Oracle® Communications Diameter Signaling Router

Diameter User Guide

Release 9.2.0.0.0
G10724-01
September 2025

Oracle Communications Diameter Signaling Router Diameter User Guide, Release 9.2.0.0.0

G10724-01

Contents

3 Diameter Maintenance

12 Diameter Capacity and Congestion Controls

List of Figures

List of Tables

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), select **1**.
   - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in this Guide

This section introduces the documentation updates for Release 9.2.0.0.0.

Release 9.2.0.0.0 - G10724-01, September 2025

- Updated the value of **MaxPeersPerRouteGroup** in the Table 2-1.
- Updated range limit of the Peer Node in the Table 2-21.
- Added **MaxPrtRulesPerPrtTable** component in the Table 2-1.
- Added the steps 30 to34 in the Adding a Peer Node section to provide information about the Dess feature.
- Added the steps 17 to 21 in the Adding a Local Node section to provide information about the Dess feature.
- Added the steps 6 to 9 in the Adding a Route List section.
- Added SCTP Parameter Configuration in the Appendix section.
- Updated value of the below components in the Table 2-1 to allow the user to configure additional components.
  - Traffic Throttle Point
  - Traffic Throttle Group
  - Shared Traffic Throttle Group
- Added the following local nodes in the Diameter Local Nodes section:
  - Dess Enable
  - CA Certificate
  - Public Certificate
  - Private Key
  - Dess Algorithm
- Added a note in the following sections to provide information about the algorithm types that match the Dess Algorithm field:
  - Diameter Local Nodes
  - Diameter Peer Nodes
- Added the following local node configuration fields in the Diameter Local Node Configuration Elements section:
  - Dess feature
  - CA Certificate
  - Public Certificate
  - Private Key
  - Dess Algorithm
- Added the following peer node configuration fields in the Diameter Peer Node Configuration Elements section:
  - Dess feature

- CA Certificate
- Public Certificate
- Dess Algorithm
- Action on verification failure
- Added the following fields in the Table 2-22 and Table 3-1.
  - Destination-Host
  - Destination-Realm
  - Origin-Host
  - Origin-Realm

1 Introduction

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

The Diameter menu options allow you to:

- Perform Diameter Signaling Router configuration tasks
- View maintenance information for Diameter components
- Generate reports
- Perform IDIH troubleshooting
- Work with AVP dictionary components
- Access Mediation GUI pages

1.1 Overview of Diameter Signaling Router Tasks

This document provides information about how to use the 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
- High-level summary for Troubleshooting with IDIH
- **AVP** Dictionary information
- High-level summary for Mediation

See *Integrated DIH User's Guide* and *Diameter Mediation User 's Guide* for more information about those applications.

1.2 References

For information about Measurement Data Streaming, see *Diameter Signaling Router Operation, Administration and Maintenance (OAM) Guide* and *Measurement Data Streaming User Guide.*

1.3 Scope and Audience

This content is intended for personnel who perform diameter signaling tasks.

This content contains procedures for performing tasks using the product GUI.

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

The Diameter software component is shared by multiple applications in the product line. For this reason, this content includes references to the shared applications, and describes GUI options that are not visible or applicable to SDM. For example, applications (such as RBAR, FABR, CPA, and Policy DRA) and IPFE are currently not used by SDM, so disregard any references to these applications.

1.4 Content Organization

This content is organized as follows:

- Introduction contains general information about the Diameter and Mediation help documentation, the organization of this manual, and how to get technical assistance.
- Configuring Diameter provides information about configuring Diameter resources.
- Diameter Maintenance provides information about how to view the status of Diameter resources, and how to enable and disable connections and applications.
- Diameter Reports provides information about how to produce Diagnostic Tool reports and MP Statistics (SCTP) reports.
- Troubleshooting with IDIH provides summary information about the Integrated Diameter Intelligence (IDIH) feature. See *Integrated DIH User's Guide* for more information.
- Diameter AVP Dictionary provides information about Attribute-Value Pairs (AVPs) that are used by the Diameter Routing Function in making decisions for routing messages to and from applications and for the Diameter Message Copy feature.
- Mediation provides information about working with the Mediation feature.
- Diameter Shared Traffic Throttle Groups provides information about all Traffic Throttle Groups (TTGs) defined as shared across the diameter routing network.
- Diameter Topology Hiding describes the components that can be configured for Diameter Topology Hiding.
- Diameter Egress Throttle List describes the components can be configured for Egress Throttle List from the NOAM.
- Diameter Message Copy describes the Diameter Message Copy feature, which is used to send a copy of a message to a Diameter Application Server (DAS).
- Diameter Capacity and Congestion Controls contains information about the various ways capacity and congestion can be managed to preserve the availability and Quality of Service (QoS).

2 Configuring Diameter

The **Diameter**, and then **Configuration** GUI allows you to manage diameter signaling routing configuration.

You can perform different tasks on an Active Network OAM (**NOAM**) and an Active System OAM (**SOAM**).

2.1 Understanding the Diameter Configuration Sequence

Use the **Diameter**, and then **Configuration** GUI pages to manage Diameter configuration.

Some components must be configured before others can be configured.

Diameter configuration on the SOAM must occur in the following order, because some are dependent on one another:

1. For DA-MPs, make any needed changes to configurable elements in the MP Profiles used for the DA-MPs in the system; and assign **MP Profiles** to the DA-MPs. See the MP Profiles information in *Diameter Common User's Guide*.
2. Configure **Application Route Tables**. See Diameter 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**. See Diameter Pending Answer Timers.
4. Configure **Peer Route Tables**. See Diameter 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**. See Diameter Routing Option Sets.
6. Configure **Application IDs**. See Using Application IDs to Identify Diameter Applications.
7. Configure **Command Codes**. See Diameter Command Codes.
8. Configure **MCC Ranges** if either the Full Address Based Resolution (FABR) or Range Based Address Resolution (RBAR) application is activated. See the MCC range information in *Diameter Common User's Guide*.
9. Configure **CEX Parameters**. See Diameter CEX Parameters.
10. Configure **CEX Configuration Sets**. See Capacity Configuration Sets.
11. Configure **Connection Configuration Sets**. See Diameter 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**. See Diameter Local Nodes.
13. Configure **Transaction Configuration Sets**. See Transaction Configuration Sets.
14. Configure **Peer Nodes**. See Diameter Peer Nodes. Enable **Topology Hiding Status** if Topology Hiding is applicable to the Peer Node. See Diameter Topology Hiding.

> **Note**
>
> Topology Hiding is available on the NOAM only.

15. Configure **Capacity Configuration Sets** for use with the Per-Connection Ingress MPS Control feature and Validating Diameter Connection Capacity. See Capacity Configuration Sets.
16. Configure **Egress Message Throttling Configuration Sets**. See Egress Message Throttling Configuration Sets.
17. Configure **Message Priority Configuration Sets**. See Message Priority Configuration Sets.
18. Configure **Connections**. IPFE Initiator DA-MP can be configured from this GUI page. See Connections.
19. Configure **Route Groups**. See Diameter Route Groups.
20. Configure **Route Lists**. See Diameter Route Lists.
21. If Alternate Implicit Routing is used, edit **Peer Nodes** and select a Route List for each **Alternate Implicit Routing** element. See Diameter Peer Nodes.
22. Configure **Message Copy Configuration Sets**. See Message Copy Configuration Sets.
23. Configure **Peer Routing Rules** in each configured Peer Route Table. See Diameter Peer Route Tables.
24. Configure **Egress Throttle Groups**. See Diameter Egress Throttle Groups.
25. Configure TTPs.
26. Configure **Reroute On Answer**, if it is used in the system. See Diameter Reroute On Answer.
27. Configure **Application Routing Rules** in each configured Application Route Table. See Diameter Application Route Tables.
28. If necessary, add **Application Priority Options**. See Diameter Application Priority Options.
29. If necessary, change the default **System Options** (see Diameter System Options):
    - Enable the **Per Connection Egress Message Throttling** feature if it is used.
    - Enable the **Message Copy Feature** if it is used.
    - Change any default values as needed.
30. If necessary, enter or change default **DNS Options**. See Diameter DNS Options.
31. Use the **Diameter**, and then **Maintenance** pages to enable configured components:
    - On the **Diameter**, and then **Maintenance**, and then **Connections** page, enable configured **Connections**.
    - On the **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups** page, enable **Egress Throttle Groups Rate Limiting**, **Egress Throttle Groups Pending Transaction Limiting**, or both, if used.
    - On the **Diameter**, and then **Maintenance**, and then **Applications** page, enable configured **Applications**.
    - On the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page, enable configured **Peer Discovery**.

- On the **Diameter**, and then **Maintenance**, and then **Traffic Throttle Groups** page, enable **Traffic Throttle Groups**.

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 is used:
   - Path Topology Hiding Configuration Sets
   - S6a/S6d Topology Hiding Configuration Sets
   - MME/SGSN Topology Hiding Configuration Sets
   - S9 PCRF Topology Hiding Configuration Sets
   - S9 AF/pCSCF Topology Hiding Configuration Sets
3. Protected Networks, which use the Trusted Network Lists and Configuration Sets in their configuration.

2.2 Next Generation Network Priority Service (NGN-PS)

Next Generation Network Priority Service (**NGN-PS**) allows National Security/Emergency Preparedness (NS/EP) users to make priority calls/sessions using public networks. When you enable the NGN-PS feature on a DSR Node, ingress messages received from Diameter Peer Nodes are examined to determine if they qualify for priority treatment based upon a set of rules. These rules, established by Standards Development Organizations, have various groups working on what is broadly called Emergency Telecommunications Services (**ETS**).

ETS is intended to be used by qualified and authorized users, for example, emergency service personnel, only during times of emergency situations and network congestion. ETS access:

- Is limited to key personnel and those with leadership
- Is provided end-to-end priority treatment beyond that offered to the general public
- Can include priority call/session set-up, access to additional resources (alternate routing), and exemption from restrictive network traffic management controls.

> **Note**
>
> If NGN-PS is disabled after being enabled, then DSR does not disable NGN-PS, but an alarm alerts the user that the runtime state and administrative state for NGN-PS are not in synch.

NGN-PS support is comprised of two major functions:

1. Identifying messages which require NGN-PS, which is based on subscription information stored in databases that is downloaded to entities that perform priority marking of transactions by way of AVPs.
   - The following messages are candidates for NGN-PS treatment:
     - Cx/Dx LIR & LIA
     - Cx/Dx SAR & SAA
     - Dh/Sh UDR & UDA
     - Gx CCR-I & CCA-I

- Gx RAR & RAA
- Rx AAR & AAA

2. If a message qualifies for priority treatment, it is considered inviolable. An inviolable message cannot be blocked, rejected, or discarded by any ingress or egress control functions due to internal resource congestion or exhaustion.

> **Note**
>
> NGN-PS messages must receive priority treatment both at the Diameter Application signaling layer and IP-layer.

The priority level for violable messages is defined as a number between zero and three, where zero has the lowest and three has the highest violable message priority. NGN-PS messages have a priority level of four.

> **Note**
>
> After a message becomes inviolable, its priority cannot be modified during the lifetime of that message within a DSR node. After an ingress Request message is marked as inviolable, all messages associated with that transaction are also marked as inviolable. Similarly, Answer messages associated with inviolable transactions are made inviolable.

You can enable any of the following diameter interfaces for NGN-PS support:

- Gx, Rx, Cx/Dx and Dh/Sh

NGN-PS messages are identified by the contents of a particular AVP for well-known set of order pairs. Most non-Gx NGN-PS messages can be identified by the presence of an AVP; Gx NGN-PS message identification requires more complex rules based upon AVP content and user-provided configuration data.

Identifying Messages for Priority Treatment

Congestion control procedures use message priorities and congestion levels to determine which messages to shed/divert when congestion exists. Lowest priority messages are assigned a priority of 0, and the highest priority messages are assigned a value of 3. Because inviolable messages must be provided a higher treatment versus violable message, the existing four priority values of 0 through 3 are reserved for violable messages, and message priority of 4 is reserved for inviolable messages.

A message is considered inviolable if:

- The message priority is greater or equal to the **Minimum Inviolable Priority** value. See Diameter System Options Elements. NGN-PS messages received from Diameter Peer Nodes are identified and tagged as inviolable before DSR ingress congestion controls are applied.
- Answer priority is equal to the Maximum of Request Priority and **Minimum Answer Priority** value. See Diameter System Options Elements.

Identifying NGN-PS Messages

NGN-PS specifications identify a well-defined and limited number of messages that are candidates for priority treatment. Inviolable messages are exempt from discard and bypass all

ingress and egress throttling controls. These messages typically represent a small portion of message traffic, and you can configure this function to avoid abuse. For information about limiting the percentage of the maximum engineered DA-MP ingress message rate, see Diameter System Options Elements **NGN-PS Maximum Message Rate Percent**.

