf# monitor subscriber supi imsi-* capture-duration 1000 internal-messages yes

ChargingRuleInstall:
                            ChargingRuleInstall[0]:
                                ChargingRuleDefinition:
                                    ChargingRuleDefinition[0]:
                                        ChargingRuleName: dynamicAdc1
                                        RatingGroup:
                                            Value: 40
                                        ServiceIdentifier:
                                            Value: 30
                                        Precedence:
                                            Value: 70
                                        QoSInformation:
                                            QoSClassIdentifier:
                                                Value: QCI_7(7)
                                            MaxRequestedBandwidthUL:
                                                Value: 2000
                                            MaxRequestedBandwidthDL:
                                                Value: 2000
                                            GuaranteedBitrateUL:
                                                Value: 1000
                                            GuaranteedBitrateDL:
                                                Value: 1000
                                            AllocationRetentionPriority:
                                                PriorityLevel: 5
                                                PreEmptionCapability:
                                                  Value: PREEMPTION_CAPABILITY_DISABLED(1)

                                                PreEmptionVulnerability:
                                                Value: PREEMPTION_VULNERABILITY_ENABLED(0)

                                        ReportingLevel:
                                            Value: RATING_GROUP_LEVEL(1)
                                        Online:
                                            Value: ENABLE_ONLINE(1)
                                        Offline:
                                            Value: DISABLE_OFFLINE(0)
                                        MeteringMethod:
```

```
    Value: DURATION_VOLUME(2)
MuteNotification:
    Value: MUTE_REQUIRED(0)
FlowStatus:
    Value: ENABLED(2)
TdfApplicationIdentifier: qci7
ToSTrafficClass: 20fe
```

Static PCC Rules Support

Feature Description

Static PCC rules are configured in the SMF. These rules can be activated immediately upon PDU session establishment. Static rule is identified by the ruledef configuration using the **action priority** CLI command.

The local configuration on SMF represents the rulebase which is sent to the UPF during session establishment. The SMF uses the configuration representing the PCC rules, QoS Desc, and Charging Data received from PCF to perform QoS flow binding. This configuration is present in the UPF as well. The SMF does not send the PDRs, QERs, and FARs, instead sends only the rulebase name in a default PDR (referred as rulebase PDR) over the N4 interface. The UPF generates the PDRs, FARs, QERs, and URRs for predefined rules based on the rulebase configuration.

Important The Static PCC Rules Support on SMF is applicable to both 4G and 5G calls.

Relationships

This feature utilizes the functionalities provided by PDU Session Lifecycle feature.

How it Works

PCF must send the rulebase name to enable the static PCC rule support on SMF.

When the PCF provides the rulebase name, the SMF performs the following steps during the PDU session creation:

1. The SMF sends Npcf_SMPolicycontrolCreate message to PCF. In response to this message, the PCF may send SMPolicyDecision with a PccRule. If the rule ID of the PccRule is in cbn# rulebase name format, the SMF assumes that the rule id is representing a rulebase name.

2. The SMF sends the rulebase name to the UPF in PFCP Session Establishment Request in a proprietary IE within Create PDR IE.

Note The SMF sends this name only in the default PDR which does not have any SDF filters. No other PDR, FAR, QER, and URR are sent to the UPF for the static rules. The UPF can derive the same from the rulebase name.

Pre-processing During Configuration

Once the Active Charging Service configuration is done (including rulebase, associated ruledefs, and charging actions), SMF processes the configured values and derives PCC Rules, QoSData, and ChargingData from the configured values. The following principles are used to create these entities:

1. QoSData:
    a. Each configured charging action results in a QoSDesc creation.
    b. The **flow-limit-bandwidth** configured under charging action provides the GBR/MBR for the QoSData.
    c. The QCI and ARP configured in charging action constitute the 5QI and ARP of the QoSData. If no QCI and ARP are configured, the 5QI and ARP of the default QoS flow are associated with this QoSData.
2. ChargingData:
    a. The **billing-action** configuration under charging action determines whether offline charging is enabled in the created ChargingData.
    b. The **cca charging credit** configuration under charging action determines whether online charging is enabled in the created ChargingData.
    c. The rating group and service ID of the ChargingData are provided by content-id and service-identifier configuration under charging action.
3. PCCRule:
    a. Each ruledef under a rulebase results in creation of a PCCRule.
    b. The **packet-filter** configured under charging action is used for the FlowInformation in the PCCRule.
    c. The QoSData and ChargingData associated with this ruledef in the rulebase configuration form the refQoS and refChg for this PCCRule.

All the created PCCRules, QoSData, and ChargingData are saved per rulebase.

During PDU Session Creation

1. During PDU session creation, PCF sends the rulebase name (value configured under upf-apn is selected if the PCF does not send it) as PCCRule with ID set to cbn# configured rulebase name. It may also send any predefined rule to be activated as another PCCRule with ID set to crn# configured ruledef name. All such PCC rules will have only the RuleId attribute present.
2. On receiving such a request, SMF selects the constructed PCCRules, QoSData, and ChargingData which correspond to the received rulebase and ruledef names, and uses these to create QoS flows in QoSModel.
3. On the N4 interface, the SMF sends the rulebase name in the CreatePDR IE in a Cisco Proprietary IW named "rulebase".
4. For all activated predefined rules, SMF sends one uplink and one downlink PDR containing the ruledef name in "Activate Predefined Rule" IE.
5. The UPF also has similar configuration for active charging service. From the rulebase name and ruledef names, it can create the corresponding QER and URR.

6. On N1 and N2 interfaces, the processing of the predefined and static rules are the same as that of dynamic rule.
7. For all static and activated predefined rules, QoSRules are sent on N1 interface if packet-filters were configured.
8. The GFBR and MFBR of a flow are computed using the GBR/MBR of the QoSData associated with all static and activated predefined rules at any point of time and the same is sent on N2 interface in an AuthorisedQoSDescription IE on N1 interface.

During PDU Session Modification

1. During PDU session modification, PCF sends the rulebase name as PCCRule with ID set to cbn#configured rulebase name. In case of predefined rule PCF can activate new rule crn#configured ruledef name or delete the existing rule (crn#"nil"). All such PCC Rules will have only the RuleId attribute present.
2. On receiving new rule addition request, SMF selects the constructed PCCRules, QoSData and ChargingData which correspond to the received rulebase and ruledef names, and uses these to create QoS flows in QoSModel.
3. On receiving an existing rule deletion request, if the SMF received a ruledef name with nil value or a rulebase name different from the existing one, the SMF deletes the QoS flows which correspond to previous rulebase name or ruledef in QoSModel.
4. On N4 interface, SMF sends the new rulebase name in the CreatePDR IE in a Cisco Proprietary IW named "rulebase" and RemovePDR with PDR ID which correspond to the old rulebase name.
5. For all activated predefined rules, SMF sends one uplink and one downlink PDR containing the ruledef name in "Activate Predefined Rule" IE.
6. For all deactivated predefined rules, SMF sends RemovePDR with PDR ID which corresponds to the predefined rule.
7. The UPF also has similar configuration for active charging service. From the rulebase name and ruledef names, it can create or delete the corresponding QER and URR.
8. On N1 and N2 interfaces, the processing of the predefined and static rules are the same as that of dynamic rule.
9. For all static and activated/deactivated predefined rules, QoSRules are sent on N1 interface if packet-filters were configured.
10. The GFBR and MFBR of a flow are computed using the GBR/MBR of the QoSData associated with all static and activated/deactivated predefined rules at any point of time and the same is sent on N2 interface in an AuthorisedQoSDescription IE on N1 interface.

Configuring the Static PCC Rules

This section describes how to configure the Static PCC Rules on SMF.

The configuration for static and predefined rules is based on the ECS configuration of the StarOS based PGW-C. This is to ensure that the UPF can work seamlessly with the SMF.

Make sure to first configure the Active Charging Service (ACS) before proceeding with the static PCC rules configuration. ACS provides flexible, differentiated, and detailed billing to subscribers through Layer 3 through Layer 7 packet inspection and the ability to integrate with back-end billing mediation systems.

Note You can configure only one active charging service per system.

Configuring the Static PCC Rules Support involves the following steps:

1. Configuring Charging Action, on page 65
2. Configuring Packet Filter, on page 67
3. Configuring ACS Ruledef, on page 68
4. Configuring ACS Group of Ruledefs, on page 69
5. Configuring Rulebase and Predefined Rule Prefix, on page 70
6. Configuring ACS Rulebase in ACS Configuration Mode, on page 72
7. Configuring URR ID, on page 70
8. Configuring GTPP Group, on page 71
9. Configuring APN, on page 71
10. Associating GTPP Group with APN, on page 72
11. Configuring ACS Rulebase in APN Configuration Mode, on page 70
12. Defining UPF APN Profile in DNN Profile Configuration, on page 74
13. Configuring QoS Parameters, on page 39

Configuring Charging Action

This section describes how to configure charging action. The charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, and so on. The charging action will also determine the metering principle—whether to count retransmitted packets and which protocol field to use for billing (L3, L4, L7, and so on).

To define the QoS and charging related parameters associated with ruledefs, use the following sample configuration.

```
config
   active-charging service service_name
      charging-action charging_action
         allocation-retention-priority priority  [ pci pci_value
         | pvi pvi_value billing-action egcdr cca
         charging credit [ rating-group coupon_ id
         ] [ preemptively-request ]
         content-id content_id
         flow action { discard [ downlink | uplink ] | redirect-url
         redirect_url | terminate-flow }
```

```
flow limit-for-bandwidth { { direction { downlink | uplink }
peak-data-rate bps peak-burst-size bytes violate-action
{ discard | lower-ip-precedence } [ committed-data-rate
bps committed-burst-size bytes
[ exceed-action { discard | lower-ip-precedence
} ] ] } | { id id } }
nexthop-forwarding-address ipv4_address/ipv6_address
qos-class-identifier qos_class_identifier
service-identifier service_id
tft packet-filter packet_filter_name
tft-notify-ue
tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32
| af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value
} [ downlink | uplink ]
end
```

NOTES:

- **charging-action** *charging_action_name*: Specify the name of a charging action. *charging_action_name* must be an alphanumeric string of 1 to 63 characters and can contain punctuation characters. Each charging action must have a unique name.
- If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.
- If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.
- **allocation-retention-priority** *priority* **[pci***pci_value* **| pvi** *pvi_value* : Configures the Allocation Retention Priority (ARP). *priority* must be an integer value in the range of 1-15.
  - **pci** *pci_value* : Specify the Preemption Capability Indication (PCI) value. The options are:
    - MAY_PREEMPT—Flow can be preempted. This is the default value.
    - NOT_PREEMPT—Flow cannot be preempted.
  - **pvi** *pvi_value*: Specify the Preemption Vulnerability Indication (PVI) value. The options are:
    - NOT_PREEMPTABLE—Flow cannot be preempted. This is the default value.
    - PREEMPTABLE—Flow can be preempted.
- **billing-action**: Configure the billing action for packets that match specific rule definitions.
- **cca charging credit**: Enable or disable Credit Control Application (CCA) and configure the RADIUS/Diameter prepaid charging behavior.
- **content-id**: Configure the rating group.
- **flow action**: Specify the action to take on packets that match rule definitions.
- **flow limit-for-bandwidth**: Configure the QoS parameters, such as MBR and GBR.
  - peakdatarate(MBR): Default is 3000 bps
  - peakburstsize: Default is 3000 bytes

  - committedDataRate(GBR): Default is 144000 bps
  - committedBurstSize: Default is 3000 bytes

- **nexthop-forwarding-address** *ipv4_address/ipv6_address*: Configure the nexthop forwarding address.
- **qos-class-identifier** *qos_class_identifier*: Configure the QoS Class Identifier (QCI) for a charging action. *qos_class_identifier* must be an integer in the range of 1–9 or from 128–254 (operator specific).
- **service_identifier** *service_id*: Configure the service identifier to use in generated billing records. *service_id* must be an integer in the range of 1–2147483647.
- **tft packet-filter** *packet_filter_name*: Specify the packet filter to add or remove from the current charging action. *packet_filter_name* must be an alphanumeric string of 1 to 63 characters.
- **tft-notify-ue**: Control the TFT updates towards the UE based on certain trigger conditions.
- **tos**: Configure the Type of Service (ToS) octets.

Configuring Packet Filter

To configure the packet filter, use the following sample configuration.

```
config
  active-charging service service_name
    packet-filter packet_filter_name
      direction { bi-directional | downlink | uplink }
      ip local-port { = port_number | range start_port_number to 
      end_port_number }
      ip protocol = protocol_number
      ip remote-port { = port_number | range start_port_number to 
      end_port_number }
      ip tos-traffic-class = { type-of-service | traffic class }
      mask { = mask-value}
      priority priority
      end
```

NOTES:

- **packet-filter** *packet_filter_name*: Configure the packet filters to be sent to UE. *packet_filter_name* must be an alphanumeric string of 1 to 15 characters.
- **direction { bi-directional | downlink | uplink }**: Configure the direction in which the packet filter has to be applied. The default value is **bi-directional**.
- **ip local-port**: Configure the IP 5-tuple local port(s) for the current packet filter.
- **ip protocol**: Configure the IP protocol(s) for the current packet filter.
- **ip remote-address**: Configure the IP remote address(es) for the current packet filter.
- **ip remote-port**: Configure the IP remote port(s) for the current packet filter.
- **ip tos-traffic-class**: Configure the Type of Service (TOS)/Traffic class under charging action in the Packet filter mode.
- **priority** *priority*: Configure the priority of the current packet filter.

Configuring ACS Ruledef

A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service.

To create, configure, or delete ACS rule definitions, use the following sample configuration.

```
config
   active-charging service service_name
      ruledef ruledef_name
         ip any-match [ = | != ] [ TRUE | FALSE ]
         ip dst-address { operator { { ipv4_address | ipv6_address
         } | { ipv4_address/mask | ipv6_address/mask} |
         address-group ipv6_address } | { !range | range }

         rule-application { charging | post-processing | routing }
         end
```

NOTES:

- **ruledef** *ruledef_name*: Specify the ruledef to add, configure, or delete. *ruledef_name* must be the name of an ACS ruledef, and must be an alphanumeric string of 1 to 63 characters, and can contain punctuation characters. Each ruledef must have a unique name. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.
- If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.
- If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef. The ACS Ruledef Configuration Mode is used to create and manage rule expressions in individual rule definitions (ruledefs).
- **ip any-match [= | !=] [TRUE | FALSE**: Define the rule expressions to match IPv4/IPv6 packets. The *operator* and *condition* in the command specifies the following:
    - *operator*
        - !=: Does not equal
        - < =: Equals
    - *condition*
        - FALSE
        - TRUE
- **ip dst-address {** *operator* **{ {** *ipv4_address* | *ipv6_address* **} | {** *ipv4_address/mask* |*ipv6_address/mask* **} | address-group** *ipv6_address* **} | { !range | range } host-pool** *host_pool_name* **}**: Define rule expressions to match IP destination address field within IP headers.
    - *ipv4_address* | *ipv6_address*: Specify the IP address of the destination node for outgoing traffic. *ipv4_address* | *ipv6_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
    - *ipv4_address/mask* | *ipv6_address/mask*: Specify the IP address of the destination node for outgoing traffic. *ipv4_address/mask* | *ipv6_address/mask* must be an IP address in IPv4 dotted-decimal or

IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.

- *address-group ipv6_address*: Specify a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2-byte range input can be configured together within a given IPv6 address.
- The *operator* in the command specifies the following:
    - !=: Does not equal
    - <: Lesser than or equals
    - =: Equals
    - >=: Greater than or equals

- **multi-line-or all-lines**: Allow a single ruledef to specify multiple URL expressions. When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the multi-line-or all-lines command is not configured, the logical AND operator is applied to all the rule expressions.
- **rule-application { charging | post-processing | routing }**: Specify the rule application for a rule definition.
    - **charging**: Specify that the current ruledef is for charging purposes.
    - **post-processing**: Specify that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.
    - **routing**: Specify that the current ruledef is for routing purposes. Up to 256 rule definitions can be defined for routing in an Active Charging Service. Default: Disabled.

Configuring ACS Group of Ruledefs

A group-of-ruledefs can contain optimizable ruledefs. Ruledef group optimization depends on the optimization ability of ruledefs in the group-of-ruledefs, and the optimization configuration of the group in a rulebase.

Upon adding a new ruledef, the following checks occur:

- Determines if the new ruledef is part of any existing group of ruledefs
- Identifies if the new ruledef requires optimization

To combine a set of ruledefs together to apply the same charging action on them, use the following sample configuration.

```
config
  active-charging service service_name
    group-of-ruledefs ruledef_group_name
      add-ruledef priority ruledef_priority ruledef ruledef_name
      exit
```

NOTES:

- **group-of-ruledefs** *ruledef_group_name* : Specify the ruledef group name to add, configure, or delete. This command allows up to a maximum of 128 group of ruledef configurations.

- **add-ruledef**: This command allows you to add or remove ruledefs from a group-of-ruledefs. This command allows up to a maximum of 128 ruledef configurations.
- **priority**: Specify the priority of the ruledef in the current group of ruledefs. *ruledef_priority* must be an integer in the range of 1–10000.
- **ruledef** *ruledef_name*: Specify the name of the ruledef to add to the current group-of-ruledefs. *ruledef_name* must be an alphanumeric string of 1 to 63 characters.

Configuring Rulebase and Predefined Rule Prefix

Rulebase and predefined rule prefix configuration is mandatory for static rule installation from PCF. The SMF supports the predefined rule installation with prefix and without prefix. The SMF also supports the group-of-ruledef installation for both predefined and static rules.

To configure the rulebase prefix and predefined rule prefix, use the following sample configuration.

```
config
  profile network-element pcf pcf_service_name
    predefined-rule-prefix predef_rule_prefix
    rulebase-prefix rulebase_prefix
    end
```

NOTES:

- **predefined-rule-prefix** *predef_rule_prefix*: Specify the predefined rule prefix to be added. For example, the prefix for predefined rule is **cbr**.
- This is an optional configuration for the predefined rule. When there is no prefix defined within the PCF network element profile, the predefined rule application behaves as defined in the *3GPP TS 29.244* specification.
- **rulebase-prefix** *rulebase_prefix*: Specify the rulebase prefix to be added. For example, the prefix for rulebase is **rbn**. This is a mandatory configuration for the static rule.

Configuring ACS Rulebase in APN Configuration Mode

To enable and configure an ACS rulebase to be used for subscribers who use the configured APN, use the following sample configuration.

```
config
  apn apn_name
    active-charging rulebase rulebase_name
    end
```

NOTES:

- **active-charging rulebase** *rulebase_name*: Specify the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.

Configuring URR ID

This section describes how to configure the Usage Reporting Rules (URR) ID for the rating and service groups.

```
config
  active-charging service service_name
  urr-list list_name
    rating-group rating_id service-identifier service_id_value
    urr-id urr_id_value
    end
```

NOTES:

- **urr-list** *list_name*: Specify the name of the URR list. *list_name* must be an alphanumeric string of 1 to 63 characters.
- **rating-group** *rating_id*: Specify the rating ID used in charging. *rating_id* must be an integer in the range of 0–2147483647.
- **service-identifier** *service_id_value*: Configure the service identifier value. *service_id_value* must be an integer in the range of 0–2147483647.
- **urr-id** *urr_id_value*: Configure URR identifier for rating/service group. *urr_id_value* must be an integer in the range of 1–8388607.
- The URR ID configuration is per rating group and service ID. For different rating group and service ID combinations, use the URR ID configuration as many times as needed.

Configuring GTPP Group

To configure the GTPP group, use the following sample configuration.

