

Diameter Signaling Router

Range Based Address Resolution (RBAR) User's Guide

Release 8.2

E89002

January 2018

Copyright © 2011, 2018, 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, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

This documentation is in preproduction status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Contents

1 Introduction

Revision History	1-1
Overview.....	1-1
Scope and Audience	1-1
Manual Organization	1-1
Documentation Admonishments	1-2
Related Publications	1-2
Locate Product Documentation on the Oracle Help Center Site	1-2
Customer Training	1-3
My Oracle Support (MOS).....	1-3
Emergency Response.....	1-3

2 User Interface Introduction

User Interface Organization	2-1
User Interface Elements.....	2-2
Main Menu Options	2-5
Missing Main Menu options	2-11
Common Graphical User Interface Widgets.....	2-11
Supported Browsers.....	2-11
System Login Page	2-12
Main Menu Icons.....	2-13
Work Area Displays	2-14
Customizing the Splash Page Welcome Message	2-17
Column Headers (Sorting).....	2-17
Page Controls	2-17
Clear Field Control.....	2-18
Optional Layout Element Toolbar.....	2-18
Filters.....	2-20
Pause Updates.....	2-22
Max Records Per Page Controls	2-22

3 Range Based Address Resolution

Range Based Address Resolution overview	3-1
Address Ranges	3-2
Individual Addresses.....	3-3
Application Chaining	3-3
Request Message Validation.....	3-4
Multiple DSR Application Invocation Prevention.....	3-11
Metadata Recording for Integrated DIH (IDIH)	3-12

4 Configuration of RBAR

Pre-Configuration Activities	4-1
Verifying Server status.....	4-1
Diameter Common Configuration for RBAR.....	4-1
Diameter Configuration for RBAR	4-2
RBAR Configuration	4-3
Applications configuration	4-3
Exceptions configuration.....	4-5
Destinations configuration.....	4-7
Address Tables configuration	4-10
Address configuration	4-12
Address Resolutions configuration	4-17
System Options configuration	4-22
Post-Configuration Activities	4-26
Enabling the RBAR Application.....	4-26
Status Verification.....	4-26
Bulk Import and Export.....	4-27

5 Maintenance of RBAR

RBAR Maintenance Overview	5-1
RBAR Administrative State and Operational Status	5-1

List of Figures

2-1	Oracle System Login.....	2-12
2-2	Paginated Table.....	2-15
2-3	Scrollable Table.....	2-15
2-4	Form Page.....	2-16
2-5	Tabbed Pages.....	2-16
2-6	Tabbed Pages.....	2-16
2-7	Report Output.....	2-17
2-8	Sorting a Table by Column Header.....	2-17
2-9	Clear Field Control X.....	2-18
2-10	Optional Layout Element Toolbar.....	2-19
2-11	Automatic Error Notification.....	2-19
2-12	Examples of Filter Styles.....	2-20
3-1	IMSI/MSISDN Overlap Range Scenario.....	3-11

List of Tables

1-1	Admonishments.....	1-2
2-1	User Interface Elements.....	2-3
2-2	Main Menu Options.....	2-6
2-3	Main Menu Icons.....	2-13
2-4	Example Action Buttons.....	2-18
2-5	Submit Buttons.....	2-18
2-6	Filter Control Elements.....	2-20
3-1	RBAR Supported AVPs.....	3-5
3-2	Combinations of User Identity Types and Associated AVPs.....	3-7
3-3	Relation between Configured User Identity Types and Data Formats.....	3-8
3-4	DSR-Application-Invoked AVP.....	3-11
3-5	RBAR Metadata-Generating Events.....	3-12
4-1	Applications Configuration Elements.....	4-4
4-2	Exceptions Configuration Elements.....	4-6
4-3	Destinations Configuration Elements.....	4-8
4-4	Address Tables Configuration Elements.....	4-10
4-5	Addresses Configuration Elements.....	4-13
4-6	Address Resolutions Configuration Elements.....	4-18
4-7	System Options Elements.....	4-22
5-1	RBAR Admin State and Operational Status.....	5-1

Introduction

The *Range Based Address Resolution (RBAR) User's Guide* and Help provides an overview of the functions and procedures to configure RBAR. The contents of this chapter include sections on the revision history, scope, audience, and organization of the document, Oracle documentation, and how to contact Oracle for assistance.

Revision History

Date	Description
June 2016	Accessibility changes throughout.
January 2017	Updates in the RBAR supported AVPs table.

Overview

The Range Based Address Resolution (RBAR) documentation provides information about the functions, explains how to use the GUI, and the following procedures to configure the RBAR application:

- Applications
- Exceptions
- Destinations
- Address Tables
- Addresses
- Address Resolutions
- System Options

Scope and Audience

The RBAR document is for anyone responsible for configuring and using the RBAR application. Users of this manual must have a working knowledge of telecommunications, network installations, and the product that is using the RBAR functions.

Manual Organization

This manual is organized into the following chapters:

- [Introduction](#) contains general information about the RBAR help documentation, the organization of this manual, and how to get technical assistance.
- [User Interface Introduction](#) describes the organization and usage of the application user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.
- [Range Based Address Resolution](#) describes the function of the application.
- [Configuration of RBAR](#) describes how to configure the application, including Applications, Exceptions, Destinations, Address Tables, Addresses, Address Resolutions, and System Options.
- [Maintenance of RBAR](#) describes maintenance functions and information that can be used with the application.

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 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of personal injury.)
	Warning: (This icon and text indicate the possibility of equipment damage.)
	Caution: (This icon and text indicate the possibility of service interruption.)

Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See [Locate Product Documentation on the Oracle Help Center Site](#) for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) 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 <http://www.adobe.com>.

1. Access the Oracle Help Center site at <http://docs.oracle.com>.

2. Click Industries.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link.

The Communications Documentation page displays. Most products covered by these documentation sets display under the headings "Network Session Delivery and Control Infrastructure" and "Platforms."

4. Click on your Product and then the Release Number.

A list of the entire documentation set for the selected product and release displays.

5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training at <http://education.oracle.com/communication>

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site at www.oracle.com/education/contacts

My Oracle Support (MOS)

MOS (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
 - For Technical issues such as creating a new Service Request (SR), Select 1
 - For Non-technical issues such as registration or assistance with MOS, Select 2

You are connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. 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.

User Interface Introduction

This section describes the organization and usage of the application's user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.

User Interface Organization

The user interface is the central point of user interaction within an application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to an application and its functions.

The core framework presents a common set of Main Menu options that serve various applications. The common Main Menu options are:

- Administration
- Configuration
- Alarms and Events
- Security Log
- Status and Manage
- Measurements
- Help
- Legal Notices
- Logout

Applications build upon this framework to present features and functions. Depending on your application, some or all of the following Main Menu options may display on the Network Operation, Administration, and Maintenance (**NOAM**) GUI:

- Communication Agent
- Diameter Common
- Diameter
- **UDR** (User Data Repository)
- MAP-Diameter IWF
- **RADIUS** (Remote Authentication Dial-In User Service)
- **SBR** (Session Binding Repository)

- Policy and Charging
- **DCA** (DOIC Capabilities Announcement) Framework

The DSR System OAM GUI may present even more Main Menu options as listed below. The end result is a flexible menu structure that changes according to the application needs and features activated.

- Transport Manager
- SS7/Sigtran
- RBAR (Range Based Address Resolution)
- FABR (Full Address Based Resolution)
- **GLA** (Gateway Location Application)
- MAP-Diameter IWF
- RADIUS
- SBR
- Mediation
- Policy and Charging
- DCA Framework
- IPFE (IP Front End)

Note that the System OAM (SOAM) Main Menu options differ from the Network OAM (NOAM) options. Some Main Menu options are configurable from the NOAM server and view-only from the SOAM (**SOAM**) server. This remains true for other applications.

User Interface Elements

[Table 2-1](#) describes elements of the user interface.

Table 2-1 User Interface Elements

Element	Location	Function
Identification Banner	Top bar across the web page	<p>The left side of the banner provides the following information:</p> <ul style="list-style-type: none"> • Displays the company name, • product name and version, and • the alarm panel.
		<p>The right side of the banner:</p> <ul style="list-style-type: none"> • Allows you to pause any software updates. • Links to the online help for all software. • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	<p>A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders.</p> <ul style="list-style-type: none"> • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.

Table 2-1 (Cont.) User Interface Elements

Element	Location	Function
Work Area	Right side of panel under status	<p>Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area.</p> <ul style="list-style-type: none"> • Page Title Area: Occupies the top of the work area. It displays the title of the current page being displayed, date and time, and includes a link to context-sensitive help. • Page Control Area: Located below the Page Title Area, this area shows controls for the Page Area (this area is optional). When available as an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see Optional Layout Element Toolbar. • Page Area: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application

Table 2-1 (Cont.) User Interface Elements

Element	Location	Function
Session Banner	Across the bottom of the web page	<p>user interface page. The page displays a user-defined welcome message. To customize the message, see Customizing the Login Message.</p> <p>The left side of the banner provides the following session information:</p> <ul style="list-style-type: none"> • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. <p>The right side of the banner shows the alarm panel.</p>

Main Menu Options

[Table 2-2](#) describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's login account. For example, the Administration menu options do not display on the screen of a user who does not have administrative privileges.

Note: Some menu items are configurable only on the Network OAM and view-only on the System OAM; and some menu options are configurable only on the System OAM.

Note: Some features do not display in the main menu until the features are activated.

Table 2-2 Main Menu Options

Menu Item	Function
Administration	<p>The Administration menu allows the user to:</p> <ul style="list-style-type: none"> General Options. Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled Set up and manage user accounts Configure group permissions View session information Manage sign-on certificates Authorize IP addresses to access the user interface Configure SFTP user information View the software versions report Upgrade management including backup and reporting Authenticate LDAP servers Configure SNMP trapping services Configure an export server Configure DNS elements
Configuration	<p>On the NOAM, allows the user to configure:</p> <ul style="list-style-type: none"> Network Elements Network Devices Network Routes Services Servers Server Groups Resource Domains Places Place Associations Interface and Port DSCP
Alarms and Events	<p>Allows the user to view:</p> <ul style="list-style-type: none"> Active alarms and events Alarm and event history Trap log
Security Log	<p>Allows the user to view, export, and generate reports from security log history.</p>
Status and Manage	<p>Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, KPIs, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, data, and ISO file management.</p>
Measurements	<p>Allows the user to view and export measurement data.</p>

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
Transport Manager (optional)	On the SOAM, allows the user to configure adjacent nodes, configuration sets, or transports. A maintenance option allows the user to perform enable, disable, and block actions on the transport entries. This option only displays with the DSR application.
Communication Agent (optional)	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. The user can perform actions to enable, disable, and block connections. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.
SS7/Sigtran (optional)	On the SOAM, allows the user to configure various users, groups, remote signaling points, links, and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data. This option only displays with the DSR application.
Diameter Common (optional)	<p>Allows the user to view or configure:</p> <ul style="list-style-type: none"> • Dashboard, configure on the NOAM; view on both OAMs • Network Identifiers on the SOAM - MCC Ranges • Network Identifiers on the NOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile Assignments <p>The DSR Bulk Import and Export functions are available on both OAMs for the data configured on that OAM.</p>
Diameter (optional)	<p>Allows the user to configure, modify, and monitor Diameter routing:</p> <ul style="list-style-type: none"> • On the NOAMP, Diameter Topology Hiding and Egress Throttle List configuration • On the SOAM, Diameter Configuration, Maintenance, Reports, Troubleshooting with IDIH, AVP Dictionary, and Diameter Mediation configuration
UDR (User Data Repository) (optional)	Allows the user to add, edit, store, and manage subscriber and pool data. The user can also monitor the import, export, and subscribing client status. This option only displays with the UDR application.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
RBAR (Range-Based Address Resolution) (optional)	<p>Allows the user to configure the following Range-Based Address Resolution (RBAR) settings:</p> <ul style="list-style-type: none"> • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options <p>This is accessible from the SOAM only. This option only displays with the DSR application.</p>
FABR (Full Address Based Resolution) (optional)	<p>Allows the user to configure the following Full Address Based Resolution (FABR) settings:</p> <ul style="list-style-type: none"> • Applications • Exceptions • Default Destinations • Address Resolutions • System Options <p>This is accessible from the SOAM only. This option is only available with the DSR application.</p>
Gateway Location Application (optional)	<p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> • Exceptions • Options <p>GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP). This option only displays with the DSR application.</p>
MAP-Diameter Interworking (optional)	<p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application:</p> <ul style="list-style-type: none"> • DM-IWF Options • Diameter Exception <p>On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application:</p> <ul style="list-style-type: none"> • MD-IWF Options • Diameter Realm • Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping <p>This option only displays with the DSR application.</p>

