Oracle® Communications Diameter Signaling Router

DSR Administration Guide

E57494 Revision 01

March 2015

Oracle® Communications DSR Administration Guide

Table of Contents

List of Figures

List of Tables

Part I

Introduction

Topics:

The chapter in this Part describes the purpose and contents of the DSR *Administration Guide* and Help.

Chapter 1

About the DSR Administration Guide

Topics:

This *DSR Administration Guide* and the DSR Administration Help describe the DSR functions, architecture, and configuration; and provide references to more detailed information. The Guide and Help are updated with each major release of the DSR software.

Introduction

This document provides administrative information for the DSR, including:

- High-level functional descriptions of the DSR and its components
- Overview of the configuration of the DSR, the Diameter protocol, DSR Applications, and IP Front End (IPFE)
- Overviews of maintenance, status, and report functions of the DSR, the Diameter protocol, and DSR Applications
- Overviews and descriptions of DSR tools and utilities:
    - Imports and Exports
    - IPsec for secure connections
    - Integrated Diameter Intelligence Hub (IDIH)
    - Database backups and restores

The sections of this Guide include references to other documents that provide more detailed information and task procedures.

This chapter includes information about the document scope, audience, and organization; how to contact Technical Support for assistance; and how to find related publications.

Scope and Audience

The *DSR Administration Guide* and DSR Administration Help are intended for anyone responsible for configuring and using the Diameter Signaling Router (DSR) and the DSR Applications that use it. Users of this guide must have a working knowledge of telecommunications and network installations.

Manual Organization

This manual is organized into the following chapters:

- *Introduction* contains general information in the user's guide and the descriptions of the GUI widgets and buttons.
    - *About the DSR Administration Guide* contains general information about this guide, the organization of this guide, descriptions of and how to locate Related Publications, 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.
- *Diameter Signaling Router (DSR)* describes the components and functions of the Diameter Signaling Router, the Diameter protocol, Diameter Mediation, DSR Applications, and IP Front End (IPFE):

  - *Diameter Signaling Router (DSR)* describes the DSR topology, architecture, components, and functions
  - *Diameter Protocol* describes the functions of the Diameter base protocol in the DSR.
  - *Diameter Mediation* describes Diameter Mediation functions.
  - *DSR Applications* describes the DSR Applications that are supported by the DSR.
  - *IP Front End (IPFE)* describes IPFE functions.

- *DSR Configuration* describes configuration of IPFE, the Diameter protocol, Diameter Mediation, and DSR Applications:

  - *DSR Configuration Overview* provides an overview of DSR configuration and GUI structure.
  - *IPFE Configuration* describes IPFE configuration.
  - *Diameter Configuration* describes configuration of Diameter protocol components.
  - *DSR Applications Configuration* describes configuration of the FABR, RBAR, CPA, Policy and Charging, MAP-Diameter IWF and GLA DSR Applications.

- *Maintenance, Status, and Reports* describes DSR Maintenance, Status, and Reports features and functions:

  - *Diameter Maintenance* describes Diameter Maintenance functions.
  - *Diameter Reports* describes the Diagnostics Tool and report, and the MP Statistics (SCTP) report.

- *Tools and Utilities* describes the following DSR tools and utilities:

  - *Imports and Exports* describes Import and Export functions for Diameter configuration data and for Diameter Mediation Rule Templates.
  - *IPsec* describes the configuration, functions, and use of IPsec for secure connections.
  - *Integrated Diameter Intelligence Hub* provides a brief description of the use of the Diameter Intelligence Hub (DIH) with the DSR.
  - *Database Backups and Restores* describes DSR-related database backup and restore functions.

Documentation Admonishments

Admonishments are icons and text that may appear in this and other manuals. Admonishments alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

The following admonishments, listed in descending order of priority, are used in Tekelec manuals.

TOPPLE

Topple: This icon and text indicate the possibility of equipment damage and personal injury from toppling.

DANGER

Danger: This icon and text indicate the possibility of *personal injury*.

WARNING **Warning:** This icon and text indicate the possibility of *equipment damage*.

CAUTION **Caution:** This icon and text indicate the possibility of *service interruption*.

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See *Locate Product Documentation on the Oracle Technology Network Site* for more information.

Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Select the **Applications** tile.
   The **Applications Documentation** page appears.
3. Select **Apps A-Z**.
4. After the page refreshes, select the **Communications** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **View** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **PDF** link and select **Save Target As**.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

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 will be 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.

Chapter 2

User Interface Introduction

Topics:

This section 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.

User Interface Organization

The user interface is the central point of user interaction with 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.

DSR GUI

In a DSR, the following Main Menu options are accessible from the System OAM (SOAM) server:

- Transport Manager
- Communication Agent
- SS7/Sigtran
- Diameter Common
- Diameter
- RBAR
- FABR
- Policy and Charging
- IPFE
- MAP-Diameter IWF
- CPA

The following Main Menu options are accessible from the Network OAM (NOAM) server:

- Communication Agent
- Diameter Common > Network Identifiers > MCCMNC, MCCMNC Mapping
- Diameter > Configuration for Topology Hiding,
- Network-wide Policy and Charging > Configuration components are configurable on the NOAM; some Configuration components are view-only on the SOAM. Policy and Charging > Maintenance components are accessible on the NOAM only.
- MAP-Diameter IWF

Bulk Import and Bulk Export functions appear on both OAMs, to be used for the data that can be configured on that OAM.

Most other Main Menu options are configurable from the Network OAM server and view-only from the System OAM server.

User Interface Elements

Table 1: User interface elements describes elements of the user interface.

Table 1: User interface elements

Element	Location	Function
Identification Banner	Top bar across the web page	Displays the company name, product name and version, and the alarm panel.

Element	Location	Function
Session Banner	Next bar across the top of the web page	The left side of the banner just above the Main Menu provides the following session information: • 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. The right side of the banner: • 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	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates that a menu item contains subfolders. • 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.
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • **Page Title Area**: Occupies the top of the work area. It displays the title of the current page being displayed, the date and time, and includes a link to context-sensitive help. • **Page Control Area**: Is located below the Page Title Area, and is used to show controls for the Page Area (this area is optional). When available for 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

Element	Location	Function
		provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Splash Page Welcome Message*.

Main Menu Options

Table 2: Main Menu Options describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options would not appear on the screen of a user who does not have administrative privileges.

Note: Some menu items are configurable only on the NOAM and view-only on the SOAM; and some menu options are configurable only on the SOAM. See *DSR GUI*.

Note: Some features will not appear in the main menu until the features are activated.

Table 2: Main Menu Options

Menu Item	Function
Administration	The Administration menu allows the user to: • 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 • Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Manage licenses and upgrades • Authenticate LDAP servers • Configure SNMP trapping services • Validate and transfer ISO files • Prepare, initiate, monitor, and complete upgrades • View the software versions report • Configure an export server • Configure DNS elements
Configuration	On the NOAM, allows the user to configure: • Network Elements • Network Devices • Network Routes

Menu Item	Function
	• Services • Servers • Server Groups • Resource Domains • Places • Place Associations On the SOAM, allows the user to configure the NOAM list plus Interface and Port DSCP.
Alarms and Events	Allows the user to view: • Active alarms and events • Alarm and event history • Trap log
Security Log	Allows the user to view, export, and generate reports from security log history.
Status & Manage	Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, and data file management.
Measurements	Allows the user to view and export measurement data.
Transport Manager	Allows the user to configure adjacent nodes, configuration sets, or transports; and edit transports.
Communication Agent	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.
SS7/Sigtran (optional)	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.
Diameter Common	Allows the user to configure: • Network Identifiers: on the NOAM - MCC Ranges • Network Identifiers on the SOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile assignments The DSR Bulk Import and Export functions are available on both OAMs for the data that is configured on that OAM.
Diameter	Allows the user to configure, modify, and monitor Diameter routing: • On the NOAM, Diameter Topology Hiding configuration

Menu Item	Function
	• On the SOAM, Diameter Configuration, AVP Dictionary and Troubleshooting for IDIH configuration; Diameter Mediation configuration: and Maintenance functions
RBAR (Range-Based Address Resolution) (optional)	Allows the user to configure the following Range-Based Address Resolution (RBAR) settings: • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options This is accessible from the SOAM only.
FABR (Full Address Based Resolution) (optional)	Allows the user to configure the following Full Address Based Resolution (FABR) settings: • Applications • Exceptions • Default Destinations • Address Resolutions • System Options This is accessible from the SOAM only.
Policy and Charging (optional)	On the NOAM, allows the user to perform configuration tasks, edit options, and view elements for: • General Options • Access Point Names • Policy DRA • PCRF Pools • PCRF Sub-Pool Selection Rules • Network-Wide Options • Online Charging DRA • OCS Session State • Realms • Network-Wide Options • Alarm Settings • Congestion Options On the NOAM, allows the user to perform maintenance tasks, edit options, and view elements for: • Maintenance • SBR Status

Menu Item	Function
	• Policy Database Query On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • General Options • Access Point Names • Policy DRA • PCRFs • Binding Key Priority • PCRF Pools • PCRF Pool to PRT Mapping • PCRF Sub-Pool Selections • Policy Clients • Site Options • Online Charging DRA • OCSs • CTFs • OCS Session State • Realms • Error Codes • Alarm Settings • Congestion Options
Gateway Location Application (Optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • Exceptions • Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP).
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only.
MAP-Diameter Interworking	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application: • DM-IWF Options • Diameter Exception On the NOAM, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application: • MD-IWF Options • Diameter Realm

Menu Item	Function
	• Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping
CPA (Charging Proxy Application) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • System Options • Message Copy • Session Binding Repository • SBR Subresource Mapping This is accessible from the SOAM only.
Help	Launches the Help system for the user interface.
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 will not appear 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.

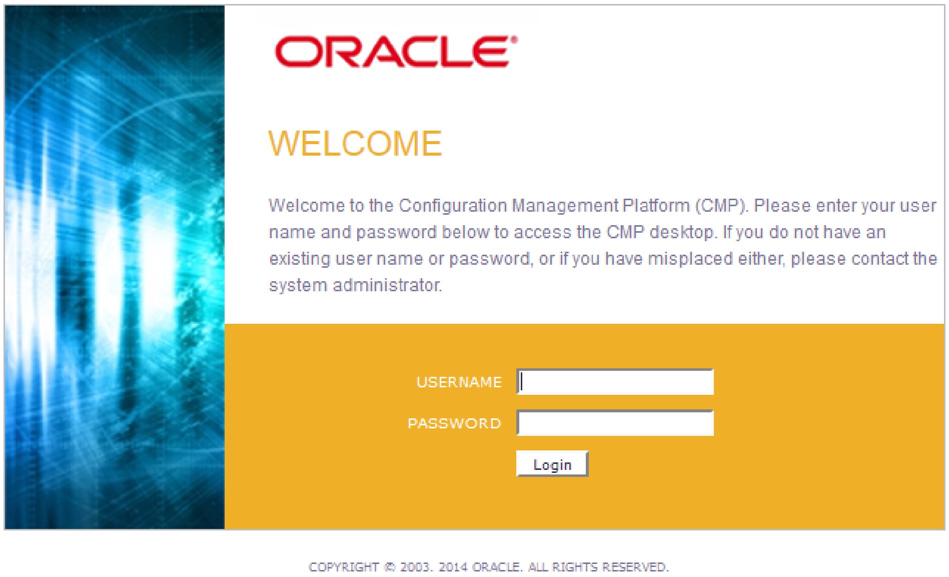
System Login Page

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 a password upon login. The System Login page also features a current date and time stamp and a customizable login message.

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.

Customizing the Login Message

Prior to logging in, the **System Login** page appears. You can create a login message that will appear just below the **Log In** button on the **System Login** page.



WELCOME

Welcome to the Configuration Management Platform (CMP). Please enter your user name and password below to access the CMP desktop. If you do not have an existing user name or password, or if you have misplaced either, please contact the system administrator.

COPYRIGHT © 2003, 2014 ORACLE. ALL RIGHTS RESERVED.

Figure 1: Oracle System Login

1. From the **Main Menu**, select **Administration > General Options**.

   The **General Options Administration** page appears.

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 appears at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log in to the user interface, the login message text is displayed.

Accessing the DSR Graphical User Interface

In a DSR, some configuration is done at the NOAM server, while some is done at the SOAM server. Because of this, you will 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 then 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 appears.
3. Enter the Username and Password for your account.
   The DSR GUI for the NOAM appears.
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 appears.

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 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 (-) will collapse the folder.
📝	Config File	Contains operations in an Options page.
🔍	File with Magnifying Glass	Contains operations in a Status View page.

Icon	Name	Description
📄	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.
?	Help	Launches the Online Help.
Zz	Logout	Logs the user out of the user interface.

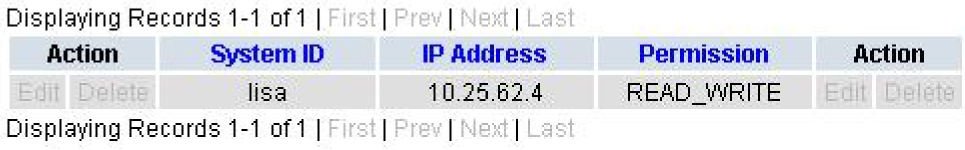
Work Area Displays

In the user interface, you will see a variety of page formats. Tables, forms, tabbed pages, and reports are the most common formats in the user interface.

Note: Screenshots 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*.



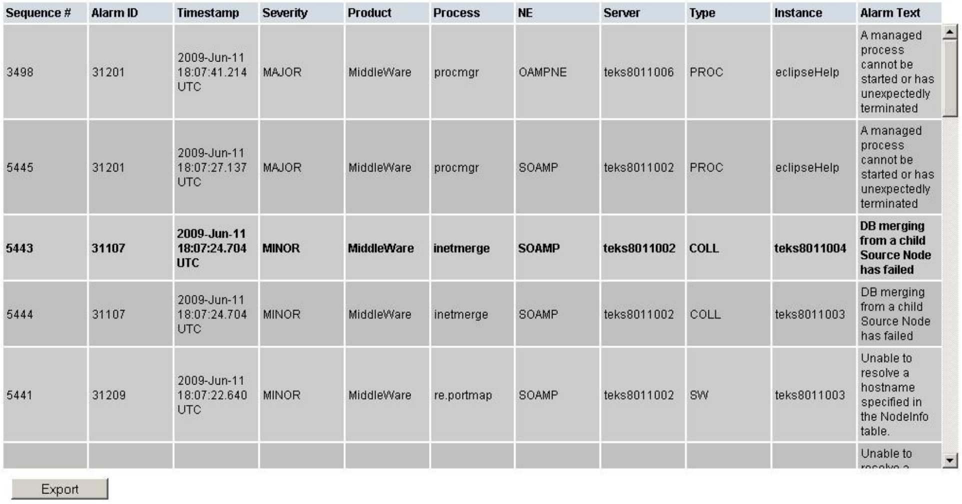
Displaying Records 1-1 of 1 | First | Prev | Next | Last

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

Figure 2: Paginated table

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*.



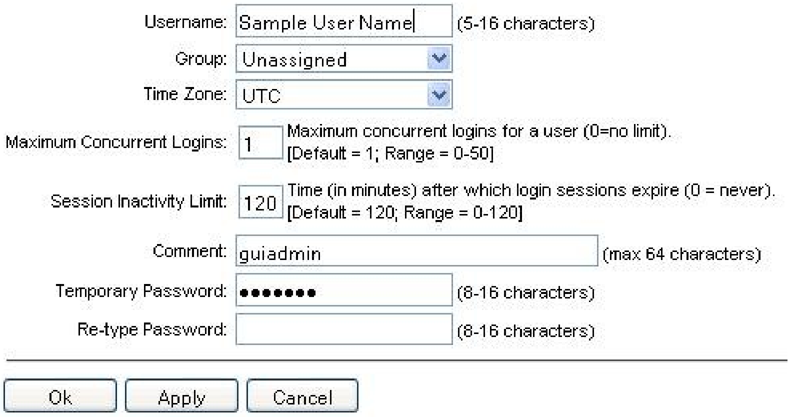
Sequence #	Alarm ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance	Alarm Text
3498	31201	2009-Jun-11 18:07:41.214 UTC	MAJOR	MiddleWare	procmgr	OAMPNE	teks8011006	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5445	31201	2009-Jun-11 18:07:27.137 UTC	MAJOR	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	re.portmap	SOAMP	teks8011002	SW	teks8011003	Unable to resolve a hostname specified in the NodeInfo table.
										Unable to

Figure 3: Scrollable table

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 pulldown lists, buttons and links.

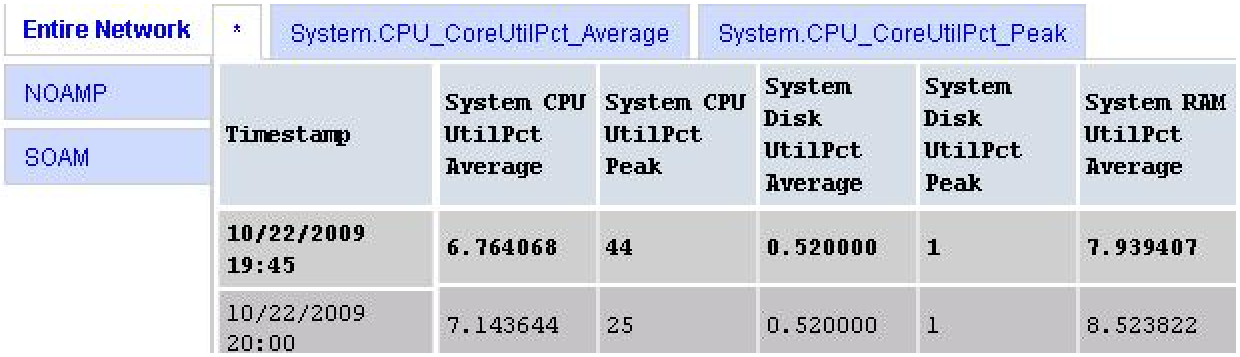


Username:	Sample User Name	(5-16 characters)
Group:	Unassigned	
Time Zone:	UTC	
Maximum Concurrent Logins:	1	Maximum concurrent logins for a user (0=no limit). [Default = 1; Range = 0-50]
Session Inactivity Limit:	120	Time (in minutes) after which login sessions expire (0 = never). [Default = 120; Range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

Figure 4: Form page

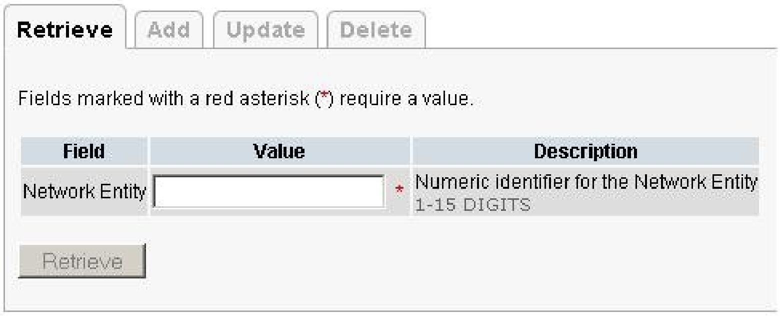
Tabbed pages

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 will populate on the page. Retrieve is always the default for tabbed pages.



Timestamp	System CPU UtilPct Average	System CPU UtilPct Peak	System Disk UtilPct Average	System Disk UtilPct Peak	System RAM UtilPct Average
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 5: Tabbed pages



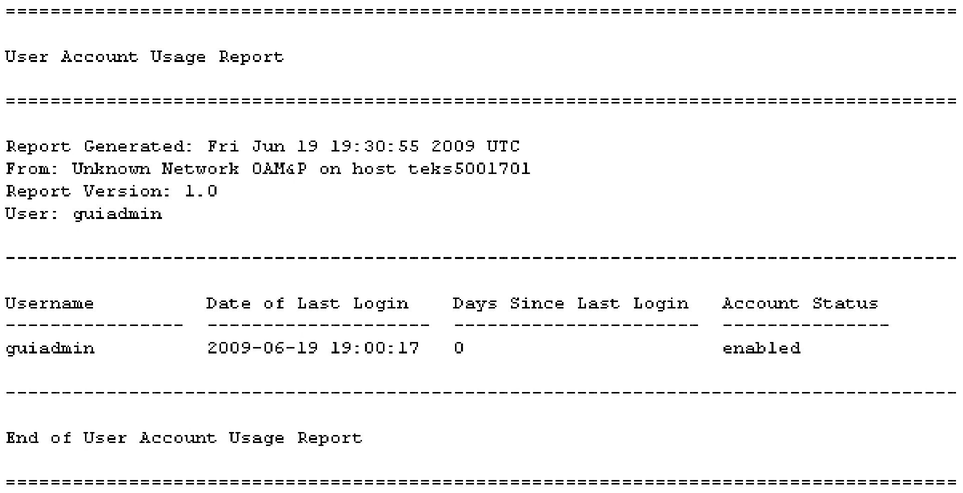
Fields marked with a red asterisk (*) require a value.

Field	Value	Description
Network Entity	*	Numeric identifier for the Network Entity 1-15 DIGITS

Figure 6: Tabbed pages

Reports

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



```
=================================================================================

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: guiadmin

---------------------------------------------------------------------------------

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

---------------------------------------------------------------------------------

End of User Account Usage Report

=================================================================================
```

Figure 7: Report output

Customizing the Splash Page Welcome Message

When you first log in to the user interface, the **User Interface** splash page appears. You can display a customized welcome message on the **User Interface** splash page. Use this procedure to customize the message.

1. From the **Main Menu**, select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Locate **WelcomeMessage** in the **Variable** column.
3. Enter the welcome message text in the **Value** column.
4. Click **Update OK** or **Apply** to submit the information.

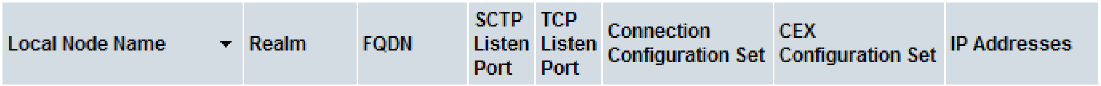
   A status message appears at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log in to the user interface, the welcome message text is displayed.

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 that the table can be sorted by, an indicator appears in the column header showing the direction of the sort. See *Figure 8: Sorting a Table by Column Header*. Clicking the column header again reverses the direction of the sort.



Local Node Name ▼	Realm	FQDN	SCTP Listen Port	TCP Listen Port	Connection Configuration Set	CEX Configuration Set	IP Addresses

Figure 8: Sorting a Table by Column Header

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 4: Example Action buttons contains examples of Action buttons.

Table 4: Example Action buttons

Action button	Function
Insert	Insert data into a table
Edit	Edit data within a table
Delete	Delete data from table
Change	Change the status of a managed object

Some Action buttons take you to another page.

