EAGLE® XG Diameter Signaling Router

Diameter Configuration, Maintenance, and DSR Applications Guide

910-6573-001 Revision B
December 2012

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter contains a brief description of the Diameter protocol and the features that use it. The contents include sections about the manual scope, audience, and organization; how to find related publications; and how to contact Tekelec for assistance.

Purpose of this document

This document provides administrative information for the EAGLE XG DSR, including:

- A functional description of the product
- Diameter configuration information
- Database backup and restore information

Scope and Audience

This manual is intended for anyone responsible for configuring and using the Diameter Signaling Router (DSR) and the applications that use it. Users of this manual must have a working knowledge of telecommunications and network installations.

Manual Organization

This document is organized into the following chapters:

- *Introduction* contains general information about the DSR documentation, the organization of this manual, and how to get technical assistance.
- *Diameter Signaling Router (DSR)* describes the DSR topology, architecture, components, and functions.
- *Diameter Configuration* describes Diameter protocol configuration.
- *Diameter Mediation* describes Diameter Mediation functions and configuration.
- *Diameter Maintenance* describes Diameter Maintenance functions and configuration.
- *Diameter Reports* describes the Diagnostics Tool and report, and the MP Statistics (SCTP) report.
- *Full Address Based Resolution (FABR)* describes the Full Address Based Resolution (FABR) DSR Application functions and configuration.
- *Range Based Address Resolution (RBAR)* describes the Range Based Address Resolution DSR Application functions and configuration.
- *Charging Proxy Application* describes the Charging Proxy Application (CPA) functions and configuration.
- *IP Front End (IPFE)* describes the IPFE functions and configuration.
- *IPsec* describes the function 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.
- *DSR Configuration Elements* contains tables that describe the configuration components and elements for Diameter and DSR Applications.

Documentation Admonishments

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

Table 1: Admonishments

	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.)

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:

  USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

  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:

    +91 124 436 8552 or +91 124 436 8553

    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.

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.

Chapter 2

Diameter Signaling Router (DSR)

Topics:

The 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 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

  For step-by-step instructions on how to configure the DSR network, see document 909-2228-001, *DSR 4.0 HP C-Class Installation*, or contact your Tekelec Support Representative.
- Routing configuration
- Transport configuration for connection management

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 what level (DSR NOAM or DSR SOAM).

The architecture includes the following characteristics:

- The DSR supports a 2-tiered or 3-tiered localized topology.
- 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. The 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 provides 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) and DSR Application data (RBAR, FABR, and CPA)

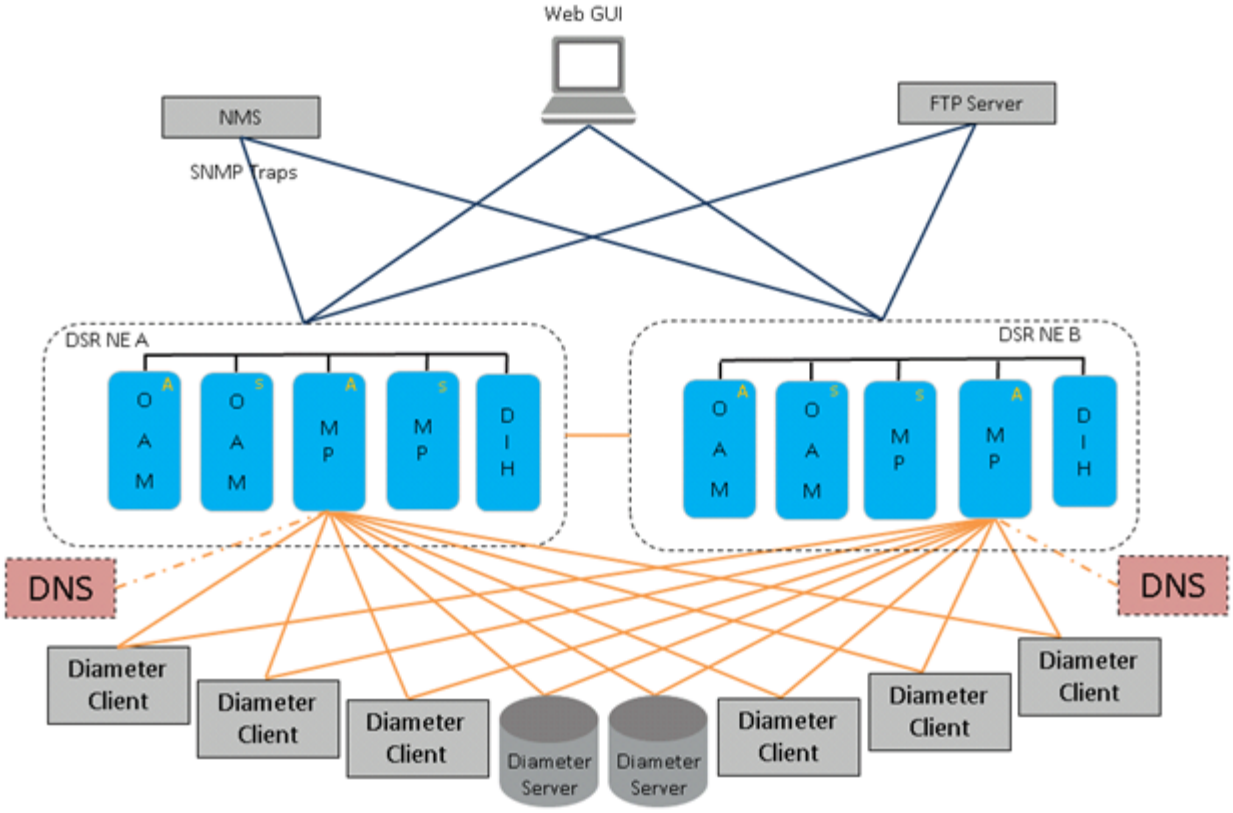

Figure 1: EAGLE XG DSR System Diagram with 2-tiered Topology

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)
- On a DSR SOAM, Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists) and DSR Application data (RBAR, FABR, and CPA)

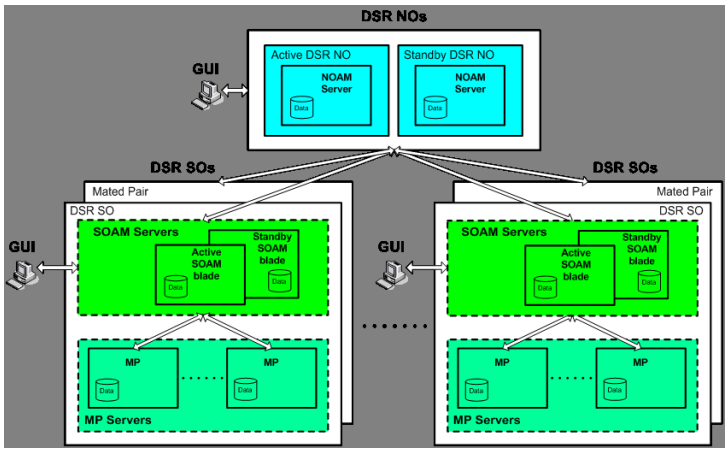

Figure 2: EAGLE XG DSR Diagram with 3-tiered Topology

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.

A pair of Operation, Administration, and Maintenance (OAM) servers make up one OAM&P 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&P Architecture illustrates the DSR OAM&P architecture.

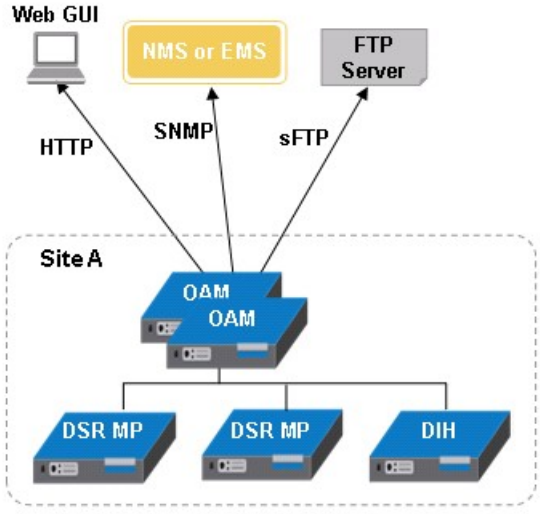

Figure 3: EAGLE XG DSR OAM&P Architecture

Message Processors

The role of the Message Processors (DA-MPs) is to provide the Diameter application messaging interfaces and processing. All Message Processors replicate configuration and provisioning 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. Specifically, the DIH provides:

- 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 diagnostic utility
- Data feed that can be used to schedule automatic export of trace data to a customer server.
- Filtering on xDR content
- A web-based GUI providing security, configuration, and application access

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 balance traffic over connections.
- 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/to Diameter Peers and the Diameter Routing Function.

- Diameter Routing Function:
  - Routing of Diameter Request and Answer messages to and from Diameter Peers (through the Diameter Transport Function) and DSR Applications.
    - Peer Routing Rules: The DSR provides the ability to configure Peer Routing Rules that define where to route a Diameter message to an upstream Peer based upon Diameter message content.
    - Processing of Diameter connection status from the Diameter Transport Function and status from DSR Applications for maintaining dynamic routing configuration data.
    - Message Rerouting: A Diameter Relay Agent is responsible for making sure that Request messages are successfully delivered and to alternate route if failures are encountered.
      - Alternate Implicit Routing: Instead of a message being routed directly to an available Peer Node, the message is routed on an "alternate implicit route" that is chosen firom 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 Control: Performing connection capacity status and control, ingress message MPS control, and egress message throttling; providing Local Congestion and Egress Transport Congestion status.
- Diameter Medation: 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.

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 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.
  - SCTP multi-homing connections

  - TCP connections
- Processing Diameter Peer-to-Peer messages and related functions
- 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.
- Diameter Watchdog (DWR/DWA) to detect Diameter transport failures
- Disconnect Peer (DPR/DPA)
- 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 MEAL data for transport configuration objects
- Performing transport capacity control
- Per Connection Ingress MPS Control, Per Connection Egress Message Throttling, and Egress Transport Congestion

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 amongst peers/connections with the same priority. A set of Peer Nodes and Diameter connections within a Route List of equal priority is a Route Group.
- Message routing to Peer Nodes with multiple Diameter connections
- Mesage 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 initated by the DSR Charging Proxy Application.

- Message rerouting on failures

  Rerouting is attempting 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 firom 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 objects SCTP uni-homing connections

Chapter 3

Diameter Configuration

Topics:

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

Diameter Configuration Overview

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 is done on the NOAM, Diameter and DSR Application configuration is done on the SOAM, and some common utilities can be accessed on either OAM.

The DSR requires configuration for Diameter routing and transport functions.

Configuration in 2-tiered and 3-tiered DSR Topology

The split of the 2-tiered DSR topology NOAM server into a 3-tiered DSR topology NOAMP server and a 3-tiered DSR topology SOAM server results in a change in 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 for managing A-sourced data. A-sourced data is Platform and topology data.
- The DSR SOAM hosts a GUI for managing B-sourced data. B-sourced data is DSR data.

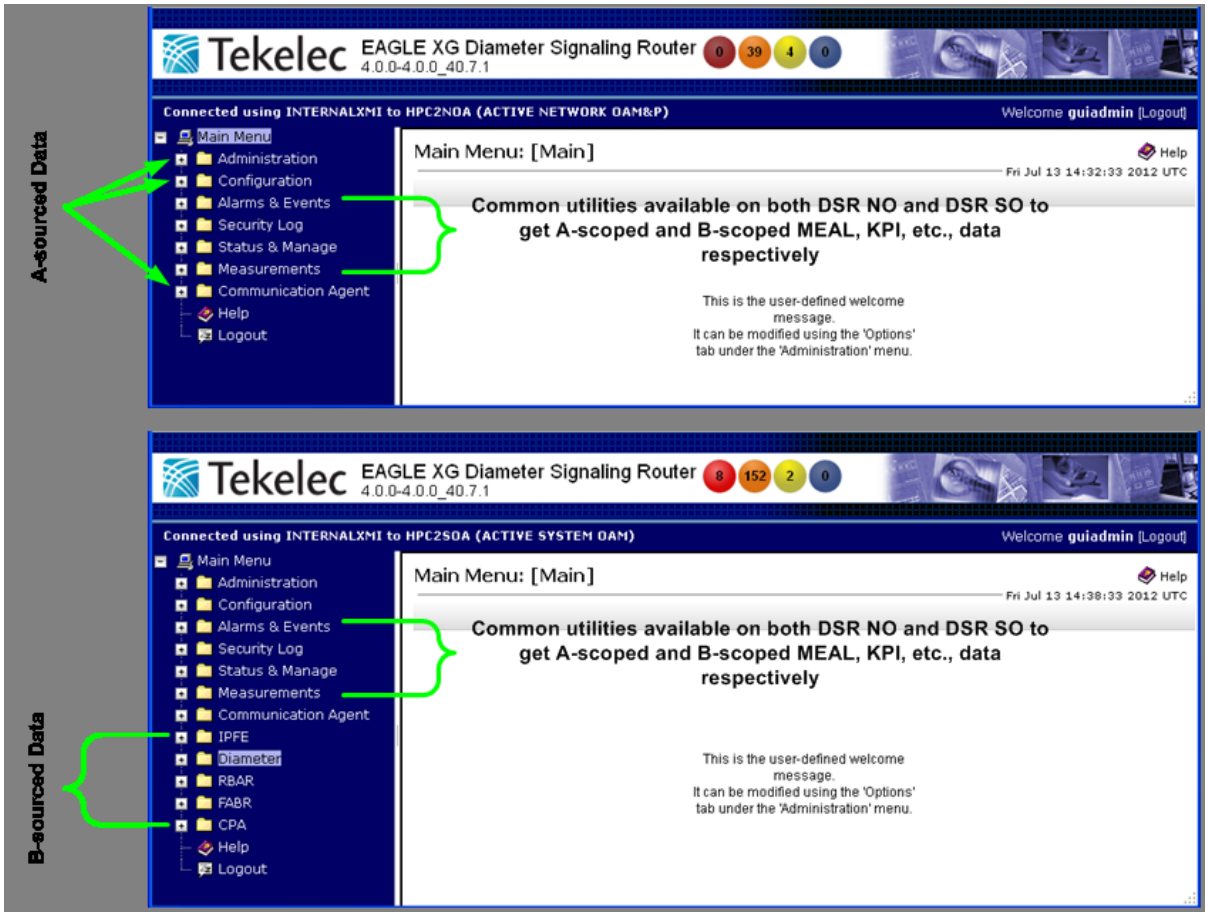

Figure 4: GUI Structure for 3-tiered DSR Topology Configuration

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.

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

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

The Diameter signaling MEAL data and DSR Application MEAL data that is generated by all MP servers and merged to SOAM servers is 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

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 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 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.

Transport Configuration

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

Diameter Configuration Sequence

The **Diameter > Configuration** GUI pages allow you to manage Diameter configuration.

Before using the **Diameter Configuration** pages, the following activities need to be completed:

- Configure the network topology. This includes network elements, servers, server groups, and network devices and routes.
- Assign IP addresses to the server groups.

  Note: For information about configuring the DSR network topology, see the Diameter online help.

Diameter configuration in a 2-tiered system is performed on the NOAM.

Diameter configuration in a 3-tiered system is performed on the SOAM.

Because some components use other configured components, Diameter configuration needs to occur in the following order:

1. Configure DA-MPs Profile Assignments.
2. Configure Peer Route Tables.

   Configure only Table Names here. Peer Routing Rules will be configured after Route Lists are configured.
3. Configure Routing Option Sets.
4. Configure Pending Answer Timers.

   A default Pending Answer Timer is provided.

   Configure one or more additional Pending Answer Timers if they are needed to invoke Implicit Routing, Alternate Implicit Routing, or Reroute on Answer.

5. Configure Application Ids.

   Can associate Peer Route Tables, Routing Option Sets, and Pending Answer Timers if used.
6. Configure Command Codes.
7. Configure CEX Parameters.
8. Configure CEX Configuration Sets.
9. Configure Connection Configuration Sets.

   The default configuration set can be modified to match the SCTP, Diameter, and TCP options that apply to your network.

   Configure any additional Connection Configuration Sets, if necessary.
10. Configure Local Nodes.
11. Configure Peer Nodes.
12. Configure Capacity Configuration Sets, if they will be used.
13. Configure Egress Message Throttling Configuration Sets.
14. Configure Message Priority Configuration Sets.
15. Configure Connections.
16. Configure Route Groups.
17. Configure Route Lists.
18. If Alternate Implicit Routing will be used, edit each Peer Node and select the Route List that will be used for the Alternate Implicit Route.
19. Edit each Peer Route Table, and enter each Peer Routing Rule that will be used in that Peer Route Table.
20. Configure Reroute On Answer.
21. Configure Application Routing Rules.
22. If necessary, change the default System Options and DNS Options, and view Local Congestion.

Configuration Capacity Summary

The Diameter ConfigurationCapacity 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:

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

Use the Capacity Summary 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 DA-MP.

An MP Profile defines maximum and threshold values for a DA-MP running the relay application, a database application, or a session application. You must assign an MP Profile to each DA-MP in your DSR configuration.

The following MP Profile types are available:

- G6:Relay - G6 DA-MP half height blade running the relay application
- G8:Relay - G8 DA-MP half height blade running the relay application
- G7:Relay - G7 DA-MP full height blade running the relay application
- G6:Database - G6 DA-MP half height blade running a database application
- G8:Database - G8 DA-MP half height blade running a database application
- G7:Database - G7 DA-MP full height blade running a database application
- G6:Session - G6 DA-MP half height blade running a session application
- G8:Session - G8 DA-MP half height blade running a session application
- G7:Session - G7 DA-MP full height blade running a session application

Table 2: MP Profile Elements describes the values that are set in an MP Profile.

Table 2: MP Profile Elements

Field	Description
Maximum Connections	The maximum number of Diameter connections the DA-MP can have configured at any one time
Engineered Ingress MPS	The maximum ingress message rate, in messages per second, that the DA-MP will support without overload. This value limits the total Reserved Ingress MPS of all Diameter Connections assigned to the DA-MP.
Maximum Ingress Message Rate Minor Alarm Set Threshold	The ingress message rate, in messages per second, above which a minor alarm is raised.
Maximum Ingress Message Rate Minor Alarm Clear Threshold	The ingress message rate, in messages per second, below which a minor alarm is cleared.
Maximum Ingress Message Rate Major Alarm Set Threshold	The ingress message rate, in messages per second, above which a major alarm is raised.
Maximum Ingress Message Rate Major Alarm Clear Threshold	The ingress message rate, in messages per second, below which a major alarm is cleared.

Field	Description
Maximum Ingress Message Rate Critical Alarm Set Threshold	The ingress message rate, in messages per second, above which a critical alarm is raised.
Maximum Ingress Message Rate Critical Alarm Clear Threshold	The ingress message rate, in messages per second, below which a critical alarm is cleared.
Routing Message Rate Minor Alarm Set Threshold	The Diameter message processing rate, in messages per second, above which a minor alarm is raised.
Routing Message Rate Minor Alarm Clear Threshold	The Diameter message processing rate, in messages per second, below which a minor alarm is cleared.
Routing Message Rate Major Alarm Set Threshold	The Diameter message processing rate, in messages per second, above which a major alarm is raised.
Routing Message Rate Major Alarm Clear Threshold	The Diameter message processing rate, in messages per second, below which a major alarm is cleared.
Routing Message Rate Critical Alarm Set Threshold	The Diameter message processing rate, in messages per second, above which a critical alarm is raised.
Routing Message Rate Critical Alarm Clear Threshold	The Diameter message processing rate, in messages per second, below which a critical alarm is cleared.

Application Ids Configuration

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

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

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

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

The GUI field descriptions, formats, ranges, and any default values are listed in *Application Ids elements*.

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.

GUI field descriptions, valid values and ranges, and any default values are listed in *CEX Parameters elements*.

Command Codes Configuration

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

GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Command Codes elements*.

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.

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.

GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Connection Configuration Set elements*.

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 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.

GUI field descriptions, formats, valid values and ranges, and any default values are listed in *CEX Configuration Set elements*.

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.

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *CEX Parameters elements*.

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.

GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Capacity Configuration Set elements*.

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.

The Message Priority Configuration Set fields are described in *Message Priority Configuration Set elements*.

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.

The options are described in *Egress Message Throttling Configuration Set elements*.

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.

Local Node Configuration

The Local Node identifies:

- Domain information
- SCTP Listen Port Number
- TCP Listen Port Number
- The supported transport type(s)
- A list of IP addresses available for establishing Diameter transport connections

The following attributes are mandatory for a Local Node:

- A unique FQDN
- The realm of the Local Node
- The IP signaling address set
- One or more transport protocol or protocol/listen port combinations
- A Connection Configuration Set for Response connections
- A CEX Configuration Set for the Local Node that is used if the CEX Configuration Set is not associated with the connection

GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Local Node configuration elements*.

After it is configured, a Local Node can be assigned to connections for use in Diameter routing.

Peer Nodes

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

Load Sharing: Peer Nodes

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

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

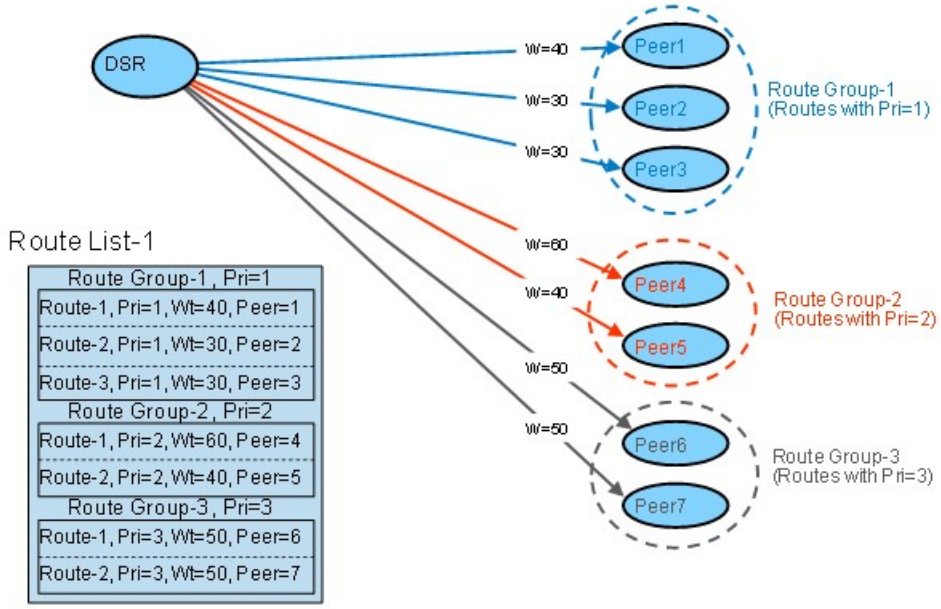

Figure 5: Weighted Load Sharing

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.

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Connection configuration elements*.

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.

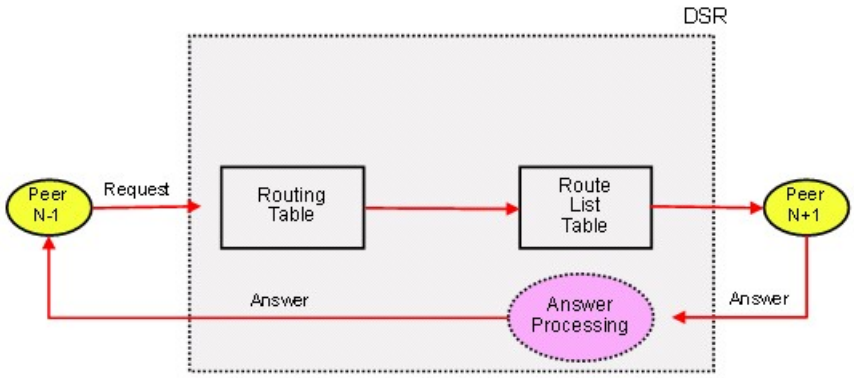

Figure 6: DSR Routing Diagram

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.

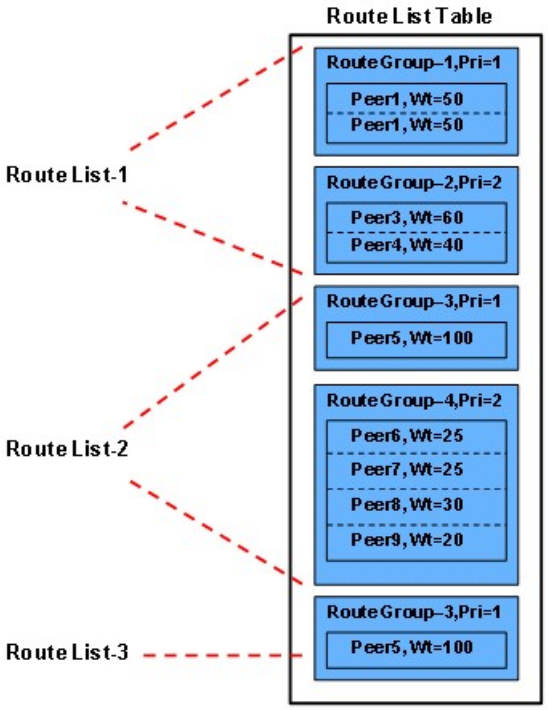

Figure 7: Route List, Route Group, and Peer Node Relationships

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.

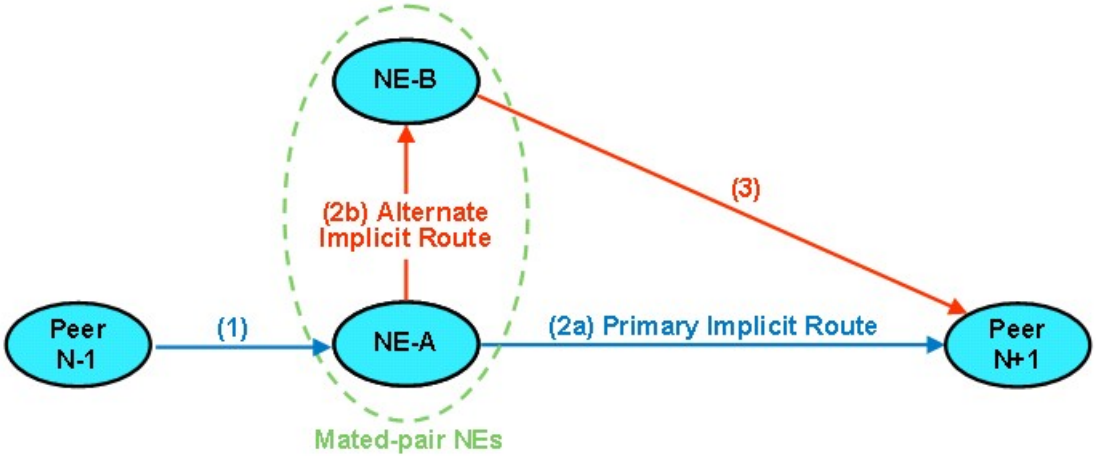

Figure 9: DSR Implicit Routing

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*.

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Route Group configuration elements*.

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.

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Route List configuration elements*.

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.

On the **Diameter > Configuration > Routing Option Sets** page, you can perform the following actions:

- Filter the list of Routing Option Sets to display only the desired Routing Option Sets.
- Sort the list by a column in ascending or descending order, by clicking the column heading. The default order is by Routing Option Set Name in ascending ASCII order.
- Click Insert.

  The **Diameter > Configuration > Routing Option Sets [Insert]** page appears. You can add a new Routing Option Set.

  The **Diameter > Configuration > Routing Option Sets [Insert]** page will not open if

  - The maximum number of Routing Option Sets (20) already exists in the system

- Select a Routing Option Set in the list, and click Edit.

  The **Diameter > Configuration > Routing Option Sets [Edit]** page appears. You can edit the selected Routing Option Set.

  If the selected Routing Option Set has been deleted by another user, the **Diameter > Configuration > Routing Option Sets [Edit]** page will not open.

- Select a Routing Options Set in the list, and click Delete. You can delete the selected Routing Option Set. You cannot delete the Default Routing Option Set.

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.

On the **Diameter > Configuration > Peer Route Tables** page, you can perform the following actions:

- Filter the list of Peer Route Tables to display only the desired Peer Route Tables.
- Sort the list by a column in ascending or descending order, by clicking the column heading. The default order is by Peer Route Table Name in ascending ASCII order.
- Click Insert.

  The **Diameter > Configuration > Peer Route Tables [Insert]** page appears. You can add a new Peer Route Table.

  The **Diameter > Configuration > Peer Route Tables [Insert]** page will not open if

  - The maximum number of Peer Route Tables (100) already exists in the system.

- Select a Peer Route Table in the list, and click Edit.

The **Diameter > Configuration > Peer Route Tables [Edit]** page appears. You can edit the selected Peer Route Table.

If the selected Peer Route Table has been deleted by another user, the **Diameter > Configuration > Peer Route Tables [Edit]** page will not open.

- Select a Peer Route Table in the list, and click Delete. You can delete the selected Peer Route Table.

Peer Routing Rule 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. There are six Peer Routing Rule parameters in the conditions:

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

When a Diameter message matches the conditions of a Peer Routing Rule then the action specified for the rule will occur. For Route to Peer, the Diameter 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 Send Answer, 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.

The GUI field descriptions, formats, ranges, and any default values are listed in *Peer Routing Rule configuration elements*.

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

The GUI field descriptions, formats, ranges, and any default values are listed in *Pending Answer Timers elements*.

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.)

The GUI field descriptions, formats, ranges, and any default values are listed in *Application Routing Rule configuration elements*.

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).

The System Options are described in *System Options elements*.

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.

The DNS Options fields are described in *DNS Options elements*.

Local Congestion configuration

The **Diameter Configuration Local Congestion** page allows you to view the Local Congestion settings. This page is read-only.

To open the **Diameter Configuration Local Congestion** page, select Diameter > Configuration > Local Congestion.

The Local Congestion variables are described in *Local Congestion elements*.

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, and CPA/SBR) Configuration data in the system.

Import CSV Files

Import CSV files can be created by using a DSR Bulk Export operation, or can be manually created using a text editor. The CSV file formats are described in *Bulk Import and Export CSV File Formats and Contents*.

CAUTION: The format of each Import CSV file record must be compatible with the configuration data in the current DSR release in the system.

- Configuration data refers to any data that is configured for one of the Export Application types (FABR, RBAR, CPA, and SBR DSR Applications; and the Diameter Configuration components).
- For the "Diameter" Export Application type, configuration data refers to any data that is configured using the GUI pages that are available from the Diameter Configuration menu folder.

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

- Each file can contain one or more records of the same format (for one configuration component, such as records for several Diameter Configuration Connections); the entire format for each record must be contained in one line of the file.

Files that are created using the DSR Bulk Export operation can be exported either to the 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 (see the **Administration Export Server** page), the files in the Export Server Directory are automatically transferred to the configured remote Export Server and are deleted from the Export Server Directory. The transferred files do not appear in the list on the local system **Status & Manage Files** page or in the list on the **Diameter Configuration Import** page.
- 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.

Import Operations

CAUTION: Bulk Import can degrade the performance of the DA MP and should be performed only in the maintenance window.

The CSV files that are used for Import operations must be in the local File Management area. The **Diameter Configuration Import** page lists all files in the File Management area (on the **Status & Manage Files** page) that have the .csv file extension.

The File Management button on the **Diameter Configuration Import** page opens the **Status & Manage Files** page.

The following Import operations can be performed:

Note: The Application Type, Keyword, and Key fields in each file record are used to identify the configuration data entry in the system.

- Insert new configuration data into the system

Only data records that do not currently exist in the system are inserted. Any records in the file that do already exist in the system are treated and logged as failures.

- Update existing configuration data in the system

  Only data records that currently exist in the system can be updated. Any records in the file that do not already exist in the system, and any records that already exist in the system but are not updated in the file, are treated and logged as failures.

- Delete existing configuration data from the system

  Only data records that currently exist in the system can be deleted. Any records in the file that do not exist in the system, and any records that exist in the system but are not changed in the file, are treated and logged as failures.

For the Import operation on each record in a file to be successful with no errors logged for the operation, each record must be valid for the configuration data format and for the Import operation that is being performed.

- Exported configuration data probably needs to be edited before the exported file is used for an Import operation on the same system.

  Insert operations - Records need to be added or edited to be able to insert new configuration data entries (such as connections or Route Lists). It is best to remove from the file any records for existing configuration data entries; they will be flagged as errors for an Insert operation. It might be difficult to distinguish between logged errors for existing data and for the records for the new entries.

  Update operations – Records need to be edited to change element values in existing configuration data entries. The Application Type, Keyword, and Key fields are NOT changed in the records, so that the entries can be identified as existing in the system. It is best to remove from the file any records for existing configuration data entries that are NOT being updated; they will be flagged as errors for an Insert operation. It might be difficult to distinguish between logged errors for existing records that are not updated and for the updated records.

  Delete operations – Using an exported file without editing it will remove from the system all of the configuration data entries in the exported records. If you do not want to delete all of the configuration data entries that are in the file records, edit the file and remove the records for the entries that are NOT to be deleted. Records for configuration data entries that do not exist in the system will be flagged as errors for a Delete operation. For example, if you want to delete 20 of 100 configured connections, edit the file and remove the records for the 80 connections that you do not want to delete.

- 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. Exceptions might be system-specific information such as IP addresses and DA-MP profiles.
- Manually created files can be created 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.

  Manually created CSV files are not required to contain a comment header. If a comment header is included in the file, it must be formatted using pound signs (#), as shown in the Export file header that is described in Export Results.

Not all of the Import operations are valid for all types of configuration data. *Table 3: Valid Import Operations* indicates the valid operations for the listed types of configuration data.

Table 3: Valid Import Operations

Configuration Data	Insert	Update	Delete
Diameter			
Application Ids	X		X
CEX Parameters	X	X	X
Command Codes	X	X	X
Connection Configuration Sets	X	X	X
CEX Configuration Sets	X	X	X
Capacity Configuration Sets	X	X	X
Egress Message Throttling Configuration Sets	X	X	X
Message Priority Configuration Sets	X	X	X
Local Nodes	X	X	X
Peer Nodes	X	X	X
Connections	X	X	X
Route Groups	X	X	X
Route Lists	X	X	X
Peer Route Tables	X	X	X
Peer Routing Rules	X	X	X
Reroute on Answer	X		X
Application Routing Rules	X	X	X
Routing Option Sets	X	X	X
Pending Answer Timers	X	X	X
System Options		X	
DNS Options		X	
Rbar			
Applications	X	X	X
Exceptions		X	
Destinations	X	X	X
Address Tables	X	X	X
Addresses	X	X	X
Address Resolution	X	X	X

Configuration Data	Insert	Update	Delete
System Options		X	
Fabr			
Applications	X	X	X
Exceptions		X	
Default Destinations	X	X	X
Address Resolution	X	X	X
System Options		X	
Cpa			
System Options		X	
Message Copy		X	
Sbr			
SBR		X	
SBR Subresource Mapping	Cannot be imported or exported		

Import Operation Results

Each Import operation creates one or two files that appear in the File Management area:

- A log file that has the same name as the Import file, but with the .log extension

  For example, ImportExportStatus/<import file name>.log

  The Bulk Import operation can be configured with the Abort On First Error check box to:

  - Log the error for each record that failed during the operation, and continue the Import operation.
  - Log the error for just the first record that failed, and end the Import operation.

  Information for records that succeed is not included in the log. The log file contains the Action (Import operation) that was performed; and the number of Successful Operations (records), Failed Operations (records), and Total Operations (records).

- A Failures file, if failures occurred during the Import operation

  The file is a .csv with the same name as the Import file, but contains _Failures in the file name.

  For example, if the Import file name is October_2_SO_DSR1_Diameter_CmdCodes.csv, the Failures file is named October_2_SO_ DSR1_Diameter_CmdCodes_Failures.csv

  A Failures file can be downloaded from the local File Management area to a computer off the local system, edited to correct each record that failed, uploaded to the local system File Management area, and used again to repeat the Import operation and successfully process the records.

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.

Exported CSV Files

Each exported CSV file contains one or more records for the configuration data that was selected for the Export operation. The record formats and contents are described in Bulk Import and Export CSV File Formats and Contents.

The selected configuration data can be exported once immediately, or can be periodically automatically exported on a defined schedule.

- Configuration data refers to any data that is configured for one of the Export Application types (FABR, RBAR, CPA, and SBR DSR Applications, and the Diameter Configuration menu folder).
- For the "Diameter" Export Application type, configuration data refers to any data that is configured using the GUI pages that are available from the Diameter Configuration folder.

  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 Export Application
- Exportable configuration data from a selected configuration component for the selected Export Application

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

For data that is exported once immediately, the default Output File Name has the following format; the name can be changed and is not required to keep this format: NeName_Timestamp-TimeZone_ApplicationType_ReportType.csv.

