

# ***EAGLE<sup>®</sup> XG Diameter Signaling Router***

---

## **DSR Administration Guide**

910-6639-001 Revision A  
May 2013



Copyright 2013 Tekelec. All Rights Reserved. Printed in USA.  
Legal Information can be accessed from the Main Menu of the optical disc or on the  
Tekelec Customer Support web site in the *Legal Information* folder of the *Product Support* tab.

# Table of Contents

<b>Part I: Introduction.....</b>	<b>7</b>
<b>Chapter 1: About the DSR Administration Guide.....</b>	<b>8</b>
Introduction.....	9
Scope and Audience.....	9
Document Organization.....	9
Documentation Admonishments .....	10
Related Publications.....	10
Customer Care Center.....	11
Emergency Response.....	14
Locate Product Documentation on the Customer Support Site.....	14
<b>Part II: Diameter Signaling Router (DSR).....</b>	<b>15</b>
<b>Chapter 2: Diameter Signaling Router (DSR).....</b>	<b>16</b>
Diameter Signaling Router Overview.....	17
DSR Functions.....	21
<b>Chapter 3: Diameter Protocol.....</b>	<b>23</b>
Diameter Overview.....	24
Diameter Transport Function.....	25
Diameter Routing Function.....	25
DSR Application Infrastructure.....	27
<b>Chapter 4: Diameter Mediation.....</b>	<b>28</b>
Mediation Overview.....	29
<b>Chapter 5: DSR Applications.....</b>	<b>31</b>
DSR Applications Overview.....	32
<b>Chapter 6: IP Front End (IPFE).....</b>	<b>36</b>

Introduction to IPFE.....	37
<b>Part III: DSR Configuration.....</b>	<b>39</b>
<b>Chapter 7: DSR Configuration Overview.....</b>	<b>40</b>
DSR Configuration.....	41
<b>Chapter 8: IPFE Configuration.....</b>	<b>46</b>
IPFE Configuration Overview.....	47
<b>Chapter 9: Diameter Configuration.....</b>	<b>48</b>
Diameter Configuration Overview.....	49
Configuration Capacity Summary.....	52
MP Profiles.....	52
Application Ids Configuration.....	52
Transport configuration.....	52
Routing Configuration.....	57
Diameter Options Configuration.....	64
Diameter Mediation Configuration Overview.....	64
<b>Chapter 10: DSR Applications Configuration.....</b>	<b>66</b>
DSR Applications Configuration Overview.....	67
FABR Configuration Overview.....	67
RBAR Configuration Overview.....	69
CPA Configuration Overview.....	70
Policy DRA Configuration Overview.....	70
<b>Part IV: Maintenance, Status, and Reports.....</b>	<b>74</b>
<b>Chapter 11: Diameter Maintenance.....</b>	<b>75</b>
Introduction.....	76
Diameter Maintenance and Status Data for Components, DSR Applications, and DA-MPs.....	77
Managing the Status of Diameter Configuration Components.....	79
<b>Chapter 12: Diameter Reports.....</b>	<b>84</b>

Diameter Diagnostics Tool.....	85
Diameter MP Statistics (SCTP) Report.....	85
<b>Part V: Tools and Utilities.....</b>	<b>86</b>
<b>Chapter 13: Imports and Exports .....</b>	<b>87</b>
DSR Bulk Import and Export Overview.....	88
Diameter Mediation Import and Export Overview.....	90
<b>Chapter 14: IPsec.....</b>	<b>93</b>
IPsec Overview.....	94
IPsec IKE and ESP elements.....	96
Accessing platcfg.....	97
Adding an IPsec connection.....	98
Editing an IPsec connection.....	98
Enabling and Disabling an IPsec Connection.....	99
Deleting an IPsec connection.....	100
Logging out of platcfg.....	100
<b>Chapter 15: Diameter Intelligence Hub.....</b>	<b>101</b>
Diameter Intelligence Hub Overview.....	102
Accessing DIH.....	102
<b>Chapter 16: Database Backups and Restores.....</b>	<b>103</b>
Database Backups and Restores.....	104
<b>Glossary.....</b>	<b>107</b>

# List of Figures

- Figure 1: EAGLE XG DSR System Diagram with 2-tiered Topology.....18
- Figure 2: EAGLE XG DSR Diagram with 3-tiered Topology.....19
- Figure 3: EAGLE XG DSR OAM Architecture.....20
- Figure 4: GUI Structure for 3-tiered DSR Topology Configuration.....42
- Figure 5: Weighted Load Sharing.....56
- Figure 6: DSR Routing Diagram.....58
- Figure 7: Route List, Route Group, and Peer Node Relationships.....59
- Figure 8: Route Group Weights.....59
- Figure 9: DSR Implicit Routing.....60
- Figure 10: GUI Structure for 3-tiered DSR Topology with Policy DRA.....72

# List of Tables

Table 1: Diameter Configuration Component Status Dependencies.....	77
Table 2: Route List Status Data.....	78
Table 3: Maintenance and Status Data Sourcing Methods.....	80
Table 4: Diameter Configuration Component Sourcing Methods.....	80
Table 5: IPsec IKE and ESP elements.....	96

# Part I

## Introduction

---

### Topics:

- [About the DSR Administration Guide.....8](#)

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.....9](#)
- [Scope and Audience.....9](#)
- [Document Organization.....9](#)
- [Documentation Admonishments .....10](#)
- [Related Publications.....10](#)
- [Customer Care Center.....11](#)
- [Emergency Response.....14](#)
- [Locate Product Documentation on the Customer Support Site.....14](#)

This *DSR Administration Guide* and the DSR Administration Help describe the EAGLE XG 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 of the Help InfoCenter DVD, 936-0403-501, contact your Tekelec Sales Representative.

## Introduction

This document provides administrative information for the EAGLE XG 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:
  - IPsec for secure connections
  - Diameter Intelligence Hub (DIH)
  - Imports and Exports
  - 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 Tekelec 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.

## 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, and Policy DRA 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.
  - [Diameter Intelligence Hub](#) provides a brief description of the use of the Diameter Intelligence Hub (DIH) with the DSR.
  - [Database Backups and Restores](#) describes DSR-related database backup and restore functions.

## Documentation Admonishments

Admonishments are icons and text that may appear in this and other Tekelec 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:** This icon and text indicate the possibility of equipment damage and personal injury from toppling.



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



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



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

## Related Publications

The Diameter Signaling Router (DSR) documentation set includes the following publications, which provide information for the configuration and use of DSR and related applications.

*Getting Started* includes a product overview, system architecture, and functions. It also explains the DSR GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets.

*Feature Notice* describes new features in the current release, provides the hardware baseline for this release, and explains how to find customer documentation on the Customer Support Site.

*Roadmap to Hardware Documentation* provides links to access manufacturer online documentation for hardware related to the DSR.

*Operation, Administration, and Maintenance (OAM) Guide* provides information on system-level configuration and administration tasks for the advanced functions of the DSR, both for initial setup and maintenance.

*Communication Agent User Guide* explains how to use the Communication Agent GUI pages to configure Remote Servers, Connection Groups, and Routed Servers, and to maintain configured connections.

*Diameter and Mediation User Guide* explains how to use the Diameter GUI pages to manage the configuration and maintenance of Local and Peer Nodes, connections, Configuration Sets, Peer Routing Rules, Application Routing Rules, and System, DNS, and Local Congestion options; and explains how to configure and use Diameter Mediation.

*IP Front End (IPFE) User Guide* explains how to use the IPFE GUI pages to configure IPFE to distribute IPv4 and IPv6 connections from multiple clients to multiple nodes.

*Range-Based Address Resolution (RBAR) User Guide* explains how to use the RBAR GUI pages to configure RBAR to route Diameter end-to-end transactions based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity address ranges and individual addresses.

*Full-Address Based Resolution (FABR) User Guide* explains how to use the FABR GUI pages to configure FABR to resolve designated Diameter server addresses based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity addresses.

*Charging Proxy Application (CPA) and Offline Charging Solution User Guide* describes the Offline Charging Solution and explains how to use the CPA GUI pages to set System Options for CPA, configure the CPA's Message Copy capability, and configure the Session Binding Repository for CPA.

*Policy DRA User Guide* describes the topology and functions of the Policy Diameter Routing Agent (Policy DRA or P-DRA) DSR application and the Policy Session Binding Repository, and explains how to use the Policy DRA GUI pages to configure P-DRA.

*DSR Alarms, KPIs, and Measurements Reference Guide* provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual Diameter measurement value; and explains how to generate reports containing current alarm, event, KPI, and measurement information.

*DSR Administration Guide* describes DSR architecture, functions, configuration, and tools and utilities (IPsec, Import/Export, DIH, and database backups); and provides references to other publications for more detailed information.

## Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

### Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

Phone:

1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

Phone:

+1-919-460-2150

TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

- **Argentina**

Phone:

0-800-555-5246 (toll-free)

- **Brazil**

Phone:

0-800-891-4341 (toll-free)

TAC Regional Support Office Hours:

8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

- **Chile**

Phone:

1230-020-555-5468

- **Colombia**

Phone:

01-800-912-0537

- **Dominican Republic**

Phone:

1-888-367-8552

- **Mexico**

Phone:

001-888-367-8552

- **Peru**

Phone:

0800-53-087

- **Puerto Rico**

Phone:

1-888-367-8552 (1-888-FOR-TKLC)

- **Venezuela**

Phone:

0800-176-6497

- **Europe, Middle East, and Africa**

Regional Office Hours:

8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

- **Signaling**

Phone:

+44 1784 467 804 (within UK)

- **Software Solutions**

Phone:

+33 3 89 33 54 00

- **Asia**

- **India**

Phone:

+91-124-465-5098 or +1-919-460-2150

TAC Regional Support Office Hours:

10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

- **Singapore**

Phone:

+65 6796 2288

TAC Regional Support Office Hours:

9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

## Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. 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 the Tekelec Customer Care Center.

## Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at [www.adobe.com](http://www.adobe.com).

1. Log into the [Tekelec Customer Support](#) site.

**Note:** If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

# Part II

## Diameter Signaling Router (DSR)

---

### Topics:

- *Diameter Signaling Router (DSR).....16*
- *Diameter Protocol.....23*
- *Diameter Mediation.....28*
- *DSR Applications.....31*
- *IP Front End (IPFE).....36*

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.

## Diameter Signaling Router (DSR)

---

### Topics:

- [Diameter Signaling Router Overview.....17](#)
- [DSR Functions.....21](#)

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

The DSR product supports:

- A 2-tiered DSR topology
- A 3-tiered DSR topology

In 2-tiered DSR topology, an independent pair of NOAM servers for each DSR interacts directly with DA-MP servers in that DSR system.

In 3-tiered 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 same functions are provided in both topologies. The 3-tiered DSR topology does not alter existing DSR functions other than separating what can be configured or managed at which level (DSR NOAM or DSR SOAM).

The architecture includes the following characteristics:

- Each DSR services signaling traffic to and from a collection of Diameter clients, servers, and agents.
- Each DSR supports :
  - OAM servers (OAM), operating in Active/Standby mode; only NOAM servers in 2-tiered DSR topology; NOAM and SOAM servers in 3-tiered DSR topology.
  - 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. Each DSR operates at 40% capacity under normal conditions.

- The Diameter Intelligence Hub (DIH) provides the ability to filter, access, and troubleshoot Diameter transactions,

Figure 1: EAGLE XG DSR System Diagram with 2-tiered Topology and Figure 2: EAGLE XG DSR Diagram with 3-tiered Topology provide an overview of the EAGLE XG DSR architecture.

**2-tiered DSR Topology**

In 2-tiered DSR topology, as shown in Figure 1: EAGLE XG DSR System Diagram with 2-tiered Topology, there are NOAM servers and MP servers. On NOAM servers, GUI screens can be used to configure and manage:

- Network topology data (such as user accounts, network elements, servers, and server groups)
- Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists) DSR Application data (Policy DRA, RBAR, FABR, and CPA) and IPFE data

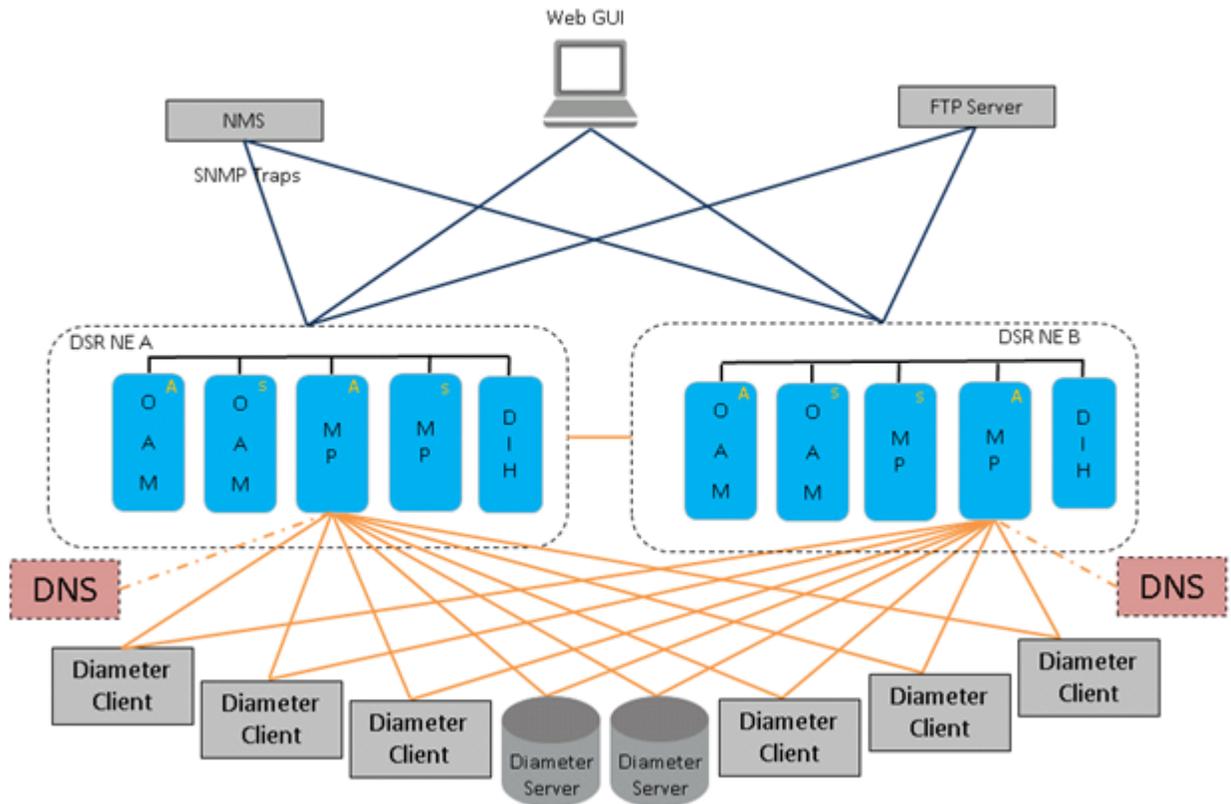


Figure 1: EAGLE XG DSR System Diagram with 2-tiered Topology

The MP servers process the database updates from NOAM servers and perform the real-time signaling functions. The MP servers also supply the Platform measurements, events, alarms, and log (MEAL) data, Diameter signaling MEAL data, and Diameter Application MEAL data to NOAM servers.

**3-tiered DSR Topology**

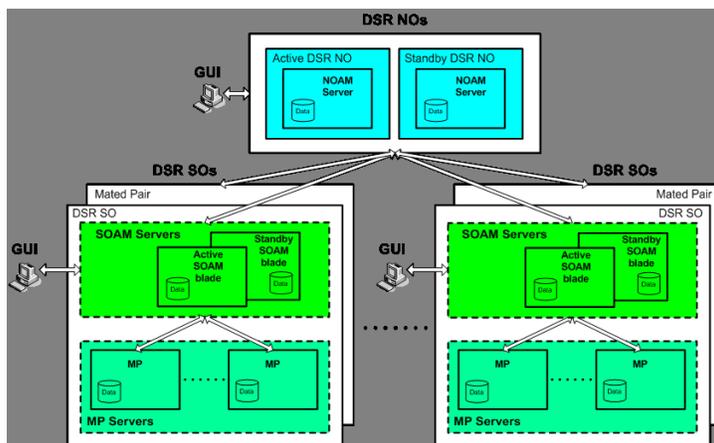
The primary change between the 2-tiered DSR topology and the 3-tiered DSR topology is the introduction of the DSR SOAM server. The role of the DSR NOAM server is changed to take on network

scope instead of the Network Element scope it has with the 2-tiered DSR topology. The role of the DSR SOAM becomes similar to the role of the NOAM in the 2-tiered DSR topology in that it is managing a single DSR system (or DSR Signaling NE).

In 3-tiered DSR topology, as shown in *Figure 2: EAGLE XG DSR Diagram with 3-tiered Topology*, there are NOAM servers, SOAM servers, and MP servers.

In 3-tiered 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). P-DRA has part of its configuration GUI on the NOAM. Diameter provides the Configuration Import and Export GUIs on the NOAM for exporting and importing the NOAM P-DRA configuration data.
- On a DSR SOAM, Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists), DSR Application data (RBAR, FABR, P-DRA, and CPA), and IPFE data. Diameter provides the Configuration Import and Export GUIs on the SOAM for exporting and importing the SOAM configuration data for Diameter Configuration and DSR Applications.



**Figure 2: EAGLE XG DSR Diagram with 3-tiered 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 2-tiered DSR topology, the SDS has its own independent NOAMP and SOAM infrastructure.

In 3-tiered DSR topology, 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.

### OAM Servers

The DSR Operations, Administration, Maintenance, and Provisioning (OAM&P) subsystem includes OAM servers (NOAMs for 2-tiered DSR topology, and NOAMs and SOAMs for 3-tiered topology) and Message Processors (MPs). Each of these must be configured separately. (Provisioning is done only in SDS, and not in DSR.)

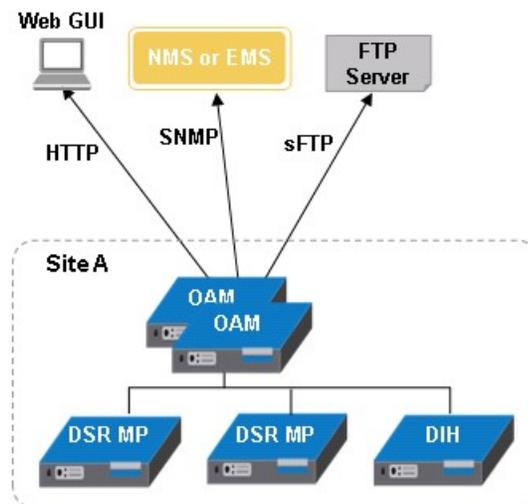
A pair of Operation, Administration, and Maintenance (OAM) servers make up one OAM component of the DSR. This pair of servers has an Active/Standby relationship. The Active server in the pair controls the virtual IP addresses (VIP) that direct XMI and IMI traffic to the Active server.

