# Gx/Sd Services

# Gx Services

This section covers the following topics:

## QoS Profile

### Overview

When UE attaches to the network for the first time, it will be assigned default bearer which remains as long as UE is attached. Default bearer is best effort service. Each default bearer comes with an IP address.

This section provides details of Gx default bearer QoS parameters and also explains how CPS derives QoS in different configurations.

# Policy Builder Configuration

## Case 1- QoS under Gx Profile

**Step 1**    Log into Policy Builder.

**Step 2**    Select the **Reference Data** tab, and click **Diameter Defaults** > **Gx Profile**.

**Step 3**    On the right side, click **Create Child** to the open the **Gx Profile** pane.

## Case 2 - Default Bearer QoS in Service

**Step 1**    Log into Policy Builder.

**Step 2**    Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 3**    Click **Use Case Template** link from the right side under **Create Child** to create a use case template.

**Step 4**    Enter the name for use case template.

**Step 5**    Select **Actions** tab.

**Step 6**    Click **Add** under **Service Configurations** to open the **Select Service Configuration** dialog box.

**Step 7**    Select **DefaultBearerQoS** under **gx** and select the required service configuration parameters.

**Step 8**    Click **OK** to add the service in the **Service Configuration** pane.

**Step 9**    On the **Services** tab, click **Services** > **Service Options** to create a service option, and add the use case template that the user just configured.

An example is shown.

*Figure 1: Creating a Service Option*



**Step 10**    On the **Services** tab, click **Services** > **Services** to create a service, and add the same use case template.

An example is shown.

**Figure 2: Creating a Service**



## Default Bearer QoS Enhancements - Gx

CPS supports the management of Default Bearer QoS attribute values for IP-CAN sessions by applying QoS-Bounding, QoS-Mirroring and QoS-Enforced on Default Bearer QoS and these actions for individual QoS attributes can be derived based on SPR or Gx session attributes.

- QoS-Bounding is the ability for the PCRF to calculate the minimum QoS between the Requested QoS (from the P-GW) and the Authorized QoS (based on internal computation of the Logic in the PCRF) and assign that in the response message back to the P-GW.

- QoS-Mirroring is the ability for the PCRF to mirror the same QoS values back that were being requested by the P-GW in the Request Message.

- QoS-Enforcement is the ability for the PCRF to enforce the Authorized QoS computed based on its internal logic back to the P-GW in the request/response message.

To support QoS Enhancements, the user can configure object DefaultBearerQoSAction with action attribute for each possible QoS attribute and bind to the QoS action columns of the Default Bearer CRD. Also CPS binds the DefaultBearerQoS service configuration object attributes to QoS columns of the Default Bearer CRD.

CPS when sends or receives a Gx request message then it needs to do a lookup from CRD tables for a match of input attributes and perform calculation of DefaultBearer QoS using values from the output attributes and the default configured in service. The QoS Actions are also applicable to PreConfigured Rules defined in CPS service configurations and are used to calculate the QoS-Information grouped AVPs of such charging rules.

CPS after calculation of default bearer QoS applies the QoS actions bounding, mirroring and enforcement to each attribute of current calculated QoS. A new class QoSInformationActions is used to override the QoS calculated from the QoSInformation and assigning the values as defined by CRD table and corresponding action from DefaultBearerQoSAction.

The DefaultBearerQoS calculations explained above are applied if the service configuration contains the service object DefaultBearerQoSAction.

CPS also supports the Gx TGPP session to store the last received QoS parameters from PCEF/PGW which helps in evaluating the QoS during CCR-U or RAR trigger.

CPS also supports QoS calculations for MPS and it takes precedence over QoS Actions while calculating default bearer QoS.

The **QoS-Information AVP** (AVP code 1016) is of type Grouped, and it defines the QoS information for resources requested by the UE, an IP-CAN bearer, PCC rule, QCI or APN. When this AVP is sent from the PCEF to the PCRF, it indicates the requested QoS information associated with resources requested by the UE, an IP CAN bearer or the subscribed QoS information at APN level.

When the QoS-Information AVP is provided within the CCR command along with the RESOURCE_MODIFICATION_REQUEST event trigger, the QoS-information AVP includes only the QoS-Class-Identifier AVP and Guaranteed-Bitrate-UL and/or Guaranteed-Bitrate-DL AVPs.

The Allocation-Retention-Priority AVP is an indicator of the priority of allocation and retention for the Service Data Flow.

- **QCI**: The QoS-Class-Identifier AVP (AVP code 1028) is of type Enumerated, and it identifies a set of IP-CAN specific QoS parameters that defines the authorized QoS, excluding the applicable bitrates and ARP for the IP-CAN bearer or service flow. Possible values: 1 - 9.

  - 1: Conversational Traffic class

  - 2: Conversational Traffic class

  - 3: Streaming

  - 4: Streaming

  - 5 to 8: Interactive

  - 9: Background

- **ARP**: The Allocation-Retention-Priority AVP (AVP code 1034) is of type Grouped, and it is used to indicate the priority of allocation and retention, the pre-emption capability and pre-emption vulnerability for the SDF if provided within the QoS-Information-AVP or for the EPS default bearer if provided within the Default-EPS-Bearer-QoS AVP.

**Note** The Priority-Level AVP of the default bearer will be set to a sufficiently high level of priority to minimize the risk for unexpected PDN disconnection or UE detach from the network according to operator specific policies.

AVP Format:

```
Allocation-Retention-Priority ::= < AVP Header: 1034 >
                { Priority-Level }
                [ Pre-emption-Capability ]
                [ Pre-emption-Vulnerability ]
```

## MIRRORING ACTION

Table 1: Mirroring Action

| CCR (INPUT) | Calculated QoS Value | QoS Action | CCA (OUTPUT) |
|---|---|---|---|
| MBR[1] | MBR | MIRROR | MBR |
| GBR[2] | GBR | MIRROR | GBR |
| QCI [3] | QCI | MIRROR | QCI |
| ARP[4] | ARP | MIRROR | ARP |

1  Maximum -Bit-Rate
2  Guaranteed-Bit-Rate
3  QoS-Class-Identifier AVP
4  Allocation-Retention-Priority

## ENFORCING ACTION

Table 2: Enforcing Action

| CCR (INPUT) | Calculated QoS Value | QoS Action | CCA (OUTPUT) |
|---|---|---|---|
| MBR | MBR | ENFORCE | MBR |
| GBR | GBR | ENFORCE | GBR |
| QCI | QCI | ENFORCE | QCI |
| ARP | ARP | ENFORCE | ARP |

## BOUNDING ACTION

*Italics* text: In the Table 3: Bounding Action, on page 6, the *MBR*, *GBR*, *QCI*, and *PL* represents values received in CCR request (CCR (INPUT)).

**Bold** text: In the Table 3: Bounding Action, on page 6, **MBR**, **GBR**, **QCI**, and **PL** represents values calculated internally in CPS (Calculated QosS Value).

*Table 3: Bounding Action*

| CCR (INPUT) | Calculated QoS Value | QoS Action | CCA (OUTPUT) |
|---|---|---|---|
| MBR | MBR | BOUND | min(*MBR*, **MBR**) <br><br> CCA value for the MBR AVP is minimum of *MBR* and **MBR**. |
| GBR | GBR | BOUND | min(*GBR*, **GBR**) <br><br> CCA value for the GBR AVP is minimum of *GBR* and **GBR**. |
| QCI | QCI | BOUND | max(*QCI*, **QCI**) <br><br> CCA value for the QCI AVP is maximum of *QCI* and **QCI**. |
| ARP-PL[5] | ARP-PL | BOUND | max(*PL*, **PL**) and PV, PC based on chosen ARP |
| ARP-PV | ARP-PV | BOUND | Set based on PL. IF PL comes from CCR set CCR Value, or retain Granted QoS Values |
| ARP-PC | ARP-PC | BOUND | Set based on PL. IF PL comes from CCR set CCR Value, or retain Calculated/Granted Values |

[5] The Priority-Level AVP (AVP code 1046) is of type Unsigned 32. The AVP is used for deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request. Values 1 to 15 are defined, with value 1 as the highest priority level. Values 1 to 8 should only be assigned for services that are authorised to receive prioritised treatment within an operator domain. Values 9 to 15 may be assigned to resources that are authorised by the home network and thus applicable when a UE is roaming.

**Note** If the received and calculated PL values are equal, then the configured/calculated (not received) ARP is considered for PCI and PVI.

## Creating the CRD Table

The user must take special care while defining the CRD table to avoid an unconditional loop in case CRD uses cross referencing data from one table to another table.

**Step 1** Log into Policy Builder.

**Step 2** Select the **Reference Data** tab.

**Step 3** Click **Custom Reference Data Tables** and create a CRD table.

| Step 4 | Select the **Services** tab, and then click **Use Case Templates** > **Summary**. |
|---|---|
| Step 5 | Click **Use Case Template** link from the right side under **Create Child** to create a use case template. |
| Step 6 | Enter the name for use case template. |
| Step 7 | Select **Actions** tab. |
| Step 8 | Click **Add** in the **Service Configuration** pane to open the **Select Service Configuration** dialog box. |
| Step 9 | Select **DefaultBearerQoSActions** and click **OK** to add it in the **Service Configurations** pane. |
| Step 10 | Click **DefaultBearerQoSActions** to open the parameters pane on the right side. |

> **Note**     By default, **Enforce** is selected.

Use the following table if the user wants to bind QoS with the CRD table.

*Figure 3: Custom Reference Data Column*
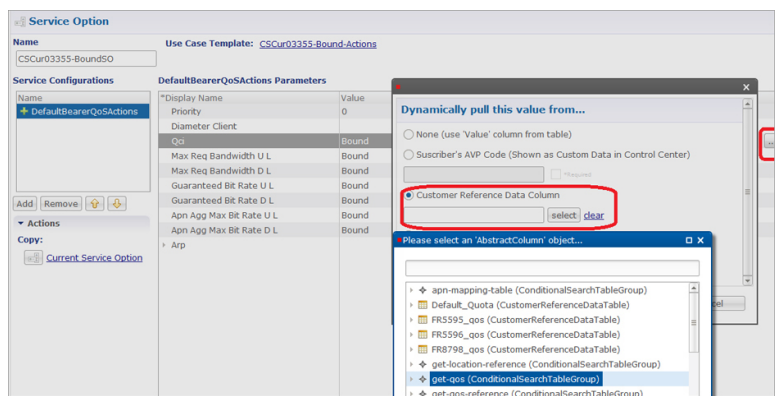


When the use case template is used in a Service Options, the user can bind each DefaultBearerQoSAction service object action attribute to the QoS action columns of the CRD. Similar binding of DefaultBearerQoS service configuration object attributes to QoS columns of the Default Bearer CRD can be done.

| Step 11 | Log into the Control Center to define the values for the parameters defined in Custom Reference Data tables. |
|---|---|
| Step 12 | Select the **Configuration** tab. |
| Step 13 | Under **Reference Data**, click the **Custom Reference Data Table** name to open a dialog box. Select a row and edit the values according to the user requirements. |

## Parameter Descriptions

The following table contains a list of common parameters:

*Table 4: QoS Profile - Common Parameters*

| Parameter | Description |
|---|---|
| Grant Requested QoS | It controls whether the requested QoS should be granted or not as the default bearer QoS.<br><br>Default value is unchecked. |
| Gx Client QoS Exclusion List | Gx client names that are allowed not to have a default bearer QoS installed. |

| Parameter | Description |
|---|---|
| Grant Requested QoS Over Global QoS | If this option is selected then the requested QoS should be granted even if the global QoS is provisioned. There are three types of QoS:<br><br>• From service<br><br>• From default QoS<br><br>• From requested<br><br>If this flag is checked then requested QoS takes priority over default QoS.<br><br>Default value is unchecked. |

**Note** For description/usage of other parameters, see Common Steps, on page 19.

# Default Bearer QoS Algorithm

*Table 5: Default Bearer QoS Algorithm*

| Service Configuration | Requested QoS | Granted QoS | |
|---|---|---|---|
| Yes | Yes | Follow the rules mentioned in QoS Authorization Algorithm, on page 8 for Granted QoS calculation. | |
| Yes | No | Granted configured. | |
| No | Yes | Reference data parameter value is "Yes". | Grant requested QoS. CPS can throttle the user based on the use case. |
| | | Reference data parameter value is "No". | Grant QoS using defaults values. If default values are not available, reject the request. CPS must define Gx QoS defaults like QCI, bit rates. |
| No | No | Grant QoS using defaults values. If default values are not available, reject the request. CPS must define Gx QoS defaults like QCI, bit rates. | |

# QoS Authorization Algorithm

CPS uses the following rules to calculate granted QoS. For default bearer, configured QoS refers to Default-Bearer-QoS and for dedicated bearers configured QoS refers to Max-QoS.