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
RADIUS (Remote Authentication Dial-In User Service) (optional)	<p>Allows the user to perform configuration tasks, edit system options, and view elements for:</p> <ul style="list-style-type: none"> • Network Options • Message Authenticator Configuration Sets • Shared Secret Configuration Sets • Ingress Status Server Configuration Sets • Message Conversion Configuration Sets • NAS Node <p>This option only displays with the DSR application.</p>
SBR (Session Binding Repository) (optional)	<p>Allows the user to perform configuration tasks, edit system options, and view elements for:</p> <ul style="list-style-type: none"> • SBR Databases • SBR Database Resizing Plans • SBR Data Migration Plans • Database Options <p>Additionally, on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> • Maintenance <ul style="list-style-type: none"> – SBR Database Status – SBR Status – SBR Database Reconfiguration Status <p>This option only displays with the DSR application.</p>
Mediation	<p>Allows the user to make routable decisions to end the reply, drop the message, or set the destination realm.</p>

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
Policy and Charging (optional)	<p>On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> • General Options • Access Point Names • Policy DRA <ul style="list-style-type: none"> – PCRF Pools – PCRF Sub-Pool Selection Rules – Network-Wide Options • Online Charging DRA <ul style="list-style-type: none"> – OCS Session State – Realms – Network-Wide Options • Alarm Settings • Congestion Options <p>Additionally on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> • Maintenance <ul style="list-style-type: none"> – SBR Database Status – SBR Status – SBR Database Reconfiguration Status – Policy Database Query <p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> • General Options • Access Point Names • Policy DRA <ul style="list-style-type: none"> – PCRFs – Binding Key Priority – PCRF Pools – PCRF Pool to PRT Mapping – PCRF Sub-Pool Selection Rules – Policy Clients – Suspect Binding Removal Rules – Site Options • Online Charging DRA <ul style="list-style-type: none"> – OCSs – CTFs – OCS Session State – Realms • Error Codes • Alarm Settings • Congestion Options <p>This option only displays with the DSR application.</p>

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
DCA Framework (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for DCA applications: <ul style="list-style-type: none"> • Custom MEALs (Measurements, Events, Alarms, and Logs) • General Options • Trial MPs assignment • Application Control • System Options
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only. This option only displays with the DSR application.
Help	Launches the Help system for the user interface
Legal Notices	Product Disclaimers and Notices
Logout	Allows the user to log out of the user interface

Missing Main Menu options

Permissions determine which Main Menu options are visible to users. Permissions are defined through the *Group Administration* page. The default group, *admin*, is permitted access to all GUI options and functionality. Additionally, members of the *admin* group set permissions for other users.

Main Menu options vary according to the group permissions assigned to a user's account. Depending on your user permissions, some menu options may be missing from the Main Menu. For example, Administration menu options do not display on your screen if you do not have administrative permissions. For more information about user permissions, see *Group Administration* in the OAM section of the online help, or contact your system administrator.

Common Graphical User Interface Widgets

Common controls allow you to easily navigate through the system. The location of the controls remains static for all pages that use the controls. For example, after you become familiar with the location of the display filter, you no longer need to search for the control on subsequent pages because the location is static.

Supported Browsers

This application supports the use of Microsoft® Internet Explorer 8.0, 9.0, or 10.0. is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details

System Login Page

Access to the user interface begins at the System Login page. The System Login page allows users to log in with a username and password and provides the option of changing the password upon login. The System Login page also features a date and time stamp reflecting the time the page was last refreshed. Additionally, a customizable login message displays just below the **Log In** button.

The user interface is accessed via HTTPS, a secure form of the HTTP protocol. When accessing a server for the first time, HTTPS examines a web certificate to verify the identity of the server. The configuration of the user interface uses a self-signed web certificate to verify the identity of the server. When the server is first accessed, the supported browser warns the user that the server is using a self-signed certificate. The browser requests confirmation that the server can be trusted. The user is required to confirm the browser request to gain access.

Customizing the Login Message

Before logging in, the System Login page displays. You can create a login message that displays just below the **Log In** button on the System Login page.

Figure 2-1 Oracle System Login

1. From the Main Menu, click **Administration > General Options**.
2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.

4. Click **OK** or **Apply** to submit the information.

A status message displays at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log into the user interface, the login message text displays.

Accessing the DSR Graphical User Interface

In DSR, some configuration is done at the **NOAM** server, while some is done at the **SOAM** server. Because of this, you need to access the DSR graphical user interface (GUI) from two servers. Certificate Management (Single Sign-On) can be configured to simplify accessing the DSR GUI on the NOAM and the SOAM.

For information on configuring Single Sign-On certificates, see **OAM > Administration > Access Control > Certificate Management** in the DSR online help.

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.

1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example <https://dsr-no.yourcompany.com>.

When using Single Sign-On, you cannot use the IP address of the server.

2. When prompted by the browser, confirm that the server can be trusted.

The System Login page displays.

3. Enter the Username and Password for your account.

The DSR GUI for the NOAM displays.

4. To access the DSR GUI for the SOAM, open another browser window and enter the fully qualified hostname of the SOAM.

The DSR GUI for the SOAM displays.

You can toggle between the DSR GUI on the NOAM and the DSR GUI on the SOAM as you perform configuration tasks.

Main Menu Icons

This table describes the icons used in the Main Menu.

Table 2-3 Main Menu Icons

Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.

Table 2-3 (Cont.) Main Menu Icons

Icon	Name	Description
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Task	Contains operations related to Tasks
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

In the user interface, tables, forms, tabbed pages, and reports are the most common formats.

Note: Screen shots are provided for reference only and may not exactly match a specific application's GUI.

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination with **First** | **Prev** | **Next** | **Last** links at both the beginning and end of this table type. Paginated tables also contain

action links on the beginning and end of each row. For more information on action links and other page controls, see [Page Controls](#).

Figure 2-2 Paginated Table

Displaying Records 1-1 of 1 First Prev Next Last										
Action	System ID		IP Address		Permission		Action			
Edit Delete	lisa		10.25.62.4		READ_WRITE		Edit	Delete		

Displaying Records 1-1 of 1 | First | Prev | Next | Last

Scrollable tables display all of the records on a single page. The scroll bar, located on the right side of the table, allows you to view all records in the table. Scrollable tables also provide action buttons that operate on selected rows. For more information on buttons and other page controls, see [Page Controls](#).

Figure 2-3 Scrollable Table

Sequence #	Alarm ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance	Alarm Text
3498	31201	2009-Jun-11 18:07:41.214 UTC	MAJOR	MiddleWare	procmgr	OAMPNE	teks8011006	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5445	31201	2009-Jun-11 18:07:27.137 UTC	MAJOR	MiddleWare	procmgr	SOAMP	teks8011002	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5443	31107	2009-Jun-11 18:07:24.704 UTC	MINOR	MiddleWare	inetmerge	SOAMP	teks8011002	COLL	teks8011004	DB merging from a child Source Node has failed
5444	31107	2009-Jun-11 18:07:24.704 UTC	MINOR	MiddleWare	inetmerge	SOAMP	teks8011002	COLL	teks8011003	DB merging from a child Source Node has failed
5441	31209	2009-Jun-11 18:07:22.640 UTC	MINOR	MiddleWare	reportmap	SOAMP	teks8011002	SW	teks8011003	Unable to resolve a hostname specified in the NodeInfo table.
										Unable to resolve a hostname specified in the NodeInfo table.

[Export](#)

Note: Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

Forms

Forms are pages on which data can be entered. Forms are typically used for configuration. Forms contain fields and may also contain a combination of lists, buttons, and links.

Figure 2-4 Form Page

Username:	<input type="text" value="Sample User Name"/>	(5-16 characters)
Group:	<input type="text" value="Unassigned"/>	<input type="button" value="▼"/>
Time Zone:	<input type="text" value="UTC"/>	<input type="button" value="▼"/>
Maximum Concurrent Logins:	<input type="text" value="1"/>	Maximum concurrent logins for a user (0=no limit). [Default = 1; Range = 0-50]
Session Inactivity Limit:	<input type="text" value="120"/>	Time (in minutes) after which login sessions expire (0 = never). [Default = 120; Range = 0-120]
Comment:	<input type="text" value="guiadmin"/> (max 64 characters)	
Temporary Password:	<input type="text" value="*****"/>	(8-16 characters)
Re-type Password:	<input type="text"/> (8-16 characters)	
<input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Tabbed pages

Tabbed pages provide collections of data in selectable tabs. Click on a tab to see the relevant data on that tab. Tabbed pages also group Retrieve, Add, Update, and Delete options on one page. Click on the relevant tab for the task you want to perform and the appropriate fields populate on the page. Retrieve is always the default for tabbed pages.

Figure 2-5 Tabbed Pages

Entire Network		*	System.CPU_CoreUtilPct_Average		System.CPU_CoreUtilPct_Peak		
		Timestamp	System CPU UtilPct Average	System CPU UtilPct Peak	System Disk UtilPct Average	System Disk UtilPct Peak	System RAM UtilPct Average
NOAMP	10/22/2009 19:45		6.764068	44	0.520000	1	7.939407
	10/22/2009 20:00		7.143644	25	0.520000	1	8.523822

Figure 2-6 Tabbed Pages

Retrieve	<input type="button" value="Add"/>	<input type="button" value="Update"/>	<input type="button" value="Delete"/>
Fields marked with a red asterisk (*) require a value.			
Field	Value	Description	
Network Entity	<input type="text"/>	* Numeric identifier for the Network Entity 1-15 DIGITS	
<input type="button" value="Retrieve"/>			

Reports

Reports provide a formatted display of information. Reports are generated from data tables by clicking **Report**. Reports can be viewed directly on the user interface, or they can be printed. Reports can also be saved to a text file.

Figure 2-7 Report Output

```
=====
User Account Usage Report
=====

Report Generated: Fri Jun 19 19:30:55 2009 UTC
From: Unknown Network OAM&P on host teks5001701
Report Version: 1.0
User: guiaadmin

=====
Username          Date of Last Login    Days Since Last Login  Account Status
-----          -----                  -----                  -----
guiaadmin        2009-06-19 19:00:17      0                   enabled

=====
End of User Account Usage Report
=====
```

Customizing the Splash Page Welcome Message

When you first log into the user interface, the splash page displays. Located in the center of the main work area is a customizable welcome message. Use this procedure to create a message suitable for your needs.

1. From the **Main Menu**, click **Administration > General Options**.
2. Locate **Welcome Message** in the **Variable** column.
3. Enter the desired welcome message text in the **Value** column.
4. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.

A status message displays at the top of the page to inform you if the operation was successful.

The next time you log into the user interface, the new welcome message text displays.

Column Headers (Sorting)

You can sort a table by a column by clicking the column header. However, sorting is not necessarily available on every column. Sorting does not affect filtering.

When you click the header of a column in a table that can be sorted, an indicator displays in the column header showing the direction of the sort. See [Figure 2-8](#). Clicking the column header again reverses the direction of the sort.

Figure 2-8 Sorting a Table by Column Header

Local Node Name	Realm	FQDN	SCTP Listen Port	TCP Listen Port	Connection Configuration Set	CEX Configuration Set
-----------------	-------	------	------------------	-----------------	------------------------------	-----------------------

Page Controls

User interface pages contain controls, such as buttons and links, that perform specified functions. The functions are described by the text of the links and buttons.

