Oracle® Communications
Diameter Signaling Router

MAP-Diameter Interworking Function User's Guide

E76930 Revision 01

March 2017

ORACLE®

Oracle Communications Diameter Signaling Router MAP-Diameter Interworking Function User's Guide

Copyright © 2014, 2017, Oracle and/or its affiliates. All rights reserved.

Table of Contents

List of Figures

List of Tables

Chapter

1

Introduction

Topics:

This section contains an overview of the available information for the DSR MAP-Diameter Interworking application.

Revision History

Date	Description
July 2016	Initial release

Overview

This document describes the features associated with the MAP-Diameter Interworking Function.

This document will also:

- Provide a conceptual overview of the MAP-Diameter Interworking Function's purpose, architecture, and functionality
- Describe the pages and elements on the MAP-Diameter Interworking Function GUI
- Provide procedures for using the the MAP-Diameter Interworking Function interface
- Explain the organization of and how to use this document

Scope and Audience

This document is intended for anyone responsible for configuring and using the DSR MAP-Diameter Interworking Function. Users of this manual must have a working knowledge of telecommunications and network installations.

Manual Organization

Information in this manual is organized into sections:

- *Introduction*
- *MAP-Diameter IWF Introduction*
- *MAP-Diameter Interworking Function Configuration*
- *MD-IWF Application Configuration*
- *DM-IWF Application Configuration*
- *Maintenance for MD-IWF*
- *Maintenance for DM-IWF*

Documentation Admonishments

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

Table 1: Admonishments

Icon	Description
DANGER	Danger: (This icon and text indicate the possibility of *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*.)
TOPPLE	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Specifications

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

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **Industries**.

3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.

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

Customer Training

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

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

User Interface Organization

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

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

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

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

- Communication Agent
- Diameter Common
- Diameter
- UDR (User Data Repository)
- MAP-Diameter IWF
- RADIUS (Remote Authentication Dial-In User Service)
- SBR (Session Binding Repository)
- Policy and Charging
- DCA (DOIC Capabilities Announcement) Framework

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

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

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

User Interface Elements

Table 2: User Interface Elements describes elements of the user interface.

Table 2: User Interface Elements

Element	Location	Function
Identification Banner	Top bar across the web page	The left side of the banner provides the following information: • Displays the company name, • product name and version, and • the alarm panel. The right side of the banner: • Allows you to pause any software updates. • Links to the online help for all software. • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates 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, date and time, and includes a link to context-sensitive help. • Page Control Area: Located below the Page Title Area, this area shows controls for the Page Area (this area is optional). When available as an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see *Optional Layout Element Toolbar*. • Page Area: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information

Element	Location	Function
		or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Login Message*.
Session Banner	Across the bottom of the web page	The left side of the banner 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 alarm panel.

Main Menu Options

Table 3: 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 do not appear on the screen of a user who does not have administrative privileges.

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

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

Table 3: Main Menu Options

Menu Item	Function
Administration	The Administration menu allows the user to: • General Options. Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Set up and manage user accounts • Configure group permissions • View session information • Manage sign-on certificates • Authorize IP addresses to access the user interface • Configure SFTP user information • View the software versions report • Upgrade management including backup and reporting

Menu Item	Function
	• Authenticate LDAP servers • Configure SNMP trapping services • Configure an export server • Configure DNS elements
Configuration	On the NOAM, allows the user to configure: • Network Elements • Network Devices • Network Routes • Services • Servers • Server Groups • Resource Domains • Places • Place Associations • 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 and Manage	Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, KPIs, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, data, and ISO file management.
Measurements	Allows the user to view and export measurement data.
Transport Manager (optional)	On the SOAM, allows the user to configure adjacent nodes, configuration sets, or transports. A maintenance option allows the user to perform enable, disable, and block actions on the transport entries. This option only appears with the DSR application.
Communication Agent (optional)	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. The user can perform actions to enable, disable, and block connections. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.
SS7/Sigtran (optional)	On the SOAM, allows the user to configure various users, groups, remote signaling points, links, and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data. This option only appears with the DSR application.

Menu Item	Function
Diameter Common (optional)	Allows the user to view or configure: • Dashboard, configure on the NOAM; view on both OAMs • Network Identifiers on the SOAM - MCC Ranges • Network Identifiers on the NOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile Assignments The DSR Bulk Import and Export functions are available on both OAMs for the data configured on that OAM.
Diameter (optional)	Allows the user to configure, modify, and monitor Diameter routing: • On the NOAMP, Diameter Topology Hiding and Egress Throttle List configuration • On the SOAM, Diameter Configuration, Maintenance, Reports, Troubleshooting with IDIH, AVP Dictionary, and Diameter Mediation configuration
UDR (User Data Repository) (optional)	Allows the user to add, edit, store, and manage subscriber and pool data. The user can also monitor the import, export, and subscribing client status. This option only appears with the UDR application.
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. This option only appears with the DSR application.
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. This option is only available with the DSR application.
Gateway Location Application (optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • Exceptions

Menu Item	Function
	• Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP). This option only appears with the DSR application.
MAP-Diameter Interworking (optional)	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 NOAMP, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application: • MD-IWF Options • Diameter Realm • Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping This option only appears with the DSR application.
RADIUS (Remote Authentication Dial-In User Service) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • Network Options • Message Authenticator Configuration Sets • Shared Secret Configuration Sets • Ingress Status Server Configuration Sets • Message Conversion Configuration Sets • NAS Node This option only appears with the DSR application.

SBR (Session Binding Repository) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for:
	
	• SBR Databases
	• SBR Database Resizing Plans
	• SBR Data Migration Plans
	• Database Options
	
	Additionally, on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:
	
	• Maintenance
	
	  • SBR Database Status
	  • SBR Status
	  • SBR Database Reconfiguration Status
	
	This option only appears with the DSR application.

Menu Item	Function
Mediation	Allows the user to make routable decisions to end the reply, drop the message, or set the destination realm.

Policy and Charging (optional)	On the NOAMP, 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
	
	Additionally on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:
	
	• Maintenance
	
	  • SBR Database Status
	  • SBR Status
	  • SBR Database Reconfiguration Status
	  • 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 Selection Rules
	  • Policy Clients
	  • Suspect Binding Removal Rules
	  • Site Options
	
	• Online Charging DRA
	
	  • OCSs
	  • CTFs

Menu Item	Function
	• OCS Session State
	• Realms
	• Error Codes
	• Alarm Settings
	• Congestion Options
	This option only appears with the DSR application.
DCA Framework (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for DCA applications:
	• Custom MEALs (Measurements, Events, Alarms, and Logs)
	• General Options
	• Trial MPs assignment
	• Application Control
	• System Options
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and IP List TSAs.
	This is accessible from the SOAM server only. This option only appears with the DSR application.
Help	Launches the Help system for the user interface
Legal Notices	Product Disclaimers and Notices
Logout	Allows the user to log out of the user interface

Missing Main Menu options

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

Main Menu options vary according to the group permissions assigned to a user's account. Depending on your user permissions, some menu options may be missing from the Main Menu. For example, Administration menu options do not 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.

is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the *Oracle Software Web Browser Support Policy* for details

System Login Page

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

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

Customizing the Login Message

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

ORACLE®

Oracle System Login

Wed Jul 8 14:20:00 2015 EDT

Log In
Enter your username and password to log in

Username: [_____]

Password: [_____]

☐ Change password

[Log In]

Welcome to the Oracle System Login.

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies.

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

Copyright © 2010, 2015, Oracle and/or its affiliates. All rights reserved.

Figure 1: Oracle System Login

1. From the **Main Menu**, click **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 displays.

Accessing the DSR Graphical User Interface

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

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

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and 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 4: Main Menu Icons

Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.

Icon	Name	Description
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Task	Contains operations related to Tasks
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

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

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

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination with **First|Prev|Next|Last** links at both the beginning and end of this table type. Paginated tables also contain action links on the beginning and end of each row. For more information on action links and other page controls, see *Page Controls*.

Figure 2: 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*.

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.

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

Figure 5: Tabbed Pages

Figure 6: Tabbed Pages

Reports

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

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

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 splash page appears. Located in the center of the main work area is a customizable welcome message. Use this procedure to create a message suitable for your needs.

1. From the **Main Menu**, click **Administration** > **General Options**.
2. Locate **Welcome Message** in the **Variable** column.
3. Enter the desired welcome message text in the **Value** column.
4. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.
    A status message appears at the top of the page to inform you if the operation was successful.

The next time you log in to the user interface, the new 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 5: Example Action Buttons contains examples of Action buttons.

Table 5: Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.
Delete	Deletes data from table.

Action Button	Function
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in *Table 6: 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 6: Submit Buttons

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

Clear Field Control

The clear field control allows you to clear the value from a 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.
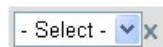
Figure 9: Clear Field Control X

Optional Layout Element Toolbar

The optional layout element toolbar appears in the Page Control Area of the GUI.
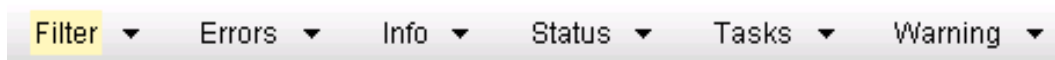
Figure 10: Optional Layout Element Toolbar

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.
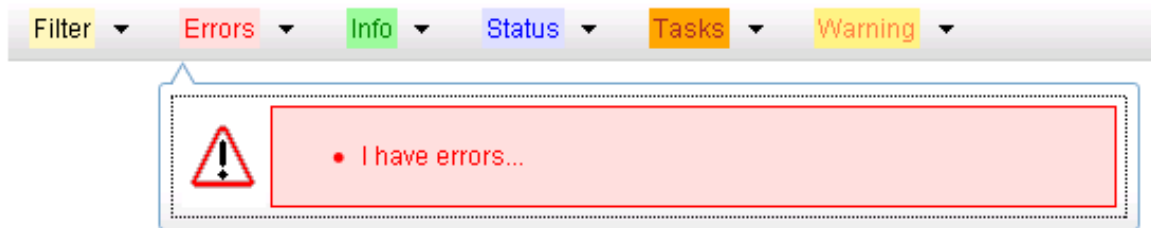
Figure 11: Automatic Error Notification

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 affect all pages that list or display data relating to the Network Element.

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

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

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

Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: 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.
<	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 are available for you to select.

Filtering on the Network Element

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

1. Click **Filter** in the optional layout element toolbar.
2. Select a Network Element from the **Network Element** 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.
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 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.
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.
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 **Add** 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**, click **Administration** > **General Options**.

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

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

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

   OK saves the change and returns to the previous page.

   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Chapter

3

MAP-Diameter IWF Introduction

Topics:

This section introduces applications, key concepts, and basic functionality related to the MAP-Diameter Interworking Function.

The MAP-Diameter Interworking Function is a feature of the Diameter Signaling Router (DSR) product, which is part of the Oracle product line of signaling products. The MAP-Diameter Interworking Function allows the DSR to support the bi-directional interworking between Diameter and SS7 (GSM MAP) messages.

Overview

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 Diameter transactions received from the Diameter network via DRL and MAP transactions received from SS7-MPs.