Submit buttons, described in *Table 5: Submit buttons*, 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 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 is a widget that allows you to clear the value from a pulldown list. The clear field control is available only on some pulldown fields.

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

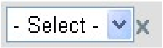


Figure 9: Clear Field Control X

Optional Layout Element Toolbar

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

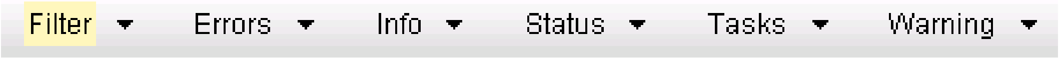


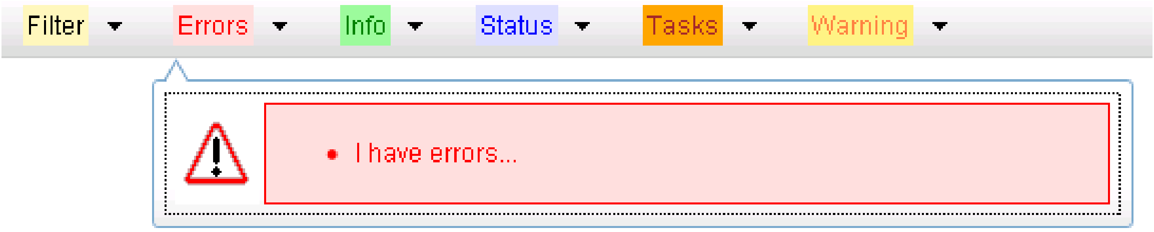
Figure 10: Optional Layout Element Toolbar

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



- I have errors...

Figure 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:

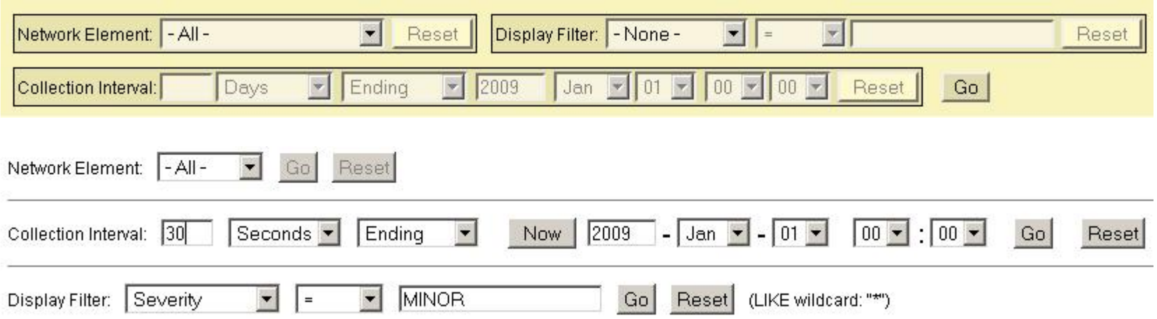
- Network Element - When enabled, the Network Element filter limits the data viewed to a single Network Element.

  Note: Once enabled, the Network Element filter will 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.



Network Element: - All -

Display Filter: - None - =

Collection Interval: Days Ending 2009 Jan 01 00 00

Network Element: - All -

Collection Interval: 30 Seconds Ending 2009 - Jan - 01 00 : 00

Display Filter: Severity = MINOR

Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 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.
>=	Displays all records with a parameter value that is greater than or equal to the specified value.

Operator	Description
<	Displays all records with a parameter value that is less than the specified value.
<=	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 will be 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.
   The filter tool appears.
2. Select a Network Element from the **Network Element** pulldown menu.
3. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

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.
   The filter tool appears.
2. Enter a duration for the **Collection Interval** filter.

   The duration must be a numeric value.
3. Select a unit of time from the pulldown menu.

   The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the pulldown menu.
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 that you have a data table displayed on your screen. This process is the same for all data tables. However, all filtering operations are not available for all tables.

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

The filter tool appears.

2. Select a field name from the **Display Filter** pulldown menu.

   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.

   The selected field name displays in the **Display Filter** field.

3. Select an operator from the operation selector pulldown menu.

   The selected operator appears in the field.

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. For data tables that support compound filtering, click the **Add** button to add another filter condition. Then repeat steps 2 through 4.
   Multiple filter conditions are joined by an AND operator.
6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

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**, select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Change the value of the **MaxRecordsPerPage** variable.

   Note: MaxRecordsPerPage 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.

Part II

Diameter Signaling Router (DSR)

Topics:

The Diameter Signaling Router (DSR) creates a Diameter signaling core that relieves LTE and IMS endpoints of routing, traffic management, and load balancing tasks.

The resulting architecture enables incremental growth of IP networks to support growing traffic and service demands.

Chapter 1

Diameter Signaling Router (DSR)

Topics:

A Diameter Signaling Router (DSR) is a signaling Network Element (NE) composed of OAM servers and Message Processors, and can include the Diameter Intelligence Hub.

The DSR can be deployed either as a core router that routes traffic between Diameter elements in the home network, or as a gateway router that routes traffic between Diameter elements in the visited network and the home network.

The DSR serves primarily as a Diameter Relay Agent to route Diameter traffic based on configured routing data.

Diameter Signaling Router Overview

A DSR is a signaling Network Element (NE) composed of OAM servers and Message Processors, and can include the Diameter Intelligence Hub.

The DSR can be deployed either as a core router that routes traffic between Diameter elements in the home network, or as a gateway router that routes traffic between Diameter elements in the visited network and the home network. The DSR serves primarily as a Diameter Relay Agent to route Diameter traffic based on configured routing data.

DSR Network Elements (NEs) are deployed in geographically diverse mated pairs with each NE servicing signaling traffic to and from a collection of Diameter clients, servers, and agents. One DSR Diameter Agent Message Processor (DA-MP) provides the Diameter message handling function and each DA-MP supports connections to all Diameter Peers (defined as an element to which the DSR has a direct transport connection).

Configuring the DSR requires:

- Network configuration, including servers, server groups, and message processors.
- Diameter protocol configuration, including configuration for routing functions and configuration for transport connection management
- Configuration of activated DSR Applications

In the DSR topology, the OAM server function is split into Network OAM (NOAM) servers and System OAM (SOAM) servers. A DSR with a pair of NOAM servers is connected to multiple DSRs in the network. A single NOAM will support up to 32 signaling servers. Each DA-MP resides with a pair of SOAM servers that interact directly with the respective DA-MPs on that DSR.

The architecture includes the following characteristics:

- Each DSR service signals traffic to and from a collection of Diameter clients, servers, and agents.
- Each DSR supports :
  - OAM servers (OAM), operating in Active/Standby mode; NOAM and SOAM servers.
  - Two message processors (DA-MPs), operating in Active/Standby or Active/Active mode.
- The DSR MPs provide the Diameter message handling function. Each DSR MP supports connections to all of the DSR Peers.
- DSRs are deployed in mated pairs for purposes of geo-redundancy.
- The Integrated Diameter Intelligence Hub (IDIH) provides the ability to filter, access, and troubleshoot Diameter transactions,

DSR Topology

In DSR topology, as shown in *Figure 13: DSR Topology*, there are NOAM servers, SOAM servers, and MP servers.

The DSR topology GUI screen is used to configure and manage:

- On a DSR NOAM, network topology data (such as user accounts, network elements, servers, and server groups). Network-wide Policy and Charging(PCA) data, MAP-Diameter Interworking data for MD-IWF and Diameter Topology Hiding data are configured on NOAM GUI pages. Diameter Common provides the Import and Export GUIs on the NOAM for exporting and importing the SOAM configuration data for Diameter Configuration, IPFE, and DSR Applications.

- On a DSR SOAM, Diameter signaling data (such as Local Nodes, Peer Nodes, Peer Node Groups, Connections, Route Groups, and Route Lists), Diameter MAP Interworking data for DM-IWF, DSR Application data (RBAR, FABR, CPA, Policy and Charging (PCA), and GLA), Profile Assignments and IPFE configuration data. Diameter Common provides the Import and Export GUIs on the SOAM for exporting and importing the SOAM configuration data for Diameter Configuration, IPFE, and DSR Applications.

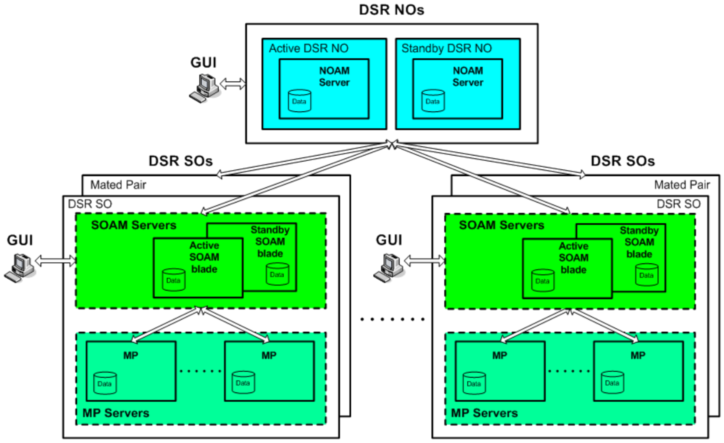


Figure 13: DSR Topology

The DA-MP servers process the database updates from NOAM servers and SOAM servers and perform the real-time signaling. The DA-MP servers also supply the Platform Measurements, Events, Alarms and Logs (MEAL) data, Diameter signaling MEAL data, and DSR Application MEAL data to SOAM servers. The SOAM servers retain the Diameter signaling MEAL data and DSR Application MEAL data, and merge the Platform MEAL data to the NOAM servers.

Deployment with SDS

DSR deployments that include support for the DSR Full Address Based Resolution (FABR) application must be deployed with the Subscriber Database Server (SDS). The SDS is used to provision the FABR subscriber data.

The SDS/DP system consists of a Primary Provisioning Site, a Disaster Recovery (DR) Provisioning Site, and up to 32 DSR Signaling Site servers with redundant DP SOAM servers. Each Provisioning Site has an Active/Standby pair of servers in a high availability (HA) configuration and a third server configured as a Query Server.

In DSR topology, the DSR SOAM and the SDS SOAMP servers are run on the DSR OAM blade using virtualization technology. It is assumed that most deployments that support both DSR and SDS will deploy the DSR NOAMP on Rack Mount Servers, as this is how the SDS NOAMP is deployed. Small deployments that minimize the amount of hardware investment require the DSR NOAMP to be deployed as a virtual server on the OAM blade. This requires running three Virtual Machines (VMs) on the blade – DSR NOAM, DSR SOAM and SDS SOAMP.

OAM Servers

A pair of Operation, Administration, and Maintenance (OAM) servers make up one OAM component of the DSR. This pair of servers has an Active/Standby relationship. The Active server in the pair controls the virtual IP addresses (VIP) that direct XMI and IMI traffic to the Active server.

The role of the OAM server is to provide a central operational interface and all OAM&P functions (for example, user administration, provisioning and configuration data, database administration, fault management and upgrade functions) for the DSR under its control. The OAM server replicates configuration and provisioning data to and collects all measurements, events, alarms, and log data from all Message Processors within the DSR.

The OAM servers provide the following services:

- A central operational interface
- Distribution of provisioned data to all MPs of the NE
- Event collection and administration from all MPs
- User and access administration
- Support for a northbound SNMP interface toward an external EMS/NMS; up to 5 SNMP destinations can be configured
- A web-based GUI for configuration tasks

Figure 14: DSR OAM Architecture illustrates the DSR OAM architecture.

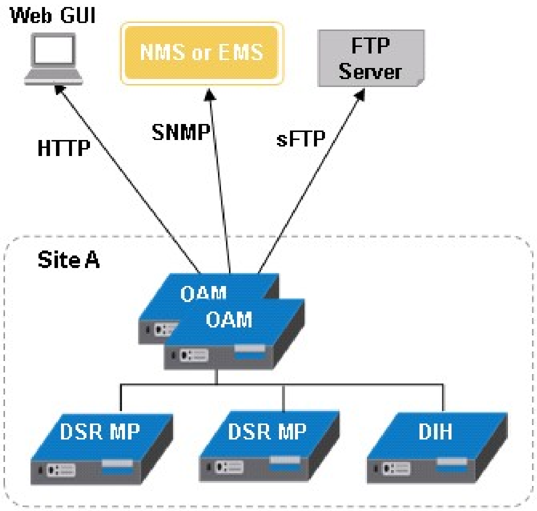


Figure 14: DSR OAM Architecture

Message Processors

The role of the Message Processors (DA-MPs) is to provide the Diameter application messaging interfaces, message processing functions, and message routing functions to the DSR Applications that run on them. All Message Processors replicate configuration data from the OAM servers and send measurements, events, alarms, and log data to the OAM servers.

Integrated Diameter Intelligence Hub

The Integrated Diameter Intelligence Hub (IDIH) provides the ability to filter, access, and troubleshoot Diameter transactions without the need for separate probes or taps. See *Integrated Diameter Intelligence Hub*.

DSR Functions

The DSR provides the following functions:

- **Base Diameter Relay Agent**: The DSR uses a Diameter Relay Agent to forward a message to the appropriate destination based on the information contained in the message.
- **Core Routing and Load Balancing**: The DSR creates a centralized Diameter signaling core that handles routing, traffic management and load balancing tasks, and provides a single interconnect point to other networks.

  The **IP Front End (IPFE)** can run in a DSR system to distribute IPv4 and IPv6 connections from multiple clients to multiple Diameter Agent Message Processors (DA-MPs).
- **DNS A and AAAA support**: The DSR supports resolving host names using DNS A and AAAA queries based on the configured peer IP address of the connection when the peer IP address is not provisioned.
  - **Diameter Common Function**: The DSR uses Diameter Common to configure the NOAM, SOAM and MP Profiles.
  - The NOAM provide access to perform the following tasks:
    - Configure up to 2500 distinct combinations of Mobile Country Code (MCC) and Mobile Network Code (MNC).
    - Configure mapping of MCC+MNC combinations to Diameter Realms, MSIN prefix digits, and CC+NDC combinations.
  - The NOAM provide access to perform the following tasks:
    - Filter the list of MCC Ranges, to display only the desired MCC Ranges.
    - Sort the list entries in ascending or descending order by Start MCC values or End MCC values by clicking the column heading. By default, the list is sorted by Start MCC values in ascending ASCII order.
    - Add new MCC Ranges. If the maximum number of MCC Ranges (10) already exists in the system
  - An MP Profile assignment for each DA-MP
- **Diameter Transport Function**:

  Diameter can be distributed over multiple MPs; however, the Diameter Transport Function is responsible for managing the transport connections only on a single MP and relies on the Diameter Routing Function to perform distributed processing.
  - **Diameter connection management**: Reporting of Diameter connection status changes,

    The DSR supports up to 64 transport connections per Peer Node, and up to 32 Local Nodes.

    The DSR supports multiple Diameter connections to any Peer Node and multiple Peer Nodes.
  - **Transport protocols**: The DSR supports both Stream Control Transmission Protocol (SCTP uni-homing and multi-homing), Transmission Control Protocol (TCP), Datagram Transport Layer Security (DTLS)/SCTP and Transport Layer Security (TLS)/TCP based transport connections.

  - **Message Processing**: Processing of Diameter Peer-to-Peer messages (CER/CEA, DWR/DWA, DPR/DPA), and delivery of Diameter Request and Answer messages from and to Diameter Peers and the Diameter Routing Function.

- **Diameter Routing Function**:

  - **Routing of Diameter Request and Answer messages** to and from Diameter Peers (through the Diameter Transport Function) and DSR Applications.

    - **Peer Routing Rules**: The DSR provides the ability to configure Peer Routing Rules that define where to route a Diameter message to an upstream Peer based upon Diameter message content.
    - **Processing of Diameter connection status** from the Diameter Transport Function and status from DSR Applications for maintaining dynamic routing configuration data.
    - **Message Rerouting**: A Diameter Relay Agent is responsible for making sure that Request messages are successfully delivered and to alternate route if failures are encountered.

      - **Alternate Implicit Routing**: Instead of a message being routed directly to an available Peer Node, the message is routed on an "alternate implicit route" that is chosen from a list that has been configured for the Peer Node.
      - **Reroute on Answer**: The DSR supports alternate routing of a Request message when an Answer response is received with a configured error code.

- **Capacity and Congestion Status and Controls**: Provides connection capacity status and controls, ingress message MPS controls, egress message throttling, and Egress Throttle Groups across DA-MPs.
- **MAP-Diameter Interworking Function**allows the DSR to support the bi-directional interworking between Diameter and SS7 (GSM MAP) messages.

  - A Diameter-to-MAP transaction is a Diameter transaction that is initiated by a Diameter Node that is routed to a DSR for MAP-Diameter interworking. The operator is required to configure DRL ART rules which associate a Request message with the DM-IWF application.

  - A MAP-to-Diameter transaction is a MAP procedure that is initiated by a SS7 Node that is routed to a DSR SS7-MP for MAP-Diameter interworking.

- **Diameter Mediation**: The DSR provides configuration and application of rules that modify message processing behavior when conditions are met at specified points in the message processing.
- **Message Copy**: For a message that was routed through the DSR, the Diameter Message Copy feature provides the ability to forward a copy of the Diameter Request message, and optionally the Answer message, to a Diameter Application Server (a DAS Peer). Diameter Message Copy can be triggered by any processing functions acting on the messages, including Diameter Mediation, DSR Applications (such as the Charging Proxy Application - CPA), and Peer Routing Rules.
- **Topology Hiding**: Topology Hiding involves hiding and restoring topology-related information in messages.

  - Diameter Topology Hiding can use Pseudo-Hostnames and encryption to hide topology-related information in messages sent from a Protected Network to an Untrusted Network, and to restore the topology-related information in messages from an Untrusted Network.
  - The Policy and Charging Application (PCA) uses a configured list of Policy Client Peer Nodes from which the PCRF name is to be hidden.
  - In the Charging Proxy Application (CPA), the Charging Proxy Function provides topology hiding using Virtual CDF and Virtual CTF Local Nodes. The CPF appears as a single CDF to

the CTFs, and as a single CTF to the CDFs. The Charging Proxy Function modifies the Origin-Host and Origin-Realm AVPs in each message being routed to a CTF or CDF.

- The **Application Chaining** is a method for invoking multiple DSR Applications in sequence on the same DSR. With respect to DSR application chaining, an accessing region is a DSR network segment where the DSR has a direct connection to a policy client who initiates and sends a Diameter request directly to the DSR and a serving region is a DSR network segment where the PCA (either P-DRA or OC-DRA functionality) application actually receives and processes the Diameter request message as forwarded by DRL. Accessing region and serving region are all relative concepts, which make sense only relevant to a specific policy client and a specific DSR application (i.e. PCA). A serving region can be an accessing region as well for a policy client and PCA application, i.e. the DSR that receives a Diameter requests hosts the P-DRA that processes the Diameter requests.
- **Integrated Diameter Intelligence Hub**: The Integrated Diameter Intelligence Hub (DIH) provides the ability to troubleshoot Diameter transactions.
- **DSR Switchover**: The DSR servers operate in redundancy mode and support automatic failover to the standby server if the active server fails. Automatic failover does not require manual intervention.
- **IPsec Support**: The DSR supports transporting messages over Internet Protocol security (IPsec) secure connections.
- **IPv4 and IPv6 Support**: The DSR supports IPv6 and IPv4 IP address formats.

Chapter 2

Diameter Protocol

Topics:

The DSR implements the Diameter base protocol to provide a centralized Diameter signaling core that handles routing, traffic management and load balancing tasks, and provides a single interconnect point to other networks.

Diameter Overview

The DSR implements the Diameter base protocol to serve primarily as a Diameter Relay Agent to route Diameter traffic based on configured routing data.

Diameter protocol configuration includes components that provide data for routing functions and for transport connection management.

The Diameter protocol functions in a 3-tiered DSR topology.

In DSR topology, the OAM server function is split into Network OAM (NOAM) servers and System OAM (SOAM) servers. A DSR with a pair of NOAM servers is connected to multiple DSRs in the network. Each DSR is connected to up to 16 mated pairs of SOAM servers (to support 3 fully populated enclosures). Each DA-MP resides with a pair of SOAM servers that interact directly with the respective DA-MPs on that DSR.

The DSR does not alter existing DSR functions other than separating what can be configured or managed at which level (DSR NOAM or DSR SOAM).

Each DSR services signaling traffic to and from a collection of Diameter clients, servers, and agents. The DSR MPs provide the Diameter message handling function. Each DSR MP supports connections to all of the DSR Peers.

DSR Topology

In DSR topology, there are NOAM servers, SOAM servers, and MP servers. The NOAM server takes on network scope and the SOAM server manages a single DSR Signaling NE.

The SOAM GUI screens can be used to configure and manage Diameter data, Diameter Common data, site-specific Policy and Charging data, IPFE data, MAP-Diameter Interworking data for DM-IWF, and DSR Application data.

Diameter Common provides the Import and Export GUIs on the NOAM and SOAM for exporting and importing the configuration data for Diameter Configuration, IPFE, and DSR Applications, and on the NOAM for exporting and importing Diameter Configuration and Policy and Charging configuration data.

Diameter Transport Function

Though Diameter can be distributed over multiple MPs, the Diameter Transport Function is a thin layer acting as an interface between a User Adaptation Layer and the IP Transport Layer. The Transport Manager that is used with the MAP-to-Diameter Interworking Function (MD-IWF), SS7/Sigtran Application supports the MTP3 User Adaptation Layer (M3UA) and the Stream Control Transmission Protocol (SCTP) IP Transport Layer.

Transport Manager enables the configuration of "Transports" (SCTP associations with remote hosts over an underlying IP network). It provides the interface to the Adaptation Layer and manages the connections and data transmission from SCTP sockets.

The Transport Manager performs the following activities:

- The Transport Manager performs the following activities:

- Handles Transport establish and tear down requests from the User.
- Manages Transport state and its User Adaptation Layer states for each Transport.
- Processes Transmit and Receive data.
- Provides multihoming for SCTP associations and validation of SCTP IP addresses.

The Transport Manager provides connection-based services, including IP-based addresses, to the MD-IWF SS7 Application on a physical MP server. Each MP has two Signaling IP Addresses. The Transport Manager uses these Signaling IP Addresses as Local IP Addresses for Transports.

Limitations

Transport Manager has the following limitations:

- Transport Manager does not support Transport Layer Security (TLS) and IPsec connections over SCTP.
- Transport Manager does not support IPv6 IP addresses.

Diameter Routing Function

The Diameter Routing Function supports the routing functions of a Diameter Relay Agent.

