Gy Interface Support

This chapter provides an overview of the Gy interface and describes how to configure the Gy interface.

Gy interface support is available on the Cisco system running StarOS 9.0 or later releases for the following products:

- GGSN
- HA
- IPSG
- PDSN
- P-GW

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in the administration guide for the product that you are deploying.

Introduction

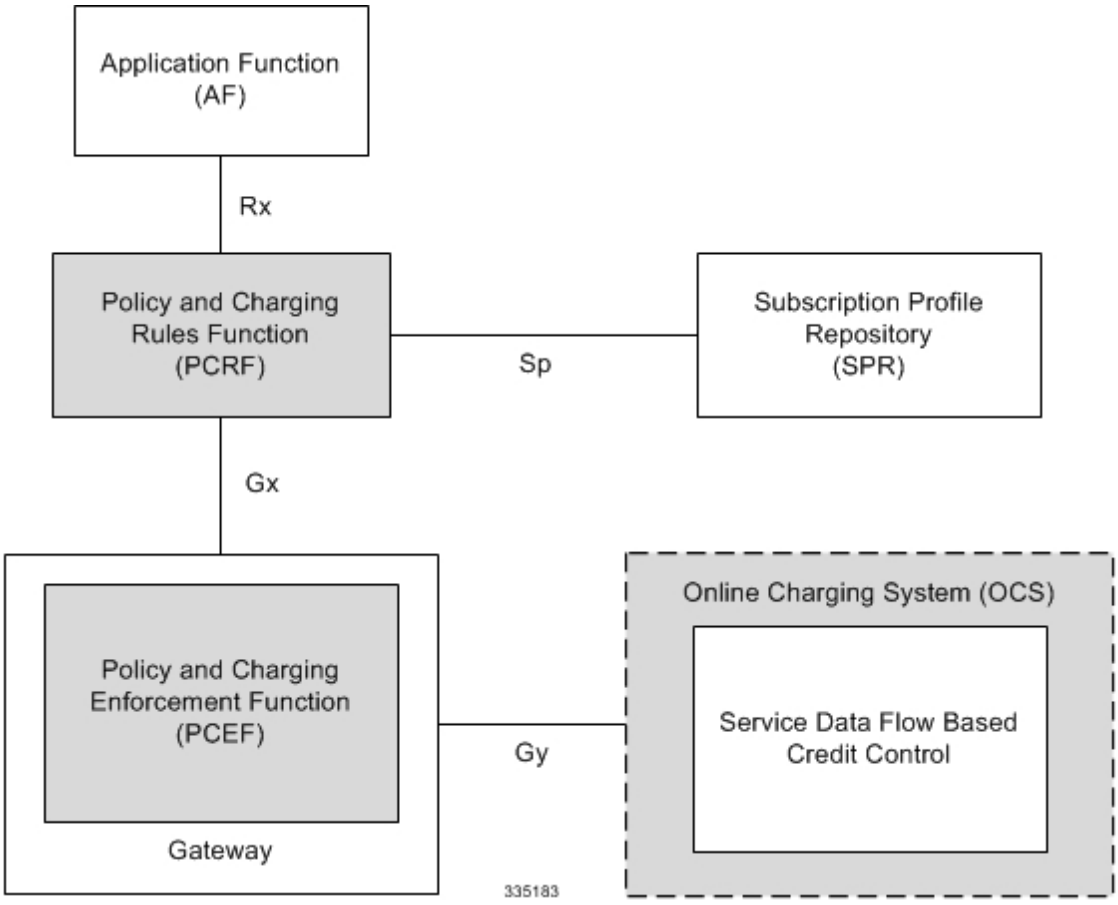
The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

The Gy interface makes use of the Active Charging Service (ACS) / Enhanced Charging Service (ECS) for real-time content-based charging of data services. It is based on the 3GPP standards and relies on quota allocation. The Online Charging System (OCS) is the Diameter Credit Control server, which provides the online charging data to the PCEF/GW. With Gy, customer traffic can be gated and billed in an online or prepaid style. Both time- and volume-based charging models are supported. In these models differentiated rates can be applied to different services based on ECS shallow- or deep-packet inspection.

In the simplest possible installation, the system will exchange Gy Diameter messages over Diameter TCP links between itself and one prepay server. For a more robust installation, multiple servers would be used. These servers may optionally share or mirror a single quota database so as to support Gy session failover from one server to the other. For a more scalable installation, a layer of proxies or other Diameter agents can be introduced to provide features such as multi-path message routing or message and session redirection features.

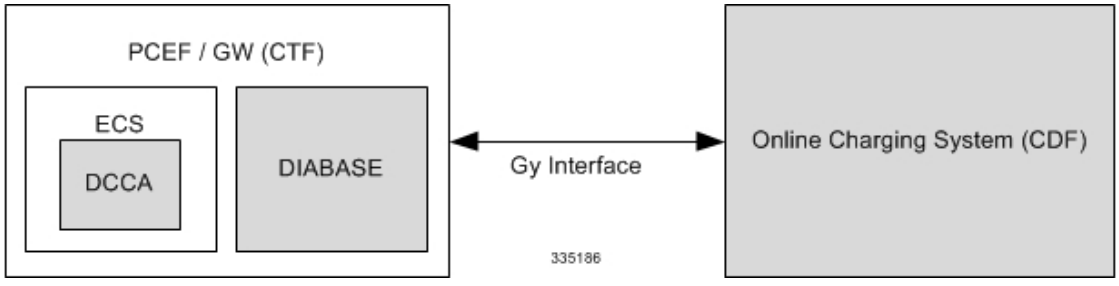
The following figure shows the Gy reference point in the policy and charging architecture.

Figure 1: PCC Logical Architecture



The following figure shows the Gy interface between CTF/Gateway/PCEF/Client running ECS and OCS (CDF/Server). Within the PCEF/GW, the Gy protocol functionality is handled in the DCCA module (at the ECS).

Figure 2: Gy Architecture



License Requirements

The Gy interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on

installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Supported Standards

Gy interface support is based on the following standards:

- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 9)

Features and Terminology

This section describes features and terminology pertaining to Gy functionality.

Charging Scenarios

Important Online charging for events ("Immediate Event Charging" and "Event Charging with Reservation") is not supported. Only "Session Charging with Reservation" is supported.

Session Charging with Reservation

Session Charging with Unit Reservation is used for credit control of sessions.

Decentralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the reservation of units prior to session supervision. An account debit operation is carried out following the conclusion of session termination.

Centralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the OCS to reserve units based on the session identifiers specified by the CTF. An account debit operation is carried out following the conclusion of session.

Decentralized Unit Determination and Decentralized Rating

Important Decentralized Rating is not supported in this release. Decentralized Unit determination is done using CLI configuration.

In this scenario, the CTF requests the OCS to assure the reservation of an amount of the specified number of monetary units from the subscriber's account. An account debit operation that triggers the deduction of the amount from the subscriber's account is carried out following the conclusion of session establishment.

Basic Operations

Important Immediate Event Charging is not supported in this release. "Reserve Units Request" and "Reserve Units Response" are done for Session Charging and not for Event Charging.

Online credit control uses the basic logical operations "Debit Units" and "Reserve Units".

- Debit Units Request; sent from CTF to OCS: After receiving a service request from the subscriber, the CTF sends a Debit Units Request to the OCS. The CTF may either specify a service identifier (centralised unit determination) or the number of units requested (decentralised unit determination). For refund purpose, the CTF sends a Debit Units Request to the OCS as well.
- Debit Units Response; sent from OCS to CTF: The OCS replies with a Debit Units Response, which informs the CTF of the number of units granted as a result of the Debit Units Request. This includes the case where the number of units granted indicates the permission to render the requested service. For refund purpose, the OCS replies with a Debit Units Response.
- Reserve Units Request; sent from CTF to OCS: Request to reserve a number of units for the service to be provided by an CTF. In case of centralised unit determination, the CTF specifies a service identifier in the Reserve Unit Request, and the OCS determines the number of units requested. In case of decentralised unit determination, the number of units requested is specified by the CTF.
- Reserve Units Response; sent from OCS to CTF: Response from the OCS which informs the CTF of the number of units that were reserved as a result of the "Reserve Units Request".

Session Charging with Unit Reservation (SCUR) use both the "Debit Units" and "Reserve Units" operations. SCUR uses the Session Based Credit Control procedure specified in RFC 4006. In session charging with unit reservation, when the "Debit Units" and "Reserve Units" operations are both needed, they are combined in one message.

Important Cost-Information, Remaining-Balance, and Low-Balance-Indication AVPs are not supported.

The consumed units are deducted from the subscriber's account after service delivery. Thus, the reserved and consumed units are not necessarily the same. Using this operation, it is also possible for the CTF to modify the current reservation, including the return of previously reserved units.

Re-authorization

The server may specify an idle timeout associated with a granted quota. Alternatively, the client may have a configurable default value. The expiry of that timer triggers a re-authorization request.

Mid-session service events (re-authorisation triggers) may affect the rating of the current service usage. The server may instruct the credit control client to re-authorize the quota upon a number of different session related triggers that can affect the rating conditions.

When a re-authorization is trigger, the client reports quota usage. The reason for the quota being reported is notified to the server.

Threshold based Re-authorization Triggers

The server may optionally include an indication to the client of the remaining quota threshold that triggers a quota re-authorization.

Termination Action

The server may specify to the client the behavior on consumption of the final granted units; this is known as termination action.

Diameter Base Protocol

The Diameter Base Protocol maintains the underlying connection between the Diameter Client and the Diameter Server. The connection between the client and server is TCP based. There are a series of message exchanges to check the status of the connection and the capabilities.

- Capabilities Exchange Messages: Capabilities Exchange Messages are exchanged between the diameter peers to know the capabilities of each other and identity of each other.
  - Capabilities Exchange Request (CER): This message is sent from the client to the server to know the capabilities of the server.
  - Capabilities Exchange Answer (CEA): This message is sent from the server to the client in response to the CER message.

Important Acct-Application-Id is not parsed and if sent will be ignored by the PCEF/GW. In case the Result-Code is not DIAMETER_SUCCESS, the connection to the peer is closed.

- Device Watchdog Request (DWR): After the CER/CEA messages are exchanged, if there is no more traffic between peers for a while, to monitor the health of the connection, DWR message is sent from the client. The Device Watchdog timer (Tw) is configurable in PCEF/GW and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is taken to be down.

Important DWR is sent only after Tw expiry after the last message that came from the server. Say if there is continuous exchange of messages between the peers, DWR might not be sent if (Current Time - Last message received time from server) is less than Tw.

- Device Watchdog Answer (DWA): This is the response to the DWR message from the server. This is used to monitor the connection state.
- Disconnect Peer Request (DPR): This message is sent to the peer to inform to shutdown the connection. PCEF/GW only receives this message. There is no capability currently to send the message to the diameter server.

- Disconnect Peer Answer (DPA): This message is the response to the DPR request from the peer. On receiving the DPR, the peer sends DPA and puts the connection state to "DO NOT WANT TO TALK TO YOU" state and there is no way to get the connection back except for reconfiguring the peer again.

  A timeout value for retrying the disconnected peer must be provided.

- Tw Timer Expiry Behavior: The connection between the client and the server is taken care by the DIABASE application. When two consecutive Tw timers are expired, the peer state is set to idle and the connection is retried to be established. All the active sessions on the connection are then transferred to the secondary connection if one is configured. All new session activations are also tried on the secondary connection.

  There is a connection timeout interval, which is also equivalent to Tw timer, wherein after a CER has been sent to the server, if there is no response received while trying to reestablish connection, the connection is closed and the state set to idle.

Diameter Credit Control Application

The Diameter Credit Control Application (DCCA) is a part of the ECS subsystem. For every prepaid customer with Diameter Credit Control enabled, whenever a session comes up, the Diameter server is contacted and quota for the subscriber is fetched.