*Table 6: QoS Authorization Algorithm*

| IP-CAN-Type/RAT-Type | Evaluation Criteria | Granted QoS | | |
|---|---|---|---|---|
| IP-CAN:GPRS<br><br>RAT Type: Any | Evaluate QoS-Upgrade, QoS-Negotiation | QoS-Negotiation | QoS-Upgrade | Result |
| | | Yes | Yes | If Requested QoS > configured QoS: Grant Configured<br><br>If Requested QoS < configured QoS: Upgrade to configured |
| | | Yes | No | Requested QoS > configured QoS: Grant configured QoS<br><br>Requested QoS < configured QoS: Grant Requested QoS |
| | | No | Yes | Requested QoS > configured QoS: Reject with BEARER_NOT_AUTHORIZED<br><br>Requested QoS < configured QoS: Grant Requested QoS |
| | | No | No | Requested QoS > configured QoS: Reject with BEARER_NOT_AUTHORIZED<br><br>Requested QoS < configured QoS: Grant Requested QoS |
| =3GPP-EPS, RAT-Type = GERAN/UTRAN/EUTRAN | Evaluated based on IP-CAN-Type | Provision both QoS-Information and Default-EPS-Bearer-QoS.<br><br>If Requested QoS > configured QoS: Grant Configured QoS<br><br>If Requested QoS < configured QoS: Upgrade to configured QoS | | |
| | If RAT-Type is GERAN | Follow the rules as in IP-CAN-Type GPRS. | | |
| IP-CAN-Type=Non-3GPP-EPS | Evaluate based on IP-CAN-Type | Provision both QoS-Information and Default-EPS-Bearer-QoS. | | |
| IP-CAN-Type=DOCSIS (1), xDSL (2), WiMAX (3), 3GPP2 (4) | Evaluate based on IP-CAN-Type | Reject CCR request with DIAMETER_ERROR_BEARER_NOT_AUTHORIZED (5143) result code. | | |

# PCC Rules

## Overview

The purpose of the PCC rule is:

- To detect a packet belonging to an SDF to map that packet to proper IP-CAN bearer in downlink and uplink direction

- To identify the service

- To provide appropriate applicable charging

- To provide policy control

There are two different types of PCC rules:

- Dynamic PCC rules: These PCC rules are dynamically provisioned by PCRF to PCEF over Gx interface.

    - Pre-configured dynamic rules: These rules can be configured using Policy Builder

    - Dynamic generated rules: These rules can be generated by CPS e.g., as result of Rx interaction.

- Pre-defined PCC rules: These PCC rules are pre-configured in the PCEF. The PCRF can advise the PCEF to activate a set of PCC rules over Gx interface.

CPS can be configured to re-attempt to install PCC rules that fail to install or activate. See Rule Retry Profiles for more information.

# Policy Builder Configuration

| **Step 1** | Log into Policy Builder. |
| **Step 2** | Select the **Services** tab, and then click **Use Case Templates** > **Summary**. |
| **Step 3** | Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *PreConfiguredRule*. |
| **Step 4** | Enter the name for use case template. For example, name the new template as **PreConfiguredRule**. |
| **Step 5** | Select **Actions** tab. |
| **Step 6** | Click **Add** to open the **Select Service Configuration** dialog box. |
| **Step 7** | Select **PreConfiguredRule**, **PreDefinedRule**, and **PreDefinedRuleBase** one after another, and select the required service configuration parameters. |
| **Step 8** | Click **OK** to add the service in the **Service Configuration** pane. |

A PCC rules consists of following parameters:

**Table 7: PCC Rules Parameters**

| Parameter | Description |
| --- | --- |
| Service Identifier | The service identifier is used to identify a service or service component the SDF relates to. |
| charging key and charging parameters | online or offline charging |
| Flow status | Defines whether the service data flow is enabled (2) or disabled (3). |
| Rating Group | The charging key for the PCC rule used for rating purposes. |

| Parameter | Description |
|---|---|
| Service Identifier | The service identifier is used to identify the service or the service component the service data flow relates to. |
| Reporting Level | The Reporting-Level AVP is of type Enumerated, and it defines on what level the PCEF reports the usage for the related PCC rule.There are three types of reporting levels:<br><br>• SERVICE_IDENTIFIER_LEVEL (0): This value shall be used to indicate that the usage shall be reported on service id and rating group combination level, and is applicable when the Service-Identifier and Rating-Group have been provisioned within the Charging-Rule-Definition AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging.<br><br>• RATING_GROUP_LEVEL (1): This value shall be used to indicate that the usage shall be reported on rating group level, and is applicable when the Rating-Group has been provisioned within the Charging-Rule-Definition AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging.<br><br>• SPONSORED_CONNECTIVITY_LEVEL (2): This value shall be used to indicate that the usage shall be reported on sponsor identity and rating group combination level, and is applicable when the Sponsor-IdentityAVP, Application-Service-Provider-Identity AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging. |
| Metering Method | The Metering-Method AVP (AVP code 1007) is of type Enumerated, and it defines what parameters shall be metered for offline charging. The PCEF may use the AVP for online charging in case of decentralized unit determination and having three values:<br><br>• DURATION (0): This value shall be used to indicate that the duration of the service data flow shall be metered.<br><br>• VOLUME (1): This value shall be used to indicate that volume of the service data flow traffic shall be metered.<br><br>• DURATION_VOLUME (2): This value shall be used to indicate that the duration and the volume of the service data flow traffic shall be metered. |
| Precedence | Indicates the precedence of QoS rules or packet filters. |
| Retry Profile | Indicates the Rule Retry Profile to be used. Upon receipt of a Charging-Rule-Report indicating the failure to install or activate one or more rules, CPS will evaluate the failed rules and take further action.<br><br>See Rule Retry Profiles for more information. |

**Step 9**    On the **Services** tab, click **Services** > **Service Options** to create a service option and add the configured use case template.

**Note** To activate a predefined charging rule at PCEF, charging rule name must be used as a reference to the predefined charging rule. To activate a group of predefined charging rules within PCEF (For example, Gold users or gaming services) charging rule base name must be used as a reference to the group of predefined charging rules.

**Step 10** On the **Services** tab, click **Services** > **Services** to create a service and add the configured use case template.

# Table (CRD) Driven Rules

## Overview

ASR5K supports handling of Service Group QoS and defines new Gx AVPs which are exchanged between PCEF and PCRF. Additionally, CPS (PCRF) already supports various use cases related to PCC Rules provisioning and usage monitoring control as defined in 3GPP specification 29.212. Also, the new AVPs related to CISCO Service Group QoS are already supported in CPS.

This feature uses capabilities of Custom Reference Data tables and Search Table Group functionality of CPS.

CPS supports defining a Custom Reference Data table where in all sub-elements of Cisco QoS Group rules are possible to be configured with different values for each element. Also, it is possible to group these rules under a logical group. The application at run time supports queries based on this configured logical group, and Search Table Group, and is able to retrieve all applicable CISCO Service QoS Group rules and its sub-elements.

This feature can be configured by using three service options namely, TableDrivenCiscoQosGroupRule (For Cisco QoS Group rules), TableDrivenChargingRule (For dynamic PCC rules), and TableDrivenPredefinedChargingRule (For predefined PCC charging rules) . Description of their common parameters is listed in the following table.

**Note** Currently, Table Driven Rules does not support wildcards.

*Table 8: Common Parameters between TableDrivenCiscoQosGroupRule, TableDrivenChargingRule, and TableDrivenPredefinedChargingRule*

| Parameter | Description |
|---|---|
| Search Group | Search Group is a constant value which CPS uses to search within the Search Table Group indicated by "Search Table" element. |
| Search Column | Search Column must be bound to the Key column of the STG (which must be given a data type of Text). |
| Rule Name Source | Rule Name Source must be a key column as well. This filed must be bound to the rule name column within the STG which should be Text. |

*Table 9: Common Parameters between TableDrivenCiscoQosGroupRule and TableDrivenChargingRule*

| Parameter | Description |
|---|---|
| Flow Status Source | Flow Status Source must be bound to the Flow status column within the STG which should be Text. |
| Monitoring key Source | Monitoring key Source must be bound to the Monitoring Key column within the STG which should be Text. |
| Encoding format Source | Encoding format Source must be bound to the Encoding format column within the STG which should be either Boolean or Text. If this is defined as Text Data Type then Valid Values must be provided as (True/False). |
| Redirect Enabled Source | Redirect Enabled Source must be bound to the Redirect Enabled column within the STG which should be either Boolean or Text. If this is defined as Text Data Type then Valid Values must be provided as (True/False). |
| Redirect Address Type Source | Redirect Address Type Source must be bound to the Redirect Address Type column within the STG which should be Text. |
| Redirect Address Source | Redirect Address Source must be bound to the Redirect Address column within the STG which should be Text. |
| Use Override Server Address | Use Override Server Address must be bound to the Use Override Server Address column within the STG which should be either Boolean or Text. If this is defined as Text Data Type then Valid Values must be provided as (True/False). If this flag is true then it will take the address from the service option and if it is false then it would not override the redirect server address. |

*Table 10: Common Parameters between TableDrivenChargingRule and TableDrivenPredefinedChargingRule*

| Parameter | Description |
|---|---|
| **Input List (List)** | |
| Crd Column | The Crd column is bound to the appropriate key column within the STG for those AVPs which are inputs to this table. |
| Referenced Output Column | Reserved for future use. |
| Column Value | The value of the AVP that is bound to the Crd Column and has a single value. |
| Referenced MultiValue AVP Name | The name of the attribute that is bound to the Crd Column and has multiple values. |

# Policy Builder Configuration

## Table Driven Cisco QoS Group Rule

**Step 1**    Log into Policy Builder.

**Step 2**    Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 3**    Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *TableDrivenCiscoQosGroupRule*.

   a) Enter the name for use case template. For example, name the new template as **TableDrivenCiscoQoSGroupRule**.
   b) Select **Actions** tab.
   c) Click **Add** under **Service Configurations**.

      **Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

   d) Scroll down to the **gx** area in the list of service configuration objects, and select **TableDrivenCiscoQoSGroupRule**.

**Step 4**    Select **Services** > **Summary**.

**Step 5**    Click the **Service Option** link from the right side under **Actions** to create a service option using the *TableDrivenCiscoQosGroupRule* use case template.

   For usage of common parameters, see Common Parameter Descriptions.

**Step 6**    To bind the **Value**, select the name from the **Display Name** column and in **Value** column click **....** to open **Please select a 'CustomerReferenceDataTable' object**.

   See to continue with the configuration.

---

## Table Driven Charging Rule

**Step 1**    Log into Policy Builder.

**Step 2**    Select the **Services** tab, and then select **Use Case Templates** > **Summary**.

**Step 3**    Click **Use Case Template** link from the right side under **Create Child** to create a use case template for Table Driven Charging Rule.

   a) Enter the name for use case template. For example, name the new template as **TableDrivenChargingRule**.
   b) Select **Actions** tab.
   c) Click **Add** under **Service Configurations**.

      **Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

   d) Scroll down to the **gx** area in the list of service configuration objects, and select **TableDrivenChargingRule**.

**Step 4**    Select **Services** > **Summary**.

**Step 5**    Click the **Service Option** link from the right side under **Actions** to create a service option using the *TableDrivenChargingRule* use case template.

