

**Oracle® Communications
Diameter Signaling Router**

DSR Administration Guide

E53475 Revision 01

July 2014

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

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

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

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

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

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

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

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

Table of Contents

Part I: Introduction.....	9
Chapter 1: About the DSR Administration Guide.....	10
Introduction.....	11
Scope and Audience.....	11
Documentation Admonishments	11
Document Organization.....	12
My Oracle Support (MOS).....	13
Emergency Response.....	13
Related Publications.....	13
Locate Product Documentation on the Oracle Technology Network Site.....	14
Part II: Diameter Signaling Router (DSR).....	15
Chapter 1: Diameter Signaling Router (DSR).....	16
Diameter Signaling Router Overview.....	17
DSR Functions.....	20
Chapter 2: Diameter Protocol.....	23
Diameter Overview.....	24
Diameter Transport Function.....	24
Diameter Routing Function.....	25
DSR Application Infrastructure.....	26
Tekelec Vendor-specific AVPs.....	27
Oracle Vendor-specific AVPs.....	29
Chapter 3: Diameter Mediation.....	32
Mediation Overview.....	33
Chapter 4: DSR Applications.....	35

DSR Applications Overview.....	36
Chapter 5: IP Front End (IPFE).....	43
Introduction to IPFE.....	44
Traffic distribution.....	44
High Availability.....	44
IPFE Associations.....	45
Association Aging.....	45
Load Balancing.....	45
IPv4 and IPv6 support.....	46
Throttling.....	46
Part III: DSR Configuration.....	47
Chapter 1: DSR Configuration Overview.....	48
DSR Configuration.....	49
Chapter 2: IPFE Configuration.....	53
IPFE Configuration Overview.....	54
IPFE Configuration Options.....	54
IPFE Target Sets Configuration.....	54
Chapter 3: Diameter Configuration.....	55
Diameter Configuration Overview.....	56
Diameter Common Configuration Overview.....	59
Configuration Capacity Summary.....	60
Connection Capacity Validation.....	64
Application Ids Configuration.....	65
Transport configuration.....	65
CEX Parameters Configuration.....	65
Command Codes Configuration.....	65
Configuration Sets.....	65
Local Nodes.....	68
Peer Nodes.....	68
Connections.....	69
Routing Configuration.....	70
Diameter Routing Functions.....	70

Route Group Configuration.....	74
Route List Configuration.....	74
Routing Option Sets Configuration.....	75
Peer Route Tables Configuration.....	75
Pending Answer Timer.....	75
Reroute On Answer.....	76
Application Routing Rules Configuration.....	77
Message Copy Configuration Set configuration.....	78
Diameter Options Configuration.....	78
System Options Configuration.....	78
DNS Options Configuration.....	78
Diameter Mediation Configuration Overview.....	78

Chapter 4: DSR Applications Configuration.....80

DSR Applications Configuration Overview.....	81
--	----

Part IV: Maintenance, Status, and Reports.....82

Chapter 1: Diameter Maintenance.....83

Introduction.....	84
Diameter Maintenance and Status Data for Components, DSR Applications, and DA-MPs.....	85
Route Lists Maintenance.....	86
Route Groups Maintenance.....	86
Peer Nodes Maintenance.....	87
Connection Maintenance.....	87
Egress Throttle Groups Maintenance.....	87
Applications Maintenance.....	87
DA-MPs Maintenance.....	88
Managing the Status of Diameter Configuration Components.....	88

Chapter 2: Diameter Reports.....93

Diameter Diagnostics Tool.....	94
Diameter MP Statistics (SCTP) Report.....	94

Part V: Tools and Utilities.....95

Chapter 1: Imports and Exports	96
DSR Bulk Import and Export.....	97
Diameter Mediation Import and Export Overview.....	98
 Chapter 2: IPsec.....	 100
IPsec Overview.....	101
IPsec IKE and ESP elements.....	103
Accessing platcfg.....	104
Adding an IPsec connection.....	105
Editing an IPsec connection.....	105
Enabling and Disabling an IPsec Connection.....	106
Deleting an IPsec connection.....	107
Logging out of platcfg.....	107
 Chapter 3: Integrated Diameter Intelligence Hub.....	 108
Integrated Diameter Intelligence Hub Overview.....	109
Accessing IDIH.....	109
 Chapter 4: Database Backups and Restores.....	 110
Database Backups and Restores.....	111
Creating a Database Backup.....	112
Transferring a Database Backup File to Another Location.....	113
Database Restores.....	113
Glossary.....	114

List of Figures

Figure 1: DSR Topology.....	18
Figure 2: DSR OAM Architecture.....	19
Figure 3: Weighted Load Sharing.....	69
Figure 4: DSR Routing Diagram.....	71
Figure 5: Route List, Route Group, and Peer Node Relationships.....	72
Figure 6: Route Group Weights.....	72
Figure 7: DSR Implicit Routing.....	73

List of Tables

Table 1: Tekelec Vendor-specific AVP Formats.....	27
Table 2: Maximum values per NE and per Configuration Component.....	61
Table 3: Diameter Configuration Component Status Dependencies.....	85
Table 4: Route List Status Data.....	86
Table 5: Maintenance and Status Data Sourcing Methods.....	88
Table 6: Diameter Configuration Component Sourcing Methods.....	89
Table 7: IPsec IKE and ESP elements.....	103

Part I

Introduction

Topics:

- [About the DSR Administration Guide.....10](#)

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

Chapter 1

About the DSR Administration Guide

Topics:

- [Introduction.....11](#)
- [Scope and Audience.....11](#)
- [Documentation Admonishments11](#)
- [Document Organization.....12](#)
- [My Oracle Support \(MOS\).....13](#)
- [Emergency Response.....13](#)
- [Related Publications.....13](#)
- [Locate Product Documentation on the Oracle Technology Network Site.....14](#)

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

For additional copies, contact your Sales Representative.

Introduction

This document provides administrative information for the DSR, including:

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

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

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

Scope and Audience

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

Documentation Admonishments

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

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



TOPPLE

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



DANGER

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



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



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

Document Organization

This document is organized into the following chapters:

- [About the DSR Administration Guide](#) contains general information about this guide, the organization of this guide, descriptions of and how to locate Related Publications, and how to get technical assistance.
- [Diameter Signaling Router \(DSR\)](#) describes the components and functions of the Diameter Signaling Router, the Diameter protocol, Diameter Mediation, DSR Applications, and IP Front End (IPFE):
 - [Diameter Signaling Router \(DSR\)](#) describes the DSR topology, architecture, components, and functions
 - [Diameter Protocol](#) describes the functions of the Diameter base protocol in the DSR.
 - [Diameter Mediation](#) describes Diameter Mediation functions.
 - [DSR Applications](#) describes the DSR Applications that are supported by the DSR.
 - [IP Front End \(IPFE\)](#) describes IPFE functions.
- [DSR Configuration](#) describes configuration of IPFE, the Diameter protocol, Diameter Mediation, and DSR Applications:
 - [DSR Configuration Overview](#) provides an overview of DSR configuration and GUI structure.
 - [IPFE Configuration](#) describes IPFE configuration.
 - [Diameter Configuration](#) describes configuration of Diameter protocol components.
 - [DSR Applications Configuration](#) describes configuration of the FABR, RBAR, CPA, Policy DRA, and GLA DSR Applications.
- [Maintenance, Status, and Reports](#) describes DSR Maintenance, Status, and Reports features and functions:
 - [Diameter Maintenance](#) describes Diameter Maintenance functions.
 - [Diameter Reports](#) describes the Diagnostics Tool and report, and the MP Statistics (SCTP) report.
- [Tools and Utilities](#) describes the following DSR tools and utilities:
 - [Imports and Exports](#) describes Import and Export functions for Diameter configuration data and for Diameter Mediation Rule Templates.
 - [IPsec](#) describes the configuration, functions, and use of IPsec for secure connections.
 - [Integrated Diameter Intelligence Hub](#) provides a brief description of the use of the Diameter Intelligence Hub (DIH) with the DSR.
 - [Database Backups and Restores](#) describes DSR-related database backup and restore functions.

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 **2** for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

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.

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology

Network (OTN) site. See [Locate Product Documentation on the Oracle Technology Network Site](#) for more information.

Locate Product Documentation on the Oracle Technology Network Site

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

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

Part II

Diameter Signaling Router (DSR)

Topics:

- *Diameter Signaling Router (DSR).....16*
- *Diameter Protocol.....23*
- *Diameter Mediation.....32*
- *DSR Applications.....35*
- *IP Front End (IPFE).....43*

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

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

Chapter 1

Diameter Signaling Router (DSR)

Topics:

- [Diameter Signaling Router Overview.....17](#)
- [DSR Functions.....20](#)

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

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

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

Diameter Signaling Router Overview

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

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

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

Configuring the DSR requires:

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

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

The architecture includes the following characteristics:

- Each DSR service signals traffic to and from a collection of Diameter clients, servers, and agents.
- Each DSR supports :
 - OAM servers (OAM), operating in Active/Standby mode; NOAM and SOAM servers.
 - Two message processors (DA-MPs), operating in Active/Standby mode, or up to 16 DA-MPs in Active/Active mode.
- The DSR MPs provide the Diameter message handling function. Each DSR MP supports connections to all of the DSR Peers.
- DSRs are deployed in mated pairs for purposes of geo-redundancy.
- The Integrated Diameter Intelligence Hub (IDIH) provides the ability to filter, access, and troubleshoot Diameter transactions,

The [Figure 1: DSR Topology](#) provides an overview of the DSR architecture.

DSR Topology

In DSR topology, as shown in [Figure 1: DSR Topology](#), there are NOAM servers, SOAM servers, and MP servers.

The DSR topology, GUI screens can be used to configure and manage:

- On a DSR NOAM, network topology data (such as user accounts, network elements, servers, and server groups). Network-wide Policy DRA data, MAP-Diameter Interlocking data for MD-IWF and Diameter Topology Hiding data are configured on NOAM GUI pages. Diameter Common provides the Import and Export GUIs on the NOAM for exporting and importing the SOAM configuration data for Diameter Configuration, IPFE, and DSR Applications.
- On a DSR SOAM, Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists), MAP-Diameter Interlocking data for MD-IWF, DSR Application data (RBAR, FABR, CPA, Policy DRA, and GLA), Profile Assignments and IPFE configuration data. Diameter Common provides the Import and Export GUIs on the SOAM for exporting and importing the SOAM configuration data for Diameter Configuration, IPFE, and DSR Applications.

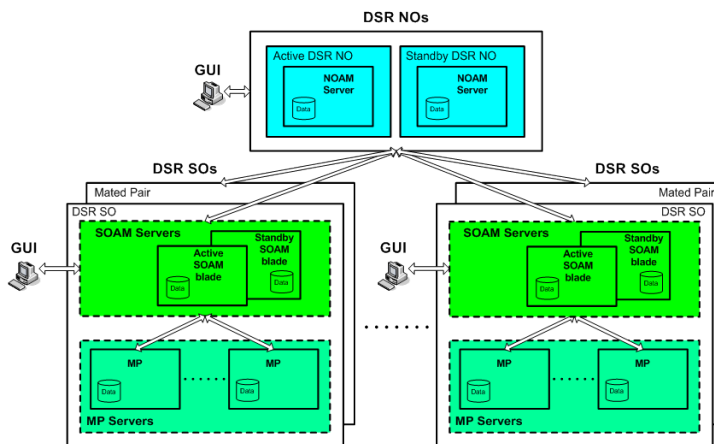


Figure 1: DSR Topology

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

Deployment with SDS

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

The SDS/DP system consists of a Primary Provisioning Site, a Disaster Recovery (DR) Provisioning Site, and up to 24 DSR Signaling Site servers with redundant DP SOAM servers and up to 2 DP blades. Each Provisioning Site has an Active/Standby pair of servers in a high availability (HA) configuration and a third server configured as a Query Server.

