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 3
- Configuring Credit Control for Usage Reporting, on page 13
- Configuring ACS Rulebase for Usage Reporting, on page 14
- Monitoring and Troubleshooting, on page 16

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI 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
The feature is enhanced to support Recalculate IE on N4 interface	2023.04.0

Revision Details	Release
The feature is enhanced to support following functionality: • PTT no-quota Limited Pass • PTT quota exhaust Limited Pass • Tariff Time • TCP Maximum Segment Size	2021.02.0
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

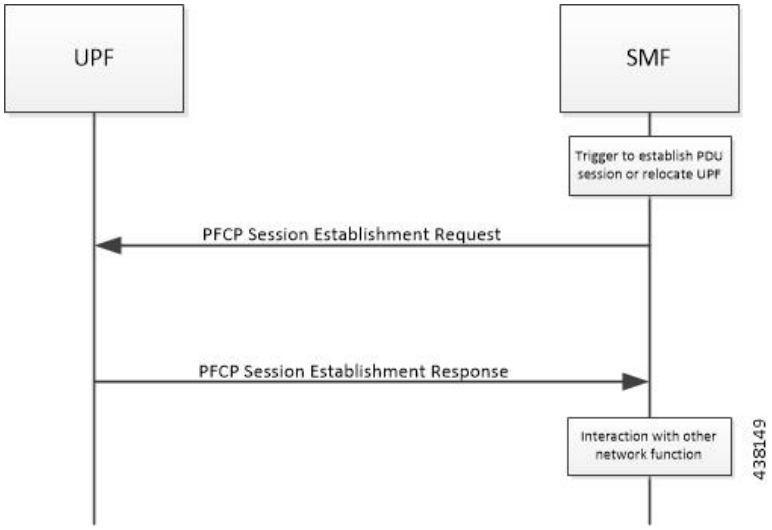
Call Flows

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 Information Element (IE), which comprises of triggers and thresholds that are intended for reporting.

The following call flow depicts the PFCP Session Establishment procedure.

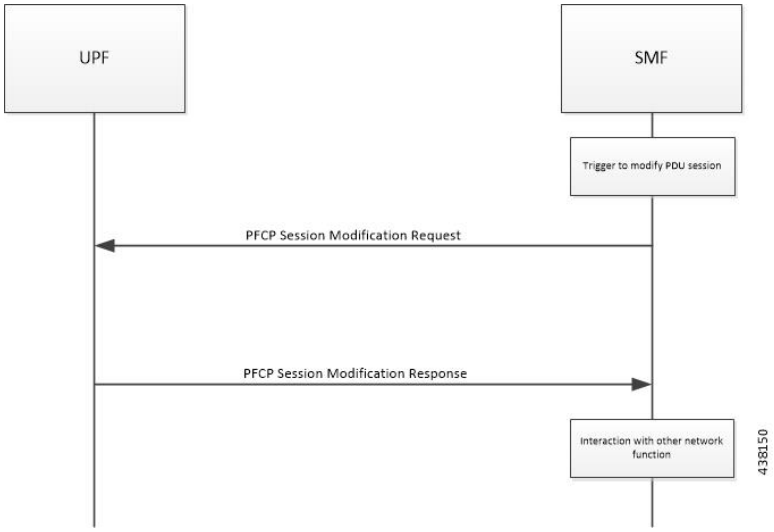


Step	Description
1	The SMF receives the trigger to establish a new PDU Session or change the UPF for an established PDU Session.
2	The SMF sends the PFCP Session Establishment Request message to the UPF. This message contains the structured control information, which defines the UPF's behavior.
3	The 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 PFCP Session Establishment Response message to the SMF. For instance, Created PDR IE, in which UPF Flow-TEID is sent to gNB for GTP-u encap for data traffic.
6	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

PFCP Session Modification Procedure

The SMF uses the PFCP Session Modification procedure to modify an existing PFCP 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 PFCP Session Modification procedure.

