



Charging Support

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 2](#)
- [How it Works, on page 2](#)
- [Configuring Credit Control for Usage Reporting, on page 9](#)
- [Configuring ACS Rulebase for Usage Reporting, on page 9](#)

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
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
Usage reporting with Rating-Group and Service ID is introduced.	2020.02.5
First introduced.	2020.02.0

Feature Description

The usage measurement and reporting function in User Plane Function (UPF) is controlled by the Session Management Function (SMF). The SMF controls these functions by:

- Creating the necessary PDRs to represent the service data flow, application, bearer or session (if they are not existing already).
- Creating the URRs for each Charging Key and combination of Charging Key and Service ID. Also, creating URRs for a combination of Charging Key, Sponsor ID, and Application Service Provider Id.
- Associating the URRs to the relevant PDRs defined for the PFCP session, for usage reporting at SDF, Session or Application level.
- For online charging, the SMF provisions Volume and Time quota, if it receives it from the Online Charging Server (OCS).

Offline Charging Events Reporting over N4

The User Plane Function (UPF) supports session-based offline charging, PDU session level reporting triggers in URR (volume and time threshold), PFCP session report procedure, and usage report IE support in the PFCP modification response for the Session-AMBR change, QoS, and User Location triggers.

Online Charging Support over N4

The UPF supports flow-based online charging support, which includes URR enhancements for Volume and Time quota and Usage reporting IE in PFCP modify response. In addition, the UPF supports online charging triggers, which include a PFCP session report request support with usage reporting IE.

How it Works

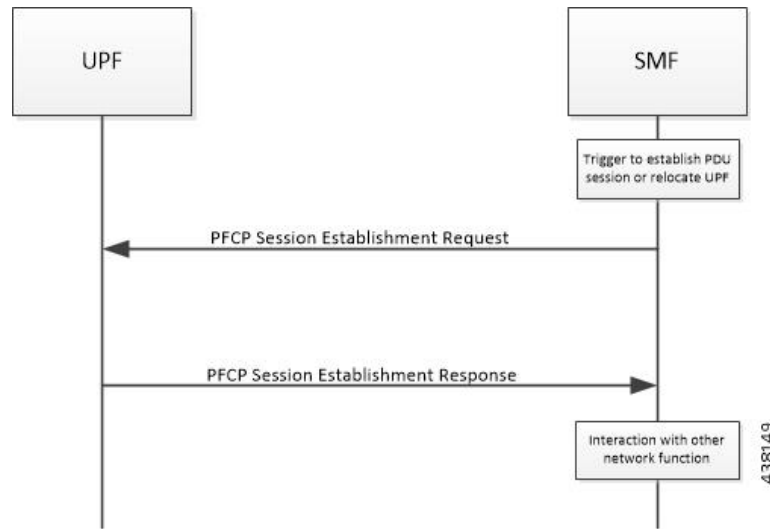
Call Flows

The following sections describe the call flows between SMF and UPF for PFCP Session Management.

PFCP Session Establishment Procedure

The PFCP Session Establishment procedure establishes a PFCP session between SMF and UPF. It also configures rules in UPF for handling incoming packets. In addition, the SMF sends Create URR IE, which comprises of triggers and thresholds that are intended for reporting.

The following call flow depicts the PFCP Session Establishment procedure.