Quota Behavior

Various forms of quotas are present that can be used to charge the subscriber in an efficient way. Various quota mechanisms provide the end user with a variety of options to choose from and better handling of quotas for the service provider.

Time Quotas

The Credit-Control server can send the CC-Time quota for the subscriber during any of the interrogation of client with it. There are also various mechanisms as discussed below which can be used in conjunction with time quota to derive variety of methods for customer satisfaction.

- Quota Consumption Time: The server can optionally indicate to the client that the quota consumption must be stopped after a period equal to the "Quota Consumption Time" in which no packets are received or at session termination, whichever is sooner. The idle period equal to the Quota Consumption Time is included in the reported usage. The quota is consumed normally during gaps in traffic of duration less than or equal to the Quota-Consumption-Time. Quota consumption resumes on receipt of a further packet belonging to the service data flow.

  If packets are allowed to flow during a CCR (Update)/CCA exchange, and the Quota-Consumption-Time AVP value in the provided quota is the same as in the previously provided quota, then the Quota-Consumption-Time runs normally through this procedure. For example, if 5 seconds of a 10 second QCT timer have passed when a CCR(U) is triggered, and the CCA(U) returns 2 seconds later, then the QCT timer will expire 3 seconds after the receipt of the CCA and the remaining unaccounted 5 seconds of usage will be recorded against the new quota even though no packets were transmitted with the new quota.

  A locally configurable default value in the client can be used if the server does not send the QCT in the CCA.

- Combinational Quota: Discrete-Time-Period (DTP) and Continuous-Time-Period (CTP) defines mechanisms that extends and generalize the Quota-Consumption-Time for consuming time-quota.

- Both DTP and CTP uses a "base-time-interval" that is used to create time-envelopes of quota used.
- Instead of consuming the quota linearly, DTP and CTP consumes the granted quota discretely in chunks of base-time-interval at the start of the each base-time-interval.
- Selection of one of this algorithm is based on the "Time-Quota-Mechanism" AVP sent by the server in CCA.
- Reporting usage can also be controlled by Envelope-Reporting AVP sent by the server in CCA during the quota grant. Based on the value of this AVP, the usage can be reported either as the usage per envelope or as usual cumulative usage for that grant.

- Discrete-Time-Period: The base-time-interval defines the length of the Discrete-Time-Period. So each time-envelope corresponds to exactly one Discrete-Time-Period. So when a traffic is detected, an envelope of size equal to Base-Time-Interval is created. The traffic is allowed to pass through the time-envelope. Once the traffic exceeds the base-time-interval another new envelope equal to the base-time-interval is created. This continues till the quota used exceeds the quota grant or reaches the threshold limit for that quota.
- Continuous-Time-Period: Continuous time period mechanism constructs time envelope out of consecutive base-time intervals in which the traffic occurred up to and including a base time interval which contains no traffic. Therefore the quota consumption continues within the time envelope, if there was traffic in the previous base time interval. After an envelope has closed, then the quota consumption resumes only on the first traffic following the closure of the envelope. The envelope for CTP includes the last base time interval which contains no traffic.

  The size of the envelope is not constant as it was in Parking meter. The end of the envelope can only be determined retrospectively.
- Quota Hold Time: The server can specify an idle timeout associated with a granted quota using the Quota-Holding-Time AVP. If no traffic associated with the quota is observed for this time, the client understands that the traffic has stopped and the quota is returned to the server. The client starts the quota holding timer when quota consumption ceases. This is always when traffic ceases, i.e. the timer is re-started at the end of each packet. It applies equally to the granted time quota and to the granted volume quota. The timer is stopped on sending a CCR and re-initialized on receiving a CCA with the previous used value or a new value of Quota-Holding-Time if received.

  Alternatively, if this AVP is not present, a locally configurable default value in the client is used. A Quota-Holding-Time value of zero indicates that this mechanism is not used.
- Quota Validity Time: The server can optionally send the validity time for the quota during the interrogation with the client. The Validity-Time AVP is present at the MSCC level and applies equally to the entire quota that is present in that category. The quota gets invalidated at the end of the validity time and a CCR-Update is sent to the server with the Used-Service-Units AVP and the reporting reason as VALIDITY_TIME. The entire quota present in that category will be invalidated upon Quota-Validity-Time expiry and traffic in that category will be passed or dropped depending on the configuration, till a CCA-Update is received with quota for that category.

  Validity-Time of zero is invalid. Validity-Time is relative and not absolute.

  In releases prior to 17.0, the AVP "SN-Remaining-Service-Unit" was not sent in the CCR-T and CCR-U messages with reporting Reason FINAL when the FUI action was received as Redirect and the granted units was zero in CCA. In 17.0 and later releases, for the Final-Reporting, the AVP "SN-Remaining-Service-Unit" will be encoded.

The "SN-Remaining-Service-Unit" AVP behavior is inherited from "Used-Service-Unit" AVP. This Final-Reporting is missing for the Remaining-Service-Unit AVP, which is now incorporated.

Volume Quota

The server sends the CC-Total-Octets AVP to provide volume quota to the subscriber. DCCA currently supports only CC-Total-Octets AVP, which applies equally to uplink and downlink packets. If the total of uplink and downlink packets exceeds the CC-Total-Octets granted, the quota is assumed to be exhausted.

If CC-Input-Octets and/or CC-Output-Octets is provided, the quota is counted against CC-Input-Octets and/or CC-Output-Octets respectively.

Important Restricting usages based on CC-Input-Octets and CC-Output-Octets is not supported in this release.

Units Quota

The server can also send a CC-Service-Specific-Units quota which is used to have packets counted as units. The number of units per packet is a configurable option.

Granting Quota

Gy implementation assumes that whenever the CC-Total-Octets AVP is present, volume quota has been granted for both uplink and downlink.

If the Granted-Service-Unit contains no data, Gy treats it as an invalid CCA.

If the values are zero, it is assumed that no quota was granted.

If the AVP contains the sub AVPs without any data, it is assumed to be infinite quota.

Additional parameters relating to a category like QHT, QCT is set for the category after receiving a valid volume or time grant.

If a default quota is configured for the subscriber, and subscriber traffic is received it is counted against the default quota. The default quota is applicable only to the initial request and is not regranted during the course of the session. If subscriber disconnects and reconnects, the default quota will be applied again for the initial request.

Requesting Quota

Quotas for a particular category type can be requested using the Requested-Service-Unit AVP in the CCR. The MSCC is filled with the Rating-Group AVP which corresponds to the category of the traffic and Requested-Service-Unit (RSU) AVP without any data.

The Requested-Service-Unit can contain the CC AVPs used for requesting specific quantity of time or volume grant. Gy CLI can be used to request quota for a category type.

Alternatively quota can also be requested from the server preemptively for a particular category in CCR- I. When the server grants preemptive quota through the Credit control answer response, the quota will be used only when traffic is hit for that category. Quota can be preemptively requested from the Credit Control server from the CLI.

In 12.3 and earlier releases, when no pre-emptive quota request is present in CCR-I, on hitting server unreachable state for initial request, MSCC AVP with RSU is present in the CCR-I on server retries. Release

14.0 onwards, the MSCC AVP is skipped in the CCR-I on server retries. Corresponding quota usage will be reported in the next CCR-U (MSCC AVP with USU and RSU).

Reporting Quota

Quotas are reported to the server for number of reasons including:

- Threshold
- QHT Expiry
- Quota Exhaustion
- Rating Condition Change
- Forced Reauthorization
- Validity Time Expiry
- Final during Termination of Category Instance from Server

For the above cases except for QHT and Final, the Requested-Service-Unit AVP is present in the CCR.

Reporting Reason is present in CCR to let the server know the reason for the reporting of Quota. The Reporting-Reason AVP can be present either in MSCC level or at Used Service Unit (USU) level depending on whether the reason applies to all quotas or to single quota.

When one of these conditions is met, a CCR Update is sent to the server containing a Multiple-Services-Credit-Control AVP(s) indicating the reason for reporting usage in the Reporting-Reason and the appropriate value(s) for Trigger, where appropriate. Where a threshold was reached, the DCCA still has the amount of quota available to it defined by the threshold.

For all other reporting reasons the client discards any remaining quota and either discards future user traffic matching this category or allows user traffic to pass, or buffers traffic according to configuration.

For Reporting-Reason of Rating Condition Change, Gy requires the Trigger Type AVP to be present as part of the CCR to indicate which trigger event caused the reporting and re-authorization request.

For Reporting-Reason of end user service denied, this happens when a category is blacklisted by the credit control server, in this case a CCR-U is sent with used service unit even if the values as zero. When more quota is received from the server for that particular category, the blacklisting is removed.

If a default quota has been set for the subscriber then the usage from the default quota is deducted from the initial GSU received for the subscriber for the Rating Group or Rating Group and Service ID combination.

Default Quota Handling

- If default quota is set to 0, no data is passed/reported.
- If default quota is configured and default quota is not exhausted before OCS responds with quota, traffic is passed. Initial default quota used is counted against initial quota allocated. If quota allocated is less than the actual usage then actual usage is reported and additional quota is requested. If no additional quota is available then traffic is denied.
- If default quota is not exhausted before OCS responds with denial of quota, gateway blocks traffic after OCS response. Gateway will report usage on default quota even in this case in CCR-U (FINAL) or CCR-T.
- If default quota is consumed before OCS responds, if OCS is not declared dead (see definition in use case 1 above) then traffic is blocked until OCS responds.

Thresholds

The Gy client supports the following threshold types:

- Volume-Quota-Threshold
- Time-Quota-Threshold
- Units-Quota-Threshold

A threshold is always associated with a particular quota and a particular quota type. in the Multiple-Services-Credit-Control AVP, the Time-Quota-Threshold, Volume-Quota-Threshold, and Unit-Quota-Threshold are optional AVPs.

They are expressed as unsigned numbers and the units are seconds for time quota, octets for volume quota and units for service specific quota. Once the quota has reached its threshold, a request for more quotas is triggered toward the server. User traffic is still allowed to flow. There is no disruption of traffic as the user still has valid quota.

The Gy sends a CCR-U with a Multiple-Services-Credit-Control AVP containing usage reported in one or more User-Service-Unit AVPs, the Reporting-Reason set to THRESHOLD and the Requested-Service-Unit AVP without data.

When quota of more than one type has been assigned to a category, each with its own threshold, then the threshold is considered to be reached once one of the unit types has reached its threshold even if the other unit type has not been consumed.

When reporting volume quota, the DCCA always reports uplink and downlink separately using the CC-Input-Octets AVP and the CC-Output-Octets AVP, respectively.

On receipt of more quotas in the CCA the Gy discard any quota not yet consumed since sending the CCR. Thus the amount of quota now available for consumption is the new amount received less any quota that may have been consumed since last sending the CCR.

Conditions for Reauthorization of Quota

Quota is re-authorized/requested from the server in case of the following scenarios:

- Threshold is hit
- Quota is exhausted
- Validity time expiry
- Rating condition change:
    - Cellid change: Applicable only to GGSN and P-GW implementations.
    - LAC change: Applicable only to GGSN and P-GW implementations.
    - QoS change
    - RAT change
    - SGSN/Serving-Node change: Applicable only to GGSN and P-GW implementations.

Discarding or Allowing or Buffering Traffic to Flow

Whenever Gy is waiting for CCA from the server, there is a possibility of traffic for that particular traffic type to be encountered in the Gy. The behavior of what needs to be done to the packet is determined by the

configuration. Based on the configuration, the traffic is either allowed to pass or discarded or buffered while waiting for CCA from the server.

