

Dynamic and Static PCC Rules

This chapter covers the following topics:

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- Provisioning of Predefined PCC Rules, on page 2
- Dynamic PCC Rules Support, on page 3
- Policing, on page 4
- Bandwidth Policy Configuration Limits, on page 6
- Rate Limiting for Static and Predefined Rules, on page 6
- Rate Limiting for Dynamic Rules, on page 7
- Standards Compliance, on page 8
- Configuring the URR IDs, on page 8
- Threshold Configuration, 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 SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G UPF Configuration and Administration Guide*

Revision History

Table 2: Revision History

Revision Details	Release
Added support for: • Flow-level policing • Increase in the the maximum number of groups per bandwidth policy	2021.01.0
First introduced.	2020.02.0

Feature Description

Dynamic PCC rules are provisioned by the PCF to the PCEF through the HTTP interface and may be either predefined/static or dynamically generated in the PCF. Dynamic PCC rules can be installed, modified and removed at any time.

Predefined PCC rules are configured in the PCEF and can be activated or deactivated by the PCF or by the PCEF at any time. Static PCC rules within the PCEF may be grouped allowing the PCF to dynamically activate a set of static PCC rules over the HTTP reference point. Those static PCC rules to be locally activated by the PCEF are not explicitly known in the PCF, but the PCF simply knows identifiers of static PCC rules to be activated from the PCF.

How it Works

Predefined PCC Rules Support

Config URR IDs are applicable for static rules and also predefined rules. When a subscriber call comes up, it traverses the static rules in rule base. The subscriber primary URR list with bucket IDs as key updates the corresponding URR buckets for the various interfaces with the charging action configuration. For dynamic rules and predefined rules, URR ID list in PDR creates the URR buckets on the User Plane.

Following are the ecosystem changes to support Cisco SMF and UPF to work independently for Charging Action (vendor agnostic way) to work:

- Configurable "Config URR IDs" at UPF
- UPF to enable the local configuration for thresholds

Provisioning of Predefined PCC Rules

Predefined PCC rule is preconfigured in the SMF (for 5GC). Predefined PCC rules can be activated or deactivated by the PCF at any time. The Predefined PCC rules may be grouped allowing the PCF to dynamically activate a set of PCC rules. The SMF may enforce an activated predefined PCC rule by the PCF in the UPF by:

- Determining the service data filters or application IDs referred by the activated predefined PCC rule(s) and the corresponding QoS and charging control information respectively.
- Creating the necessary PDR(s) to identify the service data flow(s), application(s) that the predefined PCC or ADC rule refer to, if not already existing.
- Creating the necessary QER for the QoS enforcement at service data flow or application-level accordingly.
- Creating the necessary FAR if a new FAR must be created as result of QoS flow binding and QoS control for forwarding the detected service data flow or application traffic, or to redirect or to apply traffic steering control if included in the predefined PCC rule.
- Creating the necessary URR(s) for each monitoring key, charging key, combination of charging key and service ID, or combination of charging key, sponsor ID and Application Service Provider ID if included in the predefined PCC rule.

And, later by:

- Associating the created URR(s) to the newly created PDR(s).
- Associating the existing FAR or the new FAR to the newly created PDR(s).

Optionally, the traffic handling policies common to many PFCP sessions (that is, predefined QER(s)/FAR(s)/URR(s)) can be configured in the UPF. The SMF activates these traffic handling policies by including the Activate Predefined Rules IE within one of the following:

- The Create PDR IE in an PFCP Session Establishment Request
- The Create PDR IE in an PFCP Session Modification Request

For traffic matching PDR(s) associated with the activated predefined rules, the UPF enforces the rules. For example, the UPF generates Usage Report(s) and sends it to the SMF, for URR, and the SMF handles the usage reports.

The URR IDs used in reports triggered by a predefined rule in UPF are also preconfigured at the SMF.

Note The UPF does not support the deactivation of predefined rules.