```
config
  gtpp group group_name
    gtpp trigger { time-limit | volume-limit }
    end
```

NOTES:

- **gtpp group** *group_name*: Specify the GTPP group name. *group_name* must be an alphanumeric string of 1 to 63 characters.
- **gtpp trigger { time-limit | volume-limit }**: Configure triggers for the CDR.
  - **time-limit**: Enable time-limit trigger for the CDR.
  - **volume-limit**: Enable volume-limit trigger for the CDR.

Configuring APN

This section describes how to create Access Point Name (APN) templates. This APN configuration represents the access point configuration in the UPF and further facilitates configuring a rulebase name within.

To configure the APN, use the following sample configuration.

```
config
  apn apn_name
  end
```

NOTES:

- **apn** *apn_name*: Specify a name for the APN template as an alphanumeric string of 1 to 62 characters. The name is case insensitive.

Associating GTPP Group with APN

To associate the GTTP group with the configured APN, use the following sample configuration.

```
config
   apn apn_name
      gtpp group group_name
      end
```

NOTES:

- **gtpp group** *group_name*: Associate the defined GTPP group with the already configured APN.

Configuring ACS Rulebase in ACS Configuration Mode

This section describes how to create, configure, or delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow. The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

Rulebase configuration is the one that combines all the specified configurations together to construct the static and predefined PCC rules.

To configure the ACS rulebase, use the following sample configuration.

```
config
   active-charging service service_name
      rulebase rulebase_name
         action priority action_priority { [ dynamic-only ]
         | static-and-dynamic | timedef timedef_name ]
         { group-of-ruledefs ruledefs_group_name |
         ruledef ruledef_name } charging-action charging_action_name
         [ monitoring-key monitoring_key ] [ description description ] }
         cca quota { holding-time holding_time content-id content_id
         | retry-time retry_time [ max-retries retries ] }
         cca quota time-duration algorithm { consumed-time seconds
         [ plus-idle ] | continuous-time-periods seconds |
         parking-meter seconds} [ content-id content_id]
         credit-control-group cc_group_name
         dynamic-rule order { always-first | first-if-tied }
         egcdr threshold { interval interval
         [ regardless-of-other-triggers ] | volume { downlink | total |
         uplink } bytes }
         route priority route_priority ruledef ruledef_name
         analyzer { dns | file-transfer | ftp-control | ftp-data | h323
         | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp
         | rtsp | sdp | secure-http | sip [ advanced | basic-and-advanced

         ]
         | smtp | tftp | wsp-connection-less | wsp-connection-oriented }
         [ description description ]
         tcp check-window-size
         tcp mss tcp_mss { add-if-not-present | limit-if-present }
         tcp packets-out-of-order { timeout timeout_duration|
    transmit [ after-reordering | immediately ] }
    end
```

NOTES:

- **rulebase** *rulebase_name*: Specify the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.
- **action priority** *action_priority* **{ [dynamic-only] | static-and-dynamic | timedef** *timedef_name* **] { group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[monitoring-key** *monitoring_key* **] [description** *description* **] }**: Configure the priority order in which ruledefs are matched and the associated charging action.
    - *priority* must be an integer in the range of 1–65535.
    - *monitoring_key* must be an integer in the range of 100000–4000000000.

  Use the **no action priority** *action_priority* command to remove the configured ruledef, group-of-ruledefs, and charging action.

Important Currently, the SMF does not support individual removal of ruledef, group-of-ruledefs, and charging action.

- **cca quota { holding-time** *holding_time* **content-id** *content_id* **| retry-time** *retry_time* **[max-retries** *retries* **] }**: Configure the quota for online charging.
    - *holding_time* must be an integer in the range of 1–4000000000
    - *content_id* must be an integer in the range of 1–2147483647
    - *retry_time* must be an integer in the range of 0–86400
    - *retries* must be an integer in the range of 1–65535
- **cca quota time-duration algorithm { consumed-time** *consumed_time* **[plus-idle] | continuous-time-periods** *continuous_time* **| parking-meter** *parking_meter* **} [content-id** *content_id* **]**
    - *consumed_time* must be an integer in the range of 1–4294967295 seconds
    - *content-id* must be an integer in the range of 1–2147483647
    - *continuous_time* must be an integer in the range of 1–4294967295 seconds
    - *parking_meter* must be an integer in the range of 1–4294967295 seconds
- **credit-control-group** *cc_group_name*: Configure the online charging parameters used by this rulebase. *cc_group_name* must be an alphanumeric string of 1 to 63 characters.
- **dynamic-rule order**: Configure the order of dynamic rule matching against the static rules in a rulebase.
- **egcdr threshold { interval** *interval* **[regardless-of-other-triggers] | volume { downlink | total | uplink } bytes }**: Configure the threshold for offline charging.
    - *interval* must be an integer in the range of 60–40000000.
    - **downlink** must be an integer in the range of 100000–4000000000. Default: 4000000000.

  - **uplink** must be an integer in the range of 100000–4000000000. Default: 4000000000.
  - **total** must be an integer in the range of 100000–4000000000.

- **route priority** *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced | basic-and-advanced] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description** *description* **]**: This command is used only on UPF.
  - *route_priority* must be an integer in the range of 0–65535.
  - *ruledef_name* must be an alphanumeric string of 1 to 63 characters.
- **tcp check-window-size**: This command is used only on UPF.
- **tcp mss** *tcp_mss*: This command is used only on UPF. *tcp_mss* must be an integer in the range of 496–65535.
- **tcp packets-out-of-order { timeout** *timeout_duration* **| transmit [after-reordering | immediately] }**: This command is used only on UPF.
  - *timeout_duration* must be an integer in the range of 100–30000. Default value is 5000.

Defining UPF APN Profile in DNN Profile Configuration

To configure the UPF APN profile in the existing DNN profile, use the following sample configuration.

```
config
  profile dnn dnn_profile_name
    upf apn apn_name
    end
```

NOTES:

- **upf apn** *apn_name*: Enable UPF APN profile configuration. This profile is configured under the existing DNN profile configuration. *apn_name* must be an alphanumeric string of 1 to 62 characters.

Configuring QoS Parameters

To configure the QoS parameters, use the following sample configuration.

```
config
  profile qos qos_profile_name
    ambr { ul uplink_ambr | dl downlink_ambr }
    arp { preempt-cap preemption_capability |
    preempt-vuln preemption_vulnerability |
    priority-level priority_level }
    max data-burst burst_volume
    priority qos_priority
    qi5 5qi_value
    exit
```

NOTES:

- **ambr { ul** *uplink_ambr* **| dl** *downlink_ambr* **}**: Define the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber to network) and the downlink (network to subscriber) traffic.
- **arp preempt-cap** *preemption_capability*: Specify the preemption capability flag. The options are:
  - MAY_PREEMPT—Bearer may be preempted
  - NOT_PREEMPT—Bearer cannot be preempted
- **arp preempt-vuln** *preemption_vulnerability*: Specify the preemption vulnerability flag. The options are:
  - PREEMPTABLE—Bearer may be preempted
  - NOT_PREEMPTABLE—Bearer cannot be preempted
- **arp priority-level** *priority_level*: Define the Allocation and Retention Priority (ARP) for the service data. The default value of *priority_level* is 8.
- **max data-burst** *burst_volume*: Define the maximum data burst volume. *burst_volume* must be an integer in the range of 1–4095.
- **priority** *qos_priority*: Specify the 5QI priority level. *qos_priority* must be an integer in the range of 1–127.
- **qi5** *5qi_value*: Specify the 5G QoS Identifier (5QI) for the authorized QoS parameters. *5qi_value* must be an integer in the range of 0–255.

Verifying the Static PCC Rules Support Feature Configuration

This section describes how to verify the Static PCC Rules Support configuration.

To verify the feature configuration details, use the following command.

show full-configuration

The following is an example of this show command output.

```
active-charging service acs
charging-action ca1
  arp priority-level 15 preempt-cap MAY_PREEMPT preempt-vuln PREEMPTABLE
  cca charging credit preemptively-request
  content-id 320001
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 1000000
 violate-action discard committedDataRate 2000000 committed-burst-size 2000000 exceed-action
 lower-ip-precedence
  nexthop-forwarding-address fa00:965a:c263:25::16/128
  qos-class-identifier 9
  service-identifier 32000
  tft packet-filter pf1
  tft-notify-ue
  tos af11 downlink
rulebase rb1
  cca quota time-duration algorithm parking-meter 1000 content-id 18000
  credit-control-group cg1
  dynamic-rule order first-if-tied
  egcdr threshold volume total 400000
  tcp packets-out-of-order transmit immediately
  action priority 95 timedef ruledef rd6 charging-action ca6 description ruledef
  action priority 96 ruledef rd3 charging-action ca5
  action priority 97 group-of-ruledefs grd3 charging-action ca4 monitoring-key 200000
  action priority 98 static-and-dynamic group-of-ruledefs grd2 charging-action ca2
  action priority 99 dynamic-only ruledef rd1 charging-action ca1 monitoring-key 100000
  action priority 100 dynamic-only group-of-ruledefs grd1 charging-action ca1 monitoring-key
 100000 description gruledefs
  route priority 1 ruledef rd1 analyzer dns description dns
exit
packet-filter pk1
  direction uplink
  ip local-port = 23
  ip protocol = 23
  ip remote-address = 209.165.201.0/27
  ip remote-port = 23
  ip tos-traffic-class = 23 mask = 10
  priority  4
exit
ruledef prepaidBgl
  multi-line-or all-lines
  rule-application charging
  ip any-match = TRUE
  ip server-ip-address range host-pool 12
  ip dst-address = 209.165.201.10
exit
urr-list urrlocal
  rating-group 1 service-identifier 1 urr-id 2
  rating-group 1 service-identifier 3 urr-id 2
exit
exit
```

To verify the group-of-ruledefs configuration details, use the following command.

show running-config

The following is an example of this show command output.

```
show running-config
profile network-element pcf pcf1
rulebase-prefix   rbn
predefined-rule-prefix cbr
!
active-charging service acs1
group-of-ruledefs IPV6-whtlst-https_2300
  add-ruledef priority 1 ruledef IPV6-whtlst-https_2300_01
  add-ruledef priority 2 ruledef IPV6-whtlst-https_2300_02
  add-ruledef priority 3 ruledef IPV6-whtlst-https_2300_03
  add-ruledef priority 4 ruledef IPV6-whtlst-https_2300_04
  add-ruledef priority 5 ruledef IPV6-whtlst-https_2300_05
  add-ruledef priority 6 ruledef IPV6-whtlst-https_2300_06
  add-ruledef priority 7 ruledef IPV6-whtlst-https_2300_07
  add-ruledef priority 8 ruledef IPV6-whtlst-https_2300_08
  add-ruledef priority 9 ruledef IPV6-whtlst-https_2300_09
  add-ruledef priority 10 ruledef IPV6-whtlst-https_2300_10
  add-ruledef priority 11 ruledef IPV6-2dns-whtlst-https_2300_01
  add-ruledef priority 12 ruledef IPV6-2dns-whtlst-https_2300_02
  add-ruledef priority 13 ruledef IPV6-2dns-whtlst-https_2300_03
exit
group-of-ruledefs rdg1
  add-ruledef priority 10 ruledef rd2
  add-ruledef priority 12 ruledef rd1
exit
exit
```

Predefined PCC Rules

Feature Description

Most of the concepts applicable for static rules also apply for predefined rules. The configuration set, mechanism for QoS binding and pre-constructed QoS model remain the same.

Important Predefined PCC Rules are applicable to both 4G and 5G calls.

Predefined Rules vs Static Rules

This section lists the differences between the predefined and static rules.

- Predefined rule is identified by the **dynamic-only** keyword in the action priority associated with a ruledef under rulebase configuration.
- Predefined rules are not activated automatically but are enabled or disabled by PCF on a per rule basis. The PCF sends a PCC rule with the ruledef name alone or ruledef and rulebase names together as the rule ID to activate the predefined rule and sends the PCC rule map with null entry for the ruledef previously activated to deactivate a predefined rule.
- The QoS binding and modelling is not done for predefined rules at the time of configuration unlike the static rule. Instead during PDU session activation/modification the ECS configuration of activated ruledefs are considered to create or change the QoS model applicable for the session.
- On N4 interface, one PDR and corresponding FAR per ruledef activated by the PCF is sent to the UPF with ruledef name in the Activate predefined Rule IE and rulebase name is sent in Rulebase IE in default PDR. On rule removal, the corresponding PDR is removed.

Note The PCF sends the predefined rules, and activates these rules only if the UPF APN is configured with "rulebase" name. Otherwise, the PCF must send the rule name along with the "rulebase" name.

Combined Application of Static, Predefined, and Dynamic Rules

All three static, predefined, and dynamic rules can coexist for a session. In such a case:

- Pre-constructed QoS model is prepared only for static rules. During PDU session activation/modification, any dynamic and predefined rules are evaluated to modify the QoS model and accordingly modifications are done on N1, N2, and N4 interfaces.
- If the rating-group and service ID for a dynamic rule are the same as that of a configured predefined and static rule, then the URR ID for the static and predefined rule is retained even for the dynamic rule.

Bearer QCI Support

Feature Description

The User Plane function (UPF) requires the Bearer level information (BLI) for each QoS flow like QFI for 5G and Bearer Id for 4G, 5G QoS Identifier (5QI) allocation and retention priority (ARP), and Charging ID, to support inline services. The Bearer QCI Support feature facilitates this requirement with the SMF.

Note The Bearer QCI Support feature also includes support for Bli_ID and QFI values in the “Create PDR” message.

The SMF sends the Bearer QoS Class Identifier (QCI) Information Element (IE), which is cisco proprietary IE, in the PFCP session establishment request and PFCP session modification request. The UPF implicitly derives the deletion indication. If a BLI ID is no longer associated with any PDR, the UPF removes it from the PFCP session context. The UPF adds the 5QI or QCI value in the EDR. Currently, the Bearer QCI field is used for 5G to add the 5QI.

The BLI is reported to the UPF as shown in the following table. The formats and encoding and decoding of these IEs are the same as other 3GPP IEs as described in *TS 29.244*.

Information Elements	Mandatory or Optional	Data Type	Description
valid		guint8	Validity of the Bearer level information IE
bli_id	Mandatory	PfcpBliId	QoS flow identifier (QFI) of 5G or Bearer ID (4G)
qci	Optional	PfcpQci	Used by PGW-C, not relevant for SMF
_5qi	Optional	Pfcp5qi	5QI associated with the QoS flow
arp	Mandatory	PfcpArp	ARP comprises of pre-emption capability, Pre-emption vulnerability, and priority level.
charging_id	Optional	PfcpChargingId	Charging ID associated with the QoS flow or Bearer (or both).

Bearer Level Information ID

The unique ID for each Bearer level information sent from SMF. The recommended value of this IE is QFI (in 5G) or Bearer-id (in 4G). The format of IE is as below:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 232 (decimal)							
3 to 4	Length = 1							
5	BLI_ID value							
6 to n+4	These octets are present only if explicitly specified							

QCI: This is not applicable for 5G. It is used in CUPS, if required.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 233 (decimal)							
3 to 4	Length = 1							
5	QCI value							
6 to n+4	These octets are present only if explicitly specified							

5QI: The SMF uses this IE to send the 5QI value.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 234 (decimal)							
3 to 4	Length = 1							
5	5QI value							
6 to n+4	These octets are present only if explicitly specified							

ARP: The ARP value is sent with this IE.

Note From SMF, the ARP value is encoded as arp->pci)<<4) | arp->pl)<<2)| arp->pvi)

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 235 (decimal)							
3 to 4	Length = 1							
5	ARP value							

6 to n+4	These octets are present only if explicitly specified

Charging ID: The Charging IE is sent with this IE.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 236 (decimal)							
3 to 4	Length = 1							
5	Charging Id value							
6 to n+4	These octets are present only if explicitly specified							

Triggers for Bearer Level Information IE

The following are the triggers for sending the BLI IE in PFCP messages:

PFCP Session Establishment Message

The Bearer level information IE is sent for each new QoS flow with the unique QFI ID. This IE is added in the policy decision in the N7 Policy Control Create Response message from the PCF. Therefore, SMF sends multiple instances of this IE, in a single PFCP message.

PFCP Session Modification Message:

Any new QoS flow addition or new PCC rule referring to an existing QoS flow that results in a new QER or PDR IE that has a new Bearer level information IE for each unique QFI ID.

The BLI IE is not included in the PFCP Session Modification Message if the modification is for IDFT tunnels.

Non-standard QCI Support for Dynamic PCC and Session Rules

Feature Description

The SMF supports non-standard QCI values in dynamic PCC and session rules along with the standard QCI values.

Non-standard QCIs are the values from 1 through 255 and that are not part of standard QCI values as defined in section 6.1.7.2 of 3GPP 23.203 specification.

The SMF supports non-standard QCI for DSCP marking of the data packets for the session.

Important SMF does not support CLI-based configuration of non-standard QCI values for static and predefined rules. When the PCF sends the session rule with a non-standard QCI, then the SMF reserves the non-standard QCI value for the static and predefined rules that belong to the default flow.

How it Works

The SMF receives the non-standard and standard QCIs in QoS from PCF through SmPolicyCreateResponse, SmPolicyUpdateResponse, or SmPolicyUpdateNotify message.

If the PCF does not send the session rule information or if the PCF sends an invalid QCI value, the SMF uses the UDM-provided non-standard QCI value and processes the QCI information in the same manner as sent by PCF. If neither PCF nor UDM sends the non-standard QCI information, the SMF uses the QCI information locally configured within QoS profile. For configuration details, see the Configuring QoS Parameters, on page 39 section.

When the PCF sends a PCC rule with a non-standard QCI, the SMF creates a GBR flow if the (UL and DL) GBR QoS information is available in the associated QoS-Descriptor. Otherwise, the SMF creates a non-GBR flow.

For the default session rule, the SMF assumes it as a non-GBR flow irrespective of the non-standard QCI information it receives from PCF.

The SMF initiates the session establishment or modification procedure towards RAN or UE, and communicates the same QCI information on N1, N2, N4, and S5 interfaces.

Note The SMF does not handle the QoS Characteristics sent by PCF for a non-standard QCI.

If a discrepancy or an ambiguity arises in the QCI input from PCF, the SMF performs the following validations:

- The SMF checks if the QCI value is ranging from 1 through 255. The SMF does not handle any non-standard QCI value that does not fall within the specified range.
- When the PCF sends session rule and PCC rule with the same binding parameters and non-standard QCI along with GBR UL and DL information as shown in the following example, the SMF rejects the “PccRule1” PCC rule.

```
sessRule1=>AuthDefQos{arp1, qci128}+ authSessAmbr{UL=20mbps,DL=20mbps}

PccRule1=>QosDesc{arp1, qci128, gbrUL=10mbps, gbrDL=10mbps}
```

Limitations

The Non-standard QCI Support feature has the following limitations:

- The SMF assumes session rule flow as non-GBR flow for a non-standard QCI.
- The SMF does not handle the QoS Characteristics sent by PCF for a non-standard QCI.

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The SMF uses the existing policy statistics for non-standard QCIs. The QCI label which displays standard QCI value displays the non-standard QCI value too.

Troubleshooting Information

To view the flow information associated with the non-standard QCI values, use the same **show subscriber 5qi** CLI command as used for the standard QCI values.

Use the existing **clear subscriber 5qi** CLI command to delete the flows with non-standard QCI values as well.

Support for Configuring the Bandwidth ID

Feature Description

The SMF expects the user to configure the bandwidth limitation, for both downlink and uplink packets, in all charging actions, even if the bandwidth limitation configuration is the same for all the charging actions.

To optimise these configurations, the SMF allows the user to define a bandwidth ID to include all bandwidth related configurations and associate the bandwidth ID under the charging actions.

If the bandwidth value is changed, the new subscribers use the configured bandwidth values while the existing subscribers continue to use the old values.

Limitations

The SMF imposes the following limitations related to the configuration of bandwidth-policy.

- Allows up to 64 k flow ID configurations within the bandwidth-policy
- Allows configuring up to a maximum of 64 bandwidth policies
- The maximum number of groups that can be configured per bandwidth policy is 1000.
- The maximum number of bandwidth IDs that can be configured per bandwidth policy is 1000.

Configuring Bandwidth ID

To define the bandwidth ID within the charging action, use the following sample configuration.