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

The MAP-Diameter Interworking assumes 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.
- 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 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.
- DM-IWF and MD-IWF will use ComAgent's Enhanced Routed Service for load sharing Request messages to MD-IWFs and DM-IWFs respectively. ComAgent Enhanced Routed Service self learns about the topology changes and enables deployment of transparent, elastic and scalable solutions.
- In this document, any reference to DM-IWF Routed Service or MD-IWF Routed Service implies ComAgent's Enhanced Routed Service for internal message exchange. It also indicates that the growth/degrowth of SS7-MPs and DA-MPs is non-impacting to MD-IWF and DM-IWF application instances and ensures guaranteed delivery.

  Note: DM-IWF Routed Service and MD-IWF Routed Service is displayed as DMIWFSvc and MDIWFSvc respectively on the ComAgent maintenance screens. Each DM-IWF instance acts as a service provider for the DM-IWF Routed Service and as a service user for the MD-IWF Routed Service, and vice versa.

  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.

Diameter-to-MAP Transactions

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.

Processing Diameter-to-MAP Transactions

The processing of a Diameter-to-MAP transaction involves various steps:

1. When DM-IWF receives a Request from DRL, it allocates a Pending Transaction Record (DM-IWF-PTR), starts a DM-IWF Pending Answer Timer and then forwards the unmodified Diameter Request message to a MD-IWF using the services of ComAgent.

2. When MD-IWF receives a Request message from a DM-IWF, it determines whether it can process the transaction and sends either a Success or Failure response to the ComAgent transaction.

3. If MD-IWF can process the transaction, it allocates a MD-IWF-PTR for storing the DA-MP's address and Transaction ID, converts the Diameter Request message into a MAP request message and attempts to open a MAP dialogue to the destination SS7 Node (such as HSS).

4. When MD-IWF receives the final MAP ack message closing the MAP dialogue, MD-IWF converts the MAP ack message to a Diameter Answer message. The Diameter Answer message and Transaction ID stored in the MD-IWF-PTR are sent to the DM-IWF which initiated the transaction using the services of ComAgent and the MD-IWF-PTR is deallocated.

5. When DM-IWF receives an Answer response, it uses the Transaction ID to find the DM-IWF-PTR for the transaction. If a DM-IWF-PTR is found, then DM-IWF forwards the Answer back to DRL for backward routing to the Diameter Node which initiated the transaction and the DM-IWF-PTR is deallocated. Otherwise, DM-IWF will discard the Answer.

   Note: If ComAgent (DM-IWF Routed Service) encounters an error or fails to receive a reliable acknowledgment from the SS7-MP to which the Request was originally sent, ComAgent can retry sending the Request to another MD-IWF (SS7-MP).

MAP-to-Diameter Transactions

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

Processing MAP-to-Diameter Transactions

The processing of a MAP-to-Diameter transaction involves various steps:

1. When an MD-IWF receives a MAP request message from an SS7 Node attempting to open a MAP dialogue that MD-IWF is able to process, it allocates a MD-IWF Pending Transaction Record (MD-IWF-PTR) for storing the MAP query message(s) for the MAP procedure.

2. MD-IWF converts one or more MAP request messages into a single Diameter Request message, starts a Diameter Transaction Timer and then forwards the Diameter Request message to a DM-IWF using the services of ComAgent.

3. When DM-IWF receives a Request message from an MD-IWF, it allocates a DM-IWF Pending Transaction Record (DM-IWF-PTR) for storing MD-IWF's address (used for sending the Answer response), and attempts to forward the Diameter Request message to DRL. DM-IWF does not start a DM-IWF Pending Answer Timer as the ownership of the transaction is transferred to DRL.

4. If DM-IWF successfully enqueues the Diameter Request message on DRL's Request Message Queue, it will send a Success Response to the ComAgent reliable transfer transaction. This frees the

ComAgent transaction. Otherwise, DM-IWF sends a Failure Response to the ComAgent transaction and DM-IWF processing of the transaction is complete

5. When an Answer is received from the peer Diameter node, it is received by DRL and forwarded to DM-IWF on the DA-MP. When DM-IWF receives a Diameter Answer message response from DRL, it forwards the Answer message to the MD-IWF SS7-MP which initiated the transaction and DM-IWF processing of the transaction is complete.

6. When MD-IWF receives the Diameter Answer response, it uses the Transaction ID to find the MD-IWF-PTR for the transaction. If a MD-IWF-PTR is found, it converts the Diameter Answer message into a MAP ack message response and the MAP dialogue is closed and the MD-IWF-PTR is deallocated. Otherwise, MD-IWF will discard the Answer.

Address Translation

Address Translation is the process by which Diameter routing information is mapped to an SS7 network (for Diameter originated requests) or SS7 signaling data is mapped to a Diameter network (for MAP originated requests).

Diameter requests are mapped to the SS7 network by using the Destination-Host and Destination-Realm AVPs and a series of table look ups to derive an MTP3 layer OPC and DPC as well as the SCCP Called Party Address. The Destination-Host AVP is optional. If the Destination-Host is absent, the IMSI value from the User-Name AVP is used instead. The Origin-Host and Origin-Realm for the Diameter answer are derived from the SCCP Calling Party Address.
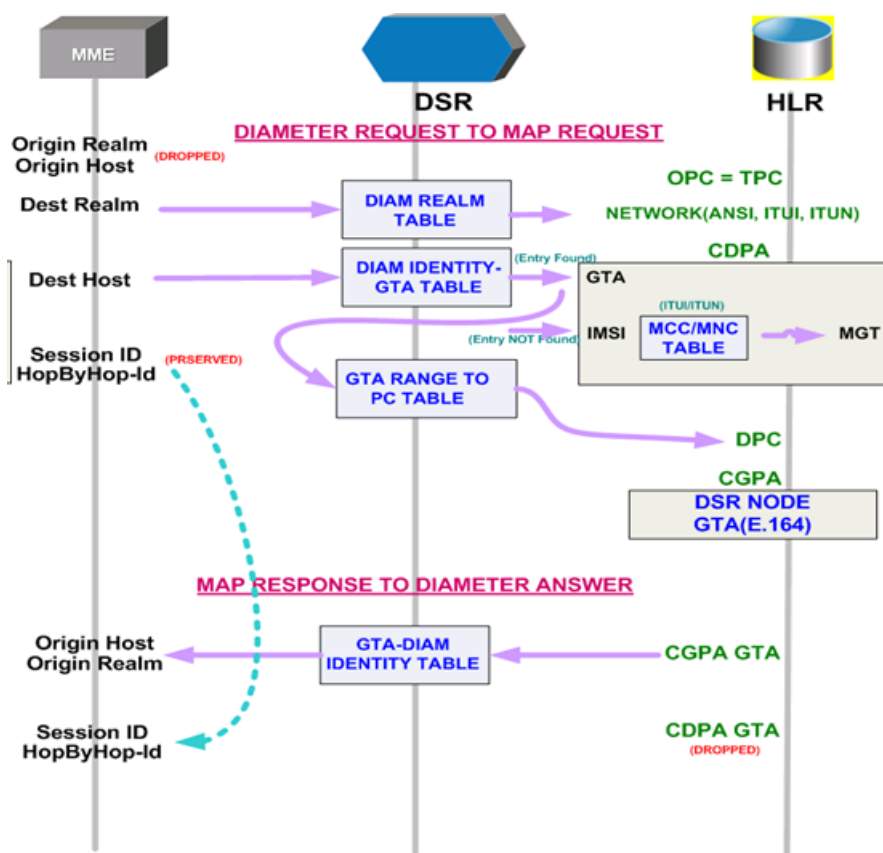
Figure 13: Diameter to MAP Requests

MAP requests are translated into the Diameter network by using the SCCP Calling Party Address to derive an Origin-Host and Origin-Realm AVP and using the SCCP Called Party Address to derive a Destination-Host and Destination-Realm AVP for the outgoing Diameter request. Address data from the MAP request is stored away for the life of the MAP Dialogue and used for populating the address information in the MAP response.
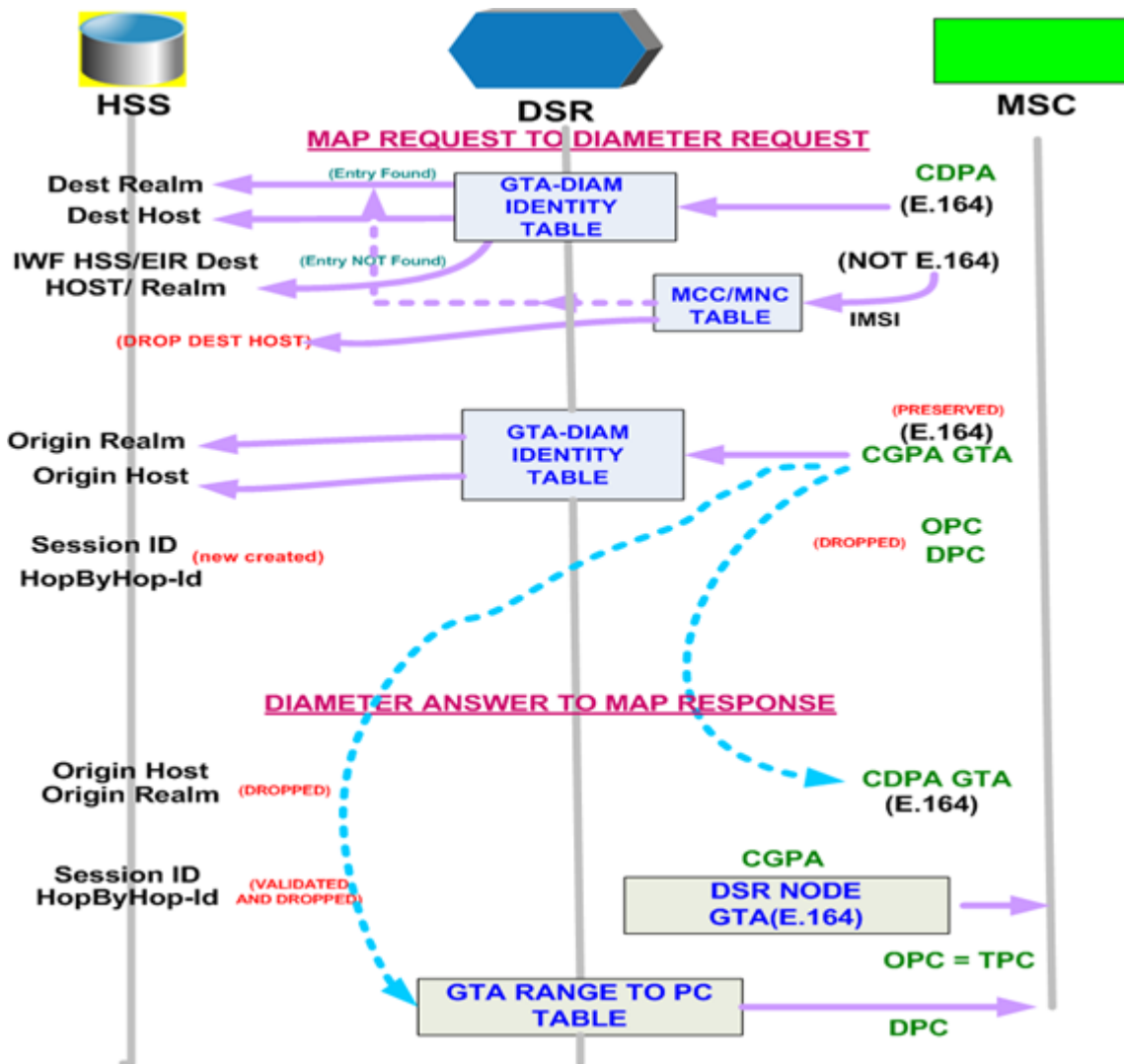
Figure 14: MAP to Diameter Requests

Request Routing with Chained DSR Applications

Application Chaining is a method for invoking multiple DSR Applications in sequence on the same DSR.