For data that is scheduled to be exported periodically, the default Task Name is DSR Configuration Export; the name can be changed.

All exported .csv files contain a comment header with the following information:

- Software revision used to generate the exported file
- Date and Time file was generated
- Name of selected Data object(s) exported
- Total number of exported records

The following example illustrates how the export file header might appear, but it might not look exactly as shown:

```
################################################################################
# Tekelec DSR Software Revision: xxxx
```

```
# Date/Time Generated: mm/dd/yy hh:mm:ss
# Exported Application: <ApplicationType>
# Exported Object: <ObjectType>
# Number of Records: nnn
################################################################################
```

Export Operations

Exported files can be written to the File Management Directory in the Status & Manage File Management area (see the **Status &Manage Files** page) 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. See *DSR Bulk Import*.

For files that are exported to the local File Management Directory,

- The files appear in the File Management area list on the local system (see the **Status & Manage Files** page) and in the list on the **Diameter Configuration Import** page.
- These files can be used for 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 (see Administration > Export Server), 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.

Export Results

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.

Chapter 4

Diameter Mediation

Topics:

The Diameter Mediation feature allows easy creation of Mediation Rules.

Mediation overview

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. Two or more Conditions in the same Rule Template are collectively referred to as a Condition Set; the Conditions are "AND"ed in the comparison process.
- An Action can be adding, altering, or deleting AVPs; modifying the message header Flags, Length, Command-Code, or Application-ID; or other operations. Two or more Actions in a Rule Template are collectively referred to as an Action Set.

Mediation can be performed on:

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

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

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

Diameter Mediation provides a Rule Templates interface, a Rule Sets interface, and other GUI screens:

- The Rule Templates interface is used primarily for the creation and modification of Rule Templates.

  When the Mediation feature is activated in the system and "Meta-Administrator" privileges are activated for the feature, the Rule Templates folder appears under the Mediation folder in the Diameter left-hand GUI menu.

  The "Meta-Administrator" privileges can be deactivated later, so that the Rule Templates folder does not appear under the Mediation folder. This can be to prevent unauthorized modification of the created Rule Templates in the system.

Note: For DSR 4.0, Tekelec Professional Services personnel are the only users that will perform the Rule Templates tasks in the role of Meta-Administrator, with the "Meta-Administrator" privileges activated.

A user, who could be designated as the "Meta-Administrator", can use the Rule Templates GUI screens and other Mediation GUI screens to perform the following tasks:

- Add, edit, and delete Enumeration Types, AVP Dictionary entries, and Vendors that are used in creating Rule Templates (see *Enumerations*, *Custom Dictionary*, and *Vendors*)
- Create, modify, delete, copy, import, and export Rule Templates (see *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 (see *Rule Templates*)
- Associate Rule Sets with Triggers, and remove Rule Set associations with Triggers (see *Triggers*)
- Set the Action Error Handling property of a Rule Set (see *State and Properties*)
- Change the state of a Rule Template (see *State and Properties*)

  When a Rule Template is being created or modified, it is in the Development state.

  The Rule Template state can be changed from Development to Test to allow its Rule Set to be tested or to allow the Rule Template to be exported.

  The Rule Template state can be changed to Active to enable use of its generated Rule Set for live traffic.

  The Rule Template state can be changed from Test or Active back to Development to allow modification of the Rule Template (all existing rule provisioning for its associated Rule Sets will be deleted).

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

  After a Rule Template has been created, the generation of the Rule Set from the Rule Template creates an entry in the Mediation Rule Sets GUI folder.

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

  - Add a rule to a Rule Set, and provision the actual data that is used by the rule in the message matching process (see *Rule Sets*)
  - Edit and delete rules in Rule Sets (see *Rule Sets*)
  - Delete Rule Sets (see *Rule Sets*)
  - Change the state of a Rule Template (see *State and Properties*)

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

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

  - Set the Action Error Handling property of a Rule Set (see *State and Properties*
  - 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*.

- Associate Rule Sets with Triggers, and remove Rule Set associations with Triggers (see *Triggers*)
- Import previously exported Rule Templates (see *State and Properties*)

  The state of an imported Rule Template is set to Test by default.
- View the Enumeration types that can be used in the rules (see *Enumerations*)
- View the Vendors that can be used in Rule Templates (see *Vendors*)

Rule Templates

Rule Templates are created by:

- Formulating the Conditions against which to match incoming requests or responses
- Defining the Mediation Actions that are applied to the message when the Conditions match

Note: The "Meta-Administrator" privileges must be activated for the Diameter Mediation feature before the Rule Templates GUI screens can be accessed to create and modify Rule Templates.

A Rule Template is created by configuring Settings, Conditions, and Actions.

Settings

Settings are the main Rule Template properties:

- Rule Template Name: A placeholder for meaningful text to describe the purpose of the Rule Template and Rule Set.
- Message type support: The type of message processing that is supported by a Rule Template; either a Request, an Answer, or both. In Diameter Mediaition for DSR 4.0, both Request and Answer are supported, and the element value cannot be changed.

Conditions

One or more (up to 5) matching expressions (Conditions) can be defined in a Rule Template. The expressions are combined into one logical expression with "AND" operatiors, so that the request or response matches the condition set if all of the expressions are true. If no matching expression is defined, the message unconditionally matches.

Each matching expression consists of a left-hand value or operand, an operator, and a right-hand value or operand.

- Left value: Allows accessing any part of a message, any information stored by the previous Rule Template, and any information that the application resolves runtime.
- Operator: Allows comparison of the Left value and the Right value
- Right value: Allows performing the syntax check for the entered data on the generated **Rule Sets** page.

Conditions can be configured to cause Mediation to use fast database lookups.of the rule data. See *Fast Search*.

Actions

Actions 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). Actions implement the mediation of a message.

When the message processing reaches a selected triggering point, the Conditions of the Rule Template are examined for the message. If the Conditions match, Mediation Actions are applied to the message. The Actions allow manipulation of some particular part of the message, adding or deleting information in the message, or forwarding the message to a specific destination.

The Actions to take when a Mediation operation is triggered and its Condition Set is matched are defined in the Rule Template. Actions belonging to the same Rule Template form an Action Set.

Fast Search

The Fast Search option is used to cause Mediation to use fast database lookups. If Fast Search is not used, the values of each condition are checked one-by-one until the first match is found.

The Fast Search option appears as the first element for each condition that is defined in the Conditions section for a Rule Template. The Fast Search option is not editable; it serves only to indicate whether Fast Search will or will not be used for the condition:

All of the conditions with the Fast Search option enabled must precede any conditions without Fast Search enabled in the Rule Set list. If any conditions without Fast Search enabled precede conditions with Fast Search enabled, a database lookup could fall back to slow search because of the order of the conditions.

The value of the Fast Search option is determined by the Operator and the Right value that are selected for the condition. The Fast Search value is either the “Yes” (check mark) sign or the “No”(red circle with a red line through it) sign.

- Fast Search is supported only by the “equals”, “begins with (longest match)”, “begins with”, “is within”, “exists”, “does not exist”, “is true”, “is false” Operators.
- If a “no” sign is displayed for the Fast Search option, then the Operator “=^^” (begins with – longest match) is disabled (cannot be selected) in the Operator drop down list for the condition.
- Regardless of the Operator, the Fast Search option is supported if the Right value is a Fixed value (a data value was entered in the Rule Template, and the value cannot be changed in the Rule Set).
- Regardless of the Operator, the Fast Search option is not supported if the “xl-value” Right value type is selected without a Fixed value.

The “Yes” sign is displayed for the Fast Search option if:

- One of the Operators “==” (equals), “=^^” (begins with-longest match), “=^ (begins with)”, “is within”, “exists”, “does not exist”, “is true, “is false” is selected and the Right value type is not “xl-value”.
- The Default value is Fixed regardless of the selected Operator and Right value type; and either the condition is the first one in the Condition Set, or all the conditions above it also have a “Yes” sign for the Fast Search option.

In any other case, the “No” sign is displayed.

When the selected Operator, the order of the conditions, or the Right value type changes, then every Fast Search “Yes” and “No” value has to be reevaluated and redrawn, and the Case-sensitive check box is either enabled or disabled accordingly.

If a “Yes” sign has to be changed to “No” under the Fast Search heading as a result of the reevaluation, and the related Operator “=^^” (begins with-longest match) was selected, a dialog box is displayed to confirm disabling of Fast Search:

Case-sensitive lookup depends on the Fast Search option; the check box is unchecked and disabled if Fast Search is also disabled. The Case-sensitive check box is enabled only for the Octet-String and UTF8String Right value types.

Formatting Value Wizard

The Formatting Value Wizard is a popup window available from both the Diameter > Mediation > Rule Templates Insert/Edit/Copy pages and the Diameter > Mediation > Rule Sets Insert/Edit pages. The wizard simplifies entry of xl-formatted strings, which require specific syntax coding. Both Log and Add Header functions require xl-formatted string coding.

An xl-formatted string can contain references to the state of the server, or to the message being processed. For example, %@ruri.user refers to the user part of the Request URI within an xl-formatted string. The references are replaced with their actual value before the log message is issued, or before the string is appended to the Request.

Enumerations

An Enumeration Type (Enum Type) consists of a name and a set of values. The purpose of the Enum Type is to strictly define the possible values of a data input field.

The allowed values are comma-separated items, which might optionally contain colons. If an item contains a colon, then everything before the colon is a label and everything after the colon is a value. If an item does not contain a colon, then the value and the label are the same.

Pre-defined Enum Types are provided with the Diameter Mediation feature. New Enum Types can be defined with their possible values. When a new Enum Type is created, it automatically appears in the Conditions section of the **Diameter Mediation Rule Templates** Insert, Copy, and Edit pages, within the list of Right value types. The Enum Type must be created before a Rule Template Condition can use it. The values of the Enum Type used by the Mediation Rule Set can be modified after the Rule Template has been created.

When a Right value of a Rule Template Condition is set to an Enum Type, the actual value can be set in a rule only to one of the valid values of the specified Enum Type. This is enforced by presenting a pulldown list instead of an input field on the **Diameter Mediation Rule Sets** [Insert] and [Edit] pages.

GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Mediation Enumerations elements*.

Vendors

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

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

GUI field descriptions, formats, valid values and ranges, and any default values are listed in .

Base Dictionary

The Diameter Mediation **Base Dictionary** page allows the operator to view the basic AVPs that are familiar to the system (defined in the Base Diameter Standard, and in Diameter Applications such as Diameter Credit Control Application and S6a interface).

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

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

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

Proprietary and additional standard AVP definitions can be added in the Custom Dictionary. Custom Doictionary entries are not displayed on the Base Dictionary View page.

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

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

GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Mediation Base Dictionary elements*.

Custom Dictionary

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

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

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

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

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

The values for AVP definitions are described in *Mediation Custom Dictionary elements*.

The **Diameter Mediation Custom Dictionary** page allows the operator to:

- Add new proprietary AVPs and additional standard AVPs familiar to the system
- Overwrite AVP definitions in the Base Dictionary, by specifying them in the Custom Dictionary with a different definition. The AVP Code, Vendor ID, and Attribute Name must remain the same in the changed definition.

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

All-AVP Dictionary

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

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

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

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

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

Triggers

An execution trigger defines a triggering point within the message processing logic. When the triggering point is reached, the mediation operations (Rule Sets) associated with that triggering point are executed. The type of the Trigger defines whether the triggering point is part of the request or the answer processing.

The available triggering points are pre-defined. One or more Rule Sets can be associated with a Trigger. The Triggers described in *Table 4: Diameter Mediation Triggers* are available for Diameter Mediation.

The behavior of an MP is exactly the same with and without a Trigger if no Rule Set is associated with the Trigger.

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

The Rule Set can be defined to be executed as a part of the Actions of another Rule Set, or it can be triggered at some specific point of the message processing

Rule Sets that are associated with a Trigger are executed in the sequence in which they are listed under the Trigger name on the **Diameter Mediation Triggers** page.

Associations of a Trigger with new Rule Sets can be added, existing associations can be removed, and the sequence of the Rule Set Name list can be changed to modify the MP behavior based on the Rule Set execution.

Table 4: Diameter Mediation Triggers

Execution Trigger Name	Message Type	Triggering Poing
Diameter request message received from connection	Request	Request Trigger Point 1; occurs upon receipt of a request
Diameter request message ready to be forwarded to connection	Request	Request Trigger Point 10; occurs just before forwarding the request upstrean
Diameter answer message received from connection	Response	Answer Trigger Point 1; occurs upon receipt of an answer
Diameter answer message ready to be forwarded to connection	Response	Answer Trigger Point 10; occurs just before forwarding the answer dwonstrean

On the Diameter Mediation Triggers page, you can perform the following actions:

- Click the Insert button under a Trigger name.

  The **Diameter Mediation Triggers [Insert]** page opens. You can associate a new Rule Set with the Trigger.
- Select a Rule Set Name in the list under a Trigger name, and click the Remove button.

  The association of the Rule Set with the the Trigger can be removed, and the Rule Set Name is deleted from the list for the Trigger.
- Use the Up and Down buttons to alter the sequence of execution of the Rule Sets associated with a Trigger.
  - For a selected Rule Set Name, clicking the Up button under the Rule Set Name list moves the selected Rule Set Name one position toward the top or beginning of the list.
  - For a selected Rule Set Name, clicking the Down button under the Rule Set Name list moves the selected Rule Set Name one position toward the bottom or end of the list.

State and Properties

The **Diameter Mediation State & Properties** page lists all of the Rule Templates that are configured in the system, and shows the State and Action Error Handling setting for each Rule Template.

Each Rule Template is in one of the following states at any point of time:

- Development
- Test
- Active

The Action Error Handling defines the error handling strategy to be used if any Action in the Rule Template fails.

Each Rule Template starts in the “Development” state when it is being created. Rule Templates in the Development state cannot be assigned to Triggers.

After all of the necessary Conditions and Actions have been added, the Rule Template must be set to the “Test” state, to indicate that the Rule Template is complete. A Rule Set entry is generated in the Rule Sets Left-hand Menu folder; the Rule Set can be provisioned with actual data in one or more rules, and can be associated with a Trigger. In the "Test" state, only limited changes can be made to the contents of the Rule Template.(See *Rule Templates*.)

The Rule Template state can be set back to "Development" only when the " Meta-Administrator" privileges are activated for the Diameter Mediation feature. All provisioned data for the Rule Template will be lost if the state is set back to "Development".

The Rule Template state can be set to "Test" or the association between the Rule Set and a Trigger can be removed to disable the Rule Set for live traffic.

In the “Test” state a Mediation Rule Set does not affect the live traffic, but the operator can test the newly created, imported, or modified Rule Set that was generated from the Rule Template. The Diagnostics Tool can be used to exercise and test the Rule Templates in the “Test” state, along with Rule Templates in the “Active” state. See *Connection Maintenance* and *Diameter Diagnostics Tool*.

When the state of a Rule Template is set to "Active", the Rule Set associated with the Rule Template begins to participate in processing of real traffic messages.

The Import function from the **Diameter Mediation Rule Templates** page is duplicated on the **Diameter Mediation State & Properties** page for use when the "Meta-Administrator" privileges are not activated and the **Diameter Mediation Rule Templates** page cannot be accessed. An imported Rule Template is set to "Test" state.

On the **Diameter Mediation State & Properties** page, you can perform the following actions:

- Filter the list to display only the desired Rule Templates.
- Sort the entries in the list, by clicking the column headings. By default, the list is in alphabetical order by Rule Template Name.
- Click Import Rule Template to import a previously exported Rule Template from a location outside of the DSR system.

  If importing a Rule Template would cause the maximum number of Rule Templates (100) in the system to be exceeded, the Rule Template is not imported and an error message appears.
- Select a Rule Template Name in the list, and click Edit. You can change the State and Action Error Handling for the selected Rule Template.

  When the "Meta-Administrator" privileges are not activated for the Diameter Mediation feature, the state of a Rule Template cannot be changed back to "Development".
- Select a Rule Template Name in the list, and click Delete to remove the selected Rule Template from the list.

  When a Rule Template is deleted from the **Diameter Mediation State & Properties** page, it is deleted from all other pages at the same time.

Rule Sets

A Rule Set is generated from a Rule Template that was defined on the Diameter Mediation Rule Templates page, when the Rule Template state is changed from Development to Test or Active. The Diameter > Mediation > Rule Sets GUI folder contains an entry for each generated Rule Set. If no Rule

Sets have been generated, the Rule Sets folder contains no entries. All rules in a Rule Set are specific to the Rule Template from which the Rule Set was generated.

Clicking a Rule Sets entry opens the **Diameter Mediation Rule Sets <name>** GUI page for the Rule Set (<name> is the name of the Rule Set).

The **Diameter Mediation Rule Sets <name>** page displays the following columns:

- Move the rule

  A Move the rule column appears at the left and at the right of the rules list when there are rules that are allowed to be moved up or down in the list to change the order of rule execution.

  Up and Down buttons in the Move the rule columns can be used to move a rule up one position in the list or down one position in the list each time the button is clicked.

  Up and Down buttons appear in the Move the rule columns for a rule or rule group when the order of the rules is allowed to be changed, with the following restrictions:

  - When the Filter function or clicking a Condition column heading is used to sort the columns, the Move the rule columns are not displayed. The Restore Order button can be clicked to return the list to its original order.
  - If all of the conditions in the rule support Fast Search, then the Move the rule columns are not displayed. See *Fast Search*.
  - If there is at least one condition that does not support Fast Search, then the Up and Down buttons are displayed according to the following rules:
    - All of the rules that support Fast Search always appear in the list before any rules that do not support Fast Search.
    - The rows that have exactly the same data in the conditions that support Fast Search form a group. Rows can be moved only within their group; the Up and Down buttons are enabled and disabled accordingly.

      Table 5: Example of Default Ordering of Rules in a Rule Set shows an example of default ordering of rules.

      Table 5: Example of Default Ordering of Rules in a Rule Set

Fast-search condition 1	Fast-search condition 2	Non fast-search condition 3
abc	1	-
abc	12	-
abc	-	-
abcd	1	-
abcd	1	a1
abcd	-	b1
-	1	a1
-	1	b1
-	-	-

- Conditions

  One column appears for each condition that is defined in the Rule Template that generated the Rule Set. The columns appear from left to right in the same order that the conditions are defined in the Rule Template for the Rule Set. The heading of each column is the Condition Name. Each entry in a condition column is the data that was entered in the Right value field of the condition for the rule.

  Each condition column heading can be clicked to sort the rules by the ascending or descending alphabetical order of the values in that column. The column contents can be used to filter the rules that are displayed in the list.

- Actions

  One column heading appears for each Action that is assigned to the conditions in the Rule Template for the Rule Set. The columns appear from left to right in the same order that the Actions are defined in the Rule Template. The Action columns cannot be sorted by clicking the heading; their contents can be used to filter the rules that are displayed in the list

- Action Attribute sub-columns for each Action

  Sub-columns appear for the attributes of each Action. The sub-columns cannot be sorted by clicking the heading; their contents can be used to filter the rules that are displayed in the list. All of the conditions in a Rule Template use the same Actions; the Action attributes can be assigned different values in different rules in the Rule Set.

Each row across the columns is created (inserted) in the list when a rule is provisioned. The rules on a **Diameter Rule Sets <name> page** are looked up in the database in the order in which they are listed on the page. By default, the rules are sorted in the list by condition in the following order:

- First the conditions, in alphabetical order from left to right, that have the Fast Search option enabled
- Followed by any conditions, in the order that they were provisioned, that do not have the Fast Search option enabled.
- Though all rules in a Rule Set have the same conditions available, rules can be provisioned with one or more of the conditions “empty” (with no values), indicating that the condition is always matched in message processing. The rules with empty conditions are listed after the rules that contain values for the same conditions.

The Rule Sets folder entries to view, insert (provision), change, or delete rules in Rule Sets.

When a Rule Set entry is selected in the Rule Sets folder, the **Diameter Mediation Rule Sets <name>** page opens for the selected Rule Set.

On each **Diameter Mediation Rule Sets <name>** page, a user can perform the following actions:

- Filter by the column contents, to display only the rules with the desired contents.
- If the Move a rule columns are displayed and contian Up and Down buttons, move rules up and down in the list to change the order of execution of the rules in the Rule Set.
- Click Insert to add a new rule.

  The **Diameter Mediation Rule Sets <name> [Insert]** page opens.

  The **Diameter Mediation Rule Sets <name> [Insert]** page will not open if adding a new rule will cause the allowed maximum number of rules in the Rule Set (250) to be exceeded.

  The **Diameter Mediation Rule Sets <name> [Insert]** page will not open if adding a new rule will cause the allowed maximum total number of rules in the system (25000) to be exceeded.

Rule Templates without any conditions form a special case, because their provisioned rule unconditionally matches. The Rule Sets generated from hese Rule Templates allow only one rule to be provisioned.

- Click Delete All Rules to delete all of the rules that have been provisioned for this Rule Set.
- Select a rule and click Edit.

  The **Diameter Mediation Rule Sets <name> [Edit]** page opens. You can change the Values of the Conditions and Actions for the selected rule.
- Select a rule and click Delete to delete the rule from the Rule Set list.

User-defined Rule Sets

Rule Templates that are defined using the Diameter Mediation Rule Templates page generate new Mediation Rule Sets when the Rule Template is set to the "Test" or "Active" state. These generated Rule Sets appear in the Diameter > Mediation > Rule Sets GUI menu.

If no Mediation Rule Sets have been generated from Rule Templates, rather than being a menu, Rule Sets is a page that displays "NO Rule Sets are defined yet".

Adding a user-defined Rule Set

If no Mediation Rule Sets are defined, Mediation > Rule Sets is a page that displays "NO Mediation Rule Sets are defined yet", and no Mediation Rule Sets are available to be added here. To define a Mediation Rule Set, use the Mediation > Rule Templates page.

Chapter 5

Diameter Maintenance

Topics:

This chapter describes:

- The maintenance and status information that is maintained by the Diameter Routing Function and the Diameter Transport Function for the Diameter Configuration components that are used to make egress Request message routing decisions
- 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 attributes 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

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.

The Diameter Configuration components are summarized in *Table 6: Diameter Configuration Component Descriptions*.Tables *Table 9: Route List Relevant Configuration Elements* through *Table 13: Connection Relevant Configuration Elements* provide a high-level description of their component configuration elements that are relevant to maintenance and status management.

DSR Application elements are described in *Table 14: DSR Application Relevant Maintenance Elements*.

DA-MP elements are described in Table 25 and Table 26.

Table 6: Diameter Configuration Component Descriptions

Diameter Component Name	Description
Route List	A Route List contains a prioritized list of Route Groups that is used for Diameter routing of Request messages. See *Table 9: Route List Relevant Configuration Elements* for a description of relevant Route List configuration elements.
Peer Route Group	A Peer Route Group contains a weighted list of Peer Nodes that is used for Diameter routing of Request messages. A Peer Route Group can be assigned to one or more Route Lists. See *Table 12: Peer Node Relevant Configuration Elements* for a description of Peer Route Group configuration elements.

Diameter Component Name	Description
Connection Route Group	A Connection Route Group contains a weighted list of Connections that is used for Diameter routing of Request messages. A Connection Route Group can be assigned to one or more Route Lists. See *Table 11: Connection Route Group Relevant Configuration Elements* for a description of Connection Route Group configuration elements.
Peer Node	A Peer Node contains the elements for an adjacent Diameter Node to which DSR has one or more SCTP/TCP connections. The elements assigned to the Peer Node are used for Diameter message routing decisions. See *Table 12: Peer Node Relevant Configuration Elements* for a description of Peer Node configuration elements.
Diameter Connection	A Diameter connection is a point-to-point TCP/SCTP Diameter Connection to an adjacent Diameter Peer (a Diameter connection between a DSR Local Node and a Peer Node). The elements assigned to the connection are used for Diameter message routing to and from that Diameter connection. See *Table 11: Connection Route Group Relevant Configuration Elements* for a description of Diameter connection configuration elements.

Table 7: DSR Application and DA-MP Description describes DSR Applications and DA-MPs.

Table 7: DSR Application and DA-MP Description

Name	Description
DSR Application	Each DSR Application Configuration component contains all of the elements associated with that DSR Application, such as the internal DSR Application ID used for message routing and the Unavailability Action attribute that defines default Request message routing when the DSR Application Operational Status is not "Available". See Table z for a description of DSR Application Configuration elements.
DA-MP	Each DA-MP tracks the impairment of MP-level elements for each of its Peer DA-MPs. It combines the impairment levels of the individual elements into a single overall value called DA-MP-CPL. These impairment levels are part of the maintenance and status data that is merged to the OAM. The maintenance and status data associated with the DA-MP is described in Table z and Table z .

Table 14: DSR Application Relevant Maintenance Elements describes the elements that are relevant to DSR Application maintenance and status management.

Table 8: DSR Application Relevant Maintenance Elements

Attribute	Description
Name	Tekelec-defined name for the DSR Application.
Admin State	User-configurable Admin State (Enabled or Disabled) of the DSR Application.

The configuration elements of each Diameter Configuration component that are related to status management are defined in Tables *Table 9: Route List Relevant Configuration Elements* through *Table 11: Connection Route Group Relevant Configuration Elements*.

Table 9: Route List Relevant Configuration Elements

Element	Description
Route List Name	User-defined name for the Route List.
Minimum Route Group Availability Weight	Each Route Group within the Route List has a weight based on the status of the Peer Nodes or connections within the Route Group. This attribute and the current weights of the Route Groups within the Route List are used to determine which Route Group will be used when a Route List is selected for routing Request messages.
Route Group	Peer or Connection Route Group name assigned to this Route List. Multiple instances of a Route Group can be assigned to a Route List.
Priority	Relative priority of the Route Group assigned to this Route List; used for determining which Route Group will be used when this Route List is selected for routing Request messages.

Table 10: Peer Route Group Relevant Configuration Elements

Attribute	Description
Route Group Name	User-defined name for the Peer Route Group.
Peer Node Name	Peer Node assigned to this Peer Route Group. Multiple instances of Peer Nodes can be assigned to a Peer Route Group.
Peer Weight	Configured relative weight of the Peer Node within the Peer Route Group. The relative weight of a Peer Node within a Peer Route Group determines the probability that a Request message is routed to this Peer when the Peer Route Group is selected for message routing.

Table 11: Connection Route Group Relevant Configuration Elements

Attribute	Description
Route Group Name	User-defined name for the Connection Route Group.
Connection Name	Connection assigned to this Connection Route Group. Multiple connections can be assigned to a Connection Route Group.
Connection Weight	Configured relative weight of the connection within the Connection Route Group. The relative weight of a connection within a Connection Route Group determines the probability that a Request message is routed to this Peer when the Connection Route Group is selected for messages routing.

Table 12: Peer Node Relevant Configuration Elements

Attribute	Description
Peer Node Name	User-defined name for the Peer Node.
Minimum Connection Capacity	The minimum number of Diameter connections to a Peer that must be able to receive forwarded Request messages from the Diameter Routing Function for the Peer's Operation Status to be considered "Available". When the number of Diameter connections drops below this threshold, the Peer's Operational Status will either be "Degraded" or "Unavailable".

Table 13: Connection Relevant Configuration Elements

Attribute	Description
Connection Name	User-defined name for the connection.
Peer Node	Peer Node Managed Object to which this Diameter connection is associated with.
Admin State	User-configurable Admin State (Enabled or Disabled) of the connection. Note: This is considered to be a Maintenance attribute, not a Configuration attribute.

Table 14: DSR Application Relevant Maintenance Elements

Attribute	Description
Name	Tekelec-defined name for the DSR Application.

Attribute	Description
Admin State	User-configurable Admin State (Enabled or Disabled) of the DSR Application.

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

Table 15: 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

Diameter Configuration Component	Component Status Dependency	Configuration Element Dependencies
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

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 16: Maintenance and Status Data Sourcing Methods*.

Table 17: 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 16: Maintenance and Status Data Sourcing Methods

Sourcing Method	Description	When to choose this Sourcing Method
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 17: Diameter Configuration Component Sourcing Methods

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

Diameter Configuration Component Name	Sourcing Method	Diameter GUI Screen (starting from Main Menu : Diameter ->)
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, the concept of a “DA-MP Leader” has been introduced. 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 two connections are established simultaneously on two different DA-MPs, which could be reporting status on the same connection. This situation will be transient, as the Diameter Routing Function will detect the collision and take down one of the connections.

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

  The Diameter Transport Function performs several validations during the Capabilities Exchange procedure to prevent and minimize the occurrence of Duplicate Connection instances.
- DA-MP Leader Transition: Assume that DA-MP1 is the Leader, and it is reporting status for a component that uses the "Leader" sourcing strategy. Now assume that DA-MP1 undergoes a non-graceful shutdown (it is not able to clean up its status), and the Leader transitions to DA-MP2. The OAM will detect that DA-MP1 has failed, and discard any status data that was previously reported by DA-MP1. However it is possible that DA-MP2 will take over as Leader and begin merging status data to the OAM before OAM has detected that DA-MP1 has failed.

Ownership of Diameter Connections

The DSR supports two types of connections:

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

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

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

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

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

Raising and Clearing Alarms

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

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

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

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

For Diameter Configuration components, DSR Applications, and DA-MPs for wich maintenance and status data is maintained, this section describes:

- The maintenance and status information that is maintained
- One or more Sourcing Methods that are used
- The Diameter GUI page that reports the maintenance and status information
- The run-time actions that result inupdates to the status data
- The strategy for merging the status information to the OAM

Route Lists Maintenance

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.

Route Gropps Maintenance

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.

Peer Nodes Maintenance

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.

Connections Maintenance

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.

Applications Maintenance

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.

DA-MPs Maintenance

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.

Route Lists Maintenance

Table 18: Route List Status Data identifies the Route List maintenance and status data that is maintained and merged to the OAM. 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.

The Route List maintenance and status data that is displayed on the following Diameter GUI page is described in *Route List maintenance elements*:

- Main Menu: Diameter -> Maintenance -> Route Lists

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 18: 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 Group Operational Status

For the Route List component, all DA-MPs (both Leader and Non-Leaders) maintain the status data listed in *Table 18: Route List Status Data*.

Because all DA-MPs have identical Route List status, the Leader sourcing method is chosen for Route Lists to avoid merging multiple copies of the same status data to the OAM. When any of the Route List component status data listed in *Table 18: Route List Status Data* changes, then:

- All DA-MPs (both Leader and Non-Leaders) update the status.
- The DA-MP Leader merges the updated status to the OAM.

  Non-Leaders do not merge their modified status to the OAM.
- The Time of Last Update is set to the current time.

The Diameter Routing Function updates a Route List's Active Route Group and Operational Status when any of the following criteria are met:

- The Operational Status of any Route Group within a Route List changes
- The Minimum Route Group Availability Weight or Route Group Priority of the Route List is changed
- A new Route List is configured
- The Current Capacity of a Route Group within the Route List is changed
- A new Route Group is added to a Route List

- A Route Group is deleted from a Route List

The Diameter Routing Function determines which Route Group within a Route List will be designated the Active Route Group for that Route List, as follows:

- If the Operational Status of one or more Route Groups within the Route List is Available, then the Active Route Group for the Route List is the Available Route Group with the highest Priority.
- If there are no Available Route Groups and the Operational Status of one or more Route Groups within the Route List is Degraded, the Active Route Group is the Degraded Route Group with the highest Current Capacity.
- If two or more Degraded Route Groups exist with equal Current Capacity, the Active Route Group is the one with the highest Priority.
- If all Route Groups within the route list are Unavailable, then the Route List is Unavailable and there is no Active Route Group.

A Route List's Operational Status is always set to the Operational Status of the Route Group within the Route List that is designated as the Active Route Group. The Active Route Group within a Route List is the initial Route Group used for routing.

When a new Route List is configured, all DA-MPs (both Leader and Non-Leader) maintain status for the new Route List instance.

When a Route List is deleted, all DA-MPs stop maintaining status for the deleted Route List instance.

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.

On the **Connections Maintenance** page, you can perform the following actions:

- Filter the list of Connections to display only the desired Connections.
- Sort the list by a column in ascending or descending order, by clicking the column heading. The default order is by Connection Name in ascending ASCII order.
- Prevent the page from automatically refreshing by clicking the Pause updates check box.
- 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.

Starting Diagnosis on a Test Connection

Use the following steps to start diagnosis on a test connection.

1. Select Diameter > Maintenance > Connections.
   The **Diameter Maintenance Connections** page appears.
2. Select a single connection with the following conditions:
   - Admin State is Enabled
   - Test Mode is YES.
   - PDUs to Diagnose is 0
3. Click Diagnose Start.
   A confirmation box appears.
4. Click OK.
   The selected test connection is under diagnosis. The PDUs to Diagnose value is set to the maximum diagnose PDU count.

   If the selected connection no longer exists (it was deleted by another user), an error message is displayed and the Connections Maintenance page is refreshed.

Ending Diagnosis on a Test Connection

Use the following steps to end diagnosis on a test connection.

1. Select Diameter > Maintenance > Connections.
   The **Diameter Maintenance Connections** page appears.
2. Select a single connection with the following conditions:
   - Admin State is Enabled
   - Test Mode is YES.
   - PDUs to Diagnose is greater than 0.
3. Click Diagnose End.
   A confirmation box appears.
4. Click OK.
   Diagnosis on the selected test connection is stopped. The PDUs to Diagnose value is set to 0.

   If the selected connection no longer exists (it was deleted by another user), an error message is displayed and the Connections Maintenance page is refreshed.

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.

DA-MPs Maintenance

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

On the **DA-MPs Maintenance** 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.

For detailed information about the fields displayed on the DA-MP Maintenance page, see *DA-MPs maintenance elements*.

Chapter 6

Diameter Reports

Topics:

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

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

The **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.

The MP Statistics (SCTP) Report is described in *MP Statistics (SCTP) report elements*.

Chapter 7

Full Address Based Resolution (FABR)

Topics:

Full Address Based Resolution (FABR) is a DSR enhanced routing application that enables network operators to resolve the designated Diameter server (IMS HSS, LTE HSS, PCRF, OCS, OFCS, and AAA) addresses based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity addresses, and route the Diameter request to the resolved destination.

Full Address Based Resolution Overview

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 Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity addresses (Individual User Identity addresses) in the incoming Diameter Request message, and routes the Diameter Request to the resolved destination.

The FABR application uses an off-board data repository for storing the mapping of Routing Entity addresses and destination addresses to support up 7.5 million subscriber entries.

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 Routing Entity address, if extracted successfully, to an off-board DP/Subscriber Database Server (SDS) for destination address resolution.

A Routing Entity supported by FABR is one of the User Identities of International Mobile Subscriber Identity (IMSI), Mobile Subscriber Integrated Services Digital Network (Number) (MSISDN), IP Multimedia Public Identity (IMPI) or IP Multimedia Public Identity (IMPU) in the supported AVPs. FABR provides the decoded and valid User Identity addresses to the DP through reliable inter-server transmission service provided by the Communication Agent (ComAgent).

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

At a high level, the FABR application accomplishes the retrieval of the desired destination address as follows.

- After receiving a Diameter Request message and performing a necessary message validation successfully, FABR sends a query for User Identity address mapping.
- A DP performs database lookup using the keys provided by FABR in the query and returns the search result (success or fail).
- Based on the response, the FABR application will either forward the Diameter Request message containing new Destination information, forward the original Diameter Request message without any alternation, or send a Diameter Answer message response with Result-Code AVP for network routing.

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 Relay Agent for egress routing into the network.

FABR supports routing of messages as a ”Proxy Agent” as follows:

- No AVPs will be added to an egress Request message except the Tekelec-specific “DSR-Application-Invoked” AVP, or Destination-Host AVP
- No AVPs from the ingress Request message will be modified except the Destination-Realm and Destination-Host AVPs
- No AVPs from the ingress Request message will be deleted
- No Request message header fields will be modified by FABR except the “Message Length” field

Configuration

The FABR FABRConfiguration pages allow you to manage FABR application configuration.

FABR routing configuration can be of these categories:

- Routing Diameter traffic to FABR.

  Use the DiameterConfigurationApplication Routing Rules GUI page to configure Application Routing Rules that will conditionally communicate Diameter Requests to FABR.
- Configuring off-board database servers (remote servers called DPs) that support address lookup and destination resolution, and connections to these remote servers.

  Use the Communication AgentConfigurationRemote Servers and Communication AgentConfigurationConnection Group GUI pages to perform this configuration.

Before using the FABR configuration pages, complete the following activities:

- Configure the network topology. This includes network elements, servers, server groups, and network devices and routes.

  For information about configuring the DSR network topology, see x.

  For information about configuring the DP and SDS, see the SDS OAM section of the online help.
- Configure Remote Servers (DP in case of DSR and DSR in case of DP)

  Remote Server configuration is performed from the Communication Agent (ComAgent) section of the respective application (DSR and DP) configuration screens.

