Rf Interface Support

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

Rf interface support is available on the Cisco system running StarOS 10.0 or later releases for the following products:

- Gateway GPRS Support Node (GGSN)
- Proxy Call Session Control Function (P-CSCF)
- Packet Data Network Gateway (P-GW)
- Serving Call Session Control Function (S-CSCF)

Important In StarOS version 19 and later releases, the Rf interface is not supported on the S-GW.

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

This chapter includes the following topics:

Introduction

The Rf interface is the offline charging interface between the Charging Trigger Function (CTF) (for example, P-GW, P-CSCF) and the Charging Collection Function (CCF). The Rf interface specification for LTE/GPRS/eHRPD offline charging is based on 3GPP TS 32.299 V8.6.0, 3GPP TS 32.251 V8.5.0 and other 3GPP specifications. The Rf interface specification for IP Multimedia Subsystem (IMS) offline charging is based on 3GPP TS 32.260 V8.12.0 and 3GPP TS 32.299 V8.13.0.

Offline charging is used for network services that are paid for periodically. For example, a user may have a subscription for voice calls that is paid monthly. The Rf protocol allows the CTF (Diameter client) to issue offline charging events to a Charging Data Function (CDF) (Diameter server). The charging events can either be one-time events or may be session-based.

The system provides a Diameter Offline Charging Application that can be used by deployed applications to generate charging events based on the Rf protocol. The offline charging application uses the base Diameter protocol implementation, and allows any application deployed on chassis to act as CTF to a configured CDF.

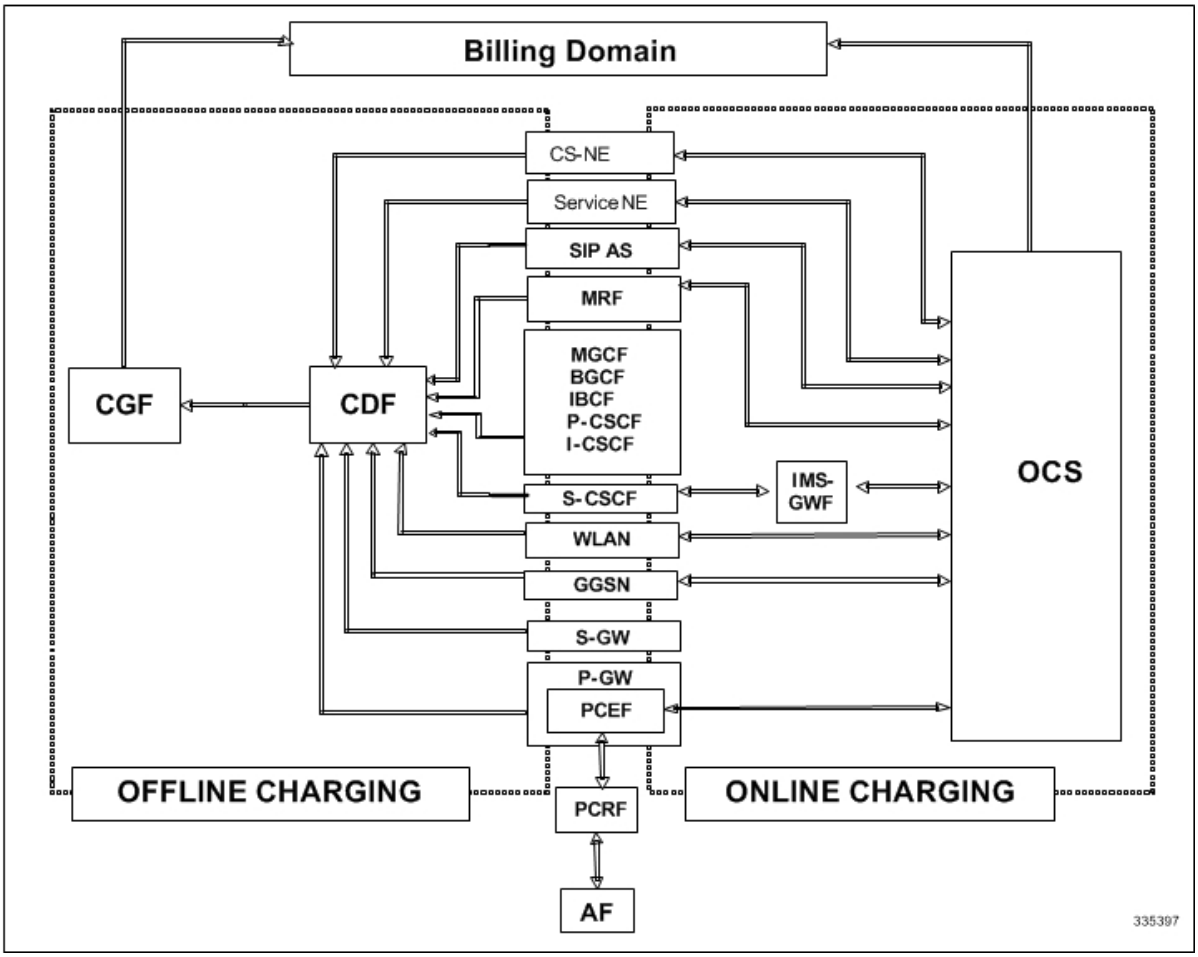
In general, accounting information from core network elements is required to be gathered so that the billing system can generate a consolidated record for each rendered service.

The CCF with the CDF and Charging Gateway Function (CGF) will be implemented as part of the core network application. The CDF function collects and aggregates Rf messages from the various CTFs and creates CDRs. The CGF collects CDRs from the CDFs and generates charging data record files for the data mediation/billing system for billing.

Offline Charging Architecture

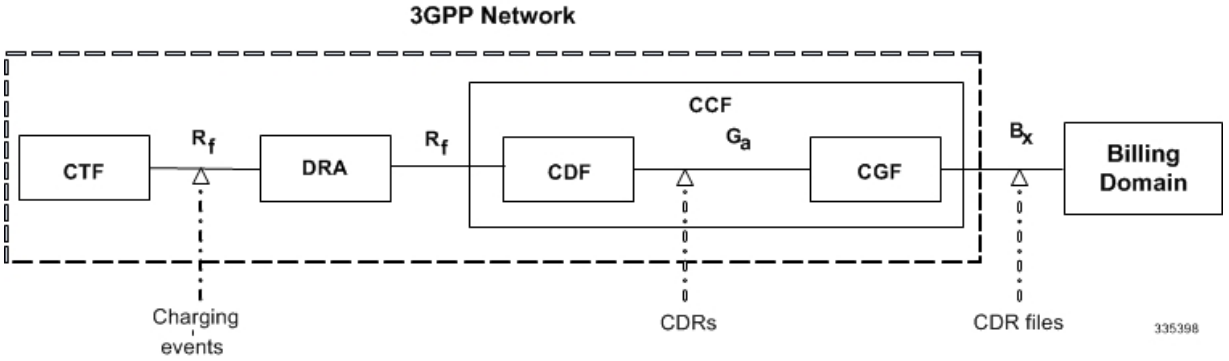
The following diagram provides the high level charging architecture as specified in 3GPP 32.240. The interface between CSCF, P-GW and GGSN with CCF is Rf interface. Rf interface for EPC domain is as per 3GPP standards applicable to the PS Domain (e.g. 32.240, 32.251, 32.299, etc.).