   For usage of common parameters, see Common Parameter Descriptions. Other parameters can be configured as follows:

*Table 11: TableDrivenChargingRule Parameters*

| Parameter | Description |
|---|---|
| Online Source | Online Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212. |

| Parameter | Description |
|---|---|
| Offline Source | Offline Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212. |
| Rating Group Source | Rating Group Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212. |
| Service Id Source | Service Id Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212. |
| Reporting Level Source | Reporting Level Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212. |
| Precedence Source | Precedence Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212. |
| Metering Method Source | Metering Method Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212. |
| Flow Information Source | Flow Information Source must be bound to the appropriate column within the STG, and Type should be Text.<br><br>**Note** A particular format should be used when adding Flow Information Source parameter so that CPS can perform proper Flow Information grouped AVP mapping. A wrongly formatted Flow Information Source can result in missing AVPs under Gx Flow Information AVP. Here is the format: `<Flow-Description>;<Flow-Direction>;<Decimal value of first octet of ToS-Class-AVP>;<Decimal value of second octet of ToS-Class-AVP>` |
| Use Override Server Address | Use Override Server Address must be bound to the appropriate column within the STG, and Type should be either True/False or Text. If this is defined as Text Type then valid values must be provided as True/False. |
| Override Server Address | Override Server Address is a constant value and if the Use Override Server Address flag is set to False, the parameter value is ignored. |
| Qci Source | Qci Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Max Req Bandwidth U L Source | Max Req Bandwidth U L Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Max Req Bandwidth D L Source | Max Req Bandwidth D L Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |

| Parameter | Description |
|---|---|
| Guaranteed Bit Rate U L Source | Guaranteed Bit Rate U L Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Guaranteed Bit Rate D L Source | Guaranteed Bit Rate D L Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Arp Priority Level Source | Arp Priority Level Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Arp Preemption Capability Source | Arp Preemption Capability Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Arp Preemption Vulnerability Source | Arp Preemption Vulnerability Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Apn Agg Max Bit Rate U L Source | Apn Agg Max Bit Rate U L Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Apn Agg Max Bit Rate D L Source | Apn Agg Max Bit Rate D L Source must be bound to the appropriate column within the STG, and Type should be Number.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Rule Retry Profile Name | Rule Retry Profile Name must be bound to the appropriate column within the STG, and Type should be Text.<br><br>For more information, refer to Common Parameters Used, on page 51. |
| Provision Default Bearer Qo S | Provision Default Bearer Qo S must be bound to the appropriate column within the STG, and Type should be either True/False or Text. If Type is defined as Text, then valid values must be provided as True/False. If the value is True, the Default Bearer QoS information from the session is applied to the rule while QoS information derived from the above parameters in this STG are ignored. |
| Tdf Application Identifier Source | Tdf Application Identifier Source references the application detection filter (for example, its value may represent an application such as a list of URLs, etc.), which the PCC rule for application detection and control in the PCEF applies. Tdf Application Identifier Source must be bound to the appropriate column within the STG, and Type should be Text. |
| Mute Notification Source | An indication whether application start/stop notification is to be muted for ADC Rule by the TDF. Mute Notification Source must be bound to the appropriate column within the STG, and it should be either Number or Decimal. |

| Parameter | Description |
|---|---|
| **Input List (List)** | |
| Crd Column | The Crd column is bound to the appropriate key column within the STG for those AVPs which are inputs to this table. |
| Referenced Output Column | Reserved for future use. |
| Column Value | The value of the AVP that is bound to the Crd Column and has a single value. |
| Referenced MultiValue AVP Name | The name of the attribute that is bound to the Crd Column and has multiple values. |

**Step 6**      To bind the value, click the **Value** field, and then click **...** to select a value.

**Step 7**      Select the required object to bind and click **OK**.

A sample selection is shown as follows:

**Figure 4: Binding a Value**
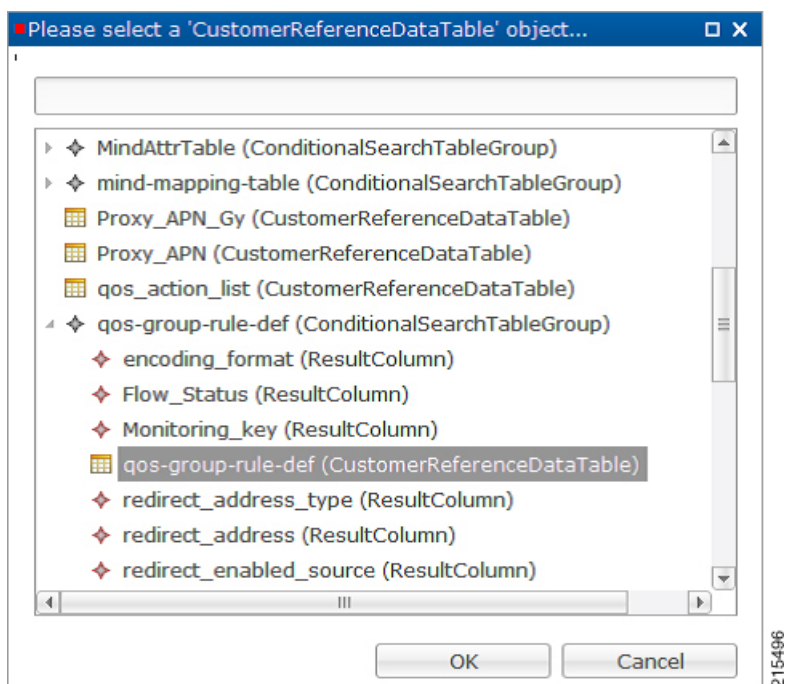


See to continue with the configuration.

## Table Driven Predefined Charging Rule

**Step 1**      Log into Policy Builder.

**Step 2**      Select the **Services** tab, and then select **Use Case Templates** > **Summary**.

**Step 3**  Click **Use Case Template** link from the right side under **Create Child** to create a use case template for Table Driven Predefined Charging Rule.

a)  Enter the name for use case template. For example, name the new template as **TableDrivenPredefinedChargingRule**.

b)  Select **Actions** tab.

c)  Click **Add** under **Service Configurations**.

   **Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d)  Scroll down to the **gx** area in the list of service configuration objects, and select **TableDrivenPredefinedChargingRule**.

e)  Save the use case template.

**Step 4**  Select **Services** > **Summary**.

**Step 5**  Click the **Service Option** link from the right side under **Actions** to create a service option using the *TableDrivenPredefinedChargingRule* use case template.

For description/usage of common parameters, see Overview, on page 12 and Common Parameter Descriptions.

**Step 6**  To bind the value, click the **Value** field and enter a value or click **...** to select a value.

**Step 7**  Select the required object to bind and click **OK**.

A sample selection is shown as follows:

**Figure 5: Binding a Value**
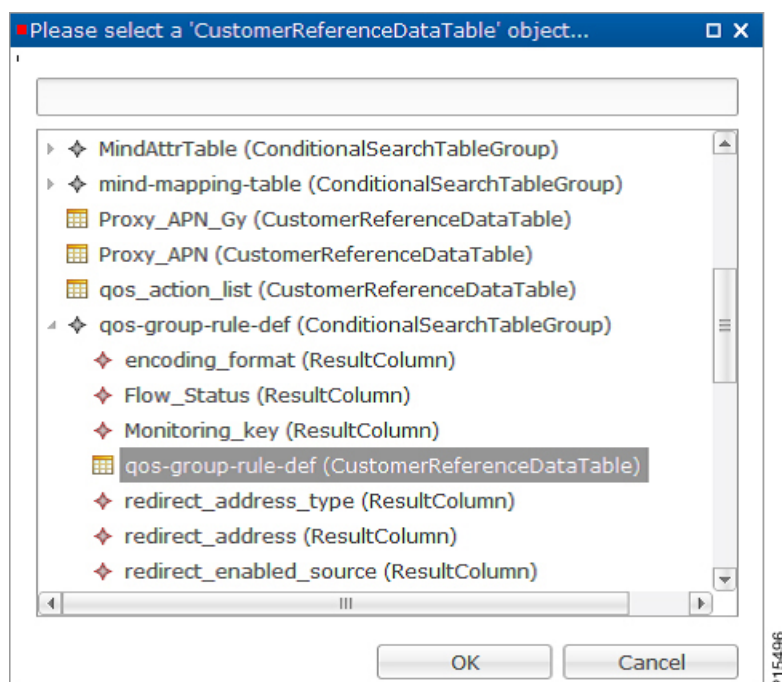
# Common Steps

**Step 1**    Since this approach leverages Custom Reference and Search Table Group capabilities of CPS, we need to configure a Search Table Group to be able to use the above Service Configuration to configure a Search-Group-Table with the output column specified.

- The "Rule_Group" in the STG is the key column indicating that searches need to be based on it.

- The "Search Group" and "Search Column" are expected to be configured or bound to the "Rule_Group" column of the STG.

**Step 2**    It is possible to retrieve the redirect Address related elements of CISCO Service Group QoS from another table.

**Note**        In other cases if Redirect URL STG is not required, and if redirect URL is being derived from other components of CPS, the use of override address is essential. The override server address can be derived from retrievers when the redirect address is not populated from CRD.

# Control Center Configuration

**Step 1**    Log into Control Center.

**Step 2**    Select the **Configuration** tab, and then select **Configuration** > **Reference Data**.

**Step 3**    Select the STG created in Policy Builder and add data by creating new rows.

# CRD Supported Features

## Table Driven Rule Name Support

This feature allows CPS to filter the table generated rules (TableDrivenCiscoQosGroupRule, TableDrivenChargingRule, and TableDrivenPredefinedChargingRule) based on what the PCEF supports (via another rule list from CRD). Only rules common to both tables are included in actual policy.

**Step 1**    Create a new STG/CRD called 'gw-version-mapping-table'.

- Based on the incoming Gx origin Host and Gx Origin Realm, determine the GW Version.

- Make this table as 'Best Match': Enable the check box for best match utility.

**Table 12: gw-version-mapping-table Parameters**

| Origin Host (Input) | Original Realm (Input) | GW Version (Output) |
|---|---|---|
| gx_origin_host | gx_origin_realm | gw_version |
| Bind to 'Gx Request Origin-Host' | Bind to 'Gx Request Origin-Realm' | NA |

**Table Driven Rule Name Support**

*Figure 6: Origin Host*



*Figure 7: Origin Realm*



*Figure 8: GW Version*

**Step 2** Create another STG/CRD called 'gw-rule-mapping-table'.

- Link the input column 'gw_version' in this table to the output from the earlier table.

- Both columns are input columns in this case.

**Table 13: gw-rule-mapping-table Parameters**

| GW Version (Input) | Rule Name (Input) |
|---|---|
| Gw_version | Rule_name |
| Bind to result column from 'gw_version_mapping-table' | NA |

**Note** For same GW version, we can define multiple rules, so we need to have each rule name as an input column.

**Figure 9: GW Version**



**Step 3** In the existing 'QoS-Group-Rules' template (where we already have the Table Driven objects) add the new object 'TableDrivenRuleNameSupport'.

**Step 4** In the same Service Configuration Object 'QoS-Group-Rules', then click add. The new service configuration object (added in the template) is available here.

Update the following fields in the new service configuration object:

- Search Table: Click the icon in the **Value** section and select **gw-rule-mapping-table** from the drop-down list.

- Search Group: Click the icon in the **Pull Value from** section and select the Group level output **gw_version** from **gw-version-mapping-table**.

- Search Column: Click the icon the **Value** section and select **gw_version** input column from **gw-rule-mapping-table**.

- Rule Name Source: Click the icon the **Value** section and select **rule_name** input column from the same **gw-rule-mapping-table** as above.