Figure 15: Request Processing with Multiple DSR Applications shows an example of Request processing for two DSR Applications executing in sequence. The Application Route Table in this example is executed three times:

1. When the Request enters the system at (1)
2. When DSR Application 1 sends the Request back to the Diameter Routing Function at (3)
3. when DSR Application 2 sends the Request back to the Diameter Routing Function at (5)

At (5) there is no matching Application Routing Rule for the Request, the Request is routed to Peer Route Table processing.
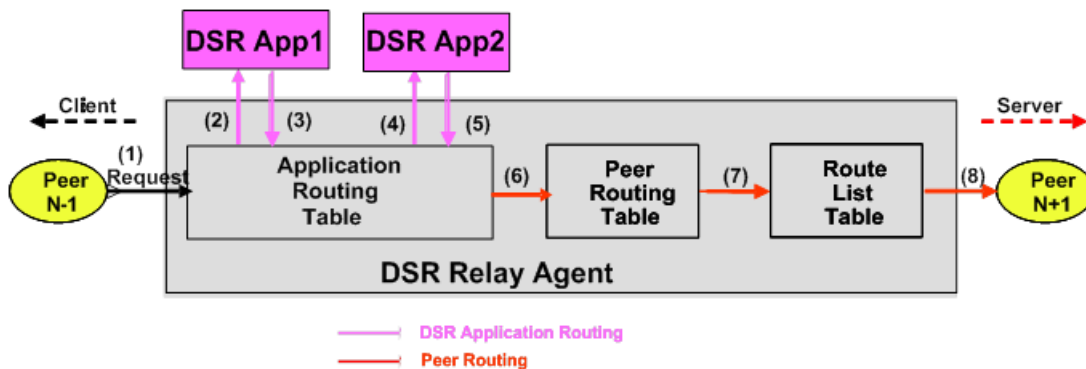
Figure 15: Request Processing with Multiple DSR Applications

- **Application Route Table (ART)**

  Application Route Tables are used for routing Request messages to DSR Applications. An ART contains a prioritized list of user-configurable Application Routing Rules . Each Application Routing Rule associates Request message content with a DSR Application.

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

- **Application Routing Rules**

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

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

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

The system always contains a Default ART that cannot be removed using the configuration GUI. The user can create additional ARTs and then define, through configuration, which ART will be searched based on ART precedence selection rules.

Each time that a Request message is received from a Peer Node or DSR Application, the Diameter Routing Function selects an ART to search based on the ART precedence selection rules (highest to lowest priority):

1. The ART provided by the DSR Application, if it exists (applies only when the Request message was received from a DSR Application)
2. The ART assigned to the ingress Peer Node from which the Request message was received, if it exists
3. The ART assigned to the Diameter Application ID in the Request message header, if it exists
4. The Default ART

The order of DSR Applications which can process an ingress Request message is determined by operator configuration of one or more Application Route Tables.

- Each time the Diameter Routing Function receives a Request message from a Peer Node or DSR Application, it searches the Application Route Tables to determine where to forward the message.
- The highest priority Application Routing Rule matched defines where to forward the message.
- If no Application Routing Rule match is found, the Diameter Routing Function begins Relay Agent routing to an upstream Peer Node.

When FABR or RBAR and the Diameter-MAP Interworking (DM-IWF) applications run in the same DA-MP, the same Diameter Request message can be processed by both applications.

For a Diameter-to-MAP Request message received from a Diameter Peer that needs to be processed by FABR or RBAR followed by DM-IWF, two Application Routing Rules are needed; one for routing the message first to FABR or RBAR and the second one to route the message to DM-IWF after FABR or RBAR processing is completed

- After the Request is received from the Peer, the Diameter Routing Function searches the Application Routing Rules for the highest priority matching rule. This rule contains the FABR or RBAR application name, and will result in the Request being routed to FABR or RBAR
- FABR or RBAR processes the message and returns it to the Diameter Routing Function.
- The Diameter Routing Function searches the Application Routing Rules for the highest priority matching rule (excluding all rules that would result in routing of the Request to FABR or RBAR again).This rule contains the DM-IWF application name, and will result in the Request being routed to DM-IWF.

- DM-IWF processes the message and sends it to an MD-IWF application (SS7-MP).

For a MAP-to-Diameter Request message received by DM-IWF from an MD-IWF application (SS7-MP) that needs to be processed by FABR or RBAR after DM-IWF processing, a single Application Routing Rule is needed for routing the message to FABR or RBAR after DM-IWF processing is completed.

- DM-IWF processes the message and sends it to the Diameter Routing Function.
- The Diameter Routing Function searches the Application Routing Rule for the highest priority matching rule (excluding all rules that would cause routing of the Request to DM-IWF again). This rule contains the FABR or RBAR application name, and will result in the Request being routed to FABR or RBAR for processing.
- FABR or RBAR returns the message to the Diameter Routing Function to complete the routing process.

Transaction Metadata Recording for Integrated DIH (IDIH)

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

The Diameter Routing Function and invoked DSR Applications record detailed information about each Diameter transaction - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the Trace Transaction Record (TTR) in the order that the metadata-generating events actually occurred. Together, all of the metadata records combine to document the processing performed on the entire transaction, and can later be used to provide diagnostic information when performing troubleshooting. Metadata is recorded to a TTR for each transaction so that, even if the transaction is selected to be sent to DIH at an Answer Troubleshooting Trigger Point (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction will be present.

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

MD-IWF does not support IDIH.

DM-IWF will record the Application-specific metadata events described in *Table 8: DM-IWF Metadata-Generating Events*.

Table 8: DM-IWF Metadata-Generating Events

DM-IWF Event	Metadata Fields			When Recorded
	Type	Scope	Instance Data	
Diameter-to-MAP Transactions				
Sent Egress Request to SS7-MP	SS7-MP Request sent	App Data	Transaction ID (such as 45631) Payload	Immediately before the egress Request is sent to ComAgent.
D-to-M Request discarded	Message Discarded	App Data	Discard Reason (such as DM-IWF PTR pool exhausted)	DM-IWF discards a Request message received from DRL.
Ingress Answer received from SS7-MP	SS7-MP Answer received	App Data	Transaction Id (such as 45631) SS7-MP IP address (such as 47.240.10.3) Payload	DM-IWF received an ingress Answer message from SS7-MP
A received Answer did not match a pending transaction	SS7-MP Answer Matching Failed	App Data	None	Immediately after PTR search fails
DM-IWF Routing Exception	DM-IWF Routing Exception	App Data	Routing Exception Type (such as Internal Processing Error) Routing Exception Action (such as Abandon Request)	When a routing exception is applied by DM-IWF

DM-IWF Event	Metadata Fields			When Recorded
	Type	**Scope**	**Instance Data**	
MD-IWF Routing Exception	MD-IWF Routing Exception	App Data	None	When DM-IWF applies Apply Unavailability Action routing exception on behalf of MD-IWF.
MAP-to-Diameter Transactions				
Ingress Request received from SS7-MP	SS7-MP Request received	App Data	Transaction ID (such as 45631) SS7-MP address (such as 47.240.10.3) Payload	Immediately after a Request is received from SS7-MP.
Egress Answer sent to SS7-MP	SS7-MP Answer Sent	App Data	Transaction ID (such as 45631) SS7-MP address (such as 47.240.10.3) Payload	Immediately after DM-IWF sends a Diameter Answer to ComAgent successfully.
D-to-M Answer discarded	Message Discarded	App Data	Discard Reason (such as Failed to create IWF Answer)	DM-IWF discards an Answer message received from DRL.

Chapter

4

MAP-Diameter Interworking Function Configuration

Topics:

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

MAP-Diameter IWF Configuration Overview

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

The DSR 3-tiered Operations, Administration, and Maintenance (OAM) topology is required for the MAP-Diameter Interworking Function application. 3-tiered OAM topology consists:

- A pair of NOAM servers running in active/standby redundancy

  OAM configuration is performed on the NOAM.

  Network-wide MAP-Diameter IWF configuration is performed on the NOAM.

- A pair or triplet of SOAM servers at each site running in active/standby, or active/standby/spare redundancy

  Diameter protocol configuration is done on the SOAM.

  Most of the OAM configuration components are viewable on the SOAM.

  Most DSR Application configuration is done on the SOAM.

  Site-specific configuration for MAP-Diameter Interworking Function is performed on the SOAM

- A set of MP servers, which can host signaling protocol stacks (for example, DA-MPs).

The MD-IWF application is configured on the NOAM. The DM-IWF application is configured on the SOAM.

An optional pair of Disaster Recovery NOAMs can be configured to manually take over in the event of loss of both the active and standby NOAMs

The three tiers allow configured data to be replicated down to the MP servers, and measurements, events, and alarms to be merged up to the OAM servers.

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

Pre-Configuration Activities

Before MAP-Diameter IWF configuration can be performed, various activities need to be performed in the system:

- Verify that the NOAM configuration is complete for MAP-Diameter IWF:
  - Server Groups

    Select **Configuration** > **Server Groups**.

    Click **Report** to generate a report about the configured Resource Domains

    Click **Print** to print the report, or **Save** to save the report as a text file.

  - Places

Select **Configuration** > **Places**.

Click **Report** to generate a report about the configured Places.

Click **Print** to print the report, or **Save** to save the report as a text file.

- Gather component information that is required for Diameter, Diameter Common, and MAP-Diameter IWF configuration, including component item naming conventions and names, IP addresses, hostnames, and numbers of items to be configured.
- Configure Diameter Common components that are required for MAP-Diameter IWF configuration. See *Diameter Common Configuration for MAP-Diameter IWF* for more information.
- Configure Diameter Configuration components that are required for MAP-Diameter IWF configuration. See *Diameter Configuration for DM-IWF* for more information.

Diameter Common Configuration for MAP-Diameter IWF

Diameter Common configuration must be done before Map-Diameter IWF configuration can be performed.

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

SOAM Diameter Common Configuration

Diameter Common configuration for MCC Ranges Network Identifiers and MP Profile assignment for Map-Diameter IWF is done from the SOAM GUI in a 3-tiered DSR topology.

1. **MPs**

   Select **Diameter Common** > **MPs** > **Profile Assignments**, and verify that the correct DA-MP Profiles and SS7 MP profiles have been assigned for Map-Diameter IWF DA-MPs and SS7-MPs shown in the **DA-MP** and **SS7-MP** lists. If assignments need to be made or changed, use the **Diameter Common** > **MPs** > **Profile Assignments** page to assign the correct MP Profiles.