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 3: EAGLE XG DSR OAM Architecture* illustrates the DSR OAM architecture.



**Figure 3: EAGLE XG 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.

### Diameter Intelligence Hub

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

## Diameter Signaling Router (DSR)

- **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, and egress message throttling; and Local Congestion and Egress Transport Congestion status.
- **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:** The DSR Charging Proxy Application (CPA) supports forwarding a copy of a Diameter Request message received by or routed through the DSR to a Diameter Application Server (DAS).
- **Diameter Intelligence Hub:** The 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 3

## Diameter Protocol

---

### Topics:

- *Diameter Overview.....24*
- *Diameter Transport Function.....25*
- *Diameter Routing Function.....25*
- *DSR Application Infrastructure.....27*

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 either:

- A 2-tiered DSR topology
- A 3-tiered DSR topology

In 2-tiered DSR topology, an independent pair of NOAM servers for each DSR interacts directly with DA-MP servers in that DSR.

In 3-tiered 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 same functions are provided in both topologies. The 3-tiered DSR topology 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.

### 2-tiered DSR Topology

In 2-tiered DSR topology, there are NOAM servers and MP servers. On NOAM servers, GUI screens can be used to configure and manage Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists) DSR Application data (Policy DRA, RBAR, FABR, and CPA) and IPFE data.

Diameter provides the Configuration Import and Export GUIs on the NOAM for exporting and importing the configuration data for Diameter Configuration and DSR Applications.

### 3-tiered DSR Topology

The NOAM server takes on network scope instead of the Network Element scope it has with the 2-tiered DSR topology. Each SOAM server manages a single DSR Signaling NE.

In 3-tiered DSR topology, there are NOAM servers, SOAM servers, and MP servers.

In 3-tiered DSR topology, SOAM GUI screens can be used to configure and manage Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists), DSR Application data (RBAR, FABR, P-DRA, and CPA), and IPFE data.

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

## Diameter Transport Function

Though Diameter can be distributed over multiple MPs, 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.

The Diameter Transport Function is responsible for the following functions:

- Managing transport connections
  - SCTP uni-homing and multi-homing connections
 

SCTP multi-homing provides fault tolerance against network failures by using alternate paths through the IP network when there are two transmission paths as part of a single SCTP association between two SCTP endpoints. Data traffic between the two nodes can flow if at least one of the paths is available. SCTP multi-homing does not provide load balancing.
  - TCP connections
- Processing Diameter Peer-to-Peer messages and related functions
- Performs Capabilities Exchange (CER/CEA)
 

After establishment of a transport connection, Diameter Peers must perform Capabilities Exchange in order to discover the identity and capabilities of the Peer. Capabilities Exchange is performed using the CER and CEA messages.
- Providing Diameter Watchdog (DWR/DWA) functions to detect Diameter transport failures
- Processing Disconnect Peer (DPR/DPA) messages
- Interfacing with the Diameter Routing Function
  - Processing connection status updates received from Diameter Routing Function
  - Sending Diameter Request messages received from Peers to a local Diameter Routing Function instance for routing
  - Sending Diameter Answer messages received from Peers to an appropriate instance of Diameter Routing Function
  - Sending Diameter messages received from the Diameter Routing Function to the appropriate Peer
  - Assigning Priority to ingress Answers and Requests for configuring preferential treatment of routing and discard for certain messages
  - Disconnect transport connections on request by Diameter Routing Function (for handling duplicate connections)
- Processing configuration and maintenance changes
- Updating alarm, event, KPI, and measurements data for transport configuration components
- Performing transport capacity control
- Providing Per Connection Ingress MPS Control, Per Connection Egress Message Throttling, and Egress Transport Congestion functions

## 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 a copy of a Diameter Request message that is received by or routed through the DSR to a Diameter Application Server (DAS). The function is triggered based on configuration and can be initiated by the DSR Charging Proxy Application.

- 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
- 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 Relay Agent (Policy DRA)

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

# Chapter 4

## Diameter Mediation

---

### Topics:

- [Mediation Overview.....29](#)

The Diameter Mediation feature allows easy creation of Mediation Rules.

## Mediation Overview

### References:

- *Diameter and Mediation User 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. 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.
- An Action can be adding, altering, or deleting AVPs; modifying the message header Flags, Length, Command-Code, or Application-ID; or other operations.

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, AVP Dictionary entries, and Vendors 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 5

## DSR Applications

---

### Topics:

- [DSR Applications Overview.....32](#)

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 Relay Agent (Policy DRA)

## 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 Relay Agent (Policy DRA)

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

### Full Address Based Resolution

#### References:

- *Full Address Based Resolution (FABR) User 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 supported by FABR is one of the following User Identities :

- International Mobile Subscriber Identity (IMSI)
- Mobile Subscriber Integrated Services Digital Network (Number) (MSISDN)
- IP Multimedia Private Identity (IMPI)
- IP Multimedia Public Identity (IMPU)

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 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.

In 2-tiered DSR topology, the SDS has its own independent NOAMP and SOAM infrastructure.

In 3-tiered DSR topology, 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 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.

## Charging Proxy Application

### References:

- *Charging Proxy Application (CPA) and Offline Charging Solution User 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 Guide*
- **Help ► Policy DRA**

The Policy Diameter Routing Agent, or Policy DRA (P-DRA) runs as a DSR Application that interfaces with the Diameter Routing Function, to solve Diameter routing problems that are specific to the Policy and Charging Control (PCC) management domain as defined in 3GPP specifications.

In Policy DRA, subscribers are dynamically assigned to a PCRF when the initial bearer session (Gx or Gxx interface) is created. All subscriber Policy sessions from anywhere in the network are routed to the assigned PCRF until that subscriber's last Gx or Gxx session ends, at which point the next Gx or Gxx session may be routed to a different PCRF. This dynamic mapping of subscribers to PCRFs provides automatic load distribution to available PCRFs, while still mapping all of a subscriber's sessions to a single PCRF.

Topology Hiding of the PCRF from some Policy Clients prevents the Policy Client from obtaining knowledge of the PCRF identity (host name or IP address), or knowledge of the number or location of PCRFs deployed in the network.

The Policy Session Binding Repository provides 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. A Session in the context of the Policy DRA application refers to a Diameter session over a policy interface (Gx/Gxx, Rx, S9) that Policy DRA processes. A Binding refers to an association between a subscriber and a PCRF that is assigned to provide policy rules to that subscriber.

The Policy SBR receives Requests from Policy DRA for session and binding database manipulations, responds to the Requests with a result, and stores the session and binding data in the Policy SBR database.

# Chapter 6

## IP Front End (IPFE)

---

### Topics:

- [Introduction to IPFE.....37](#)

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 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 presents one or more externally routable IP addresses to accept TCP or unihomed SCTP traffic from clients. These externally visible addresses are known as Target Set Addresses (TSAs). Each TSA has an associated set of IP addresses for application servers, up to 16 addresses, known as a Target Set. The IP addresses in a given Target Set are of the same IP version (that is, IPv4 or IPv6) as the associated TSA.

A typical client is configured to send TCP or SCTP traffic to one or more of the TSAs, rather than directly to an application server. When the IPFE receives a packet at a TSA, it first checks to see if it has state that associates the packet's source address and port to a particular application server.

This state is known as an "association." If no such association exists (that is, the packet was an "initial" packet), the IPFE runs a selection function to choose an application server address from the eligible addresses in the Target Set. The selection function uses a configurable weighting factor when selecting the target address from the list of eligible addresses. The IPFE routes the packet to the selected address, and creates an association mapping the source address and port to the selected address. When future packets arrive with the same source address and port, the IPFE routes them to the same selected address according to the association.

The IPFE sees only packets sent from client to server. Return traffic from server to client bypasses the IPFE for performance reasons. However, the client's TCP or SCTP stack "sees" only one address for the TSA; that is, it sends all traffic to the TSA, and perceives all return traffic as coming from the TSA.

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

In high-availability configurations, four IPFEs may be deployed as two mated pairs, with each pair sharing TSAs and Target Sets. The mated pairs share sufficient state so that they may identically route any client packet sent to a given TSA.

### Connection balancing

Under normal operation, the IPFE distributes connections among application servers according to the weighting factors defined in the Target Sets. However, certain failure and recovery scenarios can result in an application server having significantly more or fewer connections than is intended by its weighting factor. The IPFE considers the system to be "out of balance" if this discrepancy is so large that the overall system cannot reach its rated capacity even though individual application servers still have

capacity to spare, or so that a second failure is likely to cause one of the remaining servers to become overloaded. The IPFE determines this by measuring the number of packets sent to each server and applying a “balance” heuristic.

When the IPFE detects that the system is out of balance, it sets an alarm and directs any new connections to underloaded application servers to relieve the imbalance.

### Overload handling

If the IPFE itself becomes overloaded, it will drop packets. From the application server and client perspectives, this packet loss will appear as network congestion. Their transport stacks will transparently recover from minor packet loss.

If the IPFE becomes overloaded because it has exceeded the rated number of connections, it will invalidate related state entries on a least recently used basis.

If an application server becomes overloaded, the IPFE will remove the application server from the Target Set and direct client connections to the other application servers within the Target Set.