```
config
   active-charging service service_name
      bandwidth-policy policy_name
      flow limit-for-bandwidth id bandwidth_id group-id group_id
      group-id group_id direction { downlink | uplink }
      peak-data-rate peak_data_rate peak-burst-size
      peak_burst_size violate-action { discard | lower-ip-precedence }
      [ committed-data-rate committed_data_rate committed-burst-size
      committed_burst_size [ exceed-action { discard | lower-ip-precedence
      } ] ]
      exit
   active-charging service service_name
   charging-action charging_action_name
```

```
flow limit-for-bandwidth bandwidth_id
end
```

- **bandwidth-policy** *policy_name*: Specify the name of the bandwidth policy. This CLI option allows configuring up to a maximum of 64 bandwidth policies.
- **flow limit-for-bandwidth id** *bandwidth_id*: Define a bandwidth ID to include all the bandwidth related configurations within the charging action for predefined and static rules.

  bandwidth_id must be an integer in the range of 1–65535.

Note The maximum number of bandwidth IDs that can be configured per bandwidth policy is 1000.

- If the bandwidth ID is configured and the individual uplink and downlink limit-for-bandwidth are also configured in the charging actions, then the bandwidth ID configuration takes the precedence.
- **group-id** *group_id*: Specify the group ID. *group_id* must be an integer in the range of 1– 65535.

  The group ID identifies the QoS parameters, such as MBR and GBR. Each group ID is mapped to a particular bandwidth ID.
- The maximum number of groups that can be configured per bandwidth policy is 1000.

Verifying Bandwidth ID Configuration

To verify the bandwidth ID configuration, use the following show command:

```
show config
```

This show command helps in identifying any invalid configurations such as the configured bandwidth ID being removed but still defined in the charging action. For such invalid configurations, this show command displays appropriate errors as shown in the following example output:

```
ERROR COMPONENT      ERROR DESCRIPTION
------------------------------------------------------------------------------------------
RuleBase        Default bandwidth policy does not exist in rulebase <rba1> for charging
action <ca1> .Dropping ruleDef <rda1>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda60>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda61>
ChargingAction  Packet filter <pkt1234> configured for charging action <ca4> associated
with rulebase <rb1> does not exist
BandWidthPolicy Uplink peak data rate less than commited data rate in charging action
<ca6>Dropping ruleDef <rd6>
```

Generating UE Camping Report for PCF

Feature Description

PCF needs to be aware of UE location, RAT type, access type, and other details to provision relevant policies during the PDU session life cycle. To facilitate this, during PCF initiated policy update procedure, the SMF sends "UeCampingRep" attribute in the response message based on the triggers enabled by PCF.

The SMF sends the UeCampingRep to PCF as per the Table 5.5.2.2-2 defined in 3GPP specification 29.512. When validation of all the PCF provided rules succeed, the SMF sends the UeCampingRep in the update response message to the PCF.

If validation of any of the rules fail, then the SMF sends the ueCampingRep in “PartialSuccessReport” as defined in 4.2.3.2 section of 3GPP specification 29.512.

The fields in the "UeCampingRep" IE are populated based on the following triggers set by PCF.

- Access type (AC_TY_CH)
- RAT change (RAT_TY_CH)
- User location change (SAREA_CH)
- PLMN Change (PLMN_CH)

The SMF supports the following attributes:

- accessType
- ratType
- servingNetwork
- userLocationInfo

Important The SMF currently does not support the ueTimeZone attribute.

UPF Node Selection

The UPF Selection feature enables the 5GS and EPS core networks to select an UPF for reduced latency on user plane and priority-based serviceability.

The SMF selects an appropriate UPF during the setup of a PDU session. The UPF selection depends on the following query parameters:

- DNN
- Subscriber location
- Network slice information

- PDU session type
- PDU subscription type
- Priority
- Load
- Dual Connectivity with New Radio (DCNR)

When multiple UPFs meet the UPF selection criteria, UPF selection is based on priority and load. For the load metric information, the SMF fetches the Packet Forwarding Control Protocol (PFCP) IE from UPF over N4 interface. If the failure handling support exists and N4 Session Establishment fails, the SMF selects the next least-loaded UPF.

The network operator leverages this functionality for efficient handling of the user plane traffic based on priority, PDU session type, and so on. This functionality is also used for effective load balancing of the user plane connections across multiple UPFs.

In scenarios where multiple UPFs are available for a particular Subscription Permanent Identifier (SUPI), SMF provides the capability to configure multiple UP addresses for each SUPI. The SMF performs UPF selection for a particular PDU session based on the SUPI preferred configuration. For configuration details, see the Configuring UPF Address, on page 98 section.

That is, the SMF checks if any of the configured SUPI values match the current SUPI. If the match is successful, SMF uses information on the available user plane nodes and checks if the IP address matches with any of the values configured for the SUPI. The SMF performs the following validations for UPF selection:

- Check if the UP node is valid and active
- Check if the location-based DNN or the DNN received from service is available in the list of supported DNNs in UP node
- Check if the PDU session type is supported for the configured user plane. For this validation, SMF fetches the UP profile name and UPF group configured within network profile UPF. Then, SMF checks if the UPF group is empty or if the group has the PDU session type that is available in the supported PDU session types.

When all the validations are successful, the SMF skips the existing UPF selection logic involving the query parameters and uses the UPF selected by SUPI. In cases where UPF address is not configured for the SUPI or if the preceding validation checks fail, the SMF uses the default UPF selection mechanism. For co-located UPF selection, the cnSGW-C configuration remains the same as on the SMF.

UPF Selection Based on Query Parameters

This section describes how the SMF selects the UPF based on certain selection parameters.

Feature Description

The SMF selects UPF from a list of all active UPFs based on the predefined query parameters.

The 5GS and EPS core networks apply the selection mechanism to select a UPF node during the creation of a subscriber session.

When the UPF selection is based on the load of the UPFs, the SMF distributes calls among active UPFs associated with SMF. 3GPP specifies Load Control feature as optional feature over N4 reference points. This functionality enables UPF to send its load information to CP functions.

To support load-based UPF selection, the SMF uses UPF-provided Load Control information in the following Packet Forwarding Control Protocol (PFCP) messages:

- Session Establishment Response
- Session Modification Response
- Session Deletion Response
- Session Report Request

Load Control procedure details are available in *section 6.2.3* of *3GPP TS 29.244, Release 14*. The SMF adheres to the CP functionality.

How it Works

The UPF initiates an N4 Association Setup request to set up an association with SMF.

The following is a high-level summary of how SMF selects the UPF node for the core network:

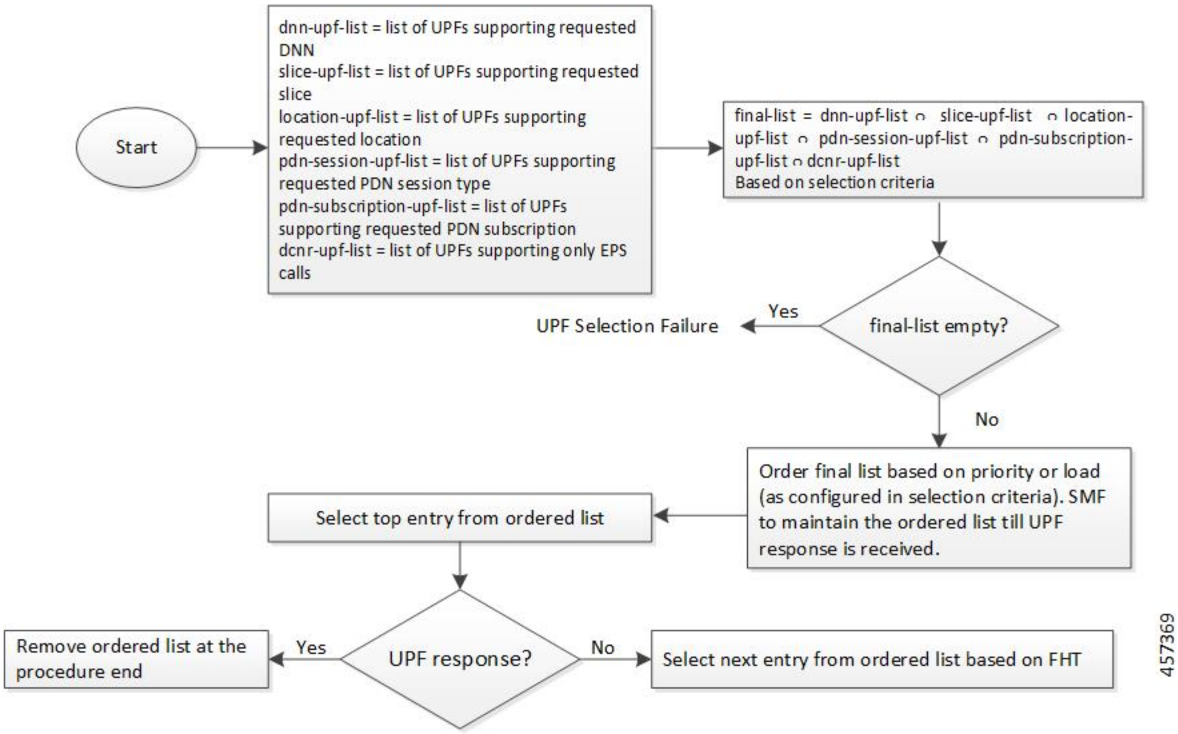
- The SMF selects the UPF node for EPS and 5GS sessions based on the UPF selection policy configured under DNN profile configuration. The UPF selection policy defines a combination of the following parameters:
    - DNN
    - Network slice
    - Subscriber location
    - DCNR (only for EPS calls)
    - PDN/PDU subscription type
    - PDN/PDU session type
- If the UPF selection policy is not defined under DNN profile configuration, then SMF selects the UPF based on the derived location DNN or requested DNN
- The SMF enables you to define the UPF selection criteria which it uses to query the appropriate node.
- If multiple UPFs match the selection criteria, then SMF selects the active UPFs and sorts them based on their priority and load information. The SMF then attempts to access the UPF one by one until the N4 Session Establishment is successful.
- The SMF stores the load information provided by UPF and uses it in selecting the UPF for the new sessions. The SMF selects the less loaded UPF among the candidate (DNN-based) active UPFs.
- The SMF considers priority and capacity configured statically against each UPF. In cases where UPF does not send the load information statically, the SMF uses the configured capacity to select the UPFs.
- The SMF selects the UPF which is given more priority in a particular location. Both the UPF priority and UPF group priority are used to determine the final priority of UPF. For information on configuring the UPF group priority, see the Assign Priority for UPF Group, on page 96 section.

UPF Selection Algorithm

The SMF determines the UPF node based on an algorithm.

The following figure depicts the UPF node selection workflow.

Figure 17: UPF Node Selection Workflow


Start
dnn-upf-list = list of UPFs supporting requested DNN
slice-upf-list = list of UPFs supporting requested slice
location-upf-list = list of UPFs supporting requested location
pdn-session-upf-list = list of UPFs supporting requested PDN session type
pdn-subscription-upf-list = list of UPFs supporting requested PDN subscription
dcnr-upf-list = list of UPFs supporting only EPS calls
final-list = dnn-upf-list ∩ slice-upf-list ∩ location-upf-list ∩ pdn-session-upf-list ∩ pdn-subscription-upf-list ∩ dcnr-upf-list
Based on selection criteria
final-list empty?
Yes
UPF Selection Failure
No
Order final list based on priority or load (as configured in selection criteria). SMF to maintain the ordered list till UPF response is received.
Select top entry from ordered list
UPF response?
Yes
Remove ordered list at the procedure end
No
Select next entry from ordered list based on FHT
457369

The SMF lists the UPF nodes based on the priority assigned to the node. When there are multiple nodes with the same priority value, then the SMF selects a UPF experiencing the lowest level of load. The load parameter is applied only for UPFs that have the same priority.

When load is not available as a selection criteria, then SMF selects a random UPF when there are multiple UPFs with the same priority.

The SMF stores UPF order list based on priority. When a failure occurs, the SMF selects the next entry in the list based on failure handling template (FHT) configuration.

If priority is not available as a selection criteria and load is available as a selection criteria, then SMF selects least loaded UPF from the list of selected UPFs.

Important The SMF performs UPF selection during initial call establishment and handover procedure.

When the subscriber location is used as the UPF selection parameter, the SMF uses the priorities that are set for the UPF and the UPF group to choose the best suitable UPF.

The following is an example to understand the UPF selection logic.

Assume two UPF groups and two UPFs with the following configurations.

- UPF groups:

        - UpfGrp1:
            - Location Area Group List:TAI1
            - Slice list
            - PDN type list
        - UpfGrp2:
            - Location Area Group List:TAI2
            - Slice list
            - PDN type list
    - UPFs
        - Upf1:
            - Priority: 500
            - Capacity: 1000
            - Upf Grp List: ((UpfGrp1, priority: 10), (UpfGrp2, priority: 30))
        - Upf2:
            - Priority: 500
            - Capacity: 1000
            - Upf Grp List: ((UpfGrp1, priority: 20), (UpfGrp2, priority: 5))

A combination of UPF group priority and UPF priority is used for selecting the UPF having more preference (less priority) in a particular location.

The SMF selects upf1 for location TAI1 as upf1 is with less priority. Similarly, upf2 is selected for TAI2 based on the UPF priority and UPF group priority.

The SMF also provides the capability to configure DNN profile based on UE location, that is, TAI or ECGI. The location-based DNN profile allows mapping of location area group with DNN profile where location area group specifies the TAI or ECGI group.

For TAI-based UPF selection, it is mandatory to first select the DNN profile based on the UE location through location-dnn-profile configuration. Then, use the UPF selection policy (for example, DNN and slice selection criteria) defined in the selected DNN profile.

For configuration details, see the Select Location-based DNN Profile, on page 96 section.

Standards Compliance

The Load-based UPF Selection feature complies with the following standard:

- *3GPP TS 29.244 Release 14 – LTE; Interface between the Control plane Plane and the User Plane of EPC Nodes*

Limitations

The Load-based UPF Selection feature has the following limitation:

- Post nodemgr POD restart, UPF association must be re-established for subsequent PDU session establishments to be successful.

Configuring the UPF Selection Feature

This section describes how to configure the UPF Selection feature.

The UPF selection depends on the query parameter. Use the following configurations based on the selected query parameter.

- Creating the ECGI Group Profile for EPS Session, on page 89
- Creating the NCGI Group Profile for 5GS Session, on page 90
- Configuring Tracking Area Identity Group, on page 91
- Creating the Location-Area-Group Profile, on page 92
- Defining the UPF Group, on page 92
- Associating the UPF Group with UPF Network Element, on page 93
- Defining UPF Selection Query Parameters, on page 94
- Associating UPF Selection Query Parameters with DNN Profile, on page 95
- Configuring UPF Address, on page 98

Creating the ECGI Group Profile for EPS Session

This section describes how to create an instance of the ECGI Group Profile.

The ECGI Group Profile allows you to configure the list of individual ECGI values and ranges.

To create an ECGI-Group, use the following sample configuration.

```
config
   profile ecgi-group profile_name
      mcc mcc_value mnc mnc_value
      ecgi list [ ecgi_value1 ecgi_value2 ecgi_valueN ]
      ecgi range start start_value end end_value
      end
```

NOTES:

- **profile ecgi-group** *profile_name*: Specify the name of the ECGI Group Profile to enter the profile configuration. The ECGI Group Profile supports a maximum number of 16 PLMNs.
- **mcc** *mcc_value* **mnc** *mnc_value*: Specify the MCC and MNC values.
- **ecgi list [** *ecgi_value1 ecgi_value2 ecgi_valueN* **]**: Specify the list of ECGI values to be configured. The accepted value is the 7-digit hex string E-UTRAN Cell ID. The SMF supports a maximum number of 64 ECGI values under a PLMN.
- **ecgi range start** *start_value* **end** *end_value*: Specify the start and end range values of ECGI. The accepted start and end range of ECGI is the 7-digit hex string E-UTRAN Cell ID. **ecgi range** is an optional

attribute. You can configure multiple ECGI range values. The SMF supports a maximum number of 64 ECGI ranges under a PLMN.

Important The SMF ignores the ECGI range values if the start range value is greater than the end range value.

Verifying the ECGI-Group Profile Creation

This section describes how to verify if the ECGI-Group Profile is created.

The following configuration is a sample output of the **show running-config profile ecgi-group** command:

```
profile ecgi-group e1
mcc 123 mnc 45
  ecgi list [ 1234567 abcdef0 ]
  ecgi range start 1111111 end fffffff
  exit
exit
exit
```

Creating the NCGI Group Profile for 5GS Session

This section describes how to create an instance of the NCGI Group Profile.

The NCGI Group Profile allows you to configure the list of individual NCGI values and range.

To create an NCGI group, use the following sample configuration.

```
config
   profile ncgi-group profile_name
      mcc mcc_value mnc mnc_value
      ncgi list [ ncgi_value1 ncgi_value2 ncgi_valueN ]
      ncgi range start start_value end end_value
      end
```

NOTES:

- **profile ncgi-group** *profile_name*: Specify the name of the NCGI Group Profile to enter the profile configuration. The NCGI Group Profile supports a maximum number of 16 PLMNs.
- **mcc** *mcc_value* **mnc** *mnc_value*: Specify the MCC and MNC values.
- **ncgi list [** *ncgi_value1 ncgi_value2 ncgi_valueN* **]**: Configure the list of NCGI values to be configured. The accepted value is the 9-digit hex string NR Cell ID. The SMF supports a maximum number of 64 NCGI values under a PLMN.
- **ncgi range start** *start_value* **end** *end_value*: Configure a specific NCGI range or multiple NCGI range lists. The accepted start and end range is the 9-digit hex string NR Cell ID. **ncgi range** is an optional attribute. You can configure multiple NCGI range values. The SMF supports a maximum number of 64 NCGI ranges under a PLMN.

Important The SMF ignores the NCGI range values if the start range value is greater than the end range value.

Verifying the NCGI-Group Profile Creation

This section describes how to verify if the NCGI-Group Profile is created.

The following configuration is a sample output of the **show running-config profile ncgi-group** command:

```
profile ncgi-group n1
mcc 123 mnc 45
  ncgi list [ 123456789 12ab34CD9 ]
  ncgi range start 111111111 end FFFFFFFFF
  exit
exit
exit
```

Configuring Tracking Area Identity Group

The SMF provides configuration to define the supported list of Tracking Areas and Tracking Area Ranges for a PLMN. Upon enabling this configuration, the SMF sends the configured Tracking Area Identity (TAI) to the NRF during the SMF Service Registration.

To define multiple TAI groups with different names, use the following sample configuration.