NOAM Diameter Common Configuration
Diameter Common configuration for MCCMNC and MCCMNC Mapping Network Identifiers for Map-Diameter IWF is done from the NOAM GUI in a 3-tiered DSR topology.

1. Use the **Diameter Common** > **Network Identifiers** > **MCCMNC [Insert]** page to configure**MCCMNC** entries.
2. Use the **Diameter Common** > **Network Identifiers** > **MCCMNC Mapping [Insert]** page to configure**MCCMNC Mapping** entries, using the configured **MCCMNC** entries.

Diameter Configuration for DM-IWF

Diameter configuration must be done before DM-IWF configuration can be performed.

All Diameter Configuration for DM-IWF is done using the SOAM GUI in a 3-tiered DSR topology.

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

1. **Application Ids**

   Use the **Diameter** > **Configuration** > **Application Ids [Insert]** page to define an Application Id from the **Application ID Value** pulldown list for each DSR application that will be used by DM-IWF in the system.

2. **Command Codes**

   Diameter Command Codes must be configured prior to using them in DM-IWF. Use the **Diameter** > **Configuration** > **Command Codes [Insert]** page to configure Diameter Command Codes.

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

3. **Local Nodes**

   Use the **Diameter** > **Configuration** > **Local Nodes [Insert]** page to configure the DM-IWF DA-MPs as Local Nodes in the system.

   The pulldown list of **IP Addresses** contains the XSI addresses configured on DSR MP Servers.

4. **Peer Nodes**

   Use the **Diameter** > **Configuration** > **Diameter > Configuration > Peer Nodes [Insert]** page to configure PCEFs, AFs, BBERFs, and any other types of nodes as Peer Nodes to the DM-IWF DA-MPs in the system

5. **Connections**

   Use the **Diameter** > **Configuration** > **Connections [Insert]** page to configure new connections

6. **Route Groups**

   Use the **Diameter** > **Configuration** > **Route Groups [Insert]** page to configure new route groups

7. **Route Lists**

   Use the **Diameter** > **Configuration** > **Route Lists [Insert]** page to configure new route lists

8. **Peer Route Tables**

   Use the **Diameter** > **Configuration** > **Peer Route Tables [Insert]** page to configure new **Peer Route Tables** if needed,

9. **Peer Routing Rules**

   Peer Routing Rules can be added to the Default Peer Route Table (PRT) or to new Peer Route Tables.

10. **Application Route Tables**

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

11. **Application Routing Rules**

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

Use the **Viewing Rules for Application Route Table** page to insert or edit an **Application Routing Rule**. Configure the ART rules by ensuring the Diameter Application ID is supported (for example S6a, S6d, S13 or, S13a) and ensuring the DSR Application ID for these Requests is configured as DM-IWF, so that these Requests get forwarded to DM-IWF.

Transport Manager Configuration

To properly use the MD-IWF application, it is necessary to configure the Transport Manager from the **Transport Manager** > **Configuration** GUI pages.

Note: Transport Manager must be configured prior to the configuration of the SS7 Networking.

Transport Manager configuration is performed on an Active SOAM.

The **Transport Manager** > **Configuration** GUI pages provide fields for entering the information needed to configure Adjacent Nodes, Configuration Sets, and Transports (SCTP associations with remote hosts over an underlying IP network).

Configured Adjacent Nodes and Configuration Sets are required in the configuration of Transports. Therefore, Adjacent Nodes and Configuration Sets must be configured before Transports can be configured.

For more detailed information on how to perform these tasks, refer to the *Transport Manager User's Guide* and help.

SS7 Network Configuration

Note: Transport Manager must be configured prior to the configuration of the SS7 Networking.

To properly use the MD-IWF application, it is necessary to configure the SS7 Networking from the **SS7/Sigtran** > **Configuration** SOAM GUI pages.

The SS7 Networking components to be configured are:

- Adjacent Server Groups
- Local Signaling Points
- Local SCCP Users
- Remote Signaling Points
- Remote MTP3 Users
- Link Sets
- Links
- Routes
- SCCP Options

For more detailed information on how to perform these tasks, refer to the *SS7/Sigtran User's Guide* and help.

Post-Configuration Activities

After MAP-Diameter Interworking configuration is complete, various activities need to be performed to make the MD-IWF and DM-IWF applications fully operational in the system:

- Enable the MD-IWF and DM-IWF DSR applications on SS7-MPs and DA-MPs respectively
- Restart Servers
- Enable Diameter Connections with Peer Nodes
- Status Verification

Enabling the MD-IWF and DM-IWF Applications

Use this task to enable the MD-IWF and DM-IWF applications.

1. From each active SOAM in a 3-tiered DSR topology or from the NOAM in a 2-tiered DSR topology, select **Diameter** > **Maintenance** > **Applications**.
   The **Diameter** > **Maintenance** > **Applications** page appears.

2. Under **DSR Application Name**, select each **MD-IWF** or **DM-IWF** row.

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

3. Click **Enable**.

4. Verify the application status on the page.

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

Bulk Import and Export

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

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

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

Bulk Import

The Bulk Import operations use configuration data in ASCII Comma-Separated Values (CSV) files (.csv), to insert new data into, update existing data in, or delete existing data from the configuration data in the system.

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

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

Note: The format of each Import CSV file record must be compatible with the configuration data in the release used to import the file. Across different release versions, column counts may not be compatible, and the import fails.

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

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

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

Multiple Import operations can be performed:

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

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

Bulk Export

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

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

Configuration data can be exported in one Export operation:

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

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

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

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

Chapter

5

MD-IWF Application Configuration

Topics:

The **MAP-Diameter IWF > Configuration** GUI pages for MD-IWF components provide fields for entering the configuration information for the MD-IWF application.

MD-IWF Options Configuration

The **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options** page is used to configure MD-IWF application Options.

Note: DM-IWF configuration can be performed only on Active SOAM servers.

The fields are described in *MD-IWF Options Elements*.

On the **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options** page, you can:

- Modify current Options values, and click **Apply** to save the changes.
- Click **Cancel** to remove and not save any changes you have made.

MD-IWF Options Elements

Table 9: MD-IWF Options Elements describes the fields on the MD-IWF Options page.

Table 9: MD-IWF Options Elements

Field (* indicates a required field)	Description	Data Input Notes
*Diameter Response Timeout	Timeout value, in seconds, to use when sending a Diameter Request message to the Diameter network (through DM-IWF) and waiting for the Diameter Answer message to arrive. It is suggested that this timer be greater than the Diameter Routing Function's Transaction Lifetime configured under **Diameter** > **Configuration** > **Routing Option Sets**. **Note:** If the Diameter Pending Answer Timer is less than this value, the Diameter Error Responses from the DSR will be seen.	Format: text box; numeric Range: 3-30 Default: 15
*MAP Response Timeout	Timeout value, in seconds, to use when sending a MAP Request message to the SS7 network and waiting for the MAP Response message to arrive. This is the time from begin-dialog to close-dialog; it controls how long all of the dialogs within a transaction can continue until the dialog times out. It is suggested that this timer shall be greater than the	Format: text box; numeric Range: 5-30 Default: 15

Field (* indicates a required field)	Description	Data Input Notes
	Segmentation/Reassembly timeout value configured under the SCCP Options folder.	
EIR Host Name	When translating an incoming MAP-CheckIMEI (EIR) Request message to a Diameter Request message, the Destination-Host AVP will be populated with this FQDN value when the GTA that is derived from the SCCP Called Party Address cannot be mapped to a Diameter Host/Realm using Diameter Identity - GTA entries. If this value is not configured, then an error response is sent back to the SS7 network.	Format: text box FQDN is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. Range: a valid FQDN or empty Default: N/A
EIR Realm	When translating an incoming MAP-CheckIMEI (EIR) Request message to a Diameter Request message, the Destination-Realm AVP will be populated with this value when the GTA that is derived from the SCCP Called Party Address cannot be mapped to a Diameter Host/Realm using Diameter Identity - GTA entries. If this value is not configured, then an error response is sent back to the SS7 network.	Format: text box Realm is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. Range: a valid Realm or empty Default: N/A
EIR Destination GTA	When translating an incoming ECR (ME-Identity-Check) Diameter Request message to a MAP Request message, if the Destination-Host AVP is absent in the ECR message, then the SCCP Called Party GTA will be populated with this value when the ECR Request Message with no	Format: text box; numeric Range: a valid Global Title Address in E.164 format, or empty Default: N/A

Field (* indicates a required field)	Description	Data Input Notes
	Dest-Host AVP option is configured as Translate Using EIR Dest GTA.	
IWF HSS Destination Host	When translating an incoming (non-EIR) MAP Request message to a Diameter Request message, the Destination-Host AVP will be populated with this FQDN value when the GTA that is derived from the SCCP Called Party Address cannot be mapped to a Diameter Host/Realm using Diameter Identity - GTA entries. If this value is not configured, then MD-IWF will not populate the Destination-Host AVP; it could be resolved on the DSR by FABR or RBAR, or by another upstream Peer.	Format: text box FQDN is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. Range: a valid FQDN or empty Default: N/A
IWF HSS Destination Realm	When translating an incoming (non-EIR) MAP Request message to a Diameter Request message, the Destination-Realm AVP will be populated with this value when the GTA that is derived from the SCCP Called Party Address cannot be mapped to a Diameter Host/Realm using Diameter Identity - GTA entries. If this value is not configured, then an error response is sent back to the SS7 network.	Format: text box Realm is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. Range: a valid Realm or empty Default: N/A
*Shutdown Mode	Allows the operator to specify the shutdown method used when the Admin State is changed to Disabled. The application can be disabled using either a graceful or forced shutdown method. Graceful allows in-process transactions to continue for a configurable time period before disabling. Forced is an immediate shutdown.	Format: radio buttons Range: Forced or Graceful

Field (* indicates a required field)	Description	Data Input Notes
*Shutdown Timer	Number of seconds that the Shutdown Timer will run during a Graceful shutdown.	Format: text box, numeric Range: 1-30 Default: 15
ECR Request Message with no Destination Host AVP		
Action	When translating an incoming ECR (ME-Identity-Check) Diameter Request message to a MAP Request message, this indicates the action to take if the Destination-Host AVP is absent in the ECR message. If the Destination-Host AVP is present, it is used in the translation to derive the SCCP Called Party GTA. • Discard: The Diameter to MAP transaction is discarded; a Diameter Answer message is NOT sent back to the Diameter network. • Send Answer: A Diameter Answer message with Experimental- Result AVP or Result-Code is sent back to the Diameter network. • Translate Using EIR: Translate the ECR message to a MAP Request message using the configured EIR Destination GTA as the SCCP Called Party GTA.	Format: radio buttons Range: Discard, Send Answer, Translate using EIR
Response Result Code AVP	If the configured Action is Send Answer, this value is used in the Result-Code or Experimental-Result AVP of the Diameter Answer message	Format: text box, 4-digit numeric; or pulldown list of known Result Codes Range: 1000-5999
Response Vendor ID	If zero, then a Result-Code AVP will be sent when the DSR Application is not Available. If non-zero, then an Experimental-Result AVP will be sent will the Vendor-Id AVP set to this value. Available when Send Answer is selected for the Action.	Format: text box; numeric Range: 0-4294967295
Response Error String	If a non-empty string, this configured string will be appended to the Error-Message AVP that is sent in the	Format: text box; string of printable ASCII characters. Range 0-64 characters