The Diameter Routing Function is responsible for the following functions:

- Message routing to local DSR Applications based upon user-defined Application Routing Rules
- Message routing to Peer Nodes based upon user-defined Peer Routing Rules, Route Lists, Route Groups, priorities, and capacities

  The Diameter Routing Function method for routing request messages to Peer Nodes is loosely based upon DNS load sharing. A Route List is comprised of a prioritized list of Peer Nodes and/or Diameter connections to which a message can be routed. Each Peer Node and Diameter connection must be assigned a "capacity" that defines the weighted distribution of messages among peers or connections with the same Priority. A set of Peer Nodes and Diameter connections within a Route List of equal Priority is called a Route Group.

- Message routing to Peer Nodes with multiple Diameter connections
- Message Copy

  The Diameter Routing Function can forward to a Diameter Application Server (DAS) a copy of a Diameter Request message, and optionally the Answer message, that is received by or routed through the DSR . Diameter Message Copy can be triggered by any processing functions acting on the messages, including Diameter Mediation, MAP-Diameter IWF, DSR Applications (such as the Charging Proxy Application - CPA), and Peer Routing Rules.

- Topology Hiding triggered by Diameter and DSR Applications
- Message rerouting on failures

  Rerouting is attempted for the following types of failures:

  - Diameter connection failure
  - Diameter connection Watchdog failure
  - Negative Answer response
  - Peer-to-Peer Pending Answer Timer expiration

The following types of rerouting can be attempted:

  - Alternate Implicit Routing

    Instead of a message being routed directly to an available Peer Node, the message is routed on an "alternate implicit route" that is chosen from a Route List that has been selected in the Peer Node configuration.

  - Reroute on Answer

    The DSR supports alternate routing of a Request message when an Answer response is received with a configured error code.

- Interfacing with the Diameter Transport Function
  - Processing Diameter connection status events received from the Diameter Transport Function
  - Issuing Diameter connection management events to the Diameter Transport Function
  - Routing Diameter messages received from Peer Nodes through the Diameter Transport Function
  - Sending Diameter messages to the Diameter Transport Function for forwarding on Diameter connections
- Interfacing with DSR Applications
  - Processing Operational Status events from DSR Applications
  - Routing Diameter messages received from Peer Nodes to DSR Applications
  - Routing Diameter messages received from DSR Applications to Peer Nodes
- Providing Egress Throttle Groups functions across DA-MPs
- Updating routing information based on connection and DSR Application status changes and on OAM configuration and state changes
- Processing routing configuration and maintenance changes from OAM
- Updating alarm, event, KPI, and measurements data for routing configuration components

DSR Application Infrastructure

The DSR Application Infrastructure (DAI) supports the following DSR Applications in the DSR:

- Full Address Based Resolution (FABR)
- Range Based Address Resolution (RBAR)
- Charging Proxy Application (CPA)
- Policy and Charging Application (PCA)
- Gateway Location Application (GLA)
- MAP - Interworking Function (MD-IWF)

The DSR Application Infrastructure is responsible for the following functions:

- Message routing to local DSR Applications based upon user-defined Application Routing Rules
- Interfacing with the Diameter Routing Function
  - Processing Operational Status events from DSR Applications
  - Routing Diameter messages received from Peer Nodes to DSR Applications
  - Routing Diameter messages received from DSR Applications to Peer Nodes

    - Application Chaining messages received from PCA to DSR Application
- Updating routing information based on connection and DSR Application status changes and on OAM configuration and state changes

Chapter 3

Diameter Mediation

Topics:

The Diameter Mediation feature allows easy creation of Mediation Rules.

Mediation Overview

References:

- *Diameter Mediation User 's Guide*
- **Help** > **Diameter** > **Mediation**
- **Help** > **Diameter** > **Reports**

Diameter message mediation helps to solve interoperability issues by using rules to manipulate header parts and Attribute-Value Pairs (AVPs) in an incoming routable message and peer to peer messages, when data in the message matches some specified conditions at a specified point of message processing. Tasks of the "if condition matches, then do some action" type can be solved in the most efficient way.

The Diameter Mediation feature can make the routable decisions of send reply, drop the message or set the destination-realm.

This feature extends the CAPM (Computer-Aided Policy Making) framework to allow for easy creation of Mediation rules for use in 3G, LTE and IMS networks. Mediation Rule Templates are created to define the Conditions that must be matched in a message and the Actions that are applied to modify on the routing decisions.

- A **Condition** defines a part of the message that is used in the comparison, an operator for the type of comparison, and a type of data that must match the data in the message part. Two or more Conditions in the same Rule Template are collectively referred to as a condition Set; the Condition Set are **ANDed**, **ORed** or **Complex Expression** in the comparison process.
- An **Action** can modify the message header **Version**, **Command-Code**, or **Application-ID** Diameter components. Two or more **Actions** in a **Rule Template** are collectively referred to as an Action Set.

After a Rule Template definition is complete, a Rule Set can be generated from the Rule Template. The data needed for the Conditions and the Actions is provisioned in the generated Rule Set. A Mediation rule is an instance of the data needed for the execution of Mediation logic. The actual data needed for the Conditions and the Actions is provisioned in one or more rules in the generated **Rule Set**. All of the rules associated with one Mediation Rule Template are collectively referred to as the **Rule Set** for the **Rule Template**.

Rule Sets can be associated with pre-defined Request or Answer Trigger Points in the DSR message processing logic.

The available Diameter Mediation Triggers are the:

- Diameter Routing Function, which supports RTP1, RTP10, ATP1, ATP10 and RTP11 triggers.
- Diameter Connection Function, which supports CER, CEA, DWR, DWA, DPR and DPA triggers.
- Application Function, which supports RTP4, RTP6, ATP4, and ATP6 triggers.

A user, who is designated as the Administrator can use the Rule Sets entries, Enumerations, Triggers, State & Properties and Internal Variables GUI screens, and other GUI screens to perform the following tasks, but cannot create, modify, copy, or export Rule Templates:

- Add a rule to a Rule Set, and provision the actual data that is used by the rule in the message matching process.
- Import/Export Rules that are provisioned in the rule templates in the "Test" or "Active" State.
- Edit and delete rules in Rule Sets.
- Delete Rule Sets.

- Change the state of a Rule Template.

  The Rule Template state can be changed to Test for testing its Rule Sets or to Active for enabling its Rule Sets for use with live traffic.

  When Administrator privileges are deactivated, the state cannot be changed back to Development.

- Set the Action Error Handling property of a Rule Set.
- Enable the Status of Rule Counters to display the Rule Counters.
- Test a Rule Set

  A Diagnostics Tool is available to test Mediation rules before they are subjected to live traffic in the network. The DSR Diagnostics Tool logs the rules applied, Actions taken, and other diagnostics information when a test message is injected into the system. The tool generates traffic and sends Diameter Messages on a test connection. As a test message traverses the system, the DSR application logic generates diagnostics messages at Trigger points. The **Diameter > Reports > Diagnostics Tool** GUI is used to view the diagnostics log reports. See Reports in the DSR Diameter User's Guide.

- Associate Rule Sets with Triggers, and remove Rule Set associations with Triggers.
- Import previously exported Rule Templates.

  The state of an imported Rule Template is set to Test by default.

- View, create, edit and delete the Internal Variables that can be used in the rules.
- View, create, edit and delete the Enumeration types that can be used in the rules.
- View, create, edit and delete the Vendors-specific AVPs that can be used in Rule Templates (see Vendors in the Diameter User's Guide)

Chapter 4

DSR Applications

Topics:

The DSR supports the following DSR Applications that use and enhance the functions of the Diameter protocol for message processing:

- Full Address Based Resolution (FABR)
- Range Based Address Resolution (RBAR)
- Charging Proxy Application (CPA)
- Policy and Charging Applications (PCA)
- Gateway Location Application (GLA)
- MAP-Diameter Interlocking (MD-IWF)

DSR Applications Overview

The DSR supports the following DSR Applications that use and enhance the functions of the Diameter protocol for message processing:

- Full Address Based Resolution (FABR)

  FABR is deployed with the Subscriber Database Server (SDS), which is used for provisioning and lookup of subscriber data for address resolution.

- Range Based Address Resolution (RBAR)
- Charging Proxy Application (CPA)
- Policy and Charging Application (PCA)
- Gateway Location Application (GLA)
- MAP-Diameter Interworking (MD-IWF)

DSR Applications run in DA-MPs. Each DA-MP supports connections to all of its DSR Peers.

The RBAR and Policy DRA DSR Applications can run on the same DA-MP.

Full Address Based Resolution

References:

- *Full Address Based Resolution (FABR) User's Guide*
- **Help** > **Full Address Based Resolution (FABR)**

Full Address Based Resolution (FABR) is a DSR enhanced routing application that resolves the designated Diameter server (IMS HSS, LTE HSS, PCRF, OCS, OFCS, and AAA) addresses based on configured Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity addresses.

The FABR application validates the ingress Diameter Request message, retrieves the Application ID and Command Code from the message, and determines the desired Routing Entity Type to be decoded from the message, based on the configuration.

The FABR application extracts the Routing Entity address from user-configured Attribute-Value Pairs (AVPs) in the ingress message and sends the successfully extracted Routing Entity address to an off-board SDS DP for destination address resolution.

A Routing Entity can be:

- 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
  - IPv6-prefix
- A general purpose data type: UNSIGNED16

The resolved destination address can be any combination of a Realm and Fully Qualified Domain Name (FQDN), such as Realm-only, FQDN-only, or Realm and FQDN.

The FABR application replaces the Destination-Host and/or Destination-Realm AVP in the ingress Request message with the corresponding values of the resolved destination, and forwards the message to the Diameter Routing Function for egress routing into the network.

FABR provides the following functions:

- Routing Based on IMSI/MSISDN Prefix Lookup, configured in Diameter Configuration, perform prefix based lookups after the full address lookup is performed. The prefix and range based lookup will only be 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.
- DP Query Bundling enhances the FABR-to-DP interface by supporting the bundling of multiple queries into a single "bundled query" stack event if bundling is enabled.
- Reserved MCC Ranges, configured in Diameter Configuration, define up to 10 distinct, non-overlapping Mobile Country Code Ranges, which are the first 3 digits of the IMSI.
- MCCMNC configured in Diameter Common to decode an IMPU from a User Identity (digit string) but cannot determine whether the User Identity is an IMSI or an MSISDN based on digit analysis, FABR needs a tie breaker to categorize the User Identity properly.
- Application Chaining is configured so that FABR and the DM-IWF applications can both process the same Diameter Request message.

FABR Deployment with SDS

References:

- SDS Online Help
- SDS Administration

DSR deployments that include support for the DSR Full Address Based Resolution (FABR) application must be deployed with the Subscriber Database Server (SDS). The SDS is used to provision the FABR subscriber data.

The SDS DP system consists of a Primary Provisioning Site, a Disaster Recovery (DR) Provisioning Site, and DSR Signaling Site servers with redundant DP SOAM servers and up to 2 DP blades. Each Provisioning Site has an Active/Standby pair of servers in a high availability (HA) configuration and a third server configured as a Query Server.

The DSR SOAMP and the SDS SOAMP servers are run on the DSR OAM blade using virtualization technology. It is assumed that most deployments that support both DSR and SDS will deploy the DSR NOAMP on Rack Mount Servers, as this is how the SDS NOAMP is deployed. Small deployments that minimize the amount of hardware investment require the DSR NOAMP to be deployed as a virtual server on the OAM blade. This requires running three Virtual Machines (VMs) on the blade – DSR NOAMP, DSR SOAMP and SDS SOAMP.

Range Based Address Resolution

References:

- *Range Based Address Resolution (RBAR) User's Guide*
- **Help** > **Range Based Address Resolution (RBAR)**

Range Based Address Resolution (RBAR) is a DSR-enhanced routing application that allows the 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:

- 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
  - IPv6-prefix
- A general purpose data type: UNSIGNED16

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 (incoming) message, with the corresponding values assigned to the resolved destination, and forwards the message to the Diameter Routing Function for egress (outgoing) routing into the network.

RBAR provides the following functions:

- Reserved MCC Ranges configured to define up to 10 distinct, non-overlapping Mobile Country Code Ranges, which are the first 3 digits of the IMSI.
- MCCMNC configured in Diameter Common 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, RBAR needs a tie breaker to categorize the user identity properly.
- Routing Exception Handling will invoke a routing exception handling procedure based on user-defined configuration, when an ingress RBAR Request message cannot be resolved to a Destination (no address matched, no valid digits decoded, or any other error is returned).

Charging Proxy Application

References:

- *Charging Proxy Application (CPA) and Offline Charging Solution User's Guide*
- **Help** > **Charging Proxy Application (CPA)**

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

The CPA communicates with an off-board (resides on a different MP) Charging Session Binding Repository (SBR) database that stores the session binding information to enable the Topology Hiding that the CPF provides. The Charging SBR stores information that the CPA uses for consistently routing Diameter requests from instances of Charging Trigger Function (CTF) to instances of Charging Data Function (CDF). For any given session, the CPA stores in the Charging SBR the identity of the CDF that the CPA has chosen to service the Diameter requests for that session, or a session binding. When the CPA routes subsequent Diameter requests for a session, it queries the Charging SBR for the session binding to determine the identity of the serving CDF. The Charging SBR database can be distributed over multiple physical servers using database slices (partitions) to reduce the volume of replication typically required for a large database.

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

The CPA is also responsible for triggering Message Copy. For the CPA, Message Copy allows ACR-Start or ACR-Event messages that match a configured rule to be copied to a Diameter Application Server (DAS). A triggering condition or rule can be defined in the CPA configuration. When a Diameter Request meeting the triggering condition is received by the DSR, the message is marked as ready to copy by the application as it is processed. When the response to the Request (the Answer) is received, if the Answer contains the correct result code as specified by the system-wide configuration, the resulting action is executed. The action for Message Copy is to copy the Request and send the copy to a DAS Peer Message Copy can be enabled and disabled without impacting the other functions of the CPA.

Policy and Charging Application

References:

- *Policy and Charging User's Guide*
- **Help** > **Policy and Charging**

A PCA DSR consists of a number of PCA DA-MP server, a number of SBR servers, OAM servers, and optional IPFE servers. The PCA DA-MPs are responsible for handling Diameter signaling and implementing the Policy DRA and Online Charging DRA functionalities, as well as the overall PCA application itself.

SBR servers host the policy session and policy binding databases for the P-DRA function and session database for the OC-DRA function. These are special purpose MP blades that provide an off-board database for use by the Policy DRA feature hosted on the Policy DRA DA-MPs. Policy SBRs host the Policy session and Policy Binding databases.

Each PCA DSR hosts connections to clients and to policy/charging servers such as OCSs and PCRFs. Clients are devices that request authorization for access to network resources on behalf of user equipment (such as mobile phones) from the PCRF, or request billing/charging instructions from an OCS. Policy Clients sit in the media stream and enforce Policy rules specified by the PCRF. Policy authorization requests and rules are carried in Diameter messages that are routed through Policy DRA. Policy DRA makes sure that all Policy authorization requests for a given subscriber are routed to the same PCRF. Charging clients (CTF) generates charging events based on the observation of network resource usage and collects the information pertaining to chargeable events within the network element, assembling this information into matching charging events, and sending these charging events towards the OCS.

PCA DSRs can be deployed in mated pairs such that policy session state is not lost, even if an entire PCA DSR fails or becomes inaccessible. When PCA mated pairs are deployed, the clients and PCRFs/OCSs are typically cross-connected such that both PCA DSRs have connections to all clients and all PCRFs/OCSs at both mated sites.

PCA DSRs can also be deployed in mated triplets such that session states are not lost, even if two PCA DSRs fail or become inaccessible. When a PCA mated triplet is deployed, clients and PCRFs/OCSs are cross-connected such that all three PCA DSRs have connections to all policy clients and all PCRFs/OCSs associated with the mated triplet.

"PCA network" is the term used to describe a set of PCA mated pairs and NOAM server pair/triplet. All clients and PCRFs/OCSs are reachable for Diameter signaling from any PCA DSR in the PCA network.

PCA is also designed to do the following:

- Reduce Diameter signaling latency where possible by doing the following:
  - Limiting the need to access off-board databases

    Note: "Off-board" in this context means on a server separate from the server handling the Diameter signaling
  - Limiting to a single WAN traversal to route a diameter message within the PCA network
  - Optimization of the most frequent "sunny day" scenarios, possibly at the expense of less common, or rainy day, scenarios
- Provide server redundancy by supporting clusters of active DA-MP servers
- Provides site redundancy by supporting mated pairs of P-DRA DSRs, as well as provide 3-site redundancy by supporting mated triplets of P-DRA DSRs
- Provide triple data redundancy for subscriber binding data by having geographically dispersed active, standby, and spare copies of each binding record for mated pair configuration
- Provide quadruple data redundancy for subscriber binding data by having geographically dispersed active, standby, spare, and spare copies of each binding record for mated triplet configuration
- Support scalability of each DSR by the addition of DA-MP blades, as well as support network scalability by the addition of PCA sites
- Limit network configuration complexity by makign use of naming conventions for clients and PCRFs/OCSs
- Facilitate troubleshooting of network-wide database accesses and Diameter signaling by including correlation information in logs and traces

Gateway Location Application

References:

- *Gateway Location Application (GLA) User's Guide*
- **Help** > **Gateway Location Application(GLA)**

Gateway Location Application (GLA) is a DSR Application that retrieves subscriber data stored in Session Binding Repository (SBR) provided by PCA. The GLA is deployed in a network model with PCA and has access to all SBR data used by PCA. A key concept is any DA-MP running GLA must be in the same Resource Domain as DA-MPs running PCA. This does not imply any additional Resource Domain configuration is needed specifically for GLA in the DSR GUI.

After a DA-MP is activated with the GLA, it receives one Request (Get Gateway Request (GGR)) generated by the Gateway Query Client (GQC), then decodes subscriber information (IMSI or MSISDN), then queries the SBR (via ComAgent within the Gateway Query Server (GQS) or DSR). The GLA generates one Answer (Get Gateway Answer (GGA)) with subscriber information that includes the number of bindings for the subscriber, and the following information is included for each session:

1. Access Point name
2. PCEF FQDN
3. Creation timestamp

The GLA is dependent on PCA to populate data in SBR and thus GLA will use Activation/Deactivation rules in the following conditions:

- The GLA is activated using the same mechanism as PCA. It will be activated at the NOAM, and activation is performed so that it activates all SOAMs under a common NOAM.

- GLA cannot be activated unless PCA is activated and PCRF-Pooling has been enabled.
- Policy DRA cannot be deactivated if GLA is activated.

To simplify deployment of GLA, it is piggybacked on PCA's configuration of DA-MPs within its Resource Domain and configuration of ComAgent connections between DA-MPs and SBRs.

The GLA uses identical access methodologies (an Active/Standby/Spare HA model combined for server redundancy, and splits the database storage resource into multiple sub-resources for load-sharing) as PCA to read the subscriber information from SBR. When GLA queries SBR for a subscriber's information, it must find the same Active sub-resource that Policy DRA is using.

ComAgent connectivity is required for the GLA DA-MPs to every SBR-B server in a Policy Binding Resource Domain since:

- The PCA must create a ComAgent connection from each DA-MP to each SBR.
- The GLA DA-MPs must exist in the same Resource Domain as Policy DRA DA-MPs. This does not imply any additional Resource Domain configuration is needed specifically for GLA in the DSR GUI (Main Menu: Configuration -> Resource Domains).
- The PCA must be activated before GLA.

Alarms are generated by the GLA based on its ingress message rate. It is a notification mechanism to the customer; that higher than expected rates of traffic are being processed by the DSR Application. The customer configures the points of the alarms for the GLA Ingress Message Rate. If GLA receives a message that cannot be decoded, it will abandon the Diameter Request message processing, generate a Message Decoding Failure, peg measurement failures and handle the exception based on the user configuration. Refer to *DSR Alarms and KPIs Reference* and *DSR Measurements Reference* for other GLA specific alarms.

MAP-Diameter Interworking Function

References:

- *MAP-Diameter Interworking Function (MAP-Diameter IWF) User's Guide*
- **Help** > **MAP-Diameter IWF**

The DSR MAP-Diameter Interworking Function feature allows the DSR to support bi-directional interworking between Diameter and SS7-MAP messages. This functionality is carried out by two applications: DM-IWF and MD-IWF.

DM-IWF is a DSR application that runs on each DA-MP. It manages MAP-Diameter Interworking transactions received from the Diameter network via DRL and MAP-Diameter Interworking transactions received from SS7-MPs.

MD-IWF is a TCAP application which runs on each SS7-MP. It manages MAP-Diameter Interworking transactions received from the SS7 network (via TCAP) and MAP-Diameter Interworking transactions received from DA-MPs.

The MAP-Diameter Interworking assumes the following things regarding the relationship between the two applications.

- All MAP-Diameter message and parameter interworking is performed on the SS7-MP.
- DM-IWF and MD-IWF exchange Diameter messages using ComAgent. No SS7/MAP message are exchanged between DA-MPs and SS7-MPs. Diameter messages are sent using a new stack event called IWF-Application-Data.
- When a transaction is initiated by either a DM-IWF or MD-IWF instance, it creates a Transaction ID which is unique to the DM-IWF/MD-IWF instance which is initiating the inter-MP transaction.

The Transaction ID is sent as an IWF-Application-Data stack event parameter that correlates the messages/responses exchanged between DM-IWF and MD-IWF associated with a transaction. When DM-IWF or MD-IWF sends a response to the request, it echoes the transaction ID from the Request to allow the recipient to correlate the response with the request it had previously sent. The internal Transaction ID eliminates the need to manage Hop-by-Hop IDs in Diameter messages exchanged between DM-IWF and MD-IWF.

- DM-IWF and MD-IWF will use ComAgent's Routed Service with Reliable Transfer now support capabilities that allow eliminating the need for DM-IWFs and MD-IWFs to track growth/degrowth of SS7-MPs and DA-MPs respectively. In this document, any reference to DM-IWF Routed Service or MD-IWF Routed Service should be understood to mean ComAgent Routed Service using Reliable Transfer, utilizing Routed Service enhancements.

  Note: Service users and providers can now dynamically register against the Routed Service. Service Providers publish their own provider status. ComAgent Routed Service accounts for each registered service provider's status and congestion level when selecting service providers to distribute Requests.

- DM-IWF and MD-IWF will use ComAgent's Direct "EventTransfer" Service to route Answer message responses to the specific MD-IWF and DM-IWF respectively which initiated the transaction.

SS7/Sigtran

References:

- *SS7/Sigtran User's Guide*
- **Help** > **SS7/Sigtran**

SS7/Sigtran provides the Signaling Network Interface for the MD-IWF SS7 Application. The interface supports standards-based M3UA, MTP3, and SCCP signaling.

Chapter 5

IP Front End (IPFE)

Topics:

The IP Front End (IPFE) is a traffic distributor that transparently provides the following functions:

- Presents a routable IP address representing a set of application servers to application clients.
- Routes packets from the clients that establish new transport connections to a selected application server.
- Routes packets in existing transport connections to the correct server for the connection.