This behavior applies to all interrogation of client with server in the following cases:

- No quota present for that particular category
- Validity timer expiry for that category
- Quota exhausted for that category
- Forced Reauthorization from the server

In addition to allowing or discarding user traffic, there is an option available in case of quota exhausted or no quota circumstances to buffer the traffic. This typically happens when the server has been requested for more quota, but a valid quota response has not been received from the server, in this case the user traffic is buffered and on reception of valid quota response from the server the buffered traffic is allowed to pass through.

Procedures for Consumption of Time Quota

- QCT is zero: When QCT is deactivated, the consumption is on a wall-clock basis. The consumption is continuous even if there is no packet flow.
- QCT is active: When QCT is present in the CCA or locally configured for the session, then the consumption of quota is started only at the time of first packet arrival. The quota is consumed normally till last packet arrival plus QCT time and is passed till the next packet arrival.

  If the QCT value is changed during intermediate interrogations, then the new QCT comes into effect from the time the CCA is received. For instance, if the QCT is deactivated in the CCA, then quota consumptions resume normally even without any packet flow. Or if the QCT is activated from deactivation, then the quota consumption resume only after receiving the first packet after CCA.
- QHT is zero: When QHT is deactivated, the user holds the quota indefinitely in case there is no further usage (for volume quota and with QCT for time quota). QHT is active between the CCA and the next CCR.
- QHT is non-zero: When QHT is present in CCA or locally configured for the session, then after a idle time of QHT, the quota is returned to the server by sending a CCR-Update and reporting usage of the quota. On receipt of CCR-U, the server does not grant quota. QHT timer is stopped on sending the CCR and is restarted only if QHT is present in the CCA.

  QHT timer is reset every time a packet arrives.

Envelope Reporting

The server may determine the need for additional detailed reports identifying start time and end times of specific activity in addition to the standard quota management. The server controls this by sending a CCA with Envelope-Reporting AVP with the appropriate values. The DCCA client, on receiving the command, will monitor for traffic for a period of time controlled by the Quota-Consumption-Time AVP and report each period as a single envelope for each Quota-Consumption-Time expiry where there was traffic. The server may request envelope reports for just time or time and volume. Reporting the quota back to the server, is controlled by Envelope AVP with Envelope-Start-Time and Envelope-End-Time along with usage information.

Credit Control Request

Credit Control Request (CCR) is the message that is sent from the client to the server to request quota and authorization. CCR is sent before the establishment of MIP session, and at the termination of the MIP session. It can be sent during service delivery to request more quotas.

- Credit Control Request - Initial (CCR-I)
- Credit Control Request - Update (CCR-U)
- Credit Control Request - Terminate (CCR-T)
- Credit Control Answer (CCA)
- Credit Control Answer - Initial (CCA-I)
- Credit Control Answer - Update (CCA-U)

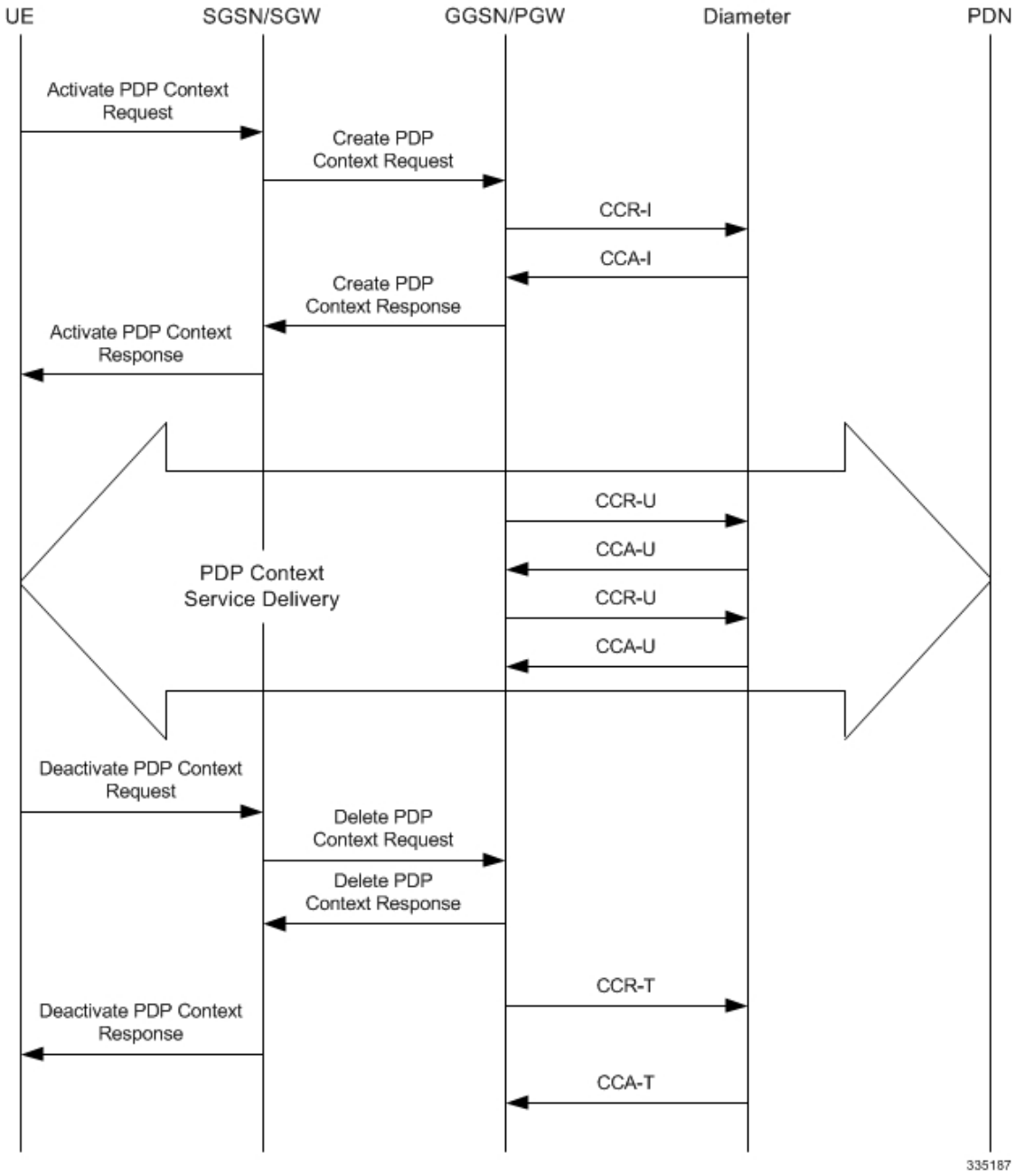
  If the MSCC AVP is missing in CCA-U it is treated as invalid CCA and the session is terminated.
- Credit Control Answer - Terminate (CCA-T)

In releases prior to 16.0, CCR-T was immediately sent without waiting for CCA-U if the call was cleared and there was a pending CCA-U. In 16.0 and later releases, if call is cleared when there is a pending update, the gateway will wait for CCA-U to arrive or timeout to happen (whichever happens first).

In releases prior to 20, CCR-Ts were not reported over Gy interface when the calls were terminated due to audit failure during ICSR switchover. In 20 and later releases, DCCA allows generation of CCR-Ts in this scenario.

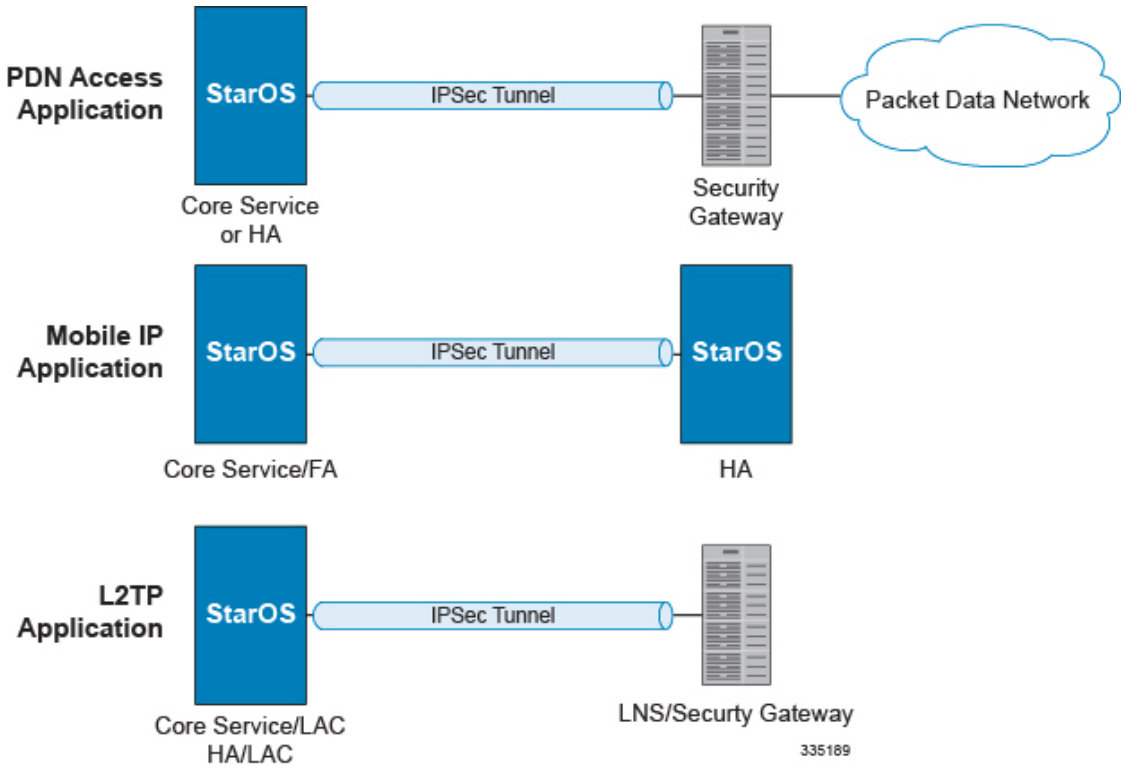
The following figure depicts the call flow for a simple call request in the GGSN/P-GW/IPSG Gy implementation.

Figure 3: Gy Call Flow for Simple Call Request for GGSN/P-GW/IPSG



The following figure depicts the call flow for a simple call request in the HA Gy implementation.

Figure 4: Gy Call Flow for Simple Call Request for HA



Tx Timer Expiry Behavior

A timer is started each time a CCR is sent out from the system, and the response has to arrive within Tx time. The timeout value is configurable in the Diameter Credit Control Configuration mode.

In case there is no response from the Diameter server for a particular CCR, within Tx time period, and if there is an alternate server configured, the CCR is sent to the alternate server after Tw expiry as described in "Tw Timer expiry behavior" section.

It also depends on the Credit-Control-Session-Failover AVP value for the earlier requests. If this AVP is present and is coded to FAILOVER_SUPPORTED then the credit-control message stream is moved to the secondary server, in case it is configured. If the AVP value is FAILOVER_NOT SUPPORTED, then the call is dropped in case of failures, even if a secondary server is configured.

In releases prior to 16.0, once a CCR-U was sent out over Gy interface, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U. In 16.0 and later releases, containers are closed only after CCA-U is received successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

Redirection

In the Final-Unit-Indication AVP, if the Final-Unit-Action is REDIRECT or Redirect-Server AVP is present at command level, redirection is performed.

The redirection takes place at the end of consumption of quota of the specified category. The Gy sends a CCR-Update without any RSU or Rating-Group AVP so that the server does not give any more quotas.

If the Final-Unit-Action AVP is RESTRICT_ACCESS, then according to the settings in Restriction-Filter-Rule AVP or Filter-Id AVP. Gy sends CCR-Update to the server with used quota.

Triggers

The Diameter server can provide with the triggers for which the client should reauthorize a particular category. The triggers can be configured locally as well but whatever trigger is present in the CCA from the server will have precedence.

Important In this release, Gy triggers are not supported for HA.