When NGN-PS is disabled, a DSR Node does not search for ingress NGN-PS messages. When NGN-PS is enabled, the DSR Node measures the ingress rate of NGN-PS which are marked as inviolable and, if the **NGN-PS Maximum Message Rate Percent** value has not been reached, DSR is allowed to tag NGN-PS messages received from Diameter Peer Nodes.

Identifying Non-Gx NGN-PS Messages

Sh/Dh and Cx/Dx messages are tagged based on the presence of Session-Priority AVP value in Diameter messages. Rx messages are identified as NGN-PS if the MPS-Identifier AVP value in Diameter message is the same as the **Rx MPS-Identifier** value in Diameter System Options Elements.

Identifying Gx NGN-PS Messages

Gx NGN-PS messages are identified by both the content of AVPs, as well as user-configurable data.

The reserved NGN-PS priority levels are network-specific and user-configurable. See **Gx NGN-PS Identifier** in Diameter System Options Elements.

The ARP AVP is not a top-level AVP, which means that it is always embedded within another Grouped AVP. The ARP AVP can be embedded in one of the following top-level grouped AVPs within the Gx message:

- Default-EPS-Bearer-QoS AVP
- Charging-Rule-Install AVP
  Usually, ARP is stored in the Default-EPS-Bearer-QoS AVP. For Gx RAR messages, if a Default-EPS-Bearer-QoS AVP cannot be located, DSR searches for up to three (3) instances of the Charging-Rule-Install AVP looking for a Priority-Level assigned to a NGN-PS user.

Priority treatment of Gx CCR-I and CCA-I messages is only required if Advance Priority is enabled in the your network. If your network supports one of the two mutually exclusive advance priority types, you can select which one to enable. See **Gx Advance Priority Type** in Diameter System Options Elements.

2.3 Diameter Overload Indication Conveyance (DOIC)

DOIC allows Diameter servers to send overload reports requesting that diameter clients reduce the traffic that they are sending to the server. It also allows for Diameter Agents to act as a proxy for either clients by reducing traffic as requested by the servers, or as a proxy for the servers by requesting that traffic be reduced by the clients. DOIC s main purpose is to act as a proxy for the clients on the routing server and reduce traffic based on information from the servers.

DOIC is comprised of two routing capabilities:

- Static ETR Throttling
- Peer Node Reported Congestion

DOIC is comprised of two primary procedures using two Diameter Grouped AVPs:

Capability Announcement Procedure
DSR as a DOIC Reacting Node advertises its supported DOIC capabilities by inserting a OC-Supported-Features Grouped AVP in each forwarded Request message sent to a DOIC Reporting Node. The DOIC Reporting Node sends an OC-Supported-Features AVP in Answer responses indicating which abatement algorithm it wants to support.

Overload Reporting Procedure
The DOIC Reporting Node can request a reduction in traffic addressed to a given application for that Reporting node by inserting one or more Applications associated with a Node/FQDN by inserting a DOIC Overload Report (**OC**-**OLR**) Grouped AVP in Answer responses to a Request containing a OC-Supported-Features AVP.

Static ETR Throttling

Static ETR Throttling allows you to limit the rate of transactions (Request messages only) that are forwarded to a particular Peer Node, which are addressed to a particular Diameter Application ID. For each (Peer Node, Application ID) ordered pair that you want to throttle, define a Traffic Throttle Point (TTP) and assign it a Maximum ETR value. All of the information required for Peer Node/Application ETR throttling is stored in a Traffic Throttle Point (TTP). If a Peer Node supports multiple Application IDs, you must create a separate TTP for each Application for which you want to enable ETR throttling. When you enable the TTP for service, the routing application begins to measure the rate of transactions that are routed to the Peer Node and Application ID (this includes transactions such as priority override and NGN-PS that might be exempt from diversion). This is referred to as the Offered Traffic Rate (**OTR**). Divertable OTRs are the transaction rates offered to a TTP that are candidates for diversion. NGN-PS and priority override transaction are exempt from TTP ETR throttling diversion. When the TTP OTR begins to exceed its user-defined Maximum ETR, the routing application routes the excess transactions alternately using all of the existing routing mechanisms.

> **Note**
>
> A TTP's OTR measurements include all transactions which are associated with an active TTP, which includes both override priority and NGN-PS transactions that might be exempt from diversion.

Traffic diversion is prioritized based upon the Discard Policy assigned to the DA-MPs. Using the Discard Policy and message priority and color OTRs measurements, the TTP Rate Shaper algorithm determines whether a Request message associated with the TTP must be diverted. TTP rate shaping is applied after a Peer Node or Connection is selected from a Route Group (or after a Peer Node is selected by Implicit Routing).

Peer Node Reported Congestion

Routing supports the ability to modify the rate of transactions forwarded to a Peer Node based on the OLRs it receives in Answer responses from the Peer Node. The information received in a OLR is stored in a TTP and applied as modifications to the Target ETR. An OLR is enforced until it expires or is cancelled by the Peer Node, at which time the routing application abates the requested traffic reduction percentage to 0 (at a gradual rate determined by a user-configurable TTP attribute).

Traffic reduction percentages for a Peer Node and Application are used during routing in the following ways:

- You can assign a Maximum Loss Percentage Threshold to a TTP. When this occurs, the routing application does not select a Peer Node or Connection from a Route Group (or

select a Peer Node for Implicit Routing) if the TTP's Current Loss Percentage exceeds this threshold.

- When a traffic reduction request is received for a TTP, the routing application updates the TTP Target ETR, which is used for ETR Throttling. ETR Throttling is applied after a Peer Node or Connection is selected from a Route Group (or a Peer Node is selected by Implicit Routing).
- When a message is diverted using a TTP ETR Throttling, the transaction is marked as Diverted in the transaction **PTR**. When a transaction is marked as Diverted, any subsequent Peer Nodes or Connections are excluded from being a candidate for routing (or re-routing) the diverted transaction if it has a TTP with a non-zero Current Loss Percentage.
- You can allow higher priority transactions to bypass routing constraints via the TTP Override Message Priority Threshold attribute. This attribute is used in the following circumstances:
  - After a transaction has been categorized as Diverted, a Request is allowed to be routed to a congested TTP if its priority is great than or equal to the TTP's Override Message Priority Threshold attribute.
  - After a Peer Node or Connection is selected from a Route Group (or a Peer Node is selected by Implicit Routing), it bypasses a TTP ETR Throttling if all of the following criteria are met:
    * An active TTP exists for the selected Peer Node/Connection and the Application ID addressed by the transaction
    * You have assigned a value to the TTP's Override Message Priority Threshold attribute
    * The Request message's priority is greater or equal to the TTP Override Message Priority Threshold attribute
    * The TTP's OTR is less than or equal to the TTP Maximum ETR

> **Note**
>
> A TTP's OTR measurements include all transactions which are associated with an active TTP, which includes both override priority and NGN-PS transactions might be exempt from diversion.

Traffic reduction requests from Peer Nodes within a Route Group can be aggregated and used for making decisions about whether Route Groups within a Route List are viable candidates for routing a transaction. Traffic reduction loss values for a group of Connection or Peer Nodes are aggregated by the Traffic Throttle Group (TTG) to which you assign a set of TTPs. The local TTG traffic reduction information is also distributed to other Nodes within the network to assist them in making decisions about sending traffic they cannot handle to the affected Node.

When a TTG is created and enabled for service, the routing application begins to maintain an aggregated Current Loss Percentage for the TTG based upon the Maximum ETR assigned to each TTP and the Current Loss Percentage for each TTP. A TTG can be assigned to a Route Group within a Route List along with a maximum loss threshold.

When you enable a TTG, the routing application does not select a Route Group from a Route List when the following criteria are met:

- TTG is assigned to the Route Group within the Route List
- TTG admin state is Enabled

- TTG Current Loss Percentage exceeds the Maximum Loss Percentage Threshold value assigned to the Route Group within the Route List

DOIC Capabilities Announcement (DCA)

The DOIC solution supports the ability for Diameter nodes to determine if other nodes in the path of a request support the DOIC solution. The DOIC Capabilities Announcement (**DCA**) procedure allows a DOIC Reacting Node to indicate which DOIC capabilities it supports to a DOIC Reporting Node which, in turn, responds with which capabilities it wants to use.

The DCA procedure is invoked only when a Request message is being forwarded to a Peer Node for which DOIC has been enabled for the application ID to which the message is addressed. The decision for determining whether an OC-Supported-Features AVP should be appended occurs after the routing application has selected a Connection for forwarding the Request. If the Peer Node associated with the selected Connection has an active TTP associated with the Application ID in the Request message, then:

- Append an OC-Supported-Features AVP to the forwarded Request message containing the list of Abatement Algorithms assigned to the TTP by user configuration.
- Save the TTP in the PTR.

A TTP is considered active, if for a transaction being forwarded to a Connection, the following criteria are met:

- TTP exists for the Peer Node to which the Request is to be forwarded and the Application-Id in the Request header, AND
- TTP's Dynamic Throttling Admin State is set to Enabled
- TTP's Operational Status is NOT set to Inactive

Each time the routing server receives an Answer message that can be associated with a **PTR**, it checks if a TTP has been stored in the PTR. If not, then the routing server ignores any DOIC AVPs in the message. If a TTP is stored in the PTR, then it searches for DOIC AVPs in the Answer response if the following criteria are met:

- TTP is still active (it may have changed between the time the Request was sent and the Answer was received)
- Diameter Node which initiated the Answer (identified by the Origin-Host AVP) is the same node associated with the TTP

If any of these validations fail, then the routing server ignores any DOIC AVPs in the message.

DOIC Overload Reports (OLR)

A DOIC Reporting Node notifies a Reacting Node of a new or change to a previously reported traffic overload condition by piggy-backing one or more OC-OLR AVPs in the Answer response to a DCA procedure. If multiple OC-OLR are found, the routing application only processes the first two OC-OLR found from the top of the Answer message and ignores the balance. It is possible in the DOIC specification to receive two OLR in the same Answer message, the only restriction is that they must have different values for the OC-Report-Type AVP.

OLR AVP Validation and Processing

The OC-OLR is a Grouped AVP. AVPs can be grouped and embedded in the OC-OLR, and they can be validated via the routing application. Optionally, you can define the amount of time (in seconds) that the OLR is enforced. You can also (optionally) define the percentage of the traffic reduction that is requested.

If a validation failure occurs with any AVP within the OC-OLR, the entire OLR is discarded. If the OLR is valid, it is handled based upon the type of request as follows:

- New overload report
- Update to an existing overload report
- Cancellation of an existing overload report

New OLR

The routing application considers an OLR to be a new request when the TTP Validity Duration stored in the local TTP RT-DB is set to 0. The routing application could be in an overload recovery state for the previously received OLR. When this occurs, the recovery procedure is abandoned by stopping the DOIC Overload Recover timer. The new OLR is then processed.

Cancel an Existing OLR

A Peer Node can cancel an active overload state by setting the OC-Reduction-Percentage to 0 or by setting the OC-Validity-Duration AVP to 0 seconds. Cancellation only applies if the routing application is processing an OLR (TTP's Validity Duration greater than 0). A cancellation is ignored if overload recovery is in progress (Operational Reason is Peer Overload Recovery). If a cancellation is received while the TTP is in Peer Overload, the routing application processes the request.

Modify an Existing OLR

An upstream Peer Node can update an in-progress overload condition. An update request must contain a Sequence Number larger than the previously one sent. The routing application treats an OLR as an update to an existing overload condition if the validation criteria are met.

DOIC Information Sharing within a Node

Traffic reduction requests from an upstream Peer Node can be sent to any DA-MP. This information must be shared with all DA-MPs within the Node so that it can be applied when routing transactions to the congested entity. When a routing application instance on a DA-MP receives a DOIC OLR that modifies a TTP, the updated TTP information is forwarded to all of its peer routing application instances within the Node via a DOIC-OLR stack event.

Overload Recovery and Abatement

When an OLR received from a Peer Node expires or is cancelled, the routing application must restore the traffic rate for the TTP to its maximum capacity. Rather than abruptly reducing the TTP's Current Loss Percent to 0, the routing application reduces the Current Loss Percent based upon a user-defined loss restoral rate defined by the TTP attribute Abatement Recovery Rate.

DOIC and NGN-PS Interaction

Next Generation Network Priority Service (NGN-PS) allows National Security/Emergency Preparedness (**NS/EP**) users (service users) to make priority calls/sessions using the public networks. When the NGN-PS feature is enabled on a DSR Node, DSR examines the content of ingress messages received from Diameter Peer Nodes to determine if they qualify for priority treatment based upon a set of rules. See Diameter System Options Elements. If priority treatment is required, the message is assigned a priority of 4 and becomes inviolable, which means that it becomes exempt from discard and bypasses all DSR ingress and egress congestion throttling controls. The following exemptions are provided to inviolable message from DOIC throttling constraints:

- Inviolable Request messages from a Route Group-TTG's Maximum Loss Percent Threshold constraint are exempt.
- Inviolable Request messages from a Peer Node-TTP's Maximum Loss Percent Threshold constraint are exempt.
- Any TTP ETR message throttling constraints for inviolable Request messages are bypassed.