IPFE Overview

References:

- *IP Front End (IPFE) User's Guide*
- **Help** > **IP Front End (IPFE)**

The IPFE acts as a specialized layer-3 router. The various servers to which the IPFE routes are divided into **Target Sets**. Each of the target sets are assigned a shared **Target Set Address**. The IPFE Architecture assumes that either two connections are maintained at all times, in active/active or active/standby, or that a single connection is maintained, with a backup address to which it can establish a connection if the first connection fails.

A packet is routed through the router and the IPFE to the application server without rewriting of the packet. This means that neither the source IP address nor the destination IP address changes as it passes through the IPFE. The IPFE behaves as an IP router and does not act as a network address translator (NAT).

The IPFE (IP Front End) is a packet-based load balancer that makes a large DSR cluster accessible to incoming connections through a minimal number of IP addresses. These incoming connections can be TCP, unihomed SCTP, or multihomed SCTP. The IPFE distributes these connections among a list of target IP addresses by forwarding incoming packets. The list is called the **Target Set IP List**, and an outward-facing IP address is called a **Target Set Address** (TSA). A packet arriving at the IPFE and destined for the TSA is forwarded to an address in the **Target Set IP List**.

When paired with a second IPFE instance, the IPFE supports active-standby or active-active high availability (HA). The mated pair of IPFEs expose typically one or two TSAs per configured IP version.

The IPFE stores an association record about each connection. The association contains the information necessary to identify packets belonging to a connection and to identify the application server that the IPFE has selected for the connection. The IPFE routes all packets associated with a particular connection to the selected application server.

Since the IPFE has no visibility into the transaction state between client and application server, it cannot know if an association no longer represents an active connection. The IPFE makes available a per **Target Set** configuration parameter, known as **Delete Age**, that specifies the elapse of time after which an association is to be deleted. The IPFE will treat packets that had their associations deleted as new packets and will run the application server selection function for them.

It will create a new association by choosing an application server from the **Target Set IP** List, if a packet is not matched by any association. The choice is based on the **Load Balance Algorithm** setting.

A **Target Set** can be created as either IPv4 or IPv6. However a **Target Set** cannot support mixed address types. This means that SCTP multihomed endpoints can contain address types of either IPv4 or IPv6 but not both.

The IPFE provides a configurable parameter which limits the IPFE's throughput rate and prevents the maxing out of its CPU, in case of signaling storms. **Throttling** causes the IPFE to drop packets in order to keep the load from overwhelming the IPFE. The packet/second rate limit implementation creates an even dropping of packets that would cause client TCP/SCTP stacks to withhold their rates to just below the threshold, as happens when there is an overloaded router in the path.

Part III

DSR Configuration

Topics:

Configuring the DSR can include network and system configuration, OAM configuration, Communication Agent configuration, IP Front End configuration, Diameter configuration, and DSR Application configuration.

This part of the Guide and Help contains overview descriptions of DSR configuration, IPFE configuration, Diameter configuration, Diameter Mediation configuration, and DSR Application configuration.

Chapter 1

DSR Configuration Overview

Topics:

Configuring the DSR can include:

- Network and system configuration
- OAM configuration
- Communication Agent configuration
- IP Front End configuration
- Diameter protocol configuration
- Configuration of activated DSR Applications

DSR Configuration

References:

- *DSR HP C-Class Installation* for the appropriate release
- *DSR Upgrade/Backout Procedure* for the appropriate release
- *DSR RMS Productization Installation*for the appropriate release
- Feature Activation Guides for any DSR Applications in the system
- *Operation, Administration, and Maintenance (OAM) Guide* and Help
- User's Guides and Help for Communication Agent, Diameter Common, MAP-Diameter IWF, SS7/Sigtran, Transport Manager, IDIH, IPFE, Diameter, Diameter Mediation, and DSR Applications

Configuring the DSR can include:

- Network hardware and firmware installation and configuration; and PM&C, TVOE, and SNMP configuration

  Customer Support personnel normally either perform or participate in performing these activities.
- DSR system topology configuration of OAM Network Elements, Communication Services, servers, and server groups, and message processors

  Customer Support personnel normally either perform or participate in performing these activities.
- OAM configuration, including MP blade servers, Server Groups, Signaling Network Devices, and VLAN Interfaces

  Customer Support personnel normally either perform or participate in performing these activities.
- Activation of DSR Applications

  Customer Support personnel normally either perform or participate in performing these activities.
- Diameter protocol configuration, including configuration for routing functions and configuration for transport connection management
- Configuration of the IP Front End (IPFE), if used
- Configuration of activated DSR Applications

Configuration of the DSR Topology

DSR supports an OAM architecture with one or more pair of NOAM servers and one or more pairs of SOAM servers per DSR NE.

- OAM configuration, some Diameter configurations, and some DSR Applications configuration are done on the NOAM
- Most Diameter and DSR Application configurations are done on the SOAM.
- Some common utilities can be accessed on either OAM.

The DSR topology NOAM server and SOAM servers, determines how various components are configured. There are two types of GUIs used for managing a network of DSR Signaling NEs.

- The DSR NOAM hosts a GUI that is primarily for managing A-sourced data. A-sourced data is Platform and topology data.

- The DSR SOAM hosts a GUI for that is primarily for managing B-sourced data. B-sourced data is DSR data.

The DSR topology allows administrators to access all DSR SOAM GUI pages from a single point. An administrator can access all of the DSR SOAM GUI pages when logged into the DSR NOAM GUI, without needing to re-enter login credentials.

A-sourced, A-scoped, B-sourced, and B-scoped Data

The bulk provisioning data and network topology data (such as user accounts, network elements, servers, server groups, and upgrade) that is to be configured and managed through a DSR NOAM are called A-sourced data. (Some Diameter configuration and some Policy and Charging application configuration is done on the NOAM.)

The Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists) and DSR Application data (FABR, RBAR, CPA, PCA, GLA) that is configured and managed through a DSR SOAM are called B-sourced data.

The platform MEAL data generated by all NOAM, MP, and SOAM servers, which is merged to NOAM servers, are called A-scoped data.

The Diameter signaling MEAL data and DSR Application MEAL data that are generated by all MP servers and merged to SOAM servers are called B-scoped data.

MEAL data is handled as follows:

- The A-Scoped MEAL data (Platform MEAL data) generated by all NOAM, MP, and SOAM servers can be viewed on NOAM servers.
- The A-Scoped MEAL data (Platform MEAL data) generated by all MP and SOAM servers can be viewed on SOAM servers.
- B-Scoped MEAL data (Diameter signaling MEAL data and DSR Application MEAL data) generated by all MP servers can be viewed on SOAM servers.

The following common utilities are available on both the NOAM and SOAM servers:

- Alarms and Events
- Security Log
- Status & Manage
- Measurements
- Communication Agent
- Diameter Common

Diameter Configuration

The DSR requires configuration for Diameter routing and transport functions.

DSR Applications require Diameter configuration that supports and is specific to the functions that the DSR Applications perform.

Diameter Configuration components and configuration procedures are described in detail in the *Diameter User 's Guide, Diameter Mediation User 's Guide* and Diameter online help.

Configuration for Diameter Routing Functions

Message routing is provided through the DSR. The DSR functions as a Diameter Relay Agent to forward messages to the appropriate destination based on information contained within the message, including header information and applicable Attribute-Value Pairs (AVP). User-defined Peer Routing Rules define where to route a message to upstream Peer Nodes. Application Routing Rules route messages to DSR Applications. The DSR provides the capability to route Diameter messages based on any combination of, or presence or absence of, the following message parameters:

- Destination-Realm
- Destination Host
- Application ID
- Command Code
- Origination Realm
- Origination Host
- IMSI

The DSR supports multiple transport connections to each Peer Node and provides the following functions:

- Routing Diameter Request and Answer messages received from Diameter Peers
- Weighted load sharing
- Priority routing
- Rerouting

Configuring DSR routing includes:

- Creating Route Groups and assigning Capacity levels to each Peer Node in each Route Group.
- Creating Route Lists and defining Active and Standby Route Groups in each Route List. Active and Standby status is determined by Peer Node Priority and Weight.
- Creating Peer Routing Rules and assigning Route Lists and Priorities to the rules.
- Creating Application Routing Rules that route messages to DSR Applications
- Creating Egress Throttling Groups and Message Copy Configuration Sets

Configuration for Diameter Transport Functions

The Diameter Transport Function communicates connection management information to the Diameter Routing Function that it needs for making routing decisions (including Operational Status changes, rerouting Requests, and Connection Priority Level changes).

A transport connection provides the reliable transport connectivity between a Local Diameter Node and a Peer Diameter Node. A transport connection must be configured in order for the Diameter Routing Function to allow a transport connection to be established with a Peer Diameter Node. A transport connection may use the SCTP or TCP transport protocol. A node using the SCTP transport protocol can be configured to advertise more than one IP address and to establish SCTP paths to more than one Peer IP address. Two IP Addresses are supported for an SCTP multi-homed connection both for the Local Node and Peer Node.

The primary transport Diameter configuration components are Local Nodes, Peer Nodes, Connections, and Configuration Sets. The DSR supports both IPv4 and IPv6 connections.

Configuration for transport includes:

- Connection TCP or SCTP transport protocol, SCTP multi-homing or uni-homing, and Fixed or Floating (IPFE TSA) connection type
- Local Node FQDN, Realm, IP Addresses, and transport protocol
- Peer Node FQDN, Realm, IP Addresses, and transport protocol

- Connection, Capability Exchange (CEX), Message Priority, and Egress Message Throttling Configuration Sets
- Common Diameter Application Ids
- Capacity (ingress and egress message rates) and Congestion Controls:
    - Diameter MP Congestion Management, including internal resource management, MP Processing Overload Control, and Maximum MPS Limitation
    - User Configurable Message Priority
    - Per connection Ingress MPS Control
    - Remote BUSY Congestion
    - Egress Transport Congestion
    - Per Connection Egress Message Throttling
    - User-Configurable Connection Pending Transaction Limiting

DSR Applications Configuration

Configuration for DSR Applications can include:

- OAM configuration, including servers and server groups
- Communication Agent configuration
- Configuration of Diameter components that is specific to the functions that the DSR Applications perform, including
    - MP Profiles for DA-MPs and SBR servers
    - Application Ids for specific Diameter interfaces
    - Command Codes
    - Peer Nodes
    - Local Nodes
    - Connections
    - Route Lists
    - Peer Routing Rules
    - Application Routing Rules
- Configuration on the NOAM or SOAM, or both, of DSR Application components

Chapter

2

IPFE Configuration

Topics:

The **IPFE > Configuration** GUI pages for IPFE components provide fields for entering the information needed to manage IPFE in the DSR.

IPFE Configuration Overview

References:

- *IP Front End (IPFE) User's Guide*
- **Help** > **IPFE**

The *IP Front End (IPFE) User 's Guide* describes the function and configuration of the following IP Front End (IPFE) components:

- Options
- Target Sets

DSR Bulk Import and Export

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

IPFE Configuration Options

The **Configuration Options** fields set up data replication between IPFEs, specify port ranges for TCP traffic, set application server monitoring parameters, and assign Target Set Addresses to IPFEs.

Internal IP addresses are used by the IPFEs to replicate association data. These addresses should reside on the IMI (Internal Management Interface) network.

A minimum port number and a maximum port number specify the range of ports for which the IPFE will accept traffic. If the port is outside of the specified range, the IPFE will ignore the packet and not forward it to the application servers.

Target Set Addresses (TSAs) are a list of public IP addresses to which clients will connect. These IP addresses must be accessible from the outside world. Through the TSA, incoming traffic will be distributed over a number of application servers that are configured as the Target Set IP List.

At least one TSA must be configured before adding any Diameter Local Nodes. Configuration of a TSA must be done after configuration of all networking interfaces.

IPFE Target Sets Configuration

The IPFE provides one or more externally visible IP addresses (Target Set Addresses) and distributes traffic sent to those addresses across a set of application servers.

A list of application server IP addresses is assigned to a Target Set; the Target Set is associated with an IPFE pair.

Before a Target Set can be added, at least one IPFE must be configured on the **IPFE > Configuration > Options** page.

Chapter

3

Diameter Configuration

Topics:

The **Diameter > Configuration** GUI pages for Diameter components provide fields for entering the information needed to manage Diameter protocol configuration in the DSR.

Diameter Configuration Overview

References:

The following documents describe Diameter Configuration components, provide configuration procedures, and list the sequence in which to perform the configuration of the components.

- *Diameter User's Guide*
- **Help** > **Diameter** > **Configuration**

Users' Guides for DSR Applications indicate Diameter Configuration components that require specific configuration for the application.

The DSR requires configuration for Diameter routing functions and Diameter transport connection management functions.

Diameter Routing Function Configuration

Message routing is provided through the DSR. The DSR functions as a Diameter Relay Agent to forward messages to the appropriate destination based on information contained within the message, including header information and applicable Attribute-Value Pairs (AVP). User-defined Peer Routing Rules define where to route a message to upstream Peer Nodes. Application Routing Rules route messages to DSR Applications. The DSR provides the capability to route Diameter messages based on any combination of, or presence or absence of, the following message parameters:

- Destination-Realm
- Destination Host
- Application ID
- Command Code
- Origination Realm
- Origination Host
- IMSI

The DSR supports multiple transport connections to each Peer Node and provides the following functions:

- Routing Diameter Request and Answer messages received from Diameter Peers
- Weighted load sharing
- Priority routing
- Rerouting
- Message Copy to a DAS

Configuring Diameter routing can include:

- Creating Route Groups and assigning Capacity levels to each Peer Node in each Route Group
- Creating Route Lists and defining Active and Standby Route Groups in each Route List. Active and Standby status is determined by Peer Node Priority and Weight
- Creating Peer Routing Rules and assigning Route Lists and Priorities to the rules
- Creating Application Routing Rules that route messages to DSR Applications
- Configuring Trusted Network Lists, Protected Networks, and Configuration Sets for Diameter Topology Hiding functions
- Creating Message Copy Configuration Sets for Diameter Message Copy functions

- Creating Egress Throttle Groups to manage egress message throttling from a DSR to a Peer Node on a specified set of Connections. The Egress Message Rate, Egress Pending Transactions, or both, can be throttled.

Diameter Transport Function Configuration

The Diameter Transport Function communicates connection management information to the Diameter Routing Function that it needs for making routing decisions (including Operational Status changes, rerouting Requests, and Connection Priority Level changes).

A transport connection provides the reliable transport connectivity between a Local Diameter Node and a Peer Diameter Node. A transport connection must be configured in order for the Diameter Routing Function to allow a transport connection to be established with a Peer Diameter Node. A transport connection may use the SCTP or TCP transport protocol. A node using the SCTP transport protocol can be configured to advertise more than one IP address and to establish SCTP paths to more than one Peer IP address. Two IP Addresses are supported for an SCTP multi-homed connection both for the Local Node and Peer Node.

The Diameter Transport Function and the Diameter Routing Function can exchange Diameter messages between instances that are on either the same or different DA-MPs within the DSR NE. Ingress Request messages accepted by the Diameter Transport Function will always be sent to the local Diameter Routing Function instance for routing. The local Diameter Routing Function instance will route the Request. The Diameter Routing Function can choose an egress connection that is owned either by the local Diameter Transport Function instance or by another (remote) Diameter Transport Function instance.

The primary transport Diameter configuration components are Local Nodes, Peer Nodes, Connections, and Configuration Sets. The DSR supports both IPv4 and IPv6 connections.

Configuration for transport includes:

- Connection TCP or SCTP transport protocol, SCTP multi-homing or uni-homing, and Fixed or Floating (IPFE TSA) connection type

  There are two types of Transport Connections:

  - A Fixed connection can be assigned to one and only one DA-MP at configuration time.
  - An IPFE floating connection is implicitly assigned to a set of DA-MPs through the IPFE Target Set Address (TSA) assigned to the connection. The location of the connection is unknown until the connection is established on one of the DA-MP location candidates. See *IP Front End (IPFE)*.

- Local Node FQDN, Realm, IP Addresses, and transport protocol
- Peer Node FQDN, Realm, IP Addresses, and transport protocol
- Connection, Capability Exchange (CEX), and Message Priority Configuration Sets

  A Connection Configuration Set provides transport protocol and Diameter "tuning" for a transport connection to account for the network QoS and Peer Node requirements, and settings for Peer-initiated connections to a Local Node.

  Diameter Peers must perform Capabilities Exchange in order to discover the Peer's identity and capabilities. Capabilities Exchange validation of a Peer's identity and capabilities includes processing and validation of the following AVPs:

  - Origin-Host
  - Origin-Realm
  - Auth-Application-ID(s)

    - Acct-Application-ID(s)
    - Vendor-Specific-Application-ID(s)
    - Host-IP-Address(es)

    A user defined Message Priority Configuration Set contains a Message Priority that can be assigned to an ingress Diameter message, for use in algorithms for preferential discard, throttling, and routing by Peer Nodes and Local Nodes.

- Common Application IDs
- Capacity (ingress and egress message rates) and Congestion Controls:
    - The **DA-MP Overload Control** (Message Priority and Color-Based DA-MP Overload Control) provides a mechanism for managing internal/local DA-MP congestion detection and control. The DA-MP Overload Control feature tracks ingress message rate, calculates the amount of traffic that needs to be shed based on CPU congestion, and sheds that traffic based on Message Priority, Message Color, and discard policy.
    - The **User Configurable Message Priority** feature provides Message Priority that can be assigned to ingress Diameter messages, based on certain configurable criteria, for use in algorithms for preferential discard, throttling, and routing by Peer Nodes and Local Nodes. Message Priority Configuration Sets are assigned to Peer Nodes and Connections to provide the Message Priority during ingress message processing.
    - The **Per Connection Ingress MPS Control** (PCIMC) feature limits to a configurable level the per-Connection ingress message rate of each connection. Correctly configured message rate controls ensure that a single Connection cannot use the majority of the resources. (No limiting is done by PCIMC for the egress message rate.)
    - The **Remote BUSY Congestion** feature addresses Remote Congestion detection. The DSR Remote BUSY allows DSR egress Request routing to select a BUSY Connection (that is abating its BUSY status) based on the User Configurable Message Priority assigned to the message.
    - The **Egress Transport Congestion** feature uses Congestion Levels to manage the egress message traffic flow on a Diameter Peer Connection when the Connection's TCP/SCTP send buffer is exhausted, as indicated by the TCP/SCTP socket being "blocked".
    - The **Per Connection Egress Message Throttling** feature targets congestion avoidance by throttling the volume of Diameter traffic being sent over a Connection when the traffic exceeds the configured maximum egress message rate of the Connection.
    - The **User-Configurable Connection Pending Transaction Limiting** feature provides the ability to configure the Connection Pending Transaction Limit for each DSR Peer Connection.

Configuration Capacity Summary

The **Diameter > Configuration > Capacity Summary** page displays information about maximum allowed and currently configured Diameter Configuration components.

The following information is displayed in each row of a read-only table:

Configuration Item	The type of Diameter Configuration component
Max Allowed Entries	The maximum number of entries for that component that can be configured in Diameter.

Configured Entries	The number of entries for that components that are currently configured.
% Utilization	The percentage of the maximum number of entries for that component that are currently configured.

Use the **Diameter > Configuration > Capacity Summary** page when planning, configuring, and maintaining the DSR Diameter Configuration. See *Diameter User's Guide* for the maximum values per NE and per Configuration Component.

Connection Capacity Validation

The Connection Capacity Validation function validates and limits the configuration of Diameter Connections, to better ensure that the configuration does not violate the Connection Count or Reserved Ingress MPS capacity limitations of the DA-MP servers that handle Connections in real time.

Validation of the number of Connections and of Reserved Ingress MPS occurs in response to changes to the configuration of Connections and Capacity Configuration Sets. Such changes reduce the available Connection capacity of a DSR and must be validated before they can be allowed. (Actions that increase Connection capacity rather than reduce it do not require validation.)

On the **Diameter > Configuration > Connection Capacity Dashboard** GUI page, the Connection Capacity Validations feature displays capacity information for configured Connections and the currently configured Reserved Ingress MPS for each Active DA-MP in the DSR NE.

Application Ids Configuration

An Application Id, along with an Application Name, is used to uniquely identify a Diameter Application.

A “Diameter Application” is not a software application, but is a protocol based on the Diameter base protocol. Each Diameter Application is defined by an Application Id and can be associated with Command Codes and mandatory AVPs.

The Internet Assigned Numbers Authority (IANA) lists standard and vendor-specific Application Ids on their iana.org website. On the website:

- Select Protocol Assignments
- Scroll to locate the Authentication, Authorization, and Accounting (AAA) Parameters heading
- Select Application IDs under the heading

Transport configuration

The DSR transport configuration elements are Local Nodes, Peer Nodes, Connections, and Connection Configuration Sets. The DSR supports both IPv4 and IPv6 connections.

CEX Parameters Configuration

Configure CEX Parameters to associate an application type and vendor ID with a Diameter Application. If specified, the vendor ID will be placed in the Vendor Id AVP.

Command Codes Configuration

The Command Code is one of the parameters contained in a Diameter message. Command Codes can be used in Peer Routing Rules and Application Routing Rules.

An Extended Command Code (ECC) is a predefined/preloaded command code extension that comprises the following attributes:

- CC value
- AVP Code value
- AVP Data value

This broadens the definition of Diameter Command Codes to include an additional application-specific single Diameter or 3GPP AVP content per Command Code. A format example might be 272.416.1 = CCR/CCA-I.

Note: A parent CC or Base CC is a Command Code without AVP code and Data extensions. All ECCs are extensions of any of the configured base command codes.

Configuration Sets

Diameter Configuration Sets include:

Connection Configuration Sets

Connection Configuration Sets provide a mechanism for adjusting a connection to account for the network quality of service and Peer Node requirements. Each connection references a single Connection Configuration Set.

A Connection Configuration Set can be created with specific SCTP, Diameter, and TCP options and then assigned to a connection.

A default Connection Configuration Set, called Default, has options that can be modified, but the Default Connection Configuration Set cannot be deleted. When a new Connection Configuration Set is created, the values of the Default Connection Configuration Set are automatically populated into the new Connection Configuration Set. Only a few options need to be adjusted to create the new Connection Configuration Set.

Connection Configuration Set parameters are divided into three categories: SCTP, Diameter, and TCP.

SCTP parameters include:

- Send and receive buffer sizes
- Initial, minimum and maximum retransmit timeout times
- The number of retransmits triggering association failure
- The number of retransmits triggering init failure
- SACK delay time

- The heartbeat interval
- The maximum number of inbound and outbound streams
- Whether datagram bundling is on or off

Diameter parameters include:

- The connect timer
- The initial value of the watchdog timer
- The Capabilities Exchange timer
- The disconnect timer
- Connection proving parameters, including the proving mode, timer, and times

TCP parameters include:

- Send and receive buffer sizes
- Whether the Nagles algorithm is on or off

CEX Configuration Sets

A CEX Configuration Set provides a mechanism for assigning up to 10 unique Application Ids and up to 10 unique supported Vendor IDs to a Local Node or connection. A default CEX Configuration Set, called Default, is always available, and is pre-populated with the “RELAY” Application Id (0xFFFFFFFF).