### High availability

When paired with another IPFE instance and configured with at least two Target Set Addresses, the IPFE supports high availability. In the case of an IPFE pair and two Target Set Addresses, each IPFE is configured to handle one Target Set Address. Each IPFE is automatically aware of the ruleset for the secondary Target Set Address. If one IPFE should become unavailable, the other IPFE becomes active for the failed IPFE's Target Set Address while continuing to handle its own.

In the case of an IPFE pair, but only one Target Set Address, then one IPFE is active for the Target Set Address and the other is standby.

# Part III

## DSR Configuration

---

### Topics:

- [DSR Configuration Overview.....40](#)
- [IPFE Configuration.....46](#)
- [Diameter Configuration.....48](#)
- [DSR Applications Configuration.....66](#)

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

## DSR Configuration Overview

---

### Topics:

- [DSR Configuration.....41](#)

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

The DSR supports 2-tiered OAM architecture, and 3-tiered OAM architecture.

## DSR Configuration

### References:

- *DSR HP C-Class Installation* for the appropriate release
- *DSR Upgrade/Backout Procedure* for the appropriate release
- *DSR 4.1 RMS Productization Installation*
- Feature Activation Guides for any DSR Applications in the system
- *Operation, Administration, and Maintenance (OAM) Guide* and Help
- User Guides and Help for Communication Agent, IPFE, Diameter and Mediation, and DSR Applications

Configuring the DSR can include:

- Network hardware and firmware installation and configuration; and PM&C, TVOE, and SNMP configuration  
Tekelec 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  
Tekelec 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  
Tekelec Support personnel normally either perform or participate in performing these activities.
- Activation of DSR Applications  
Tekelec 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 activated DSR Applications

### Configuration in 2-tiered and 3-tiered DSR Topology

DSR supports a 2-tiered OAM architecture with one pair of NOAM servers per DSR NE. The OAM, Diameter, and DSR Application configuration is all done on the NOAM.

DSR supports a 3-tiered OAM architecture with a pair of NOAM servers and a pair of SOAM servers per DSR NE.

- OAM configuration and some DSR Application configuration are done on the NOAM
- Diameter configuration and most DSR Application configuration are done on the SOAM
- some common utilities can be accessed on either OAM

The use of a 2-tiered DSR topology NOAM server, or a 3-tiered DSR topology NOAM server and a 3-tiered DSR topology SOAM server, 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.

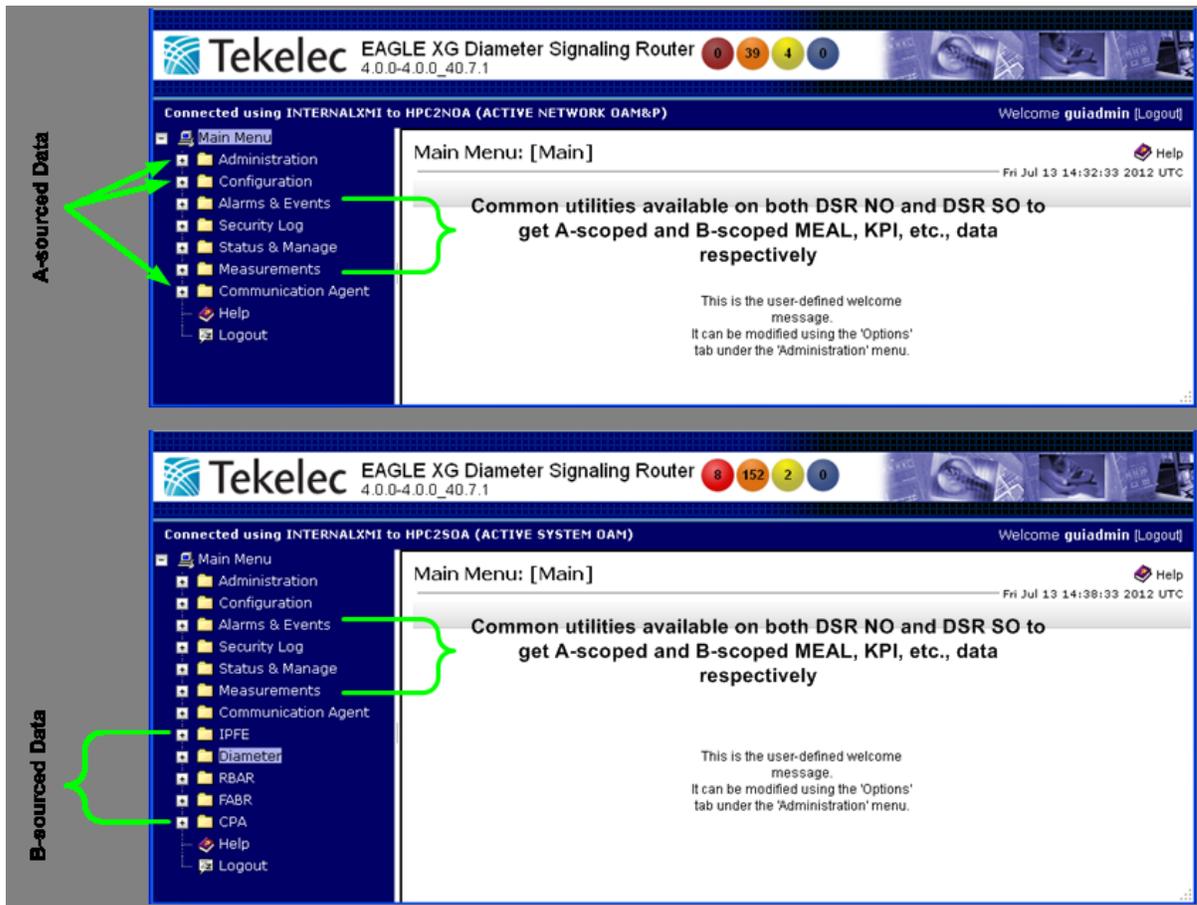


Figure 4: GUI Structure for 3-tiered DSR Topology Configuration

When the Policy DRA DSR Application is not activated in the system, the 3-tiered DSR topology GUI structure appears as illustrated in [Figure 4: GUI Structure for 3-tiered DSR Topology Configuration](#) (except that not all of the DSR Applications can be activated at the same time).

3-tiered 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.

The design of the GUI pages for the data managed by both 2-tiered DSR topology GUIs and 3-tiered DSR topology GUIs is common. The user does not need to learn new screen layouts and configuration procedures as a result of the split, with the exception of learning where each individual data element is configured. For example, the screens for configuring Route Lists are the same in the 3-tiered DSR topology SOAM GUI and the 2-tiered DSR topology NOAM GUI.

#### 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 is called A-sourced data. (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 (Policy DRA, RBAR, FABR, CPA) that is configured and managed through a DSR SOAM is 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

### 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 and Mediation User 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

### 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
  - Peer Routing Rules
  - Application Routing Rules
- Configuration on the NOAM or SOAM, or both, of DSR Application components

# Chapter 8

## IPFE Configuration

---

### Topics:

- [IPFE Configuration Overview.....47](#)

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 Guide*
- **Help ► IPFE**

The IP Front End (IPFE) User Guide describes activities that need to be performed before and after the CPA configuration is performed, including enabling the CPA.

The following IP Front End (IPFE) components can be configured:

- Configuration Options
- Target Sets

### 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 you can add a Target Set, you must configure at least one IPFE in **IPFE ► Configuration ► Options**.

## Diameter Configuration

---

### Topics:

- [Diameter Configuration Overview.....49](#)
- [Configuration Capacity Summary.....52](#)
- [MP Profiles.....52](#)
- [Application Ids Configuration.....52](#)
- [Transport configuration.....52](#)
- [Routing Configuration.....57](#)
- [Diameter Options Configuration.....64](#)
- [Diameter Mediation Configuration Overview...64](#)

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 and Mediation User Guide*
- **Help ► Diameter ► Configuration**

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

As described in [DSR Configuration](#), the DSR supports:

- A 2-tiered OAM architecture with one pair of NOAM servers per DSR NE. The OAM, Diameter, and DSR Application configuration is all done on the NOAM.
- A 3-tiered OAM architecture with a pair of NOAM servers and a pair of SOAM servers per DSR NE. OAM configuration is done on the NOAM, Diameter and most DSR Application configuration is done on the SOAM, and some common utilities can be accessed on either OAM. The 3-tiered GUI structure is illustrated in [Figure 4: GUI Structure for 3-tiered DSR Topology Configuration](#).

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

Configuring DSR 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

### 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:
  - **Diameter MP Congestion Management** monitors and provides controls for management of internal resources such as queues and buffer pools, MP Processing Overload Control, and Maximum MPS Limitation for a local MP. Engineering and user configured maximum traffic rates and alarm thresholds are used for monitoring and for alarm onset and abatement. The **Diameter > Configuration > Local Congestion** page displays the Engineering configured values for Maximum Diameter CPU Usage, percent of messages that receive specific message treatment at each Local MP Congestion Level, and Maximum MPS Limitation values for message treatment at each Local MP Congestion Level.
  - 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 configured Capacity Configuration Sets to.
  - 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.

## Configuration Capacity Summary

The **Diameter > Configuration > Capacity Summary** page allows you to view the various types of Diameter configuration items. The following information is displayed in each row of a read-only table:

<b>Configuration Item</b>	The type of Diameter configuration item
<b>Max Allowed Entries</b>	The maximum number of a row's item that can be configured in Diameter.
<b>Configured Entries</b>	The number of a row's item that are currently configured.
<b>% Utilization</b>	The percentage of the maximum number of a row's item that are currently configured.