> **Note**
>
> NGN-PS transactions are never diverted by ETR throttling; therefore, any existing diameter routing layer routing rules associated with DOIC-diverted transactions do not apply.

2.4 Diameter Capacity Summary

The **Diameter**, and then **Configuration**, and then **Capacity Summary** page viewed from the SOAM displays information about maximum allowed and currently configured Diameter Configuration components.

The following information displays 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 component that are currently configured.

% Utilization
The percentage of the maximum number of entries for that component that are currently configured.

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

2.4.1 Diameter Capacity Constraints

The following table shows the maximum values per NE and per configuration component.

Table 2-1 Maximum Values per NE and per Configuration Component

Constraint Name	Description	Value	Related Notes
AVP Removal List	Maximum AVP Removal List managed object in a NE.	128	MaxAVPRemovalListPerNE
AVP Removal List entries	Maximum number of AVP Removal List entries in a AVP Removal List managed object.	10	MaxAVPRemovalEntryPerList

Table 2-1 (Cont.) Maximum Values per NE and per Configuration Component

Constraint Name	Description		Value	Related Notes
Application IDs	Maximum number configured per network element.		1000	MaxConfiguredAppId
Application IDs per set	Maximum number of AppIds per set.		20	MaxConfiguredAppIdperSet
Application Routing Rules	Maximum number configured per network element.		50000	MaxARTRulesPerNE
Application Routing Table Rules	Maximum number configured per network element.		50000	MaxARTRulesPerNE
Application Routing Table rules with Contains operator	Maximum number of ART rules with Contains operator.		100	MaxArtRulesWithContainsPerArt
Application Routing Table rules with Contains operator	Maximum number of characters for a parameter's value with Contains operator in condition of ART rule.		50	MaxCharArtCondWithContains
Application Routing Table with Contains operator	Maximum number of conditions in an ART rule with Contains operator.		1	MaxCondWithContainsPerArr
Application Routing Tables	Maximum number configured per network element.		1500	MaxArtTablesPerNe
APN Radius Routing Tables	Maximum number of APNs in Radius Routing Table.	10000		MaxApnRadiusRoutingRules
CCNDC Mapping Entries	Maximum number of CCNDC Mapping Entries.		2500	MaxCcNdcMappingPerNe
CEX Configuration Sets	Maximum number that can be configured.		2000	MaxConfiguredCEXSets
Capacity Configuration Sets	Maximum number that can be configured.		1000	MaxCapacityCfgSets
Command Codes	Maximum number that can be configured.		1000	MaxConfiguredCmdCode
Connection Alarm Group	Maximum number of configured Connection Alarm Groups per NE.		100	MaxConnectionAlarmGroupsPerNe
Connection Alarm Group Connections	Maximum number of Connections in a Connection Alarm Group.		200	MaxConnsPerConnectionAlarmGroup
Connection Configuration Sets	Maximum number configured per network element.		2000	MaxConnConfigsPerNe
Connections	Maximum number configured per network element.		32000	MaxConnsPerNe

Table 2-1 (Cont.) Maximum Values per NE and per Configuration Component

Constraint Name	Description	Value	Related Notes
Connections per Peer Node	Maximum number of connections configured per peer node.	64	MaxConnsPerPeerNode
Connections per Route Group	Maximum number per route group.	512	MaxConnsPerRouteGroup
Connections with Message Throttling Configuration Sets	Maximum connections that can have message throttling configuration sets assigned to them.	500	MaxMsgThrottlingConnections
DA-MPs	Maximum number configured per network element.	16	
DNS Sets	Maximum number defined per SO.	64	MaxDnsSetsPerSO
Dashboard Network	Maximum number of managed objects that can be defined.	1	MaxDashboardNetworks
Dashboard Network Element	Maximum number of managed objects that can be defined.	32	MaxDashboardNetworkElements
Diagnose Connections	Maximum number of diagnosed connections in test mode.	2	MaxDiagnoseConnections
Diagnose PDUs	Maximum number of PDUs per test connection for a single diagnostic cycle.	1	MaxDiagnosePdu
Diameter Identity GTA	Maximum number of Diameter Identity GTA records per network.	5000	MaxDiamIds
Diameter Realm	Maximum number of records per network.	1000	MaxDiamRealms
Discovery Attributes	Maximum number defined per network element.	100	
Dynamic Peer Discovery Realms	Maximum number of Dynamic Peer Discovery Realms defined at SO.	100	MaxRealmsPerSO
ETG Pending Transaction Limiting Configuration Set	Maximum number of ETG Pending Transaction Limiting Configuration Set defined at SO.	128	MaxEtgsPendTransPerNe
ETG Rate Limiting Configuration Set	Maximum number of ETG Rate Limiting Configuration Set defined at SO.	128	MaxEtgsRateCfgSetPerNe
ETL Pending Transaction Limiting Configuration Set	Maximum number of ETL Pending Transaction Limiting Configuration Set defined at NO.	128	MaxEtlsPendTransPerNe

Table 2-1 (Cont.) Maximum Values per NE and per Configuration Component

Constraint Name	Description	Value	Related Notes
ETL Rate Limiting Configuration Set	Maximum number of ETL Rate Limiting Configuration Set defined at NO.	128	MaxEtlsRateCfgSetPerNe
Egress Message Throttling Configuration Sets	User-configurable Egress Message Throttling Configuration Sets per NE.	50	NA
Egress Throttle Groups	Maximum number of Egress Throttle Groups.	512	MaxEtgsPerNe
Egress Throttle Lists	Maximum number of Egress Throttle Lists	512	MaxEtlsPerNe
GTA Range to PC	Maximum number of GTA Range to PC records per NE.	5000	MaxGtaRangetoPCPerNetworkType
HSS Real Hostnames per Configuration Sets	Maximum number of HSS Real Hostnames per HSS Topology Hiding Configuration Sets that can be configured.	300	MaxHssRealHostnamesPerCfgSet
HSS Real Hostnames per NW	Maximum number of HSS Real Hostnames in the DSR network.	50000	MaxHssRealHostnamesPerNw
Host Network Suffixes	Maximum number host name suffixes per path topology hiding configuration set.	10	MaxHostNameSuffixes
IP Addresses per Local Node	Maximum number per local node.	128	MaxIpsPerLocalNode
IP addresses per Peer Node	IP addresses per peer node.	128	MaxIpsperpeernode
IPs per NAS node	Maximum IPs allowed per NAS Node.	4	MaxIpsPerNASNode
Ingress Status-Server Configuration Sets	Maximum number of Ingress Status-Server Configuration Sets allowed for a DSR node.	100	MaxIngressStatusServerCfgSet
List	Maximum managed objects in a DSR system.	128	NA
Local Nodes per Connection	Maximum number configured per connection.	48	NA
Local Nodes per NE	Maximum number configured per network element.	48	MaxLocalNodesPerNe
MCC Ranges	Maximum number of configured Reserved MCC Ranges.	10	MaxConfiguredReservedMCCRanges
MME Real Hostnames	Maximum number of in the DSR network.	50000	MaxMMERealHostNamesPerNw

Table 2-1 (Cont.) Maximum Values per NE and per Configuration Component

Constraint Name	Description	Value	Related Notes
MME Real Hostnames per MME Topology Hiding Configuration Sets	Maximum number of MME Real Hostnames per MME Topology Hiding Configuration Sets that can be configured.	300	MaxMMERealHostNames
MME/SGSN Topology Hiding Configuration Sets	Maximum number of MME/SGSN Topology Hiding Configuration Sets that can be configured.	500	MaxMMETHCfgSet
Maintenance Screen Refresh Rate	Time interval in seconds after which data is refreshed on the diameter maintenance screens.	10	MaintenanceScreenRefreshRate
MccMnc Mappings	Maximum MccMnc Mappings per NE.	2500	MaxMccMncMappingPerNe
Members in a Egress Throttle Group	Maximum number of members in a Egress Throttle Group.	128	MaxMembersPerEtg
Message Authenticator Configuration Sets	Maximum number of Message Authenticator Configuration Sets allowed for a DSR node.	100	MaxMessageAuthCfgSet
Message Priority Configuration Set Rules	Maximum number of configured rules per message priority configuration set.	50	MaxRulesPerMsgPriorityCfgSet
Message Priority Configuration Sets	Maximum number of configured Message Priority Configuration Sets.	20	MaxMsgPriorityCfgSet
Message Throttling Configuration Sets	Maximum number of configured Message Throttling Configuration Sets.	50	MaxMsgThrottlingCfgSet
Metric Threshold Configuration Sets	Maximum number of Metric Threshold Configuration Sets that can be user-defined.	32	MaxDashboardMTCfgSets
Mobile Country Codes	Maximum (Mcc) Mobile Country Codes per NE.	2500	MaxMccPerNe
NAS Nodes	Maximum number of NAS Nodes allowed for a DSR node.	16000	MaxNASNodes
Path Topology Hiding Configuration Sets	Maximum number configured.	500	MaxPathTHCfgSet
Peer Node Alarm Group	Maximum number of configured Peer Node Alarm Groups per NE.	100	MaxPeerNodeAlarmGroupsPerNe

Table 2-1 (Cont.) Maximum Values per NE and per Configuration Component

Constraint Name	Description	Value	Related Notes
Peer Node Alarm Group Peer Nodes	Maximum number of Peer Nodes in a Peer Node Alarm Group.	200	MaxPeersPerPeerNodeAlarmGroup
Peer Node Groups	Maximum number of Peer Node Groups that can be configured.	2500	MaxPeerNodeGroups
Peer Nodes per NE	Maximum number configured per network element.	32000	MaxPeerNodesPerNe
Peer Nodes per Route Group	Maximum Peer nodes per route group.	512	MaxPeersPerRouteGroup
Peer Route Tables and Application IDs Associations	Maximum number of Associations between Application IDs and Peer Route Tables.	20	MaxPrtTableDiameterAppAssocs
Peer Routing Rules	Maximum number configured per network element.	50000	MaxPrtRulesPerNe
Peer Routing Table rule with Contains operator	Maximum number of characters for a parameter's value with Contains operator in condition of PRT rule.	50	MaxCharPrtCondWithContains
Peer Routing Table rules with Contains operator	Maximum number of PRT rules with Contains operator.	100	MaxPrtRulesWithContainsPerPrt
Peer Routing Table with a condition in rule	Maximum number of conditions in a PRT rules with Contains operator.	1	MaxCondWithContainsPerPrr
Peer Routing Tables	Maximum number of configured Peer Route Table.	500	MaxPrtTablesPerNe
Pending Answer Timers	Maximum number configured per network element.	64	MaxPendingAnswerTimers
Protected Network Configuration Sets	Maximum number of Protected Network that can be configured.	500	MaxProtectedNetwork
Reroute On Answer	Maximum number of order pair combinations of Application ID and answer result code value that can cause a request re-routing.	1000	MaxRerouteOnAnsOrderPair
Rf Message Copy	Maximum number of APNs that need message copy to the Diameter MPN Proxy Peer.	10000	MaxApnRfMsgCopy
Route Groups	Maximum number configured per network element.	6000	MaxRouteGroupsPerNe

Table 2-1 (Cont.) Maximum Values per NE and per Configuration Component

Constraint Name	Description	Value	Related Notes
Route Groups per Route List	Maximum Route groups per route list.	5	MaxRouteGroupsPerRouteList
Route List/Route Group/ Shared TTG Associations	Maximum number across the entire DSR network.	5000	MaxSharedTTGAssocPerNOAM
Route Lists	Maximum number configured per network element.	2000	MaxRouteListsPerNe
Routing Option Sets	Maximum number of configured Routing Option Sets.	50	MaxRoutingOptionSets
S6a/S6d HSS Topology Hiding Configuration Sets	Maximum number configured.	500	MaxHSSTHCfgSet
S9 AF/pCSCF Host Names	Maximum number of S9 AF/pCSCF Real Hostnames in the DSR network.	200000	MaxS9AfPcscfRealHostsPerNw
S9 AF/pCSCF Host Names per set	Maximum number of S9 AF/pCSCF Real Hostnames per S9 AF/pCSCF Topology Hiding Configuration Sets that can be configured.	1200	MaxS9AfPcscfRealHostsPerCfgSet
S9 AF/pCSCF Topology Hiding Configuration Sets	Maximum number of S9 AF/pCSCF Topology Hiding Configuration Sets that can be configured.	500	MaxS9AfPcscfThCfgSet
S9 PCRF Host Names per set	Maximum number of S9 PCRF Real Hostnames per S9 PCRF Topology Hiding Configuration Sets that can be configured.	600	MaxS9PcrfRealHostnamesPerCfgSet
S9 PCRF Real Host Names	Maximum number of S9 PCRF Real Hostnames in the DSR network.	100000	MaxS9PcrfRealHostnamesPerNw
S9 PCRF Topology Hiding Configuration Sets	Maximum number that can be configured.	500	MaxS9PcrfThCfgSet
Server Ports	Maximum Server Ports Per Peer Node.	10	RADIUS UDP Server Ports
Server Ports per Local Node	Maximum Server Ports Per Local Node.	10	MaxServerPortsPerLocalNode
Server Ports per Peer Node	Maximum Server Ports Per Peer Node.	10	MaxServerPortsPerPeerNode
Shared Secret Sets	Maximum number allowed per network element.	16000	MaxSharedSecretCfgSet