Remote Server Configuration

The following Remote Server attributes are configured using the Communication Agent Remote Server Configuration GUI:

- Name
- IP Address
- Connection Mode: {client, server}
- Local Server Group: group of servers that can connect to the Remote Server

The most important attribute of a Communication Agent Remote Server is an IP Address that can be reached through a server's Internal Management Interface (IMI). The IP address uniquely identifies the Remote Server and provides the means by which Communication Agent can establish transport connections to and from the Remote Server.

The following actions add a Remote Server to the network:

1. On the Communication AgentConfigurationRemote Servers GUI page,
   a. Enter a unique name (up to 32 characters) for the Remote Server in the Remote Server Name field.
   b. Enter the IP address of the Remote Server in the Remote Server IP Address field.

      The IP Address must be a valid IPv4 address in dot notation format (for example: 255.255.255.255).

c. Configure a mode of operation from the Remote Server Mode drop down list.

   The Remote Server can operate as a:

   - Client – where the servers in the local server group will accept connections initiated by the Remote Server
   - Server – where the servers in the local server group will each initiate a connection to the Remote Server

2. On the Communication AgentConfigurationConnection Group GUI page,

   a. Assign the Remote Server to a local server Connection Group.
   b. Configure DP nodes in "Server" Connection Mode on DSR nodes.
   c. Configure DSR MP nodes in "Client" Connection Mode on DPs.

3. Configure DP nodes in "Server" Connection Mode on DSR nodes.
4. Configure DSR MP nodes in "Client" Connection Mode on DPs.

The Operational status of what was provisioned can be verified by using the Communication Agent Maintenance screens (refer to the Communication Agent online help).

- MainCommunication AgentMaintenanceConnection Status to verify that all Remote Server connections added are shown as "InService" on all local servers.
- MainCommunication AgentMaintenanceRouted Service Status to verify that the status is "Available" for all local servers that are provisioned to connect

Diameter Configuration for FABR

The following Diameter components must be configured for used by FABR:

- Application Ids

  See *Application Ids Configuration*.
- Command Codes

  See *Command Codes Configuration*.
- Application Routing Rules

  See *Application Routing Rules Configuration*.

FABR Configuration

FABR configuration typically occurs in the following order:

1. Add a Application.
2. If necessary, configure a Default Destination.
3. If necessary, edit Exceptions.

   If a Routing Exception Action of 'Forward To Destination' is used, configure a Destination in the Exception.
4. Configure an Address Resolution.
5. If necessary, change the System Options.

Applications Configuration

The **Applications** page allows access to the attributes associated with the supported Diameter Applications.

A "Diameter Application" is a protocol based on the Diameter base protocol. Each Diameter Application is defined by an Application Id and can be assigned an Application Name.

In the DSR, Diameter provides the basic routing services of a Diameter Relay Agent and owns all of the SCTP/TCP transport connections to the Peer Nodes. Diameter can support multiple Diameter Nodes, each with a unique FQDN. A Diameter Relay Agent node is referred to as a "Local Node".

If a connection between the Relay Agent and a Diameter Peer is to be used for Relay Agent routing, then the reserved Diameter Application Id 4294967295-Relay needs to be configured. This allows the Peer to send both DSR Application messages and Relay Agent messages over the same transport connection.

When an Application entry is added, Routing Exceptions (Unknown Command Code, No valid Routing Entity Address, No Address Match) are automatically inserted with the Routing Exception Action value as Forward Unchanged.

When an Application entry is deleted, the associated Routing Exceptions are automatically deleted.

FABR supports only the Proxy Agent method of routing (Routing Mode) for reveived Request messages that contain a Diameter Application Id.

Exceptions Configuration

The **Exceptions** page allows specifying 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.

When an Application entry is added, 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:

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

These Routing Exceptions that are associated with an Application entry are automatically deleted when that Application entry is deleted.

Default Destinations configuration

The **Default Destinations** page contains the attributes associated with a Default Destination to where FABR routes a message. 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.

From the **Destinations** page, you can:

- Filter the list of destinations to display only the desired destinations.
- View a list of destinations.
- Insert a destination.
- Edit a Default Destination.
- Delete a Default Destination.

Address Resolutions Configuration

FABR performs off-board database lookups for User Identities decoded from Diameter messages. The Address Resolutions page allows configuration of which (and how) User Identities are to be decoded from the messages.

Address Resolution defines the Routing Entity address searching criteria related to a supported Diameter Application Id, a Command Code, and a Routing Entity Type.

Combinations of Diameter Application ID and Command Code (the key that is matched to the messages,) the Routing Entity Types to be decoded, and a prioritized list of AVPs from which to decode these Routing Entity Types need to be configured.

A configured Address Resolution supports up to 2 prioritized Routing Entity Types for each Application ID and Command Code:

- Primary Routing Entity Type (highest priority)
- Secondary Routing Entity Type (lowest priority)

System Options Configuration

The **System Options** page allows modifification of the default system values for FABR global parameters (for example, FQDN/Realm, or Allow Subsequent FABR Invocation, or Application Unavailable action).

Chapter 8

Range Based Address Resolution (RBAR)

Topics:

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.

Range Based Address Resolution Overview

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 (integrated) DSR Relay Agent for egress (outgoing) routing into the network.

RBAR Configuration

The RBARConfiguration pages are used to manage the RBAR routing configuration.

Before using the RBAR Configuration pages, the following activities need to be completed:

- Configure the network topology. This includes network elements, servers, server groups, and network devices and routes.
- Assign IP addresses to the server groups.

RBAR configuration typically occurs in the following order:

1. Configure an Application ID.
2. Configure a Destination.
3. If necessary, edit Exceptions.
4. Configure an Address Table.
5. Configure Addresses.
   - Create an Address Range.
   - If necessary, create an Individual Address.
   - Configure an Address Resolution

6. Configure an Address Resolution.
7. If necessary, change the System Options.
8. If necessary, change the DSR OAM Configurations.

GUI field descriptions, formats, valid values and ranges, and any default values are listed in *RBAR Configuration Elements*.

Applications Configuration

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

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

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

The GUI field descriptions, formats, ranges, and any default values are listed in *Applications configuration elements*.

Exceptions Configuration

The **Exceptions** page specifies 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.

When an Application entry is added, three Routing Exception entries (Unknown Command Code, No valid Routing Entity Address, and Missing Configured Address Entry) are automatically inserted with the Routing Exception Action set to Forward Unchanged as the default action for the Application entry.

When an Application entry is deleted, these three Routing Exceptions that are associated with the Application entry are automatically deleted.

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Exceptions configuration elements*.

Destinations Configuration

The **Destinations** page contains the attributes associated with a destination to which RBAR routes a message. RBAR uses these attributes to modify the contents of a received message before forwarding the message.

Each destination can be configured with any combination of a Realm and FQDN: Realm-only, FQDN-only, or Realm and FQDN.

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Destinations configuration elements*.

Address Tables Configuration

The **Address Tables** page allows access to Address Tables and their associated attributes.

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Address Tables configuration elements*.

Addresses Configuration

The **Addresses** page allows access to the Routing Entity Address Range and Individual Address configurable options.

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

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.

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Addresses configuration elements*.

Address Resolutions Configuration

The **Address Resolutions** page allows defining of the routing relationship between message content and an address, by mapping a Diameter Application ID, Command Code, and Routing Entity Type to a user-configured address (a range or individual address). An Address Resolution supports up to two prioritized Routing Entity Types for each Application ID and Command Code (highest priority – Primary Routing Entity Type – and lowest priority – Secondary Routing Entity Type).

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *Address Resolutions configuration elements*.

System Options Configuration

The **System Options** page allows modification of the default system values for RBAR global parameters (for example, FQDN/Realm, or Allow Subsequent RBAR Invocation, or Application Unavailable action).

The GUI field descriptions, formats, valid values and ranges, and any default values are listed in *System Options elements*.

Chapter 9

Charging Proxy Application

Topics:

The Charging Proxy Application (CPA) menu options allow you to perform configuration tasks, edit system options, and view elements for:

- System Options
- Message Copy
- Session Binding Repository (SBR)
- SBR Subresource Mapping

The Offline Charging Solution

The Tekelec Offline Charging solution consists of the following components:

- Charging Proxy Application (CPA)
- Message Copy for CPA
- Session Binding Repository (SBR)
- IP Front End (IPFE) (Optional)

Configuration

CPA is a DSR Application that is responsible for routing Diameter accounting (Rf) messages that are being exchanged between clients (CTFs) and servers (CDFs). The CPA application resides in the Diameter Application Layer (DAL) of the Diameter Plug-In.

The CPA menu option allows you to perform configuration tasks for the following:

- System Options
- Message Copy
- SBR
- SBR Subresource Mapping

Note: CPA does not require any additional network configuration beyond the standard DSR configuration.

CPA System Options

The **System Options** page shows values for various CPA configuration options.

The fields are described in *System Options page elements*.

Message copy

The Diameter Message Copy feature allows users to forward a copy of a Diameter Request message received by or routed through the Diameter Signaling Router to a Diameter Application Server (DAS peer). This capability is triggered based on the CPA configuration.

A user can specify a triggering condition or rule, and 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. In the case of Message Copy, the action is to copy the Request and send the copy to a DAS peer. Message Copy copies only the Diameter portion of the Request that matches a triggering condition; thus, the transport and IP layers are not copied. Lower layer protocols that do not contain Diameter Requests are not copied; thus, Message Copy does not implement a port mirror that replicates everything received on the wire on a specific port to an egress port.

Session Binding Repository (SBR)

The Session Binding Repository (SBR) provides a high availability (HA) distributed database for the DSR Charging Proxy Application (CPA). The 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 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 SBR for the session binding to determine the identity of the serving CDF.

In the most basic form, the SBR consists of a session binding database (SBDB) in which to store session binding data, and a server process to handle requests from the CPA to manipulate session bindings. For scalability, SBR blades are divided into active/standby pairs. The SBDB is logically partitioned across each of the active/standby pairs.

The CPA determines which of the logical partitions owns (or will own, in the case of a session creation) the Session-ID. A logical partition corresponds with an SBR subresource. The CPA then submits the request to the selected SBR subresource. The SBR does not know the scheme for distributing sessions among the subresources. The distribution of sessions evenly among the subresources is accomplished solely by the CPA. Consequently, if the sessions are not evenly distributed, the SBR cannot redistribute them.

Each session binding record is stored with a timestamp that indicates when the record was last modified. Periodically, a cleanup audit deletes stale session binding records from the SBDB. The time at which the audit runs and the age at which a binding is considered stale are configurable. The cleanup audit helps to reduce the risk that stale session bindings could prevent the creation of new session bindings. Decreased database performance due to an unnecessarily large database is also remedied by cleaning up stale session binding data.

Congestion in the SBR is determined independently by each partition based on its queue depth. Congestion notifications are included with each SBR response message. The SBR will also monitor the current service time of its request queues. The service time information is provided with the congestion data included in the SBR response messages. The CPA uses the service time information to detemine whether the time for the SBR to process a request meets its needs.

If the SBR becomes overloaded or congested, the SBR will shed load in a predictable way in order to control the overload state. The load shedding strategy progressively increases the type of operation shed. Each higher level of congestion adds a new operation to be shed. At 85% congestion, create operations are shed. At 90% congestion, create and update operations are shed. At 95% congestion, read, create and update operations are shed. At 100% congestion, read, create, update and delete operations are shed. As the overload condition lessens, those levels are reversed as the system returns to normal operations.

SBR page

This section describes the configuration functions of the Session Binding Repository found on the **SBR** page, which specifies when the stale session binding audit will run and how old a binding has to be before it is considered stale.

Configuring the SBR

The configuration options fields set up the audit window, specify when a binding becomes stale and sets some alarm and measurement thresholds.

1. Select CPA > Configuration > SBR.

The **CPA -> Configuration -> SBR** page appears.

2. Inspect the defaults.

   For more information on the configurations, see *SBR elements*.

   It should not be necessary to modify the defaults.

3. Make any changes to the configurations.
4. Click Apply to apply your changes.

   Your changes will go into affect immediately.

SBR Subresource Mapping page

This section describes the configurations found on the **SBR Subresource Mapping** page. A subresource is a logical partition of the Session Binding Repository.

CAUTION: The subresource mapping must be configured after you activate the CPA, but before you enable it.

Configuring the SBR subresource mapping

CAUTION: Subresources must be configured after the CPA application is activated.

This screen can be edited only once.

You must accept the configuration to enable the CPA application.

1. Select CPA -> Configuration -> SBR Subresource Mapping.

   The **CPA -> Configuration -> SBR Subresource Mapping** page appears.

2. Inspect the defaults for Subresource Ids.

   It should not be necessary to modify the defaults. The defaults are correct for a production deployment.

3. If needed for setting up a testing environment, make changes to the configurations.

   If there is a SBR Server Group that you do not intend to use (that is, not host a subresource), change the subresource ID to "Not Hosted". This configuration would only be used in lab testing.

   Subresources must be numbered sequentially, starting with 0 and incremented by 1.

4. Click Apply.

   This step is mandatory, even if no changes to the subresource Ids were made.

   A warning displays saying that this screen can be edited only once. The update will be rejected if subresources are not numbered sequentially starting with 0.

5. Click Confirm to apply your changes.

Once the changes are confirmed, this page and the configurations for the SBR on the Configuration -> Server Groups page will be read only.

If you need to reconfigure subresources or SBR server groups, contact the Tekelec Customer Care Center for assistance.

Chapter 10

IP Front End (IPFE)

Topics:

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

- Presents a routable IP address representing a set of 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

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 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.

Failure and recovery scenarios

An IPFE that has a mate and at least two Target Set Addresses can handle different failure and recovery scenarios.

Note: The following failover scenarios describe what happens with the IPFE-A1 and IPFE-A2 pair. A failover involving the IPFE-B1 and IPFE-B2 pair is handled exactly the same way.

This section discusses how the following IPFE setup can gracefully handle the failure and recovery of various components in the system:

- Two IPFEs, IPFE-A1 and IPFE-A2, each responsible for one Target Set Address. IPFE-A1 is primary for TSA1, and IPFE-A2 is primary for TSA2.
- Two Target Sets, each with three application servers and the Target Set Addresses TSA1 and TSA2.
  - TSA1 has application servers Server1, Server2, and Server3
  - TSA2 has application servers Server4, Server5, and Server6
- Two clients, each configured with TSA1 and TSA2.

These failure and recovery scenarios apply to a single component outage.

IPFE failure and recovery

If IPFE-A1 fails, the system handles it in the following manner:

- IPFE-A1's mate, IPFE-A2, detects the failure.

- IPFE-A2 takes over IPFE-A1's TSA, TSA1.
- There are no changes to the application servers in TSA1. TSA1 continues to comprise Server1, Server2, and Server3
- Traffic for TSA1 continues to go to TSA1, which is now managed by IPFE-A2
- IPFE-A2 continues to route TSA1 traffic to Server1, Server2, and Server3 - no different than they were before the failure.
- IPFE-A2 also continues to route traffic for TSA2 to Server4, Server5, and Server6.
- No disruption of service occurs.
- New connection requests for TSA1 will be routed to Server1, Server2 or Server3.
- New connection requests for TSA2 will be routed to Server4, Server5 or Server6.

When IPFE-A1 recovers, the following happens:

- IPFE-A2 detects that IPFE-A1 has recovered and relinquishes control of TSA1.
- IPFE-A1 assumes control of TSA1.
- Traffic that went to TSA1 continues to go to TSA1.
- The clients are unaware that a recovery has occurred.
- New connection requests for TSA1 continue to be routed to Server1, Server2, or Server3.
- New connection requests for TSA2 continue to be routed to Server4, Server5, or Server6.

Application server failure and recovery

When an application server, say Server1, fails, the following occurs:

- The connections from the client will also fail.
- Other connections through TSA1 to Server2 and Server3 will survive.
- Clients who were sending traffic to the failed application server must send traffic to their secondary TSA (TSA2).
- IPFE-A1 will route new connection requests to the remaining application servers (Server2 and Server3). If all application servers in a target set fail, and IPFE-A1 receives a request for a new connection to TSA1, it will optionally notify the client that the request cannot be fulfilled, using either a TCP RST packet (for TCP connections), or a configurable ICMP message.

When Server1 recovers:

- IPFE-A1 will detect Server1's availability.
- IPFE-A1 will route new connection requests to Server1.
- Some imbalance across application servers in TSA1 will exist after recovery. IPFE-A1 will monitor for imbalances in traffic and distribute new connections to reduce the imbalance.

Enclosure failure and recovery

In the enclosure failure scenario we assume that the IPFE is colocated with the application servers in its Target Set. In this case, IPFE-A1 is in an enclosure with Server1, Server2, and Server3.

When the enclosure containing IPFE-A1, Server1, Server2, and Server3 fails:

- All connections to all servers in the enclosure will fail.
- IPFE-A2 will detect that IPFE-A1 is down and start servicing TSA1.
- Clients with existing connections to TSA1 will detect that TSA1 is unavailable and send traffic to TSA2.

- Depending on configuration, IPFE-A2 will send optionally send a TCP RST (for TCP connections) or a configured ICMP message in response to client connection requests to TSA1.

When the enclosure recovers:

- IPFE-A2 will detect that IPFE-A1 has recovered and relinquish control of TSA1.
- IPFE-A1 will take over control of TSA1.
- Since TSA1 did not have any existing connections during the failure, no special handling of existing connections is required.
- Over a period of time, clients are expected to route new connections to TSA1, resulting in connections to recovered servers in the associated Target Set.
- In the interim, there will be a substantial imbalance between the two IPFEs as well as between the servers in the two TSAs. The IPFEs will monitor the traffic for imbalances and distribute new connections to reduce the imbalance.

External connectivity failure and recovery

If external connectivity to the IPFE, say IPFE-A1, fails:

- Connections to IPFE-A1 and TSA1 fail.
- IPFE-A2 will not take over TSA1 since it sees IPFE-A1 as available. That is, internal connections still work.
- Clients with failed connections to TSA1 must send traffic to TSA2.
- Clients attempting to create new connections to TSA1 will fail.
- IPFE-A2 and TSA2 will carry all the traffic for all the clients.

When external connectivity is restored:

- There will be no existing connections for TSA1 to handle.
- IPFE-A1 will still retain control over TSA1.
- Clients will route new connections to TSA1 over time.
- In the interim, there will be a substantial imbalance between the two IPFEs as well as between the servers in the two TSAs. The IPFEs will monitor the traffic for imbalances and distribute new connections to reduce the imbalance.

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 imust 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 IPFEConfigurationTarget Sets page allows you to assign a list of application server IP addresses to a Target Set and associate the Target Set with an IPFE pair.

Chapter 11

IPsec

Topics:

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

IPsec Overview

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

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

IPsec will work for both IPv4 and IPv6.

Note: DSR Release 4.0 supports IPsec with an SCTP/IPv6 configuration.

Note: DSR Release 4.0 does not support IPsec for IP Front End (IPFE) connections.

Encapsulating Security Payload

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

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

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

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

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

Internet Key Exchange

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

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

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

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

IP Compression

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

IPsec Process

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

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

IKE operates in two phases.

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

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

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

IPsec Setup

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

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

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

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

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

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

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

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

IPsec IKE and ESP elements

Table 19: IPsec IKE and ESP elements describes IPsec IKE and ESP configuration elements and provides default values, if applicable.

Table 19: IPsec IKE and ESP elements

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

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

Accessing platcfg

To work with IPsec you need to use the 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.el5prerel4.2.3_70.83.0 on an x86_64
```

