Gx Interface Support

This chapter provides information on configuring Gx interface to support policy and charging control for subscribers.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

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 this Administration Guide.

The following topics are covered in this chapter:

Rel. 7 Gx Interface

Rel. 7 Gx interface support is available on the Cisco ASR chassis running StarOS 8.1 or StarOS 9.0 and later releases for the following products:

- GGSN
- IPSG

This section describes the following topics:

Introduction

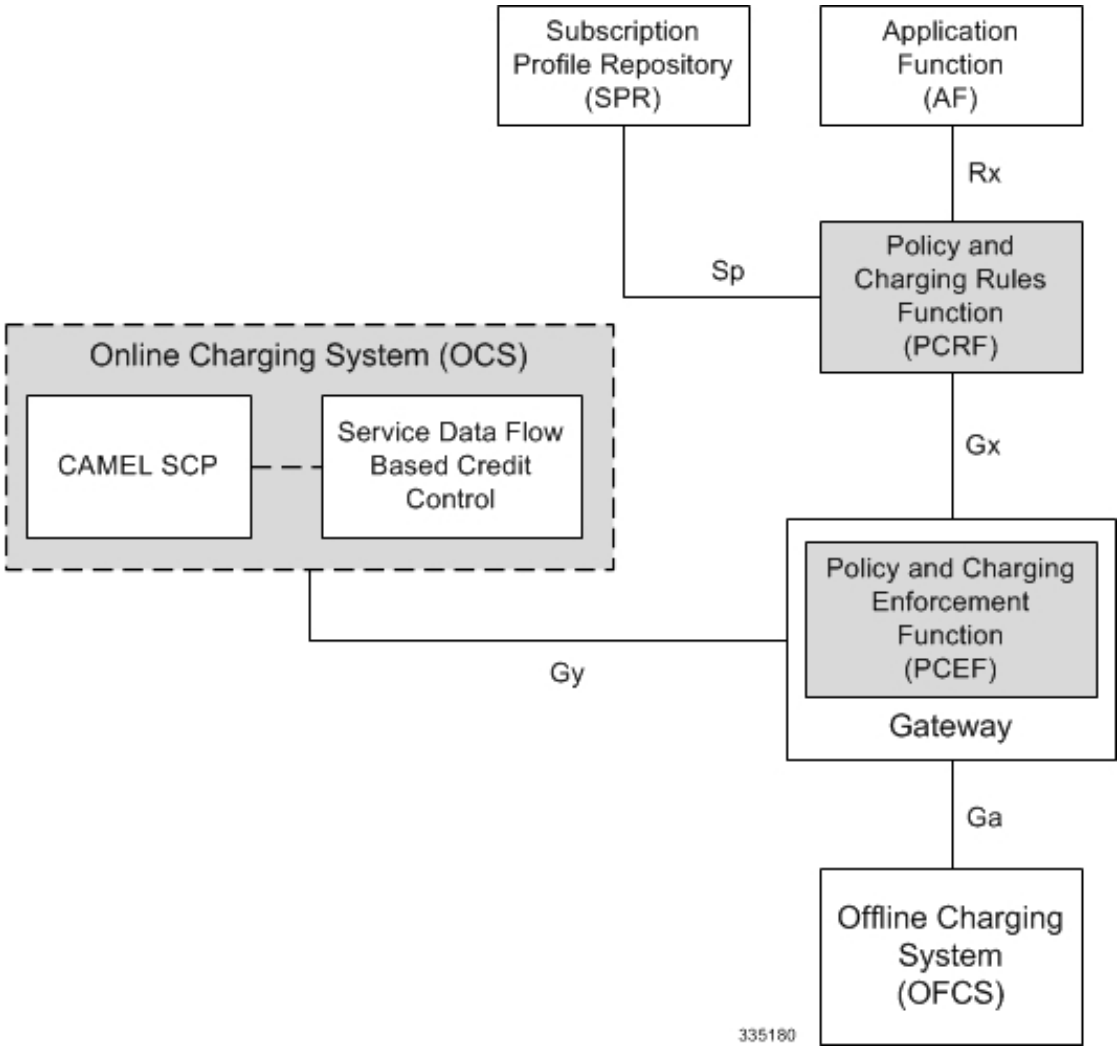
For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and do charging. Other parameters associated with the rules are used to enforce policy control.

The PCC architecture allows operators to perform service-based QoS policy, and flow-based charging control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/Cisco Systems GGSN and the Policy and Charging Rules Function (PCRF).

In GPRS/UMTS networks, the client functionality lies with the GGSN, therefore in the IMS authorization scenario it is also called the Gateway. In the following figure, Gateway is the Cisco Systems GGSN, and the PCEF function is provided by Enhanced Charging Service (ECS). The Rel 7. Gx interface is implemented as a Diameter connection. The Gx messages mostly involve installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

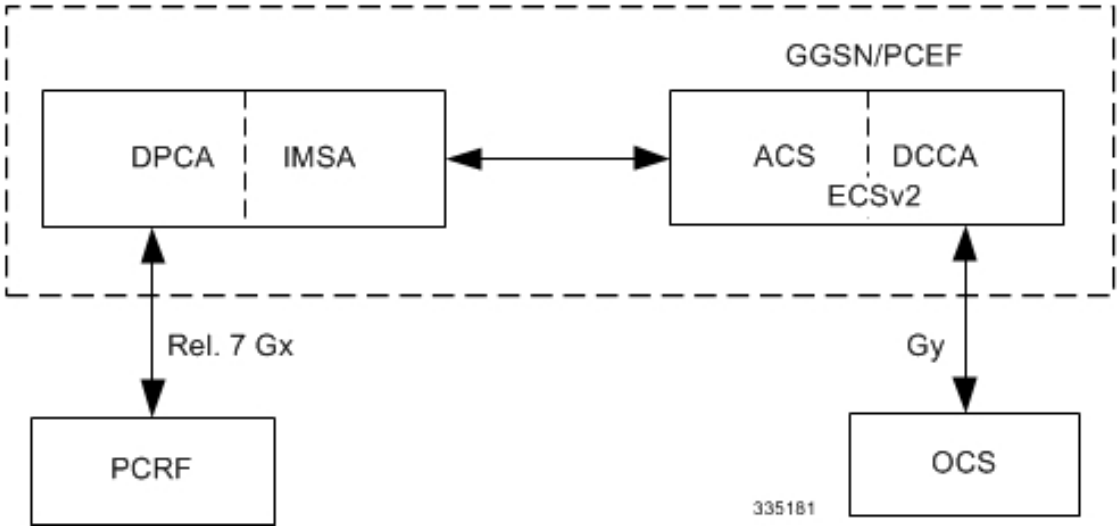
The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application. The following figure shows the reference points between various elements involved in the policy and charging architecture.

Figure 1: PCC Logical Architecture



Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS). The following figure shows the interaction between components within the Gateway.

Figure 2: PCC Architecture within Cisco PCEF



Supported Networks and Platforms

This feature is supported on all chassis with StarOS Release 8.1 and later running GGSN service for the core network services.

License Requirements

The Rel. 7 Gx 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

The Rel 7. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V7.6.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 29.212 V7.8.0 (2009-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 7 Gx functionality.

Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN bearer.

Policy control comprises the following functions:

- **Binding:** Binding is the generation of an association between a Service Data Flow (SDF) and the IP CAN bearer (for GPRS a PDP context) transporting that SDF.

  The QoS demand in the PCC rule, as well as the SDF template are input for the bearer binding. The selected bearer will have the same QoS Class as the one indicated by the PCC rule.

  Depending on the type of IP-CAN and bearer control mode, bearer binding can be executed either by the PCRF, or both PCRF and PCEF.

  - For UE-only IP-CAN bearer establishment mode, the PCRF performs bearer binding. When the PCRF performs bearer binding, it indicates the bearer (PDP context) by means of Bearer ID. The Bearer ID uniquely identifies the bearer within the PDP session.
  - For UE/NW IP-CAN bearer establishment mode, the PCRF performs the binding of the PCC rules for user controlled services, while the PCEF performs the binding of the PCC rules for the network-controlled services.

  Prior to Release 16.0, the rule binding was getting rejected. In 16.0 and later releases, the binding of PCEF rules will be successful when BCM mode is set to UE-only for EPS IP-CAN bearer without "bearer-ID" in the PCRF messages such as RAR or CCA-U.

  In the 3G to 4G handover scenario, rule binding and rule removal will be successful in UE-only mode and any filter (and related info) changes because of this modification/installation/removal will not be notified to UE as updates in UE only mode cannot be sent to UE. These rules are only considered for charging and the expectation is that the same rules are again modified in 4G (if handover is done) so that the filters (and related info) can be notified to UE.

  In releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

  This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

- **Gating Control:** Gating control is the blocking or allowing of packets, belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is opened, the packets of the related IP flows are allowed to be forwarded.
- **Event Reporting**: Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF).
  - Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Although event trigger reporting from PCEF to PCRF can apply for an IP CAN session or bearer depending on the particular event, provisioning of event triggers will be done at session level.

Note that in 11.0 and later releases, RAR with unknown event triggers are silently ignored and responded with DIAMETER_SUCCESS. In earlier releases, when unknown event triggers were received in the RAR command from PCRF, invalid AVP result code was set in the RAA command.

- The Event Reporting Function (ERF) receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response back to the PCRF. The Event Reporting Function is located in the PCEF.

  In StarOS releases prior to 14.0, SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger was sent for rules irrespective of successful installation. In 14.0 and later releases, SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger will be sent under the following conditions:

  - When a rule is installed successfully (and the event trigger is armed by PCRF and resource-allocation-notification is enabled).
  - On partial failure, i.e., when two or more rules are installed and at least one of the rules were successfully installed. (and the event trigger is armed by PCRF and resource-allocation-notification is enabled).

  On complete failure, i.e., none of the rules were installed, the event-trigger SUCCESSFUL_RESOURCE_ALLOCATION (22) will not be sent.

Important In this release, event triggers "IP-CAN_CHANGE" and "MAX_NR_BEARERS_REACHED" are not supported.

- **QoS Control:** QoS control is the authorization and enforcement of the maximum QoS that is authorized for a SDF or an IP-CAN bearer or a QoS Class Identifier (QCI). In case of an aggregation of multiple SDFs (for GPRS a PDP context), the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate.
  - QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.
  - The enforcement of the authorized QoS of the IP-CAN bearer may lead to a downgrading or upgrading of the requested bearer QoS by the Gateway (PCEF) as part of a UE-initiated IP-CAN bearer establishment or modification. Alternatively, the enforcement of the authorized QoS may, depending on operator policy and network capabilities, lead to network-initiated IP-CAN bearer establishment or modification. If the PCRF provides authorized QoS for both, the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.
  - QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. In case the PCRF provides PCC rules dynamically, authorized QoS information for the IP-CAN bearer (combined QoS) may be provided. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are

activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

Important In this release, QoS Resource Reservation is not supported.

Supported Features:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Provisioning of "Authorized QoS" Per IP CAN Bearer: The authorized QoS per IP-CAN bearer is used if the bearer binding is performed by the PCRF.
- Policy Enforcement for "Authorized QoS" per IP CAN Bearer: The PCEF is responsible for enforcing the policy-based authorization, that is to ensure that the requested QoS is in-line with the "Authorized QoS" per IP CAN Bearer.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
  - Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
  - Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule. If the PCRF provides authorized QoS for both the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.

Important In this release, coordination of authorized QoS scopes in mixed mode (BCM = UE_NW) is not supported.

- - Provisioning of Authorized QoS Per QCI: If the PCEF performs the bearer binding, the PCRF may provision an authorized QoS per QCI for non-GBR bearer QCI values. If the PCRF performs the bearer binding the PCRF does not provision an authorized QoS per QCI. The PCRF does not provision an authorized QoS per QCI for GBR bearer QCI values.

    Important Only standards-based QCI values of 1 through 9 are supported. QCI values 1 through 9 are defined in 3GPP Specification TS 23.203 "Policy and charging control architecture".

  - Policy Enforcement for Authorized QoS per QCI: The PCEF can receive an authorized QoS per QCI for non GBR-bearer QCI values.

- Other Features:
  - Bearer Control Mode Selection: The PCEF may indicate, via the Gx reference point, a request for Bearer Control Mode (BCM) selection at IP-CAN session establishment or IP-CAN session

modification (as a consequence of an SGSN change). It will be done using the "PCC Rule Request" procedure.

If the Bearer-Control-Mode AVP is not received from PCRF, the IP-CAN session is not terminated. The value negotiated between UE/SGSN/GGSN is considered as the BCM. The following values are considered for each of the service types:

- GGSN: The negotiated value between UE/SGSN/GGSN is considered.

  In the following scenarios UE_ONLY is chosen as the BCM:

  Scenario 1:

  - UE-> UE_ONLY
  - SGSN-> UE_ONLY
  - GGSN-> UE_ONLY
  - PCRF-> NO BCM

  Scenario 2:

  - UE-> UE_ONLY
  - SGSN-> UE_ONLY
  - GGSN-> Mixed
  - PCRF-> NO BCM

- GTP-PGW: BCM of UE_NW is considered.
- IPSG: BCM of UE_ONLY is considered.
- HSGW/SGW/PDIF/FA/PDSN/HA/MIPV6HA: BCM of NONE is considered.

- PCC Rule Error Handling: If the installation/activation of one or more PCC rules fails, the PCEF includes one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

  If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fails, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

  If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF sends the PCRF a new CCR command and include a Charging-Rule-Report AVP. The PCEF includes the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and sets the PCC-Rule-Status to INACTIVE.

  In releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

- Time of the Day Procedures: PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION_TIMEOUT event.

Important In 11.0 and later releases, Rule-Activation-Time / Rule-Deactivation-Time / Revalidation-Time AVP is successfully parsed only if its value corresponds to current time or a later time than the current IPSG time, else the AVP and entire message is rejected. In earlier releases the AVP is successfully parsed only if its value corresponds to a later time than the current IPSG time, else the AVP and entire message is rejected.

In releases prior to 17.0, if "Rule-Deactivation-Time" AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis. In 17.0 and later releases, if Rule-Deactivation-Time AVP is omitted in CCA/RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).

Important This behavior change is applicable only to predefined rules.

Support for Firewall Policy on Gx: The Diameter AVP "SN-Firewall-Policy" has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.

Charging Control

Charging Control is the process of associating packets belonging to a SDF to a charging key, and applying online charging and/or offline charging, as appropriate. Flow-based charging handles differentiated charging of the bearer usage based on real time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, and then no offline charging information is generated.

Supported Features:

- Provisioning of Charging-related Information for the IP-CAN Session.
- Provisioning of Charging Addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses or the peer names).

Important In this release, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method: In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline are sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

Charging Correlation

For the purpose of charging correlation between SDF level and application level (for example, IMS) as well as on-line charging support at the application level, applicable charging identifiers and IP-CAN type identifiers are passed from the PCRF to the AF, if such identifiers are available.

For IMS bearer charging, the IP Multimedia Core Network (IM CN) subsystem and the Packet Switched (PS) domain entities are required to generate correlated charging data.

In order to achieve this, the Gateway provides the GGSN Charging Identifier (GCID) associated with the PDP context along with its address to the PCRF. The PCRF in turn sends the IMS Charging Identifier (ICID), which is provided by the P-CSCF, to the Gateway. The Gateway generates the charging records including the GCID as well as the ICID if received from PCRF, so that the correlation of charging data can be done with the billing system.

PCRF also provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF.
  - Select downlink IP CAN bearers based on SDF filters in the PCC rule.
  - Enforce uplink IP flows are transported in the correct IP CAN bearer using the SDF filters within the PCC rule.
- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- Dynamic PCC Rules: Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be installed, modified, and removed at any time.
- Predefined PCC Rule: Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

Important A third type of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

- Rule Name: The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- Service Identifier: The service identifier is used to identify the service or the service component the SDF relates to.
- Service Data Flow Filter(s): The service flow filter(s) is used to select the traffic for which the rule applies.
- Precedence: For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- Gate Status: The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.
- QoS Parameters: The QoS information includes the QoS class identifier (authorized QoS class for the SDF), the Allocation and Retention Priority (ARP), and authorized bitrates for uplink and downlink.

Important In earlier releases, ECS used only the Priority-Level part of ARP byte for bearer binding, (along with QCI). Now the entire ARP byte is used for bearer binding (along with QCI). Since the capability and vulnerability bits are optional in a dynamic rule, if a dynamic rule is received without these flags, it is assumed that the capability bit is set to 1 (disabled) and vulnerability bit is set to 0 (enabled). For predefined rules, currently configuring these two flags is not supported, so as of now all predefined rules are assumed to have capability bit set to 1 (disabled) and vulnerability bit set to 0 (enabled).

- Charging key (rating group)
- Other charging parameters: The charging parameters define whether online and offline charging interfaces are used, what is to be metered in offline charging, on what level the PCEF will report the usage related to the rule, and so on.

Important In this release, configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

Important ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

In releases prior to 14.0, there were only 10 PCC rules that were recovered per bearer in the event of a session manager crash. In 14.0 and later releases, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

In releases prior to 17.0, when P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW. In 17.0 and later releases, when modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW. After the response for the pending request is received from the access network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

PCC Procedures over Gx Reference Point

Request for PCC Rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:

- At IP-CAN session establishment
- At IP-CAN session modification

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

Provisioning of PCC Rules

The PCRF indicates, via the Rel. 8 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provisioning, the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.

Important In 11.0 and later releases, the maximum valid length for a charging rule name is 63 bytes. When the length of the charging rule name is greater than 63 bytes, a charging rule report with RESOURCES_LIMITATION as Rule-Failure-Code is sent. This charging rule report is sent only when the length of the rule name is lesser than 128 characters. When the charging rule name length is greater than or equal to 128 characters no charging rule report will be sent. In earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes.

Releases prior to 14.0, when PCRF has subscribed to Out of Credit trigger, on session connect when one rule validation fails and also when an Out of Credit was received from OCS for another rule, P-GW was trying to report these failures in different CCR-U to PCRF. However, the second CCR-U of Out of credit was getting dropped internally.

In 14.0 and later releases, on session connect, P-GW combines the rule failure and out of credit in the same CCR-U and sends to PCRF.

Selecting a PCC Rule for Uplink IP Packets

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP CAN bearer by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP CAN bearer in the order of the precedence of the PCC rules.

Important When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.

Important In 11.0 and later releases, IMSA and ECS allow the PCRF to install two (or more) dynamic rules with the same precedence value. In earlier releases, for two distinct dynamic rules having the same precedence the second rule used to be rejected.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP CAN bearer are discarded.

Selecting a PCC Rule and IP CAN Bearer for Downlink IP Packets

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of all IP CAN bearers of the IP CAN session in the order of the precedence of the PCC rules.

Important When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. The Downlink IP Packet is transported within the IP CAN bearer where the selected PCC rule is mapped. Downlink IP packets that do not match any PCC rule of the IP CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Bearer Termination Implications
- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated (for example, for GPRS when the last PDP Context within the IP-CAN session is being terminated) the PCEF contacts the PCRF.
- Request of IP-CAN Bearer Termination: If the termination of the last IP CAN bearer within an IP CAN session is requested, the PCRF and PCEF apply the "Request of IP-CAN Session Termination" procedure.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

The PCEF applies IP CAN specific procedures to terminate the IP CAN session. For GPRS, the GGSN send a PDP context deactivation request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the "Indication of IP CAN Session Termination" procedure.

In 12.0 and later releases, volume or rule information obtained from PCRF is discarded if the subscriber is going down.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature, which is supported by all products supporting Rel. 7 Gx interface.

License Requirements

The Volume Reporting over Gx 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*.

Important In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V9.5.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

Important Volume Reporting over Gx is applicable only for volume quota.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

  Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

  - Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
  - Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be the same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
  - Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

  For session-level reporting, the actual usage volume is compared with the usage volume threshold.

  For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

  If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

  In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

- IP CAN Session Termination: When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- PCC Rule Removal: When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last

PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- PCRF Requested Usage Report: In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- Revalidation Timeout: In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

  In the case of standard implementation, this must be enabled by CLI configuration.

Important The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see Configuring Volume Reporting over Gx, on page 27.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

How Rel. 7 Gx Works

This section describes how dynamic policy and charging control for subscribers works with Rel. 7 Gx interface support in GPRS/UMTS networks.

The following figure and table explain the IMSA process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.