With this configuration, CPS would do a UNION operation with the QoS groups obtained from the new 'TableDrivenRuleNames' Object (based on the GW version) and the ones retrieved from 'TableDrivenCiscoQoSGroupRules' (based on Rule-Mapping table & Rule-Group-Mapping table).
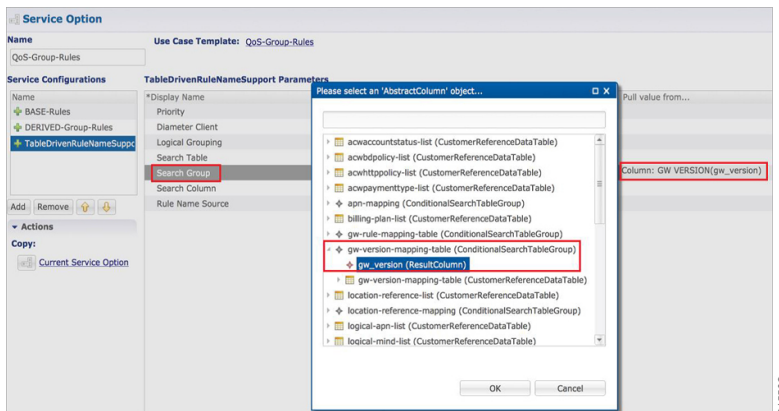
Mapping for Search Table of TableDrivenRuleNameSupport:

*Figure 10: Search Table Mapping*
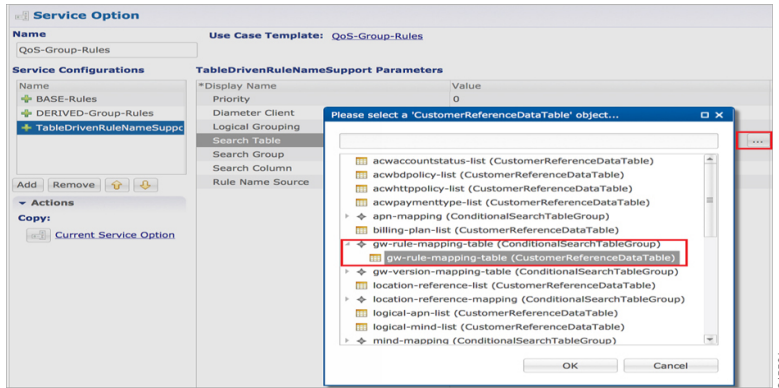


Mapping for Search Group of TableDrivenRuleNameSupport:

*Figure 11: Search Group Mapping*



Mapping for Search Column of TableDrivenRuleNameSupport:
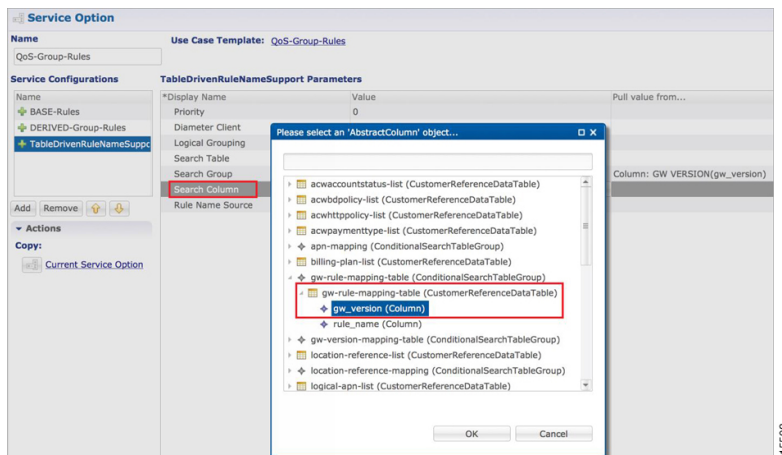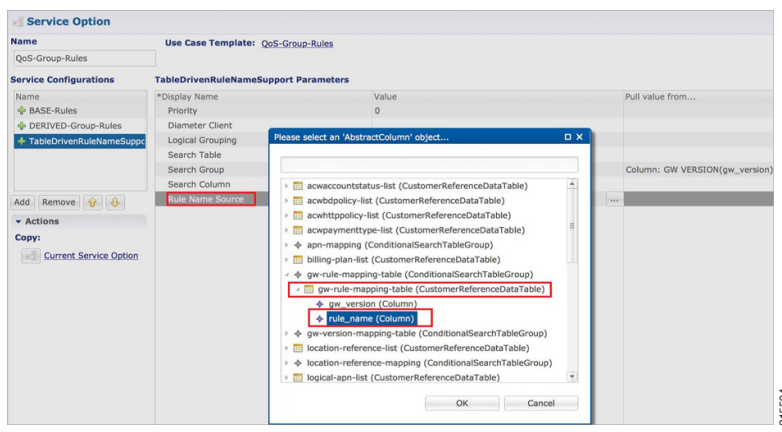
*Figure 12: Search Column Mapping*



*Figure 13: Rule Name Source*



## Best Match Table Logic

CPS supports each table look-up in CRD, which needs to be one of the match types shown in the following list, along with Best Match table. This approach is fast, efficient, and very easy to troubleshoot, and scales when there are dozens, scores, or hundreds of combinations of values.

When the **Best Match** option is selected in the Custom Reference Data Table configuration, look-ups occur within a CRD table in the following order:

- Exact string match

- Higher priority regex match (if multiple regex patterns match)

- Regular expression match (default behavior)

- Wild card character (*)

The following figures contain examples of a CRD table configuration and its corresponding output table in Control Center.

- STG Table as Input for Best Match:

*Figure 14: Best Match Option*



- Output Table, which can take an exact string match, a higher priority regex match, a regular expression match, and a wildcard entry like *.

*Figure 15: Matching Examples*



# Table (CRD) Driven Rule Refresh on Rule Failure

## Overview

CPS now supports the ability to install new charging rules based on the Charging rule name and its status reported in CCR-U from PCEF in Charging Rule Report AVP for a particular rule/rules.

- The rule name and rule status (ACTIVE(0)/INACTIVE(1)/TEMPORARILY_INACTIVE(2)) are derived from the session and then used as input for the new rules to be installed for the Gx session.

- If a rule status is received as NOT ACTIVE in CCR-U and if that rule is present as an input in the refresh table on which CPS should install new refresh rules, CPS will remove the rule in CCA-U and install the corresponding newly derived refresh rules from the table in CCA-U.

- Later if one of the new or derived refresh rules installed above comes with a Charging-Rule-Report as ACTIVE/INACTIVE/TEMP_INACTIVE, CPS will install the default bearer rule back again.

# TableDrivenChargingRuleRefresh Service Option

The TableDrivenChargingRuleRefresh service option provides support for this functionality. The specific parameters provided in this service option are described later in Table in section Create a Table Driven Refresh Rule, on page 26.

On receiving a Charging-Rule-Report AVP in Gx CCR-U, the TableDrivenRuleRefresh service option is evaluated to find if there are rows configured for the reported rule-name and reported rule-status in the table defined in the Search Table field. If there is an entry in the table, CPS takes the entry from the Output Rule Group Column and uses that value as an input for Search Group in the Table Driven Charging Rule.

If Output Search Table is configured for TableDrivenChargingRuleRefresh, CPS performs a lookup only on those TableDrivenChargingRule objects which has the Search Table matching the Output Search Table in TableDrivenChargingRuleRefresh.

If multiple rules are reported in a Gx-CCR U, then all the corresponding groups in the table are used as an input to TableDrivenChargingRule service option and all the rules from all the groups are evaluated.

The following table shows an example configuration:

*Table 14: TableDrivenChargingRuleRefresh Example Configuration*

| Rule Name | Rule Status | Rule Group |
|-----------|-------------|------------|
| Rule-A    | 2           | Group-1    |
| Rule-B    | 2           | Group-2    |
| Rule-C    | 0           | Group-3    |

In this example, if CPS receives Rule-A and Rule-B in the ChargingRule Report AVP, then the corresponding groups, Group-1 and Group-2 are evaluated. This is then used to query the TableDrivenChargingRule table with Search Group as Group-1 and Group-2. So all the rules with Group as Group-1 and Group-2 would be installed in CCA-U.

**Note**

- The TableDrivenChargingRule would have the Search Table and Search Column configured as described above. The Search Group would come as an output of the query done using TableDrivenRuleRefresh service option. Even if the Search Group is blank, if there are Output Rule Groups evaluated due to TableDrivenChargingRuleRefresh, CPS queries the TableDrivenChargingRule with the Search Group value as the Output Rule Groups. (If more than one are configured, CPS queries them one by one.)

- In case there is a value in Search Group in the TableDrivenChargingRule, CPS first evaluates the TableDrivenChargingRules with the mentioned Search Group. After finishing the above query, CPS then proceeds to look up the Output Search Groups retrieved as a result of TableDrivenChargingRuleRefresh queries.

- If the refresh rule and the default bearer rule come as OUT_OF_CREDIT immediately or simultaneously, it can create a loop. To prevent a loop, refer to Prevention of a Refresh Loop, on page 28. However, this is not an ideal situation and it is agreed upon that in production we won't encounter looping. Also CPS cannot guarantee stopping of loops in such scenario as the session may connect and disconnect and may go into loop each time.

- Also, the feature does not actually look at the event trigger but only on the rule name and status reported.

# Policy Builder Configuration

## Create a Table Driven Rule Refresh CRD Table

**Step 1**    In Policy Builder, create and configure a Search Table Group (STG).

*Figure 16: Search Table Group (STG)*
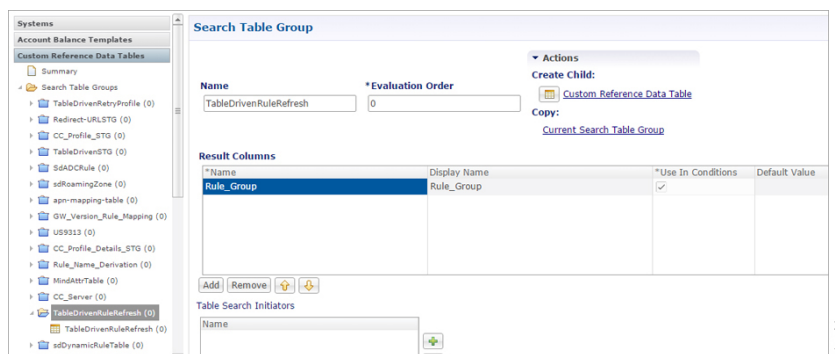
**Step 2**    Create and configure a **Custom Reference Data Table** under this STG.

*Figure 17: Custom Reference Data Table*
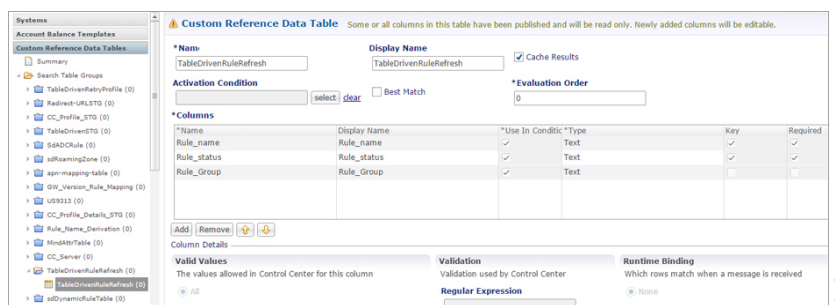
The Rule_Group output column shown above is used as an input to evaluate TableDrivenChargingRule service option.

## Create a Table Driven Refresh Rule

**Step 1**    Log into Policy Builder.

**Step 2**    Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 3**    Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *TableDrivenChargingRuleRefresh*.

**Step 4**    Select **Services** > **Summary**. Click **Service Option** link from the right side under **Actions** to create a service option using Use Case Template created above.

**Step 5**    In the Search Table row, select the 'TableDrivenRuleRefresh' CRD table created in the previous section to bind it to this service option.

To bind the value, select the name from the Display Name column and in Value column click **....** to open **Please select a 'CustomerReferenceDataTable' object**.

Note    For usage of common parameters, see Common Parameter Descriptions. Other parameters can be configured as follows:

**Table 15: TableDrivenChargingRuleRefresh Parameters**

| Parameter | Description |
|---|---|
| Search Table | The search table to lookup from. |
| Input Rule Name Column | The input column for the SearchTableGroup (STG), which contains the rule name. |
| Output Rule Status Column | The input column for the STG, which contains the rule status against which new rules are to be added. |
| Output Rule Group Column | The output column for the STG, which contains the rule group, which would be used as a group to search the TableDrivenChargingRule. |
| Output Search Table | In case there are multiple TableDrivenChargingRules mapped with multiple Search Tables, and if we want to use only one table to be looked upon for new rules installation on rule failure, we can give the table as Output Search Table so that only one TableDrivenChargingRule object, which has the 'Search Table' matching the 'Output Search Table' in TableDrivenChargingRuleRefresh, is evaluated for refresh rules and not all the objects. |

The Output Search Table in TableDrivenChargingRuleRefresh should match with the Search Table in the TableDrivenChargingRule for looking up the output groups in the table for deriving the table driven charging rules.

