

**Oracle® Communications
Diameter Signaling Router**

Charging Proxy Application (CPA) and Offline Charging Solution

User's Guide

910-6825-001 Revision B

May 2014

Oracle® Communications Charging Proxy Application (CPA) and Offline Charging Solution User's Guide
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

Chapter 1: Introduction.....	5
Overview.....	6
Scope and Audience.....	6
Documentation Admonishments.....	6
Manual Organization.....	7
Customer Care Center.....	7
Emergency Response.....	9
Related Publications.....	10
Locate Product Documentation on the Customer Support Site.....	11
Chapter 2: Offline Charging Solution.....	12
Offline Charging Solution.....	13
Introduction to the Charging Proxy Application.....	13
Introduction to the Charging Session Binding Repository.....	13
Chapter 3: Charging Proxy Application.....	15
Pre-Configuration Activities.....	16
Verifying Charging SBR Server and Server Group Configuration.....	16
Diameter Configuration for CPA.....	16
Configuration.....	19
System Options.....	20
Message copy.....	22
SBR page.....	25
SBR Subresource Mapping page.....	26
Post-Configuration Activities.....	28
Enabling the CPA.....	28
Enabling Connections.....	29
Status Verification.....	29
DSR Bulk Import and Export.....	29
Glossary.....	32

List of Tables

Table 1: Admonishments.....6

Table 2: System Options page elements.....20

Table 3: Message Copy Elements.....22

Chapter 1

Introduction

Topics:

- *Overview.....6*
- *Scope and Audience.....6*
- *Documentation Admonishments.....6*
- *Manual Organization.....7*
- *Customer Care Center.....7*
- *Emergency Response.....9*
- *Related Publications.....10*
- *Locate Product Documentation on the Customer Support Site.....11*

This chapter contains an overview of the procedures to configure the Charging Proxy Application. The contents include sections on the scope, audience, and organization of the documentation, and how to contact Oracle for assistance.

Overview

The Charging Proxy Application (CPA) document provides information about how to use the DSR GUI to configure the CPA.

The document provides procedures to:

- Edit System Options
- Edit Message Copy configuration settings
- Edit Session Binding Repository (SBR) configuration settings
- Edit SBR Subresource Mapping configuration settings

Scope and Audience

This manual does not describe how to install or replace software or hardware.

This manual is intended for personnel who configure the Charging Proxy Application.

This manual contains procedures for configuring CPA using the DSR GUI.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
 DANGER	Danger: (This icon and text indicate the possibility of <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)

Icon	Description
	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage.</i>)

Manual Organization

This manual is organized into the following chapters:

- [Introduction](#) contains general information about the CPA help documentation, the organization of this document, and how to get technical assistance.
- [Offline Charging Solution](#) contains information about the Offline Charging Solution and its components.
- [Charging Proxy Application](#) provides information about configuring System Options, Message Copy, Session Binding Repository, and SBR Subresource Mapping.

Customer Care Center

Oracle's Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Technical Assistance Centers are located around the globe in the following locations:

Related - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

Phone:

1-888-367-8552 (toll-free, within continental USA and Canada)

1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

Phone:

+1-919-460-2150

TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

- **Argentina**

Phone:

0-800-555-5246 (toll-free)

- **Brazil**

Phone:

0-800-891-4341 (toll-free)

TAC Regional Support Office Hours:

8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

- **Chile**

Phone:

1230-020-555-5468

- **Colombia**

Phone:

01-800-912-0537

- **Dominican Republic**

Phone:

1-888-367-8552

- **Mexico**

Phone:

001-888-367-8552

- **Peru**

Phone:

0800-53-087

- **Puerto Rico**

Phone:

1-888-367-8552

- **Venezuela**

Phone:

0800-176-6497

- **Europe, Middle East, and Africa**

Regional Office Hours:

8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

- **Signaling**

Phone:

+44 1784 467 804 (within UK)

- **Software Solutions**

Phone:

+33 3 89 33 54 00

- **Asia**

- **India**

Phone:

+91-124-465-5098 or +1-919-460-2150

TAC Regional Support Office Hours:

10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

- **Singapore**

Phone:

+65 6796 2288

TAC Regional Support Office Hours:

9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by Oracle's Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions

- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle's Tekelec Customer Care Center.

Related Publications

The Diameter Signaling Router (DSR) documentation set includes the following publications, which provide information for the configuration and use of DSR and related applications.

Getting Started includes a product overview, system architecture, and functions. It also explains the DSR GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets.

Feature Notice describes new features in the current release, provides the hardware baseline for this release, and explains how to find customer documentation on the Oracle Customer Support Site.

Roadmap to Hardware Documentation provides links to access manufacturer online documentation for hardware related to the DSR.

Operation, Administration, and Maintenance (OAM) Guide provides information on system-level configuration and administration tasks for the advanced functions of the DSR, both for initial setup and maintenance.

Communication Agent User's Guide explains how to use the Communication Agent GUI pages to configure Remote Servers, Connection Groups, and Routed Servers, and to maintain configured connections.