Note: Disabled buttons are grayed out. Buttons that are irrelevant to the selection or current system state, or which represent unauthorized actions as defined in Group Administration, are disabled. For example, **Delete** is disabled for users without Global Data Delete permission. Buttons are also disabled if, for example, multiple servers are selected for an action that can only be performed on a single server at a time.

[Table 2-4](#) contains examples of Action buttons.

Table 2-4 Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.
Delete	Deletes data from table.
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in [Table 2-5](#), are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information. The Submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 2-5 Submit Buttons

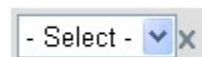
Submit Button	Function
OK	Submits the information to the server, and if successful, returns to the View page for that table.
Apply	Submits the information to the server, and if successful, remains on the current page so that you can enter additional data.
Cancel	Returns to the View page for the table without submitting any information to the server.

Clear Field Control

The clear field control allows you to clear the value from a list. The clear field control is available only on some lists.

Click the X next to a list to clear the field.

Figure 2-9 Clear Field Control X



Optional Layout Element Toolbar

The optional layout element toolbar displays in the Page Control Area of the GUI.

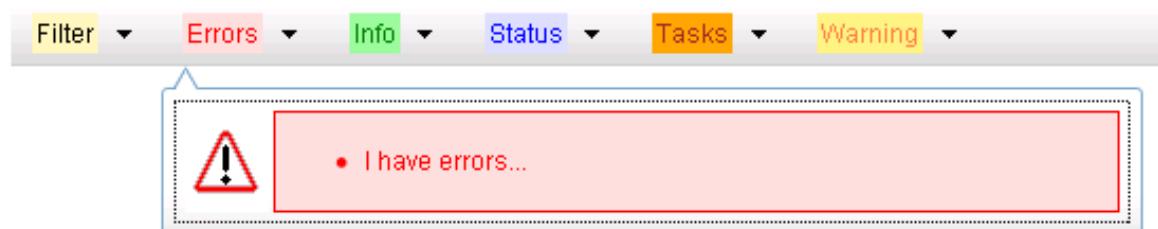
Figure 2-10 Optional Layout Element Toolbar

The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can display include:

- Filter – Allows you to filter data in a table.
- Errors – Displays errors associated with the work area.
- Info – Displays information messages associated with the work area.
- Status – Displays short status updates associated with the main work area.
- Warning – Displays warnings associated with the work area.

Notifications

Some messages require immediate attention, such as errors and status items. When new errors occur, the Errors element opens automatically with information about the error. Similarly, when new status items are added, the Status element opens. If you close an automatically opened element, the element stays closed until a new, unacknowledged item is added.

Figure 2-11 Automatic Error Notification

Note: Viewing and closing an error does not clear the Errors element. If you reopen the Errors element, previously viewed errors are still in the list.

When new messages are added to Warning or Info, the styling of the element changes to indicate new messages are available. The styling of the Task element changes when a task changes state (such as, a task begins or ends).

Opening an Element in the Toolbar

Use this procedure to open an element in the optional layout element toolbar.

1. Click the text of the element or the triangle icon to open an element.

The selected element opens and overlays the work area.

2. Click X to close the element display.

Filters

Filters are part of the optional layout element toolbar and appear throughout the GUI in the Page Control Area. For more information about optional layout element toolbar functionality, see [Optional Layout Element Toolbar](#).

Filters allow you to limit the data presented in a table and can specify multiple filter criteria. By default, table rows appear unfiltered. Three types of filters are supported, however, not all filtering options are available on every page. The types of filters supported include:

- Network Element – When enabled, the Network Element filter limits the data viewed to a single Network Element.

Note: Once enabled, the Network Element filter affect all pages that list or display data relating to the Network Element.

- Collection Interval – When enabled, the collection interval filter limits the data to entries collected in a specified time range.
- Display Filter – The display filter limits the data viewed to data matching the specified criteria.

Once a field is selected, it cannot be selected again. All specified criteria must be met in order for a row to be displayed.

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.

Figure 2-12 Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 2-6 Filter Control Elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.

Table 2-6 (Cont.) Filter Control Elements

Operator	Description
\geq	Displays all records with a parameter value that is greater than or equal to the specified value.
$<$	Displays all records with a parameter value that is less than the specified value.
\leq	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of Is Null in the specified field.

Note: Not all filterable fields support all operators. Only the supported operators are available for you to select.

Filtering on the Network Element

The global Network Element filter is a special filter that is enabled on a per-user basis. The global Network Element filter allows a user to limit the data viewed to a single Network Element. Once enabled, the global Network Element filter affects all sub-screens that display data related to Network Elements. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
2. Select a Network Element from the **Network Element** list.
3. Click **Go** to filter on the selection or click **Reset** to clear the selection.
4. For data tables that support compound filtering, click **Add** to add another filter condition and repeat steps 2 through 4.

Multiple filter conditions are joined by an AND operator.

Records are displayed according to the specified criteria.

Filtering on Collection Interval

The Collection Interval filter allows a user to limit the data viewed to a specified time interval. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
2. Enter a duration for the **Collection Interval** filter.

The duration must be a numeric value.

3. Select a unit of time from the list.

The unit of time can be seconds, minutes, hours, or days.

4. Select **Beginning** or **Ending** from the list.

5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering Using the Display Filter

Use this procedure to perform a filtering operation. This procedure assumes you have a data table displayed on your screen with the Display Filter field. This process is the same for all data tables. However, all filtering operations are not available for all tables.

Note: Display Filter does not support compound filtering. For example, you cannot filter on both severity and a server name. Try to filter on a single filter criteria, such as the server hostname for server-scoped metric cells; or the application name for St- and NE-scoped metric cells. You can also sort by congestion level (descending) to help improve your filter.

1. Click **Filter** in the optional layout element toolbar.

2. Select a field name from the **Display Filter** list.

This selection specifies the field in the table that you want to filter on. The default is **None**, which indicates that you want all available data displayed.

3. Select an operator from the operation selector list.

4. Enter a value in the value field.

This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (=) operator and a value of MINOR, the table would show only records where Severity=MINOR.

5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Note: PCA was known as PDRA and may still be seen in some filtering.

Pause Updates

Some pages refresh automatically. Updates to these pages can be paused by selecting the **Pause updates** checkbox. Uncheck the **Pause updates** checkbox to resume automatic updates. The **Pause updates** checkbox is available only on some pages.

Max Records Per Page Controls

Max Records Per Page is used to control the maximum number of records displayed in the page area. If a page uses pagination, the value of Max Records Per Page is used. Use this procedure to change the Max Records Per Page.

1. From the **Main Menu**, click **Administration > General Options**.
2. Change the value of the **MaxRecordsPerPage** variable.

Note: **Maximum Records Per Page** has a range of values from 10 to 100 records. The default value is 20.

3. Click **OK** or **Apply**.

OK saves the change and returns to the previous page.

Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Range Based Address Resolution

This section provides an overview of the function of the **Range Based Address Resolution (RBAR)** application.

Range Based Address Resolution overview

Range Based Address Resolution (RBAR) is an enhanced routing application that allows routing of Diameter end-to-end transactions based on Diameter Application ID, Command Code, **Routing Entity** Type, and Routing Entity Addresses (range and individual) as a Diameter **Proxy Agent**.

A Routing Entity can be any of the following:

- A User Identity:
 - International Mobile Subscriber Identity (**IMSI**)
 - Mobile Subscriber Integrated Services Digital Network (Number) (**MSISDN**)
 - IP Multimedia Private Identity (**IMPI**)
 - IP Multimedia Public Identity (**IMPU**)
- An IP Address associated with the User Equipment
 - IPv4 (based upon the full 32-bit value in the range of 0x00000000 to 0xFFFFFFFF)
 - IPv6-prefix (1 to 128 bits)
- A general purpose data type: **UNSIGNED16** (16-bit unsigned value)

Routing resolves to a **Destination** that can be configured with any combination of a **Realm** and **Fully Qualified Domain Name** (FQDN); Realm-only, FQDN-only, or **Realm** and **FQDN**.

When a message successfully resolves to a destination, RBAR replaces the destination information (Destination-Host and/or Destination-Realm) in the ingress message with the corresponding values assigned to the resolved destination, and forwards the message to the (integrated) **Diameter Relay Agent** for egress routing into the network.

RBAR Functions

RBAR provides the following functions:

Reserved MCC Ranges

Mobile Country Code (MCC) ranges that are reserved for future use are defined in a system-wide **MCC Ranges** table. If the MCC digits portion of the decoded IMSI digits fall within one of the ranges designated in the **MCC Ranges** table, the IMSI digits are NOT used for further Address Resolution. RBAR continues decoding the digits using

other AVP instances, or next Priority AVP (if provisioned), or next Routing Entity (if provisioned).

Identifying IMSIs and MSISDNs

Address resolution applications like Full Address Based Resolution (FABR) and (RBAR) need to categorize User Identities (digit strings) decoded from the Diameter Request AVPs as either MSISDN or IMSI, to allow looking up the User Identity in the appropriate lookup table.

If there is no plus sign before the digits, the Routing Entity Type is IMPU, and decoded digits falls within MSISDN and IMSI overlap range, configured MCC+MNC combinations can be compared to the first 5 or 6 digits of the User Identity. If a match occurs, the User Identity is considered as an IMSI and used for IMSI lookup. If a match does not occur, the User Identity is considered as an MSISDN and used for MSISDN lookup.

[Identifying IMSIs and MSISDNs](#) provides more information about identifying IMSIs and MSISDNs using digit string lengths and MCC+MNC combinations.

Application Chaining

Application Routing Rules can be configured so that RBAR and the PCA applications can be run independently on a same DSR DA-MP without interfering with each other's functionality.

Assumption and Limitation

In Diameter, all IMSIs are in the form of an ITU-T E.212 number. It is assumed that customers provision all IMSIs within the RBAR database as E.212 values. E.212 to E.214 conversion is not supported.

Address Ranges

An Address Range contains the following attributes:

- Routing Entity Type
- Start Address
- End Address
- Destination

RBAR Address Ranges are at least two addresses.

A common set of Address Ranges (such as all IMSIs associated with a LTE-HSS) is called a Digit Range Table (DRT).

For a DRT that can be associated with User Identity Types,

- RBAR supports DRT Address Ranges with different digit lengths.
or example, the range 9195550000 - 9195559999 and the range 303200 - 303299 are allowed in the same DRT.
- RBAR supports a minimum of 8 different DRT Address Range digit lengths.
For example, an MSISDN DRT could contain Address Ranges with 3 digits, 6 digits, 10 digits and 15 digits.

For a DRT that can be associated with the Routing Entity Type IPv6-Prefix Address, RBAR supports a minimum of 32 different DRT Address Range bit lengths.

The Start Address and the End Address attributes of an Address Range entry that can be associated with the Routing Entity Type UNSIGNED16 are always a 16-bit value.

Individual Addresses

An Individual Address contains the following attributes:

- (AET) Table Name
- Address
- Routing Entity Type
- Destination

A common set of Individual Addresses (such as all IMSIs associated with a LTE-HSS) is called an Address Exception Table (AET).

The Address attribute of an Individual Address that can be associated with User Identity Types contains a minimum of three (3) and a maximum of fifteen (15) digits.

The Address attribute of an Individual Address that can be associated with the Routing Entity Type (IPv4 Address) is always a 32-bit value.

The Address attribute of an Individual Address that can be associated with the Routing Entity Type (IPv6-Prefix Address) contains a minimum of one (1) and a maximum of 128 bits.

The Address attribute of an Individual Address that can be associated with the Routing Entity Type (UNSIGNED16) is always a 16-bit value.

For an AET that can be associated with User Identity Types and with the Routing Entity Type (IPv6-Prefix Address), RBAR supports addresses with different digit lengths.