```
cfg1-CMP-a login:
```

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

   The platcfg **Main Menu** appears.

Adding an IPsec connection

Use this task to add an IPsec connection.

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

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

Editing an IPsec connection

Use this task to edit an IPsec connection.

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

Enabling and Disabling an IPsec Connection

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

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

1. Open platcfg.
   See *Accessing platcfg*.
2. Select Network Configuration.
3. Select IPsec Configuration.
4. Select IPsec Connections.
5. Select Edit.
6. Select Connection Control.

7. Select the IPsec connection to enable or disable.
8. Select Enable or Disable.
9. Click OK to enable or disable the selected IPsec connection.
10. Log out of platdfg.
    See *Logging out of platcfg*.

Deleting an IPsec connection

Use this task to delete an IPsec connection.

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

Logging out of platcfg

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

1. If you have not already done so, select Exit on the final menu of the IPsec task that you were using for the IPsec connection.
2. To log out of the management server, enter exit at the prompt.
   ```
   # exit
   cfg1-CMP-a login:
   ```
3. To end the vsp session, press ESC, then Shift-9.
   ```
   cfg1-CMP-a login: </>hpiLO->
   </>hpiLO->
   ```
4. To log out of the management server iLO, enter exit.
   ```
   </>hpiLO-> exit
   ```

Chapter 12

Diameter Intelligence Hub

Topics:

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. The DIH includes:

- A web GUI that provides security, configuration, and application access
- Probeless monitoring and network intelligence data collection and monitoring
- Troubleshooting capabilities, including nodal tracing and message decoding
- Alarm forwarding for signaling and system alarms
- A self surveillance diagnostic utility
- Data feed for Diameter (S6) xDRs

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 13

Database Backups and Restores

Topics:

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 transfered 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 transfered 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.

Appendix A

DSR Configuration Elements

Topics:

The tables in this appendix describe the elements that can be configured for the Diameter protocol and DSR applications.

Diameter Configuration Elements

The tables in this section describe the elements that can be configured using the Diameter GUI pages in the DSR software.

Application Ids elements

Table 20: Application Ids elements describes the fields on the **Application Ids** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 20: Application Ids elements

Element	Description	Data Input Notes
Application Id	Used to identify a specific Diameter Application. The Application Id value is placed in the Application Id AVP. The Application Id field is required, must be unique, and cannot be edited after it is created. The Internet Assigned Numbers Authority lists standard and vendor-specific Application Ids on their iana.org website, On the website: • Select Protocol Assignments • Scroll to locate the Authentication, Authorization, and Accounting (AAA) Parameters heading • Select Application IDs under the heading	Format: numeric; maximum 10 digits Range: • 1-16777215 for Standard Application Ids • 16777216-4294967294 for Vendor-specific Application Ids • 4294967295 for Relay
Name	Application Id Name	Format: case-sensitive; alphanumeric and underscore Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha
Peer Route Table	The Peer Route Table associated with the Diameter Application.	Format: scrollable list

Element	Description	Data Input Notes
	The Peer Route Table contains Peer Routing Rules used to route messages that contain the Application Id.	Range: available Peer Route Tables Default: none
Routing Option Set	The Routing Option Set associated with the Diameter Application. Routing Option Sets contain information used to handle delivery error conditions.	Format: scrollable list Range: available Routing Option Sets Default: none
Pending Answer Timer	The Pending Answer Timer associated with the Diameter Application.	Format: scrollable list Range: available Pending Answer Timers Default: none

Command Codes elements

Table 21: Command Codes elements describes the fields on the **Command Codes** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 21: Command Codes elements

Field (* indicates a required field)	Description	Data Input Notes
* Name	Command Code Name	Format: case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters
* Command Code	Identifies the command associated with the message	Format: Pulldown menu or numeric Range: Select from predefined Command Codes or enter a numeric value: 0-16777215 Default: none

Local Node configuration elements

Table 22: Local Node Configuration Elements describes the fields on the Local Nodes View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 22: Local Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Local Node Name	Unique name of the Local Node.	Format: string, case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters
* Realm	Realm of the Local Node; defines the administrative domain with which the user maintains an account relationship.	Format: string consisting of a list of labels separated by dots. A label can contain letters, digits, dash (-), and underscore (_). A label must begin with a letter, digit, or underscore, and must end with a letter or digit. Underscore can be used only as the first character. Range: Realm - up to 255 characters; label - up to 63 characters
* FQDN	Unique Fully Qualified Domain Name; specifies exact location in the tree hierarchy of the DNS.	Format: string consisting of a list of labels separated by dots. A label must contain letters, digits, dash (-), and underscore (_). A label must begin with a letter or underscore, and must end with a letter or digit. Underscore can be used only as the first character. Range: FQDN - up to 255 characters; label - up to 63 characters
SCTP Enabled	Enables the Local Node to listen for SCTP connections	Format: check box

Field (* indicates required field)	Description	Data Input Notes
		Range: checked, unchecked Default: checked
SCTP Listen Port	SCTP listen port number for the Local Node. The SCTP Enabled box must be checked before a value can be entered in this field. This SCTP Listen Port cannot be the same as a Local Initiate Port of a connection.	Format: numeric Range: 1024 - 65535 Default: 3868
TCP Enabled	Enables the Local Node to listen for TCP connections	Format: check box Range: checked, unchecked Default: checked
TCP Listen Port	TCP listen port number for the Local Node. The TCP Enabled box must be checked before a value can be entered in this field. This TCP Listen Port cannot be the same as a Local Initiate Port of a connection.	Format: numeric Range: 1024 - 65535 Default: 3868
* Connection Configuration Set	Connection Configuration Set for the Local Node.	Format: pulldown list Range: configured Connection Configuration Sets, "Default" Connection Configuration Set
* CEX Configuration Set	CEX Configuration Set associated with the Local Node. The entries in the CEX Configuration Set field create links to the **Diameter > Configuration > CEX Configuration Sets (Filtered)** page, which shows only the selected entry. The CEX Configuration Set field for the Local Node is used if the CEX Configuration Set is not associated with the connection.	Format: pulldown list Range: configured CEX Configuration Sets, "Default" CEX Configuration Set.
* IP Addresses	IP address, or addresses, available for establishing Diameter transport connections to the Local Node. You must assign at least one IP Address, and can	Format: 128 pulldown lists Range:

Field (* indicates required field)	Description	Data Input Notes
	assign up to 128 IP addresses, to a Local Node. Up to 32 IP addresses can be IPFE target set addresses. If fewer than four XSI interfaces are configured and SCTP transport is selected, then the number of IP Addresses selected must be the same as the number of XSI interfaces.	• For a DSR that has Active/Standby DA-MPs: available Virtual Signaling IP Addresses provisioned as MP server group VIP • For a DSR that has Multiple-Active DA-MPs: static IP addresses configured for each DA-MP • configured IPFE TSAs

Peer Node configuration elements

Table 23: Peer Node Configuration Elements describes the fields on the Peer Nodes View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 23: Peer Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Peer Node Name	Unique name of the Peer Node.	Format: string, case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters
* Realm	Realm of the Peer Node.	Format: string consisting of a list of labels separated by dots. A label must contain letters, digits, dash (-), and underscore (_). A label must begin with a letter or underscore, and must end with a letter or digit. Underscore can

Field (* indicates required field)	Description	Data Input Notes
		be used only as the first character. Range: up to 255 characters; label - up to 63 characters
* FQDN	Unique Fully Qualified Domain Name; specifies exact location in the tree hierarchy of the DNS.	Format: string consisting of a list of labels separated by dots. A label must contain letters, digits, dash (-), and underscore (_). A label must begin with a letter or underscore, and must end with a letter or digit. Underscore can be used only as the first character. Range: FQDN - up to 255 characters; label - up to 63 characters
SCTP Enabled	Enables the Peer Node to listen for SCTP connections.	Format: check box Range: checked, unchecked Default: checked
SCTP Listen Port	SCTP Listen Port Number for the Peer Node. The SCTP Enabled box must be checked before a value can be entered in this field.	Format: numeric Range: 1024 - 65535 Default: 3868
TCP Enabled	Enables the Peer Node to listen for TCP connections.	Format: check box Range: checked, unchecked Default: checked
TCP Listen Port	TCP Listen Port Number for the Peer Node. The TCP Enabled box must be checked before a value can be entered in this field.	Format: numeric Range: 1024 - 65535 Default: 3868

Field (* indicates required field)	Description	Data Input Notes
IP Addresses	IP address, or addresses, available for establishing Diameter transport connections to the Peer Node. View - Each Peer Node entry displays a + sign and the number of IP Addresses assigned to that Peer Node. Click the + sign to display the IP Addresses; the + sign changes to a - sign. Click the - sign to display the number again. [Insert] and [Edit] - The field contains an Add button that can be clicked up to 127 times to create 128 text boxes for IP Addresses. Each entry is numbered, to indicate the number of IP Addresses that have been added.	Format: numeric Range: up to 128 valid IP Addresses
Alternate Implicit Route	Route List to use for routing messages to this Peer Node if all Peer Routing Rules and implicit Peer Routes are unavailable. Each entry in the Alternate Implicit Route column on the View page is a link to the **Diameter Configuration Route List [Filtered]** page for the selected entry only.	Format: pulldown list Range: configured Route Lists
Replace Dest Realm	If checked, the Destination Realm AVP of outgoing messages will be overwritten with this Peer Node Realm.	Format: check box Range: checked, unchecked Default: unchecked
Replace Dest Host	If checked, the Destination Host AVP of outgoing messages will be overwritten with this Peer Node FQDN.	Format: check box Range: checked, unchecked Default: unchecked
* Minimum Connection Capacity	The minimum number of connections that must be available to this Peer in order for it to be "Available". Otherwise, the Peer is "Degraded" if fewer than the minimum number of connections are "Available", or "Unavailable" if no connections are "Available".	Format: numeric Range: 1-64 Default: 1
* Maximum Alternate Routing Attempts	The maximum number of times that a Request can be rerouted to this Peer before the next eligible Peer is selected.	Format: numeric Range: 1-4 Default: 4

Field (* indicates required field)	Description	Data Input Notes
Alternate Routing On Connection Failure	Indicates whether to perform alternate routing on alternate connections to the same Peer before selecting the next eligible Peer of a Peer Route Group, when a connection failure occurs.	Format: radio buttons Range: Same Peer, Different Peer Default: Different Peer
Alternate Routing On Answer Timeout	Indicates whether to perform alternate routing on the same connection or on alternate connections to the same Peer before selecting the next eligible Peer of a Peer Route Group, when an Answer Timeout occurs.	Format: radio buttons Range: Same Peer, Different Peer, Same Connection Default: Different Peer
Alternate Routing On Answer Result Code	Indicates whether to perform alternate routing on alternate connections to the same Peer before selecting the next eligible Peer of a Peer Route Group, when a reroute on Answer Result Code occurs. For an Answer response received from a DAS Peer, alternate routing on Answer Result Code is determined by the Diameter > Configuration > System Options > Message Copy Options > DAS Message Copy Answer Result Code parameter.	Format: radio buttons Range: Same Peer, Different Peer Default: Different Peer
Peer Route Table	The Peer Route Table associated with the Peer Node. The Peer Route Table contains Peer Routing Rules used to route messages from the Peer Node.	Format: pulldown menu Range: available Peer Route Tables Default: none
Routing Option Set	The Routing Option Set associated with the Peer Node. Routing Option Sets contain information used to handle delivery error conditions.	Format: pulldown menu Range: available Routing Option Sets Default: none
Pending Answer Timer	The Pending Answer Timer associated with the Peer Node.	Format: pulldown menu Range: available Pending Answer Timers Default: none

Field (* indicates required field)	Description	Data Input Notes
Message Priority Setting	Defines the source of Message Priority for a request message arriving on a Connection associated with the Peer Node. The Message Priority setting for the Connection takes precedence over the Message Priority setting for the Peer Node. Possible settings are: • None - use the Default Message Priority Configuration Set • Read from Request Message - read the message priority from the ingress request • User Configured - Apply the user configured Message Priority Configuration Set	Format: radio buttons Range: None, Read from Request Message, User Configured Default: None
Message Priority Configuration Set	The Message Priority Configuration set used if Message Priority Setting is User Configured	Format: pulldown list Range: available Message Priority Configuration Sets Default: None

Connection Configuration Set elements

Table 24: Connection Configuration Sets Elements describes the fields on the Connection Configuration Sets View, Edit, and Insert pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 24: Connection Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Connection Configuration Set Name	Unique Name of the Connection Configuration Set.	Format: case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot start with a digit Range: 1 - 32 characters
SCTP Options		
* Retransmit Initial Timeout (ms)	Expected average network round-trip time in milliseconds. This is used to initialize the	Format: numeric; milliseconds

Field (* indicates required field)	Description	Data Input Notes
	round-trip time value when an association is started but the round-trip time has not yet been measured. The round-trip time is used by SCTP in calculating when to retransmit chunks.	Range: 10 - 5000 Default: 120
* Retransmit Minimum Timeout (ms)	Minimum amount of time to wait for an acknowledgment for a message sent. This value prevents the retransmit timeout from becoming too small in networks with a very short round-trip time.	Format: numeric; milliseconds Range: 10 - 5000 Default: 120
* Retransmit Maximum Timeout (ms)	Maximum amount of time to wait for an acknowledgment for a message sent. This value places an upper bound on the exponential back-off algorithm used by SCTP for retransmission timing. After this retransmit interval is reached, retransmits will be sent at a constant rate until an ACK is received or the maximum attempts is reached.	Format: numeric; milliseconds Range: 10 - 10000 Default: 120
* Retransmit Maximum Timeout for INIT	Maximum amount of time to wait for an INIT to be acknowledged. This value overrides the Retransmit Maximum Timeout for INITs and is used to bound the initial setup time. A value of 0 indicates that the Retransmit Maximum Timeout will be used for INITs as well.	Format: numeric; milliseconds Range: 0, 10 - 10000 Default: 120
* Number of Retransmits Triggering Path Failure	Number of consecutive unsuccessful retransmits that will cause a path of the SCTP association to be marked as failed. This value indicates how many SCTP retransmission attempts should be made to each destination of an SCTP association before marking the destination as failed. This value must be less than the Number of Retransmits Triggering Association Failure value.	Format: numeric; number of retransmits Range: 1 - 10 Default: 3
* Number of Retransmits Triggering Association Failure	Number of consecutive retransmits that will cause an SCTP association to be marked as failed. This value indicates how many SCTP retransmission attempts should be made to all destinations for an SCTP association before marking the association as failed.	Format: numeric; number of attempts Range: 1 - 20 Default: 5

Field (* indicates required field)	Description	Data Input Notes
	This value should not be greater than the sum of the retransmit attempts for all destinations within the association.	
* Number of Retransmits Triggering Init Failure	Number of consecutive retransmits for INIT and COOKIE-ECHO Chunks that will cause an SCTP connection to be marked as failed. This value indicates how many retransmission attempts should be made to the primary SCTP address for INIT and COOKIE-ECHO Chunks before marking the connection as failed.	Format: numeric; number of attempts Range: 1 - 20 Default: 8
* SACK Delay	The number of milliseconds to delay after receiving a DATA Chunk and prior to sending a SACK. A non-zero value for SACK Delay gives the application time to bundle DATA Chunks in the same SCTP datagram with the SACK, thereby reducing the number of packets in the network. Setting SACK Delay to zero disables this delay so that SACKs are sent as quickly as possible.	Format: numeric; milliseconds Range: 0 - 200 Default: 10
* SCTP Heartbeat Interval	The number of milliseconds between sending SCTP HEARTBEAT messages to a Peer. Heartbeat messages are sent only when no user data has been sent for the duration of the Heartbeat Interval. Setting the Heartbeat Interval to 0 disables heartbeating (not recommended).	Format: numeric; milliseconds Range: 0, 100 - 300000 Default: 500
* Socket Send Buffer Size (bytes)	Socket send buffer size for outgoing SCTP messages. The send buffer size must be greater than or equal to the product of the bandwidth and the round trip delay for the association.	Format: numeric; number of bytes Range: 8000 - 5000000 Default: 2000000
* Socket Receive Buffer Size (bytes)	Socket receive buffer size for incoming SCTP messages. The receive buffer size must be greater than or equal to the product of the bandwidth and the round trip delay for the association.	Format: numeric; number of bytes Range: 8000 - 5000000 Default: 2000000
* Maximum Burst	Specifies the maximum burst of packets that can be emitted by this association.	Format: numeric

Field (* indicates required field)	Description	Data Input Notes
		Range: 1 - 4 Default: 4
* Max Number of Inbound Streams	Maximum number of inbound SCTP streams supported locally by the SCTP connection.	Format: numeric; number of streams Range: 1 -16 Default: 8
* Max Number of Outbound Streams	Maximum number of outbound SCTP streams supported locally by the SCTP connection.	Format: numeric; number of streams Range: 1 -16 Default: 8
Datagram Bundling Enabled	If checked, datagram bundling is enabled for the SCTP connection.	Format: check box Range: checked (YES) or unchecked (NO) Default: checked
Diameter Options		
* Connect Timer (sec)	Controls the frequency that transport connection attempts are done to a Peer where no active transport connection exists. Applicable only for connections that are configured to initiate a connection with a Peer Node.	Format: numeric; seconds Range: 5 - 60 Default: 30
* Watchdog Timer Init Value (sec)	Initial value of the application watchdog timer.	Format: numeric; seconds Range: 1 - 30 Default: 30
* Capabilities Exchange Timer (sec)	Time to wait on a CER message from a Peer after a connection is initiated by the Peer. Time to wait on a CEA response from a Peer after sending the CER.	Format: numeric; seconds Range: 1 - 10 Default: 3
* Disconnect Timer (sec)	After sending a DPA message, time to wait for a Peer to disconnect transport. After sending a DPR message, time to wait for the Peer to send the DPA.	Format: numeric; seconds Range: 1 - 10

Field (* indicates required field)	Description	Data Input Notes
	If the timer expires, transport will be disconnected by the application.	Default: 3
Proving Mode	Proving mode for the Configuration Set.	Format: radio buttons Range: Suspect, Always Default: Suspect
* Proving Timer (msec)	The time to wait for a Peer to send a DWA message in response to a DWR message during connection proving.	Format: numeric; milliseconds Range: 50 - 30000 Default: 500
* Proving Times	The number of consecutive DWR and DWA exchanges within Proving Timer time during connection proving.	Format: numeric; number of exchanges Range: 1 - 1000 Default: 3
* Pending Transactions Per Connection	The maximum number of Pending Requests waiting for Answers from the Peer on this connection. If the maximum is reached, this connection will not be selected for routing until the number of Pending Requests falls below this value.	Format: numeric Range: 1 - 20000 Default: 1000
TCP Options		
Nagle Enabled	If checked, the Nagle algorithm is enabled for the TCP connection.	Format: check box Range: checked (YES), unchecked (NO) Default: checked
* Socket Send Buffer Size (bytes)	Socket send buffer size for outgoing TCP messages. The send buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the connection.	Format: numeric; bytes Range: 8000 - 5000000 Default: 2000000
* Socket Receive Buffer Size (bytes)	Socket receive buffer size for incoming TCP messages. The receive buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the connection.	Format: numeric; bytes Range: 8000 - 5000000 Default: 2000000

Capacity Configuration Set elements

This table describes the fields on the Capacity Configuration Sets View, Edit, and Insert pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 25: Capacity Configuration Sets Elements

Field (* indicates field is required)	Description	Data Input Notes
* Capacity Configuration Set	Name of the Capacity Configuration Set. The Name must be unique.	Format: String: case-sensitive; alphanumeric and underscore (_); must contain at least one alpha; cannot begin with a digit. Range: 1 - 32 characters
* Reserved Ingress MPS	Rate in messages per second for which resources are explicitly reserved for Diameter connections using this Capacity Configuration Set to process ingress Diameter signaling. These resources cannot be used by any other connection, regardless of the load offered to other connections. The sum of Reserved Ingress MPS for all connections on an MP server cannot exceed the maximum capacity of the MP server.	Format: numeric Range: 0, 10 - 5000 Ingress messages per second Default: 0
* Maximum Ingress MPS	Maximum Ingress messages per second that a Diameter connection using this Capacity Configuration Set is allowed to process. * The Maximum Ingress MPS must be equal to or greater than the Reserved Ingress MPS. Any difference between the Maximum Ingress MPS and the Reserved Ingress MPS represents MP server resources that are shared among connections that have Maximum Ingress MPS greater than Reserved Ingress MPS.	Format: numeric Range: 10 - 5000 Ingress messages per second Default: 5000
* Ingress MPS Minor Alarm Threshold (Percent)	Percentage of Maximum Ingress MPS at which a minor alarm will be raised for connections that use this Capacity Configuration Set. After an alarm is raised, it will not be cleared until the average Ingress MPS falls 5% below this value.	Format: numeric Range: 10 - 99 percent Default: 50 percent

Field (* indicates field is required)	Description	Data Input Notes
	The Ingress MPS Minor Alarm Threshold must be less than the Ingress MPS Major Alarm Threshold.	
* Ingress Major Alarm Threshold (Percent)	Percentage of Maximum Ingress MPS at which a major alarm will be raised for connections that use this Capacity Configuration Set. After an alarm is raised, it will not be cleared until the average Ingress MPS falls 5% below this value. The Ingress MPS Major Alarm Threshold must be grerater than the Ingress MPS Minor Alarm Threshold.	Format: numeric Range: 11 - 100 percent Default: 80 percent

CEX Parameters elements

Table 26: CEX Parameters elements describes the fields on the **CEX Parameters** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 26: CEX Parameters elements

Field (* indicates a required field)	Description	Data Input Notes
* Application Id	Used to identify a specific Diameter Application. The Application Id value is placed in the Application Id AVP.	Format: pulldown menu Range: configured Application Ids • 1-16777215 for Standard Application Ids • 16777216-4294967294 for Vendor-specific Application Ids • 4294967295 for Relay
Application Id Type	Type of Application Id.	Format: radio buttons Range: Authentication, Accounting
Vendor-Specific Application Id	If checked, the Vendor Id and the Application Id will be grouped in a Vendor-specific Application Id AVP.	Format: check box Range: checked, unchecked Default: unchecked

Field (* indicates a required field)	Description	Data Input Notes
Vendor Id	A Vendor Id value for this Vendor-Specific Application Id. The Vendor Id is placed in the Vendor Id AVP. The Vendor-Specific Application Id check box must be checked before a value can be entered in this field.	Format: numeric; maximum 10 digits Range: 1-4294967295

CEX Configuration Set elements

Table 27: Configuration Sets Elements describes the fields on the CEX Configuration Sets View, Edit, and Insert pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 27: Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
* CEX Configuration Set Name	Unique Name of the CEX Configuration Set. A CEX Configuration Set named Default is always available.	Format: Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
* CEX Parameters	Available CEX Parameters All unique configured CEX Parameters, showing Application Ids with Application Type, and with Vendor Id if the Application Id is Vendor-Specific.	Format: Scrollable list Range: All configured CEX Parameters
	Selected CEX Parameters CEX Parameters that are selected from the Available CEX Parameters list for this CEX Configuration Set.	Maximum of 10 entries. Default: Relay
	Must Include CEX Parameters CEX Parameters selected from the Selected CEX Parameters list that must be present in the CEx message exchanged from the Peer.	One, some, or all of the entries in the Selected CEX Parameters list; maximum of 10 entries

Field (* indicates a required field)	Description	Data Input Notes
Supported Vendor Ids	Available Supported Vendor Ids All unique Vendor Ids that have been configured in the CEX Parameters configuration.	Format: Scrollable list Range: All configured Vendor Ids
	Selected Supported Vendor Ids Application Ids that are selected from the Available Supported Vendor Ids list for this CEX Configuration Set.	Maximum of 10 entries

Message Priority Configuration Set elements

Table 28: Message Priority Configuration Set Elements describes the fields on the Message Priority Configuration Sets View, Edit, and Insert pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 28: Message Priority Configuration Set Elements

Field (* indicates a required field)	Description	Data Input Notes
* Message Priority Configuration Set Name	Unique name of the Message Priority Configuration Set.	Format: Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
* Message Priority Rules	The number of Message Priority Rules defined in the Message Priority Configuration Set	
Application Id	The Application Id used to filter incoming Diameter messages	Format: scrollable list Range: configured Application Ids. An asterisk (*) matches any Application Id.
Application Name	The name of the application associated with the Application Id	
Command Code	The Command Code used to filter incoming Diameter messages.	Format: scrollable list Range: configured Command Codes. An asterisk (*) matches any Command Code.

Field (* indicates a required field)	Description	Data Input Notes
Command Code Name	The name of the command associated with the Command Code	
Priority	The message priority assigned to incoming messages that match the combination of Application Id and Command Code.	Format: pull down list Range: 0-2

Egress Message Throttling Configuration Set elements

Egress Message Throttling Configuration Set elements describes the fields on the Egress Message Throttling Configuration Sets View, Edit, and Insert pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 29: Egress Message Throttling Configuration Set Elements

Field (* indicates required field)	Description	Data Input Notes
* Egress Message Throttling Configuration Set	Name of the Egress Message Throttling Configuration Set. The name must be unique.	Format: case-sensitive; alphanumerica and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters
* Max Egress Message Rate	The maximum Egress Message Rate (EMR) on the connection	Format: numeric Range: 10 -10000
* Throttle Threshold 1	Threshold for Congestion Level 1. When the EMR exceeds this percentage of Max EMR, the Congestion Level is set to 1	Format: numeric Range: 0 - 100% Default: 100%
* Abatement Threshold 1	Abatement Threshold for Congestion Level 1. When the EMR falls below this percentage of Max EMR, the Congestion Level returns to 0.	Format: numeric Range: 0 - 100% Default: 80%
Throttle Threshold 2	Threshold for Congestion Level 2. When the EMR exceeds this percentage of Max EMR, the Congestion Level is set to 2	Format: numeric Range: 0 - 100% Default: none
Abatement Threshold 2	Abatement Threshold for Congestion Level 2. When the EMR falls below this percentage of Max EMR, the Congestion Level returns to 1.	Format: numeric Range: 0 - 100% Default: none

Field (* indicates required field)	Description	Data Input Notes
Throttle Threshold 3	Threshold for Congestion Level 3. When the EMR exceeds this percentage of Max EMR, the Congestion Level is set to 3	Format: numeric Range: 0 - 100% Default: none
Abatement Threshold 3	Abatement Threshold for Congestion Level 3. When the EMR falls below this percentage of Max EMR, the Congestion Level returns to 2.	Format: numeric Range: 0 - 100% Default: none
* Smoothing Factor	Percentage contribution of the current EMR sample to the Smoothed EMR	Format: numeric Range: 20 - 80% Default: 50%
* Abatement Time	The amount of time a throttled connection's Smoothed EMR must remain below an abatement threshold before the Congestion Level is lowered.	Format: numeric Range: 200 - 10000 milliseconds Default: 500 milliseconds

Connection configuration elements

Table 30: Connections Configuration Elements describes the fields on the Connections View, Edit, and Insert pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 30: Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Connection Name	Name of the connection. The name must be unique in the system.	Format: alphanumeric and underscore (_). Cannot start with a digit and must contain at least one alpha (A-Z, a-z). The name is case-sensitive. Range: 1 - 32 characters
Transport Protocol	Type of transport protocol used by this connection. The selected transport protocol must be supported by both the associated Local Node and Peer Node.	Format: radio buttons Range: SCTP, TCP Default: SCTP
* Local Node	Local Node associated with the connection.	Format: pulldown list

Field (* indicates required field)	Description	Data Input Notes
	The Local Node must use the same Transport Protocol as the Peer Node. The entries in the Local Node field are links to the **Diameter > Configuration > Local Nodes (Filtered)** page which shows only the selected entry. If two IP addresses are configured for the Local Node, it is recommended that a Secondary IP Address be configured for the Peer Node. The peer's Secondary IP address is used as a fallback for the initiation of the SCTP connection establishment if the peer's primary IP address is unreachable, as well as for the validation of the IP addresses advertised by the peer in the INIT/INIT_ACK SCTP chunk. **Note:** It is recommended that separate Local Nodes be used for unihomed and multihomed SCTP connections.	Range: all configured Local Nodes
* Connection Mode	The connection can have one of the following connection modes: • Initiator Only - indicates that the Local Node will initiate the connection to the Peer Node. • Responder Only - indicates that the Local Node will only respond to the connection initiated from the Peer Node. The Local Initiate Port field is not available when the Responder Only value is selected here. • Initiator & Responder - indicates that the Local Node will initiate a connection to the Peer Node and respond to connection initiations from the Peer Node. The Connection Mode must be the same for all connections to the same Peer. For UNIHOMED connections, • If the Connection Mode is Initiator & Responder and Peer Node Identification is set to IP Address for any connections to the Peer, then the following combination must be unique for each connection to the Peer: Peer FQDN (from Peer Nodes configuration), Peer Realm (from Peer Nodes configuration), Transport Protocol, Local IP, Local Listen Port (from Local Nodes configuration), "Must	Format: pulldown list Range: Initiator Only, Responder Only, Initiator & Responder Default: Initiator & Responder

Field (* indicates required field)	Description	Data Input Notes
	Include" Application Ids in the CEX Configuration Set. • If the Connection Mode is Initiator & Responder and Peer Node Identification is Transport FQDN or Peer Diameter Identity FQDN for at least one connection to the Peer, then the following combination must be unique for each connection to the Peer: Peer FQDN (from Peer Nodes configuration), Peer Realm (from Peer Nodes configuration), Transport Protocol, Local IP, Local Listen Port (from Local Nodes configuration), "Must Include" Application Ids in the CEX Configuration Set. • The connection Local IP Address and Local initiate Port combination cannot be the same as the Local IP Address and Listen Port combination of one of the Local Nodes or of another connection. For MULTIHOMED connections, • If the Connection Mode is Initiator & Responder and Peer Node Identification is set to IP Address for any connections to the Peer, then the following combination must be unique for each connection to the Peer: Peer FQDN (from Peer Nodes configuration), Peer Realm (from Peer Nodes configuration), Transport Protocol, Local IP Pair, Local Listen Port (from Local Nodes configuration), "Must Include" Application Ids in the CEX Configuration Set. • If the Connection Mode is Initiator & Responder and Peer Node Identification is Transport FQDN or Peer Diameter Identity FQDN for any connections to the Peer, then the following combination must be unique for each connection to the Peer: Peer FQDN (from Peer Nodes configuration), Peer Realm (from Peer Nodes configuration), Transport Protocol, Local IP Pair, Local Listen Port (from Local Nodes configuration), "Must Include" Application Ids in the CEX Configuration Set. • If the Connection Mode is Initiator & Responder and Transport FQDN is NOT specified in any connections to the Peer, then the following combination must be unique for each connection the the Peer: Transport FQDN,	

Field (* indicates required field)	Description	Data Input Notes
	Peer Realm, Transport Protocol, Local IP Pair, Remote IP Pair, Local Listen Port, "Must Include" Application Ids. • The connection Local IP Address pair and Local Initiate Port combination cannot be the same as the Local IP Address pair and Listen Port combination of one of the Local Nodes or of another connection.	
Local Initiate Port	The IP source port number to be used when the connection is an Initiator. This field is not available and is set to Blank when the Connection Mode is Responder Only.	Format: numeric Range: 1024-65535 Default: Blank
IP Owner	Indicates the source of the IP Address. Possible values are: • For VIP addresses, the string "VIP" • For static IP addresses, the MP Server Hostname of the DA-MP that owns the Local IP address • For TSAs, the name of the Target Set to which the Local IP address corresponds, for example "TSA1". The IP Owner field appears only on the Connections View page.	
* Primary Local IP Address	The IP address to be used as Primary Local IP Address for this connection. Each IP address in the pulldown list has an identifying tag appended to it, as follows: • In Active/Standby DA-MP NEs, a DA-MP VIP is appended with (VIP). • In Multiple-Active DA-MP NEs, a static IP address owned by the DA-MP is appended with the Server Hostname of the DA-MP, for example, (DA-MP1). • IPFE Target Set Addresses are appended with the Target Set Name, for example, (TSA1). A Local Node must be selected before the list becomes available.	Format: pulldown list Range: all configured IP addresses for the selected Local Node
Secondary Local IP Address	The IP address to be used as the Secondary Local IP Address for this connection.	Format: pulldown list

Field (* indicates required field)	Description	Data Input Notes
	A Local Node must be selected and the selected Transport Protocol must be SCTP before the list becomes available. This address is used only for SCTP Multi-homing; it must be different from the selected Primary Local IP Address.	Range: all configured IP addresses for the selected Local Node
* Peer Node	Peer Node associated with the connection. The Peer Node must use the same IP protocol as the Local Node. The entries in the Peer Node field are links to the **Diameter > Configuration > Peer Nodes (Filtered)** page which shows only the selected entry.	Format: pulldown list Range: all configured Peer Nodes
Peer Node Identification	Specifies whether the Peer Node is identified by one or more IP addresses, a Transport FQDN, or a Peer Diameter Identity FQDN. FQDNs are used for DNS lookup. If no IP Address has been selected and no Transport FQDN has been specified, then the only acceptable choice is Peer Diameter identity FQDN. The FQDN configured for the connection takes precedence over the Peer's Diameter Identity FQDN. • If the Peer Node Identification is set to IP Address, then the Transport FQDN field cannot be changed and the Peer IP Address pulldown lists are available. • If the Peer Node Identification is set to Transport FQDN, then the Peer IP Address pulldown lists are not available and the Transport FQDN field can be changed. • If the Peer Node Identification is set to Peer Diameter Identity FQDN, then both the Transport FQDN field and the Peer IP Address pulldown lists are not available	Format: radio buttons Range: IP Address, Transport FQDN, Peer Diameter Identity FQDN Default: IP Address
Primary Peer IP Address	The Primary Peer IP Address of this connection. A Peer Node must be selected before the pulldown list becomes available.	Format: pulldown list Range: available IP addresses
Secondary Peer IP Address	The Secondary Peer IP Address of this connection.	Format: pulldown list

Field (* indicates required field)	Description	Data Input Notes
	A Peer Node must be selected and the selected Transport Protocol must be SCTP before the pulldown list becomes available. This address is used only for SCTP Multi-homing; it must be different from the selected Primary Peer IP Address.	Range: available IP addresses
Transport FQDN	Fully Qualified Domain Name for this connection. The Transport FQDN is used for DNS lookup when Peer Node Identification is set to Transport FQDN.	Format: case-insensitive string consisting of a list of labels separated by dots. A label can contain letters, digits, dash (-), and underscore (_). A label must begin with a letter, digit, or underscore, and must end with a letter or digit. Underscore can be used only as the first character. Range: FQDN - up to 255 characters; label - up to 63 characters
* Connection Configuration Set	Connection Configuration Set associated with the connection. The entries in the Connection Configuration Set field are links to the **Connection Configuration Sets (Filtered)** page, which displays the attributes of only the selected entry.	Format: pulldown list Range: all configured Connection Configuration Sets, "Default" Connection Configuration Set.
CEX Configuration Set	CEX Configuration Set associated with the connection. The entries in the CEX Configuration Set field are links to the **CEX Configuration Sets (Filtered)** page, which shows only the selected entry.	Format: pulldown list Range: all configured CEX Configuration Sets, "Default" CEX Configuration Set.
* Capacity Configuration Set	Capacity Configuration Set associated with the connection. The Capacity Configuration Set defines reserved and maximum ingress message processing rates and alarms thresholds for this connection. The entries in the Capacity Configuration Set field are links to the **Capacity Configuration Sets**	Format: pulldown list Range: available Capacity Configuration Sets, "Default" Capacity Configuration Set

Field (* indicates required field)	Description	Data Input Notes
	(Filtered) page, which displays only the selected entry. A new connection cannot be added if it uses a Capacity Configuration Set with a non-zero Reserved Ingress MPS value that would cause the Reserved Ingress MPS total for the MP server that hosts the connection to be more than the server's Engineered Ingress MPS capacity. (See the Engineered Ingress MPS setting on the DiameterConfigurationDA-MPsMP Profiles page for the engineered capacity of the MP Server.)	Default: "Default" Capacity Configuration Set
* Transport Congestion Abatement Timeout	The amount of time spent at Egress Transport Congestion Levels 3, 2, and 1 during Egress Transport Congestion Abatement	Format: numeric Range: 3 - 60 seconds Default: 5 seconds
* Remote Busy Usage	Defines which Request messages can be forwarded on this connection after receiving a DIAMETER_TOO_BUSY response from the connection's Peer. **Disabled** The connection is not considered to be BUSY after receiving a DIAMETER_TOO_BUSY response. All Request messages continue to be forwarded to (or rerouted to) this connection. **Enabled** The connection is considered to be BUSY after receiving a DIAMETER_TOO_BUSY response. No Request messages are forwarded to (or rerouted to) this connection until the Remote Busy Abatement Timeout expires.	Format: pulldown list Range:Disabled, Enabled Default: Disabled
Remote Busy Abatement Timeout	If Remote Busy Usage is set to Enabled or Host Override, this defines the length of time in seconds that the connection will be considered BUSY from the last time a DIAMETER_TOO_BUSY response was received.	Format: numeric Range: 3 - 60 seconds Default: 5 seconds

Field (* indicates required field)	Description	Data Input Notes
Message Priority Setting	Defines the source of Message Priority for a request message arriving on the connection. Possible settings are: • None - use the Default Message Priority Configuration Set • Read from Request Message - read the message priority from the ingress request • User Configured - Apply the user configured Message Priority Configuration Set	Format: radio buttons Range: None, Read from Request Message, User Configured Default: None
Message Priority Configuration Set	The Message Priority Configuration set used if Message Priority Setting is User Configured	Format: pulldown list Range: available Message Priority Configuration Sets Default: None
Egress Message Throttling Configuration Set	Egress Message Throttling Configuration Set associated with the connection. The Egress Message Throttling Configuration Set defines the maximum Egress Message Rate and thresholds used to set the congestion level for the connection. The entries in the Egress Message Throttling Configuration Set field are links to the **Egress Message Throttling Configuration Sets (Filtered)** page, which displays only the selected entry.	Format: pulldown list Range: available Egress Message Throttling Configuration Sets Default: None
Test Mode	If checked, the connection is in Test Mode.	Format: check box Range: checked (YES), not checked (NO) Default: not checked

Route Group configuration elements

Table 31: Route Groups Configuration Elements describes the fields on the Route Groups View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 31: Route Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Route Group Name	Unique name of the Route Group.	Format: case-sensitive; alphanumeric and underscore Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha
Type	A Route Group can be provisioned with either Peer Nodes (Peer Route Group) or Connections (Connections Route Group) that have the same priority within a Route List.	Format: radio buttons Range: Peer Route Group, Connection Route Group Default: Peer Route Group
Peer Node/Connection (View)	List of Peer Nodes or Connections configured for the Route Group. Each listed Peer Node or Connection entry is a link to the **Diameter > Configuration > {Entry Type} (Filtered)** page for that entry only.	Each entry displays a + sign and the number of Peer Nodes or Connections assigned to that Route Group. Click the + sign to display the Peer Nodes or Connections; the + sign changes to a - sign. Click the - sign to display the number again.
* Peer Node, Connection, and Provisioned Capacity	One entry defined for a Route Group.	Up to 64 entries can be provisioned for a Route Group. Click the Add button to insert another entry for the Route Group.
