Oracle® Communications Diameter Signaling Router

Range Based Address Resolution User Guide

Release 9.1.0.0.0
G16657-01
December 2024

Oracle Communications Diameter Signaling Router Range Based Address Resolution User Guide, Release 9.1.0.0.0

G16657-01

Contents

What's New in This guide

This section introduces the documentation updates for Release 9.1.0.0.0.

Release 9.1.0.0.0, G16657-01, December 2024

There are no updates for this release.

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.

1.1 Revision History

Date	Description
April 2022	Not updated in this release.
December 2021	Not updated in this release.
January 2017	Updates in the RBAR supported AVPs table.
June 2016	Accessibility changes throughout.

1.2 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

1.3 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.

1.4 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.
- 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.

1.5 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.

2
Range Based Address Resolution

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

2.1 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.

2.1.1 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.

2.1.2 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.

2.2 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.

2.3 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 2-1.

Table 2-1 RBAR Supported AVPs

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

Table 2-1 (Cont.) RBAR Supported AVPs

For a User Identity Type (IMSI, MSISDN, IMPI, IMPU) AVPs	Vendor ID and AVP Code	AVP Type	AVP Reference
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
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 2-2 presents all possible combinations of the user identity types and the associated AVPs.

Table 2-2 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

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

User Identity Types/AVPs	IMSI	MSISDN	IMPI	IMPU
Subscription-ID-Data (3-NAI)	Applicable	Applicable	Applicable	Applicable
Service-Information:	Applicable	Applicable	Applicable	Applicable
Subscription-ID-Data (3-NAI)				
Subscription-ID-Data (4-Private)	Applicable	Applicable	Applicable	Applicable
Service -Information:	Applicable	Applicable	Applicable	Applicable
Subscription-ID-Data (4-Private)				
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 2-3.

Table 2-3 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	
SIP URI with MSISDN Format: ASCII Examples: sip: +1-919-460-5500@xyz.com;user=phone sip:311480999995555 @my.network.org		Applicable		Applicable

Table 2-3 (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 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

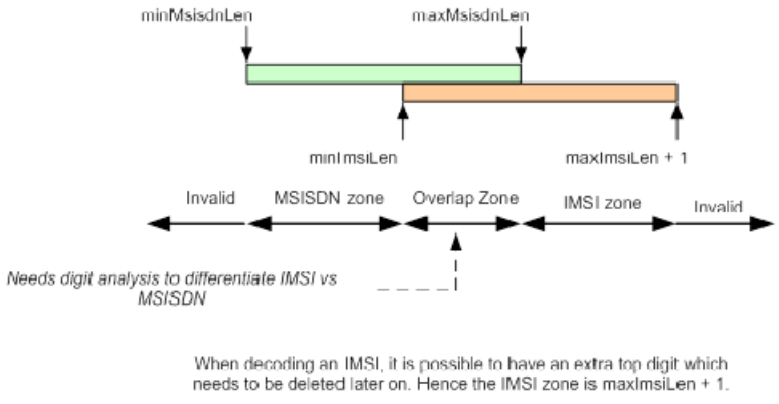
In certain cases, none of these methods allow a clear categorization (for example, if the number of digits needs to be used and the received number of digits are applicable to both IMSIs and MSISDNs, and thus leads to an ambiguous determination; or if there is no plus sign before the digits).

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 2-1, 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**, and then **Network Identifiers**, and then **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 2-1 IMSI/MSISDN Overlap Range Scenario



2.4 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 2-4 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.

2.5 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 2-5.

Table 2-5 RBAR Metadata-Generating Events

Event	Type	Scope	Instance Data	When Recorded
Address Resolution Match found	Address Resolution Match	App Data	• 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).
Routing Entity address resolved to a Destination address for request message routing	Destination Resolution	App Data	• 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	• Routing Exception Type (such as Unknown Command Code) • Routing Exception Action (such as Abandon Request)	After any Routing Exception is encountered.

3
Configuration of RBAR

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

3.1 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

3.1.1 Verifying Server status

Use this task to verify server status before RBAR configuration.

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

3.1.2 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**, and then **MPs**, and then **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**, and then **MPs**, and then **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**, and then **Network Identifiers**, and then **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**, and then **Network Identifiers**, and then **MCC Ranges [Insert]** page to configure **MCCMNC** entries.

3.1.3 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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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).

3.2 RBAR Configuration

The **Configuration** pages under **RBAR** manages 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**.

3.2.1 Applications configuration

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

From the **RBAR**, and then **Configuration**, and then **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.