Application Chaining

Application Chaining for RBAR and PCA refers to the enhanced ability to support the running of multiple DSR applications independently on a same DSR DA-MP without interfering to each other's functionality and the two applications can be invoked in turn on the same DA-MP. The order in which the applications are invoked can be configured based on the existing and enhanced **Application Routing Rule**.

When DSR receives a request, the routing layer makes the decision to forward the message, either to an application residing in the DSR or to a peer DSR node. This decision is based on the Application Routing Table (ART) rules. The ART also determines which application is initially forwarded the message.

Historically, Diameter messages use the Command Code as one of the main parameters in the ART to help with the DRL application forwarding decision. Application chaining enhances and expands the currently used Command Code parameter into an Extended Command Code (ECC) that contains the following attributes:

- ECC name, which is the actual Command Code name
- Command Code value
- AVP code Value, an AVP within the Command Code
- AVP data value

Application Route Table (ART)

Application Route Tables (ART) are used for routing Request messages to DSR Applications. An Application Route Table consists of a set of prioritized Application Routing Rules that the Diameter Routing Function searches with the content of a Request message, to determine whether the message should be forwarded to a DSR Application for processing.

The ART is searched when a Request message is received from a Peer Node or a DSR Application. Searching an ART when a Request message is received from a DSR Application allows the operator to route the ingress Diameter transaction to multiple DSR Applications in sequence. The operator can create multiple ARTs to assign an ART to a Request message based upon a set of user-defined criteria.

One ART is searched each time a Request message is received from a Peer Node or a DSR Application. This method allows forwarding a Diameter transaction to one or more DSR Applications for processing.

However, the Diameter Routing Function does not allow a DSR application to process a Diameter transaction more than once. The Diameter Routing Function internally keeps track of which DSR applications have already processed the message. When the Diameter Routing Function is searching an ART and encounters an Application Routing Rule that is associated with a DSR application that has already processed the transaction, that Application Routing Rule is bypassed.

For RBAR and PCA Application chaining, up to six parameters may be used to form Application Routing Rules:

- Application ID
- Extended Command Code
- Origin-Host
- Origin-Realm
- Destination-Host
- Destination-Realm

A priority is also assigned to each Application Routing Rule. If conditions in multiple rules are triggered simultaneously, the associated priority determines which rule applies.

Request Message Validation

The RBAR application processes the diameter request message based on the configuration, to extract the user identity addresses.

When RBAR receives a diameter request message, the following validation is performed:

- Determine whether the Application ID in the message header is defined in the configuration.

If a valid Application ID cannot be found, the message is not processed. An answer response with a Result code AVP for DIAMETER_APPLICATION_UNSUPPORTED is returned.

- If a valid (configured) Application ID is received in a diameter request message, validate whether the pair (Application ID, command code) received in the message is defined in the configuration.

If the pair cannot be found in the configuration, the appropriate routing exception handling procedure is invoked.

- If the pair is configured, search for a valid routing entity address in the message based on the highest priority routing entity type (Primary routing entity type in address resolution configuration) assigned to the pair.
- Search for a valid routing entity address in the message based on a prioritized set of AVPs assigned to the triplet.

If a valid routing entity address cannot be found in searching the configured routing entity types assigned to the pair, the routing exception handling procedure is invoked that is assigned to the Application ID and this routing entity type.

Routing Exception Handling

When an ingress RBAR request message cannot be resolved to a destination (no address matched, no valid digits decoded, or any other error returns), RBAR invokes a routing exception handling procedure based on user-defined configuration.

Routing exception handling procedures result in one for the following configured actions:

- Forward the message unchanged
- Forward the message using a user-defined default destination
- Send answer response with a user-defined result-code AVP value and error message AVP
- Send answer response with user-defined experimental-code AVP values and error message AVP
- Abandon request (discard the ingress diameter request message)

The routing exceptions support the following:

- Unknown command code
- Valid address not found
- Valid address was found and did not match a configured address or address range

Supported AVPs

RBAR supports the AVPs associated with a user identity type (IMSI, MSISDN, IMPI, IMPU) as defined in [Table 3-1](#).

Table 3-1 RBAR Supported AVPs

For a User Identity			
Type (IMSI, MSISDN, IMPI, IMPU) AVPs	Code	AVP Type	AVP Reference
User-Name	Vendor-ID: none AVP code: 1	UTF8String	Section 8.14 of RFC 3588bis

Table 3-1 (Cont.) RBAR Supported AVPs

For a User Identity			
Type (IMSI, MSISDN, IMPI, IMPU) AVPs	Vendor ID and AVP Code	AVP Type	AVP Reference
Service-Information [Subscription-ID]	Vendor-ID: 10415 (3GPP) AVP code: 873	Grouped	Section 7.2.192 of 3GPP 32.299
Subscription-ID [Subscription-ID-Data]	Vendor-ID: none AVP code: 443	Grouped	Section 8.46 of RFC 4006
Subscription-ID-Data	Vendor-ID: none AVP code: 444	UTF8String	Section 8.48 of RFC 4006
Public-Identity	Vendor-ID: 10145 (3GPP) AVP code: 601	UTF8String	Section 6.3.2 of 3GPP 29.229
MSISDN	Vendor-ID: 10415 (3GPP) AVP code: 701	OctetString	Section 6.3.2 of 3GPP 29.329
User-Identity: [Public-Identity] [MSISDN]	Vendor-ID: 10415 (3GPP) AVP code: 700	Grouped	Section 6.3.1 of 3GPP 29.329
Public-Identity	Vendor-ID: 10145 (3GPP) AVP code: 601	UTF8String	Section 6.3.2 of 3GPP 29.229
MSISDN	Vendor-ID: 10415 (3GPP) AVP code: 701	OctetString	Section 6.3.2 of 3GPP 29.329
User-Identifier: [User-Name] [MSISDN]	Vendor-ID: none AVP code: 3102	Grouped	Section 6.4.2 of 3GPP 29.336
User-Name	Vendor-ID: none AVP code: 1	UTF8String	Section 8.14 of RFC 3588bis
MSISDN	Vendor-ID: 10415 (3GPP) AVP code: 701	OctetString	Section 6.3.2 of 3GPP 29.329
For a Routing Entity Type IPv4 Address			
Framed-IP-Address	Vendor-ID: none AVP code: 8	OctetString	Section 6.11.1 of RFC 4005

Table 3-1 (Cont.) RBAR Supported AVPs

For a User Identity			
Type (IMSI, MSISDN, Vendor ID and AVP IMPI, IMPU) AVPs	Code	AVP Type	AVP Reference
For a Routing Entity Type IPv6 Prefix Address			
Framed-IPv6-Prefix	Vendor-ID: none AVP code: 97	OctetString	Section 6.11.6 of RFC 4005

Each of the configured user identity types supported in RBAR is associated with certain AVPs that contain the user identity type as defined by various diameter application standards. [Table 3-2](#) presents all possible combinations of the user identity types and the associated AVPs.

Table 3-2 Combinations of User Identity Types and Associated AVPs

User Identity Types/AVPs	IMSI	MSISDN	IMPI	IMPU
MSISDN		Applicable		Applicable
User-Identity: MSISDN		Applicable		Applicable
Public-Identity	Applicable	Applicable	Applicable	Applicable
User-Identity: Public-Identity	Applicable	Applicable	Applicable	Applicable
User-Name	Applicable	Applicable	Applicable	Applicable
User-Identifier: User-Name	Applicable		Applicable	
User-Identifier: MSISDN		Applicable		Applicable
Subscription-ID-Data (0-E.164)		Applicable		Applicable
Service-Information: Subscription-ID-Data (0-E.164)		Applicable		Applicable
Subscription-ID-Data (1-IMSI)	Applicable		Applicable	
Service-Information: Subscription-ID-Data (1-IMSI)	Applicable		Applicable	
Subscription-ID-Data (2-SIP URI)	Applicable	Applicable	Applicable	Applicable
Service-Information: Subscription-ID-Data (2-SIP URI)	Applicable	Applicable	Applicable	Applicable
Subscription-ID-Data (3-NAI)	Applicable	Applicable	Applicable	Applicable

Table 3-2 (Cont.) Combinations of User Identity Types and Associated AVPs

User Identity Types/AVPs	IMSI	MSISDN	IMPI	IMPU
Service-Information: Subscription-ID-Data (3- NAI)	Applicable	Applicable	Applicable	Applicable
Subscription-ID-Data (4- Private)	Applicable	Applicable	Applicable	Applicable
Service-Information: Subscription-ID-Data (4- Private)	Applicable	Applicable	Applicable	Applicable
Wildcarded-Public-Identity				Applicable

A user identity type can be associated with one or more data formats that is examined when deriving the user identity address from the associated AVPs. The relation between user identity types and the corresponding data formats to be encountered in the ingress diameter request message are listed in [Table 3-3](#).

Table 3-3 Relation between Configured User Identity Types and Data Formats

Configurable User Identity Types/User Identity Formats in Messages	IMSI	MSISDN	IMPI	IMPU
IMSI Format: ASCII Example: 311480123456789	Applicable		Applicable	
MSISDN Format: ASCII and TBCD Example: 19194605500		Applicable		Applicable
SIP URI with IMSI Format: ASCII Examples: sip:123456789012345@nai.epc.mnc456.mcc123.3gppnetwork.org sip:6311150999995555@ims.mnc015.mcc311.3gppnetwork.org sip:311480999995555@my.network.org sip: 6311480999995555@my.network.org	Applicable		Applicable	

Table 3-3 (Cont.) Relation between Configured User Identity Types and Data Formats

Configurable User Identity Types/User Identity Formats in Messages	IMSI	MSISDN	IMPI	IMPU
SIP URI with MSISDN Format: ASCII Examples: sip: +1-919-460-5500@xy z.com;user=phone sip: 311480999995555@ my.network.org		Applicable		Applicable
SIP URI with NAI Format: ASCII Example: sip: 311480999995555@ my.network.org			Applicable	Applicable
TEL URI with MSISDN FORMAT: ASCII Examples: tel:+1-919-460-5500; phone-context=example.com tel:+19258889999 tel:19195551212		Applicable		Applicable
NAI with IMSI/ MSISDN Format: ASCII Examples: 123456789012345@xyz.com 123456789012345 311480999995555@ims.mnc480.mcc311.3gppnetwork.org 6311150999995555@xyz.com 6311150999995555@ims.mnc015.mcc311.3gppnetwork.org	Applicable	Applicable	Applicable	Applicable
NAI Format: ASCII Example: handy.manny@xyz. com			Applicable	Applicable

Routing Based on IMSI/MSISDN Prefix Lookup

If configured, RBAR performs prefix-based lookups after the full address lookup is performed. The prefix and range based lookup is only performed if the full address lookup does not find a match and can be enabled by the operator for a combination of Application ID, Command-Code, and Routing Entity type.

If a match is found in the prefix database, that RBAR application populates the Destination-Host AVP and/or the Destination-Realm AVP based on the resolved destination.

If a match is not found in the prefix database, then RBAR performs the no address match found routing exception handling procedure.

The IMSI/MSISDN prefix and range lookup can be enabled or disabled on a system wide basis.

Identifying IMSIs and MSISDNs

In certain diameter messages over the Cx interface (and possibly over the Sh interface), certain AVPs that typically carry an IMSI sometimes can carry an MSISDN.

Address resolution applications like Full Address Based Resolution (FABR) and Range Based Address Resolution (RBAR) need to categorize user Identities (digit strings) decoded from the diameter request AVPs as either MSISDN or IMSI, to allow looking up the user identity in the appropriate lookup table.

Most of the time, these applications can clearly categorize the decoded user identity based on:

- The configured routing entity type
- The contents of the AVP

For instance, if the user identity has been decoded from a SIP URI that has a plus sign before the digits (such as sig:+1-919-460-5500@oracle.com), it can be directly categorized as an MSISDN.