Table 2-1 (Cont.) Maximum Values per NE and per Configuration Component

Constraint Name	Description	Value	Related Notes
Shared Traffic Throttle Group	Maximum number that can be marked as shared under the control of a single NOAM.	3000	MaxSharedTTGPerDSR
Supported Vendor ID(s)	Maximum number of supported vendor IDs per set.	20	MaxSupportedVendorIdperSet
Target Set Address	Maximum number of TSAs per local node.	32	MaxTsasPerLocalNode
Test Connections	Maximum number of test connections	2	MaxTestConnections
Traces	Maximum number of configured Traces.	100	
Traffic Measurements	Maximum supported Route Groups for measurement capturing.	250	
Traffic Throttle Group	Maximum number configured per network element.	1500	MaxTraficThrottleGroup
Traffic Throttle Group	Maximum TTG that can be associated with Route Group within Route List.	10	MaxTTGperRGperRL
Traffic Throttle Point	Maximum number allowed per network element.	1500	MaxTraficThrottlePoint
Traffic Throttle Point Configuration Sets	Maximum number of TTP Configuration Sets configured in a network element.	500	MaxTrafficThrottleCfgSet
Traffic Throttle Point per Traffic Throttle Group	Maximum number in a Traffic Throttle Group.	20	MaxTraficThrottlePointPerGroup
Transaction Configuration Rules per set	Maximum number of configured Transaction Configuration Rules per Transaction Configuration Set.	1000	MaxTransactionCfgRulePerSet
Transaction Configuration Set	Maximum number of configured Transaction Configuration Set defined at SO.	100	MaxTransactionCfgSetPerNe
Transaction Configuration Set Rules	Maximum number of configured Transaction Configuration Set Rules defined at SO.	1000	MaxTransactionCfgRulePerNe
Transport Layer Security Certificates	Maximum number of TLS certificates allowed for a DSR node and across DSR network.	1000	MaxTlsCertificatesAllowed
Trusted Network Lists	Maximum number of Trusted Network Lists that can be configured.	500	MaxTrustedNetworkList

Table 2-1 (Cont.) Maximum Values per NE and per Configuration Component

Constraint Name	Description		Value	Related Notes
Trusted Network Realm per Home Network Realm	Maximum number of Trusted Network Realm per Home Network Realm that can be configured.		100	MaxTrustedNetworkRealm
VRFID Radius Routing Tables	Maximum number of VRFIDs in Radius Routing Table.	10000		MaxVrfidRadiusRoutingRules
Peer Routing Rules per Table	Maximum number of Peer Routing Rules that can be configured per PRT.	5000		MaxPrtRulesPerPrtTable

2.5 Connection Capacity Dashboard Functions

The functions of the Connection Capacity Validation feature are described in Validating Diameter Connection Capacity. On the **Diameter**, and then **Configuration**, and then **Connection Capacity Dashboard** GUI page, the current Connection configuration capacity information for configured active DAMPs displays.

You can perform these tasks on an active System OAM (**SOAM**).

Each row on the page contains the information for one configured active DAMP.

The **Diameter**, and then **Configuration**, and then **Connection Capacity Dashboard** page is view-only and has two tabs.

The **Connections Table** tab contains information about the currently configured Connections for each DAMP in the NE. Fixed Connections and Floating IPFE Connections displays with Floating IPFE Connections grouped by Target Set.

The **Connection Reserved Ingress MPS Table** tab contains the currently configured Reserved Ingress MPS for each DAMP in the NE. The contribution of both Fixed Connections and Floating IPFE Connections displays with Floating IPFE Connections grouped by Target Set.

> **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 following information displays for each configured active DA-MP when the **Connections Table** tab is selected:

MP Server Hostname
Hostname of the DAMP server.

Current Connection Usage (%)
The percentage of the total Connection capacity currently used, which is the sum of Fixed Connections and Floating IPFE Connections allocated to the DAMP, divided by the total **Connection Capacity** value.
It is theoretically possible for this usage value to exceed 100%; diameter does not prevent over-configuration in certain scenarios (typically involving overlapping Target Sets, or a non-overlapping Target Set whose DAMPs have significantly different numbers of Fixed Connections assigned). For a given DAMP, if the number of Connections allocated to that DAMP exceeds the DAMP's Maximum Connections count capacity (from the assigned MP Profile), the **Current Connection Usage (%)** value exceeds 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 Connections and Floating IPFE Connections, divided by the **Maximum Reserved Ingress MPS** value.
It is theoretically possible for this usage value to exceed 100%; diameter does not prevent over-configuration in certain scenarios (typically involving overlapping Target Sets, or a non-overlapping Target Set whose DAMPs have significantly different numbers of Fixed Connections assigned).

Connection Capacity
The DAMP's total Connection capacity.
The maximum connections value assigned to the DAMP in the MP Profile.

 # Fixed Connections
The number of Fixed Connections currently configured for the DAMP.
For a given DAMP, the value displayed in the **# Fixed Connections** field should never exceed the **Connection Capacity**.
If a DAMP has one or more configured Fixed Connections, then the value appears as a hyperlink. The hyperlink opens the **Diameter**, and then **Configuration**, and then **Connections [Filtered]** page, filtered to show only the Fixed Connections assigned to the DAMP.

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

TSn: # Floating IPFE Connections
A configured Target Set, where *n* is the Target Set number. The numbering of the Target Sets is ascending, but might not be sequential.
The value displayed for a given DAMP and Target Set is the evenly-distributed allocation of Floating IPFE Connections to each DAMP in the Target Set. If the evenly-distributed allocation value is zero, then the value zero displays in the field.
The evenly-distributed allocation of Floating IPFE Connections is zero if there are more DAMPs in the Target Set than Floating IPFE Connections configured for the Target Set. In this case, to make it clear DAMP is part of the Target Set, the value zero displays (instead of a blank field).
If a DAMP has no IPFE allocation for a defined Target set, the corresponding field is blank.

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

MP Server Hostname
Hostname of the DAMP server.

Current Connection Usage (%)
The percentage of the total Connection capacity currently used, which is the sum of Fixed Connections and Floating IPFE Connections allocated to the DAMP, divided by the total **Connection Capacity** value shown in the fourth column on the **Connections** tab.
It is theoretically possible for this usage value to exceed 100%; diameter does not prevent over-configuration in certain scenarios (typically involving overlapping Target Sets, or a non-overlapping Target Set whose DAMPs have significantly different numbers of Fixed Connections assigned). For a given DAMP, if the number of Connections allocated to that DAMP exceeds the DA-MP's Maximum Connections count capacity (from the assigned MP Profile), the **Current Connection Usage (%)** value exceeds 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 DAMP's Fixed Connections and Floating IPFE Connections, divided by the **Maximum Reserved Ingress MPS** value shown in the fourth column of the **Connection Reserved Ingress MPS Table** tab.
It is theoretically possible for this usage value to exceed 100%; diameter does not prevent over-configuration in certain scenarios (typically involving overlapping Target Sets, or a non-overlapping Target Set whose DAMPs have significantly different numbers of Fixed Connections assigned).
If the total Connection Reserved Ingress MPS for Connections allocated to a given DAMP exceeds the DAMP's scaled Engineered Ingress MPS, the **Current Reserved Ingress MPS Usage (%)** exceeds 100%

Maximum Reserved Ingress MPS

The DAMP's **Engineered Ingress MPS** value, located on the **Diameter**, and then **Diameter Common**, and then **MP Profile** assigned to the DAMP, scaled by the **Connection Reserved Ingress MPS Scaling** value located on the **Diameter**, and then **Configuration**, and then **System Options** page.

Total Fixed Connection Reserved Ingress MPS
The sum of the **Maximum Reserved Ingress MPS** values for all Fixed Connections configured to a DAMP.
For a given DAMP, 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 exception – a system already configured with Fixed Connections having some non-zero **Total Fixed Connection Reserved Ingress MPS** value. If the Connection Reserved Ingress MPS Scaling is decreased, thus decreasing the scaled Engineered Ingress MPS on every DAMP in the system, it is possible the new lowered **Maximum Reserved Ingress MPS** is less than the already-configured **Total Fixed Connection Reserved Ingress MPS**.

If a DAMP has no Fixed Connections assigned to it, then the corresponding field shows a value of zero.

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

TSn: # Floating IPFE Connections Reserved Ingress MPS
A configured Target Set, where *n* is the Target Set number. The numbering of the Target Sets is ascending, but might not be sequential.

> **Note**
>
> The IPFE GUI does not require Target Sets to be configured sequentially. For example, you can define Target Sets 4, 11, 12, and 32. The Dashboard page always shows only the configured Target Sets, from the smallest configured number to the largest configured number.

The value displayed for a given DAMP and Target Set field is the evenly-distributed allocation of Floating IPFE Connections' Reserved Ingress MPS to each DAMP in the Target Set. If the evenly-distributed allocation value is zero, then the value zero displays in the field.
The evenly-distributed allocation of Floating IPFE Connections is zero if all of the Floating IPFE Connections configured for the Target Set have Reserved Ingress MPS values of zero. In this case, to make it clear DAMP is part of the Target Set, the value zero displays (instead of a blank field).
If a DAMP has no Floating IPFE allocation for a defined Target set, the corresponding field is blank.
If a DA-MP has one or more Floating IPFE Connections allocated to it for a given Target Set, the value is displayed as a hyperlink. When clicked, the **Diameter**, and then **Configuration**, and then **Connections [Filtered]** page opens, filtered to show only those Floating IPFE Connections assigned to the Target Set. Because Floating IPFE Connections are not configured to a particular DAMP, this filtered display cannot show a DAMP allocation; it instead shows all Floating IPFE Connections in the Target Set.

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

DA-MP and Target Set Associations

The DAMPs 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 DAMP and Target Set.

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

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

- If a given DAMP shows no number for any Target Set, that DAMP is not included in any Target Set; therefore, it cannot host Floating IPFE Connections.

- If a given DAMP shows a number for just one Target Set, that DAMP is not overlapped in more than one Target Set.
- If a given DAMP shows a number for more than one Target Set, then all Target Sets that include the DAMP overlap.

2.5.1 Validating Diameter Connection Capacity

The Connection Capacity Validation function validates and limits the configuration of Diameter connections to better ensure 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 Reserved Ingress MPS occurs in response to changes to the configuration of Connections and Capacity Configuration Sets. Such changes reduce the available connection capacity 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. See Connections.

The following definitions apply in this document:

Target Set
A collection of DA-MP servers, any one of which the IPFE server can select to establish a Floating IPFE Diameter connection.

Non-overlapping Target Set
A Target Set where DA-MPs do not appear in any other configured Target Set.

Overlapping Target Sets
If any single DA-MP appears in more than one Target Set, then 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 Floating 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 application does not prevent configuration changes when overlapping Target Sets are involved.
- Diameter and Connection Capacity Validation prevent or do not prevent configuration changes under the following conditions:
  - Diameter does 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 diameter routing 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, diameter routing prevents 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 Floating IPFE Connections, only Fixed Connections - diameter routing prevents connection configuration changes that could cause the individual DA-MP hosting the subject Fixed Connection to exceed its capacity.

- The **TS#: Floating IPFE Connection Reserved Ingress MPS** value (percent) is applied to a DA-MPs total Engineered Ingress MPS. The **TS#: Floating IPFE Connection Reserved Ingress MPS** 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 Floating 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 Floating 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 no effect on the actual distribution of Floating 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 Floating IPFE Connections. But if another DA-MP in the non-overlapping Target Set has fewer Fixed Connections, it has more room for Floating IPFE Connections. The capacity on the DA-MP with fewer Fixed Connections can be used for Floating IPFE Connections.