Peer Node The Peer Node field is part of the Peer Node, Connection, and Capacity fields that are combined on the [Insert] and [Edit] pages.	A Peer Node associated with the Route Group. Each Route Group can be assigned up to 64 Peer Nodes. The Peer Node field is available when the Peer Route Group radio button is selected in the Type field. The Peer Node field is required.	Format: pulldown list Range: all configured Peer Nodes

Field (* indicates required field)	Description	Data Input Notes
Connection The Connection field is part of the Peer Node, Connection, and Capacity fields that are combined on the [Insert] and [Edit] pages.	A connection associated with the Route Group. Each Route Group can be assigned up to 64 connections. The Connection field is available when the Connection Route Group radio button is selected in the Type field and a Peer Node is selected. The Connection field is required for Connection Route Groups.	Format: pulldown list Range: all configured Connections for the selected Peer Node
Provisioned Capacity The Provisioned Capacity field is combined with the Peer Node and Connection fields on the [Insert] and [Edit] pages.	View page: Provisioned capacity for a Route Group, which is the sum total of provisioned capacity of peer nodes or connections within a Route Group. [Insert] and [Edit] pages: Provisioned capacity of a Peer Node or Connection within a Route Group. The Provisioned Capacity field is required. Traffic is distributed to available Peer Nodes/Connections in a Route Group proportional to the provisioned capacity for the Peer Node/Connection. A Peer Nodes/Connection with a higher capacity will be assigned more traffic.	Format: numeric Range: 1 - 64000

Route List configuration elements

Table 32: Route Lists Configuration Elements describes the fields on the Route Lists View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 32: Route Lists Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Route List Name	Unique name for the Route List	Format: case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters
* Minimum Route Group Availability Weight	The minimum Route Group availability weight for this Route List.	Format: numeric Range: 1 - 1024000

Field (* indicates required field)	Description	Data Input Notes
	The minimum weight is used to determine a Route Group's availability status within a Route List.	
* Route Group	Route Groups associated with the Route List. Up to three Route Groups can be associated with a single Route List. On the View page, each entry displays a + sign and the number of Route Groups assigned to that Route List. Click the + sign to display the Route Groups; the + sign changes to a - sign. Click the - sign to display the number again. The Route Group entries in the expanded list are links to the **Diameter > Configuration > Route Groups [Filtered]** page for the selected Route Group.	Format: pulldown list Range: available Route Groups
* Priority	The priority of the Route Group within the Route List. Priority is set from 1 (highest priority) to 3 (lowest priority).	Format: numeric Range: 1, 2, or 3
Route Across Route Groups	Indicates whether alternate Route Groups in the Route List will be used if the Active Route Group cannot forward the request.	Format: radio button Range: Enabled, Disabled Default: Enabled

Routing Option Sets elements

Table 33: Routing Option Sets Elements describes the fields on the Routing Option Sets View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 33: Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Routing Option Set Name	Unique name of the Routing Option Set.	Format: case-sensitive; alphanumeric and underscore Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha

Field (* indicates required field)	Description	Data Input Notes
* Maximum Per Message Forwarding Allowed	Maximum number of times an application is allowed to forward a request message.	Format: numeric Range: 1 - 5 Default: 5
Transaction Lifetime	The total time DSR allows to forward initial and all subsequent routing attempts.	Format: numeric Range: 100 - 5000 ms Default: 5000 ms
* Resource Exhausted Action	Action taken by DSR when a request cannot be processed due to an internal resource being exhausted	Format: pulldown list Range: Abandon with no Answer; Send Answer Default: Abandon with no Answer
Resource Exhausted Answer Result-Code	Result-code value returned in an answer message when a message is not successfully routed due to an internal resource being exhausted.	Format: radio button for pulldown list, radio button for text box Range: 1000 - 5999 Select the code from the pulldown list or enter the code in the text box. Default: "3004 TOO_BUSY" in pulldown list
Resource Exhausted Answer Error Message	Error message for Resource Exhausted	Format: alphanumeric Range: 0 - 64 characters
Resource Exhausted Vendor Id	Vendor Id value returned in an answer message when a message is not successfully routed due to an internal resource being exhausted.	Format: numeric Range: 1 - 4294967295 Default: none
* No Peer Response Action	Action taken by DSR when the routing of a request is abandoned or the time to route exceeds the Transaction Lifetime	Format: pulldown list Range: Abandon with no Answer; Send Answer Default: Send Answer

Field (* indicates required field)	Description	Data Input Notes
No Peer Response Answer Result-Code	Result-code value returned in an answer message when a message is not successfully routed due to being abandoned or timing out	Format: radio button for pulldown list, radio button for text box Range: 1000 - 5999 Select the code from the pulldown list or enter the code in the text box. Default: "3002 UNABLE_TO_DELIVER" in pulldown list
No Peer Response Answer Error Message	Error message for No Peer Response	Format: alphanumeric Range: 0 - 64 characters
No Peer Response Vendor Id	Vendor Id value returned in an answer message when a message is not successfully routed due to being abandoned or timing out	Format: numeric Range: 1 - 4294967295 Default: none
* Connection Failure Action	Action taken by DSR when the routing of a request is abandoned because the last egress connection selection fails	Format: pulldown list Range: Abandon with no Answer; Send Answer Default: Send Answer
Connection Failure Answer Result-Code	Result-code value returned in an answer message when a message is not successfully routed due to connection failure	Format: radio button for pulldown list, radio button for text box Range: 1000 - 5999 Select the code from the pulldown list or enter the code in the text box. Default: "3002 UNABLE_TO_DELIVER" in pulldown list
Connection Failure Answer Error Message	Error message for Connection Failure	Format: alphanumeric Range: 0 - 64 characters
Connection Failure Vendor Id	Vendor Id value returned in an answer message when a message is not successfully routed due to connection failure	Format: numeric Range: 1 - 4294967295

Field (* indicates required field)	Description	Data Input Notes
		Default: none
* Connection Congestion Action	Action taken by DSR when the routing of a request is abandoned because the last connection evaluated is congested	Format: pulldown list Range: Abandon with no Answer; Send Answer Default: Send Answer
Connection Congestion Answer Result-Code	Result-code value returned in an answer message when a message is not successfully routed due to connection congestion.	Format: radio button for pulldown list, radio button for text box Range: 1000 - 5999 Select the code from the pulldown list or enter the code in the text box. Default: "3002 UNABLE_TO_DELIVER" in pulldown list
Connection Congestion Answer Error Message	Error message for Connection Congestion	Format: alphanumeric Range: 0 - 64 characters
Connection Congestion Vendor Id	Vendor Id value returned in an answer message when a message is not successfully routed due to connection congestion	Format: numeric Range: 1 - 4294967295 Default: none

Peer Route Tables elements

Table 34: Peer Route Tables Elements describes the fields on the Peer Route Tables View and Insert pages. Data Input Notes apply only to the Insert page; the View page is read-only.

Table 34: Peer Route Tables Elements

Field (* indicates required field)	Description	Data Input Notes
* Peer Route Table Name	Unique name of the Peer Route Table.	Format: case-sensitive; alphanumeric and underscore Range: 1 - 32 characters; cannot start with a digit

Field (* indicates required field)	Description	Data Input Notes
		and must contain at least one alpha
Number of Rules	The number of Peer Routing Rules in the Peer Route Table.	

Peer Routing Rule configuration elements

Table 35: Peer Routing Rules Configuration Elements describes the fields on the Peer Routing Rules View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 35: Peer Routing Rules Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Rule Name	Unique name of the Peer Routing Rule.	Format: case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters
* Peer Route Table	The Peer Route Table to which the Peer Routing Rule belongs	Format: Pulldown list Range: Available Peer Route Tables
* Priority	Priority of the Rule in relation to other Rules. The priority is set from 1 (highest priority) to 99 (lowest priority).	Format: numeric Range: 1 - 99
* Conditions	In order for a Diameter message to be matched by a Rule, the message must match each specified part of a condition. Each condition has three parts: • Parameter • Operator • Value	
	Parameter: • Destination-Realm • Destination-Host • Application-Id • Command-Code	Format: Operator and Value for each Parameter

Field (* indicates required field)	Description	Data Input Notes
	• Origin-Realm • Origin-Host	
	Operator Sets the relationship between the parameter and the value. For example, if the operator is set to Equals then the Diameter message parameter must match the set value.	Format: Pulldown list Range: See *Peer Routing Rule operators* for a description of operators available for each parameter.
	Value The value in the Diameter message the Peer Routing Rule uses to determine a match. A Value is required if the Operator is "Equals", "Starts With", or "Ends With".	Format: text box oe pulldown menu Range: • Application-ID: available configured Application Ids • Command-Code: available configured Command Codes • Destination-Realm and Origin-Realm: Realm is a case-insensitive string consisting of a list of labels separated by dots. A label may contain letters, digits, dashes (-), and underscore (_). A label must begin with a letter or underscore and must end with a letter or digit. An underscore can be used only as the first character. A label can be at most 63 characters long and a realm can be at most 255 characters long. You can specify a substring or a complete string of a valid Realm. • Destination-Host and Origin-Host: FQDN is a case-insensitive string consisting of a list of labels separated by dots. A label may contain letters, digits, dashes (-), and underscore (_). A label must begin with a letter or underscore and must end with a letter or digit. An underscore can be

Field (* indicates required field)	Description	Data Input Notes
		used only as the first character. A label can be at most 63 characters long and a realm can be at most 255 characters long. You can specify a substring or a complete string of a valid FQDN.
Action	The action that will happen if the Diameter message matches the conditions set in the Peer Routing Rule: • Route to Peer: routes a message to a Peer Node using the Route List associated with this Rule. • Send Answer: abandons message routing and sends an answer response that contains the Diameter answer code associated with this Rule.	Format: selection box Range: Route to Peer, Send Answer Default: Route to Peer
Route List	Route List associated with this Rule. A Route List is required if the Action is set to Route to Peer. The Route List entries on the View page are links to the **Diameter > Configuration > Route Lists [Filtered] page for the selected entry.**	Format: pulldown list Range: available Route Lists
Message Priority	The priority to assign to the message. The message priority is assigned only when Action is set to Route to Peer.	Format: pulldown list Range: No Change, 0, 1, 2. 0 is lowest priority Default: No Change
Answer Result-Code Value	The answer code associated with this Rule. A Diameter answer code is required if the Action is set to Send Answer.	Format: radio button for pulldown list; radio button for text box Range: • pulldown list: available Diameter answer codes • text box: 1000 - 5999 Default: 3002 UNABLE_TO_DELIVER

Field (* indicates required field)	Description	Data Input Notes
Vendor Id	The Vendor Id to place in the Vendor Id AVP of the answer message.	Format: numeric Range: 0 - 4294967295
Answer Error Message	Value returned in the Error-Message AVP of the answer message.	Format: alphanumeric, underscore (_), period (.) Range: 0 - 64 characters Default: null string

Peer Routing Rule operators

Table 36: Peer Routing Rules Operators describes the condition operators available for each parameter in a Peer Routing Rule.

Table 36: Peer Routing Rules Operators

Parameter	Operator	Meaning
Destination-Realm	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified
	Starts With	content must start with the value specified
	Ends With	content must end with the value specified
	Always True	content is not evaluated and the parameter's condition is always true
Destination-Host	Equals	content must equal the value specified
	Present and Not Equal	Destination-Host must be present and value must not equal the value specified
	Starts With	content must start with the value specified
	Ends With	content must end with the value specified
	Present	Destination-Host must be present
	Absent	Destination-Host must be absent
	Always True	content is not evaluated and the parameter's condition is always true
Application-Id	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified
	Always True	content is not evaluated and the parameter's condition is always true
Command-Code	Equals	content must equal the value specified

Parameter	Operator	Meaning
	Not Equal	content must not equal the value specified
	Always True	content is not evaluated and the parameter's condition is always true
Origin-Realm	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified
	Starts With	content must start with the value specified
	Ends With	content must end with the value specified
	Always True	content is not evaluated and the parameter's condition is always true
Origin-Host	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified
	Starts With	content must start with the value specified
	Ends With	content must end with the value specified
	Always True	content is not evaluated and the parameter's condition is always true

Application Routing Rule configuration elements

Table 37: Application Routing Rules Configuration Elements describes the fields on the Application Routing Rules View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 37: Application Routing Rules Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Rule Name	Name of the Application Routing Rule. The Name must be unique.	Format: alphanumeric and underscore (_) Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha (A-Z, a-z); is case-sensitive
* Priority	Priority of the Rule in relation to other Rules. The lower the Priority number, the higher a Priority a Application Routing Rule will have.That is, the Application Routing Rule with a Priority set to 1 has first priority, the Application Routing	Format: numeric Range: 1 - 99

Field (* indicates required field)	Description	Data Input Notes
	Rule with a Priority set to 2 has second priority, and so on.	
* Conditions	In order for a Diameter message to be matched by a Rule, the message must match each specified part of a condition. Each condition has three parts: • Parameter • Operator • Value	
	Parameter: • Destination-Realm • Destination-Host • Application-ID • Command-Code • Origin-Realm • Origin-Host	Format: Operator and Value for each Parameter
	Operator Sets the relationship between the parameter and the value. For example, if the operator is set to Equals then the Diameter message parameter must match the set value.	Format: Pulldown list Range: See *Application Routing Rule operators* for a description of operators available for each parameter.
	Value The value in the Diameter message that the Application Routing Rule uses to determine a match. The Value is required when the field is available for the Operator: "Equals", "Starts With", and "Ends With" allow a Value entry.	Format: text box or pulldown list Range: • Destination-Realm: up to 255 characters • Destination-Host: up to 255 characters • Application-ID: available configured Application Ids • Command-Code: available configured Command Codes • Origin-Realm: up to 255 characters

Field (* indicates required field)	Description	Data Input Notes
		• Origin-Host: up to 255 characters
* Application Name	Application Name associated with this Rule.	Format: Pulldown list Range: All activated Applications

Application Routing Rule operators

Table 38: Application Routing Rules Operators describes the Conditions operators available for each parameter in a Application Routing Rule.

Table 38: Application Routing Rules Operators

Parameter	Operator	Meaning
Destination-Realm	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified
	Starts With	content must start with the value specified
	Ends With	content must end with the value specified
	Always True	content is not evaluated and the parameter's condition is always true
Destination-Host	Equals	content must equal the value specified
	Present and Not Equal	Destination-Host must be present and value must not equal the value specified
	Starts With	content must start with the value specified
	Ends With	content must end with the value specified
	Present	Destination-Host must be present
	Absent	Destination-Host must be absent
	Always True	content is not evaluated and the parameter's condition is always true
Application-Id	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified
	Always True	content is not evaluated and the parameter's condition is always true
Command-Code	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified

Parameter	Operator	Meaning
	Always True	content is not evaluated and the parameter's condition is always true
Origin-Realm	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified
	Starts With	content must start with the value specified
	Ends With	content must end with the value specified
	Always True	content is not evaluated and the parameter's condition is always true
Origin-Host	Equals	content must equal the value specified
	Not Equal	content must not equal the value specified
	Starts With	content must start with the value specified
	Ends With	content must end with the value specified
	Always True	content is not evaluated and the parameter's condition is always true

Pending Answer Timers elements

Table 39: Pending Answer Timers Elements describes the fields on the Pending Answer Timers View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 39: Pending Answer Timers Elements

Field (* indicates required field)	Description	Data Input Notes
* Pending Answer Timer Name	Unique name of the Pending Answer Timer.	Format: case-sensitive; alphanumeric and underscore Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha
* Pending Answer Timer Value	The amount of time the DSR will wait for an Answer from a downstream Peer Node	Format: numeric Range: 100 - 5000 ms Default: 1000 ms

Reroute On Answer configuration elements

Table 40: Reroute On Answer Configuration Elements describes the fields on the Reroute On Answer View and Insert pages. Data Input Notes apply only to the Insert page; the View page is read-only.

Table 40: Reroute On Answer Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Answer Result-Code AVP Value	Value in the result-code AVP of the Answer message.	Format: numeric Range: 0 - 4294967295
Application Id	Application ID in the Answer message that identifies a Diameter Application. It is commonly used for screening and routing messages between Diameter nodes. The Internet Assigned Numbers Authority lists standard and vendor-specific Application IDs on their iana.org website. On the website: • Select Protocol Assignments • Scroll to locate the Authentication, Authorization, and Accounting (AAA) Parameters heading • Select Application IDs under the heading	Format: radio buttons, text box, and pulldown list Range: • first radio button: ALL • second radio button: pulldown list with available Application Ids Default: ALL

System Options elements

Table 41: System Options Elements describes the fields on the System Options page.

Table 41: System Options Elements

Field	Description	Data Input Notes
General Options		
Maximum Message Size Allowed	Maximum message size of a Diameter message (in bytes) allowed by the application. This field is Read-Only; it cannot be changed.	Format: numeric Range: 8192 - 16384 Default: 8192
EMT Feature Enabled	Controls whether Connections use Egress Message Throttling Configuration Sets to set congestion levels	Format: checkbox

Field	Description	Data Input Notes
IPFE Connection Reserved Ingress MPS Scaling	Controls whether new IPFE Connections are allowed. If the total Connection Reserved Ingress MPS for Fixed and established IPFE connections would exceed this percentage of the DA-MP's Engineered Ingress MPS, the new IPFE connection will be rejected. This field is Read-Only; it cannot be changed.	Format: numeric percentage Range: 30-100 Default: 40%
Alarm Threshold Options		
Available Alarm Budget	The number of alarms available	Format: numeric Range: 0-3000 Default: 3000 if no alarm thresholds have been set
Fixed Connection Major Aggregation Alarm Threshold	Major threshold for aggregated Fixed Connection alarms per DA-MP. The available alarm budget is decremented by this value multiplied by the number of configured DA-MPs.	Format: numeric Range: 1 to Available Alarm Budget Default: 100
Fixed Connection Critical Aggregation Alarm Threshold	Critical threshold for aggregated Fixed Connection alarms per DA-MP. This value is not counted against the Alarm Budget.	Format: numeric Range: 0 to Available Alarm Budget Default: 200
IPFE Connection Major Aggregation Alarm Threshold	Major threshold for aggregated IPFE Connection alarms per NE. The available alarm budget is decrement by this value.	Format: numeric Range: 1 to Available Alarm Budget Default: 100
IPFE Connection Critical Aggregation Alarm Threshold	Critical threshold for aggregated IPFE Connection alarms per NE. This value is not counted against the Alarm Budget.	Format: numeric Range: 0 to Available Alarm Budget Default: 100
Peer Node Critical Aggregation Alarm Threshold	Critical threshold for aggregated Peer Node alarms per NE. The available alarm budget is decremented by this value	Format: numeric Range: 1 to Available Alarm Budget Default: 600
Route List Critical Aggregation Alarm Threshold	Critical threshold for aggregated Route List alarms per NE. The available alarm budget is decremented by this value	Format: numeric Range: 1 to Available Alarm Budget

Field	Description	Data Input Notes
		Default: 600
Message Copy Options		
Route List for DAS Node	Default Route List for DAS nodes **Note:** If CPA is activated, this value is overridden by the values set on the CPA Configuration Message Copy page. Otherwise, the Route List specified here is used.	Format: pull down list Range: currently provisioned Route Lists Default: none
Message Copy Request Type	Type of request to be copied at DAS	Format: radio button Range: Original Ingress Request, Original Egress Request Default: Original Ingress Request
Diameter Message Copy Answer Result Code	Specifies the result code/experimental result code that should match with incoming Answer Result Code (whose Request has been marked for Message Copy), to allow copying a REQUEST at DAS.	Format: radio button Range: 2xxx result-code / experimental-result-code, Any result / experimental-result-code Default: 2xxx result-code / experimental-result-code
DAS Message Copy Answer Result Code	Specifies the result code/experimental result code that should match with DAS Message Copy Answer Result Code (whose request has been marked for Message Copy), to allow copying a REQUEST at DAS.	Format: radio button Range: 2xxx result-code / experimental-result-code, Any result / experimental-resullt-code Default: 2xxx result-code / experimental-result-code
Max DAS Retransmission Attempts	Maximum retransmission attempts for DAS-Request	Format: numeric 1 - Maximum Per Message Forwarding Allowed Default: 4

DNS Options elements

Table 42: DNS Options Elements describes the fields on the **Diameter > Configuration > DNS Options** page.

Table 42: DNS Options Elements

Field (* indicates required field)	Description	Data Input Notes
Primary DNS Server IP Address	IP address of the primary DNS server.	Format: valid IP address
Secondary DNS Server IP Address	IP address of the secondary DNS server.	Format: valid IP address
* DNS Query Duration Timer	The amount of time the application waits for queries to the DNS servers (in seconds).	Format: numeric Range: 1 - 4 Default: 2

Local Congestion elements

Table 43: Local Congestion Elements describes the fields on the Local Congestion page.

Table 43: Local Congestion Elements

Field	Description
Congestion Configuration Parameters	
Maximum Diameter Process CPU Utilization	The Diameter Process is responsible for all Diameter processing on a Message Processor (MP). Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 90 %
CL1 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL1. Default: 90%
CL1 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and have a Diameter Answer response sent when the local MP congestion level is CL1. Default: 0%
CL1 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL1. Default: 10%

Field	Description
CL2 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL2. Default: 70%
CL2 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and have a Diameter Answer response sent when the local MP congestion level is CL2. Default: 0%
CL2 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL2. Default: 30%
CL3 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL3. Default: 60%
CL3 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and have a Diameter Answer response sent when the local MP congestion level is CL3. Default: 0%
CL3 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL3. Default: 40%
Maximum MPS Limitation Configuration Parameters	
CL0 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and have a Diameter Answer response sent when the maximum MPS limitation is reached and the local MP congestion level is CL0. Default: 0%
CL0 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the maximum MPS limitation is reached and the local MP congestion level is CL0. Default: 0%
CL1 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and have a Diameter Answer response sent when the maximum MPS limitation is reached and the local MP congestion level is CL1. Default: 0%

Field	Description
CL1 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the maximum MPS limitation lis reached and the local MP congestion level is CL1. Default: 100%
CL2 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and have a Diameter Answer response sent when the maximum MPS limitation is reached and the local MP congestion level is CL2. Default: 0%
CL2 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the maximum MPS limitation is reached and the local MP congestion level is CL2. Default: 100%
CL3 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and have a Diameter Answer response sent when the maximum MPS limitation is reached and the local MP congestion level is CL3. Default: 0%
CL3 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the maximum MPS limitation is reached and the local MP congestion level is CL3. Default: 100%

Bulk Export elements

Table 44: Bulk Export elements describes the fields on the **Diameter Configuration Export** page.

Table 44: Bulk Export elements

Element (* indicates required field)	Description	Data Input Notes
* Export Application	Diameter or activated DSR Application from which configuration data will be exported.	Format: Pulldown list Range: ALL, Diameter, all activated DSR Applications To clear the field, select -Select- in the list.
Export Data	Data to be exported. Either Diameter or a specific activated DSR Application must	Format: Pulldown list Range: ALL, configuration folders for Diameter (except Mediation folders) or the

Element (* indicates required field)	Description	Data Input Notes
	be selected in Export Application before this list is available. This field is required when Diameter or a DSR Application is selected.	selected DSR Application. (Local Congestion data cannot be exported for Diameter; it is view-only and not configured by the user.) To clear the field, select -Select- in the list.
Output File Name	Name of the .csv export file. The default name appears in this field when Export Frequency is Once and: • ALL is selected in Export Application • Diameter or a DSR Application is selected in Export Application, and ALL or a specific configuration folder is selected in Export Data The default file name can be changed, and is not required to follow the default format. This field is required when it is available.	Format: Valid characters are alphanumeric characters, dash (-), and underscore (_) Default file name: file name in the format NeName_ReportDate-TimeZone_ApplicationType_ReportType, with the following values: NeName = Host name of the NO or SO from which the configuration data will be exported. ReportDate = Current date in the format mmddyy. TimeZone = Current Time Zone. Application Type = the selected Export Application to export from ObjectType = the selected Data to export
* Task Name	Periodic Export Task name. This field is required when the Export Frequency is not Once.	Format: text box; length must not exceed 24 characters. Valid characters are alphanumeric, minus sign (-), and spaces between words. The first character must be an alpha character. The last character must not be a minus sign. Range: 1-24 characters Default: DSR Configuration Export

Element (* indicates required field)	Description	Data Input Notes
Description	Periodic Export Task description.	Format: text box; length must not exceed 255 characters. Valid characters are alphanumeric, minus sign (-), and spaces between words. The first character must be an alpha character. The last character must not be a minus sign. Range: 1-255 characters
Export Directory	Directory in which an export file will be placed. Files that are exported to the Export Server Directory will automatically be copied over to the remote if one is configured. The files will be deleted form the local system after the transfer to the remote Export Server is complete. Files that are exported to the File Management Directory, or are exported to the Export Server Directory when no remote Export Server is configured, can be viewed and imported on the local system.	Format: radio buttons Range: radio button for Export Server Directory, radio button for File Management Directory Default: Export Server Directory
Export Frequency	How often the data will be written to the Export Server Directory or File Management Directory. When Once is selected, the export is performed immediately after Ok is clicked.	Format: radio buttons Range: radio buttons for Once, Hourly, Daily, Weekly Default: Once
Minute	The minute of each hour when the data will be exported. This field is available only when Hourly is selected for Export Frequency.	Format: text box with up and down selection arrows Range: 1-59 Default: 0

Element (* indicates required field)	Description	Data Input Notes
Time of Day	Time of day when data will be exported. This field is available only when Daily or Weekly is selected for Export Frequency.	Format: • Text box; the time can be typed in the format HH:MM AM or HH:MM PM. • Pulldown list; click in the box to display a 24-hour list of times that are at 15-minute intervals. Select the desired time in the list. Range: 12:00 AM through 11:45 PM in 15-minute intervals, or specified time Default: 12:00 AM
Day of the Week	Day of the week on which data will be exported. Thsi field is available only when Weekly is selected for Export Frequency.	Format: a radio button for each day of the week Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday Default: Sunday

Bulk Import and Export CSV File Formats and Contents

CSV File Formats and Contents

DSR Bulk Import and Export files support an ASCII Comma-Separated Values (CSV) file format.

- The configuration data described in each table in this help section is contained in a single line in the CSV file.
- The first field or column of each line defines the Application Type; see *Table 45: Application Types Supported by DSR Bulk Import and Export*.
- The second column describes the configuration data type, such as LocalNode, PeerNode, or RouteList.
- Subsequent fields or columns contain the associated configuration data.
- Fields containing text that includes spaces or commas are enclosed in double quotes.
- Element values that are selected using radio buttons on the GUI page are shown as separate fields or columns in the CSV Format tables. A selected value appears in its field or column; an unselected value is shown as just two commas in in the file (...,,...) to maintain the positioning in the file.
- The CSV file can include optional comment lines for documenting within the file. Comment lines must begin with a pound sign (#) in the first column, and can be included on any line of the file.

Table 45: Application Types Supported by DSR Bulk Import and Export

Application Type	Description
Diameter	Common Diameter PlugIn (DPI)
Rbar	Range Based Address Resolution (RBAR)
Fabr	Full Address Based Resolution (FABR)
Cpa	Charging Proxy Application (CPA)
Sbr	Session Binding Repository (SBR)

Diameter CSV File Formats

The following tables describe the CSV file content and attribute field or column positions for all configuration data supported by the Diameter Application Type.

Local Node configuration elements describes the configuration data elements listed in *Table 46: Local Node CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 46: Local Node CSV Format

Column	Data Description
0	Application Type (Diameter)
1	LocalNode (Keyword)
2	Name (Key)
3	Fqdn
4	Realm
5	Tcp Port
6	Sctp Port
7	Connection Configuration Set Name
8	Cex Configuration Set Name
9	IP Address [0]
	(repeated x 128)
136	IP Address [127]
137	IP Type [0] (LocalIp, PeerIp, IpfeTsa)
	(repeated x 128)
264	IP Type [127] (LocalIp, PeerIp, IpfeTsa)

Peer Node configuration elements describes the configuration data elements listed in *Table 47: Peer Node CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 47: Peer Node CSV Format

Column	Data Description
0	Application Type (Diameter)
1	PeerNode (Keyword)
2	Name (Key)
3	Fqdn
4	Realm
5	Tcp Port
6	Sctp Port
7	Replace Destination Host (No, Yes)
8	Replace Destination Realm (No, Yes)
9	Minimum Connection Capacity
10	Alternate Route on Connection failure (SamePeer, DifferentPeer, SameConnection)
11	Alternate Route on Answer Timeout (SamePeer, DifferentPeer, SameConnection)
12	Alternate Route on Answer Result Code (SamePeer, DifferentPeer, SameConnection)
13	Alternate Implicit Route
14	Maximum Alternate Routing Attempts
15	IP Address [0]
	(repeated x 128)
142	IP Address [127]
143	Routing Option Set
144	Pending Answer Timer
145	Peer Route Table
146	Message Priority Setting
147	Message Priority Configuration Set

Route Group configuration elements describes the configuration data elements listed in *Table 48: Route Group CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 48: Route Group CSV Format

Column	Data Description
0	Application Type (Diameter)
1	RouteGrp (Keyword)

Column	Data Description
2	Name (Key)
3	Type (Peer, Connection)
4	Peer Node 1 Name
5	Peer Node 1 Weight
	(repeated x 64) . . .
130	Peer Node 64 Name
131	Peer Node 64 Weight
132	Connection 1 Name
133	Connection 1 Weight
	(repeated x 64) . . .
258	Connection 64 Name
259	Connection 64 Weight

Route List configuration elements describes the configuration data elements listed in *Table 49: Route List CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 49: Route List CSV Format

Column	Data Description
0	Application Type (Diameter)
1	RouteList (Keyword)
2	Name (Key)
3	Minimum Route Group Availability Weight
4	Route Across Route Group (Enabled, Disabled)
5	Route Group 1 Name
6	Route Group 1 Priority
7	Route Group 2 Name
8	Route Group 2 Priority
9	Route Group 3 Name
10	Route Group 3 Priority

Peer Routing Rule configuration elements describes the configuration data elements listed in *Table 50: Peer Routing Rule CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 50: Peer Routing Rule CSV Format

Column	Data Description
0	Application Type (Diameter)
1	PeerRouteRule (Keyword)
2	Name (Key)
3	Priority
4	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode, AppID)
5	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
6	Value
7	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode, AppID)
8	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
9	Value
10	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode, AppID)
11	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
12	Value
13	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode, AppID)
14	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
15	Value
16	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode, AppID)
17	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
18	value
19	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode, AppID)
20	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
21	Value
22	Action (RouteToPeer, SendAnswer)
23	Route List Name
24	Diameter Answer Code
25	Answer Error Message

Column	Data Description
26	Message Priority (NC, PR0, PR1, PR2)
27	Vendor Id
28	Peer Route Table

Connection configuration elements describes the configuration data elements listed in *Table 51: Connection CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 51: Connection CSV Format

Column	Data Description
0	Application Type (Diameter)
1	Conn (Keyword)
2	Connection Name (Key)
3	Type (FullySpecified, LocalMpInitiator, LocalMpResponder)
4	Local Node Name
5	Peer Node Name
6	Protocol Type (Tcp, Sctp)
7	Connection Configuration Set Name
8	Cex Configuration Set Name
9	Cap Configuration Set Name
10	Primary Local IP Address
11	Secondary Local IP Address
12	Primary Peer IP Address
13	Secondary Peer IP Address
14	Transport Fqdn
15	Peer Identification (Ip, TransportFqdn, PeerFqdn)
16	Local Initiate Port
17	Transport Congestion Abatement Timeout
18	Remote Busy Usage (Enabled, Disabled)
19	Remote Busy Timeout
20	Message Priority Setting
21	Message Priority Configuration Set
22	Egress Message Throttling Configuration Set

Column	Data Description
23	Test Mode (Yes, No)

Connection Configuration Set elements describes the configuration data elements listed in *Table 52: Connection Configuration Set CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 52: Connection Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	ConnCfgSet (Keyword)
2	ConnCfgSet Name (Key)
3	retransInitialTimeout
4	retransMinTimeout
5	retransMaxTimeout
6	retransMaxTimeoutInit
7	retransPathFailure
8	retransAssocFailure
9	retransInitFailure
10	sackDelay
11	heartbeatInterval
12	sctpSockSendSize
13	sctpSockReceiveSize
14	sctpNumInboundStreams
15	sctpNumOutboundStreams
16	burstMax
17	sctpDatagramBundlingEnabled
18	tcpSockSendSize
19	tcpSockRecvSize
20	tcTimer
21	twinitTimer
22	tdpxTimer
23	tcexTimer
24	nagleEnabled

Column	Data Description
25	provingTimeout
26	provingDwrsToSend
27	provingMode
28	pendTransPerConn

Reroute On Answer configuration elements describes the configuration data elements listed in *Table 53: Reroute on Answer CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 53: Reroute on Answer CSV Format

Column	Data Description
0	Application Type (Diameter)
1	RerouteOnAns (Keyword)
2	Answer Result-Code AVP Value
3	Application ID

System Options elements describes the configuration data elements listed in *Table 54: System Options CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 54: System Options CSV Format

Column	Data Description
0	Application Type (Diameter)
1	Options (Keyword)
2	EMT Feature Enabled (Yes, No)
3	DAS Answer Result Code (2xxx, any)
4	Message Copy Answer Result Code (2xxx, any)
5	Message Copy Max retry Attempts
6	DAS Route List ID
7	DAS Route List Name
8	Message Copy Request Type (ingress, egress)
9	Fixed Connection Failure Major Aggregation Alarm Threshold
10	Fixed Connection Critical Aggregation Alarm Threshold
11	IPFE Connection Failure Major Aggregation Alarm Threshold
12	IPFE Connection Failure Critical Aggregation Alarm Threshold

Column	Data Description
13	Peer Node Failure Critical Aggregation Alarm Threshold
14	Route List Failure Critical Aggregation Alarm Threshold

DNS Options elements describes the configuration data elements listed in *Table 55: DNS Options CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 55: DNS Options CSV Format

Column	Data Description
0	Application Type (Diameter)
1	DnsOption (Keyword)
2	Primary IP
3	Secondary IP
4	Query Duration Timer

CEX Configuration Set elements describes the configuration data elements listed in *Table 56: CEX Configuration Set CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 56: CEX Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	CexCfgSet (Keyword)
2	Name
3	Selected Application ID [1]
4	Selected Type [1]
5	Selected Vendor ID[1]
	(repeated x 10)
30	Selected Application ID [10]
31	Selected Type [10]
32	Selected Vendor ID [10]
33	Must Application ID [1]
34	Must Type [1]
35	Must Vendor ID[1]
	(repeated x 10)

Column	Data Description
60	Must Application ID [10]
61	Must Type [10]
62	Must Vendor ID[10]
63	Vendor ID [1]
	(repeated x 10)
72	Vendor ID [10]

Capacity Configuration Set elements describes the configuration data elements listed in *Table 57: Capacity Configuration Set CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 57: Capacity Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	CapCfgSet (Keyword)
2	Capacity Configuration Set Name (Key)
3	Reserved Ingress MPS
4	Maximum Ingress MPS
5	Ingress MPS Minor Alarm Threshold
6	Ingress MPS Major Alarm Threshold

Application Routing Rule configuration elements describes the configuration data elements listed in *Table 58: AppRouteRule CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 58: AppRouteRule CSV Format

Column	Data Description
0	Application Type (Diameter)
1	AppRouteRule (Keyword)
2	Name (Key)
3	Priority
4	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode AppID)
5	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
6	Value

Column	Data Description
7	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode AppID)
8	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
9	Value
10	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode AppID)
11	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
12	Value
13	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode AppID)
14	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
15	Value
16	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode AppID)
17	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
18	value
19	param (DestHost, DestRealm, OrigHost,OrigRealm, CmdCode AppID)
20	condOperator (Present, Absent, Equal, Not Equal StartsWith, EndsWith, DontCare, Always True)
21	Value
22	Application Name

Application Ids elements describes the configuration data elements listed in *Table 59: Application ID CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 59: Application ID CSV Format

Column	Data Description
0	Application Type (Diameter)
1	Appids (Keyword)
2	Application ID
3	Name
4	Routing Option Set
5	Pending Answer Timer
6	Peer Route Table

CEX Parameters elements describes the configuration data elements listed in *Table 60: CEX Parameters CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 60: CEX Parameters CSV Format

Column	Data Description
0	Application Type (Diameter)
1	CexParameters (Keyword)
2	Application ID
3	Vendor Specific Application ID
4	Vendor ID

Pending Answer Timers elements describes the configuration data elements listed in *Table 61: Pending Answer Timer CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 61: Pending Answer Timer CSV Format

Column	Data Description
0	Application Type (Diameter)
1	PendingAnswerTimer (Keyword)
2	Name
3	Timer

Routing Option Sets elements describes the configuration data elements listed in *Table 62: Routing Option Set CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 62: Routing Option Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	RoutingOptionSet (Keyword)
2	Name
3	Maximum Per Message Forwarding Allowed
4	Transaction Lifetime
5	Resource Exhausted Action
6	Resource Exhausted Result Code
7	Resource Exhausted Error Message

Column	Data Description
8	Resource Exhausted Vendor Id
9	No Peer Response Action
10	No Peer Response Result Code
11	No Peer Response Error Message
12	No Peer Response Vendor Id
13	Connection Failure Action
14	Connection Failure Result Code
15	Connection Failure Error Message
16	Connection Failure Vendor Id
17	Connection Congestion Action
18	Connection Congestion Result Code
19	Connection Congestion Error Message
20	Connection Congestion Vendor Id

Peer Route Tables elements describes the configuration data elements listed in *Table 63: Peer Route Table CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 63: Peer Route Table CSV Format

Column	Data Description
0	Application Type (Diameter)
1	PeerRouteTable (Keyword)
2	Name

Message Priority Configuration Set elements describes the configuration data elements listed in *Table 64: Message Priority Configuration Set CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 64: Message Priority Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	MsgPriorityCfgSet (Keyword)
2	Name
3	Application Id[1]
4	Command Code[1]

Column	Data Description
5	Message Priority[1]
	(repeated x 50)
150	Application Id[50]
151	Command Code[50]
152	Message Priority[50]

Egress Message Throttling Configuration Set elements describes the configuration data elements listed in *Table 65: Egress Message Throttling Configuration Set CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 65: Egress Message Throttling Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	MsgThrottlingCfgSet (Keyword)
2	Name
3	Maximum EMR
4	Smoothing Factor
5	Abatement Timer
6	TT1
7	AT1
8	TT2
9	AT2
10	TT3
11	AT3

Range-Based Address Resolution (RBAR) CSV File Formats

The following tables describe the CSV file content and attribute column positions for all configuration data supported by the RBAR Application Type.