Figure 1: Charging Architecture



The following figure shows the Rf interface between CTF and CDF.

Figure 2: Logical Offline Charging Architecture



The Rf offline charging architecture mainly consists of three network elements CCF, CTF and Diameter Dynamic Routing Agent (DRA).

Charging Collection Function

The CCF implements the CDF and CGF. The CCF will serve as the Diameter Server for the Rf interface. All network elements supporting the CTF function should establish a Diameter based Rf Interface over TCP connections to the DRA. The DRA function will establish Rf Interface connection over TCP connections to the CCF.

The CCF is primarily responsible for receipt of all accounting information over the defined interface and the generation of CDR (aka UDRs and FDRs) records that are in local storage. This data is then transferred to the billing system using other interfaces. The CCF is also responsible for ensuring that the format of such CDRs is consistent with the billing system requirements. The CDF function within the CCF generates and CGF transfers the CDRs to the billing system.

The CDF function in the CCF is responsible for collecting the charging information and passing it on to the appropriate CGF via the GTP' based interface per 3GPP standards. The CGF passes CDR files to billing mediation via SCP.

Charging Trigger Function

The CTF will generate CDR records and passes it onto CCF. When a P-GW service is configured as CTF, then it will generate Flow Data Record (FDR) information as indicated via the PCRF. The P-GW generates Rf messages on a per PDN session basis. There are no per UE or per bearer charging messages generated by the P-GW.

The service data flows within IP-CAN bearer data traffic is categorized based on a combination of multiple key fields (Rating Group, Rating Group and Service -Identifier). Each Service-Data-Container captures single bi-directional flow or a group of single bidirectional flows as defined by Rating Group or Rating Group and Service-Identifier.

Dynamic Routing Agent

The DRA provides load distribution on a per session basis for Rf traffic from CTFs to CCFs. The DRA acts like a Diameter Server to the Gateways. The DRA acts like a Diameter client to CCF. DRA appears to be a CCF to the CTF and as a CTF to the CCF.

The DRA routes the Rf traffic on a per Diameter charging session basis. The load distribution algorithm can be configured in the DRA (Round Robin, Weighted distribution, etc). All Accounting Records (ACRs) in one

Diameter charging session will be routed by the DRA to the same CCF. Upon failure of one CCF, the DRA selects an alternate CCF from a pool of CCFs.

License Requirements

The Rf 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

Rf interface support is based on the following standards:

- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release9)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• 5G Non Standalone Solution Guide • AAA Interface Administration and Reference • Command Line Interface Reference • MME Administration Guide • Statistics and Counters Reference

Revision History

Revision Details	Release
The StarOS 21.22 is enhanced, where an existing User Location Information (ULI) is sent to the Accounting Record (ACR) Stop message on offline charging (RF) interface for GGSN, P-GW, and SAEGW.	21.22

Features and Terminology

This section describes features and terminology pertaining to Rf functionality.

Offline Charging Scenarios

Offline charging for both events and sessions between CTF and the CDF is performed using the Rf reference point as defined in 3GPP TS 32.240.

Basic Principles

The Diameter client and server must implement the basic functionality of Diameter accounting, as defined by the RFC 3588 Diameter Base Protocol.

For offline charging, the CTF implements the accounting state machine as described in RFC 3588. The CDF server implements the accounting state machine "SERVER, STATELESS ACCOUNTING" as specified in RFC 3588, i.e. there is no order in which the server expects to receive the accounting information.

The reporting of offline charging events to the CDF is managed through the Diameter Accounting Request (ACR) message. Rf supports the following ACR event types:

Table 1: Rf ACR Event Types

Request	Description
START	Starts an accounting session
INTERIM	Updates an accounting session
STOP	Stops an accounting session
EVENT	Indicates a one-time accounting event

ACR types START, INTERIM and STOP are used for accounting data related to successful sessions. In contrast, EVENT accounting data is unrelated to sessions, and is used e.g. for a simple registration or interrogation and successful service event triggered by a network element. In addition, EVENT accounting data is also used for unsuccessful session establishment attempts.

Important The ACR Event Type "EVENT" is supported in Rf CDRs only in the case of IMS specific Rf implementation.

The following table describes all possible ACRs that might be sent from the IMS nodes i.e. a P-CSCF and S-CSCF.

Table 2: Accounting Request Messages Triggered by SIP Methods or ISUP Messages for P-CSCF and S-CSCF

Diameter Message	Triggering SIP Method/ISUP Message
ACR [Start]	SIP 200 OK acknowledging an initial SIP INVITE
	ISUP:ANM (applicable for the MGCF)
ACR [Interim]	SIP 200 OK acknowledging a SIP
	RE-INVITE or SIP UPDATE [e.g. change in media components]
	Expiration of AVP [Acct-Interim-Interval]
	SIP Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP RE-INVITE or SIP UPDATE
ACR [Stop]	SIP BYE message (both normal and abnormal session termination cases)
	ISUP:REL (applicable for the MGCF)
ACR [Event]	SIP 200 OK acknowledging non-session related SIP messages, which are: • SIP NOTIFY • SIP MESSAGE • SIP REGISTER • SIP SUBSCRIBE • SIP PUBLISH
	SIP 200 OK acknowledging an initial SIP INVITE
	SIP 202 Accepted acknowledging a SIP REFER or any other method
	SIP Final Response 2xx (except SIP 200 OK)
	SIP Final/Redirection Response 3xx
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure
	SIP CANCEL, indicating abortion of a SIP session set-up

Event Based Charging

In the case of event based charging, the network reports the usage or the service rendered where the service offering is rendered in a single operation. It is reported using the ACR EVENT.

In this scenario, CTF asks the CDF to store event related charging data.

Session Based Charging

Session based charging is the process of reporting usage reports for a session and uses the START, INTERIM & STOP accounting data. During a session, a network element may transmit multiple ACR Interims' depending on the proceeding of the session.