Diameter User's Guide explains how to use the Diameter GUI pages to manage the configuration and maintenance of Diameter Configuration components, including Local and Peer Nodes, Connections, Configuration Sets, Peer Routing Rules, Application Route Tables, System Options, and DNS options; describes the functions of Diameter Message Copy; and describes DSR capacity and congestion controls.

Diameter Mediation User's Guide describes the functions of Diameter Mediation, and explains how to use the Diameter Mediation GUI pages (nested inside the Diameter GUI folder) to configure and test Rule Templates, how to use the Formatting Value Wizard, and how to configure Rule Sets.

IP Front End (IPFE) User's Guide explains how to use the IPFE GUI pages to configure IPFE to distribute IPv4 and IPv6 connections from multiple clients to multiple nodes.

Range-Based Address Resolution (RBAR) User's Guide explains how to use the RBAR GUI pages to configure RBAR to route Diameter end-to-end transactions based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity address ranges and individual addresses.

Full-Address Based Resolution (FABR) User's Guide explains how to use the FABR GUI pages to configure FABR to resolve designated Diameter server addresses based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity addresses.

Charging Proxy Application (CPA) and Offline Charging Solution User's Guide describes the Offline Charging Solution and explains how to use the CPA GUI pages to set System Options for CPA, configure the CPA's Message Copy capability, and configure the Session Binding Repository for CPA.

Policy DRA User's Guide describes the topology and functions of the Policy Diameter Routing Agent (Policy DRA) DSR Application and the Policy Session Binding Repository, and explains how to use the GUI pages to configure Policy DRA.

Gateway Location Application (GLA) User's Guide describes the functions of retrieving subscriber data stored in Policy Session Binding Repository (pSBR) provided by Policy DRA and explains how to use the GUI pages to configure GLA.

DSR Alarms, KPIs, and Measurements Reference provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual Diameter measurement value; and explains how to generate reports containing current alarm, event, KPI, and measurement information.

DSR Administration Guide describes DSR architecture, functions, configuration, and tools and utilities (IPsec, Import/Export, DIH, and database backups); and provides references to other publications for more detailed information.

Locate Product Documentation on the Customer Support Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the Oracle Customer Support site at <http://docs.oracle.com>.
2. Under **Applications**, click the link for **Communications**.
The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As**.

Chapter 2

Offline Charging Solution

Topics:

- *Offline Charging Solution.....13*
- *Introduction to the Charging Proxy Application.....13*
- *Introduction to the Charging Session Binding Repository.....13*

This section describes the purpose of the Offline Charging Solution and its components.

Offline Charging Solution

In order to provide load distribution and failover support for a growing number of Charging Trigger Functions (CTFs) connected to a growing number of Charging Data Functions (CDFs), a Charging Proxy Function (CPF) has been established as an intermediary between the CTFs and the CDFs.

The Charging Proxy Function provides topology hiding. The CPF appears as a single CDF to the CTFs, and as a single CTF to the CDFs.

Messages in a Diameter offline charging session consist of the ACRs from the CTFs to the CDFs and the ACAs from the CDFs to the CTFs.

The Charging Proxy Function consists of the following components:

- Charging Proxy Application (CPA)
- Charging Session Binding Repository (Charging SBR)
- Optional IP Front End (IPFE)

CPA is a DSR Application that is responsible for routing Diameter accounting (Rf) messages that are being exchanged between clients (CTFs) and server (CDFs).

The Charging SBR is a database server application. It stores data that must exist over the life of an accounting session.

IPFE distributes TCP or SCTP traffic among a set of application servers. IPFE is an optional component of the CPF.

DSR's scalability allows the CPF to support up to 16 active CPA MPs.

Introduction to the Charging Proxy Application

CPA is a DSR Application that is responsible for routing Diameter accounting (Rf) messages that are being exchanged between clients (CTFs) and servers (CDFs).

CPA enables load balancing of ACR-Start and ACR-Event messages across CDFs. CPA also sets the preferred CDF value in the Charging SBR. The preferred CDF is used for the duration of the Rf accounting session. CPA updates the preferred CDF in the event of a CDF failover.

CPA is also responsible for triggering Message Copy. Message Copy allows ACR-Start or ACR-Event messages that match a configured rule to be copied to a Diameter Application Server (DAS). Message Copy can be disabled without impacting the other functions of CPA.

Introduction to the Charging Session Binding Repository

The Charging Session Binding Repository (Charging SBR) provides a high availability (HA) distributed database for the DSR Charging Proxy Application (CPA). The Charging SBR stores information that the CPA uses for consistently routing Diameter requests from instances of Charging Trigger Function (CTF) to instances of Charging Data Function (CDF). For any given session, the CPA stores in the

Charging SBR the identity of the CDF that the CPA has chosen to service the Diameter requests for that session, or a session binding. When the CPA routes subsequent Diameter requests for a session, it queries the Charging SBR for the session binding to determine the identity of the serving CDF.