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

OAM Servers

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

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

The OAM servers provide the following services:

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

Figure 2: DSR OAM Architecture illustrates the DSR OAM architecture.

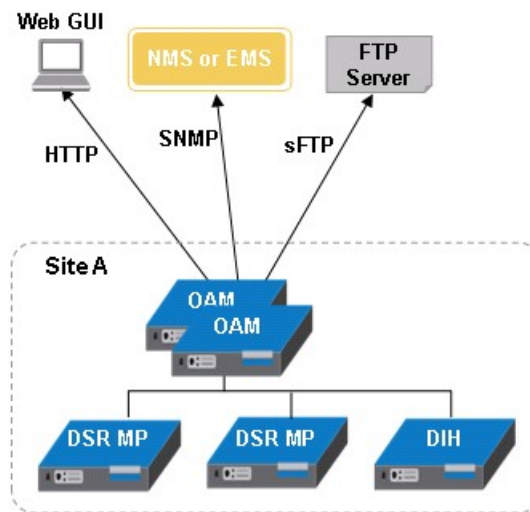


Figure 2: DSR OAM Architecture

Message Processors

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

Integrated Diameter Intelligence Hub

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

DSR Functions

The DSR provides the following functions:

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

The **IP Front End (IPFE)** can run in a DSR system to distribute IPv4 and IPv6 connections from multiple clients to multiple Diameter Agent Message Processors (DA-MPs).

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

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

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

The DSR supports multiple Diameter connections to any Peer Node and multiple Peer Nodes.

- **SCTP and TCP transport protocols:** The DSR supports both Stream Control Transmission Protocol (SCTP uni-homing and multi-homing) and Transmission Control Protocol (TCP) based transport connections.
- **Message Processing:** Processing of Diameter Peer-to-Peer messages (CER/CEA, DWR/DWA, DPR/DPA), and delivery of Diameter Request and Answer messages from and to Diameter Peers and the Diameter Routing Function.
- **Diameter Routing Function:**
 - **Routing of Diameter Request and Answer messages** to and from Diameter Peers (through the Diameter Transport Function) and DSR Applications.
 - **Peer Routing Rules:** The DSR provides the ability to configure Peer Routing Rules that define where to route a Diameter message to an upstream Peer based upon Diameter message content.
 - **Processing of Diameter connection status** from the Diameter Transport Function and status from DSR Applications for maintaining dynamic routing configuration data.
 - **Message Rerouting:** A Diameter Relay Agent is responsible for making sure that Request messages are successfully delivered and to alternate route if failures are encountered.
 - **Alternate Implicit Routing:** Instead of a message being routed directly to an available Peer Node, the message is routed on an “alternate implicit route” that is chosen from a list that has been configured for the Peer Node.
 - **Reroute on Answer:** The DSR supports alternate routing of a Request message when an Answer response is received with a configured error code.
- **Capacity and Congestion Status and Controls:** Provides connection capacity status and controls, ingress message MPS controls, egress message throttling, and Egress Throttle Groups across DA-MPs.
- **MAP-Diameter Interworking Function** allows the DSR to support the bi-directional interworking between Diameter and SS7 (GSM MAP) messages.
 - A Diameter-to-MAP transaction is a Diameter transaction that is initiated by a Diameter Node that is routed to a DSR for MAP-Diameter interworking. The operator is required to configure DRL ART rules which associate a Request message with the DM-IWF application.
 - A MAP-to-Diameter transaction is a MAP procedure that is initiated by a SS7 Node that is routed to a DSR SS7-MP for MAP-Diameter interworking.
- **Diameter Mediation:** The DSR provides configuration and application of rules that modify message processing behavior when conditions are met at specified points in the message processing.
- **Message Copy:** For a message that was routed through the DSR, the Diameter Message Copy feature provides the ability to forward a copy of the Diameter Request message, and optionally the Answer message, to a Diameter Application Server (a DAS Peer). Diameter Message Copy can be triggered by any processing functions acting on the messages, including Diameter Mediation, DSR Applications (such as the Charging Proxy Application - CPA), and Peer Routing Rules.
- **Topology Hiding:** Topology Hiding involves hiding and restoring topology-related information in messages.

Diameter Signaling Router (DSR)

- Diameter Topology Hiding can use Pseudo-Hostnames and encryption to hide topology-related information in messages sent from a Protected Network to an Untrusted Network, and to restore the topology-related information in messages from an Untrusted Network.
- The Policy DRA DSR Application uses a configured list of Policy Client Peer Nodes from which the PCRF name is to be hidden.
- In the Charging Proxy Application (CPA), the Charging Proxy Function provides topology hiding using Virtual CDF and Virtual CTF Local Nodes. The CPF appears as a single CDF to the CTFs, and as a single CTF to the CDFs. The Charging Proxy Function modifies the Origin-Host and Origin-Realm AVPs in each message being routed to a CTF or CDF.
- **Integrated Diameter Intelligence Hub:** The Integrated Diameter Intelligence Hub (DIH) provides the ability to troubleshoot Diameter transactions.
- **DSR Switchover:** The DSR servers operate in redundancy mode and support automatic failover to the standby server if the active server fails. Automatic failover does not require manual intervention.
- **IPsec Support:** The DSR supports transporting messages over Internet Protocol security (IPsec) secure connections.
- **IPv4 and IPv6 Support:** The DSR supports IPv6 and IPv4 IP address formats.

Chapter 2

Diameter Protocol

Topics:

- [*Diameter Overview.....24*](#)
- [*Diameter Transport Function.....24*](#)
- [*Diameter Routing Function.....25*](#)
- [*DSR Application Infrastructure.....26*](#)
- [*Tekelec Vendor-specific AVPs.....27*](#)
- [*Oracle Vendor-specific AVPs.....29*](#)

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

Diameter Overview

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

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

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

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

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

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

DSR Topology

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

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

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

Diameter Transport Function

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

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

The Transport Manager performs the following activities:

- The Transport Manager performs the following activities:

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

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

Limitations

Transport Manager has the following limitations:

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

Diameter Routing Function

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

The Diameter Routing Function is responsible for the following functions:

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

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

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

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

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

Rerouting is attempted for the following types of failures:

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

The following types of rerouting can be attempted:

- Alternate Implicit Routing

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

- Reroute on Answer

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

- Interfacing with the Diameter Transport Function

- Processing Diameter connection status events received from the Diameter Transport Function
- Issuing Diameter connection management events to the Diameter Transport Function
- Routing Diameter messages received from Peer Nodes through the Diameter Transport Function
- Sending Diameter messages to the Diameter Transport Function for forwarding on Diameter connections

- Interfacing with DSR Applications

- Processing Operational Status events from DSR Applications
- Routing Diameter messages received from Peer Nodes to DSR Applications
- Routing Diameter messages received from DSR Applications to Peer Nodes

- Providing Egress Throttle Groups functions across DA-MPs
- Updating routing information based on connection and DSR Application status changes and on OAM configuration and state changes
- Processing routing configuration and maintenance changes from OAM
- Updating alarm, event, KPI, and measurements data for routing configuration components

DSR Application Infrastructure

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

- Full Address Based Resolution (FABR)
- Range Based Address Resolution (RBAR)
- Charging Proxy Application (CPA)
- Policy Diameter Routing Agent (Policy DRA)
- Gateway Location Application (GLA)

The DSR Application Infrastructure is responsible for the following functions:

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

- Updating routing information based on connection and DSR Application status changes and on OAM configuration and state changes

Tekelec Vendor-specific AVPs

The following Tekelec Vendor-specific AVPs are used by the Diameter Routing Function in making decisions for routing messages to and from DSR Applications and for the Diameter Message Copy feature. The AVP formats are shown in [Table 1: Tekelec Vendor-specific AVP Formats](#).

- DSR-Application Invoked
- PDRA-Early-Binding
- Session-Release-Reason
- MsgCopyAnswer

Table 1: Tekelec Vendor-specific AVP Formats

AVP	AVP Code	AVP Length (octets)	Vendor-ID	Data	AVP Flags
DSR-Application-Invoked	2468	16	323	32-bit DSR Application ID in Unsigned32 format <ul style="list-style-type: none"> • RBAR ID = 3 • FABR ID = 4 • CPA ID = 5 • Policy DRA ID = 6 	0 (except V bit=1)
PDRA-Early-Binding	2500	30	323	<ul style="list-style-type: none"> • Master Session Reference • ComAgent Resource Id • ComAgent Subresource Id • Session Id Hash • Self Session Reference 	0 (except V bit=1)
Session-Release-Reason	2501	12+Total length of all included AVPs including headers and padding	323	Error string defined by Policy DRA or Policy SBR. UTF8 String (Max 100 chars)	0 (except V bit=1)
MsgCopyAnswer	2516	Number of octets including 12 octets	323	Octet String; contains all of the AVPs included the original terminating Answer Message.	0 (except V bit=1)

AVP	AVP Code	AVP Length (octets)	Vendor-ID	Data	AVP Flags
		of AVP header			

DSR-Application-Invoked AVP

In order to prevent the same DSR Application from being invoked on multiple DSRs in a network, a DSR can optionally add to the Request message a Tekelec Vendor-specific AVP containing the DSR Application ID.

Each DSR Application Invoked AVP in a Request message from a Peer Node is decoded by the Diameter Routing Function prior to Application Routing Rule processing, to prevent another invocation of the same DSR Application on a subsequent DSR Node. Any Application Routing Rule with this DSR Application ID will be ignored by the Diameter Routing Function.

The DSR Application Invoked AVP can be repeated in the Request to indicate different DSR Applications, but will be inserted only once per DSR Application. A configuration option in each DSR Application can prohibit the insertion of the AVP for that DSR Application.

PDRA-Early-Binding AVP

The Policy DRA application can retrieve AVPs and Group AVPs in a CC-Request message, including the DSR-Application-Invoked and PDRA-Early-Binding AVPs, and store them locally during the lifetime of the CC-Request/CC-Answer transaction.

If a CC-Request is received at the Policy DRA in which a PDRA-Early-Binding AVP is present and neither event 22704 nor 22705 is generated, Policy DRA forwards the CC-Request to the PCRF that is bound to the IMSI contained in the CC-Request. The forwarded CC-Request is modified by Policy DRA in the following way:

- The PDRA-Early-Binding AVP is removed from the original CC-Request message.
- The same Origin-Host and/or Origin-Realm AVPs from the original CC-Request are still used in the forwarded CC-Request.
- An indication is added that Policy DRA does not expect an CC-Answer to this Request.

The CC-Answer will not be sent back to the binding master Policy DRA. The binding slave Policy DRA will receive any responses to this Request and handle the subsequent processes such as applying Topology Hiding.

If a CC-Request is received with an IMSI for which a binding exists, the binding was created for less than 200 ms, and the binding has not been updated, the binding slave Policy DRA:

- Inserts a PDRA-Early-Binding AVP in the CC-Request
- Does not include a DSR-Application-Invoked AVP in the CC-Request
- Forwards the CC-Request to the binding master Policy DRA

The binding slave Policy DRA may receive a CC-Answer from the PCRF that was suggested by the binding master Policy DRA after the CC-Request message is sent to the PCRF. Or it may not receive anything when the binding master Policy DRA returns a CC-Answer with an error to the Policy Client that originated the CC-Request. In the latter case, the binding slave Policy DRA is out of the CC-Answer processing path.

Session-Release-Reason AVP

If Policy DRA initiates a release type RAR, the RAR includes the following AVPs:

- Session-Release-Cause AVP: Unspecified Reason (0)
- Session-Release-Reason AVP

If P-DRA initiates a release type RAA with a Session-Release-Reason AVP, an error string is included in the AVP.

MsgCopyAnswer AVP

The Diameter Message Copy Configuration Set 'Ingress Answer Included' attribute indicates whether the Diameter Message Copy feature needs to copy the Ingress Answer Message with the Diameter Request Message. If the attribute is set to Yes, the Answer message AVPs (Diameter header is omitted) are encoded as a MsgCopyAnswer AVP and included in the Request Message being copied.