Important In 14.0 and later releases, the DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Figure 3: Rel. 7 Gx IMS Authorization Call Flow

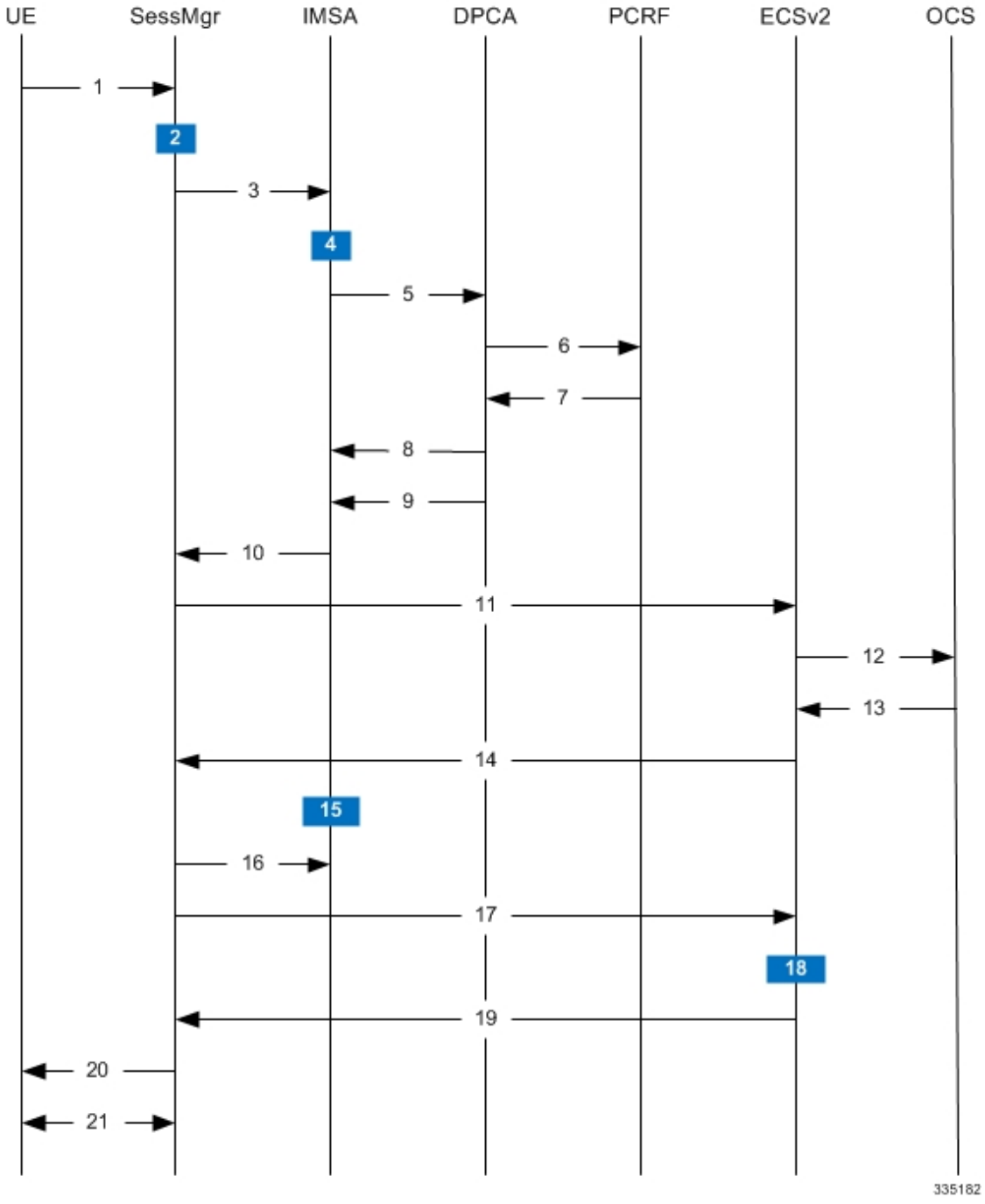


Table 1: Rel. 7 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for primary PDP context activation/creation.

Step	Description
2	SessMgr allocates an IP address to the UE.
3	SessMgr requests IMS Authorization, if IMSA is enabled for the APN.
4	IMSA allocates resources for the IP CAN session and the bearer, and selects the PCRF to contact based on the user's selection key (for example, msisdn).
5	IMSA requests the DPCA module to issue an auth request to the PCRF.
6	DPCA sends a CCR initial message to the selected PCRF. This message includes the Context-Type AVP set to PRIMARY and the IP address allocated to the UE. The message may include the Bearer-Usage AVP set to GENERAL. The Bearer-Operation is set to Establishment. The Bearer ID is included if the PCRF does the bearer binding.
7	PCRF may send preconfigured charging rules in CCA, if a preconfigured rule set for general purpose PDP context is provided in PCRF. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.
8	DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, and so on, along with the Bearer ID that corresponds to the rules received from the PCRF to IMSA. IMSA stores the information. If the Bearer ID is absent, and PCRF does the bearer binding, the rule is skipped. Whereas, if the Bearer ID is absent and the PCEF does the bearer binding, the rule is passed onto the ECS to perform bearer binding.
9	DPCA calls the callback function registered with it by IMSA.
10	IMSA stores the bearer authorized QoS information and notifies the SessMgr. Other PCRF provided information common to the entire PDP session (event trigger, primary/secondary OCS address, and so on) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.

Step	Description
11	If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The APN name, primary/secondary OCS server address, and so on are sent to the ECS from the SessMgr.
12	ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the APN/AAA) and GPRS specific attributes (for example, APN, UMTS QoS, and so on).
13	OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.
14	ECS responds to SessMgr with the response message.
15	SessMgr requests IMSA for the dynamic rules.
16	IMSA sends the dynamic rules to SessMgr. Note that, in 14.0 and later releases, the RAR messages are allowed before the session is established. In earlier releases, until the primary PDP context is established, all RAR messages from the PCRF were rejected. Also note that, in 14.0 and later releases, the RAR message is rejected and RAA is sent with 3002 result code when the recovery of dynamic rule information and audit of Session Manager are in progress. Earlier, the RAR messages were processed by DPCA even when the recovery audit was in progress.
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS. ECS performs PCEF bearer binding for rules without bearer ID.

Step	Description
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the PDP Context Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.
21	Based on the PCEF bearer binding for the PCC rules at Step 18, the outcome could be one or more network-initiated PDP context procedures with the UE (Network Requested Update PDP Context (NRUPC) / Network Requested Secondary PDP Context Activation (NRSPCA)).

Configuring Rel. 7 Gx Interface

To configure Rel. 7 Gx interface functionality, the IMS Authorization service must be configured at the context level, and then the APN configured to use the IMS Authorization service.

To configure Rel. 7 Gx interface functionality:

Step 1 Configure IMS Authorization service at the context level for IMS subscriber in GPRS/UMTS network as described in Configuring IMS Authorization Service at Context Level, on page 24.

Step 2 Verify your configuration as described in Verifying the Configuration, on page 26.

Step 3 Configure an APN within the same context to use the IMS Authorization service for IMS subscriber as described in Applying IMS Authorization Service to an APN, on page 26.

Step 4 Verify your configuration as described in Verifying Subscriber Configuration, on page 27.

Step 5 *Optional:* Configure the Volume Reporting over Gx feature as described in Configuring Volume Reporting over Gx, on page 27.

Step 6 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 IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization service at context level for IMS subscribers in GPRS/UMTS networks:

```
configure
     context <context_name>
          ims-auth-service <imsa_service_name>
               p-cscf discovery table { 1 | 2 } algorithm {
ip-address-modulus | msisdn-modulus | round-robin }
               p-cscf table { 1 | 2 } row-precedence <precedence_value> {
address <ip_address> | ipv6-address <ipv6_address> } [ secondary { address
<ip_address> | ipv6-address <ipv6_address> } ]
               policy-control
                    diameter origin endpoint <endpoint_name>
                    diameter dictionary <dictionary>
                    diameter request-timeout <timeout_duration>
                    diameter host-select table { { { 1 | 2 } algorithm {
 ip-address-modulus | msisdn-modulus | round-robin } } | prefix-table {
1 | 2 } }
                    diameter host-select row-precedence <precedence_value>
table { { { 1 | 2 } host <host_name> [ realm <realm_id> ] [ secondary host
<host_name> [ realm <realm_id> ] ] } | { prefix-table { 1 | 2 }
msisdn-prefix-from <msisdn_prefix_from> msisdn-prefix-to <msisdn_prefix_to> host
 <host_name> [ realm <realm_id> ] [ secondary host <sec_host_name> [ realm
<sec_realm_id> ] algorithm { active-standby | round-robin } ] } } [ -noconfirm
 ]
                    diameter host-select reselect subscriber-limit
<subscriber_limit> time-interval <duration>
                    failure-handling cc-request-type { any-request |
initial-request | terminate-request | update-request } {
diameter-result-code { any-error | <result_code> [ to <end_result_code> ] } }
{ continue | retry-and-terminate | terminate }
                    end
```

Notes:

- <*context_name*> must be the name of the context where you want to enable IMS Authorization service.
- <*imsa_service_name*> must be the name of the IMS Authorization service to be configured for Rel. 7 Gx interface authentication.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.
- Secondary P-CSCF IP address can be configured in the P-CSCF table. Refer to the *Command Line Interface Reference* for more information on the **p-cscf table** command.

  In 18 and later releases, the syntax for **p-cscf table** configuration command is:

  ```
  p-cscf table { 1 | 2 } row-precedence precedence_value { ipv4-address
  ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [
  ipv4-address ipv4_address ] } [ secondary { ipv4-address ipv4_address [
  ```

ipv6-address *ipv6_address* **]** **|** **ipv6-address** *ipv6_address* **[** **ipv4-address** *ipv4_address* **]** **}** **[** **weight** *value* **]**

- To enable Rel. 7 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account representative.
- When configuring the MSISDN prefix range based PCRF selection mechanism:

  To enable the Gx interface to connect to a specific PCRF for a range of subscribers configure **msisdn-prefix-from** <*msisdn_prefix_from*> and **msisdn-prefix-to** <*msisdn_prefix_to*> with the starting and ending MSISDNs respectively.

  To enable the Gx interface to connect to a specific PCRF for a specific subscriber, configure both **msisdn-prefix-from** <*msisdn_prefix_from*> and **msisdn-prefix-to** <*msisdn_prefix_to*> with the same MSISDN.

  In StarOS 8.1 and later releases, per MSISDN prefix range table a maximum of 128 rows can be added. In StarOS 8.0 and earlier releases, a maximum of 100 rows can be added.

  The MSISDN ranges must not overlap between rows.
- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- *Optional:* To configure the Quality of Service (QoS) update timeout for a subscriber, in the IMS Authorization Service Configuration Mode, enter the following command:

  qos-update-timeout <*timeout_duration*>

  Important This command is obsolete in release 11.0 and later releases.
- *Optional:* To configure signalling restrictions, in the IMS Authorization Service Configuration Mode, enter the following commands:

  signaling-flag { deny | permit }

  signaling-flow permit server-address <*ip_address*> **[server-port {** <*port_number*> **| range** <*start_number*> **to** <*end_number*> **}] [description** <*string*> **]**
- *Optional*: To configure action on packets that do not match any policy gates in the general purpose PDP context, in the IMS Authorization Service Configuration Mode, enter the following command:

  traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }
- To configure the PCRF host destinations configured in the GGSN/PCEF, use the **diameter host-select** CLI commands.
- To configure the GGSN/PCEF to use a pre-defined rule when the Gx fails, set the **failure-handling cc-request-type** CLI to **continue**. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.
- For provisioning of default charging method, use the following configurations. For this, the AVPs Online and Offline will be sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.
  - To send Enable Online:

configure

active-charging service *<ecs_service_name>*

charging-action *<charging_action_name>*

cca charging credit

exit

- To send Enable Offline:

configure

active-charging service *<ecs_service_name>*

rulebase *<rulebase_name>*

billing-records rf

exit

Verifying the Configuration

To verify the IMS Authorization service configuration:

Step 1 Change to the context where you enabled IMS Authorization service by entering the following command:

```
context <context_name>
```

Step 2 Verify the IMS Authorization service's configurations by entering the following command:

```
show ims-authorization service name <imsa_service_name>
```

Applying IMS Authorization Service to an APN

After configuring IMS Authorization service at the context-level, an APN must be configured to use the IMS Authorization service for an IMS subscriber.

Use the following example to apply IMS Authorization service functionality to a previously configured APN within the context configured as described in Configuring Rel. 7 Gx Interface, on page 23.

```
configure
   context <context_name>
      apn <apn_name>
         ims-auth-service <imsa_service_name>
         active-charging rulebase <rulebase_name>
         end
```

Notes:

- *<context_name>* must be the name of the context in which the IMS Authorization service was configured.
- *<imsa_service_name>* must be the name of the IMS Authorization service configured for IMS authentication in the context.
- For Rel. 7 Gx, the ECS rulebase must be configured in the APN.

- ECS allows change of rulebase via Gx for PCEF binding scenarios. When the old rulebase goes away, all the rules that were installed from that rulebase are removed. This may lead to termination of a few bearers (PDP contexts) if they are left without any rules. If there is a Gx message that changes the rulebase, and also activates some predefined rules, the rulebase change is made first, and the rules are activated from the new rulebase. Also, the rulebase applies to the entire call. All PDP contexts (bearers) in one call use the same ECS rulebase.
- For predefined rules configured in the ECS, MBR/GBR of a dynamic/predefined rule is checked before it is used for PCEF binding. All rules (dynamic as well as predefined) have to have an MBR associated with them and all rules with GBR QCI should have GBR also configured. So for predefined rules, one needs to configure appropriate peak-data-rate, committed-data-rate as per the QCI being GBR QCI or non-GBR QCI. For more information, in the ACS Charging Action Configuration Mode, see the **flow limit-for-bandwidth** CLI command.
- For interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF as ECS group-of-ruledefs, configure the following command in the Active Charging Service Configuration Mode:

  policy-control charging-rule-base-name active-charging-group-of-ruledefs

Verifying Subscriber Configuration

Verify the IMS Authorization service configuration for subscriber(s) by entering the following command:

show subscribers ims-auth-service <*imsa_service_name*>

<*imsa_service_name*> must be the name of the IMS Authorization service configured for IMS authentication.

Configuring Volume Reporting over Gx

This section describes the configuration required to enable Volume Reporting over Gx.

To enable Volume Reporting over Gx, use the following configuration:

```
configure
     active-charging service <ecs_service_name>
          rulebase <rulebase_name>
               action priority <priority> dynamic-only ruledef <ruledef_name>
 charging-action <charging_action_name> monitoring-key <monitoring_key>
               exit
          exit
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    event-update send-usage-report [ reset-usage ]
                    end
```

Notes:

- The maximum accepted monitoring key value by the PCEF is 4294967295. If the PCEF sends a greater value, the value is converted to an Unsigned Integer value.
- The **event-update** CLI which enables volume usage report to be sent in event updates is available only in 10.2 and later releases. The optional keyword **reset-usage** enables to support delta reporting wherein the usage is reported and reset at PCEF. If this option is not configured, the behavior is to send the usage information as part of event update but not reset at PCEF.

Gathering Statistics

This section explains how to gather Rel. 7 Gx 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.

Table 2: Gathering Rel. 7 Gx Statistics and Information

Statistics/Information	Action to perform
Information and statistics specific to policy control in IMS Authorization service.	**show ims-authorization policy-control statistics**
Information and statistics specific to the authorization servers used for IMS Authorization service.	**show ims-authorization servers ims-auth-service**
Information of all IMS Authorization service.	**show ims-authorization service all**
Statistics of IMS Authorization service.	**show ims-authorization service statistics**
Information, configuration, and statistics of sessions active in IMS Authorization service.	**show ims-authorization sessions all**
Complete information, configuration, and statistics of sessions active in IMS Authorization service.	**show ims-authorization sessions full**
Summarized information of sessions active in IMS Authorization service.	**show ims-authorization sessions summary**
Complete statistics for active charging service sessions.	**show active-charging sessions full**
Information for all rule definitions configured in the service.	**show active-charging ruledef all**
Information for all rulebases configured in the system.	**show active-charging rulebase all**
Information on all group of ruledefs configured in the system.	**show active-charging group-of-ruledefs all**
Information on policy gate counters and status.	**show ims-authorization policy-gate { counters | status }** This command is no longer an option in StarOS release 11.0 and beyond.

Rel. 8 Gx Interface

Rel. 8 Gx interface support is available on the Cisco ASR chassis running StarOS 10.0 or StarOS 11.0 and later releases.

This section describes the following topics:

HA/PDSN Rel. 8 Gx Interface Support

This section provides information on configuring Rel. 8 Gx interface for HA and PDSN to support policy and charging control for subscribers in CDMA networks.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers in CDMA networks require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

It is recommended that before using the procedures in this section you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

This section describes the following topics:

Introduction

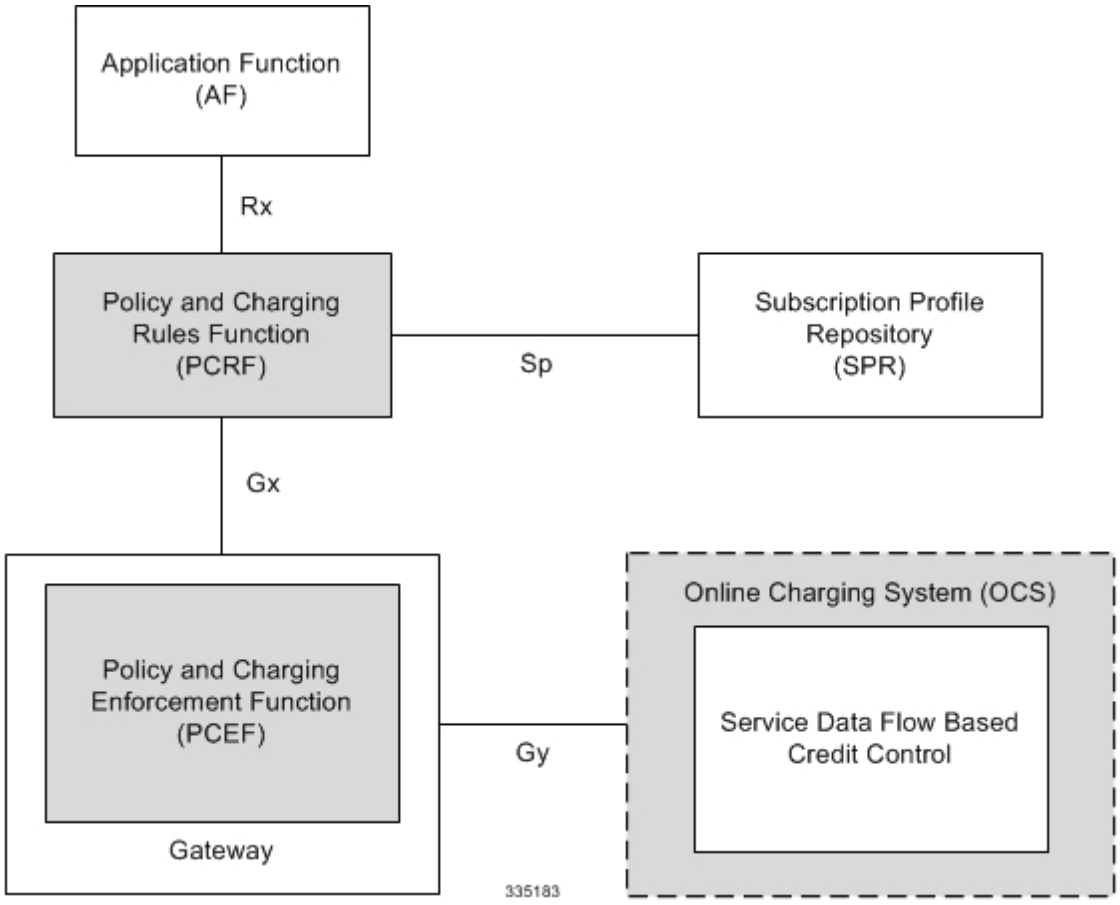
For IMS deployment in CDMA networks the system uses Rel. 8 Gx interface for policy-based admission control support and flow-based charging (FBC). The Rel. 8 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports FBC. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and to do charging. Other parameters associated with the rules are used to enforce policy control.

The PCC architecture allows operators to perform service-based QoS policy and FBC control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/HA/PDSN and the Policy and Charging Rules Function (PCRF). The client functionality lies with the HA/PDSN, therefore in the IMS Authorization (IMSA) scenario it is also called the Gateway. The PCEF function is provided by the Enhanced Charging Service (ECS). The Gx interface is implemented as a Diameter connection. The Gx messaging mostly involves installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

The Gx reference point is located between the Gateway/PCEF and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway/PCEF, and the transmission of traffic plane events from the Gateway/PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application.

The following figure shows the reference points between elements involved in the policy and charging architecture.

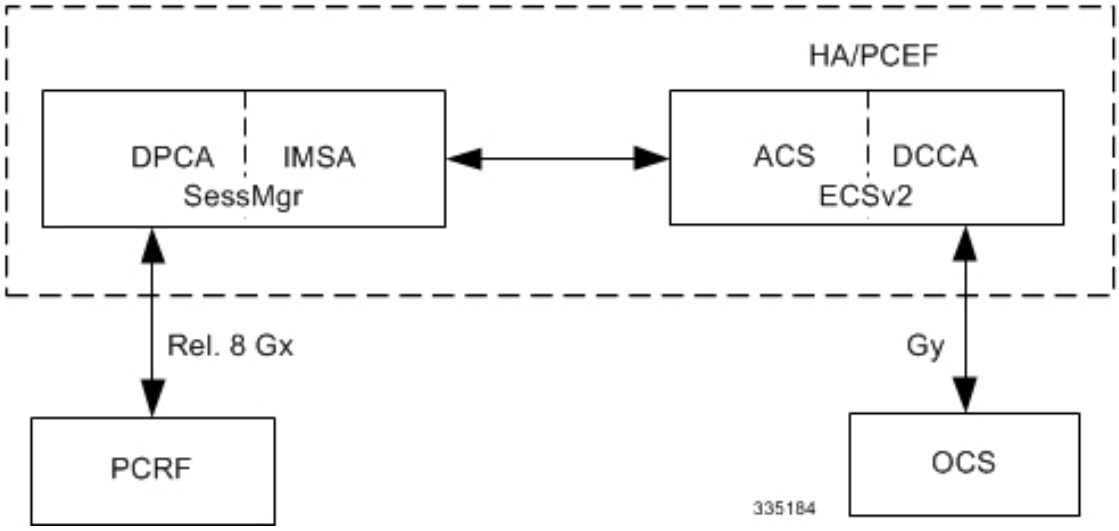
Figure 4: HA/PDSN Rel. 8 Gx PCC Logical Architecture



Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS).

The following figure shows the interaction between components within the Gateway.

Figure 5: HA/PDSN Rel. 8 Gx PCC Architecture within PCEF



License Requirements

The HA/PDSN Rel. 8 Gx 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

HA/PDSN Rel 8. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V8.3.0 (2008-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.6.0 (2009-12) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.1.1 (2008-10) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 8)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

Terminology and Definitions

This section describes features and terminology pertaining to HA/PDSN Rel. 8 Gx functionality.

Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN session.

Policy control comprises the following functions:

- Binding

- Gating Control
- Event Reporting
- QoS Control
- Other Features

Binding

In the HA/PDSN Rel. 8 Gx implementation, since there are no bearers within a MIP session the IP-CAN Bearer concept does not apply. Only authorized IP-CAN session is applicable.

Gating Control

Gating control is the blocking or allowing of packets belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is open, the packets of the related IP flows are allowed to be forwarded.

Event Reporting

Important Unconditional reporting of event triggers from PCRF to PCEF when PCEF has not requested for is not supported.

Important In the HA/PDSN Rel. 8 Gx implementation, only the AN_GW_CHANGE (21) event trigger is supported.

Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF). Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Event trigger reporting from PCEF to PCRF, and provisioning of event triggers happens at IP-CAN session level.

The Event Reporting Function (ERF) located in the PCEF, receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response to the PCRF.

QoS Control

Important In the HA/PDSN Rel. 8 Gx implementation, only authorized IP-CAN Session is supported. Provisioning of authorized QoS per IP-CAN bearer, policy enforcement for authorized QoS per QCI, and coordination of authorized QoS scopes in mixed mode are not applicable.

QoS control is the authorization and enforcement of the maximum QoS that is authorized for an SDF. In case of an aggregation of multiple SDFs, the combination of the authorized QoS information of the individual

SDFs is provided as the authorized QoS for this aggregate. QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.

QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

Supported features include:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
- Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
- Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule.

Other Features

This section describes some of the other features.

PCC Rule Error Handling

If the installation/activation of one or more PCC rules fails, the PCEF communicates the failure to the PCRF by including one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fail, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF sends the PCRF a new CCR command and includes the Charging-Rule-Report AVP. The PCEF includes the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and sets the PCC-Rule-Status to INACTIVE.

In releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

In the HA/PDSN Gx implementation, the following rule failure codes are supported:

- RATING_GROUP_ERROR (2)

- SERVICE_IDENTIFIER_ERROR (3)
- GW/PCEF_MALFUNCTION (4)
- RESOURCES_LIMITATION (5)

If the installation/activation of one or more PCC rules fails during RAR procedure, the RAA command is sent with the Experimental-Result-Code AVP set to DIAMETER_PCC_RULE_EVENT (5142).

Time of the Day Procedures

PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP-CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION_TIMEOUT event.

When installed, the PCC rule is inactive. If Rule-Activation-Time / Rule-Deactivation-Time is specified, then the PCEF sets the rule active / inactive after that time.

In releases prior to 17.0, if "Rule-Deactivation-Time" AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis. In 17.0 and later releases, if Rule-Deactivation-Time AVP is omitted in CCA/RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).

Note This behavior change is applicable only to predefined rules.

Support for Firewall Policy on Gx

The Diameter AVP "SN-Firewall-Policy" has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.

Charging Control

Important In the HA/PDSN Rel. 8 Gx implementation, offline charging is not supported.

Charging Control is the process of associating packets belonging to an SDF to a charging key, and applying online charging as appropriate. FBC handles differentiated charging of the bearer usage based on real-time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

Online charging is supported via the Gy interface. In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, then neither online nor offline charging is performed.

Supported Features:

- Provisioning of charging-related information for the IP-CAN Session
- Provisioning of charging addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses)

Important In the HA/PDSN Rel. 8 Gx implementation, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method: In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline are sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

Charging Correlation

In the HA/PDSN Rel. 8 Gx implementation, Charging Correlation is not supported. PCRF provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF in case of both uplink and downlink IP flows based on SDF filters in the PCC rule (packet rule matching).

  If no PCC rule matches the packet, the packet is dropped.
- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- Dynamic PCC Rules: Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be activated, modified, and deactivated at any time.
- Predefined PCC Rule: Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

Important A third kind of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

- Rule Name: The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- Service Identifier: The service identifier is used to identify the service or the service component the SDF relates to.
- Service Data Flow Filter(s): The service flow filter(s) is used to select the traffic for which the rule applies.
- Precedence: For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- Gate Status: The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.
- QoS Parameters: The QoS information includes the QoS class identifier (authorized QoS class for the SDF), and authorized bitrates for uplink and downlink.
- Charging Key (rating group)
- Other charging parameters: The charging parameters define whether online charging interfaces are used, on what level the PCEF will report the usage related to the rule, etc.

Important Configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

Important ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

In releases prior to 14.0, there were only 10 PCC rules that were recovered per bearer in the event of a session manager crash. In 14.0 and later releases, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

In releases prior to 17.0, when P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW.

In 17.0 and later releases, when modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW. After the response for the pending request is received from the access network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

PCC Procedures over Gx Reference Point

Request for PCC Rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:

- At IP-CAN session establishment
- At IP-CAN session modification

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

Provisioning of PCC Rules

The PCRF indicates, via the Rel. 8 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provisioning, the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.

Important In 11.0 and later releases, the maximum valid length for a charging rule name is 63 bytes. When the length of the charging rule name is greater than 63 bytes, a charging rule report with RESOURCES_LIMITATION as Rule-Failure-Code is sent. This charging rule report is sent only when the length of the rule name is lesser than 128 characters. When the charging rule name length is greater than or equal to 128 characters no charging rule report will be sent. In earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes.

Releases prior to 14.0, when PCRF has subscribed to Out of Credit trigger, on session connect when one rule validation fails and also when an Out of Credit was received from OCS for another rule, P-GW was trying to report these failures in different CCR-U to PCRF. However, the second CCR-U of Out of credit was getting dropped internally.

In 14.0 and later releases, on session connect, P-GW combines the rule failure and out of credit in the same CCR-U and sends to PCRF.

Selecting a PCC Rule for Uplink IP Packets

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP-CAN session by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP-CAN session in the order of the precedence of the PCC rules.

Important When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP-CAN session are discarded.

Selecting a PCC Rule for Downlink IP Packets

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP-CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of the IP-CAN session in the order of precedence of the PCC rules.

Important When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Downlink IP packets that do not match any PCC rule of the IP-CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated the PCEF contacts the PCRF.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP-CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

  The PCEF applies IP-CAN specific procedures to terminate the IP-CAN session. The HA/PDSN sends a MIP Revocation Request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the "Indication of IP-CAN Session Termination" procedure.
- Use of the Supported-Features AVP during session establishment to inform the destination host about the required and optional features that the origin host supports.

How it Works

This section describes how HA/PDSN Rel. 8 Gx Interface support works.

The following figure and table explain the IMS Authorization process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.

Important In 14.0 and later releases, the DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Figure 6: HA/PDSN Rel. 8 Gx IMS Authorization Call Flow

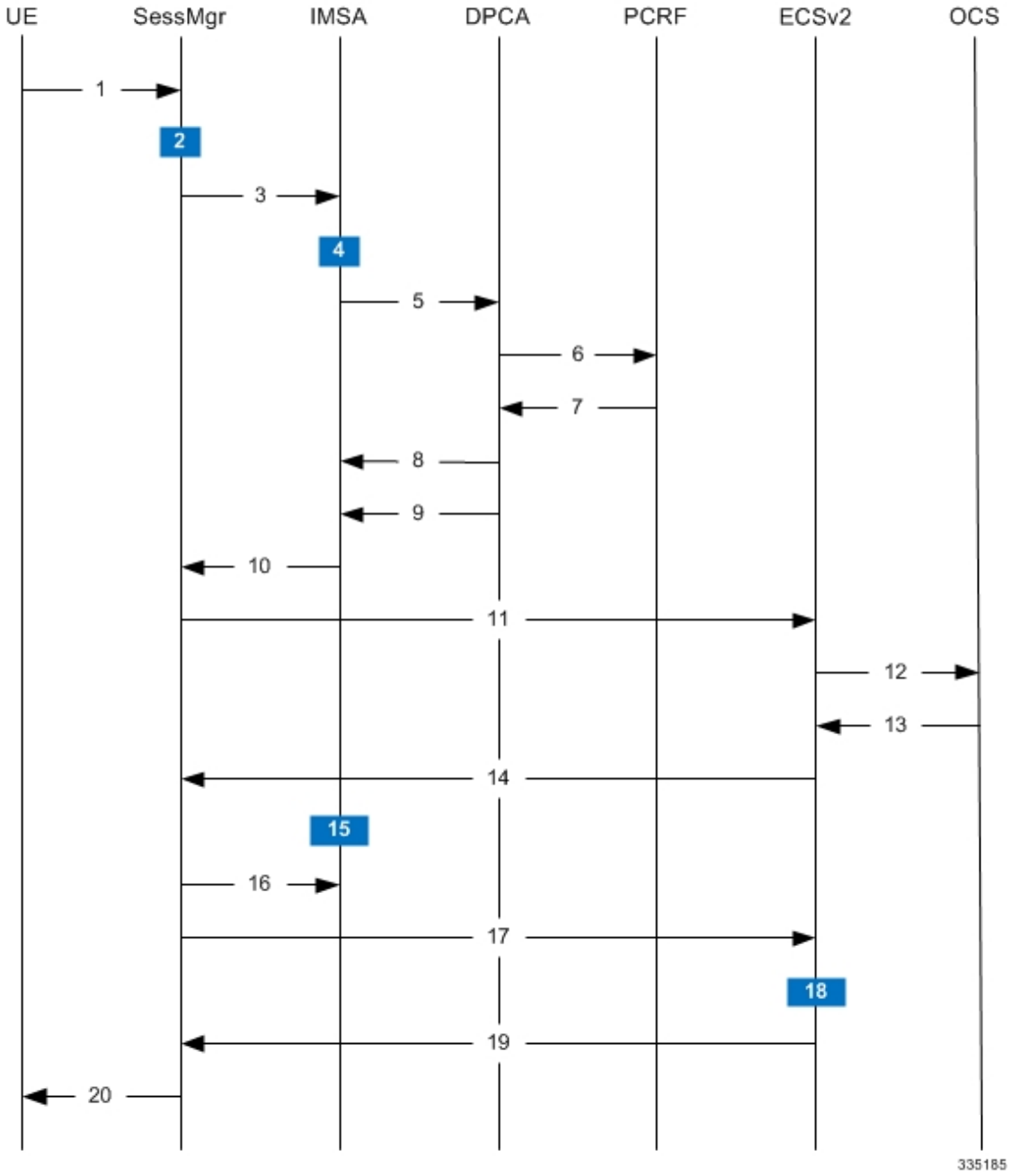


Table 3: HA/PDSN Rel. 8 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for MIP Registration Request.
2	SessMgr allocates an IP address to the UE.

Step	Description
3	SessMgr requests IMS Authorization, if IMSA is enabled for the subscriber. IMSA service can either be configured in the subscriber template, or can be received from the AAA.
4	IMSA allocates resources for the IP-CAN session, and selects the PCRF to contact based on the user's selection key (for example, round-robin).
5	IMSA requests the DPCA module to issue an auth request to the PCRF.
6	DPCA sends a CCR initial message to the selected PCRF.
7	PCRF may send preconfigured charging rules in CCA. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.
8	DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, etc. IMSA stores the information.
9	DPCA calls the callback function registered with it by IMSA.
10	PCRF-provided information common to the entire IP-CAN session (event trigger, primary/secondary OCS address, etc.) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.
11	If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The primary/secondary OCS server address, etc. are sent to the ECS from the SessMgr.
12	ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the AAA).
13	OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.
14	ECS responds to SessMgr with the response message.

Step	Description
15	SessMgr requests IMSA for the dynamic rules.
16	IMSA sends the dynamic rules to SessMgr. Note that, in 14.0 and later releases, the RAR messages are allowed before the session is established. In earlier releases, until the MIP session is established, all RAR messages from the PCRF were rejected. Also note that, in 14.0 and later releases, the RAR message is rejected and RAA is sent with 3002 result code when the recovery of dynamic rule information and audit of Session Manager are in progress. Earlier, the RAR messages were processed by DPCA even when the recovery audit was in progress.
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS.
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the MIP Session Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.

Configuring HA/PDSN Rel. 8 Gx Interface Support

To configure HA/PDSN Rel. 8 Gx Interface functionality:

1. At the context level, configure IMSA service for IMS subscribers as described in Configuring IMS Authorization Service at Context Level, on page 43.

2. Within the same context, configure the subscriber template to use the IMSA service as described in Applying IMS Authorization Service to Subscriber Template, on page 44.
3. 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 IMS Authorization Service at Context Level

Use the following example to configure IMSA service at context level for IMS subscribers:

```
configure
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    diameter origin endpoint <endpoint_name>
                    diameter dictionary <dictionary>
                    diameter request-timeout <timeout_duration>
                    diameter host-select table { 1 | 2 } algorithm
round-robin
                    diameter host-select row-precedence <precedence_value>
table { 1 | 2 } host <primary_host_name> [ realm <primary_realm_id> ] [ secondary
 host <secondary_host_name> [ realm <secondary_realm_id> ] ] [ -noconfirm ]
                    failure-handling cc-request-type { any-request |
initial-request | terminate-request | update-request } {
diameter-result-code { any-error | <result_code> [ to <end_result_code> ] } }
{ continue | retry-and-terminate | terminate }
                    exit
               exit
          diameter endpoint <endpoint_name> [ -noconfirm ]
               origin realm <realm_name>
               use-proxy
               origin host <host_name> address <ip_address>
               no watchdog-timeout
               response-timeout <timeout_duration>
               connection timeout <timeout_duration>
               connection retry-timeout <timeout_duration>
               peer <primary_peer_name> [ realm <primary_realm_name> ] address
<ip_address> [ port <port_number> ]
              peer <secondary_peer_name> [ realm <secondary_realm_name> ] address
 <ip_address> [ port <port_number> ]
               end
```

Notes:

- <*context_name*> must be the name of the context where you want to enable IMSA service.

- <*imsa_service_name*> must be the name of the IMSA service to be configured for Rel. 8 Gx interface authentication.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.
- To enable Rel. 8 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account representative.
- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- To configure the PCRF host destinations configured in the PCEF, use the **diameter host-select** CLI command.
- To configure the PCEF to use a pre-defined rule when the Gx fails, set the **failure-handling cc-request-type** CLI to **continue**. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.

Verifying the IMSA Service Configuration

To verify the IMSA service configuration:

1. Change to the context where you enabled IMSA service by entering the following command:

   context <*context_name*>

2. Verify the IMSA service configuration by entering the following command:

   show ims-authorization service name <*imsa_service_name*>

Applying IMS Authorization Service to Subscriber Template

After configuring IMSA service at the context-level, within the same context subscriber template must be configured to use the IMSA service for IMS subscribers.

Use the following example to apply IMSA service functionality to subscriber template within the context configured as described in Configuring IMS Authorization Service at Context Level, on page 43.

```
configure
   context <context_name>
      subscriber default
         encrypted password <encrypted_password>
         ims-auth-service <imsa_service_name>
         ip access-group <access_group_name> in
         ip access-group <access_group_name> out
         ip context-name <context_name>
         mobile-ip home-agent <ip_address>
         active-charging rulebase <rulebase_name>
         end
```

Notes:

- <*context_name*> must be the name of the context in which the IMSA service was configured.

- <*imsa_service_name*> must be the name of the IMSA service configured for IMS authentication in the context.
- The ECS rulebase must be configured in the subscriber template.
- For interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF as ECS group-of-ruledefs, configure the following command in the Active Charging Service Configuration Mode:

  policy-control charging-rule-base-name active-charging-group-of- ruledefs

Verifying the Subscriber Configuration

Verify the IMSA service configuration for subscriber(s) by entering the following command in the Exec CLI configuration mode:

show subscribers ims-auth-service <*imsa_service_name*>

Notes:

- <*imsa_service_name*> must be the name of the IMSA service configured for IMS authentication.

Gathering Statistics

This section explains how to gather Rel. 8 Gx 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.

Table 4: Gathering HA/PDSN Rel. 8 Gx Statistics and Information

Statistics/Information	Action to perform
Information and statistics specific to policy control in IMS Authorization service.	**show ims-authorization policy-control statistics**
Information and statistics specific to the authorization servers used for IMS Authorization service.	**show ims-authorization servers ims-auth-service**
Information of all IMS Authorization service.	**show ims-authorization service all**
Statistics of IMS Authorization service.	**show ims-authorization service statistics**
Information, configuration, and statistics of sessions active in IMS Authorization service.	**show ims-authorization sessions all**
Complete information, configuration, and statistics of sessions active in IMS Authorization service.	**show ims-authorization sessions full**
Summarized information of sessions active in IMS Authorization service.	**show ims-authorization sessions summary**
Complete statistics for active charging service sessions.	**show active-charging sessions full**
Information for all rule definitions configured in the service.	**show active-charging ruledef all**

Statistics/Information	Action to perform
Information for all rulebases configured in the system.	**show active-charging rulebase all**
Information on all group of ruledefs configured in the system.	**show active-charging group-of-ruledefs all**
Information on policy gate counters and status.	**show ims-authorization policy-gate { counters | status }** This command is no longer an option in StarOS release 11.0 and beyond.

P-GW Rel. 8 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF will report to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 8 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx 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*.

Important In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V9.5.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

Important Volume Reporting over Gx is applicable only for volume quota.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of

an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

  In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

  In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

  Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

  In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

  - immediate reporting request with monitoring key at rule level
  - immediate reporting request with or without monitoring key at session level
  - explicit disable request at rule level
  - explicit disable request at session level

  In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

  Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

  - Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.

  - Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence

enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

- Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

  For session-level reporting, the actual usage volume is compared with the usage volume threshold.

  For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

  If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

  In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

- IP CAN Session Termination: When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- PCC Rule Removal: When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

  Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- PCRF Requested Usage Report: In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.

- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

- Revalidation Timeout: In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

  In the case of standard implementation, this must be enabled by CLI configuration.

Important The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, refer to Configuring Volume Reporting over Gx, on page 27.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

Rel. 9 Gx Interface

Rel. 9 Gx interface support is available on the Cisco ASR chassis running StarOS 12.2 and later releases.

P-GW Rel. 9 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.

- If requested by the PCRF, the PCEF reports to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Important ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 9 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx 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*.

Important In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V9.5.0 (2011-01): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

Important Volume Reporting over Gx is applicable only for volume quota.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

  In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

  In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

  Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

  - Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
  - Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
  - Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

  For session-level reporting, the actual usage volume is compared with the usage volume threshold.

  For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

  If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

  In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

- IP CAN Session Termination: When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- PCC Rule Removal: When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- PCRF Requested Usage Report: In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- Revalidation Timeout: In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

  In the case of standard implementation, this must be enabled by CLI configuration.

Important The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see the Configuring Volume Reporting over Gx, on page 27 section.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

3GPP Rel.9 Compliance for IPFilterRule

This section describes the overview and implementation of 3GPP Rel.9 Compliance for IPFilterRule feature.

This section discusses the following topics for this feature:

- Feature Description, on page 57
- Configuring Rel.9 Compliant AVPs, on page 58
- Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule, on page 59

Feature Description

Currently, PCEF is 3GPP Rel. 8 compliant for IPFilterRule in Flow-Description AVP, TFT-Filter, and Packet-Filter-Content AVPs. When PCRF sends the CCA-U or RAR with Flow-Description AVP in Rel. 9 format during a network initiated dedicated bearer creation or modification, PCEF was misinterpreting the source and destination IP address, resulting in sending a wrong TFT to UE.

When the PCRF is upgraded to 3GPP Rel. 9, PCEF still sends CCR-U with Flow-Description, TFT-Filter and Packet-Filter-Content AVPs in Rel. 8 format during UE initiated secondary bearer creation or modification.

To make the PCEF 3GPP Rel. 9 compliant for Flow-Description AVP, TFT-Filter, and Packet-Filter-Content AVPs, the following changes are implemented:

- Interpretation of the source and destination IP address in IPFilterRule in Flow-Description AVP is changed to maintain 3GPP Rel.9 compliancy. That is, when a Rel. 9 Flow-Description for UPLINK is received during a network-initiated bearer creation or modification, the source IP address is interpreted as remote and the destination as local IP address.
- Traffic flow direction is interpreted from a new Diameter AVP "Flow-Direction". This new AVP indicates the direction or directions that a filter is applicable, downlink only, uplink only or both downlink and uplink (bi-directional).
- IMSA module is modified to encode TFT-Packet-Filter-Information and Packet-Filter-Information AVPs in Rel. 9 format if the negotiated supported feature is Rel. 9 and above.
- Configuration support is provided to enable Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs sent by PCEF in CCR-U. The **diameter 3gpp-r9-flow-direction** CLI command is used to enable Rel. 9 changes. When this CLI command is configured and negotiated supported feature is Rel. 9 or above (both gateway and PCRF are Rel. 9+ compliant), P-GW sends Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in Rel. 9 format.

Backward compatibility is maintained, i.e. both Rel. 8 (permit in/out) and Rel. 9 (permit out with flow-direction) formats are accepted by PCEF.

Per the 3GPP Rel. 8 standards, the IPFilterRule in Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs is sent as "permit in" for UPLINK and "permit out" for DOWNLINK direction. From 3GPP Rel. 9 onwards, the Flow-Description AVP within the Flow-Information AVP will have only "permit out" and the

traffic flow direction is indicated through Flow-Direction AVP. In 3GPP Rel. 9 format, both UPLINK and DOWNLINK are always sent as "permit out" and hence the usage of "permit in" is deprecated.

Important This feature is applicable for 3GPP Rel. 9 compliant PCEF and PCRF only when the supported feature negotiated in CCA-I is Rel. 9 or above through the **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI command.

Relationships to Other Features

This feature works only when the **diameter update-dictionary-avps** CLI command is configured as 3gpp-r9 or 3gpp-r10. That is, PCEF will send Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in 3GPP Rel. 9 format only when **diameter 3gpp-r9-flow-direction** CLI command is enabled and negotiated supported feature is Rel. 9 or above. The **diameter 3gpp-r9-flow-direction** CLI command for activating this feature must be used only after the PCRF is upgraded to Rel. 9.

Configuring Rel.9 Compliant AVPs

The following section provides the configuration commands to enable Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs.

Encoding AVPs for 3GPP Compliance

Use the following configuration commands to control PCEF from sending Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in Rel. 9 format.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter 3gpp-r9-flow-direction
end
```

- **3gpp-r9-flow-direction**: Encodes Flow-Direction, Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs based on 3GPP Rel. 9 specification. By default, this feature is disabled.
- This CLI configuration is applicable only for TFT-Filter, Packet-Filter-Content, and Flow-Description AVPs sent by PCEF in CCR-U.
- This CLI command must be used only after the PCRF is upgraded to Rel. 9.
- This CLI command works in conjunction with **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }**. When **diameter 3gpp-r9-flow-direction** is configured and negotiated supported feature is 3gpp-r9 or above, PCEF will send Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in 3GPP Rel. 9 format.

Verifying the Configuration for AVP Compliance

Use the following command to verify the configuration status of this feature.