The trigger types that are supported are:

- SGSN/Serving-Node Change
- QoS Change - Any
- RAT Change
- LAC Change
- CellID Change

On any event as described in the Trigger type happens, the client reauthorizes quota with the server. The reporting reason is set as RATING_CONDITION_CHANGE.

Tariff Time Change

The tariff change mechanism applies to each category instance active at the time of the tariff change whenever the server indicated it should apply for this category.

The concept of dual coupon is supported. Here the server grants two quotas, which is accompanied by a Tariff-Time-Change, in this case the first granted service unit is used until the tariff change time, once the tariff change time is reached the usage is reported up to the point and any additional usage is not accumulated, and then the second granted service unit is used.

If the server expects a tariff change to occur within the validity time of the quota it is granting, then it includes the Tariff-Time-Change AVP in the CCA. The DCCA report usage, which straddles the change time by sending two instances of the Used-Service-Unit AVP, one with Tariff-Change-Usage set to UNIT_BEFORE_TARIFF_CHANGE, and one with Tariff-Change-Usage set to UNIT_AFTER_TARIFF_CHANGE, and this independently of the type of units used by application. Both Volume and Time quota are reported in this way.

The Tariff time change functionality can as well be done using Validity-Time AVP, where in the Validity-Time is set to Tariff Time change and the client will reauthorize and get quota at Validity-Time expiry. This will trigger a lot of reauthorize request to the server at a particular time and hence is not advised.

Tariff-Time-Usage AVP along with the Tariff-Time-Change AVP in the answer message to the client indicates that the quotas defined in Multiple-Services-Credit-Control are to be used before or after the Tariff Time change. Two separate quotas are allocated one for before Tariff-Time-Change and one for after Tariff-Time-Change. This gives the flexibility to the operators to allocate different quotas to the users for different periods of time. In this case, the DCCA should not send the Before-Usage and After-Usage counts in the update messages to the server. When Tariff-Time-Change AVP is present without Tariff-Time-Usage AVP in the answer message, then the quota is used as in single quota mechanism and the client has to send before usage and after usage quotas in the updates to the server.

Important In this release, Gy does not support UNIT_INDETERMINATE value.

In the StarOS 21.20.22 release, support for Tariff-Time-Change AVP is enhanced to maintain continuous traffic flow in the fast path and the user's traffic rate when the Tariff-Time-Change AVP is received from Gy for a Rating Group.

Final Unit Indication

The Final-Unit-Indication AVP can be present in the CCA from the server to indicate that the given quota is the final quota from the server and the corresponding action as specified in the AVP needs to be taken.

Final Unit Indication at Command Level

Gy currently does not support FUI AVP at command level. If this AVP is present at command level it is ignored. If the FUI AVP is present at command level and the Final-Unit-Action AVP set to TERMINATE, Gy sends a CCR-Terminate at the expiry of the quota, with all quotas in the USU AVP.

Important FUI AVP at command level is only supported for Terminate action.

Final Unit Indication at MSCC Level

If the Final-Unit-Indication AVP is present at MSCC level, and if the Final-Unit-Action AVP is set to TERMINATE, a CCR-Update is sent at the expiry of the allotted quota and report the usage of the category that is terminated.

For information on redirection cases refer to the Redirection, on page 14.

Credit Control Failure Handling

CCFH AVP defines what needs to be done in case of failure of any type between the client and the server. The CCFH functionality can be defined in configuration but if the CCFH AVP is present in the CCA, it takes precedence. CCFH AVP gives flexibility to have different failure handling.

Gy supports the following Failure Handling options:

- TERMINATE
- CONTINUE
- RETRY AND TERMINATE

CCFH with Failover Supported

In case there is a secondary server is configured and if the CC-Session-Failover AVP is set to FAILOVER_SUPPORTED, the following behavior takes place:

- Terminate: On any Tx expiry for the CCR-I the message is discarded and the session is torn down. In case of CCR-Updates and Terminates the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is torn down.
- Continue: On any Tx expiry, the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is still established, but without quota management.

- Retry and Terminate: On any Tx expiry, the message is sent to the secondary server after the response timeout. In case there is a failure with secondary server too, the session is taken down.

CCFH with Failover Not Supported

In case there is a secondary server configured and if the CC-Session-Failover AVP is set to FAILOVER_NOT_SUPPORTED, the following behavior takes place as listed below. Same is the case if there is no secondary server configured on the system.

- Terminate: On any Tx expiry, the session is taken down.
- Continue: On any Tx expiry, the session is still established, but without quota management.
- Retry and Terminate: On any Tx expiry, the session is taken down.

Failover Support

The CC-Session-Failover AVP and the Credit-Control-Failure-Handling (CCFH) AVP may be returned by the CC server in the CCA-I, and are used by the DCCA to manage the failover procedure. If they are present in the CCA they override the default values that are locally configured in the system.

If the CC-Session-Failover is set to FAILOVER_NOT_SUPPORTED, a CC session will never be moved to an alternative Diameter Server.

If the value of CC-Session-Failover is set to FAILOVER_SUPPORTED, then the Gy attempts to move the CC session to the alternative server when it considers a request to have failed, i.e:

- On receipt of result code "DIAMETER_UNABLE_TO_DELIVER", "DIAMETER_TOO_BUSY", or "DIAMETER_LOOP_DETECTED".
- On expiry of the request timeout.
- On expiry of Tw without receipt of DWA, if the server is connected directly to the client.

The CCFH determines the behavior of the client in fault situations. If the Tx timer expires then based on the CCFH value the following actions are taken:

- CONTINUE: Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). Note that quota management of other categories is not affected.
- TERMINATE: Terminate the MIP session, which affects all categories.
- RETRY_AND_TERMINATE: Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). The client retries to send the CCR when it determines a failure-to-send condition and if this also fails, the MIP session is then terminated.

After the failover action has been attempted, and if there is still a failure to send or temporary error, depending on the CCFH action, the following action is taken:

- CONTINUE: Allow the MIP session to continue.
- TERMINATE: Terminate the MIP session.
- RETRY_AND_TERMINATE: Terminate the MIP session.

Recovery Mechanisms

DCCA supports a recovery mechanism that is used to recover sessions without much loss of data in case of Session Manager failures. There is a constant check pointing of Gy data at regular intervals and at important events like update, etc.

Important The DCCA supports maximum of three bearers (including default) for the ICSR Checkpointing and Recovery. When more than three bearers are configured in the DCCA, checkpointing occurs from Active to Standby for all the bearers. However, during recovery, only the first three bearers are recovered and the rest remain in the memory consuming resources.

For more information on recovery mechanisms, please refer to the *System Administration Guide*.

Error Mechanisms

Following are supported Error Mechanisms.

Unsupported AVPs

All unsupported AVPs from the server with "M" bit set are ignored.

Invalid Answer from Server

If there is an invalid answer from the server, Gy action is dependent on the CCFH setting:

- In case of continue, the MIP session context is continued without further control from Gy.
- In case of terminate and retry-and-terminate, the MIP session is terminated and a CCR-T is sent to the diameter server.

Result Code Behavior

- DIAMETER_RATING_FAILED: On reception of this code, Gy discards all traffic for that category and does not request any more quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER_END_USER_SERVICE_DENIED: On reception of this code, Gy temporarily blacklists the category and further traffic results in requesting new quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER_CREDIT_LIMIT_REACHED: On reception of this code, Gy discards all traffic for that category and waits for a configured time, after which if there is traffic for the same category requests quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE: On reception of this code, Gy allows the session to establish, but without quota management. This is supported only at the command level and not at the MSCC level.
- DIAMETER_USER_UNKNOWN: On reception of this code, DCCA does not allow the credit control session to get established, the session is terminated. This result code is supported only at the command level and not at the MSCC level.

For all other permanent/transient failures, Gy action is dependent on the CCFH setting.

Supported AVPs

The Gy functionality supports the following AVPs:

- Supported Diameter Credit Control AVPs specified in RFC 4006:
  - CC-Input-Octets (AVP Code: 412):

    Gy supports this AVP only in USU.
  - CC-Output-Octets (AVP Code: 414):

    Gy supports this AVP only in USU.
  - CC-Request-Number (AVP Code: 415)
  - CC-Request-Type (AVP Code: 416):

    Gy currently does not support EVENT_REQUEST value.
  - CC-Service-Specific-Units (AVP Code: 417)
  - CC-Session-Failover (AVP Code: 418)
  - CC-Time (AVP Code: 420):

    Gy does not support this AVP in RSU.
  - CC-Total-Octets (AVP Code: 421):

    Gy does not support this AVP in RSU.
  - Credit-Control-Failure-Handling (AVP Code: 427)
  - Final-Unit-Action (AVP Code: 449):

    Supported at Multiple-Services-Credit-Control grouped AVP level and not at command level.
  - Final-Unit-Indication (AVP Code: 430):

    Fully supported at Multiple-Services-Credit-Control grouped AVP level and partially supported (TERMINATE) at command level.
  - Granted-Service-Unit (AVP Code: 431)
  - Multiple-Services-Credit-Control (AVP Code: 456)
  - Multiple-Services-Indicator (AVP Code: 455)
  - Rating-Group (AVP Code: 432)
  - Redirect-Address-Type (AVP Code: 433):

    Gy currently supports only URL (2) value.
  - Redirect-Server (AVP Code: 434)
  - Redirect-Server-Address (AVP Code: 435)
  - Requested-Service-Unit (AVP Code: 437)
  - Result-Code (AVP Code: 268)
  - Service-Context-Id (AVP Code: 461)

- Service-Identifier (AVP Code: 439)
- Subscription-Id (AVP Code: 443)
- Subscription-Id-Data (AVP Code: 444)
- Subscription-Id-Type (AVP Code: 450)
- Tariff-Change-Usage (AVP Code: 452):

  Gy does NOT support UNIT_INDETERMINATE (2) value.
- Tariff-Time-Change (AVP Code: 451)
- Used-Service-Unit (AVP Code: 446):

  Gy sends only incremental counts for all the AVPs from the last CCA-U.
- User-Equipment-Info (AVP Code: 458)
- User-Equipment-Info-Type (AVP Code: 459):

  Gy currently supports only IMEISV value.