Field (* indicates a required field)	Description	Data Input Notes
	Diameter Answer message. Available when Send Answer is selected for the Unavailable Action field.	
ECR Request Message with Dest-Host present but Not Found in mapping table		
Action	When translating an incoming ECR (ME-Identity-Check) Diameter Request message to a MAP Request message, this indicates the action to take if the Destination-Host AVP is absent in the ECR message. If the Destination-Host AVP is present, it is used in the translation to derive the SCCP Called Party GTA. • Discard: The Diameter to MAP transaction is discarded; a Diameter Answer message is NOT sent back to the Diameter network. • Send Answer: A Diameter Answer message with Experimental- Result AVP or Result-Code is sent back to the Diameter network. • Translate Using EIR: Translate the ECR message to a MAP Request message using the configured EIR Destination GTA as the SCCP Called Party GTA.	Format: radio buttons Range: Discard, Send Answer, Translate using EIR
Response Result Code AVP	If the configured Action is Send Answer, this value is used in the Result-Code or Experimental-Result AVP of the Diameter Answer message. Available when Send Answer is selected for the associated Action.	Format: text box, 4-digit numeric; or pulldown list of known Result Codes Range: 1000-5999
Response Vendor ID	If zero, then a Result-Code AVP will be sent when the DSR Application is not Available. If non-zero, then an Experimental-Result AVP will be sent with the Vendor-Id AVP set to this value. Available when Send Answer is selected for the Action.	Format: text box; numeric Range: 0-4294967295
Response Error String	If a non-empty string, this configured string will be appended to the Error-Message AVP that is sent in the	Format: text box; string of printable ASCII characters.

Field (* indicates a required field)	Description	Data Input Notes
	Diameter Answer message. Available when Send Answer is selected for the Unavailable Action field.	Range 0-65 characters
Shutdown Mode	Allows the operator to specify the shutdown method used when the Admin State is changed to Disabled. The application can be disabled using either a graceful or forced shutdown method. Graceful allows in-process transactions to continue for a configurable time period before disabling the application. Forced is an immediate shutdown.	Format: radio buttons Range: Forced, Graceful
*Shutdown Timer	Unique number of seconds that the Shutdown Timer will run during Graceful shutdown.	Format: text box, numeric Range 1-30 Default: 15
Node GTA		
Viper-place	Global Title Address associated with the Place. When translating incoming Diameter Request messages to MAP Request messages, the SCCP Calling Party GTA is always populated with this value. Configuration is mandatory. The MD-IWF application cannot be enabled if this field is empty.	Format: text box, numeric Range: a valid Global Title Address in E.164 format Default: N/A

Diameter Realm Configuration

The **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page on an NOAM server is used to configure Diameter Realms.

The fields are described in *Diameter Realm Elements*.

On the **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page, you can:

- Filter the list of entries, to display only the desired entries.
- Sort the list entries in ascending or descending order by by clicking the column heading. By default, the list is sort in ascending alphabetical order by Signaling Network.
- Click **Insert**.

    The **MAP-Diameter IWF** > **Configuration** > **Diameter Realm [Insert]** page opens. You can add new Diameter Realms.

- Select a Diameter Realm entry in the list, and click **Edit**.

    The **MAP-Diameter IWF** > **Configuration** > **Diameter Realm [Edit]** page opens. The selected Diameter Realm entry can be edited.

- Select a Diameter Realm entry in the list, and click **Delete** to remove the selected entry.

Diameter Realm Elements

Table 10: Diameter Realm Elements describes the fields on the **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page. Data Input Notes apply to Insert and Edit pages; the View page is Read-only.

Table 10: Diameter Realm Elements

Field (* indicates a required field)	Description	Data Input Notes
*Diameter Realm	Realm that is specified in the Destination-Realm AVP of a Diameter Request message. This table describes the characteristics of the SS7 network that corresponds to a Diameter Realm. This information is used to translate a Diameter Request message to a MAP Request message that is sent to the SS7 network.	Format: text box Case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a Realm must be at most 255 characters long. Range: A valid Realm Default: N/A
Signaling Network	Signaling network (ITUI, ITUN or ANSI) of the SS7 network corresponding to the given Realm.	Format: radio buttons Range: ITUI, ITUN, or ANSI Default: N/A
MGT (E.214) Conversion Needed	Indicates whether the IMSI digits (User-Name AVP) need to be converted to MGT (E.214) format (using table MccMncMapping) when using these digits as the Called Party GTA in the MAP Request message. This is applicable for ITUI and ITUN only. If set to Yes (Checked), this treatment will be applied only if (1) Destination-Host AVP is not present in the Diameter Request message; or (2) fail to map the	Format: check box Range = Yes, No, N/A Default: No (Unchecked) for ITU/ITUN; N/A for ANSI

Field (* indicates a required field)	Description	Data Input Notes
	Destination-Host AVP to a GTA via table DiameterIdentity-GTA.	

Adding Diameter Realm Entries

Use this task to configure new **Diameter Realm** entries.

Diameter Realm fields are described in *Diameter Realm Elements*.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **Diameter Realm**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page appears.

2. Click **Insert**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Realm [Insert]** page appears.

3. Enter a value for each field.
4. Click:

   - **OK** to save the new entry and return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page.
   - **Apply** to save the new entry and remain on this page. The data displayed on the page is updated.
   - **Cancel** to return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page without saving any changes.

Editing Diameter Realm Entries

Use this task to change **Diameter Realm** entries.

Diameter Realm fields are described in *Diameter Realm Elements*.

When the **MAP-Diameter IWF** > **Configuration** > **Diameter Realm [Edit]** page opens, the fields are populated with the current configured values.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **Diameter Realm**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page appears.

2. Select the **Diameter Realm** entry to be changed.
3. Click **Edit**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Realm [Edit]** page appears.

4. Edit the fields that need to be changed.
5. Click:

   - **OK** to save the changes and return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page.
   - **Apply** to save the changes and remain on this page.

- **Cancel** to return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page without saving any changes.

Deleting Diameter Realm Entries

Use this task to delete an **Diameter Realm** entry.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **Diameter Realm**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page appears.

2. Select the **Diameter Realm** entry to be deleted.

3. Click **Delete**.

   A popup window appears to confirm the delete.

4. Click:
   - **OK** to delete the **Diameter Realm** entry.
   - **Cancel** to cancel the delete function and return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Realm** page.

Diameter Identity GTA Configuration

The **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page on an NOAM server is used to configure Diameter Identity GTAs.

A Diameter Identity GTA provides configuration to allow conversion between a Diameter identity (Diameter Host and Realm) in the Diameter network and a Global Title Address in the SS7 network. Its configuration is used to translate in both directions:

- Convert a Diameter Host/Realm to GTA while translating a Diameter message to a MAP message
- Convert a GTA to Diameter Host/Realm while translating a MAP message to a Diameter message

The fields are described in *Diameter Identity GTA Elements*.

On the **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page, you can:

- Filter the list of entries, to display only the desired entries.
- Sort the list entries in ascending or descending order by by clicking the column heading. By default, the list is sorted in ascending alphabetical order.
- Click **Insert**.

  The **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA [Insert]** page opens. You can add new Diameter IDs to GTA mapping.

- Select a Diameter Realm entry in the list, and click **Edit**.

  The **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA [Edit]** page opens. The selected Diameter Identity GTA entry can be edited.

- Select a Diameter Identity GTA entry in the list, and click **Delete** to remove the selected entry.

Diameter Identity GTA Elements

Table 11: Diameter Identity GTA Elements describes the fields on the **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page. Data Input Notes apply to Insert and Edit pages; the View page is Read-only.

Table 11: Diameter Identity GTA Elements

Field (* indicates a required field)	Description	Data Input Notes
*FQDN	Fully Qualified Domain Name of this Peer Node	Format: text box Case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and an FQDN must be at most 255 characters long. Range: A valid FQDN Default: N/A
*Realm	Diameter Realm that (along with the FQDN) is to be converted to/from a Global Title Address	Format: radio buttons Range: A valid Realm Default: N/A
*Global Title Address	Global Title Address in the SS7 network that is to be converted to/from a Diameter Host and Realm in the Diameter network.	Format: text box Range: 1-21 digits Default: N/A

Adding Diameter Identity GTA Entries

Use this task to configure new **Diameter Identity GTA** entries.

Diameter Identity GTA fields are described in *Diameter Identity GTA Elements*.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page appears.

2. Click **Insert**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA [Insert]** page appears.

3. Enter a value for each field.
4. Click:

- **OK** to save the new entry and return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page.
- **Apply** to save the new entry and remain on this page. The data displayed on the page is updated.
- **Cancel** to return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page without saving any changes.

Editing Diameter Identity GTA Entries

Use this task to change **Diameter Identity GTA** entries.

Diameter Identity GTA fields are described in *Diameter Identity GTA Elements*.

When the **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA [Edit]** page opens, the fields are populated with the current configured values.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page appears.

2. Select the **Diameter Identity GTA** entry to be changed.

3. Click **Edit**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA [Edit]** page appears.

4. Edit the fields that need to be changed.

5. Click:

   - **OK** to save the changes and return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page without saving any changes.

Deleting Diameter Identity GTA Entries

Use this task to delete an **Diameter Identity GTA** entry.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA**.

   The **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page appears.

2. Select the **Diameter Identity GTA** entry to be deleted.

3. Click **Delete**.

   A popup window appears to confirm the delete.

4. Click:

   - **OK** to delete the **Diameter Identity GTA** entry.

   - **Cancel** to cancel the delete function and return to the **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA** page.

GTA Range to PC Configuration

The **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page on an NOAM server is used to configure GTA Range to PCs.

A GTA Range to PC provides configuration to translate a Diameter Request message to a MAP Request message by identifying the destination Point Codes of the primary signaling Gateway (SGGTWY) and its mate SG corresponding to the derived Global Title Address.

The fields are described in *GTA Range to PC Elements*.

On the **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page, you can:

- Filter the list of entries, to display only the desired entries.
- Sort the list entries in ascending or descending order by by clicking the column heading. By default, the list is sorted in ascending alphabetical order by Signaling Network.
- Click **Insert**.

  The **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC [Insert]** page opens. You can add new GTA Ranges to PC mapping.

- Select a Diameter Realm entry in the list, and click **Edit**.

  The **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC [Edit]** page opens. The selected GTA Range to PC entry can be edited.

- Select a GTA Range to PC entry in the list, and click **Delete** to remove the selected entry.

GTA Range to PC Elements

Table 12: GTA Range to PC Elements describes the fields on the **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page. Data Input Notes apply to Insert and Edit pages; the View page is Read-only.