In this scenario, CTF asks the CDF to store session related charging data.

Diameter Base Protocol

The Diameter Base Protocol maintains the underlying connection between the Diameter Client and the Diameter Server. The connection between the client and server is TCP based.

In order for the application to be compliant with the specification, state machines should be implemented at some level within the implementation.

Diameter Base supports the following Rf message commands that can be used within the application.

Table 3: Diameter Rf Messages

Command Name	Source	Destination	Abbreviation
Accounting-Request	CTF	CDF	ACR
Accounting-Answer	CDF	CTF	ACA

There are a series of other Diameter messages exchanged to check the status of the connection and the capabilities.

- Capabilities Exchange Messages: Capabilities Exchange Messages are exchanged between the diameter peers to know the capabilities of each other and identity of each other.
    - Capabilities Exchange Request (CER): This message is sent from the client to the server to know the capabilities of the server.
    - Capabilities Exchange Answer (CEA): This message is sent from the server to the client in response to the CER message.
- Device Watchdog Request (DWR): After the CER/CEA messages are exchanged, if there is no more traffic between peers for a while, to monitor the health of the connection, DWR message is sent from the client. The Device Watchdog timer (Tw) is configurable and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is considered to be down.

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

- Device Watchdog Answer (DWA): This is the response to the DWR message from the server. This is used to monitor the connection state.
- Disconnect Peer Request (DPR): This message is sent to the peer to inform to shutdown the connection. There is no capability currently to send the message to the Diameter server.
- Disconnect Peer Answer (DPA): This message is the response to the DPR request from the peer. On receiving the DPR, the peer sends DPA and puts the connection state to "DO NOT WANT TO TALK TO YOU" state and there is no way to get the connection back except for reconfiguring the peer again.

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

Timer Expiry Behavior

Upon establishing the Diameter connection, an accounting interim timer (AII) is used to indicate the expiration of a Diameter accounting session, and is configurable at the CTF. The CTF indicates the timer value in the ACR-Start, in the Acct-Interim-Interval AVP. The CDF responds with its own AII value (through the DRA), which must be used by the CTF to start a timer upon whose expiration an ACR INTERIM message must be sent. An instance of the AII timer is started in the CCF at the beginning of the accounting session, reset on the receipt of an ACR-Interim and stopped on the receipt of the ACR-Stop. After expiration of the AII timer, ACR INTERIM message will be generated and the timer will be reset and the accounting session will be continued.

Rf Interface Failures/Error Conditions

The current architecture allows for primary and secondary connections or Active-Active connections for each network element with the CDF elements.

DRA/CCF Connection Failure

When the connection towards one of the primary/Active DRAs in CCF becomes unavailable, the CTF picks the Secondary/Active IP address and begins to use that as a Primary.

If no DRA (and/or the CCF) is reachable, the network element must buffer the generated accounting data in non-volatile memory. Once the DRA connection is up, all accounting messages must be pulled by the CDF through offline file transfer.

No Reply from CCF

In case the CTF/DRA does not receive an ACA in response to an ACR, it may retransmit the ACR message. The waiting time until a retransmission is sent, and the maximum number of repetitions are both configurable by the operator. When the maximum number of retransmissions is reached and still no ACA reply has been received, the CTF/DRA sends the ACRs to the secondary/alternate DRA/CCF.

Detection of Message Duplication

The Diameter client marks possible duplicate request messages (e.g. retransmission due to the link failover process) with the T-flag as described in RFC 3588.

If the CDF receives a message that is marked as retransmitted and this message was already received, then it discards the duplicate message. However, if the original of the re-transmitted message was not yet received, it is the information in the marked message that is taken into account when generating the CDR. The CDRs are marked if information from duplicated message(s) is used.

CCF Detected Failure

The CCF closes a CDR when it detects that expected Diameter ACRs for a particular session have not been received for a period of time. The exact behavior of the CCF is operator configurable.

Rf-Gy Synchronization Enhancements

Both Rf (OFCS) and Gy (OCS) interfaces are used for reporting subscriber usage and billing. Since each interface independently updates the subscriber usage, there are potential scenarios where the reported information is not identical. Apart from Quota enforcement, OCS is utilized for Real Time Reporting (RTR), which provides a way to the user to track the current usage and also get notifications when a certain threshold is hit.

In scenarios where Rf (OFCS) and Gy (OCS) have different usage information for a subscriber session, it is possible that the subscriber is not aware of any potential overages until billed (scenario when Rf is more than Gy) or subscriber believes he has already used up the quota whereas his actual billing might be less (scenario when Gy is more than Rf). In an attempt to align both the Rf and Gy reported usage values, release 12.3 introduced capabilities to provide a way to get the reported values on both the interfaces to match as much as possible. However, some of the functionalities were deferred and this feature implements the additional enhancements.

In release 15.0 when time/volume quota on the Gy interface gets exhausted, Gy triggers "Service Data Volume Limit" and "Service Data Time Limit". Now in 16.0 via this feature, this behavior is CLI controlled. Based on the CLI command " **trigger-type { gy-sdf-time-limit { cache | immediate } | gy-sdf-unit-limit { cache | immediate } | gy-sdf-volume-limit { cache | immediate } }**" the behavior will be decided whether to send the ACR-Interim immediately or to cache the containers for future transactions. If the CLI for the event-triggers received via Gy is not configured, then those ACR-Interims will be dropped.

Releases prior to 16.0, whenever the volume/time-limit event triggers are generated, ACR-Interims were sent out immediately. In 16.0 and later releases, CLI configuration options are provided in policy accounting configuration to control the various Rf messages (ACRs) triggered for sync on this feature.

This release supports the following enhancements:

- Caches containers in scenarios when ACR-I could not be sent and reported to OFCS.
- Triggers ACR to the OFCS when the CCR to the OCS is sent instead of the current implementation of waiting for CCA from OCS.

If an ACR-I could not be sent to the OFCS, the PCEF caches the container record and sends it in the next transaction to the OFCS.

In releases prior to 16.0, once a CCR-U was sent out over Gy interface, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U.

In 16.0 and later releases, the containers are closed only after receiving CCA-U successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

For more information on the command associated with this feature, see the *Accounting Policy Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

In 17.0 and later releases, a common timer based approach is implemented for Rf and Gy synchronization. As part of the new design, Gy and Rf will be check-pointed at the same point of time for periodic as well as for full check-pointing. Thus, the billing records will always be in sync at all times regardless of during an ICSR switchover event, internal events, session manager crashes, inactive Rf/Gy link, etc. This in turn avoids any billing discrepancies.