TS#: Floating IPFE Connection Reserved Ingress MPS
Because only the Client Diameter Connections are configured with non-zero Reserved Ingress MPS, **TS#: Floating IPFE Connection Reserved Ingress MPS** values (Scaling Factor) greater than 50% introduce the potential for a DA-MP to accept sufficient Floating 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 Floating IPFE Connections have non-zero **Reserved Ingress MPS** defined, and non-IPFE Connections have a zero **Reserved Ingress MPS**, the configuration restriction of the Scaling Factor = 50% enables 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 is limited by scaled Engineered Reserved Ingress MPS of the DA-MP.

Therefore, the Scaling Factor does in fact limit the total Connection Reserved Ingress MPS on a DA-MP. The intended deployment is that all Fixed Connections have a **Reserved Ingress MPS** value of zero so the Scaling Factor value of 50% affects 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 Floating 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 (for example, 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 Connection Reserved Ingress MPS is possible and explicitly allowed when overlapping Target Sets are present.
- Running a release earlier than version 5.0, which is already over-configured in some way, remains over-configured after upgrade to version 5.0 or later.
- There are no alarms or other active notifications generated by the system to indicate Connection Count or Connection Reserved Ingress MPS over-configurations.
- View the Connection Capacity Dashboard page to check 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.
- Systems having a Scaling Factor of 50% before upgrade retains the 50% value after upgrade. In older systems, this Scaling Factor was not used in configuration validation. It is possible for an older system to be over-configured immediately after upgrade, with no change in configuration.
  Look at the **Diameter**, and then **Configuration**, and then **Connection Capacity Dashboard** GUI page on tab **Connection Reserved Ingress MPS Table** to see if the **Maximum Reserved Ingress MPS** (for the capacity), **Total Fixed Connection Reserved Ingress MPS**, **Total Fixed Connection Reserved Ingress MPS**, and **Floating Connections Reserved Ingress MPS** columns show any over-configuration.

2.6 Using Application IDs to Identify Diameter Applications

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

You can perform these tasks on an Active System OAM (**SOAM**).

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

- Select Protocol Assignments

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

The Application ID fields are described in Diameter Application IDs Elements.

On the **Diameter**, and then **Configuration**, and then **Application IDs** page, you can:

- Filter the list of Application IDs to display only the desired Application IDs.
- Click **Insert**.

  On the **Diameter**, and then **Configuration**, and then **Application IDs [Insert]** page, 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, then the **Diameter**, and then **Configuration**, and then **Application IDs [Insert]** page does not display and an error message appears.
- Select an **Application ID** and click **Edit**.

  On the **Diameter**, and then **Configuration**, and then **Application IDs [Edit]** page, you can edit the selected Application ID. See Editing an Application ID.
- Select an **Application ID** and click **Delete** to delete the selected Application ID. See Deleting an Application ID.

2.6.1 Diameter Application IDs Elements

Table 2-2 describes the elements on the Application IDs View, Insert, and Edit pages.

> **Note**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 2-2 Application IDs Elements

Element	Description	Data Input Notes
Application ID Value	Identifies a specific Diameter Application ID value that is placed in the Application ID AVP. The Application ID field is required, must be unique, and cannot be edited after it is created.	Format: • List of available Application IDs Default: -Select- • Input text box; numeric, maximum 10 digits Range: – 1 - 16777215 for Standard Application IDs – 16777216 - 4294967294 for Vendor-specific Application IDs – 4294967295 for Relay

Table 2-2 (Cont.) Application IDs Elements

Element	Description	Data Input Notes
Name	Application ID Name value	Format: Input text box; case-sensitive; alphanumeric and underscore; cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters

2.6.2 Adding an Application ID

Use this task to configure a new Application ID.

The fields are described in Diameter Application IDs Elements.

1. Click **Diameter**, and then **Configuration**, and then **Application IDs**.
2. Click **Insert**.

   If the maximum number of Application IDs (1000) is already configured in the system, then the **Diameter**, and then **Configuration**, and then **Application IDs [Insert]** page does not display and an error message appears.
3. Enter a unique **Name** for the Diameter Application.
4. Select an **Application ID Value** from the list or enter a unique value in the text box to identify a specific Diameter Application.

   Application ID is required.
5. Click **OK**, **Apply**, or **Cancel**.

2.6.3 Editing an Application ID

Use this procedure to change the Name for a selected Application ID. (The **Application ID Value** field cannot be changed.)

The fields are described in Diameter Application IDs Elements.

When the **Diameter**, and then **Configuration**, and then **Application IDs [Edit]** page displays the fields are populated with the currently configured values.

1. Click **Diameter**, and then **Configuration**, and then **Application IDs**.
2. Select the **Application ID** row to be edited.
3. Click **Edit**.
4. Change the **Name** for the selected **Application ID**.
5. Click **OK**, **Apply**, or **Cancel**.

2.6.4 Deleting an Application ID

Use the following procedure to delete an Application ID.

> **Note**
>
> You cannot delete an Application ID if it is associated with any of the following Configuration components:
>
> - **CEX Configuration Sets**
> - **Transaction Configuration Sets**
> - **Peer Route Table Rules**
> - **Application Route Table Rules**
> - **Message Priority Configuration Sets**
> - Applications such as RBAR and FABR

1. Click **Diameter**, and then **Configuration**, and then **Application IDs**.
2. Select the **Application ID** to be deleted.
3. Click **Delete**.
4. Click **OK** or **Cancel**.

2.7 Diameter CEX Parameters

Configure **CEX** Capabilities Exchange) Parameters to associate an application type and vendor ID with a Diameter Application. If specified, the vendor ID is placed in the Vendor ID AVP.

You can perform these tasks on an Active System OAM (**SOAM**).

On the **Diameter**, and then **Configuration**, and then **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.
- See Adding CEX Parameters to assign a new set of CEX Parameters to an Application ID.
- See Editing CEX Parameters to edit the CEX Parameters for the selected Application ID.
- See Deleting CEX Parameters to delete the CEX Parameters for the selected Application ID.

2.7.1 Diameter CEX Parameters Elements

Table 2-3 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 2-3 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. • 0 - 16777215 for Standard Application IDs • 16777216 - 4294967294 for Vendor-specific Application IDs • 4294967295 for Relay	Format: list Range: Select from the configured Application IDs
Application ID Type	Type of Application ID.	Format: Options Range: Authentication, Accounting
Vendor-Specific Application ID	If checked, the Vendor ID and the Application ID are grouped in a Vendor-specific Application ID AVP.	Format: checkbox 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 checkbox must be checked before a value can be entered in this field.	Format: numeric Range: 1 - 4294967295

2.7.2 Adding CEX Parameters

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

The fields are described in Diameter CEX Parameters Elements.

1. Click **Diameter**, and then **Configuration**, and then **CEX Parameters**.
2. Click **Insert**.
3. Select an **Application ID** from the list.
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**, **Apply**, or **Cancel**.

2.7.3 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 Diameter CEX Parameters Elements.

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

> **Note**
>
> If a CEX parameter is being used by a connection (Enabled/disabled) it cannot be edited.

1. Click **Diameter**, and then **Configuration**, and then **CEX Parameters**.
2. Select the **Application ID** row to be changed.
3. Click **Edit**.
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**, **Apply**, or **Cancel**.

2.7.4 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 or being used in a connection.

1. Click **Diameter**, and then **Configuration**, and then **CEX Parameters**.
2. Select the **Application ID** for which you want to delete CEX Parameters.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.8 Diameter Command Codes

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.

You can perform these tasks on an Active System OAM (**SOAM**).

An (Extended) Command Code is a command code extension that includes the following attributes:

- Command Code (parent Command Code)
- AVP Code
- AVP Data value

This broadens the definition of Diameter Command Codes to include an additional application-specific single Diameter or 3GPP AVP content per Command Code. A format example might be 272.416.1 = CCR/CCA-I.

> **Note**
>
> All (E)CCs are predefined and preloaded into the configuration.

(E)CCs are synonymous with CCs, as a GUI element and as a reference for other managed objects. After (E)CCs are configured on the Command Codes page, they are listed as choices on the Inserting Rule for Application Route Table, Inserting Rule for Peer Route Table, Transaction Configuration Sets [Insert], and Message Priority Configuration Sets [Insert] pages.

> **Note**
>
> A parent CC or Base CC is a Command Code without AVP code and Data extensions. All (E)CCs are extensions of any of the configured base command codes.

On the **Diameter**, and then **Configuration**, and then **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. When comparing two cell values in the Command Code column for sorting, the Command Code part of the cell values are compared followed by AVP Code part of the cell values followed by AVP Value part of the cell values. If the AVP Code and AVP Value part is missing for a cell value, it is considered as zero for the comparison.
- Click **Insert**.

  On the **Diameter**, and then **Configuration**, and then **Command Codes [Insert]** page, 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, then the **Diameter**, and then **Configuration**, and then **Command Codes [Insert]** page does not appear and an error message displays.
- Select a **Command Code** in the list and click **Edit**.

  On the **Diameter**, and then **Configuration**, and then **Command Codes [Edit]** page, you can edit the selected Command Code. See Editing a Command Code.
- Select an **Command Code** in the list and click **Delete** to remove the selected Command Code. See Deleting a Command Code.

  > **Note**
  >
  > **Delete** is disabled for (E)CCs.

2.8.1 Diameter Command Codes Elements

Table 2-4 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 2-4 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 or extended command code associated with the message. **Note**: Only loaded, predefined ECC values display.	Format: List or numeric Range: Select from predefined Command Codes or enter a numeric value: 0 - 16777215 Default: none

2.8.2 Adding a Command Code

Use this task to configure a new Command Code.

The fields are described in Diameter Command Codes Elements.

1. Click **Diameter**, and then **Configuration**, and then **Command Codes**.
2. Click **Insert**.

   If the maximum number of Command Codes (1000) has already been configured in the system, then the **Diameter**, and then **Configuration**, and then **Command Codes [Insert]** page does not open and an error message appears.
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**, **Apply**, or **Cancel**.

2.8.3 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 Diameter Command Codes Elements.

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

1. Click **Diameter**, and then **Configuration**, and then **Command Codes**.
2. Select the Command Code row to be changed.
3. Click **Edit**.
4. Change the **Command Code Name** for the selected Command Code.

The **Name** must be unique.

5. Click **OK**, **Apply**, or **Cancel**.

2.8.4 Deleting a Command Code

Use the following procedure to delete a Command Code.

> **Note**
>
> (E)CCs cannot be deleted.

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
- Transaction Configuration Sets

1. Click **Diameter**, and then **Configuration**, and then **Command Codes**.
2. Select the **Command Code** to delete.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.9 Diameter Configuration Sets

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 Configuration Sets Elements. Each connection references a single **Connection Configuration Set**.

You can perform these tasks on an Active System OAM (**SOAM**).

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 view all of the options.
- Click **Insert**.

  On the Connection Configuration Sets [Insert] page, you can add a new Connection Configuration Set and its options. See Adding Configuration Sets.

  If the maximum number of Connection Configuration Sets per Network Element (2000) already exist in the system, then the Connection Configuration Sets [Insert] page does not appear and an error message displays.
- Select a Connection Configuration Set Name in the list and click **Edit**.

  On the Connection Configuration Sets [Edit] page, you can edit the selected Connection Configuration Set. See Editing Configuration Sets.

  If at least one connection that uses the Connection Configuration Set is in the Enabled Admin state, then the Connection Configuration Sets [Edit] page does not open.
- Select a Connection Configuration Set Name in the list and click **Delete** to remove the selected Connection Configuration Set.

  The Default Connection Configuration Set cannot be deleted. See Deleting Configuration Sets.

> **Note**
>
> You perform these tasks on the following Connection Configuration Sets tabs:
>
> - SCTP Options
> - Diameter Options
> - TCP Options
> - RADIUS Options

2.9.1 Diameter Connection Configuration Sets

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 Configuration Sets Elements. Each connection references a single **Connection Configuration Set**.

You can perform these tasks on an Active System OAM (**SOAM**).

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 view all of the options.
- Click **Insert**.

  On the Connection Configuration Sets [Insert] page, you can add a new Connection Configuration Set and its options. See Adding Configuration Sets.

  If the maximum number of Connection Configuration Sets per Network Element (2000) already exist in the system, the Connection Configuration Sets [Insert] page does not appear and an error message displays.
- Select a Connection Configuration Set Name in the list and click **Edit**.

  On the Connection Configuration Sets [Edit] page, you can edit the selected Connection Configuration Set. See Editing Configuration Sets.

  If at least one connection that uses the Connection Configuration Set is in the "Enabled" Admin state, the Connection Configuration Sets [Edit] page does not open.
- Select a Connection Configuration Set Name in the list and click **Delete** to remove the selected Connection Configuration Set.

  The Default Connection Configuration Set cannot be deleted. See Deleting Configuration Sets.

> **Note**
>
> You perform these tasks on the following Connection Configuration Sets tabs:
>
> - SCTP Options
> - Diameter Options
> - TCP Options
> - RADIUS Options
> - Priority Options

2.9.1.1 Configuration Sets Elements

Table 2-5 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.