Each Local Node will refer to a single CEX Configuration Set. The CEX Configuration Set is mandatory for Local Node. Each transport connection can optionally refer to a single CEX Configuration Set. During CEX message exchange, the CEX Configuration Set in the transport connection is used if configured. Otherwise, the CEX Configuration Set in the Local Node (associated with the transport connection) is used. A Vendor Id can be sent in the Supported-Vendor-ID AVP of a CEX even though the Vendor Id is not configured in the **Selected Supported Vendor Ids** for the CEX Configuration Set.

The application has a default CEX Configuration Set called Default, which is always available. The Default CEX Configuration Set options cannot be modified or deleted. When you create a new CEX Configuration Set the values of the Default CEX Configuration Set are automatically populated into the new CEX Configuration Set, allowing you to easily create a new CEX Configuration Set that needs to have only a few options adjusted.

CEX Parameters

Application Ids and Types (Authentication or Accounting) and Vendor Ids for Vendor Specific Application Ids can be configured on the CEX Parameters GUI pages. The configured CEX Parameters will appear for selection on the GUI pages for configuring CEX Configuration Sets.

Capacity Configuration Sets

Capacity Configuration Sets provide a mechanism for adjusting a connection to account for the network quality of service and Peer Node requirements, and allow management of capacity data for Diameter Peer connections.

Capacity Configuration Set data consists of reserved Ingress MPS, maximum Ingress MPS, Ingress MPS minor alarm threshold, and Ingress MPS major alarm threshold.

The Capacity Configuration Set called Default is always available. The Default Capacity Configuration Set options can be modified, but cannot be deleted. When you create a new Capacity Configuration

Set the values of the Default Capacity Configuration Set are automatically populated into the new Capacity Configuration Set, allowing you to easily create a new Capacity Configuration Set that needs to have only a few options adjusted.

Egress Message Throttling Configuration Sets

Egress Message Throttling Configuration Sets provide a mechanism for managing egress message traffic on a Diameter connection. An Egress Message Throttling Configuration Set can be created with a maximum allowable Egress Message Rate (EMR) and one to three pairs of EMR Threshold Throttles and Abatement Throttles.

Each connection references a single Egress Message Throttling Configuration Set. When the Egress Message Rate on a connection exceeds a Threshold Throttle value, the EMR congestion level for the connection is raised. When the Egress Message Rate on a connection falls below an Abatement Threshold, the EMR congestion level is lowered. Specifying a Convergence time and Abatement time allows control of the transitions between EMR congestion levels. The EMR congestion level, along with the Egress Transport congestion level and the Remote Busy congestion level, is used to control traffic on a connection.

Message Priority Configuration Sets

A Message Priority Configuration Set provides a mechanism for controlling how message priority is set for a request message arriving on a connection. A Message Priority Configuration contains one or more Message Priority Rules.

A Message Priority Rule consists of combination of an Application ID and a Command Code, and a priority. Incoming messages that match the Application ID and Command Code are assigned the associated priority.

Message Priority Configuration Sets can be assigned to connections or Peer Nodes.

Message Copy Configuration Set configuration

A Message Copy Configuration Set provides a mechanism for determining the messages to be copied (Request or Answer), the Result-Code/Experimental Result-Code on which the Message Copy is initiated, and number of retries to be made if the Message Copy attempt to DAS fails.

Local Nodes

A Local Node is a local addressable Diameter entity for the DSR. A Local Node can represent a Diameter client, server, or agent to external Diameter nodes.

A Local Node is a local Diameter node that is specified with a Realm and an FQDN. The DSR supports up to 32 Local Nodes.

Peer Nodes

A Peer Node is an external Diameter client, server, or agent with which the DSR establishes direct transport connections. A Peer Node can be a single computer or a cluster of computers and can support one or more transport connections.

Load Sharing: Peer Nodes

When Peer Nodes have the same priority level a weight (designated as provisioned capacity in the DSR GUI) is assigned to each Peer Node. This defines the weighted distribution of messages among the Peer Nodes. For example, if two Peer Nodes with equal priority have weights of 100 and 150, respectively, then 40% (100/(100+150)) of the messages will be forwarded to the first Peer Node and 60% (150/(100+150)) of the messages will be forward to the second.

Figure 15: Weighted Load Sharing illustrates the concept of weighted load sharing in the DSR.

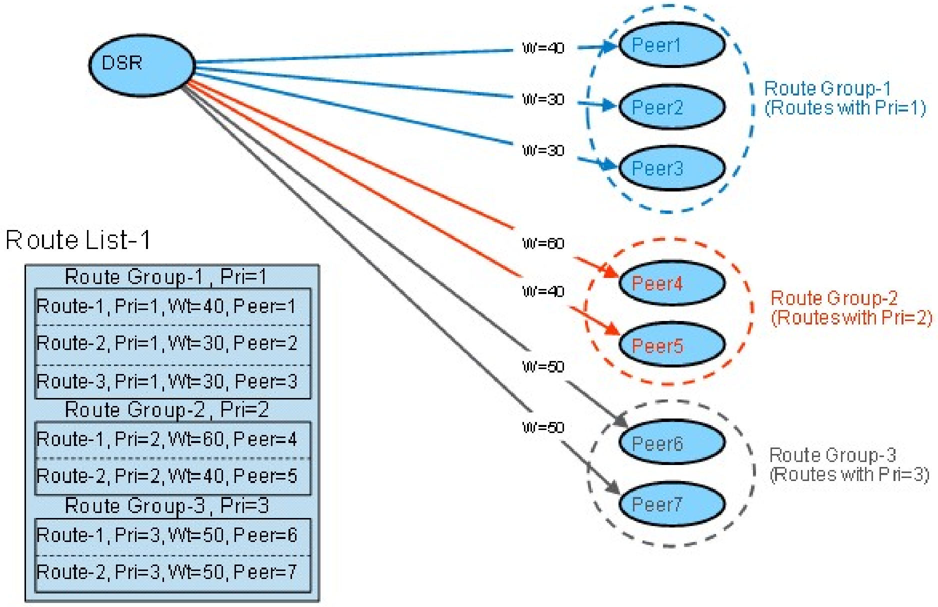


Figure 15: Weighted Load Sharing

Peer Node Group

A Peer Node Group is a collection of DSR peer nodes that cannot tolerate multiple failures within the collection. DSR peer nodes are configured in a **Peer Node Group** container to indicate that connections, which are initiated from peers in the group, are distributed across multiple DA-MPs of an IPFE Target Set. In order for the IPFE to be aware of Peer IP addresses, Peer Nodes in a Peer Node Group must be configured with one or more Peer IP addresses. Target sets can only be configured to support IPFE Initiator Connection support when its DA-MPs listening ports are within the new responder port range.

Connections

A connection provides the reliable transport connectivity between a Local Node and a Peer Node. Connections can use the SCTP or TCP transport protocol. Local Nodes and Peer Nodes respond to connection requests initiated by a Peer Node, and can also be configured to initiate a connection to a Peer Node.

For a given Peer Node, one connection can be configured for each local IP address/transport/listen port combination. For example, if there is a Local Node that supports two IP addresses then you can configure two SCTP connections for the Peer Node - one for each Local Node IP address and listen port.

IPv4 and IPv6

The DSR supports Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) simultaneously for local DSR node addressing. Optionally, either an IPv4 or IPv6 address can be defined for each Diameter connection. The DSR supports both Layer 2 and Layer 3 connectivity at the customer demarcation using 1GB and optionally 10 GB (signaling only) uplinks.

The DSR supports establishing Diameter connections with IPv4 and IPv6 Peers as follows:

- Multiple IPv4 and IPv6 addresses can be hosted simultaneously on a DSR MP.
- Each Diameter Peer connection (SCTP or TCP) configured in the DSR will specify a local DSR node (FQDN) and an associated local IPv4 or IPv6 address set for use when establishing the connection with the Peer.
- Each Diameter Peer connection (SCTP or TCP) configured in the DSR will specify a Peer Node (FQDN) and optionally the Peer Node's IPv4 or IPv6 address set.
- If the Peer Node's IP address set is specified, it must be of the same type (IPv4 or IPv6) as the local DSR IP address set specified for the connection.
- If the Peer Node's IP address set is not specified, DSR will resolve the Peer Node's FQDN to an IPv4 or IPv6 address set by performing a DNS A or AAAA record lookup as appropriate based on the type (IPv4 or IPv6, respectively) of the local DSR IP address set specified for the connection.

The DSR supports IPv4/IPv6 adaptation by allowing connections to be established with IPv4 and IPv6 Diameter Peers simultaneously and allowing Diameter Requests and Answers to be routed between the IPv4 and IPv6 Peers.

Routing Configuration

Routing is provided through the DSR. The DSR functions as a Diameter Relay Agent to forward messages to the appropriate destination based on information contained within the message, including header information and applicable Attribute-Value Pairs (AVP). User-defined Peer Routing Rules define where to route a message to upstream Peer Nodes. The DSR provides the capability to route Diameter messages based on any combination of, or presence or absence of, the following parameters:

- Destination-Realm
- Destination Host
- Application ID
- Command Code
- Origination Realm
- Origination Host
- IMSI

The DSR supports multiple transport connections to each Peer Node and provides the following functions:

- Routing Diameter Request and Answer messages received from Diameter Peers

- Weighted load sharing
- Priority routing
- Rerouting

Configuring DSR routing requires:

1. Creating Route Groups and assigning capacity levels to each Peer Node in each Route Group.
2. Creating Route Lists and defining active and standby Route Groups in each Route List. Active and standby status is determined by Peer Node priority and weight. (See *Load Sharing: Route Groups and Route Lists*.)
3. Creating Peer Routing Rules and assigning Route Lists and priorities to the rules.
4. Creating Message Copy Configuration Sets if Diameter Message Copy is used.

Diameter Routing Functions

Figure 16: DSR Routing Diagram illustrates high-level message processing and routing in the DSR.

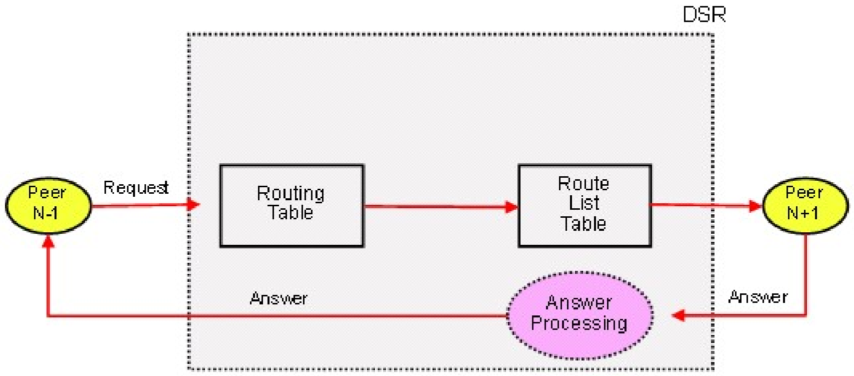


Figure 16: DSR Routing Diagram

The DSR supports the following routing functions:

- Message routing to Diameter Peers based on user-defined message content rules
- Message routing to Diameter Peers based on user-defined priorities and weights
- Message routing to Diameter Peers with multiple transport connections
- Alternate routing on connection failures
- Alternate routing on Pending Answer timeouts
- Alternate routing on user-defined Answer responses
- Route management based on Peer transport connection status changes
- Route management based on OAM configuration changes
- Diameter Message Copy triggered by Peer Routing Rules, Diameter Mediation, or the Charging Proxy Application (CPA)

Load Sharing: Route Groups and Route Lists

The DSR supports the concepts of routes, Route Groups and Route Lists to provide load balancing. A Route List is comprised of a prioritized list of Peer Nodes, organized into Route Groups for routing messages. Each Route List supports the following configurable information:

- The name of the Route List
- Up to 3 Route Groups, each with up to 16 weighted Peer Node IDs
- The priority level (1-3) of each Route Group in the Route List
- The minimum Route Group availability weight for the Route List

A set of Peer Nodes with equal priority within a Route List is called a Route Group. When multiple Route Groups are assigned to a Route List, only one of the Route Groups will be designated as the active Route Group for routing messages for that Route List. The remaining Route Groups in the Route List are referred to as standby Route Groups. The DSR designates the active Route Group in each Route List based on the Route Group's priority and available weight relative to the minimum Route Group availability weight for the Route List. Which Route Group is active at any one time may change when the operational status of Peer Nodes within a Route Group changes or if you change the configuration of either the Route List or the Route Groups in the Route List.

Figure 17: Route List, Route Group, and Peer Node Relationships illustrates the relationships between the Route List, Route Groups, and Peer Nodes.

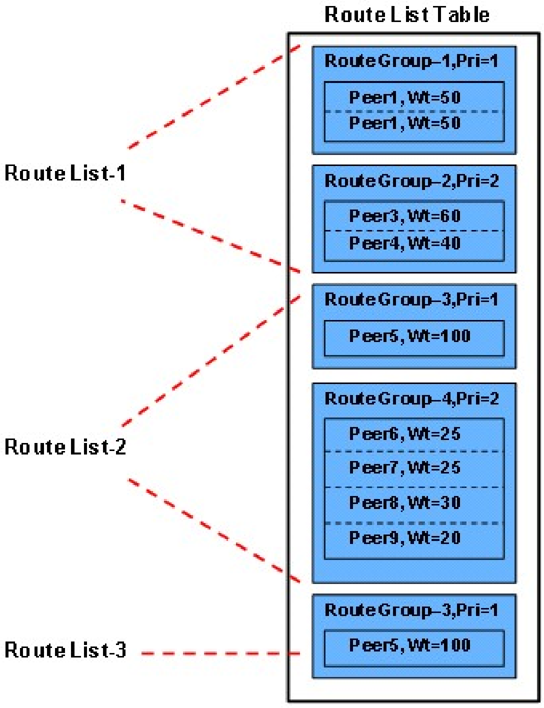


Figure 17: Route List, Route Group, and Peer Node Relationships

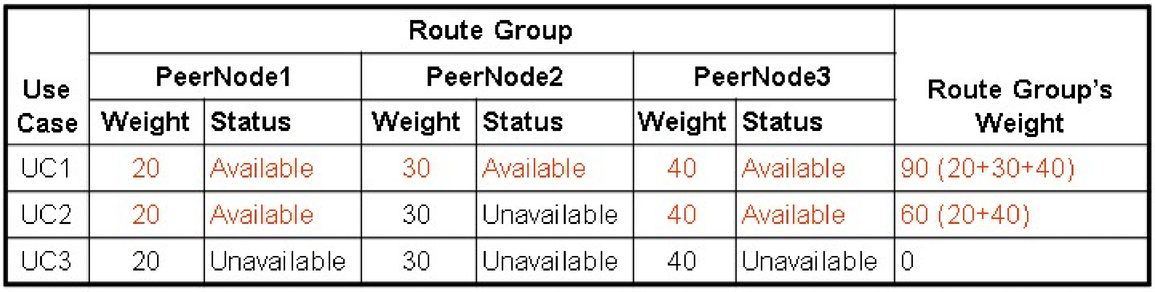
Minimum Route Group Availability Weight

Each Route List is defined by a Minimum Route Group Availability Weight, which is the minimum weight a Route Group is required to have in order to be designated the Active Route Group in a Route List.

The weight of a Route Group is the sum of the weights of its available Peer Nodes. (Peer Node weight is designated as configured capacity in the DSR GUI.) When you assign a minimum Route Group availability weight to a Route List, consider the weights assigned to each Route Group in the Route List. The Route Group with the highest priority and an available capacity that is greater than the Route

List's minimum Route Group availability weight will be selected as the Active Route Group for that Route List.

Figure 18: Route Group Weights illustrates how a Route Group's weight is calculated.



Use Case	Route Group						Route Group's Weight
	PeerNode1		PeerNode2		PeerNode3		
	Weight	Status	Weight	Status	Weight	Status	
UC1	20	Available	30	Available	40	Available	90 (20+30+40)
UC2	20	Available	30	Unavailable	40	Available	60 (20+40)
UC3	20	Unavailable	30	Unavailable	40	Unavailable	0

Figure 18: Route Group Weights

Implicit Routing

When the DSR receives a Request message from a downstream peer, it performs the following functions:

1. Verifies that the DSR has not previously processed the message (message loop detection) by looking for one or more identities in the message's Route-Record AVPs of the message.
2. Searches the Peer Routing Rules based on the contents of the received message to see where to route the message. A Peer Routing Rule can be associated with a Route List that contains a prioritized list of Peer Nodes used to route a Request message.
3. Selects a Peer Node from the Route List that is available for routing the message based on Route Group priorities and Peer Node weights.

If a message does not match a Peer Routing Rule and contains a Destination-Host AVP that is associated with a Peer Node, then the DSR invokes Implicit Routing to the Peer Node if the Peer Node Operational Status is Available.

Diameter configuration for Implicit Routing:

1. Configure each Peer Node.
2. Configure Peer Route Tables.
3. Configure Route Groups.
4. Configure Route Lists.
5. Edit Peer Route Tables and configure Peer Routing Rules in each Peer Route Table.

Peer Routing Rules are primarily intended for Realm-based routing and intra-network routing to non-Peer Nodes. For messages that are addressed to a Peer Node using the Destination-Host AVP, it is not necessary to put explicit Destination-Host entries in a Peer Routing Rule.

Figure 19: DSR Implicit Routing illustrates implicit routing in the DSR.

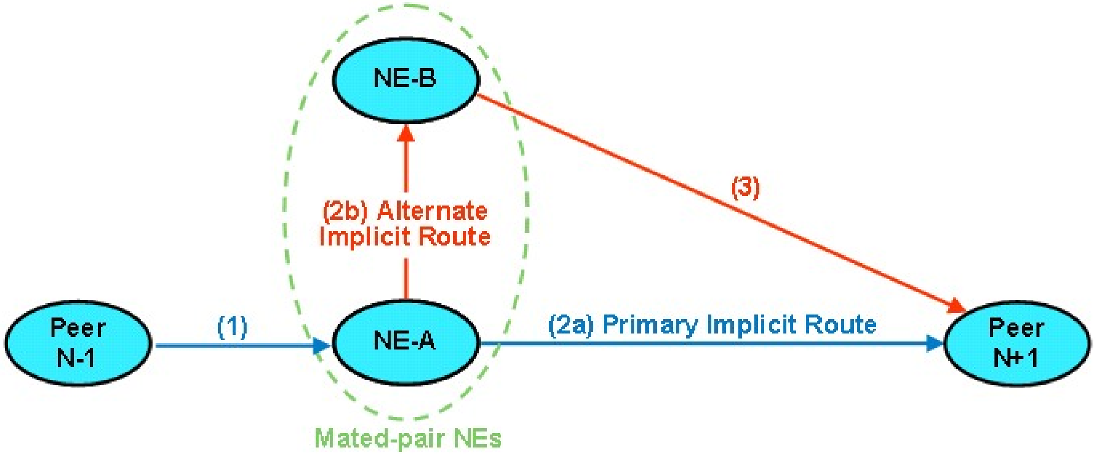


Figure 19: DSR Implicit Routing

Alternate Implicit Routing

Peer Nodes can be configured with an Alternate Implicit Route.

An Alternate Implicit Route is a Route List that specifies an alternate route to use when *Implicit Routing* is invoked and the primary route to the Peer Node is Unavailable.

Alternate Implicit Routing is commonly used to route messages between mated-pair DSR systems.

Diameter configuration of Alternate Implicit Routing:

1. Configure each Peer Node.
2. Configure Route Groups and Route Lists.
3. Edit each configured Peer Node and select a configured Route List for the **Alternate Implicit Routing** element.

Route Group Configuration

A Route Group is a user-configured set of Peer Nodes or connections used to determine the distribution of traffic to each Peer Node in the same Route Group. Traffic is distributed among available Peer Nodes or connections based on the provisioned capacity assignment of each available Peer Node or connection.

For example, if Peer Node A has a provisioned capacity of 100 and Peer Node B has a provisioned capacity of 150, then 40% of the messages sent to the Route Group will be forward to Peer Node A and 60% of the messages will be forward to Peer Node B.

Each Route Group can be assigned a maximum of 160 Peer Nodes or Connections. Route Groups are assigned to Route Lists. See *Route List Configuration*.

Route List Configuration

A Route List is a user-configured set of Route Groups used to determine the distribution of traffic between each Route Group within the Route List. Each Route List can include up to three Route Groups.

Traffic distribution to a Route Group is based on its available capacity and assigned priority within the Route List. A Route Group with a priority of 1 has the highest priority and a Route Group with a priority of 3 has the lowest priority.

Only one Route Group in a Route List is designated as the Active Route Group for routing messages for that Route List. The other Route Groups in the Route List function as Standby Route Groups. The active Route Group in each Route List is determined based on the Route Group's priority and its capacity relative to the provisioned minimum capacity of the Route List.

When the Operational Status of Peer Nodes assigned to the active Route Group changes, or the configuration of either the Route List or Route Groups in the Route List changes, then the designated Active Route Group for the Route List might change.

Route Lists are assigned to Peer Routing Rules. When a Diameter message matches a Peer Routing Rule, the Route List assigned to the Peer Routing Rule will direct the Diameter message to a Peer Node in the active Route Group.

Route Lists are assigned to Message Copy Configuration Sets, to be used for copying a message to a DAS node.

A Route List can be selected for the Alternate Implicit Route element for a Peer Node. The Route List is used to determine the Alternate Implicit Route for a message when an Implicit Route is not available.

Peer Route Tables Configuration

A Peer Route Table is a set of prioritized Peer Routing Rules that define routing to Peer Nodes based on message content.

Peer Routing Rules Configuration

Peer Routing Rules are prioritized lists of user-configured routing rules that define where to route a message to upstream Peer Nodes. Routing is based on message content matching a Peer Routing Rule's conditions. Peer Routing Rules are contained in Peer Route Tables.

When a Diameter message matches the conditions of a Peer Routing Rule then the action specified for the rule will occur. If you choose to route the Diameter message to a Peer Node, the message is sent to a Peer Node in the selected Route List based on the Route Group priority and Peer Node provisioned capacity settings. If you choose to send an answer then the message is not routed and the specified Diameter answer code is returned to the sender.

Peer Routing Rules are assigned a priority in relation to other Peer Routing Rules. A message will be handled based on the highest priority routing rule that it matches. The lower the number a Peer Routing Rule is assigned the higher priority it will have. (1 is highest priority and 99 is lowest priority.)

If a message does not match any of the Peer Routing Rules and the Destination-Host parameter contains a Fully Qualified Domain Name (FQDN) matching a Peer Node, then the message will be directly routed to that Peer Node if it has an available connection. If there is not an available connection the message will be routed using the Alternate Implicit Route provisioned for the Peer Node.