The Search Group in TableDrivenChargingRules is not bound to anything. The output Rule_Group from the Refresh Table is automatically taken as input to the TableDrivenChargingRules service option.

# Control Center Configuration

**Step 1**    Log into Control Center.

**Step 2**    Select **Configuration** > **Configuration** > **Reference Data**.

**Step 3**    Select the STG created in Policy Builder and add data by creating new rows.

*Figure 18: Configuring Reference Data*
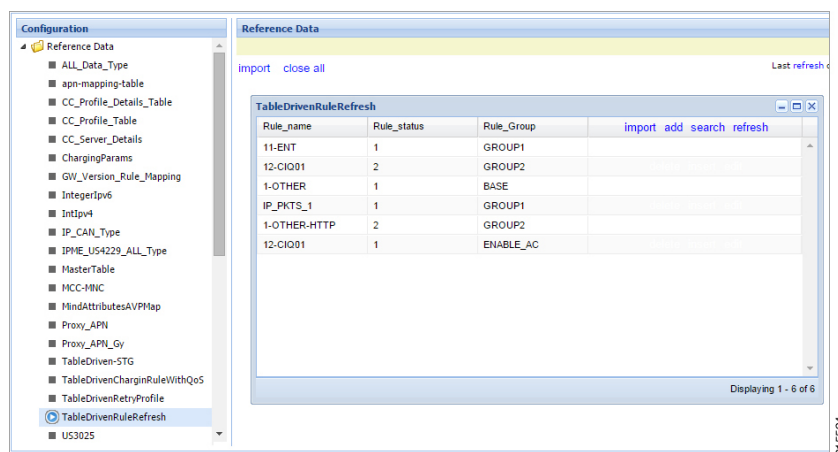


## Prevention of a Refresh Loop

To prevent a scenario where successive INACTIVE statuses would cause CPS to repeatedly attempt to install the same 2 rules, CPS tracks the number of times a refresh rule is installed within a specific time period. If a loop is detected, CPS will skip the rule installation.

The settings which control the loop detection can be customized. Contact your Cisco representative for more information.

# Custom Features

## Service Group QoS

### Overview

The goal of Service Group QoS is to provide support within PCRF in ASR5K to define and enforce Fair-Usage-Policy (FUP) per subscriber. CPS provides support for CISCO Service Group QoS in ASR5K based deployment of PCEF. Service Group QoS is sent over the Gx interface when CPS (PCRF) tries to install or remove rules for a subscription based on various triggers. These attributes are CISCO deployment specific and are enabled only for the "Gx clients" which support Service Group QoS Rules.

### Policy Builder Configuration

**Step 1**  Log into Policy Builder.

**Step 2**  Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 3**  Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *CiscoQoSGroupRule*.

a)  Enter the name for use case template. For example, name the new template as **CiscoQoSGroupRule**.

b)  Select **Actions** tab.

c)  Click **Add** under **Service Configurations**.

**Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **gx** area in the list of service configuration objects, and select **CiscoQoSGroupRule**.

User can configure various QoS Group Rule parameters depending on the network requirements. For configuration/usage of different parameters, refer to Common Steps, on page 19

**Step 4** Select **CiscoQoSGroupRule** and click required service configuration parameters that need to be configured. Click **OK** to add the service in **Service Configuration** pane.

**Step 5** In **Services** tab, click **Services** > **Service Options** to create a service option and add the configured Use Case Template in CiscoQoSGroupRule to configure Service Option.

**Step 6** In **Services** tab, click **Services** > **Services** to create a service and add the configured Use Case Template in CiscoQoSGroupRule to configure Service.

# Content Filtering

### Overview

The goal of Content Filtering is to provide support for content filtering within the network by use of Policy ID's. Policy identifiers (Policy IDs) are rules that are configured on the ASR 5000 platform and invoked by the CPS. Policy IDs are used to implement the required Content Filtering policies defined for the subscriber. The Policy IDs are selected at the ASR 5000 by provisioning their values through the Gx interface by the PCRF.

When a user initiates a session, the ASR5K communicates with the CPS to initialize the defined policies. CPS provides the Policy ID to the ASR5K to provide the necessary Content Filtering services for the user.

The main aim of this feature is for CPS to provide Policy ID's configured in the subscriber's service to the PCEF (ASR5K).

### Policy Builder Configuration

There are three sequential procedures to configure the Policy IDs using the CPS.

**Step 1** Log into Policy Builder.

**Step 2** Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 3** Click **Use Case Template** link from the right side under **Create Child** to create a use case template.

**Step 4** Provide a name for the template in the **Name** field.

**Step 5** Select **Actions** tab.

**Step 6** To define the basic template, under Service Configurations, click **Add**. Select the required configurations from the popup window and click **OK**.

**Note**
• Cisco Content Filtering Policy option must be selected along with other configurations to provide Content Filtering services.

• The check boxes in the Allow Override column are checked by default. This allows the subscriber to change the values in the Service Option. Otherwise, the value remains constant.

**Step 7** Click the save icon.

**Step 8**     In the left column, select **Services**.

**Step 9**     Locate the template that was defined in the above procedure and click **Service Option** in the summary window. The configurations that had been selected appears in the window.

**Step 10**    Click **OK**. Define the required parameters.

**Step 11**    Select the configuration to define the parameters from the list of Service Configurations.

**Step 12**    In the Parameters columns, set the required values.

**Step 13**    Click **CiscoContentFilteringPolicy** and set the Policy ID value in the parameters field.

> **Note**     Value for Policy ID should not be set to zero (0). Policy IDs can be dynamically assigned to the subscriber by referring to the Custom Reference Data Tables.

**Step 14**    Click **Pull value from** in the parameters column to assign Policy IDs dynamically from a predefined Custom Reference Data Table.

# Emergency Data Services

## Overview

CPS supports Emergency Data Services as per the procedures defined in 3GPP TS 29.212. The operator has to configure a list of Emergency Access Point Names (APNs) that are valid for the operator. These APNs are then used by CPS to identify a session as an Emergency session. CPS also supports installation of QoS and Rules for emergency sessions.

## Configure Diameter Gx Client for Emergency APNs

The emergency APNs have to be configured in the Diameter Gx Client configuration. So, first you need to configure a Diameter Gx Client.

For more details on how to configure the Diameter Gx Client, refer Diameter Clients.

**Step 1**     Log into Policy Builder.

**Step 2**     Select the **Reference Data** tab.

**Step 3**     From the left pane, select **Diameter Clients**.

**Step 4**     Expand the Gx Clients by clicking on the arrow right next to "Gx Clients". If you do not see this arrow, this means the Gx Client has not been created.

Refer Diameter Clients to create a Gx Client.

**Step 5**     Select the Gx Client name created by you. Gx Client attributes as shown below will come up in the right pane.

*Figure 19: Gx Client Attributes*



**Step 6**     Click **Add** to configure the emergency APNs. The following window is displayed.

*Figure 20: Emergency APN Configuration*



**Step 7**     Type the name of the emergency APN that you want to add in the **Value to Add (String)** text box and click **Add**.

**Step 8**     Click **OK**. In the example shown above, four APN entries are already added.To remove an APN from this list, select the APN to be removed and click Remove.

CPS supports wildcarding for the Emergency APN names. As shown in the example above, we have used '*' for wildcarding. CPS uses standard Java pattern characters for APN names. The pattern needs to follow the standard Java regular expression syntax described here.

## Configure Service for Emergency Sessions

For emergency APNs, the IMSI may not be present. Hence, CPS allows emergency sessions without subscriber authentication.

**Step 1**    Log into Policy Builder.

**Step 2**    Select the **Services** tab.

**Step 3**    From the left pane, select **Domains**.

**Step 4**    Select the domain name that you want to use for emergency subscribers. Domain attributes open up in the right pane.

To create a new Domain, refer Overview.

**Step 5**    Select the **Advanced Rules** tab.

**Step 6**    Click **select** near Anonymous Subscriber Service.

**Step 7**    In the new window displayed, select the service that you want to assign for emergency sessions and click **OK**.

## Configure Prioritizing Emergency Sessions using APNs

Emergency calls are fast-tracked through the CPS platform by bypassing authorization logic. As a user, the CPS platform enables to prioritize these emergency calls by APN. CPS uses "Emergency Message Priority", for this prioritization. These attributes are part of "Inbound Message Overload Handling" feature under "Diameter Configuration".

For more details, refer Inbound Message Overload Handling.

**Step 1**    Log into Policy Builder.

**Step 2**    Select the **Reference Data** tab.

**Step 3**    From the left pane, select **Systems** and expand your system name or cluster name.

**Step 4**    Select and expand the **Plugin Configurations**.

**Step 5**    Select **Diameter Configuration**. Diameter configuration screen appears in the right pane.

**Step 6**    Check **Inbound Message Overload Handling** check box.

**Step 7**    Click **Add** under Message Handling Rules table.

*Figure 21: Adding a New Row*



**Step 8**    Click **...** in the **Diameter Client** column.

*Figure 22: Selecting a DiameterClient Object*
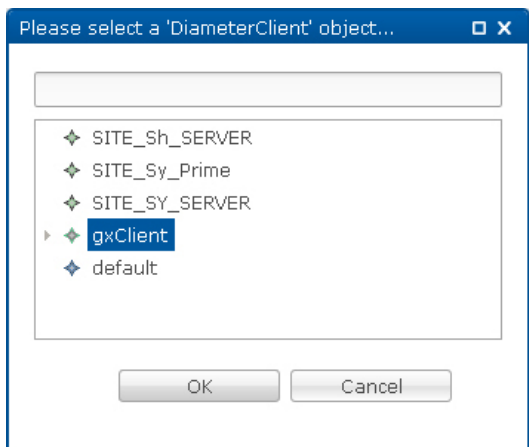


**Step 9**    Select the Gx Client in which we added the emergency APNs in Configure Diameter Gx Client for Emergency APNs, on page 30 and click **OK**.

**Step 10**    Configure the other parameters of the table.

*Figure 23: Sample Configuration*



**Note**    For the detailed explanation of all the parameters of the Inbound Message Overload Handling feature, refer Inbound Message Overload Handling. The following table explains the parameters relevant to the prioritization of emergency sessions.

*Table 16: Prioritization of Emergency Session - Parameters*

| Parameter | Description |
|---|---|
| Default Priority | Default priority to be assigned to an incoming message, if no specific one is defined in the Message Handling Rules table. <br><br> Default value is 0. |
| Emergency Message Priority | Default priority assigned to incoming messages related to an emergency session. <br><br> Default value is 0. |
| Message Handling Rules | Defines specific inbound message overload handling rules based on different criteria. Message Handling Rules are generic. This means for all CCR-I messages, if you want to process with priority, user needs to set the configuration in Message Handling Rules. |

**Note** Higher the value of the priority, the higher is the priority. User must take care that the Emergency Message Priority field value is higher than the priority column values present in the Message Handling Rules, so that the Emergency Messages are processed first than the usual messages. If we take the example values configured above, then this is how the priority is assigned to the incoming messages.

| Incoming Message | Priority | Description |
|---|---|---|
| Any message for any emergency session/APN | 5 | The default emergency message priority is assigned as this is emergency APN. |
| A Gx CCR-I message for the non-emergency APN | 3 | The protocol, command code, and request type match the message handling rules. |
| A Gx CCR-U message for the non-emergency APN | 0 | Request type does not match with the value in the "Message Handling Rules". So, the default priority is assigned. |

**Note** By default, the emergency message priority is higher than the default priority. This means, if you do not configure the Inbound Message Overload Handling, then default priority = 0 and emergency message priority = 1.

# RAN Congestion

## Overview

Currently, when RAN congestion is configured, at the hour boundary there is a check for congestion level change. If the congestion level has changed then RAR is sent in which new rules corresponding to changed congestion level are applied.

The next evaluation time for session is set to the time when the congestion level changes next. At that hour boundary again the session is evaluated, and new rules applicable to changed level are applied. Since all the sessions are getting re-evaluated at applicable hour boundaries where the congestion level changes, there is a possibility of huge amount of RAR's being generated by CPS. CPS can generate this load of RARs without any issues as it is distributed among the CPS VMs. However, there might be limitation on other network elements to handle the RAR surge.

To prevent RAR burst at the hour boundary, evaluate configured services for the next hour based on the appropriate congestion levels. Also, preinstall the rules specifying Activation and Deactivation times.