> **Note**
>
> You must assign a **Connection Configuration Set** attribute to each RADIUS Connection. When this attribute is assigned to a local node, it is ignored by RCL.

Table 2-5 Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Connection Configuration Set Name	Unique name of the Connection Configuration Set.	Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin 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. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric 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 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 are sent at a constant rate until an ACK is received or the maximum attempts is reached.	Format: numeric Range: 10 - 10000 Default: 120
* Retransmit Maximum Timeout for INIT (ms)	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 the Retransmit Maximum Timeout is used for INITs as well. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: 0, 10 - 10000 Default: 120

Table 2-5 (Cont.) Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Number of Retransmits Triggering Path Failure	Number of consecutive unsuccessful retransmits that 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 Range: 1 - 10 Default: 3
* Number of Retransmits Triggering Association Failure	Number of consecutive retransmits that 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 Range: 1 - 20 Default: 5
* Number of Retransmits Triggering Init Failure	Number of consecutive retransmits for INIT and COOKIE-ECHO Chunks that 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. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: 1 - 20 Default: 8

Table 2-5 (Cont.) Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* SACK Delay (ms)	The number of milliseconds to delay after receiving a DATA Chunk and before 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 Range: 1 - 200 Default: 10
* SCTP Heartbeat Interval (ms)	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 Range: 0, 100 - 300000 Default: 1000
* 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. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: 8000 - 5000000 Default: 1000000
* Socket Receive Buffer Size (bytes)	Socket receive buffer size for incoming SCTP messages. The receive buffer size must be greater than or equal to the product of the bandwidth and the round trip delay for the association. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: 8000 - 5000000 Default: 1000000
* Maximum Burst	Specifies the maximum burst of packets that can be emitted by this association.	Format: numeric Range: 1 - 4 Default: 4

Table 2-5 (Cont.) Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Max Number of Inbound Streams	Maximum number of inbound SCTP streams supported locally by the SCTP connection. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: 1 -16 Default: 8
* Max Number of Outbound Streams	Maximum number of outbound SCTP streams supported locally by the SCTP connection. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: 1 -16 Default: 8
Datagram Bundling Enabled	If checked, datagram bundling is enabled for the SCTP connection.	Format: checkbox Range: checked, unchecked Default: checked
* Maximum Segment Size	The Maximum Size to put in any outgoing SCTP DATA chunk. If a message is larger than this size, it is fragmented by SCTP into the specified size.	Format: numeric Range: 0, 64 - 1460 Default: 0
Fragmentation	If checked, a message exceeding the size of the PMTU (Path Max Transmission Unit) is fragmented and reassembled by the peer.	Format: checkbox Range: checked, unchecked Default: checked
Ordered Delivery	If checked, Ordered delivery of the SCTP DATA Chunk is performed. Otherwise, unordered delivery of the SCTP DATA Chunk is performed.	Format: checkbox Range: checked, unchecked Default: unchecked
	Diameter Options	
* Connect Timer (sec)	Controls the frequency of transport connection attempts to a Peer where no active transport connection exists. Applicable only for connections configured to initiate a connection with a Peer Node.	Format: numeric Range: 1 - 60 Default: 30
* Watchdog Timer Init Value (sec)	Initial value of the application watchdog timer.	Format: numeric Range: 1 - 30 Default: 30

Table 2-5 (Cont.) Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* 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. **Note**: For local nodes, CEAs are sent in response to erroneous CERs. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: 1 - 30 Default: 3
* Disconnect Timer (sec)	After sending a DPA message, time to wait for a Peer to disconnect transport. After sending a DPR message, time to wait for the Peer to send the DPA. If the timer expires, transport is disconnected by the application.	Format: numeric Range: 1 - 30 Default: 3
Proving Mode	Proving mode for the Configuration Set.	Format: Option 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 Range: 50 - 30000 Default: 500
* Proving Times	The number of consecutive DWR and DWA exchanges within Proving Timer time during connection proving.	Format: numeric 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 is not selected for routing until the number of Pending Requests falls below this value. **Note**: Because the pending transaction limit is located in the Connection Configuration Set, it cannot be edited unless the connection is disabled.	Format: numeric Range: 1 - 20000 Default: 1000
CEX Host IP Validation Enabled	If checked, Host-IP-Address AVP validation is enabled during CEX message exchange.	Format: checkbox Range: checked, unchecked Default: checked
	TCP Options	

Table 2-5 (Cont.) Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Nagle Enabled	If checked, the Nagle algorithm is enabled for the TCP connection.	Format: checkbox Range: checked, unchecked 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. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: Not Applicable, 8000 - 5000000 Default: 1000000
* 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. **Note**: The parameter with the Local Node's Connection Configuration Set is used by the peer-initiated (responder) connection.	Format: numeric Range: Not Applicable, 8000 - 5000000 Default: 1000000
*Maximum Segment Size	The Maximum Segment Size for outgoing TCP Packets. The TCP Maximum Segment Size is the IP maximum transmission unit (MTU) minus the size of the TCP and IPv4/IPv6 headers. Setting this value to 0 indicates the user is not limiting fragmentation.	Format: numeric Range: 0, 88 - 1460 Default: 1024
Keep-Alive	If checked, TCP probes a connection that has been idle for the amount of time configurable by **Keep-Alive Idle Time** parameter.	Format: checkbox Range: checked, unchecked Default: unchecked
* Keep-Alive Idle Time	Specifies the number of seconds of idle time between Keep Alive Probes if **Keep-Alive** is enabled.	Format: numeric Range: 1 - 7200 Default: 1
* Keep-Alive Probe Interval	If **Keep-Alive** is enabled, sets the interval between Keep Alive Probes in seconds. This value cannot be changed after a connection is established.	Format: numeric Range: 1 - 120 Default: 1

Table 2-5 (Cont.) Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Keep-Alive Maximum Count	If **Keep-Alive** is enabled, sets the maximum number of Keep Alive Probes TCP sends without any response from the remote server, before TCP gives up and aborts the connection.	Format: numeric Range: 1 - 16 Default: 9
	Radius Options	
Pending Transactions Per Connection	The maximum number of Pending Requests waiting for Response from Peer on this connection. If maximum Pending Transactions is reached, then this connection is not selected for routing until the Pending transactions are below this value.	Format: numeric Range: 1 - 5000 Default: 1000
Prevent duplicate transactions due to egress retransmissions	This option applies to RADIUS client connections only and determines how to handle a Request being retransmitted to the same peer as before, but the corresponding transaction record (that contains the previously used source port, RADIUS ID and Request Authenticator) has expired. If this option is selected, and if the corresponding transaction record has expired, the routing application does not forward the Request to the same peer with a new RADIUS ID, source port, and Request Authenticator. An alternate peer can be selected for routing in this case. If this option is not selected, and the corresponding transaction record has expired, DSR shall select a new source port, RADIUS ID and Request Authenticator, create a new transaction record and forward the Request to the peer.	Format: checkbox Range: checked, unchecked Default: checked

Table 2-5 (Cont.) Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Prevent duplicate transactions due to ingress retransmissions	This option applies to RADIUS server connections only and determines how DSR shall processes duplicate requests received from a client. A request is considered duplicate if the client retransmits a request with the same source IP address, source port number, RADIUS ID and Request Authenticator. If this option is selected, DSR shall create an ingress transaction record for the request (with the request's source IP address, port, RADIUS ID and Request Authenticator) which shall be used to admit only the first Request into DSR and prevent admitting of duplicate requests, if received, till the transaction record is present. If a Response has been sent previously to the peer, it shall be saved in the transaction record and shall be forwarded to the client in response to duplicate requests. If this option is not selected, DSR shall not maintain ingress transaction records and shall admit all Requests received from the client.	Format: checkbox Range: checked, unchecked Default: checked
Cached response Duration (ms)	This option applies to server connections only. Applicable only if Prevent duplicate transactions due to ingress retransmissions = Checked. This value specifies the duration for which a cached response is held in the ingress transaction record. This value should cover the potential of loss of response and further retransmissions by the client.	Format: numeric Range: 3000 - 100000 Default: 5000
	Priority Options	
CPL1 Minimum Request Priority Allowed	If 16 Priority Admin State is enabled in System Options then Connection Configuration Set shall support insertion and update of **CPL1 Minimum Request Priority Allowed** values in the range of 1-15. If 16 Priority Admin State is disabled, then this field is non-configurable.	Format: checkbox If 16 Priority Admin State is enabled: • Range: 1 - 15 • Default: 4 If 16 Priority Admin State is disabled: • Range: n/a • Default: 1

Table 2-5 (Cont.) Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
CPL1 Minimum Request Priority Allowed	If 16 Priority Admin State is enabled in System Options then Connection Configuration Set shall support insertion and update of **CPL2 Minimum Request Priority Allowed** values in the range of 2-15. If 16 Priority Admin State is disabled, then this field is non-configurable.	Format: checkbox If 16 Priority Admin State is enabled: • Range: 2 - 15 • Default: 8 If 16 Priority Admin State is disabled: • Range: n/a • Default: 2
CPL1 Minimum Request Priority Allowed	If 16 Priority Admin State is enabled in System Options then Connection Configuration Set shall support insertion and update of **CPL3 Minimum Request Priority Allowed** values in the range of 3-16. If 16 Priority Admin State is disabled, then this field is non-configurable.	Format: checkbox If 16 Priority Admin State is enabled: • Range: 3 - 15 • Default: 16 If 16 Priority Admin State is disabled: • Range: n/a • Default: 3

2.9.1.2 Adding Configuration Sets

Use this task to create new Configuration Sets.

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 Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Connection Configuration Sets**.
2. Click **Insert**.
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 the **RADIUS Options** tab. Enter the RADIUS values in the fields.
8. Click **OK**, **Apply**, or **Cancel**.

2.9.1.3 Editing Configuration Sets

Use this task to edit existing Configuration Sets.

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 do 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Connection Configuration Sets**.
2. Select the Connection Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.

   For information about each field, see Configuration Sets Elements.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.1.4 Deleting Configuration Sets

Use this task to delete Configuration Sets.

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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Connection Configuration Sets**.
2. Select the Connection Configuration Set you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.9.2 CEX Configuration Sets

A **CEX Configuration Set** provides a mechanism for assigning up to 20 unique CEX Parameters and up to 20 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).

You can perform these tasks on an Active System OAM (**SOAM**).

Each Local Node refers 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**, and then **Configuration**, and then **CEX Parameters [Filtered]** page for the selected Application ID only.
- Click **Insert**.

  On the CEX Configuration Sets [Insert] page, 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, then the CEX Configuration Sets [Insert] page does not appear and an error message displays.
- Select a CEX Configuration Set Name in the list and click **Edit**.

  On the CEX Configuration Sets [Edit] page, 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 **Delete** to remove the selected CEX Configuration Set.

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

2.9.2.1 CEX Configuration Set Elements

Table 2-6 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 2-6 CEX 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.	Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
Dynamic	Indicates whether or not the CEX Configuration Set was created dynamically (YES) or statically (NO). NO is assigned for all CEX Configuration Sets via Dynamic Peer Discovery.	Format: checkbox (read-only on the CEX Configuration Set [Edit] page) Range: checked unchecked Default: unchecked
* CEX Parameters	**Available CEX Parameters Application ID-"Name"-Type-Vendor ID** All unique configured CEX Parameters, showing Application IDs with Application Type, and with Vendor ID if the Application ID is Vendor-Specific.	Format: list Range: All configured CEX Parameters Default: none
	Selected CEX Parameters Application ID-"Name"-Type-Vendor ID CEX Parameters that are selected from the **Available CEX Parameters** list for this CEX Configuration Set.	Format: list Range: 20 entries Default: none
	Must Include CEX Parameters Application ID-"Name"-Type-Vendor ID CEX Parameters selected from the **Selected CEX Parameters** list that must be present in the CEX message exchanged from the Peer.	Format: list Range: 20 entries Default: none
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 Default: none
	Selected Supported Vendor IDs Vendor IDs selected from the **Available Supported Vendor IDs** list for this CEX Configuration Set.	Format: list Range: 20 entries Default: none
DSR Feature Status AVP	If checked, this Vendor specific AVP is sent in CER/CEA messages. It can convey the status of various features like NGN-PS to Peer DSR.	Format: checkbox Range: checked unchecked Default: unchecked

2.9.2.2 Adding a CEX Configuration Set

Use this task to create a new CEX Configuration Set.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **CEX Configuration Sets**.
2. Click **Insert**.
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 **Add** 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 **Add** 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 **Remove** 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 **Remove** 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 **Add** 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 **Remove** above the **Selected Supported Vendor IDs** list.
6. Click **OK**, **Apply**, or **Cancel**.

2.9.2.3 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **CEX Configuration Sets**.
2. Select the CEX Configuration Set that you want to edit.