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

## MP Profiles

A Diameter Agent Message Processor (DA-MP) is a computer or blade hosting the DSR. Multiple instances of the DSR are supported, each executing on a separate physical or virtualized DA-MP.

In the Diameter configuration, an MP Profile must be assigned to each DA-MP.

The MP Profile types are based on the MP blade type and the type of application that is running on the blade. An MP Profile includes definitions of the maximum and threshold message rate values for a DA-MP running the relay application, a database application, or a session application.

## 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](http://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 forwarded to the second.

Figure 5: *Weighted Load Sharing* illustrates the concept of weighted load sharing in the DSR.

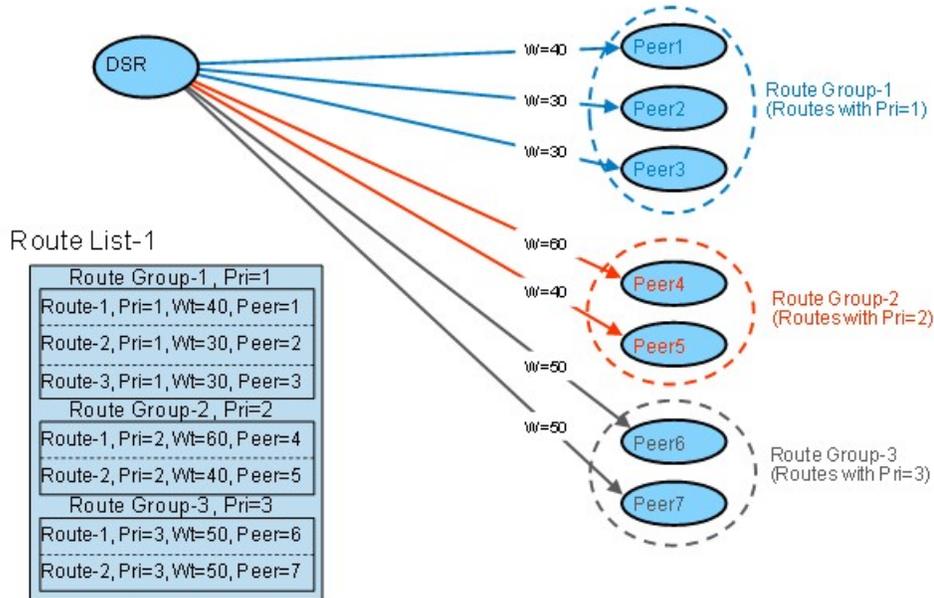


Figure 5: **Weighted Load Sharing**

## 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:

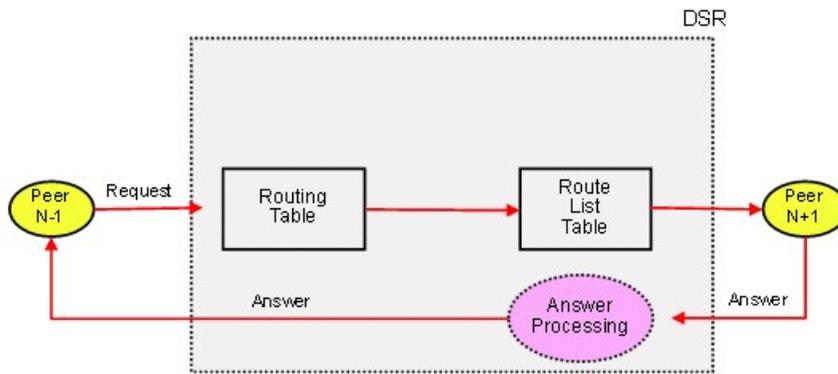
- Routing Diameter Request and Answer messages received from Diameter Peers
- Weighted load sharing
- Priority routing
- Rerouting

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.

## Diameter Routing Functions

*Figure 6: DSR Routing Diagram* illustrates high-level message processing and routing in the DSR.



**Figure 6: 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

#### ***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 7: Route List, Route Group, and Peer Node Relationships* illustrates the relationships between the Route List, Route Groups, and Peer Nodes.

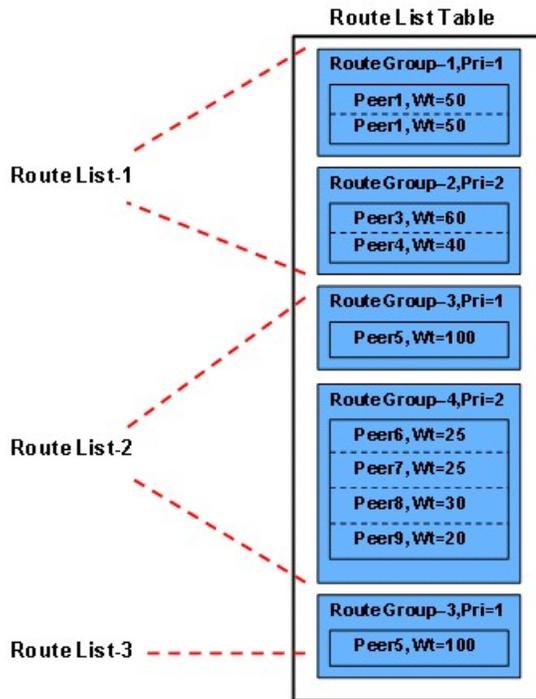


Figure 7: Route List, Route Group, and Peer Node Relationships

*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 8: *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 8: 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.

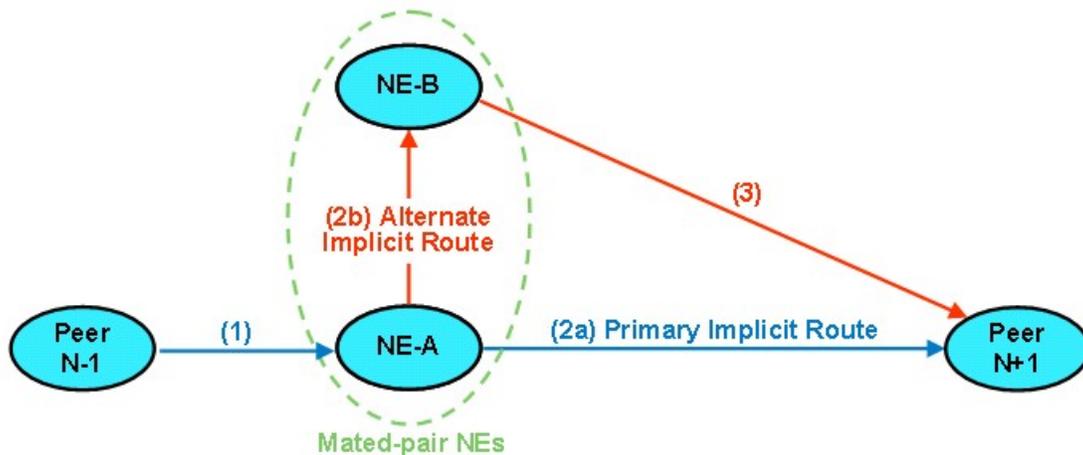
If a message does not match a Peer Routing Rule and contains a Destination-Host AVP that is associated with a Peer Node, then the DSR invokes Implicit Routing to the Peer Node if the Peer Node Operational Status is Available.

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 Routing 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 9: DSR Implicit Routing* illustrates implicit routing in the DSR.



**Figure 9: 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 64 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.

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. (Think of 1 as being first priority and 99 as being last 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.

### 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.

When Diameter selects a viable Diameter connection for forwarding a Request message to an upstream Peer Node, it determines which Pending Answer Timer value to use based on the following precedence selection rules (highest to lowest priority):

1. The Pending Answer Timer assigned to the egress Peer Node to which the Request message will be forwarded

2. The Pending Answer Timer assigned to the Diameter Application ID in the forwarded Request message (header)
3. The "DEFAULT" Pending Answer Timer

Pending Answer Timers can be assigned to the following Diameter components:

- Application Ids
- Peer Nodes

### Reroute On Answer

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

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

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

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

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

### Application Routing Rules Configuration

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

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

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

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

### Diameter Options Configuration

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

- System Options
- DNS Options

#### System Options Configuration

The **System Options** page shows values for transaction processing, message forwarding, maximum Diameter message size, and the result code for messages that are not successfully routed due to an internal resource being exhausted.

The **System Options** page also shows the options used to control how request messages are copied to a Diameter Application Server (DAS).

#### 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 and Mediation User 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.

# Chapter 10

## DSR Applications Configuration

---

### Topics:

- [DSR Applications Configuration Overview.....67](#)
- [FABR Configuration Overview.....67](#)
- [RBAR Configuration Overview.....69](#)
- [CPA Configuration Overview.....70](#)
- [Policy DRA Configuration Overview.....70](#)

This chapter contains overview descriptions 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)

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:

- User Guides and Help for the DSR Applications (FABR, RBAR, CPA, and Policy DRA)
- *Diameter and Mediation User Guide*
- **Help ► Diameter ► Configuration**

This chapter contains overview descriptions 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)

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
- 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 User 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 can include:

- MP Profiles for DA-MPs and SBR servers
- Application Ids for specific Diameter interfaces
- Command Codes
- Peer Nodes
- Local Nodes
- Connections
- Peer Routing Rules
- Application Routing Rules

### FABR Configuration Overview

#### References:

- *Communication Agent User Guide*

- *Full Address Based Resolution (FABR) User Guide*
- **Help ► Full Address Based Resolution (FABR) ► Configuration**

The *Full Address Based Resolution (FABR) User Guide* describes activities that need to be performed before and after FABR configuration is performed, including ComAgent configuration and enabling the FABR application.

