EAGLE® XG Diameter Signaling Router

Diameter and Mediation User Guide

910-6822-001 Revision A
November 2013

Table of Contents

Chapter 1: Introduction.....18

Overview.....19
Scope and Audience.....19
Document Organization.....19
Documentation Admonishments.....20
Related Publications.....20
Customer Care Center.....21
Emergency Response.....23
Locate Product Documentation on the Customer Support Site.....24

Chapter 2: Configuration.....25

Configuration Sequence.....27
Configuration Capacity Summary.....28
Connection Capacity Validation.....29
Connection Capacity Dashboard Page.....32
MP Profiles.....36
MP Profiles elements.....37
Viewing MP Profiles.....40
Editing Configurable MP Profile Parameters.....41
Assigning MP Profiles to DA-MPs.....41
Application Ids configuration.....42
Application Ids elements.....43
Viewing Application Ids.....44
Adding an Application Id.....45
Editing an Application Id.....46
Deleting an Application Id.....46
CEX Parameters configuration.....47
CEX Parameters elements.....47
Viewing CEX Parameters.....48
Adding CEX Parameters.....48
Editing CEX Parameters.....49
Deleting CEX Parameters.....50
Command Codes configuration.....50
Command Codes elements.....51

Viewing Command Codes....51
Adding a Command Code....51
Editing a Command Code....52
Deleting a Command Code....53
MCC Ranges configuration....53
MCC Ranges elements....54
Viewing MCC Ranges....54
Adding MCC Ranges....55
Editing MCC Ranges....55
Deleting MCC Ranges....56
Connection Configuration Set configuration....56
Connection Configuration Set elements....57
Viewing Connection Configuration Sets....62
Adding a Connection Configuration Set....62
Editing a Connection Configuration Set....62
Deleting a Connection Configuration Set....63
CEX Configuration Set configuration....64
CEX Configuration Set elements....65
Viewing CEX Configuration Sets....66
Adding a CEX Configuration Set....66
Editing a CEX Configuration Set....67
Deleting a CEX Configuration Set....68
Capacity Configuration Set configuration....68
Capacity Configuration Set elements....70
Viewing Capacity Configuration Sets....71
Adding a Capacity Configuration Set....71
Editing a Capacity Configuration Set....72
Deleting a Capacity Configuration Set....73
Egress Message Throttling Configuration Set configuration....73
Egress Message Throttling Configuration Set elements....74
Viewing Egress Message Throttling Configuration Sets....75
Adding an Egress Message Throttling Configuration Set....75
Editing an Egress Message Throttling Configuration Set....76
Deleting an Egress Message Throttling Configuration Set....77
Message Priority Configuration Set configuration....77
Message Priority Configuration Set elements....78
Viewing Message Priority Configuration Sets....79
Adding a Message Priority Configuration Set....79
Editing a Message Priority Configuration Set....80
Deleting a Message Priority Configuration Set....81
Message Copy Configuration Set configuration....81

Message Copy Configuration Set elements....82
Viewing Message Copy Configuration Sets....83
Adding a Message Copy Configuration Set....83
Editing a Message Copy Configuration Set....84
Deleting a Message Copy Configuration Set....84
Local Node configuration....85
Local Node configuration elements....86
Viewing Local Nodes....88
Adding a Local Node....88
Editing a Local Node....89
Deleting a Local Node....90
Peer Node configuration....91
Peer Node configuration elements....92
Viewing Peer Nodes....96
Adding a Peer Node....96
Editing a Peer Node....98
Deleting a Peer Node....99
Connection configuration....99
Connection configuration elements....101
Viewing Connections....109
Adding a Connection....110
Editing a Connection....112
Deleting a Connection....114
Route Group configuration....115
Route Group configuration elements....115
Viewing Route Groups....117
Adding a Route Group....117
Editing a Route Group....118
Deleting a Route Group....119
Route List configuration....119
Route List configuration elements....120
Viewing Route Lists....121
Adding a Route List....122
Editing a Route List....122
Deleting a Route List....123
Peer Route Tables configuration....123
Peer Route Tables elements....124
Viewing Peer Route Tables....124
Adding a Peer Route Table....124
Deleting a Peer Route Table....125
Peer Routing Rules configuration....125

Egress Throttle Groups configuration....133
Egress Throttle Groups elements....134
Viewing Egress Throttle Groups....137
Adding Egress Throttle Groups....137
Editing Egress Throttle Groups....139
Deleting Egress Throttle Groups....139
Reroute On Answer configuration....140
Reroute On Answer configuration elements....140
Viewing Reroute On Answer....141
Adding a Reroute On Answer entry....141
Deleting a Reroute On Answer....142
Application Route Tables configuration....142
Application Route Tables elements....143
Viewing Application Route Tables....143
Adding an Application Route Table....143
Deleting an Application Route Table....144
Application Routing Rules configuration....144
Routing Option Sets configuration....152
Routing Option Sets elements....152
Viewing Routing Option Sets....156
Adding a Routing Option Set....156
Editing a Routing Option Set....157
Deleting a Routing Option Set....157
Pending Answer Timers configuration....158
Pending Answer Timers elements....161
Viewing Pending Answer Timers....162
Adding a Pending Answer Timer....162
Editing a Pending Answer Timer....162
Deleting a Pending Answer Timer....163
System Options configuration....163
System Options elements....164
DNS Options configuration....166
DNS Options elements....167
Topology Hiding configuration....167
Diameter Topology Hiding....167
Trusted Networks Lists configuration....189
Path Topology Hiding Configuration Set configuration....192
S6a/S6d HSS Topology Hiding Configuration Set configuration....197
MME/SGSN Topology Hiding Configuration Set configuration....200
Protected Networks configuration....206
DSR Bulk Import....209

Bulk Import elements....215
Using an Import file to insert DSR configuration data....216
Using an Import file to update DSR configuration data....216
Using an Import file to delete DSR configuration data....217
DSR Bulk Export....218
Bulk Export elements....220
Manually Exporting a configuration data file once....223
Scheduling periodic automatic exports of configuration data....224
Bulk Import and Export CSV File Formats and Contents....225

Chapter 3: Diameter Message Copy....259
Diameter Message Copy overview....260
Diameter Message Copy feature....262

Chapter 4: Maintenance....270
Overview....271
Route List maintenance....271
Route List maintenance elements....271
Viewing Route List status....272
Route Group maintenance....272
Route Group maintenance elements....273
Viewing Route Group status....274
Peer Node maintenance....274
Peer Node maintenance elements....274
Viewing Peer Node status....275
Connection maintenance....275
Connection maintenance elements....276
Viewing Connection status....278
Enabling Connections....279
Enabling All Connections....279
Disabling Connections....279
Disabling All Connections....280
Viewing statistics for an SCTP connection....280
Starting Diagnosis on a Test Connection....281
Ending Diagnosis on a Test Connection....281
Egress Throttle Groups maintenance....282
Egress Throttle Groups maintenance elements....284
Viewing Egress Throttle Groups status....285
Enabling Egress Throttle Groups Rate Limiting....286
Disabling Egress Throttle Groups Rate Limiting....286

Enabling Egress Throttle Groups Pending Transaction Limiting....287
Disabling Egress Throttle Groups Pending Transaction Limiting....287
Application maintenance....288
Applications maintenance elements....288
Viewing Application status....289
Enabling Applications....289
Disabling Applications....289
DA-MP maintenance....290
DA-MPs maintenance elements....290
Viewing DA-MP status....292

Chapter 5: Reports....293
Overview....294
Generating Diagnostics Tool Reports....294
Viewing, Printing, and Saving Diagnostics Tool Reports....295
Updating and Viewing MP Statistics (SCTP) Reports....296
MP Statistics (SCTP) report elements....296

Chapter 6: Diameter Mediation....299
Mediation overview....300
Rule Templates....302
Rule Template elements....305
Viewing Rule Templates....321
Adding a Rule Template....321
Adding online help to a Rule Template....323
Copying a Rule Template....324
Changing a Rule Template....325
Importing a Rule Template....325
Exporting a Rule Template....327
Deleting a Rule Template....327
Formatting Value Wizard....328
Formatting Value Wizard elements....328
Using the Formatting Value Wizard....336
Enumerations....336
Mediation Enumerations elements....337
Viewing Enumerations....338
Adding an Enumeration....338
Editing an Enumeration....339
Deleting an Enumeration....339
Triggers....340

Mediation Triggers elements....341
Viewing Triggers....342
Associating a Rule Set with a Trigger....342
Removing the Association of a Rule Set with a Trigger....343
State and Properties....344
Mediation State & Properties elements....345
Importing a Rule Template....346
Editing State and Properties....346
Deleting a Rule Template....347
Base Dictionary....348
Mediation Base Dictionary elements....348
Viewing an existing AVP Dictionary entry....350
Custom Dictionary....350
Mediation Custom Dictionary elements....351
Adding a new AVP Dictionary entry....353
Changing an existing AVP Dictionary entry....354
Deleting an AVP dictionary entry....354
All-AVP Dictionary....355
Mediation All-AVP Dictionary elements....355
Viewing an existing All-AVP Dictionary entry definition....357
Vendors....357
Mediation Vendors elements....358
Viewing Vendors....358
Adding a Vendor....358
Editing a Vendor Name....359
Deleting a Vendor....360
Rule Sets....360
User-defined Rule Sets....362
Rule Sets elements - View page....363
Rule Sets elements - Insert and Edit Pages....364
Adding a Rule to a Rule Set....365
Deleting All Rules from a Rule Set....367
Changing a Rule in a Rule Set....367
Deleting One Rule from a Rule Set....367

Chapter 7: DSR Capacity and Congestion Controls....369

Introduction....370
DA-MP Overload Control....370
Per-Connection Ingress MPS Control....372
Remote Congestion Controls....376

User Configurable Message Priority....379
Remote BUSY Congestion....382
Egress Transport Congestion....384
Per Connection Egress Message Throttling....385
User Configurable Connection Pending Transaction Limiting....388
Egress Throttle Groups....389
Glossary....395

List of Figures

Figure 1: Connection Capacity Dashboard Connections Tab....32

Figure 2: Diameter Topology Hiding Boundary....169

Figure 3: Diameter Topology Hiding Trigger Points: Protected-to-Untrusted Transactions....170

Figure 4: Diameter Topology Hiding Trigger Points: Untrusted-to-Protected Transactions....170

Figure 5: TH Network Deployment with DSR in an Interworking Network....173

Figure 6: S6a/S6d HSS TH Protected-HSS to Untrusted-MME/SGSN Diameter Transaction....179

Figure 7: S6a/S6d HSS TH Untrusted-MME/SGSN to Protected-HSS Transaction....180

Figure 8: MME/SGSN TH Protected-MME/SGSN to Untrusted HSS Transaction....183

Figure 9: MME/SGSN TH Untrusted-HSS to Protected MME/SGSN Transaction....184

Figure 10: Route-Record Hiding - Request Message....185

Figure 11: Route-Record Hiding - Answer Message....186

Figure 12: Multi-DEA Route-Record Message Loop Detection....186

Figure 13: Unsupported Pseudo-Host Route-Record Loop Detection....187

Figure 14: Proxy-Host Hiding....188

Figure 15: Error-Reporting-Host AVP Hiding....189

Figure 16: Diameter Message Copy Message Flow....261

Figure 17: Diameter Mediation Trigger Points....341

Figure 18: Per Connection Message Coloring....373

List of Tables

Table 1: Admonishments....20

Table 2: MP Profile Selection....36

Table 3: MP Profile Elements....37

Table 4: Application Ids elements....43

Table 5: CEX Parameters elements....48

Table 6: Command Codes elements....51

Table 7: MCC Ranges elements....54

Table 8: Connection Configuration Sets Elements....57

Table 9: Configuration Sets Elements....65

Table 10: Capacity Configuration Sets Elements....70

Table 11: Egress Message Throttling Configuration Set Elements....74

Table 12: Message Priority Configuration Set Elements....78

Table 13: Message Copy Configuration Set Elements....82

Table 14: Local Node Configuration Elements....86

Table 15: Peer Node Configuration Elements....92

Table 16: Connections Configuration Elements....101

Table 17: Route Groups Configuration Elements....116

Table 18: Route Lists Configuration Elements....121

Table 19: Peer Route Tables Elements....124

Table 20: Peer Routing Rules Configuration Elements....127

Table 21: Peer Routing Rules Operators....130

Table 22: Egress Throttle Groups Elements....134

Table 23: Reroute On Answer Configuration Elements....141
Table 24: Application Route Tables elements....143
Table 25: Application Routing Rules Configuration Elements....145
Table 26: Application Routing Rules Operators....148
Table 27: Routing Option Sets Elements....153
Table 28: Diameter Pending Answer Timer and Transaction Lifetime Selection....159
Table 29: Pending Answer Timers Elements....161
Table 30: System Options Elements....164
Table 31: DNS Options Elements....167
Table 32: Topology Information Hiding and Restoral Procedures....170
Table 33: Example Protected Networks Configuration....173
Table 34: Example Trusted Network Lists Configuration....173
Table 35: Network Trust Relationship Matrix....174
Table 36: Example Topology Hiding Status Settings....174
Table 37: General Criteria for Determining Whether a Message is a TH Candidate....174
Table 38: Protected Network Configuration Example....176
Table 39: Topology Hiding AVPs and Hiding Methods....176
Table 40: Example of Configuration of MME/SGSN TH Hostnames for a Protected Network....181
Table 41: Trusted Network Lists elements....190
Table 42: Path Topology Hiding Configuration Sets Elements....193
Table 43: S6a/S6d HSS Topology Hiding Configuration Sets Elements....198
Table 44: MME/SGSN Topology Hiding Configuration Sets Elements....201
Table 45: Protected Network Configuration Elements....207
Table 46: Valid Import Operations....212
Table 47: Bulk Import elements....215

Table 48: Bulk Export elements....220
Table 49: Application Types Supported by DSR Bulk Import and Export....225
Table 50: Local Node CSV Format....226
Table 51: Peer Node CSV Format....226
Table 52: Route Group CSV Format....227
Table 53: Route List CSV Format....228
Table 54: Peer Routing Rule CSV Format....228
Table 55: Connection CSV Format....230
Table 56: Connection Configuration Set CSV Format....230
Table 57: Reroute on Answer CSV Format....232
Table 58: System Options CSV Format....232
Table 59: DNS Options CSV Format....232
Table 60: CEX Configuration Set CSV Format....233
Table 61: Capacity Configuration Set CSV Format....233
Table 62: AppRouteRule CSV Format....234
Table 63: Application ID CSV Format....235
Table 64: CEX Parameters CSV Format....235
Table 65: Pending Answer Timer CSV Format....236
Table 66: Routing Option Set CSV Format....236
Table 67: Peer Route Table CSV Format....237
Table 68: Message Priority Configuration Set CSV Format....237
Table 69: Message Throttling Configuration Set CSV Format....237
Table 70: Message Copy Configuration Set CSV Format....238
Table 71: Application Route Table CSV Format....238
Table 72: MP Profile CSV Format....239

Table 73: Egress Throttle Groups CSV Format....239
Table 74: Reserved MCC Ranges CSV Format....240
Table 75: Command Code CSV Format....240
Table 76: Trusted Network List CSV Format....241
Table 77: Path Topology Hiding Configuration Set CSV Format....241
Table 78: S6a/S6d HSS Topology Hiding Configuration Set CSV Format....241
Table 79: MME/SGSN Topology Hiding Configuration Set CSV Format....242
Table 80: Protected Network CSV Format....242
Table 81: Supported Application CSV Format....243
Table 82: Address Individual CSV Format....243
Table 83: Address Range CSV Format....244
Table 84: Address Table CSV Format....244
Table 85: Destination Table CSV Format....244
Table 86: Routing Exception CSV Format....245
Table 87: Address Resolution CSV Format....245
Table 88: Option CSV Format....246
Table 89: Supported Application CSV Format....247
Table 90: Routing Exception CSV Format....247
Table 91: Default Destination Table CSV Format....248
Table 92: Address Resolution CSV Format....248
Table 93: Option CSV Format....249
Table 94: System Option CSV Format....250
Table 95: Message Copy CSV Format....251
Table 96: SBR CSV Format....251
Table 97: IPFE IpfeOption CSV Format....252

Table 98: IPFE IpfeListTsa CSV Format....253

Table 99: PCRFs CSV Format....254

Table 100: Binding Key Priority CSV Format....254

Table 101: Policy DRA Topology Hiding CSV Format....254

Table 102: Policy DRA Options CSV Format....255

Table 103: Error Codes CSV Format....255

Table 104: Access Point Names CSV Format....256

Table 105: Alarm Settings CSV Format....256

Table 106: Congestion Options CSV Format....257

Table 107: Tekelec-Specific MsgCopyAnswer AVP Format....264

Table 108: Portion of the Answer Message Included as Data Value of the MsgCopyAnswer AVP....264

Table 109: Initial Values in the Default Message Copy Configuration Set....268

Table 110: Route Lists Maintenance Elements....271

Table 111: Route Group Maintenance Elements....273

Table 112: Peer Nodes Maintenance Elements....274

Table 113: Connections Maintenance Elements....276

Table 114: Connections SCTP Statistics Elements....281

Table 115: Egress Throttle Groups Admin States....282

Table 116: ETG Operational Status....282

Table 117: ETG Operational Reason....283

Table 118: Egress Throttle Groups Maintenance Elements....284

Table 119: Applications Maintenance Elements....288

Table 120: DA-MPs Maintenance Elements....290

Table 121: MP Statistics (SCTP) Report Elements....296

Table 122: Rule Template elements....305
Table 123: Rule Template Condition Operators....318
Table 124: Rule Template Condition Conversion Rules....320
Table 125: Formatting Value Wizard elements....328
Table 126: Formatting Value Wizard Specifiers....329
Table 127: Mediation Enumeration elements....337
Table 128: Diameter Mediation Triggers....340
Table 129: Mediation Triggers elements....342
Table 130: Mediation State & Properties elements....345
Table 131: Mediation Base Dictionary Elements....348
Table 132: Mediation Custom Dictionary Elements....351
Table 133: Mediation All-AVP Dictionary elements....355
Table 134: Mediation Vendors elements....358
Table 135: Example of Default Ordering of Rules in a Rule Set....361
Table 136: Rule Sets Elements - View Page....363
Table 137: Maximum Allowed Rule Sets and Rules....364
Table 138: Rule Sets Elements - Insert and Edit Pages....364
Table 139: CLs, CPLs, and Message Treatment....377
Table 140: Mapping Congestion Levels to CPL Values....378
Table 141: Remote BUSY and EMR Capacity Ranges....379
Table 142: Message Priority Treatment Methods....382
Table 143: Mapping Congestion Levels to CPL Values....384
Table 144: Congestion Levels Based on Thresholds....387
Table 145: Message Priority and ETG Congestion Level....391
Table 146: ETG Message Rate Congestion Levels Based on Threshold....391

Table 147: ETG Pending Transaction Congestion Levels Based on Threshold.....393

Chapter 1

Introduction

Topics:

- *Overview.....19*
- *Scope and Audience.....19*
- *Document Organization.....19*
- *Documentation Admonishments.....20*
- *Related Publications.....20*
- *Customer Care Center.....21*
- *Emergency Response.....23*
- *Locate Product Documentation on the Customer Support Site.....24*

The *Diameter* document provides information about how to use the DSR GUI to perform Diameter Signaling Router tasks.

Overview

The *Diameter* document provides information about how to use the DSR GUI to perform Diameter Signaling Router tasks.

The document provides the following types of information:

- Procedures to configure Diameter components
- Maintenance information about Diameter components
- Procedures to generate reports for the Diagnostics Tool and MP Statistics
- Procedures to configure Diameter Mediation Rule Templates and Rule Sets

Scope and Audience

This manual is intended for personnel who perform Diameter Signaling Router tasks.

This manual contains procedures for performing Diameter Signaling Router tasks using the DSR GUI.

This manual does not describe how to install or replace software or hardware.

Document Organization

This document is organized into the following chapters:

- *Introduction* contains general information about the Diameter and Mediation help documentation, the organization of this manual, and how to get technical assistance.
- *Configuration* provides information on configuring Diameter resources and how to do bulk imports and exports of DSR configuration data.
- *Diameter Message Copy* describes the Diameter Message Copy feature, which is used in the DSR to send a copy of a message to a DAS.
- *Maintenance* provides information on how to view the status of Diameter resources, and how to enable and disable connections and DSR Applications.
- *Reports* provides information on how to produce Diagnostic Tool reports and MP Statistics (SCTP) reports.
- *Diameter Mediation* contains information about how to use Diameter Mediation to solve interoperability problems by creating rules to manipulate header parts and Attribute-Value Pairs (AVPs) in incoming routable messages.
- *DSR Capacity and Congestion Controls* contains information about the various ways DSR capacity and congestion can be managed to preserve the availability and Quality of Service (QoS) of the DSR.

Documentation Admonishments

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

Table 1: Admonishments

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

Related Publications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Customer Care Center

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

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

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

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

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

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

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

  TAC Regional Support Office Hours:

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

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

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

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

  - **Argentina**

    Phone:

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

  - **Brazil**

    Phone:

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

    TAC Regional Support Office Hours:

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

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **Dominican Republic**

    Phone:

    1-888-367-8552

  - **Mexico**

    Phone:

    001-888-367-8552

  - **Peru**

    Phone:

    0800-53-087

- **Puerto Rico**

  Phone:

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

- **Venezuela**

  Phone:

  0800-176-6497

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

  Regional Office Hours:

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

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

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

    TAC Regional Support Office Hours:

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

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with the Tekelec Customer Care Center.

Locate Product Documentation on the Customer Support Site

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

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

Configuration

Topics:

- *Configuration Sequence.....27*
- *Configuration Capacity Summary.....28*
- *Connection Capacity Validation.....29*
- *MP Profiles.....36*
- *Application Ids configuration.....42*
- *CEX Parameters configuration.....47*
- *Command Codes configuration.....50*
- *MCC Ranges configuration.....53*
- *Connection Configuration Set configuration.....56*
- *CEX Configuration Set configuration.....64*
- *Capacity Configuration Set configuration.....68*
- *Egress Message Throttling Configuration Set configuration.....73*
- *Message Priority Configuration Set configuration.....77*
- *Message Copy Configuration Set configuration.....81*
- *Local Node configuration.....85*
- *Peer Node configuration.....91*
- *Connection configuration.....99*
- *Route Group configuration.....115*
- *Route List configuration.....119*
- *Peer Route Tables configuration.....123*
- *Egress Throttle Groups configuration.....133*
- *Reroute On Answer configuration.....140*
- *Application Route Tables configuration.....142*
- *Routing Option Sets configuration.....152*
- *Pending Answer Timers configuration.....158*
- *System Options configuration.....163*
- *DNS Options configuration.....166*
- *Topology Hiding configuration.....167*

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

- *DSR Bulk Import.....209*
- *DSR Bulk Export.....218*

Configuration Sequence

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

Because some components need to be configured before others can be configured.

Diameter configuration on the SOAM needs to occur in the following order:

1. For DA-MPs, make any needed changes to configurable elements in the MP Profiles that will be used for the DA-MPs in the system; then assign **MP Profiles** to the DA-MPs.
2. Configure **Application Route Tables**.

   Configure only the Table Names. The Application Routing Rules must be configured after Application Ids and Command Codes are configured.

3. Configure **Pending Answer Timers**.
4. Configure **Peer Route Tables**.

   Configure only the Table Names. The Peer Routing Rules must be configured after Route Lists are configured.

5. Configure **Routing Option Sets**.
6. Configure **Application Ids**.
7. Configure **Command Codes**.
8. Configure **MCC Ranges** if either the Full Address Based Resolution (FABR) or Range Based Address Resolution (RBAR) DSR Application is activated in the DSR.
9. Configure **CEX Parameters**.
10. Configure **CEX Configuration Sets**.
11. Configure **Connection Configuration Sets**.

    Modify the Default Connection Configuration Set or create new Connection Configuration Sets to match the SCTP, Diameter, and TCP options that apply to your network.

12. Configure **Local Nodes**.
13. Configure **Peer Nodes**.

    Enable **Topology Hiding Status** if Topology Hiding will be applicable to the Peer Node.

14. Configure **Capacity Configuration Sets** for use with the *Per-Connection Ingress MPS Control* feature and *Connection Capacity Validation*.
15. Configure **Egress Message Throttling Configuration Sets**.
16. Configure **Message Priority Configuration Sets**.
17. Configure **Connections**.
18. Configure **Route Groups**.
19. Configure **Route Lists**.
20. If Alternate Implicit Routing will be used, edit **Peer Nodes** and select a Route List for each **Alternate Implicit Routing** element.
21. Configure **Message Copy Configuration Sets**.
22. Configure **Peer Routing Rules** in each configured Peer Route Table.
23. Configure **Egress Throttle Groups**.
24. Configure **Reroute On Answer**, if it will be used in the system.

25. Configure **Application Routing Rules** in each configured Application Route Table.
26. If necessary, change the default **System Options**
    - Enable the **Per Connection Egress Message Throttling** feature if it is used in the DSR.
    - Enable the **Message Copy Feature** if it is used in the DSR.
    - Change any default values as needed.
27. If necessary, enter or change default **DNS Options**.
28. Use the Diameter > Maintenance pages to enable configured components:
    - On the **Diameter > Maintenance > Connections** page, enable configured **Connections**.
    - On the **Diameter > Maintenance > Egress Throttle Groups** page, enable **Egress Throttle Groups Rate Limiting**, **Egress Throttle Groups Pending Transaction Limiting**, or both, if used in the DSR.

The Diameter Topology Hiding components are configured in the following order on the NOAM:

1. Trusted Network Lists, which are used in the Protected Networks configuration
2. One or more Configuration Sets, for each Topology Hiding Type that will be used:
    - Path Topology Hiding Configuration Sets
    - S6a/S6d Topology Hiding Configuration Sets
    - MME/SGSN Topology Hiding Configuration Sets
3. Protected Networks, which use the Trusted Network Lists and Configuration Sets in their configuration.

Configuration Capacity Summary

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

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

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

Connection Capacity Validation

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

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

Connection Capacity Validation has no direct impact on the operation of any given DA-MP at run time or on IPFE servers in a DSR.

The following definitions apply in this document:

- **Target Set** - a collection of DA-MP servers, any one of which can be selected by the IPFE server for the purposes of establishing a Floating (IPFE) Diameter Connection.
- **Non-overlapping Target Set** - A Target Set each of whose DA-MPs does not appear in any other configured Target Set.
- **Overlapping Target Sets** - If any single DA-MP appears in more than one Target Set, those Target Sets "overlap" the DA-MP, sharing its capacity resources.

Connection Capacity Validation behaves according to the following general principles:

- The weighting of DA-MPs within a Target Set is assumed to be equal for the purposes of all Connection configuration validations.

  Any non-equal weighting of DA-MPs within a Target Set (achieved through IPFE server configuration) is of no consequence to -Connection Capacity Validation at configuration time.

- Over-configuration of both Connection counts and Reserved Ingress MPS is possible in certain circumstances. No alarms or other "active" notifications are generated.
  - For a system having no IPFE Connections, no over-configuration can occur under any circumstances.
  - For a system having one or more Target Sets that do not overlap each other, no over-configuration can occur (with the possible exception of upgrading an already over-configured system).
  - For a system having two or more Target Sets that overlap each other in any way, over-configuration can occur because the DSR does not prevent configuration changes when overlapping Target Sets are involved.
- The DSR and Connection Capacity Validation prevent and do not prevent configuration changes under the following conditions:
  - The DSR will not prevent Connection configuration changes that involve the DA-MPs in overlapping Target Sets. The complexities of overlapping Target Sets make it difficult to determine over-configuration conditions when a DSR with overlapping Target Sets is near or at capacity. If there are also non-overlapping Target Sets, prevention of changes affecting non-overlapping Target Sets is still enforced.
  - When only a single non-overlapping Target Set is involved, the DSR will prevent Connection configuration changes that cause the Target Set's capacity to be exceeded.

  - When there are no Target Sets involved at all - meaning there are no IPFE Connections, only Fixed Connections - the DSR will prevent Connection configuration changes that cause the individual DA-MP hosting the subject Fixed Connection to exceed its capacity.

- The **IPFE Connection Reserved Ingress MPS Scaling** value (percent) is applied to a DA-MPs total Engineered Ingress MPS. The **IPFE Connection Reserved Ingress MPS Scaling** value is effectively a scaling factor on the total Reserved Ingress MPS that can be configured for a DA-MP, encompassing the contributions of both IPFE and Fixed Connections.
- When dealing with a non-overlapping Target Set, the configuration capacity of the constituent DA-MPs can be thought of as pooled. Even though IPFE Connections are typically considered to be evenly distributed across all the DA-MPs in the Target Set, within a non-overlapping Target Set capacity from one DA-MP can be "borrowed and loaned" to another DA-MP, for the purposes of validating capacity changes. (This has absolutely no effect on the actual distribution of IPFE Connections by the IPFE server.)

  This situation can occur if the number of Fixed Connections varies significantly among DA-MPs in the non-overlapping Target Set. In that case, much of one DA-MP's capacity is taken up by Fixed Connections, which means there is less room for IPFE Connections. But if another DA-MP in the non-overlapping Target Set has fewer Fixed Connections, it has more room for IPFE Connections. The capacity on the DA-MP with fewer Fixed Connections can be used for IPFE Connections. See *Interpreting Apparent DA-MP Over-Configuration with Non-overlapping Target Sets* for a concrete example of how this works.

IPFE Connection Reserved Ingress MPS Scaling

Because only the Client Diameter Connections are configured with non-zero Reserved Ingress MPS, **IPFE Connection Reserved Ingress MPS Scaling** values (IPFE Scaling Factor) greater than 50% introduce the potential for a DA-MP to accept sufficient IPFE Connections that could result in the total ingress MPS processed by the DA-MP (including ingress MPS on non-IPFE Connections) exceeding the DA-MP's **Engineered Ingress MPS** rating.

- If ONLY IPFE Connections have non-zero **Reserved Ingress MPS** defined, and non-IPFE Connections have a zero **Reserved Ingress MPS**, the configuration restriction of the IPFE Scaling Factor = 50% will enable the system to behave optimally.
- If non-IPFE Connections have non-zero **Reserved Ingress MPS** defined, then the maximum Reserved Ingress MPS available for all DA-MP Connections will be limited by scaled Engineered Reserved Ingress MPS of the DA-MP.

Therefore, the IPFE Scaling Factor does in fact limit the total Connection Reserved Ingress MPS on a DA-MP. The intended deployment is that all Fixed Connections will have a **Reserved Ingress MPS** value of zero, so that the IPFE Scaling Factor value of 50% will affect only IPFE Connections.

Assumptions and Limitations

Connection Capacity Validation has the following assumptions and limitations:

- Configuration validation decisions never include run time or status information.
- The allocation of IPFE Connection configurations within a Target Set is *always* evenly distributed across the DA-MPs in the Target Set.
- Even in valid configurations, it is possible that Connections cannot be established at run time due to Ingress MPS variations.

- If Connections are running near capacity (say, above Reserved but below or at Maximum Ingress MPS), a DA-MP may not be able to establish a Connection that is part of a properly-configured system.
- Due to the even distribution mathematics, it is also possible for an IPFE Target Set to have sufficient Reserved Ingress MPS capacity overall, but any given DA-MP does not have sufficient capacity to establish a given IPFE Connection whose Reserved Ingress MPS is sufficiently high.

  This becomes more likely as the total Connection Reserved Ingress MPS approaches the capacity of the Target Set.

- Connection Capacity Validation does not take into account unequal weighting of DA-MPs within an IPFE Target Set.

  Weighting is primarily a Connection establishment factor. Weighting does not affect the Connection capacity of any individual DA-MP, or the total capacity of a Target Set.

Over-Configuration Considerations

Connection Capacity Validation has the following over-configuration considerations:

- Over-configuration of both Connection counts and Reserved Ingress MPS is possible and explicitly allowed when overlapping Target Sets are present.
- Any DSR that is running a DSR release earlier than 5.0, and is already over-configured in some way, will remain over-configured after upgrade to DSR 5.0 or later.
- There are no alarms or other "active" notifications generated by the DSR system to indicate Connection count or Reserved Ingress MPS over-configurations.
- The Connection Capacity Dashboard page can be viewed to see the state of the current Connection/DA-MP configuration. This is a "passive" notification.
- Over-configuration has no direct impact on the behavior of the DA-MP software when establishing Connections. The Connection Capacity Validation feature is a configuration-only feature; the logic used by the DA-MPs to determine if any given Connection establishment request can be honored is unaffected by Connection Capacity Validation Updates.

  The ability for a DA-MP to run traffic in excess of the scaled Engineered Ingress MPS value is unaffected by Connection Capacity Validation Updates.

- DSR 4.x systems having an IPFE Scaling Factor of 50% prior to upgrade will retain the 50% value after upgrade. But in DSR 4.0, this IPFE Scaling Factor was not used in configuration validation; in DSR 5.0, it is. It is possible for a DSR 4.0 system to be over-configured immediately after upgrade, with no change in configuration.

  Look at the **Diameter > Configuration > Connection Capacity Dashboard** GUI page to see if the **Maximum Reserved Ingress MPS** (for the capacity) and **Connection Reserved Ingress MPS** columns (Fixed and IPFE) show any over-configuration.

Interpreting Apparent DA-MP Over-Configuration with Non-overlapping Target Sets

Just because a particular DA-MP *appears* to be over-configured does not necessarily mean it is actually over-configured. The Connection Capacity Dashboard data must be interpreted within the context of the Target Set configuration established for the DSR.

Here is a concrete example. *Figure 1: Connection Capacity Dashboard Connections Tab* shows the Connections tab of the Connection Capacity Dashboard. And at first glance, it looks like Charger-MP3

is highly over-configured. It has a capacity of 1000 Connections, and currently has 900 Fixed and 500 IPFE Connections allocated to it.

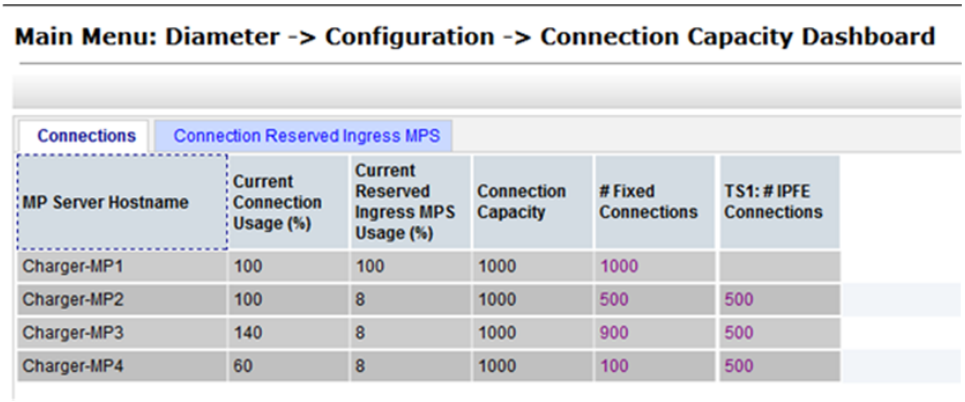

Figure 1: Connection Capacity Dashboard Connections Tab

But a deeper analysis reveals that Charger-MP3 is part of just one non-overlapping Target Set, TS1. The individual DA-MP capacities within a non-overlapping Target Set can be pooled. The total available capacity of TS1 is (3 DA-MPs * 1000) = 3000 Connections. Given that there are 1500 Fixed Connections configured across the three DA-MPs, there is still room for 1500 IPFE Connections in TS1. *Figure 1: Connection Capacity Dashboard Connections Tab* shows those 1500 IPFE Connections evenly distributed across the DA-MPs, 500 each.

Taken as a whole, the TS1 DA-MPs are not over-configured. Whenever all the Connections are actually established, 500 will be established on Charger-MP2, 100 on Charger-MP3, and 900 on Charger-MP4. The Connection Capacity Validation logic correctly determined that the DA-MPs within the non-overlapping Target Set were able to accommodate all 1500 IPFE Connections configured for TS1, given the fact that each DA-MP in the Target Set has some number of Fixed Connections consuming capacity.

Connection Capacity Dashboard Page

The functions of the Connection Capacity Validation feature are described in *Connection Capacity Validation*. On the **Diameter > Configuration > Connection Capacity Dashboard** GUI page, the Connection Capacity Validations feature displays the current Connection configuration capacity information for configured Active DA-MPs.

Each row on the page contains the information for one configured Active DA-MP.

The **Diameter > Configuration > Connection Capacity Dashboard** is a view-only page with two tabs.

The **Connections** tab contains information about the currently configured Connections for each DA-MP in the DSR NE. Fixed and IPFE Connections appear, with IPFE (Floating) Connections grouped by Target Set.

The **Connection Reserved Ingress MPS** tab contains the currently configured Reserved Ingress MPS for each DA-MP in the DSR NE. The contribution of both Fixed and IPFE Connections is displayed, with IPFE Connections grouped by Target Set.

If any configured DA-MP does not have an assigned MP Profile, the associated row on each Dashboard tab displays the **MP Server Hostname** in the first column, and all other fields in the row contain '—'.

Note: The Connection Capacity Dashboard does not use field coloring. Usage values at or in excess of 100% are not flagged by cell coloring.

The Connections Tab

The following information appears for each configured Active DA-MP when the **Connections** tab is selected:

MP Server Hostname	Hostname of the DA-MP server.
Current Connection Usage (%)	The percentage of the total Connection capacity currently used, which is the sum of Fixed and IPFE Connections allocated to the DA-MP, divided by the total **Connection Capacity** value shown in the fourth column. It is theoretically possible for this usage value to exceed 100%; the DSR does not prevent over-configuration in certain scenarios (typically involving overlapping Target Sets, or a non-overlapping Target Set whose DA-MPs have significantly different numbers of Fixed Connections assigned). For a given DA-MP, if the number of Connections allocated to that DA-MP exceeds the DA-MP's **Maximum Connections** count capacity (from the assigned MP Profile), the **Current Connection Usage (%)** value will exceed 100%.
Current Reserved Ingress MPS Usage (%)	The percentage of scaled Engineered Ingress MPS capacity currently used. This usage value is computed as the sum of Reserved Ingress MPS values for a DA-MP's Fixed and IPFE Connections, divided by the **Maximum Reserved Ingress MPS** value shown in the fourth column of the **Connection Reserved Ingress MPS** tab It is theoretically possible for this usage value to exceed 100%; the DSR does not prevent over-configuration in certain scenarios (typically involving overlapping Target Sets, or a non-overlapping Target Set whose DA-MPs have significantly different numbers of Fixed Connections assigned).
Connection Capacity	The DA-MP's total Connection capacity. The value is **Maximum Connections** value in the MP Profile that has been assigned to the DA-MP, which is the maximum number of Diameter Connections that the DA-MP can have configured at any one time.
# Fixed Connections	The number of Fixed Connections currently configured for the DA-MP. For a given DA-MP, the value displayed in the **# Fixed Connections** field should: • Never exceed the **Connection Capacity** value. • Always agree with the number of Fixed Connections displayed on the **Diameter > Configuration > Connections** page, when filtering on **IP Owner** = the given DA-MP If a DA-MP has one or more configured Fixed Connections, the value appears as a hyperlink. The hyperlink opens the **Diameter > Configuration > Connections [Filtered]**page, filtered to show only the Fixed Connections that are assigned to the DA-MP.

If the DSR NE has Target Sets configured, the following information appears, one column for each Target Set, up to a maximum of 32 Target Sets:

TSn: # IPFE Connections Reserved Ingress MPS	A configured Target Set, where n is the Target Set number. The numbering of the Target Sets will be ascending, but may not be sequential. The value displayed for a given DA-MP and Target Set is the evenly-distributed allocation of IPFE Connections to each DA-MP in the Target Set. If the evenly-distributed allocation value is zero, then the value 0 is displayed in the field. The evenly distributed allocation of IPFE Connections will be zero if there are more DA-MPs in the Target Set than IPFE Connections configured for the Target Set. In this case, to make it visually clear that the DA-MP is part of the Target Set, the value of zero will be displayed (instead of leaving the field blank). If a DA-MP has no IPFE allocation for a defined Target set, the corresponding field is blank, to help visualize how Target Sets overlap.

The Connection Reserved Ingress MPS Tab

The following information appears under the **Connection Reserved Ingress MPS** tab:

MP Server Hostname	Hostname of the DA-MP server.
Current Connection Usage (%)	The percentage of the total Connection capacity currently used, which is the sum of Fixed and IPFE Connections allocated to the DA-MP, divided by the total **Connection Capacity** value shown in the fourth column. It is theoretically possible for this usage value to exceed 100%; the DSR does not prevent over-configuration in certain scenarios (typically involving overlapping Target Sets, or a non-overlapping Target Set whose DA-MPs have significantly different numbers of Fixed Connections assigned). For a given DA-MP, if the number of Connections allocated to that DA-MP exceeds the DA-MP's **Maximum Connections** count capacity (from the assigned MP Profile), the **Current Connection Usage (%)** value will exceed 100%.
Current Reserved Ingress MPS Usage (%)	The percentage of scaled Engineered Ingress MPS capacity currently used. This usage value is computed as the sum of Reserved Ingress MPS values for a DA-MP's Fixed and IPFE Connections, divided by the **Maximum Reserved Ingress MPS** value shown in the fourth column of the **Connection Reserved Ingress MPS** tab It is theoretically possible for this usage value to exceed 100%; the DSR does not prevent over-configuration in certain scenarios (typically involving overlapping Target Sets, or a non-overlapping Target Set whose DA-MPs have significantly different numbers of Fixed Connections assigned). If the total Connection Reserved Ingress MPS for Connections allocated to a given DA-MP exceeds the DA-MP's scaled Engineered Ingress MPS, the **Current Reserved Ingress MPS Usage (%)** will exceed 100%
Maximum Reserved Ingress MPS	The DA-MP's **Engineered Ingress MPS** value, scaled by the **IPFE Connection Reserved Ingress MPS Scaling** value (from the **Diameter > Configuration > System Options** page. The DA-MP's **Engineered Ingress MPS** value comes from the **MP Profile** that has been assigned to the DA-MP.

The **IPFE Connection Reserved Ingress MPS Scaling** value, from the **Diameter > Configuration > System Options** page, is the percent of DA-MP **Engineered Ingress MPS** used by each DA-MP when validating the Reserved Ingress MPS for a newly received IPFE Connection. A newly received IPFE Connection will be rejected if the total Connection Reserved Ingress MPS for Fixed and already established IPFE Connections would exceed the DA-MP's Engineered Ingress MPS, scaled by this value.

Total Fixed Connection Reserved Ingress MPS

The sum of the **Reserved Ingress MPS** values for all Fixed Connections configured to a DA-MP.

For a given DA-MP, the value displayed in the **Total Fixed Connection Reserved Ingress MPS** field should not exceed the **Maximum Reserved Ingress MPS** value.

Note: There is one possible exception. Consider a system already configured with Fixed Connections having some non-zero **Total Fixed Connection Reserved Ingress MPS**. If the IPFE Scaling Factor is decreased, thus decreasing the scaled Engineered Ingress MPS on every DA-MP in the DSR, it is possible the new lowered **Maximum Reserved Ingress MPS** will be less than the already-configured **Total Fixed Connection Reserved Ingress MPS**.

If a DA-MP has no Fixed Connections assigned to it, the corresponding field shows a value of zero

If a DA-MP has one or more Fixed Connections, the value appears as a hyperlink. The hyperlink opens the **Diameter > Configuration > Connections [Filtered]** page, filtered to show only those Fixed Connections assigned to the DA-MP.

If the DSR NE has Target Sets configured, the following information appears following the tab columns, one column for each Target Set, up to a maximum of 32 Target Sets:

TSn: # IPFE Connections Reserved Ingress MPS

A configured Target Set, where *n* is the Target Set number. The numbering of the Target Sets will be ascending, but might not be sequential.

Note: The IPFE GUI does not require Target Sets to be configured sequentially. Target Sets 4, 11, 12, and 32 can be defined, for example. The Dashboard page will always show only the configured Target Sets, in order from the smallest configured number to the largest configured number.

The value displayed for a given DA-MP and Target Set field is the evenly-distributed allocation of IPFE Connections' Reserved Ingress MPS to each DA-MP in the Target Set. If the evenly-distributed allocation value is zero, then the value 0 shall be displayed in the field.

The evenly distributed allocation of IPFE Connections will be zero if all of the IPFE Connections configured for the Target Set have Reserved Ingress MPS values of zero. In this case, to make it visually clear that the DA-MP is part of the Target Set, the value of zero will be displayed (instead of leaving the field blank).

If a DA-MP has no IPFE allocation for a defined Target set, the corresponding field is blank, to help visualize how Target Sets overlap.

If a DA-MP has one or more IPFE Connections allocated to it for a given Target Set, the value is displayed as a hyperlink. When clicked, the **Diameter > Configuration > Connections [Filtered]** page opens, filtered to show only those IPFE Connections assigned to the Target Set. Because IPFE Connections are not configured to a particular

DA-MP, this filtered display cannot show a DA-MP allocation; it will instead show all IPFE Connections in the Target Set.

DA-MP and Target Set Associations

The DA-MPs that are included in a Target Set (TS) are easily identified because they always have a number in the Dashboard cell that is the intersection of the DA-MP and Target Set.

- If there are no IPFE Connections yet defined for a TS, each DA-MP in the TS still shows a value of zero on both the **Connections** and **Connection Reserved Ingress MPS** tabs.
- If there are fewer IPFE Connections defined for a TS than DA-MPs assigned to the TS, the evenly-distributed value shown on the **Connections** tab is zero. Each included DA-MP will show a value of zero for the Target Set.
- If all IPFE Connections in a Target Set have **Reserved Ingress MPS** values of zero, then each DA-MP included in the TS will show a value of zero on the **Connection Reserved Ingress MPS** tab.

Overlapping Target Sets can be easily identified on the Dashboard by looking for DA-MPs that have a value for more than one Target Set.

- If a given DA-MP shows no number for any Target Set, that DA-MP is not included in any Target Set - and therefore cannot host IPFE Connections.
- If a given DA-MP shows a number for just one Target Set, that DA-MP is not "overlapped" in more than one Target Set.
- If a given DA-MP shows a number for more than one Target Set, then all Target Sets that include the DA-MP overlap.

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 distinct DA-MP server.

An MP Profile defines maximum and threshold values for a DA-MP. An MP Profile must be assigned to each DA-MP in the DSR configuration. Select the appropriate MP Profile according to the DA-MP hardware and combination of DSR Applications that are running on the DA-MP, as shown in *Table 2: MP Profile Selection*. The only supported combination of session and database applications running on the same DA-MP is Policy DRA and RBAR.

Table 2: MP Profile Selection

DA-MP Hardware	Application(s)	MP Profile
G6 half height blade	Diameter Relay	G6:Relay
G8 half height blade	Diameter Relay	G8:Relay
G7 full height blade	Diameter Relay	G7:Relay
Virtual DA-MP	Diameter Relay	VM:Relay
G6 half height blade	Diameter Relay + FABR or RBAR	G6:Database
G8 half height blade	Diameter Relay + FABR or RBAR	G8:Database
G7 full height blade	Diameter Relay + FABR or RBAR	G7:Database

DA-MP Hardware	Application(s)	MP Profile
Virtual DA-MP	Diameter Relay + FABR or RBAR	VM:Database
G6 half height blade	Diameter Relay + CPA or Policy DRA	G6:Session
G8 half height blade	Diameter Relay + CPA or Policy DRA	G8:Session
G7 full height blade	Diameter Relay + CPA or Policy DRA	G7:Session
Virtual DA-MP	Diameter Relay + CPA or Policy DRA	VM:Session
G6 half height blade	Diameter Relay + RBAR + Policy DRA	G6:Session_Database
G8 half height blade	Diameter Relay + RBAR + Policy DRA	G8:Session_Database
G7 full height blade	Diameter Relay + RBAR + Policy DRA	G7:Session_Database

Table 3: MP Profile Elements describes the user-configurable and engineering-configured values in an MP Profile.

Note: The Ingress Message Rate Alarm Threshold values for the Policy DRA application are user-configurable on the **NOAM Policy DRA > Configuration > Congestion Options** GUI page; they are not shown in *Table 3: MP Profile Elements*.

MP Profiles elements

Table 3: MP Profile Elements describes the fields on the **MP Profiles** page. **The Data Input Notes** apply only to the Configurable elements.

Table 3: MP Profile Elements

Field (* indicates required field)	Description	Data Input Notes
Configurable		
* CL1 Discard Percent	The percentage below DA-MP Engineered Ingress MPS that DA-MP Overload Control will police the total DA-MP ingress MPS when the DA-MP is in congestion level 1.	Format: text box Range: 0 - 50% Default: 0
* CL2 Discard Percent	The percentage below DA-MP Engineered Ingress MPS that DA-MP Overload Control will police the total DA-MP ingress MPS to when the DA-MP is in congestion level 2.	Format: text box Range: 10 - 50% Default: 20
* CL3 Discard Percent	The percentage below DA-MP Engineered Ingress MPS that DA-MP Overload Control will police the total DA-MP ingress MPS to when the DA-MP is in congestion level 3.	Format: text box Range: 20 - 50% Default: 40
Congestion Discard Policy	The order of priority and/or color-based traffic segments to consider when determining discard	Format: pulldown list

Field (* indicates required field)	Description	Data Input Notes
	candidates for the application of treatment during DA-MP Congestion processing.	Range: Priority Only, Color Within Priority, Priority Within Color Default: Priority Only
* DOC Message Discard Percentage	The percent of total DA-MP ingress MPS above DA-MP Engineered Ingress MPS that DA-MP Overload Control will discard when the DA-MP is in danger of congestion.	Format: text box Range: 0 - 50 % Default: 20
DOC Discard Policy	The order of priority and/or color-based traffic segments to consider when determining discard candidates for the application of treatment during DA-MP DOC processing.	Format: pulldown list Range: Priority Only, Color Within Priority, Priority Within Color Default: Priority Only
View-Only		
Maximum Connections	The maximum number of Diameter connections the DA-MP can have configured at any one time	Engineering-configured
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.	Engineering-configured
Maximum Ingress Message Rate Minor Alarm Set Threshold	The ingress message rate, in messages per second, above which a minor alarm is raised.	Engineering-configured
Maximum Ingress Message Rate Minor Alarm Clear Threshold	The ingress message rate, in messages per second, below which a minor alarm is cleared.	Engineering-configured
Maximum Ingress Message Rate Major Alarm Set Threshold	The ingress message rate, in messages per second, above which a major alarm is raised.	Engineering-configured
Maximum Ingress Message Rate Major Alarm Clear Threshold	The ingress message rate, in messages per second, below which a major alarm is cleared.	Engineering-configured
Maximum Ingress Message Rate Critical Alarm Set Threshold	The ingress message rate, in messages per second, above which a critical alarm is raised.	Engineering-configured
Maximum Ingress Message Rate Critical Alarm Clear Threshold	The ingress message rate, in messages per second, below which a critical alarm is cleared.	Engineering-configured

Field (* indicates required field)	Description	Data Input Notes
Routing Message Rate Minor Alarm Set Threshold	The Diameter message processing rate, in messages per second, above which a minor alarm is raised.	Engineering-configured
Routing Message Rate Minor Alarm Clear Threshold	The Diameter message processing rate, in messages per second, below which a minor alarm is cleared.	Engineering-configured
Routing Message Rate Major Alarm Set Threshold	The Diameter message processing rate, in messages per second, above which a major alarm is raised.	Engineering-configured
Routing Message Rate Major Alarm Clear Threshold	The Diameter message processing rate, in messages per second, below which a major alarm is cleared.	Engineering-configured
Routing Message Rate Critical Alarm Set Threshold	The Diameter message processing rate, in messages per second, above which a critical alarm is raised.	Engineering-configured
Routing Message Rate Critical Alarm Clear Threshold	The Diameter message processing rate, in messages per second, below which a critical alarm is cleared.	Engineering-configured
RBAR Receive Message Rate Minor Alarm Set Threshold	The ingress request rate for the RBAR Application, in messages per second, above which a minor alarm is raised.	Engineering-configured
RBAR Receive Message Rate Minor Alarm Clear Threshold	The ingress request rate for the RBAR Application, in messages per second, below which a minor alarm is cleared.	Engineering-configured
RBAR Receive Message Rate Major Alarm Set Threshold	The ingress request rate for the RBAR Application, in messages per second, above which a major alarm is raised.	Engineering-configured
RBAR Receive Message Rate Major Alarm Clear Threshold	The ingress request rate for the RBAR Application, in messages per second, below which a major alarm is cleared.	Engineering-configured
RBAR Receive Message Rate Critical Alarm Set Threshold	The ingress request rate for the RBAR Application, in messages per second, above which a critical alarm is raised.	Engineering-configured
RBAR Receive Message Rate Critical Alarm Clear Threshold	The ingress request rate for the RBAR Application, in messages per second, below which a critical alarm is cleared.	Engineering-configured
FABR Receive Message Rate Minor Alarm Set Threshold	The ingress request rate for the FABR Application, in messages per second, above which a minor alarm is raised.	Engineering-configured

Field (* indicates required field)	Description	Data Input Notes
FABR Receive Message Rate Minor Alarm Clear Threshold	The ingress request rate for the FABR Application, in messages per second, below which a minor alarm is cleared.	Engineering-configured
FABR Receive Message Rate Major Alarm Set Threshold	The ingress request rate for the FABR Application, in messages per second, above which a major alarm is raised.	Engineering-configured
FABR Receive Message Rate Major Alarm Clear Threshold	The ingress request rate for the FABR Application, in messages per second, below which a major alarm is cleared.	Engineering-configured
FABR Receive Message Rate Critical Alarm Set Threshold	The ingress request rate for the FABR Application, in messages per second, above which a critical alarm is raised.	Engineering-configured
FABR Receive Message Rate Critical Alarm Clear Threshold	The ingress request rate for the FABR Application, in messages per second, below which a critical alarm is cleared.	Engineering-configured
CPA Receive Message Rate Minor Alarm Set Threshold	The ingress request rate for the CPA Application, in messages per second, above which a minor alarm is raised.	Engineering-configured
CPA Receive Message Rate Minor Alarm Clear Threshold	The ingress request rate for the CPA Application, in messages per second, below which a minor alarm is cleared.	Engineering-configured
CPA Receive Message Rate Major Alarm Set Threshold	The ingress request rate for the CPA Application, in messages per second, above which a major alarm is raised.	Engineering-configured
CPA Receive Message Rate Major Alarm Clear Threshold	The ingress request rate for the CPA Application, in messages per second, below which a major alarm is cleared.	Engineering-configured
CPA Receive Message Rate Critical Alarm Set Threshold	The ingress request rate for the CPA Application, in messages per second, above which a critical alarm is raised.	Engineering-configured
CPA Receive Message Rate Critical Alarm Clear Threshold	The ingress request rate for the CPA Application, in messages per second, below which a critical alarm is cleared.	Engineering-configured

Viewing MP Profiles

Use this task to view the available MP Profiles.

1. Select **Diameter** > **Configuration** > **DA-MPs** > **MP Profiles**.
   The **Diameter > Configuration > DA-MPs > MP Profiles** page appears.
2. Click the DA-MP type tabs at the top of the table to view the MP Profile settings for the following DA-MP types:

- **G6:Relay** - G6 DA-MP half height blade running relay application
- **G8:Relay** - G8 DA-MP half height blade running relay application
- **G7:Relay** - G7 DA-MP full height blade running relay application
- **VM:Relay** - Virtualized DA-MP running relay application
- **G6:Database** - G6 DA-MP half height blade running relay and database applications
- **G8:Database** - G8 DA-MP half height blade running relay and database applications
- **G7:Database** - G7 DA-MP full height blade running relay and database applications
- **VM:Database** - Virtualized DA-MP running relay and database applications
- **G6:Session** - G6 DA-MP half height blade running relay and session applications
- **G8:Session** - G8 DA-MP half height blade running relay and session applications
- **G7:Session** - G7 DA-MP full height blade running relay and session applications
- **VM:Session** - Virtualized DA-MP running relay and session applications
- **G6:Session_Database** - G6 DA-MP half height blade running relay, session, and database applications
- **G8:Session_Database** - G8 DA-MP half height blade running relay, session, and database applications
- **G7:Session_Database** - G7 DA-MP full height blade running relay, session, and database applications

The MP Profile values are read-only. For information about the MP Profile values see *MP Profiles*.

Editing Configurable MP Profile Parameters

Use this task to edit the values for configurable parameters in each MP Profile type that will be assigned to a DA-MP in the DSR.

The configurable parameters are described in *MP Profiles elements*.

1. Select **Diameter** > **Configuration** > **DA-MPs** > **MP Profiles**.
   The **Diameter > Configuration > DA-MPs > MP Profiles** page appears.
2. For each MP Profile type, edit the values for the configurable parameters.
3. Click:
   - **Apply** to save the edited parameter values.
   - **Cancel** to reset the parameter values to their previous setting.

Assigning MP Profiles to DA-MPs

Use this task to assign an MP Profile to each DA-MP in the DSR.

Note: An MP Profile assignment does not take effect until the DA-MP has been restarted.

1. Select **Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**.
   The **Diameter > Configuration > DA-MPs > Profile Assignments** page appears.
2. For each DA-MP, select one of the available MP Profiles. See *Table 2: MP Profile Selection* for help in selecting the appropriate MP Profile.
3. Click:
   - **Assign** to assign the selected MP Profiles to the DA-MPs.

- **Cancel** to reset the MP Profile assignments to their previous setting.

To correct a warning that a Standby MP has a different MP Profile assignment than its corresponding Active MP, reassign the desired MP Profile to the Active/Standby MP pair on this page.

Application Ids configuration

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

An Application Route Table, a Peer Route Table, a Routing Option Set, and a Pending Answer Timer can be associated with an Application Id. These configuration settings are used when routing messages that contain the Application Id. However, if the Application Route Table, Peer Route Table, and Routing Option Set are configured for a message's upstream Peer Node, then those settings override the ones configured for the Application Id. If the Pending Answer Timer is configured for a message's downstream Peer Node, then that setting overrides the one configured for the Application Id.

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 fields are described in *Application Ids elements*.

On the **Diameter > Configuration > Application Ids** page, you can perform the following actions:

- Filter the list of Application Ids, to display only the desired Application Ids.
- Sort the list entries in ascending or descending order by Application Id, Name, Application Route Table, Peer Route Table, Routing Option Set, or Pending Answer Timer, by clicking the column heading.

  By default, the list is sorted by Application Id in ascending ASCII order.
- Click the **Insert** button.

  The **Diameter > Configuration > Application Ids [Insert]** page opens. You can add a new Diameter Configuration Application Id and its values. See *Adding an Application Id*.

  If the maximum number of Application Ids (1000) already exists in the system, the **Diameter > Configuration > Application Ids [Insert]** page will not open, and an error message is displayed.
- Select an **Application Id** in the list, and click the **Edit** button.

  The **Diameter > Configuration > Application Ids [Edit]** page opens. You can edit the selected Application Id. See *Editing an Application Id*.
- Select an **Application Id** in the list, and click the **Delete** button to remove the selected Application Id. See *Deleting an Application Id*.

Application Ids elements

Table 4: 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 4: Application Ids elements

Element	Description	Data Input Notes
Name	Application Id Name	Format: case-sensitive; alphanumeric and underscore; cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters
Application Id Value	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 (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	Format: two radio buttons: • Pulldown list of available Application Ids • Text box; numeric, maximum 10 digits Range: • 1-16777215 for Standard Application Ids • 16777216-4294967294 for Vendor-specific Application Ids • 4294967295 for Relay Default in pulldown list: "-Select-"
Application Route Table	The Application Route Table associated with this Application Id. The Application Route Table contains Application Routing Rules that are used for routing Requests with the associated Appl-Id when the upstream Peer Node does not have an associated Application Route Table.	Format: pulldown list Range: configured Application Route Tables Default: Default Application Route Table

Element	Description	Data Input Notes
	If an Application Route Table is configured for a message's upstream Peer Node, that Application Route Table overrides the Application Route Table specified here.	
Peer Route Table	The Peer Route Table associated with this Application Id. The Peer Route Table contains Peer Routing Rules that are used for routing Requests with the associated Appl-Id when the upstream Peer Node does not have an associated Peer Route Table. If a Peer Route Table is configured for a message's upstream Peer Node, that Peer Route Table overrides the Peer Route Table specified here.	Format: pulldown list Range: configured Peer Route Tables Default: Default Peer Route Table
Routing Option Set	The Routing Option Set associated with the Diameter Application. Routing Option Sets contain information used to handle delivery error conditions. If a Routing Option Set is configured for a message's upstream Peer Node, that Routing Option Set overrides the Routing Option Set specified here.	Format: pulldown list Range: configured Routing Option Sets Default: Default Routing Option Ser
Pending Answer Timer	The Pending Answer Timer associated with the Diameter Application. If a Pending Answer Timer is configured for a message's downstream Peer Node, that Pending Answer Timer overrides the Pending Answer Timer specified here.	Format: pulldown list Range: configured Pending Answer Timers Default: Default Pending Answer Timer

Viewing Application Ids

Use this task to view all configured Application Ids.

Select **Diameter** > **Configuration** > **Application Ids**.

The **Diameter > Configuration > Application Ids** page appears with a list of configured Application Ids. The fields are described in *Application Ids elements*.

Adding an Application Id

Use this task to configure a new Application Id.

The fields are described in *Application Ids elements*.

1. Select **Diameter** > **Configuration** > **Application Ids**.

   The **Diameter > Configuration > Application Ids** page appears.

2. Click **Insert**.

   The **Diameter > Configuration > Application Ids [Insert]** page appears.

   If the maximum number of Application Ids (1000) has already been configured in the system, the **Diameter > Configuration > Application Ids [Insert]** page will not open, and an error message will appear.

3. Enter a unique **Name** for the Diameter Application.
4. Select an Application Id Value from the pulldown list or enter a unique value in the text box to identify a specific Diameter Application. (Application Id is required.)
5. Select an **Application Route Table** containing the Application Routing Rules that control routing of messages associated with this Diameter Application.

   If an Application Route Table is configured for a message's upstream Peer Node, that Application Route Table overrides the Application Route Table specified here.

6. Select a **Peer Route Table** containing the Peer Routing Rules that control routing of messages associated with this Diameter Application.

   If a Peer Route Table is configured for a message's upstream Peer Node, that Peer Route Table overrides the Peer Route Table specified here.

7. Select a **Routing Option Set** that specifies how certain routing error conditions are handled for messages associated with this Diameter Application

   A Routing Options Set that has an assigned Pending Answer Timer cannot be associated with an Application Id.

   If a Routing Option Set is configured for a message's upstream Peer Node, that Routing option Set overrides the Routing Option Set specified here.

8. Select a **Pending Answer Timer** to specify how long DSR waits for a response to a message associated with this Diameter Application.

   If a Pending Answer Timer is configured for a message's downstream Peer Node, that Pending Answer Timer overrides the Pending Answer Timer specified here.

9. Click:

   - **OK** to save the new Application Id and return to the **Diameter > Configuration > Application Ids** page.
   - **Apply** to save the new Application Id and remain on this page.

- **Cancel** to return to the **Diameter > Configuration > Application Ids** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any fields contain a value that is out of the allowed range
- The **Application Id** required field is empty (not entered)
- Adding the new Application Id would cause the maximum number of Application Ids (1000) to be exceeded
- Adding the new Application Id would cause the maximum number of Peer Route Table/Application Id combinations (20) to be exceeded.

Editing an Application Id

Use this procedure to change the Name, Application Route Table, Peer Route Table, Routing Option Set, or Pending Answer Timer for a selected Application Id. (The **Application Id Value** field cannot be changed.)

The fields are described in *Application Ids elements*.

When the **Diameter > Configuration > Application Ids [Edit]** page opens, the fields are populated with the current configured values.

1. Select **Diameter** > **Configuration** > **Application Ids**.

   The **Diameter > Configuration > Application Ids** page appears.

2. Select the **Application Id** row to be changed.
3. Click the **Edit** button.

   The **Diameter > Configuration > Application Ids [Edit]** page appears.