```
config
   profile tai-group tai_group_name
      mcc mcc mnc mnc
      tac list [ tac_value1 tac_value2 tac_valueN ]
      tac range start tac_start_value end tac_end_value
      end
```

NOTES:

- **profile tai-group** *tai_group_name*: Specify the name of the TAI Group to enter the profile configuration.
- **mcc** *mcc_value*: Specify the mobile country code.
- **mnc** *mnc_value*: Specify the mobile network code.
- **tac list [** *tac_value1 tac_value2 tac_valueN* **]**: This keyword allows you to configure—
    - multiple PLMNs and TAC values within the specified TAI group
    - a maximum number of 16 PLMNs within the specified TAI group
    - a maximum number of 64 TAC values under a PLMN
- **tac range start** *tac_start_value* **end** *tac_end_value*: This keyword allows you to configure—
    - multiple TAC range values
    - a maximum number of 64 TAC ranges under a PLMN

Important The SMF ignores TAC range values if the start range value is greater than the end range value.

- The SMF derives TAC list and TAC range from TAI group or NCGI group configuration. If the NCGI list already includes a TAC, you can skip the TAC configuration under TAI group. However, if the TAC is associated to a different UPF, this behavior is not applicable.

Creating the Location-Area-Group Profile

The SMF associates one or more serving location details to a peer UPF. Location details include individual tracking areas and/or a range of tracking areas along with optional supported cells details.

To create an instance of the location area group profile which is added under the ecgi-group and ncgi-group, use the following sample configuration.

```
config
   profile location-area-group profile_name
      tai-group tai_group_name
      ecgi-group ecgi_group_name
      ncgi-group ncgi_group_name
      end
```

NOTES:

- **profile location-area-group** *profile_name* : Specify the name of the location area group to enter the profile configuration.
- **tai-group** *group_name*: Specify the name of the TAI group.
- **ecgi-group** *group_name*: Specify the name of the ECGI group. This configuration is optional.
- **ncgi-group** *group_name*: Specify the name of the NCGI group. This configuration is optional.

Verifying the Location-Area-Group Profile Creation

This section describes how to verify if the Location-Area-Group Profile is created.

The following configuration is a sample output of the **show running-config profile location-area-group** command:

```
profile location-area-group la1
tai-group  t1
ecgi-group e1
ncgi-group n1
exit
```

Defining the UPF Group

This section describes how to configure the UPF group, and define pdn-session-type, slice-group and other parameters for the UPF group profile.

To define the UPF group profile, use the following sample configuration.

```
config
  profile upf-group upfgroup_name
    pdn-session-type [ ipv4 | ipv4v6 | ipv6 ]
    dcnr { false | true }
    slice-group-list [ slice1 slice2 sliceN ]
    location-area-group-list [ la1 la2 laN ]
    end
```

NOTES:

- **profile upf-group** *upfgroup_name*: Specify a name for the UPF group that must be associated to the specified UPF network configuration.

- **pdn-session-type [ipv4 | ipv4v6 | ipv4v6]**: Configure the PDN session type that is supported by UPF. The query parameters for pdn-session-type accept the "pdn-type-subscription" and "pdn-type-session". This parameter selects the pdn-type from UDM returned subscription or UE session, respectively.

Note If both "pdn-type-subscription" and "pdn-type-session" parameters are configured, SMF considers "pdn-type-subscription".

The SMF provides this CLI option to associate the UPF to servicing different PDN session types, such as IPv4, IPv6, and IPv4v6. An UPF serves more than one PDN session type.

- **slice-group-list [** *slice1 slice2 sliceN* **]**: Specify the configured Network Slice Selection Assistance Information (NSSAI) list. The slice value must be the same as the allowedNssai under smf-profiles. The slice group contains both the NSSAI and DNN information. When fetching the NSSAI UPF list, consider the DNN list that is configured under the slice group. The existing dnn-list under the network-element is not moved to the upf-profile group.
- **dcnr { true | false }**: Configure the Dual Connectivity with New Radio (DCNR) capability. The default configuration is false.

Note The DCNR capability is applicable only for 4G calls.

- **location-area-group-list [** *la1 la2 laN* **]**: Configure the list of location area groups with different names.

Verifying the UPF Group Profile Configuration

This section describes how to verify if the UPF Group Profile is configured.

The following configuration is a sample output of the **show running-config profile upf-group** *upfgroup_name* command:

```
profile upf-group ug1
pdn-session-type ipv4v6
slice-group-list [ slice1 ]
location-area-group-list [ loc1 ]
dcnr true
exit
```

Associating the UPF Group with UPF Network Element

To associate the defined UPF group with the UPF network element, use the following sample configuration.

The UPF profile contains a list of UPFs configured in the SMF.

```
config
  profile network-element upf upf_name
    upf-group-profile upfgroup_name
    capacity service_capacity
    priority priority_value
    dnn-list dnn_list
    end
```

NOTES:

- **profile network-element upf** *upf_name*: Configure the UPF network configuration to which the defined UPF group is associated.
- **upf-group-profile** *upf_group*: Configure the UPF group name that must be associated to the specified UPF network configuration.
- **capacity** *service_capacity*: Configure the static weight relative to other UPFs of the same type. *server_capacity* must be an integer in the range of 0–65535. Default: 10.
- **priority** *priority_value*: Configure the static priority relative to other UPFs of the same type. *priority_value* must be an integer in the range of 0–65535. Default: 1.
- **dnn-list** *dnn_list*: Specify the list of location DNNs or DNNs supported by the UPF node.

Verifying the UPF Configuration

This section describes how to verify the UPF configuration and the association of UPF group with UPF network element.

The following configuration is a sample output of the **show configuration** command:

```
profile network-element nrf nrf1
http-endpoint base-url http://209.165.200.253:8082
…
profile network-element upf upf2
upf-group-profile ug1
capacity 10
priority 1
n4-peer-address ipv4 209.165.200.234
n4-peer-port 8805
keepalive 60
dnn-list [ dnn1 intershat cisco.com ]
…
```

Defining UPF Selection Query Parameters

This section describes how to configure parameters that enable SMF to select the UPF using the selection query.

To define the UPF selection policy-specific configuration, use the following sample configuration.

```
config
   policy upf-selection upfpolicy_name
      precedence priority_value [ dcnr | dnn | location | pdn-type-session |
 pdn-type-subscription | slice ]
      end
```

NOTES:

- **policy upf-selection** *upfpolicy_name*: Specify the UPF policy name that must be associated with the DNN profile.

  The SMF selects the UPF node with the lowest precedence value. The SMF selects the node with the highest precedence selection-criteria when the previous lower precedence criteria did not return any UPF. If the configured criteria are exhausted, and nodes are not selected, then the UPF selection policy fails.

  Within the precedence value, the intersection of UPFs from each criterion is performed to retrieve the UPF list.

- **precedence** *priority_value* **[dcnr | dnn | location | pdn-type-subscription | pdn-type-session | slice]**: Assign the precedence value to the UPF policy. Specify the DNN and other parameters for the UPF selection.

  The **precedence** keyword allows a maximum of four precedence values to be configured under the UPF selection policy.

  If the DNN profile does not have any UPF selection policy associated with it, then the SMF performs UPF selection using location DNN or DNN, priority, and load information.

Verifying the UPF Selection Policy Configuration

This section describes how to verify if the UPF selection policy is configured.

The following configuration is a sample output of the **show running-config policy upf-selection** command:

```
#show running-config policy upf-selection
policy upf-selection polUpf1
   precedence 1
         [dnn location pdn-type-subscription]
   exit
   precedence 2
         [dnn pdn-type-session slice]
   exit
   precedence 3
          [dnn]
   exit
exit
```

Associating UPF Selection Query Parameters with DNN Profile

This section describes how to associate UPF selection query parameters with DNN profile.

To associate the UPF selection policy with DNN profile, use the following configuration:

```
config
   profile dnn profile_name
      upf-selection-policy upfpolicy_name
      end
```

NOTES:

- **profile dnn** *profile_name*: Specifies the DNN profile name. *profile_name* must be an alphanumeric string.
- **upf-selection-policy** *upfpolicy_name*: Specifies the name of UPF selection policy that must be associated to the DNN profile.

Verifying the Association of UPF Selection Policy and DNN Profile

This section describes how to verify if the UPF selection policy association with the DNN profile is established.

The following configuration is a sample output of the **show running-config profile dnn** *profile_name* command:

```
profile dnn intershat
upf-selection-policy upfPol1
end
```

Assign Priority for UPF Group

This section describes how to configure the UPF group list and assign priority for the UPF group.

The UPF group lists the set of locations, slices, and so on. Each UPF present in the group is given a priority which decides the final priority of that UPF.

To assign the UPF group priority, use the following sample configuration.

```
config
  profile network-element upf upf_profile_name
    upf-group-profile-list upf_group_name
      priority priority_value
      end
```

NOTES:

- **upf-group-profile-list** *group_name*: Specify the UPF group profile name.
- **priority** *priority_value*: Assign priority to the UPF group.

  The UPF group priority is used in scenarios where there are two or more UPFs with the same location (TAI).

Configuration Verification

To verify the feature configuration, use the **show running-config profile network-element upf** command.

The following is an example output of the **show running-config profile network-element upf** command.

```
[smf] smf# show running-config profile network-element upf
profile network-element upf upf1
 n4-peer-address ipv4 209.165.200.231
 n4-peer-port 8805
 dnn-list     [ intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
 intershat7 intershat_hrt intershatipex ]
 capacity     65535
 priority     65535
 upf-group-profile-list group1 priority 10
 upf-group-profile-list group2 priority 20
exit
```

In the preceding output, check the lines **upf-group-profile-list group1 priority 10** and **upf-group-profile-list group2 priority 20** to view the UPF group configurations and the UPF group priorities.

To view all the configured UPF groups, use the **show running-config profile upf-group** command.

The following is an example output of the **show running-config profile upf-group** command.

```
[smf] smf# show running-config profile upf-group
profile upf-group group1
 failure-profile FH1
exit
profile upf-group group2
 failure-profile FH2
exit
```

Select Location-based DNN Profile

The DNN policy can have a DNN profile configuration based on UE location for each UE-requested DNN. The DNN profile has a virtual or mapped DNN with its list of interfaces.

To configure location-based DNN profile, use the following sample configuration:

```
config
   policy dnn dnn_policy_name
      dnn dnn_name location-dnn-profile location_dnn_profile_name
      end
```

NOTES:

- **dnn** *dnn_name* **location-dnn-profile** *location_dnn_profile_name*: Specify the name of DNN profile that is defined based on the UE location.

  This configuration maps the UE-requested DNN with the location-based DNN profile in DNN policy.

Associate Location Area Group and DNN Profile

To associate location area group and location-based DNN profile, use the following sample configuration:

```
config
   profile location-dnn location_dnn_profile_name
      location-area-group lag_name profile dnn_profile_name
      end
```

NOTES:

- **profile location-dnn** *location_dnn_profile_name*: Specify the name of the configured DNN profile.
- **location-area-group** *lag_name* **profile** *dnn_profile_name*: Specify the name of a location area group and DNN profile.

  This configuration maps the location area group with the DNN profile.

Configuration Example

The following is an example configuration.

```
config
 policy dnn polDnn
  profile default-profile
  dnn ims location-dnn-profile loc1
  exit
  profile location-dnn loc1
   location-area-group lag1 profile dnnprof-imslag1
   location-area-group lag2 profile dnnprof-imslag2
   exit
  profile location-area-group lag1
   tai-group tai1
   ecgi-group ecgi1
   exit
  profile location-area-group lag2
   tai-group tai2
   ecgi-group ecgi2
   exit
  profile tai-group tai1
   mcc 123 mnc 456
   tac range start 4455 end 5566
   exit
  profile tai-group tai2
   mcc 123 mnc 456
   tac range start 3355 end 3366
   exit
  exit
  profile ecgi-group ecgi1
   mcc 123 mnc 456
   ecgi range start A123451 end A234567
   exit
  exit
  profile ecgi-group ecgi2
   mcc 123 mnc 456
   ecgi range start B123451 end B234567
   exit
  exit
  profile location-dnn loc1
   location-area-group lag1 profile dnnprof-imslag1
   location-area-group lag2 profile dnnprof-imslag2
   exit
  profile dnn dnnprof-imslag1
   dns primary ipv4 209.165.201.10
   dns primary ipv6 fd00:976a::9
   dns secondary ipv4 209.165.201.12
   dns secondary ipv6 fd00:976a::10
   dnn imslag1 network-function-list [ upf ]
   dnn rmgr imslag1
   upf-selection-policy       upfsecpol1
   timeout up-idle 3600 cp-idle 7320
   pcscf-profile pcscf1
   session type IPV4V6
   upf apn ims
   dcnr true
   userplane-inactivity-timer 3600
   exit
  profile dnn dnnprof-imslag2
   dns primary ipv4 209.165.201.13
   dns primary ipv6 fd00:976a::9
   dns secondary ipv4 209.165.201.14
   dns secondary ipv6 fd00:976a::10
   dnn imslag2 network-function-list [ upf ]
   dnn rmgr imslag2
   upf-selection-policy       upfsecpol2
   timeout up-idle 3600 cp-idle 7320
   pcscf-profile pcscf1
   session type IPV4V6
   upf apn ims
   dcnr true
   userplane-inactivity-timer 3600
   exit
  exit
 exit
exit
```

In the preceding example, the name of the configured DNN is "ims", location-dnn-profile is “loc1”, location-area-group is "lag1" and "lag2", and the dnn-profile is "dnnprof-imslag1" and "dnnprof-imslag2".

SMF selects location-dnn-profile “loc1” for the “ims” DNN received in PDU session request. The loc1 profile maps location-area-group to the dnn-profile. The SMF uses TAI and ECGI information from PDU session request to find the configured location-area-group "lag1". Then, the corresponding dnn-profile "dnnprof-imslag1" is selected.

After the "dnnprof-imslag1" dnn profile is selected, the SMF selects a suitable UPF based on the selection criteria that are specified in the UPF selection policy.

Configuring UPF Address

This section describes how to configure SUPI and UPF node information.

To configure the SUPI value and UPF addresses, use the following sample configuration:

```
config
   system-diagnostics supi supi_value
      preferred-up node-id upf_address
      end
```

NOTES:

- **system-diagnostics supi** *supi_value*: Specify the SUPI value or a list of SUPI values separated by comma. *supi_value* must be a string of 15 digits.
- **preferred-up node-id** *upf_address*: Specify the UPF addresses, separated by comma, for the configured SUPI. *upf_address* must be a string in the IPv4 address pattern.

  When multiple UPFs are configured for a SUPI, the SMF performs UPF selection for a particular PDU session based on the SUPI preferred configuration.

Configuration Verification

To verify the configuration, use the **show running-config system-diagnostics supi** command.

The following is an example output of the show command.

```
[smf] smf# show running-config system-diagnostics supi
system-diagnostics supi [ 123456789012345 ]
 preferred-up node-id [ 209.165.200.230 209.165.200.236 ]
exit
```

UPF Selection OA&M Support

This section describes operations, administration, and maintenance information for this feature.

Statistics

The following statistics are added in support of UPF node selection based on DNN, pdn-type-session, network slice, priority, and load.

- upf-selector

  req_type="upf-selector",

  status="Precedence:2 Dnn-Upf-List:3 Pdn-Type-Upf-List:2 Slice-Upf-List:2 Dcnr-Upf-List:0"

  status="upf_selector_empty_upf_list"

  status="upf_selector_invalid_upf_selection_policy"

  Example:

```
smf_service_resource_mgmt_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat",emergency_call="",instance_id="0",ip_req_type
="upf-selector",pdu_type="ipv4",procedure_type="PDU Session Establishment",
rat_type="NR", service_name="smf-service", status="Precedence:2 Dnn-Upf-List:3
 Pdn-Type-Upf-List:2 Slice-Upf-List:2 Dcnr-Upf-List:0"} 1
```

IP Threshold-based UPF Selection

Feature Description

This feature addresses the load balancing across overloaded UPFs. Each IP pool has existing usable threshold configuration. This configuration allows to mention percentage of IP addresses to be considered as a threshold hit for a given UPF. IPAM informs SMF when a threshold is hit for a particular DNN for a UPF, SMF gives lower priority to such UPF until UPF hits threshold condition.

Use Cases

UPFs serving same DNN and have different priority consume IP addresses unevenly, in such cases particular UPF may run out of IP addresses quickly and hit a threshold. In such cases SMF will first give preference to UPFs which have't hit the threshold while assigning new sessions.

Due to nonlinear activities in field, it is possible that initial session distribution by SMF to UPF is uniform. In the subsequent sessions, one particular UPF may stay longer and another UPF cleared, in such cases new sessions continue to distribute based on priority the UPF. On the calls which stay longer may hit a threshold and it may happen that UPF may run out of IP addresses. To cater such situation the UPF's threshold is given less priority.

How it Works

This section describes how IP Threshold SMF and IPAM Integration works.

Intimation of a threshold hit condition from IPAM to SMF: When IP addresses in a DNN for a UPF left with a “threshold” configured number of IP addresses in a IPAM module gives information to SMF using resource management response.

SMF behaviour when a threshold hit received: SMF marks a usable threshold hit for a given UPF. Since IPAM pool distribution is per node manager separately, SMF marks a threshold separately for primary and secondary node manager.

SMF behaviour choosing UPF for new session when a threshold marked: SMF performs the following checks.

- If a threshold hit for a primary node manager and secondary node manager is not hit, IP allocation request is sent for a secondary node manager.
- If a threshold hits both primary and secondary node manager, then current UPF selects the lower priority node manager, if any other UPF configured and threshold not hit is selected first.
- If all the UPFs are threshold hit, then the behaviour falls back to priority and load based which is existing behaviour. This is similar to that of a non-existence threshold hit behaviour.

Important Refer IP Address Management chapter for configuration details.

Recovery behaviour from a threshold hit: IPAM to periodically if UPF has come out of threshold hit condition. When UPF has enough free addresses to come out of threshold hit (for each DNN, and each UPF) IPAM gives information of SMF (through a callback). SMF unmarks UPF as threshold hit.

When IP addresses in a pool (for each DNN, and each UPF) left with a “threshold” configured number of IP addresses in a IPAM module gives information to SMF using resource management response.

OAM Support for IP Threshold-based UPF Selection

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

New statistics introduced to capture the following stats information:

Lables:

- Label: up_ep_key

  Label Description: When a particular IP address pools threshold is hit for usage of IP addresses, this stats will be recorded

  Example: 209.165.200.241:209.165.200.242

- Label: dnn

  Label Description: DNN of the IP pool which reached the configured threshold usgae

  Example: sampleDNN

- Label: threshold_hit

  Label Description: Indicates if the threhold hit is yes or no

  Example: yes

- Label: threshold_clear

  Label Description: Indicates if the threhold hit is cleared or not

  Example: yes

- Label: nodemgr_id

  Label Description: Indicates the instance of the nod manager which hit the threshold

  Example: 1

show userplane all

This section describes show commands that help in debugging issues.

show userplane all

- Node IP and end point
- Capacity and priority
- Serving DNN list
- Primary and peer node manager instance
- Load seq and load metrics
- Connected time
- Usable threshold hit for primary and secondary node manager

The following is an example of the show command output

```
[smf] smf# show userplane all
result
{
  "209.165.200.230:209.165.200.244": {
    "NodeIdType": 1,
    "NodeId": "209.165.200.228",
    "NodePort": 8805,
    "NodeStatus": 2,
    "Capacity": 65535,
    "Priority": 65535,
    "DnnList": [
      "intershat",
      "intershat1",
      "intershat2",
      "intershat3"
    ],
    "PrimaryNodeMgrInst": {
      "InstanceId": 1,
      "IsActive": true
    },
    "PeerNodeMgrInst": {
      "IsActive": true
    },
    "EpIp": "209.165.200.244",
    "EpPort": 8805,
    "UpEpKey": "209.165.200.230:209.165.200.244",
    "recoveryInfo": {
      "SvcRecoveryTime": 3820194022,
      "PeerRecoveryTime": 3817503651
    },
    "ConnectedTime": 3820194461,
    "IntfType": 1,
    "UpProfName": "upf1",
    "OverloadTimer": {},
    "NegotiatedCPFeatures": 2147483648
  }
}
```

Co-located UPF Selection During Initial EPS Attach

This section describes how the SMF performs UPF selection during the initial EPS Attach procedure.

Feature Description

The converged core gateway with the cnSGWc and SMF supports selection of a converged UP node to realize convergence. With this functionality, it is possible to create an optimized data path for the UE.

The SMF performs co-located UPF selection based on the SGW-U node name received in the Create Session Request (CSR) message.

How it Works

This section describes how the SMF handles the co-located UPF selection during PDN Session Establishment in 4G network.

When the SGW-U node name is available in the CSR, SMF derives the UPF from the configuration based on the node name.

Then, SMF uses the existing UPF selection logic and derives the list of UPFs accordingly. The SMF checks if the SGW-C selected UPF exists in the derived UPF list.

If the SGW-C selected UPF is present in the derived UPF list and if its priority matches with the highest priority in the derived UPF list, then SGW-C selection UPF is selected. Otherwise, priority UPF in the derived list is selected.

In the absence of the SGW-U node name, the SMF follows the existing UPF selection algorithm.

Configuring Node ID

To select the co-located UPF, use the following sample configuration.