Cessation of Rf Records When UE is IDLE

Releases prior to 16.0, when the UE was identified to be in IDLE state and not sending any data, the P-GW generated Rf records. During this scenario, the generated Rf records did not include Service Data Containers (SDCs).

In 16.0 and later releases, the Rf records are not generated in this scenario. New CLI configuration command "**session idle-mode suppress-interim**" is provided to enable/disable the functionality at the ACR level to control the behavior of whether an ACR-I needs to be generated or not when the UE is idle and no data is transferred.

That is, this CLI configuration is used to control sending of ACR-I records when the UE is in idle mode and when there is no data to report.

For more information on the command, see the *Accounting Policy Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

QoS Change Scenarios

QOS_CHANGE Trigger in Rf Records During eHRPD-LTE Handoff

In releases prior to 20, QOS_CHANGE is reported as the value for Change-Condition AVP in the Service-Data-Container (SDC) of Rf accounting records (for accounting level SDF/SDF+accounting keys QCI) when eHRPD to LTE handoff occurs. Typically, the QOS_CHANGE should not be present as the PCRF does not enforce QoS via any QoS IE in eHRPD/CDMA RAT. In 20 and later releases, the SDC in the generated Rf record does not include QOS_CHANGE trigger during handoff from eHRPD to LTE.

QoS Change for Default Bearer

Releases prior to 20, in a multi-bearer call, when an update message (CCA-U or RAR) from PCRF changes the QoS (QCI/ARP) of default bearer and in the same message installs a predefined or dynamic rule on the newly updated default bearer, spurious Normal Release (NR) Service Data Volume (SDV) containers were added to Rf interim records for the dedicated bearers. In this scenario, the system used to send Normal Release buckets for the non-default bearers even if these bearers were not changed.

In release 20 and beyond, for a change in the QoS of default bearer, NR SDV containers will not be seen unless the corresponding bearer is torn down. Only QoS change containers are closed/released for the bearer that underwent QoS Change, i.e. the default bearer.

Diameter Rf Duplicate Record Generation

This section describes the overview and implementation of Rf Duplicate Record Generation feature.

This section discusses the following topics for this feature:

Feature Description

This feature is introduced to support creation and communication of duplicate Rf records to secondary AAA group servers configured for the Rf interface.

To achieve this functionality, the following configurations must be enabled –

- **aaa group** CLI command under APN to configure a maximum of 2 AAA groups - primary and secondary AAA groups, or two different endpoints for Rf Diameter accounting servers
- **diameter accounting duplicate-record** under AAA group to allow Rf duplicate record creation

The **diameter accounting duplicate-record** is a new CLI command introduced in this release for duplicating the Rf START, INTERIM and STOP accounting records.

Important This is a license-controlled CLI command. For more information, contact your Cisco account representative.

In releases prior to 21, gateway allows only one AAA group configuration per APN for Rf accounting. The AAA group is configured to load balance across multiple servers to pass the Rf traffic and also expect an accounting answer. Note that the secondary AAA group configuration is allowed currently but is restricted to only RADIUS accounting.

In release 21 and beyond, the gateway is provided with the ability to configure a secondary AAA group per APN for the Rf interface, and send the duplicate Diameter Rf accounting records to the secondary AAA group servers. The secondary AAA group is used for non-billing purposes only.

Important The failed duplicate records will neither be written to HDD nor added to the archival list.

There is no change in the current behavior with the primary AAA group messages. The primary AAA group is independent of the secondary AAA group, and it has multiple Rf servers configured. When the Rf servers do not respond even after multiple retries as per the applicable configuration, the Rf records are archived and stored in HDD. This behavior continues as is irrespective of the configuration of secondary aaa-group.

Secondary aaa group has a very similar configuration as the primary aaa group except that the new CLI command **diameter accounting duplicate-record** is additionally included to configure the secondary aaa-group. It is also important to note that different Diameter endpoints and a separate set of Rf servers should be provisioned for both primary and secondary AAA groups.

If all the configured servers are down, the request message will be discarded without writing it in HDD or archiving at aaamgr.

The original and duplicate Rf messages use two different aaa-groups and two different Diameter endpoints. Hence, the values for Session-ID AVP will be different. Based on the configuration of primary and secondary endpoints the values for Origin-Host, Origin-Realm, Destination-Realm, and Destination-Host AVPs may be different. Also based on the configuration under policy accounting for inclusion of virtual/gn apn name for secondary group Called-Station-ID AVP might change. All other AVPs will have the same values as with the primary aaa group Rf message.

Also, note that the values such as Acct-Interim-Interval (AII) interval received in ACA from secondary group of AAA servers will be ignored.

Relationships to Other Features

This feature can be used in conjunction with Virtual APN Truncation feature to achieve the desired results.

The Virtual APN Truncation feature is new in release 21. For more information on this feature, see the administration guide for the product you are deploying.

Limitations

The following are the limitations of this feature:

- Only one secondary AAA group can be configured per APN.
- If all the Rf peers under secondary aaa group are down and duplicate Start Record is not sent, then the duplicate Interim and Stop records will also not be sent to any of the secondary aaa group servers even though they arrived later. However if the servers are up and duplicate Start record was sent but the server did not respond, duplicate Start will be dropped after all the retries. In this case, the duplicate Interim and Stop records may be sent out to the server.
- In cases when duplicate Start record was sent, but during duplicate Interim/Stop record generation peers were not responding/down, after all retries duplicate Interim and Stop records will be dropped and will not be written to HDD.
- Minimal impact to memory and CPU is expected due to the duplicate record generation for every primary Rf record.

Configuring Rf Duplicate Record Generation

The following section provides the configuration commands to enable the Rf duplicate record generation.

Configuring Secondary AAA Group

Use the following configuration commands to configure the secondary AAA group for receiving the duplicate Rf records.

```
configure
   context context_name
      apn apn_name
         aaa group group_name
         aaa secondary-group group_name
         exit
```

Notes:

- **aaa group** *group_name*: Specifies the AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.

- **secondary group** *group_name*: Specifies the secondary AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.

Configuring Duplication of Rf Records

Use the following configuration commands to configure the system to create a secondary feed of Rf records and send them to the secondary AAA group.

```
configure
   context context_name
      aaa group group_name
         diameter accounting duplicate-record
         exit
```

Notes:

- **duplicate-record**: Sends duplicate Rf records to configured secondary AAA group. This keyword is license dependent. For more information, contact your Cisco account representative.
- The default configuration is **no diameter accounting duplicate-record**. By default, this feature is disabled.
- The secondary aaa group must be configured under APN configuration mode before enabling the **diameter accounting duplicate-record** CLI command.