  Cisco GGSN and P-GW support IMEISV by default.
- User-Equipment-Info-Value (AVP Code: 460)
- Validity-Time (AVP Code: 448)

- Supported 3GPP specific AVPs specified in 3GPP TS 32.299:
  - 3GPP-Charging-Characteristics (AVP Code: 13)
  - 3GPP-Charging-Id (AVP Code: 2)
  - 3GPP-GGSN-MCC-MNC (AVP Code: 9)
  - 3GPP-GPRS-QoS-Negotiated-Profile (AVP Code: 5)
  - 3GPP-IMSI-MCC-MNC (AVP Code: 8)
  - 3GPP-NSAPI (AVP Code: 10)
  - 3GPP-PDP-Type (AVP Code: 3)
  - 3GPP-RAT-Type (AVP Code: 21)
  - 3GPP-Selection-Mode (AVP Code: 12)
  - 3GPP-Session-Stop-Indicator (AVP Code: 11)
  - 3GPP-SGSN-MCC-MNC (AVP Code: 18)
  - 3GPP-User-Location-Info (AVP Code: 22)
  - Base-Time-Interval (AVP Code: 1265)
  - Charging-Rule-Base-Name (AVP Code: 1004)
  - Envelope (AVP Code: 1266)
  - Envelope-End-Time (AVP Code: 1267)

- Envelope-Reporting (AVP Code: 1268)
- Envelope-Start-Time (AVP Code: 1269)
- GGSN-Address (AVP Code: 847)
- Offline-Charging (AVP Code: 1278)
- PDP-Address (AVP Code: 1227)
- PDP-Context-Type (AVP Code: 1247)

  This AVP is present only in CCR-I.
- PS-Information (AVP Code: 874)
- Quota-Consumption-Time (AVP Code: 881):

  This optional AVP is present only in CCA.
- Quota-Holding-Time (AVP Code: 871):

  This optional AVP is present only in the CCA command. It is contained in the Multiple-Services-Credit-Control AVP. It applies equally to the granted time quota and to the granted volume quota.
- Reporting-Reason (AVP Code: 872):

  Gy currently does not support the POOL_EXHAUSTED (8) value. It is used in case of credit-pooling which is currently not supported.
- Service-Information (AVP Code: 873):

  Only PS-Information is supported.
- SGSN-Address (AVP Code: 1228)
- Time-Quota-Mechanism (AVP Code: 1270):

  The Gy server may include this AVP in an Multiple-Services-Credit-Control AVP when granting time quota.
- Time-Quota-Threshold (AVP Code: 868)
- Time-Quota-Type (AVP Code: 1271)
- Trigger (AVP Code: 1264)
- Trigger-Type (AVP Code: 870)
- Unit-Quota-Threshold (AVP Code: 1226)
- Volume-Quota-Threshold (AVP Code: 869)

- Supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Auth-Application-Id (AVP Code: 258)
  - Destination-Host (AVP Code: 293)
  - Destination-Realm (AVP Code: 283)
  - Disconnect-Cause (AVP Code: 273)

- Error-Message (AVP Code: 281)
- Event-Timestamp (AVP Code: 55)
- Failed-AVP (AVP Code: 279)
- Multiple-Services-Credit-Control (AVP Code: 456)
- Origin-Host (AVP Code: 264)
- Origin-Realm (AVP Code: 296)
- Origin-State-Id (AVP Code: 278)
- Redirect-Host (AVP Code: 292)
- Redirect-Host-Usage (AVP Code: 261)
- Redirect-Max-Cache-Time (AVP Code: 262)
- Rating-Group (AVP Code: 432)
- Result-Code (AVP Code: 268)
- Route-Record (AVP Code: 282)
- Session-Id (AVP Code: 263)
- Service-Context-Id (AVP Code: 461)
- Service-Identifier (AVP Code: 439)
- Supported-Vendor-Id (AVP Code: 265)
- Termination-Cause (AVP Code: 295)
- Used-Service-Unit (AVP Code: 446)
- User-Name (AVP Code: 1)

Unsupported AVPs

This section lists the AVPs that are NOT supported.

- NOT Supported Credit Control AVPs specified in RFC 4006:
  - CC-Correlation-Id
  - CC-Money
  - CC-Sub-Session-Id
  - CC-Unit-Type (AVP Code: 454)
  - Check-Balance-Result
  - Cost-Information (AVP Code: 423)
  - Cost-Unit (AVP Code: 445)
  - Credit-Control

- Currency-Code (AVP Code: 425)
- Direct-Debiting-Failure-Handling (AVP Code: 428)
- Exponent (AVP Code: 429)
- G-S-U-Pool-Identifier (AVP Code: 453)
- G-S-U-Pool-Reference (AVP Code: 457)
- Requested-Action (AVP Code: 436)
- Service-Parameter-Info (AVP Code: 440)
- Service-Parameter-Type (AVP Code: 441)
- Service-Parameter-Value (AVP Code: 442)
- Unit-Value (AVP Code: 424)
- Value-Digits (AVP Code: 447)

- NOT supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Acct-Application-Id (AVP Code: 259)
  - Error-Reporting-Host (AVP Code: 294)
  - Experimental-Result (AVP Code: 297)
  - Experimental-Result-Code (AVP Code: 298)
  - Proxy-Host
  - Proxy-Info
  - Proxy-State

- NOT supported 3GPP-specific AVPs specified in 3GPP TS 32.299 V8.1.0:
  - 3GPP-CAMEL-Charging-Info (AVP Code: 24)
  - 3GPP-MS-TimeZone (AVP Code: 23)
  - 3GPP-PDSN-MCC-MNC
  - Authorised-QoS
  - Access-Network-Information
  - Adaptations
  - Additional-Content-Information
  - Additional-Type-Information
  - Address-Data
  - Address-Domain
  - Addressee-Type
  - Address-Type
  - AF-Correlation-Information
  - Alternate-Charged-Party-Address
  - Application-provided-Called-Party-Address
  - Application-Server

- Application-Server-Information
- Applic-ID
- Associated-URI
- Aux-Applic-Info
- Bearer-Service
- Called-Asserted-Identity
- Called-Party-Address
- Calling-Party-Address
- Cause-Code
- Charged-Party
- Class-Identifier
- Content-Class
- Content-Disposition
- Content-Length
- Content-Size
- Content-Type
- Data-Coding-Scheme
- Deferred-Location-Event-Type
- Delivery-Report-Requested
- Destination-Interface
- Domain-Name
- DRM-Content
- Early-Media-Description
- Event
- Event-Type
- Expires
- File-Repair-Supported
- IM-Information
- IMS-Charging-Identifier (ICID)
- IMS-Communication-Service-Identifier
- IMS-Information
- Incoming-Trunk-Group-ID
- Interface-Id
- Interface-Port
- Interface-Text
- Interface-Type
- Inter-Operator-Identifier
- LCS-APN
- LCS-Client-Dialed-By-MS
- LCS-Client-External-ID
- LCS-Client-ID
- LCS-Client-Name
- LCS-Client-Type
- LCS-Data-Coding-Scheme
- LCS-Format-Indicator
- LCS-Information

- LCS-Name-String
- LCS-Requestor-ID
- LCS-Requestor-ID-String
- Location-Estimate
- Location-Estimate-Type
- Location-Type
- Low-Balance-Indication
- MBMS-Information
- MBMS-User-Service-Type
- Media-Initiator-Flag
- Media-Initiator-Party
- Message-Body
- Message-Class
- Message-ID
- Message-Size
- Message-Type
- MMBox-Storage-Requested
- MM-Content-Type
- MMS-Information
- Node-Functionality
- Number-Of-Participants
- Number-Of-Received-Talk-Bursts
- Number-Of-Talk-Bursts
- Originating-IOI
- Originator
- Originator-Address
- Originator-Interface
- Originator-SCCP-Address
- Outgoing-Trunk-Group-ID
- Participant-Access-Priority
- Participants-Group
- Participants-Involved
- PDG-Address
- PDG-Charging-Id
- PoC-Change-Condition
- PoC-Change-Time
- PoC-Controlling-Address
- PoC-Group-Name
- PoC-Information
- PoC-Server-Role
- PoC-Session-Id
- PoC-Session-Initialtion-Type
- PoC-Session-Type
- PoC-User-Role
- PoC-User-Role-IDs
- PoC-User-Role-info-Units

- Positioning-Data
- Priority
- PS-Append-Free-Format-Data (AVP Code: 867):

  The PCEF/GW ignores this AVP if no PS free format data is stored for the online charging session.

- PS-Free-Format-Data (AVP Code: 866)
- PS-Furnish-Charging-Information (AVP Code: 865)
- RAI (AVP Code: 909)
- Read-Reply-Report-Requested
- Received-Talk-Burst-Time
- Received-Talk-Burst-Volume
- Recipient-Address
- Recipient-SCCP-Address
- Refund-Information
- Remaining-Balance
- Reply-Applic-ID
- Reply-Path-Requested
- Requested-Party-Address
- Role-of-node
- SDP-Answer-Timestamp
- SDP-Media-Component
- SDP-Media-Description
- SDP-Media-Name
- SDP-Offer-Timestamp
- SDP-Session-Description
- SDP-TimeStamp
- Served-Party-IP-Address
- Service-Generic-Information
- Service-ID
- Service-Specific-Data
- Service-Specific-Info
- Service-Specific-Type
- SIP-Method
- SIP-Request-Timestamp
- SIP-Response-Timestamp
- SM-Discharge-Time
- SM-Message-Type
- SM-Protocol-Id
- SMSC-Address
- SMS-Information
- SMS-Node
- SM-Status
- SM-User-Data-Header
- Submission-Time
- Talk-Burst-Exchange

- Talk-Burst-Time
- Talk-Burst-Volume
- Terminating-IOI
- Time-Stamps
- Token-Text
- Trunk-Group-ID
- Type-Number
- User-Participating-Type
- User-Session-ID
- WAG-Address
- WAG-PLMN-Id
- WLAN-Information
- WLAN-Radio-Container
- WLAN-Session-Id
- WLAN-Technology
- WLAN-UE-Local-IPAddress

PLMN and Time Zone Reporting

For some implementations of online charging, the OCS requires the PCEF to reporting location-specific subscriber information. For certain subscriber types, subscriber information such as PLMN, Time Zone, and ULI can be sent over the Gy interface as the subscriber changes location, time zone, and serving networks to provide accurate online charging services. Such information can be reported independently from time and volume-based reporting.

PLMN and Time Zone Reporting feature is enabled to support location event reporting based on triggers from Gx, when the following conditions are met:

- Session-based Gy is not initiated due to the absence of charging-actions in rulebase with Credit-Control enabled or due to delayed Gy session initiation.
- PLMN and Time Zone Reporting feature is either enabled in the credit control group or through the use of triggers received from Gx.

If session-based Gy initiation fails or the session goes offline due to configuration or network issues, event-based Gy session will not be initiated.

Important Note that the failure-handling will not be supported for event-based Gy.

Though, in event-based Gy, multiple events can be reported independently and simultaneously this is presently not supported. If an event occurs when the CCA-Event (CCA-E) of the previously reported event is awaited, then the new event is queued and reported only when a CCA-E is received or the message is timed out.

To enable the PLMN and Time Zone Reporting feature, the PCRF shall send the Trigger AVP (Trigger Type 1, Trigger Type 2) at the command level in a CCA.

The Event-based Gy session will be terminated in the following scenarios:

- On termination of the bearer/subscriber (subscriber level Gy).
- Initiation of session-based Gy session (delayed session initiation).

- Once the CCR-E transaction is complete and there are no further events to report.

For information on how to configure this feature, refer to the *Gy Interface Support* chapter in the administration guide for the product that uses the Gy interface functionality.

Interworking between Session-based Gy and Event-based Gy

If both session-based Gy and event-based Gy mode are activated, then session-based Gy will take precedence i.e. all the events will be reported through CCR-U if the corresponding triggers are enabled. Event-based Gy mode will be active only when session-based Gy has been disabled and has never been activated previously for this session during its lifetime.

OCS Unreachable Failure Handling Feature

The OCS Unreachable Failure Handling feature is required to handle when OCS goes down or unavailable. This feature is otherwise noted as Assume Positive for Gy.

The OCS is considered unavailable/unreachable in the following scenarios:

- PCEF transmits a CCR-U or CCR-I message but no response is received before the specified timeout
- Diameter Watchdog request times out to the current RDR, causing the TCP connection state to be marked down
- Diameter command-level error codes received in a CCA
- If the PCEF is unable to successfully verify transmission of a CCR-T, the PCEF will not assign interim quota, because the user has disconnected.

In 15.0 and later releases, the error result codes can be configured using the CLI command **servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [to end-result-code] } }** to trigger the server unreachable mode. The same is applicable for the update request also. For more information on the CLI command, see the *Credit Control Configuration Mode Commands* chapter of the *Command Line Interface Reference*. However, if the CLI command **no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error | result-code [to end-result-code] }** is configured, then the default set of hard-coded error codes are applicable.

The default set is:

- UNABLE_TO_DELIVER 3002
- UNABLE_TOO_BUSY 3004
- LOOP_DETECTED 3005
- ELECTION_LOST 4003
- Permanent failures 5001-5999 except 5002, 5003 and 5031.

In 12.2 and later releases, existing failure handling mechanism is enhanced such that the subscriber can be allowed to browse for a pre-configured amount of interim-volume and/or interim-time if OCS becomes unreachable due to transport connection failure or gives an impression that OCS is unreachable owing to slow response for Diameter request messages.