## Policy Builder Configuration

**Step 1** Log into Policy Builder.

**Step 2** Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 3** Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *PreDefinedRuleBase*.

**Step 4** Enter the name for use case template. For example, name the new template as **PreDefinedRuleBase**.

**Step 5** Select **Actions** tab.

**Step 6** Click **Add** to open **Select Service Configuration**.

**Step 7** Select **PreDefinedRuleBase** and click required service configuration parameters that need to be configured. Click **OK** to add the service in Service Configuration pane.

*Figure 24: Configuration for Current Hour*

*Figure 25: Configuration for Next Hour*



- In order to achieve the RAN congestion use case to install rules based on congestion levels, we need to configure use case initiators to modify the rules based on congestion level.

  - Use case initiator - on condition that congestionLevel = 1, changes rulename to internetlvl1

  - Use case initiator - on condition that congestionLevel = 2, changes rulename to internetlvl2

  - Use case initiator - on condition that congestionLevel = 3, changes rulename to internetlvl3

- Assume congestionLevel is 1 for current hour and 2 for next hour. When services are evaluated for current time, this evaluates only to internetlvl1. In order to also evaluate services for the look ahead hour, we need to add corresponding modified rules for each with use case initiators as follows:

  - Use case initiator - on condition that congestionNextHourLevel = 1, changes rulename to internetlvl1

  - Use case initiator - on condition that congestionNextHourLevel = 2, changes rulename to internetlvl2

  - Use case initiator - on condition that congestionNextHourLevel = 3, changes rulename to internetlvl3

Example of configuration for one of the use case modifiers is shown below:

**Figure 26: Use Case Option Tab**



**Figure 27: Use Case Initiators Tab**



# Control Center Configuration

**Step 1**    Log into Control Center.

**Step 2**    Select **Configuration** > **Configuration** > **Reference Data**.

**Step 3**    Select the STG created in Policy Builder and add data by creating new rows.

A sample configuration is as follows:

*Figure 28: Sample Configuration*



**Note**
- 0-3 are congestion levels
- Currently, we supports only current and next level congestion.

# Parameter Descriptions

The following table provides information related to RAN Congestion parameters:

*Table 17: RAN Congestion Parameters*

| Parameter | Description |
| --- | --- |
| Rule Name | Any name which you want to give for rule name. |
| Scheduled Hour: drop-down list with three values. | Default: It turns OFF Hour Boundary RAR enhancement feature for look ahead rules installation at hour boundary and causes rules to behave in normal fashion of getting installed at hour boundary as applicable<br><br>CurrentHour: For the current hour rule activation time will be current time, deactivation time will be next hour.<br><br>NextHour: For the next hour rule activation time will be next hour, deactivation time will be next-next hour. |

**Note** By default, CPS sets the next evaluation time as per the next change in congestion level. To configure CPS to do a forward lookup for multiple changes in congestion level, add the following parameter to qns.conf:

```
-DcongDataLookAhead=true
```

# Usage Monitoring

## Overview

CPS supports Usage-Monitoring over Diameter Gx interface with different Balance Code, Dosage and monitoring level. Usage monitoring key Identifies the usage monitoring control instance and is subscribed using Event-Trigger AVP = USAGE_REPORT.

CPS also supports time based Gx usage monitoring control and reporting based on as 3GPP 29.212 Rel 12 Sections 4.5.16 and 4.5.17. It supports the ability to configure a Gx usage monitoring key as volume, time or both.

## Policy Builder Configuration

**Step 1**   Login to Policy Builder.

**Step 2**   Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 3**   Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *TableDrivenCiscoQosGroupRule*.

　　a) Enter the name for use case template. For example, name the new template as **UsageMonitoringKey**.

　　b) Select **Actions** tab.

　　c) Click **Add** under **Service Configurations**.

　　　**Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

　　d) Scroll down to the **gx** area in the list of service configuration objects, and select the required usage monitoring object. For example, **UsageMonitoringKey**.

　　　For parameter descriptions under **UsageMonitoringKey**, refer to UsageMonitoringKey.

　　　For parameter descriptions under **UsageMonitoringKeyDual**, refer to UsageMonitoringKeyDual.

**Step 4**   In the left pane of the **Services** tab, click **Services** > **Service Options** to create a service option and add the *UsageMonitoringKey* use case template.

**Step 5**   In the left pane of the **Services** tab, click **Services** > **Services** to create a service and add the configured *UsageMonitoringKey* use case template.

## Scheduled Usage Monitoring

To support scheduling, CPS uses Monitoring-Time AVP in Monitoring information. To use Monitoring-Time AVP CPS supports Usage Monitoring Congestion Handling (UMCH) feature on Gx. If the PCEF does not support UMCH feature, CPS uses the RAR message to request account balance usage details of the previous or older schedule. CPS will charge the account balance usage against the old schedule and further grants a new dosage value as per the new schedule.

CPS uses the next evaluation time set on the diameter session to trigger the RAR message for requesting the usage-report on schedule's time boundary. The current Usage-Monitoring information in the Gx session is added with monitoring schedules to grant and track the usage for the PCEF, based on current and adjacent schedules. It also provides support to bind different balance code to each schedule. CPS grants, reserves and charges the respective balance as per the usage monitoring schedule defined. CPS defines dosage on each

schedule and accordingly grants single units to PCEF in Granted-Service-Units AVP. It also defines charging rate on each schedule. The default charging rate is 1.

This feature provides support to configure multiple schedules in monitoring-key service configuration.

## Configure Scheduled Usage Monitoring

Scheduled Usage Monitoring is configured in the Service Options section of the Services tab. The Service Configuration UsageMonitoringKey allows scheduled monitoring in the Monitoring Schedule (List) parameter.

Before configuring a scheduled monitoring, the following configuration must be completed in the Policy Builder:

- Configure the Account Balance Templates in the **Reference Data** tab.

  For more information, see Account Balance Templates.

- Configure a Use Case Template in the **Services** tab.

  For more information, see Use Case Templates.

Configuration restrictions while defining Monitoring schedule in Policy Builder:

- The time value should be entered in hh:mm format.

- Monitoring schedule should be complete for 24 hours.

- First monitoring schedule should start at midnight with start-time value as 00:00 and last schedule should end on next midnight with end-time value as 23:59.

- Time entry with 23:59 will be rounded-up to complete the 24 hour schedule.

| **Step 1** | Select the **Services** tab. |
|---|---|
| **Step 2** | Click **Services** > **Service Options**, and select the corresponding Service option whose name matches the Use Case Template. |
| **Step 3** | Provide a name for the service in the **Name** field. |
| **Step 4** | In the **Service Configurations** section, click **Add**. The **Select Service Configuration** dialog box is displayed. |
| **Step 5** | Select **UsageMonitoringKey** and click **OK**. |
| | For parameter descriptions under **UsageMonitoringKey**, refer to UsageMonitoringKey. |
| **Step 6** | In the Service configuration parameters, select **Monitoring Schedule** and click **Add Child** to add a **UsageMonitoringSchedule**. |
| **Step 7** | Select the **UsageMonitoringSchedule** to provide the values as shown in the example. |

*Figure 29: Usage Monitoring Schedule*



a) Enter the Start Time in 24 hrs format (00:00 to 23:59).

b) Enter the End Time in 24 hrs format (00:00 to 23:59).

c) Provide a value for the Balance Code. Click the **...** button. A window appears. Select the required **Balance Code** and click **OK**.

d) Enter the **Dosage** value.

e) Enter the **Rate** value.

To add multiple **UsageMonitoringSchedule**, click **Add Child** and add the parameters according to your requirements.

# Time Usage Monitoring

CPS supports time based Gx usage monitoring control and reporting based on as 3GPP 29.212 Rel 12 Sections 4.5.16 and 4.5.17.

It supports the ability to configure a Gx usage monitoring key as volume, time or both.

**Balance**: This feature reuses the time related units like seconds, minutes, hours, and so on for balance that are already provided by Account Balance Templates. No new threshold types have been added. Only % thresholds can be used with Time balances.

**Use Case Template**: A new UsageMonitoringKeyDual service configuration has been added to support the time usage monitoring (The existing UsageMonitoringKey is still supported for Volume Usage monitoring). This new option provides a way to configure usage monitoring for both time and volume (independently as well as together under single monitoring key). To monitor usage under one key for Volume and Time, both the balance codes need to be provided in the Service Configuration. For independent monitoring, only the relevant type of fields can be set. For example, for only Volume monitoring, fields related to time monitoring can be left blank/null and vice versa. Multiple instances of UsageMonitoringKeyDual can also be included in the service configuration each corresponding to a unique monitoring key.

Gx Message Handling: The following new AVPs are now supported under this feature:

- CC-Time (within Granted-Service-Unit and Used-Service-Unit)

- Quota-Consumption-Time (within Usage-Monitoring-Information)

For configuration in Policy Builder, refer to .

# Bandwidth Monitoring

## Overview

The purpose of this feature is to track bandwidth and apply policies based on that. Normal usage monitoring is used to track usage but not bandwidth. This feature is based on usage monitoring key being installed in order to have the usage reported by the PCEF. Using this feature, the service provider can install a monitoring key and the different thresholds that are used to flag the subscriber. This feature works in parallel with the usage monitoring feature but the usage monitoring feature has a higher priority since that one is about charging traffic. In this context 'higher priority' means that usage monitoring feature installs any usage monitoring keys it needs to do its job.

Bandwidth monitoring installs any additional monitoring keys it needs while reusing any monitoring keys that were already installed. In order to reuse a monitoring key the same monitoring key name should be used in both BandwidthMonitor and UsageMonitoringKey objects. ReportingTimeout value is in minutes and is used to set the Revalidation-Time AVP so that the subscriber has a chance to get unthrottled before the allocated dosage is used. The BandwidthThreshold Lower Value is in kbps and when the computed bandwidth used is over that value, the corresponding Label is set to the subscriber for the particular application identified by Name attribute.

## Policy Builder Configuration

**Step 1**      Log into Policy Builder.

**Step 2**      Select the **Services** tab and then click **Use Case Templates**.

**Step 3**      If you want to create a new use case template, click **Use Case Template** in the main window under **Create Child** to open the default use case template.

**Step 4**      Enter the name for the template. For our example, name it as *Bandwidth Monitoring*.

**Step 5**      Select **Actions** tab.

**Step 6**      Click **Add** under **Service Configurations** to open the **Select Service Configuration** dialog box.

**Step 7**      Select the necessary service configuration objects and click **OK** to add the objects in **Service Configurations** pane.

> **Note**      The Bandwidth Monitoring service option includes the BaseUsageMonitoringKey that enables Gx usage monitoring for this subscriber.

**Step 8**      Click **Services** > **Service Options** > *name of the Use Case Template*.

**Step 9**      Click **Service Options** in the main window under **Create Child** to open the **Select Service Configuration** dialog box, which contains already defined Service Configurations, and click **OK**.

**Step 10**      Select **BandwidthMonitor** from the **Service Configurations** pane.

     a)   We can monitor the Bandwidth usage on a per session rule base or per PCC rule base. For example, let us name this bandwidth monitor per session base as SESSION.

b) Under **Monitoring Key**, enter the values for Monitoring Key, Dosage, and Monitoring Level. For session level, the Monitoring Level should be 0.

c) Also enable the BaseUsageMonotoringKey.

d) Under **Bandwidth Threshold**, define three levels for bandwidth - Low, Medium and High.

**Step 11** Click **Services** > **Service Options** > *name of the Use Case Template*.

**Step 12** Click **Use Case Option** in the main window under **Create Child** to open the **Use Case Option** pane and name it as **Low Bandwidth Usage**.

**Step 13** Click **Add** to open the **Select Service Configuration** dialog box, select **DefaultBearerQoS** and click **OK** to add the service.

**Step 14** Rename the configured service as **LowDefaultBearerQoS**.

**Step 15** Click **Use Case Initiators** tab. Click plus sign (+) to add a service initiator. Rename the initiator as **Low**.

**Step 16** Under **Conditions**, click **Add** to open the **Select the Condition Phrase which you would like to use** dialog box, select the required condition and click **OK**.

The added condition is displayed in **Conditions** pane.