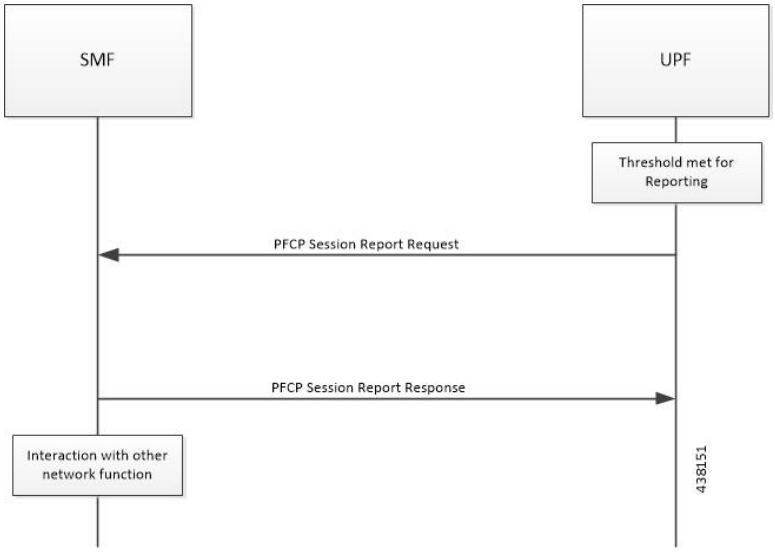


Step	Description
1	The SMF receives the trigger to modify the existing PDU Session.
2	The SMF sends an N4 session modification request message to the UPF. This message contains the structured control information, which defines the UPF's behavior.
3	The UPF identifies the PFCP session context for the 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. • The custom Information Element (IE) called Recalculate Measurement is added to the Update-URR IE (for URR-ID: Gz-Bearer) to support the PGWCDR generation due to the Max-LOSDV condition with the N4 Session Modify Request. After receiving the IE, UPF reconciles the Volume and Duration of the URR according to the URR-ID present inside the IE.
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.

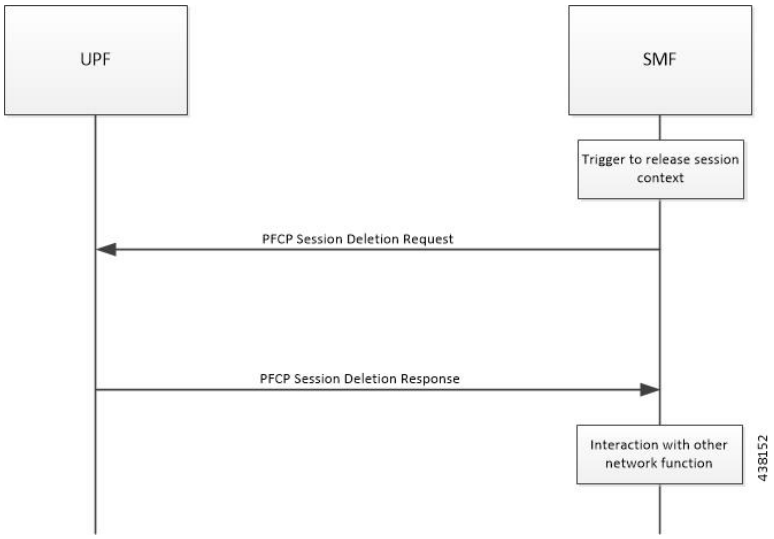


Step	Description
1	• Once the provisioned threshold is met (for time, volume or event, and trigger is set for reporting), the UPF sends PFCP Session Report Request with usage report IE and usage details for volume, time, or threshold. • The custom Information Element (IE) called Recalculate Measurement is added to the Update-URR IE (for URR-ID: Gz-Bearer) to support the PGWCDR generation due to the Max-LOSDV condition with the N4 Session Modify Request. After receiving the IE, UPF reconciles the Volume and Duration of the URR according to the URR-ID present inside the IE.
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

Table 3: Feature History

Feature Name	Release Information	Description
Recalculate Measurement IE on the N4 Interface	2023.04	UPF supports the Recalculate Measurement custom IE as received over the N4 interface. This IE is added to the Update-URR process (URR-ID: Gz-Bearer) to support the PGW-CDR generation due to the max_LOSDV change condition.

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.
- Recalculate Measurement – The custom Information Element (IE) called Recalculate Measurement is added to the Update-URR process (URR-ID: Gz-Bearer) to support the PGWCDR generation due to the Max-LOSDV condition. After receiving the IE, UPF reconcile the Volume and Duration of the URR according to the URR-ID present inside the IE.

Note

- The total usage for the given URR-ID is reset, and if there are any linked URRs, the usage is recalculated.
- The timestamps for first-pkt-time, last-pkt-time and duration are also adjusted accordingly.
- The threshold values remain unchanged.

- Recalculate Interface - The custom IE called ‘Recalculate Interface’ is sent by SMF via N4 Modify Request. When Recalculate Interface IE is received along with Query URR(s) or Update URR(s) IEs in the same Sx Modify Request, Recalculate Interface IE will be processed independently in the end. After receiving the IE, the UPF iterates through all the URRs, fetching only the URRs mentioned as per the flags mentioned by SMF and execute the recalculate functionality. The UPF subsequently reconciles the Volume and Duration of all the retrieved URRs.