4. Change the **Name**, **Application Route Table**, **Peer Route Table**, **Routing Option Set**, or **Pending Answer Timer** for the selected **Application Id**.
5. Click:

   - **OK** to save the changes and return to the **Diameter > Configuration > Application Ids** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Application Ids** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The selected Application Id no longer exists; it has been deleted by another user
   - Any fields contain values that are out of range
   - Any required field is empty (not entered)

Deleting an Application Id

Use the following procedure to delete an Application Id.

Note: An Application Id cannot be deleted if the Application Id is associated with a CEX Configuration Set.

1. Select **Diameter** > **Configuration** > **Application Ids**.

   The **Diameter > Configuration > Application Ids** page appears.

2. Select the **Application Id** to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.

4. Click:

   - **OK** to delete the Application Id.

     If the Application Id is associated with a CEX Configuration Set, the Application Id is not deleted and an error message appears.

   - Click **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Application Ids** page.

   If **OK** is clicked and the selected Application Id no longer exists (it was deleted by another user), an error message is displayed and the Application Ids view is refreshed.

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.

On the **Diameter > Configuration > CEX Parameters** page, you can perform the following actions:

- Filter the list of Application Ids, to display only the desired Application Ids.
- Sort the list entries in ascending or descending order by Application Id, Application Id Type, or Vendor Id, by clicking the column heading. By default, the list is sorted by Application Id in ascending ASCII order.
- Click an Application Id in the list to go the Application Id configuration page for that application.
- Click the **Insert** button.

  The **Diameter > Configuration > CEX Parameters [Insert]** page opens. You can assign a new set of CEX Parameters to an Application Id. See *Adding CEX Parameters*.

- Select an **Application Id** in the list, and click the **Edit** button.

  The **Diameter > Configuration > CEX Parameters [Edit]** page opens. You can edit the CEX Parameters for the selected Application Id. See *Editing CEX Parameters*.

- Select an **Application Id** in the list, and click the **Delete** button to delete the CEX Parameters for the selected Application Id. See *Deleting CEX Parameters*.

CEX Parameters elements

Table 5: 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 5: 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
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

Viewing CEX Parameters

Use this task to view CEX Parameters configured for Application Ids.

Select **Diameter** > **Configuration** > **CEX Parameters**. The **Diameter > Configuration > CEX Parameters** page appears with a list of configured Application Ids. The fields are described in *CEX Parameters elements*.

Adding CEX Parameters

Use this task to add CEX Parameters to an Application Id.

The fields are described in *CEX Parameters elements*.

1. Select **Diameter** > **Configuration** > **CEX Parameters**.

The **Diameter > Configuration > CEX Parameters** page appears.

2. Click **Insert**.

   The **Diameter > Configuration > CEX Parameters [Insert]** page appears.

3. Select an Application Id from the pulldown menu.
4. Set the Application Id Type.
5. If appropriate, check the **Vendor Specific Application Id** check box.
6. If you checked **Vendor Specific Application Id**, specify the **Vendor Id**.
7. Click:

   - **OK** to save the new CEX Parameters and return to the **Diameter > Configuration > CEX Parameters** page.
   - **Apply** to save the new CEX Parameters and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > CEX Parameters** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any fields contain a value that is out of the allowed range
   - The **Application Id**, **Application Id Type**, and **Vendor Id** combination is not unique

Editing CEX Parameters

Use this procedure to change the Application Id Type, Vendor-Specific Id, or Vendor Id for a selected Application Id. (The **Application Id** field cannot be changed.)

The fields are described in *CEX Parameters elements*.

When the **Diameter > Configuration > CEX Parameters [Edit]** page opens, the fields are populated with the current configured values.

Note: If the selected Application Id is present in a CEX Configuration Set that is a part of an Enabled connection, the CEX Parameter fields cannot be changed. An error message is displayed.

1. Select **Diameter** > **Configuration** > **CEX Parameters**.

   The **Diameter > Configuration > CEX Parameters** page appears.

2. Select the **Application Id** row to be changed.
3. Click the **Edit** button.

   The **Diameter > Configuration > Application Ids [Edit]** page appears.

4. Change the **Application Id Type**, **Vendor-Specific Id**, or **Vendor Id** for the selected **Application Id**.

   The **Vendor Id** must be unique.

5. Click:

   - **OK** to save the changes and return to the **Diameter > Configuration > CEX Parameters** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > CEX Parameters** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The selected Application Id no longer exists; it has been deleted by another user
- Any fields contain values that are out of range
- Any required field is empty (not entered)
- The **Application Id**, **Application Id Type**, and **Vendor Id** combination is not unique

Deleting CEX Parameters

Use the following procedure to delete CEX Parameters associated with an Application Id.

Note: CEX Parameters cannot be deleted if the Application Id is associated with a CEX Configuration Set.

1. Select **Diameter** > **Configuration** > **CEX Parameters**.

   The **Diameter > Configuration > CEX Parameters** page appears.

2. Select the **Application Id** for which you want to delete CEX Parameters.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.

4. Click:

   - **OK** to delete the CEX Parameters from the Application Id.

     If the Application Id is associated with a CEX Configuration Set, the CEX Parameters are not deleted and an error message appears.

   - Click **Cancel** to cancel the delete function and return to the **Diameter > Configuration > CEX Parameters** page.

   If **OK** is clicked and the selected Application Id no longer exists (it was deleted by another user), an error message is displayed and the CEX Parameters view is refreshed.

Command Codes configuration

The Command Code is one of the parameters contained in a Diameter Message. In the Command Codes configuration section, you can define the Command Code values that can be used in Peer Routing Rules and Application Routing Rules.

On the **Diameter > Configuration > Command Codes** page, you can perform the following actions:

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

The **Diameter > Configuration > Command Codes [Insert]** page opens. You can add a new Command Code. See *Adding a Command Code*. If the maximum number of Command Codes (1000) already exists in the system, the **Diameter > Configuration > Command Codes [Insert]** page will not open, and an error message is displayed.

- Select an **Command Code** in the list, and click the **Edit** button.

  The **Diameter > Configuration > Command Codes [Edit]** page opens. You can edit the selected Command Code. See *Editing a Command Code*.

- Select an **Command Code** in the list, and click the **Delete** button to remove the selected Command Code. See *Deleting a Command Code*.

Command Codes elements

Table 6: 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 6: 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

Viewing Command Codes

Use this task to view all configured Command Codes.

Select **Diameter** > **Configuration** > **Command Codes**.

The **Diameter > Configuration > Command Codes** page appears with a list of configured Command Codes. The fields are described in *Command Codes elements*.

Adding a Command Code

Use this task to configure a new Command Code.

The fields are described in *Command Codes elements*.

1. Select **Diameter** > **Configuration** > **Command Codes**.

   The **Diameter > Configuration > Command Codes** page appears.

2. Click **Insert**.

   The **Diameter > Configuration > Command Codes [Insert]** page appears.

   If the maximum number of Command Codes (1000) has already been configured in the system, the **Diameter > Configuration > Command Codes [Insert]** page will not open, and an error message will appear.

3. Enter a unique **Command Code Name** for the Command Code.
4. Select a **Command Code** from the menu or enter a unique value to identify a specific Command Code (Command Code is required.)
5. Click:

   - **OK** to save the new Command Code and return to the **Diameter > Configuration > Command Codes** page.
   - **Apply** to save the new Command Code and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Command Codes** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any fields contain a value that is out of the allowed range
   - Any required field is empty (not entered)
   - Adding the new Command Code would cause the maximum number of Command Codes (1000) to be exceeded

Editing a Command Code

Use this procedure to change the Command Code Name for a selected Command Code. (The **Command Code** field cannot be changed.)

The fields are described in *Command Codes elements*.

When the **Diameter > Configuration > Command Codes [Edit]** page opens, the fields are populated with the current configured values.

1. Select **Diameter** > **Configuration** > **Command Codes**.

   The **Diameter > Configuration > Command Codes** page appears.

2. Select the Command Code row to be changed.
3. Click the **Edit** button.

   The **Diameter > Configuration > Command Codes [Edit]** page appears.

4. Change the **Command Code Name** for the selected Command Code.

   The **Name** must be unique.

5. Click:

- **OK** to save the changes and return to the **Diameter > Configuration > Command Codes** page.
- **Apply** to save the changes and remain on this page.
- **Cancel** to return to the **Diameter > Configuration > Command Codes** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The selected Command Code no longer exists; it has been deleted by another user
- Any fields contain values that are out of range
- Any required field is empty (not entered)

Deleting a Command Code

Use the following procedure to delete a Command Code.

A Command Code cannot be deleted if it is associated with any of the following Configuration components:

- Peer Routing Rule
- Application Routing Rule
- Message Priority Configuration Set
- A FABR or RBAR Address Resolution

1. Select **Diameter** > **Configuration** > **Command Codes**.

   The **Diameter > Configuration > Command Codes** page appears.

2. Select the **Command Code** to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.

4. Click:

   - **OK** to delete the Command Code.

     If the Command Code is used in a Peer Routing Rule or Application Routing Rule, the Command Code is not deleted and an error message appears.

   - Click **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Command Codes** page.

   If **OK** is clicked and any of the following conditions exist, the selected Command Code no longer exists (it was deleted by another user), an error message is displayed and the Command Codes is refreshed.

MCC Ranges configuration

The Reserved **MCC Ranges** component defines up to 10 distinct, non-overlapping Mobile Country Code Ranges, which are the first 3 digits of the IMSI. A decoded IMSI that falls within one of these MCC ranges is considered reserved for Address Resolution in the Range Based Address Resolution

(RBAR) and Full Address Based Resolution (FABR) DSR Application. RBAR and FABR will continue decoding using other AVP instances, or next Priority AVP (if configured), or next Routing Entity (if configured).

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

- 000-199
- 800-899

On the **Diameter > Configuration > MCC Ranges** page, you can perform the following actions:

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

  The **Diameter > Configuration > MCC Ranges [Insert]** page opens. You can add new MCC Ranges. If the maximum number of MCC Ranges (10) already exists in the system, the **Diameter > Configuration > MCC Ranges [Insert]** page will not open, and an error message is displayed.
- Select an MCC Range in the list, and click the **Edit** button.

  The **Diameter > Configuration > MCC Ranges [Edit]** page opens. The selected Start MCC, End MCC, or both for the selected MCC Range can be edited.
- Select an MCC Range in the list, and click the **Delete** button to remove the selected MCC Range.

MCC Ranges elements

Table 7: MCC Ranges elements describes the fields on the **Diameter > Configuration > MCC Ranges** pages.

Table 7: MCC Ranges elements

Field (* indicates a required field)	Description	Value
* Start MCC	The start value of the Reserved Mobile Country Code Range.	Format: text box; numeric. Range: 0-999
* End MCC	The end value of the Reserved Mobile Country Code Range.	Format: text box; numeric. Range: 0-999

Viewing MCC Ranges

Use this task to view all configured MCC Ranges.

MCC Ranges fields are described in *MCC Ranges elements*.

Select **Diameter** > **Configuration** > **MCC Ranges**.

The **Diameter > Configuration > MCC Ranges** page appears with a list of configured **MCC Ranges**.

Adding MCC Ranges

Use this task to configure new **MCC Ranges**.

MCC Ranges fields are described in *MCC Ranges elements*.

1. Select **Diameter** > **Configuration** > **MCC Ranges**.

   The **Diameter > Configuration > MCC Ranges** page appears.

2. Click **Insert**.

   The **Diameter > Configuration > MCC Ranges [Insert]** page appears.

   If the maximum number of **MCC Ranges** (10) has already been configured in the system, the **Diameter > Configuration > MCC Ranges [Insert]** page will not open, and an error message will appear.

3. Enter a value for the **Start MCC** field.
4. Enter a value for the **End MCC** field.
5. Click:

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

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any fields contain a value that is out of the allowed range
   - Any required field is empty (not entered)
   - Adding the new **MCC Range** would cause the maximum number of **MCC Ranges** (10) to be exceeded
   - The **Start MCC** field value is greater than the End MCC field value
   - The **MCC Range** created lies within the ranges of other **MCC Ranges**

Editing MCC Ranges

Use this task to change **MCC Ranges**.

MCC Ranges fields are described in *MCC Ranges elements*.

When the **Diameter > Configuration > MCC Ranges [Edit]** page opens, the fields are populated with the current configured values.

1. Select **Diameter** > **Configuration** > **MCC Ranges**.

   The **Diameter > Configuration > MCC Ranges** page appears.

2. Select the **MCC Range** to be changed.
3. Click the **Edit** button.

   The **Diameter > Configuration > MCC Ranges [Edit]** page appears.

4. Change the **Start MCC** and **End MCC** fields.
5. Click:

   - **OK** to save the changes and return to the **Diameter > Configuration > MCC Ranges** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > MCC Ranges** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The selected **MCC Range** no longer exists; it has been deleted by another user
   - Any field contains values that are out of range
   - Any required field is empty (not entered)
   - The **Start MCC** field value is greater than the **End MCC** field value
   - The **MCC Range** created lies within the ranges of other MCC Ranges

Deleting MCC Ranges

Use this tak to delete a **MCC Ranges**.

1. Select **Diameter** > **Configuration** > **MCC Ranges**.

   The **Diameter > Configuration > MCC Ranges** page appears.

2. Select the **MCC Range** to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.

4. Click:

   - **OK** to delete the **MCC Ranges**.
   - Click **Cancel** to cancel the delete function and return to the **Diameter > Configuration > MCC Ranges** page.

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

Connection Configuration Set configuration

Connection Configuration Sets provide a mechanism for adjusting a connection to account for the network quality of service and Peer Node requirements. You can create a Connection Configuration Set with specific SCTP, Diameter, and TCP options and then assign it to a connection. The options are

described in *Connection Configuration Set elements*. Each connection references a single Connection Configuration Set.

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

On the **Connection Configuration Sets** page, you can perform the following actions:

- Filter the list of Connection Configuration Sets to display only the desired Connection Configuration Sets.
- Sort the list by column contents in ascending or descending order, by clicking the column heading. The default order is by **Connection Configuration Set Name** in ascending ASCII order.
- Click a tab to display the options for the Connection Configuration Set on that tab. The **Connection Configuration Set Name** remains on the left of the page when the page is scrolled to the right to see all of the options.
- Click the **Insert** button.

  The **Connection Configuration Sets [Insert]** page appears. You can add a new Connection Configuration Set and its options. See *Adding a Connection Configuration Set*.

  If the maximum number of Connection Configuration Sets per Network Element (2000) already exist in the system, the **Connection Configuration Sets [Insert]** page will not open, and an error message is displayed.

- Select a Connection Configuration Set Name in the list, and click the **Edit** button.

  The **Connection Configuration Sets [Edit]** page opens. You can edit the selected Connection Configuration Set. See *Editing a Connection Configuration Set*.

  If at least one connection that uses the Connection Configuration Set is in the "Enabled" Admin state, the **Connection Configuration Sets [Edit]** page will not open.

- Select a Connection Configuration Set Name in the list, and click the **Delete** button to remove the selected Connection Configuration Set.

  The Default Connection Configuration Set cannot be deleted. See *Deleting a Connection Configuration Set*.

Connection Configuration Set elements

Table 8: 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 8: 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

Field (* indicates required field)	Description	Data Input Notes
		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 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.	Format: numeric; milliseconds 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

Field (* indicates required field)	Description	Data Input Notes
* 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. This value should not be greater than the sum of the retransmit attempts for all destinations within the association.	Format: numeric; number of attempts Range: 1 - 20 Default: 5
* 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.	Format: numeric; number of bytes Range: 8000 - 5000000

Field (* indicates required field)	Description	Data Input Notes
	The receive buffer size must be greater than or equal to the product of the bandwidth and the round trip delay for the association.	Default: 2000000
* Maximum Burst	Specifies the maximum burst of packets that can be emitted by this association.	Format: numeric 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	Format: numeric; seconds

Field (* indicates required field)	Description	Data Input Notes
	message, time to wait for the Peer to send the DPA. If the timer expires, transport will be disconnected by the application.	Range: 1 - 10 Default: 3
Proving Mode	Proving mode for the Configuration Set.	Format: radio buttons Range: Suspect, Always, Never 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

Viewing Connection Configuration Sets

Use this task to view currently configured Connection Configuration Sets.

Select **Diameter** > **Configuration** > **Configuration Sets** > **Connection Configuration Sets**.
The **Connection Configuration Sets** page appears.

Adding a Connection Configuration Set

Use this task to create a new Connection Configuration Set.

When you add a new Connection Configuration Set all of the fields on each tab are initially populated with the values from the Default Connection Configuration Set. For details about the fields in the Connection Configuration Set, see *Connection Configuration Set elements*.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Connection Configuration Sets**.
   The **Connection Configuration Sets** page appears.
2. Click **Insert**.
   The **Connection Configuration Sets [Insert]** page appears.
3. Enter a unique name for the Configuration Set in the **Connection Configuration Set Name** field.
4. Click the **SCTP Options** tab. Enter the SCTP values in the fields.
5. Click the **Diameter Options** tab. Enter the Diameter values in the fields.
6. Click the **TCP Options** tab. Enter the TCP values in the fields.
7. Click:

   - **OK** to save the data and return to the **Connection Configuration Sets** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Connection Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any field is empty (no value was entered)
   - The value in any field is not valid or is out of range
   - The **Connection Configuration Set Name** is not unique; it already exists in the system
   - The maximum number of Connection Configuration Sets per Network Element (2000) is already configured
   - Under the **SCTP Options** tab, the **Retransmit Maximum Timeout** is less than the **Retransmit Minimum Timeout**
   - Under the **SCTP Options** tab, the **Number of Retransmits Triggering Path Failure** is greater than the **Number of Retransmits Triggering Association Failure**

Editing a Connection Configuration Set

Use this task to edit an existing Connection Configuration Set.

When the **Connection Configuration Sets** page opens, the fields are populated with the currently configured values.

If the selected Connection Configuration Set is being used by a Local Node, any changes to the selected Connection Configuration Set will not take effect for Peer-initiated connections until the next time the Peer Node connects to the Local Node.

The **Connection Configuration Set Name** cannot be edited.

Note: You must disable all Connections that use a particular Connection Configuration Set before you can edit it. See *Disabling Connections*.

Changes to the Connection Configuration Set take effect after the changes are saved and the Connections that refer to the changed Connection Configuration Set are set to the "Enabled" Admin state.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Connection Configuration Sets**.
   The **Connection Configuration Sets** page appears.
2. Select the Connection Configuration Set you want to edit.
3. Click **Edit**.
   The **Connection Configuration Sets [Edit]** page appears.
4. Update the relevant fields.

   For information about each field, see *Connection Configuration Set elements*.
5. Click:

   - **OK** to save the data and return to the **Connection Configuration Sets** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Connection Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The selected Connection Configuration Set no longer exists; it has been deleted by another user
   - Any field is empty (no value was entered)
   - The value in any field is not valid or is out of range
   - Under the **SCTP Options** tab, the **Retransmit Maximum Timeout** is less than the **Retransmit Minimum Timeout**
   - Under the **SCTP Options** tab, the **Number of Retransmits Triggering Path Failure** is greater than the **Number of Retransmits Triggering Association Failure**
   - At least one connection that is using this Connection Configuration Set is not in the "Disabled" Admin State

Deleting a Connection Configuration Set

Use this task to delete a Connection Configuration Set.

A Connection Configuration Set cannot be deleted if it is being used by any connections or Local Nodes. Before you perform this task, you must:

1. Disable any connections that use the Connection Configuration Set. See *Disabling Connections*.
2. Edit those connections to no longer use the Connection Configuration Set. See *Editing a Connection*.
3. Edit any Local Nodes that use the Connection Configuration Set to no longer do so. See *Editing a Local Node*.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Connection Configuration Sets**.
   The **Connection Configuration Sets** page appears.
2. Select the Connection Configuration Set you want to delete.

3. Click **Delete.**
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Connection Configuration Set.
   - **Cancel** to cancel the delete function and return to the **Connection Configuration Sets** page.

   If **OK** is clicked and the selected Connection Configuration Set is referenced by at least one connection or Local Node, an error message appears and the Connection Configuration Set is not deleted.

   If **OK** is clicked and the selected Connection Configuration Set no longer exists (it was deleted by another user), an error message is displayed and the Connection Configuration Sets view is refreshed.

CEX Configuration Set configuration

A CEX Configuration Set provides a mechanism for assigning up to 10 unique CEX Parameters and up to 10 unique supported Vendor IDs to a Local Node or Connection. A default CEX Configuration Set named "Default" is pre-populated with CEX Parameters for the "RELAY" Application Id (0xFFFFFFFF).

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

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

On the **CEX Configuration Sets** page, you can perform the following actions:

- Filter the list of CEX Configuration Sets to display only the desired CEX Configuration Sets.
- Sort the list in ascending or descending order, by clicking the **CEX Configurations Set Name** column heading. The default order is by CEX Configuration Set Name in ascending ASCII order.
- In the **CEX Parameters** column,
  - Click the + sign to the left of the number of Application Ids to expand the list of Application Ids for a CEX Configuration Set.
  - Click the - sign to left of the number of Application Ids to collapse the expanded list of Application Ids for a CEX Configuration Set.
  - Click a blue Application Id in an expanded list to open the **Diameter > Configuration > CEX Parameters [Filtered]** page for the selected Application Id only.
- Click the **Insert** button.

  The **CEX Configuration Sets [Insert]** page opens. You can add a new CEX Configuration Set and its values. See *Adding a CEX Configuration Set*. If the maximum number of CEX Configuration Sets

(2000) already exists in the system, the **CEX Configuration Sets [Insert]** page will not open, and an error message is displayed.

- Select a CEX Configuration Set Name in the list, and click the **Edit** button.

  The **CEX Configuration Sets [Edit]** page opens. You can edit the selected CEX Configuration Set. See *Editing a CEX Configuration Set*. The Default CEX Configuration Set cannot be edited.

- Select a CEX Configuration Set Name in the list, and click the **Delete** button to remove the selected CEX Configuration Set.

  The Default CEX Configuration Set cannot be deleted. See *Deleting a CEX Configuration Set*.

CEX Configuration Set elements

Table 9: 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 9: 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
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

Field (* indicates a required field)	Description	Data Input Notes
	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

Viewing CEX Configuration Sets

Use this task to view currently configured CEX Configuration Sets.

Select **Diameter** > **Configuration** > **Configuration Sets** > **CEX Configuration Sets**.
The **CEX Configuration Sets** page appears.

Adding a CEX Configuration Set

Use this task to create a new CEX Configuration Set.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **CEX Configuration Sets**.
   The **CEX Configuration Sets** page appears.
2. Click **Insert**.
   The **CEX Configuration Sets [Insert]** page appears.
3. Enter a unique name for the CEX Configuration Set in the **CEX Configuration Set Name** field.
4. Enter the information for the **CEX Parameters** in the fields.
   - To add CEX Parameters to the **Selected CEX Parameters** list, select the entry in the **Available CEX Parameters** list and click the **Add** button below the **Available CEX Parameters** list.
   - To add CEX Parameters to the **Must Include CEX Parameters** list, select the entry in the **Selected CEX Parameters** list and click the **Add** button above the Must Include CEX Parameters list.
   - To remove CEX Parameters from the **Selected CEX Parameters** list, select the entry in the **Selected CEX Parameters** list and click the **Remove** button below the **Selected CEX Parameters** list.
   - To remove CEX Parameters from the **Must Include CEX Parameters** list, select the entry in the **Must Include CEX Parameters** list and click the **Remove** button above the **Must Include CEX Parameters** list.
5. Enter the information for the **Supported Vendor IDs** in the fields.
   - To add a Vendor Id to the **Selected Supported Vendor Ids** list, select the entry in the **Available Supported Vendor Ids** list and click the **Add** button below the **Available Supported Vendor Ids** list.
   - To remove a Vendor Id from the **Selected Supported Vendor Ids** list, select the entry in the **Selected Supported Vendor Ids** list and click the **Remove** button above the **Selected Supported Vendor Ids** list.
6. Click:
   - **OK** to save the new CEX Configuration Set and return to the **CEX Configuration Sets** page.
   - **Apply** to save the new CEX Configuration Set and remain on this page.

- **Cancel** to return to the **CEX Configuration Sets** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The **Selected CEX Parameters** list is empty (an item was not added)
- Any item that was selected to add to a list was deleted by another user during this Insert session
- The maximum number of configured CEX Configuration Sets (2000), Selected CEX Parameters + Must Include CEX Parameters for a CEX Configuration Set (10), or Supported Vendor Ids for a CEX Configuration Set (10) was reached by another user's entries during this Insert session

Editing a CEX Configuration Set

Use this task to edit an existing CEX Configuration Set.

For information about each field, see *CEX Configuration Set elements*.

Note: You must disable connections that use a particular CEX Configuration Set before you can edit the CEX Configuration Set. See *Disabling Connections*.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **CEX Configuration Sets**.
   The **CEX Configuration Sets** page appears.
2. Select the CEX Configuration Set that you want to edit.
   The Default CEX Configuration Set cannot be changed.
3. Click **Edit.**

   The **CEX Configuration Sets [Edit]** page appears.

   When the page opens, the fields are initially populated with the currently configured values.
4. Update the relevant fields.

   If an entry is attempted that is not valid or is out of range, an error message appears.

   The **CEX Configuration Set Name** cannot be changed.

   - To add CEX Parameters to the **Selected CEX Parameters** list, select the entry in the **Available CEX Parameters** list and click the **Add** button below the **Available CEX Parameters** list.
   - To add CEX Parameters to the **Must Include CEX Parameters** list, select the entry in the **Selected CEX Parameters** list and click the **Add** button above the Must Include CEX Parameters list.
   - To remove CEX Parameters from the **Selected CEX Parameters** list, select the entry in the **Selected CEX Parameters** list and click the **Remove** button below the **Selected CEX Parameters** list.
   - To remove CEX Parameters from the **Must Include CEX Parameters** list, select the entry in the **Must Include CEX Parameters** list and click the **Add** button above the **Must Include CEX Parameters** list.
   - To add a Vendor Id to the **Selected Supported Vendor Ids** list, select the entry in the **Available Supported Vendor Ids** list and click the **Add** button below the **Available Supported Vendor Ids** list.
   - To remove a Vendor Id from the **Selected Supported Vendor Ids** list, select the entry in the **Selected Supported Vendor Ids** list and click the **Remove** button above the **Selected Supported Vendor Ids** list.
5. Click:

- **OK** to save the changes and return to the **CEX Configuration Sets** page.
- **Apply** to save the changes and remain on this page.
- **Cancel** to return to the **CEX Configuration Sets** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The **Selected CEX Parameters** list is empty (no items were added)
- Any item that was selected to add to a list was deleted by another user during this Insert session
- The selected CEX Configuration Set is being used by a connection or a Local Node
- The selected CEX Configuration Set was deleted by another user during this Edit session

Deleting a CEX Configuration Set

Use this task to delete a CEX Configuration Set.

A CEX Configuration Set cannot be deleted if it is being used by any connections or Local Nodes. Before you perform this task, you must:

1. Disable any connections that use the CEX Configuration Set. See *Disabling Connections*.
2. Edit those connections to no longer use the CEX Configuration Set. See *Editing a Connection*.
3. Edit any Local Nodes that use the CEX Configuration Set to no longer do so. See *Editing a Local Node*.

The Default CEX Configuration Set can be edited, but cannot be deleted.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **CEX Configuration Sets**.
   The **CEX Configuration Sets** page appears.
2. Select one CEX Configuration Set that you want to delete.
3. Click **Delete**
   A popup window appears.
4. Click:

   - **OK** to delete the selected CEX Configuration Set.
   - **Cancel** to cancel the delete function and return to the **CEX Configuration Sets** page.

   If **OK** is clicked and the selected CEX Configuration Set is referenced by at least one connection or Local Node, an error message appears and the CEX Configuration Set is not deleted.

   If **OK** is clicked and the selected CEX Configuration Set no longer exists (it was deleted by another user), an error message is displayed and the CEX Configuration Sets view is refreshed.

Capacity Configuration Set configuration

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

The Capacity Configuration Set called Default is always available. The Default Capacity Configuration Set options can be modified, but the Default Capacity Configuration Set 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.

On the **Capacity Configuration Sets** page, you can perform the following actions:

- Filter the list of Capacity Configuration Sets to display only the desired Capacity Configuration Sets.
- Sort the Capacity Configuration Set entries by clicking the column headings. By default, the entries are sorted by the Capacity Configuration Set column in ascending ASCII order.
- Click the **Insert** button.

  The **Capacity Configuration Sets [Insert]** page opens. You can add a new Capacity Configuration Sets and its values. See *Adding a Capacity Configuration Set*.

  If the maximum number of Capacity Configuration Sets (1000) already exists in the system, the **Capacity Configuration Sets [Insert]** page does not open and an error message is displayed.

- Select the Name of a Capacity Configuration Set in the list, and click the **Edit** button.

  The **Capacity Configuration Sets [Edit]** page opens. You can edit the selected Capacity Configuration Set. See *Editing a Capacity Configuration Set*.

- Select the Name of a Capacity Configuration Set in the list, and click the **Delete** button to remove the selected Capacity Configuration Set. See *Deleting a Capacity Configuration Set*. The Default Capacity Configuration Set can be edited, but not deleted.

Connection Capacity Validation

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

The Connection Capacity Validation function is described in *Connection Capacity Validation*.

Validation of the Reserved Ingress MPS occurs in response to changes to the configuration of Capacity Configuration Sets that increase the Reserved Ingress MPS value, including editing the value and replacing the Configuration Set with one that has a higher value. Such changes reduce the available Reserved Ingress MPS capacity of a DSR and must be validated before they can be allowed. (Actions that increase capacity rather than reduce it do not require validation.)

An error is displayed, stating the reason, when the validation determines that performing the configuration action would cause over-configuration of Reserved Ingress MPS in a DA-MP or Target Set, or that a configuration action cannot be performed for another reason such as no MP Profile assigned to the subject DA-MP.

A warning is displayed when the validation cannot determine whether the configuration action would cause over-configuration of Reserved Ingress MPS in a DA-MP or Target Set.

If an error and a warning could apply, the error is displayed.

The Diameter > Configuration > Connection Capacity Dashboard page displays the current Connection Count and Reserved Ingress MPS data per DA-MP. The page functions and contents are described in *Connection Capacity Dashboard Page*.

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 10: 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. The Ingress MPS Minor Alarm Threshold must be less than the Ingress MPS Major Alarm Threshold.	Format: numeric Range: 10 - 99 percent Default: 50 percent

Field (* indicates field is required)	Description	Data Input Notes
* 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
* Reserved Ingress MPS Abatement Time	Time (in ms) that a DSR Connection's ingress message rate must remain less than or equal to Reserved Ingress MPS, after exceeding Reserved Ingress MPS, in order to revert the ingress traffic color from Yellow to Green.	Format: numeric Range: 1000 - 5000 ms Default: 2000 ms

Viewing Capacity Configuration Sets

Use this task to view currently configured Capacity Configuration Sets.

Select **Diameter** > **Configuration** > **Configuration Sets** > **Capacity Configuration Sets**.
The **Capacity Configuration Sets** page appears.

Adding a Capacity Configuration Set

Use this task to create a new Capacity Configuration Set. For information about the fields, see *Capacity Configuration Set elements*.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Capacity Configuration Sets**.
   The **Capacity Configuration Sets** page appears.
2. Click **Insert**.
   The **Capacity Configuration Sets [Insert]** page appears.
3. Enter a unique name for the Capacity Configuration Set in the **Name** field.
4. Enter the **Reserved Ingress MPS** value in messages/second.
5. Enter the **Maximum Ingress MPS** value in messages/second.
6. Enter the **Ingress MPS Minor Alarm Threshold** as the percentage of the Maximum Ingress MPS at which a Minor alarm will be raised for connections using this Capacity Configuration Set.
7. Enter the **Ingress MPS Major Alarm Threshold** as the percentage of the Maximum Ingress MPS at which a Major alarm will be raised for connections using this Capacity Configuration Set.
8. Enter the **Reserved Ingress MPS Abatement Time** in milliseconds, if a value other than the default value is needed.
9. Click:
   - **OK** to save the changes and return to the **Capacity Configuration Sets** page.
   - **Apply** to save the changes and remain on this page.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any field value is missing (not entered)
- The Capacity Configuration Set is not unique (already exists in the system)
- The maximum number of Capacity Configuration Sets (1000) is already configured
- The **Reserved Ingress MPS** value is greater than the **Maximum Ingress MPS** value
- The **Ingress MPS Minor Alarm Threshold** value is greater than the **Ingress MPS Major Alarm Threshold** value

Editing a Capacity Configuration Set

Use this task to edit an existing Capacity Configuration Set.

The changes take effect upon receipt of the next message. Ingress MPS alarms are re-evaluated for all Connections that use the modified Capacity Configuration Set when the changes are replicated to the MP servers.

All Connections that use a particular Capacity Configuration Set must be in the Disabled Admin State before the **Reserved Ingress MPS** value can be changed. See *Disabling Connections*. (The **Reserved Ingress MPS** field is the only field that requires the Connections to be "Disabled" before it can be changed.) See *Disabling Connections*.

The **Capacity Configuration Set** name cannot be changed.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Capacity Configuration Sets**.
   The **Diameter > Configuration > Configuration Sets > Capacity Configuration Sets** page appears.
2. Select the Capacity Configuration Set to be edited.
3. Click **Edit**.
   The **Capacity Configuration Sets [Edit]** page appears.

   The **Capacity Configuration Sets [Edit]** page will be populated with the current values for the selected Capacity Configuration Set.
4. Update the relevant fields.

   The fields are described in *Capacity Configuration Set elements*.
5. Click:

   - **OK** to save the changes and return to the **Capacity Configuration Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Capacity Configuration Sets** page without saving any changes.

   When **OK** or **Apply** is clicked, a popup window appears.

   - Click **OK** to confirm that you want to change the Capacity Configuration Set values.
   - Click **Cancel** to remain on the **Capacity Configuration Sets [Edit]** page with the changes displayed but not saved.

   If **Apply** is clicked on the **Capacity Configuration Sets [Edit]** page, **OK** is clicked on the confirmation popup window, and all changes are valid, a "Data Committed" message appears.

   If **OK** is clicked on the popup window and the **Reserved Ingress MPS** field was changed for a Capacity Configuration Set that is referenced by any Connection that is in the "Enabled" Admin state, an error message appears and the changes are not saved.

6. Enable any Connections that were Disabled before the Capacity Configuration Set was changed.
   See *Enabling Connections*.

Deleting a Capacity Configuration Set

Use this task to delete a Capacity Configuration Set.

A Capacity Configuration Set cannot be deleted if it is being used by any Connections. Before you perform this task, you must disable any Connections that use the Capacity Configuration Set and edit each Connection to no longer use the Capacity Configuration Set. (See *Disabling Connections* and *Editing a Connection*.)

The Default Capacity Configuration Set can be edited, but cannot be deleted.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Capacity Configuration Sets**.
   The **Capacity Configuration Sets** page appears.
2. Select the Capacity Configuration Set you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Capacity Configuration Set and return to the **Capacity Configuration Sets** page.
   - **Cancel** to cancel the delete function and return to the **Capacity Configuration Sets** page.

   If **OK** is clicked and the selected Capacity Configuration Set is referenced by at least one Connection, an error message appears and the Capacity Configuration Set is not deleted.

Egress Message Throttling Configuration Set configuration

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

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 you to control 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*. Each connection can reference a single Egress Message Throttling Configuration Set.

On the **Egress Message Throttling Configuration Sets** page, you can perform the following actions:

- Filter the list of Egress Message Throttling Configuration Sets to display only the desired Egress Message Throttling Configuration Sets.

- Sort the list by column contents in ascending or descending order, by clicking the column heading. The default order is by **Egress Message Throttling Configuration Set Name** in ascending ASCII order.
- Click the **Insert** button.

  The **Egress Message Throttling Configuration Sets [Insert]** page appears. You can add a new Egress Message Throttling Configuration Set and its options. See *Adding an Egress Message Throttling Configuration Set*.

  If the maximum number of Egress Message Throttling Configuration Sets per Network Element (50) already exist in the system, the **Egress Message Throttling Configuration Sets [Insert]** page will not open, and an error message is displayed.

- Select an Egress Message Throttling Configuration Set Name in the list, and click the **Edit** button.

  The **Egress Message Throttling Configuration Sets [Edit]** page opens. You can edit the selected Egress Message Throttling Configuration Set. See *Editing an Egress Message Throttling Configuration Set*.

  If at least one connection is in the "Enabled" Admin state that uses the Egress Message Throttling Configuration Set, the **Egress Message Throttling Configuration Sets [Edit]** page will not open.

- Select an Egress Message Throttling Configuration Set Name in the list, and click the **Delete** button to remove the selected Egress Message Throttling Configuration Set.

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 11: 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%

Field (* indicates required field)	Description	Data Input Notes
* 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
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 - 90% Default: 80%
* 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

Viewing Egress Message Throttling Configuration Sets

Use this task to view currently configured Egress Message Throttling Configuration Sets.

Select **Diameter** > **Configuration** > **Configuration Sets** > **Egress Message Throttling Configuration Sets**.
The **Egress Message Throttling Configuration Sets** page appears.

Adding an Egress Message Throttling Configuration Set

Use this task to create a new Egress Message Throttling Configuration Set. For more information about the fields, see *Egress Message Throttling Configuration Set elements*.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Egress Message Throttling Configuration Sets**.
   The **Egress Message Throttling Configuration Sets** page appears.
2. Click **Insert**.
   The **Egress Message Throttling Configuration Sets [Insert]** page appears.
3. Enter a unique name for the Configuration Set in the **Egress Message Throttling Configuration Set Name** field.
4. Enter the maximum Egress Message Rate in the **Maximum Allowed EMR** field.
5. Enter one to three Throttle Thresholds and Abatement Thresholds as a percentage of the maximum Egress Message Rate.
6. Optionally, enter a **Smoothing Factor** and an **Abatement Time**.
7. Click:
   - **OK** to save the data and return to the **Egress Message Throttling Configuration Sets** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Egress Message Throttling Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty (no value was entered)
   - The value in any field is not valid or is out of range
   - The **Egress Message Throttling Configuration Set Name** is not unique; it already exists in the system
   - Throttle thresholds and abatement thresholds do not follow the rule: TT3 > AT3 > TT2 > AT2 > TT1 > AT1
   - The maximum number of Egress Message Throttling Configuration Sets per Network Element (50) is already configured

Editing an Egress Message Throttling Configuration Set

Use this task to edit an existing Egress Message Throttling Configuration Set.

When the **Egress Message Throttling Configuration Sets** page opens, the fields are populated with the currently configured values.

The **Egress Message Throttling Configuration Set Name** cannot be edited.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Egress Message Throttling Configuration Sets**.
   The **Egress Message Throttling Configuration Sets** page appears.
2. Select the Egress Message Throttling Configuration Set you want to edit.
3. Click **Edit**.
   The **Egress Message Throttling Configuration Sets [Edit]** page appears.
4. Update the relevant fields.

   For information about each field, see *Egress Message Throttling Configuration Set elements*.
5. Click:
   - **OK** to save the data and return to the **Egress Message Throttling Configuration Sets** page.

- **Apply** to save the data and remain on this page.
- **Cancel** to return to the **Egress Message Throttling Configuration Sets** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The selected Egress Message Throttling Configuration Set no longer exists; it has been deleted by another user
- Any field is empty (no value was entered)
- The value in any field is not valid or is out of range
- Throttle thresholds and abatement thresholds do not follow the rule: TT3 > AT3 > TT2 > AT2 > TT1 > AT1

Deleting an Egress Message Throttling Configuration Set

Use this task to delete an Egress Message Throttling Configuration Set.

Note: An Egress Message Throttling Configuration Set cannot be deleted if it is being used by any connections. Before you perform this task, you must disable and edit any connections that use the Egress Message Throttling Configuration Set. (See *Disabling Connections* and *Editing a Connection*.)

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Egress Message Throttling Configuration Sets**.
   The **Egress Message Throttling Configuration Sets** page appears.
2. Select the Egress Message Throttling Configuration Set you want to delete.
3. Click **Delete.**
   A popup window appears to confirm the delete.
4. Click:

   - **OK** to delete the Egress Message Throttling Configuration Set.
   - **Cancel** to cancel the delete function and return to the **Egress Message Throttling Configuration Sets** page.

   If **OK** is clicked and the selected Egress Message Throttling Configuration Set is referenced by at least one connection, an error message appears and the Egress Message Throttling Configuration Set is not deleted.

   If **OK** is clicked and the selected Egress Message Throttling Configuration Set no longer exists (it was deleted by another user), an error message is displayed and the Egress Message Throttling Configuration Sets view is refreshed.

Message Priority Configuration Set configuration

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

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

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

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

On the **Message Priority Configuration Sets** page, you can perform the following actions:

- Filter the list of Message Priority Configuration Sets to display only the desired Message Priority Configuration Sets.
- Sort the list by column contents in ascending or descending order, by clicking the column heading. The default order is by **Message Priority Configuration Set Name** in ascending ASCII order.
- Click the **+** in the **Message Priority Rules** field to display the Message Priority Rules associated with a Message Priority Configuration Set.
- Click the **Insert** button.

  The **Message Priority Configuration Sets [Insert]** page appears. You can add a new Message Priority Configuration Set and its Message Priority Rules. See *Adding a Message Priority Configuration Set*.

  If the maximum number of Message Priority Configuration Sets per Network Element (20) already exist in the system, the **Message Priority Configuration Sets [Insert]** page will not open, and an error message is displayed.

- Select an Message Priority Configuration Set Name in the list, and click the **Edit** button.

  The **Message Priority Configuration Sets [Edit]** page opens. You can edit the selected Message Priority Configuration Set. See *Editing a Message Priority Configuration Set*.

  If at least one connection that uses the Message Priority Configuration Set is in the "Enabled" Admin state, the **Message Priority Configuration Sets [Edit]** page will not open.

- Select an Message Priority Configuration Set Name in the list, and click the **Delete** button to remove the selected Message Priority Configuration Set. You cannot delete the Default Message Priority Configuration Set.

Message Priority Configuration Set elements

Table 12: 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 12: 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

Field (* indicates a required field)	Description	Data Input Notes
		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.
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

Viewing Message Priority Configuration Sets

Use this task to view currently configured Message Priority Configuration Sets and their associated Message Priority Rules.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Message Priority Configuration Sets**.
   The **Message Priority Configuration Sets** page appears.
2. Click the **+** in any **Message Priority Rules** field.
   The Message Priority Rules associated with the Message Priority Configuration Set are displayed.

Adding a Message Priority Configuration Set

Use this task to create a new Message Priority Configuration Set. For more information about the fields, see *Message Priority Configuration Set elements*.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Message Priority Configuration Sets**.
   The **Message Priority Configuration Sets** page appears.
2. Click **Insert**.

The **Message Priority Configuration Sets [Insert]** page appears.

3. Enter a unique name for the Configuration Set in the **Message Priority Configuration Set Name** field.
4. Select an **Application Id**, **Command Code**, and **Message Priority** for the Message Priority Rule.
5. Click **Add** to add more Message Priority Rules to the Message Priority Configuration Set.

   You can add up to 50 rules per configuration set. Click the **X** beside the **Message Priority** field to clear the values for a Message Priority Rule.
6. Click:

   - **OK** to save the data and return to the **Message Priority Configuration Sets** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Message Priority Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any required field is empty (no value was entered)
   - The value in any field is not valid or is out of range
   - The **Message Priority Configuration Set Name** is not unique; it already exists in the system
   - A wildcard is used for **Application Id**, but a specific **Command Code** is specified.
   - The maximum number of Message Priority Configuration Sets per Network Element (20) is already configured

Editing a Message Priority Configuration Set

Use this task to edit an existing Message Priority Configuration Set.

When the **Message Priority Configuration Sets** page opens, the fields are populated with the currently configured values.

The **Message Priority Configuration Set Name** cannot be edited.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Message Priority Configuration Sets**.
   The **Message Priority Configuration Sets** page appears.
2. Select the Message Priority Configuration Set you want to edit.
3. Click **Edit**.
   The **Message Priority Configuration Sets [Edit]** page appears.
4. Update the relevant fields.

   For information about each field, see *Message Priority Configuration Set elements*.
5. Click:

   - **OK** to save the data and return to the **Message Priority Configuration Sets** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Message Priority Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The selected Message Priority Configuration Set no longer exists; it has been deleted by another user
   - Any field is empty (no value was entered)
   - The value in any field is not valid or is out of range

- A wildcard (*) is used for **Application Id**, but a specific **Command Code** is specified.

Deleting a Message Priority Configuration Set

Use this task to delete a Message Priority Configuration Set.

Note: The default Message Copy Configuration Set cannot be deleted.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Message Priority Configuration Sets**. The **Message Priority Configuration Sets** page appears.
2. Select the Message Priority Configuration Set you want to delete.
3. Click **Delete.**
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Message Priority Configuration Set.
   - **Cancel** to cancel the delete function and return to the **Message Priority Configuration Sets** page.

   If **OK** is clicked and the selected Message Priority Configuration Set is referenced by at least one connection, an error message appears and the Message Priority Configuration Set is not deleted.

   If **OK** is clicked and the selected Message Priority Configuration Set no longer exists (it was deleted by another user), an error message is displayed and the Message Priority Configuration Sets view is refreshed.

Message Copy Configuration Set configuration

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

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

On the **Message Copy Configuration Sets** page, you can perform the following actions:

- Filter the list of Message Copy Configuration Sets to display only the desired Message Copy Configuration Sets.
- Sort the list by column contents in ascending or descending order, by clicking the column heading. The default order is by **Message Copy Configuration Set Name** in ascending ASCII order.
- Click the **Insert** button.

  The **Message Copy Configuration Sets [Insert]** page appears. You can add a new Message Copy Configuration Set. See *Adding a Message Copy Configuration Set*.

  If the maximum number of Message Copy Configuration Sets (100) already exists in the system, an error message is displayed.

- Select a Message Copy Configuration Set Name in the list, and click the **Edit** button.

The **Message Copy Configuration Sets [Edit]** page opens. You can edit the selected Message Copy Configuration Set. See *Editing a Message Copy Configuration Set*.

If no row is selected, or if more than one row is selected, the **Edit** button is disabled.

- Select a Message Copy Configuration Set Name in the list, and click the **Delete** button to remove the selected Message Copy Configuration Set.

  The Default Message Copy Configuration Set can be edited, but cannot be deleted. See *Deleting a Message Copy Configuration Set*.

Message Copy Configuration Set elements

Table 12: Message Priority Configuration Set Elements describes the fields on the Message Copy 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 13: Message Copy Configuration Set Elements

Field (* indicates a required field)	Description	Data Input Notes
* Message Copy Configuration Set Name	Unique name of the Message Copy Configuration Set.	Format: text box Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
* Route List for DAS Node	Route List to be used for copying a message to a DAS node.	Format: pulldown list Range: configured Route Lists. Default: "-Select-".
Message Copy Request Type	Type of Request to be copied to the DAS.	Format: radio buttons Range: Original Ingress Request, Original Egress Request Default: Original Ingress Request
Ingress Answer Included	Indicates whether the Ingress Answer received for the Diameter Message needs to be included in the copied message.	Format: radio buttons Range: Yes, No Default: No
Original Answer Result Code For Message Copy	Result Code/Experimental Result code that should match with incoming Answer Result	Format: radio buttons Range:

Field (* indicates a required field)	Description	Data Input Notes
	Code (whose Request has been marked for Message Copy), to allow copying a Request to DAS.	• 2xxx result-code/ experimental-result-code • Any result/ experimental-result-code Default: 2xxx result-code/ experimental-result-code
DAS Answer Result Code	Result Code/Experimental Result Code that should match with DAS Message Copy Answer Result Code, to terminate the Message Copy to DAS.	Format: radio buttons Range: • 2xxx result-code/ experimental-result-code • Any result/ experimental-result-code Default: 2xxx result-code/ experimental-result-code
* Max DAS Retransmission Attempts	Max Retransmission Attempts for DAS-Request A value of 0 indicates that there will not be any re-transmissions after the first copy attempt.	Format: text box; numeric Range: 0-4 Default: 0

Viewing Message Copy Configuration Sets

Use this task to view currently configured Message Copy Configuration Sets.

Select **Diameter** > **Configuration** > **Configuration Sets** > **Message Copy Configuration Sets**. The **Message Copy Configuration Sets** page appears.

Adding a Message Copy Configuration Set

Use this task to create a new Message Copy Configuration Set.

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

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Message Copy Configuration Sets**. The **Message Copy Configuration Sets** page appears.
2. Click **Insert**.

   The **Message Copy Configuration Sets [Insert]** page appears.

   If the maximum numbers of Message Copy Configuration Sets (100) allowed in the system are already configured, the **Message Copy Configuration Sets [Insert]** page will not open.
3. Enter a unique name for the Configuration Set in the **Message Copy Configuration Set Name** field.

4. Select or enter the element values.
5. Click:
   - **OK** to save the new Configuration Set and return to the **Message Copy Configuration Sets** page.
   - **Apply** to save the new Configuration Set and remain on this page.
   - **Cancel** to return to the **Message Copy Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty (no value was entered).
   - The value in any field is not valid or is out of range.
   - The **Message Copy Configuration Set Name** is not unique; it already exists in the system.

Editing a Message Copy Configuration Set

Use this task to edit an existing Message Copy Configuration Set.

When the **Message Copy Configuration Sets** page opens, the fields are populated with the currently configured values.

The **Message Copy Configuration Set Name** cannot be edited.

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

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Message Copy Configuration Sets**.
   The **Message Copy Configuration Sets** page appears.
2. Select the Message Copy Configuration Set you want to edit.
3. Click **Edit**.
   The **Message Copy Configuration Sets [Edit]** page appears.
4. Update the relevant fields.
5. Click:
   - **OK** to save the changes and return to the **Message Copy Configuration Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Message Copy Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - The selected Message Copy Configuration Set no longer exists; it has been deleted by another user.
   - Any field is empty (no value was entered) .
   - The value in any field is not valid or is out of range.

Deleting a Message Copy Configuration Set

Use this task to delete a Message Copy Configuration Set.

The Default Message Copy Configuration Set can be edited, but cannot be deleted.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Message Copy Configuration Sets**.
   The **Message Copy Configuration Sets** page appears.

2. Select the Message Copy Configuration Set you want to delete.
3. Click **Delete.**
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Message Copy Configuration Set.
   - **Cancel** to cancel the delete function and return to the **Message Copy Configuration Sets** page.

   If **OK** is clicked and the selected Message Copy Configuration Set is referenced by any other Diameter component or any DSR Application, an error message appears and the Message Copy Configuration Set is not deleted.

Local Node configuration

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.

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

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

On the **Diameter > Configuration > Local Nodes** page, you can perform the following actions:

- Filter the list of Local Nodes to display only the desired Local Nodes.
- Sort the list by a column in ascending or descending order, by clicking the column heading (except IP Addresses). The default order is by **Local Node Name** in ascending ASCII order.
- Click a field entry that is shown in blue for a Local Node. The blue entries are links to the configuration pages for those types of items.

  The **Diameter > Configuration > {Item Type} (Filtered)** page appears for the selected item.

- Click **Insert**.

  The **Diameter > Configuration > Local Nodes [Insert]** page appears. You can add a new Local Node.

  The **Diameter > Configuration > Local Nodes [Insert]** page will not open if any of the following conditions exist:

  - The maximum number of Local Nodes (32) has already been configured.
  - There is no Signaling VIP Address available in the signaling Network Element (NE) that can be added to the Local Node.

- Select a Local Node in the list, and click **Edit**.

  The **Diameter > Configuration > Local Nodes [Edit]** page appears. You can edit the selected Local Node.

- Select a Local Node in the list, and click **Delete**. You can delete the selected Local Node.

Local Node configuration elements

Table 14: 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 14: 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.

Field (* indicates required field)	Description	Data Input Notes
		Range: FQDN - up to 255 characters; label - up to 63 characters
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 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 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. On the Local Nodes GUI pages, each IP address has appended to it:	Format: 128 pulldown lists Range: • For a DSR that has Active/Standby DA-MPs: available Virtual Signaling IP Addresses , including any configured IPFE primary and secondary TSAs VIP

Field (* indicates required field)	Description	Data Input Notes
	• For VIP addresses, the string "VIP" VIPs are present only in 1+1 Active/Standby configurations • For static IP addresses, the MP Server Hostname of the DA-MP that owns the IP address Static IP addresses are present only in Multi-Active N+0 configurations • For TSAs, the name of the Target Set to which the IP address corresponds, followed by -p or -s (for example, TSA#-p for primary and TSA#-s for secondary IP Addresses where "#" is the Target Set number TSAs can be present in either, but do not have to be present at all.	• For a DSR that has Multiple-Active DA-MPs: static IP addresses configured for each DA-MP, including any configured IPFE primary and secondary TSAs • configured IPFE primary and secondary TSAs

Viewing Local Nodes

Use this task to view currently configured Local Nodes.

Select **Diameter** > **Configuration** > **Local Nodes**.
The **Diameter > Configuration > Local Nodes** page appears.

Adding a Local Node

Use this task to create a new Local Node.

1. Select **Diameter** > **Configuration** > **Local Nodes**.
   The **Diameter > Configuration > Local Nodes** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Local Nodes [Insert]** page appears.
3. Enter a unique name for the Local Node in the **Local Node Name** field.
4. Enter the **Realm** for the Local Node in the field.
5. Enter an **FQDN** in the field.
6. If you want the Local Node to listen for SCTP connections, check the **SCTP Enabled** check box.
7. If **SCTP Enabled** is checked, enter an **SCTP Listen Port** number in the field.
   This is the port that will be used by connections that use this Local Node to listen for SCTP request messages. The default 3868 is the well-known IANA port for Diameter traffic.
8. If you want the Local Node to listen for TCP connections, check the **TCP Enabled** check box.
9. If **TCP Enabled** is checked, enter a **TCP Listen Port** number in the field.

This is the port that will be used by connections that use this Local Node to listen for TCP request messages. The default 3868 is the well-known IANA port for Diameter traffic.

10. Select a **Connection Configuration Set** from the pulldown list. If you have not added additional Connection Configuration Sets, only the **Default** Connection Configuration Set will be available.
11. Select a **CEX Configuration Set** for the Local Node from the pulldown list.

    If you have not added additional CEX Configuration Sets, only the **Default** CEX Configuration Set will be available.
12. Select from 1 to 128 IP addresses from the **IP Addresses** pulldown lists.
13. Click:

    - **OK** to save the new Local Node and return to the **Diameter > Configuration > Local Nodes** page.
    - **Apply** to save the new Local Node and remain on this page.
    - **Cancel** to return to the **Diameter > Configuration > Local Nodes** page without saving any changes.

    If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

    - The maximum number of Local Nodes (32) per Network Element is already defined in the system
    - Any required field is empty; no value was entered or selected
    - The entry in any field is not valid (wrong data type or out of the valid range)
    - The selected pulldown list entry no longer exists (has been deleted by another user)
    - The **Local Node Name** is not unique; it already exists in the system
    - The **FQDN** is already assigned to a different Local or Peer Node
    - Neither the **SCTP Enabled** check box nor the **TCP Enabled** check box is checked; one must be checked
    - The **SCTP Listen Port** and **IP Address** combination is already assigned to a different Local or Peer Node
    - The **TCP Listen Port** and **IP Address** combination is already assigned to a different Local or Peer Node
    - The **SCTP Listen Port** or the **TCP Listen Port** is already used as a **Local Initiate Port** of a Connection
    - Any of the selected **IP Addresses** is duplicated

Editing a Local Node

Use this task to edit a Local Node.

When the **Diameter > Configuration > Local Nodes [Edit]** page opens, the fields are initially populated with the current values for the selected Local Node.

Configuration considerations:

- The **Local Node Name** cannot be changed.
- The following fields cannot be edited if there is at least one associated Enabled connection:
  - **Realm**
  - **FQDN**
  - **SCTP Listen Port** (and the **Transport Protocol** is **SCTP**)

- **TCP Listen Port** (and the **Transport Protocol** is **TCP**)
- **IP Address** (cannot be removed if there is an Enabled connection, but a new **IP Address** can be added)
- **Connection Configuration Set**
- **CEX Configuration Set**

1. Select **Diameter** > **Configuration** > **Local Nodes**.
   The **Diameter > Configuration > Local Nodes** page appears.
2. Select the Local Node you want to edit, then click **Edit**.
   The **Diameter > Configuration > Local Nodes [Edit]** page appears.
3. Update the relevant fields.

   For more information about each field, see *Local Node configuration elements*.

   The value for an entry in a pulldown list can be removed by selecting "--Select—" in the list, or selecting the X at the end of the list box (if an X is available).

4. Click:

   - **OK** to save the data and return to the **Diameter > Configuration > Local Nodes** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Local Nodes** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The selected Local Node no longer exists; it has been deleted by another user
   - The selected IP Address or Connection Configuration Set has been deleted by another user
   - Any required field is empty; no value was entered or selected
   - The entry in any field is not valid (wrong data type or out of the valid range)
   - The selected pulldown list entry no longer exists (has been deleted by another user)
   - The edited **FQDN** is already assigned to a different Local or Peer Node
   - Neither the **SCTP Enabled** check box nor the **TCP Enable** check box is checked; at least one of them must be checked
   - **SCTP Enabled** was changed to be disabled (unchecked) and there is at least one associated SCTP connection.
   - **TCP Enabled** was changed to be disabled (unchecked) and there is at least one associated TCP connection.
   - The edited **IP Address** and **SCTP Listen Port** combination is already assigned to a different Local Node or Peer Node
   - The edited **IP Address** and **TCP Listen Port** combination is already assigned to a different Local Node or Peer Node
   - The selected **SCTP Listen Port** or **TCP Listen Port** is already used as a **Local Initiate Port** of a connection

Deleting a Local Node

Use this task to delete a Local Node.

Note: A Local Node cannot be deleted if it is being used by any connections. Before you perform this task, disable and delete any connections that use the Local Node.

1. Select **Diameter** > **Configuration** > **Local Nodes**.
   The **Diameter > Configuration > Local Nodes** page appears.
2. Select the Local Node you want to delete.
3. Click **Delete.**

   A pop up window appears to confirm the delete.
4. Click:
   - **OK** to delete the Local Node.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Local Nodes** page.

   If **OK** is clicked and the selected Local Node no longer exists (it was deleted by another user), an error message is displayed and the Local Nodes view is refreshed.

Peer Node configuration

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

After it is configured, a Peer Node can be:

- Assigned to connections for use in Diameter routing
- Assigned to Route Groups that manage the distribution of traffic to and among Peer Nodes

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

- Filter the list of Peer Nodes, to display only the desired Peer Nodes.
- Sort the list by a column in ascending or descending order, by clicking the column heading (except **IP Addresses**). The default order is by **Peer Node Name** in ascending ASCII order.
- Click an entry that is shown in blue in a column, to open the **Diameter > Configuration > <component> [Filtered]** page and display that entry only.
- Click **Insert**.

  The **Diameter > Configuration > Peer Nodes [Insert]** page appears. You can add a new Peer Node.

  The **Diameter > Configuration > Peer Nodes [Insert]** will not open if the maximum number of Peer Nodes per Network Element (6000) already exists in the system.
- Select a Peer Node in the list, and click **Edit**.

  The **Diameter > Configuration > Peer Notes [Edit]** page appears. You can edit the selected Peer Node.
- Select a Peer Node in the list, and click **Delete**. You can delete the selected Peer Node.

Peer Node configuration elements

Table 15: 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 15: 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 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

Field (* indicates required field)	Description	Data Input Notes
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 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
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 Default: "-Select-"
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
Topology Hiding Status	If Enabled, Diameter Topology Hiding will be applicable to this Peer Node.	Format: pulldown list Range = Disabled, Enabled

Field (* indicates required field)	Description	Data Input Notes
		Default = Disabled
* 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
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 > Message Copy Configuration Set > Original Answer Result Code for Message Copy** parameter.	Format: radio buttons Range: Same Peer, Different Peer Default: Different Peer
Application Route Table	The Application Route Table associated with this Peer Node. If Application Route Table is set to is **Not Selected**, the downstream Application Ids associated Application Route Table will be used when processing transactions if it is defined.	Format: pulldown list Range: Default, configured Application Route Tables Default: Not Selected
Peer Route Table	The Peer Route Table associated with the Peer Node. The Peer Route Table contains Peer	Format: pulldown list

Field (* indicates required field)	Description	Data Input Notes
	Routing Rules used to route messages from the Peer Node. If Peer Route Table is set to **Not Selected**, the Peer Route Table configured for the Application Id contained in the message is used.	Range: Default, configured Peer Route Tables Default: Not Selected
Ingress Routing Option Set	The Routing Option Set associated with the Peer Node. Routing Option Sets contain information used to handle delivery error conditions. If Ingress Routing Option Set is set to **Not Selected**, the downstream Application Id's associated Routing Option Set will be used when processing transactions if it is defined.	Format: pulldown list Range: Default, configured Routing Option Sets Default: Not Selected
Egress Pending Answer Timer	The Pending Answer Timer associated with the egress Peer Node. If Egress Pending Answer Timer is set to **Not Selected**, the downstream Application Id's associated Pending Answer Timer will be used when processing transactions if it is defined.	Format: pulldown list Range: Default, configured Pending Answer Timers Default: Not Selected
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 User Configured is selected for the Message Priority Setting	Format: pulldown list Range: Default, configured Message Priority Configuration Sets Default: "-Select-"

Viewing Peer Nodes

Use this task to view currently configured Peer Nodes.

Select **Diameter** > **Configuration** > **Peer Nodes**.
The **Diameter > Configuration > Peer Nodes** page appears.

Adding a Peer Node

Use this task to create a new Peer Node.

1. Select **Diameter** > **Configuration** > **Peer Nodes**.
   The **Diameter > Configuration > Peer Nodes** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Peer Nodes [Insert]** page appears.
3. Enter a unique name for the Peer Node in the **Peer Node Name** field.
4. Enter the Realm in the **Realm** field.
5. Enter a Fully Qualified Domain Name in the **FQDN** field.
6. If you want the Peer Node to support SCTP, click the **SCTP Enabled** check box (a check mark appears in the box).
7. If **SCTP Enabled** is checked, enter a port number in the **SCTP Listen Port** field.
8. If you want the Peer Node to support TCP, check the **TCP Enabled** box.
9. If **TCP Enabled** is checked, enter a port number in the **TCP Listen Port** field.
10. Enter IP addresses in the **IP Addresses** fields.

    An IP address is optional if a Primary DNS Server IP Address is configured. See *DNS Options configuration*.

    To add the first IP Address, enter the IP address in the text box.

    To add another IP Address, click the **Add** button and enter the IP Address in the new text box. See *Table 15: Peer Node Configuration Elements* for limitations on the number of IP addresses you can add.

11. Select a Route List from the **Alternate Implicit Route** pulldown list

    This field is optional. This Route List will be used for routing if the Connection to the Peer is down and a message does not match any of the configured *Peer Routing Rules*.

12. To overwrite the Destination Realm of outgoing messages to the peer with the Peer Realm, click the **Replace Dest Realm** check box (a check mark appears in the box).
13. To overwrite the Destination Host of outgoing messages to the peer with the Peer Node's FQDN, click the **Replace Dest Host** check box (a check mark appears in the box).
14. In the **Minimum Connection Capacity** text box, enter the minimum number of Connections that must be "Available" for the Peer to be "Available".
15. In the **Maximum Alternate Routing Attempts** text box, enter the maximum number of times that a Request can be rerouted to this Peer.
16. Select the **Alternate Routing on Connection Failure** radio button to indicate whether or not to perform alternate routing to the same or a different Peer when a Connection failure occurs.

17. Select the **Alternate Routing on Answer Timeout** radio button to indicate whether or not to perform alternate routing to the same or a different Peer, or the same Connection, when an Answer Timeout occurs.
18. Select the **Alternate Routing on Answer Result Code** radio button to indicate whether or not to perform alternate routing to the same or a different Peer when a Reroute on Answer Result Code occurs.
19. Select a **Message Priority Setting** to indicate the source of message priority for request messages arriving on Connections associated with the Peer Node.
20. If Message Priority Setting is set to **User Configured**, specify the **Message Priority Configuration Set** that is used to determine message priority.
21. Select the **Application Route Table** to specify which Application Routing Rules are used when routing messages from the Peer Node.