FABR configuration typically occurs in the following order:

1. Add **Application IDs** to a list of FABR supported Diameter Application Ids.

**Note:** When an **Application ID** entry is added, **Routing Exceptions** are automatically inserted with the **Routing Exception Action** value as **Forward Unchanged**.

2. If necessary, configure **Default Destinations** to which FABR routes messages.

FABR uses these attributes to modify the contents of a received message before forwarding the message.

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

3. If necessary, edit **Routing Exceptions**.

**Routing Exceptions** specify the routing procedure to invoke when FABR is unable to resolve an address to a Destination for each supported Diameter Application and Routing Exception Type.

The following **Routing Exception** entries are automatically inserted with the **Routing Exception Action** set to **Forward Unchanged** as the default action for a supported Diameter Application entry when that entry is added (and automatically deleted when the Application entry is deleted).

- **Unknown Command Code**
- **No valid Routing Entity Address**
- **No Address Match Found**
- **DP Errors**
- **DP Congestion**

If a **Routing Exception Action** of **Forward Unchanged** is configured, configure a **Default Destination**.

4. Configure **Address Resolutions**.

FABR performs off-board database lookups for User Identities decoded from Diameter messages. The FABR Address Resolutions values configure which (and how) User Identities are to be decoded from the messages. Combinations of Diameter Application ID, and Command Code (the key that is matched to the messages) each Routing Entity Type to be decoded, and a prioritized list of AVPs from which to decode these entity types can be configured. An **Address Resolution** supports up to 2 prioritized Routing Entity Types for each Application ID and Command Code.

5. If necessary, change the **System Options** values for FABR global parameters, including:

- Realm and FQDN
- Allow Subsequent FABR Invocation - if No, a message cannot be processed more than once by FABR.
- Resource Exhaustion Result-Code, Error Message, and Vendor-Id
- Application Unavailable Action, Route List, Result-Code, Error Message, and Vendor-Id

## RBAR Configuration Overview

### References:

- *Range Based Address Resolution (RBAR) User Guide*
- **Help ► Range Based Address Resolution (RBAR) ► Configuration**

The *Range Based Address Resolution (RBAR) User Guide* describes activities that need to be performed before and after RBAR configuration is performed, including enabling the RBAR application.

RBAR configuration typically occurs in the following order:

1. Configure an **Application ID** to a list of RBAR supported Diameter Application Ids.

Inserting a supported Application ID automatically adds 3 Routing Exceptions (**Unknown Command Code**, **No valid Routing Entity Address**, and **Missing Configured Address Entry**) with the **Routing Exception Action** set to **Forward Unchanged** (the Exceptions are automatically deleted when the Application Id is deleted).

2. Configure a **Destination** to which RBAR routes messages.

RBAR uses these attributes to modify the contents of a received message before forwarding the message.

3. If necessary, edit **Exceptions**

**Exceptions** specify the routing procedure to invoke when RBAR is unable to resolve an address to a Destination for each supported Diameter Application and Routing Exception Type.

The following **Exception** entries are automatically inserted with the **Routing Exception Action** set to **Forward Unchanged** as the default action for a supported Diameter Application entry when that entry is added (and automatically deleted when the Application entry is deleted).

- **Unknown Command Code**
- **No valid Routing Entity Address**
- **Missing Configured Address Entry**

4. Configure an **Address Table**, which contains available Routing Entity Types.

5. Configure **Addresses** with the Routing Entity Address Range and **Individual Address** options.

- The **Routing Entity Address Range** provides the mapping between a single address range and a Destination for routing.
- The **Individual Address** provides the mapping between an individual address and a Destination for routing.

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

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

6. Configure an **Address Resolution** to define the routing relationship between message content and an address by mapping a Diameter Application ID, Command Code, and Routing Entity Type to a user-configured address (an Address Range or Individual Address).

An **Address Resolution** supports up to 2 prioritized Routing Entity Types for each Application ID and Command Code (highest priority - Primary Routing Entity Type - and lowest priority - Secondary Routing Entity Type).

7. If necessary, change the **System Options** values for RBAR global parameters, including:
  - Realm and FQDN
  - Allow Subsequent RBAR Invocation - if No, a message cannot be processed more than once by RBAR
  - Resource Exhaustion Result-Code, Error Message, and Vendor-Id
  - Application Unavailable Action, Route List, Result-Code, Error Message, and Vendor-Id

### CPA Configuration Overview

#### References:

- *Charging Proxy Application (CPA) and Offline Charging User Guide*
- **Help ► Charging Proxy Application (CPA) ► Configuration**

The *Charging Proxy Application (CPA) and Offline Charging User Guide* describes activities that need to be performed before and after the CPA configuration is performed, including enabling the CPA.

The Charging Proxy Application (CPA) components can be configured:

- System Options. including:
  - Unavailable Action, and corresponding Result Code, Vendor ID, and Error Message
  - DSR Application Invoked AVP Insertion - a message cannot be processed more than once by a DSR Application if this is set to Yes.
  - Behavior if Session Lookup Error - Generate Answer or Continue Routing
  - Generate Answer Result Code, Vendor ID, and Error Message
- Message Copy, to indicate:
  - Whether Message Copy is Enabled or Disabled
  - The Call-Station-Id AVP value in a message that will trigger Message Copy to the corresponding DAS
  - The DAS Route List that corresponds to each configured Call-Station-Id AVP value
- SBR, the Session Binding Repository, to specify when the stale session binding audit will run and how old a binding has to be before it is considered stale.
- SBR Subresource Mapping

The SBR Subresource Mapping is configured ONCE, if the default values need to be changed. The GUI page then becomes view-only, and Tekelec assistance is required to change values.

### Policy DRA Configuration Overview

#### References:

- *Policy DRA User Guide*
- **Help ► Policy DRA**

The DSR 3-tiered Operations, Administration, and Maintenance (OAM) topology is required for the Policy DRA application. 3-tiered OAM topology consists of the following tiers:

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

OAM configuration is done on the NOAM.

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

Diameter protocol configuration is done on the SOAM.

Most DSR Application configuration is done on the SOAM.

As shown in *Figure 10: GUI Structure for 3-tiered DSR Topology with Policy DRA*, some configuration for P-DRA is done on the SOAM, and some is done on the NOAM.

- A set of MP servers, which can host signaling protocol stacks (for example, DA-MPs), or in-memory database servers (for example, Policy Session Binding Repository [SBR])

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

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

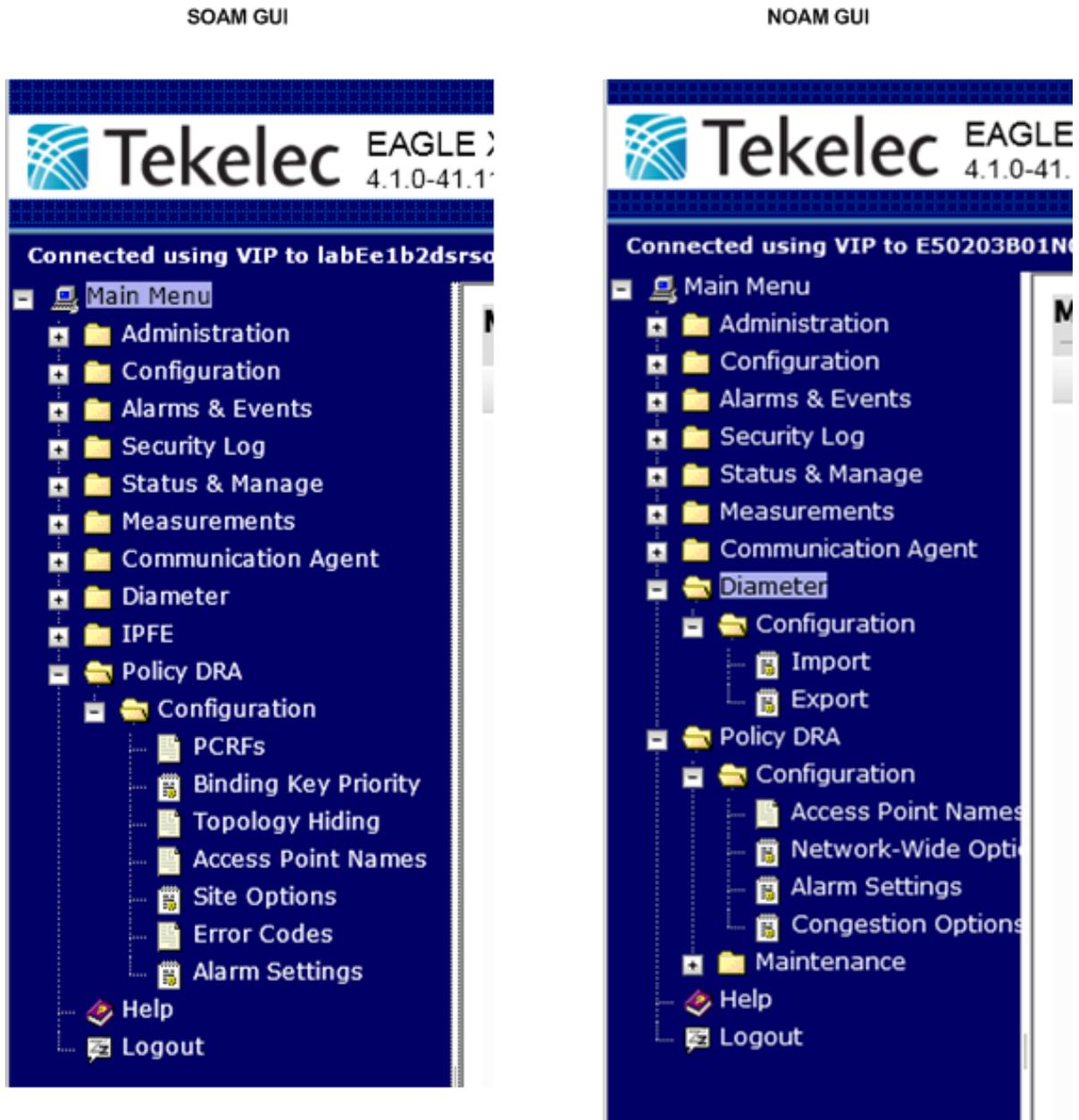


Figure 10: GUI Structure for 3-tiered DSR Topology with Policy DRA

**NOAM and SOAM Configuration**

Configuration data is divided into two categories:

- Network-wide data such as topology data, like creation of sites, assignment of servers to sites, and creation of server groups, is configured at the NOAM.
- Per-site data such as Diameter and DSR Application data is configured at the SOAM for a given site.