Oracle Vendor-specific AVPs

The following Oracle Vendor-specific AVPs are used by the Diameter Routing Function in making decisions for routing messages to and from DSR Application and for the Diameter Message Copy feature. The AVP formats are shown in Oracle Vendor-specific AVP Formats.

- Num-Bindings
- Binding-Info
- Num-Sessions
- Binding-Id
- Session-Info
- Called-Station-Id
- Session-Originator
- Session-Initiation-Timestamp

AVP	AVP Code	AVP Length (octets)	Vendor - ID	Data	AVP Flags
Num-Bindings	2527	16	111	Contains an unsigned 32-bit of the number of findings that exist for the IMSI or MSISDN included in the GGR.	0 (except V bit = 1)
Binding-Info	2520	20 bytes + additional per Session - Info AVPs	111	Contains information related to a single binding for the IMSI or MSISDN	0 (except V bit = 1)

AVP	AVP Code	AVP Length (octets)	Vendor - ID	Data	AVP Flags
				included in the GGR. Includes: Binding-Id, Num-Sessions, and a Session-Info AVP for each Session	
Num-Sessions	2521	16	111	Contains an unsigned 32-bit value of the number of sessions that exist for the binding it is describing.	0 (except V bit = 1)
Binding-Id	2522	16	111	Contains an unsigned 32-bit value uniquely identifying the binding for the subscriber.	0 (except V bit = 1)
Session-Info	2523	12 + Information for this session Call - Station - Id + Session - Originator + Session - Initiation - Timestamp	111	Contains information related to a specific session of the subscriber, including: Called - Station-ID, Session - Originator, and Session - Initiation - Timestamp	0 (except V bit = 1)
Called - Session-Id	30		0(IETF)	Contains an UTF8String with the name of the Access Point Name (APN). This AVP is not Oracle - specific, but is	0 (except V bit = 1)

AVP	AVP Code	AVP Length (octets)	Vendor - ID	Data	AVP Flags
				included within one that is Oracle specific.	
Session - Originator	2525	12 + FQDN length	111	Contains an UTF8String with the Origin - Host of the Diameter client that originated the CCR-I for the session being described.	0 (except V bit = 1)
Session - Initiation - Timestamp	2526	16	111	Contains a 32-bit timestamp of when the CCS-I for the session being described was processed. The timestamp is the number of seconds since 1 January 1900 with respect to Coordinated Universal Time.	0 (except V bit = 1)

Chapter 3

Diameter Mediation

Topics:

- [Mediation Overview.....33](#)

The Diameter Mediation feature allows easy creation of Mediation Rules.

Mediation Overview

References:

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

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

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

- A Condition defines a part of the message that is used in the comparison, an operator for the type of comparison, and a type of data that must match the data in the message part.

Two or more Conditions in the same Rule Template are collectively referred to as a condition Set; the Condition Set are “ANDed”, “ORed” or Complex Expression in the comparison process.

- An Action can be adding, altering, or deleting AVPs; modifying the message header Flags, Length, Command-Code, or Application-ID; or other operations. An Action can be used to trigger Message Copy for Request messages that are processed by Mediation. Two or more Actions in a Rule Template are collectively referred to as an Action Set.

Mediation can be performed on:

- Routable Diameter messages only (Mediation is not supported on Diameter CEA and CER, DWR and DWA, and DPR and DPA messages)
- Specific Diameter interfaces or all Diameter interfaces (“interfaces” refers to Diameter Application Ids and not hardware/network interfaces)

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

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

Diameter Mediation provides a Rule Templates GUI interface, a Rule Sets GUI interface, and other GUI screens to perform the following and other tasks:

- Add, edit, and delete Enumeration Types and Internal Variables that are used in creating Rule Templates
- Create, modify, delete, copy, import, and export Rule Templates
- Add help text to a Rule Template; the help text will be available for the Rule Set that is generated from the Rule Template
- After a Rule Template has been created, generate the Rule Set from the Rule Template and create an entry in the Rule Sets GUI folder.
- Associate Rule Sets with Triggers, and remove Rule Set associations with Triggers
- Add a rule to a Rule Set, and provision the actual data that is used by the rule in the message matching process
- Edit and delete rules in Rule Sets
- Delete Rule Sets
- Change the state of a Rule Template to Test for testing its Rule Sets or to Active for enabling its Rule Sets for use with live traffic
- Test a Rule Set

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

Chapter 4

DSR Applications

Topics:

- [DSR Applications Overview.....36](#)

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

- Full Address Based Resolution (FABR)
- Range Based Address Resolution (RBAR)
- Charging Proxy Application (CPA)
- Policy Diameter Routing Agent (Policy DRA)
- Gateway Location Application (GLA)

DSR Applications Overview

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

- Full Address Based Resolution (FABR)

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

- Range Based Address Resolution (RBAR)
- Charging Proxy Application (CPA)
- Policy Diameter Routing Agent (Policy DRA)
- Gateway Location Application (GLA)

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

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

Full Address Based Resolution

References:

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

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

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

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

A Routing Entity can be:

- A User Identity:
 - International Mobile Subscriber Identity (IMSI)
 - Mobile Subscriber Integrated Services Digital Network (Number) (MSISDN)
 - IP Multimedia Private Identity (IMPI)
 - IP Multimedia Public Identity (IMPU)
- An IP Address associated with the User Equipment:
 - IPv4
 - IPv6-prefix
- A general purpose data type: UNSIGNED16

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

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

FABR provides the following functions:

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

FABR Deployment with SDS

References:

- SDS Online Help
- SDS Administration

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

The SDS DP system consists of a Primary Provisioning Site, a Disaster Recovery (DR) Provisioning Site, and up to 24 DSR Signaling Site servers with redundant DP SOAM servers and up to 2 DP blades. Each Provisioning Site has an Active/Standby pair of servers in a high availability (HA) configuration and a third server configured as a Query Server.

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

Range Based Address Resolution

References:

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

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

A Routing Entity can be:

- A User Identity:
 - International Mobile Subscriber Identity (IMSI)
 - Mobile Subscriber Integrated Services Digital Network (Number) (MSISDN)
 - IP Multimedia Private Identity (IMPI)
 - IP Multimedia Public Identity (IMPU)
- An IP Address associated with the User Equipment:
 - IPv4
 - IPv6-prefix
- A general purpose data type: UNSIGNED16

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

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

RBAR provides the following functions:

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

Charging Proxy Application

References:

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

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

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

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

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

Policy Diameter Routing Agent

References:

- *Policy DRA User's Guide*
- **Help > Policy DRA**

Policy DRA offers a scalable, geo-diverse Diameter application that creates a binding between a subscriber and a Policy and Charging Rules Function (PCRF) and routes all policy messages for a given subscriber and APN to the PCRF that currently hosts that subscriber's policy rules. Additionally, Policy DRA can perform Topology Hiding to hide the PCRF from specified Policy Clients.

Policy DRA provides the following capabilities:

- Support for all DSR application IDIH requirements; Policy DRA captures meta data that can be used with IDIH to create traces (this assumes that the desired traces are configured in IDIH)
- Distribution of Gx, Gxx, and S9 Policy binding-capable sessions and distribution of Gx-Prime and Rx Policy binding-dependent sessions across available PCRFs

Note: Gx-Prime uses the same Application-Id and Vendor-Id as Gx.

- Binding of subscriber keys such as IMSI, MSISDN, and IP addresses to a selected PCRF when the initial Gx, Gxx, or S9 sessions are already established to that PCRF
- Network-wide correlation of subscriber sessions such that all Policy sessions for a given subscriber are routed to the same PCRF
- Creation of multiple pools of PCRFs, which are selected using the combination of IMSI and Access Point Name (APN). This capability allows you to route policy Diameter signaling initiating from a given APN to a designated subset of the PCRFs that can provide specialized policy treatment using knowledge of the APN.

Note: APNs must be configured before enabling the PCRF Pooling feature.

- Use of multiple binding keys that identify a subscriber, so that Policy Clients that use different keysessions with these binding keys can still be routed to the PCRF assigned to the subscriber
- Efficient routing of Diameter messages such that any Policy Client in the network can signal to any PCRF in the network, and vice-versa, without requiring full-mesh Diameter connectivity
- Hiding of PCRF topology information from specified Policy Clients
- The ability to divert a controlled amount of policy signaling to a small subset of the PCRFs in a PCRF Pool for purposes of testing new PCRF capabilities.

Use the Policy DRA GUI to perform configuration and maintenance tasks, edit System Options, and view elements for the Policy DRA Configuration and Maintenance components.

The Policy Session Binding Repository (Policy SBR or pSBR) hosts the Policy Session and Policy Binding databases, which provide a distributed scalable and High Available (HA) database function to the Policy DRA application for storing and managing the Policy Session data and the subscriber-PCRF Binding data.

The metadata captured by IDIH for the Policy DRA includes the results of each query that Policy DRA makes to the session and binding database and the associated result. Whenever the result of a database query is captured in Policy DRA metadata, it will include the identity of the specific server that generated the response.

The Policy DRA application uses the Session and Binding databases in the Policy Session Binding Repository. Subscribers are dynamically assigned to a PCRF; this assignment is called a binding. The binding exists as long as the subscriber has at least one Policy Diameter session.

The following points describe a high-level view of Policy DRA Binding and Session databases:

- There is one instance of the Binding database in the entire Policy DRA network.
- There is one instance of the Session database per Policy DRA Mated Pair.
- Each binding record is associated with at least one Diameter session record. Binding records contain one Session Reference for each Diameter session that is associated with that binding.
- When a binding exists, there is at least one IMSI Anchor Key, Session, and Session Reference record.
- The IPv4, MISIDN, and IPv6 Alternate Keys are optional. They represent alternate ways, other than the IMSI, to identify a subscriber.

The Policy DRA application performs the following major functions:

- Processing Diameter Request messages
- Querying subscriber binding status
- Selecting an available PCRF and routing the Diameter Requests to a selected PCRF, including the ability to route new-binding CCR-I requests to one of a configured set of PCRF pools
- Topology Hiding
- Processing Diameter Answer messages
- Managing subscriber Session and Binding databases

Gateway Location Application

References:

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

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

After a DA-MP is activated with the GLA, it receives one Request (Get Gateway Request (GGR)) generated by the Gateway Query Client (GQC), then decodes subscriber information (IMSI or MSISDN), then queries the pSBR (via ComAgent within the Gateway Query Server (GQS) or DSR). The GLA

generates one Answer (Get Gateway Answer (GGA)) with subscriber information that includes the number of bindings for the subscriber, and the following information is included for each session:

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

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

- The GLA is activated using the same mechanism as Policy DRA. It will be activated at the NOAM, and activation is performed so that it activates all SOAMs under a common NOAM.
- GLA cannot be activated unless Policy DRA is activated and PCRF-Pooling has been enabled.
- Policy DRA cannot be deactivated if GLA is activated.

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

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

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

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

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

MAP-Diameter Interworking Function

References:

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

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

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

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

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

- All MAP-Diameter message and parameter interworking is performed on the SS7-MP.
- DM-IWF and MD-IWF exchange Diameter messages using ComAgent. No SS7/MAP message are exchanged between DA-MPs and SS7-MPs. Diameter messages are sent using a new stack event called IWF-Application-Data.
- When a transaction is initiated by either a DM-IWF or MD-IWF instance, it creates a Transaction ID which is unique to the DM-IWF/MD-IWF instance which is initiating the inter-MP transaction. The Transaction ID is sent as an IWF-Application-Data stack event parameter that correlates the messages/responses exchanged between DM-IWF and MD-IWF associated with a transaction. When DM-IWF or MD-IWF sends a response to the request, it echoes the transaction ID from the Request to allow the recipient to correlate the response with the request it had previously sent. The internal Transaction ID eliminates the need to manage Hop-by-Hop IDs in Diameter messages exchanged between DM-IWF and MD-IWF.
- DM-IWF and MD-IWF will use ComAgent's Routed Service with Reliable Transfer now support capabilities that allow eliminating the need for DM-IWFs and MD-IWFs to track growth/degrowth of SS7-MPs and DA-MPs respectively. In this document, any reference to DM-IWF Routed Service or MD-IWF Routed Service should be understood to mean ComAgent Routed Service using Reliable Transfer, utilizing Routed Service enhancements.