3.2.1.1 Applications configuration elements

Table 3-1 describes the fields on the Applications insert page.

Table 3-1 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**.

3.2.1.2 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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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

3.2.1.3 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**, and then **Configuration**, and then **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.

3.2.2 Exceptions configuration

The **RBAR**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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.

3.2.2.1 Exceptions configuration elements

Table 3-2 describes the fields on the Exceptions edit page.

Table 3-2 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: • 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: • 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: • field • list Range: • 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
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

3.2.2.2 Editing a Routing Exception

Use this task to edit a Routing Exception.

1. Click **RBAR**, and then **Configuration**, and then **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`.

3.2.3 Destinations configuration

The **RBAR**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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.

3.2.3.1 Destinations configuration elements

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

Table 3-3 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.

Table 3-3 (Cont.) Destinations Configuration Elements

Field	Description	Data Input Notes
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.	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. **Note**: If the **System Options** `Allow Subsequent RBAR Invocation` option is checked, then this attribute is ignored.	Format: check box Range: checked, unchecked Default: checked

3.2.3.2 Inserting a Destination

Use this task to add a new Destination.

1. Click **RBAR**, and then **Configuration**, and then **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

3.2.3.3 Editing a Destination

Use this task to edit a Destination.

1. Click **RBAR**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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)

3.2.3.4 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**, and then **Configuration**, and then **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.

3.2.4 Address Tables configuration

The **RBAR**, and then **Configuration**, and then **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.

3.2.4.1 Address Tables configuration elements

Table 3-4 describes the fields on the Address Tables insert page.

Table 3-4 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
*Routing Entity Type	Type of routing entity. If the routing entity type is not specified, an error message appears.	Format: list Range: • 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: • Domain Identifier • Local Identifier Default: none

3.2.4.2 Inserting an Address Table

Use this task to add a new Address Table.

1. Click **RBAR**, and then **Configuration**, and then **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

3.2.4.3 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**, and then **Configuration**, and then **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.

3.2.5 Address configuration

The **RBAR**, and then **Configuration**, and then **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**, and then **Configuration**, and then **Addresses** page.

From the **RBAR**, and then **Configuration**, and then **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.

3.2.5.1 Address configuration elements

Table 3-5 describes the fields on the Addresses insert and edit pages. Data input notes apply only to the insert and edit pages.

Table 3-5 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: • IMSI • IMSISDN • IMPI • IMPU • IPv4 • IPv6 Prefix • UNSIGNED16 • External Identifier Default: none
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: • Domain Identifier • Local Identifier Default: none

Table 3-5 (Cont.) Addresses Configuration Elements

Field	Description	Data Input Notes
*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. • Routing Entity Address: – 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` 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. **Note**: 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::`
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 3-5 (Cont.) Addresses Configuration Elements

Field	Description	Data Input Notes
Address	Specific address This field is enabled and required when Individual or Domain is selected as the **Address Type**. If address is an IPv6-prefix, the prefix length must be entered in the **IPv6 Prefix length** field.	• UNSIGNED16: Hexadecimal value; valid alphanumeric characters (0-9, A-F, a-f); for example: `512`, `20`, `40`, `AA`, `50A`, `FFFF` Default: none
IPv6 Prefix length	Prefix length of an IPv6-prefix address; specifies how many of the leftmost contiguous bits of the address comprise the prefix. This field is enabled and required when `IPv6 Prefix` is selected as **Routing Entity Type**.	Format: field Range: 1–128 Default: none
*Destination	Destination of the address	Format: list Range: available user-configured destinations Default: none
Nested Table Name	Address table for a next level search using the Local Identifier of External Identifier AVP	Format: list Range: available Address Table Names of Routing Entity Type External identifier with a sub-type of Local Identifier Default: none

3.2.5.2 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**, and then **Configuration**, and then **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

3.2.5.3 Editing an Address

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

1. Click **RBAR**, and then **Configuration**, and then **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

3.2.5.4 Deleting an Address

Use this task to delete an Address.

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

3.2.6 Address Resolutions configuration

The **RBAR**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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.

3.2.6.1 Address Resolutions configuration elements

Table 3-6 describes the fields on the Address Resolutions insert and edit pages. Data input notes apply only to the insert and edit pages.