In the most basic form, the Charging SBR consists of a Session Binding Database (SBDB) in which to store session binding data, and a server process to handle requests from the CPA to manipulate session bindings. For scalability, Charging SBR blades are divided into active/standby pairs. The SBDB is logically partitioned across each of the active/standby pairs. Each logical partition corresponds with a Charging SBR subresource. The CPA then submits the request to the selected Charging SBR subresource.

Each session binding record is stored with a timestamp that indicates when the record was last modified. Periodically, stale session binding records are deleted from the SBDB by an internal audit mechanism. The time at which the audit runs and the age at which a binding is considered stale are configurable. The cleanup audit helps to reduce the risk that stale session bindings could prevent the creation of new session bindings. Decreased database performance due to an unnecessarily large SBDB is also remedied by cleaning up stale session binding data.

Congestion in the Charging SBR is determined independently by each partition based on its queue depth. Congestion notifications are included with each Charging SBR response message. The Charging SBR will also monitor the current service time of its request queues. This information is provided with the congestion data included in the Charging SBR response messages. The CPA then judges whether the time for Charging SBR to process a request meets its needs.

If the Charging SBR becomes overloaded or congested, the Charging SBR will shed load in a predictable way in order to control the overload state. The load shedding strategy progressively increases the type of operation shed. Each higher level of congestion adds a new operation to be shed. At 85% congestion, create operations are shed. At 90% congestion, create and update operations are shed. At 95% congestion, read, create and update operations are shed. At 100% congestion, read, create, update and delete operations are shed. As the overload condition lessens, those levels are reversed as the system returns to normal operations.

Chapter 3

Charging Proxy Application

Topics:

- *Pre-Configuration Activities.....16*
- *Configuration.....19*
- *Post-Configuration Activities.....28*

This section covers configuration tasks that must be done prior to configuring CPA, configuring CPA, and tasks that must be done after configuring CPA.

Pre-Configuration Activities

Before CPA configuration can be performed, the following activities need to be performed in the system:

- Verify that at least one Charging SBR Server and Charging SBR Server Group have been configured. The configuration of Charging SBR Servers and Server Groups was required for CPA activation.
- Gather information that is required for Diameter and CPA configuration.
- Configure Diameter Configuration components that are required for CPA configuration.

Verifying Charging SBR Server and Server Group Configuration

Use this task to verify that at least one Charging SBR Server and one Charging SBR Server Group have been configured. The configuration should have been done prior to CPA activation.

1. To verify Charging SBR Server configuration, select **Configuration > Servers**. The **Configuration > Servers** page appears.
2. Verify that at least one Charging SBR Server is configured.
3. To verify Charging SBR Server Group configuration, select **Configuration > Server Groups**. The **Configuration > Server Groups** page appears.
4. Verify that at least one Charging SBR Server Group is configured.

Diameter Configuration for CPA

Several Diameter Configuration components must be configured before the CPA can be configured and enabled.

All Diameter Configuration components are configured using the SOAM GUI.

Use the explanations and procedures in the Diameter Configuration help and the *Diameter User's Guide* to complete the configuration of the Diameter Configuration components for the system, including the following Diameter Configuration components for use with CPA.

1. MP Profiles

Use the **Diameter > Configuration > DA-MPs > Profile Assignments** to assign an **MP Profiles** for each configured CPA DA-MP shown in the **DA-MP** list.

From the pulldown list, select the MP Profile that is for the correct blade and for a Session application, for example **G6:Session** or **G8:Session**.

2. Application Id

Use the **Diameter > Configuration > Application Ids [Insert]** page to define an Application Id for the Rf Accounting Diameter interface (3).

From the **Application Id Value** pulldown list, select **3 - Diameter base accounting**.

3. CEX Parameters

Use the **Diameter > Configuration > CEX Parameters [Insert]** page to define the Capability Exchange parameters for the Application Id that was configured for use by CPA.

For the Application Id, select or enter:

- **Application Id Type** - Accounting
- **Vendor Specific Application Id**, if the Application Id and Vendor Id will be grouped in a Vendor-specific Application Id AVP
- **Vendor Id** - if **Vendor Specific Application Id** is selected

4. CEX Configuration Sets

Use the **Diameter > Configuration > Configuration Sets > CEX Configuration Sets [Insert]** page to configure a CEX Configuration Set to be used in connections with CTF Peer Nodes.

In the CEX Configuration Set, move **3-"Diameter base Accounting"-Accounting-** from the **Available CEX Parameters** to the **Selected CEX Parameters** field.

5. Local Nodes

Use the **Diameter > Configuration > Local Nodes [Insert]** page to configure Virtual CDF and Virtual CTF Local Nodes.

To accomplish Topology Hiding, the Charging Proxy Function appears as one large CDF to the CTFs and as one large CTF to the CDFs. The Charging Proxy Function modifies the Origin-Host and Origin-Realm AVPs in each message being routed to a CTF or CDF. The configuration of this capability is done using Virtual CDF and Virtual CTF Local Nodes.

At least one Virtual CDF Local Node must be provisioned, but two are recommended to provide each CTF Peer a redundant connection to the DSR.