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

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

SS7/Sigtran

References:

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

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

Chapter 5

IP Front End (IPFE)

Topics:

- [*Introduction to IPFE.....44*](#)

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

- Presents a routable IP address representing a set of up to 16 application servers to application clients. This reduces the number of addresses with which the clients need to be configured.
- Routes packets from the clients that establish new TCP or SCTP connections to selected application servers.
- Routes packets in existing TCP or SCTP connections to the correct servers for the connection.

Introduction to IPFE

References:

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

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

- Presents a routable IP address representing a set of up to 16 application servers to application clients. This reduces the number of addresses with which the clients need to be configured.
- Routes packets from the clients that establish new TCP or SCTP connections to selected application servers.
- Routes packets in existing TCP or SCTP connections to the correct servers for the connection.

Traffic distribution

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

There can be as many as 16 IP addresses in the Target Set IP List and thus the IPFE may distribute traffic among as many as 16 physical or virtual application servers. Each server in the Target Set IP List can have a weighting indicating that the IPFE should apportion more or fewer connections to that server. The load balancing algorithm for apportioning connections is also configurable through a number of settings. The TSA, Target Set IP List, weighting, and load balancing algorithm settings are together called a **Target Set**. There can be as many as 32 independent **Target Sets** configured on one IPFE.

The IPFE neither interprets nor modifies anything in the TCP or SCTP payload. The IPFE also does not maintain TCP or SCTP state, but keeps sufficient state to route all packets for a particular session to the same application server.

Return traffic from the application server to the client (both TCP and SCTP) does not pass through the IPFE, but routes directly to the gateway.

High Availability

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

Each TSA can operate in an active-standby mode, where all traffic to a given TSA goes to the active (for that TSA) IPFE if it is available. If the active IPFE fails or if its mate is explicitly selected as Active, traffic to the TSA will go to the mate IPFE. For active-active HA, the addresses must be configured in pairs, where one IPFE is active for one address in a pair, and the mate is active for the other.

Note that the IPFE supports more than 2 TSAs, and in fact when both IPv4 and IPv6 are supported, the IPFE will usually be configured with at least 4. An IPFE and its mate are numbered 1 and 2, whereas an IPFE pair is numbered A and B. The four IPFEs are numbered A1, A2, B1, and B2.

For multihomed SCTP connections, the **Target Set** is represented by both a Primary Address and a Secondary Address. Each application server in the Target Set must also be configured for multihomed SCTP.

IPFE Associations

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

The specific packet-identifying information is the source IPv4 or IPv6 address and the source port number. For each **Target Set**, packets matching both by source address and source port will be routed to the same target application server.

All association information is replicated between mated IPFEs, but not between IPFE pairs.

Association information is isolated to a Target Set so that the Target Sets behave independently.

Because returning packets bypass the IPFE, the IPFE has limited knowledge of the state of the connection. The IPFE cannot determine if a connection has reconnected from the same source port, nor whether the connection has been terminated.

Association Aging

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

Load Balancing

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

Regardless of the algorithm, the IPFE will raise a minor alarm of "Out of Balance: High" or "Out of Balance: Low" on an application server whenever it is receiving a statistically high or low amount of traffic in comparison to others within the same **Target Set**.

If an application server determines that it has reached fully loaded capacity, then it will notify the IPFE not to send it further new connections. This is called Stasis. Application servers may go in and out of Stasis automatically according to the current traffic.

There are two **Load Balance Algorithms** available:

Hash : load balancing achieved by sending the new connection to a server based on hashing the originating port and IP address.

Hash load balancing will remove an application server from consideration for new connections whenever it is incurring an "Out of Balance: High" alarm. In this way reconnecting connections will always be directed to application servers that are moderately loaded. This feature is independent of Stasis notifications.

Least load : chooses the server with the least load as reported by the application server.

If the loads of two or more of the least-loaded servers are within a configurable percentage of each other, they are considered equally loaded, and the IPFE distributes connections to them in a round-robin fashion.

IPv4 and IPv6 support

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

Throttling

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

Part III

DSR Configuration

Topics:

- [DSR Configuration Overview.....48](#)
- [IPFE Configuration.....53](#)
- [Diameter Configuration.....55](#)
- [DSR Applications Configuration.....80](#)

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

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

Chapter 1

DSR Configuration Overview

Topics:

- [DSR Configuration.....49](#)

Configuring the DSR can include:

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

DSR Configuration

References:

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

Configuring the DSR can include:

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

Customer Support personnel normally either perform or participate in performing these activities.

- DSR system topology configuration of OAM Network Elements, Communication Services, servers, and server groups, and message processors

Customer Support personnel normally either perform or participate in performing these activities.

- OAM configuration, including MP blade servers, Server Groups, Signaling Network Devices, and VLAN Interfaces

Customer Support personnel normally either perform or participate in performing these activities.

- Activation of DSR Applications

Customer Support personnel normally either perform or participate in performing these activities.

- Diameter protocol configuration, including configuration for routing functions and configuration for transport connection management
- Configuration of the IP Front End (IPFE), if used
- Configuration of activated DSR Applications

Configuration of the DSR Topology

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

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

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

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

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

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

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

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

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

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

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

MEAL data is handled as follows:

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

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

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

Diameter Configuration

The DSR requires configuration for Diameter routing and transport functions.

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

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

Configuration for Diameter Routing Functions

Message routing is provided through the DSR. The DSR functions as a Diameter Relay Agent to forward messages to the appropriate destination based on information contained within the message,

including header information and applicable Attribute-Value Pairs (AVP). User-defined Peer Routing Rules define where to route a message to upstream Peer Nodes. Application Routing Rules route messages to DSR Applications. The DSR provides the capability to route Diameter messages based on any combination of, or presence or absence of, the following message parameters:

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

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

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

Configuring DSR routing includes:

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

Configuration for Diameter Transport Functions

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

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

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

Configuration for transport includes:

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

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

DSR Applications Configuration

Configuration for DSR Applications can include:

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

Chapter 2

IPFE Configuration

Topics:

- [*IPFE Configuration Overview.....54*](#)

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

IPFE Configuration Overview

References:

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

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

- Configuration Options
- Target Sets

DSR Bulk Import and Export

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

IPFE Configuration Options

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

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

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

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

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

IPFE Target Sets Configuration

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

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

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

Chapter 3

Diameter Configuration

Topics:

- [Diameter Configuration Overview.....56](#)
- [Diameter Common Configuration Overview.....59](#)
- [Configuration Capacity Summary.....60](#)
- [Connection Capacity Validation.....64](#)
- [Application Ids Configuration.....65](#)
- [Transport configuration.....65](#)
- [Routing Configuration.....70](#)
- [Diameter Options Configuration.....78](#)
- [Diameter Mediation Configuration Overview...78](#)

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

Diameter Configuration Overview

References:

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

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

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

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

Diameter Routing Function Configuration

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

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

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

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

Configuring Diameter routing can include:

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

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

Diameter Transport Function Configuration

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

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

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

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

Configuration for transport includes:

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

There are two types of Transport Connections:

- A Fixed connection can be assigned to one and only one DA-MP at configuration time.
- An IPFE floating connection is implicitly assigned to a set of DA-MPs through the IPFE Target Set Address (TSA) assigned to the connection. The location of the connection is unknown until the connection is established on one of the DA-MP location candidates. See [IP Front End \(IPFE\)](#).
- Local Node FQDN, Realm, IP Addresses, and transport protocol
- Peer Node FQDN, Realm, IP Addresses, and transport protocol
- Connection, Capability Exchange (CEX), and Message Priority Configuration Sets

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

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

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

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

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

- Common Application IDs
- Capacity (ingress and egress message rates) and Congestion Controls:
 - **DA-MP Overload Control** (Message Priority and Color-Based DA-MP Overload Control) provides a mechanism for managing internal/local DA-MP congestion detection and control. The DA-MP Overload Control feature tracks ingress message rate, calculates the amount of traffic that needs to be shed based on CPU congestion, and sheds that traffic based on Message Priority, Message Color, and discard policy. Message Color is used to differentiate Diameter Connections that are under-utilized versus those that are over-utilized with respect to ingress traffic - traffic from under-utilized Connections is marked "green" by the Per-Connection Ingress MPS Control (PCIMC) feature, while traffic from over-utilized Connections is marked "yellow". In the event of Danger of Congestion or of CPU congestion and based on the specified discard policy, traffic from over-utilized Connections is considered for discard before traffic from under-utilized Connections. Traffic discarded by PCIMC due to capacity exhaustion (per-Connection or shared) is marked "red" and is not considered for any subsequent processing.
 - The **User Configurable Message Priority** feature provides Message Priority that can be assigned to ingress Diameter messages, based on certain configurable criteria, for use in algorithms for preferential discard, throttling, and routing by Peer Nodes and Local Nodes. Message Priority Configuration Sets are assigned to Peer Nodes and Connections to provide the Message Priority during ingress message processing.
 - The **Per Connection Ingress MPS Control** feature uses Capacity Configuration Sets and Ingress Message Coloring to limit to a configured level the per-Connection ingress message rate of each DSR Connection.
 - The **Remote BUSY Congestion** feature allows DSR egress Request routing to select a BUSY Connection (that is abating its BUSY status) based on the User Configurable Message Priority assigned to the message. The Connection BUSY Abatement Time defines the time spent abating each Congestion Level during abatement.
 - The **Egress Transport Congestion** feature provides a user-configurable Egress Transport Abatement Timer for each DSR Peer Connection. Egress Transport Congestion occurs when a DSR Diameter Peer Connection's TCP/SCTP send buffer is exhausted, as indicated by the TCP/SCTP socket being 'blocked' (the Diameter Transport Function attempts to write new data to the TCP/SCTP socket fail due to insufficient send buffer space). When a DSR Peer Connection becomes blocked, DSR sets the Connection's Congestion Level to CL-4 (no Requests or Answers can be sent on the Connection). The Egress Transport Abatement Timer is used to step the Congestion Level down during abatement.
 - The **Per Connection Egress Message Throttling** feature provides a mechanism that assists with the prevention of Diameter Peer overload. The Maximum Egress Message Rate (EMR) can be configured per Connection. The Per Connection Egress Message Throttling feature works in conjunction with the User Configurable Message Priority to provide intelligent load shedding based on the volume of the offered load and the Message Priority. Egress Message Throttling Configuration Sets define the maximum allowed EMR, EMR throttle thresholds, and EMR abatement thresholds.
 - The **User-Configurable Connection Pending Transaction Limiting** feature provides the ability to configure the Connection Pending Transaction Limit for each DSR Peer Connection, to use

in the distribution of the available Pending Transaction Records on a DA-MP based on the varying deployment requirements. Its use can prevent a small number of connections on a DA-MP from consuming a disproportionate number of the available Pending Transaction Records on the DA-MP.

Diameter Common Configuration Overview

References:

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

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

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

Diameter Common on the NOAM

MCCMNC Mapping

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

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

The following actions can be performed:

- Filter the list of entries, to display only the desired entries.
- Sort the list entries in ascending or descending order.
- Add new MCCMNC Mapping entries.
- An MCCMNC Mapping entry can be edited.
- Select an MCCMNC Mapping entry in the list can be removed from selected entry.