Note

- The usage accumulated for the URRs is discarded, and if there are any linked URRs, their usage is reconciled.
- The timestamps for first-pkt-time, last-pkt-time and duration are adjusted accordingly.
- The threshold values for the linked URRs remain unchanged.

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.

Note If the Update URR does not contain any time or volume threshold values, that threshold is not monitored after that point.

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.

Supported Functionality and Limitations

Basic call flow with Volume-Quota mechanism is supported with the following limitations:

- Dynamic Rules with Online Enabled is supported; both at Session-Setup and Mid-Session.
- Predefined Rules (dynamic-only) is supported; both at Session-Setup and Mid-Session. No restriction on configuring the "preemptively request".
- Static-rules with Online Charging are supported.
- Ignore-service-id is supported.
- Volume-Quota/Volume-Threshold mechanisms are supported.
- Event-Triggers (through which the Query URR occurs), and sending of usage information to the OCS is supported.
- The "updateURR" procedure, through the Sx/N4-Session-Modification procedure where the OCS grants a fresh Quota, is supported.
- Pending-Traffic-Treatment (PTT) Drop/Pass is supported with following limitations:
  - The scenarios currently supported are no-quota and quota-exhausted.
  - The trigger or re-authorization scenarios are not supported.
  - The PTT action (Forward/Drop) is considered after the quota-get is exhausted.
- Wall-Clock time-quota mechanism is supported.
- Other Time Quota Mechanisms (Discrete Time Period and Continuous-Time-Period) are not supported.
- Final-Unit-Indication Terminate mechanism is supported.
- FUI-Restrict is not supported.
- Server-Unreachable (SU) mechanism is now supported with minor change in behavior compared to non-5G UPF P-GW.
  - When an URR needs quota at UPF, the usage-report is generated to SMF and until the SMF responds with the linked SU_URR, the packets matching this URR are treated with Pending-Traffic-Treatment configuration.
  - When the SU Time Quota is used and it's reported to SMF for the Quota Exhaust, and if the session goes into Server-Unreachable state again, the time elapsed from the last Usage-Report is accounted in the usage.

- Pending-Traffic-Treatment Buffer mechanism is not supported.
- Quota-Hold-Time is supported.
- Quota-Consumption-Time mechanism is not supported.
- Quota-Validity-Time is supported.
- Configuring different "rating-group" value other than the "content-id" is supported.
  - The RG 0 is not supported.
- Trigger to PCF for the Out-of-Credit, Reallocation-of-Credit events are not qualified.

Important Event-trigger Out-of-Credit toward PCF is validated with a limitation of having only one time Grant-Quota (Keeping Total Volume and Granted Volume at same value).

- Service-Specific-Units are not supported.
- Tariff-Time change is supported as per 3GPP specification.
- FUI-Redirect is supported with following limitations:
  - Redirection for HTTPs is not supported.
  - The FUI-Redirect with Filter-IDs/Filter-Rules are not supported.
  - The WSP Protocol is not supported.
  - The **redirect-require-user-agent** CLI command is not supported; the redirection continues to work even if the user-agent is not present.
  - Appending the original URL is not supported.
  - Token-based mechanism, to come out of Redirection, is not supported. To end the redirection in 5G UPF, OCS sends Redirect Validity-Time or RAR.
  - FUI-Redirection is supported only for the URL, similar to the behavior in non-5G UPF architecture.
  - Check pointing of FUI Redirection URL is not supported.

PTT no-quota Limited Pass

This feature allows the subscriber to use the network while waiting for the response from OCS. The Limited-Pass configuration allows to specify the Volume which the subscriber can consume while waiting for the quota-response from OCS. The usage is accounted in the respective charging bucket and is adjusted against the next-quota allocation.

Use the following CLI commands to enable the feature:

```
configure
  active-charging service service_name
    credit-control
```

```
pending-traffic-treatment noquota limited-pass volume volume
end
```

Limited Pass Volume is used only for **noquota** case (Rating Group (RG) seeking quota for the first time) and not for **quota-exhausted**. Limited Pass Volume isn't used for subsequent credit requests.

The traffic is allowed to pass until the Limited-Pass Volume gets exhausted. The usage is counted in the respected charging-bucket and adjusted against the "Quota" granted. If the "Quota" allocation is less than the actual usage, immediate reporting towards OCS with the usage-report occurs requesting for more quota allocation. The subsequent incoming packets are handled as per the "quota-exhausted" PTT configuration.