At least one Virtual CTF Local Node must be provisioned on the DSR.

The **Realm** and **FQDN** values will be substituted in the Origin-Realm and Origin-Host AVPs.

6. Use the **Diameter > Configuration > Peer Nodes [Insert]** page to configure Peer Nodes for every CDF, CTF, and Diameter Application Server (DAS).

For CDF Peer Nodes, the **Replace Dest Realm** and **Replace Dest Host** options must be enabled.

Do not configure an **Alternate Implicit Route List**. The Peer Route Table will be defined such that there is a Peer Routing Rule for every CDF Peer, so that routing will always be done using a Route List.

7. Connections

Use the **Diameter > Configuration > Connections [Insert]** page to configure Connections to CTFs, CDFs, and Diameter Application Servers.

- At least one Connection must be configured to each CTF, CDF, and DAS.
- Connections communicating with a CTF Peer Node must be associated with a Virtual CDF Local Node.
- Connections communicating with a CTF Peer Node must select a CEX Configuration Set that has the Diameter base accounting Application Id (3) configured.
- Connections communicating with a CDF Peer Node must be associated with a Virtual CTF Local Node.
- On Connections communicating with a CDF Peer Node, enable the **Remote Busy Usage** option, and set the **Remote Busy Abatement Timeout** value to the desired length of time that messages will stop being sent on the CDF connection after the receipt of a DIAMETER_TOO_BUSY response.

8. Application Route Tables

Either use the default **Application Route Table** (always available), or use the **Diameter > Configuration > Application Route Tables > [Insert]** page to configure one or more **Application Route Tables** in addition to the default. **Application Route Tables** contain **Application Routing Rules** that direct messages to CPA and other DSR Applications.

9. Application Routing Rules

On the **Diameter > Configuration > Application Route Tables** page, select an **Application Route Table Name** and click **View/Edit Rules**.

Use the **Viewing Rules for Application Route Table** page to insert or edit an **Application Routing Rule** so that messages with Diameter Application ID = 3 are directed to the CPA.

When defining the **Application Routing Rule**:

- In the **Conditions** field, set the **Application-Id Operator** to **Equals** and the **Value** to **3 - Diameter base accounting**. For all other Parameters, set the **Operator** to **Always True**.
- Set the **Application Name** to **CPA**.

10. Route Groups

Use the **Diameter > Configuration > Route Groups [Insert]** to configure CDF Peer Route Groups and DAS Peer Route Groups.

- Only Peer Route Groups are used in the Offline Charging Solution.
- Configure a CDF Pool Peer Route Group that contains all of the CDF Peer Nodes, with each CDF Peer Node having the same **Provisioned Capacity**.
- For each CDF Peer Node, configure a Peer Route Group containing just this CDF Peer Node. Also configure an alternate Peer Route Group containing all CDF Peer Nodes except this one with each CDF Peer Node having the same **Provisioned Capacity**.
- For each DAS Peer Node, configure a Peer Route Group containing just this DAS Peer Node.
- Configure a DAS Pool Peer Route Group that contains all of the DAS Peer Nodes, with each DAS Peer Node having the same **Provisioned Capacity**.

11. Route Lists

Use the **Diameter > Configuration > Route Lists [Insert]** to configure CDF Route Lists and DAS Route Lists.

- For each Route List configured for the Charging Proxy Function, the **Route Across Route Groups** option should be set to **Enabled** to allow messages to be routed to alternate CDFs if the preferred CDF fails.
- Configure a CDF Pool Route List containing just the CDF Pool Route Group.
- For each CDF, configure a CDF Route List, containing the corresponding CDF Peer Route Group with a priority of 1 and the corresponding alternate CDF Peer Route Group with a priority of 2.
- Configure a DAS Pool Route List containing just the DAS Pool Route Group.
- For each DAS, configure a DAS Route List containing the corresponding DAS Peer Route Group.

12. Peer Route Tables

Use the **Diameter > Configuration > Peer Route Tables [Insert]** page to configure a Peer Route Table for the Charging Proxy Function.

Then create Peer Routing Rules to route ACR-Interim and ACR-Stop messages to the preferred CDF peer, or if the preferred CDF Peer is unavailable, then to load balance the message routing to the other CDF Peers.

Within the Charging Proxy Peer Route Table, for each CDF, create a Peer Routing Rule as follows:

- In the **Conditions** field:
 - Set the **Destination-Host Operator** to **Equals** and the **Value** to the FQDN of the CDF Peer Node.
 - Set the **Application-Id Operator** to **Equals** and the **Value** to **3 - Diameter base accounting**.
 - For all other **Parameters**, set the **Operator** to **Always True**.
- **Action** is set to **Route to Peer**.
- **Route List** is set to the corresponding CDF Route List.
- **Message Priority** is set to **1**.

Also create a Peer Routing Rule to load balance the routing of ACR-Start and ACR-Event Request messages across all CDF Peers.