   The Default CEX Configuration Set cannot be changed.
3. Click **Edit.**

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, then 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 **Add** 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 **Add** 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 **Remove** 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 **Add** 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 **Add** 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 **Remove** above the **Selected Supported Vendor IDs** list.

5. Click **OK**, **Apply**, or **Cancel**.

2.9.2.4 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **CEX Configuration Sets**.
2. Select one CEX Configuration Set that you want to delete.
3. Click **Delete**

   A popup window appears.

4. Click **OK** or **Cancel**.

2.9.3 Capacity Configuration Sets

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

You can perform these tasks on an Active System OAM (**SOAM**).

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.

> **Note**
>
> The Per Connection Ingress MPS Control feature must be purchased and enabled before Capacity Configuration Sets can be configured.

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 **Insert**.
  On the Capacity Configuration Sets [Insert] page, you can add a new Capacity Configuration Sets and its values. See Adding a Capacity Configuration Set.

  If the Per Connection Ingress MPS Control feature is not enabled, then the Capacity Configuration Sets [Insert] page does not appear and an error message displays.

  If the maximum number of Capacity Configuration Sets (1000) already exists in the system, then the Capacity Configuration Sets [Insert] page does not appear and an error message displays.
- Select the Name of a Capacity Configuration Set in the list and click **Edit**.
  On the Capacity Configuration Sets [Edit] page, you can edit the selected Capacity Configuration Set. See Editing a Capacity Configuration Set.

  If the Default Capacity Configuration Set is selected and the Per Connection Ingress MPS Control feature is not enabled, then the Capacity Configuration Sets [Edit] page does not appear and an error message displays.
- Select the Name of a Capacity Configuration Set in the list and click **Delete** 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 Validating Diameter Connection Capacity.

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 and must be validated before they can be allowed. (Actions that increase capacity rather than reduce it do not require validation.)

An error displays, 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 displays 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, then an error displays.

The **Diameter**, and then **Configuration**, and then **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 Functions.

2.9.3.1 Capacity Configuration Set Elements

Table 2-7 describes the fields on the Capacity 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 2-7 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

Table 2-7 (Cont.) Capacity Configuration Sets Elements

Field (* indicates field is required)	Description	Data Input Notes
* Reserved Ingress MPS	The capacity in ingress Diameter messages per second that are permanently reserved for the connection. If the default value is set to zero, the connections do not reserve message processing capacity. If the default is a non-zero value, the Reserved Ingress MPS Capacity ranges from 10 to the value of the Connection Engineered Capacity. If the Reserved Ingress MPS Capacity is 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.	Format: numeric Range: 0, 10 - 10000 Default: 0
* Maximum Ingress MPS	The maximum rate within Diameter ingress messages per second that the connection is allowed to process. This field ranges from 100 to the value of the MP Maximum Reserved Capacity. It is acceptable for the sum of the capacity for all connections on an MP server to exceed the MP Engineered Ingress MPS (and the MP Maximum Reserved Ingress MPS).	Format: numeric Range: 0, 10 - 10000 Default: 10000
* Ingress MPS Minor Alarm Threshold (Percent)	The percentage of the connection's maximum MPS capacity that triggers a minor alarm. The default Capacity Configuration Set has an Ingress MPS Capacity Minor Alarm Threshold default value set to 50% of the Connection Configured Maximum Ingress MPS with a range from 5% to 100%. This alarm threshold must be less than the Ingress MPS Capacity Major Alarm Threshold. The Minor Alarm Abatement threshold is set 5% lower than Minor Alarm Threshold.	Format: numeric Range: 10 - 99 Default: 50

Table 2-7 (Cont.) Capacity Configuration Sets Elements

Field (* indicates field is required)	Description	Data Input Notes
* Ingress Major Alarm Threshold (Percent)	The percentage of the connection's maximum MPS capacity that triggers a major alarm. The default Capacity Configuration Set has an Ingress MPS Capacity Major Alarm Threshold default value set to 80% of the Connection Configured Maximum Ingress MPS with a range from 5% to 100%. This alarm threshold must be greater than the Ingress MPS Capacity Minor Alarm Threshold. The Major Alarm Abatement threshold is set 5% lower than Major Alarm Threshold.	Format: numeric Range: 11 - 100 Default: 80
* Ingress MPS Alarm Abatement Time	The minimum time that connection's ingress message rate must remain less than or equal to respective abatement threshold before the alarm clears or its severity reduced from Major to Minor.	Format: numeric Range: 1000 - 5000 Default: 2000
* Convergence Time (ms)	The amount of time (msec) it takes to converge on a per second rate. If the convergence time is less than 1000 msec, the rate is extrapolated. If the convergence time is greater than 1000 msec, the rate is averaged.	Format: numeric Range: • 250 • 500 • 1000 • 2000 • 4000 Default: 1000

2.9.3.2 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Capacity Configuration Sets**.
2. Click **Insert**.
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 is 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 is raised for connections using this Capacity Configuration Set.
8. Enter the **Ingress MPS Alarm Abatement Time** in milliseconds, if a value other than the default value is needed.
9. Enter the **Convergence Time** in milliseconds, if a value other than the default value is needed
10. Click **OK**, **Apply**, or **Cancel**.

2.9.3.3 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. To assistance you in disabling connections refer to Disabling Connections. (The **Reserved Ingress MPS** field is the only field that requires the Connections to be Disabled before it can be changed.)

The Per Connection Ingress MPS Control feature must be enabled before the Default Capacity Configuration Set can be edited.

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

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Capacity Configuration Sets**.
2. Select the Capacity Configuration Set to be edited.
3. Click **Edit**.

   The Capacity Configuration Sets [Edit] page displays 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**, **Apply**, or **Cancel**.
6. Reference Enabling Connections to enable any Connections that were disabled before the Capacity Configuration Set was changed.

2.9.3.4 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 reference Disabling Connections to disable any Connections that use the Capacity Configuration Set and reference Editing a Connection to edit each Connection to no longer use the Capacity Configuration Set.

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

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Capacity Configuration Sets**.
2. Select the Capacity Configuration Set you want to delete.

3. Click **Delete**.

   A popup window appears to confirm the delete.

4. Click **OK** or **Cancel**.

2.9.4 Egress Message Throttling Configuration Sets

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.

You can perform these tasks on an Active System OAM (**SOAM**).

When the **EMR** 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 Convergence time 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 **Insert**.

  On the Egress Message Throttling Configuration Sets [Insert] page, 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, then the Egress Message Throttling Configuration Sets [Insert] page does not appear and an error message displays.
- Select an Egress Message Throttling Configuration Set Name in the list and click **Edit**.

  On the Egress Message Throttling Configuration Sets [Edit] page, 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, then the Egress Message Throttling Configuration Sets [Edit] page does not open.
- Select an Egress Message Throttling Configuration Set Name in the list and click **Delete** to remove the selected Egress Message Throttling Configuration Set.

2.9.4.1 Egress Message Throttling Configuration Set Elements

Table 2-8 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 2-8 Egress Message Throttling Configuration Set Elements

Field (* indicates required field)	Description	Data Input Notes
* Egress Message Throttling Configuration Set Name	A name that uniquely identifies the Egress Message Throttling Configuration Set.	Format: String: case-sensitive; alphanumeric and underscore (_); must contain at least one alpha; cannot begin with a digit. Range: 1 - 32 characters
* Max Egress Message Rate	A maximum Egress Message Rate (EMR) on a connection being throttled. **Note**: The EMR is calculated every 100ms by subtracting the oldest traffic count from the newest traffic count, and averaging the difference over the elapsed time between them.	Format: numeric Range: 10 - 10000 Default: none
* Throttle Threshold Level 1 (%)	Throttle Threshold Level 1. When Threshold exceeds Level 1, Congestion Level is set to 1	Format: numeric Range: 2 - 100 Default: 100
* Abatement Threshold Level 1 (%)	Abatement Threshold Level 1. When Threshold falls below Level 1, Congestion Level is set to 0.	Format: numeric Range: 1 - 99 Default: 80
Throttle Threshold Level 2 (%)	Throttle Threshold Level 2. When Threshold exceeds Level 2, Congestion Level is set to 2.	Format: numeric Range: 4 - 100 Default: none
Abatement Threshold Level 2 (%)	Abatement Threshold Level 2. When Threshold falls below Level 2, the Congestion Level is set to 1.	Format: numeric Range: 3 - 99 Default: none
Throttle Threshold Level 3 (%)	Throttle Threshold Level 3. When Threshold exceeds Level 3, Congestion Level is set to 3.	Format: numeric Range: 6 -100 Default: none
Abatement Threshold Level 3 (%)	Abatement Threshold Level 3. When Threshold falls below Level 3, the Congestion Level is set to 2.	Format: numeric Range: 5 - 99 Default: none

Table 2-8 (Cont.) Egress Message Throttling Configuration Set Elements

Field (* indicates required field)	Description	Data Input Notes
* Convergence Time (msec)	The time it takes in milliseconds to converge on a per second rate. If the convergence time is less than 1000 milliseconds, the rate is Convergence Time (msec) extrapolated. If the convergence time is greater than 1000 milliseconds, the rate is averaged. The rate convergence time is the amount of time it takes for the measured rate to converge on the actual rate.	Format: numeric Range: • 250 • 500 • 1000 • 2000 • 4000 Default: 250
* Abatement Time (msec)	This value specifies the amount of time that a throttled connection's Egress Request Rate must remain below an abatement before allowing it to abate to a lower CL. For example, if the following is true: • Max EMR = 1000 messages per second • Abatement Threshold-3 = 80% * 100=> 800 messages per second) • Abatement time = 500 milliseconds • Current Congestion Level = CL3 Then all of the message rate calculations during a contiguous 500 msec must be less than 800 MPS in order for the congestion level to be reduced from CL3 to CL2.	Format: numeric Range: 200 - 10000 Default: 500

2.9.4.2 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Egress Message Throttling Configuration Sets**.
2. Click **Insert**.
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 **Max 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 **Convergence Time** and an **Abatement Time**.
7. Click **OK**, **Apply**, or **Cancel**.

2.9.4.3 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Egress Message Throttling Configuration Sets**.
2. Select the Egress Message Throttling Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.

   For information about each field, see Egress Message Throttling Configuration Set Elements.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.4.4 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Egress Message Throttling Configuration Sets**.
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** or **Cancel**.

2.9.5 Message Priority Configuration Sets

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

You can perform these tasks on an Active System OAM (**SOAM**).

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 on 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 **Insert**.

  On the Message Priority Configuration Sets [Insert] page, 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 exists in the system, then the Message Priority Configuration Sets [Insert] page does not appear and an error message displays.
- Select a Message Priority Configuration Set Name in the list and click **Edit**.

  On the Message Priority Configuration Sets [Edit] page, 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 does not open.
- Select a Message Priority Configuration Set Name in the list and click **Delete** to remove the selected Message Priority Configuration Set. The Default Message Priority Configuration Set cannot be deleted.

2.9.5.1 Message Priority Configuration Set Elements

Table 2-9 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 2-9 Message Priority Configuration Set Elements

Field (* indicates a required field)	Description	Data Input Notes
* Message Priority Configuration Set Name	Unique name of the Message Priority Configuration Set.	Format: Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
* Message Priority Rules	The number of Message Priority Rules defined in the Message Priority Configuration Set.	

Table 2-9 (Cont.) Message Priority Configuration Set Elements

Field (* indicates a required field)	Description	Data Input Notes
Application ID	The Application ID used to filter incoming Diameter messages.	Format: List Range: Select from the configured Application IDs. **Note**: An asterisk (*) matches any Application ID.
Application Name (view only)	The name of the application associated with the Application ID.	
Command Code	The Command Code used to filter incoming Diameter messages. An ECC is a Command Code that also takes into account the value of a specific AVP for that Command Code that gives the "true" command type (for example, CCR-I, CCR-U, and so on). **Note**: This list of configured Command Codes includes Extended Command-Codes (ECC) immediately after their parent Command-Code.	Format: List Range: Select from the configured Command Codes. **Note**: An asterisk (*) matches any Command Code.
Command Code Name (view only)	The name of the command associated with the Command Code.	
Message Priority	The message priority assigned to incoming messages that match the combination of Application ID and Command Code.	Format: List Range: 0 - Max (Maximum Normal Request Priority as defined in System Options)

2.9.5.2 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Message Priority Configuration Sets**.
2. Click **Insert**.
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**, **Apply**, or **Cancel**.

2.9.5.3 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Message Priority Configuration Sets**.
2. Select the Message Priority Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.

   For information about each field, see Message Priority Configuration Set Elements.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.5.4 Deleting a Message Priority Configuration Set

Use this task to delete a Message Priority Configuration Set.