Verifying the Rf Duplicate Record Generation Configuration

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

show configuration

show aaa group all

- or -

show aaa group *group_name*

group_name must be the name of the AAA group specified during the configuration.

This command displays all the configurations that are enabled within the specified AAA group.

The following is a sample configuration of this feature.

```
configure
   context source
      apn domainname.com
         associate accounting-policy policy_accounting_name
         aaa group group1
         aaa secondary-group group2
         exit
      aaa group group1
         diameter accounting dictionary aaa-custom4
         diameter accounting endpoint rf_endpoint1
         diameter accounting server rf_server1 priority 1
         diameter accounting server rf_server2 priority 2
         exit
      aaa group group2
         diameter accounting dictionary aaa-custom4
```

```
            diameter accounting endpoint rf_endpoint2
            diameter accounting duplicate-record
            diameter accounting server rf_server3 priority 3
            diameter accounting server rf_server4 priority 4
            exit
        diameter endpoint rf-endpoint1
            use-proxy
            origin host rf-endpoint1.carrier.com address 192.50.50.3
            no watchdog-timeout
            response-timeout 20
            connection retry-timeout 5
            peer rf_server1 realm domainname.com address 192.50.50.4 port 4872
            peer rf_server2 realm domainname.com address 192.50.50.4 port 4873
            exit
        diameter endpoint rf-endpoint2
            use-proxy
            origin host rf-endpoint2.carrier.com address 192.50.50.2
            no watchdog-timeout
            response-timeout 20
            connection retry-timeout 5
            peer rf_server3 realm domainname.com address 192.50.50.5 port 4892
            peer rf_server4 realm domainname.com address 192.50.50.5 port 4893
end
```

Notes:

- The **diameter accounting duplicate-record** CLI is license specific. So, the corresponding license must be enabled for the CLI command to be configured.
- Both primary and secondary aaa groups are preferred to have different accounting endpoint names.

Monitoring and Troubleshooting the Rf Duplicate Record Generation

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

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

- Verify if the feature is enabled using **show configuration** or **show aaa group all** CLI command. If not enabled, configure the diameter accounting duplicate-record CLI command and check if it works.
- Collect the output of **show diameter aaa statistics** command and analyze the debug statistics. Also, check the reported logs, if any. For further analysis, contact Cisco account representative.

show diameter aaa-statistics

The following statistics are added to the output of this show command for duplicate Rf records which were dropped because of the failure in sending the Accounting records instead of adding them to HDD or archival list.

- Duplicate Accounting Records Stats
  - ACR-Start Dropped
  - ACR-Interim Dropped

- ACR-Stop Dropped

These statistics are maintained per aaamgr instance level. For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

These statistics can also be collected per group basis/server basis for duplicate records i.e. through **show diameter aaa-statistics group** <*group_name*> and **show diameter aaa-statistics server** <*server_name*> CLI commands.

Truncation of Virtual APN for Rf Records

This feature enables the truncation of Virtual APN (VAPN) returned by S6b server to be sent to Gx, Gy and Rf interfaces.

Feature Description

Currently there is no way to quickly turn on the Rf accounting to the Data Streaming Service (DSS) server per Virtual APN (S6b-VAPN) without reaching all nodes in the network and provision the Virtual APN on each of them. This feature is implemented to truncate the virtual APN name returned by S6b server with the configured standard delimiters. In this way a single configuration per node can be utilized for all enterprises based on a virtual APN. This approach will significantly reduce the size and time to provision new enterprises with the requested feature.

To achieve this functionality, a configuration is added per APN to enable truncation of S6b-VAPN and also to configure the delimiter(s) where the APN name is to be truncated. Standard delimiters like (.) and (-) are used since APN name supports only these two characters apart from the alphanumeric ones.

If AAA server returns both hyphen and dot delimiters or the same delimiter twice or more as a virtual-apn, then the first delimiter will be considered as a separator. For example, if the AAA server returns the virtual-apn as xyz-cisco.com, then hyphen is the separator.

AAA manager performs the truncation of the Virtual APN name based on the APN configuration and provides the correct APN profile for the truncated APN name. If the truncation is successful, the full virtual APN name will be sent to Gx, Gy and Rf interfaces.

Accounting records are required to support real-time usage notification and device management functionality. So, the **apn-name-to-be-included** CLI command is extended to enable actual APN (Gn-APN) or virtual APN (S6b returned virtual APN) name to be included in Called-Station-ID AVP in the secondary Rf accounting records (secondary server group) under policy accounting configuration. Currently, policy accounting configuration supports sending the Gn-APN/S6b-VAPN in Called-Station-ID for primary Rf server. With this CLI command, this functionality is extended for the secondary Rf server.

A new AAA attribute “Secondary-Called-Station-ID” is added to support sending Gn/Virtual APN name in the Called-Station-ID AVP for duplicate Rf records sent to secondary group Rf server.

Configuring Virtual APN Truncation for Rf Records

The following section provides the configuration commands to enable the Virtual APN Truncation feature for Rf records.

Configuring Gn-APN/VAPN for Rf Accounting

Use the following configuration commands to configure the actual APN or Virtual APN (VAPN) for Rf accounting.

```
configure
  context context_name
    policy accounting policy_name
      apn-name-to-be-included { gn | virtual } [ secondary-group { gn |
 virtual } ]
      end
```

Notes:

- **apn-name-to-be-included**: Configures the APN name to be included in the Rf messages for primary server group.
- **secondary-group { gn | virtual }**: Configures the APN name to be included in the Rf messages for secondary server group.
- **gn**: Configures the Gn APN name to be included in the Rf messages.
- **virtual**: Configures the virtual APN name to be included in the Rf messages.
- By default, the apn name to be included in Called-Station-ID AVP is Gn-APN for both primary and secondary Rf server groups.
- If the secondary group configuration is not available, the default behavior is to have Gn APN for secondary Rf group duplicate records.

Configuring Truncation of Virtual APN

Use the following configuration commands to configure the gateway to truncate the APN name returned from S6b interface.

```
configure
  context context_name
    apn apn_name
      virtual-apn { gcdr apn-name-to-be-included { gn | virtual } |
truncate-s6b-vapn delimiter { dot [ hyphen ] | hyphen [ dot ] } }
      end
```

Notes:

- For information on the existing keywords, see the *Command Line Interface Reference* guide.
- **truncate-s6b-vapn**: Allows truncation of virtual APN received from S6b at the configured delimiter character.
- **delimiter { dot [hyphen] | hyphen [dot] }**: Configures the delimiter for truncation of virtual APN received from S6b. If the CLI command is configured, the S6b returned virtual APN will be truncated at the configured delimiter.
  - **dot**: Configures the delimiter to dot (.) for truncation of S6b-VAPN
  - **hyphen**: Configures the delimiter to hyphen (-) for truncation of S6b-VAPN
- Both dot and hyphen delimiters can be configured in the same line or a new line.
- **no virtual-apn truncate-s6b-vapn**: Disables the truncation of virtual APN name. If both delimiters should be disabled at once, use the **no virtual-apn truncate-s6b-vapn** CLI command.