- The number of digits in the user identity

In certain cases, none of these methods allow a clear categorization (for example, if the number of digits needs to be used and the received number of digits are applicable to both IMSIs and MSISDNs, and thus leads to an ambiguous determination; or if there is no plus sign before the digits).

If RBAR has been configured to decode an IMPU/MSISDN from a user identity (digit string), but cannot determine whether the user identity is an IMSI or an MSISDN based on digit analysis, a tie-breaker is needed to properly categorize the user identity.

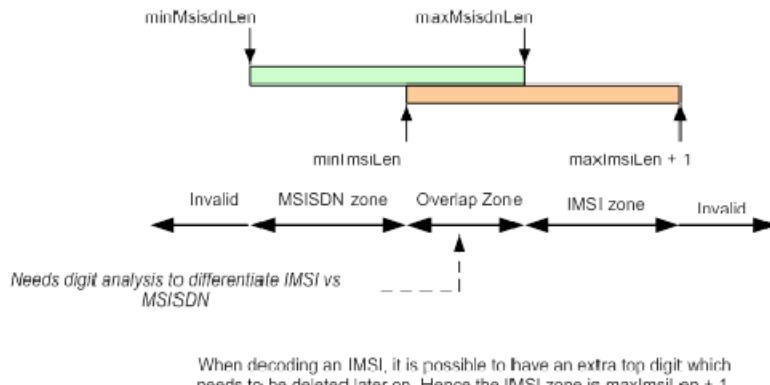
If the routing entity type is IMPU, the user identity extracted results in only digits and the length of the digits in the user identity falls within an overlap digits range of MSISDN and IMSI. As shown in [Figure 3-1](#), if the user identity is an IMSI or MSISDN the logic is determined as follows:

- RBAR extracts the first 5 or 6 digits of the user identity and compares them against a list of configured 5- or 6-digit MCC-MNC combinations.

The **Diameter Common > Network Identifiers > MCCMNC** pages can be used to configure up to 2500 distinct combinations of Mobile Country Code (MCC) and Mobile Network Code (MNC). (Refer to the *Diameter Common User's Guide* and Help for procedures to configure MCC-MNC combinations.)

- If a match occurs, the user identity is considered as an IMSI. RBAR bypasses the AVP, since RBAR does not support decoding an IMSI form a routing entity IMPU or MSISDN.
- If a match does not occur, the user identity is considered as a MSISDN and used for MSISDN lookup.

Figure 3-1 IMSI/MSISDN Overlap Range Scenario



Multiple DSR Application Invocation Prevention

The DSR provides a mechanism for preventing the same DSR Application from being invoked on two different DSR nodes:

- When a DSR Application does not want to be invoked a second time on another DSR, it can insert a DSR AVP called DSR-Application-Invoked containing its DSR Application ID.
- When the Diameter Routing Function searches an ART, it ignores any Application Routing Rules associated with a DSR-Application that has inserted the DSR-Application-Invoked AVP.

DSR-Application-Invoked AVP

To prevent the same DSR Application from being invoked on multiple DSRs in a network (and processing the same message twice by the same DSR Application), a DSR Application can (optionally) add to the Request message a DSR-Application-Invoked AVP containing the DSR Application ID as describe in [DSR-Application-Invoked AVP](#).

Table 3-4 DSR-Application-Invoked AVP

Byte 1	Byte 2	Byte 3	Byte 4
		AVP Code = 2468	
Flags=10000000		Length = 16	
		Vendor ID = 323	
	DSR Application Id = Unsigned32		

This AVP is decoded by the Diameter Routing Function before ART processing to prevent multiple invocations of the same DSR application. Any Application Routing Rule with this DSR Application ID is ignored by the Diameter Routing Function.

This AVP can be repeated in the Request to indicate different DSR Applications, but is inserted only once per DSR Application.

Insertion of a DSR Application-Invoked AVP is controlled by DSR Application-specific System Options configuration, such as:

Allow Subsequent RBAR Invocation – Checked = Yes, Unchecked = No

If checked, subsequent invocation of RBAR on a different DSR node in the network is allowed.

Metadata Recording for Integrated DIH (IDIH)

Integrated DIH (IDIH) can be used to capture detailed information about selected Diameter transactions, and transmit this information to DIH for further analysis.

The Diameter Routing Function and invoked DSR applications record detailed information about each Diameter transaction - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the Trace Transaction Record (TTR) in the order that the metadata-generating events actually occurred. Together, all of the metadata records combine to document the processing performed on the entire transaction, and can later be used to provide diagnostic information when performing troubleshooting.

Metadata is recorded to a TTR for each transaction so that, even if the transaction is selected to be sent to DIH at an Answer Troubleshooting Trigger Point (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction is present.

The functions of IDIH are described in the *Integrated DIH User's Guide* and Help.

RBAR records the application-specific metadata events described in [Table 3-5](#).

Table 3-5 RBAR Metadata-Generating Events

Event	Type	Scope	Instance Data	When Recorded
Address Resolution	Address Resolution	App Data	<ul style="list-style-type: none"> • Routing Entity Type (such as IMSI) • Routing Entity AVP (such as User Name) • Routing Entity Address (such as 123456789012345) 	After RBAR searches and finds a valid Routing Entity address in an ingress Request message using a prioritized set of AVPs associated with the highest priority Routing Entity Type assigned to the Address Resolution order pair (Diameter Application ID, Command Code).

Table 3-5 (Cont.) RBAR Metadata-Generating Events

Event	Type	Scope	Instance Data	When Recorded
Routing Entity address resolved to a Destination address for request message routing	Destination Resolution	App Data	<ul style="list-style-type: none"> • Destination Routing Table Format (such as AET) • Destination Realm (such as xyz.com) • Destination FQDN (such as hss1.hss.xyz.com) 	When a valid Routing Entity address extracted from an Ingress Request message matches an AET or DRT entry for request message routing.
Routing Exception	Routing Exception	App Data	<ul style="list-style-type: none"> • Routing Exception Type (such as Unknown Command Code) • Routing Exception Action (such as Abandon Request) 	After any Routing Exception is encountered.

Configuration of RBAR

This section describes the procedures used to configure the RBAR application.

Pre-Configuration Activities

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

- Verify server status
- Gather information that is required for Diameter, Diameter Common, and RBAR configuration
- Configure Diameter Common components that are required for RBAR configuration
- Configure Diameter components that are required for RBAR configuration

Verifying Server status

Use this task to verify server status before RBAR configuration.

1. From the active SOAM, click **Status & Manage > Server**.
2. Verify that for each server, the **Appl State** field is **Disabled**, and the **DB, Reporting Status**, and **Proc** fields are **Norm**.

Diameter Common Configuration for RBAR

The following Diameter Common configuration must be done before RBAR configuration can be performed.

Use the explanations and procedures in the Diameter Common configuration help and the *Diameter Common User's Guide* to complete the Diameter Common configuration, including the Diameter Common components needed for use with RBAR.

SOAM Diameter Common Configuration

Diameter Common configuration for MCC Ranges Network Identifiers and MP Profile assignment for RBAR is done from the **SOAM GUI** in a DSR topology.

1. MPs

Click **Diameter Common > MPs > Profile Assignments** and verify the correct Database MP Profiles have been assigned for RBAR DA-MPs. If assignments need to be made or changed, use the **Diameter Common > MPs > Profile Assignments** page to assign the correct MP Profiles.

If RBAR and **Policy DRA** are running on the same DA-MP, select a Session_Database MP Profile.

2. MCC Ranges

Use the **Diameter Common > Network Identifiers > MCC Ranges [Insert]** page to specify up to 10 distinct, non-overlapping **MCC Ranges**.

The following two **MCC Ranges** are reserved by telephony standards and are recommended to be created in addition to other specified ranges:

- a. 000-199
- b. 800-899

NOAM Diameter Common Configuration

Diameter Common configuration for MCCMNC and MCCMNC Mapping Network Identifiers for RBAR is done from the **NOAM GUI** in a DSR topology.

1. Use the **Diameter Common > Network Identifiers > MCC Ranges [Insert]** page to configure MCCMNC entries.

Diameter Configuration for RBAR

The following Diameter configuration must be done before RBAR configuration can be performed.

All Diameter Configuration is done using the **SOAM GUI** in a DSR topology.

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

1. Application IDs

Diameter Application IDs must be configured before making them available for use in an RBAR Address Resolution. Use the **Diameter > Configuration > Application IDs [Insert]** page to configure Diameter Application IDs.

The Application IDs that need to be configured depend on the types of Diameter servers being supported, including **HSS**, **PCRF**, **OFCS**, and **OCS**.

2. Command Codes

Diameter Command Codes must be configured before using them in an RBAR Address Resolution. Use the **Diameter > Configuration > Command Codes [Insert]** page to configure Diameter Command Codes.

Configure any Command Codes that need to be handled by RBAR. The Command Codes are associated with the Diameter Applications supported by the Diameter servers (for example, HSS, PCRF, OCFS, or OCS) which are the destination of Diameter Requests being routed by RBAR. For example, the combination of Application ID = S6a and Command Code = ULR/ULA might be relevant for HSS.

3. 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 RBAR and other DSR Applications.

4. 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 are directed to RBAR.

Set the **Application Name to RBAR**.

If the RBAR application and the DM-IWF application are chained so that both of them can process the same Request message, insert or edit a second Application Routing Rule with the Application Name set to DM-IWF.

Set the Priority in each of the two Application Routing Rules to indicate which application processes the message first (the higher priority processes first).

RBAR Configuration

The **RBAR > Configuration** pages manage the **RBAR** configuration, which typically occurs in the following order:

1. Add Diameter **Applications** to a list of RBAR-supported Diameter Applications.
2. Configure **Destinations**.
3. If necessary, edit the Routing Exception Action associated with routing **Exceptions**.
4. Configure **Address Tables**.
5. Configure **Addresses**, specifying either address ranges or individual addresses.
6. Configure **Address Resolutions**.
7. If necessary, change the **System Options**.

Applications configuration

The **RBAR > Configuration > Applications** page allows you to access a list of Diameter Applications supported by RBAR.

From the **RBAR > Configuration > Applications** page, you can:

- Filter the list of supported Diameter Applications to display only the desired Application(s).
- View a list of supported Diameter Applications.
- Insert a supported Diameter Application.

Note: When an Application entry is added, Routing Exceptions (Unknown Command Code, No valid Routing Entity Address, No Address Match) are automatically inserted with the Routing Exception Action value as Forward Unchanged.

- Delete a Diameter Application from the list of supported Diameter Applications.

Note: When an Application entry is deleted, the associated Routing Exceptions are automatically deleted.

Applications configuration elements

[Table 4-1](#) describes the fields on the Applications insert page.

Table 4-1 Applications Configuration Elements

Field	Description	Data Input Notes
*Application ID	Diameter application ID, used by RBAR, along with command code and routing entity type to determine address resolution for routing request messages.	Format: list Range: configured Diameter application IDs Default: none
*Routing Mode (Read only)	Method of routing for request messages received containing the diameter application ID.	Format: disabled list with a value of Proxy .

Inserting a supported Diameter application

Use this task to add an application ID in the Diameter message.

Inserting a supported application automatically adds three (3) routing exceptions (**Unknown Command Code**, **No valid Routing Entity Address**, and **Missing Configured Address Entry**) with the **Routing Exception Action** set to **Forward Unchanged**.

1. Click **RBAR > Configuration > Applications**.
2. Click **Insert**.
3. From the **Application ID** list, select the Application ID in the Diameter message.

Note:

The application IDs displayed in this list are those created using **Diameter > Configuration > Application IDs**.

Note the **Routing Mode** field is disabled.

For more information about each field, see [Application configuration elements](#).

Note: The **Routing Mode** field is disabled.

4. Perform one of the following actions:
 - Click **OK** to save the application and return to the **RBAR > Configuration > Applications** page.
 - Click **Apply** to save the application and stay on this page.

Note: If field validations succeed after clicking either **OK** or **Apply**, the new application is saved and an informational message about the automatic addition of the routing exceptions appears.