Note: Address Individual and Address Range elements are in different CSV files for performance reasons.

"Applications configuration elements" in the RBAR Help describes the configuration data elements listed in *Table 66: Supported Application CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 66: Supported Application CSV Format

Column	Data Description
0	Application Type (Rbar)
1	SuppAppl (Keyword)
2	Application ID
3	Routing Mode (Proxy)

"Addresses configuration elements" in the RBAR Help describes the configuration data elements listed in *Table 67: Address Individual CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 67: Address Individual CSV Format

Column	Data Description
0	Application Type (Rbar)
1	AddressIndv (Keyword)
2	Table Name
3	Address
4	Destination
5	Pfx Length
6	Routing Entity (Imsi, Msisdn, Impi, Impu, Ipv4, Ipv6PfxAddr, Unsigned16)
7	Old Table Name
8	Old Address
9	Old Pfx Length

"Addresses configuration elements" in the RBAR Help describes the configuration data elements listed in *Table 67: Address Individual CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 68: Address Range CSV Format

Column	Data Description
0	Application Type (Rbar)
1	AddressRange (Keyword)
2	Table Name
3	Start Address
4	End Address
5	Destination

Column	Data Description
6	Pfx Length
7	Old Table Name
8	Old Start Address
9	Old Pfx Length

"Address Tables configuration elements" in the RBAR Help describes the configuration data elements listed in *Table 69: Address Table CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 69: Address Table CSV Format

Column	Data Description
0	Application Type (Rbar)
1	AddressTable (Keyword)
2	Name
3	Comment
4	Routing Entity (Imsi, Msisdn, Impi, Impu, Ipv4, Ipv6PfxAddr, Unsigned16)

"Destinations configuration elements" in the RBAR Help describes the configuration data elements listed in *Table 70: Destination Table CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 70: Destination Table CSV Format

Column	Data Description
0	Application Type (Rbar)
1	Destination (Keyword)
2	Name
3	Realm
4	Fqdn
5	Avp Insertion (No, Yes)

"Exceptions configuration elements" in the RBAR Help describes the configuration data elements listed in *Table 71: Routing Exception CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 71: Routing Exception CSV Format

Column	Data Description
0	Application Type (Rbar)

Column	Data Description
1	RoutingException (Keyword)
2	Application ID
3	Exception Type (UnknownCmdCode, NoRoutingEntityAddress, NoDrtEntry)
4	Action (FwdUnchanged, FwdToDest, SendAnswer, SendAnsExp)
5	Destination Name
6	Answer Result Code
7	Vendor ID
8	Error Message

"Address Resolutions configuration elements" in the RBAR Help describes the configuration data elements listed in *Table 72: Address Resolution CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 72: Address Resolution CSV Format

Column	Data Description
0	Application Type (Rbar)
1	Resolution (Keyword)
2	Application ID
3	CMD Code
4	CMD Name
5	Routing Entity 1 (Imsi, Msisdn, Impi, Impu, Ipv4, Ipv6PfxAddr, Unsigned16)
6	Re 1 Avp 1 (PublicIdentity, SvcInfoSubscrId0, SvcInfoSubscrId1, SvcInfoSubscrId2, SvcInfoSubscrId3, SvcInfoSubscrId4, SubscriptionId0, SubscriptionId1, SubscriptionId2, SubscriptionId3, SubscriptionId4, UserIdentityMsisdn, UserIdentityPublic, UserName, FramedIpAddress, FramedIpv6Prefix, SvcInfoPsInfo3gppcc, Unprovisioned)
7	Re 1 Avp 2 (PublicIdentity, SvcInfoSubscrId0, SvcInfoSubscrId1, SvcInfoSubscrId2, SvcInfoSubscrId3, SvcInfoSubscrId4, SubscriptionId0, SubscriptionId1, SubscriptionId2, SubscriptionId3, SubscriptionId4, UserIdentityMsisdn, UserIdentityPublic, UserName, FramedIpAddress, FramedIpv6Prefix, SvcInfoPsInfo3gppcc, Unprovisioned)
8	Re 1 Address Table Name
9	Routing Entity 2 (Imsi, Msisdn, Impi, Impu, Ipv4, Ipv6PfxAddr, Unsigned16)
10	Re 2 Avp 1 (PublicIdentity, SvcInfoSubscrId0, SvcInfoSubscrId1, SvcInfoSubscrId2, SvcInfoSubscrId3, SvcInfoSubscrId4, SubscriptionId0, SubscriptionId1, SubscriptionId2, SubscriptionId3, SubscriptionId4, UserIdentityMsisdn, UserIdentityPublic, UserName, FramedIpAddress, FramedIpv6Prefix, SvcInfoPsInfo3gppcc, Unprovisioned)
11	Re 2 Avp 2 (PublicIdentity, SvcInfoSubscrId0, SvcInfoSubscrId1, SvcInfoSubscrId2, SvcInfoSubscrId3, SvcInfoSubscrId4, SubscriptionId0, SubscriptionId1, SubscriptionId2,

Column	Data Description
	SubscriptionId3, SubscriptionId4, UserIdentityMsisdn, UserIdentityPublic, UserName, FramedIpAddress, FramedIpv6Prefix, SvcInfoPsInfo3gppcc, Unprovisioned)
12	Re 2 Address Table name

"System Options elements" in the RBAR Help describes the configuration data elements listed in *Table 73: Option CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 73: Option CSV Format

Column	Data Description
0	Application Type (Rbar)
1	Option (Keyword)
2	Uri Supported (No, Yes)
3	RemoveDestHOst (No, Yes)
4	Exclude Space (No, Yes)
5	Allow Subsequent DSR App Invoc (No, Yes)
6	Realm
7	Fqdn
8	Resource Exhaustion Error Code
9	Resource Exhaustion Error Message
10	Resource Exhaustion Vendor ID
11	Unavailable Application Action (ContinueRouting, DefaultRoute, SendAnswer, SendAnsExp)
12	Unavailable Application Route List
13	Unavailable Application Result Code
14	Unavailable Application Error Message
15	Unavailable Application Vendor ID
16	ASCII Exluded List [0]
	(repeated x 20) . . .
35	ASCII Excluded List [19]
36	TBCD Excluded List [0]
	(repeated x 5) . . .
40	TBCD Excluded List [4]

Full Address-Based Resolution (FABR) CSV File Formats

The following tables describe the CSV file content and attribute column positions for all configuration data supported by the FABR Application Type.

"Applications configuration elements" in the FABR Help describes the configuration data elements listed in *Table 66: Supported Application CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 74: Supported Application CSV Format

Column	Data Description
0	Application Type (Fabr)
1	SuppAppl (Keyword)
2	Application ID
3	Routing Mode (Proxy)

"Exceptions configuration elements" in the FABR Help describes the configuration data elements listed in *Table 71: Routing Exception CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 75: Routing Exception CSV Format

Column	Data Description
0	Application Type (FABR)
1	RoutingException (Keyword)
2	Application ID
3	Exception Type (UnknownCmdCode, NoRoutingEntityAddress, NoAddrMatch, DpErrors, DpCongestion)
4	Action (FwdUnchanged, FwdToDest, SendAnswer, SendAnsExp)
5	Destination Name
6	Answer Result Code
7	Vendor ID
8	Error Message

"Destinations configuration elements" in the FABR Help describes the configuration data elements listed in *Table 70: Destination Table CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 76: Default Destination Table CSV Format

Column	Data Description
0	Application Type (Fabr)

Column	Data Description
1	Destination (Keyword)
2	Name
3	Realm
4	Fqdn

"Address Resolutions configuration elements" in the FABR Help describes the configuration data elements listed in *Table 72: Address Resolution CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 77: Address Resolution CSV Format

Column	Data Description
0	Application Type (Fabr)
1	Resolution (Keyword)
2	Application ID
3	CMD Code
4	Routing Entity 1 (Imsi, Msisdn, Impi, Impu)
5	Re 1 Avp 1 (PublicIdentity, SvcInfoSubscrId0, SvcInfoSubscrId1, SvcInfoSubscrId2, SvcInfoSubscrId3, SubscriptionId0, SubscriptionId1, SubscriptionId2, SubscriptionId3, UserIdentityMsisdn, UserIdentityPublic, UserName, WildCardedPubIdnty)
6	Re 1 Avp 2 (PublicIdentity, SvcInfoSubscrId0, SvcInfoSubscrId1, SvcInfoSubscrId2, SvcInfoSubscrId3, SubscriptionId0, SubscriptionId1, SubscriptionId2, SubscriptionId3, UserIdentityMsisdn, UserIdentityPublic, UserName, WildCardedPubIdnty)
7	Re 1 Destination Type (ImsHss, LteHss, Pcrf, Ocs, Ofcs, Aaa, UserDefined1, UserDefined 2)
8	Routing Entity 2 (Imsi, Msisdn, Impi, Impu)
9	Re 2 Avp 1 (PublicIdentity, SvcInfoSubscrId0, SvcInfoSubscrId1, SvcInfoSubscrId2, SvcInfoSubscrId3, SubscriptionId0, SubscriptionId1, SubscriptionId2, SubscriptionId3, UserIdentityMsisdn, UserIdentityPublic, UserName, WildCardedPubIdnty)
10	Re 2 Avp 2 (PublicIdentity, SvcInfoSubscrId0, SvcInfoSubscrId1, SvcInfoSubscrId2, SvcInfoSubscrId3, SubscriptionId0, SubscriptionId1, SubscriptionId2, SubscriptionId3, UserIdentityMsisdn, UserIdentityPublic, UserName, WildCardedPubIdnty)
11	Re 2 Destination Type (ImsHss, LteHss, Pcrf, Ocs, Ofcs, Aaa, UserDefined1, UserDefined 2)

"System Options elements" in the FABR Help describes the configuration data elements listed in *Table 73: Option CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 78: Option CSV Format

Column	Data Description
0	Application Type (Fabr)
1	Option (Keyword)
2	Exclude Space (No, Yes)
3	Allow Subsequent DSR App Invoc (No, Yes)
4	Realm
5	Fqdn
6	Resource Exhaustion Error Code
7	Resource Exhaustion Error Message
8	Resource Exhaustion Vendor ID
9	Unavailable Application Action (ContinueRouting, DefaultRoute, SendAnswer, SendAnsExp)
10	Unavailable Application Route List
11	Unavailable Application Result Code
12	Unavailable Application Error Message
13	Unavailable Application Vendor ID
15	ASCII Exluded List [0]
	(repeated x 20) . . .
33	ASCII Excluded List [19]
35	TBCD Excluded List [0]
	(repeated x 5) . . .
39	TBCD Excluded List [4]

Charging Proxy Application (CPA) CSV File Formats

The following tables describe the CSV file content and attribute column positions for all configuration data supported by the CPA Application Type.

"System Options configuration elements" in the Charging Proxy Application (CPA) Help describes the configuration data elements listed in *Table 79: System Option CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 79: System Option CSV Format

Column	Data Description
0	Application Type (Cpa)

Column	Data Description
1	Option (Keyword)
2	id
3	name
4	unavailableAction (SendAnswer)
5	unavailableAppResultCode
6	unavailableActionVendorId
7	unavailableActionErrorMessage
8	application InvokedAvpInsertion (Yes, No)
9	shutdownMode (Graceful, Force)
10	shutdownTimer
11	generateAnswerResultCode
12	generateAnswerVendorId
13	generateAnswerErrorMessage
14	behaviorIfSessionLookupError (GenerateAnswer, ContinueRouting)

"Message Copy elements" in the Charging Proxy Application (CPA) Help describes the Message Copy configuration data elements listed in *Table 80: Message Copy CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 80: Message Copy CSV Format

Column	Data Description
0	Application Type (Cpa)
1	Messagecopy (Keyword)
2	messageCopyStatus
3	messageCopyRouteList1
4	messageCopyRouteList2
5	messageCopyRouteList3
6	messageCopyRouteList4
7	messageCopyRouteList5
8	messageCopyRouteList6
9	messageCopyRouteList7
10	messageCopyRouteList8
11	messageCopyRouteList9

Column	Data Description
12	messageCopyRouteList102
13	calledStationIdString1
14	calledStationIdString2
15	calledStationIdString3
16	calledStationIdString4

"SBR elements" in the Charging Proxy Application (CPA) Help describes the Session Binding Repository (SBR) configuration data elements listed in *Table 81: SBR CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 81: SBR CSV Format

Column	Data Description
0	Application Type (Sbr)
1	Sbrconfig (Keyword)
2	sbdbAuditStartTime
3	sbdbAuditStopTime
4	staleSbdbSessionBindingAge
5	maximumActiveSessionBindings
6	mostlyStalePercent

Bulk Import elements

Table 82: Bulk Import elements describes the fields on the **Diameter Configuration Import** page.

Table 82: Bulk Import elements

Element	Description
File Name	The name of the .csv file from the Status & Manage File Management area.
Line Count	Number of lines in the file.
Time Stamp	The creation time and date of the file.

MP Statistics (SCTP) report elements

Table 83: MP Statistics (SCTP) Report Elements describes the fields for selecting MPs and the contents of the columns on the **Diameter Reports MP Statistics (SCTP)** page.

Table 83: MP Statistics (SCTP) Report Elements

Field	Description	Data Input Notes
MP Selection		
Scope	Select Network Element or Server. All of the selected MPs have the same Scope.	Format: pulldown list Range: NE, Server
Statistics for	Left list is all available MPs or NEs, depending on the selected Scope. Right box is all MPs or NEs selected for the report.	Format: List of all MPs/NEs; list of selected MPs/NEs
Report Columns		
Field	Description	
MP	Hostname of the MP Server from which status is reported	
Current Established	Current number of SCTP associations established	
Established (Local Initiated)	Number of locally-initiated SCTP associations established	
Established (Peer Initiated)	Number of peer-initiated SCTP associations established	
Packets Rcvd	Number of IP packets received. Each IP packet contains one or more SCTP chunks.	
Packets Sent	Number of IP packets sent. Each IP packet contains one or more SCTP chunks.	
DATA chunks Rcvd (excluding Duplicates)	Number of SCTP DATA Chunks received not including duplicates	
DATA chunk Sent (excluding Duplicates)	Number of SCTP DATA Chunks sent not including duplicates	
Fast Retransmits	Number of SCTP DATA Chunks retransmitted due to fast transmit rule	
Retransmits	Number of SCTP DATA Chunks retransmitted due to acknowledgment timeout	
CTRL chunk Sent	Number of SCTP Control Chunks sent. A control chunk is one of: INIT, INIT ACK, COOKIE ECHO, COOKIE ACK, SACK	
CTRL chunks Rcvd	Number of SCTP Control Chunks received. A control chunk is one of: INIT, INIT ACK, COOKIE ECHO, COOKIE ACK, SACK	
Fragmented User Messages	Number of SCTP User messages fragmented because message length exceeds path MTU	
Reassembled User Messages	Number of SCTP User messages reassembled due to fragmentation	
Aborted	Number of ABORT messages received	

Field	Description	Data Input Notes
Shutdown	Number of SHUTDOWN messages received	
Out of Blue Chunks Rcvd	Number of Out of the Blue messages received from an unknown peer	
Checksum Error	Number of SCTP Checksum Errors detected	

Diameter Maintenance Elements

The tables in this section describe the elements that appear on the Diameter Maintenance GUI pages in the DSR software.

Route List maintenance elements

This table describes fields on the Route Lists maintenance page.

Table 84: Route Lists Maintenance Elements

Field	Description
Route List Name	Name of the Route List.
Minimum Route Group Availability Weight	Minimum Route Group availability weight for this Route List.
Route Group	Route Groups assigned to the Route List.
MP Server Hostname	Hostname of the Message Processor Server from which status is reported. • For a Multiple Active DA-MP configuration, the MP Leader always reports the Route List status • For an Active/Standby DA-MP configuration, the Active DA-MP reports the Route List status
Priority	Priority of each Route Group in the Route List.
Provisioned Capacity	Capacity assignment for each Route Group in the Route List.
Current Capacity	Current capacity available for each Route Group in the Route List.
Active/Standby	A Route Group can be: • Active: this is the Route Group that Diameter messages are actively being routed to • Standby: messages are not currently being routed to this Route Group, unless the Active Route Group is unavailable and Route Across Route Groups is enabled on the Route List • Unk: information on this Route Group is not present in the database

Field	Description
Status	Route List or Route Group status can be: • Available: the available capacity of the Route Group is greater than the Minimum Route Group Availability Weight • Degraded: the available capacity of the Route Group is greater than zero, but less than the Minimum Route Group Availability Weight • Unavailable: the Route Group available capacity is zero • Unk: status information is not available in the database
Time of Last Update	Time stamp that shows the last time the status information was updated.

Route Group maintenance elements

This table describes fields on the Route Groups maintenance page.

Table 85: Route Group Maintenance Elements

Field	Description
Route Group Name	Name of the Route Group.
Peer Node/Connection	Number and names of Peer Nodes or Connections in the Route Group.
MP Server Hostname	Hostname of MP Server from which status is reported. • For a Multiple Active DA-MP configuration, the MP Leader always reports the Route Group status • For an Active/Standby DA-MP configuration, the Active DA-MP reports the Route Group status
Provisioned Capacity	• For a Peer Route Group, the sum total of the Provisioned Capacity of all the Peer Nodes in the Route Group. • For a Connection Route Group, the sum total of the Provisioned Capacity of all the Connections in the Route Group.
Provisioned Percent	The percentage of capacity assigned to each Peer Node/Connection compared to all Peer Nodes/Connections in the Route Group.
Available Capacity	• For a Peer Route Group, the sum total of the Available Capacity of all the Peer Nodes in the Route Group. • For a Connection Route Group, the sum total of Available Capacity of all the Connections in the Route Group.

Field	Description
Available Percent	The percentage of capacity the Peer Node/Connection currently has compared to the total available capacity of all Peer Nodes/Connections in the Route Group.
Peer Node/Connection Status	Peer Node/Connection Status can be: • Available: the available capacity is greater than the minimum capacity • Degraded: the available capacity is greater than zero, but less than the provisioned capacity • Unavailable: the available capacity is zero • Unk: status information is not available in the database
Time of Last Update	Time stamp that shows the last time the status information was updated.

Peer Node maintenance elements

This table describes fields on the Peer Nodes maintenance page.

Table 86: Peer Nodes Maintenance Elements

Field	Description
Peer Node Name	Name of the Peer Node.
MP Server Hostname	Hostname of MP Server from which status is reported. For the Peer Node status: • For a Multiple Active DA-MP configuration, the MP Leader always reports the Peer Node status • For an Active/Standby DA-MP configuration, the Active DA-MP reports the Peer Node status For Connection status (when the Connection field is expanded): • Fixed (non-IPFE) Connections are always reported by the DA-MP that hosts the Fixed Connection • Owned IPFE Connections are always reported by the DA-MP that hosts the established IPFE Connection • Unowned IPFE Connections (ones that have been configured, but are currently not assigned to a DA-MP by IPFE) are reported by the MP Leader
Operational Status	Peer Node Operational Status can be: • Available: at least one Peer Node connection is available for routing

Field	Description
	• Degraded: the Peer Node connection is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: all connections for a Peer Node are unavailable. The Operational Reason field provides additional information on this status.
Operational Reason	Reason for the Peer Node Operational Status. Information is also available for each connection.
Connection	Number and names of connections associated with the Peer Node.
Time of Last Update	Time stamp that shows the last time the status information was updated.

Connection maintenance elements

This table describes fields on the Connections maintenance page.

Table 87: Connections Maintenance Elements

Field	Description
Connection Name	Name of the connection
MP Server Hostname	Hostname of the MP server from which status is reported: • Fixed (non-IPFE) Connections are always reported by the DA-MP that hosts the Fixed Connection • Established IPFE Connections are always reported by the DA-MP that hosts the established IPFE Connection • Non-Established IPFE Connections (ones that have been configured, but are currently not assigned to a DA-MP by IPFE) are reported by the MP Leader
Admin State	A connection's administrative state can be: • Enabled: the connection is Enabled • Disabled: the connection is Disabled • Unk: unknown; the state of the connection is not available in the database
Operational Status	A connection's administrative state can be: • Available: the connection is available for routing • Degraded: the connection is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the connection is unavailable. The Operational Reason field provides additional information on this status.

Field	Description
CPL	The Connection Priority Level is the maximum of the following values: • Operational Status (0=available; 3=degraded; 99=unavailable) • Remote Busy Congestion Level (0-3) • Egress Transport Congestion Level (0-4) • Egress Message Rate Congestion Level (0-3)
Operational Reason	Reason for the Operational Status. The following reasons can occur: • Disabled • Connecting • Listening • Abnormal • Disconnecting • Proving • Watchdog • Remote Busy Congestion • Egress Transport Congestion • Egress Message Rate Congestion • Normal • Peer with reduced IP set
Connection Mode	The connection can have one of the following connection modes: • Initiator Only - indicates that the Local Node will initiate the connection the Peer Nodes. • Responder Only - indicates that the Local Node will only respond to the connection initiated from the Peer Node. • Initiator & Responder - indicates that the Local Node will initiate a connection in addition to responding to connection initiations from the Peer Node.
Local Node	Local Node associated with the connection
Peer Node	Peer Node associated with the connection
Remote IP Addresses	The IP address(es) of the Peer Node associated with the connection
Remote Port	The Listen Port of the Peer Node associated with the connection
Ingress Msgs Per Second	A 30-second running average of the Ingress messages processed by the connection
Common Application Ids	A comma-separated list of application IDs received in a Diameter CEA message, or a list of application names. The first 10 application IDs received in the CEA are listed.
Transport Congestion Abatement Timeout	The amount of time spent at Egress Transport Congestion Levels 3, 2, and 1 during Egress Transport Congestion Abatement

Field	Description
Remote Busy Usage	Indicates which Request messages can be forwarded on this connection after receiving a DIAMETER_TOO_BUSY response from the connection's Peer. **Disabled** The connection is not considered to be BUSY after receiving a DIAMETER_TOO_BUSY response. All Request messages continue to be forwarded to (or rerouted to) this connection. **Enabled** The connection is considered to be BUSY after receiving a DIAMETER_TOO_BUSY response. No Request messages are forwarded to (or rerouted to) this connection until the Remote Busy Abatement Timeout expires. **Host Override** The connection is considered to be BUSY after receiving a DIAMETER_TOO_BUSY response. Only Request messages whose Destination-Host AVP value is the same as the connection's Peer FQDN can be forwarded to (or rerouted to) this connection until the Remote Busy Abatement Timeout expires.
Remote Busy Abatement Timeout	If Remote Busy Usage is Enabled or Host Override, this is the time period in seconds that the connection will be considered BUSY from the last time a DIAMETER_TOO_BUSY response was received.
Message Priority Setting	Indicates the source of Message Priority for a request message arriving on the connection. Possible settings are: • None - use the Default Message Priority Configuration Set • Read from Request Message - read the message priority from the ingress request • User Configured - Apply the user configured Message Priority Configuration Set
Message Priority Configuration Set	The Message Priority Configuration Set associated with the connection
Egress Message Throttling Configuration Set	The Egress Message Throttling Configuration Set associated with the connection
Smoothed EMR	The most recent smoothed Egress Message Rate on the connection
Test Mode	Indicates if this is a test connection
PDUs to Diagnose	For a test connection currently undergoing diagnosis, this shows the number of PDUs yet to be diagnosed.
Time of Last Update	Time stamp that shows the last time the status information was updated

Applications maintenance elements

The following table describes fields on the Applications maintenance page.

Table 88: Applications Maintenance Elements

Field	Description
DSR Application Name	Name of the DSR Application
MP Server Hostname	Hostname of the Message Processor Server from which status is reported
Admin State	Admin State of the DSR Application (Enabled, Disabled). The Admin State persists over DSR Application restart and server reboot.
Operational Status	Operational Status of the DSR Application (Unavailable, Available, or Degraded)
Operational Reason	Operational Reason that is filled in by the DSR Application and extracted from the database
Congestion Level	Congestion Level of the DSR Application (Normal, CL1, CL2, CL3)
Time of Last Update	Time stamp that shows when the application changed to the status shown in Operational State
If the run-time data for Operational Status, Operational Reason, Congestion Level, and Time of Last Status change is not present in the database, the data is displayed as Unknown.	

DA-MPs maintenance elements

The following table describes fields on the DA-MPs maintenance page.

Table 89: DA-MPs Maintenance Elements

Field	Description
Peer DA-MP Status Tab	
MP ID	The numeric identifier of the reporting DA-MP Server
MP Server Hostname	The hostname of the reporting DA-MP Server
# Peer MPs Available	The number of peer DA-MPs whose status is available
# Peer MPs Degraded	The number of peer DA-MPs whose status is degraded
# Peer MPs Unavailable	The number of peer DA-MPs whose status is unavailable
MP Leader	Indicates whether a DA-MP reports itself as MP Leader. The MP Leader provides status information to the OAM for Route Lists, Route Groups, and Peer Nodes, which are resources whose scope is beyond a single DA-MP.
Note: If a configured DA-MP is not alive, the above fields will display "Unk"	

Field	Description
DA-MP Connectivity Tab	
MP ID	The numeric identifier of the reporting DA-MP Server
MP Server Hostname	The hostname of the reporting DA-MP Server
# Fixed Connections Configured (Max)	The number of configured Connections whose Primary IP Address is one of the fixed IP addresses assigned to the DA-MP. (Max) is the maximum number of connections the DA-MP can have configured at one time.
# Fixed Connections Established	The number of Connections whose operation status is available and whose Primary IP Address is one of the fixed IP addresses assigned to the DA-MP.
# IPFE Connections Established	The number of IPFE Connections owned by the DA-MP whose operation status is available.
# Total Connections Established	The total of Fixed and IPFE Connections established.
Current Total Connection Max Ingress MPS	The sum of the Maximum Ingress MPS settings for all fixed and IPFE connections currently established on the DA-MP.
Current Total Connection Reserved Ingress MPS (Max)	The sum of the Reserved Ingress MPS settings for all fixed and IPFE connections currently established on the DA-MP. (Max) is the Engineered Ingress Message Rate value from the MP Profile associated with the DA-MP, scaled by the value of the IPFE Connection Reserved Ingress MPS Scaling system option.
Note: If a configured DA-MP is not alive, the above fields will display "Unk"	
<MP Server Hostname> Tabs The <MP Server Hostname> tabs show the status of each DA-MP peer as reported by the DA-MP whose hostname appears on the tab.	
MP ID	The numeric identifier of the peer DA-MP
MP Server Hostname	The hostname of the peer DA-MP Server
Status	Peer DA-MP status. Possible settings are: • Available - CPL=0 • Degraded - CPL=1,2,3 • Unavailable - CPL = 99
CPL	Connection Priority Level (0,1, 2, 3, 99) of the configured peer DA-MP. This overall value takes into account the following status: • Operational Status of the ComAgent connection between the reporting DA-MP and the peer DA-MP • Congestion level of the peer DA-MP • Status of the DSR Process running on the peer DA-MP

Field	Description
CPL Reason	Reason for CPL setting. Possible settings are: • Available - There is no MP-level impairment on the peer DA-MP • MP Congestion - Indicates peer DA-MP is in congestion (CL1, CL2, or CL3) • Inter-MP Connection Unavailable - The ComAgent connection between the reporting DA-MP and the peer DA-MP has an Operation Status of Unavailable. • DSR Process Not Running - The DSR process is not running on the peer DA-MP.

Diameter Mediation Configuration Elements

The tables in this section describe the elements that can be configured using the Diameter Mediation GUI pages in the DSR software.

Rule Template elements

Table 90: Rule Template elements descibes the information that can be contained in a Rule Template. Some of these elements appear only when adding, editing, or copying a Rule Template.

Table 90: Rule Template elements

Element	Description	Data Input Notes
Settings: This section contains basic information for the Rule Template.		
Rule Template Name	Name used to label this Rule Template in this application. This field is required.	Format: a-z, A-Z, 0-9, -, ., @, and _ ("Unset" cannot be used as a Rule Template Name.) Range: 1-255 characters
Message Support Type	Indicates the type of message processing that is supported by the Rule Template (Request, Answer, or both). The Message Support Type depends on the selected conditions and actions.	Format: Check marks Range: Request, Answer, or both are checked. Default: Both are checked This field cannot be edited.
Conditions: This section defines a set of zero to five matching expressions. The defined matching expressions are combined to make one logical expression with AND operators, so the set matches on the message if all the expressions are true. If no matching expression is defined, the message unconditionally matches.		

Element	Description	Data Input Notes
OR operators can be simulated by setting up multiple Rule Templates. All conditions are supported by both requests and replies.		

Fast Search	If check marked, fast database lookups are used. Otherwise, the values of the specified field are checked one-by-one until the first match is found. See *Rule Templates*.
	The value of the Fast Search option is determined by:
	• The selected Operator, the Right value type, and the Default value
	  • Yes (check mark) if one of the following Operators is selected and the Right value type is not "xl-value":
	  • equals (==)
	  • begins with-longest match (=^^)
	  • begins with (=^)
	  • is within
	  • exists
	  • does not exist
	  • is true
	  • is false
	• The Condition evaluation order; Conditions are ANDed as follows:
	  • Yes (check mark) if the Condition is the first one in the Condiitions section or all Conditions above this one also have a Yes check mark for the Fast Search option.
	  • No sign for other cases.
	Fast Search is not automatically disabled when "any" instance of an AVP is looked up in the condition. Fast Search must be manually disabled for the selected instance number of "any". Disabling the Fast Search can be achieved, for example, by selecting an "xl-value" as the Right value.
		Format: Check mark (Yes) or red circle with red line through it (No); not editable
		Range: Yes sign or No sign
		Default: Yes sign
		All Conditions with the Fast Search option checked must precede the others to maintain the Fast Search.
		When the Default value is Fixed, Fast Search is enabled regardless of the selected Operator and Right value type.

Element	Description	Data Input Notes
Name	The name for the Left value to display for a Condition on the Rule Set page. This field is required.	Format: Text string Range: 1 to 64 characters
Description	The description that appears for a Condition on the **Rule Sets** page. If possible, provide information such as the format to be used (such as text string or telephone number format) and the range of values (such as 1 to 255 characters).	Format: descriptive text Range: 1 to 255 characters string
Left value	The left-hand value in a Condition. The Left value typically refers to a regular or grouped AVP component (AVP header parts or value) or a Diameter Header component. Grouped AVPs that have a depth of one are supported (one or more AVPs at the same level within an AVP). This field is required. The value can be defined using the *Formatting Value Wizard*.	Format: Text box Range: See *Formatting Value Wizard*
Operator	The operator being used to compare Left value and Right value in a Condition. "Exist" and "not exist" operators are used to check the presence of the specified Left-hand value. "Is true" and "is not true" operators are used ot verify whether the specified Left value is not 0 or equals 0 (is empty in the case of a string type).	Format: Pulldown list Range: See *Table 91: Rule Template Condition Operators* Default: equals (==)
	Case Sensitive Allows the comparison to be looked up considering case. Case-sensitive search is possible only together with Fast Search. Without Fast Search, the lookup is always case-insensitive. The check box is enabled for OctetString and UTF8String Right values.	Format: Check box Range: Checked or not checked Default: Not checked (not case-sensitive)
Right value	The type of data that is compared to the field in the message (specified by the Left	Format: Pulldown list Range: Right value types are:

Element	Description	Data Input Notes
	value) in a Condition to determine if there is a match and Mediation should be performed. The Right value can be: • Empty; the Optional check box is checked (it can be left empty in the rule provisioning in a Rule Set), or the Right value is not used by the selected Operator (such as "exists"). • One of the Right value types shown in the Range: list. Actual data of the specified type is entered in a rule in the Rule Set that is generated from the Rule Template, to use in the comparison. • An actual data value of the selected Right value type, provisioned in the Default value field of the Condition in the Rule Template.	• Integer32 • Integer64 • Unsigned32 • Unsigned64 • Float32 • Float64 • Address (IPv4 or IPv6 IP address) • Time (number of seconds since 0h on 1 January 1900) • UTF8string • DiameterIdentity (FQDN or Realm) • DiameterURI • IP/Netmask (IPv4 or IPv6 Netmask) • Enumerated (available Enum values; prefaced by "enum:") • OctetString • xl-value (references to AVPs, LAVPs, or parts of the Diameter message) • Regular expression (Perl 5 regular expression) Default: Integer32 All previously provisioned Enumerated Types shall be listed prefixed with “enum:”. For example: “enum: xyz”.
	Default value: An actual data value to display for the Right value of a Condition on the Rule Set page. When the Default value is Fixed, Fast Search is enabled regardless of the selected Operator and Right value type.	Format: Text box Range: Data value that is valid for selected Right value type. When OctetString or UTF8String is selected, any human-readable character is valid. When the "xl-value" type is selected, all Default value entries must be xl-values.
	Optional: The Optional check box can be checked so that the Right value data could be deleted or left empty in the Rule Set rule, or unchecked indicating that the	Format: Check box Range: Check mark or no check mark

Element	Description	Data Input Notes
	Right value data msut be entered and can be changed in the Rule Set rule.	Default: Checked
	Fixed: Indicates that the Right value data that is entered in the Default value in the Rule Template Condition is actual data, and cannot be changed in the Rule Set rule.	Format: Check box Range: Check mark or no check mark Default: Not checked
Actions: This section specifies the possible settings for each action to be taken for this Rule Template. All conditions are supported by both requests and replies.		
New Action	Add a new Action to the list that is applied when the conditions of the Rule Template match on the message.	Format: Pulldown list Range: Actions listed in this section of this table.
Actions performed on the Diameter Header		
Modify Diameter Header Parts	Allows modifying or overwriting of the Version, Command Code, and Application ID components of the Diameter Header. **Note:** Modifying values in the Diameter Header can result in incompatibility with the standard defined in IETF RFC3588bis (draft-ietf_dime_rfc3588bix-26.txt) *Diameter Base Protocol*.	Header Part - the component to modify Format: Pulldown list Range: Version, Command Code, Application ID Default: Version Overwrite to - the new value of the component Format: Integer Range: New value; 8-bit, 24-bit, or 32-bit unsigned integer
Set Command Flags	Allows modifying of one or more Command Flags in the processed message, including the reserved flags: • Set Command Flag • Clear Command Flag • Keep original value Flags R, P, E, and T are supported; r4, r5, r6, and r7 are reserved for future use: • R - Request; shows whether the message is a Request or a Response.	Format: Radio buttons for each Command Flag, to set, clear, or keep the flag: Range: Set : R, P, E, T, r4, r5, r6, r7 Clear: R, P, E, T, r4, r5, r6, r7 Keep: R, P, E, T, r4, r5, r6, r7 Default: Keep original

Element	Description	Data Input Notes
	• P - Proxiable; shows if the message can be proxied, relayed, or redirected, or it must be locally processed. • E - Error; shows if the message cnotains protocol or semantic errors. • T - Shows that a message can potentially be a retransmitted message after a link fail-over, or is used to aid removal of duplicate messages.	
Actions performed on the Diameter Payload (AVPs) Most of these actions can be applied to a regular AVP, to a Grouped AVP, or to an AVP within the Grouped AVP. To perform the action on a regular or Grouped AVP, the suppored AVP definition from the dictionary and the inststance number or value must be specified. The value is valid only for some of the actions. For actions that are performed on an AVP within a Grouped AVP, the parent AVP and its instance number must be specified. If an AVP is not present in the dictionary, it is unknown by the Mediation feature and must be defined in the dictionary before the specified action can be performed. Many of the actions allow xl-values, which can be defined using the *Formatting Value Wizard*.		
Add AVP	Add an AVP to the message. The Flags and the Value must be set for the new AVP. For Grouped AVPs, • If the AVP is added within a Grouped AVP, the Parent AVP and its Instance must be specified. • A Parent AVP can be added if it not present in the message; Flags for the added Parent AVP must be set. • If the Parent AVP is not found in the message and is not added to the message, the action will fail. Flags V, M and P are supported; r3, r4, r5, r6 and r7 are reserved for future use. • V - Vendor-Specific; indicates whether the optional Vendor-ID field is present in the AVP header. When set, the AVP Code belongs to the specific vendor code address space.	Parent AVP: Format: Pulldown list Range: Available AVPs Instance: Format: Pulldown list Range: First, Second, Third Fourth, Fifth Add new AVP: Format: Pulldown list Range: Available AVPs Set Flags: Format: Check box for each flag Range: V, M, P, r3, r4, r5, r6, r7 Set Value: Format: Text box and link to *Formatting Value Wizard*, or pulldown list and link to Formatting Value Wizard

Element	Description	Data Input Notes
	• M - Mandatory; indicates whether support of the AVP is required. If an AVP with the M bit set is received by a Diameter client, server, proxy, or translation agent and either the ABP or its value is unrecognized, the message MUST be rejected. Diameter Relay and Redirect Agents MUST NOT reject messages with unrecognized AVPx. AVPs with the M bit cleared are informational only. A receiver of a message with an AVP that is not supported, or whose value is not supported, can simply ignore the AVP. • P - Indicates the need for encryption for end-to-end security. Diameter base protocol specifies which AVPs must be protected by end-to-end security measures (encryption) if the message is to pass through a Diameter agent. If a message includes any of those AVPs, the message must not be sent unless there is end-to-end security between the originator and the reciipient of the message.	Range: Add parent AVP if it is not present Format: Check box Range: Checked or unchecked
Delete AVP	Delete a specified AVP in the message. If the Instance of the specified AVP is All, the action is applied to all instances of the AVP in the message. If the specified AVP is within a Grouped AVP, the Parent AVP and its Instance must be specified. If the specified AVP is the last AVP within the Grouped AVP, the action can be defined to also delete the Parent AVP. If the specified AVP is a Grouped AVP, the Grouped AVP and all of the AVPs within the group are deleted. If the specified AVP is not found in the message, the Delete AVP action is considered to be successful.	Parent AVP: Format: Pulldown list Range: Available AVPs Instance: Format: Pulldown list Range: First, Second, Third Fourth, Fifth Delete AVP: Format: Radio button for Instance with pulldown list; radio button for With the value with text box or pulldown list and link to Formatting Value Wizard Range: Instance: First, Second, Third, Fourth, Fifth, All

Element	Description	Data Input Notes
		With the value: Text, or pulldown list values that vary with selected AVP to delete (see *Formatting Value Wizard*) Delete parent AVP if it is empty Format: Check box Range: Checked or unchecked; default is checked
Save AVP	Store a specified top-level AVP from the message into the buffer associated with the transaction. A saved AVP is stored in the buffer as long as the transaction exists. Saved AVPs can be accessed through the *Formatting Value Wizard* as corresponding Linking-AVPs with the same AVP and instance number. If the Instance of the specified AVP is All, the action saves all instances of the AVP in the message. **Note:** A grouped AVP can be saved and restored, but sub-AVPs within the stored or restored grouped AVP cannot be retrieved (such as with @msg.avp["name"][index].avp["name"][index]), modified, or removed. If the same AVP is saved multiple times (the action is applied multiple times), the saved value is overwritten each time the AVP is saved. If the specified AVP is not found in the message, the Save AVP action is considered to have failed.	Save AVP: Format: Pulldown list; radio button for Instance with pulldown list; radio button for With the value with text box or pulldown list and link to Formatting Value Wizard Range: Pulldown list: Available AVPs Instance: First, Second, Third, Fourth, Fifth, All With the value: Text, or pulldown list values that vary with selected AVP to delete (see *Formatting Value Wizard*)
Restore AVP	Restore a top-level AVP that has been previously stored. AVPs can be restored in the message by either appending each AVP to the message or by replacing all of the same existing AVPs. The instance number of the saved AVP must be specified, to find the appropriate Linking-AVP (LAVP) that was stored.	Restore AVP: Format: Pulldown list Range: Available AVPs Instance: Format: Pulldown list Range: First, Second, Third Fourth, Fifth

Element	Description	Data Input Notes
	Note: A grouped AVP can be saved and restored, but sub-AVPs within the stored or restored grouped AVP cannot be retrieved (such as with @msg.avp["name"][index].avp["name"][index]), modified, or removed.	Delete before restore: Format: Check box Range: Checked, unchecked; default is unchecked.

Set LAVP	Allows constructing a top-level non-Grouped AVP by setting the Flags and specifying the value, and placing it into the buffer associated with the Diameter transaction. The AVP can be accessed as a Linking-AVP through the *Formatting Value Wizard*.
	The value is stored in the buffer as long as the transaction exists. The LAVP can be used for the Restore AVP action.
	• Instance - A new AVP overwrites any existing AVP with the same instance number.
	• Set Value
	  • The Input field is available when the selected LAVP has a data format other than "Enumerated".
	  • The Pulldown list is available when the selected LAVP has the data format "Enumerated".
	  • An error message appears if the entered value of the Input field is not an x1-value and does not correspond to the data format required by the selected AVP.
	• Value type: Select the type of value that can be assigned to this Linking-AVP. Possible value types are the same as those for the Right value in the Conditions section of this page.
	• Default Value: Default value to assign to this Linking-AVP and to display on the **Rule Sets** page. Enter a 1 to 255 character string.
	• Descr: Add text here to describe this AVP. This description appears on the
		Set LAVP - Specifies the LAVP to be set into the buffer associated with the transaction.
		Format: Pulldown list
		Range: All non-Grouped AVPs from the dictionary
		Default: First non-Grouped AVP definition from the dictionary
		Instance - The instance number of the AVP within the buffer of the transaction.
		Format: Pulldown list
		Range: First, Second, Third, Fourth, Fifth
		Default: First
		Set Flags - (see Flag definitions in Add AVP)
		• If the flag must be set, the flag is checked and disabled.
		• If the flag must not be set, the flag is unchecked and disabled.
		• If the flag can be set, the check box is available to be changed.
		Format: Check boxes for the flags
		Range: V, M, P, r3, r4, r5, r6, r7
		Default: From the dictionary
		Set Value - Specifies the value of the LAVP.
		Input field
		Format: Value entered through the Formatting Value Wizard page (click the Wizard link).

Element	Description	Data Input Notes
	Rule Sets page. A maximum of 255 characters can be entered. • Optional: Click to make this AVP optional on the **Rule Sets** page. • Delete: Click to delete an existing Linking-AVP.	Range: Values available in the Formatting Value Wizard. Default: N/A Pulldown list: Format: Pulldown list Range: All of the values of the corresponding Enumerated Type Default: First value of the Enumerated Type
Actions that allow modifying an AVP If the specified AVP is not found in the message, the action is considered to have failed.		
Change AVP Code	Replace an AVP definition with a new one, keeping the original AVP value and flag that are not strictly defined in the dictionary (that can be set). Allows changing the Code of the specified AVP and modifying its Flags.	Parent AVP: Format: Pulldown list Range: Available AVPs Instance: Format: Pulldown list Range: First, Second, Third Fourth, Fifth Old AVP: Format: Pulldown list; radio button for Instance with pulldown list; radio button for With the value with text box or pulldown list and link to Formatting Value Wizard Range: Pulldown list: Available AVPs Instance: First, Second, Third, Fourth, Fifth With the value: Text, or pulldown list values that vary with selected AVP (see *Formatting Value Wizard*) New AVP Format: Pulldown list Range: Available AVPs