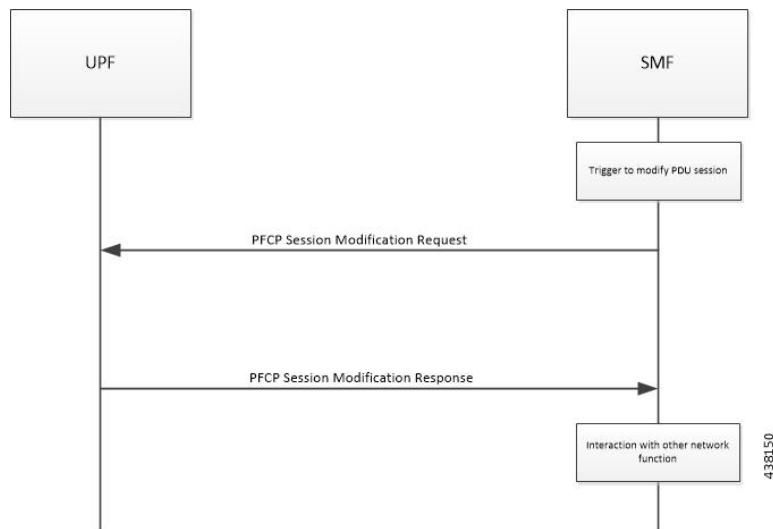


Step	Description
1	The SMF receives the trigger to establish a new PDU Session or change the UPF for an established PDU Session.
2	The SMF sends the PCFP Session Establishment Request message to the UPF. This message contains the structured control information, which defines the UPFs behavior.
3	The SMF provisions URR with Create URR IE. The Create URR associates with PDRs by adding URR-ID IE in Create PDR IE. It includes various triggers and thresholds for usage reporting.
4	When the same URR is associated with multiple PDRs, URRs are linked with another URR. Therefore, if a report for an URR is sent, its linked URR is also reported.
5	The UPF responds with the PCFP Session Establishment Response message to the SMF. For instance, Created PDR IE, in which UPF Flow-TEID is sent to gNB for GTP-u encapsulation for data traffic.
6	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

PCFP Session Modification Procedure

The SMF uses the PCFP Session Modification procedure to modify an existing PCFP session on the UPF. For instance, configuring a new rule, modifying an existing rule, or deleting an existing rule, and so on. The SMF sends the Create URR IE, Update URR IE (to update the trigger or threshold) and Remove URR IE (to remove an existing URR created earlier by SMF during Session Establishment Procedure) in the same message.

The following call flow depicts the PCFP Session Modification procedure.

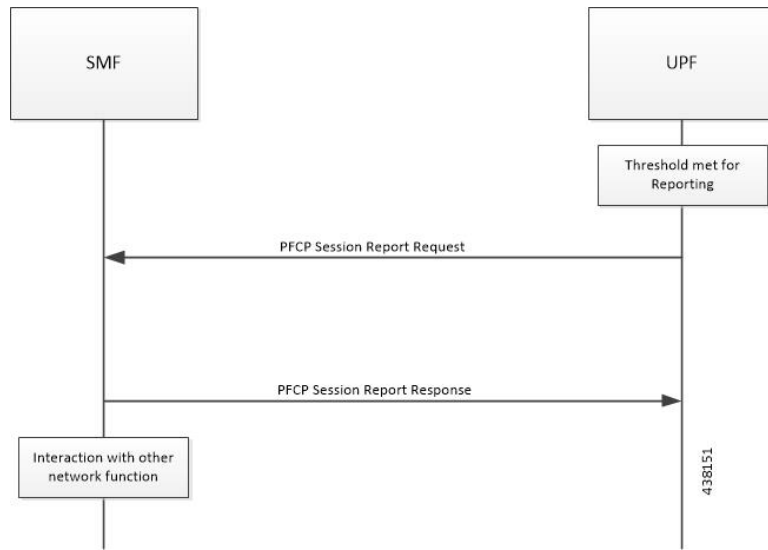


Step	Description
1	The SMF receives the trigger to modify the existing PDU Session.
2	The SMF sends an N4 session modification request message to the UPF. This message contains the structured control information, which defines the UPFs behavior.
3	The UPF identifies the PFCP session context for the Session ID to modify. It updates the parameters of this session context according to the list of parameters sent by the SMF. It then responds with a PFCP Session Modification Response message. The message contains the information, which the UPF must provide to the SMF (in response to the control information received).
4	If the SMF sends the QAURR flag set in PFCPSMReq-Flag IE or URR ID (s) with Query URR IE (e), then UPF sends the usage report IE for the corresponding URR with the PFCP Session Modification response.
5	The UPF provisions and acts based on the Create URR, Update URR or Remove URR IE sent by the SMF.
6	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

PFCP Session Reporting Procedure

The UPF uses PFCP Session Reporting procedure to report information that is related to the PFCP session to the SMF (usage report IE). Once the threshold hits the volume, time or event measurement and sets the corresponding trigger for reporting, the message is sent to the SMF by the UPF.

The following call flow depicts the PFCP Session Reporting procedure.