**Step 17** Click **Add All** under **Available Input Variables**.

a) In the **Value** column under name (String), enter the name for the bandwidth monitor that you specified in .

b) In the **Value** column under label (String), enter the Bandwidth threshold value defined in .

**Step 18** Create another initiator and add the condition **A bandwidth monitor status does not exist to it**. Add the name (String) to the condition.

**Step 19** Repeat the steps from to for Medium and High bandwidth usage.

**Step 20** Click **Services** > **Service Options** > *name of the Use Case Template* provided in . Add all the service configurations.

**Step 21** Define the different parameters for low, medium and high bandwidth usage monitoring in the **Service Configurations** pane according to the customer requirements.

A sample configuration for Low Bandwidth Usage Monitoring is shown below.

*Figure 30: Low Bandwidth Usage Monitoring*



**Step 22**     Click **Services** > **Services**, and the click **Service** under **Create Child** to open the **Service** dialog box.

**Step 23**     Enter the name in **Code** and **Name** text fields.

**Step 24**     Click **Add** to open the **Select Service Configuration** dialog box. Select the service that you configured in , and click **OK**.

**Step 25**     Select **Use V9 Event Trigger Mapping and Rel8 Usage Monitoring Supported** under **Diameter Configuration**.

- If Use V9 Event Trigger Mapping check box is not selected, the event trigger mapping ID (33) from 3GPP TS 29.212 V11.10.0 (2013-09) is used.

- If Use V9 Event Trigger Mapping check box is selected, the event trigger mapping ID (26) from 3GPP TS 29.212 V9.5.0 (2013-09) is used.

# Parameter Descriptions

The following parameters can be configured in Bandwidth Monitoring:

| Parameter | Description |
|---|---|
| Name | Any name you can give. |
| Reporting Timeout | The revalidation timer for defined dosage. |
| Lower Value | The minimum bandwidth value that you can give for that particular Label. This value is not standard and defined as per requirement and should be an integer. |
| Label | The name of label, which can depend upon the user's requirement. |

# Override Control AVP

## Overview

CPS supports Override-Control specific AVPs in CCA-i and CCA-u responses to the PCEF on the Gx Interface and Gx RAR message. These AVPs are used to override charging parameters for predefined and static rules on the PCEF.

## Policy Builder Configuration

**Step 1**   Log into Policy Builder.

**Step 2**   Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 3**   Click **Use Case Template** link from the right side under **Create Child** to create a use case template.

**Step 4**   Enter the name for the template. For our example, name the new template as *CiscoOverrideControl*.

**Step 5**   Select **Actions** tab.

**Step 6**   In the newly created template, click **Add** under the **Service Configurations** pane. This will list all the service configuration objects available on the PCRF. Select the **CiscoOverrideControl** object from the **gx** section.

**Step 7**   After selecting the necessary service configuration object, click **OK** to add the object in **Service Configurations** pane.

The following parameters can be configured for Override Control AVP.

**Table 18: Override Control AVP Parameters**

| Parameter | Description |
|---|---|
| Override Rule Name | Specifies the name of the rule (predefined or static) for which the override values are sent.<br><br>**Note**     The "Charging-Action-Name" and "Exclude-Rule" AVPs should not be sent and shall be ignored if this AVP is present. |
| Charging-Action-Name | Specifies the name of the charging action for which override values are sent. |
| Override Charging Action Exclude Rule (List) | Defines the rule name where the override will not be applied. |
| Override Service Identifier | Used to override the value of Service Identifier configured in the charging action. |
| Override Rating Group | Defines the value of the rating group configured for a static/predefined rule. |
| Override Reporitng Level | Used to override the value of reporting level configured in the charging action. |
| Override Online | If Enabled, it overrides the online value configured for static/predefined rule.<br><br>Default value is Enable. |

| Parameter | Description |
|---|---|
| Override Offline | If Enabled, it overrides the offline value configured for static/predefined rule.<br><br>Default value is Enable. |
| Override Metering Method | Used to override the value of Metering Method configured in the charging action. |
| Override QoS | This AVP is used to Override QoS-Information for a predefined rule or charging action. These values are ignored (if present) while applying override values to a static rule. |
| Override-Max-Requested-Bandwidth-UL | Defines the maximum bit rate allowed for the uplink direction. |
| Override-Max-Requested-Bandwidth-DL | Defines the maximum bit rate allowed for the downlink direction. |
| Override-Guaranteed-Bitrate-UL | Defines the guaranteed bit rate allowed for Uplink direction. This AVP should be included only for rules on dedicated bearers. |
| Override-Guaranteed-Bitrate-DL | Defines the guaranteed bit rate allowed for downlink direction. This AVP should be included only for rules on dedicated bearers. |
| Override-Allocation-Retention-Priority | This AVP is of type grouped and is used to override the pre-configured value of ARP. |
| Override Merge Wildcard | Used to merge override control charging/policy parameters between override control with specific charging action and wildcard override control. |

AVP Structure in response/request message:

```
Override-Control
  *Override-Rule-Name
  Override-Charging-Action-Parameters
                      Override-Control-Merge-Wildcard
   Charging-Action-Name
   *Online-Charging-Action-Exclude-Rule
   Override-Charging-Parameters
   Override-Service-Identifier
    Override-Rating-Group
    Override-Reporting-Level
    Override-Online
    Override-Offline
    Override-Metering-Method
   Override-Policy-Parameters
    Override-QoS-Information
     Override-QoS-Class-Identifier
     Override-Max-Requested-Bandwidth-UL
     Override-Max-Requested-Bandwidth-DL
     Override-Guaranteed-Bitrate-UL
     Override-Guaranteed-Bitrate-DL
     Override-Allocation-Retention-Priority
      Override-Priority-Level
      Override-Pre-emption-Capability
      Override-Pre-emption-Vulnerability
```

| Name | Code | Vendor-ID | Flags | | |
|---|---|---|---|---|---|
| | | | M | V | P |
| Override-Control | 132017 | 9 | 0 | 1 | 0 |
| Override-Rule-Name | 132018 | 9 | 0 | 1 | 0 |
| Override-Charging-Action-Parameters | 132019 | 9 | 0 | 1 | 0 |
| Override-Charging-Action-Exclude-Rule | 132021 | 9 | 0 | 1 | 0 |
| Override-Charging-Parameters | 132022 | 9 | 0 | 1 | 0 |
| Override-Service-Identifier | 132023 | 9 | 0 | 1 | 0 |
| Override-Rating-Group | 132024 | 9 | 0 | 1 | 0 |
| Override-Reporting-Level | 132025 | 9 | 0 | 1 | 0 |
| Override-Online | 132026 | 9 | 0 | 1 | 0 |
| Override-Offline | 132027 | 9 | 0 | 1 | 0 |
| Override-Metering-Method | 132028 | 9 | 0 | 1 | 0 |
| Override-Policy-Parameters | 132029 | 9 | 0 | 1 | 0 |
| Override-QoS-Information | 132030 | 9 | 0 | 1 | 0 |
| Override-QoS-Class-Identifier | 132031 | 9 | 0 | 1 | 0 |
| Override-Max-Requested-Bandwidth-UL | 132032 | 9 | 0 | 1 | 0 |
| Override-Max-Requested-Bandwidth-DL | 132033 | 9 | 0 | 1 | 0 |
| Override-Guaranteed-Bitrate-UL | 132034 | 9 | 0 | 1 | 0 |
| Override-Guaranteed-Bitrate-DL | 132035 | 9 | 0 | 1 | 0 |
| Override-Allocation-Retention-Priority | 132036 | 9 | 0 | 1 | 0 |
| Override-Priority-Level | 132037 | 9 | 0 | 1 | 0 |
| Override-Pre-Emption-Capability | 132038 | 9 | 0 | 1 | 0 |
| Override-Pre-Emption-Vulnerability | 132039 | 9 | 0 | 1 | 0 |
| Override Merge Wildcard | 132079 | 9 | 0 | 1 | 0 |

# Gx RAR Traffic

CPS is enhanced to support certain call flows and reduce Gx-RAR traffic towards PCEF as follows:

- Gx CCR-U reports all Rx Charging-Rule as inactive in which case PCRF terminates the Rx Session and avoids sending Gx-RAR to remove rules already reported as inactive.

- Gx CCR-U reports one or more Rx Charging Rule as inactive in which case PCRF would trigger a Rx RAR to PCSF which if responded with a DIAMETER_UNKNOWN_SESSION_ID (5002) terminates the Rx Session and avoids sending Gx RAR with Charging-Rule-Remove AVPS for rules already reported as inactive.

- Gx CCR-U reports one or more Rx Charging Rule as inactive in which case PCRF would trigger a Rx RAR to PCSF which is responded with a DIAMETER_SUCCESS (2001). Any subsequent AAR-U with MCD/MSC flow status reported as removed, removes the corresponding Rx Charging-Rule and does not trigger a Gx RAR with Charging-Rule-Remove AVP.

# Configuring Policies Based on Gx Events

This section covers the following topics:

## Overview

CPS supports the ability to make policy decisions based on the following event triggers received over the Gx interface:

- OUT_OF_CREDIT

- REALLOCATION_OF_CREDIT

- CREDIT_MANAGEMENT_SESSION_FAILURE

- CISCO_EVENT_TRIGGER

The policy decisions based on the above event triggers could be the following:

For Gx interface:

- Switch the UE from ONLINE to OFFLINE or vice versa

- Change the Charging-Rule-Base-Name of the UE

- Change (add/delete) the Charging-Rule-Name (predefined) of the UE

- Change (add/modify/delete) the Charging-Rule-Name (Dynamic) of the UE

- Ability to retry the impacted rule, number of retries, and the unique retries between each retry

For Rx interface:

- Initiate a tear down/removal of the IMS rule over Rx

- Inform the Rx client of the impacted rule and the reason for impact

For Sy interface:

- Ability to terminate or reinitiate Sy session

For Sd interface:

- Ability to terminate Sd session

## Policy Builder Configuration

The following procedure is an example of how to configure Policy Builder to use the ActionBasedOnGxEventTrigger service configuration object to make policy decisions based on event triggers and associated rule failure codes received over the Gx interface.

**Step 1**     Log into Policy Builder.

**Step 2**     Click **REFERENCE DATA** > **Custom Reference Data Tables** > **Search Table Groups**.

**Step 3**     Click **Search Table Group**.

**Step 4**     Under Table Search Initiators do the following to evaluate the CRD such that the condition is always false and table is not evaluated every time on any event by the policy engine:

a)   Click the + sign to add an initiator.

b)   Enter a name for the initiator in the Initiator Name field.

c)   Select **A customer reference data AVP exists** as the initiator conditions.

d)   Select **A customer reference data AVP exists**, click the **Add code**, and then enter **CRD-CODE** (dummy value to restrict CRD evaluation) as the code value. Similarly, click **Add value**, and then enter **true** as the value.

**Step 5**     Click the **Custom Reference Data Table** link.

**Step 6**     Under Columns, click **Add** and enter the following input and output values:

- CHARGING-RULE-NAME: This input value should be set to **Key** and **Runtime Binding** should be set to **None**.

- RULE-FAILURE-CODE: This input value should be set to **Key** and **Runtime Binding** should be set to **None**.

- CISCO-CC-FAILURE-TYPE: This input value should be set to **Key** and **Runtime Binding** should be set to **None**.

- Credit-Management-Status: This input value should be set to **Key**. For **Runtime Binding**, select **Bind to Diameter request AVP code** and enter **Credit-Management-Status**.

- Rx-Rule-Remove: Output value. Possible values are true and false.

- Session-ReInitiate: Output value. Possible value is SY_V11.

- Session-Terminate: Output value. Possible values are: SY_V11, SD_V11, or SY_V11;SD_V11.

The input AVPs and their corresponding CRD input columns must be configured in the ActionBasedOnGxEventTrigger service configuration object. When CPS receives a Gx CCR message with the Charging-Rule-Report AVP or the Credit-Management-Status AVP, CPS performs a one-time query on this CRD table.

A one-time query on this CRD is also performed when CPS receives Charging-Rule-Report AVP with ACTIVE_WITHOUT_CREDIT_CONTROL(10) for PCC-Rule-Status and Cisco-Event with Cisco-CC-Failure-Type.