    If Application Route Table is set to **Not Selected**, the Application Route Table configured for the Application Id contained in the message is used.
22. Select the **Peer Route Table** to specify which Peer Routing Rules are used when routing messages from the Peer Node.

    If Peer Route Table is set to **Not Selected**, the Peer Route Table configured for the Application Id contained in the message is used.
23. Select the **Routing Option Set** to specify which options are used when certain routing failures occur.

    If Routing Option Set is set to **Not Selected**, the Routing Option Set configured for the Application Id contained in the message is used.
24. Select the **Pending Answer Timer** to specify how long DSR waits for a response from the Peer Node.

    If Pending Answer Timer is set to **Not Selected**, the Pending Answer Timer configured for the Application Id contained in the message is used.

    - **OK** to save the changes and return to the **Diameter > Configuration > Peer Nodes** page.
    - **Apply** to save the changes and remain on this page.
    - **Cancel** to return to the **Diameter > Configuration > Peer Nodes** page without saving any changes.

    If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

    - The maximum number of Peer Nodes per Network Element (6000) is already defined in the system
    - Any required field is empty; no value was entered or selected
    - The entry in any field is not valid (wrong data type or out of the valid range)
    - The selected **Alternate Implicit Route** (Route List) no longer exists; it was deleted by another user during this Insert session
    - The **Peer Node Name** is not unique; it already exists in the system
    - The **FQDN** is already assigned to a different Local or Peer Node
    - Neither the **SCTP Enabled** check box nor the **TCP Enabled** check box is checked; at least one must be checked
    - The **SCTP Listen Port** and **IP Addresses** combination is already assigned to a different Local or Peer Node
    - The **TCP Listen Port** and **IP Addresses** combination is already assigned to a different Local or Peer Node

- The **SCTP Listen Port** or the **TCP Listen Port** is already used as a **Local Initiate Port** of a Connection
- Any of the selected **IP Addresses** is duplicated

Editing a Peer Node

Use this task to edit a Peer Node.

When the **Diameter > Configuration > Peer Nodes [Edit]** page opens, the fields are initially populated with the current values for the selected Peer Node.

Configuration considerations:

- The **Peer Node Name** cannot be changed
- **SCTP Enabled** cannot be disabled (unchecked) if there is at least one associated SCTP connection.
- **TCP Enabled** cannot be disabled (unchecked) if there is at least one associated TCP connection.
- You cannot remove an **IP Addresses** entry that is in use by at least one connection. A new IP Address can be added.
- The following fields cannot be edited if there is at least one Enabled connection:
  - **Realm**
  - **Fully Qualified Domain Name**
  - **SCTP Listen Port**
  - **TCP Listen Port**

1. Select **Diameter** > **Configuration** > **Peer Nodes**.
   The **Diameter > Configuration > Peer Nodes** page appears.
2. Select the Peer Node you want to edit, then click **Edit**.

   The **Diameter > Configuration > Peer Nodes [Edit]** page appears.
3. Update the relevant fields.

   For more information about each field please see *Peer Node configuration elements*.

   An entry in a pulldown list can be removed by selecting "--Select—" in the list, or selecting the X at the end of the list box (if an X is available).

   An IP Address can be removed by deleting the information in the text box or by clicking the X at the end of the text box.
4. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Peer Nodes** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Peer Nodes** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - The selected Peer Node no longer exists; it has been deleted by another user
   - The selected **IP Addresses** entry has been deleted by another user
   - Any required field is empty; no value was entered or selected
   - The entry in any field is not valid (wrong data type or out of the valid range)

- The selected pulldown list entry no longer exists (has been deleted by another user)
- The edited **FQDN** is already assigned to a different Local or Peer Node in the system
- Neither the **SCTP Enabled** check box nor the **TCP Enabled** check box is checked; at least one of them must be checked
- The edited **IP Addresses** entry and **SCTP Listen Port** combination is already assigned to a different Local Node or Peer Node
- The edited **IP Addresses** entry and **TCP Listen Port** combination is already assigned to a different Local Node or Peer Node
- The selected **SCTP Listen Port** or **TCP Listen Port** is already used as a **Local Initiate Port** of a connection

Deleting a Peer Node

Use this task to delete a Peer Node.

A Peer Node cannot be deleted if it is referenced by any of the following Diameter Configuration Components:

- Route Groups
- Connections
- Egress Throttle Groups

Before you perform this task, remove the Peer Node from any Route Groups or Egress Throttle Groups, and disable and delete any transport Connections that use the Peer Node.

1. Select **Diameter** > **Configuration** > **Peer Nodes**
   The **Diameter > Configuration > Peer Nodes** page appears.
2. Select the Peer Node you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Peer Node.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Peer Nodes** page.

   If **OK** is clicked and the selected Peer Node no longer exists (it was deleted by another user), an error message is displayed and the Peer Nodes view is refreshed.

Connection configuration

A connection provides the reliable transport connectivity between Diameter nodes. A connection:

- Can use the SCTP or TCP transport protocol
- Can be configured to initiate or respond to a connection to the Peer Diameter 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.

On the **Diameter > Configuration > Connections** 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.
- Click a field that is shown in blue for a Connection. The blue fields are links to the configuration pages for those types of items.

  The **Diameter > Configuration > {Item Type} (Filtered)** page appears for the selected type of item.

- Click **Insert**.

  The **Diameter >Configuration > Connections [Insert]** page appears. You can add a new Connection.

  The **Diameter > Configuration > Connections [Insert]** will not open if any of the following conditions exist:

  - There is no Local Node in the signaling Network Element (NE) to which the Connection can be assigned.
  - There is no Peer Node in the signaling Network Element (NE) to which the Connection can be assigned.

- Select a "Disabled" Connection, and click **Edit**.

  The **Diameter > Configuration > Connections [Edit]** page appears. You can change the configuration of the selected Connection.

  If the selected Connection is not in the "Disabled" Admin State, the **Diameter > Configuration > Connections [Edit]** page will not open.

  Note: For information on disabling a Connection, see *Disabling Connections*.

- Select a "Disabled" Connection, and click **Delete** to delete the Connection.

Connection Capacity Validation

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

The Connection Capacity Validation function is described in *Connection Capacity Validation*.

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

- Adding a new Connection
- Editing or replacing an existing Connection's assigned Capacity Configuration Set (where Reserved Ingress MPS value is specified)
- Removing a DA-MP from its parent Server Group
- Removing a DA-MP from an IPFE Target Set or adding a DA-MP to an IPFE Target Set
- Moving a Fixed Connection to a new DA-MP
- Moving an IPFE Connection to a new Target Set

- Converting a Fixed Connection to an IPFE Connection, or vice versa
- Assigning a different MP Profile to a configured DA-MP

An error is displayed, stating the reason, when the validation determines that performing the configuration action would cause over-configuration of Connections or Reserved Ingress MPS in a DA-MP or Target Set, or that a configuration action cannot be performed for another reason such as no MP Profile assigned to the subject DA-MP.

A warning is displayed when the validation cannot determine whether the configuration action would cause over-configuration of Connections or Reserved Ingress MPS in a DA-MP or Target Set.

If an error and a warning could apply, the error is displayed.

The Diameter > Configuration > Connection Capacity Dashboard page displays the current Connection Count and Reserved Ingress MPS data per DA-MP. The page functions and contents are described in *Connection Capacity Dashboard Page*.

Connection configuration elements

Table 16: 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 16: 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. For Floating (IPFE) Connections, the Transport Protocol selected for this Connection must be included in the **Supported Protocols** for the IPFE Target Set. • TCP Connections are not allowed when the Target Set is configured to be SCTP_ONLY • SCTP Connections are not allowed when the target set is configured to be TCP_ONLY	Format: radio buttons Range: SCTP, TCP Default: SCTP

Field (* indicates required field)	Description	Data Input Notes
	• When the Target Set is configured to be TCP_AND_SCTP, then both TCP and SCTP Connections are allowed.	
* Local Node	Local Node associated with the Connection. 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 uni-homed and multi-homed SCTP Connections.	Format: pulldown list Range: all configured Local Nodes Default: "--Select--"
* 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 UNI-HOMED 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	Format: pulldown list Range: Initiator Only, Responder Only, Initiator & Responder Default: Initiator & Responder

Field (* indicates required field)	Description	Data Input Notes
	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. • 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 MULTI-HOMED 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	

Field (* indicates required field)	Description	Data Input Notes
	specified in any Connections to the Peer, then the following combination must be unique for each Connection the Peer: Transport FQDN, 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.	View-only
* Primary Local IP Address	The IP address to be used as Primary Local Node Address for this Connection. A Local Node must be selected before the pulldown list becomes available, containing the IP Addresses corresponding to the selected Local Node. When configuring TCP Connections, only MP static IP addresses, Primary TSAs and Secondary TSAs can be selected as the Primary Local IP Address. If an IPFE Secondary Target Set Address (selected from the Local Node's IP Address list) is assigned to the Primary Local IP Address of a Diameter Connection, then the Secondary Local IP Address selection is disabled. In this case, a Uni-homed Connection is configured, but using the Target	Format: pulldown list Range: all configured IP addresses for the selected Local Node Default: "--Select--"

Field (* indicates required field)	Description	Data Input Notes
	Set's Secondary IP address as the only Local IP Address for the 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). • For each IPFE Connection listed on the View screen, the Primary Local IP Address field displays "(TSA#-p)" or "(TSA#-s)" after the IP address, where "#" is the Target Set number, -p is a Primary TSA, and -s is a Secondary TSA.	
Secondary Local IP Address	The IP address to be used as the Secondary Local Node Address for this Connection. A Local Node must be selected and the selected Connection Transport Protocol must be SCTP before the list becomes available, containing the IP Addresses of the selected Local Node. If an IPFE Primary Target Set Address (selected from the Local Node's IP Address list) is assigned to the Primary Local IP Address of a Diameter Connection, then the only valid selection for the Secondary Local IP Address is the corresponding IPFE Secondary Target Set Address (for example- if TSA1-p is assigned to Primary Local IP Address of a DSR Connection, then the only valid selection for the Secondary Local IP Address will be TSA1-s.) This address is used only for SCTP Multi-homing; it must be different from the selected Primary Local IP Address. An IPFE Primary TSA and a Secondary TSA cannot be identical. 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).	Format: pulldown list Range: all configured IP addresses for the selected Local Node **Note:** Primary TSAs, labeled TSA#-p, are not valid for selection. Default: "--Select--"

Field (* indicates required field)	Description	Data Input Notes
	• For each IPFE Connection listed on the View screen, the Primary Local IP Address field displays "(TSA#-p)" or "(TSA#-s)" after the IP address, where "#" is the Target Set number. • For each IPFE SCTP Multi-Homed Connection listed on the View screen, the Secondary Local IP Address field displays "(TSA#-s)" after the IP address, where "#" is the Target Set number. and -s is Secondary TSA.	
* 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 Default: "--Select--"
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 accepted 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 IP Address to be used as the Primary Peer Node address for this Connection. A Peer Node must be selected before the pulldown list becomes available, containing the IP Addresses of the selected Peer Node.	Format: pulldown list Range: available IP addresses Default: "--Select--"

Field (* indicates required field)	Description	Data Input Notes
Secondary Peer IP Address	The IP Address to be used as the Secondary Peer Node address for this Connection. A Peer Node must be selected and the selected Connection Transport Protocol must be SCTP before the pulldown list becomes available, containing the IP Addresses of the selected Peer Node. This address is used only for SCTP Multi-homing; it must be different from the selected Primary Peer IP Address.	Format: pulldown list Range: available IP addresses Default: "--Select--"
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. Default: "--Select--"
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. Default: "--Select--"
* Capacity Configuration Set	Capacity Configuration Set associated with the Connection. The Capacity Configuration Set	Format: pulldown list

Field (* indicates required field)	Description	Data Input Notes
	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 (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 **Diameter > Configuration > DA-MPs > MP Profiles** page for the engineered capacity of the MP Server.)	Range: all configured Capacity Configuration Sets, "Default" Capacity Configuration Set 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 ("---" appears in the Message Priority Configuration Set column) • User Configured - Apply the user-configured Message Priority Configuration Set selected for the Connection	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: all configured 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: all configured Egress Message Throttling Configuration Sets Default: None ("---" is displayed in the column)
Test Mode	If checked, the Connection is in Test Mode.	Format: check box Range: checked (YES), not checked (NO) Default: not checked

Viewing Connections

Use this task to view currently configured connections.

Select **Diameter** > **Configuration** > **Connections**.
The **Diameter > Configuration > Connections** page appears.

Adding a Connection

Use this task to create a new Connection. The fields and configuration considerations are described in *Connection configuration elements*.

1. Select **Diameter** > **Configuration** > **Connections**.

   The **Diameter > Configuration > Connections** page appears.

2. Click **Insert**.

   The **Diameter > Configuration > Connections [Insert]** page appears.

   The **Diameter > Configuration > Connections [Insert]** will not open if any of the following conditions exist:

   - There is no Local Node in the signaling Network Element (NE) to which the Connection can be assigned.
   - There is no Peer Node in the signaling Network Element (NE) to which the Connection can be assigned.

3. Enter a unique name for the Connection in the **Connection Name** field.
4. Select the radio button for either SCTP or TCP in the **Transport Protocol** field.

   The Transport Protocol that you select for your Connection must match the protocol supported by both the Local Node and the Peer Node for the Connection.

5. Select a **Local Node** for the Connection from the pulldown list.

   The Local Node must use the same IP protocol as the Peer Node you select. If you do not see the Local Node you want to use, you might need to create a new Local Node. See *Adding a Local Node*.

6. Select the **Connection Mode** for this Connection from the pulldown list.
7. If you set up the Connection Mode for the Connection to initiate Connections, you can optionally enter a **Local Initiate Port** number in the field.
8. Select the **Primary Local IP Address** of this Connection from the pulldown list.
9. If the Transport Protocol is set to SCTP, select the **Secondary Local IP Address** of this Connection from the pulldown list.
10. Select a **Peer Node** for the Connection from the pulldown list.

    The Peer Node must use the same Transport Protocol as the Local Node that you selected. If you do not see the Peer Node you want to use, you might need to create a new Peer Node. See *Adding a Peer Node*

11. Select the radio button for the type of **Peer Node Identification** to be used for this Connection.
12. If needed, select the Primary Peer IP Address of this Connection from the **Primary Peer IP Address** pulldown list.
13. If needed, select the Secondary Peer IP Address of this Connection from the **Secondary Peer IP Address** pulldown list.
14. If needed, enter a **Transport FQDN** for this Connection.
15. Select a **Connection Configuration Set** for this Connection from the pulldown list.
16. If one is needed, select a **CEX Configuration Set** for this Connection from the pulldown list .
17. If the Per Connection Ingress MPS Control feature is active in the system, select a **Capacity Configuration Set** for the Connection from the pulldown list.

18. Specify the **Transport Congestion Abatement Timeout**.
19. Select a **Remote Busy Usage** setting from the pulldown menu.
20. If you selected Enabled or Host Override for Remote Busy Usage, set the **Remote Busy Abatement Timeout** value.
21. Identify the source of Message Priorities for incoming requests by selecting a **Message Priority Setting**.
22. If you selected **User Configured** as the Message Priority Setting, select a **Message Priority Configuration Set** from the pulldown menu.
23. If you want this Connection to be a test Connection, click the **Test Mode** check box (the box is checked).
24. Click:

    - **OK** to save the data and return to the **Diameter > Configuration > Connections** page.
    - **Apply** to save the data and remain on this page.
    - **Cancel** to return to the **Diameter > Configuration > Connections** page without saving any changes.

    If **OK** or **Apply** is clicked, and a Connection Capacity Validation issue (see *Connection Capacity Validation*) or any of the following conditions exists, an error message or warning message appears:

    - The maximum number of Connections per Network Element already exists in the system. The maximum number is the lesser of:
      - 12,000
      - The sum of the Maximum Connections allowed for all DA-MPs. See *MP Profiles*.
    - The maximum number of Connections per Peer Node (64) already exists in the system
    - Any required field is empty; no value was entered or selected
    - The entry in any field is not valid (wrong data type or out of the valid range)
    - The **Connection Name** is not unique; it already exists in the system
    - A selected pulldown list entry no longer exists (has been deleted by another user)
    - The selected **Transport Protocol** is not supported by the selected Local Node or Peer Node
    - The **Connection Mode** is set to **Initiator Only** or **Initiator & Responder**, a Peer IP Address is not selected, and a *Primary DNS Server IP Address* is not configured
    - The **Connection Mode** is set to **Initiator Only** or **Initiator & Responder**, and the selected **Local IP Address** (or pair for Multi-homing), **Local Initiate Port**, and **Transport Protocol** combination is the same as the **Local IP Address** (or pair for Multi-homing), **Listen Port**, and **Transport Protocol** combination of one of the Local Nodes
    - The **Connection Mode** is set to **Initiator Only** or **Initiator & Responder**, and the selected **Local IP Address** (or pair for Multi-homing), **Local Initiate port**, and **Transport Protocol** combination is the same as the **Local IP Address** (or pair for Multi-homing) and **Local Initiate** port combination of another Connection
    - For Uni-homed and Multi-homed Connections with various **Connection Mode** and **Peer Node Identification** combinations, the element combinations that must be unique are not unique (see the **Connection Mode** element description in *Connection configuration elements*)
    - The selected Primary and Secondary Local IP Addresses and the selected Primary and Secondary Peer IP Addresses are not all of same type (IPv4 or IPv6)
    - The **Peer Node Identification** is set to **IP Address** and no IP Address has been selected
    - The **Peer Node Identification** is set to **Transport FQDN** and no Transport FQDN has been specified

- Two IP addresses that are equal have been configured for either the Local IP Addresses or Peer IP Addresses.
- The Connection that is being added is a non-IPFE Connection and uses a Capacity Configuration Set with a non-zero Reserved Ingress MPS value and the addition of the new Connection would cause the MP server that hosts the Connection to have Reserved Ingress MPS totaling more than the MP Server's Engineered Ingress MPS capacity. (See the **Engineered Ingress MPS** setting on the **Diameter > Configuration > DA-MPs > MP Profiles** page for the engineered capacity of the MP Server.)
- The Connection that is being added is a non-IPFE Connection and its addition would exceed the maximum number of Connections supported by the MP server that owns the specified Local IP Address(es). (See the **Maximum Connections** setting on the **Diameter > Configuration > DA-MPs > MP Profiles** page for the maximum number of Connections supported by the MP Server.)
- The **Connection Mode** is set to **Initiator & Responder** or **Responder Only**, the **Transport Protocol** is set to **SCTP**, the **SCTP Listen Port** matches the SCTP Listen Port of a Local Node used in another Initiator & Responder or Responder Only Connection and the **Local IP Address** conflicts with the Local IP Address of that other Connection.
- The maximum number of Test Connections (2) already exists in the system

If **OK** or **Apply** is clicked, and the following condition exists, the indicated Warning appears:

- Two IP Addresses have been configured for the Local Node and only one IP Address is configured for the Peer Node

  Warning - " It is recommended that a Secondary IP address also 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, and for the validation of the IP addresses advertised by the Peer in the INIT/INIT_ACK SCTP chunk."

25. Use the *Enabling Connections* procedure to enable the new Connection.

Editing a Connection

Use this task to edit an existing Connection.

Note: A Connection must be in the Disabled Admin State before it can be changed. See *Disabling Connections*.

1. Verify that the Connection to be edited is in the **Disabled** Admin State.
   a) Select **Diameter** > **Maintenance** > **Connections**
   b) If the **Admin State** is **Disabled** for the Connection to be edited, continue with *Step 2*.
   c) If the **Admin State** is **Enabled** for the Connection to be edited, use the *Disabling Connections* procedure to disable the Connection. Then continue with *Step 2*
2. Select **Diameter** > **Configuration** > **Connections**.
   The **Diameter > Configuration > Connections** page appears.
3. Select the Connection you want to edit.
4. Click **Edit**.

   The **Diameter > Configuration > Connections [Edit]** page appears. The page is populated with the current values for the selected Connection.

The **Diameter > Configuration > Connections [Edit]** page will not open if any of the following conditions exist:

- The selected Connection no longer exists (was deleted by another user).
- The Connection is not in the "Disabled" Admin state.

5. Update the relevant fields.

   For more information about each field see *Connection configuration elements*. The **Connection Name** cannot be edited.

   Note: A Test Connection can be changed to a normal Connection by unchecking the **Test Mode** check box. However, a normal Connection cannot be changed to a Test Connection.

   Selecting the X at the end of a field clears the field, so that a different value can be entered or selected.

6. Click:

   - **OK** to save the changes and return to the **Diameter > Configuration > Connections** page. The Connection remains in the "Disabled" Admin state.
   - **Apply** to save the changes and stay on this page. The Connection remains in the "Disabled" Admin state.
   - **Cancel** to return to the **Diameter > Configuration > Connections** page without saving the changes.

   If **OK** or **Apply** is clicked, and a Connection Capacity Validation issue (see *Connection Capacity Validation*) or any of the following conditions exists, an error message or warning message appears:

   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The edited Connection no longer exists in the system (it was deleted by another user)
   - The edited Connection is not in the "Disabled" Admin state
   - A selected pulldown list entry no longer exists (has been deleted by another user)
   - The selected **Transport Protocol** is not supported by the selected Local Node or Peer Node
   - The selected **Local IP Address** + **Local Initiate Port** combination is the same as the **Local IP Address** and **Local Node Listen Port** combination of one of the Local Nodes
   - The selected **Local IP Address** + **Local Initiate Port** combination is the same as the **Local Initiate Port** combination of another Connection
   - The **Connection Mode** is set to **Initiator Only** or **Initiator & Responder**, a Peer IP Address is not selected, and a *Primary DNS Server IP Address* is not configured
   - The **Connection Mode** is set to **Initiator Only** or **Initiator & Responder**, and the selected **Local IP Address** (or pair for Multi-homing), **Local Initiate Port**, and **Transport Protocol** combination is the same the **Local IP Address** (or pair for Multi-homing), **Listen Port**, and **Transport Protocol** combination of one of the Local Nodes
   - The **Connection Mode** is set to **Initiator Only** or **Initiator & Responder**, and the selected **Local IP Address** (or pair for Multi-homing), **Local Initiate port**, and **Transport Protocol** combination is the same the **Local IP Address** (or pair for Multi-homing) and **Local Initiate** port combination of another Connection
   - All Local Node and Peer Node IP addresses are not of the same type (IPv4 or IPv6)
   - The **Peer Node Identification** is set to **IP Address** and no IP Address has been selected
   - The **Peer Node Identification** is set to **Transport FQDN** and no Transport FQDN has been specified

- Two IP addresses that are equal have been configured for either the Local or Peer IP Addresses.
- The configured Primary and Secondary TSAs are identical for an IPFE SCTP Multi-homed Connection association
- The Connection that is being changed is a non-IPFE Connection and uses a Capacity Configuration Set with a non-zero Reserved Ingress MPS value and the change to the Connection would cause the MP server that hosts the Connection to have Reserved Ingress MPS totaling more than the MP Server's licensed Ingress MPS capacity. (See the **Engineered Ingress MPS** on the **Diameter > Configuration > MP Profiles** page for the licensed capacity of the MP Server.)
- For Uni-homed and Multi-homed Connections with various **Connection Mode** and **Peer Node Identification** combinations, the element combinations that must be unique are not unique (see the **Connection Mode** element description in *Connection configuration elements*)
- The **Connection Mode** is set to **Initiator & Responder** or **Responder Only**, the **Transport Protocol** is set to **SCTP**, the **SCTP Listen Port** matches the SCTP Listen Port of a Local Node used in another Initiator & Responder or Responder Only Connection and the **Local IP Address** conflicts with the Local IP Address of that other Connection
- **Test Mode** is changed from unchecked to checked, but the maximum number of Test Connections already exists in the system.

7. Use the *Enabling Connections* procedure to enable the edited Connection.

Deleting a Connection

Use this task to delete an existing Connection.

Note: You must disable a Connection before you can delete it. See *Disabling Connections*.

1. Select **Diameter** > **Configuration** > **Connections**.
   The **Diameter > Configuration > Connections** page appears.
2. Select the Connection you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Perform one of the following actions:
   - Click **OK** to delete the Connection.
   - Click **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Connections** page.

   If **OK** is clicked and any of the following conditions exist, an error message appears and the Connection is not deleted:

   - The selected Connection is referenced by at least one Route Group
   - The selected Connection is referenced by at least one Egress Throttle Group
   - The selected Connection is not in the "Disabled" Admin State

   If **OK** is clicked and the selected Connection no longer exists (it was deleted by another user), an error message is displayed and the Connections view is refreshed.

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 configured capacity assignment of each available Peer Node or Connection.

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

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

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

- Filter the list of Route Groups to display only the desired Route Groups.
- Sort the list by the Route Group Name column in ascending or descending order, by clicking the column heading. The default order is ascending ASCII order.
- Click an entry that is shown in blue for a Peer Node/Connection.

  The **Diameter > Configuration > Peer Nodes (Filtered)** page appears for the selected Peer Node.

- Click **Insert**.

  The **Diameter > Configuration > Route Groups [Insert]** page appears. You can add a new Route Group.

  The **Diameter > Configuration > Route Groups [Insert]** will not open if the maximum number of Route Groups (6000) already exists in the system.

- Select a Route Group in the list, and click **Edit**.

  The **Diameter > Configuration > Route Groups [Edit]** page appears. You can edit the selected Route Group.

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

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

Route Group configuration elements

Table 17: 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 17: 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 configured 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 160 entries can be configured 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 160 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: 1-160 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 160 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: 1-160 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 configured 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 configured capacity for the Peer Node/Connection. A Peer Nodes/Connection with a higher capacity will be assigned more traffic.	Format: numeric Range: 1 - 64000

Viewing Route Groups

Use this task to view currently configured Route Groups.

Select **Diameter** > **Configuration** > **Route Groups**.
The **Diameter > Configuration > Route Groups** page appears.

Adding a Route Group

Use this task to create a new Route Group.

1. Select **Diameter** > **Configuration** > **Route Groups**.
   The **Diameter > Configuration > Route Groups** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Route Groups [Insert]** page appears.
3. Enter a unique name for the Route Group in the **Route Group Name** field.
4. Select the **Type** radio button for the entries included in the Route Group (Peer Nodes or Connections).
5. Select the Peer Node, or Peer Node and Connection, and enter the Provisioned Capacity field for this Route Group entry.
   a) Select a Peer Node from the **Peer Node** pulldown list.

b) If the Connection Route Group radio button is selected for the **Type** field, select a Connection that is assigned to the selected Peer Node from the **Connection** pulldown list.
c) Enter the **Provisioned Capacity** for the selected Peer Node or Connection.

6. Perform one of the following actions:
   - If you want to add another Peer Node, Connection, and Provisioned Capacity entry to the Route Group, click **Add** and repeat *Step 5* for this next entry. Up to 160 entries can be provisioned.
   - If you do not want to add another entry, continue with *Step 7*.
7. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Route Groups** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Route Groups** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The Route Group Name is not unique; it already exists in the system
   - The selected pulldown list entry no longer exists (has been deleted by another user)
   - The selected Peer Node is a duplicate within the Route Group
   - The selected Connection is a duplicate within the Route Group for the same Peer Node
   - The maximum number of Route Groups (6000) already exists in the system

Editing a Route Group

Use this task to make changes to a Route Group.

When the **Diameter > Configuration > Route Groups [Edit]** page opens, the fields are initially populated with the current values for the selected Route Group. The **Route Group Name** cannot be changed.

1. Select **Diameter** > **Configuration** > **Route Groups**.
   The **Diameter > Configuration > Route Groups** page appears.
2. Select the Route Group you want to edit.
3. Click **Edit**

   The **Diameter > Configuration > Route Groups [Edit]** page appears.

   To delete a Peer Node or a Connection from the Route Group, clear the Peer Node and Provisioned Capacity field values either by selecting "--Select--" in the Peer Node pulldown list or by clicking the X at the end of the Provisioned Capacity box for the Peer Node.

   The **Type** field can be changed only if the Route Group is not assigned to any Route List.

   When the **Type** field is changed, the **Peer Node, Connection, and Provisioned Capacity** entries are reset to one entry with empty values. The **Connection** pulldown list is not available when **Peer Route Group** is selected for the **Type** field.
4. Update the relevant fields.
   For more information about each field see *Route Group configuration elements*.

5. Click:
   - **OK** to save the data and exit this page.
   - **Apply** to save the data and stay on this page.
   - **Cancel** to return to the **Diameter > Configuration > Route Groups** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The selected pulldown list entry no longer exists (has been deleted by another user)
   - The selected Peer Node is a duplicate within the Route Group
   - The selected Connection is a duplicate within the Route Group for the same Peer Node

Deleting a Route Group

Use this task to delete a Route Group.

Note: A Route Group cannot be deleted if it is included in any *Route Lists*.

1. Select **Diameter** > **Configuration** > **Route Groups**.
   The **Diameter > Configuration > Route Groups** page appears.
2. Select the Route Group you want to delete.
3. Click **Delete**.
   A popup window appears.
4. Perform one of the following actions:
   - Click **OK** to delete the Route Group.
   - Click **Cancel** to return to the **Diameter > Configuration > Route Groups** page without deleting the Route Group

   If **OK** is clicked and the selected Route Group is referenced by at least one Route List, an error message appears and the Route Group is not deleted.

   If **OK** is clicked and the selected Route Group no longer exists (it was deleted by another user), an error message is displayed and the Route Groups view is refreshed.

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 configured 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 may change.

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

Route Lists are assigned to Peer Nodes when Alternate Implicit Routing will be used.

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

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

- Filter the list of Route Lists to display only the desired Route Lists.
- Sort the list by the **Route List Name** column or the Minimum Route Group Availability Weight column in ascending or descending order, by clicking the column heading. The default order is by **Route List Name** in ascending ASCII order. The expanded rows of Route Groups are sorted by **Priority**.
- Click an entry that is shown in blue for a **Route Group** (in the expanded list).

  The **Diameter > Configuration > Route Groups (Filtered)** page appears for the selected Route Group.

- Click **Insert**.

  The **Diameter > Configuration > Route Lists [Insert]** page appears. You can add a new Route List.

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

  - The maximum number of Route Lists (2000) already exists in the system
  - There is no available Route Group

- Select a **Route List** in the list, and click **Edit**.

  The **Diameter > Configuration > Route Lists [Edit]** page appears. You can edit the selected Route List.

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

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

Route List configuration elements

Table 18: 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 18: 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. The minimum weight is used to determine a Route Group's availability status within a Route List.	Format: numeric Range: 1 - 1024000
* 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

Viewing Route Lists

Use this task to view currently configured Route Lists.

Select **Diameter** > **Configuration** > **Route Lists**.
The **Diameter > Configuration > Route Lists** page appears.

Adding a Route List

Use this task to create a new Route List. The fields are described in *Route List configuration elements*.

Note: You must have at least one Route Group configured before you can create a Route List.

1. Select **Diameter** > **Configuration** > **Route Lists**.
   The **Diameter > Configuration > Route Lists** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Route Lists [Insert]** page appears.
3. Enter a unique name for the Route List in the **Route List Name** field.
4. Enter the **Minimum Route Group Availability Weight** in the field.
5. Select one to three Route Groups from the **Route Group** pulldown lists.
6. In the corresponding **Priority** field, set a priority for each selected Route Group.
7. Enable or disable routing across alternate Route Groups in Route List by setting **Route Across Route Groups**.
8. Click:
   - **OK** to save the data and return to the **Diameter > Configuration > Route Lists** page .
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Route Lists** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The **Route List Name** is not unique; it already exists in the system
   - The selected pulldown list entry no longer exists (has been deleted by another user)
   - A selected **Route Group** is a duplicate within the Route List
   - A Route Group **Priority** is not unique within the Route List
   - The maximum number of Route Lists (2000) already exists in the system

Editing a Route List

Use this task to make changes to existing Route Lists.

The **Route List Name** cannot be changed.

1. Select **Diameter** > **Configuration** > **Route Lists**.
   The **Diameter > Configuration > Route Lists** page appears.
2. Select the **Route List** you want to edit.
3. Click **Edit**.

   The **Diameter > Configuration > Route Lists [Edit]** page appears.

   The page is initially populated with the current configured values for the selected Route List.
4. Update the relevant fields.
   For more information about each field see *Route List configuration elements*.

5. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Route Lists** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration >Route Lists** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The selected **Route List** no longer exists (has been deleted by another user)
   - A selected **Route Group** no longer exists (has been deleted by another user)
   - A selected **Route Group** is a duplicate within the Route List
   - A Route Group **Priority** is not unique within the Route List

Deleting a Route List

Use this task to delete a Route List.

Note: A Route List cannot be deleted if any of the following conditions are true:

- The Route List is referenced by any Peer Node as the Alternate Implicit Route
- The Route List is referenced by any Peer Routing Rule
- The Route List is set as the **Route List for DAS Node** in any Message Copy Configuration Set

1. Select **Diameter** > **Configuration** > **Route Lists**.
   The **Diameter > Configuration > Route Lists** page appears.
2. Select the **Route List** you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Route List.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Route Lists** page.

   If **OK** is clicked and the selected Route List no longer exists (it was deleted by another user), an error message is displayed and the Route Lists view is refreshed.

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 Route Tables elements

Table 19: 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 19: 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 and must contain at least one alpha
Number of Rules	The number of Peer Routing Rules in the Peer Route Table.	

Viewing Peer Route Tables

Use this task to view currently configured Peer Route Tables.

Select **Diameter** > **Configuration** > **Peer Route Tables**.
The **Diameter > Configuration > Peer Route Tables** page appears.

Adding a Peer Route Table

Use this task to create a new Peer Route Table. The fields are described in *Peer Route Tables elements*.

1. Select **Diameter** > **Configuration** > **Peer Route Tables**.

The **Diameter > Configuration > Peer Route Tables** page appears.

2. Click **Insert**.
   The **Diameter > Configuration > Peer Route Tables [Insert]** page appears.
3. Enter a unique name for the Peer Route Table in the **Peer Route Table Name** field.
4. Click:
   - **OK** to save the data and go to the **Viewing Rules for Peer Route Table** page .
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Peer Route Tables** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The **Peer Route Table Name** is not unique; it already exists in the system
   - The maximum number of Peer Route Tables (100) already exists in the system

After a Peer Route Table is added, Peer Routing Rules can be defined for it. See *Peer Routing Rules configuration*. For information on the order in which DSR components need to be configured, see *Configuration Sequence*.

Deleting a Peer Route Table

Use this task to delete a **Peer Route Table**.

Note: A Peer Route Table cannot be deleted if any of the following conditions are true:

- The **Peer Route Table** is referenced by any Peer Node
- The **Peer RouteTable** is referenced by any Application Id
- The selected **Peer Route Table** is the Default **Peer Route Table**

1. Select **Diameter** > **Configuration** > **Peer Route Tables**.
   The **Diameter > Configuration > Peer Route Tables** page appears.
2. Select the **Peer Route Table** you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the **Peer Route Table**.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Peer Route Tables** page.

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

Peer Routing Rules configuration

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

There are six Peer Routing Rule parameters:

- 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. If you choose to route the Diameter message to a Peer Node, the message is sent to a Peer Node in the selected Route List based on the Route Group priority and Peer Node configured capacity settings. If you choose to Send an Answer, then the message is not routed and the specified Diameter Answer Code is returned to the sender.

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

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

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

On the **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page, you can perform the following actions:

- Filter the list of Rule Names, to display only the desired Rules.
- Sort the list entries in ascending or descending order by column (except **Conditions**), by clicking the column heading.

  By default, the list is sorted by **Priority** in ascending ASCII order. The lowest Priority value indicates the highest priority. For Rules with the same Priority, the **Rule Name** is used for sorting.
- Select a blue **Route List** entry, to open the **Diameter > Configuration > Route Lists [Filtered]** page for the selected entry.
- Click the **Insert** button.

  The **Inserting Rule for Peer Route Table: {Peer Route Table Name}** page opens. You can add a new Peer Routing Rule and its values. See *Adding a Peer Routing Rule*.

  If the maximum number of Peer Routing Rules (1000) already exists for the Peer Route Table, the **Inserting Rule for Peer Route Table: {Peer Route Table Name}** page will not open, and an error message is displayed.
- Select the **Rule Name** of a Peer Routing Rule in the list, and click the **Edit** button.

  The **Editing Rule for Peer Route Table: {Peer Route Table Name}** page opens. You can edit the selected Peer Routing Rule. See *Editing a Peer Routing Rule*.

  If the selected Peer Routing Rule has been deleted by another user, the **Editing Rule for Peer Route Table: {Peer Route Table Name}** page will not open.

- Select the **Rule Name** of a Peer Routing Rule in the list, and click the **Delete** button to remove the selected Peer Routing Rule. See *Deleting a Peer Route Rule*.

Peer Routing Rule configuration elements

Table 20: 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 20: 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	View-only
* Priority	Priority of the Rule in relation to other Rules. The priority is set from 1 (highest priority) to 99 (lowest priority).	Format: text box; 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 • 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 *Peer Routing Rule operators* for a description of operators available for each parameter.

Field (* indicates required field)	Description	Data Input Notes
	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 or pulldown list 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 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.

Field (* indicates required field)	Description	Data Input Notes
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: configured Route Lists Default: "-Select-"
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
Message Copy Configuration Set	Message Copy Configuration Set (MCCS) used for copying the messages to the DAS. A valid MCCS will mark the messages matched by this Peer Route Rule for copy to the DAS.	Format: pulldown list Range: Default; configured Message Copy Configuration Sets Default: "-Select-"
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
Vendor Id	The Vendor Id to place in the Vendor Id AVP of the answer message.	Format: text box; numeric Range: 0 - 4294967295
Answer Error Message	Value returned in the Error-Message AVP of the answer message.	Format: text box; alphanumeric, underscore (_), period (.)

Field (* indicates required field)	Description	Data Input Notes
		Range: 0 - 64 characters Default: Null string

Peer Routing Rule operators

Table 21: Peer Routing Rules Operators describes the condition operators available for each parameter in a Peer Routing Rule.

Table 21: 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
	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

Parameter	Operator	Meaning
	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

Viewing Peer Routing Rules

Use this task to view Peer Routing Rules currently configured in a particular Peer Route Table.

1. Select **Diameter** > **Configuration** > **Peer Route Tables**.
   The **Diameter > Configuration > Peer Route Tables** page appears.
2. Select the Peer Route Table for which you want to view Peer Routing Rules and click **View/Edit Rules**.
   The **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page appears.

Adding a Peer Routing Rule

Use this task to create a new Peer Routing Rule in a Peer Route Table.

1. Select **Diameter** > **Configuration** > **Peer Route Tables**.
   The **Diameter > Configuration > Peer Route Tables** page appears.
2. Select the Peer Route Table to which you want to add a Peer Routing Rule and click **View/Insert Rules**.
   The **Viewing Rules for Peer Route Table: {Peer Route Table Name}** appears.
3. Click **Insert**.
   The **Inserting Rule for Peer Route Table: {Peer Route Table Name}** page appears.
4. Enter a unique name for the Rule in the **Name** field.
5. Set a Priority for this Rule in relation to other Rules, by entering a number between 1 and 99 in the **Priority** field.
6. Set the Peer Routing Rule **Conditions**:
   a) Locate the **Parameter** you want to set.
   b) Select the relevant operator from the **Operator** pulldown list. See *Peer Routing Rule operators* for a description of operators available for each parameter.
   c) Enter the appropriate value for the parameter in the corresponding **Value** field.
   d) Repeat this step for each parameter. For any parameter that does not need to be evaluated, set the **Operator** to **Always True**.
7. Select the **Action** you want to occur when a Diameter message matches the parameter conditions.

- **Route to Peer**: route the message to a Peer Node using the Route List associated with this Rule.
- **Send Answer**: abandon message routing and send an Answer response containing the **Answer Result-Code Value** associated with this Rule.

8. If you selected **Route to Peer** as the Action, select the **Route List** to associate with this Rule from the pulldown list.
9. If you selected **Route to Peer** as the Action, select the **Message Priority** to assign to the message.
10. If Diameter Message Copy will be used, select the **Message Copy Configuration Set** to use when this Rule is selected for PRT-triggered Message Copy.
11. If you selected **Send Answer** as the Action, select the desired **Answer Result-Code Value** selection box:
    - Select the pulldown list radio button to use an existing Answer Result-Code; then select an Answer Result-Code in the list.
    - Select the text box radio button, and enter your own Answer Result-Code value.
12. If you selected **Send Answer** as the Action, enter the desired Vendor Id AVP in the **Vendor Id** field.
13. If you selected **Send Answer** as the Action, enter the desired Error-Message AVP in the **Answer Error Message** field.
14. Click:
    - **OK** to save the changes and return to the **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page.
    - **Apply** to save the changes and remain on this page.
    - **Cancel** to return to the **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page without saving any changes.

    If OK or Apply is clicked and any of the following conditions exist, an error message appears:
    - Any required field is empty (no entry was made)
    - Any field is not valid or is out of range
    - The **Rule Name** is not unique; it already exists in the system
    - The selected **Route List** no longer exists (has been deleted by another user)
    - The Rule is similar to an already existing Rule (the same attributes except for Rule Name and Priority)
    - The maximum number of Peer Routing Rules (1000) already exists for the Peer Route Table.

Editing a Peer Routing Rule

Use this task to edit a Peer Routing Rule in a Peer Route Table.

The **Rule Name** cannot be changed.

1. Select **Diameter** > **Configuration** > **Peer Route Tables**.
   The **Diameter > Configuration > Peer Route Tables** page appears.
2. Select the Peer Route Table which contains the Peer Routing Rule you want to edit and click **View/Edit Rules**.
   The **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page appears.
3. Select the Peer Routing Rule you want to edit, then click **Edit**.
   The **Editing Rule for Peer Route Table: {Peer Route Table Name}**page appears.

4. Update the relevant fields.

   For more information about each field see *Peer Routing Rule configuration elements* and *Peer Routing Rule operators*.

5. Click:

   - **OK** to save the data and return to **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any required field is empty (no entry was made)
   - Any field is not valid or is out of range
   - The selected Peer Routing Rule no longer exists (was deleted by another user)
   - The selected Route List no longer exists (was deleted by another user)
   - The Rule is similar to an already existing Rule (the same attributes except for Rule Name and Priority)

Deleting a Peer Route Rule

Use this task to delete a Peer Routing Rule from a Peer Route Table.

1. Select **Diameter** > **Configuration** > **Peer Route Tables**.
   The **Diameter > Configuration > Peer Route Tables** page appears.
2. Select the Peer Route Table which contains the Peer Routing Rule you want to delete and click **View/Edit Rules**.
   The **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page appears.
3. Select the Peer Routing Rule you want to delete.
4. Click **Delete**.
   A popup window appears to confirm the delete.
5. Click:

   - **OK** to delete the Peer Routing Rule.
   - **Cancel** to cancel the delete function and return to the **Viewing Rules for Peer Route Table: {Peer Route Table Name}** page.

   If **OK** is clicked and the selected Peer Routing Rule no longer exists (it was deleted by another user), an error message is displayed and the Peer Routing Rules view is refreshed.

Egress Throttle Groups configuration

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

Egress Throttle Group functions are described in detail in *Egress Throttle Groups*.

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

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

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

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

On the **Diameter > Configuration > Egress Throttle Groups** page, the following actions can be performed:

- Filter the list of Egress Throttle Groups to display only the desired Egress Throttle Groups.
- Sort the list by a column in ascending or descending order, by clicking the column heading.

  All columns except **Time of Last Update** sort in ascending ASCII order. The **Time of Last Update** column sorts by timestamp.

  The default order is by **Egress Throttle Groups Name** in ascending ASCII order.

- Click **Insert**.

  The **Diameter > Configuration > Egress Throttle Groups [Insert]** page opens. You can add new Egress Throttle Groups.

  The **Diameter > Configuration > Egress Throttle Groups [Insert]** page will not open if the maximum number of Egress Throttle Groups (128 per DSR NE) already exists in the system.

- Select an Egress Throttle Group in the list, and click **Edit**.

  The **Diameter > Configuration > Egress Throttle Groups [Edit]** page opens. You can edit the selected Egress Throttle Group.

  If the selected Egress Throttle Group has been deleted by another user, the **Diameter > Configuration > Egress Throttle Groups [Edit]** page will not open.

- Select an Egress Throttle Group in the list, and click **Delete** to delete the selected Egress Throttle Group.

Egress Throttle Groups elements

Table 22: Egress Throttle Groups Elements describes the fields on the **Diameter > Configuration > Egress Throttle Groups** page.

Table 22: Egress Throttle Groups Elements

Field (* indicates a required field)	Description	Data Input Notes
*Egress Throttle Group Name	A name that uniquely identifies the Egress Throttle Group.	Format: text box; alphanumeric and underscore; must

Field (* indicates a required field)	Description	Data Input Notes
		contain at least one alpha and must not start with a digit. Range: 1- 32 characters
Egress Throttlings	Egress throttlings configurable for this Egress Throttle Group.	Format: two check boxes; one or both boxes must be checked. Range: Rate Limiting, Pending Transaction Limiting, or both. Default: both checked.
Members		
Peers	Peers associated with this Egress Throttle Group.	Format: text box; numeric Range: 0-128
Connections	Connections associated with this Egress Throttle Group.	Format: text box; numeric Range: 0-128
Rate Limiting		
*Maximum Egress Request Rate	The maximum allowed Egress Request Rate shared by associated members.	Format: text box; numeric Range: 100-250000
*Onset Threshold Level 1 (%)	When Egress Request Rate exceeds this percentage of maximum Egress Request Rate, the Congestion Level is set to 1.	Format: text box; numeric Range: 2-100 Default: 100
*Abatement Threshold Level 1 (%)	When Egress Request Rate falls below this percentage of maximum Egress Request Rate, the Congestion Level is set to 0.	Format: text box; numeric Range: 1-100 Default: 80
Onset Threshold Level 2 (%)	When Egress Request Rate exceeds this percentage of maximum Egress Request Rate, the Congestion Level is set to 2.	Format: text box; numeric Range: 4-100

Field (* indicates a required field)	Description	Data Input Notes
Abatement Threshold Level 2 (%)	When Egress Request Rate falls below this percentage of maximum Egress Request Rate, the Congestion Level is set to 1.	Format: text box; numeric Range: 3-100
Onset Threshold Level 3 (%)	When Egress Request Rate exceeds this percentage of maximum Egress Request Rate, the Congestion Level is set to 3.	Format: text box; numeric Range: 6-100
Abatement Threshold Level 3 (%)	When Egress Request Rate falls below this percentage of maximum Egress Request Rate, the Congestion Level is set to 2.	Format: text box; numeric Range: 5-100
*Smoothing Factor (%)	Percentage contribution of the current Egress Request Rate sample to the Smoothed Egress Request Rate.	Format: text box; numeric Range: 20-90 Default: 80
*Abatement Time (msec)	The amount of time in milliseconds that the Smoothed Egress Request Rate must remain below an abatement threshold before the Congestion Level is lowered.	Format: text box; numeric Range: 200-10000 Default: 500
Pending Transaction Limiting		
*Maximum Egress Pending Transactions	The maximum allowed Egress Pending Transactions for the Peers and Connections within a group.	Format: text box; numeric Range: 100-1000000
*Onset Threshold Level 1 (%)	When Egress Pending Transactions exceeds this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 1.	Format: text box; numeric Range: 2-100 Default: 100
*Abatement Threshold Level 1 (%)	When Egress Pending Transactions falls below this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 0.	Format: text box; numeric Range: 1-100 Default: 80
Onset Threshold Level 2 (%)	When Egress Pending Transactions exceeds this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 2.	Format: text box; numeric Range: 4-100

Field (* indicates a required field)	Description	Data Input Notes
Abatement Threshold Level 2 (%)	When Egress Pending Transactions falls below this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 1.	Format: text box; numeric Range: 3-100
Onset Threshold Level 3 (%)	When Egress Pending Transactions exceeds this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 3.	Format: text box; numeric Range: 6-100
Abatement Threshold Level 3 (%)	When Egress Pending Transactions falls below this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 2.	Format: text box; numeric Range: 5-100
*Abatement Time (msec)	The amount of time in milliseconds that Egress Pending Transactions must remain below an abatement threshold before the Congestion Level is lowered.	Format: text box; numeric Range: 200-10000 Default: 500

Viewing Egress Throttle Groups

Use this task to view Egress Throttle Groups.

Egress Throttle Groups fields are described in *Egress Throttle Groups elements*.

Select **Diameter** > **Configuration** > **Egress Throttle Groups.**
The **Diameter > Configuration> Egress Throttle Groups** page appears.

Adding Egress Throttle Groups

Use this task to create new Egress Throttle Groups.

Egress Throttle Groups fields are described in *Egress Throttle Groups elements*.

1. Select **Diameter** > **Configuration** > **Egress Throttle Groups**.
   The **Diameter > Configuration > Egress Throttle Groups** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Egress Throttle Groups [Insert]** page appears.
3. Enter a unique name for the Egress Throttle Group in the **Egress Throttle Group Name** field.
4. Select either or both of the Egress Throttlings choices for this Egress Throttle Group by checking one or both boxes to the right of the **Egress Throttlings** field. One or both boxes must be selected for all Egress Throttling Groups, as follows:
   a) To control the total egress Request traffic rate that a DSR will route to a user-defined group of Connections or Peers associated with this Egress Throttle Group, check the **Rate Limiting** box.
   b) To control the total number of transactions that a DSR will allow to be pending for a user-defined group of Connections or Peers associated with this Egress Throttle Group, check the **Pending Transactions Limiting** box.

5. Under the **Members** tab, enter values for the following fields:
   a) **Peers**
   Use the pulldown list to select from a list of Peer names, clicking the **Add** button after each selection. Use the **X** to the right of the pulldown list to remove a selection.
   b) **Connections**
   Use the pulldown list to select from a list of Connection names, clicking the **Add** button after each selection. Use the **X** to the right of the pulldown list to remove a selection.
6. If the **Rate Limiting** chedk box for **Egress Throttlings** is checked for this Egress Throttle Group, enter values for the required fields and for optional fields, as needed.
7. If the **Pending Transactions Limiting** check box for **Egress Throttlings** is checked for this Egress Throttle Group, enter values for the required fields and for optional fields, as needed.
8. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Egress Throttle Groups** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Egress Throttle Groups** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The maximum number of Egress Throttle Groups have already been created.
   - There is no Peer Node or Connection in the signaling network element corresponding to the Egress Throttle Group to be added.
   - Any required fields are left empty.
   - An Egress Throttle Group is configured with the greater than the maximum total number of Peers and Connections.
   - An Egress Throttle Group is configured with duplicate Peers or Connections.
   - An Egress Throttle Group is configured with thresholds at level 3 set but thresholds at level 2 are missing.
   - An Egress Throttle Group is configured with Onset Thresholds at a congestion level 2 or level 3 without providing corresponding Abatement Thresholds.
   - An Egress Throttle Group is configured with Abatement Thresholds at a congestion level 2 or level 3 without providing corresponding Onset Thresholds.
   - An Egress Throttle Group is configured with Onset Threshold at a congestion level lesser than the corresponding Abatement Threshold level at the same level.
   - An Egress Throttle Group is configured with Onset Threshold at a congestion level greater than the corresponding Abatement Threshold at the succeeding level
   - An Egress Throttle Group is configured with a Peer already configured as a member in any Egress Throttle Group. (Explicit association of Peer with another Egress Throttle Group)
   - An Egress Throttle Group is configured with a Peer which is associated with a Connection configured as a member in any Egress Throttle Group. (Implicit association of Peer with another Egress Throttle Group)
   - An Egress Throttle Group is configured with a Connection already configured as a member in any Egress Throttle Group. (Explicit association of Connection with another Egress Throttle Group)
   - An Egress Throttle Group is configured with a Connection which is associated with a Peer configured as a member in any Egress Throttle Group. (Implicit association of Connection with another Egress Throttle Group)

- An Egress Throttle Group is configured with a Connection and a Peer associated with each other.

Editing Egress Throttle Groups

Use this task to edit Egress Throttle Groups.

When the **Diameter > Configuration > Egress Throttle Groups [Edit]** page opens, the columns are initially populated with the current configuration of the selected Egress Throttle Group.

The existing **Egress Throttle Groups Name** cannot be changed.

Changes can be made to an Egress Throttle Group configuration with either Rate Limiting Admin State or Pending Transaction Limiting Admin State in the **Enabled** or the **Disabled** state.

Changes can be made to an Egress Throttle Group configuration irrespective of the Operational Status of the associated Peer Connections.

Egress Throttle Groups fields are described in *Egress Throttle Groups elements*.

1. Select **Diameter** > **Configuration** > **Egress Throttle Groups**.
   The **Diameter > Configuration > Egress Throttle Groups** page appears.
2. Select the Egress Throttle Groups to be edited, then click **Edit**.

   The **Diameter > Configuration > Egress Throttle Groups [Edit]** page appears.
3. Update the relevant fields.

   An entry in a pulldown list can be removed by selecting the entry in the list, and then clicking the **X** to the right of the pulldown list.
4. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Egress Throttle Groups** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Egress Throttle Groups** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - An attempt is made to remove the Rate Limiting Egress Throttling by removing the check from the corresponding **Egress Throttlings** check box for an Egress Throttle Group for which the Rate Limiting Admin State is set to **Enabled**.
   - An attempt is made to remove Pending Transaction Egress Throttling by removing the check from the corresponding **Egress Throttlings** check box for an Egress Throttle Group for which the Pending Transaction Limiting Admin State is set to **Enabled**.

Deleting Egress Throttle Groups

Use this task to delete Egress Throttle Groups.

An Egress Throttle Group cannot be deleted if either its corresponding Rate Limiting Admin State or Pending Transaction Limiting Admin State is not in the Disabled admin state. Before you perform

this task, ensure that the Rate Limiting Admin State or Pending Transaction Limiting Admin State for the Egress Throttle Group is in the Disabled admin state.

1. Select **Diameter** > **Configuration** > **Egress Throttle Groups**
   The **Diameter > Configuration > Egress Throttle Groups** page appears.
2. Select the Egress Throttle Group to be deleted.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:

   - **OK** to delete the Egress Throttle Group.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Egress Throttle Groups** page.

   If **OK** is clicked and the following condition exists, an error message appears:

   - The Egress Throttle Group Rate Limiting Admin State for the Egress Throttle Group to be deleted is not in the Disabled admin state.
   - The Egress Throttle Group Pending Transaction Limiting Admin State for the Egress Throttle Group to be deleted is not in the Disabled admin state.

Reroute On Answer configuration

Using Reroute On Answer, you can configure rerouting scenarios based on the Application Id and Result-Code AVP values in Answer messages. If these values match the configured order pair of Application Id and Result-Code AVP value, the message is rerouted to another available Peer Node from the 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.

On the **Diameter > Configuration > Reroute on Answer** page, you can perform the following actions:

- Filter the list to display only the desired entries.
- Sort the list by column in ascending or descending order, by clicking the column heading. The default order is by **Answer Result Code-AVP Value** in ascending ASCII order.
- Click **Insert**.

  The **Diameter > Configuration > Reroute on Answer [Insert]** page appears. You can add a new entry.

  The **Diameter > Configuration > Reroute on Answer [Insert]** will not open if the maximum number of Reroute on Answer entries (1000) already exists in the system.

- Select a Reroute on Answer entry, and click **Delete** to delete the selected entry.

Reroute On Answer configuration elements

Table 23: 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 23: 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

Viewing Reroute On Answer

Use this task to view Reroute On Answer.

Select **Diameter** > **Configuration** > **Reroute On Answer**.
The **Diameter > Configuration > Reroute on Answer** page appears.

Adding a Reroute On Answer entry

Use this task to create a new Reroute On Answer entry.

The fields are described in *Reroute On Answer configuration elements*.

1. Select **Diameter** > **Configuration** > **Reroute On Answer**.
   The **Diameter > Configuration > Reroute on Answer** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Reroute On Answer [Insert]** page appears.
3. Enter the desired Result-Code AVP in the **Answer Result-Code AVP Value** field.
4. Perform one of the following actions for **Application Id**:
   - Select **ALL** to apply the Reroute On Answer entry to all Application Ids.
   - Select the second radio button, and select the appropriate **Application Id** from the pulldown list.
5. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Reroute on Answer** page.

- **Apply** to save the changes and remain on this page.
- **Cancel** to return to the **Diameter > Configuration > Reroute on Answer** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- A field is empty; a value was not entered
- A value is not valid
- The **Answer Result-Code AVP Value** and **Application Id** combination is not unique; it already exists in the system
- Adding the new Reroute on Answer entry would cause the maximum number of Reroute on Answer entries (1000) to be exceeded

Deleting a Reroute On Answer

Use this task to delete a Reroute On Answer entry.

1. Select **Diameter** > **Configuration** > **Reroute On Answer**.
   The **Diameter > Configuration > Reroute On Answer** page appears.
2. Select the **Answer Result-Code AVP Value** for the Reroute On Answer you want to delete.
   A popup window appears to confirm the delete.
3. Click **Delete**.
4. Click:
   - **OK** to delete the Reroute on Answer entry.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Reroute On Answer** page.

   If **OK** is clicked and the selected entry no longer exists (it was deleted by another user), an error message is displayed and the Reroute on Answer page is refreshed.

Application Route Tables configuration

An **Application Route Table** contains one or more Application Routing Rules that can be used for routing Request messages to DSR Applications.

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

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

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

  The **Diameter > Configuration > Application Route Tables [Insert]** page will not open if the maximum number of Application Route Tables (100) already exists in the system.

- Select an **Application Route Table** in the list, and click **Delete**. You can delete the selected **Application Route Table**.
- Select an **Application Route Table** in the list, and click **View/Edit Rules**.

  The **Diameter > Configuration > Application Route Tables [View/Edit Rules]** page appears. You can edit the selected Application Route Table Rules.

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

Application Route Tables elements

Table 24: Application Route Tables elements describes the fields on the **Application Route Tables** View and Insert pages. Data Input Notes apply only to the Insert page; the View page is read-only.

Table 24: Application Route Tables elements

Field (* indicates required field)	Description	Data Input Notes
* Application Route Table Name	Unique name of the Application Route Table.	Format: text box; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters

Viewing Application Route Tables

Use this task to view currently configured **Application Route Tables**. The fields are described in *Application Route Tables elements*

Select **Diameter** > **Configuration** > **Application Route Tables**.
The **Diameter > Configuration > Application Route Tables** page appears.

Adding an Application Route Table

Use this task to create a new **Application Route Table**. The fields are described in *Application Route Tables elements*.

1. Select **Diameter** > **Configuration** > **Application Route Tables**.
   The **Diameter > Configuration > Application Route Tables** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Application Route Tables [Insert]** page appears.
3. Enter a unique name for the Application Route Table in the **Application Route Table Name** field.
4. Click:

- **OK** to save the new Application Route Table and go to the **Diameter > Configuration > Application Route Tables** page .
- **Apply** to save the new Application Route Table and remain on this page.
- **Cancel** to return to the **Diameter > Configuration > Application Route Tables** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any required field is empty; no value was entered or selected
- The entry in any field in not valid (wrong data type or out of the valid range)
- The **Application Route Table Name** is not unique; it already exists in the system
- Adding this Application Route Table would cause the maximum number of **Application Route Tables** (100) allowed in the system to be exceeded
- Adding this Application Route Table would cause the maximum number of **Application Routing Rules** (1000) allowed in the system to be exceeded

After an **Application Route Table** is added, Application Routing Rules can be defined for it. See *Application Routing Rules configuration*.

Deleting an Application Route Table

Use this task to delete an **Application Route Table**.

Note: A Peer Route Table cannot be deleted if any of the following conditions are true:

- The **Peer Route Table** is referenced by any Peer Node
- The **Peer RouteTable** is referenced by any Application Id
- The selected **Peer Route Table** is the Default **Peer Route Table**

1. Select **Diameter** > **Configuration** > **Application Route Tables**.
   The **Diameter > Configuration > Application Route Tables** page appears.
2. Select the **Application Route Table** you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the **Application Route Table**.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Application Route Tables** page.

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

Application Routing Rules configuration

An Application Routing Rule defines message routing to a DSR Application based on message content matching the Application Routing Rule's conditions. There are six Application Routing Rule parameters:

- Destination-Realm
- Destination-Host
- Application-Id

- Command-Code
- Origin-Realm
- Origin-Host

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

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

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

On the **Viewing Rules for Application Route Table: {Application Route Table Name}** page, you can perform the following actions:

- Filter the list of Rule Names, to display only the desired Rules.
- Sort the list entries in ascending or descending order by Rule Name, Priority, or Application Name, by clicking the column heading.

  By default, the list is sorted by Priority in ascending ASCII order. The lowest Priority value indicates the highest priority. For Rules with the same Priority, the Rule Name is used for sorting.

- Click the **Insert** button.

  The **Inserting Rule for Application Route Table: {Application Route Table Name}** page opens. You can add a new Application Routing Rule and its values. See *Adding an Application Routing Rule*. If the maximum number of Application Routing Rules (1000) already exists in the system, the **Inserting Rule for Application Route Table: {Application Route Table Name}** page will not open, and an error message is displayed.

- Select the **Rule Name** of an Application Routing Rule in the list, and click the **Edit** button.

  The **Editing Rule for Application Route Table: {Application Route Table Name}** page opens. You can edit the selected Application Routing Rule. See *Editing an Application Routing Rule*.

- Select the **Rule Name** of an Application Routing Rule in the list, and click the **Delete** button to remove the selected Application Routing Rule. See *Deleting an Application Routing Rule*

Application Routing Rule configuration elements

Table 25: 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 25: 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: text box; case-sensitive; alphanumeric and underscore (_); cannot start with a digit and

Field (* indicates required field)	Description	Data Input Notes
		must contain at least one alpha (A-Z, a-z) Range: 1 - 32 characters
* Application Route Table	Application Route Table associated with this Rule.	View Only
* 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 Rule with a Priority set to 2 has second priority, and so on.	Format: text box; numeric Range: 1 - 99
* Conditions	Conditions associated with this Rule. 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. Default: "-Select-"
	Value The value in the Diameter message that the Application Routing Rule uses to determine a match. The Value field is required when the Operator is "Equals", "Starts With", and "Ends With".	Format: text box or pulldown list • Destination-Realm and Origin-Realm: text box; case-insensitive string consisting of a list of labels

Field (* indicates required field)	Description	Data Input Notes
	The Value field is disabled for the Operators "Present", "Absent", and "Always True".	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 can be at most 63 characters long and a Realm cab be at most 255 characters long. • Destination-Host and Origin-Host (FQDN): text box; case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label can be at most 63 characters long and a FQDN can be at most 255 characters long. • Application-ID: pulldown list of configured Application Ids • Command-Code: pulldown list of configured Command Codes

Field (* indicates required field)	Description	Data Input Notes
		Range: One or more Parameters with Operator and Value for each Parameter Default for Application-Id and Command Code: "-Select-"
* Application Name	DSR Application Name associated with this Rule.	Format: pulldown list Range: All activated DSR Applications Default: "-Select-"

Application Routing Rule operators

Table 26: Application Routing Rules Operators describes the **Conditions** operators available for each parameter in a Application Routing Rule.

Table 26: 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

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
Command-Code	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
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

Viewing Application Routing Rules

The use of Application Routing Rules is described in *Application Routing Rules configuration*.

The fields are described in *Application Routing Rule configuration elements*.

To view currently configured Application Routing Rules in a selected Application Route Table,

1. Select **Diameter** > **Configuration** > **Application Route Tables**.

   The **Diameter > Configuration > Application Route Tables** page appears with a list of configured Application Route Tables.
2. Select an Application Route Table Name in the list.
3. Click **View/Edit Rules**.