The purpose of this feature is to support Gy based data sessions in the event of an OCS outage. Diameter client allows the user's data session to continue for some fixed quota and then retries the OCS server to restore normal functionality. This feature adds more granularity to the existing failure handling mechanism.

With the implementation of this feature, Gy reporting during outages is supported. A temporary time and/or volume quota is assigned to the user in the event of an OCS outage which will be used during the outage period.

When the OCS returns to service, the GW reports all used quota back to OCS and continues with normal Gy reporting.

For each DCCA-service, CLI control is available for the following options:

- Interim quota volume (in bytes) and quota time (seconds). Both values will apply simultaneously, if configured together and if either quota time or quota volume is exhausted, the Diameter client retries the OCS.
- Option to limit the number of times a session can be assigned a temporary quota. If the user exceeds this amount, the session will be terminated/converted to postpaid.

The quota value is part of the dcca-service configuration, and will apply to all subscribers using that dcca-service. The temporary quota will be specified in volume (bytes) and/or time (seconds) to allow enforcement of both quota tracking mechanisms individually or simultaneously.

When a user consumes the interim total quota or time configured for use during failure handling scenarios, the GW retries the OCS server to determine if functionality has been restored. In the event that services have been restored, quota assignment and tracking will proceed as per standard usage reporting procedures. Data used during the outage will be reported to the OCS.

In the event that the OCS services have not been restored, the GW re-allocates the configured amount of quota and/or time to the user. The GW reports all accumulated used data back to OCS when OCS is back online. If multiple retries and interim allocations occur, the GW reports quota used during all allocation intervals. This cycle will continue until OCS services have been successfully restored, or the maximum number of quota assignments has been exhausted.

Support for OCS unreachable CLI commands is added under Diameter Credit Control Configuration mode.

For the P-GW/XGW/GGSN, this behavior will apply to all APNs and subscribers that have online charging enabled by the PCRF. In the HA, this behavior will apply to all users that have online charging enabled by the AAA. Settings will be applied to the dcca-service.

In Release 15.0, the following enhancements are implemented as part of the Assume Positive Gy feature:

- Configurable per error code treatment to enter assume positive mode
- Graceful session restart upon receipt of a 5002 error

Important Note that the Graceful session restart feature is customer specific. For more information contact your Cisco account representative.

Configurable per Error Code Treatment

This feature allows the customers to configure error result codes using the CLI command "**servers-unreachable behavior-triggers**" that will trigger entering assume positive mode on the fly for CCR-Initial and CCR-Update messages. CCR-Terminate message is currently not supported.

Any error result codes from the range 3xxx to 5xxx can be specified using the CLI commands. This feature has been implemented to provide more flexibility and granularity in the way assume positive mode is triggered for error result codes.

Graceful Session Restart

Graceful session restart upon receipt of a 5002 error code is supported for server retried CCR-U messages during assume positive state. Also, any unreported usage from the time, server retried CCR-U sent till CCA-I is received, will be reported immediately by triggering CCR-U with usages for the same.

Important Note that the Graceful session restart feature is customer specific. For more information contact your Cisco account representative.

Any pending updates are aborted once CCA-U with 5002 is received from the server. Also CCR-U is triggered immediately following session restart only if there are any unreported usages pending.

Important When the server responds with 5002 error result code, it does not include any granted service units for the requested rating groups.

For more information on the commands introduced in support of this feature, see the *Credit Control Configuration Mode Command* chapter in the *Command Line Interface Reference*.

Enhancement to OCS Failure Reporting for Gy

Feature Description

When Cisco-Event-Trigger-Type AVP is installed by PCRF in CCA-I, CCA-U or in RAR messages with value CREDIT_CONTROL_FAILURE (5), then the Cisco-Event grouped AVP is sent by the P-GW to PCRF in CCR-U message with the exact value of OCS failure code. This trigger is sent only when Gy failure occurs and based on the configuration (Credit-Control-Failure-Handling), the ‘Continue’ action is taken and Gy session moves to Offline state.

In releases prior to the implementation of this enhancement, if a failure code was received from OCS in the range of 3000-3999, then Cisco-CC-Failure-Type was sent with the value 3XXX. Similarly, for error codes in the range of 4000-4999 or 5000-5999, Cisco-CC-Failure-Type was reported as 4XXX or 5XXX respectively. With this enhancement, the exact failure code is reported to the PCRF instead of the range. For example, when the Cisco-Event-Trigger-Type is CREDIT_CONTROL_FAILURE (5) and OCS failure code is 3002 in CCA-U, then in CCR-U towards PCRF Cisco-CC-Failure-Type (as part of grouped AVP Cisco-Event) is sent with a value of 3002.

Backpressure Handling

Diameter base (Diabase) maintains an outbound stream. When an application wants to write a message into a socket, the message handle of those messages are stored in the outbound stream. Only on receiving the response to the corresponding request, the stored message handle is removed from the outbound stream. In order to rate-limit the message transactions based on the responses received from the server, ASR 5500 maintains a limit on the number of messages stored in the outbound stream. This is done using "max-outstanding <>" CLI (default value is 256). If the number of messages created by the application exceeds the max-outstanding limit, diabase sends a 'Backpressure' indication to the application to wait till it receives a decongestion indication from diabase to try again.

On receiving a response from the server, the corresponding request message handle will be removed from the outbound stream, creating a slot for another message to be written by the application. In order to intimate this

slot availability, decongestion notification is sent to the registered application. The application in turn loops through all sessions and processes the pending trigger to be sent.

When the application loops through the sessions in the system, it traverse the sessions in a sorted order and checks each session whether it has to send a pending CCR-Initial or CCR-Terminate or CCR-Update. When the first session gets the slot to fill the outbound stream, it writes the message into the stream. Now the slot gets back into filled state, reaching the max-outstanding limit again. So the rest of the sessions will still continue to be in backpressured state.

Backpressured request like Credit-Control-Initial and Credit-Control-Terminate are given higher priority over Credit-Control-Update as they are concerned with the creation or termination of a session. So on top of the decongestion notification, DCCA has some internal timers which periodically try to send the message out. So in case of heavy backpressure condition, the probability of CCR-I or CCR-T being sent out is more than CCR-U.

Gy Backpressure Enhancement

This feature facilitates maintaining a list of DCCA sessions that hit backpressure while creating a message i.e., backpressured list, eliminating the current polling procedure. This will maintain a single queue for all types of messages (CCR-I, CCR-U, CCR-T, CCR-E) that are backpressured. The messages will be sent in FIFO order from the queue.

After processing a session from the backpressure queue DCCA will check for the congestion status of the peer and continue only if the peer has empty slots in the outstanding message queue to accommodate further CCRs.

Releases prior to 16.0, the gateway has a max-outstanding configuration to manage a number of messages that are waiting for response from OCS. When the max-outstanding is configured to a low value, then the frequency to be in congested state is very high.

CPU utilization is very high if the max-outstanding count is low and network is congested.

In 16.0 and later releases, all DCCA sessions associated with the CCR messages that are triggered BACKPRESSURE (when max-outstanding has been reached) will be queued in backpressure list which is maintained per ACS manager instance (credit-control) level.

This list will not have any specific configurable limits on the number of sessions that will be queued in it. This is because there is an inherent limit that is already present which is dependent on the number of subscriber/DCCA sessions.

With this new separate backpressured list, CPU utilization will come down under high backpressure case.

Gy Support for GTP based S2a/S2b

For WiFi integration in P-GW, Gy support is provided for GTP based S2a/S2b in Release 18.0. This implementation is in compliance with standard Rel-11 non-3GPP access spec of 32.399: S5-120748 S5-131017 S5-143090.

As part of this enhancement, the following AVP changes are introduced:

- Added TWAN as a new enum value for Serving-Node-Type AVP
- Added a new Diameter AVP "TWAN-User-Location-Info". This is a grouped AVP and it contains the UE location in a Trusted WLAN Access Network (TWAN): BSSID and SSID of the access point.

The TWAN AVPs will be effective only for 3GPP release 11 and it is added only to the standard Gy dictionary. That is, the TWAN AVP will be included in CCR-I/CCR-U/CCR-T messages only when the CLI command "**diameter update-dictionary-avps 3gpp-rel11**" is configured.

Generating OOC/ROC with Changing Association between Rule and RG

The existing Gy implementation prevents duplicate Out-of-Credit (OOC) / Reallocation of Credit (ROC) report for the same rule to the PCRF. Subscriber throttling with the same rule with different Rating-Group across OOC event does not work. To overcome this, the following implementation is considered:

When a Rating-Group runs out of credit, OOC is sent to all rules that are currently associated with that Rating-Group. This is done irrespective of whether that rule was already OOC'd or not. Similarly, when a Rating-Group gets quota after being in OOC state, a ROC is sent to all rules that are currently associated with that Rating-Group. This is done irrespective of whether that rule was already ROC'd or not.

In releases prior to 18, MSCC's state was previously being maintained at MSCC and rule-level to suppress OOC/ROC events. So if MSCC triggered an OOC/ROC the same was suppressed by the status maintained at the rule-level if the previous event on the rule was the same.

In 18 and later releases, the rule level status bits are no longer used to avoid similar back-to-back OOC/ROC events. Now, the triggering of OOC/ROC events will solely be dependent on the MSCC state and triggers.

Customers might see an increase in OOC/ROC events on Gx if they change the association of the rule and RG or if they use the Override feature.

Static Rulebase for CCR

An APN/subscriber can have a single rulebase applied to it, but allowing a static rulebase configuration to always pass a different or same rulebase to the OCS through CCR messages.

A new CLI command "**charging-rulebase-name** *rulebase_name*" has been introduced under Credit Control (CC) group to override/change the rulebase name present in APN/subscriber template, in the CCR AVP "Charging-Rule-Base-Name". The rulebase value configured in CC group will be sent to OCS via CCR. If this CLI command is not configured, then the rulebase obtained from APN/subscriber template will be sent to OCS.

The configured value of rulebase under CC group is sent in all CCR (I/U/T) messages. This implies that any change in rulebase value in CC group during mid-session gets reflected in the next CCR message.

This feature, when activated with the CLI command, reduces the complication involved in configuration of services like adding and removing services per enterprise on the OCS system.

CC based Selective Gy Session Control

This section describes the overview and implementation of the Selective Gy Session Control feature based on Charging Characteristics (CC) profile of the subscriber.

This section discusses the following topics for this feature:

Feature Description

The functionality that allows users to configure certain Charging Characteristics (CC) values as prepaid/postpaid is available for GGSN service. In Release 17, this functionality is extended to P-GW service.

To enable/disable Gy session based on the CC value received, the APN configuration is extended so that additional credit-control-groups/prepaid prohibited value can be configured for each of the CC values.

The **cc profile** *cc-profile-index* **prepaid prohibited** CLI command is used to configure the CC values to disable Credit-Control based charging. The P-GW/GGSN/SAEGW service subscriber sessions using this APN, can use this configuration to stop the triggering of Gy messages towards the OCS.

The UE provides the charging characteristics value and the active subscriber is connected through an APN. The CC index mapping is done for a corresponding CC group/prepaid prohibited value configured under the APN. Depending on the match, the Gy session is enabled or disabled towards the OCS.

The Session controller stores/updates the APN configuration in the AAA manager. During the session setup, the session manager fills the CC value received in session authenticate request, and sends it to AAA manager. The AAA manager matches this against the locally stored APN configuration, and selects the desired credit-control-group/prepaid-prohibited configuration for the session. Then the session manager passes this credit-control-group/prepaid-prohibited information received from the AAA manager to ACS manager.

When the local authentication (session setup request) is done, the credit-control group with the matching charging characteristic is selected and used. If there is no matching charging characteristic configuration found for the credit-control group selection, then the default credit-control group for the APN is selected.