- In the **Conditions** field:
 - Set the **Destination-Host Operator** to **Absent**.
 - Set the **Application-Id Operator** to **Equals** and the **Value** to **3 - Diameter base accounting**.
 - For all other **Parameters**, set the **Operator** to **Always True**.
- **Action** is set to **Route to Peer**.
- **Route List** is set to the corresponding CDF Pool Route List.
- **Message Priority** is set to **0**.

13. Application Id (edit)

Use the **Diameter > Configuration > Application Ids [Edit]** page to assign the Charging Proxy Peer Route Table to the Diameter base accounting Application Id.

14. Reroute On Answer

Use the **Diameter > Configuration > Reroute on Answer [Insert]** page to configure Reroute On Answer to perform alternate routing when a **DIAMETER_TOO_BUSY** Answer Result-Code is received from a CDF Peer.

- Set the **Answer Result-Code AVP Value** to **3004**.
- For the **Application Id**, select **3 - Diameter base accounting** from the pulldown list.

Configuration

The CPA menu option allows you to perform configuration tasks for the following:

- System Options
- Message Copy
- SBR
- SBR Subresource Mapping

Note: CPA does not require any additional network configuration beyond the standard DSR configuration.

System Options

The **System Options** page shows values for various CPA configuration options.

For more information about each field, see [System Options page elements](#).

System Options page elements

This section describes the elements on the **CPA > Configuration > System Options** page.

Table 2: System Options page elements

Field (* indicates required field)	Description	Data Input Notes
Unavailable Action	Action to be taken when the CPA has an Operational State of Degraded or Unavailable.	This field is read-only. Default: Send Answer
Unavailable Action Result Code	Because the Unavailable Action must be Send Answer, if the CPA is not available, this value is used in the Result-Code or Experimental-Result AVP of the Answer message.	Format: Two radio button group with a text box and drop-down box. Default: 3004 DIAMETER_TOO_BUSY
Unavailable Action Vendor ID	If zero, then a Result-Code AVP will be sent when the CPA is not available. If non-zero, then an Experimental-Result AVP will be sent with the Vendor-Id AVP set to this value.	Format: Unsigned integer Default: 0
Unavailable Action Error Message	If a non-null string, this configured string will be appended to the Error-Message AVP that is sent in the Answer response when the CPA is not available.	Format: Text box (string up to 64 characters) Default: CPA Unavailable
DSR Application-Invoked AVP Insertion	If set to Yes, this AVP will be inserted into the Request message that is routed to prevent multiple invocations of CPA on different DSRs or MPs.	Format: Yes/No Default: No
Shutdown Mode	Allows the operator to specify the shutdown method used when the CPA Admin State is changed to Disabled. The CPA can be disabled using either a graceful or forced shutdown method. Graceful allows in-process transactions to continue for a configurable time period before disabling the CPA. Forced is an immediate shutdown.	Format: Forced/Graceful Default: Graceful

Field (* indicates required field)	Description	Data Input Notes
* Shutdown Timer	Number of seconds that the Shutdown Timer will run during a graceful shutdown.	Range: 1 to 15 seconds Default: 5
Generate Answer Result Code	The Result-Code or Experimental-Result AVP value to be populated in the Answer message when the DSR generates an Answer message to the downstream (CTF) peer.	Format: Two radio button group with a text box and drop-down box. The drop-down box contains several Result-Code values and corresponding names. The user can also choose to specify their own Result-Code value in the text box. Range: 1000 - 5999 Default: 3004 DIAMETER_TOO_BUSY
Generate Answer Vendor ID	If zero, then a Result-Code AVP will be sent when the DSR generates an Answer message. If non-zero, then the Experimental-Result AVP will be sent in the Answer message with the Vendor-Id AVP set to this value. The value of the Result-Code or Experimental-Result AVP will be the configured Generate Answer Result Code.	Format: Unsigned integer Default: 0
Generate Answer Error Message	If a non-null string, this configured string will be appended to the Error-Message AVP that is sent in the generated Answer message.	Format: Text box (string up to 64 characters) Default: DSR Generated Answer
Behavior if Session Lookup Error	Behavior to use when CPA attempts to query the preferred CDF that is associated with the given Diameter session, but the query is not successful. The possible behaviors are <ul style="list-style-type: none"> • Generate Answer (send an Answer message with the configured Generate Answer Result-Code to the CTF) • Continue Routing (load balance the Request message to an available CDF) 	The range of allowable values in the drop-down box shall be: <ul style="list-style-type: none"> • Generate Answer • Continue Routing Default: Continue Routing

Editing System Options

Use this task to edit the System Options.

1. Select **CPA > Configuration > System Options**.
The **CPA > Configuration > System Options** page appears.
 2. Update the relevant fields.
For more information about each field, see [System Options page elements](#).
 3. Perform one of the following actions:
 - Click **Apply** to save the changes and stay on this page.
 - Click **Cancel** to return to the **CPA > Configuration > System Options** page without saving the changes.
- If **Apply** is clicked and any of the following conditions exist, an error message appears:
- Any required field is empty; no value was entered
 - The entry in any field is not valid (wrong data type or out of the valid range)

Message copy

The Diameter Message Copy feature allows users to forward a copy of a Diameter Request message received by or routed through the Diameter Signaling Router to a Diameter Application Server (DAS peer). This capability is triggered based on the CPA configuration.