Dynamic PCC Rules Support

For dynamic PCC rules multiple flows are supported on per Packet Forwarding Control Protocol (PFCP) session:

- The 5G QoS model allows classification and differentiation of specific services based on subscription-related and invocation-related priority mechanisms. These mechanisms provide abilities such as invoking, modifying, maintaining, and releasing QoS Flows with priority, and delivering QoS Flow packets according to the QoS characteristics under network congestion conditions.
- The 5G QoS model is based on QoS Flows. The 5G QoS model supports both QoS Flows that require guaranteed flow bit rate (GBR QoS Flows) and QoS Flows that do not require guaranteed flow bit rate (Non-GBR QoS Flows).

- The QoS Flow is the finest granularity of QoS differentiation in the PDU session. A QoS Flow ID (QFI) is used to identify a QoS Flow in the 5G System. User Plane traffic with the same QFI within a PDU session receives the same traffic forwarding treatment (Example - scheduling, admission threshold).
- Within the 5GS, a QoS Flow associated with the default QoS rule is required to be established for a PDU session and remains established throughout the lifetime of the PDU session. This QoS Flow must be a Non-GBR QoS Flow.
- A QoS flow is associated with QoS requirements as specified by QoS parameters and QoS characteristics. A QoS flow can either be "GBR" or "Non-GBR" depending on its QoS profile.
  - For each QoS Flow, the QoS profile includes the QoS parameters:
    - 5G QoS Identifier (5QI)
    - Allocation and Retention Priority (ARP)
  - For each GBR QoS flow only, the QoS profile must also include the QoS parameters:
    - Guaranteed Flow Bit Rate (GFBR) - UL and DL
    - Maximum Flow Bit Rate (MFBR) - UL and DL
  - In case of a GBR QoS Flow only, the QoS profile may also include one or more of the QoS parameters:
    - Notification control
    - Maximum Packet Loss Rate - UL and DL

During PDR creation or modification UPF receives the QER for QoS enforcement on flows.

The QoS enforcement rule correlation ID is assigned by the CP function to correlate QERs from multiple PFCP session contexts. For instance, the enforcement of APN-AMBR in the PGW-U is achieved by setting the same QoS enforcement rule correlation ID to the QERs from different PFCP sessions associated with all the PDRs corresponding to the non-GBR bearers of all the UE's PDN connections to the same APN. The QERs that are associated to the same QoS Enforcement Rule Correlation ID in multiple PFCP sessions will be provisioned with the same QER contents in each of these PFCP sessions. The QoS enforcement rule correlation ID is only used to enforce the APN-AMBR when the UE is in EPC, it may be provided by the CP function over N4 to the UP function for a PDU session may move to EPC in a later stage.

If the UPF receives QoS Enforcement Rule Correlation ID for 5G PFCP sessions, then it enforces it.

Policing

The policer configuration uses inputs from the session manager, these inputs are received either from PCF as AMBR or from flow-level QoS information. The values received from the PCF are always accepted for session-level AMBR policing. However, the flow-level policing is prioritized, if available, and AMBR policing is applied sequentially. That is to say, the policer engine applies the hierarchical policing—first the flow-level/rule bandwidth limiting and then the session-level bandwidth limiting.

Note AMBR modifications during session run-time through RAR or CCA-U is applicable.

The input values received from the session manager are pushed into a policer configuration and a policer token bucket. For each direction - uplink or downlink, a new record is created for Policer configuration and Policer token bucket.

The Policer configuration is the reference for the policer engine, and the policer token bucket is used for calculation and restoration of values.

Currently, Policing is supported for AMBR received from PCF and rule-level QoS information for dynamic rules. For static and predefined rules, bandwidth limiting is achieved by the bandwidth policy configuration. Extended bit rates configured in bandwidth-policy configuration in Active Charging Service Configuration mode on SMF is provided to the UPF by RCM, and same is applied for policing by the UPF. An example configuration of bandwidth policy, with extended bit rate, is given below:

```
configure
  active-charging service ACS
    bandwidth-policy BWP

      flow limit-for-bandwidth id 1 group-id 2

      flow limit-for-bandwidth id 2 group-id 3
      flow limit-for-bandwidth id 100 group-id 100

     group-id 2 direction uplink peak-data-rate 256000 peak-burst-size 1000 violate-action
 discard
     group-id 3 direction downlink peak-data-rate 256000 peak-burst-size 1000 violate-action
 discard
     group-id 4 direction uplink peak-data-rate 300000 peak-burst-size 1200 violate-action
 lower-ip-precedence
     group-id 5 direction downlink peak-data-rate 300000 peak-burst-size 1200 violate-action
 lower-ip-precedence committed-data-rate 256000 committed-burst-size 1000 exceed-action
lower-ip-precedence
      group-id 100 direction downlink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard
     group-id 100 direction uplink peak-data-rate-kbps 4294967295 peak-burst-size 4294967295
 violate-action discard
      exit
    charging-action catchall
      flow limit-for-bandwidth id 1
      exit
    rulebase cisco
      bandwidth default-policy BWP
      exit
    end
```