If a particular delimiter needs to disabled, it should be done explicitly. For example, if the dot delimiter should be disabled, use the **no virtual-apn truncate-s6b-vapn delimiter dot** CLI command.

- By default this feature will be disabled and no delimiter will be configured.
- This CLI command takes effect only when S6b server returns virtual APN name in Authentication Authorization Accept (AAA) message.
- If the separator character is not present in the received S6b virtual APN name, then the whole virtual APN name will be considered for configuration look-up.

Verifying the Virtual APN Truncation Configuration

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

show configuration apn *apn_name*

apn_name must be the name of the APN specified during the feature configuration.

This command displays all the configurations that are enabled within the specified APN name. The following is a sample output of this show command.

```
[local]st40# show configuration apn intershat
configure
   context ingress
      apn intershat
         pdp-type ipv4 ipv6
         bearer-control-mode mixed
         virtual-apn truncate-s6b-vapn delimiter hyphen
         end
```

Monitoring and Troubleshooting the Virtual APN Truncation

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

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

- Verify if the feature is enabled using **show configuration apn** *apn_name* CLI command. If not enabled, configure the **virtual-apn truncate-s6b-vapn delimiter { dot [hyphen] | hyphen [dot] } }** CLI command and check if it works.
- Collect the output of **show apn statistics** CLI command and analyze the debug statistics. For further assistance, contact Cisco account representative.

Important For P-GW, GGSN and SAEGW services, if the truncation of S6b returned virtual APN name fails and the virtual APN name is not configured, the call will be rejected with ‘unknown-apn-name’ cause.

show apn statistics

This show command uses the existing APN statistics to populate the truncated virtual APN name, if this feature is enabled.

show subscribers ggsn-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

show subscribers pgw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

show subscribers saegw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

Accounting Record Stop Location Report

Previous Behavior: When P-GW or S-GW sends new User Location Information (ULI) message in an ACR stop message to Offline Charging System (OFCS) through the Rf interface, the reported location at the end of sessions was not aligning with the expected location reporting. The location used in the Accounting Stop Record (ACR Stop) was inconsistent and during location reporting it caused an `ACR stop` interim messages rather than the location before the ACR was sent

New Behavior: In the StarOS 21.22 and later releases, an existing User Location Information (ULI) is sent to the Accounting Record (ACR) Stop message on offline charging (RF) interface for GGSN, P-GW, and SAEGW when Delete Session Request is received with a New ULI.

How it Works

This section describes how offline charging for subscribers works with Rf interface support in GPRS/eHRPD/LTE/IMS networks.

The following figure and table explain the transactions that are required on the Diameter Rf interface in order to perform event based charging. The operation may alternatively be carried out prior to, concurrently with or after service/content delivery.

Figure 3: Rf Call Flow for Event Based Charging

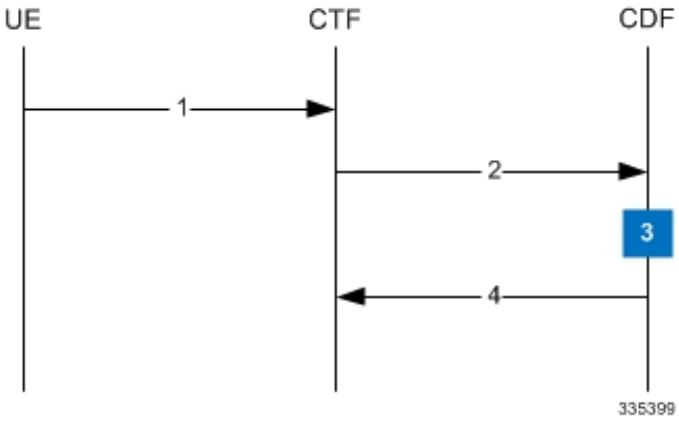


Table 4: Rf Call Flow Description for Event Based Charging

Step	Description
1	The network element (CTF) receives indication that service has been used/delivered.
2	The CTF (acting as Diameter client) sends Accounting-Request (ACR) with Accounting-Record-Type AVP set to EVENT_RECORD to indicate service specific information to the CDF (acting as Diameter server).
3	The CDF receives the relevant service charging parameters and processes accounting request.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type AVP set to EVENT_RECORD to the CTF in order to inform that charging information was received.

The following figure and table explain the simple Rf call flow for session based charging.

Figure 4: Rf Call Flow for Session Based Charging

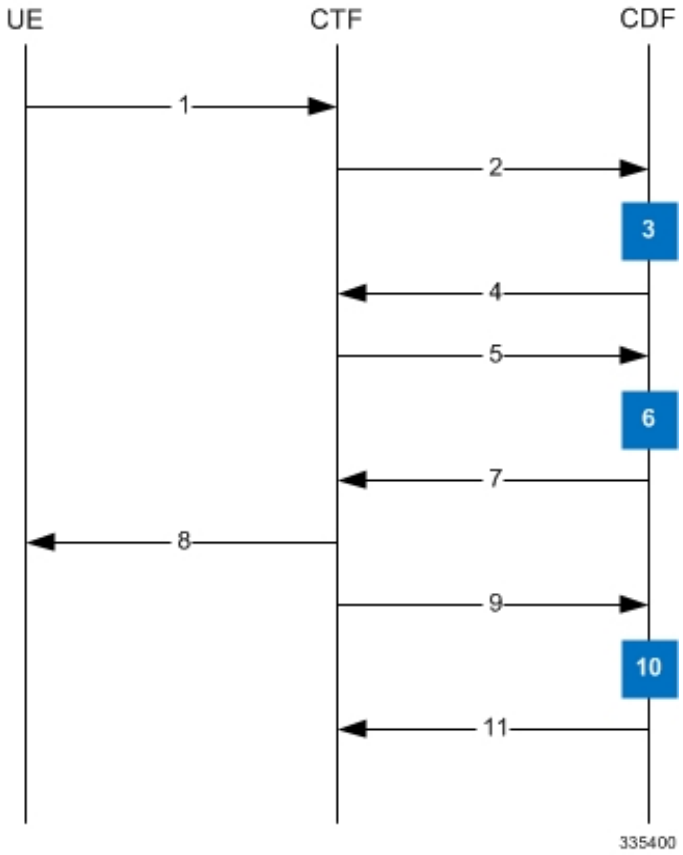


Table 5: Rf Call Flow Description for Session Based Charging

Step	Description
1	The CTF receives a service request. The service request may be initiated either by the user or the other network element.
2	In order to start accounting session, the CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to START_RECORD to the CDF.
3	The session is initiated and the CDF opens a CDR for the current session.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to START_RECORD to the CTF and possibly Acct-Interim-Interval AVP (AII) set to non-zero value indicating the desired intermediate charging interval.