Table 12: GTA Range to PC Elements

Field (* indicates a required field)	Description	Data Input Notes
Default Configuration	For each Signaling Network (ITUI, ITUN, or ANSI), a default Point Code configuration can optionally be specified. The default Point Codes will be used if Global Title Address digits are queried but no GTA Range to PC match is found.	Format: check box Range = Yes, No, N/A Default: No (Unchecked) for ITU/ITUN; N/A for ANSI
Global Title Start	Global Title Address (GTA) start digits. Along with the GTA End digits, this forms a GTA Range. The GTA Range (within a given Signaling Network) is mapped to the Point Codes of the primary Signaling	Format: text box Range: 1-21 digits Default: N/A

Field (* indicates a required field)	Description	Data Input Notes
	Gateway (SG) and the secondary (mate) SG. When translating a Diameter Request message to a MAP Request message, the configured GTA Ranges are queried to see if the derived GTA digits fall within a configured GTA Range.	
Global Title End	Global Title Address (GTA) end digits.	Format: text box Range: 1-21 digits Default: N/A
Signaling Network	Signaling Network (ITUI, ITUN, or ANSI) that the given GTA Range (or default configuration) applies to.	Format: text box Range: ITUI, ITUN, or ANSI Default: ITUI
*Primary Point Code	Point Code of the primary Signaling Gateway (SG) that is associated with the given GTA Range (or default configuration).	Format: text box ITU International (ITUI) Point Code format: J-NNN-J ITU International Point (ITUI) Code range: Each J can be 0-7, Each NNN can be 0-255 ITU National Point (ITUN) Code format: NNNNN ITU National (ITUN) Point Code range: NNNNN can be 0-16383 ANSI Point Code format: NNN-NNN-NNN ANSI Point Code range: Each NNN can be 0-255
Secondary Point Code	Point Code of the secondary (mate) Signaling Gateway (SG) that is associated with the given GTA Range (or default configuration).	Format: text box Range: A valid Point Code for the given Signaling Network type Default: N/A
Load Sharing	Load Sharing indicates, when translating Diameter Request messages, the algorithm to use when routing MAP messages to the Primary and Secondary (mate) Signaling Gateways.	Format: radio buttons Range: Active/Active, Active/Standby, Solitary

Field (* indicates a required field)	Description	Data Input Notes
	Active/Active (Round Robin): when routing the MAP Request messages, alternate between the Primary and Secondary Point Codes in round-robin fashion if both PCs are configured and available. If there is only one Point Code configured, or only one Point Code is available, then mesages are routed to only that Point Code. Active/Standby: MAP Request messages are routed to the Primary Point Code if it is available. If the Primary Point Code is not available, the messages are routed to the Secondary Point Code (assuming it is configured and available). If there is only one Point Code configured, the messages are routed to only that Point Code. Solitary: MAP Request messages are routed to a single Point Code. This will be the Primary Point Code.	Default: Solitary

Adding GTA Range to PC Entries

Use this task to configure new **GTA Range to PC** entries.

GTA Range to PC fields are described in *GTA Range to PC Elements*.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC**.

   The **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page appears.

2. Click **Insert**.

   The **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC [Insert]** page appears.

3. Enter a value for each field.

4. Click:

   - **OK** to save the new entry and return to the **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page.
   - **Apply** to save the new entry and remain on this page. The data displayed on the page is updated.
   - **Cancel** to return to the **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page without saving any changes.

Editing GTA Range to PC Entries

Use this task to change **GTA Range to PC** entries.

GTA Range to PC fields are described in *GTA Range to PC Elements*.

When the **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC [Edit]** page opens, the fields are populated with the current configured values.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC**.

   The **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page appears.

2. Select the **GTA Range to PC** entry to be changed.

3. Click **Edit**.

   The **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC [Edit]** page appears.

4. Edit the fields that need to be changed.

5. Click:

   - **OK** to save the changes and return to the **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page without saving any changes.

Deleting GTA Range to PC Entries

Use this task to delete an **GTA Range to PC** entry.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC**.

   The **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page appears.

2. Select the **GTA Range to PC** entry to be deleted.

3. Click **Delete**.

   A popup window appears to confirm the delete.

4. Click:

   - **OK** to delete the **GTA Range to PC** entry.

   - **Cancel** to cancel the delete function and return to the **MAP-Diameter IWF** > **Configuration** > **GTA Range to PC** page.

MAP Exception Configuration

The **MAP-Diameter IWF** > **Configuration** > **MAP Exception** page on an NOAM server is used to configure MAP Exceptions.

The fields are described in *MD-IWF Map Exception Elements*.

MAP-Diameter IWF supports various MAP Exception types:

- Internal Processing Errors (internal to the DSR) such as:

    - Resource Exhaustion
    - ComAgent Routed Service Error, timeout, or NACK immediate response
    - Unexpected software validation error (such as NULL pointer)

- Diameter to MAP Transaction Timeout (a timeout occurred waiting for a response from the SS7 network)
- Translation Error (an error occurred while performing Message Translation or Address Translation, or while translating between a TCAP User error cause value and a Diameter Result-Code)
- Congestion (MD-IWF congestion)

On the **MAP-Diameter IWF** > **Configuration** > **MAP Exception** page, you can:

- Modify current Options values, and click **Apply** to save the changes.
- Click **Cancel** to remove and not save any changes you have made.

MD-IWF Map Exception Elements

Table 13: MD-IWF Map Exception Elements describes the fields on the MD-IWF Map Exception page.

Table 13: MD-IWF Map Exception Elements

Field (* indicates a required field)	Description	Data Input Notes
IWF Internal Processing Error		
Action	Indicates the action to take if the given exception occurs.	Format: radio buttons Range: Discard Send Error to SS7 Network
Error Cause	If the configured Action is Send Answer, this Error Cause value is used in those cases where a TC-U-ERROR message is sent to the SS7 network.	Format: pulldown list Range: System Failure, Data Missing, Unexpected Data Value, Facility Not Supported, Incompatible Terminal, Resource Limitation

Field (* indicates a required field)	Description	Data Input Notes
Abort Reason	If the configured Action is Send Answer, this Abort Reason value is used in those cases where a MAP-U-ABORT message is sent to the SS7 network.	Format: pulldown list Range: User Defined, Application Context Not Supported, Dialog Refused
Abort Choice	Abort Choice further qualifies the Abort action as either Specific Reason, Resource Limitation or Resource Unavailable when the reason is configured as User Defined.	Format: pulldown list Range: Resource Unavailable, User Specific Reason, Resource Limitation (Congestion)
Resource Unavailable Reason	Unavailable Reason provides additional detail regarding whether the Resource Unavailable specified for the Abort Choice field is as a result of a short or long term limitation.	Format: pulldown list Range: Short Term or Long Term Limitation
MAP to Diameter Transaction Timeout		
Action	Indicates the action to take if the given exception occurs.	Format: radio buttons Range: Discard Send Error to SS7 Network
Error Cause	If the configured Action is Send Answer, this Error Cause value is used in those cases where a TC-U-ERROR message is sent to the SS7 network.	Format: pulldown list Range: System Failure, Data Missing, Unexpected Data Value, Facility Not Supported, Incompatible Terminal, Resource Limitation
Abort Reason	If the configured Action is Send Answer, this Abort Reason value is used in those cases where a MAP-U-ABORT message is sent to the SS7 network.	Format: pulldown list Range: User Defined, Application Context Not Supported, Dialog Refused
Abort Choice	Abort Choice further qualifies the Abort action as either Specific Reason, Resource Limitation or Resource Unavailable when the reason is configured as User Defined.	Format: pulldown list Range: Resource Unavailable, User Specific Reason, Resource Limitation (Congestion)
Resource Unavailable Reason	Unavailable Reason provides additional detail regarding whether the Resource Unavailable specified for the Abort Choice field	Format: pulldown list Range: Short Term or Long Term Limitation

Field (* indicates a required field)	Description	Data Input Notes
	is as a result of a short or long term limitation.	
Translation Error		
Action	Indicates the action to take if the given exception occurs.	Format: radio buttons Range: Discard Send Error to SS7 Network
Error Cause	If the configured Action is Send Answer, this Error Cause value is used in those cases where a TC-U-ERROR message is sent to the SS7 network.	Format: pulldown list Range: System Failure, Data Missing, Unexpected Data Value, Facility Not Supported, Incompatible Terminal, Resource Limitation
Abort Reason	If the configured Action is Send Answer, this Abort Reason value is used in those cases where a MAP-U-ABORT message is sent to the SS7 network.	Format: pulldown list Range: User Defined, Application Context Not Supported, Dialog Refused
Abort Choice	Abort Choice further qualifies the Abort action as either Specific Reason, Resource Limitation or Resource Unavailable when the reason is configured as User Defined.	Format: pulldown list Range: Resource Unavailable, User Specific Reason, Resource Limitation (Congestion)
Resource Unavailable Reason	Unavailable Reason provides additional detail regarding whether the Resource Unavailable specified for the Abort Choice field is as a result of a short or long term limitation.	Format: pulldown list Range: Short Term or Long Term Limitation
Congestion		
Action	Indicates the action to take if the given exception occurs.	Format: radio buttons> Range: Discard, Send Error to SS7 Network
Error Cause	If the configured Action is Send Answer, this Error Cause value is used in those cases where a TC-U-ERROR message is sent to the SS7 network.	Format: pulldown list Range: System Failure, Data Missing, Unexpected Data Value, Facility Not Supported, Incompatible Terminal, Resource Limitation

Field (* indicates a required field)	Description	Data Input Notes
Abort Reason	If the configured Action is Send Answer, this Abort Reason value is used in those cases where a MAP-U-ABORT message is sent to the SS7 network.	Format: pulldown list Range: User Defined, Application Context Not Supported, Dialog Refused
Abort Choice	Abort Choice further qualifies the Abort action as either Specific Reason, Resource Limitation or Resource Unavailable when the reason is configured as User Defined.	Format: pulldown list Range: Resource Unavailable, User Specific Reason, Resource Limitation (Congestion)
Resource Unavailable Reason	Unavailable Reason provides additional detail regarding whether the Resource Unavailable specified for the Abort Choice field is as a result of a short or long term limitation.	Format: pulldown list Range: Short Term or Long Term Limitation

CCNDC Mapping Configuration

The **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page is used to configure mapping of a Country Code (CC) plus National Destination Code (NDC) to a Diameter Realm in the MD-IWF application.

CCNDC Mapping is used when translating a MAP Request message to a Diameter Request message, when the MAP message Global Title Address (GTA) digits are in MGT format (for ITU, the SCCP CdPA Numbering Plan is E.214).

When a CCNDC Mapping entry matches the CCNDC in the GTA digits, the configured Diameter Realm from the entry is populated into the Destination-Realm AVP of the Diameter Request Message.

The fields are described in *CCNDC Mapping Elements*.

On the **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page, you can:

- Filter the list of entries, to display only the desired entries.
- Sort the list entries in ascending or descending order by by clicking the column heading. By default, the list is sorted by **CCNDC** in ascending ASCII order.
- Click **Insert**.

  The **Diameter Common** > **Network Identifiers** > **CCNDC Mapping** page opens. You can add new CCNDC Mapping entries. If the maximum number of CCNDC Mapping entries (2500) already exists in the system, the **Diameter Common** > **Network Identifiers** > **CCNDC Mapping [Insert]** page will not open, and an error message is displayed.

- Select a CCNDC Mapping entry in the list, and click **Edit**.

The **Diameter Common** > **Network Identifiers** > **CCNDC Mapping [Edit]** page opens. The selected CCNDC Mapping entry can be edited.