- Click **Cancel** to return to the **RBAR > Configuration > Applications** page without saving the changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The **Application ID** is empty; no value was entered or selected
- The **Application Name** or **Application ID** is not unique; it already exists in the system
- The entry in any field is not valid (wrong data type or out of the valid range)
- The maximum number of supported Diameter applications (16) is already defined in the system

Deleting a Diameter application

Use this task to delete a Diameter application ID from the list of supported Diameter applications.

An application ID cannot be deleted if it is being used by an address resolution. Before you perform this task, delete any address resolution that uses the application.

1. Click **RBAR > Configuration > Applications**.
2. Select the application ID you want to delete and click **Delete**.
3. Click **OK** or **Cancel** on the confirmation screen.

If **OK** is clicked and the application is in use by an address resolution, an error message displays.

Exceptions configuration

The **RBAR > Configuration > Exceptions** page allows you to specify the routing exception action to take when **RBAR** is unable to resolve an address to a destination for each supported Diameter application and routing exception type.

There are three (3) routing exception entries (**No Address Match**, **No valid Routing Entity Address**, and **Unknown Command Code**) automatically inserted with the **Routing Exception Action** set to **Forward Unchanged** as the default action for a supported Diameter application entry when that application entry is added. Similarly, these Routing Exceptions that are associated with an application entry are automatically deleted when that application entry is deleted.

From the **RBAR > Configuration > Exceptions** page, you can:

- Filter the list of exceptions to display only the desired exceptions.
- View a list of supported Diameter applications and their associated routing exception types and routing exception actions.
- Edit the routing exception action and its associated attributes for a supported Diameter application.

Exceptions configuration elements

[Table 4-2](#) describes the fields on the Exceptions edit page.

Table 4-2 Exceptions Configuration Elements

Field	Description	Data Input Notes
*Application ID	Application ID in a Diameter message - read only	none
Application Name	Name of the application - read only	none
*Routing Exception Type	The routing exception that prevented address resolution - read only. This field displays one of the following values: <ul style="list-style-type: none"> • Unknown Command Code • No valid Routing Entity Address • No Address Match 	none
Routing Exception Action	The action applied to modify the Routing Exception Type message.	Format: options Range: <ul style="list-style-type: none"> • Forward • Unchanged • Forward to Destination • Send Answer with Result-Code AVP • Send Answer with Experimental-Result AVP • Abandon • Request
Destination	Destination to where the message is forwarded associated with the Routing Exception Type . This field is enabled when the Routing Exception Action is set to Forward to Destination.	Format: list Range: available user-configured destinations
Result-Code Value	Result code associated with this Routing Exception Type . This field is enabled when the Routing Exception Action is set to either Send Answer with Result-Code AVP or Send Answer with Experimental-Result AVP.	Format: <ul style="list-style-type: none"> • field • list Range: <ul style="list-style-type: none"> • field: 1000-5999 • list of available diameter answer codes
Vendor-ID	Value returned in the vendor-ID AVP of the answer message associated with this Routing Exception Type . This field is enabled when the Routing Exception Action is set to Send Answer with Experimental-Result AVP.	Format: field Range: 1-4294967295 Default: none

Table 4-2 (Cont.) Exceptions Configuration Elements

Field	Description	Data Input Notes
Error Message	Value returned in the Error-Message AVP of the answer message. This field is enabled when the Routing Exception Action is set to either Send Answer with Result-Code AVP or Send Answer with Experimental-Result AVP.	Format: alphanumeric, underscore (_), period (.) Range: 0–64 characters Default: none

Editing a Routing Exception

Use this task to edit a Routing Exception.

1. Click **RBAR > Configuration > Exceptions**.
2. Select the Application ID/Name you want to edit and click **Edit**.
3. Update the relevant fields.

For more information about each field, see [Exception configuration elements](#).

4. Click **OK, Apply, Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- A valid **Vendor-ID** is missing when the **Routing Exception Action** is Send Answer with Experimental Result-Code AVP.
- A valid **Destination** is missing when the **Routing Exception Action** is Forward to Destination.
- A valid **Result-Code Value** is missing when the **Routing Exception Action** is Send Answer or Send Answer with Experimental-Result AVP.

Destinations configuration

The **RBAR > Configuration > Destinations** page contains the attributes associated with a destination to which RBAR routes a message. RBAR uses these attributes to modify the contents of a received message before forwarding the message.

Each destination can be configured with any combination of a Realm and FQDN such as Realm-only, FQDN-only, or Realm and FQDN.

From the **RBAR > Configuration > Destinations** page, you can:

- Filter the list of destinations to display only the desired destinations.
- View a list of destinations.
- Insert a destination.
- Edit a destination.
- Delete a destination.

Destinations configuration elements

Table 4-3 describes the fields on the Destinations insert and edit pages.

Table 4-3 Destinations Configuration Elements

Field	Description	Data Input Notes
*Name	Unique name of the destination If a duplicate name is entered or the name is not specified, an error message appears.	Format: field Range: 1–32 characters; cannot start with a digit and must contain at least one alpha Default: none
Realm	Realm of the destination The Realm and Fully Qualified Domain Name cannot both be empty; otherwise, an error message appears.	Format: Text box; string consisting of a list of labels separated by dots, where a label must contain letters, digits, hyphen (-) and underscore (_). A label must start with a letter or underscore and must end with a letter or digit. Underscores may be used only as the first character. Range: A valid FQDN or Realm. A label consists of up to 63 characters and a Realm or FQDN up to 255 characters Default: none
Fully Qualified Domain Name	Unique Fully Qualified Domain Name of the destination If a duplicate FQDN is entered, an error message appears. The Fully Qualified Domain Name and Realm cannot both be empty; otherwise, an error message appears.	Format: Text box; string consisting of a list of labels separated by dots, where a label must contain letters, digits, hyphen (-) and underscore (_). A label must start with a letter or underscore and must end with a letter or digit. Underscores may be used only as the first character. Range: A valid FQDN or Realm. A label consists of up to 63 characters and a Realm or FQDN up to 255 characters Default: none
Allow Subsequent RBAR invocation	Enables the subsequent invocation of RBAR on a different DSR node in the network, when RBAR resolves to this destination.	Format: check box Range: checked, unchecked Default: checked

Note: If the **System Options Allow Subsequent RBAR Invocation** option is checked, then this attribute is ignored.

Inserting a Destination

Use this task to add a new Destination.

1. Click **RBAR > Configuration > Destinations**.
2. Click **Insert**.
3. Enter a unique name for the destination in the **Name** field.

For more information about each field, see [Destinations configuration elements](#).

4. Enter the realm in the **Realm** field.
5. Enter a unique FQDN in the **Fully Qualified Domain Name** field.
6. If you want to allow subsequent invocation of RBAR on a different DSR node in the network, leave the **Allow Subsequent RBAR invocation** check box selected (by default, this option is checked).

Note: If you do not want to allow subsequent invocation of RBAR on a different DSR node in the network when RBAR resolves to this destination, uncheck this check box. In addition, the **Allow Subsequent RBAR invocation** check box on the System Options page must be unchecked. For more information about the System Options attributes, see [System options elements](#).

7. Click **OK**, **Apply**, or **Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Both the **Realm** and **Fully Qualified Domain Name** are empty; no value was entered
- The **Name** or **Fully Qualified Domain Name** is not unique; it already exists in the system
- The entry in any field is not valid (wrong data type or out of the valid range)
- The required **Name** is empty
- The maximum number of destinations (1024) is already defined in the system

Editing a Destination

Use this task to edit a Destination.

1. Click **RBAR > Configuration > Destinations**.
2. Select the Destination you want to edit and click **Edit**.
3. Update the relevant fields.

For more information about each field, see [Destinations configuration elements](#).

The **Name** field is read-only and cannot be edited.

4. Perform one of the following actions:
 - Click **OK** to save the changes and return to the **RBAR > Configuration > Destinations** page.
 - Click **Apply** to save the changes and stay on this page.
 - Click **Cancel** to return to the **RBAR > Configuration > Destinations** page without saving the changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Both the **Realm** and **Fully Qualified Domain Name** are empty; no value was entered
- The **Fully Qualified Domain Name** is not unique; it already exists in the system
- The entry in any field is not valid (wrong data type or out of the valid range)

Deleting a Destination

Use this task to delete a destination. A destination cannot be deleted if it is being used by any Address Range, Individual Address, or Routing Exception. Before this task is performed, delete the association with any Individual Address, Address Range, or Routing Exception.

1. Click **RBAR > Configuration > Destinations**.
2. Select the destination you want to delete and click **Delete**.
3. Click **OK** or **Cancel** on the confirmation screen.

If **OK** is clicked and the destination is in use by an Address Range, Individual Address, or Routing Exception, an error message displays.

Address Tables configuration

The **RBAR > Configuration > Address Tables** page accesses an Address Table and its associated attributes.

From this page, you can:

- Filter the list of address tables to display only the desired application(s).
- View a list of address tables.
- Insert an address table.
- Delete an address table.

Address Tables configuration elements

[Table 4-4](#) describes the fields on the Address Tables insert page.

Table 4-4 Address Tables Configuration Elements

Field	Description	Data Input Notes
*Name	Unique name of the address table. If a duplicate name is entered or the name is not specified, an error message appears.	Format: field Range: 1–32 characters; cannot start with a digit and must contain at least one alpha Default: none
Comment	Information about the address table.	Format: field Range: up to 64 characters

Table 4-4 (Cont.) Address Tables Configuration Elements

Field	Description	Data Input Notes
*Routing Entity Type	Type of routing entity. If the routing entity type is not specified, an error message appears.	Format: list Range: <ul style="list-style-type: none">• IMSI• MSISDN• IMPI• IMPU• IPv4• IPv6 Prefix• UNSIGNED16• External Identifier Default: none
Routing Entity Component	Assists with enhanced address resolution. This field is enabled when External Identifier is selected as the Routing Entity Type .	Format: list Range: <ul style="list-style-type: none">• Domain Identifier• Local Identifier Default: none

Inserting an Address Table

Use this task to add a new Address Table.

1. Click **RBAR > Configuration > Address Table**.
2. Click **Insert**.
3. Enter a unique name for the Address Table in the **Name** field.
For more information about each field, see [Address Table configuration elements](#).
4. If needed, enter a comment or additional information about the Address Table in the **Comment** field.
5. Select the type of routing entity from the **Routing Entity Type** list.
6. If External Identifier was selected as the Routing Entity Type, then select the **Routing Entity Component** from the list.
7. Click **OK, Apply, Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any required field is empty; no value was entered or selected
- The **Name** is not unique; it already exists in the system
- The entry in any field is not valid (wrong data type or out of the valid range)
- The maximum number of Address Tables (40) is already defined in the system

Deleting an Address Table

Use this task to delete an Address Table. An Address Table cannot be deleted if it is being used by any Individual Address, Address Range, or Address Resolution. Before you perform this task, delete the association with any Individual Address, Address Range, or Address Resolution.

1. Click **RBAR > Configuration > Address Table**.
2. Select the Address Table you want to delete and click **Delete**.
3. Click **OK** or **Cancel** on the confirmation screen.

If **OK** is clicked and the Address Table is in use by an Address Range, Individual Address, or Address Resolution, an error message displays.

Address configuration

The **RBAR > Configuration > Addresses** page allows you to access the Routing Entity Address Range, Individual Address, and Domain Address configurable options.

- The Address Range provides the mapping between a single address range and a Destination for routing.
- The Individual Address provides the mapping between an individual address and a Destination for routing.
- The Domain Address provide the mapping between a domain address and a Destination for routing.

Note: If an incoming message maps both an Address Range and an Individual Address, then the Individual Address entry takes priority.

The Address Range and Individual Address entries have their own associated attributes, which are accessed from this **RBAR > Configuration > Addresses** page.