Limitations

In this release, Policing has the following limitations:

- Modification of **bandwidth-policy** isn't supported.
- Interaction with other features, such as token replenishment (both APN-level and ACL-level) isn't supported.
- Currently, policer-based statistics aren't supported. You can verify bandwidth limiting using network performance monitoring tools.

Bandwidth Policy Configuration Limits

The user can configure bandwidth limits in both SMF and UPF, for both downlink and uplink packets. The configuration is done in all charging actions of predefined PCC rules, even if the bandwidth limitation configuration is the same for all charging actions.

To optimize these configurations, you must define a bandwidth ID to include all bandwidth-related configurations and associate the bandwidth ID under charging actions.

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

The following are the bandwidth-policy configuration limits:

- Maximum number of bandwidth policies—64
- Maximum number of groups per bandwidth policy—1000
- Maximum number of bandwidth IDs per bandwidth policy—1000
- Maximum number of groups across bandwidth policies—10000
- Maximum number of bandwidth IDs across bandwidth policies—10000

Rate Limiting for Static and Predefined Rules

For static and predefined rules, bandwidth limiting is achieved by the bandwidth policy configuration. Bandwidth Policy must be configured on SMF and UPF under Active Charging Service Configuration Mode.

The following is an example configuration of bandwidth policy with extended bit rate:

```
config
   active-charging service ACS
      bandwidth-policy BWP
         flow limit-for-bandwidth id 1 group-id 2
         flow limit-for-bandwidth id 2 group-id 3
         flow limit-for-bandwidth id 100 group-id 100
        group-id 2 direction uplink peak-data-rate 256000 peak-burst-size 1000 violate-action
 discard
         group-id 3 direction downlink peak-data-rate 256000 peak-burst-size 1000
violate-action discard
        group-id 4 direction uplink peak-data-rate 300000 peak-burst-size 1200 violate-action
 lower-ip-precedence
         group-id 5 direction downlink peak-data-rate 300000 peak-burst-size 1200
violate-action
         lower-ip-precedence committed-data-rate 256000 committed-burst-size 1000
exceed-action
         lower-ip-precedence
         group-id 100 direction downlink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard
         group-id 100 direction uplink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard
         exit
      charging-action catchall
         flow limit-for-bandwidth id 1
         exit
      rulebase cisco
```

```
bandwidth default-policy BWP
exit
end
```

Note UPF does not support the modification of bandwidth-policy configuration.

Rate Limiting for Dynamic Rules

As per 3GPP TS 29.244, the following Information Element (IE) is received from SMF for QoS enforcement in Create QER or Update QER in Session Establishment or Modification Request:

- Maximum Bitrate: This IE is present if an MBR enforcement action is applied to packets matching this PDR. When present, this IE indicates the uplink and/or downlink maximum bit rate to be enforced for packets matching the PDR. For 5GC, this IE may be set to the value of:
  - Session-AMBR—for a QER that is referenced by all the PDRs of the non-GBR QoS flows of a PDU session.
  - QoS Flow MBR—for a QER that is referenced by all the PDRs of a QoS Flow.
  - SDF MBR—for a QER that is referenced by all the PDRs of an SDF.
- Guaranteed Bitrate: This IE is present if a GBR has been authorized to packets matching this PDR. When present, this IE indicates the authorized uplink and/or downlink guaranteed bit rate. This IE may be set to the value of:
  - Aggregate GBR—for a QER that is referenced by all the PDRs of a GBR bearer
  - QoS Flow GBR—for a QER that is referenced by all the PDRs of a QoS Flow
  - SDF GBR—for a QER that is referenced by all the PDRs of an SDF
- QoS flow identifier (QFI): This IE is present if the QoS flow identifier is inserted by the UPF.
- Gate Status: This IE indicates whether the packets are allowed to be forwarded (the gate is open) or it is discarded (the gate is closed) in the uplink and/or downlink directions.
- QER Correlation ID: This IE is present if the UP function is required to correlate the QERs of several PFCP sessions, for APN-AMBR enforcement of multiple UE's PDN connections to the same APN.