   The **Viewing Rules for Application Route Table: {Application Route Table Name}** page opens, with a list of the Rules that are currently configured in the selected Application Route Table.

Adding an Application Routing Rule

Use this procedure to create a new Application Routing Rule in a selected Application Route Table. The fields are described in *Application Routing Rule configuration elements*.

1. Select **Diameter** > **Configuration** > **Application Route Tables**.

   The **Diameter > Configuration > Application Routie Tables** page appears.

2. Select an Application Route Table Name in the list.
3. Click **View/Edit Rules**.

   The **Viewing Rules for Application Route Table: {Application Route Table Name}** page appears.

4. Click **Insert**.

   The **Inserting Rule for Application Route Table: {Application Route Table Name}** page appears.

   If the maximum number of Application Routing Rules (1000) already exists in the system, the **Diameter > Configuration > Application Routing Rules [Insert]** page will not open.

5. Enter a unique name for the Rule in the **Rule Name** field.
6. Set a Priority for this Rule in relation to other Rules, by entering a number between 1 and 99 in the **Priority** field.
7. Set the Application Routing Rule **Conditions**:
   a) Locate the **Parameter** you want to set.
   b) Select the relevant operator from the **Operator** pulldown list.

      See *Application Routing Rule operators* for a description of operators available for each Parameter.

   c) Enter the appropriate value for the Parameter in the corresponding **Value** field.

      The **Value** text box is disabled for some Operators that do not require a value.

   d) Repeat this step for each Parameter. For any Parameter that does not need to be evaluated, set the **Operator** to **Always True**.
8. From the pulldown list, select the DSR **Application Name** associated with this Rule.
9. Click:

   - **OK** to save the Rule and return to the **Diameter > Configuration > Application Routing Rules** page.
   - **Apply** to save the Rule and remain on this page.
   - **Cancel** to return to the **Viewing Rules for Application Route Table: {Application Route Table Name}** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any required field is empty (no entry was made)
   - Any field is not valid or is out of range
   - The **Rule Name** is not unique
   - The Rule is similar to an already existing Rule (the same attributes except for Rule Name and Priority)
   - Adding the Application Routing Rule would cause the maximum number of Application Routing Rules (1000) allowed in the system to be exceeded

   For Application Route Tables that are associated with Application Ids, a warning appears for an attempt to add an Application Routing Rule with an Application-Id that does not match the Application Id with which the Application Route Table is associated.

Editing an Application Routing Rule

Use this task to edit an Application Routing Rule in a selected Application Route Table.

Note: The **Rule Name** field cannot be edited.

1. Select **Diameter** > **Configuration** > **Application Route Tables**.

   The **Diameter > Configuration > Application Routie Tables** page appears.

2. Select an Application Route Table Name in the list.
3. Click **View/Edit Rules**.

   The **Viewing Rules for Application Route Table: {Application Route Table Name}** page appears.

4. Select a Rule to edit.
5. Click **Edit**.

   The **Editing Rule for Application Route Table: {Application Route Table Name}** page appears.

6. Update the relevant fields.

   For more information about each field see *Application Routing Rule configuration elements* and *Application Routing Rule operators*.

7. Click:

   - **OK** to save the changes and return to the **Viewing Rules for Application Route Table: {Application Route Table Name}** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Viewing Rules for Application Route Table: {Application Route Table Name}** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The selected Application Routing Rule no longer exists; it has been deleted by another user
   - Any required field is empty (no entry was made)
   - Any field is not valid or is out of range
   - The Rule is similar to an already existing Rule (the same attributes except for Rule Name and Priority)

Deleting an Application Routing Rule

Use this task to delete an Application Routing Rule from a selected Application Route Table.

1. Select **Diameter** > **Configuration** > **Application Route Tables**.

   The **Diameter > Configuration > Application Route Tables** page appears with a list of configured Application Route Tables.

2. Select an Application Route Table Name in the list.
3. Click **View/Edit Rules**.

   The **Viewing Rules for Application Route Table: {Application Route Table Name}** page opens, with a list of the Rules that are currently configured in the selected Application Route Table.

4. Select the Application Routing Rule you want to delete, then click **Delete**.
   A popup window appears.

5. Perform one of the following actions:
   - Click **OK** to delete the Application Routing Rule.
   - Click **Cancel** to cancel the delete function and return to the **Viewing Rules for Application Route Table: {Application Route Table Name}** page.

   If **OK** is clicked and the selected Application Routing Rule no longer exists (it was deleted by another user), an error message is displayed and the Application Routing Rules view is refreshed.

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. The Default Routing Option Set cannot be deleted.

Routing Option Sets elements

Table 27: 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 27: Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Routing Option Set Name	Unique name of the Routing Option Set.	Format: text box; case-sensitive; alphanumeric and underscore Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha
* Maximum Per Message Forwarding Allowed	Maximum number of times an application is allowed to forward a Request message.	Format: text box; numeric Range: 1 - 5 Default: 1
Transaction Lifetime	The total time DSR allows to forward a Request, including initial and all subsequent routing attempts.	Format: text box; numeric Range: 100 - 540000 ms Default: 1000 ms
Pending Answer Timer	Pending Answer Timer of this Routing Option Set If the Pending Answer Timer value is "Not Selected", the egress Peer Node's associated Pending Answer Timer, if it is defined, will be used when processing transactions. A Pending Answer Timer cannot be assigned to the Default Routing Option Set.	Format: pulldown list Range: Default, configured Pending Answer Timers Default: "Not Selected."
* 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	Value to be placed in the Result-Code AVP of the Answer message. An Answer Result-Code value is required if Resource Exhausted Action is 'Send Answer'	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.

Field (* indicates required field)	Description	Data Input Notes
		Default: "3004 TOO_BUSY" in pulldown list
Resource Exhausted Answer Error Message	String to be placed in the Error-Message AVP of the Answer message for Resource Exhaustion	Format: text box; alphanumeric Range: 0 - 64 characters
Resource Exhausted Vendor Id	Resource Exhausted Vendor-Id Value. When specified, the Answer generated will be an Experimental-Result-Code grouped AVP with the specified Vendor-Id value placed in the Vendor-Id AVP.	Format: text box; numeric Range: 1 - 4294967295
* 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
No Peer Response Result-Code	Result-code value returned in an Answer message when a message is not successfully routed due to being abandoned or timing out This Result-Code value is required if if the No Peer Response Action is 'Send Answer'.	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 Error Message	String to be placed in the Error-Message AVP of the Answer message for No Peer Response	Format: text box; alphanumeric Range: 0 - 64 characters Default: Null string
No Peer Response Vendor Id	No Peer Response Vendor-Id value. When specified, the Answer generated will be an Experimental-Result-Code grouped AVP with the specified Vendor-Id value placed in the Vendor-Id AVP.	Format: numeric Range: 1 - 4294967295
* 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

Field (* indicates required field)	Description	Data Input Notes
		Default: Send Answer
Connection Failure Answer Result-Code	Value to be placed in the Result-Code AVP of the Answer message when a message is not successfully routed due to connection failure. An Answer Result-Code value is required if the Connection Failure Action is 'Send Answer'.	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	String to be placed in the Error-Message AVP of the Answer message for Connection Failure.	Format: text box; alphanumeric Range: 0 - 64 characters Default: Null string
Connection Failure Vendor Id	Vendor Id value returned in an Answer message when a message is not successfully routed due to connection failure. When specified, the Answer generated will be an Experimental-Result-Code grouped AVP with the specified Vendor-Id value placed in the Vendor-Id AVP.	Format: text box; numeric Range: 1 - 4294967295
* 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	Value to be placed in the Result-Code AVP of the 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	String to be placed in the Error-Message AVP of the Answer message for Connection congestion	Format: alphanumeric Range: 0 - 64 characters

Field (* indicates required field)	Description	Data Input Notes
		Default: Null string
Connection Congestion Vendor Id	Vendor Id value returned in an Answer message when a message is not successfully routed due to Connection congestion. When specified, the Answer generated will be an Experimental-Result-Code grouped AVP with the specified Vendor-Id value placed in the Vendor-Id AVP.	Format: numeric Range: 1 - 4294967295

Viewing Routing Option Sets

Use this task to view currently configured Routing Option Sets.

Select **Diameter** > **Configuration** > **Routing Option Sets**.
The **Diameter > Configuration > Routing Options Sets** page appears.

Adding a Routing Option Set

Use this task to create a new Routing Option Set. The fields are described in *Routing Option Sets elements*.

1. Select **Diameter** > **Configuration** > **Routing Option Sets**.
   The **Diameter > Configuration > Routing Option Sets** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Routing Option Sets [Insert]** page appears.
3. Enter a unique name for the Routing Option Set in the **Routing Option Set Name** field.
4. Enter or select the values for the Routing Option Set elements.
   Required elements are marked with a red asterisk (*).
5. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Routing Option Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Routing Option Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The **Routing Option Set Name** is not unique; it already exists in the system
   - The maximum number of Routing Option Sets (20) already exists in the system
   - The **Pending Answer Timer** value is greater than the Routing Option Set **Transaction Lifetime** value.

Editing a Routing Option Set

Use this task to make changes to existing Routing Option Sets.

The **Routing Option Set Name** cannot be changed.

1. Select **Diameter** > **Configuration** > **Routing Option Sets**.
   The **Diameter > Configuration > Routing Option Sets** page appears.
2. Select the **Routing Option Set** you want to edit.
3. Click **Edit**.

   The **Diameter > Configuration > Routing Option Sets [Edit]** page appears.

   The page is initially populated with the current configured values for the selected Routing Option Set.

4. Update the relevant fields.

   The fields are described in *Routing Option Sets elements*.

5. Click:

   - **OK** to save the changes and return to the **Diameter > Configuration > Routing Options Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Routing Option Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The selected **Routing Option Set** no longer exists (has been deleted by another user)
   - The **Pending Answer Timer** value is greater than the Routing Option Set **Transaction Lifetime** value.
   - A Pending Answer Timer is assigned to the Routing Option Set when the Routing Option Set has been assigned to an Application Id.

Deleting a Routing Option Set

Use this task to delete a Routing Option Set.

Note: A Routing Option Set cannot be deleted if any of the following conditions are true:

- The Routing Option Set is referenced by any Peer Node
- The Routing Option Set is referenced by any Application Id
- The Routing Option Set is the Default Routing Option Set

1. Select **Diameter** > **Configuration** > **Routing Option Sets**.
   The **Diameter > Configuration > Routing Option Sets** page appears.
2. Select the **Routing Option Set** you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.

4. Click:
   - **OK** to delete the Routing Option Set.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Routing Option Sets** page.

   If **OK** is clicked and the selected Routing Option Set no longer exists (it was deleted by another user), an error message is displayed and the Routing Option Sets view is refreshed.

Pending Answer Timers configuration

A Pending Answer Timer sets the amount of time the DSR waits for an Answer after sending a Request to a Peer Node.

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

A Pending Answer Timer can be associated with:

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

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

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

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

  Use Ingress Peer Node Routing Option Set Pending Answer Timer

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

  Use Egress Peer Node Pending Answer Timer

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

  Use Application-ID Pending Answer Timer

- Else

  Use the system Default Pending Answer Timer

The Diameter Routing Option Set provides an optional Pending Answer Timer element. If a configured Pending Answer Timer is specified in a Routing Option Set:

- Routing Option Set **Maximum per Message Forwarding Allowed** must be > 1
- Routing Option Set **Transaction Lifetime** must be greater than or equal to the value of the Pending Answer Timer specified for the Routing Option Set

The Routing Option Set **Transaction Lifetime** value controls the total time that Diameter will attempt to process a transaction, including re-routing attempts. Although the Routing Option Set can be

associated with an Ingress Peer Node, Diameter evaluates the Routing Option Set **Transaction Lifetime** for expiration only at re-routing attempts, which means:

- Transaction Lifetime is not applicable or configurable if the Routing Option Set has re-routing disabled (**Maximum per Message Forwarding Allowed** value is set to 1)
- Transaction Lifetime maybe extended by as much as 1 Pending Answer Timer interval in some cases

A Routing Option Set referenced by a Diameter Application-ID entry cannot have a Pending Answer Timer configured, because each Diameter Application-ID entry always has an associated Pending Answer Timer. The Default Pending Answer Timer is assigned to each Application Id if a configured Pending Answer Timer is not assigned.

Diameter selection of the **Pending Answer Timer** and **Transaction Lifetime** values to be used when routing Requests upstream will operate as indicated in *Table 28: Diameter Pending Answer Timer and Transaction Lifetime Selection*.

Table 28: Diameter Pending Answer Timer and Transaction Lifetime Selection

Routing Option Set specified in Ingress Peer Node?	Pending Answer Timer specified in Ingress Peer Node Routing Option Set?	Egress Pending Answer Timer specified in Egress Peer Node?	Application-ID entry exists for Appl-ID in Request being processed?	1. Resultant Pending Answer Timer value used 2. Resultant Transaction Lifetime value used (if re-routing is enabled in the Routing Option Set - Maximum Forward Routing Attempts value is greater than 1)
Yes	Yes	N/A	N/A	1. Pending Answer Timer in Ingress Peer Node Routing Option Set 2. Transaction Lifetime in Ingress Peer Node Routing Option Set
Yes	No	Yes	N/A	1. Egress Pending Answer Timer in Egress Peer Node 2. Transaction Lifetime in Ingress Peer Node Routing Option Set
Yes	No	No	Yes	1. Pending Answer Timer in Application-ID table entry for Request's Appl-ID 2. Transaction Lifetime in Ingress Peer Node Routing Option Set

Routing Option Set specified in Ingress Peer Node?	Pending Answer Timer specified in Ingress Peer Node Routing Option Set?	Egress Pending Answer Timer specified in Egress Peer Node?	Application-ID entry exists for Appl-ID in Request being processed?	1. Resultant Pending Answer Timer value used 2. Resultant Transaction Lifetime value used (if re-routing is enabled in the Routing Option Set - Maximum Forward Routing Attempts value is greater than 1)
Yes	No	No	No	1. System Default Pending Answer Timer 2. Transaction Lifetime in Ingress Peer Node Routing Option Set
No	N/A	Yes	Yes	1. Egress Pending Answer Timer in Egress Peer Node 2. Transaction Lifetime in Routing Option Set associated with configured Application-ID entry for Request's Appl-ID
No	N/A	Yes	No	1. Egress Pending Answer Timer in Egress Peer Node 2. Transaction Lifetime in system Default Routing Option Set
No	N/A	No	Yes	1. Pending Answer Timer in Application-ID table entry for Request's Appl-ID 2. Transaction Lifetime in Routing Option Set associated with Application-ID entry for Request's Appl-ID
No	N/A	No	No	1. System Default Pending Answer Timer 2. Transaction Lifetime in system Default Routing Option Set

The Diameter > Configuration > Pending Answer Timers page

On the **Diameter > Configuration > Pending Answer Timers** page, you can perform the following actions:

- Filter the list of Pending Answer Timers to display only the desired Pending Answer Timers.
- Sort the list by a column in ascending or descending order, by clicking the column heading. The default order is by **Pending Answer Timer Name** in ascending ASCII order.
- Click **Insert**.

  The **Diameter > Configuration > Pending Answer Timers [Insert]** page appears. You can add a new Pending Answer Timer.

  The **Diameter > Configuration > Pending Answer Timers [Insert]** page will not open if

  - The maximum number of Pending Answer Timers (8) already exists in the system.

- Select a Pending Answer Timer in the list, and click **Edit**.

  The **Diameter > Configuration > Pending Answer Timers [Edit]** page appears. You can edit the selected Pending Answer Timer.

  If the selected Pending Answer Timer has been deleted by another user, the **Diameter > Configuration > Pending Answer Timers [Edit]** page will not open.

- Select a Pending Answer Timer in the list, and click **Delete**. You can delete the selected Pending Answer Timer. You cannot delete the Default Pending Answer Timer.

Pending Answer Timers elements

Table 29: 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 29: 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 - 180000 ms Default: 1000 ms

Viewing Pending Answer Timers

Use this task to view currently configured Pending Answer Timers Sets.

Select **Diameter** > **Configuration** > **Pending Answer Timers**.
The **Diameter > Configuration > Pending Answer Timers** page appears.

Adding a Pending Answer Timer

Use this task to create a new Pending Answer Timer. The fields are described in *Pending Answer Timers elements*.

1. Select **Diameter** > **Configuration** > **Pending Answer Timers**.
   The **Diameter > Configuration > Pending Answer Timers** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Pending Answer Timers [Insert]** page appears.
3. Enter a unique name for the Pending Answer Timer in the **Pending Answer Timer Name** field.
4. Set the **Pending Answer Timer Value**.
5. Click:
   - **OK** to save the data and return to the **Diameter > Configuration > Pending Answer Timers** page .
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Pending Answer Timers** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The **Pending Answer Timer Name** is not unique; it already exists in the system
   - Adding the Pending Answer Timer would cause the maximum number of Pending Answer Timers (8) allowed in the system to be exceeded

Editing a Pending Answer Timer

Use this task to make changes to existing Pending Answer Timers.

The **Pending Answer Timer Name** cannot be changed.

1. Select **Diameter** > **Configuration** > **Pending Answer Timers**.
   The **Diameter > Configuration > Pending Answer Timers** page appears.
2. Select the **Pending Answer Timer** you want to edit.
3. Click **Edit**.

   The **Diameter > Configuration > Pending Answer Timers [Edit]** page appears.

   The page is initially populated with the current configured values for the selected Pending Answer Timer.
4. Update the relevant fields.

For more information about each field see *Pending Answer Timers elements*.

5. Click:

   - **OK** to save the changes and return to the **Diameter > Configuration > Pending Answer Timers** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Pending Answer Timers** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The selected **Pending Answer Timer** no longer exists (has been deleted by another user)
   - For a Pending Answer Timer that is assigned to a Routing Option Set, the **Pending Answer Timer** value is greater than the **Transaction Lifetime** value in the Routing Option Set.

Deleting a Pending Answer Timer

Use this task to delete a Pending Answer Timer.

Note: A Pending Answer Timer cannot be deleted if the Pending Answer Timer is referenced by any of the following components:

- Peer Node
- Application Id
- Routing Option Set

The Default Pending Answer Timer cannot be deleted.

1. Select **Diameter** > **Configuration** > **Pending Answer Timers**.
   The **Diameter > Configuration > Pending Answer Timers** page appears.
2. Select the **Pending Answer Timer** you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:

   - **OK** to delete the Pending Answer Timer.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Pending Answer Timers** page.

   If **OK** is clicked and the selected Pending Answer Timer no longer exists (it was deleted by another user), an error message is displayed and the Pending Answer Timers view is refreshed.

System Options configuration

Diameter System Options can be viewed and set on the **Diameter > Configuration > System Options** page.

The following System Options are described in *System Options elements*:

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

    Note: Options specific to Message Copy are configured in Message Copy Configuration Sets. See *Message Copy Configuration Set configuration*.

To open the **Diameter > Configuration > System Options** page, select **Diameter** > **Configuration** > **System Options**.

On the **Diameter > Configuration > System Options** page, you can:

- Modify current System Options values, and click **Apply** to save the changes.
- Click **Cancel** to remove and not save any changes you have made.
- Click the **General Options**, **Alarm Threshold Options**, or **Message Copy Options** tab to access those options.

If **Apply** is clicked and the following condition exists, an error message is displayed:

- Any field has no value entered or has an entry that is not valid

System Options elements

Table 30: System Options Elements describes the fields on the System Options page.

Table 30: 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 - 30000 Default: 8192
Per Connection Egress Message Throttling Enabled	Controls whether Connections use Egress Message Throttling Configuration Sets to set congestion levels.	Format: checkbox Range: Checked (Enabled), Not checked (Disabled

Field	Description	Data Input Notes
		Default: Checked (Enabled)
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 View-Only; it cannot be user-configured.	Format: numeric percentage Range: 30-100 Default: 50%
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 Available 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 Available Alarm Budget.	Format: numeric Range: 0 to Available Alarm Budget Default: 100
Peer Node Failure Critical Aggregation Alarm Threshold	Critical threshold for aggregated Peer Node Failure alarms per NE. The Available Alarm Budgets decremented by this value	Format: numeric Range: 1 to Available Alarm Budget Default: 600

Field	Description	Data Input Notes
Route List Failure Critical Aggregation Alarm Threshold	Critical threshold for aggregated Route List Failure alarms per NE. The Available Alarm Budget is decremented by this value	Format: numeric Range: 1 to Available Alarm Budget Default: 600
Message Copy Options		
Message Copy Feature	Enables the Message Copy Feature system wide if this option is enabled.	Format: radio button Range: Enabled. Disabled Default: Disabled
MP Congestion Level	The MP congestion at or above which the Message Copy function is disabled.	Format: radio button Range: CL1, CL2 Default: CL1

DNS Options configuration

The 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.

To open the **Diameter > Configuration > DNS Options** page, select **Diameter** > **Configuration** > **DNS Options**.

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

On the **Diameter > Configuration > DNS Options** page, you can set the DNS Options values and click:

- **Apply** to save the changes
- **Cancel** to remove and not save any changes

If **Apply** is clicked and any of the following conditions exist, an error message appears:

- The DNS Query Duration Timer field has no value
- The DNS Query Duration Timer value is not valid
- The Primary or Secondary DNS Server IP Address field value is not valid
- The Secondary DNS Server IP Address field has a value, but the Primary DNS Server IP Address field is blank
- The Primary DNS Server IP Address field is blank and there is at least one Initiator Connection without a Peer IP Address

DNS Options elements

Table 31: DNS Options Elements describes the fields on the **Diameter > Configuration > DNS Options** page.

Table 31: 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

Topology Hiding configuration

The following components can be configured for Diameter Topology Hiding:

- Trusted Network Lists
- Path Topology Hiding Configuration Sets
- S6a/S6d HSS Topology Hiding Configuration Sets
- MME/SGSN Topology Hiding Configuration Sets
- Protected Networks

Diameter Topology Hiding

Diameter messages contain sensitive information such as addresses of entities from a Diameter Network or the number of such entities. Therefore, an operator may choose to hide this information in order to minimize the risk of attacks and to be able to perform changes to the internal network at will.

Topology Hiding (TH) is based upon the relationships between Diameter Networks. A Diameter Network is identified by a Realm. The Diameter Network from which a message was initiated is defined in its Origin-Realm AVP. The intended Diameter Network destination of the message is defined in its Destination-Realm AVP. Both of these AVPs are mandatory parameters in all Diameter messages.

For the purpose of discussing network relationships, a network can be defined as one of the following types:

- Protected Network - A network whose topology information must be protected when messages are exchanged with Untrusted Networks. A network trust/untrust relationship is always viewed from the perspective of a Protected Network. For example, if Networks "N1" and "N2" are Protected

Networks, it's perfectly acceptable for Network "N1" to trust Network "N2" while Network "N2" does not trust Network "N1". If this asymmetric relationship exists, then the topology information of N1 will not be protected from N2 but the topology information of N2 will be protected from N1.

- Trusted Network - A network that a particular Protected Network trusts; no information from that Protected Network will be hidden or modified when forwarded to a Trusted Network.
- Untrusted Network - A network that a particular Protected Network does not trust; topology-related information from that Protected Network will be hidden or modified when forwarded to an Untrusted Network.

Topology Hiding involves hiding topology-related information in messages sent from a Protected Network to an Untrusted Network, as well as restoring the topology-related information in messages from an Untrusted Network. The restoral process can occur during the same Diameter transaction or can occur on subsequent unrelated Diameter transactions. The following Topology Hiding techniques are supported:

- Topology information hiding
  - Host identity hiding - Hiding the identity of any host (embedded in a Diameter message) that is a member of a Protected Network when a message is originated by any Diameter node in a Protected Network to any Diameter node that is a member of a network that is Untrusted by that Protected Network.

    Techniques for address hiding include encryption and replacing an Actual Hostname with a Pseudo Hostname.

  - Number of Hosts hiding - A method that prevents the Untrusted Network from deducing how many hosts are members of a Protected Network based upon the content of messages that the Untrusted Network receives from the Protected Network.

    Techniques for Number of Hosts hiding include replacing Protected Network host names with a single Pseudo Hostname for the Protected Network, and replacing Protected Network host names with randomly generated Pseudo Hostnames.

    The second technique is used when a message sent from the Untrusted Network to the Protected Network contains one or more Pseudo Hostnames that must be mapped back to the Actual Hostnames for purposes such as message routing. Mapping of Pseudo-to-Actual Hostnames may occur during a transaction Request/Answer message exchange or may need subsequent Untrusted Network initiated transactions to the Protected Network.

- Topology information restoral - When an Actual Hostname is replaced by a Pseudo Hostname, it is many times necessary to replace the Pseudo Hostname with the Actual Hostname in the following cases:
  - When an Answer message response for a Diameter transaction is returned from the Untrusted Network

    A Diameter node that is receiving the Answer response associated with a Diameter transaction for which Topology Hiding occurred is expecting to see the Actual Hostname, not a Pseudo Hostname, in the Answer message.

  - When a new Diameter transaction is initiated from the Untrusted Network to the Protected Network

    An Untrusted Network node may actually save the Pseudo Hostname received in a transaction for use in subsequent transactions to the Protected Network. This can occur, for example, for Untrusted-HSS to Protected-MME/SGSN transactions whereby the Untrusted-HSS saves the

MME/SGSN's host name when it initiates subsequent Diameter transactions (such as CLR) to that MME/SGSN.

The need to replace a Pseudo Hostname with an Actual Hostname in subsequent Untrusted-to-Protected Network transactions is required for routing purposes, and is required when the destination host in the Protected Network requires that messages sent to it contain its Actual Hostname.

Diameter Edge Agent (DEA) Topology Hiding procedures are always invoked on the interface closest to an Untrusted Network, as illustrated in *Figure 2: Diameter Topology Hiding Boundary*.

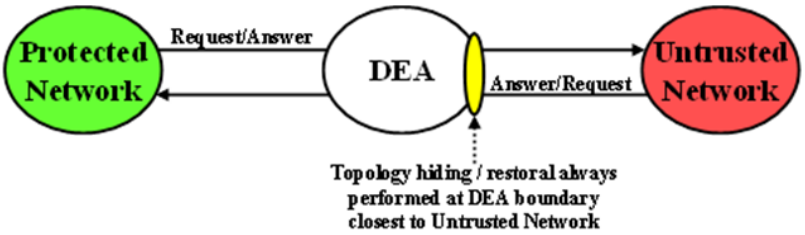

Figure 2: Diameter Topology Hiding Boundary

Topology Hiding Trigger Points

Diameter Topology Hiding is performed at well-known locations within the Diameter Routing Function software, on both Protected-to-Untrusted Diameter transactions and Untrusted-to-Protected Diameter transactions. These well-known locations are referred to as Topology Hiding (TH) Trigger Points. Two types of TH Trigger Points are defined:

- Information hiding Trigger Point: A TH Trigger Point that, when invoked, attempts to hide any topology related-information within a Diameter message that is being sent to an Untrusted Network. This type of TH Trigger Point is identified by the "TH" suffix in the Trigger Point name.
- Information restoral Trigger Point: A TH Trigger Point that, when invoked, attempts to restore any topology hidden information within a Diameter message received from an Untrusted Network to its original or actual value. This type of TH Trigger Point is identified by the "TR" suffix (Topology Restoral) in the Trigger Point name.

For Protected-to-Untrusted Network Diameter transactions, any topology-sensitive information in the Protected-to-Untrusted Network Request message is hidden just prior to forwarding the Request message to a Peer Node that serves as a gateway to the Untrusted Network. (The adjacent Peer Node may be a member of a Untrusted Network or may be connected directly or indirectly to Diameter nodes that are members of an Untrusted Network from the Protected Network's perspective.)

For the purposes of Diameter Routing Function transaction processing, the Trigger Point for evaluating whether topology-related information should be hidden is called Request Topology Hiding (RTH).

When the Diameter Edge Agent (DEA) receives an Answer message associated with a Protected-to-Untrusted Diameter transaction, it must consider whether the Answer message contains any hidden topology-related information that must be restored to its original value. This Trigger Point is called Answer Topology Restoral (ATR).

The high level logical locations of the RTH and ATR TH Trigger Points for Protected-to-Untrusted Network Diameter transactions are shown in *Figure 3: Diameter Topology Hiding Trigger Points: Protected-to-Untrusted Transactions*.

Figure 3: Diameter Topology Hiding Trigger Points: Protected-to-Untrusted Transactions

For Untrusted-to-Protected Network Diameter transactions, any topology-hidden information embedded in the Untrusted-to-Protected Network Request message may be a candidate for topology information restoral. The Trigger Point for evaluating whether topology-related information in a Request message should be restored is called Request Topology Restoral (RTR).

When the DEA forwards an Answer message to an Untrusted Network, it must consider whether the Answer message contains any topology-sensitive information about the Protected Network. This Trigger Point is called Answer Topology Hiding (ATH).

The high level logical locations of the RTR and ATH TH Trigger Points for Untrusted-to-Protected Diameter transactions are shown in *Figure 4: Diameter Topology Hiding Trigger Points: Untrusted-to-Protected Transactions*.

Figure 4: Diameter Topology Hiding Trigger Points: Untrusted-to-Protected Transactions

All Diameter Topology Hiding Trigger Points are adjacent to the existing Diameter Mediation Trigger Points. The following Topology Hiding-Mediation relationship rules apply:

- Information hiding Trigger Points - immediately prior to Mediation
- Information restoral Trigger Points: immediately after Mediation

The Diameter Routing Function has the ability to edit messages just prior to forwarding them to Peer Nodes. Any Diameter Routing Function message editing must be performed prior to any TH treatment. For example, a DSR Application, when forwarding a Request message to the Diameter Routing Function, can ask the Diameter Routing Function to replace the Origin-Realm and Origin-Host AVP values with the Realm and FQDN values assigned to the Local Node associated with the egress Diameter Connection just prior to forwarding the message to the Diameter Transport Function. This Origin-Realm/Origin-Host AVP replacement function must be performed before the TH Trigger Point.

Table 32: Topology Information Hiding and Restoral Procedures summaries the topology information hiding and restoral procedures that are supported at each TH Trigger Point.

Table 32: Topology Information Hiding and Restoral Procedures

Trigger	TH Type	AVP	Information Hiding / Restoral Procedure
RTH	Path	Route-Record	All AVPs containing Protected Network host names are replaced with a single AVP containing a Pseudo Hostname assigned to the Protected Network.

Trigger	TH Type	AVP	Information Hiding / Restoral Procedure
		Proxy-Host	Each AVP containing Protected Network host names is replaced with a unique AVP Pseudo Hostname.
	HSS	Origin-Host	Replaced the AVP value with the single HSS Pseudo Hostname assigned to the Protected Network
		Session-Id	Host portion replaced by the single HSS Pseudo Hostname assigned to the Protected Network.
	MME/SGSN	Origin-Host	Replaced by one of the Pseudo Hostnames assigned to the MME/SGSN.
		Session-Id	Host portion of this AVP value replaced by one of the Pseudo Hostnames assigned to the MME/SGSN
RTR	Path	Route-Record	Message loop detection and rejection if a Route-Record AVP contains a pseudo-name that is assigned to the Protected Network that initiated the message. Note: Message Loop Detection is done at a Loop Detect point just prior to RTR.
	HSS	None; HSS Pseudo Hostname to Actual Hostname restoral is performed by a HSS Address Resolution application like DSR's FABR or RBAR.	N/A
	MME/SGSN	Destination-Host	Replace the MME/SGSN Pseudo Hostname with the MME/SGSN's Actual Hostname.
ATH	Path	Route-Record	All AVPs containing Protected Network host names are replaced with a single AVP containing a Pseudo Hostname assigned to the Protected Network.
		Error-Reporting-Host	For each AVP containing a Protected Network host name, encrypt the value using the encryption key assigned to the Protected Network.
	HSS	Origin-Host	Replace the HSS host name with the single HSS Pseudo Hostname assigned to the Protected Network.

Trigger	TH Type	AVP	Information Hiding / Restoral Procedure
	MME/SGSN	Origin-Host	Replace the MME/SGSN host name with one of the MME/SGSN's Pseudo Hostnames based on content of the User-Name AVP (containing an IMSI).
ATR	Path	Proxy-Host	Each AVP instance that was hidden in the forwarded in the Request message must be restored to its original value that is stored in the PTR
	HSS	Session-Id	Restore the HSS's host name received in the Request Session-Id AVP that is stored in the PTR.
	MME/SGSN	Session-Id	Restore the HSS's host name received in the Request Session-Id AVP that is stored in the PTR.

Message Candidates for Topology Hiding and Restoral

Topology Hiding and Restoral Trigger Points are located at the DEA's boundary to an Untrusted Network. Thus, to even consider whether a message is a potential candidate for Topology Hiding and Restoral, the Diameter Routing Function must know the following information at those TH Trigger Points:

- Is the message that was just received (or about to be sent) a potential Topology Hiding and Restoral candidate?
- If the message is a potential candidate, is this a message between a Protected Network and an Untrusted Network?

To facilitate potential candidates, the Peer Node configuration element called **Topology Hiding Status** must be set to Enabled on any Peer Node that is associated with at least one Untrusted Network.

The trust/untrust relationship is always from the perspective of the Protected Network. The use of the following Diameter Configuration Topology Hiding components and the Peer Node component is illustrated in the example in *Figure 5: TH Network Deployment with DSR in an Interworking Network*:

- **Protected Networks**: Defines, for each Protected Network, the Protected Realm Name and an optional reference to a Trusted Network List. The assumption is that all networks are Untrusted to a Protected Network unless they appear in a Trusted Network List that is assigned to that Protected Network. In essence, the Trusted Network List is a white list; any Network Realm Name that is not in that list is an Untrusted Network. If a Protected Network is not assigned a Trusted Network List, then it is assumed that all networks (except itself) are Untrusted.
- **Trusted Network List**: A list of Trusted Network Realm Names. A Trusted Network List can be assigned to any Protected Network.

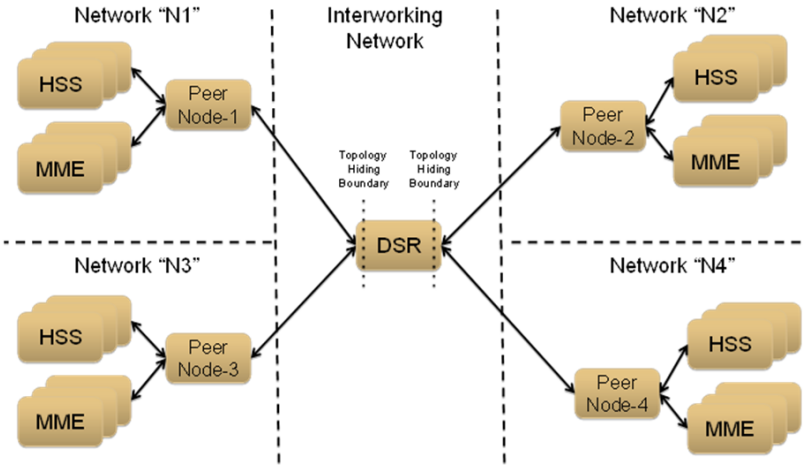

Figure 5: TH Network Deployment with DSR in an Interworking Network

For the sake of discussion, assume that all of the networks are Protected Networks and the Protected Networks and Trusted Network Lists shown in *Table 33: Example Protected Networks Configuration* and *Table 34: Example Trusted Network Lists Configuration* are configured:

Table 33: Example Protected Networks Configuration

Protected Network Name	Protected Network Realm Name	Trusted Network List Name
N1	n1.com	Trusted Networks-1
N2	n2.com	Trusted Networks-2
N3	n3.com	Trusted Networks-3
N4	n4.com	Trusted Networks-4

Table 34: Example Trusted Network Lists Configuration

Protected Network Name	Network Realm List
Trusted Networks-1	n3.com
Trusted Networks-2	n3.com n4.com
Trusted Networks-3	n2.com
Trusted Networks-4	n1.com n2.com n3.com

Based on the example Protected Networks and Trusted Network Lists, the "trust" relationship matrix among the four networks in this example configuration is shown in *Table 35: Network Trust Relationship Matrix*.

Table 35: Network Trust Relationship Matrix

Protected Network	Relationship with Peer Network			
	N1	N2	N3	N4
N1	Trusted	Not Trusted	Trusted	Not Trusted
N2	Not Trusted	Trusted	Trusted	Trusted
N3	Not Trusted	Trusted	Trusted	Not Trusted
N4	Trusted	Trusted	Trusted	Trusted
Is this network Untrusted by at least one other network?	***Yes***	***Yes***	***No***	***Yes***

Based on the Network Trust Relationship Matrix, the Peer Node element settings for the network shown in *Table 36: Example Topology Hiding Status Settings* would be used:

Table 36: Example Topology Hiding Status Settings

Peer Node	Topology Hiding Status Element Setting
Peer Node-1	Enabled
Peer Node-2	Enabled
Peer Node-3	Disabled
Peer Node-4	Enabled

With the information in *Table 36: Example Topology Hiding Status Settings*, the TH type-independent criteria for determining whether a message is a potential candidate for Topology Hiding/Restoral are defined in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*.

Table 37: General Criteria for Determining Whether a Message is a TH Candidate

TH Trigger	Message	Message Path	General Topology Hiding/Restoral Candidate Criteria
RTH	Request	Protected-to-Untrusted	Egress Peer Node Topology Hiding Status is Enabled, AND Origin-Realm is a Protected Network X, AND Destination-Realm is an Untrusted Network to Protected Network X
RTR	Request	Untrusted-to-Protected	Ingress Peer Node Topology Hiding Status is Enabled, AND

TH Trigger	Message	Message Path	General Topology Hiding/Restoral Candidate Criteria
			Destination-Realm is a Protected Network X, AND Origin-Realm is an Untrusted Network to Protected Network X
ATH	Answer	Protected-to-Untrusted	Egress Peer Node Topology Hiding Status is Enabled, AND Origin-Realm is a Protected Network X, AND Realm of the Diameter Node that originated the transaction is an Untrusted Network to Protected Network X TH Trigger point ATH occurs after the Diameter Routing Function deallocates the PTR for the transaction. Therefore, the Origin-Realm value that was received in the Request message must be stored in the Application-Data stack event just prior to deallocating the PTR in order for the Diameter Routing Function to make an evaluation at ATH of whether the Answer response is being sent to an Untrusted Network.
ATR	Answer	Untrusted-to-Protected	PTR contains one or more indications that topology information restoral is required For Untrusted-to-Protected Answer messages, any information that was hidden in the egress Request is a candidate for restoral regardless of which "Network" sends the Answer message response. Topology information restoral at ATR is always performed regardless of the egress Peer Node's Topology Hiding Status if Topology Hiding was performed on the egress Request message for this Diameter transaction.

If the TH Trigger Point criteria defined in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate* are met, then the Diameter Routing Function must determine which TH types are enabled for the associated Protected Network. Each TH type might have additional criteria that must be met in order to determine whether topology-related information hiding or restoral is required.

The Protected Networks configuration component defines which TH types are enabled for the Protected Network. If a Configuration Set for the TH type is assigned to the Protected Network, then that TH type is enabled for that Protected Network and the rules for that TH type are applied. The Path, S6a/S6d HSS, and MME/SGSN TH types are supported. An example Protected Network component

for the use case network defined in this section could look like the configuration in *Table 38: Protected Network Configuration Example*:

Table 38: Protected Network Configuration Example

Protected Network Name	Protected Network Realm Name	Trusted Network List Name	Path TH	S6a/S6d HSS TH	MME/SGSN TH
N1	n1.com	Trusted Networks-1	Path Config Set-1	S6a/S6d HSS Config Set-1	MME/SGSN Config Set-1
N2	n2.com	Trusted Networks-2	Path Config Set-2	S6a/S6d HSS Config Set-1	MME/SGSN Config Set-1
N3	n3.com	Trusted Networks-3	Path Config Set-3	NULL	NULL
N4	n4.com	Trusted Networks-4	Path Config Set-4	NULL	NULL

In the example, if a message associated with Protected Network N3 is a candidate for topology hiding/restoral, then the Diameter Routing Function will invoke only the Path Topology Hiding Configuration Set rules for that message.

The TH type-specific Hiding/Restoral rules are defined in *Topology Hiding Types*.

Supported AVPs

Table 39: Topology Hiding AVPs and Hiding Methods shows the AVPs that are supported by Topology Hiding. The following information hiding methods are supported:

- Pseudo Hostname Replacement: Actual Hostnames are replaced with Pseudo Hostnames.
- Encryption: AVP value is encrypted

Table 39: Topology Hiding AVPs and Hiding Methods

Diameter Applications	AVP Name	Information Hiding Method	
		Pseudo-Host Name Replacement	Encryption
S6a, S6d	Session-Id	X	
S6a, S6d	Origin-Host	X	
Any	Route-Record	X	
Any	Proxy-Host	X	
Any	Error-Reporting-Host		X

Encryption

Any encryption required by Topology Hiding uses Advanced Encryption Standard (AES), which is a specification for the encryption of electronic data established by the U.S. National Institute of

Standards and Technology (NIST) in 2001. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) that was published in 1977.

AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits (with 256 being the hardest to crack), and encrypts and decrypts data in blocks of 128 bits (16 bytes). Unlike public-key ciphers that use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by block ciphers have the same number of bits that the input data had. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of the input data. All three key lengths are sufficient to protect classified information up to the SECRET level.

AES must be used in conjunction with a FIPS (Federal Information Processing Standard) approved or NIST recommended mode of operation. The mode specifies how data will be encrypted (cryptographically protected) and decrypted (returned to original form). Diameter Topology Hiding supports AES-Cipher BlockChaining (CBC) mode and a 128-bit key size.

Note: If assistance is needed in troubleshooting encrypted Error-Reporting-Host AVPs, contact your *Customer Care Center*. You will need the Encryption Key that is configured in the **Diameter > Configuration > Topology > Path Topology Configuration Set** GUI page.

Assumptions

Diameter Topology Hiding has the following assumptions:

- In order to detect message looping for Request messages containing a Route-Record Pseudo Hostname, all Diameter Edge Agents in the service provider's network must have the same Topology Hiding configuration.
- A message loop for Request messages containing a Route-Record Pseudo Hostname may not be detected for messages returned to any Diameter Edge Agent from any network that is trusted by the Protected Network that initiated the Diameter transaction.

Topology Hiding Types

Topology Hiding can be a Diameter application-specific or Diameter application-independent procedure.

- Topology Hiding is Diameter application-specific if the rules apply only to a Diameter application-specific message set (such as S6a).
- Topology Hiding is Diameter application-independent if the rules apply to any Diameter message (any Command Code).

The information to be hidden can be controlled based upon the following Topology Hiding types:

- S6a/S6d Topology Hiding

  S6a/S6d Topology Hiding is applied only to the S6a/S6d Command Codes defined in 3GPP TS 29.272, "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol", and requires knowing which S6a/S6d messages are HSS-initiated versus MME/SGSN-initiated.

  - S6a/S6d HSS Topology Hiding

    S6a/S6d HSS Topology Hiding is concerned with hiding the identity(s) of a Protected Network's HSS when it exchanges messages with Untrusted Networks. An HSS's Hostname is embedded in the Origin-Host and Session-Id AVPs sent in Request messages and in the Origin-Host AVP sent in Answer messages.

S6a/S6d HSS Topology Hiding determines which entity (HSS or MME/SGSN) initiated a message, based on the Command Code in the message.

S6a/S6d HSS Topology Hiding can be enabled for each Protected Network, by assigning an S6a/S6d HSS Topology Hiding Configuration Set to the configured Protected Network.

- MME/SGSN Topology Hiding

  MME/SGSN Topology Hiding is concerned with hiding the identity of a Protected Home Network's MME/SGSNs, as well as the number of MME/SGSNs in the network, when it exchanges messages with Untrusted Networks. A MME/SGSN's identity is embedded in the Origin-Host and Session-Id AVPs sent in Request messages and in the Origin-Host AVP sent in Answer messages.

  MME/SGSN Topology Hiding determines which entity (HSS or MME/SGSN) initiated an S6a/S6d message, based on the Command Code in the message.

  MME/SGSN Topology Hiding can be enabled for each Protected Network, by assigning an MME/SGSN Topology Hiding Configuration Set to the configured Protected Network.

- Path Topology Hiding

  Path Topology Hiding is Diameter application-independent, and can be applied to any Diameter Command Code.

  Path Topology Hiding is concerned with hiding a Protected Network's Hostnames and the number of hosts in the following AVPs:

  - Route-Record AVP: Sent in Request messages. More than one Route-Record AVP can exist in a Request message.
  - Proxy-Host AVP: An AVP embedded in the grouped Proxy-Info AVP that is sent in Request and Answer messages. More than one Proxy-Host AVP can exist in a message.
  - Error-Reporting-Host AVP: Sent in Answer messages. More than one Error-Reporting-Host AVP can exist in an Answer message.

  Path Topology Hiding can be enabled for each Protected Network, by assigning a Path Topology Hiding Configuration Set to the configured Protected Network.

S6a/S6d HSS Topology Hiding

S6a/S6d HSS Topology Hiding is concerned with hiding the identities of a Protected Network's HSS when it exchanges messages with Untrusted Networks. An HSS's host name is embedded in the Origin-Host and Session-Id AVPs sent in Request messages and the Origin-Host AVP sent in Answer messages. This capability is associated with the Diameter S6a/S6d application message set defined in 3GPP TS 29.272, "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

S6a/S6d HSS Topology Hiding determines which entity (HSS or MME/SGSN) initiated a message based on the Command Code in the message.

HSS identities are hidden by replacing the Hostname portion of the Origin-Host and Session-Id AVPs (Session-Id format: <host name><implementation portion>) with an operator-defined HSS Pseudo Hostname that is assigned to the Protected Network in the S6a/S6d HSS Topology Hiding Configuration Set.

Protected-HSS to Untrusted-MME/SGSN Transactions

For Protected-HSS to Untrusted-MME/SGSN Diameter transactions, S6a/S6d HSS Topology Hiding is concerned with the following topology information hiding and restoral issues:

- The AVPs containing an HSS's Actual Hostname in Request messages must be hidden with the single HSS Pseudo Hostname assigned to the Protected Network at TH Trigger Point RTH.
- The MME/SGSN will send an Answer response to the transaction with the Session-Id received in the Request (which also contains an HSS Pseudo Hostname). Because the Session-Id value returned in the Answer must match the value sent in the Request, the HSS Pseudo Hostnames in the Answer message Session-Id AVP must be restored with the HSS Hostname or Hostnames sent in the Request message.

  The Session-Id AVP values are restored at TH Trigger Point ATR, from the Hostname portion of the Session-Id AVP value that is saved in the Pending Transaction Record (PTR).

  The Hostname restoral procedure is not required for Answers initiated by DSR internal nodes (Diameter Routing Function and DSR Applications) as these Answer responses are based upon the original Request message content and thus do not contain Pseudo Hostnames.

An example of a Protected-HSS to Untrusted-MME/SGSN Diameter transaction is shown in *Figure 6: S6a/S6d HSS TH Protected-HSS to Untrusted-MME/SGSN Diameter Transaction*.

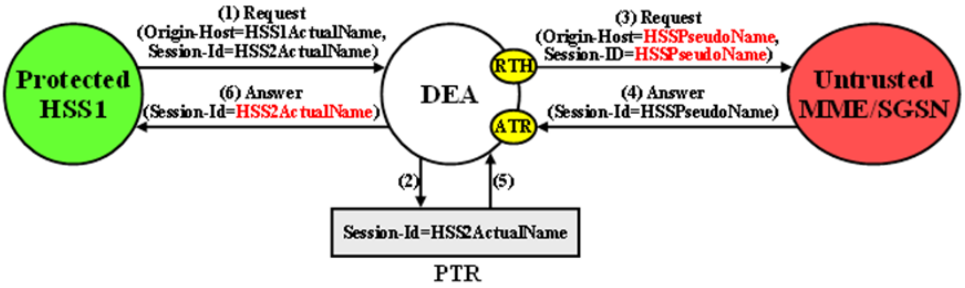

Figure 6: S6a/S6d HSS TH Protected-HSS to Untrusted-MME/SGSN Diameter Transaction

For Protected-HSS to Untrusted-MME/SGSN transactions, S6a/S6d HSS topology information hiding is required only on Request messages that meet the following criteria:

- Message was a candidate for Topology Hiding as defined by TH Trigger Point RTH in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- S6a/S6d HSS Topology Hiding is enabled for the Protected Network (an S6a/S6d HSS Topology Hiding Configuration Set is assigned to the Protected Network)
- The Request message is a member of the S6a/S6d message set and was initiated by an HSS as determined from the Command Code in the message

For Protected-HSS to Untrusted-MME/SGSN transactions, S6a/S6d HSS topology information hiding is performed only on Answer messages that meet the following criterion:

- At TH Trigger Point ATR, the "S6a/S6d HSS TH ATR" flag in the PTR associated with the Answer message is set to "Enabled".

When the above criterion is met, Session-Id AVP restoral will be performed using the HSS's Actual Hostname stored in the PTR.

Untrusted-MME/SGSN to Protected-HSS Transactions

For Untrusted-MME/SGSN to Protected-HSS Diameter transactions, S6a/S6d HSS TH is concerned with the following topology information hiding and restoral issue:

- The HSS-initiated Answer response will contain an HSS Actual Hostname in the Origin-Host AVP. The Actual Hostname must be hidden with the HSS Pseudo Hostname or Hostnames assigned to the Protected Network at TH Trigger Point ATH.

Restoral of a Protected-HSS's Actual Hostname in the Untrusted-MME/SGSN to Protected-HSS Request message is not performed by Topology Hiding. Instead, this replacement function is required of an HSS Address Resolution application such as the FABR and RBAR DSR Applications.

For Untrusted-MME/SGSN to Protected-HSS transactions, S6a/S6d HSS topology information hiding is required only on Answer messages that meet the following criteria:

- Message was a candidate for Topology Hiding as defined by topology Trigger Point ATH in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- S6a/S6d HSS Topology Hiding is enabled for the Protected Network (an S6a/S6d HSS Topology Hiding Configuration Set is assigned to the Protected Network)
- The Answer message is a member of the S6a/S6d message set and was initiated by an HSS as determined from the Command Code in the message

An example of an Untrusted-MME/SGSN to Protected-HSS Diameter transaction is shown in *Figure 7: S6a/S6d HSS TH Untrusted-MME/SGSN to Protected-HSS Transaction*.

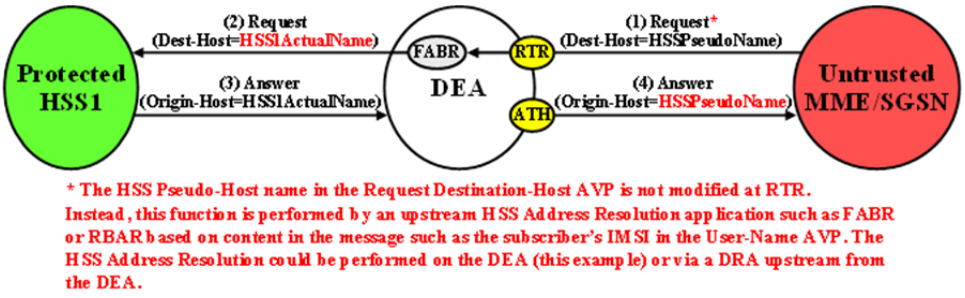

Figure 7: S6a/S6d HSS TH Untrusted-MME/SGSN to Protected-HSS Transaction

MME/SGSN Topology Hiding

MME/SGSN Topology Hiding is concerned with hiding the identity of a Protected Home Network's MME/SGSNs and the number of MME/SGSNs in the network, when it exchanges messages with Untrusted Networks. A MME/SGSN's identity is embedded in the Origin-Host and Session-Id AVPs sent in Request messages and in the Origin-Host AVP sent in Answer messages. MME/SGSN Topology Hiding is associated with the Diameter S6a/S6d application message set defined in 3GPP TS 29.272, "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

MME/SGSN Topology Hiding determines which entity (HSS or MME/SGSN) initiated an S6a/S6d message based on the Command Code in the message.

MME/SGSN identities are hidden by replacing the Actual Hostname portion of the Origin-Host and Session-Id AVPs (Session-Id format: <host name><implementation portion>) with an MME/SGSN Pseudo Hostname. The Origin-Host and Session-Id AVPs can have different MME/SGSN Hostnames. A unique Pseudo Hostname must be created for each MME/SGSN in a Protected Network. When the MME/SGSN initiates a transaction to the HSS, the HSS saves the MME/SGSN's identity for use in

subsequent HSS-to-MME/SGSN transactions. This MME/SGSN Pseudo Hostname must not only be unique, but the DEA must be able to convert the MME/SGSN's Pseudo Hostname to an Actual MME/SGSN Hostname for these subsequent HSS-to-MME/SGSN transactions.

In order to hide the number of MME/SGSNs in a network, each MME/SGSN will be assigned either a random or fixed number of Pseudo Hostnames. A maximum number is defined by the Count in the **Pseudo Hostname Generation** attribute of the MME/SGSN Topology Hiding Configuration Set. The Randomize Count creates a random number of Pseudo Hostnames, between 1 and the Count value, that are associated with an Actual Hostname. This procedure of creating randomized MME/SGSN Pseudo Hostnames and assigning them to an Actual Pseudo Hostname is performed by the GUI, then used by the Diameter Routing Function. The created MME/SGSN TH Hostnames allow the Diameter Routing Function to map a Protected-MME/SGSN Actual Hostname to a set of MME/SGSN Pseudo Hostnames, and to map a MME/SGSN Pseudo Hostname received from an Untrusted-HSS to a Protected-MME/SGSN Actual Hostname.

Table 40: Example of Configuration of MME/SGSN TH Hostnames for a Protected Network shows an example of MME/SGSN TH Host Names configuration for a Protected Network with a maximum of 3 randomly created Pseudo Hostnames.

Table 40: Example of Configuration of MME/SGSN TH Hostnames for a Protected Network

MME/SGSN TH Configuration Set Name	MME/SGSN Actual Hostname	MME/SGSN Pseudo Hostnames
Protected Network-1 MME/SGSN Config	mme1.westregion.example.com	mme042.example.com mme821.example.com
Protected Network-1 MME/SGSN Config	mme1.westregion.example.com	mme123.example.com
Protected Network-1 MME/SGSN Config	mme2.westregion.example.com	mme533.example.com mme773.example.com mme092.example.com
Protected Network-1 MME/SGSN Config	mme1.eastregion.example.com	mme922.example.com mme729.example.com
Protected Network-1 MME/SGSN Config	mme2.eastregion.example.com	mme411.example.com mme002.example.com mme655.example.com
Protected Network-1 MME/SGSN Config	mme2.eastregion.example.com	mme218.example.com
Protected Network-1 MME/SGSN Config	mme2.eastregion.example.com	mme331.example.com mme249.example.com mme447.example.com
Protected Network-1 MME/SGSN Config	mme1.texasregion.example.com	mme776.example.com

MME/SGSN TH Configuration Set Name	MME/SGSN Actual Hostname	MME/SGSN Pseudo Hostnames
		mme077.example.com
Protected Network-1 MME/SGSN Config	mme1.texasregion.example.com	mme295.example.com mme622.example.com mme861.example.com
Protected Network-1 MME/SGSN Config	mme1.texasregion.example.com	mme333.example.com

Protected-MME/SGSN to Untrusted-HSS Transactions

For Protected-MME/SGSN to Untrusted-HSS Diameter transactions, MME/SGSN Topology Hiding is concerned with the following topology information hiding and restoral issues:

- The AVPs containing an MME/SGSN's Actual Hostname in Request messages must be hidden with one of the Pseudo Hostnames assigned to the MME/SGSN at TH Trigger Point RTH.
- The HSS saves the subscriber's location using the Origin-Host AVP contents containing a Pseudo Hostname. In subsequent HSS-to-MME/SGSN transactions, the MME/SGSN will be addressed by one of its Pseudo Hostnames, requiring a Pseudo-to-Actual Hostname restoral.
- All MME/SGSN-to-HSS transactions associated with a particular subscriber must use the same MME/SGSN Pseudo Hostname. Otherwise, the HSS will think that the subscriber has moved to another MME/SGSN and unnecessarily change the subscriber's location. For S6a/S6d transactions, the subscriber associated with the transaction is identified by an IMSI, which for the S6a/S6d message set is embedded in the User-Name AVP, a mandatory AVP in all MME/SGSN-to-HSS Request messages.

  Note: Although the Origin-Host and Session-Id AVPs both have MME/SGSN Actual Hostnames, the names could be different. Because the HSS associates the MME/SGSN's location based on the Origin-Host AVP content, it is the MME/SGSN Actual Hostname in the Origin-Host AVP that must be used for selecting a MME/SGSN Pseudo Hostname. This MME/SGSN Pseudo Hostname can be used to replace both of the Hostname fields in the forwarded Request message.

- The HSS sends an Answer response to the transaction with the Session-Id received in the Request and containing an MME/SGSN Pseudo Hostname. Because the Session-Id value returned in the Answer must match the value in the Request, the MME/SGSN Pseudo Hostname in the Session-Id AVP must be replaced with its corresponding value received in the Request message. The value is restored at TH Trigger Point ATR, with the Hostname portion of the Session-Id AVP value that is stored in the PTR.

  This Hostname restoral procedure is not required for Answers initiated by DSR internal nodes (the Diameter Routing Function and DSR Applications) as these Answer responses are based upon the original Request message content.

An example of a Protected-MME/SGSN to Untrusted-HSS Diameter transaction is shown in *Figure 8: MME/SGSN TH Protected-MME/SGSN to Untrusted HSS Transaction*.

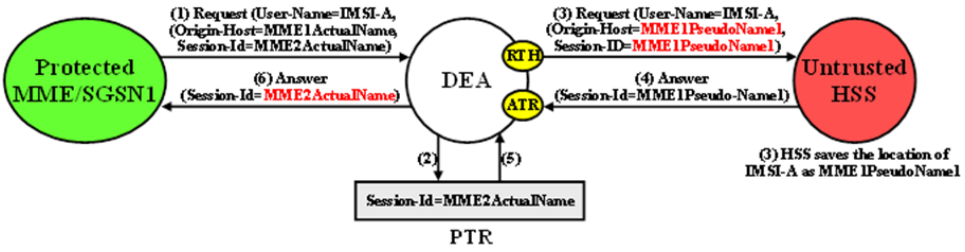

Figure 8: MME/SGSN TH Protected-MME/SGSN to Untrusted HSS Transaction

In S6a/S6d, the subscriber's IMSI is carried in the User-Name AVP. The content of the User-Name AVP content can be one of the following forms:

- IMSI
- IMSI@realm

It is not necessary to extract the IMSI portion from the User-Name AVP value. The User-Name AVP value content will be the same in all transactions associated with subscriber.

For Protected-MME/SGSN to Untrusted-HSS transactions, S6a/S6d HSS Topology Hiding is required only on Request messages that meet the following criteria:

- Message was a candidate for Topology Hiding as defined by topology Trigger Point RTH in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- MME/SGSN Topology Hiding is enabled for the Protected Network (an MME/SGSN TH Configuration Set is assigned to the Protected Network)
- The Request message is a member of the S6a/S6d message set and was initiated by an MME/SGSN as determined from the Command Code in the message
- The Origin-Host and/or Session-Id AVPs in the Request contain an MME/SGSN Actual Hostname assigned to the Protected Network in its MME/SGSN Topology Hiding Configuration Set.

For Protected-MME/SGSN to Untrusted-HSS transactions, MME/SGSN topology information restoral is performed only on Answer messages that meet the following criterion:

- At TH Trigger Point ATR, the MME/SGSN TH ATR flag in the PTR associated with the Answer message is set to "Enabled".

Untrusted-HSS to Protected-MME/SGSN Transactions

When an Untrusted-HSS initiates a transaction to a Protected-MME/SGSN, it is typically addressed to one of the MME/SGSN's Pseudo Hostnames that the HSS saved in a previous MME/SGSN-to-HSS transaction for which MME/SGSN Topology Hiding was applied. For Untrusted-HSS to Protected-MME/SGSN Diameter transactions, MME/SGSN Topology Hiding is concerned with the following topology information hiding and restoral issues:

- The Destination-Host AVP contains a MME/SGSN Pseudo Hostname that must be replaced with the MME/SGSN's Actual Hostname at TH Trigger Point RTR. Pseudo-to-Actual Hostname mapping is performed using the list of created MME/SGSN TH Hostnames described in *MME/SGSN Topology Hiding*. It is acceptable that an Untrusted-HSS to Protected-MME/SGSN Request message does not contain a MME/SGSN Pseudo Hostname. If the Destination-Host AVP value does not match an entry in the MME/SGSN TH Host Names list, then no Hostname conversion is required and the Request message will be routed normally. Destination-Hostname conversion is performed to prevent the following problems:
- Certain MME/SGSNs will not accept messages that do not contain its Actual Hostname.

- DSR routing problems associated with Pseudo Hostnames. For example, Diameter "Implicit Routing" works only with Actual Hostnames (such as the FQDN assigned to the Peer Node and used for the Capabilities Exchange procedure [CER/CEA]).
- An Origin-Host AVP containing an MME/SGSN's Actual Hostname in the Answer response from the Protected-MME/SGSN must be hidden with one of the Pseudo Hostnames assigned to that MME/SGSN. This is done at TH Trigger Point ATH.

An example of an Untrusted-HSS to Protected-MME/SGSN Diameter transaction is shown in *Figure 9: MME/SGSN TH Untrusted-HSS to Protected MME/SGSN Transaction*.

Figure 9: MME/SGSN TH Untrusted-HSS to Protected MME/SGSN Transaction

For Untrusted-HSS to Protected-MME/SGSN transactions, S6a/S6d HSS Topology Hiding is invoked only on Request messages that meet the following criteria:

- Message was a candidate for topology Hiding as defined by TH Trigger Point RTR in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- MME/SGSN Topology Hiding is enabled for the Protected Network (an MME/SGSN Topology Hiding Configuration Set is assigned to the Protected Network)
- The Request message is a member of the S6a/S6d message set and was initiated by an MME/SGSN as determined from the Command Code in the message
- The Destination-Host AVP contains a MME/SGSN Pseudo Hostname that is assigned to the Protected Network as determined from the list of created MME/SGSN TH Host Names described in *MME/SGSN Topology Hiding*.

For Untrusted-HSS to Protected-MME/SGSN transactions, S6a/S6d HSS Topology Hiding is invoked only on Answer messages at TH Trigger Point ATH that meet the following criteria:

- Message was a candidate for Topology Hiding as defined by topology Trigger Point ATH in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- MME/SGSN Topology Hiding is enabled for the Protected Network (an MME/SGSN Topology Hiding Configuration Set is assigned to the Protected Network)
- The Answer message is a member of the S6a/S6d message set and was initiated by an MME/SGSN as determined from the Command Code in the message
- The Origin-Host AVP contains an MME/SGSN Actual Hostname that is assigned to the Protected Network in its MME/SGSN Topology Hiding Configuration Set.

Path Topology Hiding

Path Topology Hiding is concerned with hiding the identities of a Protected Network's hiding a Protected Network's Hostnames and the number of hosts in the following AVPs:

- Route-Record AVP: Sent in Request messages. More than one Route-Record AVP may exist in a Request message.
- Proxy-Host AVP: An AVP embedded in the Grouped Proxy-Info AVP that is sent in Request and Answer messages. More than one Proxy-Host AVP may exist in a message.
- Error-Reporting-Host AVP: Sent in Answer messages. More than one Error-Reporting-Host AVP could exist in an Answer message.

Path Topology Hiding can be enabled for each Protected Network, by assigning a Path TH Configuration Set to the configured Protected Network.

Route-Record AVP Hostname Hiding - Request Messages

Route-Records AVPs are appended to Request messages to assist in message loop detection. When Diameter node N relays a Request message received from Diameter node –1 to Diameter node N+1, Diameter node N appends a Route-Record AVP to the Request message containing the Hostname of Diameter node –1. For Request messages that are forwarded from a Protected Network N1 to an Untrusted Network, there could be Protected Network N1 Hostnames embedded in one or more of the Route-Record AVPs.