From the **RBAR > Configuration > Addresses** page, you can:

- Filter the list of addresses to display only the desired records. You can filter the list by the following criteria:
 - Address table
 - Address table and Individual address
 - Address table and Domain address
 - Address table and Range (start address, end address)
 - Address table, Individual address, and Range (start address, end address)
 - Destination
 - Destination and Address table
 - Destination, Address table, and Individual address

- Destination, Address table, and Range (start address, end address)
- Destination, Address table, Individual address, and Range (start address, end address)
- View a list of addresses.
- Insert an address.
- Edit an address.
- Delete an address.

Address configuration elements

[Table 4-5](#) describes the fields on the Addresses insert and edit pages. Data input notes apply only to the insert and edit pages.

Table 4-5 Addresses Configuration Elements

Field	Description	Data Input Notes
Table Name	Address table name	none
Address	Address of destination	none
Entry Type	Address type (Individual, Range, or Domain Name)	none
Routing Entity	Routing entity type	none
Individual Address	Specific address	none
Start Address	Starting address of the range	none
End Address	Ending address of the range	none
Destination	Destination of the address	none
Nested Table Name	Address table for a next level search	none

Insert and Edit pages

*Routing Entity Type	Routing Entity Type	Format: list Range: <ul style="list-style-type: none">• IMSI• IMSISDN• IMPI• IMPU• IPv4• IPv6 Prefix• UNSIGNED16• External Identifier
		Default: none

Table 4-5 (Cont.) Addresses Configuration Elements

Field	Description	Data Input Notes
Routing Entity Component	The Routing Entity Component of the address assists with enhanced address resolution. This field is enabled when External Identifier is selected as the Routing Entity Type .	Format: list Range: <ul style="list-style-type: none">• Domain Identifier• Local Identifier Default: none
*Table Name	Address table name	Format: list Range: available user-configured address table names associated to the selected Routing Entity Type Default: none
Address Type	Type of address for the routing entity type	Format: options Range: range or individual address or a domain name Default: range
Start Address	Starting address for an address range This field is required when Range is selected as Address Type . If address is an IPv6-prefix, the prefix length must be entered in the IPv6 Prefix length field.	Format: field Range: end address must be greater than start address. <ul style="list-style-type: none">• Routing Entity Address:<ul style="list-style-type: none">– IMSI: 15 digit string– MSISDN: 3-15 digit string– IMPI: 15 digit string– IMPU: 3-15 digit string– External Identifier: 1-20 digit string for start and end addresses; 1-128 for an individual address• IPv4 address: a 15 character string; quad-dotted format; valid characters are numeric (0-9) and dot (.) ; both compressed and expanded form are supported; for example: 192.168.1.15 or 192.168.001.015• IPv6-Prefix address: Hexadecimal value; up to 39 characters; valid alphanumeric characters (0-9, A-F, a-f) and colon (:); both compressed and expanded form are supported; for example: 1 :: 2 or 0001:0000:0000:0000:0000:0000:0000:0002
End Address	Ending address for an address range This field is required when Range is selected as Address Type . If address is an IPv6-prefix, the prefix length must be entered in the IPv6 Prefix length field.	

Table 4-5 (Cont.) Addresses Configuration Elements

Field	Description	Data Input Notes
Address	<p>Specific address</p> <p>This field is enabled and required when Individual or Domain is selected as the Address Type.</p> <p>If address is an IPv6-prefix, the prefix length must be entered in the IPv6 Prefix length field.</p>	<p>Note: If this IPv6 address portion of the IPv6-prefix address is expressed in binary form (converting hexadecimal digits to bits), then no bit that is set (value=1) can be at an index that is greater than the configured IPv6 Prefix length. For example: 0001:0001:: for prefix length 28 is invalid as the 32nd bit is set.</p> <p>In addition, trailing zeros (0) can be dropped in this IPv6 address portion of the IPv6-prefix address but not the leading zeros (0); for example: 8:: for prefix length 1 is invalid because 8:: is treated as 0008::</p> <ul style="list-style-type: none"> • UNSIGNED16: Hexadecimal value; valid alphanumeric characters (0-9, A-F, a-f); for example: 512, 20, 40, AA, 50A, FFFF <p>Default: none</p>
IPv6 Prefix length	<p>Prefix length of an IPv6-prefix address; specifies how many of the leftmost contiguous bits of the address comprise the prefix.</p> <p>This field is enabled and required when IPv6 Prefix is selected as Routing Entity Type.</p>	<p>Format: field</p> <p>Range: 1-128</p> <p>Default: none</p>
*Destination	Destination of the address	<p>Format: list</p> <p>Range: available user-configured destinations</p> <p>Default: none</p>
Nested Table Name	Address table for a next level search using the Local Identifier of External Identifier AVP	<p>Format: list</p> <p>Range: available Address Table Names of Routing Entity Type External identifier with a sub-type of Local Identifier</p> <p>Default: none</p>

Inserting an Address

Use this task to add a new address or range of addresses to a Routing Entity type.

Before this task is performed, make sure there is at least one Address Table and one Destination configured in the system.

1. Click **RBAR > Configuration > Addresses**.

2. Click **Insert**.

3. Select the **Routing Entity Type** from the list.

For more information about each field, see [Addresses configuration elements](#).

4. If External Identifier was selected as the Routing Entity Type, then select the **Routing Entity Component** from the list.

5. Select the **Address Table** from the list.

6. Select the desired **Address Type** option (Range, Individual Address, or Domain Name).

7. Enter the appropriate address data depending on the selection of the **Address Type**:

- For Range:

- a. Enter the starting address for the range in the **Start Address** field.

- b. Enter the ending address for the range in the **End Address** field.

- For Individual Address or Domain Name, enter the specific address in the **Address** field.

8. If the address entered is an IPv6-prefix, enter the prefix length in the **IPv6 Prefix length** field.

9. Select the **Destination** from the list.

10. (Optional) Select the **Nested Table Name** from the list.

11. Click **OK**, **Apply**, or **Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- **Start Address** is greater than the **End Address**
- **Start Address** and **End Address** for an Address Range are overlapping or already exists
- At least one **Address Table** and one **Destination** have not been configured; they do not exist in the system
- Address already exists for a **Table Name**
- The entry in any field is not valid (wrong data type or out of the valid range)
- Any required field is empty

- The maximum number of records for the Address Type (1,000,000 for each type) is already defined in the system

Editing an Address

Use this task to edit an address associated with a Routing Entity type.

1. Click **RBAR > Configuration > Addresses**.
2. Select the Address you want to edit and click **Edit**.
3. Update the relevant fields.

For more information about each field, see [Addresses configuration elements](#).

The following fields are read-only and cannot be edited:

- **Routing Entity Type**
- **Routing Entity Component**
- **Address Type**

4. Click **OK**, **Apply**, or **Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- **Start Address** is greater than the **End Address**
- **Start Address** and **End Address** for an Address Range are overlapping or already exists
- Address already exists for a **Table Name**
- The entry in any field is not valid (wrong data type or out of the valid range)
- Any required field is empty

Deleting an Address

Use this task to delete an Address.

1. Click **RBAR > Configuration > Addresses**.
2. Select the Address you want to delete and click **Delete**.
3. Click **OK** or **Cancel**.

Address Resolutions configuration

The **RBAR > Configuration > Address Resolutions** page defines the routing relationship between message content and an address by mapping a Diameter Application ID, Command Code, and Routing Entity Type to a user-configured address (a range or individual address). An Address Resolution supports up to three prioritized Routing Entity Types for each Application ID and Command Code (from highest priority to lowest priority – Primary Routing Entity Type, Secondary Routing Entity Type, and Tertiary Routing Entity Type).

From the **RBAR > Configuration > Address Resolutions** page, you can:

- Filter the list of address resolutions to display only the desired records.
- View a list of address resolutions.
- Insert an address resolution.
- Edit an address resolution.
- Delete an address resolution.

Address Resolutions configuration elements

Table 4-6 describes the fields on the Address Resolutions insert and edit pages. Data input notes apply only to the insert and edit pages.

Table 4-6 Address Resolutions Configuration Elements

Field	Description	Data Input Notes
*Application ID	Application ID in a diameter message The application ID is an IANA-assigned diameter application ID, which is a 32-bit field that is mandatory in all diameter messages. It is commonly used for screening and routing messages between diameter nodes. If a combination of the application ID and command code already exists, an error message displays.	Format: list Range: Application IDs configured for RBAR
*Command Code	Command Code in a diameter message If a combination of the application ID and command code already exists, an error message displays.	Format: list Range: Command Codes configured for diameter

Primary Routing Entity/Secondary/Tertiary Routing Entity sections

*Routing Entity	Routing Entity Type The same routing entity type cannot be selected for both the primary and the secondary routing entity; if the same type is selected, an error message displays. If the routing entity type is not specified for the primary routing entity, an error message displays.	Format: list Range: <ul style="list-style-type: none">• IMSI• MSISDN• IMPI• IMPU• IPv4• IPv6 Prefix• UNSIGNED16• External Identifier
------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 4-6 (Cont.) Address Resolutions Configuration Elements

Field	Description	Data Input Notes
*Primary AVP	<p>Primary AVP used for extracting the routing entity address.</p> <p>The same primary AVP and secondary AVP cannot be selected for either the primary routing entity or for the secondary routing entity; if the same AVP is selected, an error message displays.</p> <p>If primary AVP is not selected for the primary routing entity, an error message displays.</p>	<p>Format: list</p> <p>Range:</p> <ul style="list-style-type: none"> • User Identity Routing Entity Type: <ul style="list-style-type: none"> – MSISDN – Public Identity – ServiceInfo.Subscription -Id(0) – ServiceInfo.Subscription -Id(1) – ServiceInfo.Subscription -Id(2) – ServiceInfo.Subscription -Id(3) – ServiceInfo.Subscription -Id(4) – Subscription-Id(0) – Subscription-Id(1) – Subscription-Id(2) – Subscription-Id(3) – Subscription-Id(4) – UserIdentifier.MSISDN – UserIdentifier.UserName – UserIdentity.MSISDN – UserIdentity.Public-Identity – UserName • IPv4 Routing Entity Type: Framed IP Address • IPv6 Prefix Routing Entity Type: Framed IPv6 Prefix • UNSIGNED16 Routing Entity Type: ServiceInfo.PSInfo.3GPP-CC • External Identifier: <ul style="list-style-type: none"> – UserIdentifier.External-Identifier – DeviceAction.External-Identifier <p>Default: none</p>
*Address Table Name	<p>Address table for this routing entity type.</p> <p>If Address table name is not selected for the primary routing entity, an error message displays.</p>	<p>Format: list</p> <p>Range: available configured address table names</p>

Inserting an Address Resolution

Use this task to add a new Address Resolution.

Before this task is performed, make sure there is at least one supported Diameter Application and one Address Table configured in the system.

1. Click **RBAR > Configuration > Address Resolutions**.
2. Click **Insert**.
3. Select an **Application ID** from the list.

Note: The Application IDs presented in this list are those created using **RBAR > Configuration > Applications**.

For more information about each field, see [Address Resolution configuration elements](#).

4. Select the **Command Code** from the list.

Note: The Command Codes presented in this list are those created using **Diameter > Command Codes**.

5. For the Primary Routing Entity section, perform the following:
 - a. Select the **Routing Entity Type** from the list.
 - b. Select the **Primary AVP** from the list.
 - c. If needed, select the **Secondary AVP** from the list.
6. If needed, for the Secondary Routing Entity section, perform the following:
 - a. Select the appropriate Routing Entity type from the **Routing Entity Type** list.
 - b. Select the Primary AVP from the **Primary AVP** list.
 - c. If needed, select the Secondary AVP from the **Secondary AVP** list.

Note: The **Secondary AVP** field is disabled if **IPv4, IPv6 Prefix**, or **UNSIGNED16** is selected as the **Routing Entity Type**.

- d. Select the Address Table name from the **Address Table Name** list.
7. If needed, for the Tertiary Routing Entity section, perform the following:
 - a. Select the appropriate Routing Entity type from the **Routing Entity Type** list.

- b.** Select the Primary AVP from the **Primary AVP** list.
- c.** If needed, select the Secondary AVP from the **Secondary AVP** list.