Diameter Common on the SOAM

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

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

MCC Ranges

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

While searching for an IMSI in the Diameter message AVPs, if the MCC digits portion of decoded IMSI digits fall within one of the configured MCC Ranges, the IMSI digits will NOT be used for further Address Resolution. The FABR and RBAR applications will continue to search other AVP instances (if present) , or next priority AVP (if configured) or next Routing Entity (if configured) for a valid address.

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

- 000-199
- 800-899

The following actions can be performed:

- Filter the list of entries, to display only the desired entries.
- Sort the list entries in ascending or descending order.
- Add new MCC Ranges entries.
- An MCC Ranges entry can be edited.
- Select an MCC Ranges entry in the list can be removed from selected entry.

MPs

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

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

An MP Profile defines maximum and threshold values for an MP. An MP Profile must be assigned to each DA-MP and SS7-MP in the system configuration. Select the appropriate MP Profile according to the hardware and application or applications that are running on the MP. The only supported combination of session and database applications running on the same DA-MP is Policy DRA and RBAR.

Note: The profiles listed here and that appear on the MPs GUI pages might not include all of the profiles that are available for all Oracle Communications products. Product-specific profiles and instructions for assigning them are included in the *Installation Guide* for each product.

Configuration Capacity Summary

The **Diameter > Configuration > Capacity Summary** page displays information about maximum allowed and currently configured Diameter Configuration components. The following information is displayed in each row of a read-only table:

Configuration Item	The type of Diameter Configuration component
Max Allowed Entries	The maximum number of entries for that component that can be configured in Diameter.
Configured Entries	The number of entries for that components that are currently configured.
% Utilization	The percentage of the maximum number of entries for that component that are currently configured.

Use the **Diameter > Configuration > Capacity Summary** page when planning, configuring, and maintaining the DSR Diameter Configuration.

Diameter Capacity Constraints

The following table shows the Maximum values per NE and per Configuration Component.

Table 2: Maximum values per NE and per Configuration Component

Constraint Name	Description	Value	Related Notes
Application Routing Rules	Maximum number that can be configured per Network Element	128	Calculated using this formula: [(16 Application IDs) * (4 Command Codes) * (2 Routing Entity Types per Preference List)]
Capacity Configuration Sets	Maximum number that can be configured	1000	
Application Ids	Maximum number that can be configured	1000	
Application Ids	Maximum number per Configuration Set Per Connection	10	
Connection Configuration Sets	Maximum number per Network Element	2000	
Connections	Maximum number per Network Element	Lesser of 12,000 OR [sum of individual DA-MP maximums]	
Connections	Maximum number per Peer Node	64	
Connections	Maximum number per Connection Route Group	64	
CEX Configuration Sets	Maximum number that can be configured	2000	
Supported Application Ids	Maximum number per CEX Configuration Set		<p>An Application ID configured can be any one of the following types:</p> <ol style="list-style-type: none"> 1. · Auth-Application-ID 2. · Acct-Application-ID 3. · Vendor-Specific-Application-ID <p>Configuration of Vendor-ID will be required for each of the Vendor-Specific-Application-ID.</p>

Diameter Configuration

Supported Vendor ID(s)	Maximum number per CEX Configuration Set	10	If set, it contains the Vendor-Ids configured for the Vendor-Specific-Application-Ids.
Diagnose Connections	Maximum number of connections in Test Mode that are being diagnosed	2	In Diagnostics Tool
Diagnose PDUs	Maximum number of PDUs per Test Connection for a single diagnostic cycle.	1	
Signaling IP Addresses	Maximum number per Local Node	start here 8 Any combination of IPv4 and IPv6	
IP Addresses	Maximum number per Peer Node	128	
Local Nodes	Maximum number per Network Element	32	
Peer Nodes	Maximum number per Network Element	6000	One Peer Node per connection.
Peer Nodes	Maximum number per Route Group	160	
Route Groups	Maximum number per Network Element	1000	
Route Groups Per Route List	Maximum number per Route List	3	Supports priority values 1 thru 3 .
Reroute On Answer	Maximum number of Order Pair combinations of Application Id and Answer Result Code value that can cause a Request re-routing.	1000	
Route Lists	Maximum number per Network Element	1000	
Unique Priorities	Maximum per Route List		
Supported Vendor Ids	Maximum number per set	10	Supported Vendor Ids cannot be greater than the number of Vendor-SpecificApplication Ids.

Test Connections	Maximum number of connections in Test Mode for testing with the Diagnostics Tool	2	
Target Set Addresses	Maximum number of TSAs per Local Node	32	
Maintenance Screen Refresh Rate	Time interval in seconds after which data is refreshed on the Diameter Maintenance screens	10	
DA-MPs	Maximum number that can be configured	16	
Pending Answer Timers	Maximum number that can be configured	8	
Peer Route Tables	Maximum number configured Per Network Element	100	
Peer Routing Rules	Maximum number per Peer Route Table	1000	
Peer Routing Rules	Maximum number per Network Element		
Associations between Application Ids and Peer Route Tables	Maximum number allowed	20	
Routing Option Sets	Maximum number that can be configured	20	
Command Codes	Maximum number that can be configured	1000	
Message Priority Configuration Sets	Maximum number that can be configured	20	
Message Priority Configuration Set Rules	Maximum number of configured Rules per Message Priority Configuration Set	50	
Message Throttling Configuration Sets	Maximum number that can be configured	50	
Connections with Message Throttling Configuration Sets assigned	Maximum connections that can have Message Throttling Configuration Sets assigned to them	50	

Invalid MCC Ranges	Maximum number that can be Configured	10	
Trusted Network Lists	Maximum number that can be configured.	500	
Trusted Network Realms	Maximum number of Trusted Network Realms per Trusted Network List that can be configured.	100	
Path Topology Hiding Configuration Sets	Maximum number that can be configured.	500	
Host Network Suffixes	Maximum number per Path Topology Hiding Configuration Set	10	
HSS Topology Hiding Configuration Sets	Maximum number that can be configured.	500	
MME Topology Hiding Configuration Sets	Maximum number that can be configured.	500	
MME Real Host Names	Maximum number per MME Topology Hiding Configuration Set	300	
Protected Network Configuration Sets	Maximum number that can be configured.	500	

Connection Capacity Validation

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

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

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

Application Ids Configuration

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

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

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

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

Transport configuration

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

CEX Parameters Configuration

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

Command Codes Configuration

The Command Code is one of the parameters contained in a Diameter message.

Command Codes can be used in Peer Routing Rules and Application Routing Rules.

Configuration Sets

A Connection Configuration Set provides a mechanism for tuning a connection to account for the network quality of service and Peer Node requirements. Each connection references a single Connection Configuration Set. Each Local Node also references a Connection Configuration Set to provide the default settings for peer-initiated connections.

A CEX Configuration Set provides a mechanism for assigning up to 10 unique Application Ids and up to 10 unique supported Vendor IDs to a Local Node or Connection.

A Capacity Configuration Set provides a mechanism for adjusting a connection to account for the network quality of service and Peer Node requirements, and allows management of capacity data for Diameter Peer connections. Capacity Configuration Set data consists of reserved Ingress MPS, maximum Ingress MPS, Ingress MPS minor alarm threshold, and Ingress MPS major alarm threshold.

An Egress Message Throttling Configuration Set provides a mechanism for managing egress message traffic on a Diameter connection. An Egress Message Throttling Configuration Set can be created with a maximum allowable Egress Message Rate (EMR) and 1 to 3 pairs of EMR Threshold Throttles and Abatement Throttles.

A Message Priority Configuration Set provides a mechanism for controlling how message Priority is set for a Request message arriving on a connection. A Message Priority Configuration Set contains one or more Message Priority Rules. A Message Priority Rule consists of combination of an Application ID and a Command Code, and a Priority. Incoming messages that match the Application ID and Command Code are assigned the associated Priority. Message Priority Configuration Sets can be assigned to connections or Peer Nodes.

Connection Configuration Sets

Connection Configuration Sets provide a mechanism for adjusting a connection to account for the network quality of service and Peer Node requirements. Each connection references a single Connection Configuration Set. Each Local Node also references a Connection Configuration Set to provide the default settings for peer-initiated connections.

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

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

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

SCTP parameters include:

- Send and receive buffer sizes
- Initial, minimum and maximum retransmit timeout times
- The number of retransmits triggering association failure
- The number of retransmits triggering init failure
- SACK delay time
- The heartbeat interval
- The maximum number of inbound and outbound streams
- Whether datagram bundling is on or off

Diameter parameters include:

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

TCP parameters include:

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

CEX Configuration Sets

A CEX Configuration Set provides a mechanism for assigning up to 10 unique Application Ids and up to 10 unique supported Vendor IDs to a Local Node or connection.

Application Ids can be optionally marked as “Must Include”. If any of the Application-Ids in the CEX Configuration Set are configured as “MUST Include CEX Parameters” but DO NOT exist in the CEX message received from the Peer, DCL Peer validation fails and the Peer connection is disconnected. When attempting to map a Peer-initiated connection to a configured Diameter connection, Diameter includes any Application-Ids in the CEX Configuration Set that are configured as “MUST Include” when finding a connection.

A Vendor Id can be sent in the Supported-Vendor-ID AVP of a CEX even though the Vendor Id is not configured in the **Selected Supported Vendor Ids** for the CEX Configuration Set.

Each Local Node must refer to a single CEX Configuration Set. Each transport connection can optionally refer to a single CEX Configuration Set. During CEX message exchange, the CEX Configuration Set in the transport connection is used if configured. Otherwise, the CEX Configuration Set in the Local Node (associated with the transport connection) is used.

A default CEX Configuration Set, called Default, is always available, and is pre-populated with the “RELAY” Application Id (0xFFFFFFFF or 4294967295-Relay). The Default CEX Configuration Set values cannot be modified or deleted. When a new CEX Configuration Set is created, the values of the Default CEX Configuration Set are automatically populated into the new CEX Configuration Set, so that the new CEX Configuration Set needs to have only a few options adjusted.

CEX Parameters

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

Capacity Configuration Sets

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

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

A Capacity Configuration Set can be created with specific SCTP, Diameter, and TCP options, and assigned to a connection. Each connection references a single Capacity Configuration Set.

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

Message Priority Configuration Sets

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

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

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

Egress Message Throttling Configuration Sets

Egress Message Throttling Configuration Sets provide a mechanism for managing egress message traffic on a Diameter connection. An Egress Message Throttling Configuration Set can be created with a maximum allowable Egress Message Rate (EMR) and 1 to 3 pairs of EMR Threshold Throttles and Abatement Throttles.

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

Local Nodes

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

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

Peer Nodes

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

Load Sharing: Peer Nodes

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

Figure 3: Weighted Load Sharing illustrates the concept of weighted load sharing in the DSR.