```
show ims-authorization service name service_name
```

service_name must be the name of the IMS Authorization service configured for IMS authentication.

The "3GPP R9 Flow Direction Compliance" field can be used to determine whether this feature is enabled or disabled.

```
[local]st40# show ims-authorization service name gngp-gx
  Context: gngp
  IMS Authorization Service name: gngp-gx
  Service State: Enabled
  Service Mode: Single Interface Policy and Charging
...
  Diameter Policy Control:
   Endpoint: gx
   Origin-Realm: xyz.com
   Dictionary: r8-gx-standard
   Supported Features:
      3gpp-r9
...
   Host Selection: Table: 1 Algorithm: Round-Robin
   Host Reselection Subscriber Limit: Not Enabled
   Host Reselection Interval: Not Enabled
   Sgsn Change Reporting: Not Enabled
    3GPP R9 Flow Direction Compliance: Enabled
  Host Selection Table[1]: 1 Row(s)
   Precedence: 1
...
```

Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule

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

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

- Verify if the feature is enabled using **show ims-authorization service name** <*service_name*> CLI command. If not enabled, configure the **diameter 3gpp-r9-flow-direction** CLI command and check if it works.
- Execute **monitor protocol** command, and check if supported feature negotiated in CCA-I is Rel. 9 or above. If not, this feature will not work. Set the supported feature using **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI command.
- If the failure is still observed, obtain the following information and contact Cisco account representative for further analysis:
  - monitor protocol log with options 24 (GTPC) and 75-3 (App Specific Diameter - DIAMETER Gx/Ty/Gxx) turned on
  - logs with acsmgr enabled
  - Output of **show active-charging sessions full all** and show ims-authorization sessions CLI commands

show ims-authorization service name

A new field "3GPP R9 Flow Direction Compliance" is added to the output of this show command to indicate whether the Rel. 9 Flow-Direction change is enabled or disabled.

Rel. 10 Gx Interface

Rel. 10 Gx interface support is available on the Cisco ASR chassis running StarOS 15.0 and later releases.

This section describes the following topic:

P-GW Rel. 10 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF will report to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Important ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 10 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 10 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx 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*.

Important In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V10.5.0 (2012-01): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 10).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

Important Volume Reporting over Gx is applicable only for volume quota.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit

AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

  Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

  - Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
  - Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
  - Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage

monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

  For session-level reporting, the actual usage volume is compared with the usage volume threshold.

  For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

  If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

  In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

- IP CAN Session Termination: When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to

terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- PCC Rule Removal: When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

  Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- PCRF Requested Usage Report: In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.

- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

- Revalidation Timeout: In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

  In the case of standard implementation, this must be enabled by CLI configuration.

Important The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, refer to Configuring Volume Reporting over Gx, on page 27.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

Use of the Supported-Features AVP on the Gx Interface

The Supported-Features AVP is used during session establishment to inform the destination host about the required and optional features that the origin host supports. The client will, in the first request in a Diameter session indicate the set of features required for the successul processing of the session. If there are features supported by the client that are not advertised as part of the required set of features, the client will provide in the same request this set of optional features that are optional for the successful processing of the session. The server will, in the first answer within the Diameter session indicate the set of features that it has in common with the client and that the server will support within the same Diameter session. Any further command messages will always be compliant with the list of supported features indicated in the Supported-Features AVPs and features that are not indicated in the Supported-Features AVPs during session establishment. Features that are not advertised as supported will not be used to construct the command messages for that Diameter session. Unless otherwise stated, the use of the Supported-Features AVP on the Gx reference point will be compliant with the requirements for dynamic discovery of supported features and associated error handling.

The base functionality for the Gx reference point is the 3GPP Rel. 7 standard and a feature is an extension to that functionality. If the origin host does not support any features beyond the base functionality, the Supported-Features AVP may be absent from the Gx commands. As defined in 3GPP TS 29.229, when extending the application by adding new AVPs for a feature, the new AVPs will have the M bit cleared and the AVP will not be defined mandatory in the command ABNF.

The Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the Gx reference point, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, the Vendor-Id AVP will contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the Gx reference point, the Feature-List-ID AVP will differentiate those lists from one another.

Feature bit	Feature	M/O	Description
0	Rel8	M	This feature indicates the support of base 3GPP Rel-8 Gx functionality, including the AVPs and corresponding procedures supported by the base 3GPP Rel-7 Gx standard, but excluding those features represented by separate feature bits.
1	Rel9	M	This feature indicates the support of base 3GPP Rel-9 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 feature bit, but excluding those features represented by separate feature bits.
3	Rel10	M	This feature indicates the support of base 3GPP Rel-10 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 and Rel9 feature bit, but excluding those features represented by separate feature bits.
4	SponsoredConnectivity	O	This feature indicates support for sponsored data connectivity feature. If the PCEF supports this feature, the PCRF may authorize sponsored data connectivity to the subscriber.

In releases prior to 15.0, the Supported-Features AVP was not encoded in CCR-U messages, but it was supported only in CCR-I message. If Rel. 8 dictionary or any dictionary beyond Rel. 8 is used and PCRF does not provide Supported-Features AVP in CCA-I, then the call gets dropped.

In 15.0 and later releases, if PCEF configures Diameter dictionary as release 8, 9 or 10, then PCRF sends Supported-Features AVP so that PCEF will know what feature PCRF supports. If PCEF receives supported features lesser than or greater than requested features then supported feature will be mapped to the lower one.

Whenever the custom dictionary "dpca-custom24" is configured, the Supported-Features AVP including Vendor-Id AVP will be sent in all CCR messages.

Rule-Failure-Code AVP

The Rule-Failure-Code AVP indicates the reason that the QoS/PCC rules cannot be successfully installed/activated or enforced. The Rule-Failure-Code AVP is of type Enumerated. It is sent by the PCEF to the PCRF within a Charging-Rule-Report AVP to identify the reason a PCC Rule is being reported.

In releases prior to 15.0, only 11 rule failure codes were defined as the values for this AVP. In 15.0 and later releases, two new rule failure codes INCORRECT_FLOW_INFORMATION (12) and NO_BEARER_BOUND (15) are added. The name of the existing rule failure code 9 is changed to MISSING_FLOW_INFORMATION. For 3GPP Rel. 10, rule failure code 9 maps to GW/PCEF_MALFUNCTION.

Sponsored Data Connectivity

With Sponsored Data Connectivity, the sponsor has a business relationship with the operator and the sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

Sponsored Data Connectivity feature is introduced in Rel. 10 of 3GPP TS 29.212 specification. If Sponsored Data Connectivity is supported, the sponsor identity for a PCC rule identifies the 3rd party organization (the sponsor) who is willing to pay for the operator's charge for connectivity required to deliver a service to the end user.

The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level "SPONSORED_CONNECTIVITY_LEVEL" is added for reporting at Sponsor Connection level and two new AVPs "Sponsor-Identity" and "Application-Service-Provider-Identity" have been introduced at the rule level.

Sponsored Data Connectivity will be performed for service data flows associated with one or more PCC rules if the information about the sponsor, the application service provider and optionally the threshold values are provided by the Application Function (AF).

The provisioning of sponsored data connectivity per PCC rule will be performed using the PCC rule provisioning procedure. The sponsor identity will be set using the Sponsor-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. The application service provider identity will be set using the Application-Service-Provider-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. Sponsor-Identity AVP and Application-Service-Provider-Identity AVP will be included if the Reporting-Level AVP is set to the value SPONSORED_CONNECTIVITY_LEVEL.

When receiving the flow based usage thresholds from the AF, the PCRF will use the sponsor identity to generate a monitoring key. The PCRF may also request usage monitoring control, in this case, only the flow based usage is applied for the sponsored data connectivity. If requested, the PCEF may also report the usage to the PCRF.

A new CLI command "**diameter encode-supported-features**" has been added in Policy Control Configuration mode to send supported features with Sponsor Identity. For more information on the command, see the *Command Line Interface Reference*.

Sponsored connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also sponsored connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature will be turned off.

This feature implementation impacts only the Gx dictionary "dpca-custom15". Also note that this feature is supported only for the dynamic rules.

Volume Reporting

For Volume Reporting over Gx, PCRF generates a unique monitoring key based on sponsor identity. Since flows with different monitoring keys are treated differently, flows with sponsor ID are charged differently.

Supported Gx Features

Assume Positive for Gx

In a scenario where both the primary and secondary PCRF servers are overloaded, the PCRF returns an error to P-GW and HSGW. Current behavior for the P-GW and HSGW is to terminate the session if both primary and secondary return a failure or timeout.

This feature is developed to enhance this behavior by applying local policy on the GW to ensure that the subscriber session continues. P-GW / HSGW should implement Assume Positive feature to handle errors and based on the event type implement specific rules.

Important Use of Gx Assume Positive requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

The failure handling behavior is enhanced to ensure that the subscriber service is maintained in case of PCRF unavailability. It is also required that the GW reduces the traffic towards the PCRF when receiving a Diameter Too Busy (3004) by stopping the transmission and reception of Diameter messages (CCRs and RARs) to and from the PCRF for a configurable amount of time.

In case of any of the following failures with PCRF, the GW chooses to apply failure handling which results in subscriber termination or to allow browsing without any more policy enforcement.

- TCP link failure
- Application Timer (Tx) expiry
- Result code based failures

In 14.1 and later releases, the PCRF is allowed to fall back to Local Policy for all connection level failures, result code/experimental result code failures. Local Policy may choose to allow the subscriber for a configured amount of time. During this time any subscriber/internal event on the call would be handled from Local Policy. After the expiry of the timer, the subscriber session can be either terminated or else PCRF can be retried. Note that the retry attempt to PCRF happens only when the **timer-expiry event** is configured as **reconnect-to-server**.

The fallback support is added to the failure handling template and the local policy service needs to be associated to IMS Authorization service.

Once the local policy is applied, all PCRF enabled event triggers will be disabled. When the subscriber session is with the local-policy, the GW skips sending of CCR-T and cleans up the session locally.

For a session that was created with active Gx session, the GW sends the CCR-T to primary and on failure sends the CCR-T to the secondary PCRF. If the CCR-T returns a failure from both primary and secondary or times out, the GW cleans up the session locally.

Fallback to Local Policy is done in the following scenarios:

- Tx timer expiry
- Diabase Error

- Result Code Error (Permanent/Transient)
- Experimental Result Code
- Response Timeout

The following points are applicable only in the scenario where reconnect to PCRF is attempted.

- If the subscriber falls back to local-policy because of CCR-I failure, CCR-I will be sent to the PCRF after the timer expiry. On successful CCA-I call will be continued with PCRF or else the call will be continued with local-policy and retry-count will be incremented.
- If the subscriber falls back to local-policy because of the CCR-U failure, IMS Authorization application waits for some event change to happen or to receive an RAR from PCRF.
- In case of event change after the timer expiry, CCR-U will be sent to PCRF. On successful CCA-U message, call will be continued with PCRF or else call will be with local-policy and retry-count will be incremented.
- If RAR is received after the timer-expiry the call will be continued with the PCRF. On expiry of maximum of retries to connect to PCRF, call will be disconnected.

Default Policy on CCR-I Failure

The following parameters are supported for local configuration on P-GW. The configuration parameters are configurable per APN and per RAT Type.

The following fields for a Default Bearer Charging Rule are configurable per APN and per RAT Type:

- Rule Name
- Rating Group
- Service ID
- Online Charging
- Offline Charging
- QCI
- ARP
  - Priority Level
  - QCI
  - QVI
- Max-Requested-Bandwidth
  - UL
  - DL

Flow Description and Flow Status are not configurable but the default value will be set to Any to Any and Flow Status will be set to Enabled.

The following command level fields are configurable per APN and per RAT Type:

- AMBR
  - UL
  - DL
- QCI
- ARP

- Priority Level
- QCI
- QVI

Gx Back off Functionality

This scenario is applicable when Primary PCRF cluster is unavailable but the secondary PCRF is available to handle new CCR-I messages.

When the chassis receives 3004 result-code then back-off timer will be started for the peer and when the timer is running no messages will be sent to that peer.

The timer will be started only when the value is being configured under endpoint configuration.

Releases prior to 15.0, when the IP CAN session falls back to local policy it remained with local policy until the termination timer expires or the subscriber disconnects. Also, the RAR message received when the local-policy timer was running got rejected with the cause "Unknown Session ID".

In 15.0 and later releases, P-GW/GGSN provides a fair chance for the subscriber to reconnect with PCRF in the event of CCR failure. To support this feature, configurable validity and peer backoff timers are introduced in the Local Policy Service and Diameter endpoint configuration commands. Also, the RAR received when the local-policy timer is running will be rejected with the cause "DIAMETER_UNABLE_TO_DELIVER".

In releases prior to 17.0, rule report was not sent in the CCR messages when PCRF is retried after the expiry of validity timer. In 17.0 and later releases, rule report will be sent to the PCRF during reconnect when the CLI command **diameter encodeevent-avps local-fallback** is configured under Policy Control Configuration mode.

Support for Volume Reporting in Local Policy

This feature provides support for time based reconnect to PCRF instead of the event based for CCR-U failure scenarios.

In releases prior to 17.0, the following behaviors were observed with respect to the Volume Reporting for Local Policy:

- In the event of CCR-U failure, CCR-U was triggered to PCRF only on receiving subscriber event.
- When a CCR-U failure happened and a call continued without Gx, unreported volume is lost as the threshold is set to infinity. In next CCR-U triggered to PCRF, the cumulative volume was sent to PCRF.
- RAR was rejected with result-code diameter_unable_to_comply (3002) when the validity timer is running.

In 17.0 and later releases, with the timer-based implementation, this feature introduces the following changes to the existing behavior:

- When send-usage-report is configured, the CCR-U with usage report will be sent immediately after the local-policy timer-expiry.
- The unreported usage will not be returned to ECS. Thus, usage since last tried CCR-U will be sent to PCRF.
- RAR will be accepted and the rules received on RAR will be installed even when the timer is running.

Session can be connected to PCRF immediately instead of waiting for subscriber event, and the updated usage report can be sent.

Support for Session Recovery and Session Synchronization

Currently PCRF and ASR 5500 gateway node are in sync during normal scenarios and when Gx assume positive is not applied. However, there are potential scenarios where the PCRF might have been locally deleted or lost the Gx session information and it is also possible that due to the loss of message, gateway node and PCRF can be out of sync on the session state.

While these are rare conditions in the network, the desired behavior is to have PCRF recover the Gx session when it is lost and also to have PCRF and gateway sync the rule and session information. This feature provides functionality to ensure PCRF and gateway can sync on session information and recover any lost Gx sessions. Configuration support has been provided to enable session recovery and session sync features.

In releases prior to 17.0, the implementation is as follows:

- If the PCRF deletes or loses session information during a Gx session update (CCR-U) initiated by the gateway, PCRF will respond back with DIAMETER_UNKNOWN_SESSION_ID resulting in session termination even in the case of CCR-U.
- If the PCRF deletes or loses session information and an Rx message is received, PCRF will not be able to implement corresponding rules and will result in failure of subscriber voice or video calls.
- For subscriber's existing Rx sessions and active voice/video calls, PCRF will not be able to initiate cleanup of the sessions towards the gateway and can result in wastage of the resources in the network (dedicated bearers not removed) or can result in subscriber not able to place calls on hold or conference or remove calls from hold.
- For out of sync scenarios, PCRF and gateway could be implementing different policies and can result in wastage of resources or in poor subscriber experience. Existing behavior does not provide for a way to sync the entire session information.

In 17.0 and later releases, the gateway (GW) node and PCRF now supports the ability to exchange session information and the GW provides the complete subscriber session information to enable PCRF to build the session state. This will prevent the occurrence of the above mentioned scenarios and ensure that GW and PCRF are always in sync. The keywords **session-recovery** and **session-sync** are used with the **diameter encode-supported-features** CLI command in Policy Control Configuration mode to support Gx Synchronization.

Configuring Gx Assume Positive Feature

To configure Gx Assume Positive functionality:

Step 1 At the global configuration level, configure Local Policy service for subscribers as described in the Configuring Local Policy Service at Global Configuration Level, on page 72.

Step 2 At the global configuration level, configure the failure handling template to use the Local Policy service as described in the Configuring Failure Handling Template at Global Configuration Level, on page 73.

Step 3 Within the IMS Authorization service, associate local policy service and failure handling template as described in the Associating Local Policy Service and Failure Handling Template, on page 73.

Step 4 Verify your configuration as described in the Verifying Local Policy Service Configuration, on page 73.

Step 5 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 Local Policy Service at Global Configuration Level

Use the following example to configure Local Policy Service at global configuration level for subscribers:

```
configure
    local-policy-service  LOCAL_PCC
          ruledef 2G_RULE
               condition priority 1 apn match .*
               exit
          ruledef all-plmn
               condition priority 1 serving-plmn match .*
               exit
          actiondef 2G_UPDATE
               action priority 1 activate-ambr uplink 18000 downlink 18000
               action priority 2 reject-requested-qos
               exit
          actiondef action1
               action priority 2 allow-requested-qos
               exit
          actiondef allow
               action priority 1 allow-session
               exit
          actiondef delete
               action priority 1 terminate-session
               exit
          actiondef lp_fall
               action priority 1 reconnect-to-server
               exit
          actiondef time
               action priority 1 start-timer timer duration 10
          exit
          eventbase default
               rule priority 1 event fallback ruledef 2G_RULE actiondef time
 continue
             rule priority 2 event new-call ruledef 2G_RULE actiondef action1

            rule priority 3 event location-change ruledef 2G_RULE actiondef
 action1
               rule priority 5 event timer-expiry ruledef 2G_RULE actiondef
 lp_fall
              rule priority 6 event request-qos default-qos-change ruledef
 2G_RULE actiondef allow
               end
```

Notes:

- On occurrence of some event, event will be first matched based on the priority under the eventbase default. For the matched rule and if the corresponding ruledef satisfies, then specific action will be taken.

Configuring Failure Handling Template at Global Configuration Level

Use the following example to configure failure handling template at global configuration level:

```
configure
   failure-handling-template <template_name>
      msg-type any failure-type any action continue local-fallback
      end
```

Notes:

- When the TCP link failure, Application Timer (Tx) expiry, or Result code based failure happens, the associated failure-handling will be considered and if the failure-handling action is configured as local-fallback, then call will fall back to local-fallback mode.

Associating Local Policy Service and Failure Handling Template

Use the following example to associate local policy service and failure handling template:

```
configure
   context <context_name>
      ims-auth-service <service_name>
         associate local-policy-service <lp_service_name>
         associate failure-handling <failure-handling-template-name>
         end
```

Verifying Local Policy Service Configuration

To verify the local policy service configuration, use this command:

```
show local-policy statistics service service_name
```

Time Reporting Over Gx

This section describes the Time Reporting over Gx feature supported for GGSN in this release.

License Requirements

No separate license is required for Time Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

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*.

Feature Overview

This non-standard Time Usage Reporting over Gx feature is similar to Volume Usage Reporting over Gx. PCRF provides the time usage threshold for entire session or particular monitoring key in CCA or RAR. When the given threshold breached usage report will be sent to PCRF in CCR. This time threshold is independent of data traffic. Apart from the usage threshold breach there are other scenarios where usage report will be send to PCRF.

Important Time reporting over Gx is applicable only for time quota.

The PCEF only reports the accumulated time usage since the last report for time monitoring and not from the beginning.

If the time usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

Time usage reporting on bearer termination is supported. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

The following steps explain how Time Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the time monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the time monitoring information from PCRF, the PCEF (ECS) starts tracking the time usage.
4. For session-level monitoring, the ECS maintains the amount of time usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the time usage information per monitoring key.
6. The PCEF continues to track time usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then time monitoring does not continue in the PCEF for that IP CAN session.

Limitations

This section lists the limitations for Time Reporting over Gx in this release.

- Only integer monitoring key will be supported like Volume Reporting over Gx
- If the same monitoring key is used for both time and data volume monitoring then disabling monitoring key will disable both time and data usage monitoring.
- If the same monitoring key is used for both time and data usage monitoring and if an immediate report request is received, then both time and volume report of that monitoring key will be sent.

Usage Monitoring

Two levels of time usage reporting are supported:

- Usage Monitoring at Session Level
- Usage Monitoring at Flow Level

Usage Monitoring at Session Level

PCRF subscribes to the session level time reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL (0).

Usage Monitoring at Flow Level

PCRF subscribes to the flow level time reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow level monitoring since the rules are associated with the monitoring key and enabling or disabling of usage monitoring at flow level can be controlled by PCRF using it. Usage monitoring is supported for both predefined rules and dynamic rule definition.

Usage Monitoring for Predefined and Static Rules

If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the time being tracked for multiple rules having the same monitoring key. Similarly, usage monitoring information is sent from PCRF for the static rules also.

Usage Monitoring for Dynamic Ruledefs

If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This results in the usage monitoring being done for all the rules associated with that monitoring key.

Usage Reporting

Time usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber usage and checks if the usage threshold provided by PCRF is reached. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "CC-Time" in "Used-Service-Unit" set to track the time usage of the subscriber.
- Usage Monitoring Disabled: If PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger.
- IP CAN Session Termination: When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.
- PCC Rule Removal: When the PCRF deactivates the last PCC rule associated with a usage monitoring key, PCEF sends a CCR with the usage time for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key.

- PCRF Requested Usage Report: When PCRF provides the Usage-Monitoring-Information with the Usage-Monitoring-Report set to USAGE_MONITORING_REPORT_REQUIRED, PCEF sends the time usage information. If the monitoring key is provided by PCRF, time usage for that monitoring key is notified to PCRF regardless of usage threshold. If the monitoring key is not provided by PCRF, time usage for all enabled monitoring keys is notified to PCRF.
- Event Based Reporting: The event based reporting can be enabled through the CLI command **event-update send-usage-report events**. When an event like sgsn change, qos change or revalidation-timeout is configured under this CLI, time usage report is generated whenever that event happens.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track time usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then time usage monitoring does not continue in the PCEF for that IP CAN session.

For information on how to configure the Time Reporting over Gx feature, see the Configuring Time Reporting over Gx, on page 76.

Configuring Time Reporting over Gx

This section describes the configuration required to enable Time Reporting over Gx.

To enable Time Reporting over Gx, use the following configuration:

```
configure
     active-charging service <ecs_service_name>
          rulebase <rulebase_name>
               action priority <priority> dynamic-only ruledef <ruledef_name>
 charging-action <charging_action_name> monitoring-key <monitoring_key>
               exit
          exit
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    event-update send-usage-report [ reset-usage ]
                    end
```

Notes:

- The configuration for enabling Time Reporting over Gx is same as the Volume Reporting over Gx configuration. If a time threshold is received from PCRF then Time monitoring is done, and if a volume threshold is received then Volume monitoring will be done.
- The maximum accepted monitoring key value by the PCEF is 4294967295. If the PCEF sends a greater value, the value is converted to an Unsigned Integer value.
- The **event-update** CLI enables time usage report to be sent in event updates. The optional keyword **reset-usage** enables to support delta reporting wherein the usage is reported and reset at PCEF. If this option is not configured, the behavior is to send the time usage information as part of event update but not reset at PCEF.

Support for Multiple Active and Standby Gx Interfaces to PCRF

In the earlier Gx implementation, Diameter Policy Control Application has the limitation to mandatorily configure hosts as part of IMS Authorization service or associate a host template and select the hosts to be communicated for each subscriber session. Since the peer selection can happen at diabase and application need not select any hosts, this feature is developed to remove the restrictions imposed in the application and allow diabase to pick the peers in a round robin fashion. In addition, this feature will take care of peer selection at diabase even when the hosts picked by application are not active. This change in behavior is controlled through the CLI command "**endpoint-peer-select**" as the default behavior is to drop the call if the server discovery fails at application.

When the call is established, IMSA module checks the host selection table/prefix table/host template associated in IMSA service to pick the primary and secondary peers to be contacted. If no host table/prefix table/host template is configured or none of the rows in prefix table are matching or the hosts selected by IMSA are inactive, then based on the CLI configuration the control is given to diabase module which will select the peers in a round robin fashion or terminate the call based on the CLI configuration.

When the CCR message results in a diabase error/Tx expiry/response timeout, then IMSA will let diabase select an alternate route by excluding the peer which resulted in the failure and switch to the peer if the lookup is successful.

When CCR/CCA message is exchanged with the directly connected host selected by diabase and RAR message is received from new host, then IMSA will skip host configuration check and let further communication to happen with the new host. If the directly connected host is selected by application during call establishment, then IMSA will check if the new host is the secondary server per application. When the CCR/CCA message is exchanged with indirectly connected host through DRA which is picked by diabase and RAR message is received from same host through another DRA, then IMSA will skip host configuration check and let further communication to happen with the same host through the new DRA. If the DRA is selected by application during call establishment, then IMSA will check if the new DRA is the secondary server per application. Even if RAR message is received from different host though another DRA, IMSA will skip host configuration check and let further communication to happen with the new host through the new DRA.

Configuring Diameter Peer Selection at Diabase in Failure Scenarios

The following configuration enables diabase to select the Diameter peers when IMSA fails.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            endpoint-peer-select [ on-host-select-failure |
on-inactive-host ]
            { default | no } endpoint-peer-select
            end
```

Notes:

- This command is used to perform server selection at diabase when the hosts could not be selected by IMS Authorization application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts.
- **on-host-select-failure**: Specifies to perform server selection at Diabase when the hosts could not be selected by IMS Authorization application.

- **on-inactive-host**: Specifies to perform server selection at diabase when the hosts selected by application are inactive.
- This CLI command is added in policy control configuration mode to maintain backward compatibility with the old behavior of terminating the call when server selection fails at IMS Authorization application.

Support for Multiple CCR-Us over Gx Interface

ASR 5500 node earlier supported only one pending CCR-U message per session over Gx interface. Any request to trigger CCR-U (for access side updates/internal updates) were ignored/dropped, when there was already an outstanding message pending at the node. PCEF and PCRF were out of synch if CCR-U for critical update was dropped (like RAT change/ULI change).

In 17.0 and later releases, ASR 5500 supports multiple CCR-U messages at a time per session through the use of a configurable CLI command "**max-outstanding-ccr-u**" under IMS Authorization Service configuration mode. That is, this CLI will allow the user to configure a value of up to 12 as the maximum number of CCR-U messages per session.

The CLI-based implementation allows sending request messages as and when they are triggered and processing the response when they are received. The gateway does re-ordering if the response messages are received out of sequence.

To support multiple outstanding messages towards PCRF, the following items should be supported:

- Allowing IMSA to send multiple CCR-U messages – This can be achieved through the use of **max-outstanding-ccr-u** command in the IMS Authorization Service configuration mode.
- Queuing of response message for ordering – DPCA should parse the received message irrespective of order in which they are received. IMSA will check whether to forward the response to session manager or queue it locally.
- Peer switch – When multiple CCR-Us are triggered, IMSA will start Tx timer for each request sent out. On first Tx expiry, IMSA/DPCA will do peer switch. That is, IMSA will stop all other requests' Tx timers and switch to secondary peer (if available) or take appropriate failure handling action.
- Failure handling – On peer switch failure due to Tx expiry, DPCA will take failure handling action based on the configuration present under ims-auth-service.
- Handling back pressure – In case of multiple CCR-Us triggered to Primary PCRF and due to Tx timeout all the messages are switched to Secondary PCRF. If Secondary server is already in backpressure state, then IMSA will put first message in the backpressure queue and once after message is processed next pending request will be put into BP queue.
- Volume reporting – In case of multiple CCR-Us for usage report is triggered (for different monitoring keys) and failure handling is configured as "**continue send-ccrt-on-call-termination**", on first Tx timeout or response timeout, usage report present in all the CCR-Us will be sent to ECS. All the unreported usage will be sent in CCR-T message when the subscriber goes down. If "**event-update send-usage-report**" CLI is present, then there are chances of reporting usage for same monitoring key in multiple CCR-Us.

Though the **max-outstanding-ccr-u** CLI command supports configuring more than one CCR-U, only one outstanding CCR-U for access side update is sent out at a time and multiple CCR-Us for internal updates are sent.

These are the access side updates for which CCR-U might be triggered:

- Bearer Resource Command
- Modify Bearer Request (S-GW change, RAT change, ULI change)
- Modify Bearer Command

These are the following internal updates for which CCR-U is triggered:

- S-GW restoration
- Bearer going down (GGSN, BCM UE_Only)
- ULI/Timezone notification
- Default EPS bearer QoS failure
- APN AMBR failure
- Charging-Rule-Report
- Out of credit / reallocation of credit
- Usage reporting
- Tethering flow detection
- Access network charging identifier

Configuring Gateway Node to Support Back-to-Back CCR-Us

The following configuration enables or disables the gateway to send multiple back-to-back CCR-Us to PCRF.

```
configure
   context  context_name
      ims-auth-service   service_name
         policy-control
            [ default ] max-outstanding-ccr-u value
            end
```

Notes:

- *value* must be an integer value from 1 through 12. The default value is 1.

Support for RAN/NAS Cause IE on Gx Interface

New supported feature "Netloc-RAN-NAS-Cause" has been introduced to be in compliance with the Release 12 specification of 3GPP TS 29.212. This feature is used to send detailed RAN and/or NAS release cause code information from the access network to PCRF. It requires that the NetLoc feature is also supported.

Important This feature can be enabled only when the NetLoc feature license is installed.

A new Diameter AVP "RAN-NAS-Release-Cause" will be included in the Charging-Rule-Report AVP and in CCR-T for bearer and session deletion events respectively, when the NetLoc-RAN-NAS-Cause supported feature is enabled. This AVP will indicate the cause code for the subscriber/bearer termination.

Configuring Supported Feature Netloc-RAN-NAS-Cause

The following configuration enables the supported feature "Netloc-RAN-NAS-Cause".

```
configure
    context  context_name
         ims-auth-service  service_name
              policy-control
                 diameter encode-supported-features netloc-ran-nas-cause

                   end
```

Notes:

- **netloc-ran-nas-cause**: Enables the Netloc-RAN-NAS-Cause feature. By default, this supported feature will be disabled.
- If the supported features "netloc-ran-nas-code" and "netloc" are enabled, then netloc-ran-nas-cause code will be sent to PCRF.

To disable this supported feature, use the following command:

```
[ default | no ] diameter encode-supported-features
```

Support ADC Rules over Gx Interface

In this release, P-GW will use Application Detection and Control (ADC) functionality over Gx as defined in the Release 11 specification of 3GPP standard.

ADC extension over Gx provides the functionality to notify PCRF about the start and stop of a specific protocol or a group of protocols, and provide the possibility to PCRF that with the knowledge of this information, change the QoS of the user when the usage of application is started and until it is finished.

The provision of ADC information is done through the ADC rule, the action initiated by PCRF is done through the PCC rule.

ADC rules are certain extensions to dynamic and predefined PCC rules in order to support specification, detection and reporting of an application flow. These rules are installed (modified/removed) by PCRF via CCA-I/CCA-U/RAR events. ADC rules can be either dynamic PCC or predefined PCC rules, and the existing attributes of dynamic and predefined rules will be applicable.

Dynamic PCC rule contains either traffic flow filters or Application ID. When Application ID is present, the rule is treated as ADC rule. Application ID is the name of the ruledef which is pre-defined in the boxer configuration. This ruledef contains application filters that define the application supported by P2P protocols.

PCEF will process and install ADC rules that are received from PCRF interface, and will detect the specified applications and report detection of application traffic to the PCRF. PCRF in turn controls the reporting of application traffic.

PCEF monitors the specified applications that are enabled by PCRF and generates Start/Stop events along with the Application ID. Such application detection is performed independent of the bearer on which the ADC PCC rule is bound to. For instance, if ADC rule is installed on a dedicated bearer whereas the ADC traffic is received on default bearer, application detection unit still reports the start event to PCRF.

Important ADC Rule support is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

In support of this feature, the following Diameter AVPs are newly added to the Charging-Rule-Definition AVP, which PCEF will receive from PCRF.

- TDF-Application-Identifier: It references the application detection filter which the PCC rule for application detection and control in the PCEF applies. The TDF-Application-Identifier AVP references also the application in the reporting to the PCRF.
- Redirect-Information: This indicates whether the detected application traffic should be redirected to another controlled address.
- Mute-Notification: This AVP is used to mute the notification to the PCRF of the detected application's start/stop for the specific ADC/PCC rule from the PCEF.

- Application Detection Information: If Mute-Notification AVP is not enclosed with charging rule report and APPLICATION_START/APPLICATION_STOP event trigger is enabled then PCEF will send Application-Detection-Information to PCRF corresponding TDF-Application-Identifier.

In addition, these two new event triggers "APPLICATION_START" and "APPLICATION_STOP" are generated for reporting purpose.

Limitations

The limitations for the ADC over Gx feature are:

- ADC does not support group of ruledefs.
- Registration of the duplicate application IDs are not supported.
- Readdress/Redirection for P2P flows will not be supported.
- Redirection happens only on transactions of GET/Response.
- Port based, IP Protocol based, and URL based applications are not supported.
- Pre-configured options (precedence, redirect-server-ip) for dynamic ADC rules are not supported.
- Simultaneous instances of an application for the same subscriber are not distinguished.
- Flow recovery is not supported for application flows.

Configuring ADC Rules over Gx

The following configuration enables ADC rules over Gx interface.

```
configure
   context  context_name
      ims-auth-service   service_name
         policy-control
            diameter encode-supported-features adc-rules
            end
```

Notes:

- The keyword "**adc-rules**" will be available only when the feature-specific license is configured.
- For ADC 6th bit of supported feature will be set.

To disable the support for ADC Rules over Gx, use the following command:

```
[ default | no ] diameter encode-supported-features
```

GoR Name Support in TDF-Application-Identifier

ASR 5500 supports dynamic rules to be installed with GoR name as TDF-Application-Identifier. When ADC rule is installed as a dynamic rule from PCRF, the TDF-Application-Identifier can include the GoR name pre-configured in the P-GW.

If the ADC feature is enabled, PCRF can send TDF-Application-Identifier as the name of GoR predefined in the P-GW configuration.

- When dynamic charging-rules with the Charging-Rule-Definition AVP are activated from PCRF, the PCRF can specify the GoR name configured in ECS as TDF-Application-Identifier.
- When dynamic charging-rules with the Charging-Rule-Definition AVP are activated, the PCRF can remove or modify the rule through the Charging-Rule-Definition using RAR. During rule activation or modification, the PCRF can add, modify or remove the charging-rule attributes of the rule.

The configuration changes for TDF-Application-Identifier from PCRF are listed below:

- A non-ADC dynamic rule can be changed to ADC dynamic rule by sending TDF-Application-Identifier AVP with relevant ruledef or GoR name.

  ADC dynamic rule cannot be changed to non-ADC dynamic rule.

- The following AVPs will be modified and applied when received from PCRF:
  - Precedence
  - Rating-Group/Service-Identifier/Sponsor-Identity (mandatory depending on the Reporting-Level)
  - Metering-Method
  - Online/Offline
  - QoS-Information
  - Monitoring-Key
  - Redirect-Information
- Dynamic route will be updated for all protocols of rules that are part of TDF-Application-Identifier GoR.
- Any change in dynamic rule priority or TDF-Application-Identifier value will lead to sending of APP-START and APP-STOP event notifications as new rule match. If an APP-START notification was sent already before rule modification, the corresponding APP-STOP notification will not be sent.
- Runtime deletion of associated GoR will take immediate effect and APP-STOP notification will not be sent if an APP-START was already sent. Addition of GoR at service level will need to have rules to be re-installed for the new addition to take effect for both dynamic and predefined ADC rules.

ADC Mute Customization

Earlier, 3GPP ADC over Gx did not support application MUTE status change. Once the application was muted, it was not possible to unmute it. From release 21.1, this feature introduces custom MUTE/UNMUTE functionality. ASR 5500 PCEF now supports customization to control reporting of the Application Detection Information CCRUs. For this, an AVP has been introduced with two possible values - custom MUTE and custom UNMUTE.

- A Gx message might contain both Standards based MUTE and the custom MUTE.
- Standards based MUTE is given preference over the custom MUTE/UNMUTE.
- A dynamic ADC rule can be installed and modified with a custom MUTE.
- Custom-Mute-Notification AVP can be sent by the PCRF in CCA-I and RAR.
- A dynamic ADC rule can be modified with a custom UNMUTE.
- On a custom MUTE for a given dynamic ADC rule, PCEF sends a single APPLICATION_START/ APPLICATION_STOP response for the entire application traffic rather the per flow APPLICATION_START /APPLICATION_STOP response.
- On a custom MUTE for a given dynamic ADC rule, if no APPLICATION_START has been sent prior to the custom MUTE then a single APPLICATION_START is sent on the next flow packet that hits the dynamic rule.
- On a custom MUTE for a given dynamic rule, the APPLICATION_START response is sent with the flow's 5-tuple information.

- On a custom MUTE for a given dynamic rule, the APPLICATION_START response is sent with TDF-Application-Instance-Identifier = 0.
- On a custom MUTE for a given dynamic rule, a single APPLICATION_STOP is sent when the last flow associated with the given dynamic rule is terminated. Such an APPLICATION_STOP will not contain 5-tuple information of the last flow and is sent with TDF-Application-Instance-Identifier = 0.
- On a custom UNMUTE for a given dynamic rule, APPLICATION STARTs response is matched with the given dynamic rule and then sent to all the forthcoming flows.
- There is no change in behavior for a custom UNMUTE, which has not been custom MUTED or standard MUTED before UNMUTING. APPLICATION_STARTs and APPLICATION_STOPs is continued to be sent per flow as before.
- On a custom UNMUTE, PCEF sends an APPLICATION_STOP each for all flows that terminate then onwards.
- A given dynamic rule is recovered in both SR and ICSR including the Custom MUTE/UNMUTE status. The APPLICATION_START status for a given dynamic rule is check-pointed and recovered. This ensures that an extra APPLICATION_START is not sent to the PCRF post recoveries.

Enhancement to the ADC Custom Mute/Unmute Functionality

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvd00699
Related Changes in This Release	Not Applicable
Related Documentation	Command Line Interface Reference SAEGW Administration Guide

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
Modified in this release.	21.2	April 27, 2017

Feature Changes

The "ADC mute customization" feature introduced custom MUTE/UNMUTE functionality to control reporting of the Application Detection Information CCRUs. With the custom MUTE PCRF AVP, the PCRF informed P-GW when to disable/enable the ADC application notifications.

This feature enhances the "ADC mute customization" feature further and report the flow activities between custom mute and unmute events. P-GW learns the flow activities between custom mute events and then reports them to PCRF after the custom unmute event has occurred on the ADC rule. It minimizes the ADC application start and stop mechanism in standard ADC mute and unmute case.

A new CLI command has been implemented at the rulebase, which when configured, reports ADC application start and stop notifications only once per rule. This helps in reducing messaging flows towards the PCRF.

Limitations

Following are the limitations of this feature:

- P-GW stores maximum of 12 learned flows per ADC rule. Once the limit 12 has been reached, P-GW forgets the oldest flow and learns about the latest flow. Once P-GW receives the custom unmute event, it notifies the PCRF about the learned notifications. P-GW sends application stop notification, if the application start notification for the flow is sent.
- Flow information stored for sending the application start notifications to the PCRF after the event of the custom unmute is not recovered.
- On LTE to WiFi handover, the values received from the PCRF for custom mute or custom unmute per ADC dynamic rule gets applied in the new RAT. If there is no value received in the handover context, the previous values before the RAT change are retained for all the ADC dynamic rules which are present.
- If the CLI command **adc notify** is enabled, then the single ADC application start and stop notification is notified to the PCRF. If there are multiple flows which match the same ADC dynamic rule, only one application start and stop notification is sent to the PCRF.
- This feature is implemented only for the dynamic rules.

How it Works

Following is the sequence of events that occur when P-GW receives packet and ADC rule event occurs from PCRF:

1. Packet reaches the ECS rule matching engine.
2. The rule matching engine checks if the ADC dynamic rule is matched. It also checks if the custom mute is applied through the PCRF or rulebase level CLI. A single application start notification is sent, if not sent earlier.
3. For all the subsequent flows matching the same ADC rule, application start notification is stored. These notifications are sent in the CCRU after the custom unmute event is received.

Following are some important points:

- The values received from the PCRF has the highest priority. Hence, standard mute has the highest priority than custom-mute/custom-unmute. The CLI *adc notify once* has the least priority.
- If the CLI **adc notify once** is configured at the rulebase, the converse **no adc notify** does not have any impact. To converse the CLI impact, do either of the following tasks:

- Switch the rulebase in which the CLI **adc notify once** is not configured.
- Send the "custom unmute" for that particular dynamic rule.

Configuring the ADC Notifications

The new CLI command, **adc notify**, has been added to the active charging service mode.

When this CLI is configured, a single application start or application stop notification for the ADC flow matching per rule is sent to the PCRF. If this CLI is configured and the PCRF sends the custom mute notification, then the PCRF notification takes precedence over the standard behavior for reporting the notification.

The default value of this keyword is false. If this CLI is not configured, then no action is taken on sending the ADC notifications.

To enable or disable the feature, enter the following commands:

```
configure
  active-charging service <service_name>
    rulebase <rulebase_name>
      [no] adc notify [once]
      end
```

For configuring single notification use the following command:

```
adc notify once
```

Notes:

- **no:** Disables the ADC notifications and ADC notifications are sent as per default behavior.
- **adc:** Configures the ADC notifications.
- **notify:** Configures the application notification. If this keyword is not configured, ADC notifications are sent as per default behavior.
- **once:** Configures the application notification only once. PCRF takes the priority.

Support for TAI and ECGI Change Reporting

This section describes the overview and implementation of TAI and ECGI Change Reporting feature.

This section discusses the following topics for this feature:

- Feature Description, on page 85
- How it Works, on page 86
- Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature, on page 87

Feature Description

For activating User Location Reporting for a UE over Gx, PCRF sends RAR/CCA with the "USER_LOCATION_CHANGE (13)" event trigger. On receiving this event trigger, P-GW typically sends

Change Reporting Action (CRA) Information Element (IE) with "Start Reporting" towards MME to enable the Location-Change reporting for the UE in MME.

In the current architecture, the "USER_LOCATION_CHANGE (13)" trigger is used to report the changes in User Location Information (ULI), Tracking Area Identity (TAI) and E-UTRAN Cell Global Identifier (ECGI). In release 19.4 and beyond, separate event triggers TAI_CHANGE (26) and ECGI_CHANGE (27) are supported for reporting the changes in TAI and ECGI correspondingly. CLI changes are done to display the new event triggers in show configuration commands.

Important For TAI reporting to work, the **diameter map usage-report** CLI command must be configured in Policy Control configuration mode to use the value 33.

PCRF subscribes to the CRA event for reporting change of TAI and ECGI. P-GW sends event trigger in CCR-U only if it is subscribed by PCRF. When PCRF installs the event trigger for ECGI Change and/or TAI change, any change in ECGI and TAI (based on installed triggers) is reported.

The TAI and ECGI Change Reporting feature complies with 3GPP TS 29.212 v9.7.0. This feature is supported on Gx interface so that UE can be tracked on ECGI/TAI change and reported to PCRF. For more information on the User Location Information Reporting feature, see the administration guide for the product that you are deploying.

In releases prior to 19.3, the CRA event included in Create Session Response (CSRsp) for reporting location change was always set to START_REPORTING_ECGI (4).

In release 19.4 and beyond, the CRA value varies based on the event triggers received from PCRF.

Change Reporting Support Indication (CRSI) and ULI are also supported in Bearer Resource Command.

P-GW sends the ULI received in Delete Bearer Command from MME to PCRF when the corresponding Delete Bearer Response is received. When the ULI is included in both Delete Bearer Command and Delete Bearer Response, the ULI in Delete Bearer Response is sent to the PCRF. In the absence of ULI in Delete Bearer Response, then the ULI received in Delete Bearer Command is sent to PCRF.

Relationships to Other Features

This feature has a dependency on USAGE_REPORT value of Event-Trigger AVP. This feature works only when the value of USAGE_REPORT is set to 33. This can be achieved using the **diameter map usage-report** CLI command in Policy Control configuration mode.