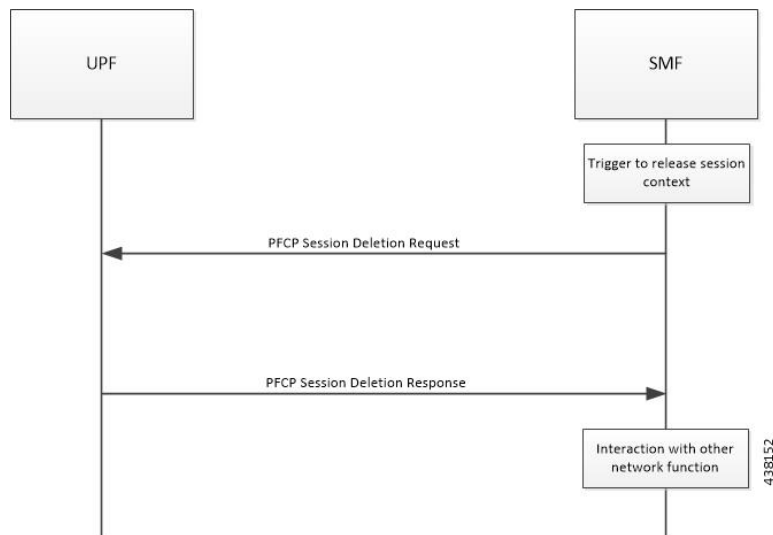


Step	Description
1	Once the provisioned threshold is met (for time, volume or event, and trigger is set for reporting), the UPF sends PFCP Session Report Request with usage report IE and usage details for volume, time, or threshold.
2	The SMF responds with PFCP Session Modification Response with success or failure message. No failure handling is needed on the UPF.
3	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

PFCP Session Deletion Procedure

The PFCP Session Deletion procedure deletes an existing PFCP session between the SMF and UPF. The SMF initiates a PFCP Session Deletion procedure toward the UPF to delete an existing PFCP session. The UPF sends the Session Deletion Response including the Usage Report for all URRs provisioned earlier.

The following call flow depicts the PFCP Session Deletion procedure.



Step	Description
1	The SMF receives the trigger to remove the PFCP session context for the PDU Session.
2	It sends the PFCP Session Delete Request message to the UPF.
3	The UPF identifies the PFCP session context for the Session ID to remove. It then removes the whole session context. In addition, the UPF responds with a PFCP Session Delete Response message that contains any information the UPF provides to the SMF. For instance, the UPF sends usage report for all the URR provisioned for this session.
4	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

IEs Supported for Offline Charging Reporting

The following trigger Information Elements (IEs) support offline charging Reporting over N4:

- **Periodic Reporting** – When this trigger is set, the UPF sends resource usage report periodically to Session Management Function (SMF). The intervals that are required for periodic reporting are sent with the measurement period IE.
- **Volume Threshold (when the volume threshold reaches UL, DL, and Total)** – This trigger is set when the volume-based measurement is required. The SMF sends the traffic volume value along with the volume threshold IE, while the UPF sends the traffic usage report when the traffic volume is reached for the specific Usage Reporting Rule (URR).
- **Time Threshold (when the time threshold is reached)** – This trigger is set when the time-based measurement is set. The SMF sends the time threshold value along with the time threshold IE, while the UPF sends resource usage report when the time threshold is reached for the specific URR.
- **Linked Usage Reporting** – The UPF sends the usage report of this specific URR when this trigger is set. In addition, the usage report is sent to any of the URRs linked to UPF when this trigger is set. The UPF sends the linked URR-Id along with the linked URR-Id IE.

- Packet Forwarding Control Protocol (PFCP) Session Deletion – A usage report generates (in a PFCP Deletion Response) for a URR due to the termination of the PFCP session. Similarly, a usage report generates (in a PFCP modification response) for a URR due to the removal of a specific URR.
- Update URR – This trigger is set when update URR request is received.

IEs Supported for Online Charging Reporting

The following IEs support online charging:

- Volume Quota – The SMF requests the UPF to stop forwarding packets or allow forwarding some limited user plane traffic (based on the operator policy in UPF) with this IE. If no Volume Threshold is provisioned – to generate a usage report – and when the measured traffic reaches the quota, this IE is used.
- Time Quota - The SMF requests the UPF to stop forwarding packets or allow forwarding some limited user plane traffic (based on operator policy in UPF) with this IE. If no Volume Threshold is provisioned – to generate a usage report – and when the measured traffic reaches the quota, this IE is used.
- Monitoring Time – This IE is used by the SMF to send the time (UTC format) at which the UPF can re-apply the volume or time threshold. Also, the SMF sends any one of the Subsequent Volume, Time, Volume Quota, Time Quota, and Quota IEs, which is re-applied at the Monitoring Timestamp.
- FAR (Forwarding Action Rule) ID for Quota Action – This IE is used by the SMF to identify the substitute FAR the UPF applies – for the traffic that is associated to the URR – when any of the Volume, Time or quota is exhausted. This FAR requires the UPF to drop the packets or redirect the traffic toward a redirect destination.
- Subsequent Volume Threshold – When volume-based measurement is used and Monitoring Time IE is available, this IE is also present. The presence of this IE indicates the existence of the traffic volume value (the network resources usage reported by the UPF to the SMF) for this specific URR and the period after the Monitoring Time.
- Subsequent Time Threshold - When time-based measurement is used and Monitoring Time IE is available, this IE is also present. The presence of this IE indicates the existence of the time usage (the network resources usage reported by the UP function to the CP function) for this specific URR and the period after the Monitoring Time.
- Linked URR ID – When the linked usage reporting is required, this IE is used. It is possible to link multiple URR-IDs with an URR. Also, linked usage reporting is also sent in the Reporting Trigger IE.
- Measurement Method – The SMF specifies the measurement method of the network usage with the presence of this IE. The measurement method is based on volume and duration.
- Measurement Period – This IE is present to modify the measurement period.
- Periodic Reporting - When this trigger is set, the UPF sends resource usage report periodically to the SMF. The intervals that are required for periodic reporting are sent with the measurement period IE. When the trigger is set to 1, a request for periodic reporting is sent.
- Volume Threshold – This trigger is set when volume-based measurement is required. The SMF sends the traffic volume value along with the volume threshold IE, while the UPF sends the traffic usage report when the traffic volume is reached for the specific Usage Reporting Rule (URR). When the trigger is set to 1, a request for reporting – when the data volume usage reaches a volume threshold – is sent.
- Time Threshold - This trigger is set when time-based measurement is set. The SMF sends the time threshold value along with the time threshold IE, while the UPF sends resource usage report when the

time threshold is reached for the specific URR. When the trigger is set to 1, a request for reporting – when the time usage reaches a time threshold - is sent.

- Start of Traffic – The UPF sends the Usage Report once the traffic starts for an application, when this trigger is set.
- Linked Usage Reporting - The UPF sends the usage report of this specific URR when this trigger is set. In addition, the usage report is sent to any of the URRs linked to UPF when this trigger is set. The UPF sends the linked URR-Id along with the linked URR-Id IE. When the trigger is set to 1, a request for linked usage reporting is sent.

Usage Reporting in PFCP Modification Response

The UPF sends session modification response after receiving session modification request based on the IEs received in the request message. The UPF includes usage report IE in the session modification response for the following scenarios:

- Query URR Handling—The URR-Id IE is included when the SMF requests immediate usage reports from the UPF in the session modification response (for the URR-Id present in this specific IE).
- Query All URRs (QAURR) Handling—The UPF sends the usage report with session modification response for all the URRs provisioned prior by the SMF for this PFCP session once it receives the QUARR flag set in PFCPSMReq-Flags IE from SMF.
- Update URR—The SMF updates the new value of the existing IE with the old value during the session modification procedure.
- Remove URR—During the session modification procedure, the SMF removes the IE, which is not received but was available earlier.

Usage Reporting for Online and Offline Charging

Usage Reporting for Online and Offline Charging is supported in the following ways:

- URR for online charging based on Rating-Group level even if the Service ID is present under Charging-Action. This behavior is seen when diameter ignore-service-id is configured under Credit Control Group.
- URR for offline charging based on a combination of Rating-Group level and Service ID, for static and predefined rules, as configured in the Charging-Action.

Both URRs are linked by the SMF. These URRs are linked such that when an online URR is reported, an offline URR is also reported.

Usage Reporting with Rating-Group and Service ID

The functionality enables usage reporting to the SMF with the Rating-Group (RG) and/or Service ID (SI) populated in the Usage Report IE within the Session Report Request.

The RG and SI are populated using proprietary PFCP IEs and are applicable for usage reporting of URRs associated only with Static and Predefined configured rules. The values are derived from the configured

charging-action associated with the ruledefs, resulting in creation of the URRs during predefined activation or traffic hit for static rules.

Any change in RG/SI properties of the charging-action is reflected only in new URRs. The existing URRs associated with such charging-actions continue to report usage with the earlier RG+SI values.

UPF does not differentiate between usage reporting for Online and Offline URRs, and reports the RG+SI/RG/SI values configured in the charging-action, resulting in creation of the URRs.

NOTE: To know how SMF handles this functionality, refer *Dynamic Configuration Change Support* section in the *SMF Charging* chapter of *UCC 5G SMF Configuration and Administration Guide*.