Step	Description
5	When either AII elapses or charging condition changes are recognized at CTF, the CTF sends an Accounting-Request (ACR) with Accounting-Record-Type AVP set to INTERIM_RECORD to the CDF.
6	The CDF updates the CDR in question.
7	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to INTERIM_RECORD to the CTF.
8	The service is terminated.
9	The CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to STOP_RECORD to the CDF.
10	The CDF updates the CDR accordingly and closes the CDR.
11	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to STOP_RECORD to the CTF.

Configuring Rf Interface Support

To configure Rf interface support:

1. Configure the core network service as described in this Administration Guide.
2. Enable Active Charging Service (ACS) and create ACS as described in the *Enhanced Charging Services Administration Guide*.

Important The procedures in this section assume that you have installed and configured your chassis including the ECS installation and configuration as described in the *Enhanced Charging Services Administration Guide*.

3. Enable Rf accounting in ACS as described in Enabling Rf Interface in Active Charging Service, on page 22.
4. Configure Rf interface support as described in the relevant sections:
   - Configuring GGSN / P-GW Rf Interface Support, on page 22
   - Configuring P-CSCF/S-CSCF Rf Interface Support, on page 37

Important In StarOS versions 19 and later, the Rf interface is not supported on the S-GW.

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.

Enabling Rf Interface in Active Charging Service

To enable the billing record generation and Rf accounting, use the following configuration:

```
configure
   active-charging service <service_name>
      rulebase <rulebase_name>
         billing-records rf
        active-charging rf { rating-group-override | service-id-override
 }
         end
```

Notes:

- Prior to creating the Active Charging Service (ACS), the **require active-charging** command should be configured to enable ACS functionality.
- The **billing-records rf** command configures Rf record type of billing to be performed for subscriber sessions. Rf accounting is applicable only for dynamic and predefined ACS rules.

  For more information on the rules and its configuration, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- The **active-charging rf** command is used to enforce a specific rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

  For more information on this command, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring GGSN / P-GW Rf Interface Support

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

```
configure
   context <context_name>
      apn <apn_name>
         associate accounting-policy <policy_name>
         exit
      policy accounting <policy_name>
         accounting-event-trigger { cgi-sai-change | ecgi-change |
```

```
flow-information-change | interim-timeout | location-change | rai-change
 | tai-change } action { interim | stop-start }
         accounting-keys qci
accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }
         cc profile index { buckets num | interval seconds | sdf-interval
seconds | sdf-volume { downlink octets { uplink octets } | total octets |
uplink octets { downlink octets } }  | serving-nodes num | tariff time1 min
hrs [ time2 min hrs...time4 min hrs ] | volume { downlink octets { uplink octets
 } | total octets | uplink octets { downlink octets } } }
         max-containers { containers | fill-buffer }
         end
```

Notes:

- The policy can be configured in any context.
- For information on configuring accounting levels/policies/modes/event triggers, refer to the *Accounting Policy Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- Depending on the triggers configured, the containers will either be cached or released. In the case of GGSN/P-GW, the containers will be cached when the event trigger is one of the following:
  - QOS_CHANGE
  - FLOW_INFORMATION_CHANGE
  - LOCATION_CHANGE
  - SERVING_NODE_CHANGE
  - SERVICE_IDLE
  - SERVICE_DATA_VOLUME_LIMIT
  - SERVICE_DATA_TIME_LIMIT
  - IP_FLOW_TERMINATION
  - TARIFF_CHANGE

  If the event trigger is one of the following, the containers will be released:
  - VOLUME_LIMIT
  - TIME_LIMIT
  - RAT_CHANGE
  - TIMEZONE_CHANGE
  - PLMN_CHANGE

Important Currently, SDF and flow level accounting are supported in P-GW.

The following assumptions guide the behavior of P-GW, GGSN and CCF for Change-Condition triggers:

- Data in the ACR messages due to change conditions contain the snapshot of all data that is applicable to the interval of the flow/session from the previous ACR message. This includes all data that is already sent and has not changed (e.g. SGSN-Address).
- All information that is in a PDN session/flow up to the point of the Change-Condition trigger is captured (snapshot) in the ACR-Interim messages. Information about the target Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change/etc will be in subsequent Rf messages.

Table 6: P-GW/GGSN and CCF Behavior for Change-Condition in ACR-Stop and ACR-Interim for LTE/e-HRPD/GGSN

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Stop	Normal Release	YES	NO	YES	Normal Release	Normal Release	When PDN/IP session is closed, C-C in both level will have Normal Release.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Normal Release	YES	NO	NO	N/A	Normal Release	Flow is closed, SDC CC is populated and closed container is added to record. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.
Stop	Abnormal Release	YES	NO	YES	Abnormal Release	Abnormal Release	When PDN/IP session is closed, C-C in both level will have Abnormal Release.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Abnormal Release	YES	NO	NO	N/A	Abnormal Release	Flow is closed, SDC CC is populated and closed container is added to record. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	QoS-Change	YES	NO	NO	N/A	QoS-Change	The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Volume Limit	YES	YES	NO	Volume Limit	Volume Limit	For PDN/IP Session Volume Limit. The Volume Limit is configured as part of the Charging profile and the ChargingCharacteristics AVP will carry this charging profile that will passed on from the HSS/AAA to P-GW/GGSN through various interfaces. The charging profile will be provisioned in the HSS.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Time Limit	YES	YES	NO	Time Limit	Time Limit	For PDN/IP Session Time Limit. The Time Limit is configured as part of the Charging profile and the Charging Characteristics AVP will carry this charging profile that will passed on from the HSS/AAA to P-GW/GGSN through various interfaces. The charging profile will be provisioned in the HSS.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Serving Node Change	YES	NO	NO	N/A	Serving Node Change	The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.
Interim	Serving Node PLMN Change	YES	YES	NO	Serving Node PLMN Change	Serving Node PLMN Change	