How it Works

P-GW sends Event Trigger value based on the event trigger detected by P-GW in CCR-U. P-GW sends Event Trigger and ULI Type in CCR-U to PCRF as per the following table.

Event Trigger from PCRF	CRA Value	Event Detected at P-GW	What to Inform PCRF
ULI_CHANGE	6	TAI_CHANGE or ECGI_CHANGE	Event Trigger: ULI_CHANGE ULI Type: TAI + ECGI
TAI_CHANGE	3	TAI_CHANGE	Event Trigger: TAI_CHANGE ULI Type: TAI

Event Trigger from PCRF	CRA Value	Event Detected at P-GW	What to Inform PCRF
ECGI_CHANGE	4	ECGI_CHANGE	Event Trigger: ECGI_CHANGE ULI Type: ECGI
ULI_CHANGE + TAI_CHANGE	6	TAI_CHANGE	Event Trigger: ULI_CHANGE+ TAI_CHANGE ULI Type: TAI+ECGI
ULI_CHANGE + ECGI_CHANGE	6	ECGI_CHANGE	Event Trigger: ULI_CHANGE + ECGI_CHANGE ULI Type: TAI+ECGI
ULI_CHANGE + TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI has changed	Event Trigger: ULI_CHANGE + TAI/ECGI CHANGE ULI_Type: TAI+ECGI
TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI has changed	Event Trigger: TAI_CHANGE/ECGI_CHANGE ULI_Type: TAI+ECGI
For combinations not specifically mentioned above	6		Event Trigger: ULI_CHANGE ULI_Type: TAI+ECGI

Limitations

TAI and ECGI Change Reporting feature is supported only when ***diameter map usage-report*** CLI command is configured as 33.

Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature

This section provides information regarding show commands and/or their outputs in support of the TAI and ECGI Change Reporting feature.

show ims-authorization sessions full all

The following fields are added to the output of this show command in support of this feature:

- TAI-Change - Displays this event trigger when TAI has changed for a subscriber session.
- ECGI-Change - Displays this event trigger when ECGI has changed for a subscriber session.

show ims-authorization service statistics all

The following statistics are added to the output of this show command in support of this feature:

- TAI Change - Displays the total number of times P-GW has reported TAI_CHANGE (26) event trigger to PCRF.
- ECGI Change - Displays the total number of times P-GW has reported ECGI_CHANGE (27) event trigger to PCRF.

Location Based Local-Policy Rule Enforcement

This section describes the overview and implementation of Location-based Local-Policy (LP) Rule Enforcement feature.

This section discusses the following topics for this feature:

Feature Description

This feature is introduced to activate different predefined rules for different E-UTRAN Cell Global Identifiers (ECGIs) when the subscriber is connected to a corporate APN. The subscriber has to explicitly bring down the connection with the corporate APN and re-establish session with Internet APN when out of the company area. It is assumed that corporate APN does not use PCRF and use only Local-Policy. In this case, all calls matching the APN is directed to the Local-Policy.

Important For this feature to work, the license to activate Local-Policy must be configured. For more information on the licensing requirements, contact your local Cisco account representative.

To activate different predefined rules for ECGI, Local-Policy configurations are enhanced to support:

- Configuration and validation of a set of ECGIs
- Installation of ECGI_CHANGE event trigger through Change Reporting Action (CRA) event
- Detection of ECGI_CHANGE event

This feature supports the following actions to be applied based on the ECGI match with Local-Policy ruledef condition:

- Enable a redirect rule on ECGI_CHANGE event notification when the ECGI belongs to a certain group
- Enable a wild card rule for any other ECGIs

Relationships to Other Features

This feature has a dependency on TAI and ECGI Change Reporting feature, which provides a framework to report ECGI-Change from session manager module to IMSA/Local-Policy module.

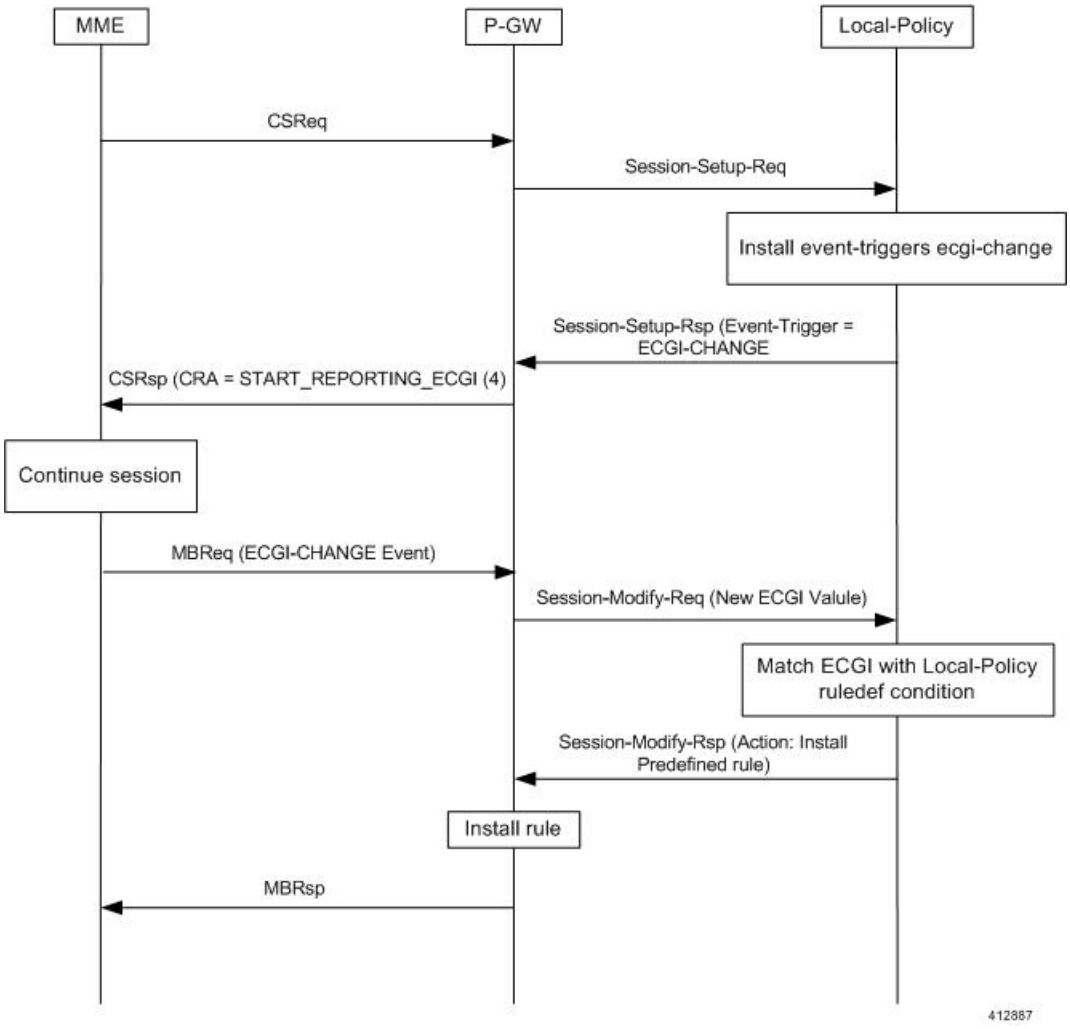
How it Works

This section describes how the Local Policy Rule selection and enforcement happens based on ECGI-CHANGE event trigger.

Flows

The following figure describes how the ECGI-CHANGE event is being handled in Local-Policy, MME and P-GW.

Figure 7: ECGI-CHANGE Event Handling



When a new call is established the ECGI-CHANGE event trigger is sent from Local-Policy. P-GW requests the MME for ECGI reporting by sending CRA of 4 in Create Session Response (CSRsp). MME informs the P-GW of ECGI Change through Change Notification request/Modify Bearer Request (MBReq). Local-Policy configuration at P-GW will handle the ECGI-CHANGE event and take appropriate action based on the ECGI group to which the new ECGI belongs. One action could be to activate a certain redirect rule when ECGI belongs to a certain group, and other action could be to enable a wildcard rule for any other ECGI.

Limitations

This section identifies the known limitations of this feature.

- ECGI Change detection and triggering is a pre-requisite for this feature.
- This feature is supported for Local-Policy-only (lp-only) mode wherein, all requests and responses within a particular APN directly go to Local-Policy without contacting PCRF. That is, this feature does not work in Local-Policy fallback mode and dual mode wherein both PCRF and Local-Policy co-exist.

Configuring Location Based Local Policy Rule Enforcement Feature

This section provides the configuration of parameters within Local-Policy to enable rule enforcement based on ECGI-Change event notification.

Configuring ECGI Change Trigger

Use the following configuration to install ECGI-Change trigger from local-policy.

```
configure
   local-policy-service service_name
      actiondef actiondef_name
         action priority priority event-triggers ecgi-change
         exit
      eventbase default
         rule priority priority event new-call ruledef ruledef_name actiondef
 actiondef_name [ continue ]
         end
```

Notes:

- **priority** *priority*: Specifies a priority for the specified action. *priority* must be unique and an integer from 1 to 2048.
- **ecgi-change**: This keyword specifies to install ECGI-CHANGE event trigger. If enabled, ECGI-CHANGE event trigger is sent from local-policy.
- This CLI command is configured in local-policy if operator wants to enable ECGI-Change notification in MME by sending a CRA value.

Applying Rules for ECGI-Change Event

Use the following configuration to enable ECGI Change detection and take specific action for ECGI-CHANGE event reported by MME.

```
configure
   local-policy-service service_name
      eventbase eventbase_name
         rule priority priority event ecgi-change ruledef ruledef_name
actiondef actiondef_name [ continue ]
         end
```

Notes:

- **priority** *priority*: Specifies a priority for the specified rule. *priority* must be unique and an integer from 1 to 2048.

- **ruledef** *ruledef_name*: Associates the rule with a specific ruledef. *ruledef_name* must be an existing ruledef within this local QoS policy service.
- **actiondef** *actiondef_name*: Associates the rule with a specific actiondef. *actiondef_name* must be an existing actiondef within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.
- **ecgi-change**: Enables a new event to detect ECGI-CHANGE and applies specific action for the ECGI-CHANGE event as defined in actiondef configuration.
- **continue**: Subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

Enforcing Local Policy Rule based on ECGI Value

Use the following configuration to apply rules based on the ECGI value received in ECGI-Change event notification by MME.

```
configure
   local-policy-service service_name
      ruledef ruledef_name
         condition priority priority ecgi mcc mcc_num mnc mnc_num eci { eq |
ge | gt | le | lt | match | ne | nomatch } regex | string_value | int_value |
 set }
         end
```

Notes:

- **priority** *priority*: Specifies a priority for the specified condition. *priority* must be unique and an integer from 1 to 2048.
- **ecgi mcc** *mcc_num* **mnc** *mnc_num* **eci**: Configures ECGI with values for MCC, MNC and ECI.
  - **mcc** *mcc_num* : MCC is a three digit number between 001 to 999. It is a string of size 3 to 3.
  - **mnc** *mnc_num* : MNC is a two/three digit number between 01 to 999. It is a string of size 2 to 3.
  - **eci**: ECI is a hexadecimal number between 0x1 to 0xfffffff. It is a string of size 1 to 7.
- This CLI command is configured in local-policy if operator wants to take specific action based on certain ECGI value received in ECGI-Change event notification by MME.

Verifying the Location Based LP Rule Enforcement Configuration

Use the following command to verify the configuration of this feature.

```
show configuration context
```

Important This feature is supported for Local-Policy-only mode wherein, all requests and responses within a particular APN directly go to Local-Policy without contacting PCRF.

Here is an example configuration for this feature.

```
configure
   context source
```

```
      apn corporate-apn
         ims-auth-service LocalPolicy_1
      exit
   exit
end

configure
   local-policy-service LocalPolicy_1
      ruledef any-imsi
         condition priority 1 imsi match *
      exit
      ruledef ecgi-group
         condition priority 1 ecgi mcc 123 mnc 456 eci eq ffff
      exit
      actiondef ecgi-trigger
         action priority 1 event-triggers ecgi-change
      exit
      actiondef ecgi-redirect-rule
         action priority 1 activate-rule namerule-1
      exit
      eventbase default
        rule priority 1 event new-call ruledef any-imsi actiondef ecgi-trigger

         rule priority 2 event ecgi-change ruledef ecgi-group actiondef
ecgi-redirect-rule
         rule priority 3 event location-change ruledef ecgi-group actiondef
 ecgi-redirect-rule
      exit
   exit
end
```

Monitoring and Troubleshooting the Location Based LP Rule Enforcement Feature

This section provides information regarding show commands and/or their outputs in support of the Location Based Local Policy Rule Enforcement feature.

Use the following CLI commands to troubleshoot if any issue is encountered with this feature.

show configuration context

logging filter active facility local-policy level debug

show local-policy statistics

show active-charging sessions full

show local-policy statistics summary

The following statistics are added to the output of this show command to support the ECGI-CHANGE event trigger installation:

- Event Statistics:
  - ECGI Change - Displays the number of ECGI-CHANGE event triggers that has been received by Local-Policy.

- Variable Matching Statistics
  - ECGI - Displays the number of times the ECGI is matched and the specific action is applied based on the event.

Gx Support for GTP based S2a/S2b

In releases prior to 18, for WiFi integration in P-GW, Gx support was already available for GTP based S2a/S2, but the implementation was specific to a particular customer.

In 18 and later releases, the Gx support for GTP based S2a/S2 interface is extended to all customers. This implementation is in compliance with standard Rel.8 Non-3GPP specification part of 29.212, along with C3-101419 C3-110338 C3-110225 C3-120852 C3-130321 C3-131222 CRs from Rel.10/Rel.11.

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

- AVP support for TWAN ID is provided
- TWAN-ID is added to r8-gx-standard dictionary

Gx-based Virtual APN Selection

This section describes the overview and implementation of Gx based Vitrual APN Selection feature.

This section discusses the following topics for this feature:

- Feature Description, on page 93
- Configuring Gx based Virtual APN Selection Feature , on page 94
- Monitoring and Troubleshooting the Gx based Virtual APN Selection, on page 94

Feature Description

Overview

The current implementation supports Virtual APN (VAPN) Selection through RADIUS or local configuration. In Release 19, ASR 5500 uses PCRF and Gx interface for Virtual APN selection to achieve signaling reduction.

A new supported feature "**virtual-apn**" with feature bit set to 4 is added to the IMSA configuration. This configuration enables Gx based Virtual APN Selection feature for a given IMS authorization service. When this configuration is enabled at P-GW/GGSN, then P-GW/GGSN advertises this feature to PCRF through the Supported-Features AVP in CCR-I. When the VAPN is selected, then the PCRF rejects the CCR-I message with the Experimental-Result-Code AVP set to 5999 (DIAMETER_GX_APN_CHANGE), and sends a new APN through the Called-Station-Id AVP in CCA-I message. The existing call is then disconnected and reestablished with the new virtual APN. Note that the Experimental Result Code 5999 will have the Cisco Vendor ID.

Important Enabling this feature might have CPU impact (depending on the number of calls using this feature).

License Requirements

This feature requires a valid license to be installed prior to configuring this feature. 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*.

Limitations

The following are the limitations of this feature:

- Virtual APN supported feature negotiation, Experimental Result Code (5999), Called-Station-Id AVP should be received to establish the call with new virtual APN. When any one of conditions is not met then the call will be terminated.
- Failure-handling will not be taken into account for 5999 result-code when received in the CCA-I message.
- When the Experimental Result Code 5999 is received in the CCA-U then failure-handling action will be taken.
- If the Called-Station-Id AVP is received in CCA-U or CCA-T, then the AVP will be ignored.
- If virtual-apn is received in local-policy initiated initial message then the call will be terminated.
- When PCRF repeatedly sends the same virtual-apn, then the call will be terminated.

Configuring Gx based Virtual APN Selection Feature

The following section provides the configuration commands to enable the Gx based Virtual APN Selection.

```
configure
    context context_name
        ims-auth-service service_name
            policy-control
                diameter encode-supported-features virtual-apn
                end
```

Notes:

- **virtual-apn**: This keyword enables configuration of Gx-based Virtual APN Selection feature. By default, this feature is disabled.
- This keyword is license dependent. For more information, contact your Cisco account representative.

Verifying the Gx based Virtual APN Configuration

Use the following command in Exec mode to display whether the Gx based Virtual APN Selection feature is configured as part of the Supported-Features AVP.

```
show ims-authorization sessions full all
```

The "Negotiated Supported Features" field in this show command output displays the configuration status. This supported feature is displayed only when the feature license is configured.

Monitoring and Troubleshooting the Gx based Virtual APN Selection

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

show ims-authorization policy-control statistics

The following field has been added to the output of this show command to track the number of times the PCRF sends the Diameter Experimental Result Code (5999) when a new virtual APN is selected.

- **Gx APN Change**

For descriptions of this statistics, see the *Statistics and Counters Reference* guide.

Debugging Statistics

Use the following command to debug the Gx based Virtual APN calls.

```
show session subsystem facility sessmgr debug-info
```

This command displays the detailed statistics associated with the Gx-based VAPN feature. For example, number of Gx VAPN received, number of AAAMGR/SGX/DHCP messages after enabling Gx VAPN, and Gx VAPN calls setup time.

Bulk Statistics for Gx based Virtual APN Selection Feature

IMSA Schema

The following new bulk statistic variable is added to the IMSA schema to track the number of times the PCRF sends the Diameter Experimental Result Code (5999) when a new virtual APN is selected.

- dpca-expres-gx-apn-change

For descriptions of this variable, see the *Statistics and Counters Reference* guide.

System Schema

The following new disconnect reason is added to the System schema to track the number of times a P-GW/GGSN/SAEGW session was disconnected due to validation failure of virtual APN received from PCRF.

- gx-vapn-selection-failed (618)

For descriptions of this variable, see the *Statistics and Counters Reference* guide.

Graceful Handling of RAR from Different Peers

In StarOS Gx architecture, every Diameter session is associated with a Primary and a Secondary peer when host select is configured at the IMSA service. The behavior for processing RAR prior to release 20 is as follows:

- If the RAR is received from the Primary peer for the session, the RAR is responded using the Primary peer connection.
- If the RAR is received from a Secondary peer for the session, host-switch takes effect. This results in the RAA (and any further session signaling) happening via the Secondary peer.
- If the RAR is received via a third peer which is neither the Primary nor the Secondary peer for the session, the RAR is dropped.

In certain networks where PCRF and PCEF are connected through multiple DRAs the PCRF may select the DRA in a round-robin fashion and the RAR for a session may come from a peer which is neither Primary nor Secondary. In order to handle such a scenario, the ability to respond to the RAR received from a non-primary and non-secondary peer was added. In this case, the RAR is answered via the peer from which RAR was received. However any future signaling for the session will still occur via the previously communicating peer. If the RAR is received via the secondary peer, the host-switch occurs and the behavior remains unchanged. In order to be able to process the RAR from a third peer, that peer must be configured in the Diameter endpoint configuration. Further, this issue is seen only when host select is configured at IMSA service. When the host selection happens at endpoint level, this issue is not seen.

Assume there are three DRAs and they are configured as shown in the sample configuration below:

```
configure
   context test
      diameter endpoint Gx
         ...
         peer DRA1 realm realmName address 192.168.23.3
         peer DRA2 realm realmName address 192.168.23.3 port 3869
         peer DRA3 realm realmName address 192.168.23.3 port 3870
         exit
      ims-auth-service imsa-Gx
         policy-control
            diameter host-select row-precedence 1 table 1 host DRA1
secondary host DRA2
end
```

Without the feature, when RAR is received from DRA3, it is rejected. With the feature enabled, RAR from DRA3 is responded via DRA3 only and Peer switch will not occur in this case and subsequent messaging will be sent through DRA1 or DRA2 if any prior peer switch had happened.

Limitations

This section identifies the limitations for this feature.

- RAR will be rejected when received from different origin host.
- RAR will be rejected when received from a DRA not configured in Diameter endpoint.

NetLoc Feature Enhancement

This feature adds compliance with 3GPP standard R13 version to the existing NetLoc feature functionality.

Feature Description

Important This is a license controlled feature. Netloc feature license key is required to be enabled. Contact your Cisco account representative for information on how to obtain a license.

This feature adds compliance with 3GPP standard R13 version to the existing NetLoc feature functionality. Using this NetLoc feature, the IMS network can retrieve location information of the UE from the access or LTE network. This enhances the location related functionality and charging based on the location information.

This feature introduces the following behavior changes:

- Assuming that NetLoc feature is enabled on chassis and Access Network Information (ANI-45) Event trigger is installed, following behavior changes have been introduced:

Table 5: Gx Interface Behavior Change Towards PCRF

PCRF Gx Interface Interaction	Access Side Interaction	ULI & MS TZ Behavior Before 21.1 Release(Standard Gx-R8/Custom15 (AT&T))	ULI & MS TZ Behavior Change(Standard Gx-R8/Custom15 (AT&T))
RAI AVP with '0 - ULI' is received in the charging rule install request.	Create Bearer Response is received with **only New ULI** parameter.	Create Bearer Response is received with **only New ULI** parameter.	No change in the behavior.
RAI AVP with '0 - ULI' is received in the charging rule install request.	Create Bearer Response is received with **No ULI** parameter.	Old ULI parameter is sent towards the PCRF in the CCR-U message.	PLMN-id in 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '0 - ULI' is received in the charging rule modify request.	Update Bearer Response is received with **only New ULI** parameter.	New ULI parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '0 - ULI' is received in the charging rule Modify request.	Update Bearer Response is received with **No ULI** parameter.	Old ULI parameter is sent towards the PCRF in the CCR-U message.	PLMN-id in 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '0 - ULI' is received in the charging rule modify request.	Delete Bearer Response is received with **only New ULI** parameter and No MS TZ parameter.	New ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only New ULI is sent towards the PCRF in the CCR-U message.
RAI AVP with '0 - ULI' is received in the charging rule Modify request.	Delete Bearer Response is received with **No ULI** parameter and No MS TZ parameter.	Old ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	PLMN-id in the 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '1 -MSTZ' is received in the charging rule install request.	Create Bearer Response is received with **only new MS TZ** parameter.	New MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule install request.	Create Bearer Response is received with **No MS TZ** parameter.	Old MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.