Some Policy DRA data must be configured at the NOAM, and some data must be configured at the SOAM.

P-DRA-specific data configured at the NOAM include:

- Assignment of Servers to Site places
- Assignment of Servers to Policy SBR Server Groups
- Assignment of Policy SBR Server Groups to Policy Session and/or Policy Binding Resource Domains
- Assignment of Sites to Policy DRA Mated Pair Place Associations
- Assignment of Sites to Policy DRA Binding Region Place Associations
- Configuration of Policy DRA Alarm Thresholds for:
  - Policy DRA Application Ingress Message Rate
  - Policy Session Database Capacity
  - Policy Binding Database Capacity
- Configuration of Access Point Names (APN)
- Configuration of Maximum Session Inactivity Time per APN
- Configuration of Policy DRA Congestion Options

Policy DRA-specific data configured at the SOAM include:

- PCRFs adjacent to the site
- Binding Key Priority for the site
- Topology Hiding configuration for the site
- Error response configuration for the site
- Mate Policy DRA Diameter Peer Name

The *Policy DRA User Guide* describes activities that are performed before and after the Policy DRA configuration is performed, including enabling the application, enabling connections, and verifying system and component status.

# Part IV

## Maintenance, Status, and Reports

---

### Topics:

- [Diameter Maintenance.....75](#)
- [Diameter Reports.....84](#)

### 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 11

## Diameter Maintenance

---

### Topics:

- *Introduction.....76*
- *Diameter Maintenance and Status Data for Components, DSR Applications, and DA-MPs.....77*
- *Managing the Status of Diameter Configuration Components.....79*

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

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 Configuration and Mediation User 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

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 1: Diameter Configuration Component Status Dependencies* summarizes the status dependencies of Diameter Configuration components.

**Table 1: 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 2: 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.

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 following Diameter GUI page:

- Main Menu: **Alarms & Events**

**Table 2: 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 **Route Groups Maintenance** page allows you to view the provisioned and available capacity for Route Groups and to view 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 **Peer Nodes Maintenance** page provides the Operational Status of Peer Node connections, including a Reason for the status.

### Connection Maintenance

The **Connections Maintenance** page allows you to view information about existing connections, including the Operational Status of each connection.

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

- Enable connections.
- Disable connections.
- View statistics for an SCTP connection.
- Run diagnostics on a test connection.

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

### *Connections SCTP Statistics*

The **Connections SCTP Statistics** page allows you to view statistics about paths within an SCTP connection.

Each line on the **Connections SCTP Statistics** page represents a path within an SCTP connection.

### Applications Maintenance

The **Applications Maintenance** page allows you to view status, state, and congestion information about activated DSR Applications. The data is refreshed every 10 seconds.

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

### Diameter DA-MPs Maintenance

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

On the **Diameter > Maintenance > DA-MPs** page, you can:

- Click the **Peer DA-MP Status** tab to view peer status information for the DA-MPs.
- Click the **DA-MP Connectivity** tab to view information about connections on the DA-MPs.
- Click the tab for an individual DA-MP to see 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 3: Maintenance and Status Data Sourcing Methods](#).

[Table 4: 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 3: Maintenance and Status Data Sourcing Methods**

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

**Table 4: 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

Diameter Configuration Component Name	Sourcing Method	Diameter GUI Screen ( starting from Main Menu : Diameter -> )
Route Group	Leader	Maintenance -> Route Lists <b>Note:</b> 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.

A Time of Last Update field is displayed on each Diameter Maintenance GUI page for each component, to indicate the last time that the status was updated for the component.

In a system with 2-tiered DSR topology, status data is merged for DA-MPs to the NOAM.

In a system with 3-tiered DSR topology, 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 the same configured connection is established simultaneously on two different DA-MPs, which could be reporting status on the same connection. This situation will be transient, as the Diameter Routing Function will detect the collision and take down one of the connections.

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

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

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

### Ownership of Diameter Connections

The DSR supports two types of connections:

- Fixed Connection

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

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

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

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

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

### Raising and Clearing Alarms

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

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

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

# Chapter 12

## Diameter Reports

---

### Topics:

- [Diameter Diagnostics Tool.....85](#)
- [Diameter MP Statistics \(SCTP\) Report.....85](#)

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 Configuration and Mediation User 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 Configuration and Mediation User Guide*, "Diameter", "Reports"
- **Help > Diameter > Reports > DSR Bulk Import > 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 Exports .....87*
- *IPsec.....93*
- *Diameter Intelligence Hub.....101*
- *Database Backups and Restores.....103*

### This part describes:

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

# Chapter 13

## Imports and Exports

---

### Topics:

- [DSR Bulk Import and Export Overview.....88](#)
- [Diameter Mediation Import and Export Overview.....90](#)

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 and DSR Application Configuration data
- Diameter Mediation Rule Template Export and Import

## DSR Bulk Import and Export Overview

### References:

- *Diameter Configuration and Mediation User Guide*, "Diameter Configuration", "DSR Bulk Import", "DSR Bulk Export"
- **Help > Diameter > Configuration > DSR Bulk Import > DSR Bulk Export**

The DSR DSR Bulk Import and Export functions export Diameter and DSR Application configuration data in CSV files to a location outside the system, and 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, P-DRA, or CPA and SBR DSR Applications; and the Diameter Configuration components).

### DSR Bulk Export

The DSR Bulk Export operation creates ASCII Comma-Separated Values (CSV) files (.csv) containing Diameter 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 can be periodically automatically exported on a defined schedule.

**Note:** Diameter Mediation configuration data cannot be exported with DSR Bulk Export; Mediation has its own Import and Export functions

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 or Diameter
- Exportable configuration data from a selected configuration component for the selected DSR Application or Diameter

When ALL is selected, the exported data for each configuration component appears in a separate .csv file.

Exported files can be written to the File Management Directory in the Status & Manage File Management area or to the Export Server Directory.

Files that are created by a DSR Bulk Export operation must be in the local File Management area before they can be used for Bulk Import operations on the local system.

For files that are exported to the local Export Server Directory,

- If a remote Export Server has been configured, the files in the local Export Server Directory are transferred to the configured remote Export Server location. The files in the local Export Server Directory are transferred to the configured remote Export Server location and are deleted from the local Export Server Directory. These transferred files do not appear in the File Management area on the local system, and cannot be used for Import operations on the local system.

- If a remote Export Server has not been configured, the files in the local Export Server Directory appear in the list on the **Status & Manage Tasks Active Tasks** page and in the File Management area list on the local system. These files can be used for Import operations on the local system.

The result of each Bulk Export operation is logged into a file with the same name as the exported file, but with extension .log. The log file appears in the File Management area. The log file contains the names of the selected configuration data components, the number of records exported for each configuration component, and either the first error or all errors that occurred during the Export operation.

### 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 Diameter Configuration or DSR Applications (FABR, RBAR, P-DRA, and CPA/SBR ) Configuration data in the system.

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.

**Note:** Diameter Mediation configuration data cannot be imported with DSR Bulk Import operations; Mediation has its own Import and Export functions.

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.

For files that are exported to the Export Server Directory,

- If a remote Export Server has been configured, the files in the Export Server Directory are automatically transferred to the configured remote Export Server and are deleted from the Export Server Directory.
- If a remote Export Server has not been configured, the files in the Export Server Directory appear in the list on the **Status & Manage Tasks Active Tasks** page, and also appear in the list on the local system **Status & Manage Files** page.

For files that are exported to the File Management Directory,

- The files appear in the File Management area list on the local system **Status & Manage Files** page and in the list on the **Diameter Configuration Import** page.
- The files can be downloaded, edited, uploaded, and used for Import operations.
- Import CSV files must be in the File Management area of the local system before they can be used for Import operations on the local system.
- The **Download** function on the **Status & Manage Files** page can be used to download the files to a location off of the local system for editing or transfer to another system.
- The **Upload** function on the **Status & Manage Files** page can be used to upload the files to the File Management area of the local system.

For files that are created manually using a text editor on a computer,

- Import CSV files that are located off of the local system 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 **Upload** function on the **Status & Manage Files** page can be used to upload the files to the File Management area of the local system.

Files that were created using the DSR Bulk Export operation and are transferred to another system for importing configuration data on that other system may not need to be edited.

Files can be created manually so that they contain only the configuration data that is needed for the desired Import operation. The files can be edited later for use with a different Import operation.

The following Import operations can be performed:

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

Each Import operation creates a log file and, if errors occur, a failures file that appear in the File Management area. Failures files can be downloaded, edited to correct the errors, and imported to successfully process the records that failed.