- Select a CCNDC Mapping entry in the list, and click **Delete** to remove the selected entry.

CCNDC Mapping Elements

Table 14: CCNDC Mapping Elements describes the fields on the **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** pages. Data Input Notes apply to Insert and Edit pages; the View page is Read-only.

Table 14: CCNDC Mapping Elements

Field (* indicates a required field)	Description	Data Input Notes
*CCNDC	Country Code (CC) plus National Destination Code (NDC) that is used when translating a MAP message received with a E.214 Global Title Address	Format: text box; numeric string; valid digits are 0-999999999999999 Range: 0-15 digits
*Realm	Diameter Realm that is associated with the CCNDC.	Format: text box Case-insensitive string consisting of a list of labels separated by dots, where a label can contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores can be used only as the first character. A label can be at most 63 characters long, and a Realm can be at most 255 characters long. Range: A valid Realm, or empty
Description	Optional description of the mapping, or a note.	Format: text box Range: 0-255 characters

Adding CCNDC Mapping Entries

Use this task to configure new **CCNDC Mapping** entries.

CCNDC Mapping fields are described in *CCNDC Mapping Elements*.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping**.

   The **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page appears.

2. Click **Insert**.

   The **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping [Insert]** page appears.

3. Enter a value for each field.

4. Click:

- **OK** to save the new entry and return to the **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page.
- **Apply** to save the new entry and remain on this page. The data displayed on the page is updated.
- **Cancel** to return to the **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page without saving any changes.

Editing CCNDC Mapping Entries

Use this task to change **CCNDC Mapping** entries.

CCNDC Mapping fields are described in *CCNDC Mapping Elements*.

When the **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping [Edit]** page opens, the fields are populated with the current configured values.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping**.

   The **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page appears.

2. Select the **CCNDC Mapping** entry to be changed.

3. Click **Edit**.

   The **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping [Edit]** page appears.

4. Edit the fields that need to be changed.

5. Click:

- **OK** to save the changes and return to the **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page.
- **Apply** to save the changes and remain on this page.
- **Cancel** to return to the **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page without saving any changes.

Deleting CCNDC Mapping Entries

Use this task to delete an **CCNDC Mapping** entry.

1. On the NOAM, select **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping**.

   The **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page appears.

2. Select the **CCNDC Mapping** entry to be deleted.

3. Click **Delete**.

   A popup window appears to confirm the delete.

4. Click:

- **OK** to delete the **CCNDC Mapping** entry.

- **Cancel** to cancel the delete function and return to the **MAP-Diameter IWF** > **Configuration** > **CCNDC Mapping** page.

If **OK** is clicked and the selected **CCNDC Mapping** entry no longer exists (it was deleted by another user), an error message is displayed.

Chapter

6

DM-IWF Application Configuration

Topics:

The **MAP-Diameter IWF > Configuration** SOAM GUI pages for DM-IWF components provide fields for entering the configuration information for the DM-IWF application.

DM-IWF Options Configuration

The **MAP-Diameter IWF** > **Configuration** > **DM-IWF Options** page is used to configure DM-IWF application Options.

Note: DM-IWF configuration can be performed only on Active SOAM servers.

The fields are described in *DM-IWF Options Elements*.

On the **MAP-Diameter IWF** > **Configuration** > **DM-IWF Options** page, you can:

- Modify current Options values, and click **Apply** to save the changes.
- Click **Cancel** to remove and not save any changes you have made.

DM-IWF Options Elements

Table 15: DM-IWF Options Elements describes the fields on the **DM-IWF Options** page.

Table 15: DM-IWF Options Elements

Field (* indicates a required field)	Description	Data Input Notes
*Unavailable Action	Specifies what action to take if the DM-IWF application is unavailable	Format: pulldown list Range: Continue Routing, Send Answer, Default Route Default: Send Answer
Application Unavailable Route List	Specifies the name of a configured Route List. This Route List is used if the Unavailability Action is set as Default Route and the DM-IWF application is not available. In this case, this Route List will be used for routing the request messages and the PRT Rules will be bypassed.	Format: pulldown list Range: list of possible Route Lists Default: Not Selected
Application Unavailable Result Code	Given that the Unavailable Action must be Send Answer, if the DSR application is not Available, then this value is used in the Result-Code or Experimental-Result AVP of the Answer message.	Format: text box, pulldown list Range: 1000-5999 Default: 3002 UNABLE_TO_DELIVER
Application Unavailable Vendor ID	If zero, then a Result-Code AVP will be sent when the DSR Application is not Available. If non-zero, then an Experimental-Result AVP will be sent will the Vendor-Id AVP set to this value.	Format: text box Range: 0-4294967295 Default: 0

Field (* indicates a required field)	Description	Data Input Notes
Application Unavailable Error Message	If a non-null string, then an Error-Message AVP will be sent in the Answer response containing this string when the DSR Application is not Available.	Format: text box Range: 0-64 characters Default: DM-IWF Unavailable
*DSR Application-Invoked AVP Insertion	If set to Yes, this AVP will be inserted into the Request message that is routed to prevent multiple invocations of the same DSR Application on different DSRs or MPs.	Format: radio buttons Range: Yes or No
*Shutdown Mode	Allows the operator to specify the shutdown method used when the Admin State is changed to Disabled. The application can be disabled using either a graceful or forced shutdown method. Graceful allows in-process transactions to continue for a configurable time period before disabling. Forced is an immediate shutdown.	Format: radio buttons Range: Forced or Graceful
*Shutdown Timer	Number of seconds that the Shutdown Timer will run during a Graceful shutdown.	Format: text box, 2-digit numeric Range: 1-30 seconds Default: 15 seconds
Realm	If the DM-IWF originates Answers, this value is used as Origin Realm. If no value is supplied the local node realm of the ingress connection is used. Realm and FQDN must either both be provisioned or must both be NULL. This applies to MAP to Diameter Requests only.	Format: text box Range: a valid Realm or empty
Fully Qualified Domain Name	If the DM-IWF originates Answers, this value is used as the Origin Host. If no value is supplied the local node FQDN of the ingress connection is used. Realm and FQDN must both be provisioned or must both be NULL.	Format: text box Range: a valid FQDN or empty
ART	Optional attribute which specifies which ART to search when DM-IWF forwards a Request message to DRL. If this value is NULL, DRL will select an ART to search based on a well-defined set of rules.	Format: pulldown list Default: N/A

Field (* indicates a required field)	Description	Data Input Notes
PRT	Optional attribute which specifies which PRT to search if no ART rules match the content of the Request message forwarded from DM-IWF to DRL. If this value is NULL, DRL will select an PRT to search based on a well-defined set of rules.	Format: pulldown list Default: N/A

Diameter Exception Configuration

The **MAP-Diameter IWF** > **Configuration** > **Diameter Exception** page on an SOAM server is used to configure Diameter Exceptions.

The fields are described in *Diameter Exception Elements*.

MAP-Diameter IWF supports various Diameter Exception types:

- Internal Processing Errors (internal to the DSR) such as:

  - Resource Exhaustion
  - Congestion
  - Unexpected software validation error

- Diameter to MAP Transaction Timeout (a timeout occurred waiting for a response from the SS7 network)
- Translation Error (an error occurred while performing Message Translation or Address Translation, or while translating between a TCAP User error cause value and a Diameter Result-Code)

On the **MAP-Diameter IWF** > **Configuration** > **Diameter Exception** page, you can:

- Modify current Options values, and click **Apply** to save the changes.
- Click **Cancel** to remove and not save any changes you have made.

Diameter Exception Elements

Table 16: DM-IWF Diameter Exception Elements describes the fields on the **Diameter Exception** page.

Table 16: DM-IWF Diameter Exception Elements

Field (* indicates a required field)	Description	Data Input Notes
IWF Internal Processing Error		
Action	Indicates the action to take if the given exception occurs.	Format: radio buttons Range: Discard, Send Answer, or Apply Unavailability Action

Field (* indicates a required field)	Description	Data Input Notes
Response Result Code AVP	If the configured Action is Send Answer, this value is used in the Result-Code or Experimental-Result AVP of the Diameter Answer message.	Format: text box, pulldown list Range: 1000-5999
Response Vendor ID	If zero, then a Result-Code AVP will be sent in the Diameter Answer message. If non-zero, then an Experimental-Result AVP will be sent with the Vendor-Id AVP set to this value.	Format: text box Range: 0-4294967295
Response Error String	If a non-empty string, this configured string will be appended to the Error-Message AVP that is sent in the Diameter Answer message.	Format: text box Range: 0-64 characters
Diameter to MAP Transaction Timeout		
Action	Indicates the action to take if the given exception occurs.	Format: radio buttons Range: Discard, Send Answer, or Apply Unavailability Action
Response Result Code AVP	If the configured Action is Send Answer, this value is used in the Result-Code or Experimental-Result AVP of the Diameter Answer message.	Format: text box, pulldown list Range: 1000-5999
Response Vendor ID	If zero, then a Result-Code AVP will be sent in the Diameter Answer message. If non-zero, then an Experimental-Result AVP will be sent with the Vendor-Id AVP set to this value.	Format: text box Range: 0-4294967295
Response Error String	If a non-empty string, this configured string will be appended to the Error-Message AVP that is sent in the Diameter Answer message.	Format: text box Range: 0-64 characters
Translation Error		
Action	Indicates the action to take if the given exception occurs.	Format: radio buttons Range: Discard, Send Answer, or Apply Unavailability Action

Field (* indicates a required field)	Description	Data Input Notes
Response Result Code AVP	If the configured Action is Send Answer, this value is used in the Result-Code or Experimental-Result AVP of the Diameter Answer message.	Format: text box, pulldown list Range: 1000-5999
Response Vendor ID	If zero, then a Result-Code AVP will be sent in the Diameter Answer message. If non-zero, then an Experimental-Result AVP will be sent with the Vendor-Id AVP set to this value.	Format: text box Range: 0-4294967295
Response Error String	If a non-empty string, this configured string will be appended to the Error-Message AVP that is sent in the Diameter Answer message.	Format: text box Range: 0-64 characters

Chapter

7

Maintenance for MD-IWF

Topics:

This section describes maintenance functions and information that can be used with the MD-IWF application.

Overview

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

- The **Diameter** > **Maintenance** > **Applications** page displays MD-IWF status information including Admin State, Operational Status, and Operational Reason. The page also provides functions to enable and disable the application. Refer to the *Diameter User Guide* and Help for explanations of the page and the status information.
- The **Communication Agent** > **Maintenance** > **Routed Services Status** page displays ComAgent Status information for MD-IWF Routed Service (MDIWFSvc) Service Providers and Users. Refer to the *Communication Agent User's Guide* for explanations of the page and status information.

MD-IWF Administrative State and Operational Status

The MD-IWF application has an Administrative State and an Operational Status. The Administrative State (or Admin State - enabled or disabled) indicates the state that the operator desires the MD-IWF application to be in. The Admin State can be manually modified by the operator. The Operational Status indicates the actual status of the MD-IWF application.

Table 17: MD-IWF Admin State and Operational Status lists the MD-IWF Admin State and Operational Status related to the MD-IWF Routed Service State, MD-IWF Routed Service Congestion Level and MD-IWF (internal) congestion levels. It specifies the actions that MD-IWF will take in various situations.