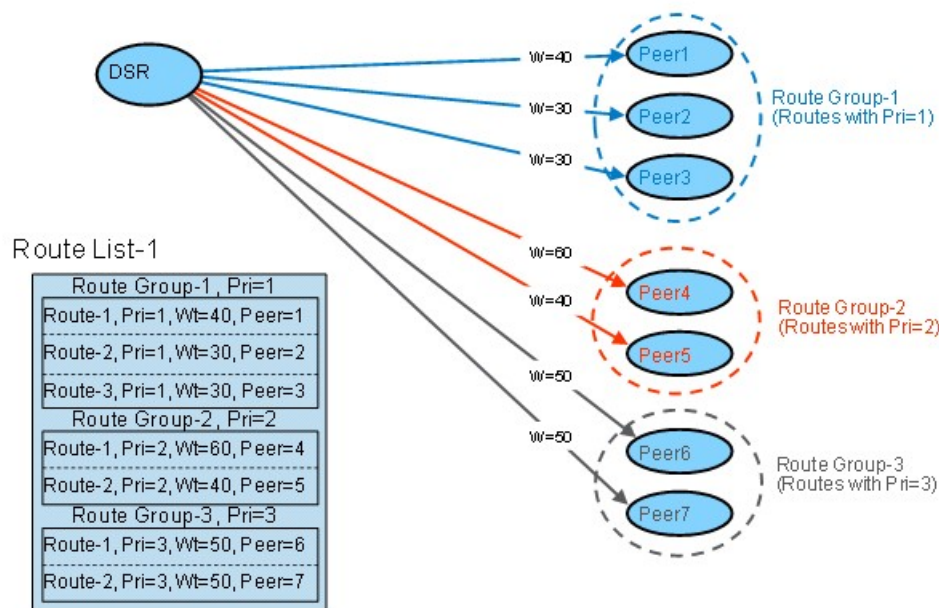


Figure 3: Weighted Load Sharing

Connections

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

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

IPv4 and IPv6

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

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

- Multiple IPv4 and IPv6 addresses can be hosted simultaneously on a DSR MP.
- Each Diameter Peer connection (SCTP or TCP) configured in the DSR will specify a local DSR node (FQDN) and an associated local IPv4 or IPv6 address set for use when establishing the connection with the Peer.
- Each Diameter Peer connection (SCTP or TCP) configured in the DSR will specify a Peer Node (FQDN) and optionally the Peer Node's IPv4 or IPv6 address set.
- If the Peer Node's IP address set is specified, it must be of the same type (IPv4 or IPv6) as the local DSR IP address set specified for the connection.

- If the Peer Node's IP address set is not specified, DSR will resolve the Peer Node's FQDN to an IPv4 or IPv6 address set by performing a DNS A or AAAA record lookup as appropriate based on the type (IPv4 or IPv6, respectively) of the local DSR IP address set specified for the connection.

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

Routing Configuration

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

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

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

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

Configuring DSR routing requires:

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

Diameter Routing Functions

Figure 4: DSR Routing Diagram illustrates high-level message processing and routing in the DSR.

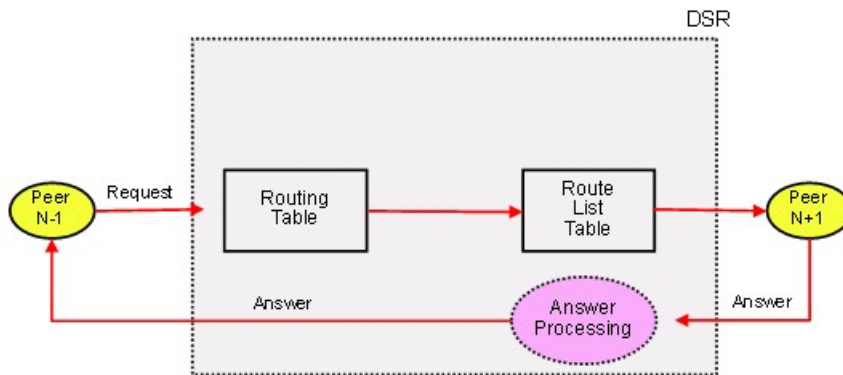


Figure 4: DSR Routing Diagram

The DSR supports the following routing functions:

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

Load Sharing: Route Groups and Route Lists

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

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

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

Figure 5: Route List, Route Group, and Peer Node Relationships illustrates the relationships between the Route List, Route Groups, and Peer Nodes.

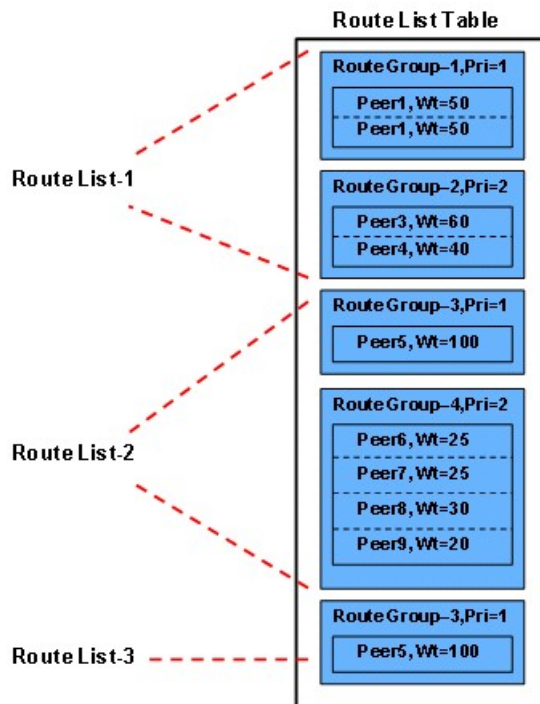


Figure 5: Route List, Route Group, and Peer Node Relationships

Minimum Route Group Availability Weight

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

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

Figure 6: Route Group Weights illustrates how a Route Group's weight is calculated.

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

Figure 6: Route Group Weights

Implicit Routing

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

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

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

Diameter configuration for Implicit Routing:

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

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

Figure 7: DSR Implicit Routing illustrates implicit routing in the DSR.

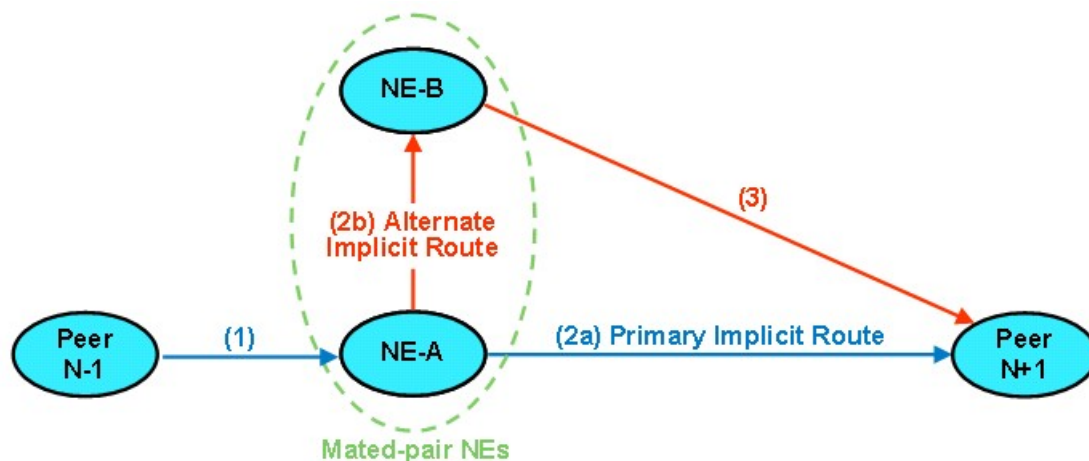


Figure 7: DSR Implicit Routing

Alternate Implicit Routing

Peer Nodes can be configured with an Alternate Implicit Route.

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

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

Diameter configuration of Alternate Implicit Routing:

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

Route Group Configuration

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

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

Each Route Group can be assigned a maximum of 160 Peer Nodes or Connections. Route Groups are assigned to Route Lists. See [Route List Configuration](#).

Route List Configuration

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

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

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

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

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

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

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

Routing Option Sets Configuration

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

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

Peer Route Tables Configuration

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

Peer Routing Rules Configuration

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

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

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

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

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

Pending Answer Timer

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

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

- [Implicit Routing](#)

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

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

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

A Pending Answer Timer can be associated with:

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

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

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

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

Use Ingress Peer Node Routing Option Set Pending Answer Timer

- Else If a Pending Answer Timer is configured for the Egress Peer Node

Use Egress Peer Node Pending Answer Timer

- Else If a configured Application-ID exists for the Application-ID in the Request

Use Application-ID Pending Answer Timer

- Else

Use the system Default Pending Answer Timer

Reroute On Answer

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

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

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

1. On the **Diameter Configuration Reroute On Answer** GUI,
 - a. Enter the **Answer Result-Code AVP Value**.

- b. If Reroute On Answer is to be triggered by a specific Application Id and Result-Code AVP pair, select the **Application Id** for the specified AVP.
 - c. If Reroute On Answer is to be triggered for all available Application Ids for a Result-Code AVP, do not select an **Application Id**.
- 2. Configure Peer Nodes.
 - a. **Alternate Routing on Answer Timeout**
 - Select **Same Peer** to perform alternate routing on alternate connections on the same Peer before selecting the next eligible Peer in the Peer Route Group.
 - Select **Same Connection** perform alternate routing on the same connection on the same Peer before selecting the next eligible Peer in the Peer Route Group.
 - Select **Different Peer** to perform routing on a different Peer in the Peer Route Group.
 - b. **Alternate Routing on Answer Result Code**
 - Select **Same Peer** to perform alternate routing on alternate connections on the same Peer before selecting the next eligible Peer in a Peer Route Group when a Reroute on Answer Result Code occurs.
 - Select **Different Peer** to perform routing on different Peer in the Peer Route Group.
- 3. Configure Route Groups as Peer Route Groups (not Connection Route Groups).
- 4. Configure Pending Answer Timers

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

Application Routing Rules Configuration

Application Route Tables contain one or more Application Routing Rules that can be used for routing Request messages to DSR Applications.

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

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

One or more DSR Applications must be activated before Application Routing Rules can be configured.

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

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

Message Copy Configuration Set configuration

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

Diameter Message Copy can be triggered by a Peer Routing Rule, Diameter Mediation, or the Charging Proxy Application (CPA). The Message Copy trigger point must specify a Message Copy Configuration Set when the message is marked for copying, except the values in the Default Message Copy Configuration Set are used for CPA Message Copy.

Diameter Options Configuration

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

- System Options
- DNS Options

System Options Configuration

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

- General Options
 - Maximum Message Size Allowed
 - Per Connection Egress Message Throttling Enabled/Disabled
 - IPFE Connection Reserved Ingress MPS Scaling
- Alarm Threshold Options - Aggregation Thresholds for Fixed Connection, IPFE Connection, Peer Node, and Route List failures.
- Message Copy Options
 - Message Copy Feature enabled/disabled
 - MP Congestion Level at or above which Message Copy is disabled.

DNS Options Configuration

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

Diameter Mediation Configuration Overview

References:

- *Diameter Mediation User's Guide*

- **Help > Diameter Mediation**

The Diameter Mediation feature and its Meta Administration privileges must be activated in the system before all of the Diameter Mediation GUI pages are available for configuring Diameter Mediation components.

Diameter Mediation is supported for both Request and Answer messages.

Note: CEA, CER, DWA, DWR, DPA, and DPR messages are never handled by the Mediation feature.

Rule Templates define Conditions that must be matched for Diameter Mediation to modify the processing behavior for a message, and the types of Actions that are applied to accomplish the modification.

- Conditions can be configured to cause Mediation to use fast database lookups (Fast Search) of the Rule data.
- Actions are configured to indicate what to do when the Conditions match (such as modify the part of a message, forward a message, send a reply, insert or remove headers, or set attributes for further processing).

Rule Sets define one or more Rules that contain the actual data for the Conditions and Actions defined in their corresponding Rule Templates.

On the **Triggers** GUI page, Active Rule Templates with defined Rule Sets are associated with specific Trigger Points. When the message processing reaches a selected Trigger Point the Conditions of the Rule Template are examined for the message. If the Conditions match, Mediation Actions are applied to the message.

The Enumerations, AVP Dictionaries, and Vendors Diameter Mediation components are configured for use in defining Rule Templates and Rule Sets.

A Formatting Wizard assists in defining data with complicated formats and operators in the configuration.