```
config
  profile network-element upf upf_name
    node-id value
    end
```

NOTES:

- **profile network-element upf** *upf_name*: Specify a profile name for the UPF.
- **node-id** *value*: This keyword aids in configuring the node ID of UPF. The SMF compares this node name with SGW-U node name to select the co-located UPF. *value* is an alphanumeric string.

Statistics Support

The SMF maintains the following statistics in support of this feature.

upf_selection_stats

Description: Displays the total number of times the same co-located UPF is selected by SMF.

Metrics-Type: Counter

Labels:

- upf_selection_type
- upf_fqdn
- preferred
- upf_not_associated
- upf_profile_not_found
- upf_not_active
- n4_failed
- pdu_session_type
- pdu_subscription_type
- snssai

Status:

- attempted
- failure

Reason: If the status is failure, the value can be one of the following:

- upf_not_associated
- upf_profile_not_found
- upf_not_active
- n4_failed

Co-located UPF Selection During Handover

This section describes how the SMF performs UPF selection during 5G to 4G handover and EPS fallback scenarios.

Feature Description

During the UE session establishment in 5G core network, the SMF uses the existing UPF selection logic and records the index of the selected UPF in PGW-C Control Tunnel Endpoint Identifier (TEID).

Upon receiving Create Session Request (CSR) from MME, cnSGWc checks whether or not the TEID value is zero. If it is zero, then cnSGWc sends Remote Procedure Call (gRPC) message to SMF and fetches UP ID and UPF IP.

If the TEID is non-zero, the SMF checks the bits from 21 through 30 of control TEID value, and extracts the UPF index. The SMF uses the extracted UPF index to select the preferred UPF.

The SGW-C uses this as the preferred UPF when the UE session is handed over to EPS network. If the preferred UPF is present in the list returned by the UPF selection algorithm, then the cnSGWc selects the UPF with highest priority. That is, the cnSGWc selects the same UPF that was chosen by SMF. This operation enables creating an optimized data path for the UE.

If the preferred UPF does not exist in the returned list, cnSGWc selects a different UPF.

Configuring Parameters for Co-located UPF Selection

This section describes how to perform co-located UPF selection during handover scenario.

Configuring the parameters for co-located UPF selection involves the following steps:

- Enabling Co-located UPF Selection, on page 104
- Configuring Index and Session Count for UPF Selection, on page 105

Enabling Co-located UPF Selection

To enable or disable co-located UPF selection, use the following sample configuration.

```
config
   profile converged-core cc_profile_name
      up-selection { disable | enable }
      end
```

NOTES:

- **profile converged-core** *cc_profile_name*: Specify the name of the converged core profile. This keyword allows you to enter the converged core profile configuration mode.

- **up-selection { disable | enable }**: Enable or disable the co-located UPF selection. By default, this configuration is enabled.

Configuring Index and Session Count for UPF Selection

To define the UPF index value and maximum session count for co-located UPF selection, use the following sample configuration.

```
config
  profile converged-core cc_profile_name
    max-upf-index upf_index_value
    max-session-count up_session_count
    end
```

NOTES:

- **profile converged-core** *cc_profile_name*: Specify the name of the converged core profile. This keyword allows you to enter the converged core profile configuration mode.
- **max-upf-index** *upf_index_value*: Specify the maximum number of supported UPF index values for UPF selection.

  upf_index_value must be an integer in the range of 0–1023.

  The SMF validates the configured UPF index value against the UP ID received in the N4 Association Setup request from UPF. If the validation fails, the SMF rejects the corresponding request. If the validation is successful, the SMF acknowledges the request and stores the UP ID along with other UPF details.
- **max-session-count** *up_session_count*: Specify the maximum number of UP sessions supported.

  up_session_count must be an integer in the range of 1000000–12000000. Default value is 1000000.

  The SMF uses the configured session count to associate the UP session with IdMgr context. Note that IdMgr maintains a separate context per million UP sessions.

Block UPF to handle continuous N4 session creation failures

Table 17: Feature History

Feature Name	Release Information	Description
Blocking UPF to handle N4 session establishment failures	2025.02.0	This feature allows the SMF to blocklist a specific UPF node when it continuously rejects session establishment requests. The UPF may reject these requests from the SMF due to various errors, such as licensing issues. However, without information on the issues at the UPF, the SMF might repeatedly select the same UPF, leading to an increased number of session creation failures. By enabling this feature, the network operators can prevent the SMF from repeatedly selecting the same UPF for a defined time interval. **Commands Introduced:** • **[no] activated-features upf-blocklisting [use-alert** *custom_rule_name* **]**: This CLI is configured under converged core profile configuration mode to enable UPF blocklisting feature on SMF. • **reactivate-peer condition [blocked] attributes [frequency** *frequency_timer* **]**: This CLI is configured under the endpoint configuration mode to reactivate blocked UPF after the frequency timer is over. **Default Setting:** Disabled—Configuration Required to Enable

During the N4 session creation process, the SMF selects a UPF based on configured options and parameters received in the create request. However, the selected UPF might occasionally be unable to handle the requests due to various issues, such as licensing problems, leading to repeated rejection of session establishment requests.

Since the SMF lacks information about the issues at the UPF, it may continue to select the same UPF, resulting in repeated session creation failures.

This feature allows network operators to blocklist a UPF node by configuring alerts that trigger when the N4 session establishment failure rate exceeds a defined threshold. It also enables the configuration of a time interval during which the specified UPF node remains blocklisted and allows for reactivating the blocked UPF once the timer expires.

How handling continuous N4 session creation failures works

The network operator configures the alerts in the Alert Manager with rule name, procedure type, status, interface type, and other parameters defining the conditions for triggering.

Here is a sample of alert configuration:

```
alerts rules group PeerFailure
    rule upf_inactive
    expression "(sum by (namespace,upf_id,gr_instance_id)
    (proto_pfcp_msg_stats{status='failed'})) >= 1000”
    duration   5m
    severity   major
    type       "Communications Alarm"
    annotation summary
    value "NF=UPF Value={{ $value }} - UPF inactive"
    exit
   exit
exit
```

Note The rule name specified in the configuration for enabling UPF blockin activation configuration should be same as the rule name configured in the alert.

The Alert Manager informs the SMF, when the session creation failure reaches a threshold limit. If UPF blocklisting and reactivation configurations are enabled, SMF blocks the specific UPF for the defined frequency timer, and looks for an alternate UPF for session creation.

For more information on UPF blosklisting and UPF reactivation, see the Configure UPF selection during session creation failures topic.

Once the defined frequency timer expires, SMF removes that UPF from the blocked status and considers it for session creation.

Configure SMF to handle continuous N4 session creation failures

Perform these tasks to resolve the continuous N4 session creation failures:

- Enable UPF blocking
- Reactivate the blocked UPF

Enable UPF blocking

This task allows the operator to enable or disable the UPF blocklisting functionality. Also, it allows the operator to configure an optional custom rule name to be used for subscribing the alerts for UPF blocklisting and notification from Event Manager.

Follow these steps to enable UPF blocklisting:

Procedure

Step 1 Use the command **profile converged-core** *cc_profile_name* to enter the converged-core profile configuration mode.

Example:

```
[smf] smf# config
[smf] smf(config)# profile converged-core ccg1
[smf] smf(config-converged-core-ccg1)#
```

Step 2 Use the command **[no] activated-features upf-blocklisting [use-alert** *custom_rule_name* **]** to enable the UPF blocklisting and setting a custom rule name.

Example:

```
[smf] smf(config-converged-core-ccg1)# activated-features upf-blocklisting use-alert
upf_inactive1
[smf] smf(config-converged-core-ccg1)#
```

The **[use-alert** *custom_rule_name* **]** is an optional CLI. It allows the network operator to configure a custom rule name for alert subscriptions.

Note

- The default value of the Command **[use-alert** *custom_rule_name* **]**, is "upf_inactive". If the custom rule name is not configured, the system takes "upf_inactive" for blocklisting the UPF.
- Changing the custom rule name during run-time requires the previous rule name to be removed. Configuring the new custom rule name before removing the previous rule name, results in activating both the both the rule names.
- The new alert configuration parameters should be configured with the new rule name in CEE alert configuration (CEE ops-center).

Step 3 Use the command **exit** to save and exit the converged core profile configuration mode.

Example:

```
[smf] smf(config-converged-core-ccg1)# exit
[smf] smf(config)#
```

This task enables blocklisting of a defined UPF.

Reactivate blocked UPF

This task allows the network operator to configure the frequency interval during which the specific UPF is marked as blocked for selection. Once the frequency interval ends, the UPF becomes available for selection.

Follow these steps to reactivate the blocklisted UPF:

Before you begin

Before performing this task, you may configure the custom rule name for UPF blocklisting, which is an optional configuration.

Procedure

Step 1 Use the command **instance instance-id***gr_instance_id* to create an instance of the instance profile.

Example:

```
[smf] smf# config
[smf] smf(config)# instance instance-id 1
[smf] smf(config-instance-id-1)#
```

Step 2 Use the command **endpoint pfcp** to enter the endpoint configuration mode.

Example:

```
[smf] smf(config-instance-id-1)# endpoint pfcp
[smf] smf(config-endpoint-pfcp)#
```

Step 3 Use the command **interface** *interface_type*to configure the parameters for N4 interface.

Example:

```
[smf] smf(config-endpoint-pfcp)# interface n4
[smf] smf(config-interface-n4)#
```

Step 4 Use the command **reactivate-peer condition [blocked] attributes [frequency** *frequency_timer* **]** to reactivate the blocked UPF once the timer is over.

Example:

```
[smf] smf(config-interface-n4)# reactivate-peer condition blocked attributes frequency
 60
[smf] smf(config-interface-n4)#
```

- The value of the command **frequency** ranges between 60 to 86400.
- The frequency parameter does not have any default values.
- It is mandatory to configure the frequency parameter within the defined range. If the frequency parameter is not configured within the range, the system by default takes 0 as the input. As a result, the identified UPF does not get blocklisted even if the alarm is triggered.

Step 5 Use the command **exit** to save and exit the interface configuration mode.

Example:

```
[smf] smf(config-interface-n4)# exit
[smf] smf(config-endpoint-pfcp)#
```

Monitoring and Troubleshooting

This section discusses the bulkstatistics and show commands used for monitoring and troubleshooting this feature.

Show command and output

The show command **show userplane all** displays the current status of UPF under the NodeStatus parameter. The new state **BLOCKED (5)**indicates that the specific UPF's current status is blocked.

Here is an example of the show command output:

```
[smf] smf#show userplane all
{
  "10.1.46.72:10.1.47.208": {
    "NodeIdType": 1,
    "NodeId": "10.1.46.72",
    "NodePort": 8805,
  "NodeStatus": 5,
  "Capacity": 65535,
  "Priority": 10,
  "DnnList": [
    "ims1",
    "ims2",
    "intershat"
  ],
  "PrimaryNodeMgrInst": {
    "IsActive": true
  },
  "PeerNodeMgrInst": {
    "InstanceId": 1,
    "IsActive": true
  },
  "EpIp": "10.1.47.208",
  "EpPort": 8805,
  "UpEpKey": "10.1.46.72:10.1.47.208",
  "recoveryInfo": {
    "SvcRecoveryTime": 3948948938,
    "PeerRecoveryTime": 3948786054
  },
  "ConnectedTime": 3948949630,
  "IntfType": 4,
  "UpProfName": "upf1",
  "OverloadTimer": {},
  "NegotiatedCPFeatures": 2147483648,
  "IsAssocUpdSuccess": true,
  "UpfInactiveValidityTime": 1739960992
}
```

Bulkstats

These statistics are introduced as part of this feature:

Statistics	Description	Label(s)
prometheus_alert_received_total	Total number of valid Prometheus alerts received on event manager on its rest ep.	alert_rule
prometheus_alert_invalid_data_total	Total number of Prometheus alerts with invalid data received on event manager on its rest ep.	err_code
pubsub_subscriptions_total	Total number of subscription for producer pod.	event_name, consumer_instance
pubsub_events_produced_total	Total number of event published to subscribed pod.	event_name, instance, retry, retry_attempt, cause
pubsub_events_produced_ack_total	Total number of event published status to subscribed pod.	event_name, consumer_instance, status, retry, retry_attempt
pubsub_events_consumed_ack_total	Total number of event publish ack to producer.	event_name, dest_host, retry, retry_attempt

Statistics	Description	Label(s)
proto_pfcp_msg_stats	The number of failures observed during session establishment procedure.	app_name, cause, cluster, data_center, gr_instance_id, instance_id, interface_type, message_name,upf_id, service_name, status, trans_type

Note The statistics **proto_pfcp_msg_stats** counter increases only when the UPF blocklisting feature is enabled under converged core profile configuration activated-feature list. It is mandatory to specify the "**upf_id**" under the list of labels grouped by as part of the expression to make this feature work. This parameter helps identify the UPF, which needs to be blocklisted. Without this, the functionality does not work as expected.

Support for UPF Node Reports and Proprietary Session Reports

Feature Description

The SMF triggers the Packet Forwarding Control Protocol (PFCP) Node Report procedure as per the *3GPP TS 29.244, section 6.2.9*. The UPF sends this report to indicate a user plane path failure affecting all the PFCP sessions towards a remote GTP-U peer. The UPF notifies this failure to the SMF through User Plane Path Failure Report (UPFR). When the UPF detects a GTP-U path failure, the SMF clears the PDU sessions belonging to the GTP-U peer and UPF node ID.

In addition to the existing UPF session report, the SMF supports the following proprietary report types:

- Graceful Termination Report (GTER)—This type of report is sent when the UPF is unable to recover a PDU session during Session Recovery (SR) or Inter-Chassis Session Recovery (ICSR).
- Session Replacement Report (SRIR)—This type of report is sent to replace a session due to identical GTP-U tunnel endpoint identifier (TEID) allocated by gNB. This is possible with the restart of gNB. In this case, the old session with the same TEID is deleted.
- Self-protection Termination Report (SPTER)—This type of report is sent to terminate a PFCP session during overload scenarios.

How it Works

This section describes how the SMF supports the UPF node report and the proprietary session reports.

PFCP Node Report Handling

For proper handling of PFCP node report, the GTP-U peer address must include a non-unique secondary session key. The Common Data Layer (CDL) stores the peer address and the UPF IP address along with the session details. If the GTP-U peer address changes during idle to active transition procedure, N2 handover (HO), 5G to 4G HO, or 4G to 5G HO, the CDL database deletes the old key and adds the new one.

1. The UPF sends PFCP Node Report Request to the SMF along with the IP address of the failed GTP-U peer.
2. The SMF protocol checks the node ID, that is, the UPF IP address included in the request. If the node ID is not found or if the node ID is not in associated state, the SMF protocol sends a failure response.
3. If the node ID is found, the node manager queries the CDL for EPS session with the GTP-U peer IP address and node ID. The node manager sends bulk notification to the CDL to clear the corresponding sessions.
4. The CDL sends the notification to rest endpoint (REST-EP) pod to clear the sessions.
5. The REST-EP pod sends the subscriber clear notification to the SMF service based on the affinity. The SMF service clears the sessions on all interfaces.

PFCP Session Report Handling

The UPF sends PFCP session report along with GTER, SRIR, and SPTER to the SMF. If the session is found, the SMF sends a successful PFCP session report response. Then, the SMF triggers the PDU session release procedure and deletes the sessions on all interfaces.

Collision Handling

For the newly supported messages (node report and session report), the SMF triggers the PDU session release procedure. If the PDU session release procedure collides with the HO procedure, the SMF does not abort the HO procedure as the GTP-U peer IP changes during the HO. To achieve this, the PDU release procedure involves comparing the GTP-U peer IP address received in release request with the one present in the PDU session. If the two addresses are different, then the SMF aborts the release procedure.

Important The collision handling depends on the arrival time of the incoming HO message and **clear subscriber** command triggered by node report.

Resiliency Handling

The SMF uses a retry timer to check and report any pending session deletions for a GTP-U peer. After the restart of SMF node manager, if any sessions are not deleted, then these sessions remain as is.

Standards Compliance

The UPF Node Report and Session Report Support feature complies with the following standard:

- *3GPP TS 29.244 Version 15.6.0 – LTE; Interface between the Control Plane and the User Plane nodes*

Limitations

This feature has the following limitations:

- If the CDL notifications are lost and the sessions are not cleared, the SMF node manager retries the bulk deletion operation only once after 10 minutes.

- If the node report request arrives and the system is in overload state, some CDL notifications are dropped. In this case, the SMF performs the session clean-up based on error indication report request from the UPF.
- The UPF currently sends only one Remote GTP-U peer in the Node Report request. So, the SMF can validate only one remote GTP-U peer.

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Monitoring Support

An alarm is added when the following configuration is performed on CEE Ops-Center. This alarm indicates that a GTP-U peer for a particular UPF has gone down. The alarm data includes GTP-U peer IP and UPF IP addresses.

The following is a sample configuration performed on the CEE Ops-Center to configure alert rules related to the UPF Node Report Request.

```
config
   alerts rules group alert_group_name
   interval-seconds seconds
   rule rule_name
      expression promql_expression
      severity severity_level
      type alert-type
      annotationannotation_name
      value annotation_value
      exit
   exit
```

NOTES:

- **alerts rules**: Specify the Prometheus alerting rules.
- **group** *alert_group_name*: Specify the Prometheus alerting rule group. One alert group can have multiple lists of rules. *alert-group-name* is the name of the alert group. The *alert-group-name* must be a string in the range of 0–64 characters.
- **interval-seconds** *seconds*: Specify the evaluation interval of the rule group in seconds.
- **rule** *rule_name*: Specify the alerting rule definition. *rule_name* is the name of the rule.

The following is an example configuration of the alert.

```
config
   alerts rules group NodeReportGTPURemotePeer
   interval-seconds 300
   rule NodeReportGTPURemotePeerDown
      expression smf_protocol_udp_res_msg_total{message_name=\"n4_node_report_req\",
message_direction= \“inbound\”, status=\“accepted\”}”
      severity major
      type "Communications Alarm"
      annotation summary
      value “This alert is fired when the UPF Sends Node Report Request to SMF”
      exit
   exit
```

Show Command Support

Use the **show subscriber all** command to view the configuration related to GTP-U peer IP address and GTP-U peer endpoint key. This configuration data helps to identify the failed sessions or collision of procedures.

The following is an example output.