When a particular CC is configured as postpaid, any session with this CC does not trigger Gy connection. Any change in the CC during the lifetime of session is ignored.

The CC based Gy Session Controlling feature is applicable only for the CC value received via GTP-Auth-Request, and during the session establishment. The CC value updated via AAA/PCRF after the session setup will not cause any change in already selected credit-control group. Once the credit-control group is selected after session setup, this feature is not applicable.

Diamter Error Code and Counters

SaMOG supports Diameter error code counters for all transactions and diameter interfaces on SaMOG (Web-auth) services through P-GW LBO module on various StarOS platforms ASR5500/ASR5700.

The following set of result code specific counters are available for the responses received from the OCS (Online Charging System), on Gy interface. DCCA (Diameter Credit Control Application) is the protocol used on the Gy interface.

Table 1: Result Code Specific Counters

Error Category	Result Code	Result Code Value
Transient Failures [4XXX]	DIAMETER_END_USER_SERVICE_DENIED	4010
	DIAMETER_CREDIT_LIMIT_REACHED	4012
Permanent Failures [5XXX]	DIAMETER_RATING_FAILED	5031

Relationships to Other Features

This feature can also be used when the CC profile configuration is enabled through the GGSN service. When the CC profile is configured under APN service and GGSN service, the prepaid prohibited configuration for the matching CC profile is applied irrespective of the services.

Limitations

The following are the limitations of this feature:

- One charging characteristic value can be mapped to only one credit-control-group/prepaid-prohibited configuration within one APN.
- The charging-characteristic based OCS selection is possible only during the session-setup. Once the credit-control-group is selected (after session setup), this feature is not applicable.

Configuring CC based Selective Gy Session Control

The following sections provide the configuration commands to configure the Gy Session Control feature based on the CC profile of the subscriber.

Configuring CC Value

The following commands are used to configure Charging Characteristic values as postpaid/prepaid to disable/enable Gy session towards the OCS.

```
configure
   context context_name
      apn apn_name
         cc-profile { cc_profile_index | any } { prepaid-prohibited |
credit-control-group cc_group_name }
         end
```

Notes:

- *cc_profile_index*: Specifies the CC profile index. *cc_profile_index* must be an integer from 0 through 15.
- **any**: This keyword is applicable for any non-overridden cc-profile index. This keyword has the least priority over specific configuration for a CC profile value. So, configuring **any** keyword will not override other specific configurations under APN.
- **prepaid-prohibited**: Disables prepaid Gy session for the configured profile index.
- *cc_group_name*: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.
- **no cc-profile** *cc_profile_index*: This command falls back to "any" cc-profile behavior irrespective of the CC profile index value configured.

Verifying the Selective Gy Session Control Configuration

Use the following command in Exec mode to display/verify the configuration of Selective Gy Session Control feature.

```
show configuration
```

Monitoring and Troubleshooting the Selective Gy Session Control Feature

This section provides information regarding show commands and/or their outputs in support of the Selective Gy Session Control feature.

show active-charging sessions

The "Credit-Control" field that appears as part of the **show active-charging sessions [callid | imsi | msisdn]** command output enables the user to determine the credit control state as "On" for online charging enabled session or "Off" for prepaid prohibited session and monitor the subscriber session.

Credit-Control Group in Rulebase Configuration

This section describes the overview and implementation of the Credit-Control (CC) Group Selection based on the rulebase of the subscriber.

This section discusses the following topics for this feature:

Feature Description

This feature is introduced to customize the behavior for different types of subscribers in the Assume Positive scenario. This customization is made by enabling the users to specify a desired Credit-Control (CC) group based on the rulebase dynamically selected by PCRF.

Typically, the behavior for Assume Positive is configured within the CC group. In releases prior to 20, there were options to choose the CC group through APN/subscriber-profiles, IMSA, or AAA configurations. In this release, the CC group selection functionality is extended to rulebase configuration.

This feature is explicitly required in scenarios where IMSA was not used, AAA server could not send CC group during authentication, and only a single APN/subscriber-profile was used for all the subscribers. In such situations, this feature targets to provide a premium CC group within rulebase to enable premium treatment to subscribers based on their types.

This feature introduces a new configurable option inside the rulebase configuration, so that the users can specify the desired CC group whenever the rulebase is selected during the subscriber session setup. This configured CC group overrides or has a higher priority than the CC group configured within the subscriber profile/APN. If the AAA or PCRF server sends the CC-Group AVP, the CC group value defined through the AVP overrides the rulebase configured CC group.

When this feature is enabled, the configuration allows specifying an association between the rulebase name and the CC group so that when a premium subscriber connects, a premium rulebase and a premium CC group are selected.

Important Mid-session configuration change will not impact the existing subscribers in the system. This configuration change will be effected only to the new sessions.

Implementing this new configuration option enables different types of Assume-Positive behavior for subscribers based on the available quota. This results in achieving preferential treatment for premium customers.

The precedence order for selection of the CC group is defined as:

- PCRF provided CC group
- AAA provided CC group
- Rulebase configured CC group
- Subscriber Profile/APN selected CC group
- Default Credit-Control group

Important This feature should not be used when there is an option for AAA server to send the CC group during authentication process. If during the authentication, AAA server sends a CC group, and the rulebase selected has a CC group defined within, then the rulebase defined CC group is selected for the session.

Limitations

There are no limitations or restrictions with this feature. However, it is important to keep in mind the precedence order for CC group selection.

Configuring Credit-Control Group in Rulebase

The following sections provide the configuration commands to configure the Credit-Control Group based on the rulebase of the subscriber.

Defining Credit-Control Group

The following commands are used to configure a desired Credit-Control group name when using the rulebase selected by PCRF.

```
configure
require active-charging
active-charging service service_name
   rulebase rulebase_name
      credit-control-group cc_group_name
      end
```

- *cc_group_name*: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.
- **no credit-control-group**: Removes the previously configured CC group from the rulebase configuration. This is the default setting.
- This CLI configuration is applicable only during the session setup. Mid-session change in the CC group is not allowed.
- This is an optional CLI configuration, and used only when customized Assume Positive behavior is required for subscribers.

- If this CLI command is configured, the selection of the CC group will be based on the precedence order. That is, the rulebase defined CC group has higher precedence over the CC group value specified in the Subscriber/APN profile.
- If the CC group configuration is not present in the rulebase, the default subscriber/APN profile configuration is applied.

Verifying the Credit-Control Group Configuration

Use the following command in Exec mode to display/verify the configuration of CC group in rulebase.

```
show configuration verbose
```

Monitoring and Troubleshooting the CC-Group Selection in Rulebase

This section provides information regarding show commands and/or their outputs in support of this feature.

show active-charging sessions full

The output of this show CLI command displays the selected credit-control-group for the session. The output details are useful in verifying and troubleshooting the issues with this feature.

show configuration errors

This show CLI will list an error if the credit-control group that is configured inside the rulebase is not defined.

show configuration verbose

This command will show the "credit-control-group" option specified for the rulebase. For troubleshooting purpose, capture the output of **show configuration verbose** and **show subscribers full** along with the **monitor-protocol** output containing "Radius Access-Accept".

Combined CCR-U Triggering for QoS Change Scenarios

In release 20, the number of CCR-Us sent to the OCS is controlled for QoS change scenarios in P-GW call. This new behavior is introduced in the system to easily handle the issues with Transactions Per Second (TPS) on OCS.

In releases prior to 20, for a change in the default EPS bearer QoS and APN AMBR received from PCRF for LTE or S2b WiFi calls, P-GW used to send two separate CCR-Us to OCS through Gy interface, one each for QoS change and AMBR change. In 20 and later releases, when default EPS bearer QoS and APN AMBR values are changed, P-GW sends update request to access side to change default bearer and APN AMBR in a single message. P-GW will apply APN AMBR and default bearer QoS accordingly and will send only one CCR-U on Gy for this change condition.

Important This behavior change is applicable only to P-GW calls. This change has no impact to the Rf/CDR records, and GGSN/P-GW eHRPD calls.

Also, note that this behavior is not applicable for split TFT case (QoS + APN AMBR + TFT) wherein multiple Update Bearer Requests are sent towards the access side.

Re-activating Offline Gy Session after Failure

This section describes the feature to re-enable Offline Gy session on detecting failure at Diameter Credit Control Application.

This section includes the following topics:

Feature Description

With this feature, a mechanism to re-enable the Offline Gy session back to Online charging, based on indication from PCRF is introduced in this release. Upon receiving the Online AVP from PCRF, the gateway will establish the Gy session.

In previous releases, there was no provision to activate Gy once the session was marked as Offline. On detecting failure at Diameter Credit Control Application, the configured Credit Control Failure Handling (CCFH) action would be taken. Once the Gy session has taken the CCFH Continue action, the subscriber session could not be retried/re-enabled.

The Online AVP in the Charging-Rule-Definition is considered as the trigger/indication from PCRF to enable the Offline Gy session, after the CCFH Continue action been taken. The Online AVP at the command level from PCRF will not be considered as a trigger to enable the Offline Gy session. As per 3GPP 29.212 (release 12.12.0), the Online AVP (1009) is an optional AVP inside the Charging-Rule-Definition grouped AVP (1003).

Limitations and Restrictions

This section lists the limitations and configuration restrictions with this feature:

- This feature is limited only to Volume Quota mechanism. Special handling is not done for Quota-Validity-Time (QVT) and Quota-Hold-Time (QHT) timers. When the Gy session goes offline and comes back again, these timers are not started. The timers will be started only when the next CCA-U provides the information from OCS.
- When the Gy session is marked Online, CDR closure is not required and this is handled by the billing system.
- This feature is not extended to the event-based credit-control sessions.
- When the CCFH action is taken due to MSCC level failure, the existing behavior is retained and the following behavior is observed:
  - CCFH Continue – Continue the category (MSCC) without charging at Gy and this is applicable to the MSCC (not to the entire session). The MSCC state in the output of the **show active-charging sessions full** command will display "No Charge".
  - CCFH Terminate/Retry-and-Terminate – The bearer gets terminated.
- When the Result-Code 4011 (DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE) is received at MSCC level, the category is marked Free-of-Charge and no further accounting for this category is done. When this result code is received at command level, the Gy session is made Offline. The Offline Gy session can be made Online again using the Online AVP from PCRF and the accounting will resume normally (CCR-U will be seen at OCS for this session).
- When CCFH Continue is configured and CCR-I failure occurs, the following behavior is observed:

- Diabase Error – When diabase error (TCP connection down) occurs, the Gy session is marked Offline and the session-state is maintained (session-ID created). When re-enabling the Gy session, a new CCR-I is sent immediately (without waiting for data).
- Response Timeout – When the response timeout happens, if the CCR-I is sent at session-setup and the session-setup timeout happens before response-timeout, then the bearer itself will be terminated. The **diameter send-crri traffic-start** configuration can be used optionally so that the CCR-I timeout does not affect the bearer creation.
- When the Gy session goes Offline due to CCR-I response timeout and the Gy session is marked Online, the same Session-ID will be used.
- If the Gy session went offline due to CCR-I error response, the session-information is deleted (next session-ID used will be different).

- In case of rule-movement across bearers (LTE to WiFi or vice-versa) where the Online rule is moved/associated to an existing bearer, the status of the Gy session is not changed.
- The trigger for marking the Offline Gy Session to Online is only based on the Online AVP received from the PCRF in the Charging-Rule-Definition.

Configuring Offline Gy Session after Failure

The following section provides the configuration commands to re-enable the offline Gy session.