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	User Location Change	YES	NO	NO	N/A	User Location Change	This is BSID Change in eHRPD. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.
Interim	RAT Change	YES	YES	NO	RAT Change	RAT Change	
Interim	UE Timezone Change	YES	YES	NO	UE Timezone change	UE Timezone change	This is not applicable for eHRPD.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Tariff Time Change	YES	NO	NO	N/A	Tariff Time Change	Triggered when Tariff Time changes. Tariff Time Change requires an online charging side change. The implementation of this Change Condition is dependent on implementation of Online Charging update.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Idled Out	YES	NO	NO	N/A	Service Idled Out	Flow Idled out. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Volume Limit	YES	NO	NO	N/A	Service Data Volume Limit	Volume Limit reached for a specific flow. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Time Limit	YES	NO	NO	N/A	Service Data Time Limit	Time Limit reached for a specific flow. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Max Number of Changes in Charging Conditions	YES	YES	NO	YES	YES, Will include SDC that correponds to the CCs that occurred (Normal Release of Flow, Abnormal Release of Flow, QoS-Change, Serving Node Change, User Location Change, Tariff Time Change, Service Idled Out, Service Data Volunme Limt, Service Data Time Limit)	

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
							This ACR[Interim] is triggered at the instant when the Max Number of changes in charging conditions takes place. Max Change Condition is applicable for QoS-Change, Service-Idled Out, ULI change, Flow Normal Release, Flow Abnormal Release, Service Data Volume Limit, Service Data Time Limit, AII Timer ACR Interim and Service Node Change CC only. The Max Number of Changes in Charging Conditions is set at 10. Example assuming 1 flow in the PDN Session: [1] Max Number of Changes in Charging Conditions

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
							set at P-GW/GGSN = 2. [2] Change Condition 1 takes place. No ACR Interim is sent. P-GW/GGSN stores the SDC. [3] Change Condition 2 takes place. An ACR Interim is sent. Now Max Number of Changes in Charging conditions is populated in the PS-Information 2 Service Data Containers (1 for each change condition) are populated in the ACR Interim. [4] CCF creates the partial record.
Stop	Management Intervention	YES	NO	YES	YES	YES	Management intervention will close the PDN session from P-GW/GGSN.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	-	YES	NO	NO	N/A	N/A	This is included here to indicate that an ACR[Interim] due to AII timer will contain one or more populated SDC/s for a/all flow/s, but Change-Condition AVP will NOT be populated.

Configuring P-CSCF/S-CSCF Rf Interface Support

To configure P-CSCF/S-CSCF Rf interface support, use the following configuration:

```
configure
   context vpn
      aaa group default
         diameter authentication dictionary aaa-custom8
         diameter accounting dictionary aaa-custom2
         diameter accounting endpoint <endpoint_name>
         diameter accounting server <server_name> priority <priority>
         exit
      diameter endpoint <endpoint_name>
         origin realm <realm_name>
         use-proxy
         origin host <host_name> address <ip_address>
         peer <peer_name> address <ip_address>
         exit
      end
```

Notes:

- For information on commands used in the basic configuration for Rf support, refer to the *Command Line Interface Reference*.

Gathering Statistics

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

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

Statistics/Information	Action to perform
Complete statistics for Diameter Rf accounting sessions	**show diameter aaa-statistics**

The following is a sample output of the **show diameter aaa-statistics** command:

```
Authentication  Servers Summary
 ------------------------------
Message Stats :
  Total MA Requests:            0       Total MA Answers:             0
  MAR - Retries:                0       MAA Timeouts:                 0
  MAA - Dropped:                0
  Total SA Requests:            0       Total SA Answers:             0
  SAR - Retries:                0       SAA Timeouts:                 0
  SAA - Dropped:                0
  Total UA Requests:            0       Total UA Answers:             0
  UAR - Retries:                0       UAA Timeouts:                 0
  UAA - Dropped:                0
  Total LI Requests:            0       Total LI Answers:             0
  LIR - Retries:                0       LIA Timeouts:                 0
  LIA - Dropped:                0
  Total RT Requests:            0       Total RT Answers:             0
  RTR - Rejected:               0
  Total PP Requests:            0       Total PP Answers:             0
  PPR - Rejected:               0
  Total DE Requests:            0       Total DE Answers:             0
  DEA - Accept:                 0       DEA - Reject:                 0
  DER - Retries:                0       DEA Timeouts:                 0
  DEA - Dropped:                0
  Total AA Requests:            0       Total AA Answers:             0
  AAR - Retries:                0       AAA Timeouts:                 0
  AAA - Dropped:                0
  ASR:                          0       ASA:                          0
  RAR:                          0       RAA:                          0
  STR:                          0       STA:                          0
  STR - Retries:                0
Message Error Stats:
  Diameter Protocol Errs:       0       Bad Answers:                  0
  Unknown Session Reqs:         0       Bad Requests:                 0
  Request Timeouts:             0       Parse Errors:                 0
  Request Retries:              0
Session Stats:
  Total Sessions:               0       Freed Sessions:               0
  Session Timeouts:             0       Active Sessions:              0
STR Termination Cause Stats:
  Diameter Logout:              0       Service Not Provided:         0
  Bad Answer:                   0       Administrative:               0
  Link Broken:                  0       Auth Expired:                 0
  User Moved:                   0       Session Timeout:              0
  User Request:                 0       Lost Carrier                  0
  Lost Service:                 0       Idle Timeout                  0
  NAS Session Timeout:          0       Admin Reset                   0
  Admin Reboot:                 0       Port Error:                   0
  NAS Error:                    0       NAS Request:                  0
  NAS Reboot:                   0       Port Unneeded:                0
  Port Preempted:               0       Port Suspended:               0
  Service Unavailable:          0       Callback:                     0
  User Error:                   0       Host Request:                 0
 Accounting Servers Summary
```

```
 ---------------------------
Message Stats :
  Total AC Requests:             0        Total AC Answers:              0
  ACR-Start:                     0        ACA-Start:                     0
  ACR-Start  Retries :           0        ACA-Start  Timeouts:           0
  ACR-Interim:                   0        ACA-Interim:                   0
  ACR-Interim  Retries :         0        ACA-Interim  Timeouts:         0
  ACR-Event:                     0        ACA-Event:                     0
  ACR-Stop :                     0        ACA-Stop:                      0
  ACR-Stop  Retries :            0        ACA-Stop  Timeouts:           0
  ACA-Dropped :                  0
AC Message Error Stats:
  Diameter Protocol Errs:        0        Bad Answers:                   0
  Unknown Session Reqs:          0        Bad Requests:                  0
  Request Timeouts:              0        Parse Errors:                  0
  Request Retries:               0
```