## Diameter Mediation Import and Export Overview

### References:

- *Diameter Configuration and Mediation User 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 the file selected for importing must be compatible with the DSR release into which the file is imported.

If an imported Rule Template references another Rule Template 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).

### Mediation Rule Template Export

The DSR Bulk Export operation creates ASCII Comma-Separated Values (CSV) files (.csv) containing Diameter 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 can be periodically automatically exported on a defined schedule.

**Note:** Diameter Mediation configuration data cannot be exported with DSR Bulk Export; Mediation has its own Import and Export functions

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 or Diameter

- Exportable configuration data from a selected configuration component for the selected DSR Application or Diameter

When ALL is selected, the exported data for each configuration component appears in a separate .csv file.

Exported files can be written to the File Management Directory in the Status & Manage File Management area or to the Export Server Directory.

Files that are created by a DSR Bulk Export operation must be in the local File Management area before they can be used for Bulk Import operations on the local system.

For files that are exported to the local Export Server Directory,

- If a remote Export Server has been configured, the files in the local Export Server Directory are transferred to the configured remote Export Server location. The files in the local Export Server Directory are transferred to the configured remote Export Server location and are deleted from the local Export Server Directory. These transferred files do not appear in the File Management area on the local system, and cannot be used for Import operations on the local system.
- If a remote Export Server has not been configured, the files in the local Export Server Directory appear in the list on the **Status & Manage Tasks Active Tasks** page and in the File Management area list on the local system. These files can be used for Import operations on the local system.

The result of each Bulk Export operation is logged into a file with the same name as the exported file, but with extension .log. The log file appears in the File Management area. The log file contains the names of the selected configuration data components, the number of records exported for each configuration component, and either the first error or all errors that occurred during the Export operation.

### Mediation Rule Template 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 Diameter Configuration or DSR Applications (FABR, RBAR, P-DRA, and CPA/SBR ) Configuration data in the system.

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.

**Note:** Diameter Mediation configuration data cannot be imported with DSR Bulk Import operations; Mediation has its own Import and Export functions.

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.

For files that are exported to the Export Server Directory,

- If a remote Export Server has been configured, the files in the Export Server Directory are automatically transferred to the configured remote Export Server and are deleted from the Export Server Directory.
- If a remote Export Server has not been configured, the files in the Export Server Directory appear in the list on the **Status & Manage Tasks Active Tasks** page, and also appear in the list on the local system **Status & Manage Files** page.

For files that are exported to the File Management Directory,

- The files appear in the File Management area list on the local system **Status & Manage Files** page and in the list on the **Diameter Configuration Import** page.
- The files can be downloaded, edited, uploaded, and used for Import operations.
- Import CSV files must be in the File Management area of the local system before they can be used for Import operations on the local system.
- The **Download** function on the **Status & Manage Files** page can be used to download the files to a location off of the local system for editing or transfer to another system.
- The **Upload** function on the **Status & Manage Files** page can be used to upload the files to the File Management area of the local system.

For files that are created manually using a text editor on a computer,

- Import CSV files that are located off of the local system 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 **Upload** function on the **Status & Manage Files** page can be used to upload the files to the File Management area of the local system.

Files that were created using the DSR Bulk Export operation and are transferred to another system for importing configuration data on that other system may not need to be edited.

Files can be created manually so that they contain only the configuration data that is needed for the desired Import operation. The files can be edited later for use with a different Import operation.

The following Import operations can be performed:

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

Each Import operation creates a log file and, if errors occur, a failures file that appear in the File Management area. Failures files can be downloaded, edited to correct the errors, and imported to successfully process the records that failed.

# Chapter 14

## IPsec

---

### Topics:

- [IPsec Overview.....94](#)
- [IPsec IKE and ESP elements.....96](#)
- [Accessing platcfg.....97](#)
- [Adding an IPsec connection.....98](#)
- [Editing an IPsec connection.....98](#)
- [Enabling and Disabling an IPsec Connection.....99](#)
- [Deleting an IPsec connection.....100](#)
- [Logging out of platcfg.....100](#)

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 `placfg`. See [Accessing placfg](#).
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 5: IPsec IKE and ESP elements](#) describes IPsec IKE and ESP configuration elements and provides default values, if applicable.

**Table 5: 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. <b>Note:</b> 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. Tekelec recommends setting the lifetime to the lowest possible time that	Number of time units	60

Description	Valid Values	Default
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 Tekelec Platform Configuration Utility, platcfg. Platcfg provides a user interface to the Tekelec Platform Distribution (TPD), the core platform underlying the DSR.

**Note:** You will need the Tekelec platcfg password to access platcfg. Contact Tekelec 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 platdfig.  
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 platdfig.  
See *Logging out of platcfg*.

## Deleting an IPsec connection

Use this task to delete an IPsec connection.

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

## Logging out of platcfg

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

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

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

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

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

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

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

# Chapter 15

## Diameter Intelligence Hub

---

### Topics:

- [Diameter Intelligence Hub Overview.....102](#)
- [Accessing DIH.....102](#)

The Diameter Intelligence Hub (DIH) provides the ability to troubleshoot Diameter transactions. The DIH can also be used to filter and access these transactions from external servers.

### Diameter Intelligence Hub Overview

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

### Accessing DIH

To access and log into DIH:

1. Using a Web browser, type the following URL into the Address bar:

`http://nspserver_IPAddress/nsp`

**Note:** Contact your system administrator to find out the IP address for the NSP portal.

The login screen opens.

2. To log into NSP, enter the following:
  - a) **User name**
  - b) **Password**

**Note:** You must have a username and password assigned to you by your system administrator.

3. Click **Login**.

The NSP Application Board opens and you are logged into DIH.

# Chapter 16

## Database Backups and Restores

---

### Topics:

- [Database Backups and Restores.....104](#)

The database contains the provisioning and configuration information for a DSR deployment.

The ability to restore a DSR database from a database backup file can aid in disaster recovery. Tekelec 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.

### Database Backups and Restores

The database contains the provisioning and configuration information for a DSR deployment.

The ability to restore a DSR database from a database backup file can aid in disaster recovery. Tekelec 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 and Provisioning data. Data is safely collected from the database management system without impact to database users.

- Configuration Data is data used to configure a system and the applications that run in the system.
- Provisioning Data is subscriber data for a system that can be provisioned through a bulk interface or a GUI.

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

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.ProvisioningAndConfiguration.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 and Provisioning data on Active Network OAM&P servers. By default, automatic backups for Configuration data are scheduled for 2:45 AM, while backups for Provisioning data are scheduled for 3:15 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 provisioning data, configuration data, or both.

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, check the **Provisioning** box, the **Configuration** box, or both boxes for the desired data to be backed up.

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; Provisioning and 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. Tekelec 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 and Provisioning 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 Tekelec [Customer Care Center](#) for assistance before attempting a database restore.

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

# Glossary

## A

APN	<p>Access Point Name</p> <p>The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.</p>
Application Routing Rule	<p>A set of conditions that control message routing to a DSR application based on message content.</p>
AVP	<p>Attribute-Value Pair</p> <p>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.</p>

## C

CEX Configuration Set	<p>A mechanism for assigning Application IDs and supported Vendor IDs to a Local Node or to a Connection.</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 application such as CPA can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.</p>
-------	---

## D

DAS	Diameter Application Server Diameter Agent Server
Diameter	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 is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.
DIH	Diameter Intelligence Hub  A troubleshooting solution for LTE, IMS, and 3G Diameter traffic processed by the DSR. DIH does not require separate probes or taps.
DSR	Diameter Signaling Router  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.
DSR Application	Any DSR software feature or function that is developed as a user of the Diameter base protocol.

## E

EMS	Element Management System
-----	---------------------------

**E**

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

**F**

FQDN

Fully qualified domain name

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

**G**

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.

**I**

IMI

Internal Management Interface

IP

Internet Protocol

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.

IPFE

IP Front End

A traffic distributor that routes TCP traffic sent to a target set address by

**I**

application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.

IPsec

Internet Protocol Security

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

IPv4

Internet Protocol version 4

IPv6

Internet Protocol version 6

**M**

MEAL

Measurements, Events, Alarms,  
and Logs

**N**

NE

Network Element

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

NMS

Network Management System

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

## N

NSP  
 Network Services Part  
 The lower layers of the SS7 protocol, comprised of the three levels of the Message Transfer Part (MTP) plus the signaling Connection Control Part (SCCP), are known collectively as the Network Services Part (NSP).

## O

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

OAM&P  
 Operations – Monitoring the environment, detecting and determining faults, and alerting administrators.  
 Administration – Typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning, using usage data, and maintaining system reliability.  
 Maintenance – Provides such functions as upgrades, fixes, new feature enablement, backup and restore tasks, and monitoring media health (for example, diagnostics).  
 Provisioning – Setting up user accounts, devices, and services.

## P

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

## S

SBR  
 For DSR, Session Binding Repository

## S

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

## SCTP

Stream Control Transmission Protocol

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

The transport layer for all standard IETF-SIGTRAN protocols.

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

## SNMP

Simple Network Management Protocol.

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

## T

## 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.

**T**

TPD

Tekelec Platform Distribution

TPD is a standard Linux-based operating system packaged and distributed by Tekelec. TPD provides value-added features for managing installations and upgrades, diagnostics, integration of 3rd party software (open and closed source), build tools, and server management tools.

**U**

URL

Uniform Resource Locator

**V**

VIP

Virtual IP Address

Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.

**X**

XMI

External Management Interface