Note: The **Secondary AVP** field is disabled if **IPv4, IPv6 Prefix**, or **UNSIGNED16** is selected as the **Routing Entity Type**.

- d.** Select the Address Table name from the **Address Table Name** list.
- 8.** Click **OK, Apply, or Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The combination of **Application ID** and **Command Code Value** is not unique; it already exists in the system
- At least one supported Diameter **Application** and one **Address Table** have not been configured; they do not exist in the system
- The entry in any field is not valid (wrong data type or out of the valid range)
- Any required field is empty
- Duplicate Routing Entity Types were selected in the **Primary** and **Secondary** Routing Entity sections
- Duplicate AVPs were selected in the **Primary AVP** and **Secondary AVP** fields
- The maximum number of Address Resolutions (64) is already defined in the system

Editing an Address Resolution

Use this task to edit an Address Resolution.

- 1.** Edit **RBAR > Configuration > Address Resolution**.
- 2.** Select the Address Resolution you want to edit and click **Edit**.
- 3.** Update the relevant fields.

For more information about each field, see [Address Resolution configuration elements](#).

The following fields are read-only and cannot be edited:

- **Application ID**
- **Command Code**
- 4.** Click **OK, Apply, or Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The entry in any field is not valid (wrong data type or out of the valid range)
- Any required field is empty

- Duplicate Routing Entity Types were selected in the **Primary** and **Secondary** Routing Entity sections
- Duplicate AVPs were selected in the **Primary AVP** and **Secondary AVP** fields

Deleting an Address Resolution

Use this task to delete an Address Resolution.

1. Click **RBAR > Configuration > Address Resolutions**.
2. Select the Address Resolution you want to delete and click **Delete**.
3. Click **OK** or **Cancel** on the confirmation screen.

System Options configuration

The **RBAR > Configuration > System Options** page allows you to modify the default system values for RBAR global parameters (for example, FQDN/Realm, or Allow Subsequent RBAR Invocation, or Application Unavailable action).

System Options elements

[Table 4-7](#) describes the fields on the System Options page.

Table 4-7 System Options Elements

Field	Description	Data Input Notes
URI Local Number Enabled	<p>This only applies to the routing entity type IMPU; defines whether local numbers are considered valid addresses within a SIP or TEL URI. An address of this form is considered a local number if it does not start with the global number prefix character plus sign (+).</p> <p>If checked, both local and global numbers are valid addresses for IMPU decoded from diameter requests.</p> <p>If unchecked, only global numbers are valid addresses.</p>	<p>Format: check box Range: checked, unchecked Default: unchecked</p>
ASCII Excluded Digits	<p>List of ASCII characters to ignore while parsing digits from a raw AVP data field of AVP Type UTF8String.</p> <p>If an invalid character is entered, an error message appears.</p>	<p>Format: fields Range: ASCII-printable characters except the percent sign (%)</p>
Exclude Space	<p>Defines whether ASCII character space is ignored while parsing digits from a raw AVP data field of AVP Type UTF8String.</p> <p>If checked, ASCII character space is ignored.</p> <p>If not checked, ASCII character space is not ignored.</p>	<p>Format: check box Range: checked, unchecked Default: unchecked</p>

Table 4-7 (Cont.) System Options Elements

Field	Description	Data Input Notes
TBCD Excluded Digits	Defines whether the associated character is ignored while parsing digits from a raw AVP data field of AVP Type OctetString encoded as a TBCD-string. If checked, character is ignored. If not checked, character is not ignored.	Format: check boxes Range: checked, unchecked for each option: *(0010), #(1011), a(1100), b(1101), c(1110) Default: all unchecked
Allow Subsequent RBAR Invocation	Enables the subsequent invocation of RBAR on a different DSR node in the network. If checked, this setting overrides the Allow Subsequent RBAR Invocation attribute in Destination .	Format: check box Range: checked, unchecked Default: unchecked
Remove Destination-Host	If checked, RBAR deletes any instance of Destination-Host AVPs in the message when performing Realm only resolution.	Format: check box Range: checked, unchecked Default: unchecked
Realm	Value to be placed in the Origin-Realm AVP of the Answer message generated by RBAR. A Realm must be paired with a Fully Qualified Domain Name. If entering a value for Realm, then a value for Fully Qualified Domain Name must also be entered; otherwise, an error message appears. If not configured, the local node Realm for the egress connection is used to populate Origin-Realm AVP.	Format: field Range: A valid Realm or FQDN. A label consists up to 63 characters and a Realm or FQDN up to 255 characters Default: none
Fully Qualified Domain Name	Value to be placed in the Origin-Host AVP of the Answer message generated by RBAR. A Fully Qualified Domain Name must be paired with a Realm. If entering a value for Fully Qualified Domain Name, then a value for Realm must also be entered; otherwise, an error message appears. If not configured, the local node FQDN for the egress connection is used to populate the Origin-Host AVP.	

Table 4-7 (Cont.) System Options Elements

Field	Description	Data Input Notes
Resource Exhaustion Result-Code	Result-Code or Experimental-Result-Code value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted. If Vendor-Id is configured, this result-code value is encoded as Experimental-Result-Code AVP; otherwise the result-code is encoded as Result-Code AVP.	Format: <ul style="list-style-type: none">• field• list Range: <ul style="list-style-type: none">• field: 1000–5999• list of available code values Default: 3004
Resource Exhaustion Error Message	Error-Message AVP value to be returned in an answer message when a message is not successfully routed because of internal resource being exhausted.	Format: Alphanumeric, underscore (_), and period (.) Range: 0–64 characters Default: RBAR Resource Exhausted
Resource Exhaustion Vendor-Id	Vendor-Id AVP value to be returned in an answer message when a message is not successfully routed because of internal resource being exhausted.	Format: field Range: 1–4294967295
Application Unavailable Action	Defines action to be taken when RBAR is not available to process messages If the Default Route option is selected, an entry must be provided for the Application Unavailable Route List.	Format: Options Range: <ul style="list-style-type: none">• Continue Routing• Default Route• Send Answer with Result-Code AVP• Send Answer with Experimental-Result AVP Default: Continue Routing
Application Unavailable Route List	Defines where the requests are routed when RBAR is not available. Peer Routing Rules are bypassed. A route list must be entered if Default Route is selected as the Application Unavailable Action .	Format: list Range: Available route list entries

Table 4-7 (Cont.) System Options Elements

Field	Description	Data Input Notes
Application Unavailable Result-Code	<p>Result-Code or Experimental-Result-Code value returned in an Answer message when a message is not successfully routed because RBAR is not available.</p> <p>If Vendor-Id is configured, this result-code value is encoded as Experimental-Result-Code AVP; otherwise, the result-code is encoded as Result-Code AVP.</p> <p>A code must be entered if either the <i>Send Answer with Result-Code AVP</i> or the <i>Send Answer with Experimental Result-Code AVP</i> option is selected as the Application Unavailable Action.</p>	Format: <ul style="list-style-type: none"> • field • list Range: <ul style="list-style-type: none"> • field: 1000–5999 • list of available Code values Default: 3002
Application Unavailable Error Message	<p>Error-Message AVP value to be returned in an Answer message when a message is not successfully routed because RBAR is not available.</p> <p>A message can be entered, if needed, when either the <i>Send Answer with Result-Code AVP</i> or the <i>Send Answer with Experimental Result-Code AVP</i> option is selected as the Application Unavailable Action.</p>	Format: field Range: 0–64 characters Default: RBAR Unavailable
Application Unavailable Vendor-Id	<p>Vendor-Id AVP value to be returned in an Answer message when a message is not successfully routed because RBAR is not available.</p> <p>A vendor-Id must be entered if the <i>Send Answer with Experimental Result-Code AVP</i> option is selected as the Application Unavailable Action.</p>	Format: field Range: 1–4294967295 Default: none
Allow Longest Sub-Domain Match	This configuration is used for searching domain address. When checked, if an exact match is not found using the Domain Identifier component of the External identifier received in an ingress Diameter message, then RBAR continues the search looking for the longest matching sub-domain.	Format: check box Range: checked, unchecked Default: unchecked

Editing System Options

Use this task to edit System Options.

1. Click RBAR > Configuration > System Options.
2. Update the relevant fields.

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

3. Click **OK**, **Apply**, or **Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Either the **Realm** or **Fully Qualified Domain Name** is empty; no value was entered; these fields must be configured as a pair
- 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)

Post-Configuration Activities

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

- Enabling the RBAR application
- Status Verification

Enabling the RBAR Application

Use this task to enable the RBAR application.

1. From the each active **SOAM**, click **Diameter > Maintenance > Applications**.
2. Under **DSR Application Name**, select each **RBAR** 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**.

Status Verification

Use this task to verify RBAR status after configuration is complete.

1. Verify Communication Agent (ComAgent) Connection status.
 - a. From the active **SOAM**, click **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, click **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**.

Bulk Import and Export

The *Diameter Common User's Guide* describes the use and operation of Bulk Import and Export functions:

- **Help > Diameter Common > Bulk Import**
- **Help > Diameter Common > Bulk Export**

The Bulk Import and Export functions can be used to export Diameter, IPFE, and 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.

Bulk Import

The 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 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 *Diameter Common User's Guide* or the **Diameter Common > Import** Help for valid Import operations.

Import CSV files can be created by using a 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 release used to import the file. Across different release versions, column counts may not be compatible, and the import fails.

Files that are created using the 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; 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.

Multiple 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.

Bulk Export

The Bulk Export operation creates ASCII Comma-Separated Values (CSV) files (.csv) containing Diameter, IPFE, and Application configuration data. Exported configuration data can be edited and used with the 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 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.

Configuration data can be exported in one Export operation:

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

Exported files can be written to the File Management Directory in the local File Management area (**Status & Manage > Files** 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 are not logged.

Maintenance of RBAR

The **Diameter > Maintenance** GUI provides the RBAR specific maintenance functions. In this section describes Admin State, Operational Status, Operational Reason, and Congestion Levels on the **Diameter > Maintenance > Applications** page.

RBAR Maintenance Overview

The RBAR application has no maintenance GUI pages of its own. The following **Diameter > Maintenance** pages provide functions and information that can be used with the RBAR application:

- The **Diameter > Maintenance > Applications** page displays RBAR status information including Admin State, Operational Status, and Operational Reason. The page also provides functions to enable and disable the application. Refer to the *Diameter User's Guide* and Help for explanations of the page and the status information.
- The **Diameter > Maintenance > DA-MPs** page displays status and connectivity information for the DA-MP that is running the RBAR application. Refer to the *Diameter User's Guide* and Help for explanations of the page and the status information.

RBAR Administrative State and Operational Status

The RBAR Administrative State (Admin State) indicates the state the operator wants the RBAR application to be in, and can be manually enabled or disabled. The Operational Status indicates the actual status of the RBAR application. The RBAR Admin State and Operational Status is updated when the application is started or restarted and when RBAR congestion is detected.

Next Generation Network Priority Service (NGN-PS) allows National Security / Emergency Preparedness (NS/EP) users to make priority calls/sessions using public networks. The NGN-PS requests are never discarded due to congestion. NGN-PS messages are always processed by RBAR application except when application is unavailable, in that case configured Exception Action is used for further Routing. For a detailed description of NGN-PS, refer to the *Diameter User's Guide* and Help.

[RBAR Admin State and Operational Status](#) describes the Admin State, Operational Status, Operational Reason, and Congestion Levels on the **Diameter > Maintenance > Applications** page.

Table 5-1 RBAR Admin State and Operational Status

Admin State	Operational Status	Operational Reason	Congestion Level
Disabled	Unavailable	The default shutdown state	Any

Table 5-1 (Cont.) RBAR Admin State and Operational Status

Admin State	Operational Status	Operational Reason	Congestion Level
Enabled	Available	RBAR receives Requests from the DRL normally	Normal/CL1/CL2
	Degraded	The DRL only forwards NGN-PS Requests to RBAR	CL3