If the Remove-Rx-Rule AVP exists in the output with value = true, the following conditions can occur:

- In case the query is based on Charging-Rule-Report AVP, then the rule status is updated as INACTIVE for all the reported rules and CPS sends Rx RAR for those rules.

| Note | Rx RAR will only be sent if Specific-Action = INDICATION_OF_FAILED_RESOURCES_ALLOCATION is subscribed by the AF or Specific-Action = INDICATION_OF_OUT_OF_CREDIT is subscribed by the AF and OUT_OF_CREDIT event trigger (Gx) is received in CCR-U. |
|------|------|

- In case the query is based on Credit-Management-Status AVP, then all Rx rules are removed and Rx session is terminated by sending Rx ASR.

**Step 7** Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

**Step 8** Click the **Use Case Template** link from the right side under **Create Child** to create a use case template.

**Step 9** Enter the name for the template. In this example, name the new template as *ActionBasedOnGxEventTrigger* .

**Step 10** Click the **Actions** tab.

**Step 11** In the newly created template, click **Add** under the **Service Configurations** pane. This will list all the service configuration objects available on PCRF. Select the **ActionBasedOnGxEventTrigger** object under the **gx** section.

**Step 12** Click **OK** to add the object in **Service Configurations** pane.

For the list of configurable parameters see ActionBasedOnGxEventTrigger

| Important | The **AVP Name** must be the same as mentioned in the following table while defining parameter values for ActionBasedOnGxEventTrigger Service Configuration object. The **Column** values are referenced from example CRD table columns created in . The other values mentioned in the table are used for example purpose only. |
|-----------|------|

*Table 19: Parameter Values for ActionBasedOnGxEventTrigger Service Configuration Object*

| Parameter | Value |
|-----------|-------|
| Stg Reference | Event-Rule-Failure-Mapping |
| **List of Input Column Avp Pairs** | |
| Avp Name | Charging-Rule-Name |
| Column | CHARGING-RULE-NAME |
| Avp Name | Rule-Failure-Code |
| Column | RULE-FAILURE-CODE |
| Avp Name | Cisco-CC-Failure-Type |
| Column | CISCO-CC-FAILURE-TYPE |
| **List of Output Column Avp Pairs** | |
| Avp Name | Remove-Rx-Rule |
| Column | Rx-Rule-Remove |
| Avp Name | Terminate-Session |
| Column | Session-Terminate |

| Parameter | Value |
|-----------|-------|
| Avp Name | Reinitiate-Session |
| Column | Session-ReInitiate |

**Important** For any Gx action, a generic output column can be added which can be used as an input to any other CRD table.

**Step 13** Click **Use Case Initiators** and do the following so that the use case is true only in the following conditions:

When CPS receives event trigger CREDIT_MANAGEMENT_SESSION_FAILURE:

a) Click the + sign to add a service initiator.
b) Enter a name for the initiator in the Initiator Name field.
c) Select **A Gx Event Triggr exists** as the initiator conditions.
d) Select **A Gx Event Triggr exists**, click the **Add All**, and then enter **46** as the **eventTrigger** value.

When CPS receives event trigger CREDIT_MANAGEMENT_SESSION_FAILURE (46) and/or Cisco-Event with CREDIT-CONTROL-FAILURE (5):

a) Click the + sign to add a service initiator.
b) Enter a name for the initiator in the Initiator Name field.
c) Select **CustomCiscoEvent** as the initiator conditions.
d) Select **A Cisco Custom Gx Event Trigger exists**, click the **Add All**, and then enter **5** as the **eventTrigger** value.
e) Select **A Gx Event Trigger exists** as the initiator conditions.
f) Select **A Gx Event Trigger exists**, click the **Add All**, and then enter **46** as the **eventTrigger** value.

# Common Parameters Used

The following table contains the common parameters that can be configured under all the sections mentioned in this chapter:

**Table 20: Common Parameters**

| Parameter | Description |
|-----------|-------------|
| Qci | The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS, excluding the applicable bitrates and ARP. It is applicable both for uplink and downlink direction. The QCI values 0, 10 – 255 are divided for usage as follows:<br><br>• 0: Reserved<br><br>• 10-127: Reserved<br><br>• 128-254: Operator specific<br><br>• 255: Reserved |
| Max Req Bandwidth UL | It defines the maximum bit rate allowed for the uplink direction. |

| Parameter | Description |
|---|---|
| Max Req Bandwidth DL | It defines the maximum bit rate allowed for the downlink direction. |
| Guaranteed Bit Rate UL | It defines the guaranteed bit rate allowed for the uplink direction. |
| Guaranteed Bit Rate DL | It defines the guaranteed bit rate allowed for the downlink direction. |
| Apn Agg Max Bit Rate UL | It defines the total bandwidth usage for the uplink direction of non-GBR QCIs at the APN. |
| Apn Agg Max Bit Rate DL | It defines the total bandwidth usage for the downlink direction of non-GBR QCIs at the APN. |
| Priority Level Values: 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain. Values: 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming. | The priority level is used to decide whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request.<br><br>Values 1 to 15 are defined, with value 1 as the highest level of priority.<br><br>• Values: 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain.<br><br>• Values: 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming. |
| Preemption Capability | If it is provided within the QoS-Information AVP, the AVP defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the default bearer can get resources that were already assigned to another bearer with a lower priority level.<br><br>• 0: This value indicates that the service data flow or bearer is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level.<br><br>• 1: This value indicates that the service data flow or bearer is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied. |

| Parameter | Description |
|---|---|
| Preemption Vulnerability | If it is provided within the QoS-Information AVP, the AVP defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the default bearer can lose the resources assigned to it in order to admit a pre-emption capable bearer with a higher priority level. <br><br>• 0: This value indicates that the resources assigned to the service data flow or bearer can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied. <br><br>• 1: This value indicates that the resources assigned to the service data flow or bearer shall not be pre-empted and allocated to a service data flow or bearer with a higher priority level. |
| Monitoring Key | Identifies a usage monitoring control instance. Any value can be given. |
| Priority | It is priority of the service option within the service. |
| Diameter Client | The client configuration is used to apply different policies based on PCEF type. This is optional parameter. |
| Rule Group | Rule Group is to classify rules at PCRF to change set of predefined rules based on policy. This is an optional parameter. |
| Enable Resource Allocation Notification | This is having two values Enabled and Disabled. Default value is disabled. |
| Dual Stack Session | This is having two values Enabled and Disabled. Default value is disabled. |
| Framed I P Type | It is having four options. Default option is ANY_ONE. <br><br>• ANY_ONE <br><br>• BOTH <br><br>• IPv4_ADDRESS <br><br>• IPv6_ADDRESS |
| ToD Schedule | Identifies the schedule for rule activation and deactivation. |

# Sd Services

## Overview

The Sd reference point is located between the Policy and Charging Rules Function (PCRF) and the Traffic Detection Function (TDF). The Diameter session on Sd is established either at the request of the PCRF in

case of solicited application reporting by initiating a (TSR - TDF Session Request) or at the request of the TDF by initiating an (CCR-I) in case of unsolicited application reporting. Session modifications may be initiated by either TDF or PCRF.

### Solicited Application

For the solicited application reporting, the Sd reference point is used for:

- Establishment and termination of TDF session between PCRF and TDF.

- Provisioning of Application Detection and Control rules from the PCRF for the purpose of traffic detection and enforcement at the TDF.

- Usage monitoring control of TDF session and of detected applications.

- Reporting of the start and the stop of a detected application's traffic and transfer of service data flow descriptions for detected applications, if deducible, from the TDF to the PCRF.

### Unsolicited Application

For the unsolicited application reporting, the Sd reference point is used for:

- Establishment and termination of TDF session between PCRF and TDF.

- Reporting of the start and the stop of a detected application's traffic.

- Transfer of service data flow descriptions for detected applications, if deducible, and transfer of Application instance identifier, if service data flow descriptions are deducible, from the TDF to the PCRF.

As part of the IP-CAN Session Establishment or Modification procedure, in case of solicited application reporting with a TDF, the PCRF initiates a TDF Session Establishment with the selected TDF. The TDF is selected based on data received from the PCEF or a local configuration at the PCRF and or SPR data for the subscriber.

TDF Session Termination happens in any of the following cases:

- The corresponding IP-CAN session is terminated.

- At any point of time when the PCRF decides that the session with TDF is to be terminated (for example, subscriber profile changes).

# Policy Builder Configuration

**Step 1**     Log into Policy Builder.

**Step 2**     Select the **Services** tab, and then click **Use Case Templates**. Click **Summary** and select **Use Case Template**.

**Step 3**     Click **Actions** tab.

**Step 4**     Click **Add** to open the **Select Service Configuration** dialog box.

**Step 5**     Select **ADC-Predefined-Rule** and click required service configuration parameters that need to be configured. Click **OK** to add the service in **Service Configuration** pane.

**Step 6**     In the **Services** tab, click **Services** > **Service Options** to create a service option and add the Use Case Template that you just configured.

**Step 7**     In the **Services** tab, click **Services** > **Services** to create a service and add the Use Case Template that you just configured.

# Common Parameters Used

The following table contains the common parameters configured for Sd Services:

*Table 21: Common Parameters*

| Parameter | Description |
|---|---|
| Qci | The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS, excluding the applicable bitrates and ARP. It is applicable both for uplink and downlink direction. The QCI values 0, 10 – 255 are divided for usage as follows:<br><br>• 0: Reserved<br><br>• 10-127: Reserved<br><br>• 128-254: Operator specific<br><br>• 255: Reserved |
| Max Req Bandwidth UL | It defines the maximum bit rate allowed for the uplink direction. |
| Max Req Bandwidth DL | It defines the maximum bit rate allowed for the downlink direction. |
| Guaranteed Bit Rate UL | It defines the guaranteed bit rate allowed for the uplink direction. |
| Guaranteed Bit Rate DL | It defines the guaranteed bit rate allowed for the downlink direction. |
| Apn Agg Max Bit Rate UL | It defines the total bandwidth usage for the uplink direction of non-GBR QCIs at the APN. |
| Apn Agg Max Bit Rate DL | It defines the total bandwidth usage for the downlink direction of non-GBR QCIs at the APN. |
| Priority Level Values: 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain. Values: 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming. | The priority level is used to decide whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request.<br><br>Values 1 to 15 are defined, with value 1 as the highest level of priority.<br><br>• Values: 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain.<br><br>• Values: 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming. |

| Parameter | Description |
|---|---|
| Preemption Capability | If it is provided within the QoS-Information AVP, the AVP defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the default bearer can get resources that were already assigned to another bearer with a lower priority level.<br><br>• 0: This value indicates that the service data flow or bearer is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level.<br><br>• 1: This value indicates that the service data flow or bearer is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied. |
| Preemption Vulnerability | If it is provided within the QoS-Information AVP, the AVP defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the default bearer can lose the resources assigned to it in order to admit a preemption capable bearer with a higher priority level.<br><br>• 0: This value indicates that the resources assigned to the service data flow or bearer can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied.<br><br>• 1: This value indicates that the resources assigned to the service data flow or bearer shall not be pre-empted and allocated to a service data flow or bearer with a higher priority level. |
| Monitoring Key | Identifies a usage monitoring control instance. Any value can be given. |
| Priority | It is priority of the service option within the service. |
| Diameter Client | The client configuration is used to apply different policies based on PCEF type. This is optional parameter. |
| Rule Group | Rule Group is to classify rules at PCRF to change set of predefined rules based on policy. This is an optional parameter. |
| Flow Status | Defines whether the service data flow is enabled or disabled. |
| Redirect Address Type | Defines the address type of the address given in the Redirect-Server-Address AVP. |
| Redirect Support | This value indicates that redirection is enabled for a detected application's traffic. |
| Redirect Server Address | This value indicates the target for redirected application traffic. |

| Parameter | Description |
|-----------|-------------|
| Event-Trigger | This is not to re-request rules. Primarily to notify start/stop of applications or report usage. |

*Table 22: Sd Parameters*

| Parameter | Description |
|-----------|-------------|
| Tdf Application Identifier | This references the application detection filter (for example, its value may represent an application such as a list of URLs, etc.), which the PCC rule for application detection and control in the PCEF applies. |
| Mute Notification | An indication whether application start/stop notification is to be muted for ADC Rule by the TDF. |