A user can specify a triggering condition or rule, and when a Diameter Request meeting the triggering condition is received by the DSR, the message is marked as ready to copy by the application as it is processed. When the response to the request (the answer) is received, if the answer contains the correct result code as specified by the system-wide configuration, the resulting action is executed. In the case of Message Copy, the action is to copy the Request and send the copy to a DAS peer. Message Copy copies only the Diameter portion of the Request that matches a triggering condition; thus, the transport and IP layers are not copied. Lower layer protocols that do not contain Diameter Requests are not copied; thus, Message Copy does not implement a port mirror that replicates everything received on the wire on a specific port to an egress port.

Message Copy elements

This table describes the fields on the **CPA > Configuration > Message Copy** page.

Table 3: Message Copy Elements

Field	Description	Data Input Notes
Message Copy Status	Enable or disable the triggering of Message Copy.	Format: Two radio buttons: <ul style="list-style-type: none"> • Enable • Disable Default: Disable
Called-Station-ID match string 1	If the Called-Station-Id AVP value in an ACR-Start or ACR-Event message contains this case-sensitive string, then Message Copy will be triggered.	Format: Text box (up to 64 characters) Default: Empty string

Field	Description	Data Input Notes
Called-Station-ID match string 2	If the Called-Station-Id AVP value in an ACR-Start or ACR-Event message contains this case-sensitive string, then Message Copy will be triggered.	Format: Text box (up to 64 characters) Default: Empty string
Called-Station-ID match string 3	If the Called-Station-Id AVP value in an ACR-Start or ACR-Event message contains this case-sensitive string, then Message Copy will be triggered.	Format: Text box (up to 64 characters) Default: Empty string
Called-Station-ID match string 4	If the Called-Station-Id AVP value in an ACR-Start or ACR-Event message contains this case-sensitive string, then Message Copy will be triggered.	Format: Text box (up to 64 characters) Default: Empty string
DAS Copy Route List 1	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.
DAS Copy Route List 2	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.
DAS Copy Route List 3	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.
DAS Copy Route List 4	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.
DAS Copy Route List 5	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route

Field	Description	Data Input Notes
		Lists configuration screen.
DAS Copy Route List 6	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.
DAS Copy Route List 7	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.
DAS Copy Route List 8	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.
DAS Copy Route List 9	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.
DAS Copy Route List 10	Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Copy Route Lists.	Format: Pull down of Route Lists that have been configured on the Diameter > Configuration > Route Lists configuration screen.

Configuring Message Copy

Use this task to configure Message Copy.

1. Select **CPA > Configuration > Message Copy**.
The **CPA > Configuration > Message Copy** page appears.
2. Update the relevant fields.
For more information about each field, see [Message Copy elements](#).

3. Perform one of the following actions:

- Click **Apply** to save the changes and stay on this page.
- Click **Cancel** to return to the **CPA > Configuration > Message Copy** page without saving the changes.

Clicking **Apply** when Message Copy is enabled will generate an error message if at least one Called-Station-ID AVP match string and at least one DAS Route List are not configured.

If a user attempts to delete a Route List that is being referenced as a Message Copy DAS Route List, the deletion will not be allowed.

SBR page

This section describes the configuration functions of the Charging SBR found on the **CPA > Configuration > SBR** page, which specifies when the stale session binding audit will run and how old a binding has to be before it is considered stale.

SBR elements

This table describes the fields on the **CPA > Configuration > SBR** page.

Field (* indicates required field)	Description	Data Input Notes
* SBDB audit Start Time	<p>Time of day in UTC to start the audit process.</p> <p>The audit process removes stale bindings from the Charging SBR. Since the audit window is configurable, the audit process calculates the rate at which to delete records based on the number of expected stale bindings and the configured duration of the daily audit. The longer the audit window is, the slower the deletion rate.</p> <p>If your system has a daily period of lower customer activity, you may wish to schedule the audit for that time. Otherwise, you can reduce the performance load of the process by allowing it more time during the day to complete its audit.</p>	<p>Format: pull-down list</p> <p>Range: 12:00 AM - 11:00 PM, UTC</p> <p>Default: 2:00 AM</p>
* SBDB audit Stop Time	<p>Time of day in UTC to stop the audit process. Must be at least 1 hour past the start time.</p>	<p>Format: pull-down list</p> <p>Range: 12:00 AM - 11:00 PM, UTC</p> <p>Default: 3:00 AM</p>

Field (* indicates required field)	Description	Data Input Notes
* Stale SBDB session binding age	Age after which a session will be considered stale and eligible for removal during audit. Note that increasing the age will increase memory usage. Age is specified in days.	Format: numeric Range: 1-30 Default: 2
* Maximum active session bindings	Session binding count used to calculate the session binding count alarms. Once this setting is reached, the Charging SBR will issue an alarm; however, it will continue to store bindings.	Format: numeric Range: 1 - 100,000,000 Default: 35,000,000
* SBDB Mostly Stale Percentage	Percent of stale session age when a session binding is considered mostly stale. This setting is not used by the audit process. However, it is used to generate measurements.	Format: numeric Range: 1-99 Default: 90

Configuring the Charging SBR

The Charging SBR configuration options set up the audit window, specify when a binding becomes stale, and set some alarm and measurement thresholds.