Note Although it is not applicable, but if UPF receives QoS Enforcement Rule Correlation ID for 5G PFCP sessions then it enforces it.

The SMF provisions QoS enforcement in UPF by creating necessary PDRs to represent SDF, QoS Flow and session and associating respective QERs as follows:

- Creating QERs for the QoS enforcement at session level, SDF level.
- Creating QERs for the QoS enforcement of the aggregate of SDFs with the same GBR QFI.

- Associating the session level QER to all the PDRs defined for the session.
- Associating the SDF or application QER to the PDRs associated to the SDF or application.
- Associating the QER of the aggregate of SDFs to the PDRs associated to SDFs or applications that share the QER.

Standards Compliance

The N4 interface between SMF and UPF is specified in 3GPP TS 23.501 and 3GPP TS 23.502.

Configuring the URR IDs

Config URR IDs are applicable for static rules and predefined rules that are bound to the default bearer. When a subscriber call comes up, static rules in the Rulebase are traversed. The corresponding URR buckets for the various interfaces configured in the Charging Action are updated in the subscriber primary URR list with bucket IDs as key. For Dynamic rules and Predefined rules that are bound to dedicated bearers, the URR ID list in PDR is used for creating URR buckets on the UP.

Currently, the Config URR IDs are generated using running counter at SessCtrl.

To achieve the configurable Config URR IDs:

- Configuration template outside of Charging Action allows URR-ID mapping with “Rating Group” and “Service-id”.
- If a separate Rating Group (RG) is configured for Gy, then that RG is applied to the Gy bucket. If no separate RG is configured for Gy, then the same “Content-id” is applicable for all interfaces.
- “Service-id” is optional for URR-ID mapping.
- URR-ID is unique. This must be ensured through **show configuration error** CLI command, a separate validation script, or checking during config time.
- For UPF, the value for URR-ID generation is taken from the configuration. The UP receives Config URR-ID from configuration rather than PFD message. The PFD mechanism is not used between SMF and UPF.
- SMF does not support the URR-ID list configuration.
- URR-ID is generated independently on UPF and SMF for Static or Predefined rules having rating group/content-id,service-id, and so on.

The following is a sample configuration for URR-ID profile template:

```
rg <x> si <y> urr-id <abc>
rg <x1> si <y1> urr-id <abc1>
rg <x> urr-id <abc2>
```

Use the following configuration to enable Config URR ID.

```
configure
   active-charging service service_name
      urr-list list_name
```

```
        rating-group group_number { service-identifier service_number | urr-id
id_range }
         end
```

NOTES:

- **urr-list** *list_name:* Configures the active charging service URR list. *list_name* must be an alphanumeric string of 1 to 63 characters.
- **rating-group** *group_number* **:** Specifies the rating ID used in prepaid charging. *group_number* must be an integer in the range of 0 to 2147483647.
- **service-identifier** *service_number* **:** Specifies the number given to the service.
- **urr-id** *id_range* **:** Specifies the URR identifier for rating/service group. *id_range* must be an integer in the range of 1-134217727.
- The values can be changed dynamically. However, it will take effect only for new sessions.

Threshold Configuration

The GTPP group configuration is required for threshold calculation at UPF.

UPF uses GTPP group name available from APN configuration. Only one GTPP group should be associated under APN configuration.

The following is a sample configuration:

```
configure
  context context_name
    apn apn_name
      gtpp group group_name
      ip context-name name
      exit
    gtpp group group_name
      gtpp egcdr service-data-flow threshold interval interval
      gtpp egcdr service-data-flow threshold volume downlink bytes
      gtpp egcdr service-data-flow threshold volume uplink bytes
      gtpp egcdr service-data-flow threshold total bytes
      end
```

If any one of the above service-data-flow thresholds is hit for offline URR, the UPF sends SX_SESSION_REPORT_REQUEST towards SMF reporting the data volume.