Route-Record AVP Hostname hiding is performed only on Request messages that meet the following criteria:

- Message is a candidate for Topology Hiding as defined by topology Trigger Point RTH in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- Path Topology Hiding is enabled for the Protected Network (a Path TH Configuration Set is assigned to the configured Protected Network)
- At least one of the Route-Record AVPs contains a Protected Network Hostname.

An example of Route-Record AVP Hostname hiding for a Request message routed from a Protected Network to an Untrusted Network is shown in *Figure 10: Route-Record Hiding - Request Message*.

Figure 10: Route-Record Hiding - Request Message

The Path Topology Hiding Configuration Set assigned to the Protected Network has the following elements that are used for Route-Record Topology Hiding:

- Hostname Suffixes - A list of Protected Network Hostname Suffixes that are used to specify which Hostnames to hide when messages are forwarded to Untrusted Networks. Any Route-Record AVPs containing a Hostname not matching an entry in this Hostname Suffixes list will not be hidden.
- Route-Record Pseudo Hostname - The Pseudo Hostname to be used when replacing all of the Route-Record AVPs that contain a Hostname that meets the Route-Record AVP hiding criteria.

Route-Record AVP Hostname hiding is performed by replacing all of the Route-Record AVPs that meet the Route-Record AVP hiding criteria with a single Route-Record AVP that contains a single configured Pseudo Hostname. Route-Record AVP Hostname hiding occurs after the Diameter Routing Function appends any Route-Record AVPs to the Request message.

Route-Record AVP Hostname Hiding - Answer Messages

Diameter Relay and Proxy Agents are required to append a Route-Record AVP into any forwarded Request message. There are no Relay Agent or Proxy Agent requirements to perform this function for Answer messages. However, in certain Diameter specifications (such as S6a/S6d and RFC 4006), the Route-Record AVP is specified as an optional AVP in certain Answer messages (including CCA and most of the S6a/S6d Answer messages). Thus, it is probable that Answer messages initiated by a Protected Network node and forwarded to an Untrusted Network by a DEA can contain one or more Route-Record AVPs with Protected Network Hostnames. Therefore, Route-Record AVP Hostname hiding will be applied to Answer messages using the same procedure that is used for Request messages.

Route-Record AVP Hostname hiding is performed only on Answer messages that meet the following criteria:

- Message is a candidate for Topology Hiding as defined by topology Trigger Point ATH in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- Path Topology Hiding is enabled for the Protected Network (a Path Topology Hiding Configuration Set is assigned to the configured Protected Network)
- At least one of the Route-Record AVPs contains a Protected Network Hostname

An example of Route-Record AVP Host Name hiding for an Answer message initiated by a Protected Network to an Untrusted Network is shown in *Figure 11: Route-Record Hiding - Answer Message*.

Figure 11: Route-Record Hiding - Answer Message

Route-Record AVP Hiding and Inter-Network Message Loop Detection

The technique of replacing one or more Route-Record AVPs with a single Route-Record AVP containing a Pseudo Hostname must not defeat the fundamental purpose of the Route-Record AVP - message loop detection. Because Route-Record Topology Hiding is considered a DEA function and is applied only to Request messages leaving a network, inter-network ingress message loop detection is needed at the inter-network boundary. For example, a Request message can egress the network from DEA-1 but loop back to the network through DEA-2 as shown in *Figure 12: Multi-DEA Route-Record Message Loop Detection*. If an inter-network message loop is not detected by a DEA, the loop will not be detected within the Protected Network because a DEA replaced the Route-Records for the internal nodes with a single Route-Record AVP containing a Pseudo Hostname.

Topology Hiding configuration components must be managed from the NOAM so that an identical copy of all Topology Hiding configured components will be distributed to all DEAs controlled by the NOAM. This allows inter-network ingress message loop detection to be supported by any DEA.

Inter-network ingress message loop detection is supported at the RTR Trigger Point. A typical message loop path between two DEAs with Path Topology Hiding enabled is illustrated in Figure 9.

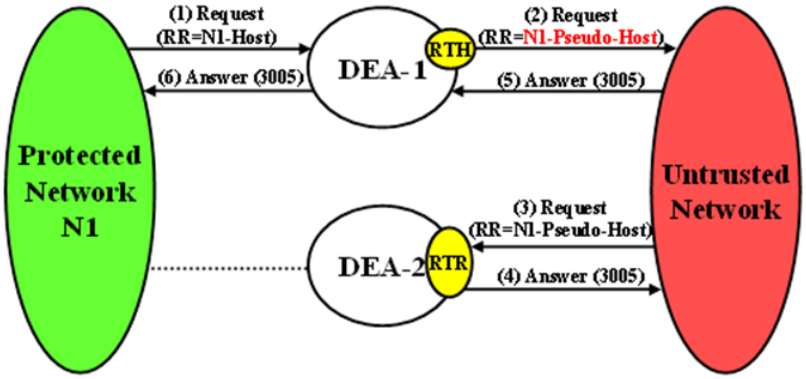

Figure 12: Multi-DEA Route-Record Message Loop Detection

It is possible but highly unlikely (as in an invalid inter-network relationship) that a Request message that leaves the Protected Network addressed to an Untrusted Network will loop back to the Protected

Network through a Trusted Network, as shown in *Figure 13: Unsupported Pseudo-Host Route-Record Loop Detection*. This type of message loop detection is NOT supported.

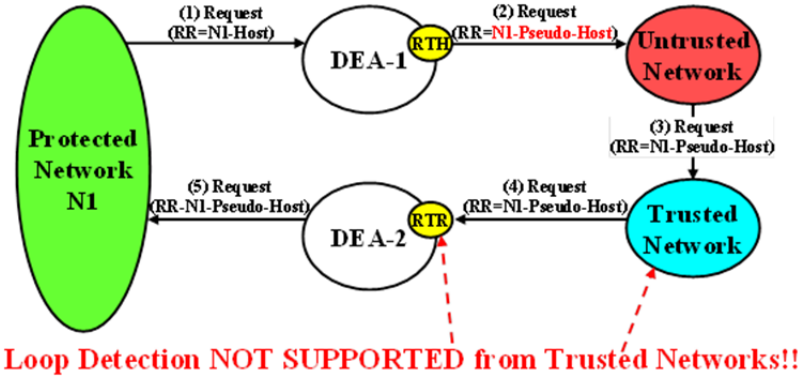

Figure 13: Unsupported Pseudo-Host Route-Record Loop Detection

Inter-network ingress message loop detection occurs when all of the following criteria are met:

- Message is a candidate for Topology Hiding as defined by TH Trigger Point RTR in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- Path Topology Hiding is enabled for the Protected Network (a Path Topology Hiding Configuration Set is assigned to the configured Protected Network)
- A Route-Record AVP contains the Protected Network's Pseudo Hostname used for Route-Record AVP Host Name hiding

Proxy-Host AVP Hiding and Restoral

The grouped Proxy-Info AVP allows stateless agents to add local state to a Diameter Request message, with the guarantee that the same state will be present in the Answer message response. The embedded Proxy-Host AVP identifies the Diameter node that appended the Proxy-Info AVP to the Request message. A Protected Network Hostname in any Proxy-Host AVP must be hidden when the AVP is forwarded to an Untrusted Network. More than one Proxy-Host AVP instance can exist in a Request message. Every instance that contains a Protected Network Hostname must be hidden with a uniquePseudo Hostname.

The Path Topology Hiding Configuration Set assigned to the Protected Network has the following elements that are used for Proxy-Host AVP Hiding:

- Hostname Suffixes - A list of Protected Network Hostname Suffixes that are used to specify which Hostnames to hide when messages are forwarded to Untrusted Networks. Any Proxy-Host AVPs with a Hostname not matching an entry in this Hostname Suffixes list will not be hidden.
- Proxy-Host Pseudo Hostname Suffix - In order to hide the number of Proxy Agents in the Protected Network, a random Proxy-Host pseudo-host name of the format <prefix><suffix> will be used, where the "prefix" is a random 3-digit value created each time Proxy-Host name substitution is performed and "suffix" is a fixed-length string defined by this configured element. All of the Proxy-Host pseudo-host names inserted into any Request message must be unique.

Proxy-Host AVP Hiding is performed only on Request messages that meet the following criteria:

- Message is a candidate for Topology Hiding as defined by TH Trigger Point RTH in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- At least one of the Proxy-Host AVPs contains a Protected Network's Hostname

- Path Topology Hiding is enabled for the Protected Network (a Path Topology Hiding Configuration Set is assigned to the Protected Network)

An example of Proxy-Host AVP Hiding for a Request message initiated by a Protected Network to an Untrusted Network is shown in *Figure 14: Proxy-Host Hiding*.

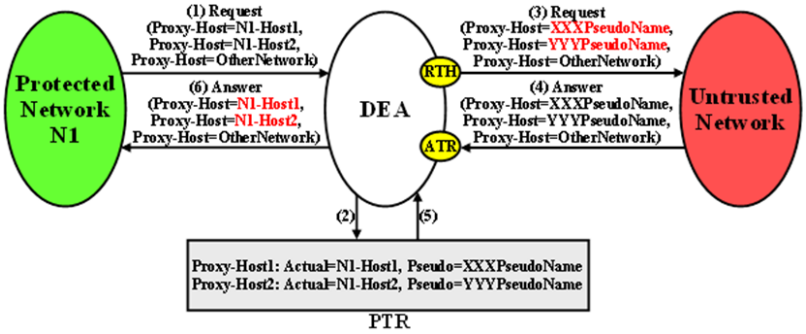

Figure 14: Proxy-Host Hiding

Because the Proxy-Info AVP is used by stateless agents to store local transaction state information into a Request message and retrieve that information from the Answer response, it is important that the DEA restore the original Proxy-Host AVP values (received in the original Request message) when it forwards the Answer response message. Thus, any Proxy-Host AVP value that is replaced at TH Trigger Point RTH must be saved in its respective Diameter Routing Function PTR.

Proxy-Host AVP Restoral is performed only on Answer messages that meet the following criterion:

- At TH Trigger Point ATR, the Restore Proxy-Host AVPs flag in the PTR associated with the Answer message is set to Enabled.

When the criterion is met, Proxy-Host AVP Restoral will be performed. The Diameter Routing Function will replace every Proxy-Host AVP value that matches a Proxy-Host Pseudo Hostname (stored in the PTR) with the original Hostname (also stored in the PTR).

Error Reporting Host AVP Hiding

The Error-Reporting-Host AVP contains the identity of the Diameter node that set the Result-Code AVP to a value other than 2001 (Success), only if the host setting the Result-Code is different from the one encoded in the Origin-Host AVP.

From a Topology Hiding perspective, the Hostname in this AVP must be hidden if it contains a Protected Network Hostname and is being sent to an Untrusted Network.

The content of this AVP will be hidden using encryption. Troubleshooters in the Protected Network must have the ability to decrypt the value. Topology Hiding uses Advanced Encryption Standard (AES), which is described in *Encryption*.

Although unlikely, more than one Error-Reporting-Host AVP could exist in an Answer message; each Error-Reporting-Host AVP containing a Protected Network's Hostname must be encrypted.

Error-Reporting-Host AVP Hiding is performed only on Answer messages that meet the following criteria:

- Message is a candidate for Topology Hiding as defined by topology Trigger Point ATH in *Table 37: General Criteria for Determining Whether a Message is a TH Candidate*
- At least one of the Error-Reporting-Host AVPs contains a Protected Network's Hostname

- Path Topology Hiding is enabled for the Protected Network (a Path Topology Hiding Configuration Set is assigned to the Protected Network)

An example of Error-Reporting-Host AVP Hiding for an Answer message received from a Protected Network that is being forwarded to an Untrusted Network is shown in *Figure 15: Error-Reporting-Host AVP Hiding*.

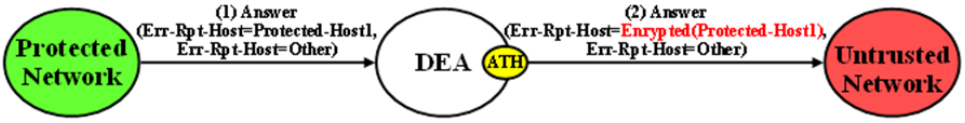

Figure 15: Error-Reporting-Host AVP Hiding

The Path Topology Hiding Configuration Set assigned to the Protected Network has the following elements that are used for Error-Reporting-Host Topology Hiding:

- Hostname Suffixes - A list of Protected Network Hostname Suffixes that are used to specify which host names to hide when messages are forwarded to Untrusted Networks. Any Error-Reporting-Host AVPs with a Hostname not matching an entry in this Hostname Suffixes list will not be hidden.
- Error-Reporting-Host Encryption Key - User-configured encryption key that must be used for encrypting the Error-Reporting-Host AVP value. A user-configured encryption key allows the Error-Reporting-Host AVP value to be decrypted in troubleshooting, if required.

Trusted Networks Lists configuration

A Trusted Network List is a list of Realms identifying networks where Topology Hiding will NOT be invoked for messages to and from that network. Up to 500 Trusted Network Lists can be configured. Each Trusted Network List can contain up to 100 Trusted Network Realms.

Trusted Network Lists can be configured only on an NOAM.

On the **Diameter > Configuration > Trusted Networks Lists** page, you can perform the following actions:

- Filter the list of Trusted Networks Lists, to display only the desired Trusted Networks Lists.
- Sort the list entries in ascending or descending order by Trusted Networks List Name by clicking the column heading. By default, the list is sorted by Trusted Networks List Name in ascending numerical order.
- Click the **Insert** button.

  The **Diameter > Configuration > Trusted Networks Lists [Insert]** page opens. You can add a new Trusted Networks List. See *Adding a Trusted Network List*. If the maximum number of Trusted Networks Lists (500) already exists in the system, the **Diameter > Configuration > Trusted Networks Lists [Insert]** page will not open, and an error message is displayed.
- Select a **Trusted Networks List Name** in the list, and click the **Edit** button.

  The **Diameter > Configuration > Trusted Networks Lists [Edit]** page opens. You can edit the selected Trusted Networks List. See *Editing a Trusted Network List*.
- Select a **Trusted Networks List Name** in the list, and click the **Delete** button to remove the selected Trusted Networks List. See *Deleting a Trusted Network List*.

Trusted Network Lists elements

Table 41: Trusted Network Lists elements describes the fields on the **Diameter > Configuration > Trusted Network Lists** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 41: Trusted Network Lists elements

Field (* indicates a required field)	Description	Data Input Notes
* Trusted Network List Name	A name that uniquely identifies the Trusted Network List.	Format: case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters
* Trusted Network Realms	Trusted Network Realms for this Trusted Network List. For Trusted Network Realms the Topology Hiding Feature will not be applied. Click the **Add** button to enter another Realm. Click the X next to a Realm to delete the entry.	Format: Test box; case- insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores can be used only as the first character. A label can be at most 63 characters long and a Realm can be at most 255 characters long. Range: 1-100 entries

Viewing Topology Hiding Trusted Network Lists

Use this task to view configured Topology Hiding Trusted Network Lists.

On the NOAM, select **Diameter** > **Configuration** > **Topology Hiding** > **Trusted Network Lists**.
The **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page appears.

Adding a Trusted Network List

Use this task on the NOAM to create a new Trusted Network List. The fields are described in *Trusted Network Lists elements*.

1. Select **Diameter** > **Configuration** > **Topology Hiding > Trusted Network Lists**.
   The **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Topology Hiding > Trusted Network Lists [Insert]** page appears.
3. Enter a unique name for the Trusted Network List in the **Trusted Network List Name** field.
4. Enter one or more, up to 100, **Trusted Network Realms**.

5. Click:
   - **OK** to save the data and return to the **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page .
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The **Trusted Network List Name** is not unique; it already exists in the system
   - The maximum number of Trusted Network Lists (100) would be exceeded in the system

Editing a Trusted Network List

Use this task to make changes to existing Trusted Network Lists.

The **Trusted Network List Name** cannot be changed.

1. Select **Diameter** > **Configuration** > **Topology Hiding > Trusted Network Lists**.
   The **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page appears.
2. Select the **Trusted Network List** you want to edit.
3. Click **Edit**.

   The **Diameter > Configuration > Topology Hiding > Trusted Network Lists [Edit]** page appears.

   The page is initially populated with the current configured values for the selected Trusted Network List.

4. Update the relevant fields.

   For more information about each field see *Trusted Network Lists elements*.

5. Click:
   - **OK** to save the data and return to the **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page .
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)

Deleting a Trusted Network List

Use this task on the NOAM to delete a Trusted Network List.

Note: A Pending Answer Timer cannot be deleted if the Pending Answer Timer is referenced by any of the following components:

- Peer Node
- Application Id
- Routing Option Set

The Default Pending Answer Timer cannot be deleted.

1. Select **Diameter** > **Configuration** > **> Topology Hiding > Trusted Network Lists**.
   The **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page appears.
2. Select the **Trusted Network List** you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Trusted Network List.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Topology Hiding > Trusted Network Lists** page.

   If **OK** is clicked and the selected Trusted Network List no longer exists (it was deleted by another user), an error message is displayed and the Trusted Network Lists view is refreshed.

Path Topology Hiding Configuration Set configuration

Path Topology Hiding Configuration Sets provide information that is used to perform Path Topology Hiding for Protected Networks. Each Protected Network can reference a single Path Topology Hiding Configuration Set.

The fields are described in *Path Topology Hiding Configuration Set elements*.

Each Path Topology Hiding Configuration Set contains the following information:

- Path Topology Hiding Configuration Set Name - Unique name for this Configuration Set.
- Hostname Suffixes - List of Hostname suffixes that are used to identify the Protected Network's host name that must be hidden in Route-Record, Proxy-Host, and Error-Reporting-Host AVPs.
- Route-Record Pseudo Hostname - Pseudo-host name to be used when replacing Route-Record headers.
- Encryption Key - Encryption key used for Error-Reporting-Host obscuring.

On the **Diameter > Configuration > Topology Hiding > Path Topology Hiding Configuration Sets** page, you can perform the following actions:

- Filter the list of Path Topology Hiding Configuration Sets to display only the desired Path Topology Hiding Configuration Sets.
- Sort the list by column contents in ascending or descending order (except Hostname Suffixes), by clicking the column heading. The default order is by **Path Topology Hiding Configuration Set Name** in ascending ASCII order.
- In the **Hostname Suffixes** column,
  - Click the + sign to the left of the number of Hostname Suffixes to expand the list of Hostname Suffixes for the Configuration Set.
  - Click the -sign to the left of the number of Hostname Suffixes to collapse the list of Hostname Suffixes for the Configuration Set.
- Click the **Insert** button.

The **Diameter > Configuration > Topology Hiding > Path Topology Hiding Configuration Sets [Insert]** page appears. You can add a new Path Topology Hiding Configuration Set and its elements. See *Adding a Path Topology Hiding Configuration Set*.

If the maximum number of Path Topology Hiding Configuration Sets per Network Element (500) already exist in the system, the **Diameter > Configuration > Topology Hiding > Path Topology Hiding Configuration Sets [Insert]** page will not open, and an error message is displayed.

- Select a Path Topology Hiding Configuration Set Name in the list, and click the **Edit** button.

  The **Diameter > Configuration > Topology Hiding > Path Topology Hiding Configuration Sets [Edit]** page opens. You can edit the selected Connection Configuration Set. See *Editing a Path Topology Hiding Configuration Set*.

  If at least one Protected Network references the Path Topology Hiding Configuration Set the **Diameter > Configuration > Topology Hiding > Path Topology Hiding Configuration Sets [Edit]** page will not open.

- Select a Path Topology Hiding Configuration Set Name in the list, and click the **Delete** button to remove the selected Path Topology Hiding Configuration Set. See *Deleting a Path Topology Hiding Configuration Set*.

  If at least one Protected Network references the selected Path Topology Hiding Configuration Set, the Configuration Set will not be deleted.

Path Topology Hiding Configuration Set elements

Table 42: Path Topology Hiding Configuration Sets Elements describes the fields on the Path Topology Hiding 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 42: Path Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Path Topology Hiding Configuration Set Name	A name that uniquely identifies the Path Topology Hiding 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
* Hostname Suffixes	List of Hostname Suffixes that are used to identify the Protected Network's host name that must be hidden in Route-Record, Proxy-Host, and Error-Reporting-Host AVPs. Up to 10 Hostname Suffixes can be configured for each Path Topology Hiding Configuration Set.	Format: 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

Field (* indicates required field)	Description	Data Input Notes
		must end with a letter or digit. Underscores can be used only as the first character. Label - up to 63 characters; Hostname Suffix - up to 255 characters.
* Route-Record Pseudo Hostname	A pseudo-host name that is used in replacing Route-Record headers.	Format: 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 can be used only as the first character. Label - up to 63 characters; Route-Record Pseudo Hostname - up to 255 characters.
* Proxy Host Pseudo Hostname	A pseudo-host name that is used in replacing the host name in the Proxy-Host AVP.	Format: 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 can be used only as the first character. Label - up to 63 characters; Proxy Host Pseudo Hostname - up to 255 characters.
* Encryption Key	Encryption Key to be used in Error-Reporting Host obscuring.	Format: alphanumeric string

Field (* indicates required field)	Description	Data Input Notes
		Range: up to 16 characters; valid Encryption Key

Viewing Path Topology Hiding Configuration Sets

Use this task to view currently configured Path Topology Hiding Configuration Sets.

Select **Diameter** > **Configuration** > **Topology Hiding** > **Path Topology Hiding Configuration Sets**.
The **Path Topology Hiding Configuration Sets** page appears.

Adding a Path Topology Hiding Configuration Set

Use this task to create a new Path Topology Hiding Configuration Set.

For more information about the fields, see *Path Topology Hiding Configuration Set elements*.

1. Select **Diameter** > **Configuration** > **Configuration Sets** > **Path Topology Hiding Configuration Sets**.
   The **Path Topology Hiding Configuration Sets** page appears.
2. Click **Insert**.
   The **Path Topology Hiding Configuration Sets [Insert]** page appears.

   Note: If the maximum number of Configuration Sets allowed in the system (500) has been configured, the **S6a/S6d HSS Topology Hiding Configuration Sets [Insert]** page will not open.
3. Enter a unique name for the Configuration Set in the **Path Topology Hiding Configuration Set Name** field.
4. Enter a suffix for the Hostname in the **Hostname Suffix** field.
5. Enter a value to be used when replacing the Route-Record headers in the **Route-Record Pseudo Hostname** field.
6. Enter a value to be used when replacing the host name in the Proxy-Host AVP in the **Proxy-Host Pseudo Hostname** field.
7. Enter an encryption key value in the **Encryption Key** field.
8. Click:
   - **OK** to save the new Configuration Set and return to the **Path Topology Hiding Configuration Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Path Topology Hiding Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty (no value was entered).
   - The value in any field is not valid or is out of range.
   - The **Path Topology Hiding Configuration Set Name** is not unique; it already exists in the system.

Editing a Path Topology Hiding Configuration Set

Use this task to edit an existing Path Topology Hiding Configuration Set.

When the **Path Topology Hiding Configuration Sets** page opens, the fields are populated with the currently configured values.

The **Path Topology Hiding Configuration Set Name** cannot be edited.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **Path Topology Hiding Configuration Sets**.
   The **Path Topology Hiding Configuration Sets** page appears.
2. Select the Path Topology Hiding Configuration Set you want to edit.
3. Click **Edit**.
   The **Path Topology Hiding Configuration Sets [Edit]** page appears.
4. Update the relevant fields.
   For information about each field, see *Path Topology Hiding Configuration Set elements*.
5. Click:
   - **OK** to save the changes and return to the **Path Topology Hiding Configuration Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Path Topology Hiding Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - The selected Path Topology Hiding Configuration Set no longer exists; it has been deleted by another user.
   - Any required field is empty (no value was entered) .
   - The value in any field is not valid or is out of range.

Deleting a Path Topology Hiding Configuration Set

Use this task to delete a Path Topology Hiding Configuration Set.

Note: A Path Topology Hiding Configuration Set that is used in a Protected Network cannot be deleted.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **Path Topology Hiding Configuration Sets**.
   The **Path Topology Hiding Configuration Sets** page appears.
2. Select the Path Topology Hiding Configuration Set you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Path Topology Hiding Configuration Set.
   - **Cancel** to cancel the delete function and return to the **Path Topology Hiding Configuration Sets** page.

S6a/S6d HSS Topology Hiding Configuration Set configuration

S6a/S6d HSS Topology Hiding Configuration Sets provide information that is used to perform S6a/S6d HSS Topology Hiding for Protected Networks. Each Protected Network can reference a single S6a/S6d HSS Topology Hiding Configuration Set.

The fields are described in *S6a/S6d HSS Topology Hiding Configuration Set elements*.

Each S6a/S6d HSS Topology Hiding Configuration Set contains the following information:

- S6a/S6d HSS Topology Hiding Configuration Set Name - Unique name for this Configuration Set.
- S6a/S6d HSS Pseudo Hostname - Pseudo-host name to be used when replacing the HSS host name.

On the **Diameter > Configuration > Topology Hiding > S6a/S6d HSS Topology Hiding Configuration Sets** page, you can perform the following actions:

- Filter the list of S6a/S6d HSS Topology Hiding Configuration Sets to display only the desired S6a/S6d HSS Topology Hiding Configuration Sets.
- Sort the list by column contents in ascending or descending order (except Hostname Suffixes), by clicking the column heading. The default order is by **S6a/S6d HSS Topology Hiding Configuration Set Name** in ascending ASCII order.
- Click the **Insert** button.

  The **Diameter > Configuration > Topology Hiding > S6a/S6d HSS Topology Hiding Configuration Sets [Insert]** page appears. You can add a new S6a/S6d HSS Topology Hiding Configuration Set and its elements. See *Adding an S6a/S6d HSS Topology Hiding Configuration Set*.

  If the maximum number of S6a/S6d HSS Topology Hiding Configuration Sets (500) already exists in the system, the **Diameter > Configuration > Topology Hiding > Path Topology Hiding Configuration Sets [Insert]** page will not open, and an error message is displayed.

- Select a S6a/S6d HSS Topology Hiding Configuration Set Name in the list, and click the **Edit** button.

  The **Diameter > Configuration > Topology Hiding > S6a/S6d HSS Topology Hiding Configuration Sets [Edit]** page opens. You can edit the selected S6a/S6d HSS Configuration Set. See *Editing an S6a/S6d HSS Topology Hiding Configuration Set*.

- Select a S6a/S6d HSS Topology Hiding Configuration Set Name in the list, and click the **Delete** button to remove the selected S6a/S6d HSS Topology Hiding Configuration Set. See *Deleting an S6a/S6d HSS Topology Hiding Configuration Set*.

  If the selected S6a/S6d HSS Topology Hiding Configuration Set is used in a Protected Network, the Configuration Set will not be deleted.

S6a/S6d HSS Topology Hiding Configuration Set elements

Table 43: S6a/S6d HSS Topology Hiding Configuration Sets Elements describes the fields on the S6a/S6d HSS Topology Hiding 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 43: S6a/S6d HSS Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* S6a/S6d HSS Topology Hiding Configuration Set Name	A name that uniquely identifies the S6a/S6d HSS Topology Hiding 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
* S6a/S6d HSS Pseudo Hostname	The name to be used in replacing the HSS Hostname.	Format: 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 can be used only as the first character. Label - up to 63 characters; S6a/S6d HSS Pseudo Hostname - up to 255 characters.

Viewing S6a/S6d HSS Topology Hiding Configuration Sets

Use this task to view currently configured S6a/S6d HSS Topology Hiding Configuration Sets.

Select **Diameter** > **Configuration** > **Topology Hiding** > **S6a/S6d HSS Topology Hiding Configuration Sets**.
The **S6a/S6d HSS Topology Hiding Configuration Sets** page appears.

Adding an S6a/S6d HSS Topology Hiding Configuration Set

Use this task to create a new S6a/S6d HSS Topology Hiding Configuration Set.

For more information about the fields, see *S6a/S6d HSS Topology Hiding Configuration Set elements*.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **S6a/S6d HSS Topology Hiding Configuration Sets**.
   The **S6a/S6d HSS Topology Hiding Configuration Sets** page appears.

   Note: If the maximum number of Configuration Sets allowed in the system (500) has been configured, the **S6a/S6d HSS Topology Hiding Configuration Sets [Insert]** page will not open.

2. Click **Insert**.
   The **S6a/S6d HSS Topology Hiding Configuration Sets [Insert]** page appears.
3. Enter a unique name for the Configuration Set in the **S6a/S6d HSS Topology Hiding Configuration Set Name** field.
4. Enter a unique name to be used when replacing the S6a/S6d HSS Hostname in the **S6a/S6d HSS Pseudo Hostname** field.
5. Click:
   - **OK** to save the changes and return to the **S6a/S6d HSS Topology Hiding Configuration Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **S6a/S6d HSS Topology Hiding Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty (no value was entered).
   - The value in any field is not valid or is out of range.
   - The **S6a/S6d HSS Topology Hiding Configuration Set Name** is not unique; it already exists in the system.

Editing an S6a/S6d HSS Topology Hiding Configuration Set

Use this task to edit an existing S6a/S6d HSS Topology Hiding Configuration Set.

When the **S6a/S6d HSS Topology Hiding Configuration Sets** page opens, the fields are populated with the currently configured values.

The **S6a/S6d HSS Topology Hiding Configuration Set Name** cannot be edited.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **S6a/S6d HSS Topology Hiding Configuration Sets**.
   The **S6a/S6d HSS Topology Hiding Configuration Sets** page appears.
2. Select the S6a/S6d HSS Topology Hiding Configuration Set you want to edit.
3. Click **Edit**.
   The **S6a/S6d HSS Topology Hiding Configuration Sets [Edit]** page appears.
4. Update the relevant fields.
   For information about each field, see *S6a/S6d HSS Topology Hiding Configuration Set elements*.
5. Click:
   - **OK** to save the data and return to the **S6a/S6d HSS Topology Hiding Configuration Sets** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **S6a/S6d HSS Topology Hiding Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - The selected S6a/S6d HSS Topology Hiding Configuration Set no longer exists; it has been deleted by another user.
   - Any field is empty (no value was entered).
   - The value in any field is not valid or is out of range.

Deleting an S6a/S6d HSS Topology Hiding Configuration Set

Use this task to delete an S6a/S6d HSS Topology Hiding Configuration Set.

Note: An S6a/S6d HSS Topology Hiding Configuration Set that is used in a Protected Network cannot be deleted.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **S6a/S6d HSS Topology Hiding Configuration Sets**.
   The **S6a/S6d HSS Topology Hiding Configuration Sets** page appears.
2. Select the S6a/S6d HSS Topology Hiding Configuration Set you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the S6a/S6d HSS Topology Hiding Configuration Set.
   - **Cancel** to cancel the delete function and return to the **S6a/S6d HSS Topology Hiding Configuration Sets** page.

MME/SGSN Topology Hiding Configuration Set configuration

MME/SGSN Topology Hiding Configuration Sets provide information that is used to perform MME/SGSN Topology Hiding for Protected Networks.

Each Protected Network can reference a single MME/SGSN Topology Hiding Configuration Set.

The fields are described in *MME/SGSN Topology Hiding Configuration Set elements*.

Each MME/SGSN Topology Hiding Configuration Set contains the following information:

- MME/SGSN Topology Hiding Configuration Set Name - Unique name for this Configuration Set.
- Pseudo Hostname Generation - Attributes to control the format and generation of Pseudo Hostnames corresponding to an Actual Hostname.
  - Count - The maximum number of Pseudo Hostnames associated with an Actual Hostname.
  - Randomize Count - Allows random number of Pseudo Hostnames between 1 and Count to be associated with an Actual Hostname.
  - Auto Generate - Allows Pseudo Hostnames to be automatically generated corresponding to an Actual Hostname.
  - Prefix - Prefix for the auto-generated Pseudo Hostname.
  - Suffix - Suffix for the auto-generated Pseudo Hostname.
  - Length - Length of the random number used in the auto-generated Pseudo Hostname.
- Hostnames - List of Actual Hostnames and their Pseudo Hostnames in this MME/SGSN Topology Hiding Configuration Set.
- MME/SGSN Actual Hostname Not Found Action - Action to be taken when the Orig-Host in the Diameter message is not configured as Actual Hostname.
- MME/SGSN Actual Hostname Not Found Answer Result-Code Value - Value to be placed in the Result-Code AVP of the Answer message.
- MME/SGSN Actual Hostname Not Found Vendor Id - Value to be placed in the Vendor ID AVP.
- MME/SGSN Actual Hostname Not Found Answer Error Message - String to be placed in the Error-Message AVP of the Answer message.

On the **Diameter > Configuration > Topology Hiding > MME/SGSN Topology Hiding Configuration Sets** page, you can perform the following actions:

- Filter the list of MME/SGSN Topology Hiding Configuration Sets to display only the desired MME/SGSN Topology Hiding Configuration Sets.
- Sort the list by column contents in ascending or descending order (except Hostname Suffixes), by clicking the column heading. The default order is by **MME/SGSN Topology Hiding Configuration Set Name** in ascending ASCII order.
- Click the **Insert** button.

  The **Diameter > Configuration > Topology Hiding > MME/SGSN Topology Hiding Configuration Sets [Insert]** page appears. You can add a new MME/SGSN Topology Hiding Configuration Set and its elements. See *Adding an MME/SGSN Topology Hiding Configuration Set*.

  If the maximum number of MME/SGSN Topology Hiding Configuration Sets (500) already exist in the system, the **Diameter > Configuration > Topology Hiding > MME/SGSN Topology Hiding Configuration Sets [Insert]** page will not open, and an error message is displayed.

- Select a MME/SGSN Topology Hiding Configuration Set Name in the list, and click the **Edit** button.

  The **Diameter > Configuration > Topology Hiding > MME/SGSN Topology Hiding Configuration Sets [Edit]** page opens. You can edit the selected Configuration Set. See *Editing an MME/SGSN Topology Hiding Configuration Set*.

- Select an MME/SGSN Topology Hiding Configuration Set Name in the list, and click the **Delete** button to remove the selected MME/SGSN Topology Hiding Configuration Set. See *Deleting an MME/SGSN Topology Hiding Configuration Set*.

  If at least one Protected Network references the selected MME/SGSN Topology Hiding Configuration Set, the Configuration Set will not be deleted.

MME/SGSN Topology Hiding Configuration Set elements

Table 44: MME/SGSN Topology Hiding Configuration Sets Elements describes the fields on the MME/SGSN Topology Hiding 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 44: MME/SGSN Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* MME/SGSN Topology Hiding Configuration Set Name	A name that uniquely identifies the MME/SGSN Topology Hiding 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
Pseudo Hostname Generation	Attributes to control the format and generation of Pseudo Hostnames corresponding to an Actual Hostname:	

Field (* indicates required field)	Description	Data Input Notes
	Count - The maximum number of Pseudo Hostnames associated with an Actual Hostname.	Format: pulldown list Range: 1 -3 Default: 3
	Randomize Count - If checked, random number of Pseudo Hostnames between 1 and Count are associated with an Actual Hostname.	Format: checkbox Default = checked
	Auto Generate - If checked, Pseudo Hostnames are automatically generated corresponding to an Actual Hostname.	Format: checkbox Default: checked
	Prefix - Prefix for the auto generated Pseudo Hostname.	Format: 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 can be used only as the first character. Range: up to 63 characters
	Suffix - Suffix for the auto generated Pseudo Hostname.	Format: 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 can be used only as the first character. Range: up to 63 characters
	Length - Length of the random number used in the auto generated Pseudo Hostname.	Format: pull-down list Range: 4, 5 Default: 4

Field (* indicates required field)	Description	Data Input Notes
* Hostnames	List of Actual Hostnames and their Pseudo Hostnames in this MME/SGSN Topology Hiding Configuration Set. • Text boxes for **Actual Hostname** and **Pseudo Hostnames** • Click the **Add** button to open up to 300 entries. • Click the X at the end of an entry to delete the Actual Hostname entry and its corresponding Pseudo Hostnames.	Format: Each Actual and Pseudo Hostname 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 can be used only as the first character. Label - up to 63 characters; Actual or Pseudo Hostname - up to 255 characters. Range: Actual Hostname - 1 - 300 entries. Pseudo Hostname - 1 - 3 entries per actual Hostname.
MME/SGSN Actual Hostname Not Found Action	Action to be performed when the Orig-Host in the Diameter message is not configured as Actual Hostname in this MME/SGSN Topology Hiding Configuration Set.	Format: radio button group Range: • Send Answer • Abandon • Forward Default: Send Answer
MME/SGSN Actual Hostname Not Found Answer Result-Code Value	Value to be placed in the Result-Code AVP of the Answer message. This value is required if the **MME/SGSN Actual Hostname Not Found Action** is Send Answer.	Format: radio button group with values as a text box and a pull-down list. Range: 1000 - 5999 Default: 3002
MME/SGSN Actual Hostname Not Found Vendor Id	Vendor ID to be placed in Vendor Id AVP.	Format: text box Range: 1 - 4294967295

Field (* indicates required field)	Description	Data Input Notes
MME/SGSN Actual Hostname Not Found Answer Error Message	String to be placed in the Error-Message AVP of the Answer message.	Format: text box Range: 0 - 64 characters Default: Null string. No Error-Message AVP in Answer message.

Viewing MME/SGSN Topology Hiding Configuration Sets

Use this task to view currently configured MME/SGSN Topology Hiding Configuration Sets.

Select **Diameter** > **Configuration** > **Topology Hiding** > **MME/SGSN Topology Hiding Configuration Sets**.
The **MME/SGSN Topology Hiding Configuration Sets** page appears.

Adding an MME/SGSN Topology Hiding Configuration Set

Use this task to create a new MME/SGSN Topology Hiding Configuration Set.

For more information about the fields, see *MME/SGSN Topology Hiding Configuration Set elements*.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **MME/SGSN Topology Hiding Configuration Sets**.
   The **MME/SGSN Topology Hiding Configuration Sets** page appears.
2. Click **Insert**.
   The **MME/SGSN Topology Hiding Configuration Sets [Insert]** page appears.

   Note: If the maximum number of Configuration Sets allowed in the system (500) has been configured, the **S6a/S6d HSS Topology Hiding Configuration Sets [Insert]** page will not open.
3. Enter a unique name for the Configuration Set in the **MME/SGSN Topology Hiding Configuration Set Name** field.
4. Enter values for the **Actual Hostname** and associated **Pseudo Hostnames** in the appropriate fields.
5. Complete the optional fields as desired.
6. Click:

   - **OK** to save the changes and return to the **MME/SGSN Topology Hiding Configuration Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **MME/SGSN Topology Hiding Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any required field is empty (no value was entered).
   - The value in any field is not valid or is out of range.
   - The **MME/SGSN Topology Hiding Configuration Set Name** is not unique; it already exists in the system.

Editing an MME/SGSN Topology Hiding Configuration Set

Use this task to edit an existing MME/SGSN Topology Hiding Configuration Set.

When the **MME/SGSN Topology Hiding Configuration Sets** page opens, the fields are populated with the currently configured values.

Configured **Actual Hostname** and **Pseudo Hostnames** entries cannot be edited. New **Actual Hostnames** and **Pseudo Hostnames** can be added, and configured entries can be deleted.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **MME/SGSN Topology Hiding Configuration Sets**.
   The **MME/SGSN Topology Hiding Configuration Sets** page appears.
2. Select the MME/SGSN Topology Hiding Configuration Set you want to edit.
3. Click **Edit**.
   The **MME/SGSN Topology Hiding Configuration Sets [Edit]** page appears.
4. Update the relevant fields.
   For information about each field, see *MME/SGSN Topology Hiding Configuration Set elements*.
5. Click:
   - **OK** to save the changes and return to the **MME/SGSN Topology Hiding Configuration Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **MME/SGSN Topology Hiding Configuration Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - The selected MME/SGSN Topology Hiding Configuration Set no longer exists; it has been deleted by another user.
   - Any required field is empty (no value was entered) .
   - The value in any field is not valid or is out of range.

Deleting an MME/SGSN Topology Hiding Configuration Set

Use this task to delete an MME/SGSN Topology Hiding Configuration Set.

An MME/SGSN Topology Hiding Configuration Set that is being used by a Protected Network cannot be deleted.

1. Select **Diameter** > **Configuration** > **Toplogy Hiding** > **MME/SGSN Toplogy Hiding Configuration Sets**.
   The **MME/SGSN Toplogy Hiding Configuration Sets** page appears.
2. Select the MME/SGSN Topology Hiding Configuration Set you want to delete.
3. Click **Delete.**
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the MME/SGSN Topology Hiding Configuration Set.
   - **Cancel** to cancel the delete function and return to the **MME/SGSN Toplogy Hiding Configuration Sets** page.

Protected Networks configuration

A Protected Network component contains Topology Hiding (TH) configuration data that is used when messages to and from that network are to be protected using Topology Hiding. The following fields are described in *Protected Network configuration elements*:

- Protected Network Realm - Realm of a network that is to be protected.
- Trusted Network List - A Trusted Network List of networks that are trusted by this Protected Network. If a Trusted Network List is not assigned to the Protected Network, then no networks are trusted for the Protected Network.
- Path Topology Hiding Configuration Set - The set of Path TH elements for this Protected Network. If a Path TH Configuration Set is not assigned to the Protected Network, then Path TH is disabled for the Protected Network.
- MME/SGSN Topology Hiding Configuration Set - The set of MME/SGSN TH elements for this Protected Network. If a MME/SGSN TH Configuration Set is not assigned to the Protected Network, then MME/SGSN TH is disabled for the Protected Network.
- S6a/S6d HSS Topology Hiding Configuration Set - The set of S6a/S6d HSS TH elements for this Protected Network. If a S6a/S6d HSS TH Configuration Set is not assigned to the Protected Network, then S6a/S6d HSS TH is disabled for the Protected Network.

On the **Diameter > Configuration > Topology Hiding > Protected Networks** page, you can perform the following actions:

- Filter the list of Protected Networks, to display only the desired Protected Networks.
- Sort the list by a column in ascending or descending order, by clicking the column heading. The default order is by **Protected Network Realm** in ascending ASCII order.
- Click an entry that is shown in blue for a Trusted Network List or a Configuration Set, to open the **Diameter > Configuration > Topology Hiding [Filtered]** view page for that entry only.
- Click **Insert**.

  The **Diameter > Configuration > Topology Hiding > Protected Networks [Insert]** page appears. You can add a new Protected Network.

  The **Diameter > Configuration > Topology Hiding > Protected Networks [Insert]** will not open if the maximum number of Protected Networks per Network Element (500) already exists in the system.
- Select a Protected Network in the list, and click **Edit**.

  The **Diameter > Configuration > Topology Hiding > Protected Networks [Edit]** page appears. You can edit the selected Protected Network
- Select a Protected Network in the list, and click **Delete**. You can delete the selected Protected Network.

Protected Network configuration elements

Table 45: Protected Network Configuration Elements describes the fields on the **Topology Hiding > Protected Networks** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 45: Protected Network Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Protected Network Realm	Protected Network Realm that uniquely identifies the Protected Network.	Format: 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 can be used only as the first character. Range: Label - up to 63 characters; Protected Network Realm - up to 255 characters.
Trusted Network List	Trusted Network List name for this Protected Network.	Format: Pulldown list Range: "-Disabled-"; configured Trusted Network Lists Default: Disabled
Path Topology Hiding Configuration Set	Path Topology Hiding Configuration Set name for this Protected Network.	Format: Pulldown list Range: "-Disabled-"; configured Path Topology Configuration Sets Default: Disabled
MME/SGSN Topology Hiding Configuration Set	MME/SGSN Topology Hiding Configuration Set name for this Protected Network.	Format: Pulldown list Range: "-Disabled-"; configured MME/SGSN Topology Configuration Sets Default: Disabled
S6a/S6d HSS Topology Hiding Configuration Set	S6a/S6d Topology Hiding Configuration Set name for this Protected Network.	Format: Pulldown list Range: "-Disabled-"; configured S6a/S6d HSS Topology Configuration Sets

Field (* indicates required field)	Description	Data Input Notes
		Default: Disabled

Viewing Topology Hiding Protected Networks

Use this task to view configured Topology Hiding Protected Networks.

On the NOAM, select **Diameter** > **Configuration** > **Topology Hiding** > **Protected Networks**.
The **Diameter > Configuration > Topology Hiding > Protected Networks** page appears.

Adding a Protected Network

Use this task on the NOAM to create a new Protected Network.

The fields are described in *Protected Network configuration elements*.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **Protected Networks**.
   The **Diameter > Configuration > Topology Hiding > Protected Networks** page appears.
2. Click **Insert**.
   The **Diameter > Configuration > Topology Hiding > Protected Networks [Insert]** page appears.
3. Enter a unique name in the **Protected Network Realm** field, to identify the Protected Network.
4. Select a **Trusted Network List** for the Protected Network, if required.
5. Select a Configuration Set for each required type of Topology Hiding:
   - Path Topology Hiding Configuration Set
   - S6a/S6d HSS Topology Hiding Configuration Set
   - MME/SGSN HSS Topology Hiding Configuration Set
6. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Topology Hiding > Protected Networks** page .
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Topology Hiding > Protected Networks** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)
   - The **Protected Network Realm** is not unique; it already exists in the system
   - Adding this Protected Network would exceed the maximum number of Protected Networks (500) allowed in the system

Editing a Protected Network

Use this task to make changes to existing Protected Networks.

The **Protected Network Realm** cannot be changed.

1. Select **Diameter** > **Configuration** > **Topology Hiding** > **Protected Networks**.
   The **Diameter > Configuration > Topology Hiding > Protected Networks** page appears.
2. Select the **Protected Network** you want to edit.
3. Click **Edit**.

   The **Diameter > Configuration > Topology Hiding > Protected Networks [Edit]** page appears.

   The page is initially populated with the current configured values for the selected Protected Network
4. Update the relevant fields.
   For more information about each field see *Protected Network configuration elements*
5. Click:
   - **OK** to save the changes and return to the **Diameter > Configuration > Topology Hiding > Protected Networks** page .
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter > Configuration > Topology Hiding > Protected Networks** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field in not valid (wrong data type or out of the valid range)

Deleting a Protected Network

Use this task on the NOAM to delete a Protected Network

1. Select **Diameter** > **Configuration** > **> Topology Hiding > Protected Networks**.
   The **Diameter > Configuration > Topology Hiding > Protected Networks** page appears.
2. Select the **Protected Network** you want to delete.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Protected Network.
   - **Cancel** to cancel the delete function and return to the **Diameter > Configuration > Topology Hiding > Protected Networks** page.

   If **OK** is clicked and the selected Protected Network no longer exists (it was deleted by another user), an error message is displayed and the Protected Networks view is refreshed.

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, IPFE Configuration, or DSR Applications (FABR, RBAR, Policy DRA, and Charging 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, Policy DRA, and SBR DSR Applications; IPFE; 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 > Remote Servers > Data Export** 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, but not on the **Diameter > Configuration > Import** 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 on the OAM where the data can be configured - the NOAM for Diameter Topology Hiding and network-wide Policy DRA data, and the SOAM for the rest of the Diameter data, site-specific Policy DRA data, IPFE data, and DSR Application data.

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 from CSV 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 from CSV 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 from CSV 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 46: Valid Import Operations* indicates the valid operations for the listed types of configuration data.

Table 46: Valid Import Operations

Configuration Data	Insert	Update	Delete
Diameter			
MP Profiles		X	
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

Configuration Data	Insert	Update	Delete
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	
Trusted Network List	X	X	X
Path Topology Hiding Configuration Set	X	X	X
S6a/S6d HSS Topology Hiding Configuration Set	X	X	X
MME/SGSN HSS Topology Hiding Configuration Set	X	X	X
Protected Network	X	X	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
System Options		X	
Fabr			
Applications	X	X	X
Exceptions		X	
Default Destinations	X	X	X
Address Resolution	X	X	X
System Options		X	

Configuration Data	Insert	Update	Delete
Cpa			
System Options		X	
Message Copy		X	
Sbr			
SBR		X	
SBR Subresource Mapping	Cannot be imported or exported		
Pdra			
PCRFs	X	X	X
Binding Key Priority		X	
Topology Hiding	X	X	X
Site Options		X	
Error Codes		X	
Alarm Settings		X	
Access Point Names	X	X	X
Network-Wide Options		X	
Congestion Options		X	
Ipfe			
IPFE Options		X	
IPFE List Tsa	X	X	X

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.

Any Failures .csv files in the File Management Directory that remain unchanged for more than 14 days and any log files older than 14 days will be automatically removed. The task to remove these files runs once a day.

The Diameter > Configuration > Import page

On the **Diameter > Configuration > Import** page, you can perform the following actions:

- Sort the list of files by column, by clicking the column heading. The default sort is by File Name in ascending ASCII order.
- Select a file and click the **Insert From CSV** button, the **Update From CSV** button, or the **Delete From CSV** button.

  A popup window appears to confirm the selected Import operation.

  One import or export task at a time is allowed.

- Click **Tasks** to display the status and progress of an Import operation.

  The progress of the import operation can also be viewed on the **Status & Manage > Tasks > Active Tasks** page.

- Click the **File Management** button to open the **Status & Manage > Files** page.

  Exported .csv files can be viewed, downloaded to an external location, uploaded from an external location, and deleted.

  Log files from Import operations can be viewed and deleted.

- Click the **Abort On First Error** check box.

  When a check mark appears in the box, only the first record that failed is recorded in the log and the Failures .csv file. The Bulk Import operation stops after the error is detected and logged.

  When there is no check mark in the box (the default), all records that failed are recorded in the log and the Failures .csv file.

Bulk Import elements

Table 47: Bulk Import elements describes the fields on the **Diameter > Configuration > Import** page.

Table 47: 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.

Using an Import file to insert DSR configuration data

Use the following procedure to insert into the system new configuration data entries from the records in a DSR Bulk Import CSV file for Diameter, IPFE, or a DSR Application.

1. Select **Diameter** > **Configuration** > **Import**.

   The **Diameter > Configuration > Import** page appears. The page lists all of the .csv files from the **Status & Manage > Files** File Management area.

2. Select the **File Name** for the file to be used to insert the configuration data.
3. Specify whether the Import operation should stop processing on the first error that occurs, or should continue processing if errors occur during the Import operation.
   - To log all errors and continue processing when errors occur, click the **Abort On First Error** check box so that the box is empty (the default).
   - To log the first error that occurs and stop processing, click the **Abort On First Error** check box so that a checkmark appears in the check box.
4. Click the **Insert From CSV** button.

   A popup window appears to confirm the file that you want to use for the **Insert From CSV** operation.
5. On the popup window, click:
   - **OK** to perform the Import **Insert From CSV** operation.

     An indication is displayed that the operation is in progress.
   - **Cancel** to cancel the **Insert From CSV** operation and return to the **Diameter > Configuration > Import** page.
6. To view the progress of the Import operation, you can:
   - Select the **Tasks** icon near the top left of the **Diameter > Configuration > Import** page.
   - Select **Status & Manage** > **Tasks** > **Active Tasks** to open the **Status & Manage > Tasks > Active Tasks (Filtered)** page.
7. To view the log file from the Import operation, click **File Management** button on the **Diameter > Configuration > Import** page to open the **Status & Manage > Files (Filtered)** page.

Using an Import file to update DSR configuration data

Use the following procedure to use the contents of a DSR Bulk Import .csv file to update existing Diameter, IPFE, or DSR Application configuration data in the system.

1. Select **Diameter** > **Configuration** > **Import**.

   The **Diameter > Configuration > Import** page appears. The page lists all of the .csv files from the **Status & Manage > Files** File Management area.

2. Select the **File Name** for the file to be used to update the configuration data.
3. Specify whether the Import operation should stop processing on the first error that occurs, or should continue processing if errors occur during the Import operation.

- To continue processing when errors occur, click the **Abort On First Error** check box so that the box is empty (the default).
- To stop processing on the first error, click the **Abort On First Error** check box so that a checkmark appears in the check box.

4. A popup window appears to confirm the file to use for the **Update From CSV** operation.
5. On the popup window, do one of the following actions:
   - **OK** to perform the Import **Update From CSV** operation.

     An indication is displayed that the operation is in progress.
   - **Cancel** to cancel the **Update From CSV** operation and return to the **Diameter > Configuration > Import** page.
6. To view the progress of the Import operation, you can:
   - Select the **Tasks** icon near the top left of the **Diameter > Configuration > Import** page.
   - Select **Status & Manage** > **Tasks** > **Active Tasks** to open the **Status & Manage > Tasks > Active Tasks (Filtered)** page.
7. To view the log file from the Import operation, and the Failures.csv file if one was created, click **File Management** button to open the **Status & Manage > Files (Filtered)** page.

Using an Import file to delete DSR configuration data

Use the following procedure to use the contents of a DSR Bulk Import .csv file to delete Diameter, IPFE, or DSR Application configuration data.

Note: This operation does NOT delete a .csv file from the list of files on the page.

1. Select **Diameter** > **Configuration** > **Import**.

   The **Diameter > Configuration > Import** page appears. The page lists all of the .csv files from the **Status & Manage > Files** File Management area.
2. Select the **File Name** for the file to be used to delete the configuration data.
3. Click the **Delete From CSV** button.

   A popup window appears to confirm the file that you want to use for the **Delete From CSV** operation.
4. On the popup window, click:
   - **OK** to perform the Import **Delete From CSV** operation.

     An indication is displayed that the operation is in progress.
   - Click **Cancel** to cancel the **Delete From CSV** operation and return to the **Diameter > Configuration > Import** page.
5. To view the progress of the Import operation, you can:
   - Select the **Tasks** icon near the top of the **Diameter > Configuration > Import** page.

- Select **Status & Manage** > **Tasks** > **Active Tasks** to open the **Status & Manage > Tasks > Active Tasks (Filtered)** page.

6. To view the log file from the Import operation, click **File Management** button to open the **Status & Manage > Files (Filtered)** page.

DSR Bulk Export

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

Note: Exported CSV files are not intended for long-term backup of configuration data. (Use the Database Backup function described in the *DSR Administration Guide* and DSR Administration Help for long-term backups of configuration data.)

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, Policy DRA, and SBR DSR Applications; IPFE; and the **Diameter Configuration** menu folder).

  Exports must be performed on the OAM where the data can be configured - the NOAM for Diameter Topology Hiding and network-wide Policy DRA data, and the SOAM for the rest of the Diameter data, site-specific Policy DRA data, IPFE data, and DSR Application data.

- 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: `NE Name_Timestamp-TimeZone_ApplicationType_DataType.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 each selected Data object 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.

Any .csv files that are exported to the File Management Directory and remain unchanged for more than 14 days will be automatically removed. The task to remove these files runs once a day.

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

- If a remote Export Server has been configured (see **Administration > Remote Servers > Data Export**), 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, but not on the **Diameter > Configuration > Import** page. These files cannot be used for Import operations on the local system.

Export Results

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

The Diameter Configuration Export page

On the **Diameter > Configuration > Export** page, you can perform the following actions:

- Manually export configuration data one time immediately in a CSV file to either the Export Server or the File Management area.
- Schedule periodic automatic exports of configuration data in CSV files to either the Export Server or the File Management area. Scheduled exports are listed on the **Status & Manage > Tasks > Scheduled Tasks** page.
- Click **Tasks** to display the status and progress of an Export operation.

  The progress of the export operation can also be viewed on the **Status & Manage > Tasks > Active Tasks** page.

- Click the **File Management** button on the **Diameter > Configuration > Export** page to open the **Status & Manage > Files** page.

  On the **Status & Manage > Files** page, exported .csv files can be viewed, downloaded to an external location, uploaded from an external location, and deleted. Log files from Export operations can be viewed and deleted.

Bulk Export elements

Table 48: Bulk Export elements describes the fields on the **Diameter Configuration Export** page.

Table 48: 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**, **Ipfe**, all activated DSR Applications To clear the field, select **-Select-** in the list.
Export Data	Data to be exported. **Diameter**, **Ipfe**, or a specific activated DSR Application must be selected in Export Application before this list is available. This field is required when **Diameter** or a DSR Application is selected.	Format: Pulldown list Range: ALL; configuration folders for **Diameter** (except Mediation folders), **Ipfe**, or the selected DSR Application. To clear the field, select **-Select-** in the list.

Element (* indicates required field)	Description	Data Input Notes
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**, **Ipfe**, 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
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

Element (* indicates required field)	Description	Data Input Notes
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
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

Element (* indicates required field)	Description	Data Input Notes
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

Manually Exporting a configuration data file once

Use the following procedure to export a configuration data .csv file once immediately to the **Status & Manage** File Management area or to the Export Server Directory.

Note: The exported file appears the File Management area list on the **Status & Manage > Files** page if the **File Management Directory** is selected as the **Export Directory**, or if the **Export Server Directory** is selected and no remote Export Server is configured.

1. Select **Diameter** > **Configuration** > **Export**.

   The **Diameter > Configuration > Export** page appears.

2. Verify that the **Once** radio button is selected in the **Export Frequency** list. (Select **Once** if another radio button is currently selected.)
3. In the **Export Application** pulldown list, select **ALL**, **Diameter**, **Ipfe**, or the activated DSR Application from which the configuration data will be exported.

   If you selected **ALL**, go to *Step 5*.
4. In the **Export Data** pulldown list, select **ALL** or the configuration folder that contains the data that will be exported from the selected **Export Application** type.
5. Either use (do not change) the default **Output File Name**, or change the entry to the desired name.
6. Select the radio button for the **Export Directory** to which the file will be exported.

   Select either the Export Server Directory (the default), or the File Management Directory.
7. Select **Ok** to perform the Export operation.

   An indication is displayed that the operation is in progress.
8. To view the progress of the Export operation, you can:
   - Select the **Tasks** icon near the top of the **Diameter > Configuration > Export** page.
   - Select **Status & Manage** > **Tasks** > **Active Tasks** to open the **Status & Manage > Tasks > Active Tasks (Filtered)** page.
9. To locate a file in the File Management area or to view the log file from an Export operation, click **File Management** button to open the **Status & Manage > Files (Filtered)** page.

Scheduling periodic automatic exports of configuration data

Use the following procedure to schedule periodic automatic Exports of configuration data files to the local Export Server Directory or to the local File Management area.

Note: When the selected **Export Directory** is the **Export Server Directory,** the file is exported to a temporary Export directory on the local system. A remote Export Server must be configured before the exported file can be transferred to the specified directory on the configured remote Export Server. See the online help for the Administration > Remote Servers > Data Export page for instructions to configure a remote Export Server.

If no remote Export Server is configured, or if the exported configuration data could be used for Import operations on the local system, select **File Management Directory** as the **Export Directory**.

1. Select **Diameter** > **Configuration** > **Export**.

   The **Diameter > Configuration > Export** page appears.

2. In the **Export Application** pulldown list, select **ALL**, **Diameter**, **Ipfe**, or the activated DSR Application from which the configuration data will be exported.

   If you selected **ALL**, go to *Step 4*.

3. In the **Export Data** pulldown list, select **ALL** or the configuration folder that contains the data that will be exported from the selected **Export Application** type.
4. Select the radio button for the **Export Frequency** of the scheduled Exports. (Do not select **Once**.)
5. Either use the default **Task Name** (DSR Configuration Export), or change the name if desired for the Export operation.

   The **Task Name** is required when the **Export Frequency** is not **Once**.

6. If a description of the Export task is desired, enter the **Description** in the text box (up to 255 characters).
7. Select the radio button for the **Export Directory** to which the file will be exported.

   Select either the **Export Server Directory** (the default), or the **File Management Directory**.

   Select the **File Management Directory** if no remote Export Server has been configured.

8. Enter or select the time or day information to specify when the scheduled Export operations will occur.
   - If **Export Frequency** is **Hourly**, enter (type or click the arrows) the **Minute** of each hour (0-59) when the file will be exported.
   - If **Export Frequency** is **Daily**, enter (type, or click in the box and select from the pulldown list) the **Time of Day** when the file will be exported. Select from 15-minute intervals or enter a specific time.
   - If **Export Frequency** is **Weekly**,
     - Select the radio button for the **Day of Week** on which the file will be exported.
     - Enter (type, or click in the box and select from the pulldown list) the **Time of Day** when the file will be exported. Select from 15-minute intervals or enter a specific time.

9. Click **Ok** to save the schedule.

   To view, edit, or delete the saved schedule task, select **Status & Manage** > **Tasks** > **Active Tasks** or click the link in the indication to open the **Status & Manage > Tasks > Scheduled Tasks** page.

The schedule can be changed or deleted on the **Status & Managed > Tasks > Scheduled Tasks** page.

10. To view the progress of an Export operation, you can:
    - Select the **Tasks** icon near the top of the **Diameter > Configuration > Export** page.
    - Select **Status & Manage** > **Tasks** > **Active Tasks** to open the **Status & Manage > Tasks > Active Tasks (Filtered)** page.
11. To locate a file in the File Management area or to view the log file from an Export operation, click **File Management** button to open the **Status & Manage > Files (Filtered)** page.

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 49: 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 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 49: 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 (Charging SBR)
Pdra	Policy Diameter Routing Agent (Policy DRA)
Ipfe	IP Front End (IPFE)

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 50: 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 50: 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 51: 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 51: 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)

Column	Data Description
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
148	Application Route Table
149	Topology Hiding Status (Enabled, Disabled)

Route Group configuration elements describes the configuration data elements listed in *Table 52: 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 52: Route Group CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**RouteGrp** (Keyword)
2	Name (Key)
3	Type (Peer, Connection)
4	Peer Node 1 Name
5	Peer Node 1 Weight
	(repeated x 160) . . .
322	Peer Node 160 Name
323	Peer Node 160 Weight

Column	Data Description
324	Connection 1 Name
325	Connection 1 Weight
	(repeated x 160) . . .
643	Connection 160 Name
644	Connection 160 Weight

Route List configuration elements describes the configuration data elements listed in *Table 53: 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 53: 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 Groups (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 54: 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 54: 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)

Column	Data Description
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
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 55: Connection CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 55: 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
23	Test Mode (Yes, No)

Connection Configuration Set elements describes the configuration data elements listed in *Table 56: 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 56: Connection Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)

Column	Data Description
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 (Yes, No)
18	tcpSockSendSize
19	tcpSockRecvSize
20	tcTimer
21	twinitTimer
22	tdpxTimer
23	tcexTimer
24	nagleEnabled (Yes, No)
25	provingTimeout
26	provingDwrsToSend
27	provingMode (Always, Suspect, Never)
28	pendTransPerConn

Reroute On Answer configuration elements describes the configuration data elements listed in *Table 57: 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 57: 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 58: 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 58: System Options CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**Options** (Keyword)
2	EMT Feature Enabled (Yes, No)
3	Fixed Connection Failure Major Aggregation Alarm Threshold
4	Fixed Connection Critical Aggregation Alarm Threshold
5	IPFE Connection Failure Major Aggregation Alarm Threshold
6	IPFE Connection Failure Critical Aggregation Alarm Threshold
7	Peer Node Failure Critical Aggregation Alarm Threshold
8	Route List Failure Critical Aggregation Alarm Threshold
9	Message Copy Feature Enabled (Enabled, Disabled)
10	Message Copy Disable Congestion Level (CL1, CL2)

DNS Options elements describes the configuration data elements listed in *Table 59: 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 59: 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 60: 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 60: 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)
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 61: 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 61: Capacity Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	CapCfgSet (Keyword)
2	Capacity Configuration Set Name (Key)

Column	Data Description
3	Reserved Ingress MPS
4	Maximum Ingress MPS
5	Ingress MPS Minor Alarm Threshold
6	Ingress MPS Major Alarm Threshold
7	Reserved Ingress MPS Abatement Time

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

Table 62: 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
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)

Column	Data Description
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
23	Application Route Table

Application Ids elements describes the configuration data elements listed in *Table 63: 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 63: 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
7	Application Route Table

CEX Parameters elements describes the configuration data elements listed in *Table 64: 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 64: CEX Parameters CSV Format

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

Pending Answer Timers elements describes the configuration data elements listed in *Table 65: 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 65: 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 66: 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 66: 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	Pending Answer Timer
6	Resource Exhausted Action
7	Resource Exhausted Result Code
8	Resource Exhausted Error Message
9	Resource Exhausted Vendor Id
10	No Peer Response Action
11	No Peer Response Result Code
12	No Peer Response Error Message
13	No Peer Response Vendor Id
14	Connection Failure Action
15	Connection Failure Result Code
16	Connection Failure Error Message
17	Connection Failure Vendor Id
18	Connection Congestion Action
19	Connection Congestion Result Code
20	Connection Congestion Error Message

Column	Data Description
21	Connection Congestion Vendor Id

Peer Route Tables elements describes the configuration data elements listed in *Table 67: 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 67: Peer Route Table CSV Format

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

Message Priority Configuration Set elements describes the configuration data elements listed in *Table 68: 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 68: Message Priority Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**MsgPriorityCfgSet** (Keyword)
2	Name
3	applId[1]
4	cmdCode[1]
5	msgPriority[1]
	(repeated x 50)
151	applId[50]
152	cmdCode[50]
153	msgPriority[50]

Egress Message Throttling Configuration Set elements describes the configuration data elements listed in *Table 68: 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 69: Message Throttling Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**MsgThrottlingCfgSet** (Keyword)

Column	Data Description
2	Name
3	maxEMR
4	smoothFactor
5	abateTime
6	TT1
7	AT1
8	TT2
9	AT2
10	TT3
11	AT3

Message Copy Configuration Set elements describes the configuration data elements listed in *Table 70: Message Copy 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 70: Message Copy Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	MessageCopyCfgSet (Keyword)
2	Message Copy Configuration Set Name (Key)
3	requestTypeForMessageCopy
4	originalAnswerForMessageCopy
5	routeListName
6	answerIncluded
7	dasAnswerResultCode
8	msgCopyMaxRetryAttempts

Table 24: Application Route Tables elements describes the configuration data elements listed in *Table 71: Application 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 71: Application Route Table CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**ApplicationRouteTable** (Keyword)

Column	Data Description
2	Name (Key)

MP Profiles elements describes the configuration data elements listed in *Table 72: MP Profile CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 72: MP Profile CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**EditableDaMpProfileParameters** (Keyword)
2	profileName (Key)
3	CL1DiscardPercent
4	CL2DiscardPercent
5	CL3DiscardPercent
6	CongestionDiscardPolicy (ColorWithinPriority, PriorityWithinColor, PriorityOnly)
7	DOCMsgDiscardPercent
7	DOCDiscardPolicy (ColorWithinPriority, PriorityWithinColor, PriorityOnly)

Table 118: Egress Throttle Groups Maintenance Elements describes the configuration data elements listed in *Table 73: Egress Throttle Groups CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited n the CSV files.