PCRF Gx Interface Interaction	Access Side Interaction	ULI & MS TZ Behavior Before 21.1 Release(Standard Gx-R8/Custom15 (AT&T))	ULI & MS TZ Behavior Change(Standard Gx-R8/Custom15 (AT&T))
RAI AVP with '1 -MSTZ' is received in the charging rule modify request.	Update Bearer Response is received with **only New MS TZ** parameter.	New MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule Modify request.	Update Bearer Response is received with **No MS TZ** parameter.	Old MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule modify request.	Delete Bearer Response is received with **only New MS TZ** parameter.	Old ULI and New MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only New MS TZ is sent towards the PCRF in the CCR-U message.
RAI AVP with '1 -MSTZ' is received in the charging rule Modify request.	Delete Bearer Response is received with **No MS TZ** parameter.	New ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only old MS TZ is sent towards the PCRF.
Nothing is received.	Delete Session Request is received with New ULI and New MS TZ parameters.	New ULI and New MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.
Nothing is received.	Delete Session Request is received with New ULI and No MS TZ parameter.	New ULI and Old MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.
Nothing is received.	Delete Session Request is received with No ULI and No MS TZ parameter.	Old ULI and Old MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.

Important ULI and ULI timestamp is considered as paired. If the ULI timestamp is forwarded, it is forwarded and received with the ULI. If the ULI is received and the ULI timestamp is not received, then that P-GW does not forward the old timestamp.

- Inclusion of AVP support of NETLOC-ACCESS-NOT-SUPPORTED on Gx interface. This inclusion of AVP is based on the below conditions:
  - RAT type is other than E-UTRAN, UTRAN, WCDMA, GPRS, GERAN, and W-LAN
  - IP CAN type is other than 3GPP EPS, GPRS, and non 3GPP EPS

- Re-Auth-Request is received with Required-Access-Info AVP.
- NetLoc feature is enabled on the chassis.
- Event-Trigger ACCESS_NETWORK_INFO_REPORT (45) is installed.

Before Release 21.1 Behavior (Standard Gx-R8/Custom15(AT&T))	New Behavior(Standard Gx-R8/Custom15(AT&T))
Earlier, if IP-CAN type or RAT type was not support NETLOC, P-GW(PCEF) ignored RAI received from the PCRF.	New AVP NetLoc-Access-Support has been added in the Re-Auth-Answer message in the R8-Gx-standard and the Custom15 Gx Dictionary.

- ***Table 6: Behavior Change Regarding LastUserLocationInformation AVP and LastMSTimeZone AVP***

P-GW CDR Behavior	Post 21.1 Release, Behavior in Custom 35/Custom 24/Custom 48 Dictionaries	Custom52 Dictionary (standard compliance new dictionary)/ Custom 35 Dictionary (Customer Specific)
ULI is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	ULI was not part of P-GW CDR generation.	ULI is recorded as **LastUserLocationInformation** AVP in the P-GW CDR generation. (AVP is not controlled using the CLI command.)
MS TZ is received in the Delete Bearer Command/Delete Bearer Request /Delete Session Request.	MS TZ was not part of P-GW CDR generation.	MS TZ is recorded as **LastMSTimeZone** AVP in the P-GW CDR generation. CDR is released as Normal Release. MS TZ is not detected in this case as full trigger and does not release extra CDR with MS TZ changes cause. AVP is not controlled using the CLI command.

S-GW CDR behavior	Post 21.1 Release behavior in Custom 35/Custom 24 Dictionary	Custom24 Dictionary (standard dictionary)/ Custom 35 Dictionary (AT&T)
ULI is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	ULI was not part of CDR generation.	ULI is Recorded as **LastUserLocationInformation** AVP in the S-GW CDR generation. The attribute is controlled using a CLI command.

MS TZ is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	MS TZ was not part of CDR generation.	MS TZ is Recorded as **LastMSTimeZone** AVP in S-GW CDR generation. The attribute is controlled using a CLI command. CDR is released as Normal Release. MS TZ is not detected in this case as full trigger and does not release extra CDR with MS TZ changes cause.

Limitations

1. This feature enhancement is applicable only for S-GW, P-GW, and SAEGW. For GGSN ad SGSN, there is no change in the behavior of the NetLoc feature.
2. The attributes **Last-MS-Timezone** and **Last ULI attributes** have been added in the dictionaries custom24 and custom35 for S-GW CDR generation only.
3. The keywords **last-ms-timezone** and **last-uli** added to the CLI command **gtpp attribute** are applicable and limited to only S-GW CDR generation.
4. **Last-MS-Timezone** and **Last ULI attributes** added in dictionary custom35 (customer specific dictionary) and custom52 (3GPP R13 standard compliance) are applicable and limited to P-GW CDR generation only. These attributes are not CLI controlled.

Command Changes

gtpp-attribute

This CLI command allows the specification of the optional attributes to be present in the Call Detail Records (CDRs) that the GPRS/PDN/UMTS access gateway generates. It also defines that how the information is presented in CDRs by encoding the attribute field values. The keywords **last-ms-timezone** and **last-uli** have been added to this CLI command to control attribute while CDR generation.

Important The keywords added are applicable only for S-GW CDR. They are not applicable for P-GW CDR.

```
configure
   context <context_name>
      gtpp group group_name
        gtpp attribute { last-ms-timezone | last-uli | .. }
        [no | default ] gtpp attribute { last-ms-timezone | last-uli |
.. }
    end
```

Notes:

- **no:** Removes the configured GTPP attributes from the CDRs.
- **default:** Sets the default GTPP attributes in the generated CDRs. It also sets the default presentation of attribute values in generated CDRs.

- **last-ms-timezone:** Sets the "Last MS-Timezone" in the CDR field. This option would be disabled when the default option is used.
- **last-uli:** Sets the "Last ULI" in the CDR field. This option would be disabled when the default option is used.

Performance Indicator Changes

show configuration

This command has been modified to display the following output:

- Last-MS-Timezone present
- Last-User Location Information present

show gtpp group name *group_name*

This command has been modified to display the following output:

```
     Last-MS-Timezone present: yes
     Last-User Location Information present:
yes
```

RAN-NAS Cause Code Feature Enhancement

This chapter describes the RAN-NAS Cause Code Feature Enhancement.

Feature Description

Important This is a license controlled feature. You must enable the existing license of NPLI. Contact your Cisco account representative for information on how to obtain a license.

This feature introduces support for 3GPP RAN/NAS cause code IE for "Failed Create Bearer Response", "Failed Updated Bearer Response", and "Delete Bearer Response" at the Gx interface, the P-GW, and S-GW CDRs. This will enable the operator to get detailed RAN/NAS release cause code information from the access network. RAN/NAS cause can be received from the access side in either of the following messages:

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request
- Delete Bearer Response
- Delete Bearer Command

This support of 3GPP Release 12 RAN/NAS cause IE on the S4, S11, S5, and S8 interfaces exists for "Delete Session Request" and "Delete Bearer" command through private extension as well as Standard IE for customer specific dictionaries Gx- dpca-custom15 and Gz-Custom35.

However, RAN/NAS cause received in the "ERAB creation Failure", "ERAB modification Failure", and "ERAB release indication" messages were not processed at the S-GW and P-GW. Hence, it was also not forwarded to the PCRF by P-GW neither populated in the P-GW and S-GW CDRs. With this feature enhancement, support has been added to process the RAN/NAS cause codes at the S-GW (S4,S11 interface) and P-GW (S5,S8 interface) for the "Create bearer response", "Update bearer response", and "Delete bearer response". Also, RAN/NAS cause codes will be forwarded to the PCRF by the P-GW and will be populated in the P-GW and S-GW CDRs.

There is no requirement to add the support for the 3GPP Release 12 RAN/NAS cause IE received in the private extension for "Create Bearer Response", "Update Bearer Response", and "Delete Bearer Response". Private extension support for 3GPP Release 12 cause code IE in "Delete Session Request" and "Delete Bearer Command" will continue to be supported.

This feature enhancement introduces the following RAN/NAS cause IE behavior changes at the Gx interface for dpca-custom15 dictionary and at Gz interface for custom35 dictionary.

Table 7: Gx Interface Requirements for RAN/NAS Cause

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Create Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.4-2. So if it is received, it is ignored and is not forwarded to the PCRF.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if received it is ignored and is not forwarded to the PCRF.
	Other GTP Causes	CCR-U
Update Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.16-2. So if it is received, it is ignored and is not forwarded to the PCRF.
	No Resources	CCR-U
	Available	**Important** If the UE-initiated (MBC) bearer modification fails with the GTP cause "NO RESOURCES AVAILABLE", then P-GW deletes the entire PDN session. In this case, RAN-NAS cause information is forwarded as part of the CCR-T message.
	Context Not Found	If the update bearer response is received with the message level cause as "CONTEXT NOT FOUND", which leads to the PDN deletion, then the RAN-NAS cause information is forwarded as part of the CCR-T message.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if this cause is received, it is ignored and is not forwarded to the PCRF.
	Other GTP Causes	CCR-U

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Delete Bearer Response	Temporarily rejected due to HO in progress	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if this cause is received, it is ignored and is not forwarded to the PCRF. **Important** As per existing design of S-GW, if "Delete Bearer Response" is received with GTP cause "Temporarily rejected due to handover/ TAU/ RAU procedure in progress" it changes GTP cause to "Request Accepted" and forwards it to the P-GW. In this case, if RAN/NAS cause is received in the "Delete Bearer Response", S-GW will forward it to the P-GW. And at the P-GW since "Delete Bearer Response" is received with the GTP cause "Request Accepted" hence RAN/NAS cause is forwarded to the PCRF and populated in the P-GW CDR. This behavior will be seen for SAEGW and S-GW + P-GW combination call.
	Accepted / Other GTP CCR-UCauses	**Important** If RAN/NAS cause is received in the delete bearer response that is initiated by the network through RAR/CCA-U, then P-GW will not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in 29.212 release 13.5 with "Enhance RAN/NAS" feature".

Table 8: Gz Interface Requirements for RAN/NAS Cause

Message	S-GW CDR	P-GW CDR
Delete Session Request	Yes	Yes
Delete Bearer Command	Yes	Yes NOTE: RAN/NAS cause if received in delete bearer response will overwrite the RAN/NAS cause received in delete bearer command
Failed Create Bearer Response	No	No
Failed Update Bearer Response	No	No
Delete Bearer Response	No	Yes

Limitations

Following are the limitations of this feature:

- Support of RAN/NAS cause over S2a and S2b interfaces is not supported.

- Support of RAN/NAS cause information has not been added for standard Gx and Gz dictionaries.
- P-GW processes first two RAN/NAS cause IE (max one RAN and max one NAS) information received from the GTP interface. For example, if the access network misbehaves and sends RAN/NAS cause list with two NAS and one RAN then only first two causes are considered and validated. In this case, these are two NAS causes, only first NAS cause will be populated at the Gx interface and in the CDRs as only one NAS is allowed.
- As per spec 32.251 Table 5.2.3.4.1.1 and Table 5.2.3.4.2.1, there is no trigger to generate the S-GW CDRs and P-GW CDRs for failed create bearer response and failed update bearer response. Hence, RAN/NAS cause received in "Failed Create Bearer" response and "Failed Update Bearer" response will not be sent to the Gz interface.
- In "Delete Bearer" scenario, S-GW CDRs are generated immediately after receiving "Delete Bearer" request. Hence, RAN/NAS cause received in the "Delete Bearer" response is not populated in the S-GW CDRs.
- If RAN/NAS cause is received in the "Delete Bearer" response that is initiated by the network through RAR/CCA-U, P-GW will not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in spec 29.212 release 13.5 with "Enhance RAN/NAS" feature".
- If the RAN-NAS-Cause feature is supported, only RAN/NAS cause is forwarded to PCRF . ANI information will be forwarded only when NetLoc feature is enabled. Below table describes various scenarios,

Scenario	RAN/NAS Cause Behavior	ANI Behavior
IP-CAN Bearer Termination	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in the Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to bearer termination, in the RAN-NAS-Release-Cause AVP included in the Charging-Rule-Report AVP.	ANI information received during bearer termination is populated in the CCR-U, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in Gx CCR-I/CCA-I).
IP-CAN Session Termination	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in the Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to session termination, in the RAN-NAS-Release-Cause AVP at the command level.	ANI information received during session termination is populated in CCR-T, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in the CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in the Gx CCR-I/CCA-I).

Scenario	RAN/NAS Cause Behavior	ANI Behavior
PCC Rule Error Handling	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to rule installation/ activation/ modification failure, in the RAN-NAS-Release-Cause AVP included in the Charging-Rule-Report AVP.	ANI information received due to rule installation/activation/modification failure is populated in CCR-U, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in the Gx CCR-I/CCA-I).

Command Changes

diameter encode-supported-features netloc netloc-ran-nas-cause

The behavior of this CLI command has been modified in this feature enhancement.

Previous Behavior: To enable the RAN/NAS Cause feature, it was mandatory to enable the NetLoc feature. For this, it was mandatory to configure the **netloc** keyword in the CLI command **diameter encode-supported-features netloc netloc-ran-nas-cause** .

New Behavior: Now, you can enable the RAN/NAS feature without configuring the NetLoc feature. This implied that it is not mandatory to configure the **netloc** keyword in the CLI command **diameter encode-supported-features netloc netloc-ran-nas-cause** .

```
configure > context context_name > ims-auth-service service_name > policy-control
 diameter encode-supported-features netloc netloc-ran-nas-cause
```

Session Disconnect During Diamproxy-Session ID Mismatch

This section describes how to clear the subscriber sessions that are impacted due to the mismatch in Diamproxy grouping information and Session ID.

This section discusses the following topics for this feature:

Feature Description

During rapid back-to-back ICSR switchovers or extensive multiple process failures, the Diameter proxy-Session manager mapping information is not preserved across ICSR pairs. This mismatch in the Diameter proxy-Session ID results in rejection of RAR with 5002 - DIAMETER_UNKNOWN_SESSION_ID cause code. This behavior impacts the VoLTE call setup procedure. Hence, this feature is introduced to clear the subscriber sessions that are impacted due to the mismatch in the Diameter proxy-session manager mapping. New CLI configuration

is provided to control the behavior and new bulk statistic counter is supported to report the Diamproxy-Session ID mismatch.

The bulk statistic counter will be incremented only when session is cleared upon receiving RAR message with 5002 result code and detecting session-ID Diamproxy mapping mismatch. A Delete Bearer Request is sent to S-GW with a Reactivation Requested as the cause code while suppressing the CCR-T from being sent to PCRF. So, the subscriber reattaches immediately without impacting the subsequent VoLTE calls, encountering only one failure instead of manual intervention.

Important This enhancement is applicable only to IMS PDN so that there is a limit of one failure when encountering this situation instead of manual intervention. This is applicable to only the Gx RARs.

Configuring System to Delete Diamproxy-Session ID Mismatched Sessions

The following section provides the configuration commands to enable the system to clear the subscriber sessions that are impacted due to the mismatch in Diamproxy grouping information and Session ID.

Clearing Mismatched Subscriber Sessions

Use the following configuration commands to configure the system to disconnect the subscriber sessions based on signaling trigger when session ID and Diamproxy mismatch is identified.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
             diameter clear-session sessid-mismatch
end
```

- **sessid-mismatch**: Clears the session with mismatched session ID. This CLI configuration is optional.
- The default configuration is **no diameter clear-session**. By default, the sessions will not be cleared.

Verifying the Configuration to Delete Mismatched Sessions

Use the following command to verify the configuration status of this feature.

```
show ims-authorization service name service_name
```

service_name must be the name of the IMS Authorization service configured for IMS authentication.

This command displays all the configurations that are enabled within the specified IMS authorization service. The "Session-Id Mismatch Clear Session" field can be used to determine whether this feature is enabled or disabled.

```
[local]st40# show ims-authorization service name service1
  Context: test
  IMS Authorization Service name: service1
  Service State: Enabled
  Service Mode: Single Interface Policy and Charging
...
  Diameter Policy Control:
   Endpoint: gx
   Origin-Realm: xyz.com
   Dictionary: standard
```

```
    Supported Features:
       3gpp-r9
...
    Host Selection: Table: 1 Algorithm: Round-Robin
    Host Reselection Subscriber Limit: Not Enabled
    Host Reselection Interval: Not Enabled
    Sgsn Change Reporting: Not Enabled
      Session-Id Mismatch Clear Session: Enabled
    3GPP R9 Flow Direction Compliance: Not Enabled
  Host Selection Table[1]: 1 Row(s)
    Precedence: 1
...
```

Monitoring and Troubleshooting the Mismatched Session Deletion Feature

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

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

- Verify if the feature is enabled using **show ims-authorization service name** <*service_name*> CLI command. If not enabled, configure the **diameter clear-session sessid-mismatch** CLI command and check if it works.
- Collect the output of **show ims-authorization policy-control statistics debug-info** and **show diameter statistics proxy debug-info** commands and analyze the debug statistics.
- Check the system logs that are reported while deleting the affected sessions. For further analysis, contact Cisco account representative.

show ims-authorization service name

A new field "Session-Id Mismatch Clear Session" is added to the output of this show command to indicate whether this feature is enabled or disabled within the specified IMS authorization service.

IMSA Schema

The following bulk statistic variable is added to this schema to report the Diamproxy-Session ID mismatch.

- dpca-rar-dp-mismatch - This counter displays the total number of sessions cleared while receiving RAR because of session-ID Diamproxy mapping mismatch.

Support for Negotiating Mission Critical QCIs

This section describes the overview and implementation of the Mission Critical QCIs Negotiation feature.

This section includes the following topics:

- Feature Description, on page 108
- Configuring DPCA for Negotiating Mission Critical QCIs, on page 108
- Monitoring and Troubleshooting the Mission Critical QCI, on page 109

Feature Description

To support Mission Critical (MC) Push to Talk (PTT) services, a new set of standardized QoS Class Identifiers (QCIs) (65, 66, 69, 70) have been introduced. These are 65-66 (GBR) and 69-70 (non-GBR) network-initiated QCIs defined in 3GPP TS 23.203 v13.6.0 and 3GPP TS 23.401 v13.5.0 specifications. These QCIs are used for Premium Mobile Broadband (PMB)/Public Safety solutions.

Important The MC-PTT QCI feature requires Wireless Priority Service (WPS) license to be configured. For more information, contact Cisco account representative.

Previous Behavior: The gateway accepted only standard QCIs (1-9) and operator defined QCIs (128-254). If the PCRF sends QCIs with values between 10 and 127, then the gateway rejects the request. MC QCI support was not negotiated with PCRF.

New Behavior: PCRF accepts the new standardized QCI values 69 and 70 for default bearer creation and 65, 66, 69 and 70 for dedicated bearer creation.

For this functionality to work, a new configurable attribute, **mission-critical-qcis**, is introduced under the **diameter encode-supported-features** CLI command. When this CLI option is enabled, the gateway allows configuring MC QCIs as a supported feature and then negotiates the MC-PTT QCI feature with PCRF through Supported-Features AVP.

The gateway rejects the session create request with MC-PTT QCIs when the WPS license is not enabled and Diameter is not configured to negotiate MC-PTT QCI feature, which is part of Supported Feature bit.

For more information on this feature and associated configurations, refer to *P-GW Enhancements for 21.0* section in the *Release Change Reference* guide.

Configuring DPCA for Negotiating Mission Critical QCIs

The following section provides the configuration commands to enable support for MC-PTT QCI feature.

Enabling Mission Critical QCI Feature

Use the following configuration commands to enable MC-PTT QCI feature.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features mission-critical-qcis
            end
```

Notes:

- **mission-critical-qcis**: This keyword enables MC-PTT QCI feature. By default, this feature will not be enabled.
- This keyword can be enabled only if the WPS license is configured. For more information, contact your Cisco account representative.
- To disable the negotiation of this feature, the existing **no diameter encode-supported-features** command needs to be configured. On executing this command, none of the configured supported features will be negotiated with PCRF.

Verifying the Mission Critical QCI Feature Configuration

The **show ims-authorization sessions full all** command generates a display that indicates the configuration status of this feature.

The following sample display is only a portion of the output which shows *mission-critical-qcis* among the Negotiated Supported Features.

```
show ims-authorization sessions full all

 CallId: 00004e29            Service Name:  ims-ggsn-auth
   IMSI: 123456789012341
   ....

 Negotiated Supported Features:
   3gpp-r8
   mission-critical-qcis
 Bound PCRF Server: 192.1.1.1
 Primary PCRF Server: 192.1.1.1
 Secondary PCRF Server: NA
 ....
```

Monitoring and Troubleshooting the Mission Critical QCI

The following section describes commands available to monitor the Mission Critical QCI feature.

Mission Critical QCI Show Command(s) and/or Outputs

show ims-authorization sessions full all

On running the above mentioned show command, statistics similar to the following are displayed and will indicate if the Mission Critical QCI feature is enabled or not.

```
show ims-authorization sessions full all

 CallId: 00004e29            Service Name:  ims-ggsn-auth
   IMSI: 123456789012341
   ....

 Negotiated Supported Features:
   3gpp-r8
   mission-critical-qcis
   ....
```

HSS and PCRF-based P-CSCF Restoration Support for WLAN

This section describes the overview and implementation of the HSS-based and PCRF-based P-CSCF Restoration feature for WLAN and EPC networks.

This section includes the following topics:

Feature Description

The P-CSCF restoration procedures were standardized to minimize the time a UE is unreachable for terminating calls after a P-CSCF failure. In compliance with 3GPP standard Release 13, this feature is developed to include the following P-CSCF restoration mechanisms:

- HSS-based P-CSCF Restoration for Trusted/Untrusted WLAN Access (S2a/S2b)
- PCRF-based P-CSCF Restoration for LTE (S5/S8) and Trusted/Untrusted WLAN Access (S2a/S2b)

Important HSS-based P-CSCF Restoration was supported at P-GW for LTE (S5/S8) prior to StarOS release 21.0.

This feature provides support for both basic and extended P-CSCF Restoration procedures.