Element	Description	Data Input Notes
Change AVP Flags	Allows setting, clearing, and keeping the original value of AVP flags. Flags V, M and P are supported; r3, r4, r5, r6 and r7 are reserved for future use. • V - Vendor-Specific; indicates whether the optional Vendor-ID field is present in the AVP header. When set, the AVP Code belongs to the specific vendor code address space. • M - Mandatory; indicates whether support of the AVP is required. If an AVP with the M bit set is received by a Diameter client, server, proxy, or translation agent and either the ABP or its value is unrecognized, the message MUST be rejected. Diameter Relay and Redirect Agents MUST NOT reject messages with unrecognized AVPx. AVPs with the M bit cleared are informational only. A receiver of a message with an AVP that is not supported, or whose value is not supported, can simply ignore the AVP. • P - Indicates the need for encryption for end-to-end security. Diameter base protocol specifies which AVPs must be protected by end-to-end security measures (encryption) if the message is to pass through a Diameter agent. If a message includes any of those AVPs, the message must not be sent unless there is end-to-end security between the originator and the reciipient of the message.	Parent AVP Format: Pulldown list Range: Available AVPs Instance - The instance number of the AVP within the buffer of the transaction. AVP Format: Pulldown list; radio button for Instance with pulldown list; radio button for With the value with text box or pulldown list and link to Formatting Value Wizard; Set Flag, Clear Flag, and Keep original radio buttons for flags. Range: Pulldown list: Available AVPs Instance: First, Second, Third, Fourth, Fifth With the value: Text, or pulldown list values that vary with selected AVP (see *Formatting Value Wizard*) Flags: V, M, P, r3, r4, r5, r6, r7
Set AVP Value	Alows overwriting of the value of an AVP.	Parent AVP: Format: Pulldown list Range: Available AVPs Instance: Format: Pulldown list Range: First, Second, Third Fourth, Fifth AVP:

Element	Description	Data Input Notes
		Format: Pulldown list; radio button for Instance with pulldown list; radio button for With the value with text box or pulldown list and link to *Formatting Value Wizard* Range: Instance: First, Second, Third, Fourth, Fifth With the value: Text, or pulldown list values that vary with selected AVP (see *Formatting Value Wizard*) Set Value: Format: Text box or pulldown list and link to *Formatting Value Wizard* Range: Text, or pulldown list values that vary with selected AVP (see *Formatting Value Wizard*)
Strip from AVP Value	Strips the defined number of characters from either the beginning or the ending of the AVP value. This action can be used in combination with the Prefix/Suffix to AVP Value action.	Parent AVP: Format: Pulldown list Range: Available AVPs Instance: Format: Pulldown list Range: First, Second, Third Fourth, Fifth AVP: Format: Pulldown list; radio button for Instance with pulldown list; radio button for With the value with text box and link to *Formatting Value Wizard* Range: Pulldown list: Available AVPs Instance: First, Second, Third, Fourth, Fifth With the value: Text (see *Formatting Value Wizard*) Strip from: Format: Radio buttons, text box

Element	Description	Data Input Notes
		Range: Radio button for Beginning of the value; radio button for End of the value; text - number of characters to strip
Prefix/Suffix to AVP Value	Add the defined data as a prefix or suffix to the AVP value. This action can be used in combination with the Strip for AVP Value action.	Parent AVP: Format: Pulldown list Range: Available AVPs Instance: Format: Pulldown list Range: First, Second, Third Fourth, Fifth AVP: Format: Pulldown list; radio button for Instance with pulldown list; radio button for With the value with text box and link to Formatting Value Wizard; radio buttons for Prefix or Suffix; text box for prefix or suffix with link to *Formatting Value Wizard* Range: Pulldown list: Available AVPs Instance: First, Second, Third, Fourth, Fifth With the value: Text box (see *Formatting Value Wizard*) Radio buttons: Prefix to the value, Suffix to the value Text: The prefix or suffix (see *Formatting Value Wizard*)
Substitute in AVP Value	Use a defined pattern to locate a field in the AVP value, and replace the data in the field with the specified new data.	Parent AVP: Format: Pulldown list Range: Available AVPs Instance: Format: Pulldown list Range: First, Second, Third Fourth, Fifth

Element	Description	Data Input Notes
		AVP: Format: Pulldown list; radio button for Instance with pulldown list; radio button for With the value with text box and link to *Formatting Value Wizard* Range: Pulldown list: Available AVPs Instance: First, Second, Third, Fourth, Fifth With the value: Text box (see *Formatting Value Wizard*) Pattern: Format: Text box Range: Patten to locate the field Replacement: Format: Text box Range: Text of the replacement data (see *Formatting Value Wizard*)
Other Actions		
Execute Rule template	**Note:** The value needs to be set at the time the new Rule Template is defined. Only Rule Templates in "Test" or "Active" state are listed in the pulldown list. This field is displayed on **Diameter Mediation Rule Template** Insert and Edit pages, but not on the View page.	Format: Pulldown list Range: Available Rule Templates in "Test" and "Active" states Default: First Rule Template Name in the list
Exit from Execution Trigger	Exits from the Execution Trigger, bypassing any subsequent Rule Set associated with it.	N/A

Table 91: Rule Template Condition Operators describes the Operators that can be used between the Left Value and the Right value in a Rule Template Condition.

The value can be an AVP, another part of a Diameter message, a constant, or an internal variable.

Table 91: Rule Template Condition Operators

Operator	Operator Type	Returns true when...
		Example of use
equals (==)	Generic	Value exists AND equals...
		@msg.command.code==316
does not equal (!=)	Generic	Value does not exist OR does not equal...
		@msg.command.code!=316
begins with (longest match) (=^^)	String	Value exists AND begins with (longest match)...
		@msg.avp["Destination-Realm"]=^^test
begins with (=^)	String	Value exists AND begins with...
		@msg.avp["Destination-Realm"]=^testlb
does not begin with (!=^)	String	Value does not exist OR does not begin with...
		@msg.avp["Destination-Realm"]!=^testlb
ends with (=$)	String	Value exists AND ends with...
		@msg.avp["Origin-Host"][1]=$entity.com
does not end with (!=$)	String	Value does not exist OR does not end with...
		@msg.avp["Origin-Host"][1]!=$entity.com
regular expression match (=~)	String	Value exists AND matches the regular expression...
		@msg.avp[Session-Id]!=~.*\.example\..*
regular expression does not match (!=~)	String	Value does not exist OR does not match the regular expression...
		@msg.avp["Session-Id"]!=~.*\example\..*
less than (<)	Numeric	Value exists AND is less than...
		@msg.avp["Validity-Time"]<30
greater than (>)	Numeric	Value exists AND is greater than...
		@msg.avp["Validity-Time"]>30
less than or equal to (<=)	Numeric	Value exists AND is less than or equal to...
		@msg.avp["Validity-Time"]<=30
greater than or equal to (>=)	Numeric	Value exists AND is greater than or equal to...
		@msg.avp["Validity-Time"]>=30
is within	Subnet	Value exists AND is within...

Operator	Operator Type	Returns true when... Example of use
		@msg.avp["Served-Party-IP-Address] is within 192.168.0.0/24
is not within	Subnet	Value does not exist OR is not within... @msg.avp["Served-Party-IP-Address] is not within 192.168.0.0/24
exists		AVP specified as Left value exists... @msg.avp["Vendor-Specific-Application"] exists
does not exist		AVP specified as Left value does not exist... @msg.avp["Vendor-Specific-Application"] does not exist
is true		AVP specified as Left value exists AND it is not empty/non-zero... @msg.avp["Disconnect-Cause"] is true
is false		AVP specified as Left value does not exist OR it is empty/0... @msg.avp["Disconnect-Cause"] is false
"is true" and "is false" work only on numbers (Integer32, Integer32, Unsigned32, Unsigned64, Float32, Float64, Enumeratied, Time) and strings (OctetString, UTF8String, DiameterIdentity, DiameterURI). For an IP Address, "is true" always succeeds; the address can be converted to a string that is never empty. If the condition cannot be evaluated (for example, the AVP does not exist or the xl-value is imcompatible), then "is true" will fail and "is false" will succeed.		

Based on the type of operator selected, the Left value and the Right value are converted according to the rules in *Table 92: Rule Template Condition Conversion Rules*.

Table 92: Rule Template Condition Conversion Rules

Left value Type	Operator Type	Right value Type	Conversion
-	String	-	Convert Left value and Right value to strings.
-	Numeric	-	Convert Left value and Right value to numbers.
-	Subnet	-	Convert Left value to an IP address. Convert Right value to a subnet
String	Generic	String	No conversion is needed.

Left value Type	Operator Type	Right value Type	Conversion
Numeric	Generic	Numeric	No conversion is needed.
IP address	Generic	IP address	No conversion is needed.
String	Generic	Numeric	Convert Left value to a number.
Numeric	Generic	String	Convert Right value to a number.
IP address	Generic	String	Convert Right value to an IP address.
String	Generic	IP address	Convert Left value to an IP address.
None of these cases			Conversion cannot be done.
Operators by Type (see also *Table 91: Rule Template Condition Operators*)			
String	=~, !=~, =^, =^^, !=^, =$, !=$		
Numeric	<, >, <=, >=		
Subset	is within, is not within		
Generic	==, !=		

The conversion fails if the input value is reasonably not convertible to the new format (such as the numeric input cannot be converted to an IP Address).

If the conversion is impossible or fails, the condition is evaluated to false unless the operator is negated (begins with !, or "is not within").

For float to string conversion, the double argument is rounded and converted to decimal notation in the style [-]ddd.dddddd, with 6 characters of precision. If the conversion does not fit into 21 characters, then it will fail.

For IPv6 to string conversion, the following rules apply:

- Leading zeros are ignored (01->1)
- Lowercase to uppercase (ffff->FFFF)
- 1:0:0:0:0:0:0:0->1:0:0:0:0:0:0:0
- 1::2->1:0:0:0:0:0:0:2
- ::ffff->0:0:0:0:0:0:0:FFFF
- ffff::->FFFF:0:0:0:0:0:0:
- ::->0:0:0:0:0:0:0:0

Rule Templates Help elements

When Set Help is clicked for an existing Rule Template on the **Diameter Mediation Rule Templates** page, the following information appears:

Element	Description	Data Input Notes
Title	Title to appear at the top of the Help page. This field is required when providing Help.	Format: Text string Range: 1-64 characters
Text	Detailed explanation of this Rule Set: how to use it and description of any interrelated features.	Format: Text string (HTML tags allowed) Range: 1 - 10000 characters
Path	(Generated and used by software)	

Formatting Value Wizard elements

When [wizard] is clicked, the information shown in *Table 93: Formatting Value Wizard elements* appears:

Table 93: Formatting Value Wizard elements

Element	Description
Value	The value of the variable in xl-format. The components of this value can be entered manually, by clicking on one or more specifiers, or both.
Specifiers	List of elements that can be part of an xl-formatted string. A specifier is either a single item, or a group of items forming a sublist. Every specifier that is selected is put into the Value field where the cursor is currently located. The Specifiers are described in *Table 94: Formatting Value Wizard Specifiers*.
Preview	The readable description of the xl-formatted string in the Value field.

The specifiers described in *Table 94: Formatting Value Wizard Specifiers* can be used to create or update the variables in the Value field.

Note: [Index] that is either a [<number>] or [any] can be excluded from all of the expressions that refer to the first instance of the AVP.

The instance number "any" can be present in the Left value of the Condition only once.

The instance number "any" can be present in the Right value of the Condition only once.

Table 94: Formatting Value Wizard Specifiers

Specifier			
New Line	Sub-Items	xl-formatted Value	Preview Value
		\r\n	 (This causes a line break on the GUI screen.)

Specifier			
String Constant	Type the string constant	string constant	{"string constant"}
Diameter Head	Sub-Items	xl-formatted Value	Preview Value
	Version	@msg.version	{Version}
	Message Length	@msg.length	{Message Length}
	Command Flags: R	@msg.command.flags.R	{R Command Flag}
	Command Flags: P	@msg.command.flags.P	{P Command Flag}
	Command Flags: E	@msg.command.flags.E	{E Command Flag}
	Command Flags: T	@msg.command.flags.T	{T Command Flag}
	Command Flags: r4	@msg.command.flags.r4	{r4 Command Flag}
	Command Flags: r5	@msg.command.flags.r5	{r5 Command Flag}
	Command Flags: r6	@msg.command.flags.r6	{r6 Command Flag}
	Command Flags: r7	@msg.command.flags.r7	{r7 Command Flag}
	Application ID	@msg.application_id	{Application ID}
	Hop-by-Hop Identifier	@msg.hbh_id	{Hop-to-Hop Identifier}
	End-to-End Identifier	@msg.e2e_id	{End-to-End Identifier}
AVP	Sub-Items		
	Parent AVP Pulldown list containing all AVP definitions from the dictionary that have the type "Grouped".		
	Parent AVP Instance number Pulldown list containing the index of the Parent AVP, if a Parent AVP is selected (First, Second, Third, Fourth, Fifth).		
	AVP Pulldown list containing all AVP definitins from the dictionary (except for the case where the selected Parent AVP is grouped; then only those AVPs that belont the group are available).		
	AVP instance number Pulldown list containing the indexes of AVP (First, Second, Third, Fourth, Fifth, Any).		
	AVP Component Pulldown list containing the following components: • Data • Data Length		

Specifier	
	• AVP Code • Flag V • Flag M • Flag P • Flag r3 • Flag r4 • Flag r5 • Flag r6 • Flag r7 • Vendor-ID Flags V, M, and P are supported; flags r3, r4, r5, r6, and r7 are reserved for future use.
	xl-formatted Value
	@msg.avp[“name”] @msg.avp[“name”][index] @msg.avp[“name”][index].code @msg.avp[“name”][index].flags.V @msg.avp[“name”][index].flags.M @msg.avp[“name”][index].flags.P @msg.avp[“name”][index].flags.r3 @msg.avp[“name”][index].flags.r4 @msg.avp[“name”][index].flags.r5 @msg.avp[“name”][index].flags.r6 @msg.avp[“name”][index].flags.r7 @msg.avp[“name”][index].vendor_id @msg.avp[“name”][index].data @msg.avp[“name”][index].data_length @msg.avp[“name”][index].avp[“name”][index] @msg.avp[“name”][index].avp[“name”][index].code @msg.avp[“name”][index].avp[“name”][index].flags.V @msg.avp[“name”][index].avp[“name”][index].flags.M @msg.avp[“name”][index].avp[“name”][index].flags.P @msg.avp[“name”][index].avp[“name”][index].flags.r3 @msg.avp[“name”][index].avp[“name”][index].flags.r4 @msg.avp[“name”][index].avp[“name”][index].flags.r5 @msg.avp[“name”][index].avp[“name”][index].flags.r6

Specifier	
	@msg.avp[“name”][index].avp[“name”][index].flags.r7 @msg.avp[“name”][index].avp[“name”][index].vendor_id @msg.avp[“name”][index].avp[“name”][index].data @msg.avp[“name”][index].avp[“name”][index].data_length
	Preview Value
	{AVP:“Name”} {AVP:“Name”[Index]} {AVP:“Name”[Index].Code} {AVP:“Name”[Index].Flag V} {AVP:“Name”[Index].Flag M} {AVP:“Name”[Index].Flag P} {AVP:“Name”[Index].Flag r3} {AVP:“Name”[Index].Flag r4} {AVP:“Name”[Index].Flag r5} {AVP:“Name”[Index].Flag r6} {AVP:“Name”[Index].Flag r7} {AVP:“Name”[Index].Vendor-ID} {AVP:“Name”[Index].Data} {AVP:“Name”[Index].Data_Length} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index]} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Code} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Flag V} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Flag M} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Flag P} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Flag r3} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Flag r4} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Flag r5} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Flag r6} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Flag r7} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Vendor-ID} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Data} {AVP:“Parent AVP Name”[Index]."AVP Name"[Index].Data_Length}

Specifier	
Linking AVP	Sub-Items
	Parent Linking-AVP Pulldown list containing all AVP definitions from the dictionary that have the type "Grouped".
	Parent Linking-AVP Instance number Pulldown list containing the indexes of the Parent AVP (First, Second, Third, Fourth, Fifth, Any).
	Linking-AVP Pulldown list containing all AVP definitions from the dictionary (except for the case where the selected Parent AVP is grouped; then only those AVPs that belong to the group are available). **Note:** Sub-LAVPs within a grouped LAVP cannot be retrieved (such as with @msg.avp["name"][index].avp["name"][index]), modified, or removed.
	Linking-AVP Instance number Pulldown list containing the indexes of the AVP. (First, Second, Third, Fourth, Fifth, Any)
	Linking-AVP Component Pulldown list containing the following components: • AVP Code • Flag V • Flag M • Flag P • Flag r3 • Flag r4 • Flag r5 • Flag r6 • Flag r7 • Vendor ID • Data • Data Length Flags V, M, and P are supported; flags r3, r4, r5, r6, and r7 are reserved for future use.
	xl-formatted Value
	@store.avp[“name”] @store.avp[“name”][index] @store.avp[“name”][index.code] @store.avp[“name”][index].flags.V

Specifier	
	@store.avp[“name”][index].flags.M @store.avp[“name”][index].flags.P @store.avp[“name”][index].flags.r3 @store.avp[“name”][index].flags.r4 @store.avp[“name”][index].flags.r5 @store.avp[“name”][index].flags.r6 @store.avp[“name”][index].flags.r7 @store.avp[“name”][index].length @store.avp[“name”][index].vendor_id @store.avp[“name”][index].avp[“name”][index] @store.avp[“name”][index].avp[“name”][index].code @store.avp[“name”][index].avp[“name”][index].flags.V @store.avp[“name”][index].avp[“name”][index].flags.M @store.avp[“name”][index].avp[“name”][index].flags.P @store.avp[“name”][index].avp[“name”][index].flags.r3 @store.avp[“name”][index].avp[“name”][index].flags.r4 @store.avp[“name”][index].avp[“name”][index].flags.r5 @store.avp[“name”][index].avp[“name”][index].flags.r6 @store.avp[“name”][index].avp[“name”][index].flags.r7 @store.avp[“name”][index].avp[“name”][index].vendor-id @store.avp[“name”][index].avp[“name”][index].data @store.avp[“name”][index].avp[“name”][index].data_length
	Preview Value
	{LAVP:“Name”} {LAVP:“Name”[Index]} {LAVP:“Name”[Index].Code} {LAVP:“Name”[Index].Flag V} {LAVP:“Name”[Index].Flag M} {LAVP:“Name”[Index].Flag P} {LAVP:“Name”[Index].Flag r3} {AVP:“Name”[Index].Flag r4} {AVP:“Name”[Index].Flag r5}

<table>
<tr><td>Specifier</td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3">{LAVP:“Name”[Index].Flag r6}
{LAVP:“Name”[Index].Flag r7}
{LAVP:“Name”[Index].Vendor-ID
{LAVP:“Name”[Index].Data}
{LAVP:“Name”[Index].Data_Length}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index]}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Code}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Flag V}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Flag M}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Flag P}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Flag r3}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Flag r4}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Flag r5}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Flag r6}
{AVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Flag r7}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Vendor-ID}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Data}
{LAVP:“Parent LAVP Name”[Index]."LAVP Name"[Index].Data_Length}</td></tr>
<tr><td>Functions</td><td>Sub-Items</td><td>xl-formatted Value</td><td>Preview Value</td></tr>
<tr><td></td><td>Length of</td><td>strlen(<string></td><td>{Length of (<string>)}</td></tr>
<tr><td></td><td colspan="3">Used to determine the length of a number and then to determine if additional digits should be prepended or removed.
For example, if a 7-digit number is received, a default area code might have to be prepended to the number.
“Length of” always works on string types. If the parameter happens to be a number, then it will be automatically treated as a string by these functions. Hence, strlen(123) will work the same as strlen("123"), and return 3.
The input of the function "string" might include other xl-values such as contants, Diameter Header parts, AVP or LAVP parts, or other functions.</td></tr>
<tr><td></td><td>Hash</td><td>hash(<string>, <range>)</td><td>{Hash (<string>), <range>)}</td></tr>
<tr><td></td><td colspan="3">Used for making a routing decision based on the hash generated on the "session-id" AVP. This AVP is present in charging messages such as ACR and CCR.
For example, if session-id hashes to 1, then set dest-host to host1, if it hashes to 2, then set dest-host to host2.</td></tr>
</table>

<table>
<tr><td>Specifier</td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3">Because all messages in a session need to go to the same host and they all have the same session-id, the mechanism can be used to send them to the same host without maintaining state.
The input of the function "string" might include other xl-values such as contants, Diameter Header parts, AVP or LAVP parts, or other functions.</td></tr>
<tr><td></td><td>Substring</td><td>substr(<string>, <position>,<length>)
Postion can be negative, (counted from the end).</td><td>Substring (<string>,<position>, <length>)}</td></tr>
<tr><td></td><td colspan="3">Used to inspect a part of a string or number and make changes if needed.
For example, if the first 4 characters match "+011", then delete the characters.
“Substring” works always on string types.
The input of the function "position" specifies the position(character) at whch the counting of the substring will start. Position 0 inidcates the first character of the string. -1 indicates the last character of the string.
The input of the function "length" specifies the number of characters to include in the substring.
The specified substring will be extracted.
For example: substr(@msg.avp["APN-OI-Replacement"][1],0,5)</td></tr>
<tr><td></td><td>X hours</td><td>hour2sec(<hours>)</td><td>{<x>hours}</td></tr>
<tr><td></td><td>Y minutes</td><td>min2sec(<minutes>)</td><td>{<y>minutes}</td></tr>
<tr><td></td><td>GMT</td><td>time( )</td><td>{GMT time}</td></tr>
<tr><td></td><td colspan="3">Can be used to perform time of day routing.
Certain AVPs carry time, which can be compared against a specified hour and minute to perform time of day routing.
The inputs "hours" or "minutes" might include other xl-values.</td></tr>
<tr><td>Operators</td><td>Provide the ability to perform mathematical operations on the AVP.
• Plus
• Minus</td><td>• +
• -</td><td>• +
• -</td></tr>
<tr><td>Back Reference</td><td>Number of occurence of the back reference: input field for one digit; default is 0.</td><td>\<number></td><td>\<number></td></tr>
</table>

Specifier	
	Because Back Reference can be part of only a replacement string, this specifier is presented only for the Substitute in AVP Value Action.

Mediation Enumerations elements

Table 95: Mediation Enumeration elements describes the fields on the **Diameter Mediation Enumerations** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 95: Mediation Enumeration elements

Element	Description	Data Input Notes
Name	Name used to label this Enumeration Type in the system. A unique value is required in this field.	Format: String, with valid characters a-z, A-Z, 0-9, dash (-), period (.), @, and underscore (_) Range: 1-64 characters
Values	Comma-separated list of possible values. The allowed values are comma-separated items, which might optionally contain colons. If an item contains a colon, then everything before the colon is a label and everything after the colon is a value. If an item does not contain a colon, then the value and the label are the same. A value is required in this field.	Format: List of values that can be separate items (a,b,c) or in the form of <label>:<value> (a:1, b:2,c:3). Range: 1-2048 characters

Mediation Triggers elements

Table 96: Mediation Triggers elements describes the fields on the **Diameter Mediation Triggers** and **Diameter Mediation Triggers [Insert]** pages. Data Input Notes apply only to the **Diameter MediationTriggers [Insert]** page; the Triggers page is read-only.

Table 96: Mediation Triggers elements

Element	Description	Data Input Notes
Rule Set Name	The name of each Rule Set that is associated with a Trigger and executed by the triggering point. .	Triggers page: The Rule Sets that are associated with a Trigger are listed under the name of the associated Trigger.

Element	Description	Data Input Notes
		Triggers [Insert] page: Format: Pulldown list Range: The Rule Sets (supported by the Trigger and in the "Active" or "Test" state) are listed in the Rule Set Name pulldown list. Default: First Rule Set that is supported by the Trigger and is in the "Active" or "Test" state.
Live	A yes sign (check mark) indicates that the Rule Set has been set to the "Active" state (enabled for the live traffic).	The Rule Set state is set on the **State & Properties** page for the Rule Template Name that corresponds to the Rule Set.

Mediation State & Properties elements

Table 97: Mediation State & Properties elements describes the fields on the **Diameter Mediation State & Properties** and **Diameter Mediation State & Properties [Edit]** pages. Data Input Notes apply only to the **Diameter Mediation State & Properties [Edit]** page; the **Diameter Mediation State & Properties** page is read-only.

Table 97: Mediation State & Properties elements

Element	Description	Data Input Notes
Rule Template Name	The name of a configured Rule Template.	The **Diameter Mediation State & Properties [Edit]** page shows Selected Rule Template; the Name cannot te edited.
State	The state of the Rule Template. "Development" - the Rule Template is disabled for any live or test traffic; it is under development. "Test" - the the Rule Sets entry is generated and the Rule Set is enabled only for the special test messages. "Active" - the Rule Template and Rule Set are enabled for any kind of traffic.	Format: pulldown list Range: Development (only for creating and modifying Rule Templates), Test, Active Default: Development

Element	Description	Data Input Notes
Action Error Handling	Specifies the type of error handling to be used if an Action in a Rule Template fails.	Format: pulldown list Ramge: ignore the error, immediately exit from the rule template, immediately exit from the trigger point Default: ignore the error

Mediation Base Dictionary elements

Table 98: Mediation Base Dictionary Elements describes the fields on the **Mediation Base Dictionary** view-only pages.

Table 98: Mediation Base Dictionary Elements

Field	Description	Data Notes
Attribute Name	Name of the AVP; the unique combination of AVP Code - Vendor Id.	Format: alphanumeric, underscore (_), and dash (-). Range: 1 - 255 characters
AVP Code	AVP Code	Format: numberic Range: 0-4294967295
Vendor-ID	Vendor-ID	Format: pulldown list Range: all configured Vendors
Flags	Setting indicator for AVP Flags: V, M, P, r3, r4, r5, r6, r7 Flags V, M, and P are supported; r3, r4, r5, r6 and r7 are reserved for future use. • V - Vendor-Specific; indicates whether the optional Vendor-ID field is present in the AVP header. When set, the AVP Code belongs to the specific vendor code address space. • M - Mandatory; indicates whether support of the AVP is required. If an AVP with the M bit set is received by a Diameter client, server, proxy, or translation agent and either the AVP or its value is unrecognized, the message	Format: 3 buttons for each flag Range: Must, Must Not, May be set for each flag

Field	Description	Data Notes
	MUST be rejected. Diameter Relay and Redirect Agents MUST NOT reject messages with unrecognized AVPs. AVPs with the M bit cleared are informational only. A receiver of a message with an AVP that is not supported, or whose value is not supported, can simply ignore the AVP. • P - Indicates the need for encryption for end-to-end security. Diameter base protocol specifies which AVPs must be protected by end-to-end security measures (encryption) if the message is to pass through a Diameter agent. If a message includes any of those AVPs, the message must not be sent unless there is end-to-end security between the originator and the reciipient of the message.	
Data Type	AVP data format If the Data Type is "Enumerated", the name of the Enumerated Type is indicated in the dictionary. If the Data Type is "Grouped", the list of grouped AVPs is included in the dictionary.	Format: pulldown list Range: all available AVP data formats
Include AVP in the group	Include an AVP into the Grouped AVP This field is active when the selected Data Type is Grouped.	Format: pulldown list, Add AVP and Delete AVP buttons Range: all available AVPs from the Base Dictionary and the Custom Dictionary. If a Base Dictionary entry has been overwritten in the Custom Dictionary, only the Custom Dictionary entry appears in the list.
Protocol	Protocol standard where the AVP is defined.	Format: string Range: up to 64 characters

Mediation Custom Dictionary elements

Table 99: Mediation Custom Dictionary Elements describes the fields on the **Mediation Custom Dictionary** view, insert, and edit pages.

Table 99: Mediation Custom Dictionary Elements

Field	Description	Data Input Notes
Attribute Name	Name of the AVP; the unique combination of AVP Code - Vendor Id. The field is required.	Format: alphanumeric, underscore (_), and dash (-). Range: 1 - 255 characters
AVP Code	AVP Code The field is required.	Format: numberic Range: 0-4294967295
Vendor-ID	Vendor-ID The field is required.	Format: pulldown list Range: all configured Vendors
Flags	AVP Flags V, M, P, r3, r4, r5, r6, r7 When the operator tries to modify the AVP flags in the message, setting and clearing of the flag depends on the value defined in the dictionary. If the flag has a value "Must" be set or "Must Not" be set, modifying of the flag is restricted accordingly. If the flag has a value of "May" be set, the operator can change the flag without any limitations. Flags V, M and P are supported; r3, r4, r5, r6 and r7 are reserved for future use. • V - Vendor-Specific; indicates whether the optional Vendor-ID field is present in the AVP header. When set, the AVP Code belongs to the specific vendor code address space. • M - Mandatory; indicates whether support of the AVP is required. If an AVP with the M bit set is received by a Diameter client, server, proxy, or translation agent and either the ABP or its value is unrecognized, the message MUST be rejected. Diameter Relay and Redirect Agents MUST NOT reject messages with unrecognized AVPs. AVPs	Format: 3 buttons for each flag Range: Must, Must Not, May for each flag

Field	Description	Data Input Notes
	with the M bit cleared are informational only. A receiver of a message with an AVP that is not supported, or whose value is not supported, can simply ignore the AVP. • P - Indicates the need for encryption for end-to-end security. Diameter base protocol specifies which AVPs must be protected by end-to-end security measures (encryption) if the message is to pass through a Diameter agent. If a message includes any of those AVPs, the message must not be sent unless there is end-to-end security between the originator and the recipient of the message.	
Data Type	AVP Data Format The field is requried.	Format: pulldown list Range: all available AVP data formats
Include AVP in the group (insert and edit pages only)	Include an AVP into the Grouped AVP This field is active when the selected Data Type is Grouped. To include another AVP in the Grouped AVP, click on the Add AVP button. A new row for AVP selection appears. To remove an AVP from the Grouped AVP, click on the Delete AVP button.	Format: pulldown list, Add AVP and Delete AVP buttons Range: all available AVPs from the Base Dictionary and the Custom Dictionary. If a Base Dictionary entry has been overwritten in the Custom Dictionary, only the Custom Dictionary entry appears in the list.
Protocol	Protocol standard where the AVP is defined. The field is required.	Format: string Range: up to 64 characters

Mediation All-AVP Dictionary elements

Table 100: Mediation All-AVP Dictionary elements describes the fields on the **Mediation All-AVP Dictionary** pages.

Table 100: Mediation All-AVP Dictionary elements

Field	Description	Data Notes
Attribute Name	Name of the AVP; the unique combination of AVP Code - Vendor Id.	Format: alphanumeric, underscore (_), and dash (-). Range: 1 - 255 characters
AVP Code	AVP Code	Format: numberic Range: 0-4294967295
Vendor-ID	Vendor-ID	Format: pulldown list Range: all configured Vendors
Flags	AVP Flags V, M, P, r3, r4, r5, r6, r7 Flags V, M, and P are supported; r3, r4, r5, r6 and r7 are reserved for future use. • V - Vendor-Specific; indicates whether the optional Vendor-ID field is present in the AVP header. When set, the AVP Code belongs to the specific vendor code address space. • M - Mandatory; indicates whether support of the AVP is required. If an AVP with the M bit set is received by a Diameter client, server, proxy, or translation agent and either the AVP or its value is unrecognized, the message MUST be rejected. Diameter Relay and Redirect Agents MUST NOT reject messages with unrecognized AVPs. AVPs with the M bit cleared are informational only. A receiver of a message with an AVP that is not supported, or whose value is not supported, can simply ignore the AVP. • P - Indicates the need for encryption for end-to-end security. Diameter base protocol specifies which AVPs must be protected by end-to-end security measures (encryption) if the message is to pass through a Diameter agent. If a message includes any of those AVPs, the message must not be sent unless there is end-to-end security between the	Format: 3 buttons for each flag Range: Must, Must Not, May for each flag

Field	Description	Data Notes
	originator and the recipient of the message.	
Data Type	AVP Data Format	Format: pulldown list Range: all available AVP data formats
Include AVP in the group	Include an AVP into the Grouped AVP This field is active when the selected Data Type is Grouped.	Format: pulldown list, Add AVP and Delete AVP buttons Range: all available AVPs from the Base Dictionary and the Custom Dictionary. If a Base Dictionary entry has been overwritten in the Custom Dictionary, only the Custom Dictionary entry appears in the list.
Protocol	Protocol standard where the AVP is defined.	Format: string Range: up to 64 characters

Mediation Vendors elements

Table 101: Mediation Vendors elements describes the fields on the **Vendors** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 101: Mediation Vendors elements

Element	Description	Data Input Notes
Vendor-ID	A number that identifies the Vendor. The number must be unique within the Custom Dictionary. The field is required.	Format: 32-bit integer Range: 1-4294967295
Vendor Name	Name of a Vendor that implements a Vendor-Specific Diameter AVP.	Format: Character string Range: 1-255 characters

Element	Description	Data Input Notes
	A unique name is required in this field.	

FABR Configuration Elements

The tables in this section describe the elements that can be configured using the Full Address Based Resolution (FABR) application GUI pages in the DSR software.

Applications configuration elements

This table describes the fields on the Applications View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 102: Applications Configuration Elements

Field	Description	Data Input Notes
Application ID	Application ID in a Diameter message The Application ID is an IANA-assigned Diameter Application ID, which is a 32-bit field that is mandatory in all Diameter messages. It is commonly used for screening and routing messages between Diameter nodes. If a combination of the Application ID and Command Code already exists, an error message appears.	Format: Radio button to select Pulldown list or text box entry Range: Available Application IDs (0–4294967295)
Application Name	Name of the Application corresponding to the Application ID. If provisioned, this overrides any existing application name.	Format: Alphanumeric and underscore (_) Range: 1–32 characters; Must contain at least one alphabetic character and must start with alphanumeric or underscore.
Routing Mode (Read only)	Method of routing for Request messages received containing the Diameter Application ID	Format: Disabled pulldown list with a value of Proxy.

Exceptions configuration elements

This table describes the fields on the Exceptions View and Edit pages only.

Table 103: Exceptions Configuration Elements

Field	Description	Data Input Notes
Application ID (Read only)	Application ID in a Diameter message	N/A
Application Name (Read only)	Name of the application corresponding to the Application ID	N/A
Routing Exception Type (Read only)	The routing exception that prevented address resolution. This field displays one of the following values: • Invalid command code • Valid address not found • Valid address was found did not match a provisioned address or address range	N/A
Routing Exception Action	Action that FABR takes associated with the Routing Exception Type	Format: Radio buttons Range: • Forward Unchanged • Forward to Destination • Send Answer with Result-Code AVP • Send Answer with Experimental-Result AVP • Abandon Request
Destination	Destination to where the message is forwarded associated with the Routing Exception Type. This field is enabled when the Routing Exception Action is set to Forward to Destination.	Format: Pulldown list Range: Available user-configured destinations
Result-Code Value	Answer code associated with this Routing Exception Type. This field is enabled when the Routing Exception Action is set to either Send Answer with Result-Code AVP or Send Answer with Experimental-Result AVP.	Format: • Selection text box; numeric • Selection pulldown list Range: • Selection box: 1000–5999 • Selection pulldown list: available Diameter answer codes

Field	Description	Data Input Notes
Vendor-ID	Value returned in the Vendor-ID AVP of the answer message associated with this Routing Exception Type. This field is enabled when the Routing Exception Action is set to Send Answer with Experimental-Result AVP.	Format: Text box; numeric Range: 1–4294967295
Error Message	Value returned in the Error-Message AVP of the answer message. This field is enabled when the Routing Exception Action is set to either Send Answer with Result-Code AVP or Send Answer with Experimental-Result AVP.	Range: 0–64 characters Default: Null string

Default Destinations configuration elements

This table describes the fields on the Default Destinations View, Insert, and Edit pages.

Table 104: Destinations Configuration Elements

Field	Description	Data Input Notes
Name	Unique name of the Destination If a duplicate Name is entered or the Name is not specified, an error message appears.	Format: Alphanumeric and underscore (_) Range: 1–32 characters; cannot start with a digit and must contain at least one alphabetic character
Realm	Realm of the Default Destination The Realm and Fully Qualified Domain Name cannot both be empty; otherwise, an error message appears.	Format: Text box; Realm is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a Realm must be at most 255 characters long. At least Realm or Fully Qualified Domain
Fully Qualified Domain Name	Unique Fully Qualified Domain Name of the Default Destination If a duplicate FQDN is entered, an error message appears. The Fully Qualified Domain Name and Realm cannot both be empty; otherwise, an error message appears.	

Field	Description	Data Input Notes
		Name is required to configure a Destination.[Default = n/a; Range = A valid Realm.]

Address Resolutions configuration elements

This table describes the fields on the Address Resolutions View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 105: Address Resolutions Configuration Elements

Field	Description	Data Input Notes
Application ID	Application ID in a Diameter message The Application ID is an IANA-assigned Diameter Application ID, which is a 32-bit field that is mandatory in all Diameter messages. It is commonly used for screening and routing messages between Diameter nodes. If a combination of the Application ID and Command Code already exists, an error message appears.	Format: Pulldown list Range: Available Application IDs (0–4294967295)
Command Code	Command Code in a Diameter message If a combination of the Application ID and Command Code already exists, an error message appears.	Format: Pulldown list Range: Available Command Codes
Primary Routing Entity and Secondary Routing Entity sections		
Routing Entity	Routing Entity type The same Routing Entity Type cannot be selected for both the Primary and the Secondary Routing Entity; if the same type is selected, an error message appears. If the Routing Entity Type is not specified for the Primary Routing Entity, an error message appears.	Format: Pulldown list Range: • IMSI • MSISDN • IMPI • IMPU
Primary AVP	Primary AVP used for extracting the Routing Entity address The same Primary AVP and Secondary AVP cannot be selected for either the Primary Routing Entity or for the Secondary Routing Entity; if the same AVP is selected, an error message appears.	Format: Pulldown list Will be used for extracting the Routing Entity address. Range of User Identity routing entity types include:

Field	Description	Data Input Notes
	If Primary AVP is not selected for the Primary Routing Entity, an error message appears.	• Public Identity • ServiceInfo.Subscription-Id(0) • ServiceInfo.Subscription-Id(1) • ServiceInfo.Subscription-Id(2) • ServiceInfo.Subscription-Id(3) • Subscription-Id(0) • Subscription-Id(1) • Subscription-Id(2) • Subscription-Id(3) • UserIdentity.MSISDN • UserIdentity.Public-Identity • UserName • Wildcarded-Public-Identity
Secondary AVP	Secondary AVP used for extracting the Routing Entity address The same Primary AVP and Secondary AVP cannot be selected for either the Primary Routing Entity or for the Secondary Routing Entity; if the same AVP is selected, an error message appears.	
Destination Type	Type of Destination for this Routing Entity Type.	Format: Pulldown list Range: • IMS-HSS • LTE-HSS • PCRF • OCS • OFCS • AAA • USERDEF1 • USERDEF2

System Options elements

This table describes the fields on the System Options page.

Table 106: System Options Elements

Field	Description	Data Input Notes
ASCII Excluded Digits	List of ASCII characters to ignore while parsing MSISDN digits from a raw AVP data field of AVP Type UTF8String. If an invalid character is entered, an error message appears.	Format: Text boxes Default = n/a Range = ASCII printable characters except '%', '@', ':' and ';'
Exclude Space	Defines whether ASCII character space is ignored while parsing MSISDN digits from a raw AVP data field of AVP Type UTF8String If checked, ASCII character space is ignored.	Format: Check box Range: Checked, unchecked

Field	Description	Data Input Notes
	If not checked, ASCII character space is not ignored.	Default: Unchecked
TBCD Excluded Digits	Defines whether the associated digits is ignored while parsing digits from a raw AVP data field of AVP Type OctetString encoded as a TBCD-string If checked, digits is ignored. If not checked, digits is not ignored.	Format: Check boxes Range: Checked, unchecked for each option: *(1010), #(1011), a(1100), b(1101), c(1110) Default: Unchecked
Allow Subsequent FABR Invocation	Enables the subsequent invocation of FABR on a different DSR node in the network	Format: Check box Range: Checked, unchecked Default: Unchecked
Remove Destination-Host	If checked, FABR deletes any instance of "Destination-Host" AVPs in the message when performing "Realm only" resolution.	Format: Check box Range: Checked, unchecked Default: Unchecked
Realm	Value to be placed in the Origin-Realm AVP of the Answer message generated by FABR. A Realm must be paired with a Fully Qualified Domain Name. If entering a value for Realm, then a value for Fully Qualified Domain Name must also be entered; otherwise, an error message appears. If a value is not entered, the local node Realm for the egress connection is used.	Default = n/a; Range = A valid Realm
Fully Qualified Domain Name	Value to be placed in the Origin-Host AVP of the Answer message generated by FABR A Fully Qualified Domain Name must be paired with a Realm. If entering a value for Fully Qualified Domain Name, then a value for Realm must also be entered; otherwise, an error message appears. If not configured, local node FQDN for the egress connection is used.	Default = n/a; Range = A valid FQDN

Field	Description	Data Input Notes
Resource Exhaustion Result-Code	Result-Code or Experimental-Result-Code value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted If Vendor-Id is configured, this result-code value is encoded as Experimental-Result-Code AVP; otherwise the result-code is encoded as Result-Code AVP.	Format: • Selection text box; numeric • Selection pulldown list Range: • Selection box: 1000–5999 • Pulldown list: available Code values Default: 3004
Resource Exhaustion Error Message	Error-Message AVP value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted	Range: 0–64 characters Default: FABR Resource Exhausted
Resource Exhaustion Vendor-Id	Vendor-Id AVP value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted	Format: Text box; numeric Range: 1–4294967295
Application Unavailable Action	Defines action to be taken when FABR is not available to process messages If the Default Route option is selected, an entry must be provided for the Application Unavailable Route List.	Format: Radio buttons Range: • Continue Routing • Default Route • Send Answer with Result-Code AVP • Send Answer with Experimental-Result AVP Default: Continue Routing
Application Unavailable Route List	Defines where the requests will be routed when FABR is not available. Peer Routing Rules will be bypassed. A route list must be entered if Default Route is selected as the Application Unavailable Action.	Format: Pulldown list Range: Available Route List entries
Application Unavailable Result-Code	Result-Code or Experimental-Result-Code value to be returned in an Answer message when a message is not successfully routed because FABR is not available.	Format: • Selection Text box; numeric

Field	Description	Data Input Notes