Table 73: Egress Throttle Groups CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**Etg** (Keyword)
2	Name (Key)
3	Maximum Egress Rate
4	RateSmoothFactor
5	RateAbateTime
6	RateOnsetThres1
7	RateAbateThres1
8	RateOnsetThres2
9	RateAbateThres2
10	RateOnsetThres3

Column	Data Description
11	RateAbateThres3
12	Maximum Number of Pending Transactions
13	PendTransAbateTime
14	PendTransOnsetThres1
15	PendTransAbateThres1
16	PendTransOnsetThres2
17	PendTransAbateThres2
18	PendTransOnsetThres3
19	PendTransAbateThres3
20	Peers
	repeated x 128
147	Conns
	repeated x 128

Table 7: MCC Ranges elements describes the configuration data elements listed in *Table 74: Reserved MCC Ranges CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 74: Reserved MCC Ranges CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**ReservedMccRanges** (Keyword)
2	startMccRange
3	endMccRange

Table 6: Command Codes elements describes the configuration data elements listed in *Table 75: Command Code CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 75: Command Code CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**CmdCodes** (Keyword)
2	cmdCode
3	name

Table 41: Trusted Network Lists elements describes the configuration data elements listed in *Table 76: Trusted Network List CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 76: Trusted Network List CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**TrustedNetworkList** (Keyword)
2	Name (Key)
3	trustedRealm [1]
	(repeated x 100)

Table 42: Path Topology Hiding Configuration Sets Elements describes the configuration data elements listed in *Table 77: Path Topology Hiding 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 77: Path Topology Hiding Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**PathTopologyHidingCfgSet** (Keyword)
2	Name (Key)
3	hostnameSuffix
	(repeated x 10)
13	pseudoRouteRecord
14	pseudoProxy
15	encryptionKey

S6a/S6d HSS Topology Hiding Configuration Set elements describes the configuration data elements listed in *Table 78: S6a/S6d HSS Topology Hiding 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 78: S6a/S6d HSS Topology Hiding Configuration Set CSV Format

Column	Data Description
0	Application Type
1	**HssTopologyHidingCfgSet** (Keyword)
2	Name (Key)
3	pseudoHssHostname

MME/SGSN Topology Hiding Configuration Set elements describes the configuration data elements listed in *Table 79: MME/SGSN Topology Hiding 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 79: MME/SGSN Topology Hiding Configuration Set CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**MmeTopologyHidingCfgSet** (Keyword)
2	Name (Key)
3	count
4	randomizeCount
5	autoGenerate
6	prefix
7	suffix
8	length
9	Action (SendAnswer, Forward, Abandon)
10	resultCode
11	vendorId
12	errMsg
13	actualHostname[1]
14	pseudoHostname1
15	pseudoHostname2
16	pseudoHostname3
	(combination of actual and pseudo hostnames repeated x 300)

Table 45: Protected Network Configuration Elements describes the configuration data elements listed in *Table 80: Protected Network CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 80: Protected Network CSV Format

Column	Data Description
0	Application Type (Diameter)
1	**ProtectedNetwork** (Keyword)
2	protectedRealm (Key)
3	trustedNetList
4	pathTopologyHidingCfgSet

Column	Data Description
5	mmeTopologyHidingCfgSet
6	hssTopologyHidingCfgSet

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 81: 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 81: 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 82: 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 82: 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 82: 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 83: 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
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 84: 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 84: 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 85: 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 85: Destination Table CSV Format

Column	Data Description
0	Application Type (Rbar)
1	**Destination** (Keyword)

Column	Data Description
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 86: 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 86: Routing Exception CSV Format

Column	Data Description
0	Application Type (Rbar)
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 87: 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 87: 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,

Column	Data Description
	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, 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 88: Option CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 88: 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)

Column	Data Description
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 81: 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 89: 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 86: 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 90: 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)

Column	Data Description
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 85: 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 91: Default Destination Table CSV Format

Column	Data Description
0	Application Type (Fabr)
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 87: 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 92: 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)

Column	Data Description
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 88: Option CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 93: Option CSV Format

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

Column	Data Description
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 94: 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 94: System Option CSV Format

Column	Data Description
0	Application Type (Cpa)
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 95: 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 95: 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
12	messageCopyRouteList10
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 96: SBR CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 96: SBR CSV Format

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

IP Front End CSV File Formats

The following tables describe the CSV file content and attribute column positions for all configuration data supported by the IP Front End (IPFE) Application Type.

"Configuration Options elements" in the IPFE Help describes the configuration data elements listed in *Table 97: IPFE IpfeOption CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 97: IPFE IpfeOption CSV Format

Column	Data Description
0	Application Type (Ipfe)
1	**Options** (Keyword)
2	Ipfe1IpAddress
3	Ipfe2IpAddress
4	Ipfe3IpAddress
5	Ipfe4IpAddress
6	StatSyncTcpPort
7	StateSyncReconnectS
8	ApplicationMinPort
9	ApplicationMaxPort
10	RejectOption (tcpreset, drop, icmphostunreachable, icmpportunreachable, icmpadminprohibited)
11	SctpRejectOption (drop, icmphostunreachable, icmpportunreachable, icmpadminprohibited)
12	OverloadStart
13	LeastLoadStart
14	Accounting Support (enabled, disabled)
15	ConnectTryPort
16	ConnectTimeoutS
17	ConnectTryIntervalS
18	MonitorProtocol (tcpconnectonly, fullmonitoring, disabled)
19	PacketRateLimit
20	Tsa1DeleteAge
21	Tsa1IPAddress
22	Tsa1IPSecondaryAddress
23	Tsa1IPSecondaryPreferredIpfe

Column	Data Description
24	Tsa1LoadAlgorithm (hash, roundrobin, leasttraff, leastconns, leastload, leastloadtest)
25	Tsa1PreferredIpfe (1, 2, 3, 4)
26	Tsa1Protocols (SCTP, TCP, SCTP_AND_TCP)
27	Tsa1TsDisable (0, 1)
28	Tsa1AllowedDeviation (0-50)
29	Tsa1LoadFactorMPS (0-100)
30	Tsa1LoadFactorConn (0-100)
	(repeated x 31)
330	Tsa32DeleteAge
331	Tsa32IPAddress
332	Tsa132PSecondaryAddress
333	Tsa32IPSecondaryPreferredIpfe
334	Tsa32LoadAlgorithm (hash, roundrobin, leasttraff, leastconns, leastload, leastloadtest)
335	Tsa32PreferredIpfe
336	Tsa32Protocols (SCTP, TCP, SCTP_AND_TCP)
337	Tsa32TsDisable (0, 1)
338	Tsa32AllowedDeviation (0-50)
339	Tsa32LoadFactorMPS (0-100)
340	Tsa32LoadFactorConn (0-100)

"Target Sets configuration elements" in the IPFE Help describes the configuration data elements listed in *Table 98: IPFE IpfeListTsa CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 98: IPFE IpfeListTsa CSV Format

Column	Data Description
0	Application Type (Ipfe)
1	**IPListTsa** (Keyword)
2	tsa
3	server
4	ipAddress
5	description
6	extcol07

Policy Diameter Routing Agent CSV File Formats

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

"PCRFs elements" in the Policy DRA Help describes the configuration data elements listed in *Table 99: PCRFs CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 99: PCRFs CSV Format

Column	Data Description
0	Application Type (Pdra)
1	**Pcrf** (Keyword)
2	PCRF Peer Node Name (Key)
3	Comments

"Binding Key Priority elements" in the Policy DRA Help describes the configuration data elements listed in *Table 100: Binding Key Priority CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 100: Binding Key Priority CSV Format

Column	Data Description
0	Application Type (Pdra)
1	**BindPriority** (Keyword)
2	Priority 1
3	Binding Key Type 1 (Imsi, Msisdn, Ipv4, Ipv6)
4	Priority 2
5	Binding Key Type 2 (Imsi, Msisdn, Ipv4, Ipv6)
6	Priority 3
7	Binding Key Type 3 (Imsi, Msisdn, Ipv4, Ipv6)
8	Priority 4
9	Binding Key Type 4 (Imsi, Msisdn, Ipv4, Ipv6)

"Topology Hiding elements" in the Policy DRA Help describes the configuration data elements listed in *Table 101: Policy DRA Topology Hiding CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 101: Policy DRA Topology Hiding CSV Format

Column	Data Description
0	Application Type (Pdra)

Column	Data Description
1	**TopoHiding** (Keyword)
2	Policy Client Peer Node Name (Key)
3	Comments

"Site Options elements" and "Network-Wide Options elements" in the Policy DRA Help describes the configuration data elements listed in *Table 102: Policy DRA Options CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 102: Policy DRA Options CSV Format

Column	Data Description
0	Application Type (Pdra)
1	**PdraOptions** (Keyword)
2	Policy DRA Mate DSR Peer Node Name
3	Topology Hiding Enabled
4	Topology Hiding Scope
5	Topology Hiding FQDN
6	Topology Hiding Realm
7	Peer Route Table Name
8	Policy DRA Unavailable (Relay, Discard)
9	Default Stale Session Timeout
10	Origin-Host and Origin-Realm for Policy DRA generated RAR messages (Local Host, PCRF)
11	Audit Default Max Frequency

"Error Codes elements" in the Policy DRA Help describes the configuration data elements listed in *Table 103: Error Codes CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 103: Error Codes CSV Format

Column	Data Description
0	Application Type (Pdra)
1	**ErrorCodes** (Keyword)
2	Error Condition (Key) (PdraUnavailCong, BindingNotFound, BindingFoundButUnableToRoute, SbrError, BindingKeyNotFoundCondition, BindingNotCreatedUnableToRoute)

Column	Data Description
3	Gx/Gxx Result Code
4	Gx/Gxx Experimental Code
5	Gx/Gxx Vendor ID
6	Rx Result Code
7	Rx Experimental Code
8	Rx Vendor ID
9	S9 Result Code
10	S9 Experimental Code
11	S9 Vendor ID
12	All Result Code
13	All Experimental Code
14	All Vendor ID

"Access Point Names elements" in the Policy DRA Help describes the configuration data elements listed in *Table 102: Policy DRA Options CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 104: Access Point Names CSV Format

Column	Data Description
0	Application Type (Pdra)
1	**AccessPointName** (Keyword)
2	Access Point Name
3	Stale Session Timeout

"Alarm Settings elements" in the Policy DRA Help describes the configuration data elements listed in *Table 105: Alarm Settings CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 105: Alarm Settings CSV Format

Column	Data Description
0	Application Type (Pdra)
1	**AlarmSupp** (Keyword)
2	Alarm Name 1 (PdraIngressMessageRate, OutstandingPdraSessionsThresholdExceeded)
3	Critical Alarm Threshold (Percent) 1

Column	Data Description
4	Suppress Critical 1 (Yes, No)
5	Major Alarm Threshold (Percent) 1
6	Suppress Major 1 (Yes, No)
7	Minor Alarm Threshold (Percent) 1
8	Suppress Minor 1 (Yes, No)
9	Alarm Name 2 (PsbrActiveSessionsThreshold)
10	Critical Alarm Threshold (Percent) 2
11	Suppress Critical 2 (Yes, No)
12	Major Alarm Threshold (Percent) 2
13	Suppress Major 2 (Yes, No)
14	Minor Alarm Threshold (Percent) 1
15	Suppress Minor 2 (Yes, No)
16	Alarm Name 3 (PdraActiveBindingsThreshold)
17	Critical Alarm Threshold (Percent) 3
18	Suppress Critical 3 (Yes, No)
19	Major Alarm Threshold (Percent) 3
20	Suppress Major 3 (Yes, No)
21	Minor Alarm Threshold (Percent) 3
22	Suppress Minor 3 (Yes, No)

"Congestion Options elements" in the Policy DRA Help describes the configuration data elements listed in *Table 102: Policy DRA Options CSV Format* and configuration considerations for the data elements that must be observed when the elements are edited in the CSV files.

Table 106: Congestion Options CSV Format

Column	Data Description
0	Application Type (Pdra)
1	**CongOptions** (Keyword)
2	Critical Alarm Onset Threshold 1
3	Critical Alarm Abatement Threshold 1
4	Major Alarm Onset Threshold 1
5	Major Alarm Abatement Threshold 1
6	Minor Alarm Onset Threshold 1

Column	Data Description
7	Minor Alarm Abatement Threshold 1
8	Congestion Level 1- Discard Session Creation Requests 1
9	Congestion Level 1- Discard Session Update Requests 1
10	Congestion Level 1- Discard Session Terminate Requests 1
11	Congestion Level 2- Discard Session Creation Requests 1
12	Congestion Level 2- Discard Session Update Requests 1
13	Congestion Level 2- Discard Session Terminate Requests 1
14	Congestion Level 3- Discard Session Creation Requests 1
15	Congestion Level 3- Discard Session Update Requests 1
16	Congestion Level 3- Discard Session Terminate Requests 1

Chapter 3

Diameter Message Copy

Topics:

- *Diameter Message Copy overview.....260*
- *Diameter Message Copy feature.....262*

The Diameter Message Copy function provides the ability to forward a copy of a Diameter Request message, and optionally the Answer message, routed through the DSR to a Diameter Application Server (a DAS Peer). Diameter Message Copy can be triggered by a configuration or can be dictated by a DSR Application.

Diameter Message Copy overview

For a message that was routed through the DSR, the Diameter Message Copy feature provides the ability to forward a copy of the Diameter Request message, and optionally the Answer message, to a Diameter Application Server (a DAS Peer). Diameter Message Copy can be triggered by a configuration or can be dictated by a DSR Application.

Diameter Message Copy copies both Diameter Request and Answer messages as directed by one or more Trigger Points within the DSR node. The Trigger Points can be any processing functions acting on the messages, including Diameter Mediation, DSR Applications, and Peer Routing Rules. Message Copy Configuration Sets define the contents and conditions on which the copy needs to be performed.

Message Copy Configuration Sets provide a mechanism for determining the messages to be copied (Request or Answer), the Result-Code/Experimental Result-Code on which the Message Copy is initiated, and number of retries to be made if the Message Copy attempt to DAS fails. The Message Copy Trigger Point must specify a Message Copy Configuration Set when the message is marked for copying.

Trigger Points mark the message ready for copy, based on the circumstances and requirements specific to the Trigger Points. The Diameter Message Copy feature determines the condition at which the copy needs to made and ensures that the copied message is delivered to DAS. A triggering condition or rule can be configured. The Trigger Points also supply a Message Copy Configuration Set to specify the conditions on which the copy needs to be initiated and the contents to be included in the Copied Message.

A copy of certain Diameter Request messages that transit a DSR network can be used for such functions as bookkeeping and verification or for offering additional services. The criteria or triggering condition to copy a Request to a DAS Peer can be simple or complex, and might be based on the presence of certain AVPs and their values in the Request message and certain Result Codes in the Answer received in response to the Request.

When a Diameter Request meeting the triggering condition is received by the DSR, the message is marked as 'ready to copy' by the entity that processes the message.

When the response to the Request (the Answer) is received, if the Answer contains the matching Result Code as specified by a Message Copy Configuration Set, the resultant action is executed - in the case of Diameter Message Copy, the action would be to copy the Request and optionally the Answer and send the Copied Message to a DAS Peer.

The Message Copy feature copies only the Diameter portion of the Request, and optionally the Answer, matching a triggering condition; the transport and IP layers are not copied. Diameter Message Copy is not a 'port mirror' that replicates everything received on the wire on a specific port to an egress port. Figure 1 depicts this message flow overview:

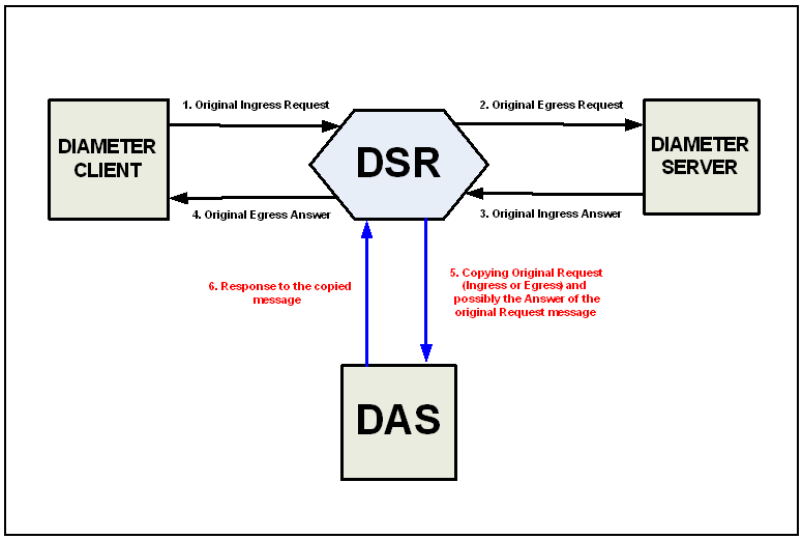

Figure 16: Diameter Message Copy Message Flow

Possible use cases for Diameter Message Copy include the following cases:

- Use Case 1: A copy of all Requests that match certain basic criteria are sent to a DAS. For example, an incoming ULR over the S6a interface. In this case, the operator may wish to send a welcome SMS based on the success of the ULR. (It is assumed that the DAS has additional intelligence to distinguish an initial registration from a re-registration)
- Use Case 2: A copy of all Requests that match some advanced criteria (like the presence of an application level AVP or if its value equals a pre-configured value) are sent to a DAS. For example, a Lawful Intercept server maybe in interested in the registration of a specific IMSI.
- Use Case 3: A DSR Application determines the Requests to be copied to a DAS. For example, the Charging Proxy Application (CPA) marks all messages in a session that has the Called-Station-Id AVP set to a specific value in the ACR-Start message.

Message Copy Trigger Points

The Diameter Message Copy feature can be separated into a trigger action and the actual copy operation. The actual copy operation is performed by the Diameter Routing Function. The trigger action is executed either within the Diameter Routing Function or from a local DSR Application. When a Request message received by the DSR, the different tasks that could process a message can determine whether the messages should be tagged for copy.

The Diameter message to be copied can be the Request Message as it arrived at the DSR Node (Ingress Request Message) or the final processed Request message routed out of the DSR Node (Egress Request Message). The Trigger Point can determine whether the response Answer message received by the DSR (Ingress Answer Message) to the Request message also needs to be copied along with the Request message. The Trigger Point tags the message for copy and uses a Message Copy Configuration Set to convey the details and conditions for copying the message.

Each Trigger Point must specify a Message Copy Configuration Set. If there are multiple Trigger Points acting on the same message (from Mediation or PRT triggering, or both), the Message Copy Configuration Set specified by the last Trigger Point will be used (with its specified Route List).

Note: CPA still provides a Route List in place of a Message Copy Configuration Set. See *Charging Proxy Application (CPA) Message Copy*. Diameter Message Copy implementation ensures that CPA functioning is not affected by the introduction of the Message Copy Configuration Sets.

The copy rules and trigger actions could be implemented as described in the following examples:

- The Charging Proxy Application (CPA) allows configuration of rules based on the value of the Diameter Called-Station-Id AVP in the Diameter Accounting Request (ACR) message. If CPA receives an ACR message with a value in the Called-Station-Id AVP that matches the configured rule, the Message Copy action is triggered.
- A Message Copy trigger can be initiated from the Diameter Peer Routing Rules. Peer Routing Rules determine the Route List based on the characteristics of the egress Request message. The criteria configured in the Peer Routing Rules can also be used for triggering a message copy, by specifying a Message Copy Configuration Set in a Peer Routing Rule.
- The Diameter Mediation feature can trigger a Message Copy, by specifying a Message Copy Configuration Set in a Rule Template Action. See *Rule Templates*.

Diameter Message Copy feature

The Diameter Message Copy feature provides flexible ways to specify the conditions under which the copy of the Request (or both Request and Answer) must be made. It makes use of the existing routing principles supported by DSR to provide routing of the messages to DAS. The Message Copy is performed only after the completion of the original transaction.

Message processing

While Message Copy Trigger Points tag the messages to be copied, the Diameter Message Copy feature in the Diameter Routing Function encodes and copies the messages to the DAS based on the details specified in the Message Copy Configuration Sets.

As a Diameter Request message is passed from the ingress side to the egress side, the message can go through modifications before being routed out to the upstream Peer. During the DSR processing, the Diameter Message header and data portions can get modified; a function like Mediation, a local DSR Application, and the Diameter Routing function could change the message as part of its processing. Thus, the two points of interest in the message processing are: 1) before the Diameter message is modified by DSR, and 2) after all the modifications by DSR and the Diameter message is sent out to the upstream Peer.

Some customers need the Answer messages received for the original Diameter Request messages from the upstream Peer to be copied along with the Request message, because the Answer message contains critical information that will be useful at the DAS while processing the copied data. The Diameter Message Copy feature supports copying the Ingress Answer messages along with the Request messages (Ingress or Egress); the Answer message alone cannot be copied to a DAS. The Diameter Message Copy feature copies to the DAS the ingress Answer received to original Request Message, as described in *Ingress Answer Message Encoding*.

When the Diameter Request message that is marked for copying is sent out, the message is stored as a normal Diameter Pending Transaction. When the Answer message arrives, it has been matched to the Request message, and the message is checked for rerouting. After all required rerouting, the terminating message is checked for copy eligibility. If eligible, the Answer is further qualified as containing the desired Result Code; then the message is copied and routed to a DAS Peer.

The Diameter Message Copy feature can be treated as another form of rerouting. The copy of the original Request and Answer are combined into one single message that is encoded as a copied message, processed as a new Diameter transaction, and passed to Peer Routing for Connection selection and transmission. The new Diameter/copy transaction is processed as any other Diameter Request, requiring a new Answer from the DAS Peer with a qualifying Result Code (separate from the original transaction) to complete the copy transaction. However, with Message Copy, the Answer message from the DAS Peer is released by the Diameter Routing Function and not forwarded on, because the Diameter Routing Function on the local DA-MP was the originator of the transaction. (Message Copy is not performed if DSR generates the Answer, or if the original Request times out.)

After a message is selected for copying, a DAS is selected for routing and the normal existing Diameter routing and congestion handling is applied. Copied Messages are assigned a Message Priority of 2, and are processed in the same way as any Priority 2 message.

Each Diameter Request successfully copied will be treated as a new transaction. When a received Diameter Request is copied it becomes two transactions - one for the original and one for the Message Copy. Thus, a copied Request/Answer transaction deducts two MPS from the net MPS rating of the DSR. No additional flow control or congestion mechanism specific to Message Copy is required. The additional MPS for Message Copy also accounts for copying the original Answer messages to the DAS.

Routing to a DAS Peer

A DAS Peer is treated just as another Diameter Peer. Copied messages will be routed to an available DAS Peer selected from Route Lists configured or specified in the Diameter Routing Function. Route Lists are configured and intended to point to a Peer Node. The DAS Route List to which the message needs to be copied is specified in a Message Copy Configuration Set (or by CPA configuration).

Note: The DAS servers are expected to be direct Peers of the DSR. Message Copy cannot be supported to DAS servers that are connected through other DSRs, relays, and proxy servers.

Only Requests matching the advertised Application-Id are copied to the DAS.

If a message has been marked for Message copy to a certain DAS-Route List and all the available Connections to the Peers in the Route List do not support the Application-Id present in the copied message, the copy is not performed, an Event is raised, and the copy action is ignored.

Note: Diameter Message Copy does not support copying the same message to multiple DAS Peers simultaneously.

If the DSR tries to route the original Diameter Request message to Peer in a Route List and the Answer is not received, the DSR must attempt alternate routing by selecting other Peers in the Route Group and Route List. If alternate routing is attempted, only one copy of the original Request (Ingress or Egress), and optionally the Answer, will be sent to the DAS Peer to avoid flooding the DAS Peer due to failure recovery and rerouting on the signaling side.

The Diameter Message Copy feature evaluates the copy eligibility based only on the original terminating transaction. The Result Code/Experimental Result Code of the terminating Answer is used to evaluate the copy eligibility. This ensures that the copy of the message is sent only once to the DAS, regardless of the number of alternate routing attempts. Message Copy is evaluated based on the value of the Result code/Experimental Result code AVP in the Original terminating Answer. If an Egress Request message is selected for copying, the Egress Request corresponding to the terminating Answer is copied to the DAS.

Regardless of which message is actually copied, the copy action is always performed by the Diameter Message Copy feature only once on the original Diameter Request messages. The Message Copy triggering will not be performed on the rerouted Diameter Request messages. A Diameter Request message can be marked for copy only before the first routing attempt of the original Request message.

The Message Copy triggering could happen multiple times on the Answer Messages in the alternate routing scenario (from Mediation and PRT triggering). Only the last trigger that is set on the original terminating Answer is considered for Message Copy.

DAS Peer Response and Error Handling

The DAS Peer is expected to respond to the copied message with either a 2xxx (Success) or an error Result code/Experimental Result code. When such a response is not received (either due to an unexpected response or outbound Connection failure), a retry mechanism will resend the message until the expected response is received or the maximum number of retries is exhausted. The mechanism consists of a configurable number of retries and a retry timer. If a response is received, it will be discarded after the release of the associated resources. If the intended Route List for the DAS Peer is unavailable, the copy is not performed (or is discarded).

Reroute on Answer based on a DAS Answer response is not supported. Message Copy provides its own rerouting mechanism.

Ingress Answer Message Encoding

When the Message Copy Configuration Set specifies that the Ingress Answer message need to be included in the copied message, the header-stripped Answer message is encoded in the copied Request message in the data portion of a Tekelec-specific 'MsgCopyAnswer' AVP. This AVP has the format described in *Table 107: Tekelec-Specific MsgCopyAnswer AVP Format*.

Table 107: Tekelec-Specific MsgCopyAnswer AVP Format

Byte 1	Byte 2	Byte 3	Byte 4
AVP Code = 2516(0x9d4)			
Flags=10000000	Length = (number of octets including 12 octets of AVP header)		
Vendor ID = 323(0x143)			
Data = Answer Message (Octet String)			

The value of the MsgCopyAnswer AVP has the AVP portion of the received Ingress Answer message. The Diameter header is stripped out from the original Ingress Answer message, and the remaining portion of the message that contains all the AVPs is included as the value of the MsgCopyAnswer AVP, as shown in *Table 108: Portion of the Answer Message Included as Data Value of the MsgCopyAnswer AVP*.

Table 108: Portion of the Answer Message Included as Data Value of the MsgCopyAnswer AVP

Byte 1	Byte 2	Byte 3	Byte 4
Version	Message Length		
Command Flags	Command-Code		
Application-ID			
Hop-by-Hop Identifier			
End-to-End Identifier			
AVPs (This is the only portion included as the value of the 'MsgCopyAnswer' AVP.)			

Rerouting of Copied Messages

The rerouting of the Copied Messages to DAS is different from rerouting the original Request messages. A Copied Message will be retried when the Result Code in the Answer from DAS is different from the one specified in the Message Copy Configuration Set. This is not influenced by the "Reroute on Answer" configured for the Application-Id. The maximum attempts to resend the Copied Message is limited by the Max DAS Retransmission Attempts value specified in the Message Copy Configuration Set. These attempts are not influenced by the maximum reroutes specified in the Routing Option Sets, Application-Id, or Peer configuration. The total transaction life time of a message is controlled by the settings on the ingress Peer node. In the case of a Copied Message, the Local Node is the ingress Peer. Therefore, there is no specific Transaction Lifetime for the Copied Messages. The maximum retry attempts and the Pending Answer Timer configured for the Peers will limit the Total Transaction Lifetime of the Copied Message.

DSR and Message Copy congestion

The Diameter Message Copy feature can be manually enabled or disabled system-wide. The discussions here assume that the Diameter Message Copy feature is enabled.

The Diameter Routing Function can automatically disable the Diameter Message Copy feature if the DA-MP enters into a certain level of congestion. This congestion level at which the Diameter Message Copy feature gets disabled is configurable on the Diameter > Configuration > System Options > Message Copy Options GUI page.

If the local DA-MP enters into congestion based on the value of the configured MP Congestion Level for Message Copy, the Diameter Message Copy feature on that DA-MP will be disabled automatically as a load-shedding mechanism. Messages that are awaiting the copy action - those that have been marked and are awaiting an original Answer from a Diameter Peer - will not be copied. Those that have already been copied to the DAS and are awaiting a response from the DAS to complete the transaction will be processed until normal completion (either an Answer is received from the DAS Peer, or the number of DAS retries has been exhausted and the Copy pending transaction is deleted); that is, their transactions will not be deleted by the Pending Transaction Manager.

An original Request is not eligible for copy until a matching Answer is received from the upstream Peer. Between when a message is marked for copy and is actually ready to be copied, the local DA-MP's status can change. Therefore, the Diameter Message Copy feature will be declared as disabled when the next Answered marked message is processed by the Pending Transaction Manager to have a copy made and the local DA-MP has congested (based on the Message Copy MP Congestion Level). A Message Copy alarm will also be raised at this time.

The Diameter Message Copy feature will be enabled again when the local DA-MP Congestion Level abates (based on the configured Message Copy MP Congestion Level) and an attempt is made to copy a message that is marked for copy. The Message Copy disabled alarm will be cleared only when the local DA-MP congestion (Message Copy) is abated below the configured Message Copy MP Congestion Level and a message marked for copy is processed by the Diameter Message Copy feature.

If the Diameter Message Copy feature processing capacity reaches 100% congestion, further Message Copy actions cannot be completed. In order to process the messages, the Diameter Message Copy feature will not be disabled; but an alarm is raised indicating the processing capacity status until the congestion abates.

Message Copy Configuration Sets

A Message Copy Configuration Set (MCCS) is a collection of attributes that determine the messages to be copied (Request or optionally the Answer), the Result code/Experimental Result code on which

the Message Copy is initiated, and the number of retries to be made if the Message Copy attempt to the DAS fails. A Message Copy Trigger Point must specify a Message Copy Configuration Set when the message is marked for copying.

Note: The Diameter Routing Function uses the values in the Default Message Copy Configuration Set for Charging Proxy Application (CPA) Message Copy. CPA specifies the Route List for the DAS that is to be used for the CPA Message Copy. See *Charging Proxy Application (CPA) Message Copy*

The DSR supports up to 100 Message Copy Configuration Sets. The following elements can be configured for each Message Copy Configuration Set; the fields are described in *Message Copy Configuration Set elements*:

- **Message Copy Configuration Set Name** - Each Message Copy Configuration Set is assigned a unique name. A default Message Copy Configuration Set named "Default" is always provided, and can be edited but not deleted.
- **Route List of the DAS Node** - The required Route List of the DAS Node element of the MCCS specifies the Route List to use for copying the message. This Route List consists of either a Peer Route Group or Connection Route Group. The DAS Peers are treated like any other Diameter Peers with respect to Connection establishment and management. The CEx messages are exchanged upon establishing a Connection and the DWx/DPx messages are exchanged as needed. Only Requests matching the advertised Application-Id are copied to the DAS. If a message has been marked for Message Copy to a certain DAS Route List and all the available Connections to the Peers in the Route List do not support the Application-Id present in the copied message, the copy is not performed, an Event is raised, and the copy action is ignored.

  The Route List must exist before the MCCS can select it. Route Groups must be configured before Route Lists can be configured in Diameter Configuration.

  The DAS servers are expected to be direct Peers of the DSR. Message Copy is not supported to DAS servers that are connected through other DSRs, relays, and proxy servers.

- **Message Copy Request Type** - The DSR alters the original Request significantly as it traverses the DSR. Depending on the function provided by the DAS, the DAS might be interested in seeing the Request prior to or after the modifications made by the DSR. The DAS can receive a copy of the Original Ingress Request or the Original Egress Request. The Original Ingress Request is the Request as received prior to any manipulation by the DSR. The Original Egress Request is the Request as sent by the DSR to the upstream Peer. The default is Original Ingress Request.
- **Ingress Answer Included** - In some cases, DAS must be interested in the contents of the original Answer received for the Request message, for accomplishing the function. When the Ingress Answer Included element is set to YES, the Diameter Message Copy feature copies the ingress Answer that is received for the original Request Message to the DAS, as described in *Ingress Answer Message Encoding*. The default is NO, Answer not included.
- **Original Answer Result Code for Message Copy** - The Result Code of the Answer messages corresponding to the Original Requests could influence the Message Copy action. For example, a DAS may not be interested in receiving a copy of the Request if the Original Transaction ended with an Answer that contained a non-2xxx Result Code/Experimental Result Code. The DAS can receive a copy of the message based on the outcome of the Original Transaction. If 2xxx is selected, the Diameter Message Copy feature is performed only if the value of the Result Code/Experimental Result Code AVP in the Original Answer is a 2xxx. If Any Result Code is selected, the Message Copy is performed regardless of the Result Code/Experimental Result Code AVP value as long as the DSR receives an Answer from the upstream Peer. The default is to copy on 2xxx only.

  The Diameter Message Copy is not performed if the DSR generates the Answer or if the original Request times out.

The DSR could attempt alternate routing on a given Request, but in such cases the Diameter Message Copy is attempted just once regardless of the number of alternate routing attempts. Message Copy is evaluated based on the value of the Result Code/Experimental Result Code AVP in the Original terminating Answer.

- **DAS Answer Result Code** - DAS servers are expected to respond with a 2xxx Result Code or an error Result Code/Experimental Result Code upon the receipt of the copied message. If an appropriate Answer is not received, the DSR retransmits the copied message for the configured maximum number of times until the appropriate response is received. The DAS Message Copy Answer Result Code can be configured with one of the following choices:
  - 2xxx Result Code/Experimental Result Code in the DAS Answer
  - Any Result Code/Experimental Result Code in the DAS Answer
- **Max DAS Retransmission Attempts** - This value determines the maximum number of times a copied message is retransmitted using the specified Route List, until the DAS Answer containing the specified Result Code is received.

  In the event that an appropriate Answer is not received, the DSR retransmits the copied message for this configured number of times until the appropriate response is received. The default is 0 and the range is 0-4. If the value is 0, there will be no retransmission attempts.

Diameter Configuration for Message Copy

The following Diameter Configuration components need to be configured if the Diameter Message Copy feature will be used in the system:

- For PRT-Triggered Message Copy:
  - One or more Route Groups
  - One or more Route Lists
  - One or more Message Copy Configuration Sets
  - One or more Peer Route Tables
  - One or more Peer Routing Rules

    A Message Copy Configuration Set must be specified in each Peer Routing Rule that will be used to trigger Message Copy.

  - Set the **Message Copy Feature** element to Enabled in **Diameter > Configuration > System Options**
- For Mediation-Triggered Message Copy:
  - One or more Route Groups
  - One or more Route Lists
  - One or more Message Copy Configuration Sets

    A Message Copy Configuration Set must be specified in each Rule Template Action that will be used to trigger Message Copy for Mediation.

  - Set the **Message Copy Feature** element to Enabled in **Diameter > Configuration > System Options**
- For Charging Proxy Application (CPA) Message Copy:
  - One or more Route Groups

- One or more Route Lists
- Message Copy must be configured correctly in CPA configuration as described in the *Charging Proxy Application (CPA) and Offline Charging Solution User Guide* and Help.

  CPA specifies the Diameter-configured Route List to use for the DAS.

  The Diameter Routing Function uses the values in the Default Message Copy Configuration Set (except for the Route List of the DAS Node).

- Set the **Message Copy Feature** element to Enabled in **Diameter > Configuration > System Options**

PRT-Triggered Message Copy

A Peer Routing Rule can be configured such that Request messages routed through that Peer Routing Rule can be marked for copying to a Diameter Application Server (DAS). The Diameter Message Copy feature uses the contents and conditions that are specified in a Message Copy Configuration Set (MCCS) for copying the message. If there is valid MCCS configured in the Peer Routing Rule, the Diameter Routing Function marks the message for copy and attaches the specified MCCS. The Diameter Message Copy feature validates the transaction using the MCCS and copies the message to the DAS.

Charging Proxy Application (CPA) Message Copy

The Diameter Message Copy feature using Message Copy Configuration Sets is backward compatible with the Trigger Points specifying only the Route Lists.

CPA configuration specifies only the DAS Route List for copying to the DAS (Route Lists must be configured in Diameter before they can be configured in CPA); CPA does not specify any Message Copy Configuration Sets. The additional details for the Message Copy of a CPA message are retrieved from the Default Message Copy Configuration Set.

Only Request messages are copied to the DAS Destination. The copy operation is carried out when the corresponding Answer message is received.

During a new DSR installation, the Default Message Copy Configuration Set is created on the DSR, and initialized with the values shown in *Table 109: Initial Values in the Default Message Copy Configuration Set*.

Table 109: Initial Values in the Default Message Copy Configuration Set

Element	Value
Message Copy Configuration Set Name	Default
Route List of DAS	(no value)
Message Copy Request Type	Original Ingress Request
Ingress Answer Included	No
Original Answer Result code For Message Copy	2xxx Result Code/Experimental Result Code
DAS Answer Result Code	2xxx Result Code/Experimental Result Code
Max DAS Retransmission Attempts	0

On upgrade from a DSR source release that does not support Message Copy Configuration Sets to a DSR that supports Message Copy Configuration Sets, the Message Copy values that are configured in the Diameter > Configuration > System Options > Message Copy tab of the source release are moved to the Default Message Copy Configuration Set of the target release.

The Default Message Copy Configuration Set can be edited if different values are needed for CPA Message Copy.

Mediation-Triggered Diameter Message Copy

The Mediation Rule Template "Message Copy" Action can be defined to trigger Diameter Message Copy for messages that are processed by Diameter Mediation.

The Message Copy Action triggers Diameter Message Copy, and specifies the Diameter-configured Message Copy Configuration Set (MCCS) that contains the Request/Answer content criteria to be used by the Diameter Message Copy feature to copy the message to a DAS. The Message Copy Configuration Set specifies a configured Route List for the DAS. See *Message Copy Configuration Set configuration*.

Mediation Message Copy can be performed only for Request messages; the Message Copy Action is ignored if set at Mediation Trigger Point ATP10 (Diameter Answer message prior to be forwarded to connection).

If Diameter Message Copy is triggered for the same message from multiple locations, the Message Copy Configuration Set for the latest Message Copy triggering is used.

In the case of Request re-route due to invalid Result code, only the Message Copy Configuration Set that is associated with the Answer that completes the transaction at ATP1 is considered.

The Message Copy is performed after the completion of the original transaction. The Copied Message is not processed by the Mediation Triggering Points.

Chapter 4

Maintenance

Topics:

- *Overview.....271*
- *Route List maintenance.....271*
- *Route Group maintenance.....272*
- *Peer Node maintenance.....274*
- *Connection maintenance.....275*
- *Egress Throttle Groups maintenance.....282*
- *Application maintenance.....288*
- *DA-MP maintenance.....290*

The **Diameter > Maintenance** pages display status information for Route Lists, Route Groups, Peer Nodes, Connections, Egress Throttle Groups, DSR Applications, and Diameter Agent Message Processors (DA-MPs).

On the **Diameter > Maintenance > ConnectionsDiameterMaintenance** page you can enable and disable Connections.

On the **Diameter > Maintenance > Applications** page you can enable and disable DSR Applications.

Overview

The **Diameter > Maintenance** pages allow you to view the following information and perform the following actions:

- On the **Diameter > Maintenance** pages you can view status information for Route Lists, Route Groups, Peer Nodes, Connections, Egress Throttle Groups, DSR Applications, and Diameter Agent Message Processors (DA-MPs).
- On the **Diameter > Maintenance > Connections** page you can enable and disable Connections.
- On the **Diameter > Maintenance > Applications** page you can enable and disable DSR Applications.

Route List maintenance

The **Diameter > Maintenance > Route Lists** page displays the Minimum Availability Weight and Route Group assignments for configured Route Lists. You can also view the Priority, Active/Standby assignments, Provisioned Capacity, Current Capacity, and the Status of Route Groups assigned to a Route List.

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

On the **Diameter > Maintenance > Route Lists** page, you can perform the following actions:

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

Route List maintenance elements

This table describes fields on the Route Lists maintenance page.

Table 110: 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

Field	Description
	• 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
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.

Viewing Route List status

Use this task to view the current status of configured Route Lists.

Select **Diameter** > **Maintenance** > **Route Lists**.
The **Diameter > Maintenance > Route Lists** page appears.

Route Group maintenance

The **Diameter > Maintenance > Route Groups** page allows you to view the Provisioned Capacity 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.

On the **Diameter > Maintenance > Route Groups** page, you can perform the following actions:

- Filter the list of Route Groups to display only the desired Route Groups.
- Sort the list by **Route Group Name**, in ascending or descending order, by clicking the column heading. The default order is ascending ASCII order.
- Click the **+** in any entry in the **Peer Node/Connection** field to view information about the Peer Nodes or Connections in a Route Group.
- With an entry in the **Peer Node/Connection** field expanded, click the Peer Node or Connection Name to go to the maintenance page for the Peer Node or Connection.
- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.

Route Group maintenance elements

Table 111: Route Group Maintenance Elements describes fields on the **Diameter > Maintenance Route Groups** page.

Table 111: 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.
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

Field	Description
	• 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.

Viewing Route Group status

Use this task to view the status of configured Route Groups.

Select **Diameter** > **Maintenance** > **Route Groups**.
The **Diameter > Maintenance > Route Groups** page appears.

Peer Node maintenance

The **Diameter > Maintenance > Peer Nodes** page provides the operational status of Peer Node connections, including a reason for the status.

On the **Diameter > Maintenance > Peer Nodes** page, you can perform the following actions:

- Filter the list of Peer Nodes to display only the desired Peer Nodes.
- Sort the list by a column, in ascending or descending order, by clicking the column heading (except **MP Server Hostname** and **Connection**). The default order is by **Peer Node Name** in ascending ASCII order.
- Click the **+** in any entry in the **Connection** field to view information about the Connections associated with the Peer Node.
- With an entry in the **Connection** field expanded, click the Connection Name to go to the maintenance page for the Connection.
- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.

Peer Node maintenance elements

This table describes fields on the Peer Nodes maintenance page.

Table 112: 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

Field	Description
	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 • 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.

Viewing Peer Node status

Use this task to view the current status of configured Peer Nodes.

Select **Diameter** > **Maintenance** > **Peer Nodes**.
The **Diameter > Maintenance > Peer Nodes** page appears.

Connection maintenance

The **Diameter > Maintenance > Connections** page allows you to view information about existing connections, including the operational status of each connection.

On the **Diameter > Maintenance > Connections** 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.
- Click a Local Node to go the configuration page for the Local Node.
- Click a Peer Node to go to the maintenance page or the Peer Node.

- Click a Message Priority or Egress Message Throttling Configuration Set to go to the configuration page for the Configuration Set.
- 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 *Viewing, Printing, and Saving Diagnostics Tool Reports*.

Connection maintenance elements

This table describes fields on the Connections maintenance page.

Table 113: 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.
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)

Field	Description
	• 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
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.

Field	Description
	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

Viewing Connection status

Use this task to view the current status of configured connections.

Select **Diameter** > **Maintenance** > **Connections**.
The **Diameter > Maintenance > Connections** page appears.

Enabling Connections

Use the following steps to enable one or more connections.

1. Select **Diameter** > **Maintenance** > **Connections**.
   The **Diameter > Maintenance > Connections** page appears.
2. Select 1 - 20 connections to enable.

   To select multiple connections, press the CTRL key when selecting each connection. To select multiple contiguous connections, click the first connection you want, then press the SHIFT key and select the last connection you want. All the connections between are also selected.
3. Click **Enable**.
   A confirmation box appears.
4. Click **OK**.
   The selected connections are enabled.

   If any of the selected connections no longer exist (they have been deleted by another user), an error message is displayed, but any selected connections that do exist are enabled.

Enabling All Connections

Use the following steps to enable all connections that are displayed as result of the application of a filter. If a filter is applied, then all connections that meet the filter requirements and that are currently disabled will be enabled. If no filter is applied, then **all** currently disabled connections will be enabled.

1. Select **Diameter** > **Maintenance** > **Connections**.
   The **Diameter > Maintenance > Connections** page appears.
2. Optionally, click **Filter** and add up to four filters to limit the number of connections displayed. Click **Go** to apply the filter.
3. Click **Enable All**.
   A confirmation box appears.
4. Click **OK**.
   The connections are enabled.

   If any of the selected connections no longer exist (they have been deleted by another user), an error message is displayed, but any selected connections that do exist are enabled.

Disabling Connections

Use the following steps to disable one or more connections.

1. Select **Diameter** > **Maintenance** > **Connections**.
   The **Diameter > Maintenance > Connections** page appears.
2. Select 1 - 20 connections to disable.

   To select multiple connections, press the CTRL key when selecting each connection. To select multiple contiguous connections, click the first connection you want, then press the SHIFT key and select the last connection you want. All the connections between are also selected.
3. Click **Disable**.

A confirmation box appears.

4. Click **OK**.
   The selected connections are disabled.

   If any of the selected connections no longer exist (they have been deleted by another user), an error message is displayed, but any selected connections that do exist are disabled.

Disabling All Connections

Use the following steps to disable all connections that are displayed as result of the application of a filter. If a filter is applied, then all connections that meet the filter requirements and that are currently enabled will be disabled. If no filter is applied, then **all** currently enabled connections will be disabled.

1. Select **Diameter > Maintenance > Connections**.
   The **Diameter Maintenance Connections** page appears.
2. Optionally, click **Filter** and add up to four filters to limit the number of connections displayed. Click **Go** to apply the filter.
3. Click **Disable All**.
   A confirmation box appears.
4. Click **OK**.
   The connections are disabled.

   If any of the selected connections no longer exist (they have been deleted by another user), an error message is displayed, but any selected connections that do exist are disabled.

Viewing statistics for an SCTP connection

Use the following steps to view statistics for an SCTP connection.

1. Select **Diameter** > **Maintenance** > **Connections**.
   The **Diameter > Maintenance > Connections** page appears.
2. Select an SCTP connection that has an Operational Status of Available or Degraded.
3. Click **SCTP STATISTICS**.
   The **Diameter > Maintenance > Connections > SCTP Statistics** page appears.

Connections SCTP Statistics

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

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

On the **Diameter > Maintenance > Connections > SCTP Statistics** page, you can do the following actions:

- Filter the list of paths to display only the desired paths.
- Get information about the SCTP connection by clicking **Info**.
- Sort the list by **IP Address**, in ascending or descending order, by clicking the column heading. The default order is ascending ASCII order.

- Refresh the statistics by clicking **Update**.

Connections SCTP Statistics elements

This table describes fields on the **Diameter > Maintenance > Connections > SCTP Statistics** page.

Table 114: Connections SCTP Statistics Elements

Field	Description
IP Address	The Peer Remote IP Address associated with the path
State	Indicates whether the path is active or inactive
Congestion Window (cwnd)	The maximum amount of data, in bytes, that can be sent before an acknowledgment must be received
Smoothened Round Trip Time (srtt) (ms)	The round-trip time, in milliseconds, associated with the path, smoothened to remove sample-to-sample fluctuations
Retr. Timeout (rto) (ms)	Retransmission timeout; the amount of time, in milliseconds, to wait for an acknowledgment before declaring a transmission error
Path MTU (pmtu)	Maximum transmission unit; the maximum data unit size, in bytes, that can be sent on the path without fragmentation

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 **Diameter > Maintenance > Connections** 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 **Diameter > Maintenance > Connections** page is refreshed.

Egress Throttle Groups maintenance

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

Each function has an individual Administration State (Enable/Disable) and Operational Status.

Table 115: Egress Throttle Groups Admin States

Admin State	Description
Enable	ETG status monitoring is enabled for the function.
Disable	ETG status monitoring is disabled for the function. All monitoring is stopped in this state and alarms are cleared.

The Egress Throttle Group maintenance status is displayed on the **Diameter > Maintenance > Egress Throttle Groups** GUI page, on the NOAM in DSR 2-tiered topology and on the SOAM in DSR 3-tiered topology. Egress Throttle Groups use the Leader sourcing method for reporting of maintenance status. The Leader sourcing method is used because each DA-MP will have identical status data; only the DA-MP Leader will report the maintenance status to the GUI.

Table 116: ETG Operational Status

ETG Operational Status	Description
Available	ETG monitoring is active and Request throttling is not occurring for this ETG.
Degraded	ETG monitoring is active and Request throttling is occurring for this ETG. Some Requests may be getting throttled based on their Priority

ETG Operational Status	Description
Inactive	ETG monitoring is inactive and Request Throttling is not occurring for this ETG. The Operational Reason indicates why this ETG is Inactive. When Operational Reason is "Disabled" the ETG is Inactive due to maintenance actions. When the Operational Reason is "SMS Service Degraded" or "No DA-MP Leader" the ETG is Inactive due to a fault condition.

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

Table 117: ETG Operational Reason

ETG Operational Reason	Description
Disabled	ETG is "Disabled" due to maintenance actions.
Normal	No Requests are getting throttled for this ETG for the function.
Congestion Level 1	Request throttling is happening for Requests with Priority 0.
Congestion Level 2	Request throttling is happening for Requests with Priority 0 and 1.
Congestion Level 3	Request throttling is happening for Requests with Priority 0, 1, and 1.
SMS Service Degraded	ETG monitoring is Inactive due to "Degraded" status reported to the Diameter Routing Function.
No DA-MP Leader	ETG Monitoring is Inactive due to HA reporting "No DA-MP Leader" condition to the Diameter Routing Function.

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

Egress Throttle Groups maintenance fields are described in *Egress Throttle Groups maintenance elements*

If the column data is not present in the database, the columns for the Egress Throttle Group Name are displayed as **Unk**.

On the **Diameter > Maintenance > Egress Throttle Groups** page, you can perform the following actions:

- Filter the list of Egress Throttle Groups to display only the Egress Throttle Groups.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by **Egress Throttle Groups** in ascending ASCII order.
- Select one or more (up to 20) Egress Throttle Groups records at a time.
- Enable Rate Limiting for up to 20 selected **Egress Throttle Groups**.

- Disable Rate Limiting for up to 20 selected **Egress Throttle Groups**.
- Enable Pending Transaction Limiting for up to 20 selected **Egress Throttle Groups**.
- Disable Pending Transactions Limiting for up to 20 selected **Egress Throttle Groups**.
- Prevent the page from automatically refreshing every 10 seconds, by clicking the **Pause updates** check box.

Egress Throttle Groups maintenance elements

This table describes fields on the Egress Throttle Groups maintenance page.

Table 118: Egress Throttle Groups Maintenance Elements

Field	Description
Egress Throttle Group Name	Name of the Egress Throttle Group.
Rate Limiting Admin State	Rate Limiting Admin State can be Enabled or Disabled.
Rate Limiting Operational Status	Rate Limiting Operational Status can be: • Available: at least one Egress Throttle Groups peer or connection is available. • Degraded: the Egress Throttle Groups peer or connection is not unavailable but it is not operating as expected. The Rate Limiting Operational Reason field provides additional information on this status. • Inactive: all connections for an Egress Throttle Group are unavailable. The Rate Limiting Operational Reason field provides additional information on this status. • Unk: data is not available in the database.
Rate Limiting Operational Reason	Rate Limiting Operational Reason as corresponding to the Rate Limiting Operational Status: • Available - Normal • Degraded - Congestion Level 1, Congestion Level 2, Congestion Level 3 • Inactive - SMS Service Degraded, No DA-MP Leader, Disabled • Unk - Unk The cell background color associated with value of Pending Transaction Limiting Operational Reason is as follows: • Disabled - normal/no special coloring • Normal - normal/no special coloring • SMS Service Degraded - red • No DA-MP Leader - red • Unk - red • Congestion Level 1 - yellow • Congestion Level 2 - yellow • Congestion Level 3 - yellow

Field	Description
Smoothed Rate	The rate resulting from the application of the Smoothing Factor to the Egress Request Rate.
Pending Transaction Limiting Admin State	Pending Transaction Limiting Admin State can be Enabled or Disabled.
Pending Transaction Limiting Operational Status	Pending Transaction Limiting Operational Status can be: • Available: at least one Egress Throttle Groups peer or connection is available. • Degraded: the Egress Throttle Groups peer or connection is not unavailable but it is not operating as expected. The Pending Transaction Limiting Operational Reason field provides additional information on this status. • Inactive: all connections for an Egress Throttle Group are unavailable. The Pending Transaction Limiting Operational Reason field provides additional information on this status. • Unk: data is not available in the database.
Pending Transaction Limiting Operational Reason	Pending Transaction Limiting Reason as corresponding to the Pending Transaction Limiting Operational Status: • Available - Normal • Degraded - Congestion Level 1, Congestion Level 2, Congestion Level 3 • Inactive - SMS Service Degraded, No DA-MP Leader, Disabled • Unk - Unk The cell background color associated with value of Pending Transaction Limiting Operational Reason is as follows: • Disabled - normal/no special coloring • Normal - normal/no special coloring • SMS Service Degraded - red • No DA-MP Leader - red • Unk - red • Congestion Level 1 - yellow • Congestion Level 2 - yellow • Congestion Level 3 - yellow
Number of Pending Transactions	The combined number of Pending Transactions for the Peers and Connections of an ETG.
Time of Last Update	Displayed as yyyy-month name-date hr:min:sec UTC.

Viewing Egress Throttle Groups status

Use this task to view the current status of configured Egress Throttle Groups .

Select **Diameter** > **Maintenance** > **Egress Throttle Groups** .
The **Diameter > Maintenance > Egress Throttle Groups** page appears.

Enabling Egress Throttle Groups Rate Limiting

Use the following procedure to Enable Egress Throttle Groups Rate Limiting.

The Egress Throttle Groups Rate Limiting Admin State of Egress Throttle Groups can be updated irrespective of the Operational Status of the associated Peer Node Connections.

1. Select **Diameter** > **Maintenance** > **Egress Throttle Groups**.
   The **Diameter > Maintenance > Egress Throttle Groups** page appears.
2. Select at least 1, but no more than 20 Egress Throttle Groups to Disable.

   To select multiple Egress Throttle Groups, press and hold the CTRL key when selecting each Egress Throttle Group. To select multiple contiguous Egress Throttle Groups, click the first Egress Throttle Group to be selected, then press the SHIFT key and select the last Egress Throttle Group to be selected. All Egress Throttle Groups between are also selected.
3. Click **Enable Rate Limiting**.
   a) A confirmation box appears if between 1 and 20 Egress Throttle Group Names are selected.
   Click **OK** in the confirmation box to Enable the selected Egress Throttle Group Names.
   Click **Cancel** in the confirmation box to cancel the Enable action. The Admin State of the selected Egress Throttle Groups remains unchanged.
   If **OK** is clicked and any of the following conditions exist, an error message appears:
   - Any of the selected Egress Throttle Groups do not exist in the database.
   - Any of the selected Egress Throttle Groups do not have Egress Throttle Groups Rate Limiting configured.

   b) An Alert Box is displayed if more than 20 Egress Throttle Group Names are selected.

Disabling Egress Throttle Groups Rate Limiting

Use the following steps to Disable Egress Throttle Groups Rate Limiting.

The Egress Throttle Groups Rate Limiting Admin State of Egress Throttle Groups can be updated irrespective of the Operational Status of the associated Peer Node Connections.

1. Select **Diameter** > **Maintenance** > **Egress Throttle Groups**.
   The **Diameter > Maintenance > Egress Throttle Groups** page appears.
2. Select at least 1, but no more than 20 Egress Throttle Groups to Disable.

   To select multiple Egress Throttle Groups, press and hold the CTRL key when selecting each Egress Throttle Group. To select multiple contiguous Egress Throttle Groups, click the first Egress Throttle Group to be selected, then press the SHIFT key and select the last Egress Throttle Group to be selected. All Egress Throttle Groups between are also selected.
3. Click **Disable Rate Limiting**.
   a) A confirmation box appears if between 1 and 20 Egress Throttle Groups are selected.
   Click **OK** in the confirmation box to Disable the selected Egress Throttle Groups.
   Click **Cancel** in the confirmation box to cancel the Disable action. The Admin State of the selected Egress Throttle Groups remains unchanged.
   If **OK** is clicked and any of the following conditions exist, an error message appears:
   - Any of the selected Egress Throttle Groups do not exist in the database.

- Any of the selected Egress Throttle Groups do not have the Egress Throttling Groups Rate Limiting configured.

b) An Alert Box is displayed if more than 20 Egress Throttle Groups are selected.

Enabling Egress Throttle Groups Pending Transaction Limiting

Use the following steps to Enable Egress Throttle Groups Pending Transaction Limiting.

The Egress Throttle Groups Pending Transaction Limiting Admin State of Egress Throttle Groups can be updated irrespective of the Operational Status of the associated Peer Node Connections.

1. Select **Diameter** > **Maintenance** > **Egress Throttle Groups**.
   The **Diameter > Maintenance > Egress Throttle Groups** page appears.
2. Select at least 1, but no more than 20 Egress Throttle Groups to Disable.

   To select multiple Egress Throttle Groups, press and hold the CTRL key when selecting each Egress Throttle Group. To select multiple contiguous Egress Throttle Groups, click the first Egress Throttle Group to be selected, then press the SHIFT key and select the last Egress Throttle Group to be selected. All Egress Throttle Groups between are also selected.
3. Click **Enable Pending Transaction Limiting**.
   a) A confirmation box appears if between 1 and 20 Egress Throttle Group Names are selected.
   Click **OK** in the confirmation box to Enable the selected Egress Throttle Group Names.
   Click **Cancel** in the confirmation box to cancel the Enable action. The Admin State of the selected Egress Throttle Groups remains unchanged.
   If **OK** is clicked and any of the following conditions exist, an error message appears:

   - Any of the selected Egress Throttle Groups do not exist in the database.
   - Any of the selected Egress Throttle Groups do not have Egress Throttling Groups Pending Transaction Limiting configured.

   b) An Alert Box is displayed if more than 20 Egress Throttle Groups are selected.

Disabling Egress Throttle Groups Pending Transaction Limiting

Use the following steps to Disable Egress Throttle Groups Pending Transaction Limiting.

The Egress Throttle Groups Pending Transaction Limiting Admin State of Egress Throttle Groups can be updated irrespective of the Operational Status of the associated Peer Node Connections.

1. Select **Diameter** > **Maintenance** > **Egress Throttle Groups**.
   The **Diameter > Maintenance > Egress Throttle Groups** page appears.
2. Select at least 1, but no more than 20 Egress Throttle Groups to Disable.

   To select multiple Egress Throttle Groups, press and hold the CTRL key when selecting each Egress Throttle Group. To select multiple contiguous Egress Throttle Groups, click the first Egress Throttle Group to be selected, then press the SHIFT key and select the last Egress Throttle Group to be selected. All Egress Throttle Groups between are also selected.
3. Click **Disable Pending Transaction Limiting**.
   a) A confirmation box appears if between 1 and 20 Egress Throttle Groups are selected.
   Click **OK** in the confirmation box to Disable the selected Egress Throttle Groups.

Click **Cancel** in the confirmation box to cancel the Disable action. The Admin State of the selected Egress Throttle Groups remains unchanged.
If **OK** is clicked and any of the following conditions exist, an error message appears:

- Any of the selected Egress Throttle Groups do not exist in the database.
- Any of the selected Egress Throttle Groups do not have the Egress Throttling Pending Transaction Limiting configured.

b) An Alert Box is displayed if more than 20 Egress Throttle Groups are selected.

Application maintenance

The **Diameter > Maintenance > Applications** page allows you to view state and congestion information about existing DSR applications.

On the **Diameter > Maintenance > Applications** page, you can perform the following actions:

- Filter the list of Applications to display only the desired Applications.
- Sort the list by column, in ascending or descending order, by clicking the column heading. The default order is by **DSR Application Name** in ascending ASCII order.
- Change the Admin State of a selected DSR Application to Enabled or Disabled on a selected MP Server. See *Enabling Applications* and *Disabling Applications*.
- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.

Applications maintenance elements

The following table describes fields on the Applications maintenance page.

Table 119: 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

Field	Description
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.	

Viewing Application status

Use this task to view the current status of configured applications.

Select **Diameter** > **Maintenance** > **Applications**.
The **Diameter > Maintenance > Applications** page appears.

Enabling Applications

Use this task to enable one or more applications.

Applications are enabled only on the MP servers shown in the rows you select.

1. Select **Diameter** > **Maintenance** > **Applications**.
   The **Diameter > Maintenance > Applications** page appears.
2. Select one or more applications to enable.

   To select multiple applications, press the CTRL key when selecting each application. To select multiple contiguous applications, click the first application you want, then press the SHIFT key and select the last application you want. All the applications between are also selected.
3. Click **Enable**.
   A popup window appears.
4. Click

   - **OK** to enable the selected applications and bring the applications to the Available Operational State.
   - **Cancel** to return to the **Diameter > Maintenance > Applications** page without enabling the applications.

   If **OK** is clicked and an application no longer exists in the system (it was deleted by another user), an error message is displayed and the **Diameter > Maintenance > Applications** page is refreshed.

Disabling Applications

Use this task to disable one or more applications.

Applications are disabled only on the MP servers shown in the rows you select.

1. Select **Diameter** > **Maintenance** > **Applications**.
   The **Diameter > Maintenance > Applications** page appears.
2. Select one or more applications to disable.

   To select multiple applications, press the CTRL key when selecting each application. To select multiple contiguous applications, click the first application you want, then press the SHIFT key and select the last application you want. All the applications between are also selected.
3. Click **Disable**.

A confirmation box appears.

4. Click
   - **OK** to disable the selected applications and bring the applications to the Unavailable Operational State.
   - **Cancel** to return to the **Diameter > Maintenance > Applications** page without disabling the applications.

   If **OK** is clicked and an application no longer exists in the system (it was deleted by another user), an error message is displayed and the **Diameter > Maintenance > Applications** page is refreshed.