```
[unknown] smf# show subscriber all nf-service smf
subscriber-details
{
  "subResponses": [
    [
      "supi:imsi-123456789012345",
      "gpsi:msisdn-223310101010101",
      "pei:imei-123456786666660",
      "psid:5",
      "dnn:intershat",
      "emergency:false",
      "rat:e-utran",
      "access:3gpp access",
      "connectivity:4g",
      "udm-sdm:10.84.17.111",
      "pcfGroupId:PCF-dnn=;",
      "policy:2",
      "pcf:10.84.17.111",
      "upf:10.84.17.111",
      "upfEpKey:10.84.17.111:10.84.17.112",
      "ipv4-addr:poolv4/209.165.202.129",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.202.129",
      "ipv4-startrange:poolv4/209.165.202.129",
      "gtp-peer:10.84.17.112",
      "peerGtpuEpKey:10.84.17.111:10.84.17.111",
      "namespace:smf"
    ]
  ]
}
```

Use the **show subscriber count peerGtpuEpKey** command to view the number of sessions associated with the specified GTP-U peer and the UPF node.

Important Use the **show subscriber count peerGtpuEpKey** command carefully and sensibly as it might impact the system performance.

The following is an example output of **show subscriber count peerGtpuEpKey** command.

```
smf# show subscriber count peerGtpuEpKey 30.30.30.63:50.50.0.58
  subscriber-details
  {
    "sessionCount": 12568
  }
```

Statistics Support

The SMF maintains the following statistics to track the total number of attempted, successful, and failed node-level and session-level requests.

- SMF_SERVICE_STATS for the following procedure types:
  - upf_node_report_pdu_sess_rel

    attempted: Total number of attempted PDU session release requests triggered due to the node report.

    successful: Total number of successful PDU session release requests triggered due to the node report.

    failure: Total number of failed PDU session release requests triggered due to the node report.
  - upf_sess_report_gter_pdu_sess_rel

    attempted: Total number of attempted PDU session release requests triggered due to the session report “GTER”.

    successful: Total number of successful PDU session release requests triggered due to the session report “GTER”.

    failure: Total number of failed PDU session release requests triggered due to the session report “GTER”.
- SMF_PROTOCOL_UDP_REQ_MSG_TOTAL for the following message types:
  - n4_node_report_req

    attempted: Total number of attempted N4 requests triggered due to the node report.

    successful: Total number of successful N4 requests triggered due to the node report.

    failure: Total number of failed N4 requests triggered due to the node report.
  - n4_session_report_req

    attempted: Total number of attempted N4 requests triggered due to the session report.

    successful: Total number of successful N4 requests triggered due to the session report.

    failure: Total number of failed N4 requests triggered due to the session report.
- SMF_PROTOCOL_UDP_RES_MSG_TOTAL for the following message types:
  - n4_node_report_res

    attempted: Total number of attempted N4 responses triggered due to the node report.

    successful: Total number of successful N4 responses triggered due to the node report.

    failure: Total number of failed N4 responses due to the node report.
  - n4_session_report_res

    attempted: Total number of attempted N4 responses triggered due to the session report.

    successful: Total number of successful N4 responses triggered due to the session report.

    failure: Total number of failed N4 responses due to the session report.
- SMF_DISCONNECT_STATS triggered for the following disconnect reasons:

gtpu_peer_path_failure : This statistic is triggered when the session is deleted due to the node report.

upf_sess_report_gter_pdu_sess_rel: This statistic is triggered when the session is deleted due to the session report.

The following is an example of the statistics:

Node Report SMF-service stats:

```
smf_service_stats{app_name="SMF",cluster="Local",data_center="DC",dnn="intershat",
emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_node_report_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="attempted",up_state=""}
```

```
smf_service_stats{app_name="SMF",cluster="Local",data_center="DC",dnn="intershat",
emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_node_report_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="success",up_state=""} 1
```

Session Report SMF-service stats:

```
smf_service_stats{always_on="",app_name="smf",cluster="smf",data_center="unknown",
dcnr="",dnn="intershat",emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_sess_report_gter_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="attempted",up_state=""} 1
```

```
smf_service_stats{always_on="",app_name="smf",cluster="smf",data_center="unknown",
dcnr="",dnn="intershat",emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_sess_report_gter_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="success",up_state=""} 1
```

Node Report SMF-protocol stats:

```
smf_proto_udp_req_msg_total{app_name="smf",cluster="smf",data_center="unknown",
instance_id="0",message_direction="inbound",message_name="n4_node_report_req",
msgpriority="",service_name="smf-protocol",status="accepted",
transport_type="origin"} 15
```

```
smf_proto_udp_res_msg_total{app_name="smf",cause="1",cluster="smf",
data_center="unknown",instance_id="0",message_direction="outbound",
message_name="n4_node_report_res",msgpriority="",service_name="smf-protocol",
status="accepted",transport_type="origin"} 15
```

Session Report SMF-protocol stats:

```
smf_proto_udp_req_msg_total{app_name="smf",cluster="smf",data_center="unknown",
instance_id="1",message_direction="inbound",message_name="n4_session_report_req",
msgpriority="",service_name="smf-protocol",status="accepted",
transport_type="origin"} 43
```

```
smf_proto_udp_res_msg_total{app_name="smf",cause="1",cluster="smf",
data_center="unknown",instance_id="1",message_direction="outbound",
message_name="n4_session_report_res",msgpriority="",service_name="smf-protocol",
status="accepted",transport_type="origin”}
```

The SMF also maintains labels to track the number of session deletions due to the node report and session report types – GTER, SRIR, and SPTER.

For example, the label "LABEL_DISC_PDNREL_GTER_SESSION_REP" is added to track the session deletion due to the presence of GTER.

Outer Header Format

Table 18: Feature History

Feature Name	Release Information	Description
Dual Stack Support on N3	2024.01	SMF enables the dual stack transport for N3 tunnel using the **dual-stack-transport { false | true }** CLI command in the UPF network profile. **Default Setting:** Disabled – Configuration Required

SMF sends the Outer Header IE to UPF in the Packet Detection Rule (PDR) of the PFCP session. The Outer Header IE is available in the N4 Session Establishment Request message sent over the Sx interface. The version 16.4.0 of 3GPP TS 29.244 specification defines the format of this IE.

The following table identifies the encoding format of the Outer Header Creation (OHC) Description field. It takes the form of a bitmask where each bit indicates the outer header to be added to the outgoing packet. SMF ignores the spare bits.

Table 19: Header Encoding Format

Octet / Bit	Outer Header Created in the Outgoing Packet
5/1	GTP-U/UDP/IPv4
5/2	GTP-U/UDP/IPv6
5/3	UDP/IPv4
5/4	UDP/IPv6
5/5	IPv4
5/6	IPv6
5/7	C-TAG
5/8	S-TAG
6/1	N19 Indication
6/2	N6 Indication
6/3	TCP/IPv4
6/4	TCP/IPv6

NOTES:

- Currently, UPF doesn't support the following values of Outer Header Creation Description:
  - IPv4
  - IPv6

  - C-TAG
  - S-TAG
  - N19 Indication
  - N6 Indication

- The third and fourth bits of the sixth octet (that is, 6/3 and 6/4) are spare bits (that is, not part of 3GPP TS 29.244, version 16.4.0) used for LI over TCP.

Important SMF and UPF must support the same format of Outer Header IE for a successful session establishment.

Feature Configuration for Outer Header IE

SMF enables dual stack connection in the UPF profile. When the dual stack is configured, the Outer Header Removal (OHR) Description field in the OHR IE is set to 6 to remove the GTP-U or UDP or IP header for the IPv4 and IPv6 addresses.

To enable dual stack on the N3 interface, use the following sample configuration:

```
config
   profile network-element upf upf_profile_name
       dual-stack-transport { true | false }
       end
```

NOTES:

- **dual-stack-transport { true | false }**: Enable or disable dual stack transport on the N3 interface.
  - When the **dual-stack-transport true** command is configured, SMF sends the OHR IE with the value 6 for the IPv6 address on the supported interfaces.
  - SMF saves the configured dual stack value during session establishment. SMF uses the same dual stack value in the subsequent N4 messages until the session gets disconnected.

Note This CLI configuration is applicable for the SMF with legacy interfaces as well.

Enhanced PFCP Association Release Procedure for Graceful Session Termination

Table 20: Feature History

Feature Name	Release	Description
Indication for UPF-initiated PFCP Association Release	2024.03.0	This feature enables SMF to receive notification on UPF-initiated PFCP Association Release procedure. This notification indicates to clear the sessions and association simultaneously in UPF and SMF. If the SMF is not notified, the call remains connected until UPF receives the next Session Modify Request from the SMF. This leads to loss of subscriber usage reports. Here, the Enhanced PFCP Association Release (EPFAR) feature improves the signalling efficiency and effective handling of usage reports by SMF. **Default Setting:** Disabled – Configuration Required to Enable

When the UPF decides to clear the call due an error or a partial failure, the UPF clears the calls locally without informing the SMF on the call clearance. The call remains connected until the next Session Modify Request received by UPF from the SMF.

To avoid losing the usage reports and improving the signalling efficiency during call clearance, the Enhanced PFCP Association Release (EPFAR) feature is applied for the UPF to initiate the session report request to gracefully clear the session between UPF and SMF or UPF and cnSGWc simultaneously. This feature complies with the Release 16.9.0 of 3GPP TS 29.244, section 5.18.1 and section 5.18.2.

EPFAR Negotiation

EPFAR feature negotiation is an aggregate communication between the SMF and UPF. When both the SMF and UPF support the EPFAR feature, the session and association release actions are accomplished. You can enable the EPFAR feature using the configuration command when the UPF needs to release the association with the SMF.

SMF indicates the support of EPFAR feature by setting the EPFAR bit in CP Function Features IE in the PFCP Association Setup Response towards UPF.

In case of rolling upgrade, whenever the chassis becomes active, UPF or SMF sends the PFCP Association Update with UP or CP Function Features, so that EPFAR feature can be negotiated again.

The UPF initiated release is triggered using these procedures:

1. UPF-initiated PFCP Session Release
2. UPF-initiated Enhanced PFCP Association Release

UPF-initiated PFCP Session Release

UPF-initiated PFCP Session Release consists of these courses of action:

1. UPF enables the feature for a peer node only if it is negotiated during Association Setup or Modify procedure. When the UPF needs to delete a PFCP sesssion due to an error or a partial failure, it initiates the PFCP Session Report requests for the affected session. SMF receives the PFCP Session Report Request from UPF with Report Type and User Report Trigger IEs.

    - The Report Type is set as USAR (Usage Report) when there is a non-zero usage report for the PFCP session or UISR (UP Initiated Session Request) if there is no usage report to send.

      The fifth bit of Octet 6 in Report Type IE is a proprietary IE bit used for indicating UISR for PFCP Session Report Request.

    - User Report Trigger is set as TEBUR (Termination By UP function Report) for a non-zero usage report.

   UPF sets the PSDBU (PFCP Session Deleted By the UP function) flag as 1 to indicate the PFCP session deletion

2. UPF sends the Cause IE to the peer node in PFCP Session Report Request message. The Cause IE uses these values for communicating the cause of session deletion:

    - 201 - Subscriber Clear
    - 202 - Association Release initiated by UP
    - 203 - Recovery Failure
    - 204 - IP Source Violation
    - 205 - PFCP Cause Self Protection Termination

   The table lists the causes sent to SMF on legacy interfaces:

Cause from UPF	Gx Termination-Cause	Gy Termination-Cause	Radius Accounting Stop Acct-Terminate-Cause	Gtpc Cause	Gz CauseForRecClosing
Subscriber Clear (201)	Diameter Logout	Diameter Logout	Nas Request	Reactivation requested	Management intervention
Association Release initiated by UP (202)	Diameter Logout	Diameter Logout	Nas Request	Reactivation requested	Management intervention
Recovery Failure (203)	Diameter Administrative	Diameter Administrative	Nas Request	Reactivation requested	abnormal release

Cause from UPF	Gx Termination-Cause	Gy Termination-Cause	Radius Accounting Stop Acct-Terminate-Cause	Gtpc Cause	Gz CauseForRecClosing
IP Source Violation (204)	Diameter Administrative	Diameter Administrative	Nas Request	Reactivation requested	abnormal release
Self-Protection Termination (205)	Diamater Administrative	Diamater Administrative	Nas Request	Reactivation requested	abnormal release

3. SMF handles these Usage Reports as a part of the release procedure:
    - TEBUR without PSDBU
    - TEBUR with PSDBU
    - Session Reports with UISR and PSDBU
4. The Usage Reports are reported together to CHF in the session release.

Note The maximum supported clear subscriber rate at SMF is 500 sessions per second. So, the session report throttle rate is maintained as 500 per second at UPF. If the combined rate of Session Reports from multiple UPFs exceed the maximum supported rate, it can still lead to throttling on SMF and subsequent retransmissions.

UPF-initiated Enhanced PFCP Association Release

UPF-initiated PFCP Association Release consists of these courses of action:

1. When both the SMF and UPF support EPFAR feature, UPF would initiate the PFCP association release. SMF receives the PFCP Association Update Request with PARPS (PFCP Association Release Preparation Start) flag set from the UPF on PFCP Association Release and SMF stops selecting the UPF.
2. SMF receives Usage Reports with these flags set from UPF:
    - TEBUR without PSDBU and TEBUR with PSDBU for all sessions with final non-zero usage reports.
    - Session Reports with UISR and PSDBU flags for all sessions with no usage reports.
3. SMF receives PFCP Association Update Request from UPF with the URSS flag set to 1 that indicates all the non-zero Usage Reports for the affected PFCP Sessions are sent. SMF deletes all the remaining Sessions for this UPF.
4. After all the sessions for the UPF are cleared, the SMF triggers PFCP Association Release procedure towards UPF to clear the PFCP Association.

Enable the EPFAR Feature

Enable the EPFAR feature at SMF using the **[smf] smf(config)# profile converged-core cc supported-features [epfar]** CLI command.

Procedure

Step 1 Enter the **profile converged-core cc supported-features** command in the Context Configuration mode.

Example:

```
[smf] smf(config)# profile converged-core cc supported-features [ epfar ]
```

Note

epfar—enables support for Enhanced PFCP Association Release

Step 2 You can verify if the EPFAR feature is enabled or disabled using the **show running-config profile converged-core** show command.

Example:

```
[smf] smf# show running-config profile converged-core
Mon May  6  03:09:36.813 UTC+00:00
profile converged-core cc
 supported-features [ epfar ]
exit
[smf] smf#
```

Bulk Statistics

New labels are added as a part of this feature for the existing statistics:

- smf_disconnect_stats

  Example Query1:

  ```
  smf_disconnect_stats {an_type=""app_name ="SMF",cluster="SMF",
  data_center="DC",gr_instance_id="1",instance_id="0",rat_type=
   "EUTRA"reason=" disc_subscriber_clear",roaming_status="homer",
  service_name="smf-service",severity="normal",snssai=""} 1
  ```

  Example Query 2:

  ```
  smf_disconnect_stats {an_type="3GPP_ACCESS", app_name="SMF",
  cluster="SMF",data_center="DC",gr_instance_id="1",instance_id="0",
  rat_type="NR",reason="disc_pdurel_upf_urss_init_ association_release",
  roaming_status="homer",service_name="smf-service",severity="normal",
  snssai=""} 1
  ```

  Example Query3:

  ```
  smf_disconnect_stats {an_type="",app_name="SMF",cluster="SMF",
  data_center="DC",gr_instance_id="1",instance_id="0",rat_type="EUTRA",
  reason=" disc_pdn_upf_urss_init_release",roaming_status="homer",
  service_name="smf-service",severity="normal",snssai=""} 1
  ```

  Labels:

  - disc_subscriber_clear
  - disc_association_release_initiated_by_up
  - disc_recovery_failure
  - disc_ip_source_violation
  - disc_psdbu_timer_expiry
  - disc_pdurel_upf_urss_init_association_release

- smf_sess_report_stats

  Example Query 1:

  ```
  smf_sess_report_stats {app_name="SMF",cluster="SMF",
  data_center= "DC",gr_instance_id="1",instance_id="0",
  rat_type="EUTRA",reason="psdbu",service_name="smf-service",
  sess_report_type="sess_report_type_uisr"} 1
  ```

  Example Query 2:

  ```
  smf_sess_report_stats {app_name="SMF",cluster="SMF",
  data_center="DC",gr_instance_id="1",instance_id="0",
  rat_type="EUTRA",reason="psdbu",service_name="smf-service",
  sess_report_type="sess_report_type_usar"} 2
  ```

  Labels:

  report_type and reason have these labes in the statistics:

  - sess_report_type_uisr
  - sess_report_type_usar
  - psdbu

- smf_pfcp_usar_rpt_type_stats

  Example Query:

  ```
  smf_pfcp_usar_rpt_type_stats {app_name="SMF",
  charging_trigger_type="TEBUR,",cluster="SMF",
  data_center="DC",instance_id="0",service_name=
  "smf-service",status="validated"} 2
  ```

  Label:

  - charging_trigger_type="TEBUR,"

- nodemgr_up_pathfail_reasons

  Example Query:

  ```
  nodemgr_up_pathfail_reasons {app_name="SMF",
   cluster="SMF",data_center="DC",gr_instance_id="1",
  instance_id="0",service_name="nodemgr",
  up_pathfail_reason="up_urss_reason_association_release"} 1
  ```

  Label:

  - up_urss_reason_association_release

Usage Monitoring over PCF

Feature Description

SMF supports usage monitoring functionality over the PCF N7 interface for 4G and 5G PDU sessions. After SMF reports the usage data to PCF, SMF supports the modification of usage monitoring parameters, such as Total Volume, Uplink Volume or Downlink Volume thresholds and the disabling of usage monitoring based on non-reception of usage monitoring threshold or related triggers from PCF.

How it Works

This section describes how the SMF usage monitoring over PCF N7 interface works.

Usage Reporting

UPF measures the volume and the time usage of all traffic for the PDU session or the corresponding service data flows. UPF sends the accumulated usage report in either the PFCP Session Report Request or the PFCP Session Modification Response to SMF. Then, SMF includes one or multiple accumulated usage reports in the "accuUsageReports" attribute in one of the following messages towards PCF.

- HTTP POST message

Note This message also includes the "US_RE" value in the "repPolicyCtrlReqTriggers" attribute.

- Message to include the SM Policy Delete Data data structure during the terminate procedure.

Each AccuUsageReport data structure includes the accumulated usage within one or two usage report information elements. These elements are corresponding to a usage monitoring control instance that PCF requested. If the PCF provides both volume and time thresholds and the threshold for one of the measurements reaches, then the UPF communicates this event to the SMF along with the accumulated volume and time measurements. Then, SMF sends the accumulated usage since the last report to PCF for both the measurements.

The SMF receives the accumulated usage report from UPF in the PFCP Session Report Request. After receiving this report, the SMF identifies the list of usage report corresponding to the usage monitoring control instance. Then, SMF posts a PDU Modify or PDU Dedicated bearer procedure. This procedure includes new event type, list of usage reports, and the list of URRs to process them.

Accumulated Usage Report

The following table lists the information available in the accumulated usage report.

Table 21: Accumulated Usage Report

Attribute Name	Data Type	P	Cardinality	Description
refUmIds	String	M	1	Indicate the reference ID for the UsageMonitoringData objects that is associated with the usage report.
volUsage	Volume	O	0.1	Indicate the total accumulated volume usage.
volUsageUplink	Volume	O	0.1	Indicate an accumulated volume usage in the uplink.
volUsageDownlink	Volume	O	0.1	Indicate an accumulated volume usage in the downlink.
timeUsage	DurationSec	O	0.1	Indicate an accumulated time usage.
nextVolUsage	Volume	C	0.1	Indicate an accumulated volume usage after the monitoring time.
nextVolUsageUplink	Volume	O	0.1	Indicate an accumulated volume usage in the uplink after the monitoring time.
nextVolUsageDownlink	Volume	O	0.1	Indicate an accumulated volume usage in the downlink after the monitoring time.
nextTimeUsage	DurationSec	C	0.1	Indicate an accumulated time usage after monitoring.

Usage Monitoring Data Modification

Following are the available data modification scenarios for the usage monitoring over PCF.

- If the PCF needs to remove the threshold level for one or multiple monitoring keys, the PCF provides the corresponding attribute with the NULL value to the corresponding usage monitoring control instance.
- When the PCF receives the accumulated usage in the HTTP POST message, the PCF communicates to SMF whether the usage monitoring continues for the following usage monitoring control instance:
  - If the monitoring continues for the specific levels, the PCF provides the new thresholds for the levels in the response of the HTTP POST message. This message includes the existing attributes, such as "volumeThreshold", "volumeThresholdUplink", and "volumeThresholdDownlink".
  - If the PCF stops monitoring for the specific levels, the PCF doesn't include an updated threshold in the response of the HTTP POST message for the stopped levels. It implies that PCF doesn't include the corresponding attributes in the entry of the "umDecs" attribute. These attributes are "volumeThreshold", "volumeThresholdUplink", "volumeThresholdDownlink", "timeThreshold", "nextVolThreshold", "nextVolThresholdUplink", "nextVolThresholdDownlink", and "nextTimeThreshold".

If the PCF stops the monitoring for the usage monitoring control instance, the PCF doesn't include any thresholds of the usage monitoring control instance in the response of the HTTP POST message. In addition, the PCF doesn't remove the reference of the usage monitoring control instance from the dynamic PCC rule or session rule.

Based on the following scenarios, SMF sends the PFCP Session Modification Request to PCF:

- In case of modification in the existing thresholds, SMF updates the URR with the new thresholds and initiates Update URR towards UPF in the PFCP Session Modification Request.
- In case of stopped monitoring for the usage monitoring control instance, SMF removes the URR and initiates Remove URR toward UPF in the PFCP Session Modification Request.
- In case of new usage monitoring control instance, SMF creates a new URR with the thresholds. SMF also associates the URR to the corresponding PDRs and initiates Create URR along with Update PDR toward UPF in the PFCP Session Modification Request.

Error Handling

While provisioning the usage monitoring on SMF and its actions, following errors can occur:

- If PCF has defined invalid thresholds, the SMF marks the PCC rule as failed or invalid when the Session rule or PCC rule has the reference of monitoring key (UmId) with the invalid thresholds.
- If PCF removes or doesn't configure the US_RE flag between the message exchanges where usage monitoring is active in the SMF, the SMF sends the Remove URR request to UPF in the Modification Request with the available URRs that are created for the N7 interface.

Call Flows

This section describes the following call flows.

- Usage Monitoring Activation call flow
- Usage Reporting call flow

Usage Monitoring Activation Call Flow

This section describes the Usage Monitoring Activation call flow.

Figure 18: Usage Monitoring Activation Call Flow

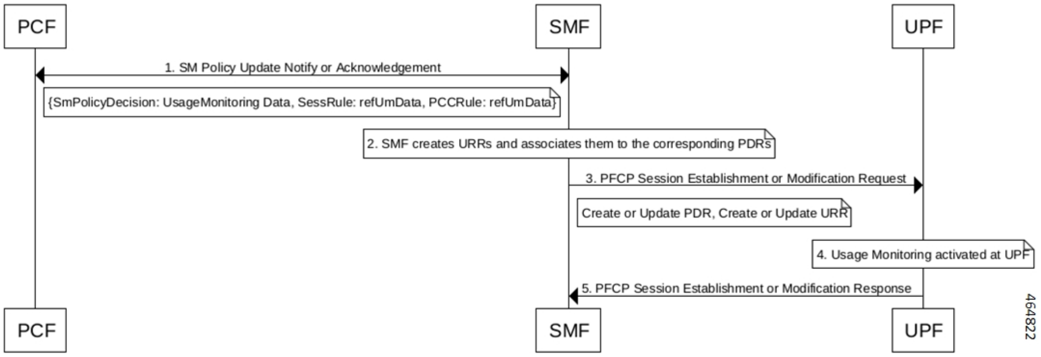

PCF
SMF
UPF
1. SM Policy Update Notify or Acknowledgement
{SmPolicyDecision: UsageMonitoring Data, SessRule: refUmData, PCCRule: refUmData}
2. SMF creates URRs and associates them to the corresponding PDRs
3. PFCP Session Establishment or Modification Request
Create or Update PDR, Create or Update URR
4. Usage Monitoring activated at UPF
5. PFCP Session Establishment or Modification Response
PCF
SMF
UPF
464822

Table 22: Usage Monitoring Activation Call Flow Description

Step	Description
1	PCF sends the list of Usage Monitoring data with thresholds to be monitored and association of the thresholds to either Session or PCC rule level.
2	SMF creates the URR for each monitoring data and associates it to the corresponding PDRs.
3	SMF sends Create or Update URR and links the URR with the corresponding PDR in PFCP Session Establishment or Modification request.
4	UPF activates the monitoring on the received URR.
5	UPF sends the response to SMF with the corresponding cause code.

Usage Reporting Call Flow

This section describes the Usage Reporting call flow.

Figure 19: Usage Reporting Call Flow

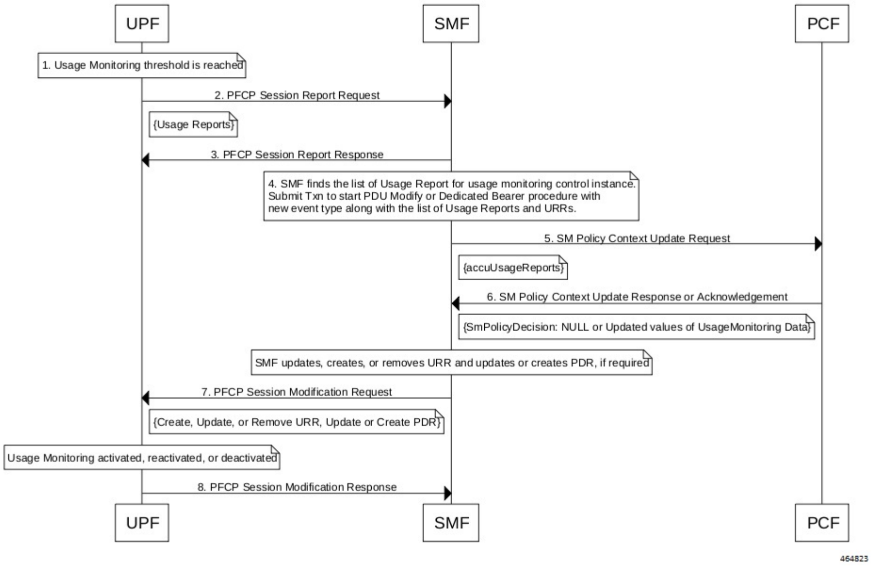

UPF
SMF
PCF
1. Usage Monitoring threshold is reached
2. PFCP Session Report Request
{Usage Reports}
3. PFCP Session Report Response
4. SMF finds the list of Usage Report for usage monitoring control instance. Submit Txn to start PDU Modify or Dedicated Bearer procedure with new event type along with the list of Usage Reports and URRs.
5. SM Policy Context Update Request
{accuUsageReports}
6. SM Policy Context Update Response or Acknowledgement
{SmPolicyDecision: NULL or Updated values of UsageMonitoring Data}
SMF updates, creates, or removes URR and updates or creates PDR, if required
7. PFCP Session Modification Request
{Create, Update, or Remove URR, Update or Create PDR}
Usage Monitoring activated, reactivated, or deactivated
8. PFCP Session Modification Response
UPF
SMF
PCF
464823

Table 23: Usage Reporting Call Flow Description

Step	Description
1	On UPF, the configured usage monitoring threshold limit reaches.
2	UPF sends the PFCP Session Report Request along with the usage information for the URR to SMF.
3	SMF sends PFCP Session Report Response with Cause: PFCP Cause Request Accepted.
4	SMF sends the received usage information to PCF in the Policy Update Request.

Step	Description
5	PCF acknowledges with either updated threshold for monitoring or none to SMF. In case of none, monitoring to SMF is disabled.
6	SMF removes or updates the corresponding URR and sends the modification request to UPF.
7	UPF deactivates or reactivates the monitoring based on the received information.
8	UPF sends the acknowledgment response with the corresponding cause code to SMF.

Standards Compliance

The usage monitoring over PCF feature complies with the following standards.

- *3GPP TS 29.512 version 16.5.0 Release 16—5G; 5G System; Session Management Policy Control Service*

Limitations

This feature has the following limitations:

- If you have enabled the PCC Rule level monitoring, then by default this monitoring gets linked with the URR of the refUmData that is associated with the PCC rule and Session level URR, if exists. The linking exists until PCF excludes it from the session level monitoring in "exUsagePccRuleId".
- While the usage monitoring is in progress, any update of parameters from PCF for a Session or PCC rule without refUmData implies disabling or removal of usage monitoring for that rule. This rule must always include the refUmData even if no change exists.
- SMF doesn't honor the usage report received from UPF after SMF notifies the usage report to PCF and PCF responds with 204—No Content (PCF disables the usage monitoring). In this case, SMF notifies only the UPF with the remove URR for the disabled UmId and locally discards any received usage report.
- By default, SMF links the URR, if it exists, of the Session level to all the active static rules as part of the session. As no URR information exchange happens for static rules between SMF and UPF, the UPF is responsible to monitor the static rules data usage as part of the PDU and Session level monitoring. Then, UPF sends the response to SMF through the Usage report.

Configuring Usage Monitoring Key for Pre-defined Rules

To configure the usage monitoring key for pre-defined rules, use the following sample configuration:

```
config
   active-charging service  service_name
      rulebase  rulebase_name
         action priority  priority_name dynamic-only ruledef ruledef_name
charging-action charging-action_name umid usage-monitoring_identifier
         end
```

NOTES:

- **umid** *usage-monitoring_identifier*: Specify the usage monitoring identifier. The *usage-monitoring_identifier* must be a string.

Note You can associate the usage monitoring identifier for pre-defined rules by local configuration in the **action priority** *priority_name* **dynamic-only ruledef** *ruledef_name* command. After PCF activates this rule, the SMF fetches usage monitoring thresholds that SMF receives from PCF. SMF creates the URR and associates it with the created PDRs of the pre-defined rules and then sends them to UPF. Then, UPF honors these URR and reports the usage back to SMF.

Configuration Verification

To verify the configuration, use the following command:

show running-config active-charging service *active-charging_service_name* **rulebase** *rulebase_name* **action priority** *action_priority* **dynamic-only ruledef**

If the usage monitoring key is configured, then the value appears as part of the **umid** configuration in the following output.

```
show running-config active-charging service acs1 rulebase rba1
   active-charging service acs1
      rulebase rba1
        action priority 1 dynamic-only ruledef rda1 charging-action ca1 description myrule1

        action priority 2 dynamic-only ruledef rda1 charging-action ca1 description myrule2
 umid 54
        action priority 3 dynamic-only ruledef rda3 charging-action ca3 description myrule3

      exit
     exit
```

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Usage Monitoring Statistics

The SMF-Service (smf-service) pod supports the following statistics:

PolicyPcfUpdatesTotal

- Description: Display the number of times Usage Report sent towards PCF.
- Metrics-Type: Statistics
- Labels:
  - Label: **smf_current_procedure**
    - Description: Display the current running procedure.
    - Value: PDU Session Modify – PCF-initiated or PDN Session Modify—Bearer Add, Delete, or Modify
  - Labels:

- Label: **trigger**
  - Description: Displays the trigger for the procedure initiated at SMF
  - Value: usage_report

QoS Group of Ruledefs Support over N7

Feature Description

The QoS Group of Ruledef feature enables the PCF to define and enforce Fair-Usage-Policy (FUP) per subscriber. This feature enables changing certain charging-action parameters and all QoS-of-ruledefs parameters per individual subscriber session.

QoS Group of Ruledefs is also called as QGR.

The following attributes of QoS-group-of-ruledefs are supported:

- Precedence or Priority: Priority of a QoS-group-of-ruledefs implies priority of applying QoS-parameters of a QoS-group-of-ruledefs to an incoming data packet. If a packet matches a ruledef which is part of multiple QoS-groups activated for the session, then QoS parameters of the QoS-group-of-ruledefs with highest priority (precedence) is applied to the packet. A lower priority number indicates higher priority of application of QoS parameters of that group. Priority of a QoS-group-of-ruledefs is set by PCF for each subscriber session.
- Flow-Status: Describes whether the IP flows are enabled or disabled. Possible values are:
  - Enabled uplink
  - Enabled downlink
  - Enabled
  - Disabled
  - Removed

  Default value is Enabled.

Note Attributes of QosGroupRuleDefs IE cannot be defined using CLI commands. These attributes can only be set and changed by PCF.

Individual ruledefs cannot be dynamically added or removed from a predefined QoS-group-of-ruledefs received over the N7 interface.

How it Works

This section describes how the QoS Group of Ruledef feature is implemented.

UPF provisions the configuration of QoS-group-of-ruledefs under the Active Charging Service (ACS). The CLI allows addition and removal of charging and dynamic ruledefs to a named QoS-group-of-ruledefs. A single ruledef can be part of multiple QoS-group-of-ruledefs. In this scenario, a QGR with higher priority is enforced or considered, where priority is communicated through Precedence IE by PCF over N7 interface.

PCF is aware of the names of all QoS-group-of-ruledefs and their related ruledefs configured on SMF. The PCF activates and removes QoS-group-of-ruledefs for a subscriber session using proprietary AVP in N7 message. This AVP specifies the name of the QoS-group-of-ruledefs to activate or to remove.

A subscriber may not have any QoS-group-of-ruledefs activated. Incoming traffic may match a ruledef, which has no associated QoS-group-of-ruledef for that subscriber session. In that case, action is taken based only on the configuration for that ruledef.

QGR Processing Flow

The following is the QGR processing logic at UPF.

- On receiving a IE ‘Qos-Group-Of-Ruledef', search for the QGR in static configuration. For each ruledef or group-of-ruledef in QGR, look up for its corresponding PDR and update the FAR and QER list with the received QGR FAR and QER IDs.
- For each ruledef or group-of-ruledef PDR on UPF, associate high priority QGR’s FAR-ID and QER-ID.
- Maintain QGR map at both SMF and UPF. It consists of QGR name, precedence, QER-ID, and FAR-ID. Use QGR map for recovery and lookup whenever required.

QGR Parameters

The SMF sends the QGR parameters in Session Establishment or Modification Request to UPF through N4 interface.

QGR Name and Precedence is sent in a custom IE "QGR-INFO-LIST". Flow-action and bandwidth parameters create a new FAR and QER respectively.

Any changes to QGR dynamic parameters trigger an update to FAR and QER.

This IE is sent in Session Establishment or Modification Request.

QGR IE