A Message Copy Configuration Set can be assigned to a Peer Routing Rule, to provide information for sending a copy of the message to a DAS.

Egress Throttle Groups

Egress Throttle Groups are used to monitor egress Request rate and pending transactions for multiple Peers and Connections across multiple DA-MPs in a DSR.

Egress Throttle Group Rate Limiting is used to control the total egress Request traffic rate that a DSR will route to a configured group of Peers or Connections.

Egress Throttle Group Pending Transaction Limiting is used to control the total number of transactions that a DSR will allow to be pending for a configured group of Peers or Connections.

The Egress Throttle Group Rate Limiting and Egress Throttle Group Pending Transaction Limiting provide DSR egress throttling capability that enables:

- A group of Peers and Connections to be associated with an Egress Throttle Group
- The maximum egress Request rate of Egress Throttle Groups to be set
- The maximum pending transaction limit of Egress Throttle Groups to be set

Reroute On Answer

Reroute On Answer allows configuration of rerouting scenarios based on the Application ID and Result-Code AVP values in Answer messages. If the values in the message match a configured order pair of Application ID and Result-Code AVP values, the message can be rerouted to another available connection or Peer Node from the Peer Route Group selected during the routing process.

If there are no additional available Peer Nodes in the selected Route Group, or the maximum number of transmits has been met, then reroute is not attempted and the Answer is sent back to the originator.

Diameter configuration for each Reroute on Answer Result-Code AVP:

1. On the **Diameter Configuration Reroute On Answer** GUI,
    a. Enter the **Answer Result-Code AVP Value**.
    b. If Reroute On Answer is to be triggered by a specific Application Id and Result-Code AVP pair, select the **Application Id** for the specified AVP.
    c. If Reroute On Answer is to be triggered for all available Application Ids for a Result-Code AVP, do not select an **Application Id**.
2. Configure Peer Nodes.
    a. **Alternate Routing on Answer Timeout**
        - Select **Same Peer** to perform alternate routing on alternate connections on the same Peer before selecting the next eligible Peer in the Peer Route Group.
        - Select **Same Connection** perform alternate routing on the same connection on the same Peer before selecting the next eligible Peer in the Peer Route Group.
        - Select **Different Peer** to perform routing on a different Peer in the Peer Route Group.

    b. **Alternate Routing on Answer Result Code**
        - Select **Same Peer** to perform alternate routing on alternate connections on the same Peer before selecting the next eligible Peer in a Peer Route Group when a Reroute on Answer Result Code occurs.
        - Select **Different Peer** to perform routing on different Peer in the Peer Route Group.

3. Configure Route Groups as Peer Route Groups (not Connection Route Groups).
4. Configure Pending Answer Timers

   A *Pending Answer Timer* can be configured and assigned to each Application Id and Peer Node. The timer expiration can be used to trigger Reroute on Answer rerouting of a message.

Application Routing Rules Configuration

An Application Routing Rule defines message routing to a DSR Application based on message content matching the following parameters in the Application Routing Rule's Conditions:

- Destination-Realm
- Destination-Host
- Application-Id
- Command-Code
- Origin-Realm
- Origin-Host

When a Diameter message matches the conditions of an Application Routing Rule then message is routed to the DSR Application specified in the rule.

Application Routing Rules are assigned a priority in relation to other Application Routing Rules. A message will be handled based on the highest priority routing rule that it matches. The lower the number an Application Routing Rule is assigned the higher priority it will have. (1 is highest priority and 99 is lowest priority.)

Routing Option Sets Configuration

A Routing Option Set is a collection of Routing Options that are used when a Request message is received to control the number of times an application can forward the request message and how certain delivery error situations are handled.

A Routing Option Set can be associated with the Peer Node that the Request is received from, or with the Diameter Application Id contained in the Request message header. If Routing Option Sets are associated with both the Peer Node and the Application Id, the one associated with the Peer Node takes precedence. If neither the Peer Node nor the Application Id have an associated Routing Option Set, then the Default Routing Option Set is used.

Pending Answer Timer

A Pending Answer Timer limits the time that Diameter will wait for an Answer response after forwarding a Request message to an upstream Peer Node. The timer is started when Diameter queues a Request message for forwarding on a Diameter connection, and the timer is stopped when an Answer response to the message is received by Diameter.

When the time limit is exceeded, Diameter will invoke one of the following methods of message rerouting:

- *Implicit Routing*
- *Alternate Implicit Routing*
- *Reroute On Answer*

One or more Pending Answer Timers can be configured; each Pending Answer Timer can be configured to be assigned to an egress Peer Node to be used for a forwarded transaction. The Default Pending Answer Timer, is available to be used if no other Pending Answer Timer selection rule takes precedence.

In many cases, the Pending Answer Timer used by DSR is based on Diameter client response time requirements. Different Diameter clients for a single Application-ID can have differing response time requirements. The DSR Pending Answer Timer can be controlled based on Ingress Peer Node.

A Pending Answer Timer can be associated with:

- The Peer Node that the Request is sent to
- The configured Diameter Application Id that is contained in the Request message header
- A Routing Option Set

If Pending Answer Timers are associated with both the Peer Node and the Application Id, the one associated with the Peer Node takes precedence. If neither the Peer Node nor the Application Id have an associated Pending Answer Timer, then the Default Pending Answer Timer is used.

When forwarding a Request upstream, the Diameter Routing Function determines the Pending Answer Timer to be used as follows:

- If a Routing Option Set is configured for the Ingress Peer Node and Pending Answer Timer is configured in the Routing Option Set

  Use Ingress Peer Node Routing Option Set Pending Answer Timer
- Else If a Pending Answer Timer is configured for the Egress Peer Node

  Use Egress Peer Node Pending Answer Timer
- Else If a configured Application-ID exists for the Application-ID in the Request

  Use Application-ID Pending Answer Timer
- Else

  Use the system Default Pending Answer Timer

Diameter Options Configuration

The DSR provides GUI pages for configuring the following types of options:

- System Options
- DNS Options

System Options Configuration

The following three types of Diameter System Options can be displayed and edited:

- General Options
  - The maximum Diameter message size allowed
  - Per Connection Egress Message Throttling - Enabled or Disabled

  - IPFE Connection Reserved Ingress MPS Scaling - % of DA-MP Engineered Ingress MPS used by each DA-MP when validating the Reserved Ingress MPS for a newly received IPFE connection
- Alarm Threshold Options -
  - Available Alarm Budget
  - Aggregation alarm thresholds for Fixed Connections, Floating (IPFE) Connections, Peer Nodes, and Route Lists.
- Message Copy Options
  - Message Copy Feature - Enabled, Disabled
  - Message Congestion Level, at or above which Message Copy functions are disabled

    Note: Options specific to Message Copy are configured in Message Copy Configuration Sets.

DNS Options Configuration

The **Diameter Configuration DNS Options** page allows you to set the length of time the application will wait for queries from the Domain Name System (DNS) server. You can also provide an IP address for the primary and secondary DNS servers.

Diameter Common Configuration Overview

References:

The following documents describe Diameter Common Configuration components, provide configuration procedures, and list the sequence in which to perform the configuration of the components.

- *Diameter Common User's Guide*
- **Help** > **Diameter Common**

The *Diameter Common User's Guide* and Help provide information about how to use the Diameter Common GUI pages to configure Network Identifiers and MP Profiles, and how to export and import configuration data for Diameter, Diameter Common, IPFE, MAP-Diameter Interworking, and DSR Applications.

The Diameter Common GUI pages perform configuration and DSR Bulk Import/Export tasks.

Diameter Common on the NOAM

The Diameter Common menu items on the NOAM provide access to GUI pages to perform the following tasks:

- Configure Diameter Common > Network Identifiers >MCCMNC
- Configure Diameter Common > Network Identifiers >MCCMNC Mapping
- Perform DSR Bulk Import/Export operations (see *DSR Bulk Import and Export*)

MCCMNC Mapping

MCCMNC Mapping is used to configure mapping of MCC+MNC combinations to Diameter Realms, MSIN prefix digits, and CC+NDC combinations.

The MCC+MNC combinations must first be configured using the MCCMNC GUI pages before the MCCMNC Mapping configuration is performed.

Diameter Common on the SOAM

The Diameter Common menu items on the SOAM provide access to GUI pages to perform the following tasks:

- Configure Diameter Common > Network Identifiers >MCC Ranges
- Configure Diameter Common > MPs > Profiles and Diameter Common > MPs > Profile Assignments
- Perform DSR Bulk Import/Export operations (see *DSR Bulk Import and Export*)

MCC Ranges

The MCC Ranges component defines up to 10 distinct, non-overlapping Mobile Country Code (MCC) Ranges, which are the first 3 digits of the IMSI. The FABR and RBAR applications consider an IMSI to be invalid for address lookup if the MCC portion of the decoded IMSI falls within any of the Reserved MCC Range configured by the user.

MPs

A Diameter Agent Message Processor (DA-MP) is a computer or blade hosting the Diameter base protocol and one or more DSR Applications. Multiple DA-MPs are supported in a DSR system.

An SS7 Message Processor (SS7-MP) is a computer or blade hosting the MD-IWF SS7/TCAP Application that is used in translating MAP Request messages to Diameter Request messages.

Troubleshooting with IDIH Overview

References:

- *Integrated DIH User's Guide*
- **Help** > **Diameter** > **Troubleshooting with IDIH**

The IDIH feature allows you to capture detailed information about selected DIAMETER transactions, and transmit this information to IDIH for further analysis. The integration of troubleshooting capabilities provided in the DSR provides a way to troubleshoot issues that might be identified with the Diameter traffic that transits the DSR. These troubleshooting capabilities can supplement other network monitoring functions provided by the OSS and network support centers to help to identify the cause of signaling issues associated with connections, peer signaling nodes, or individual subscribers.

AVP Dictionary Overview

References:

- *Diameter User's Guide*
- **Help** > **Diameter** > **AVP Dictionary**

The AVP Dictionary function provides the ability to work with Attribute-Value Pairs (AVPs) that are used by the Diameter Routing Function in making decisions for routing messages to and from applications and for the Diameter Message Copy feature.

The cloning function allows operators to edit the base AVP and puts the modified AVP in Custom Dictionary. The AVPs in Custom Dictionary supersede Base Dictionary AVPs.

The cloning function is available from the following pages:

- **Diameter > AVP Dictionary > Base Dictionary**
- **Diameter > AVP Dictionary > Custom Dictionary**
- **Diameter > AVP Dictionary > All-AVP Dictionary**

Base Dictionary

References:

- *Diameter User's Guide*
- **Help** > **Diameter** > **AVP Dictionary** > **Base Dictionary**

The Base Dictionary allows you to view or clone the basic AVPs that are familiar to the system (defined in the Base Diameter Standard and in Diameter Applications, such as Diameter Credit Control Application and S6a interface). The cloning function allows you to update the base AVP by specifying it once more in the Custom Dictionary.

The AVP Attribute Name, AVP Code, AVP Flag settings, Vendor ID, Data Type, and Protocol are included in the AVP definition.

If the Data Type is Enumerated, the name of the Enumerated Type is also included.

Proprietary and additional standard AVP definitions can be added in the Custom Dictionary.

Custom Dictionary

References:

- *Diameter User's Guide*
- **Help** > **Diameter** > **AVP Dictionary** > **Custom Dictionary**

The **Diameter > AVP Dictionary > Custom Dictionary** page displays all proprietary AVPs defined by the operator in the system. Base Dictionary AVPs are not displayed in the Custom Dictionary list.

AVP names that are defined in the dictionary can be used in creating Rule Templates and in provisioning Rule Sets.

The Attribute Name, AVP Code, AVP Flag settings, Vendor ID, Data Type, and Protocol must be specified in the AVP definition.

If the Data Type is Enumerated, the name of the Enumerated Type is also included.

If the Data Type is Grouped, the list of Grouped AVPs appears in the dictionary.

The Custom Dictionary allows the operator to:

- Add new proprietary AVPs and additional standard AVPs familiar to the system

- Overwrite AVP definitions in the Base Dictionary, by specifying them in the Custom Dictionary with a different definition. The AVP Code, Vendor ID, and Attribute Name must remain the same in the changed definition.

  If the Attribute Name of an AVP appears in both the Base and Custom Dictionaries, the Custom Dictionary definition is used when the AVP is selected in Rule Template Actions and Conditions.

- Clone AVPs.

All-AVP Dictionary

References:

- *Diameter User's Guide*
- **Help** > **Diameter** > **AVP Dictionary** > **All-AVP Dictionary**

The All-AVP Dictionary allows the operator to view all AVP entries that are in the Base and Custom Dictionaries. The Base Dictionary entries are black and the Custom Dictionary entries are blue. (The term "AVP Dictionary" refers to the combined contents of the Base and Custom Dictionaries.)

If a Base Dictionary AVP has been overwritten in the Custom Dictionary, only the Custom Dictionary entry is shown in the All-AVP Dictionary list.

The list and the entries cannot be changed from this page.

Proprietary and additional standard AVP definitions can be added in the Custom Dictionary.

The AVP definitions in the Base Dictionary can be changed (overwritten) by specifying them in the Custom Dictionary with a different definition. The code, Vendor ID, and attribute name must remain the same in the changed definition.

Vendors

References:

- *Diameter User's Guide*
- **Help** > **Diameter** > **AVP Dictionary** > **Vendors**

The Vendors page lists the Names and IDs of all Vendors made known to the system.

Vendors are used in defining new Vendor-specific AVPs in the Custom Dictionary.

Diameter Mediation Configuration Overview

References:

- *Diameter Mediation User's Guide*
- **Help** > **Diameter > Mediation**

The Diameter Mediation feature and its Administration privileges must be activated in the system before all of the Diameter Mediation GUI pages are available for configuring Diameter Mediation components. The Administrator privileges can be deactivated later, so that the Rule Templates folder does not appear under the Mediation folder. This prevents unauthorized modification of the created Rule Templates in the system.

Diameter message mediation helps to solve interoperability issues. Mediation uses rules to manipulate header parts and Attribute-Value Pairs (AVPs) in incoming routable messages and peer to peer messages, when data in the message matches some specified conditions at a specified point of message processing. Tasks of the "if condition matches, then do some action" type can be solved in the most efficient way.

The Diameter Mediation feature can make the routable decisions of send reply, drop the message or set the destination-realm.

Mediation Rule Templates are created to define the Conditions that must be matched in a message and the Actions that are applied to modify the message on the routing decisions. After a Rule Template definition is complete, a Rule Set can be generated from the Rule Template. The data needed for the Conditions and the Actions is provisioned in the generated Rule Set.

A Mediation rule is an instance of the data needed for the execution of Mediation logic. The actual data needed for the Conditions and the Actions is provisioned in one or more rules in the generated Rule Set.

The Rule Sets interface is used primarily for the provisioning of rules and actual data in Rule Sets.

Rule Sets can be associated with pre-defined Request or Answer Trigger Points in the DSR message processing logic. When message processing reaches a Trigger point and the Conditions in an associated Rule Set are met, the Actions for that Rule Set are applied to the message. The changes to the message content can result in modifying the message processing behavior and the routing decision at that Trigger point in the processing logic.

The available Diameter Mediation Triggers are Diameter Routing Functions, Diameter Connection Functions and Application Functions.

Chapter 4

DSR Applications Configuration

Topics:

This chapter contains an overview of the configuration for the following DSR Applications:

- Full Address Based Resolution (FABR)
- Range Based Address Resolution (RBAR)
- Charging Proxy Application (CPA)
- Policy and Charging Application (PCA)
- Gateway Location Application (GLA)

DSR Applications Configuration Overview

References:

- Users' Guides and Help for the configuration of the DSR Applications (FABR, RBAR, CPA, PCA and GLA)
- *Diameter User's Guide*
- **Help** > **Diameter** > **Configuration**

In addition to functioning as a Diameter Relay Agent to route messages to upstream Peer Nodes, the DSR can be configured with Diameter Application Ids and Application Routing Rules to forward messages a specific DSR Application. Each application performs message precessing using specific Diameter interfaces and its own configuration data.

Configuration for DSR Applications can include:

- OAM configuration, including servers and server groups
- Communication Agent (ComAgent) configuration (FABR requires specific ComAgent configuration)
- Configuration of Diameter components that is specific to the functions that the DSR Applications perform
- Configuration on the NOAM or SOAM, or both, of DSR Application components

The Users' Guides and Help for DSR Applications include descriptions and procedures for performing activities that are needed before and after the DSR Application configuration is performed. The activities can include:

- Configuration of OAM, ComAgent, and Diameter components
- Enabling the DSR Application and configured Connections
- Verifying the operating status of the DSR system after the configuration is complete

Configuration of Diameter components that is specific to the functions that the DSR Applications perform must include:

- MP Profiles for DA-MPs and SBR servers
- Application Routing Rules

Configuration of Diameter components that is specific to the functions that the DSR Applications perform can include:

- Application Ids for specific Diameter interfaces
- Command Codes
- Peer Nodes
- Local Nodes
- MCCMNC Ranges
- MCCMNC Mapping
- Connections
- CEX Parameters
- Peer Routing Rules

Part IV

Maintenance, Status, and Reports

Topics:

This part describes:

- The maintenance and status information that is available on the Diameter > Maintenance GUI pages.
- The Diagnostics Tool and Report, and the MP Statistics (SCTP) Report, which are available on the Diameter > Reports GUI pages.

Chapter 1

Diameter Maintenance

Topics:

This chapter describes the maintenance and status information that is maintained by the Diameter Routing Function and the Diameter Transport Function for the following Diameter Configuration components, which are used to make egress Request message routing decisions.

- Route Lists
- Route Groups
- Peer Nodes
- Connections
- Egress Throttle Groups
- Applications
- DA-MPs

This chapter also describes:

- The strategy for reporting (merging) status data to the OAM
- How modification of relevant configuration elements can affect the status of a given component

Maintenance and status information is displayed on the **Diameter Maintenance** GUI pages and is used to generate alarms.

Introduction

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Maintenance**

The **Diameter - > Maintenance** GUI pages display maintenance and status information for Route Lists, Route Groups, Peer Nodes, Connections, Egress Throttle Groups, DSR Applications, and DA-MPs.

The **Diameter Maintenance Connections** page also provides functions to enable and disable connections.

The **Diameter Maintenance Applications** page also provides functions to enable and disable DSR Applications.

Diameter Configuration Component Status for Egress Message Routing Decisions

DSR supports multiple instances of the Diameter protocol, each executing on a separate DA-MP. The Diameter Routing Function supports routing of Diameter Requests to Diameter Peer Nodes through Diameter Transport Function instances executing on either the same DA-MP (Intra-DA-MP routing) or an alternate DA-MP (Inter-DA-MP routing) that has connectivity to the given Peer Node.

Each Diameter Transport Function instance is required to share run-time status information for the Diameter connections it controls with all Diameter Routing Function instances.

Similarly, each Diameter Routing Function instance is also required to share Diameter Connection-related events it detects (such as Remote Busy Congestion) with the Diameter Transport Function instance that is controlling the Diameter connection.

Diameter Connection status is shared among all Active DA-MPs in the DSR NE in order for the Ingress DA-MP to intelligently select an egress connection based on the current status.

Diameter egress message routing is based upon a hierarchy of the Diameter Configuration components that are used for making egress message routing decisions.

The Operational Status of a component is based on the lower-level components that are contained in the components and on user-configurable elements:

- The Diameter Routing Function is responsible for maintaining the Operational Status of each Peer.
- The Operational Status of a Peer is an aggregation of status of Diameter Connections of the Peer.
- Changes to the Operational Status of a Peer can affect the Operational Status of any Route Group that has a route associated with the Peer.
- Changes to the Operational Status of a Route Group can affect the Operational Status of any Route List that is associated with the Route Group.
- When the Operational Status of a Diameter connection changes to either Available or Unavailable, the status of any component that is directly or indirectly dependent upon that Diameter connection might need to be changed (Peer Nodes, Route Groups, and Route Lists).

Table 7: Diameter Configuration Component Status Dependencies summarizes the status dependencies of Diameter Configuration components.

Table 7: Diameter Configuration Component Status Dependencies

Diameter Configuration Component	Component Status Dependency	Configuration Element Dependencies
Route List	Peer Route Groups within a Route List Connection Route Groups within a Route List	None
Peer Route Group within a Route List	Peer Nodes within the Peer Route Group	Route List element "Minimum Route Group Availability Weight" Peer Route Group element "Peer Node Provisioned Capacity"
Connection Route Group within a Route List	Diameter Connections within the Connection Route Group	Route List element "Minimum Route Group Availability Weight" Connection Route Group element "Connection Provisioned Capacity"
Peer Node	Diameter Connections	Peer Node element "Minimum Connection Capacity"
Diameter Connection	None	Admin State

Diameter Maintenance and Status Data for Components, DSR Applications, and DA-MPs

This section describes the maintenance pages for Diameter Configuration components, DSR Applications, and DA-MPs.

Route Lists

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Maintenance** > **Route Lists**

The Route List maintenance and status data is derived from the current Operational Status of Route Groups assigned to a given Route List.

The Diameter Routing Function maintains the Operational Status of each Route List. The status determines whether the Route List can be used for egress routing of Request messages, as follows:

- **Available**: Any Request message can be routed with this Route List .

- **Unavailable**: No Request message can be routed with this Route List

  When a Route List is selected for routing a Request message by a Peer Routing Rule and the Route List's Operation Status is Unavailable, the Diameter Routing Function abandons transaction processing and sends an Answer response.

This information can be used to determine if changes need to be made to the Peer Routing Rules Route List assignments to better facilitate Diameter message routing. Additionally, this information is useful for troubleshooting alarms.

The Route List maintenance and status data is displayed on the **Diameter > Maintenance > Route Lists** GUI page.

Alarms that are active on this Route List (only those alarms that are to be raised and cleared on the OAM) are shown on the **Alarms & Events** GUI page.

Route Groups

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Maintenance** > **Route Groups**

The **Diameter > Maintenance > Route Groups** page displays the provisioned and available capacity for Route Groups and displays information about Peer Nodes or Connections assigned to a Route Group.

This information can be used to determine if changes need to be made to the Peer Node or Connection assignments in a Route Group in order to better facilitate Diameter message routing. Additionally, this information is useful for troubleshooting alarms.

Peer Nodes

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Maintenance** > **Peer Nodes**

The **Diameter > Maintenance > Peer Nodes** page displays the Operational Status of Peer Node connections, including a Reason for the status.

Connections

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Maintenance** > **Connections**

The **Diameter > Maintenance > Connections** page displays information about existing connections, including the Operational Status of each connection.

The **Diameter > Maintenance > Connections** page provides the following functions:

- Enable connections.

- Disable connections.
- View statistics for an SCTP connection.