1. Select **CPA > Configuration > SBR**.

The **CPA > Configuration > SBR** page appears.

2. Inspect the defaults.

For more information on the configuration options, see [SBR elements](#).

It should not be necessary to modify the defaults.

3. Make any changes to the configuration options.
4. Click **Apply** to apply your changes.

Your changes will go into affect immediately.

SBR Subresource Mapping page

This section describes the configuration found on the **CPA > Configuration > SBR Subresource Mapping** page. A subresource is a logical partition of the Charging SBR.



Caution: The subresource mapping must be configured after the CPA is activated, but before it is enabled. The page can be edited only once.

SBR Subresource Mapping elements

The **SBR Subresource Mapping** page is organized by server group, which must be configured before accepting the configurations on this page. To configure server groups, select **Configuration > Server Groups**.



Caution: After configuration, this page becomes read-only.

Element	Description	Data Input Notes
SBR Server Group Name	Server Group Name from the Configuration > Server Groups page	This field cannot be edited
Resource Name	The resource name is cSBR.	This field cannot be edited
Subresource Id	<p>A subresource is a logical partition of the Charging SBR consisting of an active/standby pair.</p> <p>The Subresource Id is a monotonically increasing integer starting with 0.</p> <p>An selection of "Not Hosted" indicates that the server group will not be used. The "Not Hosted" ID is typically used only in testing environments.</p> <p>An asterisk after the value field means that the configuration is mandatory.</p>	<p>Format: pull-down list</p> <p>Range: "Not Hosted", 0-N, where N is the number of subresources-1</p> <p>Default: 0, 1, 2, 3, ..., N</p>

Configuring the Charging SBR subresource mapping



Caution: Subresources must be configured after the CPA is activated.

This screen can be edited only once.

You must apply the configuration before enabling the CPA.

1. Select **CPA > Configuration > SBR Subresource Mapping**.

The **CPA > Configuration > SBR Subresource Mapping** page appears.

2. Inspect the defaults for Subresource Ids.

It should *not* be necessary to modify the defaults. The defaults are correct for a production deployment.

3. If needed for setting up a testing environment, make changes to the configurations.

If there is a Charging SBR Server Group that you do not intend to use (that is, not host a subresource), change the subresource ID to “Not Hosted”. This configuration would be used only in lab testing.

Subresources must be numbered sequentially, starting with 0 and incremented by 1.

4. Click **Apply**.

This step is mandatory, even if no changes to the subresource Ids were made.

A warning displays saying that this screen can be edited only once. The update will be rejected if subresources are not numbered sequentially starting with 0.

5. Click **Confirm** to apply your changes.

Once the changes are confirmed, this page and the configurations for the Charging SBR on the **Configuration > Server Groups** page will be read only.

If you need to reconfigure subresources or Charging SBR server groups, contact the [Customer Care Center](#) for assistance.

Post-Configuration Activities

After CPA configuration is complete, the following activities need to be performed to make the CPA fully operational in the system:

- Enable CPA
- Enable Connections
- Status Verification

Enabling the CPA

Use this task to enable the CPA.

1. From each active SOAM, select **Diameter > Maintenance > Applications**.

The **Diameter > Maintenance > Applications** page appears.

2. Under **DSR Application Name**, select each CPA row.

To select more than one row, press and hold **Ctrl** while you click each row.

3. Click **Enable**.

4. Verify the application status on the page.

The **Admin State**, **Operational Status**, **Operational Reason**, and **Congestion Level** in each of the selected rows should have changed respectively to **Enabled**, **Available**, **Normal**, and **Normal**.

Enabling Connections

Use this task to enable the connections to the CTFs, CDFs, and Diameter Application Servers.

1. From the active SOAM, select **Diameter > Maintenance > Connections**.
The **Diameter > Maintenance > Connections** page appears.
2. Select 1 - 20 connections to enable.
To select more than one row, press and hold **Ctrl** while you click each row. To select multiple contiguous connections, click the first connection you want, then press and hold **Shift** and select the last connection you want. All the connections between are also selected.
3. Click **Enable**.
A confirmation box appears.
4. Click **OK**.
The selected connections are enabled.
5. Verify the connection status on the page.
The **Admin State** and **Operational Status** in each of the selected rows should have changed respectively to **Enabled** and **Available**.

Status Verification

Use this procedure to verify CPA status after configuration is complete.