DSR Applications Configuration

Topics:

- [*DSR Applications Configuration Overview.....81*](#)

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

- Full Address Based Resolution (FABR)
- Range Based Address Resolution (RBAR)
- Charging Proxy Application (CPA)
- Policy Diameter Relay Agent (Policy DRA)
- Gateway Location Application (GLA)

Configuration for DSR Applications can include:

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

DSR Applications Configuration Overview

References:

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

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

Configuration for DSR Applications can include:

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

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

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

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

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

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

- Application Ids for specific Diameter interfaces
- Command Codes
- Peer Nodes
- Local Nodes
- Connections
- Peer Routing Rules

Part IV

Maintenance, Status, and Reports

Topics:

- [Diameter Maintenance.....83](#)
- [Diameter Reports.....93](#)

This part describes:

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

Chapter 1

Diameter Maintenance

Topics:

- *Introduction.....84*
- *Diameter Maintenance and Status Data for Components, DSR Applications, and DA-MPs.....85*
- *Managing the Status of Diameter Configuration Components.....88*

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

- Route Lists
- Route Groups
- Peer Nodes
- Connections
- Egress Throttle Groups

This chapter also describes:

- The maintenance and status data that is maintained by DSR Applications and by DA-MPs
- The strategy for reporting (merging) status data to the OAM
- How modification of relevant configuration elements can affect the status of a given component

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

Introduction

References:

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

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

- Route Lists
- Route Groups
- Peer Nodes
- Connections
- Egress Throttle Groups

This chapter also describes:

- The maintenance and status data that is maintained by DSR Applications and by DA-MPs
- The strategy for reporting (merging) status data to the OAM
- How modification of relevant configuration elements can affect the status of a given component

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

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

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

Diameter Configuration Component Status for Egress Message Routing Decisions

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

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

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

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

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

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

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

Table 3: Diameter Configuration Component Status Dependencies summarizes the status dependencies of Diameter Configuration components.

Table 3: Diameter Configuration Component Status Dependencies

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

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

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

Route Lists Maintenance

The Route List maintenance and status data that is maintained and merged to the OAMs identified in [Table 4: Route List Status Data](#). The data is derived from the current Operational Status of Route Groups assigned to a given Route List.

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

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

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

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

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

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

Table 4: Route List Status Data

Name on Diameter GUI	Description
MP Server Hostname	MP Server Hostname of the DA-MP that is reporting the maintenance status of the given Route List.
Route List Name	Route List identifier.
Status	Operational Status of the Route List. Supported values: Available, Degraded, Unavailable.
Active / Standby	The Route Group that is active within the Route List.
Time of Last Update	Time when status was last updated

Route Groups Maintenance

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

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

Peer Nodes Maintenance

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

Connection Maintenance

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

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

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

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

- Run diagnostics on a test connection.

For information about Diagnostics Reports, see [Diameter Diagnostics Tool](#).

Egress Throttle Groups Maintenance

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

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

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

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

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

Applications Maintenance

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

On the **Diameter > Maintenance > Applications** page, you can change the Admin State of the selected DSR Application to Enabled or Disabled.

DA-MPs Maintenance

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

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

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

Managing the Status of Diameter Configuration Components

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

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

Maintenance and Status Data Sourcing Methods

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

Various strategies called “Sourcing Methods” can be used by DA-MPs to merge their status. The sourcing methods are summarized in [Table 5: Maintenance and Status Data Sourcing Methods](#).

[Table 6: Diameter Configuration Component Sourcing Methods](#) summarizes the Diameter Configuration components used in egress message routing, each Sourcing Method that can be used by each component, and the Diameter Maintenance GUI page where the status is reported.

Table 5: Maintenance and Status Data Sourcing Methods

Sourcing Method	Description	When this Sourcing Method is Used
Report-All	For a given component, all DA-MPs will report status data on any component instances for which it can determine the status.	The component instance status reported by each DA-MP is unique. For example, for the Inter-MP connection status, MP1 and MP2 each have a unique status to report regarding the connection between itself and MP3.

Sourcing Method	Description	When this Sourcing Method is Used
Report-Mine	For a given component, a DA-MP will report its status data on an component instance only if it is directly responsible for managing and owning the component instance.	Each component instance is owned by a single DA-MP. For example, each Fixed connection is owned by a single DA-MP. Each DA-MP will report the status of those connections that it owns.
Leader	One DA-MP is elected Leader. For a given component, only the DA-MP Leader will report status data on instances of the given component .	Each DA-MP has the identical status on each component instance. If each DA-MP were to merge its status data, the OAM would receive identical status from each DA-MP. To avoid this duplication, a DA-MP Leader is elected and only the Leader will report the status.

Table 6: Diameter Configuration Component Sourcing Methods

Diameter Configuration Component Name	Sourcing Method	Diameter GUI Screen (starting from Main Menu : Diameter ->)
Route List	Leader	Maintenance -> Route Lists
Route Group	Leader	Maintenance -> Route Lists Note: A Route Group has a status only within the context of a Route List
Peer Node	Leader	Maintenance -> Peer Nodes
Fixed Connection	Report-Mine	Maintenance -> Connections
Floating Connection	Report-Mine / Leader	Maintenance -> Connections
DSR Application	Report-All	Maintenance -> Applications
DA-MP	Report-All	Maintenance -> DA-MPs DA-MP Status data is shown on the "Peer DA-MP Status" tab. DA-MP Peer Status data is shown on multiple tabs, one for each Peer DA-MP (tab name is the Hostname of the Peer DA-MP)

DA-MP Leader

Maintenance and status data is maintained by DA-MPs for each Diameter Configuration component. Some components have a scope that is beyond that of a single DA-MP. Examples are the Route Lists,

Route Groups, and Peer Nodes. For these components, every DA-MP will contain the identical status of each component instance.

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

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

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

Merging of Status to the OAM

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

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

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

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

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

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

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

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

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

The Diameter Routing Function instance that is currently controlling the Diameter Connection from an egress Request message routing perspective is defined by the Diameter Connection “Current

Location". The Current Location defines the DA-MP that the Diameter Routing Function considers to be the current owner of the connection for the purpose of routing egress Request messages.

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

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

Ownership of Diameter Connections

The DSR supports two types of connections:

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

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

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

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

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

Raising and Clearing Alarms

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

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

- Raising an alarm
 1. For a given component instance, a fault condition is detected on the DA-MP.
 2. The status is merged to the OAM.
 3. The OAM looks at the set of active alarms on the given component instance.

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

Diameter Reports

Topics:

- [*Diameter Diagnostics Tool.....94*](#)
- [*Diameter MP Statistics \(SCTP\) Report.....94*](#)

Diameter Reports GUIs provide access to the following Diameter functions:

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

Diameter Diagnostics Tool

References:

- *Diameter User's Guide*, "Connection Maintenance", "Reports"
- **Help > Diameter > Maintenance > Connection Maintenance**
- **Help > Diameter > Reports > Generating Diagnostics Tool Reports**

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

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

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

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

Diameter MP Statistics (SCTP) Report

References:

- *Diameter User's Guide*, "Diameter", "Reports"
- **Help > Diameter > Reports > Updating and Viewing MP Statistics (SCTP) Reports**

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

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

Part V

Tools and Utilities

Topics:

- *Imports and Exports96*
- *IPsec.....100*
- *Integrated Diameter Intelligence Hub.....108*
- *Database Backups and Restores.....110*

This part describes:

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

Chapter 1

Imports and Exports

Topics:

- *DSR Bulk Import and Export.....97*
- *Diameter Mediation Import and Export Overview.....98*

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

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

DSR Bulk Import and Export

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

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

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

Configuration data refers to any data that is configured for one of the Export **Export Application** types (FABR, RBAR, PDRA, GLA, MAPIWF, or CPA and SBR DSR Applications; IPFE; and the Diameter components). "Diameter" includes Diameter Configuration components and Diameter Common Network Identifiers and MPs components.

DSR Bulk Export

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

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

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

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

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

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

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

DSR Bulk Import

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

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

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

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

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

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

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

The following Import operations can be performed:

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

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

Diameter Mediation Import and Export Overview

References:

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

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

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

Mediation Rule Template Export

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

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

- The Rule Template without any provisioned Rules data
- All of the Enumeration Type definitions with the possible values to which the Rule Template refers

- Mediation version number
- Help pages related to the Rule Template

Mediation Rule Template Import

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

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

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

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

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

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

Chapter 2

IPsec

Topics:

- [IPsec Overview.....101](#)
- [IPsec IKE and ESP elements.....103](#)
- [Accessing platcfg.....104](#)
- [Adding an IPsec connection.....105](#)
- [Editing an IPsec connection.....105](#)
- [Enabling and Disabling an IPsec Connection...106](#)
- [Deleting an IPsec connection.....107](#)
- [Logging out of platcfg.....107](#)

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

IPsec Overview

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

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

IPsec will work for both IPv4 and IPv6.

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

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

Encapsulating Security Payload

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

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

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

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

The supported ESP encryption and authentication algorithms are described in [IPsec IKE and ESP elements](#).

Internet Key Exchange

Internet Key Exchange (IKE) is used to exchange secure keys to set up IPsec security associations.

There are two versions of IKE: IKEv1 and IKEv2. The following main differences exist between IKEv1 and IKEv2:

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

The encryption algorithms and authentication transformations that are supported for IKE are described in [IPsec IKE and ESP elements](#).

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

IP Compression

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

IPsec Process

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

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

IKE operates in two phases.

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

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

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

IPsec Setup

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

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

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

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

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

1. Open platcfg. See [Accessing platcfg](#).
2. Add and configure an IPsec connection. See [Adding an IPsec connection](#).
 - a. Select an IKE version.
 - b. Complete the IKE configuration for the IPsec connection.

- c. Complete the ESP configuration for the IPsec connection
 - d. Complete the IPsec connection configuration entries.
 - e. Wait for the connection to be added.
3. Enable the IPsec connection. See [Enabling and Disabling an IPsec Connection](#).
 4. Log out of platcfg. (See [Logging out of platcfg](#).)

IPsec IKE and ESP elements

[Table 7: IPsec IKE and ESP elements](#) describes IPsec IKE and ESP configuration elements and provides default values, if applicable.

Table 7: IPsec IKE and ESP elements

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

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

Accessing platcfg

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

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

Use the following task to access platcfg.

1. Using ssh, open a terminal window to the iLO IP address of the management server.
Contact your system administrator if you need assistance accessing the management server.
2. Log into the iLO as Administrator.
3. At the iLO command prompt, enter **vsp** to start the virtual serial port feature.

```
</>hpiLO-> vsp

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

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

4. Press ENTER to access the login prompt.

```
CentOS release 5.5 (Final)
Kernel 2.6.18-194.32.1.el5prere14.2.3_70.83.0 on an x86_64