Table 3-6 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	

Table 3-6 (Cont.) Address Resolutions Configuration Elements

Field	Description	Data Input Notes
***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: • IMSI • MSISDN • IMPI • IMPU • IPv4 • IPv6 Prefix • UNSIGNED16 • External Identifier
***Primary AVP**	Primary AVP used for extracting the routing entity address. 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. If primary AVP is not selected for the primary routing entity, an error message displays.	Format: list Range: • User Identity Routing Entity Type: – 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) – UserIdentitifer.MSISDN – UserIdentitifer.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: – UserIdentifier.External-Identifier – DeviceAction.External-Identifier Default: none
Secondary AVP	Secondary AVP used for extracting the routing entity address. 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. The Secondary AVP field is available for User Identity routing types only; this field is disabled if `IPV4`, `IPV6 Prefix`, and `UNSIGNED16` are selected as the routing entity type.	

Table 3-6 (Cont.) Address Resolutions Configuration Elements

Field	Description	Data Input Notes
***Address Table Name**	Address table for this routing entity type. If Address table name is not selected for the primary routing entity, an error message displays.	Format: list Range: available configured address table names

3.2.6.2 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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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**, and then **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.

> **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.
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

3.2.6.3 Editing an Address Resolution

Use this task to edit an Address Resolution.

1. Edit **RBAR**, and then **Configuration**, and then **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

3.2.6.4 Deleting an Address Resolution

Use this task to delete an Address Resolution.

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

3.2.7 System Options configuration

The **RBAR**, and then **Configuration**, and then **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).

3.2.7.1 System Options elements

Table 3-7 describes the fields on the System Options page.

Table 3-7 System Options Elements

Field	Description	Data Input Notes
URI Local Number Enabled	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 (+). If checked, both local and global numbers are valid addresses for IMPU decoded from diameter requests. If unchecked, only global numbers are valid addresses.	Format: check box Range: checked, unchecked Default: unchecked
ASCII Excluded Digits	List of ASCII characters to ignore while parsing digits from a raw AVP data field of AVP Type UTF8String. If an invalid character is entered, an error message appears.	Format: fields Range: ASCII-printable characters except the percent sign (%)

Table 3-7 (Cont.) System Options Elements

Field	Description	Data Input Notes
Exclude Space	Defines whether ASCII character space is ignored while parsing digits from a raw AVP data field of AVP Type UTF8String. If checked, ASCII character space is ignored. If not checked, ASCII character space is not ignored.	Format: check box Range: checked, unchecked Default: unchecked
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.	
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: • field • list Range: • field: 1000–5999 • list of available code values Default: 3004

Table 3-7 (Cont.) System Options Elements

Field	Description	Data Input Notes
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: • 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
Application Unavailable Result-Code	Result-Code or Experimental-Result-Code value returned in an Answer message when a message is not successfully routed because RBAR is not available. 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. A code must be entered if either the `Send Answer with Result-Code AVP` or the `Send Answer with Experimental Result-Code AVP` option is selected as the **Application Unavailable Action**.	Format: • field • list Range: • field: 1000–5999 • list of available Code values Default: 3002
Application Unavailable Error Message	Error-Message AVP value to be returned in an Answer message when a message is not successfully routed because RBAR is not available. A message can be entered, if needed, when either the `Send Answer with Result-Code AVP` or the `Send Answer with Experimental Result-Code AVP` option is selected as the **Application Unavailable Action**.	Format: field Range: 0–64 characters Default: RBAR Unavailable

Table 3-7 (Cont.) System Options Elements

Field	Description	Data Input Notes
Application Unavailable Vendor-Id	Vendor-Id AVP value to be returned in an Answer message when a message is not successfully routed because RBAR is not available. A vendor-Id must be entered if the `Send Answer with Experimental Result-Code AVP` option is selected as the **Application Unavailable Action**.	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

3.2.7.2 Editing System Options

Use this task to edit System Options.

1. Click **RBAR**, and then **Configuration**, and then **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)

3.3 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

3.3.1 Enabling the RBAR Application

Use this task to enable the RBAR application.

1. From the each active **SOAM**, click **Diameter**, and then **Maintenance**, and then **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**.

3.3.2 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**, and then **Maintenance**, and then **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**, and then **Server**.
   b. Verify that for each server, the **Appl State** field is **Enabled**, and the **DB**, **Reporting Status**, and **Proc** fields are **Norm**.

3.3.3 Bulk Import and Export

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

- **Help**, and then **Diameter Common**, and then **Bulk Import**
- **Help**, and then **Diameter Common**, and then **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**, and then **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**, and then **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**, and then **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.

4
Maintenance of RBAR

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

4.1 RBAR Maintenance Overview

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

- The **Diameter**, and then **Maintenance**, and then **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**, and then **Maintenance**, and then **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.

4.2 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**, and then **Maintenance**, and then **Applications** page.

Table 4-1 RBAR Admin State and Operational Status

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