Re-enabling Offline Gy Session

Use the following configuration to re-enable offline Gy session after failure.

```
configure
  active-charging service service_name
    credit-control
      [ no ] offline-session re-enable
      end
```

Notes:

- When **offline-session re-enable** is configured and the PCRF installs/modifies a rule with "Online" AVP value set to 1, then the Offline DCCA will be marked Online.
- The default configuration is **no offline-session re-enable**. This feature is disabled by default and when disabled only the **show configuration verbose** command will display this configuration.

Verifying the Configuration

Use the following command to verify the offline/online state transition timestamp:

```
show active-charging sessions full
```

Monitoring and Troubleshooting the Offline Gy Session after Failure

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations should be performed to troubleshoot any failure related to this feature:

- The CLI output of the **show active-charging sessions full** command can be verified. The "Last State Change Time" field indicates the timestamps at which a session went Offline and came back Online.
- The messages from **monitor subscriber next-call** command can be enabled with "verbosity 3" to analyze the message exchanges happening for the subscriber.
- The "acsmgr" and "debug" level logs can be enabled for further debugging.

show active-charging sessions full

The following new fields are added to the output of this command to display the state transition timestamp:

- Last State Change Time:
  - Offline/Online – The Offline timestamp is updated when the Gy session goes Offline. The Online timestamp is updated when the session is back Online.

Suppress AVPs

This feature adds enhancement to the *Support MVNO Information in Gx, Gy and CDRs* feature.

Feature Description

This feature adds enhancement to the *Support MVNO Information in Gx, Gy and CDRs* feature. SAEGW sends MVNO-Reseller-ID and MVNO-Subclass-ID AVPs in the Gy messages towards the OCS and CDR, whenever these AVPs are received by SAEGW from the PCRF.

With this enhancement, this behavior is now CLI controlled and a new CLI command has been introduced to suppress the AVPs being sent in the Gy interface.

Old Behavior: Reseller-id and subclass-id AVPs were send in Gy when the same were received from PCRF for the ATT dictionary.

New Behavior: New CLI command **suppress_avp**has been added which allows to suppress the Reseller-id and subclass-id AVPs.

Command Changes

suppress_avp

New CLI command has been added to the Credit Control Group configuration mode to suppress the AVPs. Configuring this CLI command would suppress the MVNO-subclass-id and MVNO-Reseller-Id AVPs.

```
configure
  active-charging service <acs_service_name>
    credit-control group <group_name>
      diameter suppress-avp reseller-id subclass-id
      [ no | default ] diameter suppress-avp reseller-id subclass-id
  end
```

Notes:

- **no:** Disables AVP suppression. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.

- **default:** Sets the default configuration. AVPs are not suppressed by default. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.
- **suppress-avp:** Suppresses both MVNO-subclassid and MVNO-Reseller-id AVPs.
- **reseller-id:** Supresses the MVNO-Reseller-Id AVP.
- **subclass-id:** Supresses the MVNO-Sub-Class-Id AVP.

Performance Indicator Changes

show configuration

This command has been modified to display the following output:

```
credit-control group default
      diameter origin endpoint sundar
      diameter peer-select peer minid1 secondary-peer minid2
      diameter session failover
      diameter dictionary dcca-custom32
      failure-handling initial-request continue
      failure-handling update-request continue
      diameter dynamic-rules request-quota on-traffic-match
      diameter suppress-avp reseller-id subclass-id
```

Configuring Gy Interface Support

To configure Gy interface support:

Step 1 Configure the core network service as described in this Administration Guide.

Step 2 Configure Gy interface support as described in the sections Configuring GGSN / P-GW / IPSG Gy Interface Support, on page 41 and Configuring HA / PDSN Gy Interface Support, on page 42.

Step 3 Configure Event-based Gy support as described in Configuring PLMN and Time Zone Reporting, on page 44.

Step 4 *Optional.* Configure OCS Unreachable Failure Handling Feature or Assume Positive for Gy Feature as described in Configuring Server Unreachable Feature, on page 45.

Step 5 *Optional.* Configure Static Rulebase for CCR as described in Configuring Static Rulebase for CCR, on page 46.

Step 6 *Optional.* Configure Gy for GTP based S2a/S2b as described in Configuring Gy for GTP based S2a/S2b, on page 46.

Step 7 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring GGSN / P-GW / IPSG Gy Interface Support

To configure the standard Gy interface support for GGSN/P-GW/IPSG, use the following configuration:

```
configure
     context <context_name>
          diameter endpoint <endpoint_name>
               origin realm <realm>
               origin host <diameter_host> address <ip_address>
               peer <peer> realm <realm> address <ip_address>
               exit
          exit
     active-charging service <ecs_service_name>
          credit-control [ group <cc_group_name> ]
               diameter origin endpoint <endpoint_name>
               diameter peer-select peer <peer> realm <realm>
               diameter pending-timeout <timeout_period>
               diameter session failover
               diameter dictionary <dictionary>
               failure-handling initial-request continue
               failure-handling update-request continue
               failure-handling terminate-request continue
               exit
          exit
     context <context_name>
           apn <apn_name>
               selection-mode sent-by-ms
               ims-auth-service <service>
               ip access-group <access_list_name> in
               ip access-group <access_list_name> out
               ip context-name <context_name>
               active-charging rulebase <rulebase_name>
               credit-control-group <cc_group_name>
               end
```

Notes:

- For information on configuring IP access lists, refer to the *Access Control Lists* chapter in the *System Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring HA / PDSN Gy Interface Support

To configure HA / PDSN Gy interface support, use the following configuration:

```
configure
     context <context_name>
          diameter endpoint <endpoint_name>
               origin realm <realm>
```

```
                origin host <diameter_host> address <ip_address>
                peer <peer> realm <realm> address <ip_address>
                exit
          exit
     active-charging service <ecs_service_name>
          ruledef <ruledef_name>
                ip any-match = TRUE
                exit
          charging-action <charging_action_name>
                content-id <content_id>
                cca charging credit rating-group <rating_group>
                exit
          rulebase <rulebase_name>
                action priority <action_priority> ruledef <ruledef_name>
charging-action <charging_action_name>
                exit
          credit-control [ group <cc_group_name> ]
                diameter origin endpoint <endpoint_name>
                diameter peer-select peer <peer> realm <realm>
                diameter pending-timeout <timeout>
                diameter session failover
                diameter dictionary <dictionary>
                failure-handling initial-request continue
                failure-handling update-request continue
                failure-handling terminate-request continue
                pending-traffic-treatment noquota buffer
                pending-traffic-treatment quota-exhausted buffer
                exit
          exit
     context <context_name>
          subscriber default
                ip access-group <acl_name> in
                ip access-group <acl_name> out
                ip context-name <context_name>
                active-charging rulebase <rulebase_name>
                credit-control-group <cc_group_name>
                end
```

Notes:

- For information on configuring IP access lists, refer to the *Access Control Lists* chapter in the *System Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring PLMN and Time Zone Reporting

PLMN and Time Zone Reporting feature requires a credit-control group to be defined in the APN or subscriber configuration or there must be a default credit-control group configured. The following CLI commands are available to enable/disable PLMN and Time Zone Reporting feature.

To enable PLMN and Time Zone Reporting through subscriber-template, use the following configuration:

```
configure
     context <context_name>
          subscriber name <subscriber_name>
               dns primary <primary_ipaddress>
               dns secondary <secondary_ipaddress>
               ip access-group test in
               ip access-group test out
               ip context-name <context_name>
               credit-control-client event-based-charging
               active-charging rulebase <rulebase_name>
               exit
               end
```

Notes:

- The **credit-control-client event-based-charging** command should be used to enable PLMN and Time Zone Reporting.

  For more information on configuring PLMN and Time Zone Reporting feature, refer to the *Command Line Interface Reference*.

To enable PLMN and Time Zone Reporting through APN template, use the following configuration:

```
configure
     context <context_name>
          apn <apn_name>
               selection-mode sent-by-ms
               accounting-mode none
               ip access-group test in
               ip access-group test out
               ip context-name <context_name>
               ip address pool name<pool_name>
               credit-control-client event-based-charging
               active-charging rulebase <rulebase_name>
               exit
               end
```

Rest of the parameters needed for Event-based Gy such as dictionary, endpoint will be picked from the credit-control group.

In a scenario where the triggers are configured through the CLI command and another set of triggers are also received from Gx, then the triggers from Gx will have a higher priority.

Configuring Server Unreachable Feature

The Server Unreachable feature requires a failure handling behavior to be defined in the Diameter Credit Control configuration. The following CLI commands are available to enable/disable OCS Unreachable Failure Handling feature.

To enable OCS Unreachable Failure Handling feature, use the following configuration:

```
configure
require active-charging
         active-charging service <service_name>
              credit-control
                   servers-unreachable { initial-request | update-request
 } { continue | terminate }  [ { after-interim-volume <bytes> |
after-interim-time <seconds> } +   server-retries <retry_count> ]
                  servers-unreachable behavior-triggers { initial-request
 | update-request } transport-failure [ response-timeout | tx-expiry ]
                   servers-unreachable behavior-triggers initial-request
 { result-code { any-error | result-code [ to end-result-code ] } }
                   servers-unreachable behavior-triggers update-request
{ result-code { any-error | result-code [ to end-result-code ] } }
                  end
```

Important After you configure **configure**, **require active-charging** , **active-charging service** <*service_name*>, and **credit-control** CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Notes:

- This CLI command "**servers-unreachable { initial-request | update-request } { continue | terminate } [{ after-interim-volume ...**" allows configuring interim-volume and interim-time in the following ways:
  - after-interim-volume <bytes> alone followed by server-retries.
  - after-interim-time <secs> alone followed by server-retries.
  - after-interim-volume <bytes> after-interim-time <secs> followed by server-retries.
- This CLI command "**servers-unreachable behavior-triggers**" is used to trigger the servers-unreachable failure handling at either Tx expiry or Response timeout (This CLI is similar to retry-after-tx-expiry in "**failure-handling update-request continue retry-after-tx-expiry**" command.).
- This CLI command "**servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [to end-result-code] } }**" is used to trigger the servers-unreachable failure handling based on the configured Diameter error result codes.

For more information on configuring this feature, refer to the *Command Line Interface Reference*.

Configuring Static Rulebase for CCR

To allow static configuration of rulebase name to be passed to OCS via CCR message, use the following configuration:

```
configure
    require active-charging
    active-charging service service_name
         credit-control group  ccgroup_name
              charging-rulebase-name rulebase_name
              no charging-rulebase-name
              end
```

Important After you configure **configure**, **require active-charging**, **active-charging service** *service_name*, and **credit-control group** *ccgroup_name* CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Notes:

- By default, the rulebase obtained from APN/subscriber template will be sent to OCS through the CCR message.

For more information on configuring this feature, refer to the *Command Line Interface Reference*.

Configuring Gy for GTP based S2a/S2b

To provide Gy Support for WiFi integration in P-GW for GTP based S2a/S2b, use the following configuration:

```
configure
    require active-charging
    active-charging service service_name
         credit-control group  ccgroup_name
              diameter update-dictionary-avps 3gpp-rel11
              [  default | no ] diameter update-dictionary-avps
              end
```

Notes:

- **3gpp-rel11**: Provides support for 3GPP Rel.11 specific AVPs in the standard Gy dictionary.

Gathering Statistics

This section explains how to gather Gy related statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Statistics/Information	Action to perform
Complete statistics for ECS sessions.	**show active-charging sessions full**

Statistics/Information	Action to perform
Detailed information for the Active Charging Service (ACS)	**show active-charging service all**
Information on all rule definitions configured in the service.	**show active-charging ruledef all**
Information on all charging actions configured in the service.	**show active-charging charging-action all**
Information on all rulebases configured in the service.	**show active-charging rulebase all**
Statistics of the Credit Control application, DCCA.	**show active-charging credit-control statistics**
States of the Credit Control application's sessions, DCCA.	**show active-charging credit-control session-states [rulebase** *<rulebase_name>* **] [content-id** *<content_id>* **]**