Implementing the QAURR Flag

The SMF sets the QAURR flag of PFCPSMReq-Flags IE to request immediate usage reports for all the URRs previously provisioned earlier. Alternatively, SMF queries report for selected URR by sending URR-ID with Query URR IE. The UPF sends the usage report IE for corresponding URR with PFCP session modification response when the SMF sends the QAURR flag set in PFCPSMReq-Flag IE or URR-Id with Query URR IE.

Configuring Credit Control for Usage Reporting

This configuration enables to accept/ignore service ID in the Service-Identifier AVP defined in the Diameter dictionaries.

```
configure
  require active charging
  active-charging service service_name
    credit-control group group_name
      diameter ignore-service-id
    end
```

- **diameter ignore-service-id** : This command can be used to disable the usage of the Service-Identifier AVP for Gy interface implementations even if any of the Diameter dictionaries support the Service-Identifier AVP, and if this AVP should not be used for Gy interactions but must be present in GCDRs/eGCDRs.

Configuring ACS Rulebase for Usage Reporting

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.

```
configure
  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 ] }
  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*: Specifies 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*]}: Configures the priority order in which ruledefs are matched and the associated charging action.
 - *priority* must be an integer value in the range of 1-65535.
 - *monitoring_key* must be an integer value in the range of 100000-4000000000.
- **cca quota** { **holding-time** *holding_time* **content-id** *content_id* | **retry-time** *retry_time* [**max-retries** *retries*]}: Configures the quota for the online charging.
 - *holding_time*: must be an integer value in the range of 1-4000000000
 - *content_id*: must be an integer value in the range of 1-2147483647
 - *retry_time*: must be an integer value in the range of 0-86400
 - *retries*: must be an integer value in the range of 1-65535
- **credit-control-group** *cc_group_name*: Configures the online charging parameters used by this rulebase. *cc_group_name* must be an alphanumeric string of 1 to 63 characters.
- **dynamic-rule order**: Configures the order of dynamic rule matching vs the static rules in a rulebase.
- **egcdr threshold** { **interval** *interval* [**regardless-of-other-triggers**] | **volume** { **downlink** | **total** | **uplink** } **bytes** }: Configures the threshold for offline charging.
 - **interval**: must be an integer value in the range of 60-40000000.
 - **downlink**: must be an integer value in the range of 100000-4000000000. Default: 4000000000.
 - **uplink**: must be an integer value in the range of 100000-4000000000. Default: 4000000000.

- **total**: must be an integer value in the range of 100000-4000000000.
- **route priority** *route_priority* **ruledef** *ruledef_name* **analyzer** { **dns** | **file-transfer** | **ftp-control** | **ftp-data** | **h323** | **http** | **imap** | **mip6** | **mms** | **pop3** | **pptp** | **radius** | **rtcp** | **rtp** | **rtsp** | **sdp** | **secure-http** | **sip** [**advanced** | **basic-and-advanced**] | **sntp** | **tftp** | **wsp-connection-less** | **wsp-connection-oriented** } [**description** *description*]: This command is used only on UPF.
 - *route_priority* must be an integer value 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 value in the range of 496-65535.
 - **add-if-not-present** : Specifies to add the TCP MSS if not present in the packet.
 - **limit-if-present** : Specifies to limit the TCP MSS if present in the packet.
- **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 value in the range of 100-30000. Default value is 5000.

Sample Configuration

```

active-charging service acs
  ruledef ip-any-rule
    ip any-match = TRUE
  #exit
  urr-list upf
    rating-group 10 ser 10 urr-id 10
    rating-group 10 urr-id 50
  #exit
  charging-action starent
    content-id 10
    service-identifier 10
    billing-action egcdr
    cca charging credit rating-group 10
  exit
  credit-control group CCG
    diameter ignore-service-id
  #exit
  rulebase starent
    billing-records egcdr
    action priority 30 ruledef ip-any-rule charging-action starent
    egcdr threshold interval 3600
    egcdr threshold volume total 200000
    egcdr threshold volume downlink 100000 uplink 100000
    dynamic-rule order first-if-tied
    credit-control-group CCG
  #exit
#exit

context ISP
  apn starent.com
  accounting-mode gtp
  gtp group my_grp accounting-context ISP

```

```
    ip context-name ISP
  #exit
  gtpv group my_grp
    gtpv egcdr service-data-flow threshold interval 1200
    gtpv egcdr service-data-flow threshold volume downlink 13000
    gtpv egcdr service-data-flow threshold volume uplink 17000
    gtpv egcdr service-data-flow threshold volume total 22222
  #exit
end
```