If the Limited Pass Volume is NOT exhausted before the OCS responds with denial of quota, traffic is blocked after the OCS response. The gateway reports usage on Limited-Pass Volume in next SX_SESSION_REPORT_REQUEST.

If the Limited Pass Volume is exhausted before the OCS responds, then the subsequent incoming packets for the session are dropped until quota is granted from OCS.

The default pending-traffic-treatment for **noquota** is Drop. The **default pending-traffic-treatment noquota** command removes any Limited Pass Volume size configured.

PTT quota exhaust Limited Pass

Quota Exhausted Limited pass is proposed as an alternative to the Quota Exhausted Buffer due to the practical issues of the latter in the high-speed network. Buffering requires packet buffering for large number of packets at the gateway. The large number of packets can result in risking to run out of memory affecting the bandwidth speed. So, Limited Pass is an alternate to the Buffer option. Limited Pass allows the traffic to pass through until the configured limit on the Quota-Exhaust scenarios.

Use the following CLI command to enable the feature:

```
configure
  active-charging service service_name
    credit-control
     pending-traffic-treatment quota-exhausted limited-pass volumevolume

     end
```

Note The above CLI is only applicable for the 5G UPF architecture.

After the Limited-Pass volume exhausts, the further packets drop until the quota allocation comes.

Limited Pass allows the traffic until the Limited-Pass volume exhausts. The Limited Pass counts and adjusts the usage in the respective charging-bucket against the "Quota" granted. If the "Quota" allocation is less than the actual usage, there’s immediate reporting toward OCS with the usage-report and asking for more quota allocation.

If the limited pass volume doesn’t exhaust before the OCS responds with denial of quota, there’s traffic blockage after the OCS response. Gateway reports the usage in SX_SESSION_REPORT_REQUEST.

If the limited pass volume exhausts before the OCS responds, then further incoming packets for the session drop until grant quota from OCS.

The default pending-traffic-treatment for quota-exhausted is drop. The default pending-traffic-treatment quota-exhausted command removes any Limited Pass Volume size configured.

Tariff Time Support

The Tariff switch time functionality is applied when a subscriber switch from one tariff plan to another.

The Tariff-Time-Change AVP is used to determine the tariff switch time, and the Monitoring-Time IE is used to support the Tariff Time support functionality.

After a tariff timer expiry, the Gateway accumulates the usage separately in a charging bucket and continues to consume from the original quota value. At the time of next reporting (Quota exhausted or another control events), the Gateway reports both usages (before and after tariff time change) for the same Charging Bucket.

The first reporting of this charging-bucket will have the Reporting-Reason: Monitoring Time and the second bucket will contain the last reporting reason, and the quota usage after the tariff-timer expiry.

The data traffic usage can be split into resource usage before a tariff switch and resources used after a tariff switch. The Tariff-Change-Usage AVP is used within the Used-Service-Units AVP to distinguish reported usage before and after the tariff time change.

Limitations

Following are the known limitations of this feature:

- Only one tariff time per RG/Service ID combination is supported.
- Allocation of different quota before and after tariff time change isn't supported. This functionality isn’t in compliance with the 3GPP standards.

TCP Maximum Segment Size

TCP/IP Stack always inserts Maximum Segment Size (MSS) field in the header. This causes difference in MSS insertion behavior with and without TCP Proxy.

Using **tcp mss** configurations, TCP MSS can be limited if already present in the TCP SYN packets. If there are no errors detected in IP header or TCP mandatory header, and there are no memory allocation failures, TCP optional header is parsed. If TCP MSS is present in the optional header and its value is greater than the configured MSS value, the value present in the TCP packet is replaced with the one that is configured.

If the TCP optional header is not present in the SYN packet and there are no errors in already-present TCP header, the configured TCP MSS value is inserted while sending out the current packet.

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 |
limit-if-present add-if-not-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 | 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 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.
  - **limit-if-present add-if-not-present** : Specifies to limit the TCP MSS if present, else, adds it to the packets.

Note The **tcp mss** *tcp_mss* **limit-if-present add-if-not-present** CLI command is available in 2021.02.0 and later releases.

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

Monitoring and Troubleshooting

Show Commands and/or Outputs

This section provides information about the show CLI commands that are available in support of the feature.

show-user-plane-service statistics rulebase name <name>

Use this CLI command to see the following fields that are available in support of TCP Maximum Segment Size (MSS) feature:

- TCP MSS Inserted Pkts: Displays the total number of MSS Inserted packets.
- TCP MSS Limited Pkts: Displays the total number of TCP MSS Limited packets.