	If Vendor-Id is configured, this result-code value is encoded as Experimental-Result-Code AVP; otherwise the result-code is encoded as Result-Code AVP. A code must be entered if either the Send Answer with Result-Code AVP or the Send Answer with Experimental Result-Code AVP option is selected as the Application Unavailable Action.	• Selection pulldown list Range: • Selection box: 1000–5999 • Pulldown list: available Code values Default: 3002
Application Unavailable Error Message	Error-Message AVP value to be returned in an Answer message when a message is not successfully routed because FABR is not available. A message can be entered, if needed, when either the Send Answer with Result-Code AVP or the Send Answer with Experimental Result-Code AVP option is selected as the Application Unavailable Action.	Range: 0–64 characters Default: FABR Unavailable
Application Unavailable Vendor-Id	Vendor-Id AVP value to be returned in an Answer message when a message is not successfully routed because FABR is not available. A vendor-Id must be entered if the Send Answer with Experimental Result-Code AVP option is selected as the Application Unavailable Action.	Format: Text box; numeric Range: 1–4294967295

RBAR Configuration Elements

The tables in this section describe the elements that can be configured using the Range-Based Address Resolution (RBAR) application GUI pages in the DSR software.

Applications configuration elements

This table describes the fields on the Applications View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 107: Applications Configuration Elements

Field	Description	Data Input Notes
Application ID	Application ID in a Diameter message The Application ID is an IANA-assigned Diameter Application ID, which is a 32-bit field that is	Format: • Selection text box; numeric

Field	Description	Data Input Notes
	mandatory in all Diameter messages. It is commonly used for screening and routing messages between Diameter nodes. If a combination of the Application ID and Command Code already exists or an Application ID is not specified, an error message appears. To enter an Application ID, select the appropriate radio button and either enter the numeric information or select an ID from the pulldown list.	• Selection pulldown list: Available Application IDs **Note:** If a combination of the Application ID and Command Code already exists, an error message appears. Range: • Selection text box: 0–4294967295
Application Name	Name of the Application If a duplicate Application Name is entered, an error message appears.	Format: Alphanumeric and underscore (_) Range: 1–32 characters; cannot start with a digit and must contain at least one alpha
Routing Mode (Read only)	Method of routing for Request messages received containing the Diameter Application ID	Format: Disabled pulldown list with a value of Proxy.

Exceptions configuration elements

This table describes the fields on the Exceptions View and Edit pages only.

Table 108: Exceptions Configuration Elements

Field	Description	Data Input Notes
Application ID (Read only)	Application ID in a Diameter message	N/A
Application Name (Read only)	Name of the application	N/A
Routing Exception Type (Read only)	The routing exception that prevented address resolution. This field displays one of the following values: • Invalid command code • Valid address not found • Valid address was found did not match a provisioned address or address range	N/A

Field	Description	Data Input Notes
Routing Exception Action	Action that RBAR takes associated with the Routing Exception Type	Format: Radio buttons Range: • Forward Unchanged • Forward to Destination • Send Answer with Result-Code AVP • Send Answer with Experimental-Result AVP • Abandon Request
Destination	Destination to where the message is forwarded associated with the Routing Exception Type. This field is enabled when the Routing Exception Action is set to Forward to Destination.	Format: Pulldown list Range: Available user-configured destinations
Result-Code Value	Answer code associated with this Routing Exception Type. This field is enabled when the Routing Exception Action is set to either Send Answer with Result-Code AVP or Send Answer with Experimental-Result AVP.	Format: • Selection text box; numeric • Selection pulldown list Range: • Selection box: 1000–5999 • Selection pulldown list: available Diameter answer codes
Vendor-ID	Value returned in the Vendor-ID AVP of the answer message associated with this Routing Exception Type. This field is enabled when the Routing Exception Action is set to Send Answer with Experimental-Result AVP.	Format: Text box; numeric Range: 1–4294967295
Error Message	Value returned in the Error-Message AVP of the answer message. This field is enabled when the Routing Exception Action is set to either Send Answer with Result-Code AVP or Send Answer with Experimental-Result AVP.	Format: Alphanumeric, underscore (_), period (.) Range: 0–64 characters Default: Null string

Destinations configuration elements

This table describes the fields on the Destinations View, Insert, and Edit pages.

Table 109: Destinations Configuration Elements

Field	Description	Data Input Notes
Name	Unique name of the Destination If a duplicate Name is entered or the Name is not specified, an error message appears.	Format: Alphanumeric and underscore (_) Range: 1–32 characters; cannot start with a digit and must contain at least one alpha
Realm	Realm of the Destination The Realm and Fully Qualified Domain Name cannot both be empty; otherwise, an error message appears.	Format: Text box; string consisting of a list of labels separated by dots, where a label must contain letters, digits, hyphen (-) and underscore (_). A label must start with a letter or underscore and must end with a letter or digit. Underscores may be used only as the first character. Range: A label consists up to 63 characters and a Realm or FQDN up to 255 characters
Fully Qualified Domain Name	Unique Fully Qualified Domain Name of the Destination If a duplicate FQDN is entered, an error message appears. The Fully Qualified Domain Name and Realm cannot both be empty; otherwise, an error message appears.	
Allow Subsequent RBAR invocation	Enables the subsequent invocation of RBAR on a different DSR node in the network, when RBAR resolves to this destination **Note:** If the System Options Allow Subsequent RBAR Invocation option is checked, then this attribute will be ignored.	Format: Check box Range: Checked, unchecked Default: Checked

Address Tables configuration elements

This table describes the fields on the Address Tables View and Insert pages only.

Table 110: Address Tables Configuration Elements

Field	Description	Data Input Notes
Name	Unique name of the Address Table If a duplicate Name is entered or the Name is not specified, an error message appears.	Format: Alphanumeric and underscore (_) Range: 1–32 characters; cannot start with a digit and must contain at least one alpha
Comment	Information about the Address Table	Format: Text box; free form Range: up to 64 characters
Routing Entity Type	Type of Routing Entity If the Routing Entity Type is not specified, an error message appears.	Format: Pulldown list Range: • IMSI • MSISDN • IMPI • IMPU • IPv4 • IPv6 Prefix • UNSIGNED16

Addresses configuration elements

This table describes the fields on the Addresses View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 111: Addresses Configuration Elements

Field	Description	Data Input Notes
View pages		
Table Name	Address Table name	N/A
Address	Address of destination	N/A
Entry Type	Address type (Individual or Range)	N/A
Routing Entity	Routing Entity type	N/A
Individual Address	Specific address	N/A
Start Address	Starting address of the Range	N/A
End Address	Ending address of the Range	N/A

Field	Description	Data Input Notes
Destination	Destination of the Address	N/A
Insert and Edit pages		
Routing Entity Type	Routing Entity type	Format: Pulldown list Range: • IMSI • IMSISDN • IMPI • IMPU • IPv4 • IPv6 Prefix • UNSIGNED16
Table Name	Address Table name	Format: Pulldown list Range: Available user-configured address table names associated to the selected Routing Entity Type
Address Type	Type of address for the Routing Entity type	Format: Radio buttons Range: Range or Individual Address
Start Address	Starting address for an Address Range This field is required when Range is selected as Address Type. If Address is an IPv6-prefix, the prefix length must be entered in the IPv6 Prefix length field.	Format: Text box; • User Identity Address (IMSI, MSISDN, IMPI, IMPU): numeric string; 3–15 digits; valid digits (0–9) • IPv4 Address: up to 15-character string; quad-dotted format; valid characters are numeric (0–9) and dot (.); both compressed and expanded form are supported; for example: 192.168.1.15 or 192.168.001.015 • IPv6-Prefix Address: Hexadecimal value; up to 39 characters;
End Address	Ending address for an Address Range This field is required when Range is selected as Address Type. If Address is an IPv6-prefix, the prefix length must be entered in the IPv6 Prefix length field.	
Address	Specific address This field is enabled and required when Individual Address is selected as Address Type. If Address is an IPv6-prefix, the prefix length must be entered in the IPv6 Prefix length field.	

Field	Description	Data Input Notes
		valid alphanumeric characters (0-9, A-F, a-f) and colon (:); both compressed and expanded form are supported; for example: 1:::2 or 0001:0000: 0000:0000: 0000:0000: 0000:0002 **Note:** If this IPv6 address portion of the IPv6-prefix address is expressed in binary form (converting hexadecimal digits to bits), then no bit that is set (value=1) can be at an index that is greater than the configured IPv6 Prefix length. For example: 0001:0001:: for prefix length 28 is invalid as the 32nd bit is set. In addition, trailing zeros (0) can be dropped in this IPv6 address portion of the IPv6-prefix address but not the leading zeros (0); for example: 8:: for prefix length 1 is invalid because 8:: is treated as 0008:: • UNSIGNED16: Hexadecimal value; valid alphanumeric characters (0-9, A-F, a-f); for example: 512, 20, 40, AA, 50A, FFFF Range:

Field	Description	Data Input Notes
		• User Identity Address (IMSI, MSISDN, IMPI, IMPU): 3–15 digits • IPv4 Address: valid IPv4 address • IPv6-Prefix Address: valid IPv6 address • UNSIGNED16: 0–FFF
IPv6 Prefix length	Prefix length of an IPv6-prefix address; specifies how many of the leftmost contiguous bits of the address comprise the prefix. This field is enabled and required when IPv6 Prefix is selected as Routing Entity Type.	Format: Text box; numeric Range: 1–128
Destination	Destination of the Address	Format: Pulldown list Range: Available user-configured destinations

Address Resolutions configuration elements

This table describes the fields on the Address Resolutions View, Insert, and Edit pages. Data Input Notes only apply to the Insert and Edit pages; the View page is read-only.

Table 112: Address Resolutions Configuration Elements

Field	Description	Data Input Notes
Application ID	Application ID in a Diameter message The Application ID is an IANA-assigned Diameter Application ID, which is a 32-bit field that is mandatory in all Diameter messages. It is commonly used for screening and routing messages between Diameter nodes. If a combination of the Application ID and Command Code already exists, an error message appears.	Format: Pulldown list Range: Available Application IDs (0–4294967295)
Command Code	Command Code in a Diameter message If a combination of the Application ID and Command Code already exists, an error message appears.	Format: Pulldown list Range: Available Command Codes

Field	Description	Data Input Notes
Primary Routing Entity and Secondary Routing Entity sections		
Routing Entity Type	Routing Entity type The same Routing Entity Type cannot be selected for both the Primary and the Secondary Routing Entity; if the same type is selected, an error message appears. If the Routing Entity Type is not specified for the Primary Routing Entity, an error message appears.	Format: Pulldown list Range: • IMSI • MSISDN • IMPI • IMPU • IPv4 • IPv6 Prefix • UNSIGNED16

Primary AVP	Primary AVP used for extracting the Routing Entity address
	The same Primary AVP and Secondary AVP cannot be selected for either the Primary Routing Entity or for the Secondary Routing Entity; if the same AVP is selected, an error message appears.
	If Primary AVP is not selected for the Primary Routing Entity, an error message appears.
		Format: Pulldown list
		Range:
		• User Identity routing entity type:
		  • Public Identity
		  • ServiceInfo.SubscriptionId(0)
		  • ServiceInfo.SubscriptionId(1)
		  • ServiceInfo.SubscriptionId(2)
		  • ServiceInfo.SubscriptionId(3)
		  • ServiceInfo.SubscriptionId(4)
		  • Subscription-Id(0)
		  • Subscription-Id(1)
		  • Subscription-Id(2)
		  • Subscription-Id(3)
		  • Subscription-Id(4)
		  • UserIdentity.MSISDN
		  • UserIdentity.PublicIdentity
		  • UserName
		• IPv4 routing entity type: Framed IP Address
		• IPv6 Prefix routing entity type: Framed IPv6 Prefix
		• UNSIGNED16 routing entity type: ServiceInfo.PSInfo.3GPP-CC

Secondary AVP	Secondary AVP used for extracting the Routing Entity address The same Primary AVP and Secondary AVP cannot be selected for either the Primary Routing Entity or for the Secondary Routing Entity; if the same AVP is selected, an error message appears. The Secondary AVP field is available for User Identity routing types only; this field is disabled if IPV4, IPV6 Prefix, and UNSIGNED16 are selected as the Routing Entity Type.	

Field	Description	Data Input Notes
Address Table Name	Address Table for this Routing Entity Type If Address Table Name is not selected for the Primary Routing Entity, an error message appears.	Format: Pulldown list Range: Available user-configured Address Table names

System Options elements

This table describes the fields on the System Options page.

Table 113: System Options Elements

Field	Description	Data Input Notes
IMPU URI Local Number Enabled	This only applies to the Routing Entity Type IMPU; defines whether Local Numbers are considered valid addresses within a SIP or TEL URI. An address of this form is considered a "Local Number" if it does not start with the Global Number prefix character "+". If checked, both Local and Global Numbers are valid addresses for IMPU decoded from Diameter Requests. If unchecked, only Global Numbers are valid addresses.	Format: Check box Range: Checked, unchecked Default: Unchecked
ASCII Excluded Digits	List of ASCII characters to ignore while parsing digits from a raw AVP data field of AVP Type UTF8String. If an invalid character is entered, an error message appears.	Format: Text boxes Range: ASCII-printable characters except "%"
Exclude Space	Defines whether ASCII character space is ignored while parsing digits from a raw AVP data field of AVP Type UTF8String If checked, ASCII character space is ignored. If not checked, ASCII character space is not ignored.	Format: Check box Range: Checked, unchecked Default: Unchecked
TBCD Excluded Digits	Defines whether the associated character is ignored while parsing digits from a raw AVP data field of AVP Type OctetString encoded as a TBCD-string If checked, character is ignored. If not checked, character is not ignored.	Format: Check boxes Range: Checked, unchecked for each option: *(0010), #(1011), a(1100), b(1101), c(1110) Default: Unchecked

Field	Description	Data Input Notes
Allow Subsequent RBAR Invocation	Enables the subsequent invocation of RBAR on a different DSR node in the network If checked, this setting overrides the Allow Subsequent RBAR Invocation attribute in Destination.	Format: Check box Range: Checked, unchecked Default: Unchecked
Remove Destination-Host	If checked, RBAR deletes any instance of "Destination-Host" AVPs in the message when performing "Realm only" resolution.	Format: Check box Range: Checked, unchecked Default: Unchecked
Realm	Value to be placed in the Origin-Realm AVP of the Answer message generated by RBAR A Realm must be paired with a Fully Qualified Domain Name. If entering a value for Realm, then a value for Fully Qualified Domain Name must also be entered; otherwise, an error message appears. If not configured, the local node Realm for the egress connection is used to populate Origin-Realm AVP.	Format: Text box; string consisting of a list of labels separated by dots, where a label must contain letters, digits, hyphen (-) and underscore (_). A label must start with a letter or underscore and must end with a letter or digit. Underscores may be used only as the first character. Range: A label consists up to 63 characters and a Realm or FQDN up to 255 characters
Fully Qualified Domain Name	Value to be placed in the Origin-Host AVP of the Answer message generated by RBAR A Fully Qualified Domain Name must be paired with a Realm. If entering a value for Fully Qualified Domain Name, then a value for Realm must also be entered; otherwise, an error message appears. If not configured, the local node FQDN for the egress connection is used to populate the Origin-Host AVP.	
Resource Exhaustion Result-Code	Result-Code or Experimental-Result-Code value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted If Vendor-Id is configured, this result-code value is encoded as Experimental-Result-Code AVP; otherwise the result-code is encoded as Result-Code AVP.	Format: • Selection text box; numeric • Selection pulldown list Range: • Selection box: 1000–5999 • Pulldown list: available Code values

Field	Description	Data Input Notes
		Default: 3004
Resource Exhaustion Error Message	Error-Message AVP value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted	Format: Alphanumeric, underscore (_), and period (.) Range: 0–64 characters Default: RBAR Resource Exhausted
Resource Exhaustion Vendor-Id	Vendor-Id AVP value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted	Format: Text box; numeric Range: 1–4294967295
Application Unavailable Action	Defines action to be taken when RBAR is not available to process messages If the Default Route option is selected, an entry must be provided for the Application Unavailable Route List.	Format: Radio buttons Range: • Continue Routing • Default Route • Send Answer with Result-Code AVP • Send Answer with Experimental-Result AVP Default: Continue Routing
Application Unavailable Route List	Defines where the requests will be routed when RBAR is not available. Peer Routing Rules will be bypassed. A route list must be entered if Default Route is selected as the Application Unavailable Action.	Format: Pulldown list Range: Available Route List entries
Application Unavailable Result-Code	Result-Code or Experimental-Result-Code value to be returned in an Answer message when a message is not successfully routed because RBAR is not available. If Vendor-Id is configured, this result-code value is encoded as Experimental-Result-Code AVP; otherwise the result-code is encoded as Result-Code AVP. A code must be entered if either the Send Answer with Result-Code AVP or the Send Answer with Experimental Result-Code AVP option is selected as the Application Unavailable Action.	Format: • Selection Text box; numeric • Selection pulldown list Range: • Selection box: 1000–5999 • Pulldown list: available Code values Default: 3002

Field	Description	Data Input Notes
Application Unavailable Error Message	Error-Message AVP value to be returned in an Answer message when a message is not successfully routed because RBAR is not available. A message can be entered, if needed, when either the Send Answer with Result-Code AVP or the Send Answer with Experimental Result-Code AVP option is selected as the Application Unavailable Action.	Format: Alphanumeric, underscore (_), and period (.) Range: 0–64 characters Default: RBAR Unavailable
Application Unavailable Vendor-Id	Vendor-Id AVP value to be returned in an Answer message when a message is not successfully routed because RBAR is not available. A vendor-Id must be entered if the Send Answer with Experimental Result-Code AVP option is selected as the Application Unavailable Action.	Format: Text box; numeric Range: 1–4294967295

CPA Configuration Elements

The tables in this section describe the elements that can be configured using the following Charging Proxy Application (CPA) GUI pages in the DSR software:

- System Options
- Message Copy
- Session Binding Repository (SBR)

System Options page elements

This section describes the elements on the **System Options** page.

Table 114: System Options page elements

Elements	Description	Data Input Notes
Unavailable Action	Action to be taken when the CPA has an operational state of Degraded or Unavailable.	Default: Send Answer
Unavailable Action Result Code	Because the Unavailable Action must be Send Answer, if the DSR Application is not available, this value is used in the Result-Code or Experimental-Result AVP of the Answer message.	Format: Two radio button group with a text box and drop-down box. Default: 3004 DIAMETER_TOO_BUSY

Elements	Description	Data Input Notes
Unavailable Action Vendor ID	If zero, then a Result-Code AVP will be sent when the DSR application is not available. If non-zero, then an Experimental-Result AVP will be sent with the Vendor-Id AVP set to this value.	Format: Unsigned integer Default: 0
Unavailable Action Error Message	If a non-null string, then an Error-Message AVP will be sent in the Answer response containing this string when the DSR application is not available.	Format: Text box (string up to 64 characters) Default: CPA Unavailable
DSR Application-Invoked AVP Insertion	If set to Yes, this AVP will be inserted into the Request message that is routed to prevent multiple invocations of the same DSR application on different DSRs or MPs.	Format: Yes/No Default: No
Shutdown Mode	Allows the operator to specify the shutdown method used when the CPA Admin State is changed to disabled. The CPA can be disabled using either a graceful or forced shutdown method. Graceful allows in-process transactions to continue for a configurable time period before disabling the CPA. Forced is an immediate shutdown.	Format: Forced/Graceful Default: Graceful
Shutdown Timer	Number of seconds that the Shutdown Timer will run during a graceful shutdown.	Range: 1 to 15 seconds Default: 5
Generate Answer Result Code	The Result-Code or Experimental-Result AVP value to be populated in the Answer message when the DSR generates an Answer message to the downstream (CTF) peer.	Format: Two radio button group with a text box and drop-down box. The drop-down box contains several Result-Code values and corresponding names. The user can also choose to specify their own Result-Code value in the text box. Range: 1000 - 5999 Default: 3004 DIAMETER_TOO_BUSY
Generate Answer Vendor ID	If zero, then a Result-Code AVP will be sent when the DSR generates an Answer message. If non-zero, then the Experimental-Result AVP will be sent in the Answer message with the Vendor-Id	Format: Unsigned integer Default: 0

Elements	Description	Data Input Notes
	AVP set to this value. The value of the Result-Code or Experimental-Result AVP will be the configured Generate Answer Result Code.	
Generate Answer Error Message	If a non-null string, then an Error-Message AVP will be sent in the Answer message that the DSR generates containing this string.	Format: Text box (string up to 64 characters) Default: DSR Generated Answer
Behavior if Session Lookup Error	Behavior to use when CPA attempts to query the preferred CDF that is associated with the given Diameter session, but the query is not successful. The possible behaviors are • Generate Answer (send an Answer message with the configured Generate Answer Result-Code to the CTF) • Continue Routing (load balance the Request message to an available CDF)	The range of allowable values in the drop-down box shall be: • Generate Answer • Continue Routing Default: Continue Routing

Message Copy elements

This table describes the fields on the Message Copy page.

Table 115: Message Copy Elements

Elements	Description	Data Input Notes
Message Copy Status	Enable or disable the triggering of Message Copy.	Format: Two radio buttons: • Enable • Disable Default: Disable
Called-Station-ID match string 1	If the Called-Station-Id AVP value in an ACR-Start or ACR-Event message contains this case-sensitive string, then Message Copy will be triggered.	Format: Text box (up to 64 characters) Default: Empty string
Called-Station-ID match string 2	If the Called-Station-Id AVP value in an ACR-Start or ACR-Event message contains this case-sensitive string, then Message Copy will be triggered.	Format: Text box (up to 64 characters) Default: Empty string
Called-Station-ID match string 3	If the Called-Station-Id AVP value in an ACR-Start or ACR-Event message contains this case-sensitive string, then Message Copy will be triggered.	Format: Text box (up to 64 characters) Default: Empty string

Elements	Description	Data Input Notes
Called-Station-ID match string 4	If the Called-Station-Id AVP value in an ACR-Start or ACR-Event message contains this case-sensitive string, then Message Copy will be triggered.	Format: Text box (up to 64 characters) Default: Empty string
DAS Route List 1	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.
DAS Route List 2	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.
DAS Route List 3	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.
DAS Route List 4	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.
DAS Route List 5	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.
DAS Route List 6	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.
DAS Route List 7	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.
DAS Route List 8	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.

Elements	Description	Data Input Notes
DAS Route List 9	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.
DAS Route List 10	DAS Route List for distributing copies of Request messages to Diameter Application Servers. A round robin scheme is used to distribute copies among the configured DAS Route Lists.	Format: Pull down of Route Lists that have been configured on the DRL configuration screen.

SBR elements

An asterisk after the value field means that the configuration is mandatory.

Element	Description	Data Input Notes
SBDB audit Start Time	Time of day in UTC to start the audit process. The audit process removes stale bindings from the SBR. Since the audit window is configurable, the audit process calculates the rate at which to delete records based on the number of expected stale bindings and the configured duration of the daily audit. The longer the audit window is, the slower the deletion rate. If your system has a daily period of lower customer activity, you may wish to schedule the audit for that time. Otherwise, you can reduce the performance load of the process by allowing it more time during the day to complete its audit.	Format: pull-down list Range: 12:00 AM - 11:00 PM, UTC Default: 2:00 AM
SBDB audit Stop Time	Time of day in UTC to stop the audit process. Must be at least 1 hour past the start time.	Format: pull-down list Range: 12:00 AM - 11:00 PM, UTC Default: 3:00 AM
Stale SBDB session binding age.	Age after which a session will be considered stale and eligible for removal during audit.	Format: numeric Range: 1-30 Default: 2

Element	Description	Data Input Notes
	Note that increasing the age will increase memory usage. Age is specified in days.	
Maximum active session bindings.	Session binding count used to calculate the session binding count alarms. Once this setting is reached, the SBR will issue an alarm; however, it will continue to store bindings.	Format: numeric Range: 1 - 100,000,000 Default: 35,000,000
SBDB Mostly Stale Percentage.	Percent of stale session age when a session binding is considered mostly stale. This setting is not used by the audit process. However, it is used to generate measurements.	Format: numeric Range: 1-99 Default: 90

SBR Subresource Mapping elements

The **SBR Subresource Mapping** page is organized by server group, which must be configured before accepting the configurations on this page. To configure server groups, select Configuration -> Server Groups.

CAUTION: After configuration, this page becomes read-only.

Element	Description	Data Input Notes
SBR Server Group Name	Server Group Name from the Configuration -> Server Groups configuration page	This field cannot be edited
Resource Name	Resource name as cSBR	This field cannot be edited
Subresource Id	A subresource is a logical partition of the Session Binding Repository consisting of an active/standby pair. The Subresource Id is a monotonically increasing integer starting with 0. An selection of "Not Hosted" indicates that the server group	Format: pull-down list Range: "Not Hosted", 0-N, where N is the number of subresources-1 Default: 0, 1, 2, 3, ..., N

Element	Description	Data Input Notes
	will not be used. The "Not Hosted" ID is typically used only in testing environments. An asterisk after the value field means that the configuration is mandatory.	

IPFE Configuration Elements

The tables in this section describe the elements that can be configured using the Internet Protocol Front End (IPFE) GUI pages in the DSR software.

Configuration Options elements

An asterisk after the value field means that the configuration is mandatory.

Table 116: IPFE Configuration Elements

Element	Description	Data Input Notes
Inter-IPFE Synchronization		
IPFE-A1 IP Address	The IPv4 or IPv6 address of IPFE-A1. This address must reside on the IMI (internal management interface) network. This address is used for replicating association data between IPFEs and is not exposed to application clients. If left blank, the IPFE will not replicate association data. Although optional, this configuration is required for a fully-functioning installation.	Format: IPv4 or IPv6 address, or left blank Default: blank
IPFE-A2 IP Address	The IPv4 or IPv6 address of IPFE-A2. This address must reside on the IMI (internal management interface) network. This address is used for replicating association	Format: IPv4 or IPv6 address, or left blank Default: blank

Element	Description	Data Input Notes
	data between IPFEs and is not exposed to application clients. If left blank, the IPFE will not replicate association data. Although optional, this configuration is required for a fully-functioning installation.	
IPFE-B1 IP Address	The IPv4 or IPv6 address of IPFE-B1. This address must reside on the IMI (internal management interface) network. This address is used for replicating association data between IPFEs and is not exposed to application clients. If left blank, the IPFE will not replicate association data. Although optional, this configuration is required for a fully-functioning installation.	Format: IPv4 or IPv6 address, or left blank Default: blank
IPFE-B2 IP Address	The IPv4 or IPv6 address of IPFE-B2. This address must reside on the IMI (internal management interface) network. This address is used for replicating association data between IPFEs and is not exposed to application clients. If left blank, the IPFE will not replicate association data. Although optional, this configuration is required for a fully-functioning installation.	Format: IPv4 or IPv6 address, or left blank Default: blank
State Sync TCP Port	TCP port to use for syncing kernel state between IPFEs. This port is used on both IPFEs.	Format: numeric Range: 1-65535 Default: 19041
State Sync Reconnect Interval	Reconnect interval in seconds for syncing kernel state between IPFEs.	Format: numeric, seconds Range: 1-255 seconds

Element	Description	Data Input Notes
		Default: 1
Traffic Forwarding		
Per-TSA Association Limit	The maximum number of concurrent TCP or SCTP connections for one TSA. To limit memory consumption, the IPFE limits the number of associations with the most recent packet activity to this setting. Memory is consumed at a rate of 224 bytes per association per TSA. This configuration should be set to 10% higher than the expected load. If this value is set to a lower value than the current number of associations stored, then the IPFE will remove the oldest entries until the number of stored associations is no more than this setting. Setting this value too low could cause current connections to be dropped when the state of the application servers change.	Format: numeric Range: 0-65535 Default: 12000
Application Traffic Min Port	Traffic balancing port range. This is the minimum of the range. This is 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. Setting the range to 0-65535 removes the port constraint.	Format: numeric Range: 0 - less than or equal to the Load Balance Max Port Default: 0
Application Traffic Max Port	Traffic balancing port range. This is the maximum of the range. This is the range of ports for which the IPFE will accept traffic. If the port is outside of	Format: numeric Range: greater than or equal to the Load Balance Min Port - 65535 Default: 65535

Element	Description	Data Input Notes
	the specified range, the IPFE will ignore the packet and not forward it. Setting the range to 0-65535 removes the port constraint.	
Application Traffic TCP Reject Option	How to reject connections when no application servers are available. When no application servers are available, the IPFE must reject the TCP traffic that it receives. The IPFE can either drop packets or it can communicate to the application clients with TCP or ICMP messages. Select the option that can be best handled by the application client.	Format: pull-down list Range: • TCP Reset • Drop Packet • ICMP Host Unreachable • ICMP Port Unreachable • ICMP Administratively Prohibited Default: TCP Reset
Application Traffic SCTP Reject Option	How to reject connections when no application servers are available. When no application servers are available, the IPFE must reject the STCP traffic that it receives. The IPFE can either drop packets or it can communicate to the application clients with ICMP messages. Select the option that can be best handled by the application client.	Format: pull-down list Range: • Drop Packet • ICMP Host Unreachable • ICMP Port Unreachable • ICMP Administratively Prohibited Default: ICMP Host Unreachable
Packet Counting		
Imbalance Detection Throughput Minimum	Value below which no throughput analysis is performed regarding imbalance detection. This setting should not be changed from its default unless the IPFE is being tested with a very low load. This setting ensures that the IPFE will not mark application servers as imbalanced when it is distributing very few messages between them.	Format: numeric, packets per second Range: 1-2147483647 Default: 20000

Element	Description	Data Input Notes
Cluster Rebalancing and Accounting	Support for cluster rebalancing and packet accounting in measurements. When this is disabled, all accumulation of packet and byte measurements cease. Overload detection also stops. The disabled state is useful only for troubleshooting, which should be done by Tekelec Customer Care. Contact Tekelec Customer Care before disabling measurements and overload detection.	Format: pull-down list Range: • Enabled • Disabled Default: Enabled
Application Server Monitoring		
Monitoring Port	TCP port to try periodic connections or monitoring of application servers. The IPFE opens a TCP connection to the application server's IP address and this port. The application server must listen on this port, and it should either accept TCP connections or send heartbeats, depending on the monitoring protocol selected.	Format: numeric Range: 1-65535 Default: 9675
Monitoring Connection Timeout	How long to wait for a connection to complete when polling the application servers for aliveness in seconds. If the IPFE detects that an application server has missed a configurable number of heartbeats - that is, more than that number of seconds have elapsed since the most recent heartbeat was received - then it considers the application server to be down. The IPFE will remove a down application server from the traffic balancing pool and	Format: numeric, seconds Range: 1 - 255 Default: 3

Element	Description	Data Input Notes
	attempt to reconnect to the server.	
Monitoring Connection Try Interval	Interval in seconds of periodically connecting to application servers to test for aliveness. While an application server is down, the IPFE will periodically attempt to re-connect to it based on this configuration. This configuration is used for both monitoring protocols.	Format: numeric, seconds Range: 1 - 255 Default: 10
Monitoring Protocol	Application liveness monitoring method. The monitoring protocol allows the IPFE to determine the liveness of the application servers. The IPFE can determine this either by sending TCP traffic to the application servers or by listening for heartbeat messages from the application servers. • TCP Connection - The IPFE connects to the monitoring port and drops the connection immediately if it is successful, which indicates that the application server is live. This is only selected if the application server (for instance, a non-Tekelec server) cannot send a heartbeat. • Heartbeat - The IPFE connects to the monitoring port, sustains the connection, and receives heartbeat packets from the application server. In this case, the failure to receive a heartbeat packet within the period Back-end Connection Timeout indicates the server is dead.	Format: pull-down list Range: • TCP Connection • Heartbeat • None Default: Heartbeat

Element	Description	Data Input Notes
	A dead server is removed from the traffic balancing pool. The IPFE attempts connections on the monitoring port until the server responds. When the server responds, the IPFE adds it back to the pool.	

Target Sets configuration elements

A Target Set maps a single externally available IP address to a set of IP addresses for application servers. A Target Set is associated with an IPFE.

Table 117: Target Sets configuration elements describes the fields on the Target Sets View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 117: Target Sets configuration elements

Field	Description	Data Input Notes
Target Set Number	Unique ID identifying the Target Set	Format: numeric Range: 1-32
Target Set Address	Public IP address to present to the outside world	Format: IPv4 or IPv6 address The Target Set Address must be on the XSI network
Target Set IP List	List of IP addresses of the associated application servers	Format: IPv4 or IPv6 address. IP address type must match that of the Target Set Address. The IP addresses in Target Set IP List must be on the XSI network.
Weighting	Weighting value is used to apportion load between application servers within the Target Set. The following formula is used to determine the selection of an application server: Application server's % chance of selection = (Application server weight / Sum of all weights in the Target Set) * 100.	Format: numeric Range: 0-65535 Default: 100

Field	Description	Data Input Notes
	If all application servers have an equal weight, they have an equal chance of being selected. If application servers have unequal capacities, give a higher weight to the servers with the greater capacity.	
Supported Protocols	The protocols supported by this Target Set	Format: radio buttons Range: TCP only, SCTP only, Both TCP and SCTP Default: Both TCP and SCTP
Preferred Active	The IPFE that will primarily handle traffic for this Target Set. "Disabled" means that the Target Set is defined, but not currently in use by an IPFE.	Format: radio buttons Range: IPFE-A1, IPFE-A2, IPFE-B1, IPFE-B2 Default: IPFE-A1 If a radio button is not activate, you need configure the IPFE address under IPFEConfigureOptions.
Preferred Standby	The mate of the Preferred Active IPFE. If the Preferred Active IPFE is unavailable, the Preferred Standby server takes over.	If the Preferred Standby IPFE has been configured, it will be set when you select the Preferred Active IPFE.

Glossary

A

ACK	Data Acknowledgement
Application Routing Rule	A set of conditions that control message routing to a DSR application based on message content.
AVP	Attribute-Value Pair The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization or accounting information.

C

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

C

	with a Capability-Exchange-Answer (CEA) message.
CEX Configuration Set	A mechanism for assigning Application IDs and supported Vendor IDs to a Local Node or to a Connection.
Charging Proxy Application	A DSR Application that is responsible for sending and receiving Diameter accounting messages.
ComAgent	Communication Agent A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.
Communication Agent	See ComAgent.
CPA	Charging Proxy Application A local application running on the DSR.
CPU	Central Processing Unit
CTF	Charging Trigger Function

D

DAL	Dedicated Access Line DSR Application Layer
DA-MP	Diameter Agent MP

D

	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.
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.
DNS	Domain Name System A system for converting Internet host and domain names into IP addresses.
DP	Data Processor The repository of subscriber data on the individual DSR node elements.

D

	The DP hosts the full address resolution database.
DPA	Disconnect-Peer-Answer A message used by a Diameter node to answer the Disconnect-Peer-Request (DPR).
DPR	Disconnect-Peer-Request A message used by a Diameter node to inform its peer of its intent to disconnect the transport layer. Upon receipt of a DPR, the Disconnect-Peer-Answer (DPA) is returned.
DRL	Diameter Routing Layer The software layer of the Eagle XG Diameter stack that implements Diameter routing.
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.
DWA	Device-Watchdog-Answer A Diameter message used with the Device-Watchdog-Request (DWR) message to proactively detect connection failures. If no traffic is

D

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

E

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

F

F

FABR	Full Address Based Resolution Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.
FQDN	Fully qualified domain name The complete domain name for a specific computer on the Internet (for example, www.tekelec.com).
Full Address Based Resolution	See FABR.

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

IANA	Internet Assigned Numbers Authority An organization that provides criteria regarding registration of values related to the Diameter protocol.
IMI	Internal Management Interface
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity

I

IMSI	International Mobile Subscriber Identity
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.
IP Address	The location of a device on a TCP/IP network. The IP Address is either a number in dotted decimal notation which looks something like (IPv4), or a 128-bit hexadecimal string such as (IPv6).
IPFE	IP Front End A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.
IPsec	Internet Protocol Security A protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a data stream.
IPv4	Internet Protocol version 4

I

IPv6	Internet Protocol version 6

L

Local Node	A local Diameter node specified with a fully qualified domain name. It identifies a list of IP addresses for the Local node, a listen port number, supported transport types, etc.

M

MEAL	Measurements, Events, Alarms, and Logs
MP	Message Processor The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM&P components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.
MPS	Multi-Purpose Server The Multi-Purpose Server provides database/reload functionality and a variety of high capacity/high speed offboard database functions for applications. The MPS resides in the General Purpose Frame. Messages Per Second A measure of a message processor's performance capacity. A message is any Diameter message (Request or Answer) which is received and processed by a message processor.
MSISDN	Mobile Station International Subscriber Directory Number

M

The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.

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).

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.

O

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.
Peer Routing Rule	A set of conditions that control message routing to an upstream peer node based on message content.
Proxy Agent	Performs the basic forwarding functions of a Relay Agent, but unlike a Relay Agent, a Proxy Agent can modify the message content and provide value-added services, enforce rules on different messages, or perform administrative tasks for a specific realm.

R

Range Based Address Resolution	See RBAR.
RBAR	Range Based Address Resolution

R

	A DSR enhanced routing application which allows the user to route Diameter end-to-end transactions based on Application ID, Command Code, "Routing Entity" Type, and Routing Entity address ranges.
realm	A fundamental element in Diameter is the realm, which is loosely referred to as domain. Realm IDs are owned by service providers and are used by Diameter nodes for message routing.
Relay Agent	Diameter agent that forwards requests and responses to other Diameter nodes based on routing-related AVPs (such as Destination-Realm) and routing configuration. Because relays do not make policy decisions, they do not examine or alter non-routing AVPs. As a result, relays never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are capable of handling any Diameter application or message type.

S

SBR	Session Binding Repository A highly available, distributed database for storing Diameter session binding data.
SCTP	Stream Control Transmission Protocol An IETF transport layer protocol, similar to TCP that sends a message in one operation.

S

	The transport layer for all standard IETF-SIGTRAN protocols. SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.
SDS	Subscriber Database Server Subscriber Database Server (SDS) provides the central provisioning of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query Server and the Data Processor System Operations, Administration, and Maintenance (DP SOAM) servers at each Diameter Signaling Router (DSR) site or a standalone DP site to replicate and recover provisioned data to the associated components.
Session Binding Repository	See SBR.
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol

S

	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.
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.
TSA	Target Set Address An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.

U

URI	Uniform Resource Identifier An internet protocol element consisting of a short string of characters that conform to a certain syntax. The string comprises a name or address that can be used to refer to a resource.
URL	Uniform Resource Locator

V

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