cfg1-CMP-a login:
```


5. Log into the server as the platcfg user.
 - username: **platcfg**
 - password: **<platcfg_password>**

The platcfg **Main Menu** appears.

Adding an IPsec connection

Use this task to add an IPsec connection.

1. Open platcfg.
See [Accessing platcfg](#).
2. Select **Network Configuration**.
3. Select **IPsec Configuration**.
4. Select **IPsec Connections**.
5. Select **Edit**.
6. Select **Add Connection**.
7. Select the Internet Key Exchange Version: either **IKEv1** or **IKEv2**.
8. Complete the **IKE Configuration** fields for the desired connection, then click **OK**.
9. Select the desired **ESP Encryption** algorithm, then click **OK**.
10. Complete the **Add Connection** fields for the desired connection.
 - Enter the **Local Address**.
 - Enter the **Remote Address**.
 - Enter the **Pass Phrase**.
 - Select the **Mode**.
11. Click **OK**.
Wait for the connection to be added.

When the connection has been successfully added, the **Internet Key Exchange Version Menu** appears.
12. Select **Exit**.
13. Log out of platdfg.
See [Logging out of platcfg](#).

Editing an IPsec connection

Use this task to edit an IPsec connection.

1. Open platcfg.
See [Accessing platcfg](#).

2. Select **Network Configuration**.
3. Select **IPsec Configuration**.
4. Select **IPsec Connections**.
5. Select **Edit**.
6. Select **Edit Connection**.
7. Select the IPsec connection to edit.
8. View the IPsec connection's current configuration.
9. Select **Edit**.
10. Select either **IKEv1** or **IKEv2**.
11. Change the **IKE Configuration** fields if needed; then click **OK**.
The fields are described in [IPsec IKE and ESP elements](#).
12. Change the **ESP Configuration** fields if needed; then click **OK**.
The fields are described in [IPsec IKE and ESP elements](#).
13. Complete the **Add Connection** fields for the desired connection.
 - Enter the **Local Address**.
 - Enter the **Remote Address**.
 - Enter the **Pass Phrase**.
 - Select the **Mode**.
14. Click **OK**.
15. Select **Yes** to restart the connection.
When the connection has been updated, the **Internet Key Exchange Version Menu** appears.
16. Select **Exit**.
17. Log out of platcfg.
See [Logging out of platcfg](#).

Enabling and Disabling an IPsec Connection

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

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

1. Open platcfg.
See [Accessing platcfg](#).
2. Select **Network Configuration**.
3. Select **IPsec Configuration**.
4. Select **IPsec Connections**.
5. Select **Edit**.
6. Select **Connection Control**.
7. Select the IPsec connection to enable or disable.
8. Select **Enable** or **Disable**.

9. Click **OK** to enable or disable the selected IPsec connection.
10. Log out of platcfg.
See [Logging out of platcfg](#).

Deleting an IPsec connection

Use this task to delete an IPsec connection.

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

Logging out of platcfg

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

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

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

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

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

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

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

Integrated Diameter Intelligence Hub

Topics:

- [*Integrated Diameter Intelligence Hub Overview.....109*](#)
- [*Accessing IDIH.....109*](#)

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

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

Integrated Diameter Intelligence Hub Overview

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

- Probeless monitoring and network intelligence data collection and monitoring
- Nodal tracing (DSR ingress and egress traffic) and message protocol decode
- Ladder diagrams showing the continuous flow between elements
- Alarm forwarding for signaling and system alarms
- A self-surveillance diagnostic utility
- Data feed that can be used to schedule automatic export of trace data to a customer server.
- Data feed for and filtering on Diameter (S6) xDR content
- A web-based GUI providing security, configuration, and application access
- The metadata captured by IDIH for the Policy DRA application includes the results of each query that Policy DRA makes to the session and binding database and the associated result.

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

Accessing IDIH

To log into IDIH from DSR SOAM GUI:

1. Using a Web browser, type the **IP Address** for a DSR SOAM.

Note: Contact the system administrator for the IP Address.

The login screen opens.

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

Note: Check with the system administrator for the user name and password.

Note: If logging into IDIH from DSR, only the ProTrace application will be available for use unless logging in as idihadmin.

3. Navigate to **Diameter > Troubleshooting with DIH > Maintenance > Traces**.
4. Click the **Launch DIH** button.
5. Alternatively, select a trace and click **Analyze With IDIH**.

Chapter 4

Database Backups and Restores

Topics:

- [*Database Backups and Restores.....111*](#)

The database contains the configuration information for a DSR deployment.

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

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

Database Backups and Restores

The database contains the configuration information for a DSR deployment.

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

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

Manual Backups

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

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

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

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

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

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

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

Example of a backup file name:

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

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

Automatic Backups

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

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

The automatically generated backup archive files include a “.AUTO” extension to distinguish them from manually generated backup archive files.

Creating a Database Backup

Use this task to create a backup of the DSR database configuration data.

1. Select **Status & Manage > Database**. The **Status & Manage > Database** page appears.
2. Click the **Disable Provisioning** button.

Although the backup subsystem is designed to be used without interruption to provisioning service, it may be desirable to stop provisioning briefly in order to note exactly which data has and which data has not been provisioned to the network when the backup is taken.

3. Click OK.

The **Disable Provisioning** button changes to **Enable Provisioning**.

4. Select the active Network OAM&P server to be backed up.

A backup can be created only for an Active server.

5. Click **Backup**.

The **Status & Manage > Database [Backup]** page appears.

6. In the **Select data for backup** field, verify that the **Configuration** box is checked.

The DSR has no Provisioning data; the Provisioning check box is disabled.

7. Select a **Compression** type, if different from the default.

8. If you want to change the backup file name from the default name, enter the backup file name in the **Archive Name** field.

It is recommended that the default name not be changed.

9. Enter an optional **Comment**.

10. Click OK.

The backup begins. The **Database Status** page appears again. The status of the backup appears in the information message box with a message similar to the following:

```
Backup on <server_name> status MAINT_IN_PROGRESS.
```

11. Click the **Enable Provisioning** button.

You do not need to wait until the backup completes before enabling provisioning again in the system.

12. Click OK.

The **Enable Provisioning** button changes to **Disable Provisioning**; Configuration updates are enabled for all servers.

13. Wait for the backup to complete.

The backup is complete when the status message changes to:

```
Backup on <server_name> status MAINT_CMD_SUCCESS. Success
```

The backed up data is stored in a compressed file and copied to the File Management Storage Area of the server that was backed up. To access the backup file, use the **Status & Manage > Files** page. To transfer the file to a secure location, use the [Transferring a Database Backup File to Another Location](#) procedure.

Transferring a Database Backup File to Another Location

Use this task to transfer a database backup file from the File Management Storage Area to an alternate location outside of the DSR system.

1. Select **Status & Manage > Files**.
The **Status & Manage Files** page appears.
2. Select the tab for an active Network Element server, to list the files for that server.
3. Select the name of the backup file you want to transfer.
4. Click **Download**.
The **File Download** box appears.
5. Click **Save**.
Your browser's **Save As** window appears.
6. Navigate to the location where the file will be saved.
7. Click **Save**.
The file is saved to the selected location.

Database Restores

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

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

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

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

A

AAA Authentication, Authorization, and Accounting (Rx Diameter command)

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

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

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

C

CDF Charging Data Function

CEA Capability-Exchange-Answer
The Diameter response that the prepaid rating engine sends to the Mobile Originated application during capability exchanges.

C

CER	<p>Capabilities-Exchange-Request</p> <p>A Diameter message that the Mobile Originated application sends to a prepaid rating engine to perform a capability exchange. The CER (indicated by the Command-Code set to 257 and the Command Flags' 'R' bit set) is sent to exchange local capabilities. The prepaid rating engine responds with a Capability-Exchange-Answer (CEA) message.</p>
CEX Configuration Set	<p>A mechanism for assigning Application IDs and supported Vendor IDs to a Local Node or to a Connection.</p>
CPA	<p>Capability Point Code ANSI</p> <p>Charging Proxy Application</p> <p>The Charging Proxy Application (CPA) feature defines a DSR-based Charging Proxy Function (CPF) between the CTFs and the CDFs. The types of CTF include GGSN, PGW, SGW, HSGW, and CSCF/TAS.</p>
CPF	<p>Charging Proxy Function</p> <p>A CPF instance is a DSR running the CPA application.</p>
CTF	<p>Charging Trigger Function</p>

D

DA-MP	<p>Diameter Agent Message Processor</p> <p>A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local</p>
-------	--

D

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

DAS

Diameter Application Server
Diameter Agent Server

Diameter

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

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

Diameter Agent Message
Processor

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

D

DIH	<p>Diameter Intelligence Hub</p> <p>A troubleshooting solution for LTE, IMS, and 3G Diameter traffic processed by the DSR. DIH does not require separate probes or taps.</p>
DM-IWF	<p>Diameter –MAP Interworking DSR Application, which translates Diameter messages into MAP messages</p>
DPA	<p>Disconnect-Peer-Answer</p> <p>A message used by a Diameter node to answer the Disconnect-Peer-Request (DPR).</p>
DPR	<p>Disconnect-Peer-Request</p> <p>A message used by a Diameter node to inform its peer of its intent to disconnect the transport layer. Upon receipt of a DPR, the Disconnect-Peer-Answer (DPA) is returned.</p>
DSR	<p>Data Set Ready</p> <p>Diameter Signaling Router</p> <p>A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes.</p> <p>Delete Subscriber Data Request</p>
DSR Application	<p>Any DSR software feature or function that is developed as a user of the Diameter base protocol.</p>

D**DWA****Device-Watchdog-Answer**

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

DWR**Device-Watchdog-Request**

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

E**EMS****Element Management System**

The EMS feature consolidates real-time element management at a single point in the signaling network to reduce ongoing operational expenses and network

E

downtime and provide a higher quality of customer service.

F

FABR

Full Address Based Resolution

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

FQDN

Fully qualified domain name

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

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

G

GGA

Get-Gateway-Answer A reply to a GGR. It contains session information for the subscriber present in the GGR. GGA includes the bindings for the subscriber such as, Access Point Name, PCEF FQDN and Creation timestamp. The session information is aggregated in the GGA based on the PCRF to which it is assigned.

GGR

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

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.

GQC Gateway Query Client also known as Diameter Node

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

H

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

HSS Home Subscriber Server
A central database for subscriber information.

I

I

IDIH	Integrated Diameter Intelligence Hub
IMI	Internal Management Interface
IMS	<p>IP Multimedia Subsystem</p> <p>These are central integration platforms for controlling mobile communications services, customer management and accounting for mobile communications services based on IP. The IMS concept is supported by 3GPP and the UMTS Forum and is designed to provide a wide range of application scenarios for individual and group communication.</p>
IP	<p>Intelligent Peripheral</p> <p>Internet Protocol</p> <p>IP specifies the format of packets, also called datagrams, and the addressing 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.</p>
IPFE	<p>IP Front End</p> <p>A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.</p>

I

IPsec	<p>Internet Protocol Security</p> <p>A protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a data stream.</p>
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

L

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

M

MAP	<p>Mated Application Part</p> <p>Mobile Application Part</p> <p>An application part in SS7 signaling for mobile communications systems.</p>
MCC	<p>Mobile Country Code</p> <p>A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies</p>

M

a particular subscriber. See also
MNC, IMSI.

MD-IWF

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

MEAL

Measurements, Events, Alarms,
and Logs

MP

Measurement Platform

Message Processor

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

MTP3

Message Transfer Part, Level 3

N

NE

Network Element

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

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

NMS

Network Management System

N

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

NOAMP

Network Operations,
Administration, Maintenance, and
Provisioning

O

OAM

Operations, Administration, and
Maintenance

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

OCS

Online Charging Server

OFCS

Offline Charging Server

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.

P

Peer	A Diameter node to which a given Diameter node has a direct transport connection.
Policy DRA	Policy Diameter Relay Agent. A scalable, geo-diverse DSR application that creates a binding between a subscriber and a PCRF, and routes all policy messages for a given subscriber to the PCRF that currently hosts that subscriber's policy rules. Policy DRA is capable of performing Topology Hiding to hide the PCRF from the Policy Client.
Proxy Agent	Performs the basic forwarding functions of a Relay Agent, but unlike a Relay Agent, a Proxy Agent can modify the message content and provide value-added services, enforce rules on different messages, or perform administrative tasks for a specific realm.
pSBR	Policy SBR

R

RBAR	Range Based Address Resolution A DSR enhanced routing application which allows the user to route Diameter end-to-end transactions based on Application ID, Command Code, "Routing Entity" Type, and Routing Entity address ranges.
------	---

S

SCTP	Stream Control Transmission Protocol
------	--------------------------------------

S

An IETF transport layer protocol, similar to TCP that sends a message in one operation.

The transport layer for all standard IETF-SIGTRAN protocols.

SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.

SDS

System Debug Services

Subscriber Database Server

Subscriber Database Server (SDS) provides the central provisioning of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query Server and the Data Processor System Operations, Administration, and Maintenance (DP SOAM) servers at each Diameter Signaling Router (DSR) site or a standalone DP site to replicate and recover provisioned data to the associated components.

SNMP

Simple Network Management Protocol.

An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol

S

arranges managed objects into groups.

SS7

Signaling System #7

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.

TCP

Transmission Control Protocol

A connection-oriented protocol used by applications on networked hosts to connect to one another and to exchange streams of data in a reliable and in-order manner.

V

VIP

Virtual IP Address

Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more

V

IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.

X

XMI

External Management Interface