DA-MP maintenance

The **Diameter > Maintenance > DA-MPs** page allows you to view state and congestion information about Diameter Agent Message Processors.

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

- 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.

  If there are more tabs than fit on one page, click the left and right arrow buttons to scroll through the tabs, or click the down arrow button to select a specific tab from a menu.
- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.

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

DA-MPs maintenance elements

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

Table 120: 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,

Field	Description
	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"	
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

Field	Description
	• Congestion level of the peer DA-MP • Status of the DSR Process running on the peer DA-MP
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.

Viewing DA-MP status

Use this task to view the current status of configured Diameter Agent Message Processors.

Select **Diameter** > **Maintenance** > **DA-MPs**.
The **Diameter > Maintenance > DA-MPs** page appears.

Chapter 5

Reports

Topics:

- *Overview.....294*
- *Generating Diagnostics Tool Reports.....294*
- *Updating and Viewing MP Statistics (SCTP) Reports.....296*

The Diameter Reports GUI pages provide access to the following reports:

- Diagnostics Tool reports
- MP Statistics (SCTP) reports

Overview

The Diameter Reports GUI pages provide access to the following reports:

- Diagnostics Tool reports

  The DSR Diagnostics Tool provides the capability to test Mediation Rule Templates that are in "Test" or "Active" state before they are subjected to live traffic in the network. A test message is injected into the system on a connection that is in Test Mode (see *Connection maintenance*). At various tracepoints, 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. The Diagnostics Tool Reports can be used to view the logged information for each test.

- MP Statistics (SCTP) reports

  The **MP Statistics (SCTP) Reports** 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.

Generating Diagnostics Tool Reports

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

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

All incoming messages on a test connection are marked as TestMode messages. When the **Diagnose Start** button is clicked on the **Diameter > Maintenance > Connections** 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.

Use this task to generate Diagnostics Tool reports from the test logs.

1. Select **Diameter** > **Reports** > **Diagnostics Tool**.
   The **Diameter > Reports > Diagnostics Tool** page appears.
2. Select zero records, or select one or more connection records under one or more connection names in the **Connection** list.
   - If zero records are selected, the report will include all available Diagnostics Tool data.
   - If one or more records are selected, the report will include data for the selected test runs.
3. Click the **Report** button.

   The **Diameter > Reports > Diagnostics Tool [Report]** page appears and displays the generated report. You can save and print the report.

Viewing, Printing, and Saving Diagnostics Tool Reports

Use this task to view, print, and save reports that are generated from Diagnostics Tool test logs.

When the **Report** button is clicked on the **Diameter > Reports > Diagnostics Tool** page, a report is generated for all available or the selected test records.

The report has two parts:

- **Title Block**

  The Title Block contains the following information:

  - <Application Name> Diagnostics Tool Report
  - Report Generated: <time and date in UTC>
  - From: <active/standby><server Role> on host <Hostname>
  - Report Version: <application version>
  - User: userid of the GUI user who generated the report>

- **Section Block**

  One or more Section Blocks follow the Title Block. Each Section Block corresponds to one test run on one connection.

  Each section in a Section Block corresponds to reports for a test run. A section displays the following header information:

  - Report for <connection name>
  - Test run begun: <timestamp when the test run was started>

  Each message that was diagnosed in a test run is identified by a PDU ID. The log entries corresponding to the message are reported in ascending order of the timestamp.

  Each subsection has the following line as a header: `PDU ID <pduId>`. The heading is followed by the zero or more lines of log entries corresponding to the PDU, in the following format: `<timestamp> <tracepoint name> : <log text>`.

  For example:

```
Report for Connection1
Test Run begun: Tue May 24 19:51:39 2011 UTC
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-

PDU ID 4
2011-May-16 10:46:10 UTC Tracepoint0 :Message Received
2011-May-16 10:49:51 UTC Tracepoint1 :Message Sent to DRL
.....................................................................

PDU ID 5
2011-May-18 04:18:25 UTC Tracepoint0 : Message Received
.....................................................................
```

1. To print the report, click the **Print** button.
   A dialog box opens, allowing you to choose the printer to be used for printing the report.
2. To save the report, click the **Save** button.

A dialog box opens, allowing you to choose the location in which to save the report.

Updating and Viewing MP Statistics (SCTP) Reports

The **Diameter > Reports > MP Statistics (SCTP)** 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 are updated on the page each time the **Update** button is clicked. The counts are not refreshed automatically.

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

Use this task to update and view MP Statistics (SCTP) reports.

1. Select **Diameter** > **Reports** > **MP Statistics (SCTP)**.
   The **Diameter > Reports > MP Statistics (SCTP)** page appears.
2. Select the Scope of the report from the **Scope** pulldown list.
   - To be able to select individual MPs, choose **Server**.
   - To select all MPs in a Network Element, choose **NE**.
3. In the box on the right, list the MPs to be included in the report.
   - To add a specific MP to the list on the right, so that its statistics will be shown in the report, select the MP in the box on the left, and click **Add**.

     Repeat this action for each specific MP that is to be listed in the report.
   - To add all of the available MPs to the list on the right, click the **AddAll** button.
   - To remove a specific MP from the report, select the MP in the box on the right, and click **Remove**. The selected MP moves to the box on the left.
   - To remove all of the listed MPs from the box on the right (to prepare to create a new list), click **RemoveAll**. All of the MPs from the box on the right move to the box on the left.
4. When the list in the box on the right contains the MPs for the report, click **Go**.
   The selected MPs and their statistics are listed in the columns of the report.
5. Click **Update** to display the current statistics for the listed MPs.

MP Statistics (SCTP) report elements

Table 121: 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 121: MP Statistics (SCTP) Report Elements

Field	Description	Data Input Notes
MP Selection		

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

Field	Description	Data Input Notes
Checksum Error	Number of SCTP Checksum Errors detected	

Chapter 6

Diameter Mediation

Topics:

- *Mediation overview.....300*
- *Rule Templates.....302*
- *Formatting Value Wizard.....328*
- *Enumerations.....336*
- *Triggers.....340*
- *State and Properties.....344*
- *Base Dictionary.....348*
- *Custom Dictionary.....350*
- *All-AVP Dictionary.....355*
- *Vendors.....357*
- *Rule Sets.....360*

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.

  A Message Copy Action can also be defined to trigger Diameter Message Copy for copying a message to a DAS.

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)

Mediation Message Copy can be performed only for Request messages, and is ignored if set at Mediation Trigger Point ATP1.

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.

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 (*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 *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*)

Mediation-Triggered Diameter Message Copy

The Rule Template "Message Copy" Action can be defined to trigger Diameter Message Copy for messages that are processed by Diameter Mediation.

The Message Copy Action triggers Diameter Message Copy, and specifies the Message Copy Configuration Set (MCCS) that contains the Request/Answer content criteria to be used by the Message Copy function to copy the message to a DAS. The Message Copy Configuration Set specifies a Route List for the DAS. See *Message Copy Configuration Set configuration*.

The Message Copy Action is ignored if set at ATP10 (Diameter Answer message prior to be forwarded to connection).

If Message Copy is triggered for the same message from multiple locations, the Message Copy Configuration Set for the latest Message Copy triggering prevails.

In the case of Request re-route due to invalid Result-Code, only the Message Copy Configuration Set that is associated with the Answer that completes the transaction at ATP1 is considered.

The Message Copy is performed after the completion of the original transaction. The copy of the message is not processed by the Mediation Triggering Points.

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 Mediation, 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" operators, 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, forwarding the message to a specific destination, or triggering of Diameter Message Copy to send a copy of the message to a DAS.

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. See *Rule Template elements* for the Actions available in Rule Templates.

On the **Diameter > Mediation > Rule Templates** page, you can perform the following actions:

- Filter the list of Rule Template Names to display only the desired Rule Templates.
- Click the **Insert** button.

  The **Diameter Mediation Rule Templates [Insert]** page opens. You can add a new Rule Templates and its values. See *Adding a Rule Template*. If the maximum number of Rule Templates (100) already exist in the system, the **Rule Templates [Insert]** page will not open, and an error message is displayed.

- Click the **Import** button.

  The **Diameter > Mediation > Rule Templates [Import]** page opens. You can import a Rule Template from a location outside the Diameter system, to which the Rule Template was previously exported from Mediation. See *Importing a Rule Template*. If the maximum number of Rule Templates (100) already exist in the system, the **Rule Templates [Import]** page will not open, and an error message is displayed.

- Select a Rule Template Name in the list, and click the **Copy** button.

  The **Diameter > Mediation > Rule Templates [Copy]** page opens. You can change the information for the copied Rule Template to create a new Rule Template. See *Copying a Rule Template*. If the

maximum number of Rule Templates (100) already exist in the system, the **Rule Templates [Copy]** page will not open, and an error message is displayed.

- Select a Rule Template Name in the list, and click the **Edit** button.

  The **Diameter > Mediation > Rule Templates [Edit]** page opens. You can edit the selected Rule Template. See *Changing a Rule Template*.

- Select a Rule Template Name in the list, and click the **Delete** button to remove the selected Rule Template. See *Deleting a Rule Template*.

- Select a Rule Template Name in the list, and click the **Export** button.

  The **Diameter > Mediation > Rule Templates [Export]** page opens. You can export the selected Rule Template to a location outside of the Diameter system. See *Exporting a Rule Template*.

- Select a Rule Template Name in the list, and click the **Set Help** button.

  The **Diameter > Mediation > Rule Templates [Set Help]** page opens. You can create online help for the selected Rule Template. See *Adding online help to a Rule Template*.

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.

Rule Template elements

Table 122: Rule Template elements describes 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 122: 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. 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 *Fast Search*.	Format: Check mark (Yes) or red circle with red line through it (No); not editable Range: Yes sign or No sign Default: Yes sign

Element	Description	Data Input Notes

	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 Conditions 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.
		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.

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

Element	Description	Data Input Notes
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 to 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 123: 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 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	Format: Pulldown list Range: Right value types are: • 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)

Element	Description	Data Input Notes
	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.	• 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 Right value data must be entered and can be changed in the Rule Set rule.	Format: Check box Range: Check mark or no check mark 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.

Element	Description	Data Input Notes
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. • P - Proxiable; shows if the message can be proxied, relayed, or redirected, or it must be locally processed. • E - Error; shows if the message contains 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.	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
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 supported AVP definition from the dictionary and the instance 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.		

Element	Description	Data Input Notes
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. • 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 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	**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 Range: **Add parent AVP if it is not present** Format: Check box Range: Checked or unchecked

Element	Description	Data Input Notes
	the originator and the recipient of the message.	
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 or Grouped 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 deleted AVP has been the last AVP within the Grouped AVP, then **Delete parent AVP if it is empty** can be checked to delete the Parent AVP as well. 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 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	**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

Element	Description	Data Input Notes
	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.	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. **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.	**Restore AVP:** Format: Pulldown list Range: Available AVPs **Instance:** Format: Pulldown list Range: First, Second, Third Fourth, Fifth **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".	**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)

Element	Description	Data Input Notes
	• 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 **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.	• 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). 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

Element	Description	Data Input Notes
		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
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	**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

Element	Description	Data Input Notes
	there is end-to-end security between the originator and the recipient of the message.	
Set AVP Value	Allows 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:** 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;

Element	Description	Data Input Notes
		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 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

Element	Description	Data Input Notes
		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 **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		
Message Copy	Trigger Diameter Message Copy for the message, based on the values in the Message Copy Configuration Set that is specified for the Action. See *Message Copy Configuration Set configuration*.	Format: Pulldown list for **Select Message Copy Configuration Set** field Range: Default; configured Message Copy Configuration Sets Default: "-Select-"
Execute Rule template	**Note:** The value needs to be set at the time the new Rule Template is defined.	Format: Pulldown list

Element	Description	Data Input Notes
	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.	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 123: 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 123: 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\..*

Operator	Operator Type	Returns true when... Example of use
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... @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, Enumerated, 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 incompatible), 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 124: Rule Template Condition Conversion Rules*.

Table 124: 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.
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 123: 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

Viewing Rule Templates

Use this procedure to view all existing Rule Templates.

Select **Diameter** > **Mediation** > **Rule Templates**.

The **Diameter > Mediation > Rule Templates** page appears.

Adding a Rule Template

Use this procedure to define a new Rule Template. A maximum of 64 Rule Templates can be defined.

There are three sections of the **Diameter > Mediation > Rule Templates [Insert]** page: **Settings**, **Conditions**, and **Actions**. For a list of Rule Template elements and their definitions, see *Rule Template elements*.

After the definition is complete and the Rule Template State is set to "Active" or "Test", this Rule Template appears as a Rule Set in the **Diameter** > **Mediation** > **Rule Sets** menu folder.

1. If Mediation-Triggered Message Copy will be used (the Message Copy Action will be selected in one or more Rule Templates), the following Diameter Configuration is required before each Action can be configured.
   a) Configure one or more Route Groups that will be used for one or more Route Lists for the Message Copy DAS.
   b) Configure one or more Route Lists for the DAS.
   c) Configure one or more Message Copy Configuration Sets that can be assigned to one or more Rule Template Message Copy Actions.
2. Verify that the required Diameter Mediation Enumeration Types, AVP Dictionary entries, and Vendors have been defined in the system.

   Use the following GUI pages to view the entries, and to access the GUI pages to enter, change, or delete entries as needed

   - *Enumerations*
   - *All-AVP Dictionary*
   - *Vendors*
3. Select **Diameter** > **Mediation** > **Rule Templates**.

   The **Diameter > Mediation > Rule Templates** page opens.
4. Click the **Insert** button.

   The **Diameter > Mediation > Rule Templates [Insert]** page opens.

   If the maximum number of Rule Templates (100) already exist in the system, the **Rule Templates [Insert]** page will not open, and an error message is displayed.
5. Enter the **Settings** values for the Rule Template.
   a) Enter the name for the Rule Template in the **Name** text box.

      The Name describes the purpose of the Rule Template.
   b) The **Message type support** for the Rule Template cannot be provisioned.

      Request and **Answer** are both supported.

6. Enter the values to define up to 5 Conditions in the Rule Template.

   Note: A Rule Template can be defined with no Conditions. It will unconditionally match for all processed messages.

   The order in which conditions appear on the **Diameter > Mediation > Rule Templates** page determines the order in which the conditions are processed. The **Up** and **Down** buttons are used to change the order of processing.

   The **Fast Search** check mark or stop symbol displayed for a condition is determined by the **Operator** and the **Optional** fields. A check mark appears for **Fast Search** when the **Operator** is either "equals", "begins with-longest match", or "begins with", and the **Optional** element is not check marked.

   A check mark in **Optional** indicates that a matching expression is optional. This means that the user can leave this condition's **Value** field blank on the **Diameter > Mediation > Rule Set** page, and this condition will then not be used during message processing.

   a) Enter a **Name** for the condition. This name appears on the generated **Rule Set** page after this Rule Template is saved.
   b) Enter a **Left value** in the text box, or use the *Formatting Value Wizard* to select the components of the Left value.

      The Left value appears in the text box.

   c) Select an **Operator** from the pulldown menu.
   d) Select a **Right value** from the pulldown list.
   e) Provide a **Default value** for the Right value that will appear on the **Rule Set** page that is generated from the Rule Template.
   f) Click the appropriate check boxes to display a check mark in the boxes that apply for this Rule Template.

      Click the **Case sensitive** check box to indicate that the values must match in case as well as content.

      Click the **Optional** check box to indicate that the user can decide to exclude the matching expression form the condition set by leaving the Right value empty.

      Click the **Fixed** check box to indicate that the Right value cannot be changed in the rule.

   g) To add another condition, click **Add** and repeat the substeps in this step for each additional condition.

7. Enter the values to define one or more Actions in the Rule Template.

   When any defined Conditions are met, the Actions specified in this section of the page are taken. At least one Action must be specified for a Rule Template.

   a) From the **New Action** pulldown list, select an Action to take for this Rule Template.
   b) Click **[Add]** to open the GUI fields for the selected Action.
   c) Enter the information in the fields. The fields are described in *Rule Template elements*.

8. When the Rule Template definition is complete, click:

   - **OK** to save the Rule Template and return to the **Diameter > Mediation > Rule Templates** page. The Rule Template Name appears in the list on the page.
   - **Apply** to save the Rule Template and remain on the **Diameter > Mediation > Rule Templates [Insert]** page for additional changes.
   - **Cancel** to return to the **Diameter > Mediation > Rule Templates** page without saving the Rule Template.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error or warning message appears:

- Any of the Default value fields in the Conditions contain a value that cannot fit into the range of the selected Right value with a supported Operator.
- Any of the Default value fields in the Conditions contain a value that is not valid or is not the correct format for the selected Right value with a supported Operator.
- Adding the new Rule Template would cause the maximum number (100) of Rule Templates allowed in the system to be exceeded.

9. If you want to add online help to describe this Rule Template in its generated Rule Set, perform the *Adding online help to a Rule Template* procedure. Then continue with *Step 10*.
10. When the Rule Template definition is complete, go to the **Diameter Mediation State & Properties** page.
    a) Change the Rule Template **State** from Development to either Test or Active.
    b) Set the **Action Error Handling** property.

    After the Rule Template definition is completed and saved, the Rule Template state and properties can be changed to make the Rule Template available for testing and to generate the Rule Set from the Rule Template.

    The Rule Template state can be changed to Test to allow testing, provisioning of the Rule Set data, and associating the Rule Set with a Trigger (see *Triggers*) before the Rule Set is used in live traffic.

    The state can be changed to Active after the testing is successful, the Rule Set data is provisioned, the Rule Set is associated with a Trigger, and the Rule Set is ready to use in live traffic.
11. If one or more Rule Template Actions for Message Copy have been configured, go to the **Diameter > Configuration > System Options** page, select the **Message Copy Options** tab, and select the **Enabled** radio button for the **Message Copy Feature** element.

Adding online help to a Rule Template

When a Rule Template is created, online help can be added to the Rule Template to describe it in its generated Rule Set.

After online help is added, when the user clicks the context-sensitive help icon in the upper right corner of the associated **Diameter > Mediation > Rule Sets {name}** page, this online help explains how to use the **Diameter > Mediation > Rule Sets {name}** page to configure the Rule Set.

This help is standalone, and is not part of the online help provided by Tekelec as part of the Mediation feature.

Use this procedure to add context-sensitive online help to an existing Rule Template:

1. Select **Diameter** > **Mediation** > **Rule Templates**.

   The **Diameter > Mediation > Rule Templates** page appears.
2. Select the **Rule Template Name** to which online help will be added.
3. Click **Set Help**.

   The **Diameter > Mediation > Rule Templates [Set Help]** page appears.
4. Change the contents of the **Title** box to an appropriate title for this help.

The Rule Template Name appears in the **Title** box as the default.

5. In the **Text** field, add specific details on how to configure a rule using this Rule Set, such as a procedure and result. You can also add detail on how the various fields interrelate, and provide any cautions to prevent loss of data.
6. To see how the help text you have entered will look from the **Rule Set** page, click **Preview**.

   A separate window opens and displays the help text.

   Close the preview window when you are finished previewing the help text.

7. When the help page is complete, click:

   - **OK** to save the help page and return to the **Diameter > Mediation > Rule Templates** page.
   - **Apply** to save the changes and remain on the **Diameter > Mediation > Rule Templates [Set Help]** page for additional changes.
   - **Cancel** to return to the **Diameter > Mediation > Rule Templates** page without saving any changes.

   The new help text is now available from the help icon on the **Diameter > Mediation > Rule Sets {name}** page for this Rule Template.

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 - 1500 characters
Path	(Generated and used by software)	

Copying a Rule Template

Use this procedure to copy an existing Rule Template and save it as a new Rule Template. For a list of Rule Template elements and their definitions, see *Rule Template elements*.

1. Select **Diameter** > **Mediation** > **Rule Templates**.

   The **Diameter > Mediation > Rule Templates** page appears.

2. Select the Rule Template that you want to copy.
3. Click **Copy**.

   The **Diameter > Mediation > Rule Templates [Copy]** page appears.

   If the maximum number of Rule Templates (100) already exist in the system, the **Rule Templates [Copy]** page will not open, and an error message is displayed.

4. Enter a different **Rule Template Name** for the new Rule Template.
5. Make any changes as needed.
6. Click:
   - **OK** to save the definition and return to the **Diameter > Mediation > Rule Templates** page.
   - **Apply** to save the definition and remain on the **Diameter > Mediation > Rule Templates [Copy]** page.
   - **Cancel** to return to the **Diameter > Mediation > Rule Templates** page without saving any changes.

Changing a Rule Template

Use this procedure to change values for an existing Rule Template (for a list of Rule Template elements and their definitions, see *Rule Template elements*).

When a Rule Template is in the Development state, all elements can be changed.

After the Rule Template state has been changed to Test or Active, only the following elements can be changed. The Rule Template state must be set back to Development to change any other elements (all provisioning of rules for the Rule Template will be lost when the state is changed back to Development). (See *State and Properties*.)

- Rule Template Name
- Name of the Conditions
- Default value of the Conditions (except when the Fixed box has been checked)
- Description of the Condition
- Default value of the Actions (except for the value of the "Execute Rule Template")

1. Select **Diameter** > **Mediation** > **Rule Templates**.

   The **Diameter > Mediation > Rule Templates** page appears.

2. Click **Edit** on the Rule Template row to be changed.

   The **Diameter > Mediation > Rule Templates [Edit]** page appears.

3. Change **Conditions** and **Actions** as needed.
4. Click:
   - **OK** to save the changes and return to the **Diameter > Mediation > Rule Templates** page.
   - **Apply** to save the changes and remain on the **Diameter > Mediation > Rule Templates [Edit]** page.
   - **Cancel** to return to the **Diameter > Mediation > Rule Templates** page without saving any changes.

Importing a Rule Template

A Rule Template can be imported into the DSR system using the **Import** function on the **Diameter > Mediation > Rule Templates** page.

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

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

A successfully imported Rule Template file appears in the list on the **Diameter > Mediation > Rule Templates** page, the **Diameter > Mediation > State & Properties** page, and as a Rule Set in the **Diameter** > **Mediation** > **Rule Sets** menu folder (no Rule Set is generated if the only Action is "Execute Rule Template").

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

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

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

Use the following procedure to import an existing Rule Template that is located outside of the DSR file system (stored on a local computer):

1. Select **Diameter** > **Mediation** > **Rule Templates**.

   The **Diameter > Mediation > Rule Templates** page appears.

2. Click **Import**.

   The **Diameter > Mediation > Rule Templates [Import]** page appears.

   If the maximum number of Rule Templates (100) already exist in the system, the **Diameter > Mediation > Rule Templates [Import]** page will not open, and an error message is displayed.

3. Click **Browse** to open the **Choose File** popup window.
4. Navigate to the location of the Rule Template file you want to import, and select the file.
5. With the Rule Template filename displayed in the **File name** field, click **Open**.

   The filename appears in the **Choose a file to import** field.

6. Click **Import File**.

   If the Import File button is clicked and any of the following conditions exist, the file is not imported and an error message appears:

   - The selected file does not exist
   - The selected file is larger than 1 MB
   - The selected file has wrong .xml structure or missing data
   - The Mediation version of the file is not compatible with the DSR system into which the file is being imported
   - The Name field of the imported Rule Template is empty
   - Any Operator field in a Condition contains an operator that is not valid
   - Any Right value field in a Condition
   - A value type specifies an Enumerated Type that is not defined either in the system or in the imported file
   - A Condition or Action in the selected file includes an Enumerated Type that is already present in the system, but that contains different Enumerated Type values
   - The selected file contains an Action that is not defined in the system
   - The selected file contains more than the allowed maximum number of Conditions (5)

- A Condition in the selected file includes a Right value that is not supported by the selected Operator
- The Right value of a Condition in the file is not a supported value type
- The selected file contains more than the allowed maximum number of Actions (5), unless the maximum number is exceeded because of automatically added final actions (some actions actually result in multiple actions)
- Importing the file would cause the allowed maximum number of Rule Templates (100) in the system to be exceeded
- The selected Rule Template references another Rule Template (as an Execute Rule Template action) that is not present in the system
- The selected file contains mutually exclusive Actions (that cannot be used together in the same Rule Template)

Exporting a Rule Template

Use this procedure to export a Rule Template from within the DSR to an external location, such as your hard drive or a memory stick.

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

- The Rule Template without any provisioned data
- All of the Enumeration Type definitions with the possible values to which the Rule Template refers
- Mediation version number
- Help pages related to the Rule Template

Note: The Export button is not available (grayed out) for Rule Templates that are in the "Development" state (see the **Diameter > Mediation > State and Properties** page).

1. Select **Diameter** > **Mediation** > **Rule Templates**.

   The **Diameter > Mediation > Rule Templates** page appears.

2. Select the **Rule Template Name** row for the Rule Template to be exported.
3. Click the **Export** button.

   A **File Download** popup window appears.

4. Click **Browse** to pop up the **Choose File** window.
5. Navigate to the location to which you want to export the Rule Template.
6. Click **Export File**.

   The selected file is saved to the specified location.

Deleting a Rule Template

When a Rule Template is deleted, it is removed from the entire system, including the **Diameter > Mediation > State and Properties** page, the **Diameter > Mediation > Triggers** page, and the **Daimeter > Mediation > Rule Sets** page.

Any Rule Sets that were generated from this Rule Template are also deleted automatically.

If a Rule Set belonging to the selected Rule Template is enabled for live traffic ("Active" state on the **State and Properties** page), an error message appears indicating that the Rule Template cannot be deleted as long as it is being used by the system for live traffic.

Use this procedure to delete an existing Rule Template.

1. Select **Diameter** > **Mediation** > **Rule Templates**.

   The **Diameter > Mediation > Rule Templates** page appears.

2. Select the **Rule Template Name** of the Rule Template to be removed.
3. Click **Delete**.
4. A popup window appears to confirm the delete when the selected Rule Template is in the "Development" state or the "Test" state (see the **State and Properties** page).
   - Click **OK** to confirm the delete.
   - Click **Cancel** to cancel the delete function and return to the **Diameter > Mediation > Rule Templates** page.
5. If the selected Rule Template has any data provisioned, another confirmation popup window appears indicating that all of the provisioned data that belongs to any Rule Set generated from the Rule Template will be deleted.
   - Click **OK** to confirm the delete of the provisioned data.
   - Click **Cancel** to cancel the delete function and return to the **Diameter > Mediation > Rule Templates** page.

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.

Formatting Value Wizard elements

When **[wizard]** is clicked, the information shown in *Table 125: Formatting Value Wizard elements* appears:

Table 125: 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.

Element	Description
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 126: Formatting Value Wizard Specifiers*.
Preview	The readable description of the xl-formatted string in the Value field.

The specifiers described in *Table 126: 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 126: 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.)
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}

Specifier			
	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 • 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		

Specifier	
	@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
	@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}

Specifier	
	{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}
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

Specifier	
	• 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 @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

Specifier			
	@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} {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}		
Functions	**Sub-Items**	**xl-formatted Value**	**Preview Value**
	Length of	strlen(<string>	{Length of (<string>)}

<table>
<tr><td>Specifier</td><td colspan="3"></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.

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.</td></tr>
</table>

Specifier			
	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.		
Operators	Provide the ability to perform mathematical operations on the AVP. • Plus • Minus	• + • -	• + • -
Back Reference	Number of occurence of the back reference: input field for one digit; default is 0.	\<number>	\<*number*>
	Because Back Reference can be part of only a replacement string, this specifier is presented only for the **Substitute in AVP Value** Action.		

Using the Formatting Value Wizard

Use the following procedure to code an xl-formatted string using the wizard. See *Formatting Value Wizard elements* for:

- A list of wizard elements and their descriptions
- A list of xl-code specifiers, their sub-items, xl-formatted values, and preview values

1. On a **Diameter > Mediation** GUI page, click **Wizard**.

   The wizard popup window appears.

2. Click the specifier you want to add to the Value, or type characters directly into the Value field.

   If a specifier requires additional information, a popup window prompts for this information.

   The selected characters or specifier in xl-format appears in the **Value** field. The specifier description also appears in the **Preview** section of the window.

3. Add additional specifiers or text as needed.
4. When the Value is complete, click **Ok**.

   The xl-formatted string appears in the **Value** field on the **GUI** page.

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.

On the **Diameter > Mediation > Enumerations** page, you can perform the following actions:

- Filter the list of Enumerations to display only the desired Names.
- Click the **Insert** button.

  The **Diameter > Mediation > Enumerations [Insert]** page opens. You can add a new Enumeration Type and its values. See *Adding an Enumeration*.

  If the maximum number of Enumeration Types (64) already exist in the system, the **Diameter > Mediation > Enumerations [Insert]** page will not open, and an error message is displayed.
- Select the **Name** of an Enumeration in the list, and click the **Edit** button.

  The **Diameter > Meditation > Enumerations [Edit]** page opens. You can edit the selected Enumeration Type. See *Editing an Enumeration*.
- Select the **Name** of an Enumeration Type in the list, and click the **Delete** button to remove the selected Enumeration Type. See *Deleting an Enumeration*.

Mediation Enumerations elements

Table 127: 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 127: 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.	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).

Element	Description	Data Input Notes
	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.	Range: 1-2048 characters

Viewing Enumerations

Use this task to view all configured Mediation Enumerations.

The use of Mediation Enumerations is described in *Enumerations*.

Select **Diameter** > **Mediation** > **Enumerations**.

The **Diameter > Mediation > Enumerations** page appears with a list of configured Enumerations and their values. The fields are described in *Mediation Enumerations elements*.

Adding an Enumeration

The following procedure can be used to configure a new Enumeration Type.

A new Enumeration Type can be used when defining **Rule Template Conditions** and **Linking-AVPs**.

The fields are described in *Mediation Enumerations elements*.

1. Select **Diameter** > **Mediation** > **Enumerations**.

   The **Diameter > Mediation > Enumerations** page appears.

2. Click **Insert**.

   The **Diameter > Mediation > Enumerations [Insert]** page appears.

   Note: If the maximum number of Mediation Enumerations (64) has already been configured in the system, the **Diameter > Mediation > Enumerations [Insert]** page will not open, and an error message will appear.

3. Enter a unique **Name** for the Enumeration Type that is being added.
4. Enter one or more **Values** to associate with this Enumeration Name. Use a comma to separate multiple values.
5. Click:

   - **OK** to save the changes and return to the **Diameter > Mediation > Enumerations** page.

     OK is not available until a **Name** is entered.

   - **Apply** to save the changes and remain on the **Diameter > Mediation > Enumerations [Insert]** page.

Apply is not available until a **Name** is entered.

- **Cancel** to return to the **Diameter > Mediation > Enumerations** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- The **Name** or **Value** contains characters that are not valid
- The **Value** is empty (not entered)
- The **Name** is not unique
- Creating this new Enum Type will cause the allowed maximum number of Enum Types (64) to be exceeded

Editing an Enumeration

Use this procedure to change the Name, or Values, or both, associated with an Enumeration.

An item cannot be removed from the comma-separated list of values that is already used by the configured data of a Rule Template or by the Rule Template.

The fields are described in *Mediation Enumerations elements*.

1. Select **Diameter** > **Mediation** > **Enumerations**.

   The **Diameter > Mediation > Enumerations** page appears.

2. Select the row containing the Enumeration to be changed.
3. Click the **Edit** button.

   The**Diameter > Mediation > Enumerations [Edit]** page appears.

4. Change the **Name** or **Values**, or both, associated with the selected Enumeration.
5. Click:

   - **OK** to save the changes and return to the **Diameter > Mediation > Enumerations** page.

     OK is not available if the **Name** field is empty.

   - **Apply** to save the changes and remain on the **Diameter > Mediation > Enumerations [Edit]**.

     Apply is not available if the **Name** field is empty.

   - **Cancel** to return to the **Diameter > Mediation > Enumerations** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The **Name** or **Value** contains characters that are not valid
   - The **Name** is not unique
   - An item has been removed from the comma-separated list of values that is already used by the configured data of a Rule Template or by the Rule Template

Deleting an Enumeration

Use the following procedure to delete an Enumeration.

An Enumeration Type cannot be deleted if any Rule Templates refer to the Enumeration Type.

1. Select **Diameter** > **Mediation** > **Enumerations**.

   The **Diameter > Mediation > Enumerations** page appears.

2. Select the **Name** of the Enumeration Type to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.

4. Click **OK**.

   - **OK** delete the Enum Type and return to the **Diameter > Mediation > Enumerations** page.
   - **Cancel** to cancel the delete function and return to the **Diameter > Mediation > Enumerations** page.

   When **OK** is clicked and any configured Rule Templates refer to the Enum Type that is being deleted, the Enum Type is not deleted and an error message appears.

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 128: Diameter Mediation Triggers* and shown in *Figure 17: Diameter Mediation Trigger Points* 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 128: Diameter Mediation Triggers

Execution Trigger Name	Message Type	Triggering Point
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 upstream

Execution Trigger Name	Message Type	Triggering Point
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 downstream

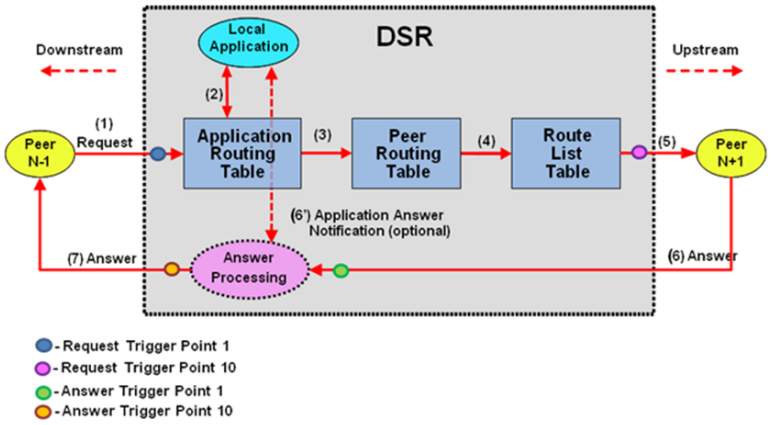

Figure 17: Diameter Mediation Trigger Points

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. See *Associating a Rule Set with a 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. See *Removing the Association of a Rule Set with a 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.

Mediation Triggers elements

Table 129: 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 > Mediation > Triggers [Insert]** page; the Triggers page is read-only.

Table 129: 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. **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.

Viewing Triggers

The operation of Diameter Mediation Triggers is explained in *Triggers*.

To view all existing Mediation Triggers, select **Diameter** > **Mediation** > **Triggers**.

The **Diameter > Mediation > Triggers** page appears, with a list of existing Triggers, and with the Rule Sets that are associated with each Trigger listed under the Trigger name. The fields on the page are described in *Mediation Triggers elements*.

Associating a Rule Set with a Trigger

Use this procedure to associate a Rule Set with a Trigger.

Only Rule Sets with Rule Templates in "Test" or "Active" state can be associated with a Trigger.

1. Select **Diameter** > **Mediation** > **Triggers**.

   The **Diameter > Mediation > Triggers** page appears.

2. Click **Insert** under the Trigger with which the new Rule Set is to be associated.

   The **Diameter > Mediation > Triggers [Insert]** page opens.

   The **Diameter > Mediation > Triggers [Insert]** page does not open and an error message appears if any of the following conditions exist:

   - There are no Rule Sets that support the Trigger and that are in the "Active" or "Test" state

- Associating another Rule Set to the Trigger would cause the total allowed number of associated "Test" Rule Sets (10) or "Active" Rule Sets (5) to be exceeded

3. Select the desired **Rule Set Name** from the pulldown list.

   The default is the first Rule Set in the pulldown list.

4. The newly assigned Rule Set appears at the bottom of the list of Rule Sets for the Trigger. If the Rule Set sequence needs to be changed, use the **Up** and **Down** buttons to move the Rule Sets to different positions in the list.

   Clicking a Rule Set and the **Up** button moves the selected Rule Set up one position toward the top of the list.

   Clicking a Rule Set and the **Down** button moves the selected Rule Set down one position toward the bottom of the list.

   The Live column will show a check mark if the Rule Template for the newly associated Rule Set is in the "Active" state for use with live traffic (see the **State & Properties** page).

5. Click:

   - **OK** to save the new Rule Set association and return to the **Diameter > Mediation > Triggers** page.
   - **Apply** to save the new Rule Set association and remain on the **Diameter > Mediation > Triggers [Insert]** page.

   If **OK** or **Apply** is clicked and the selected Rule Set no longer exists (was deleted by another user), an error message appears.

Removing the Association of a Rule Set with a Trigger

Use the following procedure to remove the association of a Rule Set with a Trigger and delete the Rule Set Name from the list for the Trigger.

1. Select **Diameter** > **Mediation** > **Triggers**.

   The **Diameter > Mediation > Triggers** page appears.

2. Select the **Rule Set Name** in the list under the Trigger name.
3. Click the **Remove** button below the **Rule Set Name** list for the Trigger.

   A popup window appears to confirm the removal.

4. Click:

   - **OK** to remove the association of the Rule Set with the Trigger and delete the Rule Set Name from the list for the Trigger.
   - **Cancel** to cancel the Remove function and return to the **Diameter > Mediation > Triggers** page.

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 *Generating Diagnostics Tool Reports*.

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. See *Importing a Rule Template*.

  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. See *Editing State and Properties*.

  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. See *Deleting a Rule Template*.

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

Mediation State & Properties elements

Table 130: 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 130: 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
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

Importing a Rule Template

A Rule Template can be imported into the DSR system using the **Import Rule Template** action on the **Diameter > Mediation > State & Properties** page.

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

Use the following procedure to import a Rule Template located outside of the EAGLE XG DSR file system (stored on the local computer):

1. Select **Diameter** > **Mediation** > **State & Properties**.

   The **Diameter > Mediation > State & Properties** page appears.

2. Click **Import Rule Template**.

   The **Diameter > Mediation > State & Properties [Import]** page appears.

3. Click **Browse** to open the **Choose File** popup window.
4. Navigate to the location of the Rule Template file that you want to import.
5. With the Rule Template filename displayed in the **File name** field, click **Open**.

   The filename appears in the **Choose a file to import** field.

6. Click **Import File**.

   The selected Rule Template file is imported, and appears in the **Rule Template Name** list on the **Diameter > Mediation > State & Properties** page.

Editing State and Properties

Use this procedure to change the state and properties associated with a Rule Template. The changes take effect immediately after **OK** or **Apply** is clicked.

The state of a Rule Template can be changed to or from the "Development" state only when the "Meta-Administrator" privileges are activated for the Diameter Mediation feature.

A Rule Template state cannot be changed from "Test" to "Development" for a Rule Template that is referenced by another instance such as another Rule Template or the Execution Trigger.

When a Rule Template state is changed back to "Development", any associated Rule Sets will be deleted from the **Rule Sets** folder.

The fields are described in *Mediation State & Properties elements*.

1. Select **Diameter** > **Mediation** > **State & Properties**.

   The **Diameter > Mediation > State & Properties** page appears.

2. Select the row containing the Rule Template to be changed.
3. Click the **Edit** button.

   The **Diameter > Mediation > State & Properties [Edit]** page appears.

4. Change the **State** or **Action Error Handling**, or both, associated with the selected Rule Template.
5. Click:
   - **OK** to save the changes and return to the **Diameter > Mediation > State & Properties** page.
   - **Apply** to save the changes and remain on **Diameter > Mediation > State & Properties [Edit]** page.
   - **Cancel** to return to the **Diameter > Mediation > State & Properties** page without saving any changes.

   If **OK** or **Apply** is clicked, and the Rule Template state was changed to "Active", and the maximum number of Active Rule Templates (5) already exists in the system, an error message appears.

   When the state of a Rule Template is changed from "Test" to "Development" and the Rule Template is not referenced anywhere, a popup window appears to confirm the change to "Development" state.

   When the state of a Rule Template is changed from "Development" to "Test", a new Rule Set appears in the left-hand GUI menu **Rule Sets** folder; the Rule Set has the same name as the Rule Template. (If the Rule Template contains only the "Execute Rule Template" Action, then a Rule Set is not generated.) If the new Rule Set has help defined in the Rule Template, the **Help** folder in the left-hand GUI menu is updated to include the Rule Set help.

Deleting a Rule Template

Use the following procedure to delete a Rule Template from the **Diameter > Mediation > State & Properties** 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.

1. Select **Diameter** > **Mediation** > **State & Properties**.

   The **Diameter > Mediation > State & Properties** page appears.

2. Select the **Rule Template Name** to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.

4. Click:
   - **OK** to delete the Rule Template and return to the **Diameter > Mediation > State & Properties** page.
   - **Cancel** to cancel the delete function and return to the **Diameter > Mediation > State & Properties** page.

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 included 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. See *Custom Dictionary*. Custom Dictionary 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.

On the **Diameter > Mediation > Base Dictionary** page, you can perform the following actions:

- Filter the list to display only the desired entries. (The Flags cannot be filtered.)
- Sort the list entries in ascending or descending order in a column, by clicking the column heading. The default order is by Attribute Name in alphabetical order. The Flags cannot be sorted.
- Select an AVP definition in the list, and click the **View** button.

  The **Diameter > Mediation > Base Dictionary [View]** page appears. The detailed definition for the selected AVP is displayed. The fields are described in *Mediation Base Dictionary elements*.

Mediation Base Dictionary elements

Table 131: Mediation Base Dictionary Elements describes the fields on the **Mediation > Base Dictionary** view-only pages.

Table 131: 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

Field	Description	Data Notes
		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 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.	Format: 3 buttons for each flag Range: Must, Must Not, May be set for each flag
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

Field	Description	Data Notes
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

Viewing an existing AVP Dictionary entry

Use the following task to view a selected Mediation Base Dictionary AVP entry.

On the **Diameter > Mediation > Base Dictionary** page:

1. Select an AVP entry in the list.
2. Click the **View** button.

   The **Diameter > Mediation > Base Dictionary [View]** page displays the attributes that are configured for the selected AVP dictionary entry.
3. Click the **Cancel** button to return to the **Diameter > Mediation > Base Dictionary** page..

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.

On the **Diameter > Mediation > Custom Dictionary** page, you can perform the following actions:

- Filter the list to display only the desired entries. All column headings are supported in the filters except the Flags.
- Sort the list entries in ascending or descending order in a column (except for Flags), by clicking the column heading. By default, the AVPs are sorted by Attribute Name in alphabetical order.
- Click the **Insert** button.

  The **Diameter > Mediation > Custom Dictionary [Insert]** page opens. You can add a new AVP and its values.

  If the maximum number of AVPs (1024) already exist in the system, the **Diameter > Mediation > Custom Dictionary [Insert]** page will not open, and an error message is displayed.
- Select an AVP definition in the list, and click the **Edit** button.

  The **Diameter > Mediation > Custom Dictionary [Edit]** page appears. The detailed definition for the selected AVP is displayed. You can change the AVP definition except for the AVP Code, Vendor ID, and Attribute Name.
- Select an AVP definition in the list, and click the **Delete** button to remove the selected AVP definition from the dictionary.

Mediation Custom Dictionary elements

Table 132: Mediation Custom Dictionary Elements describes the fields on the **Diameter > Mediation > Custom Dictionary** view, [Insert], and [Edit] pages.

Table 132: 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: numeric Range: 0-4294967295
Vendor-ID	Vendor-ID The field is required.	Format: pulldown list Range: all configured Vendors

Field	Description	Data Input Notes
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 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 originator and the recipient of the message.	Format: 3 buttons for each flag Range: Must, Must Not, May for each flag
Data Type	AVP Data Format The field is required.	Format: pulldown list Range: all available AVP data formats

Field	Description	Data Input Notes
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

Adding a new AVP Dictionary entry

Use the following task to add a new AVP Dictionary entry to the Custom Dictionary, or overwrite a Base Dictionary AVP.

The attributes are described in *Mediation Custom Dictionary elements*.

1. Select **Diameter** > **Mediation** > **Custom Dictionary**.

   The **Diameter > Mediation > Custom Dictionary** page appears.

   The **Diameter > Mediation > Custom Dictionary** page will not open if the maximum number of AVPs (1024) have already been created in the dictionary.

2. Click the **Insert** button.

   The **Diameter > Mediation > Custom Dictionary [Insert]** page opens.

3. Enter the attribute values for the new AVP, or customize a Base Dictionary AVP by changing fields except the Attribute Name, AVP Code, and Vendor-ID.
4. Click:

   - **OK** to save the changes and return to the **Diameter > Mediation > Custom Dictionary** page.
   - **Apply** to save the changes and remain on the **Diameter > Mediation > Custom Dictionary [Insert]** page.
   - **Cancel** to return to the **Diameter > Mediation > Custom Dictionary** page without saving any changes.

   If **OK** or **Apply** is clicked and if a Base Dictionary entry is overwritten and the original entry is used by any Rule Templates, the original entry is used until the application is restarted.

Changing an existing AVP Dictionary entry

Use the following task to change an existing Custom Dictionary AVP entry.

Note: Base Dictionary entries cannot be edited directly. To change a Base Dictionary entry, use the *Adding a new AVP Dictionary entry* procedure to enter a new AVP in the Custom Dictionary that has the same Attribute Name, AVP Code, and Protocol as the Base Dictionary entry that you want to change. Enter different values for the attributes that you want to change.

The fields are described in *Mediation Custom Dictionary elements*.

1. Select **Diameter** > **Mediation** > **Custom Dictionary**.

   The **Diameter > Mediation > Custom Dictionary** page appears.

2. In the list, select the entry to be changed, and click the **Edit** button.

   The **Diameter > Mediation > Custom Dictionary [Edit]**page appears.

3. Change the available attributes as needed .

   The Attribute Name, AVP Code, and Protocol cannot be changed.

4. Click:

   - **OK** to save the changes and return to the **Diameter > Mediation > Custom Dictionary** page.
   - **Apply** to save the changes and remain on the **Diameter > Mediation > Custom Dictionary [Edit]** page.

     Cancel to return to the **Diameter > Mediation > Custom Dictionary** page without saving any changes.

   If the old version of the AVP is referred to by any Rule Template, the application must be restarted to begin use of the changed AVP. The old version will be used until the restart is done.

Deleting an AVP dictionary entry

Use the following procedure to delete an AVP entry from the Custom Dictionary.

1. Select **Diameter** > **Mediation** > **Custom Dictionary**.

   The **Diameter > Mediation > Custom Dictionary** page appears.

2. Select the **Attribute Name** of the AVP entry to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.

4. Click:

   - **OK** to delete the AVP and return to the **Diameter > Mediation > Custom Dictionary** page.
   - **Cancel** to return to the**Diameter > Mediation > Custom Dictionary** page without deleting the AVP.

   When **OK** is clicked and any configured Rule Template or Rule Set refers to the AVP that is being deleted, the AVP is not deleted and an error message appears.

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 *Base Dictionary* and *Custom Dictionary*.

On the **Diameter > Mediation > All-AVP Dictionary** page, you can perform the following actions:

- Filter the list to display only the desired entries.
- Sort the list entries in ascending or descending order in a column, by clicking the column heading (except the flag headings).
- Select an AVP definition in the list, and click the **View** button.

  The **Diameter > Mediation > All-AVP Dictionary > [View]** page appears. The detailed definition for the selected AVP is displayed (the definition cannot be changed on this page). The definition elements are described in *Mediation All-AVP Dictionary elements*.

Mediation All-AVP Dictionary elements

Table 133: Mediation All-AVP Dictionary elements describes the fields on the **Diameter > Mediation > All-AVP Dictionary** pages.

Table 133: 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: numeric Range: 0-4294967295
Vendor-ID	Vendor-ID	Format: pulldown list

Field	Description	Data Notes
		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 originator and the recipient of the message.	Format: 3 buttons for each flag Range: Must, Must Not, May for each flag
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

Field	Description	Data Notes
		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

Viewing an existing All-AVP Dictionary entry definition

Use the following task to view a selected Mediation All-AVP Dictionary AVP entry definition. (The definition cannot be changed on this page.)

1. Select **Diameter** > **Mediation** > **All-AVP Dictionary**.
   The **Diameter > Mediation > All-AVP Dictionary** page appears.
2. Select an AVP entry in the list and click the **View** button.
   The **Diameter > Mediation > All-AVP Dictionary [View]** page displays the attributes that are configured for the selected AVP dictionary entry.
3. Click the **Cancel** button to return to the **Diameter > Mediation > All-AVP Dictionary** page.

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.

On the **Diameter > Mediation > Vendors** page, you can perform the following actions:

- Filter the list of Vendors to display only the desired Vendors.
- Sort the displayed Vendors by ascending or descending Vendor ID or Vendor Name, by clicking the column heading.
- Click the **Insert** button.

  The **Diameter > Mediation > Vendors [Insert]** page opens. You can add a new Vendor. See *Adding a Vendor*.

  If the maximum number of Vendors (128) already exist in the system, the **Diameter > Mediation > Vendors [Insert]** page will not open, and an error message is displayed.

- Select a Vendor row in the list, and click the **Edit** button.

  The **Diameter > Mediation > Vendors [Edit]** page opens. You can edit the Vendor Name for the selected Vendor. See *Editing a Vendor Name*.

The **Diameter > Mediation > Vendors [Edit]** page will not open if the selected Vendor is used in any of the AVP definitions in the dictionary.

- Select a Vendor row in the list, and click the **Delete** button to remove the selected Vendor. See *Deleting a Vendor*.

  A Vendor cannot be deleted if it is used in any AVP definitions in the AVP Dictionary.

Mediation Vendors elements

Table 134: Mediation Vendors elements describes the fields on the **Diameter > Mediation > Vendors** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 134: 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. A unique name is required in this field.	Format: Character string Range: 1-255 characters

Viewing Vendors

The use of Mediation Vendors is described in *Vendors*.

To view all configured Mediation Vendors, select **Diameter** > **Mediation** > **Vendors**.

The **Diameter > Mediation > Vendors** page appears with a list of configured Vendors. The fields are described in *Mediation Vendors elements*.

Adding a Vendor

The following procedure can be used to configure a new Vendor.

The fields are described in *Mediation Vendors elements*.

1. Select **Diameter** > **Mediation** > **Vendors**.

   The **Diameter > Mediation > Vendors** page appears.

2. Click **Insert**.

The **Diameter > Mediation > Vendors [Insert]** page appears.

If the maximum number of Vendors (128) has already been configured in the system, the **Diameter > Mediation > Vendors [Insert]** page will not open, and an error message will appear.

3. Enter a unique **Vendor Name** for the Vendor that is being added.
4. Enter a **Vendor ID** for the Vendor.
5. Click:
   - **OK** to save the changes and return to the **Diameter > Mediation > Vendors** page.
   - **Apply** to save the changes and remain on the **Diameter > Mediation > Vendors [Insert]** page.
   - **Cancel** to return to the **Diameter > Mediation > Vendors [Insert]** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - The Vendor Name or Vendor ID contains any characters that are not valid or are out of the allowed range
   - The Vendor Name or Vendor ID is empty (not entered)
   - The Vendor Name is not unique

Editing a Vendor Name

Use this procedure to change a Vendor Name.

The Vendor ID cannot be changed.

The Vendor Name cannot be changed if the Vendor is used in any of the AVP definitions in the dictionary.

The fields are described in *Mediation Vendors elements*.

1. Select **Diameter** > **Mediation** > **Vendors**.
   The **Diameter > Mediation > Vendors** page appears.
2. Select the Vendor Name to be changed.
3. Click the **Edit** button.
   The **Diameter > Mediation > Vendors [Edit]** page appears.
4. Change the Vendor Name of the selected Vendor.
5. Click:
   - **OK** to save the changes and return to the **Diameter > Mediation > Vendors** page
   - **Apply** to save the changes and remain on the **Diameter > Mediation > Vendors [Edit]** page.
   - **Cancel** to return to the **Diameter > Mediation > Vendors** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - The Vendor Name is not unique
   - The Vendor Name contains characters that are not valid

Deleting a Vendor

Use the following procedure to delete a Vendor.

A Vendor cannot be deleted if the Vendor is used in any AVP definitions in the dictionary.

1. Select **Diameter** > **Mediation** > **Vendors**.

   The **Diameter > Mediation > Vendors** page appears.

2. Select the row that contains the Vendor to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.

4. Click:

   - **OK** to delete the Vendor.
   - **Cancel** to cancel the delete function and return to the **Diameter > Mediation > Vendors** page.

   If the Vendor is used in any AVP definitions in the dictionary, the Vendor is not deleted and an error message appears.

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

Table 135: 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 these 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.

Rule Sets elements - View page

Table 136: Rule Sets Elements - View Page describes the elements that appear on each **Diameter > Mediation > Rule Sets > {name}** page.

Table 136: Rule Sets Elements - View Page

Element	Description	Data Notes
Move the rule	Used to move a rule up or down in the list, to change the order of execution of the rules. The rules are executed in the order shown in the list, from the top of the list to the bottom of the list. The element appears at the left of and at the right of each rule row.	Format: Buttons in two columns under the heading Range: Up, Down One, both, or no buttons appear in the columns, depending on the rule definition.
All Conditions defined on the Rule Template page for this Rule Set	Each condition name has a separate column in the list.	Format, Range, and Default Value vary depending on the Rule Template that was configured for the Rule Set.
All Actions defined on the Rule Template page for this Rule Set	Each Action defined for this Rule task has a separate column in the list that shows the name of the Action, and one or more sub-columns that show the attributes that were defined for the Action and the current values of the attributes. If the Parent AVP or AVP is indexed, then the index is displayed in the square brackets after the AVP attribute name. If an AVP is looked up in the message by its value, “AVP” shall contain the value prefixed with “=” (if it is a constant) or an xl-value prefixed with “=” (if it is an xl-value).	Format, Range, and Default Value vary depending on the Rule Template that was configured for the Rule Set.

Element	Description	Data Notes
	A value can be prefixed with an appropriate indicator of its type or function (such as =, beginning, end, prefix, or suffix).	
Each rule in the Rule Set is a row in the list. The Values assigned to the Conditions and the Values assigned to each attribute of the Actions for a rule are shown in the row for that rule.		

Rule Sets elements - Insert and Edit Pages

Table 137: Maximum Allowed Rule Sets and Rules indicates the maximum number of Rule Sets and rules that are allowed.

Table 137: Maximum Allowed Rule Sets and Rules

Description	Value
Maximum number of provisioned rules in the system	25000
Maximum number of provisioned rules per Rule Set	250

Table 138: Rule Sets Elements - Insert and Edit Pages describes the elements that are shown on a **Diameter > Mediation > Rule Sets > {name}** [Insert] or [Edit] page.

Table 138: Rule Sets Elements - Insert and Edit Pages

Element	Description	Data Input Notes
Field: This element has two sections: IF and THEN.		
IF	The list of Condition names (if any Conditions were defined for the Rule Template). AND appears between each two Conditions.	Format: Name of the Condition, followed by its Operator The name and operator cannot be entered or changed.
THEN	The name of each Action that was defined for the Rule Template.	Format: Name An Action cannot be deleted and a new Action cannot be defined for the rule.
Value: This element shows the fields for the Condition and Action data Values that can be entered or changed. For the [Insert] page, the fields are either empty or show default values. For the [Edit] page, the fields show the currently defined or default values.		

Element	Description	Data Input Notes
Condition expression Right value	For each defined Condition in the rule, the data value for the Right value type in the Condition. If the **Optional** check box was checked in the Rule Template for this Rule Set, the Right value can be empty (not provisioned). A red asterisk appears after each data value that is required (not optional) in the rule. If the **Fixed** check box was checked in the Rule Template for this Rule Set, the Right value cannot be changed in the rules. If the selected Right value type was an **Enumerated Type**, then the Value column contains a pulldown list with the corresponding Enumerated Type values, unless the selected Operator was “exists”, “does not exist”, “is true” or “is false”.	Format: text box Range: Varies depending on the Right value type Default: Varies depending on the Right value type See *Rule Template elements*. The *Formatting Value Wizard* is available to provision Condition Right values that are xl-formatted values; click **[wizard]** that appears after the data value field.
Action fields	The fields to use to define the data values for Action attributes.	Format: Varies for each type of attribute Range: Varies for each type of attribute See *Rule Template elements*. The *Formatting Value Wizard* is available to provision Action attributes that are xl-formatted values; click **[wizard]** that appears after the data value field.
Description	The description that was defined in the Rule Template for a Condition or an Action on the **Rule Sets** page. The description can 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

Adding a Rule to a Rule Set

Use this procedure to define a new rule in a Rule Set. A maximum of 250 rules can be defined in one Rule Set.

There are two sections of a **Diameter > Mediation > Rule Sets > {name} [Insert]** page: **IF** (zero, one, or more Conditions) and **THEN** (an Action). For a list of the Rule Template elements that appear in a rule and their definitions, see *Rule Template elements*.

When a Rule Template is in the "Active" or "Test" state, this Rule Template appears as a Rule Set in the **Diameter** > **Mediation** > **Rule Sets** menu folder. The order in which rules appear on a **Diameter > Mediation > Rule Sets > {name}** page determines the order in which the conditions are processed. The **Up** and **Down** buttons next to the rules can be used to change the order of processing.

1. Select **Diameter** > **Mediation** > **Rule Sets** > **{name}**.

   The selected **Diameter > Mediation > Rule Sets > {name}** page opens.

2. Click the **Insert** button.

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

   If the maximum number of rules are already defined for the Rule Set (250) , the **Diameter > Mediation > Rule Sets > {name} [Insert]** page will not open, and an error message is displayed.

3. Enter the Value for each condition that appears under **IF** in the **Field** section for the new rule.
4. Enter the Value for each attribute of the Action that appears under **THEN** in the **Field** section for the new rule.
5. When the rule definition is complete, click:

   - **OK** to save the new rule and return to the **Diameter > Mediation > Rule Sets > {name}** page. The rule name appears in the list on the page.
   - **Apply** to save the new rule and remain on the **Diameter > Mediation > Rule Sets > {name} [Insert]** page for additional changes.
   - **Cancel** to return to the **Diameter > Mediation > Rule Sets > {name}** page without saving the changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error or warning message appears:

   - Any mandatory input fields are empty
   - Any input Value fields in the Conditions or Actions did not conform to the required syntax defined by the Right value type or the Action definition
   - Another rule exists within the Rule Set with the same Values in the Condition section; the rule Condition already exists in the Rule Set
   - Adding the new rule would cause the allowed maximum number (250) of rules in a Rule Set in the system to be exceeded
   - Adding the new rule would cause the allowed maximum number (250000) of rules in the system to be exceeded

6. When the Rule Set definition and testing are complete, go to the **Diameter Mediation State & Properties** page.
   a) Change the Rule Template **State** from Test to Active.
   b) Set the **Action Error Handling** property, if needed.

   The state can be changed to Active after the testing is successful, the Rule Set data is provisioned, the Rule Set is associated with a Trigger, and the Rule Set is ready to use in live traffic.

Deleting All Rules from a Rule Set

Use this procedure to delete all rules from a Rule Set.

1. Select **Diameter** > **Mediation** > **Rule Sets** > **{name}**.

   The selected **Diameter > Mediation > Rule Sets > {name}** page appears.

2. Click **Delete All Rules**.

   A popup window appears to confirm the delete.

3. On the popup window, click:

   - **OK** to delete all rules and return to the **Diameter > Mediation > Rule Sets > {name}** page.
   - **Cancel** to cancel the delete operation and return to the **Diameter > Mediation > Rule Sets > {name}** page.

Changing a Rule in a Rule Set

Use this procedure to change values for a rule in a Rule Set (for a list of Rule Sets elements and their definitions, see *Rule Sets elements - Insert and Edit Pages*):

1. In the **Diameter** > **Mediation** > **Rule Sets** folder, select the Rule Set that contains the rule to be edited.

   The **Diameter > Mediation > Rule Sets > {name}** page appears for the selected Rule Set.

2. Select the rule that needs to be changed.
3. Click **Edit**.

   The **Diameter > Mediation > Rule Sets > {name} [Edit]** page appears.

4. Change values for Conditions under **IF** and Actions under **THEN** as needed.
5. Click:

   - **OK** to save the changes and return to the **Diameter > Mediation > Rule Sets > {name}** page.
   - **Apply** to save the changes and remain on the **Diameter > Mediation > Rule Sets > {name} [Edit]** page.
   - **Cancel** to return to the **Diameter > Mediation > Rule Sets > {name}** page without saving any changes.

Deleting One Rule from a Rule Set

Use this procedure to delete one rule from a Rule Set.

1. Select **Diameter** > **Mediation** > **Rule Sets** > **{name}**.

   The selected **Diameter > Mediation > Rule Sets > {name}** page appears.

2. Select the row for the rule to be deleted.
3. Click **Delete**.

   A popup window appears to confirm the delete.

4. On the popup window, click:
   - **OK** to delete the rule and return to the **Diameter > Mediation > Rule Sets > {name}** page.
   - **Cancel** to cancel the delete operation and return to the **Diameter > Mediation > Rule Sets > {name}** page.

Chapter 7

DSR Capacity and Congestion Controls

Topics:

- *Introduction.....370*
- *DA-MP Overload Control.....370*
- *Per-Connection Ingress MPS Control.....372*
- *Remote Congestion Controls.....376*
- *Egress Throttle Groups.....389*

The DSR provides the features and functions for per-connection and per-MP capacity and congestion control. Egress Throttle Groups can monitor Egress Message Rate and Pending Transactions across multiple DA-MPs in a DSR.

Introduction

The DSR provides the following features and functions for capacity and congestion control:

- DA-MP Overload Control
- Per-Connection Ingress MPS Control
- User Configurable Message Priority
- Remote BUSY Congestion
- Egress Transport Congestion
- Per-Connection Egress Message Throttling
- User-Configurable Connection Pending Transaction Limiting
- Egress Throttle Groups
- Functions associated with Message Priority and Connection Congestion:
  - DSR egress Request routing incorporates Request Message Priority and Connection Congestion Level in its Connection selection criteria.
  - The Routing Option Set associated with the ingress Request specifies what action is taken by the DSR when routing of a Request is abandoned and the last Connection evaluated was congested.
  - The maintenance status for a congested Connection indicates whether the congestion is due to Remote BUSY Congestion, Egress Transport Congestion, or Egress Message Throttling.

The Diameter Transport Function services its per-Connection ingress sockets with per-Connection MPS controls that ensure fairness in reading ingress messages for all established Connections.

The Diameter Transport Function services its per-Connection egress queues with controls that ensure fairness in forwarding egress messages to Peers for all established Connections.

Egress Throttle Groups monitor Egress Message Rate, Pending Transactions, or both, for logical groups of Diameter Connections or Peers, or both, across multiple DA-MPs on a DSR Network Element.

DA-MP Overload Control

DA-MP Overload Control (Message Priority and Color-Based DA-MP Overload Control) provides a mechanism for managing internal/local DA-MP congestion detection and control.

The DA-MP Overload Control feature tracks ingress message rate, calculates the amount of traffic that needs to be shed based on CPU congestion, and sheds that traffic based on Message Priority, Message Color, and discard policy.

Message Color is used as a means for differentiating Diameter Connections that are under-utilized versus those that are over-utilized with respect to ingress traffic - traffic from under-utilized Connections is marked "green" by the *Per-Connection Ingress MPS Control* (PCIMC) feature, while traffic from over-utilized Connections is marked "yellow". In the event of (Danger of Congestion or of CPU congestion and based on the specified discard policy, traffic from over-utilized Connections is considered for discard before traffic from under-utilized Connections. Traffic discarded by PCIMC due to capacity exhaustion (per-Connection or shared) is marked "red" and is not considered for any subsequent processing.

The following DA-MP Congestion Controls are associated with reducing the traffic processing load on the DA-MP when congestion is detected:

- Internal Resource Monitoring and Control

  The availability of key traffic-sensitive internal software resources (stack queues and buffer pools) is monitored in real-time against their static maximum capacity.

  When resource availability drops below engineered thresholds, alarms are generated. When resource availability is exhausted, controls are invoked to prevent over-utilization. Resource utilization KPIs and measurements provide real-time and long-term information for making decisions about system capacity and growth.

- DA-MP Overload Control

  Traffic loads, if allowed to exceed the DA-MP's engineered capacity, will degrade the effective performance of the DA-MP, increase message latency, and can result in message loss. DA-MP Overload Control is responsible for reducing the traffic processing load to insure that the MP meets its performance specifications. MP Processing Overload Control monitors the Diameter Process CPU utilization of the Diameter Process.