  The **Connections SCTP Statistics** page displays statistics about paths within an SCTP connection. Each line on the **Connections SCTP Statistics** page represents a path within an SCTP connection.
- Run diagnostics on a test connection.

Egress Throttle Groups

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Maintenance** > **Egress Throttle Groups**

Egress Throttle Groups are used to perform 2 functions: Rate Limiting and Pending Transaction Limiting. Each of the functions is independent of the other and can be optionally configured and controlled separately.

Each function has an individual Administration State (Enable/Disable) and Operational Status (Available, Degraded, or Inactive).

The **Diameter > Maintenance > Egress Throttle Groups** page provides the Operational Status of the Egress Throttle Groups Rate Limiting and Pending Transactions Limiting functions, including an Operational Reason for the status.

Egress Throttle Groups use the Leader sourcing method for reporting of maintenance status. The Leader sourcing method is used because each DA-MP will have identical status data; only the DA-MP Leader will report the maintenance status to the GUI.

If either Rate Limiting or Pending Transaction Limiting Operational Status is Degraded, then the Diameter Routing Function will throttle the Request messages according to highest severity. For example, if Rate Limiting Operational Status is Congestion Level 1 and Pending Transaction Limiting Operational Status is Congestion Level 2 , then the Diameter Routing Function will throttle Request messages according to Congestion Level 2 (all Request messages with Priority 0 or 1 will be throttled).

Applications

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Maintenance** > **Applications**

The **Diameter > Maintenance > Applications** page displays status, state, and congestion information about activated DSR Applications. The data is refreshed every 10 seconds.

If DSR MAP-Diameter InterWorking Function (IWF) is activated, you can view and configure items in the Map Internetworking folder. After activation, all selectable MAP-Diameter IWF related menu items are present on the SOAM and NOAM GUI, which allows full MAP-Diameter IWF configuration and provisioning. By default, MAP Interworking is not activated.

Note: All DSR applications can co-exist on the same DSR , and all DSR applications can run on the same Diameter agents.

The following application limitations exist.

The following applications are mutually exclusive on the same DSR Signaling node:

- Exception - CPA (OFCS) and PDRA
- Exception - GLA is only supported on nodes with PDRA
- Exception - CPA (OFCS) and OC-DRA

The following application combinations are not supported on the same Diameter Agent Server. All are supported with the following exceptions:

- Exception - CPS (OFCS) and PDRA
- Exception - all three of FABR, RBAR and PDRA
- Exception - G6 24G RAM blade does not support DM IWF application
- Exception - Rack mount server in DSR 7.0 does not support PDRA, GLA, FABR, CPA, and OC-DRA

DA-MPs

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Maintenance** > **DA-MPs**

The **Diameter > Maintenance > DA-MPs** page provides state and congestion information about Diameter Agent Message Processors.

Clicking the tabs on the **Diameter > Maintenance > DA-MPs** page displays the following information:

- **Peer DA-MP Status** tab - view peer status information for the DA-MPs.
- **DA-MP Connectivity** tab - view information about connections on the DA-MPs.
- The tab for an individual DA-MP - DA-MP and connection status from the point-of-view of that DA-MP.

Managing the Status of Diameter Configuration Components

Whereas configuration data is sourced at the OAM and replicated down to each DA-MP, status data is sourced at the DA-MP and merged up to the OAM. Most of the status data is displayed on the GUI pages, but some of it is used for other purposes such as alarm generation.

Status data, such as Operational Status, is maintained for each Diameter Configuration component instance. For example, the Operational Status is maintained for each configured Route List instance and for each configured Peer Node instance.

Maintenance and Status Data Sourcing Methods

In merging status data from DA-MPs to the OAM, the status of every configured component instance is merged from a DA-MP to the OAM and multiple DA-MPs will not report the identical status on a given component instance.

Various strategies called “Sourcing Methods” can be used by DA-MPs to merge their status. The sourcing methods are summarized in *Table 8: Maintenance and Status Data Sourcing Methods*.

Table 9: Diameter Configuration Component Sourcing Methods summarizes the Diameter Configuration components used in egress message routing, each Sourcing Method that can be used by each component, and the Diameter Maintenance GUI page where the status is reported.

Table 8: Maintenance and Status Data Sourcing Methods

Sourcing Method	Description	When this Sourcing Method is Used
Report-All	For a given component, all DA-MPs will report status data on any component instances for which it can determine the status.	The component instance status reported by each DA-MP is unique. For example, for the Inter-MP connection status, MP1 and MP2 each have a unique status to report regarding the connection between itself and MP3.
Report-Mine	For a given component, a DA-MP will report its status data on an component instance only if it is directly responsible for managing and owning the component instance.	Each component instance is owned by a single DA-MP. For example, each Fixed connection is owned by a single DA-MP. Each DA-MP will report the status of those connections that it owns.
Leader	One DA-MP is elected Leader. For a given component, only the DA-MP Leader will report status data on instances of the given component .	Each DA-MP has the identical status on each component instance. If each DA-MP were to merge its status data, the OAM would receive identical status from each DA-MP. To avoid this duplication, a DA-MP Leader is elected and only the Leader will report the status.

Table 9: Diameter Configuration Component Sourcing Methods

Diameter Configuration Component Name	Sourcing Method	Diameter GUI Screen (starting from Main Menu : Diameter ->)
Route List	Leader	Maintenance -> Route Lists
Route Group	Leader	Maintenance -> Route Lists **Note:** A Route Group has a status only within the context of a Route List
Peer Node	Leader	Maintenance -> Peer Nodes
Fixed Connection	Report-Mine	Maintenance -> Connections
Floating Connection	Report-Mine / Leader	Maintenance -> Connections

Diameter Configuration Component Name	Sourcing Method	Diameter GUI Screen (starting from Main Menu : Diameter ->)
DSR Application	Report-All	Maintenance -> Applications
DA-MP	Report-All	Maintenance -> DA-MPs DA-MP Status data is shown on the "Peer DA-MP Status" tab. DA-MP Peer Status data is shown on multiple tabs, one for each Peer DA-MP (tab name is the Hostname of the Peer DA-MP)

DA-MP Leader

Maintenance and status data is maintained by DA-MPs for each Diameter Configuration component. Some components have a scope that is beyond that of a single DA-MP. Examples are the Route Lists, Route Groups, and Peer Nodes. For these components, every DA-MP will contain the identical status of each component instance.

To avoid duplicate status reporting in a multi-active cluster, the concept of a “DA-MP Leader” has been introduced. (In an Active/Standby system, the Active DA-MP is always the "Leader".) A single DA-MP is elected as the DA-MP Leader; the remaining DA-MPs are Non-Leaders. Only the Leader will merge its status data to the OAM. Non-Leader DA-MPs will maintain up-to-date status in case they become the Leader, but they will not merge their status data to the OAM. This approach is referred to as the “Leader” sourcing method.

If a component does not use the Leader sourcing method, then its modified status is always merged.

The mechanism for electing a DA-MP Leader is to define a “DA-MP Leader” HA policy and resource. Each DA-MP registers for “DA-MP Leader” resource HA notifications. Each DA-MP assumes that it is a Non-Leader when it initializes. A DA-MP is notified of the HA role changes “Leader -> Non-Leader” and “Non-Leader -> Leader”.

Merging of Status to the OAM

For components that use the Leader sourcing method, only the Leader DA-MP merges status data to the OAM for that component. Non-Leader DA-MPs maintain up-to-date component status data (in case they become the Leader), but this data is not merged to the OAM.

Each DA-MP maintains the status of the connections that it owns. Each DA-MP merges its status to the OAM (“Report-Mine” sourcing method). On the OAM, the status records from the DA-MPs are merged into a single status. The OAM contains the status of all connections. Most of the data is then formatted and displayed on the GUI. However some status data is used for other purposes such as alarm generation.

If there is more than one active DA-MP in a cluster, the OAM receives status records from all of the DA-MPs and merges them together.

A MP Server Hostname element indicates to the OAM which DA-MP has merged the given record. The MP Server Hostname element appears on the Diameter Maintenance GUI page for each component.

The status data is merged for DA-MPs to the SOAM and stops there. Status data is not merged to the NOAM.

Multiple DA-MPs Reporting Status of a Given Diameter Configuration Component

Each DA-MP normally reports the status of a non-overlapping set of component instances (as compared to those component instances reported by other DA-MPs). No two DA-MPs report the status of the identical component instance. For example, every DA-MP reports the status of those Fixed Connections that it owns (a Fixed Connection is owned by a single DA-MP). Two DA-MPs do not report the status of the same Fixed Connection.

However, the following known transient conditions are exceptions, where it is possible for two DA-MPs to temporarily report status on the same component instance. The merged status on the OAM can temporarily contain status for a given component instance from multiple DA-MPs:

- **Duplicate Connection scenario**: A Duplicate Connection scenario can occur where where the same configured connection is established simultaneously on two different DA-MPs, which could be reporting status on the same connection. This situation will be transient, as the Diameter Routing Function will detect the collision and take down one of the connections.

  The Diameter Routing Function instance that is currently controlling the Diameter Connection from an egress Request message routing perspective is defined by the Diameter Connection "Current Location". The Current Location defines the DA-MP that the Diameter Routing Function considers to be the current owner of the connection for the purpose of routing egress Request messages.

  The Diameter Transport Function performs several validations during the Capabilities Exchange procedure to prevent and minimize the occurrence of Duplicate Connection instances.

- **DA-MP Leader Transition**: Assume that DA-MP1 is the Leader, and it is reporting status for a component that uses the "Leader" sourcing strategy. Now assume that DA-MP1 undergoes a non-graceful shutdown (it is not able to clean up its status), and the Leader transitions to DA-MP2. The OAM will detect that DA-MP1 has failed, and discard any status data that was previously reported by DA-MP1. However it is possible that DA-MP2 will take over as Leader and begin merging status data to the OAM before OAM has detected that DA-MP1 has failed.

Ownership of Diameter Connections

The DSR supports two types of connections:

- Fixed Connection
- Floating Connection (the only type of floating connection is an IPFE connection)

A fixed connection is assigned to one and only one DA-MP by the operator at configuration time. This DA-MP owns the connection, and is responsible for maintaining the connection status and merging the status to the OAM.

An IPFE floating connection is implicitly assigned to a set of DA-MPs through the IPFE Target Set Address (TSA) assigned to the connection. The location of the connection is unknown until the connection is established on one of the DA-MP location candidates.

If a floating connection has not been established on a DA-MP, then no DA-MP owns it. However, the status of non-established floating connections is reported to the OAM. The DA-MP Leader is responsible for reporting the status of non-established floating connections to the OAM. The DA-MP Leader is referred to as the "owner" of non-established floating connections, only in terms of status reporting responsibility. The DA-MP Leader can own a non-established IPFE connection even if the Leader is not part of the IPFE TSA.

After a floating connection is established, the DA-MP Leader relinquishes ownership and the DA-MP where the connection is established takes over ownership. If an established connection is taken down, then ownership transfers back to the DA-MP Leader.

Raising and Clearing Alarms

For some alarms, the fault condition will be detected on the DA-MP but the alarm will actually be raised and cleared on the OAM. The OAM also has the ability to roll up multiple alarms into a single aggregate alarm.

For alarms that are raised and cleared on the OAM, the DA-MP for the given Diameter Configuration component maintains a list of alarms corresponding to the faults that have been detected on the component instance. Alarms are raised and cleared as follows:

- Raising an alarm
    1. For a given component instance, a fault condition is detected on the DA-MP.
    2. The status is merged to the OAM.
    3. The OAM looks at the set of active alarms on the given component instance.
        - If the detected alarm condition is not currently active, the OAM will normally raise the alarm. However there could be some circumstances where the alarm is not raised; for example if an aggregate alarm is currently raised, it could mask an individual alarm.
        - If an alarm is already active for the detected condition, then no action is taken by the OAM on that alarm.
- Clearing an alarm:
    1. For a given component instance, the clearing of a fault condition is detected on the DA-MP.
    2. The status is merged to the OAM.
    3. The OAM looks at the set of active alarms on the given component instance.

       If an alarm is currently active for the detected condition, the OAM clears the alarm.

Chapter 2

Diameter Reports

Topics:

Diameter Reports GUIs provide access to the following Diameter functions:

- The DSR Diagnostics Tool provides the capability to test Diameter Mediation Rule Templates that are in "Test" or "Active" state before they are subjected to live traffic in the network.
- MP Statistics (SCTP) displays the Message Processor (MP) SCTP statistics per MP, for all MPs or for a selected set of MPs. Each row shows the statistics for one MP.

Diameter Diagnostics Tool

References:

- *Diameter User's Guide*
- **Help** > **Diameter** > **Maintenance** > **Connections**
- **Help** > **Diameter** > **Reports** > **Diagnostics Tool**

The DSR Diagnostics Tool provides the capability to test Mediation Rule Templates that are in "Test" or "Active" state before they are subjected to live traffic in the network.

The Rule Templates are tested for a message that is injected into a connection that is set to Test Mode. A connection can be set to Test Mode only when it is created; an existing non-test connection cannot be changed into a test connection. A maximum of two test connections can exist in the system at one time.

All incoming messages on a test connection are marked as TestMode messages. When the **Diagnose Start** button is clicked on the **Maintenance Connection** page, TestMode messages are sent on a test connection that is selected, in Test Mode, and not Disabled.

At various trace points, the DSR Diagnostics Tool logs the Rules that are applied, actions taken, and other diagnostic information on a test message that is injected into the system. Reports are provided that are based on the logs. Logging begins when the **Diagnose Start** button is clicked. The test can be stopped by clicking the **Diagnose Stop** button on the **Maintenance Connection** page.

Diameter MP Statistics (SCTP) Report

References:

- *Diameter User 's Guide*
- **Help** > **Diameter** > **Reports** > **MP Statistics (SCTP) Reports**

The **Diameter > Maintenance > MP Statistics (SCTP) Reports** GUI page displays the Message Processor (MP) SCTP statistics per MP, for all MPs or for a selected set of MPs. Each row shows the statistics for one MP.

The statistics must be updated on the page by clicking the **Update** button; the counts are not refreshed automatically.

Part V

Tools and Utilities

Topics:

This part describes:

- Imports and Exports
- IPsec for secure connections
- Diameter Intelligence Hub (DIH)
- Database Backups and Restores

Chapter 1

Imports and Exports

Topics:

The DSR provides functions to export data in files to a location outside the system, and import the files (usually edited) into the system where the Import function is executed. The following Import and Export functions are provided:

- DSR Bulk Import and Export for Diameter, IPFE, and DSR Application Configuration data
- Diameter Mediation Rule Template Export and Import

DSR Bulk Import and Export

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

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

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

DSR Bulk Import

The DSR Bulk Import operations use configuration data in ASCII Comma-Separated Values (CSV) files (.csv), to insert new data into, update existing data in, or delete existing data from the 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 DSR Bulk Export operation, or can be manually created using a text editor.

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

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

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

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

The following Import operations can be performed:

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

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

DSR Bulk Export

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

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

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

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

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

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

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

Diameter Mediation Import and Export

This section describes the import and export functions for Diameter Mediation Rule Templates and Rules.

Import and Export Rules Templates

References:

- *Diameter Mediation User 's Guide*.
- **Help** > **Diameter** > **Diameter Mediation** > **Rule Templates**

The Diameter Mediation Export and Import functions allow a Rule Template to be exported to a file in the form of an .xml file and imported from the file to a system for testing in a lab environment or enabling for live traffic.

The Mediation version in a file selected for importing must be compatible with the release of the DSR into which the file is imported.

Mediation Rule Template Export

A Rule Template can be exported from within the DSR to an external location, such as a hard drive or a memory stick.

The selected file is saved in .xml format, and contains the following information:

- The Rule Template without any provisioned Rules data

- All of the Enumeration Type definitions with the possible values to which the Rule Template refers
- Mediation version number
- Help pages related to the Rule Template

Mediation Rule Template Import

A Rule Template can be imported into the DSR system from a location outside of the DSR file system (stored on the local computer), using the Import function on the **Diameter > Mediation > Rule Templates** page or the **Diameter > Mediation > State & Properties** page.

Existing Rule Templates can be imported. Existing Rule Templates are previously generated Rule Templates that have been exported from Diameter Mediation using the Export function on the **Diameter > Mediation > Rule Templates** page.

A successfully imported Rule Template file appears in the list on the **Diameter > Mediation > Rule Templates** page, in the list on the **Diameter > Mediation > State & Properties** page, and as a Rule Set in the **Diameter > Mediation > Rule Sets** menu folder.

The imported Rule Template is automatically set to the "Test" state.

The Enumeration Types that are used in the Rule Template are imported, if they do not already exist in the system.

If the selected Rule Template references another Rule Template (as an "Execute Rule Template" action) that is not already present in the system, the referenced Rule Template is also imported (unless there is already a Rule Template with the same Name but a different definition).

Export and Import Rules

References:

- *Diameter Mediation User 's Guide*.
- **Help** > **Diameter Mediation** > **Rule Sets** > **{name} [Export]** or **{name} Import**.

The Import and Export Rules function is for the operator to import and export all mediation rules associated with a template. Rules associated with a template can be imported or exported from the corresponding template screen in the Rule Sets menu. Exported Rule Sets are packaged in .xml format rules are validated rule by rule during the import process.

The rules import process will automatically match up conditions based on condition names and matches actions based on action type. If the target template differs from the source template in the number of conditions or types of conditions, the operator may have to manually edit the exported .xml file to include the values for the newly added condition. If the exported .xml file does not values for the newly added condition, the default values populated for the condition in the template are used during the import.

Similarly, the rules import process will also be able to match on the Actions based on "Action types" but deleting an action or modifying an action in the target template may require the operator to manually edit the exported xml file before the rules can be imported. If new actions are added in the target template, the default values associated with those actions in the template are used.

The operator will be able to specify on a per Rule Set basis, if the import process should be continued or abandoned when DSR encounters an error with a specific rule during the import process.

Chapter 2

IPsec

Topics:

IPsec is a network layer security protocol used to authenticate and encrypt IP packets. IPsec provides Host-to-Host encrypted connections or Network-to-Network packet tunneling. IPsec will work for both IPv4 and IPv6 connections (except SCTP/IPv6 connections). DSR IPsec uses the Encapsulating Security Payload (ESP) protocol for encryption and authentication.

IPsec Overview

Internet Protocol Security (IPsec) provides network layer security protocols used for authentication , encryption, payload compression, and key exchange. IPsec provides Host-to-Host encrypted connections or Network-to-Network packet tunneling.

Network traffic between two end-points is encrypted and decrypted by authenticated hosts at the end-points, using a shared private key. The shared private key forms a Security Association that can be automatically changed by Security Policies based on traffic volume, expiry time, or other criteria.

IPsec will work for both IPv4 and IPv6.

Note: DSR supports IPsec with an SCTP/IPv6 configuration.

Note: DSR does not support IPsec for IP Front End (IPFE) connections.

Encapsulating Security Payload

DSR IPsec uses the Encapsulating Security Payload (ESP) protocol for encryption and authentication.

The ESP protocol uses encryption algorithms to encrypt either the packet payload or the entire packet, depending on whether IPsec is configured to use transport mode or tunnel mode. When IPsec is in transport mode, the packet payload is encrypted and the IP header is not encrypted. When IPsec is in tunnel mode the packet payload and the original IP header are both encrypted and a new IP header is added.

ESP also provides authentication of the encrypted packets to prevent attacks by ensuring the packet is from the correct source.

Many encryption algorithms use an initialization vector (IV) to encrypt. The IV is used to make each message unique. This makes it more difficult for cryptanalysis attempts to decrypt the ESP.

The supported ESP encryption and authentication algorithms are described in *IPsec IKE and ESP elements*.

Internet Key Exchange

Internet Key Exchange (IKE) is used to exchange secure keys to set up IPsec security associations. There are two versions of IKE: IKEv1 and IKEv2. The following main differences exist between IKEv1 and IKEv2:

- IKEv1
  - Security associations are established in in 8 messages
  - Does not use a Pseudo Random Function
- IKEv2
  - Security associations are established in in 4 messages
  - Uses an increased number of encryption algorithms and authentication transformations
  - Uses a Pseudo Random Function

The encryption algorithms and authentication transformations that are supported for IKE are described in *IPsec IKE and ESP elements*.

racoon - an open source implementation of IKE that is used to exchange keys and set up the IPsec connections. There are two versions of racoon: racoon (which uses only IKEv1) and racoon2 (which can use IKEv1 or IKEv2). Newer implementations of IPsec use racoon2.

IP Compression

IPsec uses IPcomp to compress packets after encryption, to help with efficient handling of large packets.

IPsec Process

When an IPsec connection is configured, Security Polices are created using the IPsec connection configuration files. IPsec uses Security Policies to define whether a packet should be encrypted or not. The Security Policies help determine whether an IPsec procedure is needed for a connection. The Security Polices do not change over time.

After the Security Policies exist and initial network connectivity has been made, the Internet Key Exchange (IKE) process occurs.

IKE operates in two phases.

- Phase 1 acts as an initial handshake and creates the IKE security associations, which are used to determine how to set up an initial secure connection to begin the IPsec security association negotiation.
- In phase 2, the keys are exchanged and the IPsec Security Associations are created. After the IPsec security Associations exist, the IPsec connection setup process is complete. IPsec now knows how to encrypt the packets.

IPsec uses Security Associations to determine which type of encryption algorithm and authentication transportation should be used when creating an IPsec packet, and to apply the correct decryption algorithm when a packet is received. Because security associations change with time, a lifetime parameter is used to force the security associations to expire so that IPsec must renegotiate them.

An IPsec connection can be set up on a virtual IP, which can be used for HA. However, when a switchover occurs and the VIP is added on the new box a SIGHUP is sent to the iked daemon on the newly active box, so that the VIP is under iked management. Also, the switchover will not occur until the security associations have expired and the renegotiation can begin.

IPsec Setup

Adding an IPsec connection also configures it. An existing IPsec connection can edited or deleted, and an IPsec connection can be started (enabled) and stopped (disabled) without having to fully delete the connection.

IPsec setup needs to be performed on each MP that can control the connection.

Note: IPsec should not be enabled on a live connection. Disable a connection before enabling IPsec.

This chapter provides procedures for adding, editing, deleting, enabling, and disabling an IPsec connection.

The following steps refer to procedures for setting up a new IPsec connection:

1. Open platcfg. See *Accessing platcfg*.
2. Add and configure an IPsec connection. See *Adding an IPsec connection*.
   a. Select an IKE version.
   b. Complete the IKE configuration for the IPsec connection.

c. Complete the ESP configuration for the IPsec connection
d. Complete the IPsec connection configuration entries.
e. Wait for the connection to be added.

3. Enable the IPsec connection. See *Enabling and Disabling an IPsec Connection*.
4. Log out of platcfg. (See *Logging out of platcfg*.)

IPsec IKE and ESP elements

Table 10: IPsec IKE and ESP elements describes IPsec IKE and ESP configuration elements and provides default values, if applicable.