1. Verify Communication Agent (ComAgent) Connection status.
 - a) From the active SOAM, select **Communication Agent > Maintenance > Connection Status**
 - b) Verify that the **Automatic Connections Count** field displays **X of X in service** where X is the number of peer server connections.
2. Verify Server status.
 - a) From the active SOAM, select **Status & Manage > Server**
 - b) Verify that for each Server, the **Appl State** field is **Enabled**, and the **DB, Reporting Status**, and **Proc** fields are **Norm**.

DSR Bulk Import and Export

The following documents describe the use and operation of DSR Bulk Import and Export functions:

- *Diameter User's Guide*, "Diameter Configuration", "DSR Bulk Import", "DSR Bulk Export"
- **Help > Diameter > Configuration > DSR Bulk Import**
- **Help > Diameter > Configuration > DSR Bulk Export**

The DSR Bulk Import and Export functions can be used to export Diameter, IPFE, and DSR Application configuration data in CSV files to a location outside the system, and to import the files (usually edited) into the system where the Import function is executed.

Configuration data refers to any data that is configured for one of the Export **Export Application** types (FABR, RBAR, Policy DRA, GLA, or CPA and SBR DSR Applications; IPFE; and the Diameter Configuration components).

DSR Bulk Export

The DSR Bulk Export operation creates ASCII Comma-Separated Values (CSV) files (.csv) containing Diameter, IPFE, and DSR Application configuration data. Exported configuration data can be edited and used with the DSR Bulk Import operations to change the configuration data in the local system without the use of GUI pages. The exported files can be transferred to and used to configure another DSR system.

Each exported CSV file contains one or more records for the configuration data that was selected for the Export operation. The selected configuration data can be exported once immediately, or exports can be scheduled to periodically occur automatically at configured times.

The following configuration data can be exported in one Export operation:

- All exportable configuration data in the system
- All exportable configuration data from the selected DSR Application, IPFE, or Diameter (each component's data is in a separate file)
- Exportable configuration data from a selected configuration component for the selected DSR Application, IPFE, or Diameter

Exported files can be written to the File Management Directory in the local File Management area (**Status & Manage > File** page), or to the Export Server Directory for transfer to a configured remote Export Server.

CSV files that are in the local File Management area can be used for Bulk Import operations on the local system.

If the export has any failures or is unsuccessful, the results of the export operation are logged to a log file with the same name as the exported file but with a ".log" extension. Successful export operations will not be logged.

DSR Bulk Import

The DSR Bulk Import operations use configuration data in ASCII Comma-Separated Values (CSV) files (.csv), to insert new data into, update existing data in, or delete existing data from the Diameter Configuration, IPFE Configuration, or DSR Applications (FABR, RBAR, Policy DRA, GLA, and CPA/SBR) Configuration data in the system.

Note: Some configuration data can be imported only with the Update operation, and other data can be imported with Insert and Delete operations but not Update. Refer to the "DSR Bulk Import" section of the *Diameter User's Guide* or the **Diameter > Configuration > Import** Help for valid Import operations.

Import CSV files can be created by using a DSR Bulk Export operation, or can be manually created using a text editor.

Note: The format of each Import CSV file record must be compatible with the configuration data in the DSR release that is used to import the file.

Files that are created using the DSR Bulk Export operation can be exported either to the local Status & Manage File Management Directory (**Status & Manage > Files** page), or to the local Export Server Directory.

CSV files that are in the local File Management area can be used for Bulk Import operations on the local system.

Files can be created manually using a text editor on a computer; the files must be uploaded to the File Management area of the local system before they can be used for Import operations on the local system.

The following Import operations can be performed:

- Insert new configuration data records that do not currently exist in the system
- Update existing configuration data in the system
- Delete existing configuration data from the system

Each Import operation creates a log file. If errors occur, a Failures CSV file is created that appears in the File Management area. Failures files can be downloaded, edited to correct the errors, and imported to successfully process the records that failed. Failures files that are unchanged for more than 14 days and log files that are older than 14 days are automatically deleted from the File Management area.

A

ACA	<p>Accounting Answer</p> <p>Diameter message type responding to an Accounting Request message.</p>
ACR	<p>Accounting Request</p> <p>Diameter message type for creating an accounting transaction. An ACR is sent by an IMS network element that describes a stage in the processing of a SIP service.</p>
AVP	<p>Attribute-Value Pair</p> <p>The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization or accounting information.</p>

C

CDF	<p>Charging Data Function</p>
CPA	<p>Charging Proxy Application</p> <p>The Charging Proxy Application (CPA) feature defines a DSR-based Charging Proxy Function (CPF) between the CTFs and the CDFs. The types of CTF include GGSN, PGW, SGW, HSGW, and CSCF/TAS.</p>
CTF	<p>Charging Trigger Function</p>

D

DAS Diameter Application Server

DSR Diameter Signaling Router
A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes.

I

IPFE IP Front End
A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.

P

pSBR Policy SBR

S

SBR Session Binding Repository - A highly available, distributed database for storing Diameter session binding data

SOAM System Operations, Administration, and Maintenance
Site Operations, Administration, and Maintenance

U

UTC Coordinated Universal Time