```
Qos-Group-Of-Ruledef:
Name:
Operation:  (0 – Add  1 - Modify 2 - Delete)
Precedence:
FAR ID:
QER ID:
```

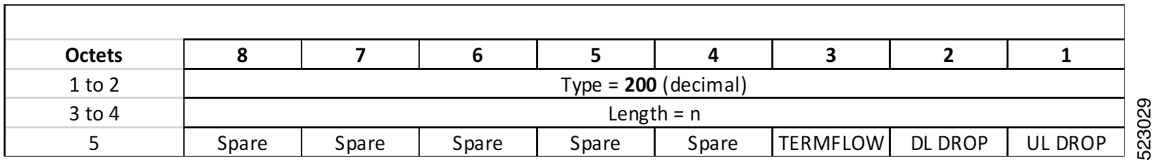
Custom IEs at UPF

This section lists the custom IEs that are available at UPF.

Extended Apply Action

The Extended Apply Action IE indicates the action(s) the UPF is required to apply to packets. It is coded as shown in the following figure.

Figure 20: Extended Apply Action IE



Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **200** (decimal)							
3 to 4	Length = n							
5	Spare	Spare	Spare	Spare	Spare	TERMFLOW	DL DROP	UL DROP

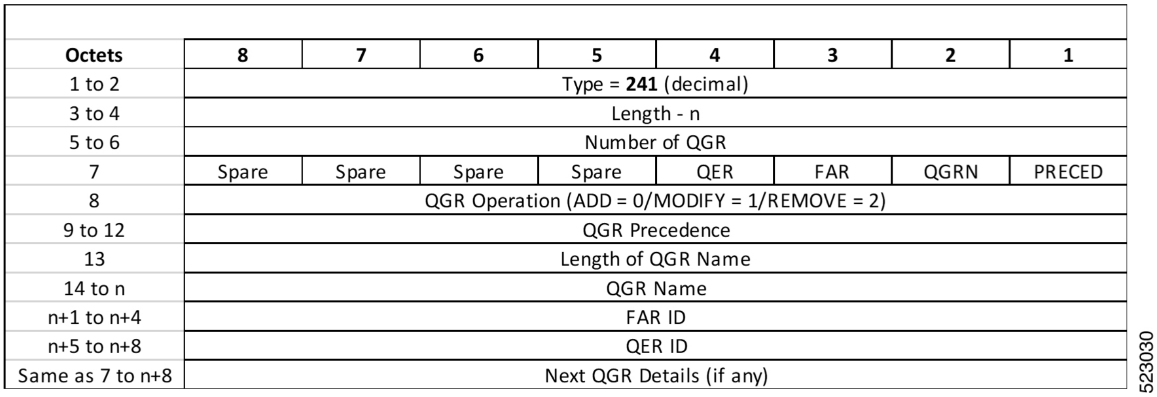
The octet 5 is encoded as follows:

- Bit 1 – UL DROP (Drop Uplink): when set to 1, this indicates a request to drop uplink packets.
- Bit 2 – DL DROP (Drop Downlink): when set to 1, this indicates a request to drop downlink packets.
- Bit 3 – TERMFLOW (Terminate/Kill Flow) : when set to 1, this indicates a request to terminate the flow.
- Bit 4 to 8 – Spare, for future use and set to 0.

QGR-INFO List

The QGR-INFO List IE indicates the information about the QoS Group received from the PCF to UPF which identifies the flow and applies the received parameters. It is coded as shown in the following figure.

Figure 21: QGR-INFO List IE



Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **241** (decimal)							
3 to 4	Length - n							
5 to 6	Number of QGR							
7	Spare	Spare	Spare	Spare	QER	FAR	QGRN	PRECED
8	QGR Operation (ADD = 0/MODIFY = 1/REMOVE = 2)							
9 to 12	QGR Precedence							
13	Length of QGR Name							
14 to n	QGR Name							
n+1 to n+4	FAR ID							
n+5 to n+8	QER ID							
Same as 7 to n+8	Next QGR Details (if any)							

The octet 7 (bit vector for the QGR Information) is encoded as follows:

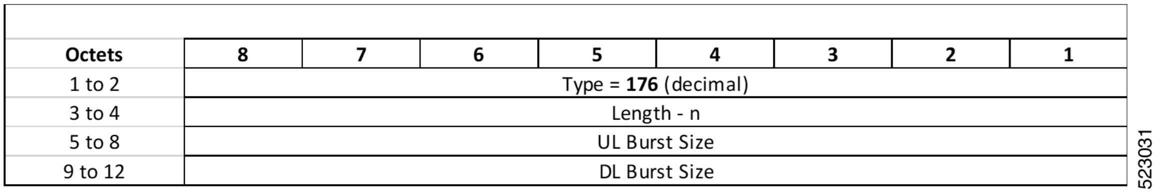
- Bit 1 – PRECED (Precedence): when set to 1, this indicates precedence is present.
- Bit 2 – QGRN (QGR Name): when set to 1, this indicates QGR Name is present.
- Bit 3 – FAR : when set to 1, this indicates FAR ID is present.
- Bit 4 – QER: when set to 1, this indicates QER ID is present.
- Bit 5 to 8 – Spare, for future use and set to 0.

SMF encodes the QGR information based on this bit vector field.

Burst Size

The Burst Size IE indicates the information about the UL and DL burst size for MBR to UPF. It is coded as shown in the following figure.

Figure 22: Burst Size IE

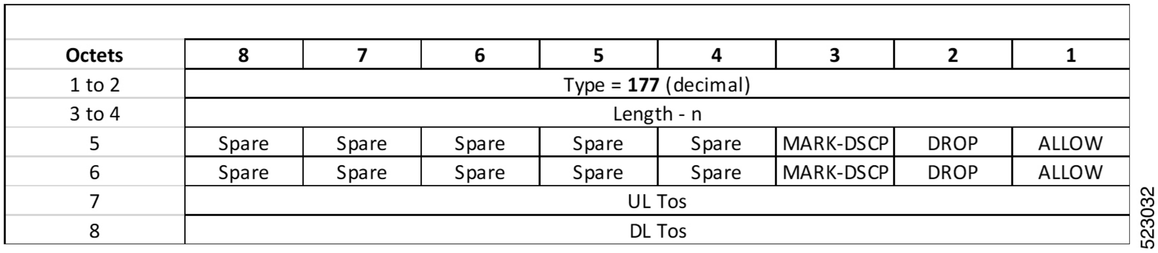


Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **176** (decimal)							
3 to 4	Length - n							
5 to 8	UL Burst Size							
9 to 12	DL Burst Size							

Conform Action

The Conform Action IE indicates the action(s) the UPF is required to apply to packets for both UL and DL. It is coded as shown in the following figure.

Figure 23: Conform Action IE

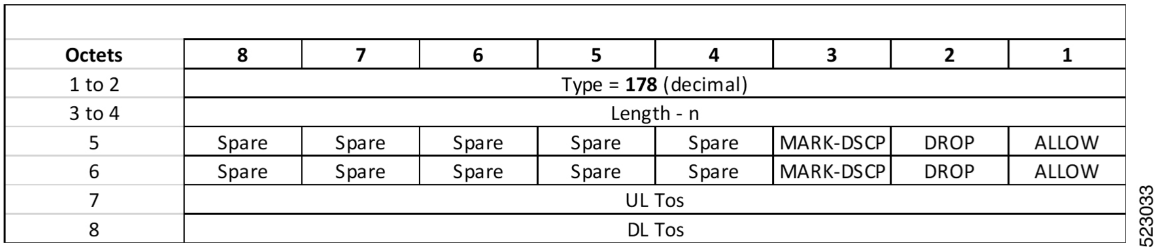


Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **177** (decimal)							
3 to 4	Length - n							
5	Spare	Spare	Spare	Spare	Spare	MARK-DSCP	DROP	ALLOW
6	Spare	Spare	Spare	Spare	Spare	MARK-DSCP	DROP	ALLOW
7	UL Tos							
8	DL Tos							

Exceed Action

The Exceed Action IE indicates the action(s) the UPF is required to apply to packets for both UL and DL. It is coded as shown in the following figure.

Figure 24: Exceed Action IE



Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **178** (decimal)							
3 to 4	Length - n							
5	Spare	Spare	Spare	Spare	Spare	MARK-DSCP	DROP	ALLOW
6	Spare	Spare	Spare	Spare	Spare	MARK-DSCP	DROP	ALLOW
7	UL Tos							
8	DL Tos							

The following tables provide information on the custom IEs included in the N4 messages.

Table 24: FAR Format

FAR ID	Unique ID
Extended Apply Action	Private IE to include Flow-Action Allow as well Discard Uplink, Discard Downlink, and Terminate Flow. The value of Extended Apply Action is derived from FlowStatus IE value received in QosGroupOfRuledef IE from PCF.

Table 25: QER Format

QER ID	Unique ID
Maximum Bitrate	MBR of QGR in Kbps. • UL MBR • DL MBR
Burst Size	Private IE to include the burst size. • UL Burst • DL Burst
Conform Action	Private IE to configure the conform action. • Uplink Action • Uplink ToS • Downlink Action • Downlink ToS
Exceed Action	Private IE to configure the exceed action. • Uplink Action • Uplink ToS • Downlink Action • Downlink ToS

Custom IEs at PCF

The PCF sends the custom IE "QosGroupRuleDefinition" in SmPolicyDecision attribute to the SMF. This IE comprises QosGroupRuleName, refQosGroupQosData, FlowStatus, and Precedence attributes.

PCF triggers “Add/Update QGR” by sending QosGroupRuleName as key and QosGroupRuleDefinition as value (with all attributes) in QGRDefs map.

For QGR removal, PCF triggers “Remove QGR” by sending QosGroupRuleName as key and the value is set to NULL.

The following tables list the custom IEs that are sent by the PCF.

Table 26: SmPolicyDecision Attribute

Attribute name	**Data type**	**P**	**Cardinality**	**Description**	**Applicability**
qosGroupQosData	Map(QosGroupQosData)	O	1..N	A map of qosGroupQosInfo with the content being the QosGroupQosData.	qosGroupQosInfo
qosGroupRuleDefs	Map(QosGroupRuleDef)	O	1..N	A map of QosGroupOfRuledefs with the content being the QosGroupRule Definition.	

Table 27: QosGroupRuleDef Attribute

Attribute name	Data type	P	Cardinality	Description	Applicability
qosGroupRuleId	string	M	1	Uniquely identifies the Qos Group of Ruledef (QGR) configured at SMF	
refQosGroupQosData	string	M	1	A reference to QosGroupQosData	
flowStatus	FlowStatus	O	0..1	Describes whether the IP Flows are enabled or disabled. Possible values: Enabled uplink, Enabled downlink, Enabled, Disabled, Removed Default value "Enabled" is applied.	
precedence	Uinteger	M	0..1	Describes the priority of the Qos Group of Ruledef identified with QosGroupRuleName.	

Table 28: QosGroupQoSData Attribute

Attribute Name	Data type	P	Cardinality	Description	Applica
qosId	String	M	1	Univocally identifies the QoSGroupQosData	

maxbrDL	BitRateRm	M		Indicates the maximum bandwidth in downlink.	
maxbrUL	BitRateRm	M		Indicates the maximum bandwidth in uplink.	
mbrBurstSizeUL	MaxDataBurstVol	O		Describes the amount of data that can be sent at peak rate in uplink	
mbrBurstSizeDL	MaxDataBurstVol	O		Describes the amount of data that can be sent at peak rate in downlink	
mbrConformActionUL	RateLimitAction	O		Describes the ratelimiting action to be taken as long as traffic stays within maxbitrate in uplink.	
mbrConformActionDL	RateLimitAction	O		Describes the ratelimiting action to be taken as long as traffic stays within maxbitrate in downlink.	
mbrExceedActionUL	RateLimitAction	O		Describes the ratelimiting action to be taken if traffic exceeds maxbitrate in uplink.	
mbrExceedActionDL	RateLimitAction	O		Describes the ratelimiting action to be taken if traffic exceeds maxbitrate in downlink.	

Table 29: RateLimitAction Attribute

Attribute Name	Data type	P	Cardinality	Description	Applicability
action	Action	M		Describes the ratelimiting action. Enum Action with possible values: ALLOW, DROP,MARK_DSCP	
tosTrafficClass	string	C		Contains the IPv4 Type-of-Service and mask field or the IPv6 Traffic-Class field and mask field. tosTrafficClass IE is present only in case action IE has value MARK_DSCP.	

Data Path Enforcement

The following is the sequence for the data traffic enforcement performed at UPF.

1. Verify whether the incoming data traffic matches the http ruledef.
2. Check if there is a QGR with the matched ruledef or group of ruledefs. If a match is found, the highest priority QGR is returned.

Note The ruledef or group of ruledefs can be either static or predefined.

3. If the QGR matches, then Flow-Action enforcement is first performed at Charging-Action level and then at QGR level assuming Charging-Action has allowed the packet. If the packet is dropped, then QGR-level Flow-Action enforcement is skipped.
4. If Flow-Action at QGR allows the packet to pass, then the Bandwidth Limiting or QoS Enforcement Rule (QER) Limiting is enforced on the data packet. If it is dropped at QGR, QER Limiting is skipped.
5. Unlike the Flow-Action enforcement, the QER Limiting is also performed first at Charging-Action Level and then at the QGR subject to packet being allowed at Charging-Action.

Call Flows

This section describes the key call flows for this feature.

QoS Group of Ruledef Activation Call Flow

This section describes the call flow associated with the activation of QoS Group of Ruledefs.

Figure 25: Qos-Group-of-Ruledef Activation Call Flow

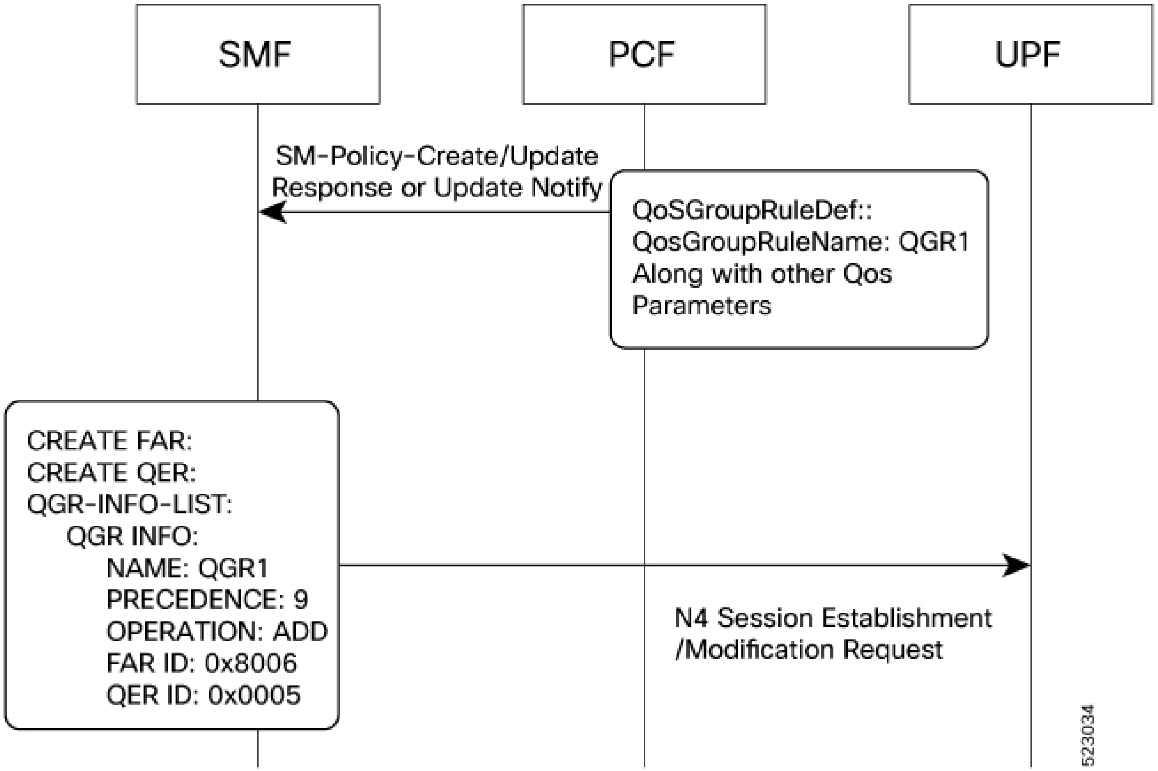


Table 30: Call Flow Description for Activation of QoS Group of Ruledefs

Step	Description
1	PCF activates the qos-group-of-ruledefs through the custom IE 'QosGroupRuleDefs' received in N7 messages. The QosGroupRuleDefs IE comprises QosGroupRuleName, refQosGroupQosData, FlowStatus, and Precedence. PCF triggers "Add QGR" by sending QosGroupRuleName as key and QosGroupRuleDef as value (with all attributes) in QGRDefs map. PCF sends the QosGroupRuleDefs IE to the SMF through N7 Policy association establishment response or policy association update request message.
2	The SMF prepares Create FAR and QER for each QGR received from PCF and encodes QoS group names along with the corresponding FAR IDs and QER IDs in QGR-INFO-LIST IE to be sent on N4 interface session establishment or modification request.

QoS Group of Ruledef Modification Call Flow

This section describes the call flow associated with the modification of QoS Group of Ruledefs.

Figure 26: Qos-Group-of-Ruledef Modification Call Flow

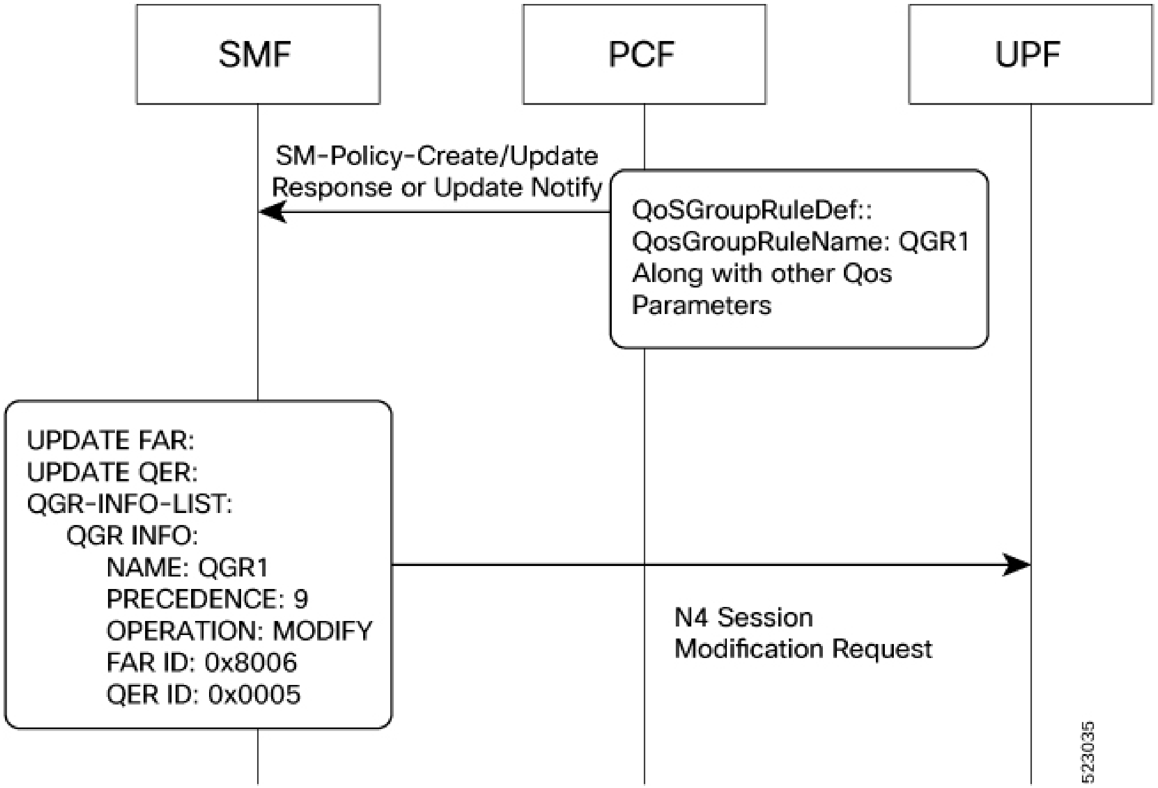


Table 31: Call Flow Description for Modification of QoS Group of Ruledefs

Step	Description
1	Once qos-group-of-ruledefs is activated, PCF modifies the QoS parameters through 'QoSGroupRuleName' IE sent in SM policy association establishment response and SM policy association update request from N7 messages. PCF triggers "Modify QGR" by sending QosGroupRuleName as key and QosGroupRuleDef as value (with all attributes) in QGRDefs map. PCF sends the QosGroupRuleDefs IE to the SMF through N7 policy association establishment response or policy association update request message.
2	SMF prepares Update FAR and QER for each QGR received for modification and encodes the activated QoS group names along with the corresponding FAR IDs and QER IDs in QGR-INFO-LIST to be sent on N4 session establishment or modification request.

QoS Group of Ruledef Deactivation Call Flow

This section describes the call flow associated with the deactivation of QoS Group of Ruledefs.

Figure 27: Qos-Group-of-Ruledef Deactivation Call Flow

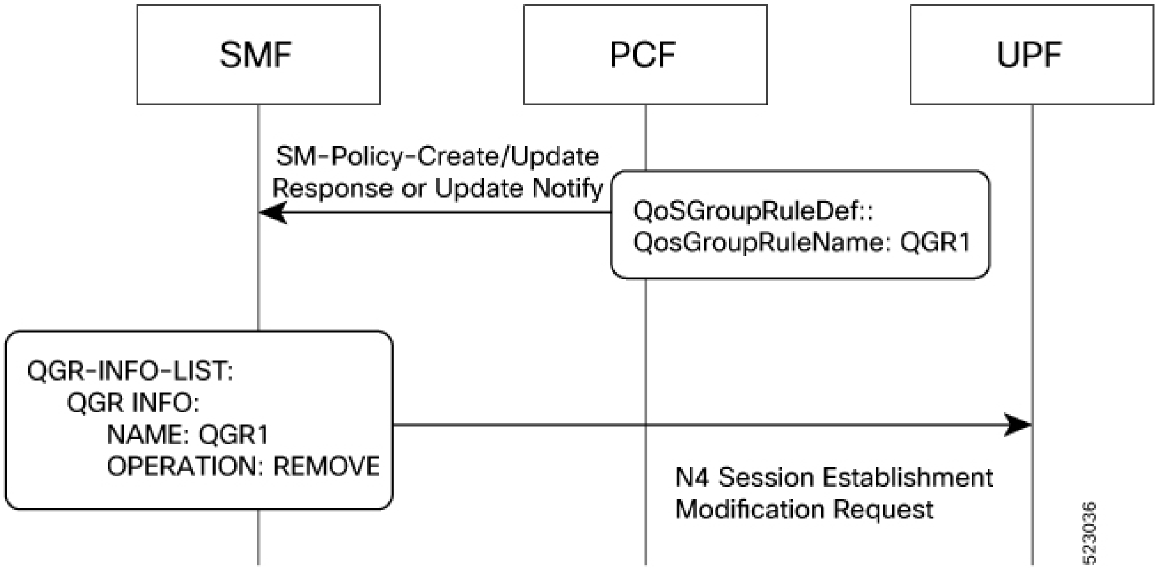


Table 32: Call Flow Description for Deactivation of QoS Group of Ruledefs

Step	Description
1	PCF deactivates qos-group-of-ruledefs through 'QosGroupRuleDefs' IE by sending only the map key which is QosGroupRuledefName with a value as NULL.
2	SMF encodes the deactivated QoS group of ruledef names along with the operation "Remove" in QGR-INFO-LIST to be sent in N4 session modification request.

Limitations

The QoS Group of Ruledefs support feature has the following limitations:

- Monitoring-Key associated with the QGR will not be usage monitored. That is, URR creation and enforcement are not supported.
- PCF will not send the QosGroupRuleDef IE separately. It will be sent along with the PCC rules.
- SMF supports up to a maximum 20 QosGroupRuleDefs. That is, SMF accepts only initial 20 QosGroupRuleDefs from PCF.
- QosGroupRuleDef attribute from PCF will not be ignored if invalid value is received for FlowStatus attribute. FlowStatus will be considered as ENABLED which is the default value of the attribute.