Table 10: IPsec IKE and ESP elements

Description	Valid Values	Default
Internet Key Exchange Version	ikev1, ikev2	ikev2
IKE Configuration		
IKE Encryption	aes128_cbc, aes192_cbc, aes256_cbc, 3des_cbc, hmac_md5	aes128_cbc hmac_md5
IKE Authentication	hmac_sha1, aes_xcbc, hmac_md5	hmac_md5
Psuedo Random Runction. This is used for the key exchange only for ikev2.	hmac_sha1, aes_xcbc (ikev2)	-
Diffie-Hellman Group The group number is used to generate the group (group - set of numbers with special algebraic properties) that is used to select keys for the Diffie-Hellman algorithm. The larger the group number, the larger the keys used in the algorithm.	2, 14 (ikev2) 2 (ikev1)	2 (IKEv1) 14 (IKEv2)
IKE SA Lifetime Lifetime of the IKE/IPsec security associations. A correct lifetime value would be <hours/mins/secs>. Example: 3 mins. **Note:** If a connection goes down it will not reestablish until the lifetime expires. If the lifetime is set to 60 minutes and a failure causing a switchover of a VIP is required, the switchover will not occur until the 60 minutes expire. The recommendation is to set the lifetime to the lowest possible time	Number of time units	60

Description	Valid Values	Default
that will not impact network connectivity, such as 3-5 minutes.		
Lifetime Units	hours, mins, secs	mins
Perfiect Forward Secrecy This is an algorithm used to ensure that if one of the private keys is compromised the other keys are not compromised.	yes, no	yes
ESP Configuration		
ESP Authentication Algorithm used to authenticate the encrypted ESP	hmac_sha1, hmac_md5	hmac_sha1
Encryption Encryption Algorithm used to encrypt the actual IPsec packets	aes128_cbc, aes192_cbc, aes256_cbc, 3des_cbc	aes128_cbc

Accessing platcfg

To work with IPsec you need to use the Platform Configuration Utility, platcfg. Platcfg provides a user interface to the Platform Distribution, the core platform underlying the DSR.

Note: You will need the platcfg password to access platcfg. Contact the Customer Care Center if you do not have this password.

Use the following task to access platcfg.

1. Using ssh, open a terminal window to the iLO IP address of the management server.

   Contact your system administrator if you need assistance accessing the management server.
2. Log into the iLO as Administrator.
3. At the iLO command prompt, enter **vsp** to start the virtual serial port feature.

```
</>hpiLO-> vsp

Starting virtual serial port.
Press 'ESC (' to return to the CLI Session.

</>hpiLO-> Virtual Serial Port active: IO=0x03F8 INT=4
```

4. Press ENTER to access the login prompt.

```
CentOS release 5.5 (Final)
Kernel 2.6.18-194.32.1.el5prerel4.2.3_70.83.0 on an x86_64

cfg1-CMP-a login:
```

5. Log into the server as the platcfg user.

   - username: **`platcfg`**
   - password: **`<platcfg_password>`**

   The platcfg **Main Menu** appears.

Adding an IPsec connection

Use this task to add an IPsec connection.

1. Open platcfg.
   See *Accessing platcfg*.
2. Select **Network Configuration**.
3. Select **IPsec Configuration**.
4. Select **IPsec Connections**.
5. Select **Edit.**
6. Select **Add Connection**.
7. Select the Internet Key Exchange Version: either **IKEv1** or **IKEv2**.
8. Complete the **IKE Configuration** fields for the desired connection, then click **OK**.
9. Select the desired **ESP Encryption** algorithm, then click **OK**.
10. Complete the **Add Connection** fields for the desired connection.

    - Enter the **Local Address**.
    - Enter the **Remote Address**.
    - Enter the **Pass Phrase**.
    - Select the **Mode**.

11. Click **OK**.
    Wait for the connection to be added.

    When the connection has been successfully added, the **Internet Key Exchange Version Menu** appears.

12. Select **Exit**.
13. Log out of platdfg.
    See *Logging out of platcfg*.

Editing an IPsec connection

Use this task to edit an IPsec connection.

1. Open platcfg.
   See *Accessing platcfg*.

2. Select **Network Configuration**.
3. Select **IPsec Configuration**.
4. Select **IPsec Connections**.
5. Select **Edit.**
6. Select **Edit Connection**.
7. Select the IPsec connection to edit.
8. View the IPsec connection's current configuration.
9. Select **Edit**.
10. Select either **IKEv1** or **IKEv2**.
11. Change the **IKE Configuration** fields fif needed; then click **OK**.

    The fields are described in *IPsec IKE and ESP elements*.

12. Change the **ESP Configuration**fields if needed; then click **OK**.

    The fields are described in *IPsec IKE and ESP elements*.

13. Complete the **Add Connection** fields for the desired connection.

    - Enter the **Local Address**.
    - Enter the **Remote Address**.
    - Enter the **Pass Phrase**.
    - Select the **Mode**.

14. Click **OK**.
15. Select **Yes** to restart the connection.
    When the connection has been updated, the **Internet Key Exchange Version Menu** appears.
16. Select **Exit**.
17. Log out of platcfg.

    See *Logging out of platcfg*.

Enabling and Disabling an IPsec Connection

Use the following task to enable or disable an IPsec connection.

Note: IPsec should not be enabled on a live connection. Disable a connection before enabling IPsec.

1. Open platcfg.

   See *Accessing platcfg*.

2. Select **Network Configuration**.
3. Select **IPsec Configuration**.
4. Select **IPsec Connections**.
5. Select **Edit.**
6. Select **Connection Control**.
7. Select the IPsec connection to enable or disable.
8. Select **Enable** or **Disable**.

9. Click **OK** to enable or disable the selected IPsec connection.
10. Log out of platdfg.

    See *Logging out of platcfg*.

Deleting an IPsec connection

Use this task to delete an IPsec connection.

1. Open platcfg.

   See *Accessing platcfg*.
2. Select **Network Configuration**.
3. Select **IPsec Configuration**.
4. Select **IPsec Connections**.
5. Select **Edit.**
6. Select **Delete Connection**.
7. Select the IPsec connection to be deleted.
8. Click **Yes** to confirm the delete.
9. Wait for the connection to be deleted.
   When the IPsec connection has been successfully deleted, the **Connection Action Menu** appears.
10. Select **Exit**.
11. Log out of platcfg.

    See *Logging out of platcfg*.

Logging out of platcfg

After working with IPsec connections, use this task to log out of platcfg and the management server interface.

1. If you have not already done so, select **Exit** on the final menu of the IPsec task that you were using for the IPsec connection.
2. To log out of the management server, enter `exit` at the prompt.

```
# exit
cfg1-CMP-a login:
```

3. To end the vsp session, press ESC, then Shift-9.

```
cfg1-CMP-a login: </>hpiLO->
</>hpiLO->
```

4. To log out of the management server iLO, enter `exit`.

```
</>hpiLO-> exit
```

Chapter 3

Integrated Diameter Intelligence Hub

Topics:

The Integrated Diameter Intelligence Hub (IDIH) provides the user to capture detailed information about selected Diameter transactions and transmit this information to IDIH for further analysis. The integration of troubleshooting capabilities into the DSR product provides a high value proposition for customers to be able to troubleshoot issues that might be identified with the Diameter traffic transmitted to the DSR.

These troubleshooting capabilities can supplement other network monitoring functions provided by the customer's OSS and network support centers to help quickly pinpoint the root cause of signaling issues associated with connections, peer signaling nodes, or individual subscribers.

Integrated Diameter Intelligence Hub Overview

References:

- *Integrated DIH User 's Guide*.
- **Help** > **Integrated DIH**

The Integrated Diameter Intelligence Hub (IDIH) provides the ability to filter, access, and troubleshoot Diameter transactions without the need for separate probes or taps. The IDIH provides:

- Allows the user to create and manage trace filters on DSR to capture messages needed for troubleshooting service issues
- Presents traces to the user via the graphical visualization capabilities provided by IDIH
- Allows the user to filter, view, and store the results with IDIH

The IDIH feature allows the user to capture detailed information about selected Diameter transactions and transmit this information to IDIH for further analysis. The integration of troubleshooting capabilities into the DSR product provides a high value proposition for customers to be able to troubleshoot issues that might be identified with the Diameter traffic transmitted to the DSR.

These troubleshooting capabilities can supplement other network monitoring functions provided by the customer's OSS and network support centers to help quickly pinpoint the root cause of signaling issues associated with connections, peer signaling nodes, or individual subscribers.

Note: IDIH is not a replacement of the features in previous DIH releases.

Accessing IDIH

To log into IDIH from DSR SOAM GUI:

1. Using a Web browser, type the FQDN for a DSR SOAM.

   Note: Contact the system administrator for the FQDN Address.

   The login screen opens.
2. Log into the SOAM by typing entering the correct **User Name** and the corresponding **Password**.

   Note: Check with the system administrator for the user name and password.
3. Navigate to **Diameter** > **Troubleshooting with IDIH** > **Maintenance** > **Traces**.
4. Click the **Launch IDIH** button.
5. Alternatively, select a trace and click **Analyze With IDIH** under the **Action** column.

In the absence of a DNS server, the user may authenticate directly on the IDIH server using the "idihtrace" user ID. This user ID provides the same level of functionality as using single sign-on from the SOAM.

The procedure for accessing IDIH with the "idihtrace" user ID is almost the same as for signing in via single sign-on with the exception of replacing **FQDN** with **IP Address** in the above procedure.

Chapter 4

Database Backups and Restores

Topics:

The database contains the configuration information for a DSR deployment.

The ability to restore a DSR database from a database backup file can aid in disaster recovery. We recommend backing up the database on a regular basis, perhaps as part of routine daily operations.

After a backup has been created, the file can be transferred to an external server in a secure location.

Database Backups and Restores

References:

- *Operations, Administration, and Maintenance (OAM) User 's Guide.*
- **Help** > **Operations, Administraction, and maintenance (OAM)** > **Status and Manage** > **Database**

The database contains the configuration information for a DSR deployment.

The ability to restore a DSR database from a database backup file can aid in disaster recovery. Oracle recommends backing up the database on a regular basis, perhaps as part of routine daily operations.

After a backup has been created, the file can be transferred to an external server in a secure location.

Manual Backups

The database backup process allows capturing and preserving vital collections of Configuration data. Data is safely collected from the database management system without impact to database users. The Configuration Data is data used to configure a system and the applications that run in the system.

A backup of data can be performed only from the Active Network OAM&P and can include all Configuration data.

The backup process collects all files required to perform the requested backup and stores them as a single file in the File Management Storage Area. The backup process operates asynchronously from the Status & Manage GUI screens, allowing the user to perform other operations and monitor progress.

The **Status & Manage Database** GUI page provides:

- The ability to disable and enable provisioning system-wide on all servers in the system.
- Access to database functions, such as backing up and restoring a database (and the status of these functions); displaying a database status report; inhibiting and allowing replication; and comparing a database backup to an existing database. With the exceptions of restore and replication, these functions affect a single OAM server only.
- The status of database backups

Before saving the file in the File Management Storage Area, the default filename can be changed. The '.tbz2' file extension cannot be changed. The default name of a backup file has the following format:

```
Backup.<appname>.<hostname>.<groupname>[And<groupname>…[And
<GroupName>]].<NodeType>.YYYYMMDD_HHMMSS.(AUTO | MAN).tbz2
```

Example of a backup file name:

```
Backup.Appworks.teks5001401.Configuration.NOAMP.20090223_031500.MAN.tbz2
```

Although the backup process is designed to be used without interruption to provisioning service, it may be desirable to disable provisioning briefly in order to note exactly which data has and which data has not been provisioned to the network when the backup is taken. Provisioning can be enabled after the backup has started; it is not necessary to wait until the backup is finished to enable provisioning again.

Automatic Backups

Automatic backups are scheduled and are executed for Configuration data on Active Network OAM&P servers. By default, automatic backups for Configuration data are scheduled for 2:45 AM, local time.

Automatically generated backup archive files are stored in the File Management Storage Area. The File Management Storage Area is pruned as part of the automatic backup process to remove any automatic backup archive files that are older than 14 days.

The automatically generated backup archive files include an "AUTO" extension to distinguish them from manually generated backup archive files.

Database Restores

The ability to restore a DSR database from a database backup file can aid in disaster recovery. Oracle recommends backing up the database on a regular basis, perhaps as part of routine daily operations.

Database backup files can be used to restore Configuration data to servers in a network. The very nature of database restoration is destructive. Operators need to take great care to know exactly what data is being restored and how it differs from the existing data.

The Database restoration requires careful planning and execution and taking some sensible precautions. Contact your *My Oracle Support (MOS)* for assistance before attempting a database restore.

The security logs of both the controlled and the controlling server can be checked to determine how a restoration has progressed.

Glossary

A

AAA

Authentication, Authorization, and Accounting (Rx Diameter command)

ACR

Accounting Request

Diameter message type for creating an accounting transaction. An ACR is sent by an IMS network element that describes a stage in the processing of a SIP service.

Application Routing Rule

A set of conditions that control message routing to a DSR application based on message content.

ATP1

Mediation trigger point located immediately after the Diameter Routing Function decodes an ingress Request message received from the Diameter Transport Function.

ATP10

Mediation trigger point located immediately prior to Request message encoding that occurs before forwarding the message to the Diameter Transport Function.

AVP

Attribute-Value Pair

The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as

A

well as authentication, authorization or accounting information.

C

CDF

Charging Data Function

CEA

Capability-Exchange-Answer

The Diameter response that the prepaid rating engine sends to the Mobile Originated application during capability exchanges.

CER

Capabilities-Exchange-Request

A Diameter message that the Mobile Originated application sends to a prepaid rating engine to perform a capability exchange. The CER (indicated by the Command-Code set to 257 and the Command Flags' 'R' bit set) is sent to exchange local capabilities.The prepaid rating engine responds with a Capability-Exchange-Answer (CEA) message.

CEX Configuration Set

A mechanism for assigning Application IDs and supported Vendor IDs to a Local Node or to a Connection.

CPA

Capability Point Code ANSI

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

C

CPF

Charging Proxy Function

A CPF instance is a DSR running the CPA application.

CTF

Charging Trigger Function

D

DA-MP

Diameter Agent Message Processor

A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application such as CPA can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.

DAS

Diameter Application Server

Diameter Agent Server

Diameter

Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.

Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment.

D

Diameter Agent Message Processor

A computer or blade that is hosting the DSR. Multiple instances of the DSR each execute on a separate physical DA-MP. Each instance shares run-time status information with all other instances for the Diameter connections that it controls. In inter-MP routing, an instance can route an ingress Answer message to another instance that performed routing for the corresponding ingress Request message. See DA-MP.

DIH

Diameter Intelligence Hub

A troubleshooting solution for LTE, IMS, and 3G Diameter traffic processed by the DSR. DIH does not require separate probes or taps.

DM-IWF

Diameter –MAP Interworking DSR Application, which translates Diameter messages into MAP messages

DPA

Disconnect-Peer-Answer

A message used by a Diameter node to answer the Disconnect-Peer-Request (DPR).

DPR

Disconnect-Peer-Request

A message used by a Diameter node to inform its peer of its intent to disconnect the transport layer. Upon receipt of a DPR, the Disconnect-Peer-Answer (DPA) is returned.

DSR

Data Set Ready

Diameter Signaling Router

D

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

Delete Subscriber Data Request

DSR Application

Any DSR software feature or function that is developed as a user of the Diameter base protocol.

DWA

Device-Watchdog-Answer

A Diameter message used with the Device-Watchdog-Request (DWR) message to proactively detect connection failures. If no traffic is detected on a connection between the Mobile Originated application and the prepaid rating engine within the configured timeout period, a DWR message is sent to the prepaid rating engine. If the prepaid rating engine fails to respond with a DWA within the required time, the connection is closed with the prepaid rating engine and initiates failover procedures. All new and pending requests are then sent to the secondary server.

DWR

Device-Watchdog-Request

A Diameter message used with the Device-Watchdog-Answer (DWA) message to proactively detect connection failures. If no traffic is detected on a connection between the Mobile Originated application and the Diameter server within the configured timeout period, a DWR message is sent to the Diameter Server. If the Diameter server fails

D

to respond within the required time, the connection is closed with the Diameter server and initiates failover procedures. All new and pending requests are then sent to the secondary Diameter server.

E

EMS

Element Management System

The EMS feature consolidates real-time element management at a single point in the signaling network to reduce ongoing operational expenses and network downtime and provide a higher quality of customer service.

F

FABR

Full Address Based Resolution

Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.

FQDN

Fully qualified domain name

The complete domain name for a specific computer on the Internet (for example, www.oracle.com).

A domain name that specifies its exact location in the tree hierarchy of the DNS.

G

GGA

Get-Gateway-Answer A reply to a GGR. It contains session information for the subscriber present in the GGR. GGA includes the bindings for the subscriber such as, Access Point Name, PCEF

G

FQDN and Creation timestamp. The session information is aggregated in the GGA based on the PCRF to which is it assigned.

GGR

Get-Gateway-Request A request for information for either an IMSI or an MSISDN. Only one subscriber (IMSI or MSISDN) is allowed to be queried per GGR. The GGR is generated by the GQC.

GLA

Gateway Location Application A DSR Application that provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding and session information is populated in the pSBR-B by the Policy Diameter Routing Agent (Policy DRA). GLA provides methods for a Diameter node to query binding information stored in the pSBR-B. The query can be by either IMSI or MSISDN. GLA processes Diameter Requests and generates Diameter Answers.

GQC

Gateway Query Client also known as Diameter Node

GUI

Graphical User Interface

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HA

High Availability

H

High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.

HSS

Home Subscriber Server

A central database for subscriber information.

I

IDIH

Integrated Diameter Intelligence Hub

IMI

Internal Management Interface

IMS

IP Multimedia Subsystem

These are central integration platforms for controlling mobile communications services, customer management and accounting for mobile communications services based on IP. The IMS concept is supported by 3GPP and the UMTS Forum and is designed to provide a wide range of application scenarios for individual and group communication.

IPFE

IP Front End

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

IPsec

Internet Protocol Security

I

A protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a data stream.

IPv4

Internet Protocol version 4

IPv6

Internet Protocol version 6

IWF

InterWorking Function

L

LTE

Long Term Evolution

The next-generation network beyond 3G. In addition to enabling fixed to mobile migrations of Internet applications such as Voice over IP (VoIP), video streaming, music downloading, mobile TV, and many others, LTE networks will also provide the capacity to support an explosion in demand for connectivity from a new generation of consumer devices tailored to those new mobile applications.

M

MAP

Mated Application Part

Mobile Application Part

An application part in SS7 signaling for mobile communications systems.

MCC

Mobile Country Code

A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International

M

Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber. See also MNC, IMSI.

MD-IWF

MAP-Diameter Interworking SS7 Application, which translates MAP messages into Diameter messages

MEAL

Measurements, Events, Alarms, and Logs

MP

Measurement Platform

Message Processor - The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM&P components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.

MTP3

Message Transfer Part, Level 3

N

NE

Network Element

An independent and identifiable piece of equipment closely associated with at least one processor, and within a single location.

In a 2-Tiered DSR OAM system, this includes the NOAM and all MPs underneath it. In a 3-Tiered DSR OAM system, this includes the NOAM, the SOAM, and all MPs associated with the SOAM.

Network Entity

N

NMS

Network Management System

An NMS is typically a standalone device, such as a workstation, that serves as an interface through which a human network manager can monitor and control the network. The NMS usually has a set of management applications (for example, data analysis and fault recovery applications).

NOAM

Network Operations, Administration, and Maintenance

NOAMP

Network Operations, Administration, Maintenance, and Provisioning

O

OAM

Operations, Administration, and Maintenance

The application that operates the Maintenance and Administration Subsystem which controls the operation of many products.

OCS

Online Charging Server

OFCS

Offline Charging Server

OSS

Operations Support System

Computer systems used by telecommunications service providers, supporting processes such as maintaining network inventory, provisioning services, configuring network components, and managing faults.

Operator Specific Services

P

P

PCRF

Policy and Charging Rules Function. The ability to dynamically control access, services, network capacity, and charges in a network.

Maintains rules regarding a subscriber’s use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.

Peer

A Diameter node to which a given Diameter node has a direct transport connection.

Proxy Agent

Performs the basic forwarding functions of a Relay Agent, but unlike a Relay Agent, a Proxy Agent can modify the message content and provide value-added services, enforce rules on different messages, or perform administrative tasks for a specific realm.

R

RBAR

Range Based Address Resolution

A DSR enhanced routing application which allows the user to route Diameter end-to-end transactions based on Application ID, Command Code, “Routing Entity” Type, and Routing Entity address ranges.

RTP1

Mediation trigger point located immediately after the Diameter Routing Function finds a valid PTR associated with the ingress Answer message.

R

RTP10

Mediation trigger point located immediately prior to queuing an Answer message to the Diameter Transport Function.

S

SBR

Subsystem Backup Routing

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

SCTP

Stream Control Transmission Protocol

An IETF transport layer protocol, similar to TCP that sends a message in one operation.

The transport layer for all standard IETF-SIGTRAN protocols.

SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.

SDS

System Debug Services

Subscriber Data Server

Provides new ways of accessing, extracting, and finding value from subscriber data, and thus enables operators to leverage the wealth of subscriber information previously fragmented all over their network. By simplifying the management of subscriber data and profiling customer behavior, the Subscriber Data Server allows carriers to exploit real-time data, deliver

S

monetized personalized services, and even bind to third part services easily.

Subscriber Database Server

Subscriber Database Server (SDS) provides the central provisioning of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query Server and the Data Processor System Operations, Administration, and Maintenance (DP SOAM) servers at each Diameter Signaling Router (DSR) site or a standalone DP site to replicate and recover provisioned data to the associated components.

SNMP

Simple Network Management Protocol.

An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.

SOAM

System Operations, Administration, and Maintenance

Site Operations, Administration, and Maintenance

SS7

Signaling System #7

A communications protocol that allows signaling points in a

S

network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.

T

TCAP

Transaction Capabilities Application Part - A protocol in the SS7 protocol suite that enables the deployment of advanced intelligent network services by supporting non-circuit related information exchange between signaling points using the Signaling Connection Control Part connectionless service. TCAP also supports remote control - ability to invoke features in another remote network switch.

TCP

Transfer-Cluster-Prohibited

Transfer Control Protocol

Transmission Control Protocol

A connection-oriented protocol used by applications on networked hosts to connect to one another and to exchange streams of data in a reliable and in-order manner.

TLS

Transport Layer Security

A cryptographic protocol that provides security for communications over networks such as the Internet. TLS encrypts the segments of network connections at the transport layer end-to-end. TLS is an IETF standards track protocol.

T

TSA

Target Set Address

An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.

V

VIP

Virtual IP Address

Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.

X

XMI

External Management Interface