Important The P-CSCF Restoration is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

- **HSS-based P-CSCF Restoration for WLAN**:

  If the P-CSCF restoration mechanism is supported, gateway indicates the restoration support to AAA server through Feature-List AVP in the Authorization Authentication Request (AAR) message sent over S6b interface. The Feature-List AVP is part of the Supported-Features grouped AVP. The Bit 0 of the Feature-List AVP is used to indicate P-CSCF Restoration support for WLAN.

  During the P-CSCF Restoration, 3GPP AAA server, after having checked that the PGW supports the HSS-based P-CSCF restoration for WLAN, sends a P-CSCF restoration indication to the P-GW over S6b in a Re-authorization Request (RAR) command. A new Diameter AVP "**RAR-Flags**" is encoded in the RAR message with the Bit 1 set, would indicate to the gateway that the AAA server requests the execution of HSS-based P-CSCF restoration procedures for WLAN.

  The existing CLI command **diameter authentication** under AAA Group configuration is extended to encode P-CSCF Restoration feature as part of Supported-Features AVP in the AAR message.

  Important Supported-Features will be sent in every AAR message for RAT type WLAN. Feature negotiation is required in every AAR. ReAuth AAR will also do the feature renegotiation.

- **PCRF-based P-CSCF Restoration**:

  PCEF supporting P-CSCF restoration mechanism indicates the restoration support in CCR-I message through the Supported-Features AVP. The 24th Bit of the Supported-Feature-List AVP indicates whether this mechanism is supported or not.

  The existing CLI command **diameter encode-supported-features** in Policy Control configuration is extended to allow the negotiation of P-CSCF Restoration feature support with PCRF. A new Diameter AVP "**PCSCF-Restoration-Indication**" is introduced to indicate to PCEF that a P-CSCF Restoration is requested. This is achieved by setting AVP value to 0.

Supported-Features AVP is negotiated in CCR-I of all access types (eHRPD, P-GW, GGSN); however, Restoration trigger, if received, is ignored in eHRPD and GGSN.

Limitations

- As per the 3GPP standard specification, if S6b re-authorization request is used for P-CSCF Restoration for WLAN, then for extended P-CSCF Restoration the gateway may send authorization request with only mandatory AVPs. However, in the current implementation, ReAuth used for extended P-CSCF Restoration is a common authorization request of normal ReAuth. It will contain all the AVP of ReAuthorization AAR.

For more information on this feature and associated configurations, refer to *P-GW Enhancements for 21.0* and *SAEGW Enhancements for 21.0* section in the *Release Change Reference* guide.

Configuring the HSS/PCRF-based P-CSCF Restoration

The following section provides the configuration commands to enable support for HSS-based and PCRF-based P-CSCF Restoration feature.

Enabling P-CSCF Restoration Indication on S6b AAA interface

Use the following configuration commands for encoding Supported-Features AVP in the AAR message sent to AAA server via S6b interface.

```
configure
   context context_name
      aaa group group_name
         diameter authentication encode-supported-features
pcscf-restoration-indication
         end
```

Notes:

- **encode-supported-features**: Encodes Supported-Features AVP.
- **pcscf-restoration-indication**: Enables the P-CSCF Restoration Indication feature.
- **default encode-supported-features**: Configures the default setting, that is not to send the Supported-Features AVP in AAR message.
- **no encode-supported-features**: Disables the CLI command to not send the Supported-Features AVP.
- The **pcscf-restoration-indication** keyword is license dependent. For more information, contact your Cisco account representative.

Enabling P-CSCF Restoration Indication on Gx interface

Use the following configuration to enable P-CSCF Restoration Indication feature on Gx interface.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features pcscf-restoration-ind
            end
```

Notes:

- **pcscf-restoration-ind**: Enables the P-CSCF Restoration Indication feature. This keyword is license dependent. For more information, contact your Cisco account representative. By default, this feature is disabled.
- **default encode-supported-features**: The default configuration is to remove/reset the supported features.
- **no encode-supported-features**: Removes the previously configured supported features.

Verifying the HSS/PCRF-based P-CSCF Restoration

show ims-authorization sessions full all

This command generates a display that indicates the negotiation status of this feature.

The following sample display is only a portion of the output which shows **pcscf-restoration-ind** among the Negotiated Supported Features.

```
show ims-authorization sessions full all

CallId: 00004e22            Service Name:  imsa-Gx
  IMSI: 123456789012341
  ....
Negotiated Supported Features:
  3gpp-r8
  pcscf-restoration-ind
....
```

show aaa group all

This show command displays **pcscf-restoration-ind** as part of Supported-Features, if this feature is configured under AAA group.

```
show aaa group all
 Group name:    default
 Context:   local

 Diameter config:
  Authentication:
....
Supported-Features:   pcscf-restoration-ind
....
```

Monitoring and Troubleshooting the HSS/PCRF-based P-CSCF Restoration

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

The following operations can be performed for troubleshooting any failure related to this feature:

- Verify if the feature is enabled using **show ims-authorization sessions full all** and **show aaa group all** CLI commands. If not enabled, configure the required CLI commands both under Policy Control and AAA group configuration and check if it works.
- Execute **monitor protocol** command and check if the support for P-CSCF Restoration feature is negotiated in CCR-I and AAR messages. If not, enable the respective CLI commands for this feature to work.
- If the failure is still observed, obtain the following information and contact Cisco account representative for further analysis:

- Monitor protocol log with options 74 (EGTPC) and 75 (App Specific Diameter –Gx/S6b) turned on
- Logs with sessmgr, imsa, and diameter-auth enabled
- Output of **show session disconnect reason** CLI command and the relevant statistics at service level

Show Commands and/or Outputs

show ims-authorization sessions full all

The **Negotiated Supported Features** field in this show command output displays whether or not the P-CSCF Restoration feature is negotiated with PCRF.

This supported feature is displayed only when the feature license is configured.

show aaa group all

The **Supported Features** field in this show command output displays whether or not the P-CSCF Restoration feature is configured as part of the Supported-Features AVP.

This supported feature is displayed only when the feature license is configured.

show license information

If the license to enable the P-CSCF Restoration feature is configured, then the **show license information** command displays the associated license information.

Monitoring Logs

This section provides information on how to monitor the logs that are generated relating to the HSS/PCRF-based P-CSCF Restoration feature.

S6b Diameter Protocol Logs

The **Supported-Features** field is available in AAR/AAA section. The log output generated will appear similar to the following:

```
<<<<OUTBOUND  15:37:23:561 Eventid:92870(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....

INBOUND>>>>>  15:37:23:562 Eventid:92871(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....
```

The **RAR-Flags** field is available in RAR section. The log output generated will appear similar to the following:

```
INBOUND>>>>>  15:37:43:562 Eventid:92871(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] RAR-Flags: 2
....
```

Gx Diameter Protocol Logs

Under **Supported-Features**, the P-CSCF Restoration **Feature-List** is available in CCR-I/CCA-I section. The output generated will appear similar to the following:

```
<<<<OUTBOUND  13:52:06:117 Eventid:92820(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777217
....
INBOUND>>>>>  13:52:06:118 Eventid:92821(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777216
....
```

The **PCSCF-Restoration-Indication** AVP is available in RAR. The output generated will appear similar to the following:

```
INBOUND>>>>>  13:52:26:119 Eventid:92821(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] PCSCF-Restoration-Indication: 0
....
```

Loop Prevention for Dynamic Rules

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	P-GW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvc97345, CSCvd02249
Related Changes in This Release	Not Applicable
Related Documentation	P-GW Administration Guide Command Line Interface Reference

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

When a PCC (Dynamic or Predefined) rule installation fails, the PCEF initiates a CCR-U toward the PCRF to report the failed rule. In case the PCRF responds back with same rule definition, then the rule failure CCR-U is initiated again. This results in a loop of rule failure.

With this feature, gateways have the ability to prevent the loop by reporting the rule install failure to PCRF only once until it is successfully installed.

How It Works

This feature is configurable through a CLI command with which, once a failure is being reported for a subscriber, failure for the same rule is suppressed for that subscriber until it is installed successfully. The rulenames are preserved for a subscriber for which the failures are reported. However, when the condition of the rule failure is rectified for an error (for example, rule definition is added to the configuration and the rule is successfully installed), then the gateway removes the rulename from the failed rules list. So, if the failure for that particular rule occurs again, it is reported to the PCRF.

The failed rulename is not checkpointed and so, if a recovery event like session recovery or an ICSR occurs then the failure of these rules are reported once again.

Configuring Loop Prevention for Dynamic Rules

This section explains the configuration procedures required to enable the feature.

Enabling ACS Policy to Control Loop Prevention

Use the following commands under ACS Configuration Mode to enable or disable the feature which prevents the rule failure loop between PCRF and PCEF:

```
configure
  active-charging service<service_name>
      policy-control report-rule-failure-once
      end
```

Notes:

- When configured, CCR-U will be sent only once for the same rule failure.
- By default, the feature is disabled.
- If previously configured, use the **no policy-control report-rule-failure-once** to disable the feature.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for the Loop Prevention for Dynamic Rules feature.

show active-charging service all

The output of the above command has been enhanced to display the status (Enabled/Disabled) of the feature. For example:

```
show active-charging service all
  .
  .
  .
  Report Rule Failure Once: Enabled
```

show active-charging subscribers full all

The output of the above command has been enhanced to display the new parameter which shows the total number of rule failures not reported. For example:

```
 Callid:                         4e21        ACSMgr Card/Cpu:            15/0
 Active Charging Service name:                                           acs
 Active charging service scheme:
 ACSMgr Instance:                 1          Number of Sub sessions:     1
 Data Sessions Active:            0          Dynamic Routes created:     0
 Uplink Bytes:                    0          Downlink Bytes:             0
 Uplink Packets:                  0          Downlink Packets:           0
 Accel Packets:                   0
 FastPath Packets:                0
 Total NRSPCA Requests:           0          NRSPCA Req. Succeeded:      0
 NRSPCA Req. Failed:              0
 Total NRUPC Requests:            0          NRUPC Req. Succeeded:       0
 NRUPC Req. Failed:               0
 Pending NRSPCA Requests:         0          Pending NRUPC Requests:     0
 Total Bound Dynamic Rules:       0          Total Bound Predef. Rules:  0
 Data Sessions moved:             0
 Bearers Terminated for no rules:                                        0
 Failed Rulebase Install (unknown bearer-id):                            0
 Failed Rule Install (unknown bearer-id):                                0
 Total number of rule failures not reported:                             1
```

show active-charging subsystem all

The output of the above command has been enhanced to display the new parameter which shows the total number of rule failures not reported. For example:

```
 Total ACS Managers:            2
 Session Creation Succ:         1      Session Creation Fail:      0
 .
 .
 .
 Total Number of Unsolicited Downlink packets received : 0
 Total Number of ICMP-HU packets sent :                  0
```

```
RADIUS Prepaid Statistics:
Total prepaid sess:            0      Current prepaid sess:       0
Total prepaid auth req:        0      Total prepaid auth success: 0
Total prepaid auth fail:       0      Total prepaid errors:       0
Total number of rule failures not reported :           4

Content Filtering URL Cache Statistics:
Total cached entries:          0
Total hits:                    0      Total misses:               0
.
.
.
```

Separation of Accounting Interim Interval Timer for RADIUS and Diameter Rf

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	eHRPD, GGSN, P-GW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvc97616
Related Changes in This Release	Not Applicable
Related Documentation	AAA Interface Administration and Reference Command Line Interface Reference

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

Prior to Release 21.2, the Cisco StarOS platform had a single configuration parameter for sending accounting interim records to RADIUS and Diameter Rf servers. Consequently, it was not possible to send accounting

interim records to RADIUS and Diameter Rf servers with different intervals using the available CLI options. This feature provides a CLI controlled mechanism to have different interim intervals for Diameter Rf and RADIUS accounting applications. Having a separate configurable CLI and interim interval timer values for RADIUS and Diameter Rf servers provides enhanced usability.

How It Works

Currently, the Diameter accounting uses the value configured for RADIUS accounting interim interval. With this feature, configurable through a CLI command, provides an option to separately configure Diameter accounting interim interval for Rf interface. Until Diameter interim CLI is configured with either "**no**" option or any specific timer value, as a measure for compatibility, RADIUS interim interval value is used for Diameter interim interval. Once Diameter configuration takes effect, any change to RADIUS configuration will not affect Diameter configuration and vice versa. The following table shows the Diameter interim interval values used for different scenarios.

Radius Configuration	Diameter Configuration	Diameter Interim Behavior
No configuration OR Interim Interval: X OR Interim disabled	Interim Interval: Y	Interim Interval: Y Note: X may or may not be same as Y
No configuration OR Interim Interval: X OR Interim disabled	Interim disabled using "No" option	Interim disabled
No configuration OR Interim Interval: X OR Interim disabled	No configuration	Fallback to RADIUS configuration

- Recovery/ICSR behavior: Interim interval configuration used at the time of PDN creation is applicable for entire lifetime of PDN. Recovery/ICSR will not have any impact of existing PDN behavior with regard to Diameter interim interval.
- ICSR Upgrade/Downgrade behavior:
  - Existing session will be recovered based on RADIUS configuration present in old chassis.
  - New session behavior is as per configuration available on newly active chassis.

Limitations

Following are the known limitations of this feature:

1. In case Diameter interim interval CLI is not configured, the P-GW retains the older behavior where Diameter accounting uses the same interim interval value configured for RADIUS accounting.
2. Once diameter accounting configuration is done, it's not possible to go back to the older behavior.

Configuring Diameter Accounting Interim Interval

Use the following commands under AAA Server Group Configuration Mode to configure Diameter accounting interim interval independently from RADIUS accounting interim interval:

```
configure
    context context_name
       aaa group group_name
          diameter accounting interim interval interval_in_seconds
          end
```

Notes:

- *interval_in_seconds:* Specifies the interim interval, and must be in the range of 50 through 40000000.
- If previously configured, use the **no diameter accounting interim interval** to disable the interim accounting messages on Rf interface.
- There is no default Diameter interim interval value.
- In case Diameter interim interval CLI is not configured, the P-GW retains the older behavior where Diameter accounting uses RADIUS interim interval configuration available in AAA server group configuration block.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of the feature.

show aaa group { name <group_name> | all }

The output of the above command is modified to display the following new field to show the current configuration for interim interval used for upcoming Diameter Rf accounting sessions:

- Interim-timeout: <50-40000000> or <None>

Following is a sample output where Diameter interim interval is not configured:

```
show aaa group name default
Group name:                   default
Context:                      pgw

Diameter config:
  Accounting:
```

```
      Request-timeout:          20
      Interim-timeout:          None
```

Following is a sample output where Diameter interim interval is configured with the value 900:

```
show aaa group name default
Group name:                     default
Context:                        pgw

Diameter config:
  Accounting:
    Request-timeout:            20
    Interim-timeout:            900
```

show configuration [verbose]

The output of the above command is modified to display the following new field to show the interval of interim messages in seconds:

- diameter accounting interim interval <*value_in_seconds*>

Following is a sample output where Diameter interim interval is configured with the value 60:

```
show configuration context isp verbose
config
    context isp
        aaa group default
            diameter accounting interim interval 60
```

Enhancement to OCS Failure Reporting for Gy

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	P-GW, SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Enabled
Related CDETS ID(s)	CSCvc93904
Related Changes in This Release	Not Applicable
Related Documentation	AAA Interface Administration and Reference P-GW Administration Guide SAEGW Administration Guide

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

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.

Support Added for RAN/NAS Cause Code for S5/S8 and S2b Interfaces

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	P-GW, S-GW, SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCuy93748/CSCvc97356
Related Changes in This Release	Not Applicable

Related Documentation	*P-GW Administration Guide* *S-GW Administration Guide* *SAEGW Administration Guide* *Command Line Interface Reference*

Revision History

Important Revision history details are not provided for features introduced before Release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Changes

Important This is a license controlled feature. There are separate licenses for this feature. You must enable the existing license of NPLI or contact your Cisco account representative for information on how to obtain the custom license.

For billing co-ordination at IMS domain and VoWiFi deployments, an operator may require access to the RAN or NAS (or both) release cause code information available at P-CSCF. The P-GW provides detailed RAN/NAS cause information with ANI information received from the access network to the P-GW and further down to the PCRF based on the following events:

- Bearer deactivation (Delete Bearer Response/Delete Bearer Command)
- Session deactivation (Delete Session Request)
- Bearer creation/modification failures (Create/Update Bearer Response with cause as FAILURE)

The IMS network can retrieve detailed RAN and/or NAS release cause codes information from the access network that is used for call performance analysis, user QoE analysis, and proper billing reconciliation. This feature is supported on the S5, S8, Gx, and S2b interfaces.

This feature includes support RAN/NAS cause IE in Create Bearer Response, Update Bearer Response, Delete Bearer Response, Delete Bearer Command, and Delete Session Request. The following table shows the supported protocol type for RAN/NAS cause IE.

Table 9: Protocol Type for RAN/NAS IE

Interface	Supported Protocol Type for RAN/NAS IE
S5/S8	S1AP Cause (1)/EMM Cause (2)/ESM Cause (3)
S2b	Diameter Cause (4)/IKEv2 Cause (5)

Note Any protocol type value that is received apart from the supported protocol type values listed in the table are ignored and not forwarded to the PCRF.

GTP interface Requirements for RAN/NAS Cause

For S5/S8 interface, RAN/NAS cause is supported for the following messages for the dpca-custom8 dictionary.

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request
- Delete Bearer Response
- Delete Bearer Command

For S2b interface, RAN/NAS cause is supported for the following messages for the custom dpca-custom8 dictionary:

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request

Gx interface Requirements for RAN/NAS Cause

The RAN/NAS cause is added for the custom dpca-custom8 dictionary to ensure that the RAN/NAS cause is populated. The Gx interface behavior to handle RAN/NAS cause is as follows:

Table 10: Gx Interface Requirements for RAN/NAS Cause

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Create Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.4-2. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Other GTP Causes	CCR-U

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Update Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.16-2. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	No Resources Available	CCR-U **Note** If UE-initiated (MBC) bearer modification fails with GTP cause “NO RESOURCES AVAILABLE”, P-GW deletes the entire PDN session. In this case, RAN-NAS cause information is forwarded as part of CCR-T message.
	Context Not Found	CCR-U **Note** If the Update Bearer Response is received with the message level cause as "CONTEXT NOT FOUND", which leads to the PDN deletion, then the RAN-NAS cause information is forwarded as part of the CCR-T message.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Other GTP Causes	CCR-U

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Delete Bearer Response	Temporarily rejected due to HO in progress	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF. **Note** • If RAN/NAS cause is received in the Delete Bearer Response, which is triggered as a part of the Delete Bearer command and cause as “Request Accepted”, P-GW forwards the RAN/NAS cause (received in Delete Bearer Response) to the PCRF. • If RAN/NAS cause is received in the Delete Bearer command and Delete Bearer Response with HO in progress, the RAN/NAS Cause received in the Delete Bearer command is forwarded to the PCRF. • If RAN/NAS Cause is received in the Delete Bearer command and Delete Bearer Response with Accepted/Other Cause and new RAN/NAS Cause, the new RAN/NAS cause is forwarded to the PCRF.
	Accepted / Other GTP CCR-UCauses	CCR-U **Note** If RAN/NAS cause is received in the delete bearer response that is initiated through RAR/CCA-U, then P-GW doesl not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in 29.212 release 13.5 with "Enhance RAN/NAS" feature".
Delete Session Request	Accepted	CCR-T

ANI Behavior Towards PCRF

Section 4.5.6, 4.5.7, 4.5.12 of 3GPP 29.212 v13.4.0 mentions that if the RAN-NAS-Cause feature is supported, the PCEF should provide the available access network information within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier (if available and Trusted-WLAN feature is supported), User-Location-Info-Time AVP (if available), and 3GPP-MS-TimeZone AVP (if available).

In the earlier releases, the dpca-custom8 dictionary did not support USER-LOCATION-INFO-TIME AVP.

In this release, the USER-LOCATION-INFO-TIME AVP is added to the dpca-custom8 dictionary, which is sent to the PCRF (if available) as a part of ANI. Also, new PROTOCOL-TYPE, 1 to 5 are supported for RAN/NAS. This AVP can be seen in the CCR-U and CCR-T (whenever applicable). Also the new PROTOCOL-TYPE (S1AP Cause, EMM Cause, ESM Cause, IKEv2, DIAMETER) is visible on the Gx interface (if the same is received over the S5/S8/S2b interface).

ANI Behavior for S5/S8 Interface

Along with RAN/NAS cause, P-GW also sends following information to the PCRF, if available, for the dpca-custom8 dictionary:

Table 11: Mapping of GTP IE to ANI AVPs on Gx Interface

GTP IE	Gx AVP
UE Time Zone	3GPP-MS-TimeZone
ULI Timestamp	User-Location-Info-Time
User Location Information	3GPP-User-Location-Info

ANI information is sent to the PCRF irrespective of the event triggers configured when the RAN/NAS feature is enabled.

ANI Behavior for S2b Interface

ANI information is not sent towards PCRF for the dpca-custom8 dictionary. Also, the TWAN-Identifier is not supported as part of ANI for the dpca-custom8 dictionary.

Limitations

Following are the limitations of this feature:

- Support of RAN/NAS cause information is added only for the dpca-custom8 dictionary.
- PGW processes first two RAN/NAS cause IE (max one RAN and max one NAS) information received from the GTP interface. For example, if the access network misbehaves and sends RAN/NAS cause list with two NAS and one RAN then only first two causes are considered and validated. In this case, there are two NAS causes, only first NAS cause is populated at the Gx interface.
- RAN/NAS information is populated only on the Gx interface, no other interface is impacted.

Command Changes

diameter encode-supported-features netloc-ran-nas-cause

Use the existing CLI command, **diameter encode-supported-features netloc-ran-nas-cause** to enable the RAN/NAS cause on each of the S5/S8 and S2b interfaces.

This feature is disabled by default.

To enable this feature, enter the following commands:

```
configure
  context ISP1
     ims-auth-service IMSGx
       policy-control
       diameter encode-supported-features netloc-ran-nas-cause
       end
```