ComAgent DM-IWF Routed Service presents an aggregated view of the all DM-IWF instances (one instance per DA-MP) that have registered as service providers for the DM-IWF Routed Service. ComAgent reports the DM-IWF Routed Service State and the DM-IWF Routed Service Congestion Level to each MD-IWF instance.

In the Diameter to MAP direction, the MD-IWF Operational Status and the DM-IWF Routed Service congestion level determine whether a given Request from DRL can be forwarded to an MD-IWF. The MD-IWF Operational Status is determined by multiple attributes including MD-IWF Admin State, MD-IWF (internal) congestion level, MD-IWF Routed Service State and MD-IWF Service Congestion Level. In *Table 17: MD-IWF Admin State and Operational Status*, MD-IWF Congestion Level is the maximum of the MD-IWF (internal) Congestion Level and MD-IWF Routed Service Congestion Level.

In *Table 17: MD-IWF Admin State and Operational Status*, the MD-IWF Admin State, DM-IWF ComAgent Provider Status, MD-IWF Congestion State, and SS7-MP isolated from SS7 network? are the inputs for calculating the MD-IWF Operational Status, MD-IWF Operational Reason, and MD-IWF Operational Color.

Table 17: MD-IWF Admin State and Operational Status

MD-IWF Admin State	DM-IWF ComAgent Provider Status (rolled-up state of all DM-IWF providers)	MD-IWF Congestion State	SS7-MP isolated from SS7 network?	MD-IWF Operational Status	MD-IWF Operational Reason	MD-IWF Operational Color	MD-IWF ComAgent Provider Status (calculated on each SS7-MP)
N/A	N/A	N/A	N/A	Unavailable	Not Initialized	Orange	Unregistered
Disabled	N/A	N/A	N/A	Unavailable	Shut Down	Orange	Unregistered
Enabled	Down	N/A	No	Degraded	Diam Network Unavailable	Red	Available
Enabled	Degraded (CL1, CL2, CL3)	CL0	No	Degraded	Diam Network Degraded	Yellow	Available
Enabled	Degraded (CL1, CL2, CL3)	CL1, CL2, CL3	No	Degraded	Diam Network Degraded/ Congested	Yellow	CL1, CL2, CL3
Enabled	Normal	CL1, CL2, CL3	No	Degraded	Congested	Yellow	CL1, CL2, CL3
Enabled	N/A	N/A	Yes	Unavailable	Isolated from SS7 network	Red	Unavailable
Enabled	Normal	CL0	No	Available	Normal	Gray	Available

MD-IWF Alarms, KPIs, and Measurements

This section describes how to access alarm, KPI, and measurements information that is available for MD-IWF in the DSR GUI. For more detailed information, refer to the *Alarms, KPIs, and Measurements Reference*.

Active alarms and events, as well as alarm and event history can be displayed on the **Alarms & Events** > **View Active** and **Alarms & Events** > **View History** GUI pages.

Key Performance Indicators, or KPIs, provide a means to convey performance information to the user in near real-time. KPIs can be displayed on the **Status & Manage** > **KPIs** GUI page.

Measurements for MD-IWF are collected and reported in various measurement groups. A measurement report and measurement group can be associated with a one-to-one relationship. Measurement reports may be generated from the **Measurements** > **Report** GUI page.

Chapter

8

Maintenance for DM-IWF

Topics:

This section describes maintenance functions and information that can be used with the DM-IWF application.

Overview

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

- The **Diameter** > **Maintenance** > **Applications** page displays DM-IWF status information including Admin State, Operational Status, and Operational Reason. The page also provides functions to enable and disable the application. Refer to the *Diameter User Guide* and Help for explanations of the page and the status information.
- The **Diameter** > **Maintenance** > **DA-MPs** page displays status and connectivity information for the DA-MP that is running the DM-IWF application. Refer to the *Diameter User Guide* and Help for explanations of the page and the status information.
- The **Communication Agent** > **Maintenance** > **Routed Services Status** page displays ComAgent Status information for Service Providers and Users of DM-IWF Routed Service (DMIWFSvc) and MD-IWF Routed Service (MDIWFSvc). Refer to the *Communication Agent User's Guide* for explanations of the page and status information.

DM-IWF Administrative State and Operational Status

The DM-IWF application has an Administrative State and an Operational Status. The Administrative State (or Admin State - enabled or disabled) indicates the state that the operator desires the DM-IWF application to be in. The Admin State can be manually modified by the operator. The Operational Status indicates the actual status of the DM-IWF application.

Table 18: DM-IWF Admin State and Operational Status lists the DM-IWF Admin State and Operational Status related to the MD-IWF Routed Service State, MD-IWF Routed Service Congestion Level and DM-IWF (internal) congestion levels. It specifies the actions that DM-IWF will take in various situations.

ComAgent MD-IWF Routed Service presents an aggregated view of the all MD-IWF instances (one instance per SS7-MP) that have registered as service providers for the MD-IWF Routed Service. ComAgent reports the MD-IWF Routed Service State and the MD-IWF Routed Service Congestion Level to each DM-IWF instance.

In the Diameter to MAP direction, the DM-IWF Operational Status and the MD-IWF Routed Service congestion level determine whether a given Request from DRL can be forwarded to an MD-IWF. The DM-IWF Operational Status is determined by multiple attributes including DM-IWF Admin State, DM-IWF (internal) congestion level, MD-IWF Routed Service State and MD-IWF Service Congestion Level. In *Table 18: DM-IWF Admin State and Operational Status*, DM-IWF Congestion Level is the maximum of the DM-IWF (internal) Congestion Level and MD-IWF Routed Service Congestion Level.

In *Table 18: DM-IWF Admin State and Operational Status*, the DM-IWF Admin State, DM-IWF Congestion State, DM-IWF Shutting Down State, and the MD-IWF Routed Service State are used as inputs for calculating the DM-IWF Operational Status, DM-IWF Operational Reason, and DM-IWF Operational Reason Color.

Table 18: DM-IWF Admin State and Operational Status

DM-IWF Admin State	DM-IWF Congestion State	DM-IWF Shutting Down State	MD-IWF Routed Service State	DM-IWF Operational Status	DM-IWF Operational Reason	DM-IWF Operational Reason Color
Disabled	N/A	False	N/A	Unavailable	Shut down	Orange
Enabled	0	N/A	Available	Available	Normal	Gray
Enabled	1	N/A	Available	Available	Congested	Yellow
Enabled	2	N/A	Available	Degraded	Congested	Yellow
Enabled	3	N/A	Available	Unavailable	Congested	Red
Enabled	0	N/A	Degraded[1]	Available	SS7 Degraded	Yellow
Enabled	1	N/A	Degraded	Available	SS7 Degraded/ Congested	Yellow
Enabled	2	N/A	Degraded	Degraded	SS7 Degraded/ Congested	Yellow
Enabled	3	N/A	Degraded	Unavailable	SS7 Degraded/ Congested	Red
Enabled	0	N/A	Unavailable	Unavailable	SS7 Unavailable	Red
Enabled	1, 2, 3	N/A	Unavailable	Unavailable	SS7 Unavailable/ Congested	Red

DM-IWF Alarms, KPIs, and Measurements

This section describes how to access alarm, KPI, and measurements information that is available for DM-IWF in the DSR GUI. For more detailed information, refer to the *Alarms, KPIs, and Measurements Reference*.

Active alarms and events, as well as alarm and event history can be displayed on the **Alarms & Events** > **View Active** and **Alarms & Events** > **View History** GUI pages.

Key Performance Indicators, or KPIs, provide a means to convey performance information to the user in near real-time. KPIs can be displayed on the **Status & Manage** > **KPIs** GUI page

---

[1] MD-IWF Route Service State of Degraded does not impact DM-IWF's Operational Status.

Measurements for DM-IWF are collected and reported in various measurement groups. A measurement report and measurement group can be associated with a one-to-one relationship. Measurement reports may be generated from the **Measurements** > **Report** GUI page.

Glossary

A

ART

Application Routing Table

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 (for example, routing information) as well as authentication, authorization or accounting information.

C

ComAgent

Communication Agent

A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.

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 that can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.

D

DCA

DOIC Capabilities Announcement

DM-IWF

Diameter MAP–Interworking

DSR application that translates Diameter messages into MAP messages.

DNS

Domain Name System

A system for converting Internet host and domain names into IP addresses.

DRA

Diameter Routing Agent

A functional element in a 3G or 4G (such as LTE) wireless network that provides real-time routing capabilities to ensure that messages are routed among the correct elements in a network.

DSCP

Differentiated Services Code Point

Provides a framework and building blocks to enable deployment of scalable service discrimination in the internet. The differentiated services are realized by mapping the code point contained in a field in the IP packet header to a particular forwarding treatment or per-hop behavior (PHB). Differentiated services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.

G

G

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.

GTA

Global Title Address

GUI

Graphical User Interface

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

H

HA

High Availability

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

I

IDIH

Integrated Diameter Intelligence Hub

IP

Internet Protocol - IP specifies the format of packets, also called datagrams, and the addressing

I

scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

K

KPI

Key Performance Indicator

L

LDAP

Lightweight Directory Access Protocol

A protocol for providing and receiving directory information in a TCP/IP network.

M

MAP

Mobile Application Part

An application part in SS7 signaling for mobile communications systems.

MD-IWF

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

MEAL

Measurements, Events, Alarms, and Logs

MP

Message Processor - The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM components. All Message Processors replicate from their

M

Signaling OAM's database and generate faults to a Fault Management System.

N

NAS

Network Access Server

A single point of access or gateway to a remote resource. NAS systems are usually associated with AAA servers.

NOAM

Network Operations, Administration, and Maintenance

NOAMP

Network Operations, Administration, Maintenance, and Provisioning

O

OAM

Operations, Administration, and Maintenance. These functions are generally managed by individual applications and not managed by a platform management application, such as PM&C.

Operations – Monitoring the environment, detecting and determining faults, and alerting administrators.

Administration – Typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning, using usage data, and maintaining system reliability.

Maintenance – Provides such functions as upgrades, fixes, new feature enablement, backup and restore tasks, and monitoring media health (for example, diagnostics).

O

OCS

Online Charging System

A system allowing a Communications Service Provider to charge customers in real time based on service usage.

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.

In the Policy Management system, PCRF is located in the MPE device.

Software node designated in real-time to determine policy rules in a multimedia network.

Peer Route Table

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

PRT

Peer Route Table or Peer Routing Table

R

RADIUS

Remote Authentication Dial-In User Service

A client/server protocol and associated software that enables remote access servers to communicate with a central server to authorize their access to the requested service. The MPE device

R

functions with RADIUS servers to authenticate messages received from remote gateways. See also Diameter.

S

SBR

Session Binding Repository

A highly available, distributed database for storing Diameter session binding data.

SFTP

SSH File Transfer Protocol (sometimes also called Secure File Transfer Protocol)

A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network over any reliable data stream. It is typically used over typically used with version two of the SSH protocol.

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

SS7

Signaling System #7

S

A communications protocol that
allows signaling points in a
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.

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.

U

UDR

User-Data-Request

A user-identity and service
indication sent by a Diameter client
to a Diameter server in order to
request user data.