Limitations

- DA-MP Overload Control is limited to local MP congestion management and does not address remote Diameter node congestion management.
- Automatic recovery from persistent MP or egress Connection congestion is not supported. Manual intervention is required.

Diameter Configuration for DA-MP Overload Control

The following Diameter Configuration components are used for DA-MP Overload Control:

- **MP Profiles**

  A DA-MP Profile is assigned to each DA-MP in the system, using the **Diameter > DA-MPs > Profile Assignments** GUI page.

  The assigned DA-MP Profile indicates the Engineered Maximum MPS for the DA-MP and the Message Rate Alarm Set and Clear Thresholds. These engineering-configured MP Profiles values shown on the **Diameter > DA-MPs > MP Profiles** GUI page vary depending on the type of blade or Rack Mount Server used for the DA-MP.

  The following elements can be user-configured on the **Diameter > DA-MPs > MP Profiles** GUI page for use by the DA-MP Overload Control feature:

  - Congestion Level 1 Discard Percentage - The percent below the DA-MP Engineered Ingress MPS that DA-MP Overload Control will police the total DA-MP ingress MPS to when the DA-MP is in Congestion Level 1.
  - Congestion Level 2 Discard Percentage - The percent below the DA-MP Engineered Ingress MPS that DA-MP Overload Control will police the total DA-MP ingress MPS to when the DA-MP is in Congestion Level 2.
  - Congestion Level 3 Discard Percentage - The percent below the DA-MP Engineered Ingress MPS that DA-MP Overload Control will police the total DA-MP ingress MPS to when the DA-MP is in Congestion Level 3.
  - Congestion Discard Policy - The order of Message Priority and Color-based traffic segments to consider when determining discard candidates for the application of treatment during DA-MP

Congestion processing. The following order is considered: Color within Priority, Priority within Color, and Priority Only.

- Danger of Congestion Discard Percentage - The percent of total DA-MP ingress MPS above the DA-MP Engineered Ingress MPS that DA-MP Overload Control will discard when the DA-MP is in danger of congestion,
- Danger of Congestion Discard Policy - The order of Message Priority and Color-based traffic segments to consider when determining discard candidates for the application of treatment during DA-MP Danger of Congestion (DOC) processing. The following order is considered: Color within Priority, Priority within Color, and Priority Only.

- **Routing Option Sets**

  A Routing Option Set is a set of user-configurable routing options assigned to an ingress Diameter transaction. A Routing Option Set can be assigned to Peer Nodes and Diameter Application IDs.

  DA-MP Overload Control uses the following options:

  - Resource Exhausted Action
  - Resource Exhausted Result-Code Value
  - Resource Exhausted Vendor-ID Value
  - Resource Exhausted Error-Message Value

Per-Connection Ingress MPS Control

The Per-Connection Ingress MPS Control (PCIMC) feature limits to a configurable level the per-Connection ingress message rate of each DSR Connection. Correctly configured message rate controls ensure that a single Connection cannot use the majority of the resources. (No limiting is done by PCIMC for the egress message rate.)

The Per-Connection Ingress MPS Control feature:

- Is always available in the system
- Applies to per-Connection MPS control for Connections that are statically assigned to MP servers through configuration and do not move from one MP to another
- Is applied in the Diameter Transport Function, which is used by all DSR Applications

Capacity management for this feature can be logically separated into:

- Management of the ability of the MP server to process ingress Diameter messages - how the MP server's resources are distributed to configured Connections
- Management of the ability of a given Connection to process ingress Diameter messages - how each Connection behaves given its configured reserved and maximum ingress MPS settings

Per Connection Capacity Management

Per-Connection Ingress MPS Control allocates a DA-MP's ingress message processing capacity among the Diameter Peer Connections that it hosts. Each Peer Connection is allocated, through user-configuration, a Reserved Ingress MPS message processing capacity and a Maximum Ingress MPS message processing capacity.

The Reserved capacity for a Connection is available for exclusive use by the Connection. The capacity between a Connection's Reserved and Maximum capacity is shared with other Connections hosted by the DA-MP.

The DA-MP reads messages arriving from a Peer Connection and attempts to process them as long as Reserved or shared ingress message capacity is available for the Connection. When no Reserved or shared ingress message capacity is available for a Connection, the DA-MP enforces a short discard period, during which time all ingress messages are read from the Connection and discarded without generation of any response to the Peer.

Per Connection Ingress Message Coloring

In addition to enforcing ingress message rate limits on a per Connection basis, Per-Connection Ingress MPS Control colors ingress messages based on the Reserved and average ingress message rates. Message color can be used at other traffic shedding points in the DSR, such as *DA-MP Overload Control*.

Traffic from under-utilized Connections is marked "green" by Per-Connection Ingress Message Controls, while traffic from over-utilized Connections is marked "yellow". Traffic discarded by PCIMC due to capacity exhaustion (per-Connection or shared) is marked "red" and is not considered for any subsequent processing.

The following items describe the numbered items in *Figure 18: Per Connection Message Coloring*:

- When the Connection's average ingress MPS rate is equal to or below its configured Reserved Ingress MPS, all messages processed by the Connection are colored green.
- When the Connection's average ingress MPS rate is above its configured Reserved Ingress MPS, all messages processed by the Connection are colored yellow.

  Note: If the Connection's Reserved Ingress MPS is 0, all the messages processed by the Connection are colored yellow.

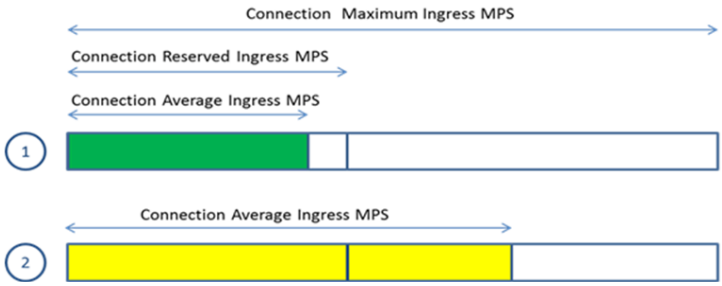

Figure 18: Per Connection Message Coloring

Per MP Server Capacity Management

Tekelec-engineered MPS rates and thresholds are used to manage ingress message MPS as it relates to the MP server as a whole.

A DA-MP has two Tekelec-configured ingress message rate capacity limits:

- **Engineered Ingress MPS** - Maximum ingress message rate that a DA-MP will support without overload.

  This value provides a limit to the total Reserved Ingress MPS of all Diameter Connections assigned to the DA-MP. The value is displayed on the Diameter > Configuration > DA-MPs > MP Profiles GUI page for the MP Profile assigned to the DA-MP.

- **MP Engineered Maximum Ingress MPS** - A Tekelec-configurable ingress MPS limit that dictates the maximum rate at which the DA-MP will attempt to process messages from all Diameter Connections.

  This value may be greater than the MP Engineered Ingress MPS.

The DA MP monitors its MPS rate and limits the rate to an MP Engineered Ingress MPS value. If the MP Engineered Ingress MPS rate is exceeded, overload can occur and ingress messages are discarded (due to MP Ingress MPS Limiting and MP Congestion Controls).

Diameter Configuration for Per Connection Ingress MPS Control

Each Diameter Connection is associated with a Capacity Configuration Set that includes the following configurable elements:

- **Reserved Ingress MPS** - Defines the capacity reserved exclusively for the Connection and not available for use by other Connections

  The Reserved Ingress MPS cannot exceed the configured Maximum Ingress MPS for a given Connection. A Connection can be configured with a zero Reserved Ingress MPS value; such Connections will not reserve message processing capacity.

  The Reserved Ingress MPS for a Connection cannot be used by any other Connection, regardless of the load offered to other Connections.

  If the Reserved Ingress MPS Capacity is set to a non-zero value, that value times the number of Connections using that Capacity Configuration Set on a given MP server must not be allowed to exceed the MP Maximum Reserved Ingress MPS (which is equal to the MP Engineered Ingress MPS - the highest MPS rate at which the MP server can process ingress Diameter messages).

- **Maximum Ingress MPS** - Defines the maximum rate in ingress Diameter messages per second that the Connection is allowed to process

  The Maximum Ingress MPS must be greater than or equal to 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 are using the same Capacity Configuration Set.

  The configured Maximum Ingress MPS of a Connection cannot exceed the Engineered Ingress MPS of the Connection (the ingress MPS that a Connection can process at a sustained rate without errors). If the Connection has Reserved Ingress MPS, the configured Maximum Ingress MPS must be greater than or equal to the Reserved Ingress MPS. All Connections must have a non-zero configured Maximum Ingress MPS; otherwise they would not be allowed to process traffic at all. (The Maximum Ingress MPS value in the Default Capacity Configuration Set is non-zero.)

  The sum of the Maximum Ingress MPS configured for all Connections on the MP server can exceed the MP Engineered Ingress MPS - the highest MPS rate at which the MP server can process ingress Diameter messages.

- **Ingress MPS Minor Alarm Threshold** - Defines the percent of the Connection's Maximum Ingress MPS at which a Minor alarm is triggered

  The Ingress MPS Minor Alarm Threshold value must be less than the Ingress MPS Major Alarm Threshold value

- **Ingress MPS Major Alarm Threshold** - Defines the percent of the Connection's Maximum Ingress MPS at which a Major alarm is triggered.

The Ingress MPS Major Alarm Threshold must be greater than the Ingress MPS Minor Alarm Threshold.

- **Reserved Ingress MPS Abatement Time** - Defines the minimum time (in ms) that a Connection's ingress message rate must remain less than or equal to Reserved Ingress MPS, after exceeding Reserved Ingress MPS, in order to revert the ingress traffic color from Yellow to Green.

A Default Capacity Configuration Set is provided; additional Capacity Configuration Sets can be configured. The Default Capacity Configuration Set is used for a Connection if no other Capacity Configuration Set is assigned to the Connection. The elements of the Default Capacity Configuration Set have the following default values:

- Reserved Ingress MPS - zero MPS
- Maximum Ingress MPS - value equal to the Engineered Ingress MPS for the Connection
- Ingress MPS Minor Alarm Threshold - 50% of the configured Maximum Ingress MPS
- Ingress MPS Major Alarm Threshold - 80% of the configured Maximum Ingress MPS
- Reserved Ingress MPS Abatement Time - 2000 ms

Maintenance and Monitoring for Per Connection Ingress MPS Control

The Per Connection Ingress MPS Control feature provides the following maintenance and monitoring information:

- Alarms and measurements to assist the network operator to detect and avoid possible capacity issues related to messaging rates
- The ability to view the average ingress Diameter MPS for each Connection

The Per Connection Ingress MPS Control feature uses the following GUI information:

- The **Diameter > Configuration > Connections** GUI page specifies which Capacity Configuration Set the Connection uses.
- The **Diameter > Configuration > Configuration Sets > Capacity Configuration Sets** GUI pages provide elements for configuring Capacity Configuration Sets.
- The Diameter > Maintenance > Connections GUI page reports KPI 10500 for average ingress MPS for each Diameter Connection (Ingress Msgs Per Second).

  For each Connection, the MP server maintains the average number of ingress Diameter messages per second read from the socket. This is the rate at which ingress Diameter messages are read from the socket, not the rate at which ingress Diameter messages arrive at the socket. There is no efficient means to know the rate at which messages actually arrive.

  The average ingress message rate is a running average, smoothed over approximately 30 seconds. This provides a good picture of the level of ingress messages being read by each Connection while avoiding erratic readings caused by short duration spikes in the rate.

Connection Alarm

The Per Connection Ingress MPS Control feature provides a Connection alarm with two severities to alert the network operator when the average ingress MPS rate goes above the configured thresholds for percentage of the configured maximum ingress MPS for the Connection.

The Connection Ingress MPS Alarm is a per Connection alarm that can be configured in a Connection's Capacity Configuration Set to trigger at a Minor and Major capacity threshold.

The Minor alarm is asserted when the 30-second average MPS rate exceeds the configured Ingress MPS Minor Alarm Threshold value for the Connection. The Minor alarm is cleared when the 30-second

average MPS rate falls 5% below the Ingress MPS Minor Alarm Threshold value configured for the Connection.

The Major alarm is asserted when the 30-second average MPS rate exceeds the Ingress MPS Major Alarm Threshold value configured for the Connection. The Major alarm is converted to a Minor alarm when the 30-second average MPS rate falls 5% below the Ingress MPS Major Alarm Threshold value configured for the Connection.

An alarm cannot be abated until an abatement time delay has expired. For example, if a Minor alarm is asserted, the alarm cannot be cleared until the abatement time delay has expired and the average ingress MPS for the Connection is 5% below the Minor alarm assert percentage. The abatement time delay is 15 seconds.

The alarm abatement time delay affects only clearing of alarms, not asserting of alarms. Therefore, it is possible to transition rapidly from a Minor alarm to a Major alarm.

Limitations

- PCIMC relies on a configured relationship between a Connection and the MP server that will host the Connection.
- PCIMC does not prevent the total Reserved Ingress MPS of all Connections hosted by a DA MP from exceeding the MP Maximum Reserved MPS capacity when the MP Maximum Reserved MPS capacity is reduced after Connections are already configured with non-zero Reserved Ingress MPS.

Remote Congestion Controls

The following features provide remote congestion controls in the DSR:

- **Remote BUSY Congestion** - addresses Remote Congestion detection

  The DSR Remote BUSY Congestion feature calls for the server to send a "DIAMETER_TOO_BUSY" Answer, which is can be used by the clients to stop sending traffic for some duration. The feature addresses Remote Congestion detection and the steps to be taken to alleviate the situation.

- **Egress Transport Congestion** - supports use of transport congestion status

  The Egress Transport Congestion feature uses Congestion Levels to manage the egress message traffic flow on a Diameter Peer Connection when the Connection's TCP/SCTP send buffer is exhausted, as indicated by the TCP/SCTP socket being "blocked". The socket is blocked when the Diameter Transport Function attempts to write new data to the TCP/SCTP socket fail due to insufficient send buffer space. When a Diameter Connection socket becomes blocked, the Diameter Transport Function sets the Egress Transport Congestion Level to CL-4 and discards any received Request or Answer messages.

- **Per-Connection Egress Message Throttling** - targets congestion avoidance

  The Per Connection Egress Message Throttling feature targets congestion avoidance by throttling the volume of Diameter traffic being sent over a Connection when the traffic exceeds the configured maximum egress message rate of the Connection.

- **User-Configurable Connection Pending Transaction Limiting** - provides a pending transaction limit for each DSR Peer Connection

User-Configurable Connection Pending Transaction Limiting (UC-CPTL) provides a configurable pending transaction limit for each DSR Peer Connection, to customize the distribution of the available Pending Transaction Records on a DA-MP based on the varying deployment requirements. The limit can be configured independently for each DA-MP in the DSR.

Routing Based on Congestion Level

Features such as Remote BUSY Congestion, Egress Transport Congestion, and Per Connection Egress Throttling Control are used by the DSR to control the flow of egress traffic by setting a feature-specific Congestion Level for a Diameter Connection. Certain Requests can be prioritized over others, using the User Configurable Message Priority feature.

The Connection Priority Level (CPL) is an overall Congestion Level for the Connection that is based upon the highest Congestion Level of the various egress traffic control features. The CPL is used by the Diameter Routing Function when making egress message routing decisions based on the Priority provided by the User Configurable Message Priority feature. No message can be forwarded to a Diameter Connection that has a Priority level less than the CPL for that Connection

The DSR supports up to five Congestion Levels (CL-0 to CL-4), with CL-0 indicating no congestion to CL-4 indicating that the Connection is blocked. The intermediate Congestion Levels CL-1, CL-2, and CL-3 indicate the increasing severity of congestion.

Each feature has a Congestion Level range, as follows:

- Remote BUSY Congestion Levels: CL-0. CL-1, CL-2, and CL-3
- Egress Transport Congestion Levels: CL-0. CL-1, CL-2, CL03, and CL-4
- Per Connection Egress Message Throttling Congestion Levels: CL-0. CL-1, CL-2, and CL-3

The CPL value for a Connection (CONN-CPL) is based on the maximum Congestion Level of the features.

DSR egress Request routing and Answer forwarding functions use the Connection Congestion Level in conjunction with the Message Priority to determine how Requests and Answers must be handled over an egress Connection. Message Priority and Connection Congestion Level in the Connection selection criteria are used to avoid sending messages of Priority x and lower to Connections currently at Congestion Level x+1.

All Answers are assigned a Message Priority of 3 by the DSR, while Requests can be assigned Message Priorities 0 through 2. Messages with a Priority greater than or equal to the Congestion Level are allowed, while messages with lower Priorities are not delivered on this Connection. This arrangement ensures that Answers have the highest Priority and are always routed unless a Connection becomes blocked, and depending upon the level of congestion some or all of the Requests may be allowed. *Table 139: CLs, CPLs, and Message Treatment* summarizes this behavior.

Table 139: CLs, CPLs, and Message Treatment

Connection CL/CPL Value	Message Priorities Allowed	Message Priorities Not Allowed	Comment
CL-4 /4	None	All	Requests nor Answers can be sent on the Connection
CL-3/3	3	0,1,2	Allow only Answers to be sent on the Connection

Connection CL/CPL Value	Message Priorities Allowed	Message Priorities Not Allowed	Comment
CL-2/2	3, 2	0,1	Allow only Answers and Pri=2 Requests to be sent on the Connection
CL-1/1	3, 2, 1	0	Allow only Answers and Pri=2,1 Requests to be sent on the Connection
CL-0/0	All	None	All Requests and Answers can be sent on the Connection

Congestion Levels can be set by multiple features. For example, a particular Connection may have received a DIAMETER_TOO_BUSY for a Priority 1 Request (resulting in CL-2 congestion), and while abating may have experienced transport congestion (CL-4). Therefore, the DSR uses the concept of Connection Priority Level (CPL) to consider the Congestion Levels reported by all the features while making routing decisions.

The CPL value is a function of Operational Status and the Congestion Levels reported by the Remote BUSY Congestion, Egress Transport Congestion, and Per Connection Egress Message Throttling features. *Table 140: Mapping Congestion Levels to CPL Values* summarizes this behavior.

- The CPL Value for a Connection is based on the worst-case (highest) value:

  CPL Value of a Connection = Max (X1, X2, X3, X4)

- This composite CPL value is then used by the Diameter Routing Function as shown in *Table 139: CLs, CPLs, and Message Treatment*.

Table 140: Mapping Congestion Levels to CPL Values

Attribute	Value	CPL Value
X1: Diameter Connection Operational Status	Available Degraded Unavailable	0 3 99
X2: Diameter Connection Remote BUSY Congestion	CL-0 through CL-3	0-3
X3: Diameter Connection Egress Transport Congestion	CL-0 through CL-4	0-4
X4: Diameter Connection Egress Message Throttling	CL-0 through CL -3	0-3

Capacity and Ranges

Table 141: Remote BUSY and EMR Capacity Ranges specifies the capacity and ranges for Remote BUSY and Egress Message Rate.

Table 141: Remote BUSY and EMR Capacity Ranges

Item	Maximum	Description
Remote BUSY processing	1000	Remote BUSY processing on up to 1000 simultaneous Diameter connections on a single G6 DA-MP
Remote BUSY processing	2000	Remote BUSY processing on up to 2000 simultaneous Diameter connections on a single G7 DA-MP
Remote BUSY processing	1000	Remote BUSY processing on up to 1000 simultaneous Diameter connections on a single G8 DA-MP
Egress Transport Congestion processing	1000	Egress Transport Congestion processing on up to 1000 simultaneous Diameter connections on a single G6 DA-MP
Egress Transport Congestion processing	2000	Egress Transport Congestion processing on up to 2000 simultaneous Diameter connections on a single G7 DA-MP
Egress Transport Congestion processing	1000	Egress Transport Congestion processing on up to 1000 simultaneous Diameter connections on a single G8 DA-MP
Egress Message Throttling	500	Egress Message Throttling on up to 500 simultaneous Diameter connections on a single G6 DA-MP
Egress Message Throttling	500	Egress Message Throttling on up to 500 simultaneous Diameter connections on a single G7 DA
Egress Message Throttling	500	Egress Message Throttling on up to 500 simultaneous Diameter connections on a single G8 DA
Egress Message Throttling Configuration Sets	50	Up to 50 in a DSR

User Configurable Message Priority

User Configurable Message Priority provides the following functions to set the Priority of messages handled by the DSR and to use that Priority to as input into decisions for load shedding, message throttling, and egress Connection selection:

- A method to assign Message Priorities to incoming Diameter Requests.

  The Priorities assigned are based on the combination of Application-Id and Command-Code, and the Connection upon which the Request arrives. A combination of Application-Id, Command-Code, and associated Priority is called a Message Priority Rule.

- Association of a Message Priority Configuration Set with a Connection.

- Association of a Message Priority Configuration Set with a Peer Node.
- Definition of a Message Priority in a Peer Routing Rule.
- A method for Request messages arriving at the DSR to be marked with a Message Priority.
- A method for the Message Priority determined by the first DSR to handle a Request to be communicated to any other DSR that also handles the Request.

  Message Priority will be determined based in part on the Connection on which the Request arrives at the first DSR to handle the Request. A second DSR to handle the Request is not able to establish the Priority based on the original ingress Connection.

- A method for exception routing and load shedding that allows the Remote BUSY Congestion feature to use the Message Priority when determining which messages are exception-routed or shed.
- A method for exception routing and load shedding that allows the Egress Transport Congestion feature to use the Message Priority when determining which messages are exception-routed or shed.
- A method for the message throttling that allows the Per Connection Egress Message Throttling feature to use the Message Priority when determining which message are exception routed or shed.

Request messages can be assigned a Message Priority value of 0, 1, or 2 (lowest to highest Priority).

Answer messages are always assigned a Message Priority value of 3 (the highest Priority).

Messages that are given a higher Priority have a lower probability of being dropped as part of shedding or throttling logic, but having a higher Priority does not imply that the message is routed before a message with a lower Priority. Having a higher Priority does not guarantee that a messages will never be dropped as a result of shedding of messages due to congestion or resource exhaustion. The arrival pattern of the Requests has an impact on which messages are shed.

Message Priority can be assigned to ingress messages as they enter the DSR, based on:

- The Connection on which a message arrives
- The Peer Node from which a message is sent
- A Peer Routing Rule

A configured Message Priority Configuration Set can be assigned to a Connection or to a Peer Node

A Message Priority Configuration Set is configured with one or more Message Priority Rules that specify Application Ids, Command Codes, and the Message Priority that is assigned to Request messages that enter a DSR on a Connection that has been assigned the Message Priority Configuration Set.

Message Priority is assigned to ingress Request messages based on message content using the strongest matching entry in the Configuration Set:

- Application-ID + Command-Code combination
- Application-ID
- All Request messages (Application Id and Command Code values are *)

In a network where Diameter messages traverse multiple DSRs, Request Message Priority may need to be assigned on one DSR and used by any and all DSRs in the routing path.

Diameter embeds Priority in all Requests that it handles. The method used for embedding Priority in egress Requests is transparent to non-DSR Diameter nodes.

DSR egress Request routing and Answer forwarding will use Message Priority and Connection Congestion Level in its Connection selection criteria to avoid sending Priority x messages to Connections currently at Congestion-Level x+1.

Diameter Configuration for User Configurable Message Priority

The User Configurable Message Priority feature provides the ability to define Message Priority Configuration Sets (MPCS). Each MPCS contains the following information:

- MPCS Name - The Name is used when associating the Configuration Set with a Connection or Peer Node
- Message Priority Rules - Sets of Application-ID, Command-Code, and Priority
  - Application-ID - The Diameter Application-ID. The Application-Id can be an asterisk (*) indicating that all Application-Ids match this Message Priority Rule
  - Command-Code - The Diameter Command-Code. The Command-Code can be an asterisk (*) indicating that all Command-Codes within the specified application match this Message Priority Rule

    If multiple Command-Codes with the same Application-Id are to get the same Message Priority, then there must be a separate Message Priority Rule combination for each Command-Code.
  - Priority - The Priority applied to all Request messages that match the Application-Id and Command-Code combination

The Application Id and Command Code must be configured in Diameter Configuration before they can be used to configure a Message Priority Rule.

A Default Message Priority Configuration Set is provided that contains one Message Priority Rule; the Message Priority Rule is set to accept all Application Ids and all Command Codes (values are *) and has Message Priority set to 0 . The Default Message Priority Configuration Set can be assigned and used if no other Message Priority Configuration Set is assigned to the Connection or the Peer Node (it can be edited if needed).

A total of 20 Message Priority Configuration Sets can be configured per DSR NE. Each Message Priority Configuration Set supports up to 50 Message Priority Rules.

A Connection or Peer can be configured with either a MPCS or to get Message Priority from the ingress Request. If it is configured to get Message Priority from the ingress Request, then it is not possible to configure a MPCS for the Connection or Peer.

In Peer Routing Rules, Message Priority valid values are 'No Change', 0, 1 and 2. 0 is the lowest priority. The Message Priority value is applied to the message only when the Peer Routing Rule Action value is set to Route to Peer.

The following Message Priority treatment configuration options can be selected:

- None (default)
- Apply a MPCS (by selecting from a list of configured MPCSs)
- Read from message - Used to indicate that the Priority should be taken from the ingress message. This is used for DSR-to-DSR Connections as a way of conveying Message Priority

  This option does not apply to Peer Routing Rules, which have the options None (default) and Apply an MPCS.

Table 142: Message Priority Treatment Methods indicates how DSR determines which method is used. If the Request does not match a rule in the selected Message Priority Configuration Set, then the Request is assigned a Priority value of zero ("0").

Table 142: Message Priority Treatment Methods

Message Priority Configuration Set Connection Setting	Message Priority Configuration Set Peer Node (for Connection) Setting	How Priority is Set for Ingress Requests on Connection
Not Set	Not Set	Use DSR NE
Not Set	MPCS X	Use MPCS X to assign Priority to Ingress Requests
Not Set	Get Priority from Ingress Requests	Extract Priority from Ingress Requests
MPCS Y	(Don't Care)	Use MPCS Y to assign Priority to Ingress Requests
Get Priority from Ingress Requests	(Don't Care)	Extract Priority from Ingress Requests

Remote BUSY Congestion

The Remote BUSY Congestion feature can be used per Connection to reduce the amount of message traffic sent to a Diameter Connection when an adjacent Diameter Peer Node is unable to process messages as fast as they are sent to it on the Connection.

Note: The User Configured Message Priority feature is a prerequisite for the Remote BUSY Congestion feature.

A Connection is considered congested or BUSY if the following conditions exist:

- An Answer message containing 'Diameter_TOO_BUSY' Result Code is received on the Connection
- The Answer message was originated by the Peer Node (the Origin-Host of the Answer message is the same as the Connection's Peer FQDN.

The DSR sets the status 'BUSY' only for the Connection of a Peer on which 'DIAMETER TOO BUSY' is received. The other Connections between the DSR and the Peer may or may not be BUSY.

Remote BUSY Congestion applies only to adjacent nodes. If the node which initiated the DIAMETER_TOO_BUSY, as determined by the Origin-Host AVP value, is not a DSR Peer Node, then the DIAMETER_TOO_BUSY will be ignored.

Message traffic reduction is managed through the use of 4 Remote BUSY Congestion Levels: CL-0. CL-1, CL-2, and CL-3, where CL-0 indicates "no congestion" and CL-3 is the highest level of congestion.

A Remote BUSY Congestion Level for a Connection is determined from the Priority of the egress transactions rejected by a "DIAMETER_TOO_BUSY" response. When a transaction of Priority "X" is rejected by a "DIAMETER_TOO_BUSY" on a Connection whose Remote BUSY Congestion Level is X or smaller, then the Remote BUSY Congestion of the Connection is set to a value that prevents the Diameter Routing Function from sending subsequent transactions of the same or lower Priority than the rejected transaction (in this case, the Remote BUSY Congestion Level is set to X+1). For example, if a "DIAMETER_TOO_BUSY" response is received for a Priority 1 transaction, then the Remote BUSY

Congestion Level will be set to CL-2 to prevent subsequent transactions of Priority 1 and lower from being forwarded on the Connection.

Whenever the Remote BUSY Congestion Level is increased, Remote BUSY Congestion abatement is re-started, using the configured Remote Busy Abatement Timeout value. When the Remote Busy Abatement Timeout expires, the Congestion Level is decremented by 1, allowing transactions with the next lower Priority to be forwarded on the Connection; the Remote Busy Abatement Timeout is restarted. This process continues until the Congestion Level of the Connection drops back to CL-0.

Whenever the Remote BUSY Congestion Level is increased, Remote BUSY Congestion abatement is re-started, by starting the Remote BUSY Congestion Abatement Timer. When the Remote Busy Abatement Timeout expires, the Congestion Level is decremented by 1, thus allowing transactions with the next lower Priority to be forwarded on the Connection; and the Remote Busy Abatement Timeout is restarted. This process continues until the transactions of the Connection drop back to CL-0.

Because Remote BUSY Congestion is detected by inspecting the Result-Code AVP embedded in an Answer response, detection is performed by the Diameter Routing Function.

Except for Remote BUSY Congestion detection, the Diameter Transport Function is responsible for handling all of the tasks associated with Remote BUSY Congestion, such as:

- Managing the Remote BUSY Congestion Level
- Managing Remote BUSY abatement
- Updating the Connection Priority Level (CPL) for the Connection
- Keeping OAM informed of the Remote BUSY Congestion status

When the Diameter Routing Function determines that the Remote BUSY Congestion Level needs to be increased, it notifies the Diameter Transport Function instance that is currently controlling the Diameter Connection.

Because multiple Diameter Routing Function instances can be simultaneously forwarding transactions to the same Diameter Connection and detecting Remote BUSY Congestion, an internal procedure minimizes the number of simultaneous the Diameter Routing Function-to-Diameter Transport Function detection notifications that are associated with any single Diameter Connection.

The Connection Congestion Levels CL-0, CL-1, CL-2, CL-3 and CL-4 are mapped to Connection Priority Level (CPL) values 0, 1, 2, 3, 4 respectively.

Diameter Configuration for Remote BUSY Congestion

The Remote BUSY Congestion feature is configured using the following elements on the Diameter > Configuration > Connections GUI page:

- Remote Busy Usage: Enabled, Disabled
- Remote Busy Abatement Timeout - time period (in seconds) that a Connection will be considered BUSY from the last time a DIAMETER_TOO_BUSY response was rec

The configuration elements cannot be modified when the Connection is in service (Connection Admin State=Enabled).

The Remote BUSY Congestion feature can be enabled and disabled for each configured Diameter Connection.

Egress Transport Congestion

The Egress Transport Congestion feature manages the egress message traffic flow on a Diameter Peer Connection when the Connection's TCP/SCTP send buffer is exhausted, as indicated by the TCP/SCTP socket being "blocked" (the Diameter Transport Function attempts to write new data to the TCP/SCTP socket fail due to insufficient send buffer space). This can happen for variety of reasons such as under-engineered TCP or SCTP buffers or the inability of the adjacent Diameter Peer to handle the rate of egress message traffic currently being offered on a Connection. In general, this condition should not occur during normal traffic loads, or during abnormal or peak traffic loads if the Per Connection Egress Message Throttling feature is enabled and properly configured for a Connection.

Egress Transport Congestion detection and abatement are solely the responsibility of the Diameter Transport Function.

Message traffic reduction is managed through the use of 5 Egress Transport Congestion Levels: CL-0. CL-1, CL-2, CL-3, and CL-4.

The Connection Congestion Levels CL-0, CL-1, CL-2, CL-3 and CL-4 are mapped to Connection Priority Level (CPL) values 0, 1, 2, 3, 4 respectively, as shown in *Table 143: Mapping Congestion Levels to CPL Values*.

Table 143: Mapping Congestion Levels to CPL Values

Attribute	Value	CPL Value
Diameter Connection Operational Status	Available Degraded Unavailable	0 3 99
Diameter Connection Remote BUSY Congestion	CL-0 through CL-3	0-3
Diameter Connection Egress Transport Congestion	CL-0 through CL-4	0-4
Diameter Connection Egress Message Throttling	CL-0 through CL-3	0-3

Diameter messages initiated by the Diameter Transport Function are not impacted by Egress Transport Congestion Levels CL-0, CL-1, CL-2 or CL-3. This includes Peer-to-Peer messages such as DPR/DPA, DWR/DWA and any non-Peer-to-Peer messages such as Diameter Transport Function-initiated Answer responses associated with DA-MP Overload.

The Diameter Transport Function suppresses the creation and attempt to forward any Diameter messages to a Diameter Peer Node when the Egress Transport Congestion Level is CL-4. This includes Peer-to-Peer messages such as DPR/DPA, DWR/DWA and any non- Peer-to-Peer messages such as Diameter Transport Function-initiated Answer responses associated with DA-MP Overload.

The Egress Transport Congestion feature behaves as follows:

- Messages that are already committed to the Connection by the Diameter Routing Function when a Connection initially becomes transport congested will be discarded.
- When a Diameter Connection socket becomes blocked (such as when a TCP or SCTP socket becomes full), the Diameter Transport Function sets the Egress Transport Congestion Level to CL-4 to prevent the Diameter Routing Function from forwarding any further Request or Answer messages to the Connection.

  Any messages received while the Egress Transport Congestion Level is set to CL-4 are automatically discarded by the Diameter Transport Function. This would normally occur for messages that the

Diameter Routing Function has already forwarded to the Diameter Transport Function before receiving notification that the Connection Priority Level (CPL) was changed to a value of 4.

- When the Diameter Transport Function is notified that the socket is no longer blocked, the Diameter Transport Function sets the Egress Transport Congestion Level to CL-3, and starts Egress Transport Congestion abatement using a time-based step-wise abatement algorithm.

  The Transport Congestion Abatement Timeout that is configured for each Diameter Connection defines the time spent abating each Congestion Level during abatement. For example, if the Transport Congestion Abatement Timeout value is set to 5 seconds when the Egress Transport Congestion Level enters CL-3, it will remain in CL-3 for the full 5 seconds before the Egress Transport Congestion Level can be reduced to CL-2.

  If the TCP or SCTP socket becomes full while the Diameter Transport Function is in Egress Transport Congestion abatement, the entire abatement procedure is restarted.

- A throttled event with "Egress Transport Congestion" as the reason for the event is logged every time the Connection Priority Level (CPL) changes due to Egress Transport Congestion.
- When the Diameter Transport Function successfully establishes an IPFE TCP or SCTP connection, it sets the Egress Transport Congestion Level for the Diameter Connection to CL-0.

When Egress Transport Congestion occurs, the "Connection degraded" alarm is raised, indicating "Egress Transport Congestion" and the CL.

Note: The "Connection degraded" alarm can be raised by DSR for other reasons, and will not be raised for Egress Transport Congestion if it is already asserted.

When the Connection CL is 0 upon decrementing (the Egress Transport Congestion condition and all other conditions that could raise the alarm are mitigated), abatement is complete and the "Connection degraded" alarm is cleared.

Diameter Configuration for the Egress Transport Congestion Feature

The Egress Transport Congestion feature is always enabled on all DSR Diameter Connections and cannot be disabled by the operator.

For the Egress Transport Congestion feature, the Transport Congestion Abatement Timeout element can be configured for each Diameter Connection, using the Diameter Configuration Connections GUI page. The Transport Congestion Abatement Timeout value is the time period (in seconds) spent by the Connection in abating each Congestion Level during abatement.

The Transport Congestion Abatement Timeout value cannot be modified when the Connection is in service (Connection Admin State=Enabled).

Per Connection Egress Message Throttling

To protect servers in periods of excessive load, explicit egress message throttling and user-configurable Connection Pending Transaction limiting can be used as messages are aggregated from several ingress Peers (clients) and can overload the egress Peer (server).

To assist with prevention of Diameter Peer overload, DSR provides a method for throttling the volume of Diameter Request traffic sent to a Peer Connection. The Egress Message Rate (EMR) on a Connection being throttled by the DSR is equivalent to the egress Request rate + the egress Answer rate on the Connection. The allowed maximum egress message rate (Max EMR) can be configured per Connection.

The Per Connection Egress Message Throttling (PCEMT) feature works in conjunction with the User Configurable Message Priority feature to provide intelligent load shedding based on the volume of the offered load as shown in *Table 144: Congestion Levels Based on Thresholds*. The load shedding is performed by dropping Requests based on Priority and the offered message rate. PCEMT sheds messages as the offered message rate gets closer to the configured Max EMR.

The *User Configurable Message Priority* feature provides the ability to configure Message Priority Configuration Sets that define the Priority. If a Message Priority Configuration Set is not assigned to the Connection to specify the Priority, load shedding is still performed but it is primarily restricted to Requests as all Requests are assigned a Priority of 0.

PCEMT uses configurable Egress Message Throttling Configuration Sets to govern Connection egress message throttling behavior. The Egress Message Throttling Configuration Set elements (Max EMR, Throttling Thresholds, Abatement Thresholds, a smoothed EMR, and an Abatement Time) provide a high degree of user control over the characteristics of transitions between Congestion Levels due to throttling.

- A DSR supports up to 50 Egress Message Throttling Configuration Sets.
- Up to 500 Peer Connections can have egress message throttling enabled in a single DSR NE.

Interaction with the Alternate Routing Across Route Groups in a route List Feature

PCEMT can be used in conjunction with the Alternate Routing Across Route Groups feature to route all throttled Requests using non-preferred Route Groups when all Connections in the preferred Route Group are congested. Eligible Peers or Connections from the other priority Route Groups of the Route List can be used to deliver a Request after all the Peers or Connections in the current Route Group are exhausted. Alternate Routing Across Route Groups is attempted only if the Maximum Per Message Forwarding Allowed (configured in the Diameter Configuration Routing Option Sets) is not exceeded.

For example, a Route List is configured with two Route Groups. The Preferred Route Group contains two HSSs, HSS-1 and HSS-2 each with one Connection and the Non-Preferred Route Group contains HSS-3 and HSS-4, each with one Connection. If the Connection(s) to both HSS-1 & HSS-2 exceed Throttle Threshold X, Requests with Priority below X are routed to HSS-3 and HSS-4, while Requests with Priorities equal to or greater than X continue to be routed to HSS-1& HSS-2. If both, HSS-3 and HSS-4 exceed Throttle Threshold X, Requests with Priority less than X are discarded.

Diameter Configuration for Per-Connection Egress Message Throttling

The Message Priority Configuration Sets are provided by the User-Configurable Message Priority feature.

Egress Throttling Configuration Sets can be configured and assigned to Connections to control egress throttling behavior. In each Egress Message Throttling Configuration Set, the following elements can be configured:

- Max EMR - the maximum volume of traffic that can be served over a particular Connection

  For Peers that are deployed with multiple Connections, it is recommended as a guideline to set the Max EMR on each Connection by dividing the total capacity of the Peer by the number of Connections to the Peer.

- Throttle Threshold Levels and Abatement Levels 1, 2, and 3 -

  Abatement Threshold Levels - percent of Max EMR; when Threshold falls below the specified Level, the Connection Congestion Level is lowered.

Throttle Threshold Levels - percent of Max EMR; when the Threshold exceeds the specified Level, the Connection Congestion Level is raised.

The Max EMR and the TT-1 and AT-1 Thresholds must be configured. TT-2, AT-2, TT-3 and AT-3 are optional but have to be configured in pairs. For example, if TT-2 is configured, AT-2 must also be configured; and if TT-3/AT-3 is configured, TT-2/AT-2 must be configured.

Each EMR Throttle and Abatement Threshold Level pair dictates how the Connection congestion state will be updated as indicated in *Table 144: Congestion Levels Based on Thresholds*. The offered rate is the value computed for Smoothed EMR.

If TT-x (where x can be 1, 2 or 3) of a Connection is exceeded, only Requests with Priority below x are throttled while Requests with Priority x or greater are allowed over the Connection.

In an Egress Message Throttling Configuration Set, the Max EMR and the TT-1 and AT-1 Thresholds must be configured. TT-2, AT-2, TT-3 and AT-3 are optional but have to be configured in pairs. For example, if TT-2 is configured, AT-2 must also be configured; and if TT-3/AT-3 is configured, TT-2/AT-2 must be configured.

EMR throttling and onset requires only one EMR sample to exceed a Throttling Threshold to advance the EMR Congestion Level. Multi-step throttling is supported. For example, the EMR Congestion Level can be increased from CL-0 to either CL-1, CL-2, or CL-3 after one EMR sample period (every 90 milliseconds). This allows for a rapid response to traffic load increases while taking a more conservative approach to traffic load decreases.

Only single-step abatement is supported. For example, CL-3->CL-2 abatement is supported, but not CL-3->CL-1.

- **Table 144: Congestion Levels Based on Thresholds**

Throttle (TT-X) and Abatement Thresholds (AT-X)	Connection Congestion Level Impact	Comments
TT-3	When offered rate exceeds Threshold, Set Congestion Level (CL) = 3.	Allows Answers; Blocks Priority 0,1,2 Requests
AT-3	When offered rate falls below Threshold, Set Congestion Level = 2	Allows Answers and Priority 2 Requests; Blocks Priority 0,1 Requests
TT-2	When offered rate exceeds Threshold, Set Congestion Level = 2	Allows Answers and Priority 2 Requests; Blocks Priority 0,1 Requests
AT-2	When offered rate falls below Threshold, Set Congestion Level = 1	Allows Answers and Priority 2, 1 Requests; Blocks Priority 0 Requests
TT-1	When offered rate exceeds Threshold, Set Congestion Level = 1.	Allows Answers and Priority 2, 1 Requests; Blocks Priority 0 Requests
AT-1	When offered rate falls below Threshold, Set Congestion Level = 0	Allows Answers and Priority 2, 1,0 Requests; Blocks None.

- Smoothing Factor - Allows control of the sensitivity of the smoothed EMR by specifying the percent contribution of the smoothed EMR sample to the latest EMR

  Higher values signify a higher contribution of the previously computed smoothed EMR toward the smoothed EMR; the smoothed EMR converges slowly to the current EMR.

  Lower values signify a higher contribution of the current EMR toward the smoothed EMR; the smoothed EMR converges quickly to the current EMR.

  The current EMR sample is the raw measure of total messages (Requests and Answers) transmitted over a Connection, and is measured is sampled every 90 milliseconds and normalized to messages per second. The smoothed EMR is calculated as an "exponential moving average" that is used in EMR Congestion Level abatement.

  The most recent Smoothed EMR value is displayed on the Diameter > Maintenance > Connections GUI page for all Connections that have been assigned an Egress Message Throttling Configuration Set.

- Abatement Time - amount of time that a throttled Connection's smoothed EMR must remain below an abatement level before allowing it to abate to a lower Congestion Level.

To enable Egress Message Throttling on a Connection,

- A configured Egress Message Throttling Configuration Set must be configured.
- The configured Egress Message Throttling Configuration Set must be assigned to the DSR Peer Connection that is to be throttled using the settings in that Egress Message Throttling Configuration Set.
- The Per Connection Egress Message Throttling Enabled option must be checked on the Diameter > Configuration > System Options GUI page.

  Disabling Egress Message Throttling will have the same effect as un-assigning the Egress Message Throttling Configuration Set for all the Connections that have been previously associated with an Egress Message Throttling Configuration Set.

All Egress Message Throttling Configuration Set parameters can be modified, but the Configuration Set cannot be deleted, while the associated Connections are in service.

Limitations

Given that the Per Connection Egress Message Throttling feature works per Connection and does not consider the throttling status on all the Connections to a Peer, it is possible that certain Connections to a Peer can experience Egress Message Throttling and discard messages while other Connections to the same Peer are not congested, thereby underutilizing the capacity of the Peer.

Because EMR is calculated every 90 milliseconds, EMR abatement can only occur on an integer-multiple of 90 milliseconds. For example, if the user defines an EMR Abatement Time of 500 milliseconds, then the actual abatement period would be 540 milliseconds (6 * 90 milliseconds).

User Configurable Connection Pending Transaction Limiting

User-Configurable Connection Pending Transaction Limiting (UC-CPTL) provides a configurable pending transaction limit for each DSR Peer Connection, to customize the distribution of the available Pending Transaction Records on a DA-MP based on the varying deployment requirements. The limit can be configured independently for each DA-MP in the DSR.

DSR Peer Nodes have differing requirements for the maximum number of pending transactions required on the DSR:

- DSR-to-Server Connections typically carry higher traffic volumes than DSR-to-Client Connections due to DSR aggregation of traffic from many client Connections to few server Connections.
- A high percentage of the traffic on DSR-to-Server Connections requires Pending Transaction Records in the DSR, because Requests are the majority of the DSR egress traffic on these Connections.
- A low percentage of the traffic on DSR-to-Client Connections requires Pending Transaction Records in the DSR, because Answers are the majority of the DSR egress traffic on these Connections.
- DSR-to-Server Connections might encounter significant increases in offered load for a very short time immediately following network events such as MME failures or failures of redundant Servers providing the service. Handling these types of sudden increases in traffic volume can require higher Pending Transaction Limits on the Connections.

A DA-MP allocates a Pending Transaction Record for a Request message sent by the DA-MP to a Peer, and holds the PTR until the transaction completes or otherwise terminates (including Answer received and timeout termination). (An Answer message sent by a DA-MP to a Peer does not require a Pending Transaction Record.)

Multiple Active DA-MPs can route Requests to a single Connection. As a result, the maximum number of pending transactions that can exist in the DSR for a single Connection is dictated by the sum of the Pending Transaction Per Connection values enforced independently by each Active DA-MP that is routing Requests to the Connection.

The primary use of pending transaction limits for Connections on a DSR DA-MP is to prevent a small number of Connections on a DA-MP from consuming a disproportionate number of the available Pending Transaction Records on the DA-MP, which could result in limited Pending Transaction Record availability for the remaining Connections.

Diameter Configuration for the Pending Transactions Per Connection Option

The DSR provides a configurable Pending Transactions Per Connection option for each DSR Peer Connection. The value is configured in the Diameter Options of the Connection Configuration Set that is assigned to the Connection. The configured limit is enforced independently by all DA-MPs in the DSR.

The Pending Transaction Per Connection value for a Connection can be modified while the Connection is in-service. If the Pending Transactions Per Connection value is modified to a value below the current value, any pending transactions on the Connection that are above the new limit will continue to be processed and the new Pending Transactions Per Connection value will be applied only for new transactions that are initiated after the change.

Egress Throttle Groups

An Egress Throttle Group is a collection of Diameter Connections or Peers, or both, that are logically grouped together to monitor Egress Message Rate and Pending Transactions for multiple Peers and Connections across multiple DA-MPs on a DSR Network Element. If a Peer is assigned to the Egress Throttle Group, then all Diameter Connections to that Peer are implicitly part of the Egress Throttle Group.

The following Egress Throttle Group (ETG) features provide management of egress message throttling from a DSR to Peer Diameter Nodes on a specified set of Diameter Connections:

- Egress Throttle Group Rate Limiting
- Egress Throttle Group Pending Transaction Limiting

ETG Rate Limiting and Pending Transaction Limiting throttling are done for Request Messages only.

Note: The Per Connection Egress Message Throttling and User Configurable Connection Pending Transaction Limiting features for Egress Message Throttling are defined at a single Diameter Connection level and are local to each DA-MP. These features are described in *Per Connection Egress Message Throttling* and *User Configurable Connection Pending Transaction Limiting*.

Aggregated egress traffic controls falls into 2 categories:

- Egress Message Rate (EMR)
- Egress Pending Transactions (EPT)

Egress Message Rate controls are used to throttle traffic levels to a set of Diameter Nodes so that the cumulative rate of traffic is controlled. EMR controls are across a set of configured connections and/or peers.

Egress Pending Transactions controls are used to control the maximum number of Pending Requests that can be sent to a set of Diameter Nodes. This can be used for load-balancing when a network element is not responding at expected rates, and limits the total number of Requests that can be pending to a set of Diameter Nodes. EPT controls are across a set of connections and/or peers, and are cumulative across all DA-MPs.

Egress Throttle Groups Description

Egress Throttle Groups are implemented as part of the Diameter Routing Function.

An Egress Throttle Group is independent of a Route Group (Connection Route Group or Peer Route Group). The members of an Egress Throttle Group may or may not be same as defined in a Route Group; there is no defined relationship between Egress Throttle Groups and Route Groups.

The Egress Message Rate throttling is controlled by the configured maximum Egress Message Rate (EMR) on an aggregated basis and the "Egress Throttle Group - Rate Limiting Congestion Level (ETG-R CL-) (range: CL-0- CL-3) for the ETG.

The Egress Pending Transaction Limiting throttling is controlled by the configured maximum Egress Pending Transactions (EPT) on an aggregated basis and the "Egress Throttle Group - Pending Transaction Limiting Congestion Level (ETG-PCL) (range: CL-0- CL-3) for the ETG.

An Egress Throttle Group can contain the following configuration data:

- Up to 128 Peers, Connections, or Peers and Connections
- Maximum Egress Message Rate (EMR), used for calculation of Onset and Abatement Thresholds
  - Onset and Abatement Thresholds, as percentages of the Maximum EMR, to use with Message Priority to determine which Requests to throttle
  - Smoothing Factor to control responsiveness of egress Request rate control
  - Abatement Time
- Maximum Egress Pending Transactions(EPT), used for calculation of Onset and Abatement Thresholds
  - Onset and Abatement Thresholds, as percentages of the Maximum EPT, to use with Message Priority to determine which Requests to throttle
  - Abatement Time

DSR supports a maximum of 5 congestion levels (CL-0 to CL-4) that indicate the Congestion Level of a resource. CL0 indicates that the resource has no congestion, and CL-4 indicates that the resource is completely blocked. CL-1, CL-2, and CL-3 indicate increasing levels of congestion.

Egress Throttle Groups (ETG) can be configured in Diameter Configuration; each Egress Throttle Group will have its own Congestion Level states based on its configuration.

1. As an Egress Throttle Group 's egress Request message traffic rate increases and exceeds the Egress Throttle Group Rate Limiting onset thresholds configured in the Egress Throttle Group, the Egress Throttle Group 's Congestion Level also increases.

1. As the Egress Throttle Group 's total number of Pending Transactions increases and exceeds the Egress Throttle Group Pending Transaction Limiting onset thresholds configured in the Egress Throttle Group , the Egress Throttle Group 's Congestion Level also increases.

As the Egress Throttle Group 's Congestion Level increases, Message Priority becomes a factor in determining if a message can be routed to a member of the Egress Throttle Group, or will be throttled. Requests with Message Priority less than Congestion Level will not be routed to any member of the Egress Throttle Group.

Diameter Request messages are assigned a Message Priority 0, 1, or 2; Answers always have Priority 3. The Priority of the Request message controls when an ETG performs throttling is shown in *Table 145: Message Priority and ETG Congestion Level*

Table 145: Message Priority and ETG Congestion Level

Request Message Priority	When Permitted to route to Member of ETG
0	Congestion Level 0
1	Congestion Level 0, 1
2	Congestion Level 0, 1, 2

When the EMR for an Egress Throttle Group reaches the Egress Throttle Group 's Maximum Egress Request Rate or the Egress Throttle Group 's Pending Transactions reaches the Egress Throttle Group 's Maximum Egress Pending Requests, no Requests will be routed to any members of the Egress Throttle Group.

Egress Throttle Group Rate Limiting

The ETG Message Rate Controls are optional, but if defined and enabled, then ETG Message Rate Congestion level will be updated as indicated in *Table 146: ETG Message Rate Congestion Levels Based on Threshold*.

Table 146: ETG Message Rate Congestion Levels Based on Threshold

Onset and Abatement Thresholds	ETG Rate Congestion Level (ETG-RCL) Impact
Onset Threshold-3 (OT-3)	When ETG rate exceeds Threshold, set ETG-RCL = CL-3
Abatement Threshold-3 (AT-3)	When ETG rate falls below Threshold, set ETG-RCL = CL-2
Onset Threshold-2 (OT-2)	When ETG rate exceeds Threshold, set ETG-RCL = CL-2

Onset and Abatement Thresholds	ETG Rate Congestion Level (ETG-RCL) Impact
Abatement Threshold-2 (AT-2)	When ETG rate falls below Threshold, set ETG-RCL = CL-1
Onset Threshold-1 (OT-1)	When ETG rate exceeds Threshold, set ETG-RCL = CL-1
Abatement Threshold-1 (AT-1)	When ETG rate falls below Threshold, set ETG-RCL = CL-0

In an Egress Throttling Group, if Maximum Egress Request Rate is configured, then OT-1 and AT-1 thresholds must be configured. OT-2, AT-2, OT-3 and AT-3 are optional but must be configured in pairs; for example, if OT-2 is configured, AT-2 must also be configured. Finally, AT-3 must be configured if OT-3 is expected to be configured.

In addition to the thresholds, the Smoothing Factor and the Abatement Time provide a high degree of user control over the characteristics of transitions between Congestion Levels due to throttling.

- Smoothing Factor - Allows control of the sensitivity of the smoothed EMR, by specifying the % contribution of the smoothed EMR sample to the latest EMR.

  Higher values signify a higher contribution of the previously computed smoothed EMR towards the smoothed EMR; the smoothed EMR converges slowly to the current EMR.

  Lower values signify a higher contribution of the current EMR towards the smoothed EMR; the smoothed EMR converges quickly to the current EMR.

  The local EMR sample is the raw measure of routable Request Messages transmitted over the set of Connections and/or Peers defined in the Egress Throttle Group across all DA-MPs. The local EMR is measured every 90 milliseconds and normalized to messages per second. The local EMR sample is then aggregated by the DA- MP Leader, then the smoothed aggregated EMR is calculated as an "exponential moving average" that is used in EMR Congestion Level abatement.

- EMR Abatement Time - Amount of time that a throttled connection's smoothed EMR must remain below an abatement level before allowing it to abate to a lower Congestion Level.

EMR onset requires only one EMR sample to exceed an onset threshold to advance the ETG-RCL. Multi-step throttling is supported. For example, the EMR Congestion Level can be increased from CL-0 to CL-1, CL-2, or CL-3 after one EMR sample period. This allows for a rapid response to traffic load increases while taking a more conservative approach to traffic load decreases.

Only single step abatement is supported. For example CL-3-> CL-2 abatement is supported but not CL-3-> CL-1.

Rate Limiting must be enabled on the **Diameter > Maintenance > Egress Throttle Groups** GUI page before Egress Message Rate throttling can be started for Egress Throttle Groups. If Rate Limiting is enabled, then any routable Request message sent to a Peer or Connection on any DA-MP on that NE contained in the ETG will be used for rate calculation purposes. (Diameter management messages such as CER/CEA, DWR/DWA, and DPR/DPA are not counted in the egress message rate.)

Egress Throttle Group Pending Transaction Limiting

If Egress Throttle Group Rate Limiting is configured and enabled in an Egress Throttle Group, then the ETG Pending Transaction Congestion Level will be updated as indicated in *Table 147: ETG Pending Transaction Congestion Levels Based on Threshold*.

Table 147: ETG Pending Transaction Congestion Levels Based on Threshold

Onset and Abatement Thresholds	ETG Pending Transaction Congestion Level (ETG-PCL) Impact
Onset Threshold-3 (OT-3)	When ETG Pending Transactions exceeds Threshold, set ETG-PCL = CL-3
Abatement Threshold-3 (AT-3)	When ETG Pending Transactions falls below Threshold, set ETG-PCL = CL-2
Onset Threshold-2 (OT-2)	When ETG Pending Transactions exceeds Threshold, set ETG-PCL = CL-2
Abatement Threshold-2 (AT-2)	When ETG Pending Transactions falls below Threshold, set ETG-PCL = CL-1
Onset Threshold-1 (OT-1)	When ETG Pending Transactions exceeds Threshold, set ETG-PCL = CL-1
Abatement Threshold-1 (AT-1)	When ETG Pending Transactions falls below Threshold, set ETG-PCL = CL-0

In an Egress Throttling Group, if Maximum Egress Pending Transactions is configured, then OT-1 and AT-1 thresholds must be configured. OT-2, AT-2, OT-3 and AT-3 are optional but must be configured in pairs; for example, if OT-2 is configured, AT-2 must also be configured. Finally, AT-3 must be configured if OT-3 is expected to be configured.

The local sample of number of pending Transactions to an ETG is periodically collected and sent to the DA-MP Leader for aggregation. The aggregated value is then sent back to each DA-MP for threshold and abatement calculation. No smoothing is applied to EPT, and aggregated values are sent back to each DA-MP.

The EPT Abatement Time is the amount of time that egress Pending Transactions must remain below an abatement level before allowing it to abate to a lower Congestion Level. No smoothing is applied to EPT abatement.

Pending Transaction Limiting must be enabled Maintenance GUI before Egress Pending Transaction Limiting can be started for Egress Throttle Groups. If Egress Pending Transaction Limiting is enabled, then any pending Request sent to a Peer or Connection on any DA-MP on that NE contained in the Egress Throttle Group will be used for Pending Transaction Limiting calculation.

Assumptions and Limitations

Egress Throttling Groups have the following assumptions and limitations:

- EMR abatement can occur only on an integer-multiple of 125ms. For example, if an EMR Abatement Time of 600ms is configured, then the "actual" abatement period would be 625ms (5 * 125ms). Egress Pending Transactions are updated every 125ms; if an EPT Abatement of 600ms is configured, then the "actual" abatement period would be 625ms (5 * 125 ms).
- Local EMR for a 90 ms sample period is the normalized per-second message rate based on the amount of traffic transmitted during the sample period. With a particular combination of traffic characteristic, thresholds, and Smoothing Factor, this can cause EMR congestion onset to occur in the presence of short traffic bursts that would normally, over a second, not have resulted in an EMR threshold being crossed. As an example, suppose local messages transmitted to an ETG during a 90ms sample X are 100 and subsequent samples (X+n) during subsequent 910 ms (1 second -

90ms) are less than 100 msgs. Local EMR for sample period X will be: 100*(1000ms/90ms) = 1100 messages/sec even though in reality the Local Message Rate was lower than 1100 msgs/sec. With a higher Smoothing Factor, the effect of this limitation can be reduced.

- Because the sampling timer and MP Leader aggregation are asynchronous, the ETG aggregated rate can lag by up to 250 ms.

Diameter Configuration for Egress Throttle Groups

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

The **Diameter > Configuration > Egress Throttle Groups** GUI pages provide fields for configuring each function. Each function, if configured in the system, must have its Admin State changed to Enabled on the **Diameter > Maintenance > Egress Throttle Groups** GUI page.

Egress Throttle Groups configuration procedures are provided in *Egress Throttle Groups configuration*.

Egress Throttle Groups maintenance information and procedures are provided in *Egress Throttle Groups maintenance*.

Glossary

A

ACK	Data Acknowledgement
AES	Advanced Encryption Standard
Application Routing Rule	A set of conditions that control message routing to a DSR application based on message content.
ASCII	American Standard Code for Information Interchange
ATH	Application Trouble Handler Answer Topology Hiding
ATR	Answer Topology Restoral (DSR)
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

CCA	Credit Control Answer The Diameter message that is received from the prepaid rating engine to acknowledge a CCR command.

C

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

D

DA-MP	Diameter Agent Message Processor A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application such as CPA can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.
DAS	Diameter Application Server
DEA	Diameter Edge Agent
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.
Diameter Agent Message Processor	A computer or blade that is hosting the DSR. Multiple instances of the DSR each execute on a separate physical DA-MP. Each instance shares run-time status information with all other instances for the Diameter connections that it controls. In inter-MP routing, an instance can route an ingress Answer message to another instance that performed routing for

D

	the corresponding ingress Request message. See DA-MP.
Diameter Network	A set of Diameter Nodes identified by a Realm name. A Diameter Node that initiates a Diameter message is identified by the mandatory Origin-Realm AVP in the message. A Diameter Node that is the intended destination of a Diameter message is identified by the mandatory Destination-Realm AVP in the message.
DNS	Domain Name System A system for converting Internet host and domain names into IP addresses.
DPA	Disconnect-Peer-Answer A message used by a Diameter node to answer the Disconnect-Peer-Request (DPR).
DPR	Disconnect-Peer-Request A message used by a Diameter node to inform its peer of its intent to disconnect the transport layer. Upon receipt of a DPR, the Disconnect-Peer-Answer (DPA) is returned.
DSR	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.

D

DSR Application	Any DSR software feature or function that is developed as a user of the Diameter base protocol.
DWA	Device-Watchdog-Answer A Diameter message used with the Device-Watchdog-Request (DWR) message to proactively detect connection failures. If no traffic is detected on a connection between the Mobile Originated application and the prepaid rating engine within the configured timeout period, a DWR message is sent to the prepaid rating engine. If the prepaid rating engine fails to respond with a DWA within the required time, the connection is closed with the prepaid rating engine and initiates failover procedures. All new and pending requests are then sent to the secondary server.
DWR	Device-Watchdog-Request A Diameter message used with the Device-Watchdog-Answer (DWA) message to proactively detect connection failures. If no traffic is detected on a connection between the Mobile Originated application and the Diameter server within the configured timeout period, a DWR message is sent to the Diameter Server. If the Diameter server fails 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.

F

FABR	Full Address Based Resolution

F

	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.
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name The complete domain name for a specific computer on the Internet (for example, www.tekelec.com). A domain name that specifies its exact location in the tree hierarchy of the DNS.
Full Address Based Resolution	See FABR.

H

HSS	Home Subscriber Server A central database for subscriber information.

I

IMSI	International Mobile Subscriber Identity A unique internal network ID identifying a mobile subscriber. International Mobile Station Identity

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

L

	listen port number, supported transport types, etc.

M

MCC	Mobile Country Code A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber. See also MNC, IMSI.
MCCS	Message Copy Configuration Set
MME	Mobility Management Entity
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.

N

NIST	National Institute of Standards and Technology

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

P

	peer node based on message content.
Pending Answer Timer	A timer that limits the maximum time that Diameter will wait for an Answer response from an upstream Peer Node. This timer is started when a Request message is queued for forwarding on a Diameter connection, and the timer is stopped when an Answer response to the message is received.
Policy DRA	Policy Diameter Relay Agent. A scalable, geo-diverse DSR application that creates a binding between a subscriber and a PCRF, and routes all policy messages for a given subscriber to the PCRF that currently hosts that subscriber's policy rules. Policy DRA is capable of performing Topology Hiding to hide the PCRF from the Policy Client.
Protected Network	A Diameter network whose topology information is being hidden by one of the Diameter Topology Hiding features.
PTR	Pending Transaction Record

R

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

R

	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.
RTH	Request Topology Hiding - A Topology Hiding trigger point that identifies a location within Diameter routing where topology-related information in a Request message is hidden or obscured based upon a set of Topology Hiding rules.
RTR	Router Routes all types of SMS traffic.

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. 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

S

	to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.
Session Binding Repository	See SBR.
SGSN	Serving GPRS Support Node

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.
TH	Topology Hiding
Topology Hiding	The CPF will appear as a single large CDF to the CTFs, and vice-versa. CPF topology hiding occurs for both Request and Answer messages. When sending a Request message upstream, it refers to the hiding of the downstream (CTF) host ID by the DSR when sending a message to the upstream (CDF) peer. Topology hiding involves modifying the Origin-Host and Origin-Realm AVPs. The removal of Diameter host names from messages. This is most often required at the boundary between two service providers with the goal of limiting the information that another service provider can discover as a result of Diameter traffic traveling between the carrier's networks. For DSR CPA,

T

	the CPF will appear as a single large CDF to the CTFs, and vice-versa. CPF topology hiding occurs for both Request and Answer messages. When sending a Request message upstream, it refers to the hiding of the downstream (CTF) host ID by the DSR when sending a message to the upstream (CDF) peer. Topology hiding involves modifying the Origin-Host and Origin-Realm AVPs.
Trusted Network	A Diameter network that does not have home network topology information hidden by the Diameter Topology Hiding features.

U

Untrusted Network	A Diameter network which has topology information hidden by the Topology Hiding features.
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.
UTC	Coordinated Universal Time

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

V

	the perspective of the IP network, these IP hosts appear as a single host.
VM	Virtual Machine