> **Note**
>
> The Default Message Priority Configuration Set cannot be deleted.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Message Priority Configuration Sets**.
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** or **Cancel**.

2.9.6 Message Copy Configuration Sets

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.

You can perform these tasks on an Active System OAM (**SOAM**).

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 **Insert**.
  On the Message Copy Configuration Sets [Insert] page, 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 displays.
- Select a Message Copy Configuration Set Name in the list and click **Edit**.
  On the Message Copy Configuration Sets [Edit] page, 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, **Edit** is disabled.
- Select a Message Copy Configuration Set Name in the list and click **Delete** 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.

2.9.6.1 Message Copy Configuration Set Elements

Table 2-10 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 2-10 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.	Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
* Route List of the DAS Node	Route List to be used for copying a message to a DAS node.	Format: List Range: Select from the configured Route Lists. Default: -Select-
Message Copy Request Type	Type of Request to be copied to the DAS.	Format: Options Range: Original Ingress Request or 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: Options Range: Yes, No Default: No
Original Answer Result Code For Message Copy	Result Code/Experimental Result code that should match with incoming Answer Result Code (whose Request has been marked for Message Copy) to allow copying a Request to DAS.	Format: Options Range: • 2xxx result-code/ experimental-result-code • Any result/experimental-result-code Default: 2xxx result-code/ experimental-result-code

Table 2-10 (Cont.) Message Copy Configuration Set Elements

Field (* indicates a required field)	Description	Data Input Notes
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: Options 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 there are no re-transmissions after the first copy attempt.	Format: numeric Range: 0 - 4 Default: 0

2.9.6.2 Adding a Message Copy Configuration Set

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

The fields are described in Message Copy Configuration Set Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Message Copy Configuration Sets**.
2. Click **Insert**.

   If the maximum numbers of Message Copy Configuration Sets (100) allowed in the system are already configured, the Message Copy Configuration Sets [Insert] page does 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**, **Apply**, or **Cancel**.

2.9.6.3 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Message Copy Configuration Sets**.
2. Select the Message Copy Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.6.4 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. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Message Copy Configuration Sets**.
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** or **Cancel**.

2.9.7 Rate Limiting Configuration Sets

Rate Limiting Configuration Sets provide the mechanism to enter data needed by Egress Throttle Groups (on the SOAM GUI) and Egress Throttle Lists (on the NOAM GUI) to perform egress throttling by egress message rate. For details about the NOAM functionality, see Rate Limiting Configuration Sets on the NOAM.

You can perform these tasks on an Active System OAM (**SOAM**).

An Egress Throttling Group is always associated with a Rate Limiting Configuration Set, which provides the following data for performing Egress Message Rate Throttling:

- Maximum Message Rate
- Onset and Abatement Thresholds:
  - Percentages of the maximums
  - Used with Message Priority to determine which requests to throttle
- Convergence time, which allows you to control the sensitivity of request traffic bursts on an ETG.
- Abatement time

Rate Limiting can be enabled on the SOAM Main Menu: **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups** page.

For NOAM functionality, you must change the **Egress Throttling Control Scope** of the Egress Control Group to ETL and enable Egress Message Rate Throttle on the Egress Throttle Group before Egress Message Rate Throttling can be started on Egress Throttle Lists.

The Rate Limiting Configuration Set fields are described in Rate Limiting Configuration Sets Elements.

On the Rate Limiting Configuration Sets page, you can perform the following actions:

- Filter the list of Rate Limiting Configuration Sets to display only the desired Rate Limiting Configuration Sets.
- Sort the list by column contents in ascending or descending order by clicking the column heading. The default order is by **Rate Limiting Configuration Set Name** in ascending ASCII order.
- Click **Insert**.
  On the Rate Limiting Configuration Sets [Insert] page, you can add a new Rate Limiting Configuration Set. See Adding a Rate Limiting Configuration Set.

If the maximum number of Rate Limiting Configuration Sets already exists in the system, an error message displays.

- Select a **Rate Limiting Configuration Set Name** in the list and click **Edit**.
  On the Rate Limiting Configuration Sets [Edit] page, you can edit the selected Rate Limiting Configuration Set. See Editing a Rate Limiting Configuration Set.

  If no row is selected, or if more than one row is selected, **Edit** is disabled.
- Select a **Rate Limiting Configuration Set Name** in the list and click **Delete** to remove the selected Rate Limiting Configuration Set.
  The Default Rate Limiting Configuration Set can be edited, but cannot be deleted. See Deleting a Rate Limiting Configuration Set.

2.9.7.1 Rate Limiting Configuration Sets Elements

Table 2-11 describes the fields on the Rate Limiting Configuration Sets View, Edit, and Insert pages. Data input notes apply only to the Insert and Edit pages; the View page is read-only.

> **Note**
>
> This GUI page is available from the SOAM and NOAM menu.

Table 2-11 Rate Limiting Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
Rate Limiting Configuration Set Name	Unique name of the Rate Limiting Configuration Set.	Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
* Maximum Egress Request Rate	The maximum allowed Egress Request Rate shared by associated members.	Format: numeric Range: 100 - 250000 Default: 6000
* Onset Threshold Level 1 (%)	When Egress Request Rate exceeds this percentage of maximum Egress Request Rate, the Congestion Level is set to 1. Onset Threshold Level 1 is ignored if ETG Mode is Limit.	Format: numeric Range: 2 - 100 Default: 60
* Abatement Threshold Level 1 (%)	When Egress Request Rate falls below this percentage of maximum Egress Request Rate, the Congestion Level is set to 0. Abatement Threshold Level 1 is ignored if ETG Mode is Limit.	Format: numeric Range: 1 - 100 Default: 55
Onset Threshold Level 2 (%)	When Egress Request Rate exceeds this percentage of maximum Egress Request Rate, the Congestion Level is set to 2. Onset Threshold Level 2 is ignored if ETG Mode is Limit.	Format: numeric Range: 4 - 100 Default: none

Table 2-11 (Cont.) Rate Limiting Configuration Sets Elements

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. Abatement Threshold Level 2 is ignored if ETG Mode is Limit.	Format: numeric Range: 3 - 100 Default: none
Onset Threshold Level 3 (%)	When Egress Request Rate exceeds this percentage of maximum Egress Request Rate, the Congestion Level is set to 3. Onset Threshold Level 3 is ignored if ETG Mode is Limit.	Format: numeric Range: 6 - 100 Default: none
Abatement Threshold Level 3 (%)	When Egress Request Rate falls below this percentage of maximum Egress Request Rate, the Congestion Level is set to 2. Abatement Threshold Level 3 is ignored if ETG Mode is Limit.	Format: numeric Range: 5 - 100 Default: none
* Convergence Time (msec)	The time it takes in milliseconds to converge on a per second rate. If the convergence time is less than 1000 milliseconds, the rate is extrapolated. If the convergence time is greater than 1000 milliseconds, the rate is averaged. The rate convergence time is the amount of time it takes for the measured rate to converge on the actual rate.	Format: List Range: 250, 500, 1000, 2000, 4000 Default: 1000
* Abatement Time (msec)	The amount of time in milliseconds that the Egress Request Rate must remain below an abatement threshold before the Congestion Level is lowered.	Format: numeric Range: 50 - 10000 Default: 50

2.9.7.2 Adding a Rate Limiting Configuration Set

Use this task to create a new Rate Limiting Configuration Set.

> **Note**
>
> This GUI page is available from the SOAM and NOAM menu.

The fields are described in Rate Limiting Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Rate Limiting Configuration Sets** on the SOAM or **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Rate Limiting Configuration Sets** on the NOAM.
2. Click **Insert**.

3. Enter a unique name for the Rate Limiting Configuration Set in the **Rate Limiting Configuration Set Name** field.
4. Select or enter the element values.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.7.3 Editing a Rate Limiting Configuration Set

Use this task to edit an existing Rate Limiting Configuration Set.

> **Note**
>
> This GUI page is available from the SOAM and NOAM menu.

When the Rate Limiting Configuration Sets page opens, the fields are populated with the currently configured values.

The **Rate LimitingConfiguration Set Name** cannot be edited.

The fields are described in Rate Limiting Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Rate Limiting Configuration Sets** on the SOAM or **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **-Rate Limiting Configuration Sets** on the NOAM.
2. Select the Rate Limiting Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click:
   - **OK** to save the changes and return to the Rate Limiting Configuration Sets page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the Rate Limiting Configuration Sets page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then an error message appears:
   - The selected Rate Limiting 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.

2.9.7.4 Deleting a Rate Limiting Configuration Set

Use this task to delete a Rate Limiting Configuration Set.

> **Note**
>
> This GUI page is available from the SOAM and NOAM menu.

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

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Rate Limiting Configurations Sets** on the SOAM or **Diameter**, and then **Configuration -> Egress Throttle List**, and then **-Rate Limiting Configuration Sets** on the NOAM.
2. Select the Rate Limiting Configuration Set you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.9.8 Pending Transaction Limiting Configuration Sets

Pending Transaction Limiting Configuration Sets configuration provides the mechanism to enter configuration data needed by Egress Throttle Groups to determine when to start throttling for pending transactions. For details about the NOAM functionality, see Pending Transaction Limiting Configuration Sets on the NOAM.

An ETG is always associated with a Pending Transaction Limiting Configuration Set that provides the following data for performing Egress Message Rate Throttling based on pending transactions:

- Maximum pending transactions
- Onset and Abatement Thresholds:
  - Percentages of the maximums
  - Used with Message Priority to determine which requests to throttle
- Abatement time

You must enable Pending Transaction Limiting before Egress Pending Transaction Limiting can be started on Egress Throttle Groups.

The Pending Transaction Limiting Configuration Sets fields are described in Pending Transaction Limiting Configuration Sets Elements.

On the Pending Transaction Limiting Configuration Sets page, you can perform the following actions:

- Filter the list of Pending Transaction Limiting Configuration Sets to display only the desired Pending Transaction Limiting Configuration Sets.
- Sort the list by column contents in ascending or descending order by clicking the column heading. The default order is by **Pending Transaction Limiting Configuration Sets** in ascending ASCII order.
- Click **Insert**.
  On the Pending Transaction Limiting Configuration Sets [Insert] page, you can add a new Pending Transaction Limiting Configuration Sets. See Adding a Pending Transaction Limiting Configuration Set.

  If the maximum number of Pending Transaction Limiting Configuration Sets already exists in the system, an error message displays.
- Select a Pending Transaction Limiting Configuration Set Name in the list and click **Edit**.
  On the Pending Transaction Limiting Configuration Sets [Edit] page, you can edit the selected Pending Transaction Limiting Configuration Set. See Editing a Pending Transaction Limiting Configuration Set.

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

- Select a **Pending Transaction Limiting Configuration Set Name** in the list and click **Delete** to remove the selected Pending Transaction Limiting Configuration Set.
  The Default Pending Transaction Limiting Configuration Set can be edited, but cannot be deleted. See Deleting a Pending Transaction Limiting Configuration Set.

2.9.8.1 Pending Transaction Limiting Configuration Sets Elements

Table 2-12 describes the fields on the Pending Transaction Limiting 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 2-12 Pending Transaction Limiting Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
Pending Transaction Limiting Configuration Set Name	Unique name of the Pending Transaction Limiting Configuration Set.	Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
*Maximum Egress Pending Transactions	The maximum allowed Egress Pending Transactions for the Peers and Connections within a group.	Format: numeric Range: 100 - 1000000 Default: none
*Onset Threshold Level 1 (%)	When Egress Pending Transactions exceeds this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 1. Onset Threshold Level 1 is ignored if ETG Mode is Limit.	Format: numeric Range: 2 - 100 Default: 60
*Abatement Threshold Level 1 (%)	When Egress Pending Transactions falls below this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 0. Abatement Threshold Level 1 is ignored if ETG Mode is Limit.	Format: numeric Range: 1 - 100 Default: 55
Onset Threshold Level 2 (%)	When Egress Pending Transactions exceeds this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 2. Onset Threshold Level 2 is ignored if ETG Mode is Limit.	Format: numeric Range: 4 - 100 Default: none
Abatement Threshold Level 2 (%)	When Egress Pending Transactions falls below this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 1. Abatement Threshold Level 2 is ignored if ETG Mode is Limit.	Format: numeric Range: 3 - 100 Default: none

Table 2-12 (Cont.) Pending Transaction Limiting Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
Onset Threshold Level 3 (%)	When Egress Pending Transactions exceeds this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 3. Onset Threshold Level 3 is ignored if ETG Mode is Limit.	Format: numeric Range: 6 - 100 Default: none
Abatement Threshold Level 3 (%)	When Egress Pending Transactions falls below this percentage of maximum Egress Pending Transactions, the Congestion Level is set to 2. Abatement Threshold Level 3 is ignored if ETG Mode is Limit.	Format: numeric Range: 5 - 100 Default: none
*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: numeric Range: 50 - 10000 Default: 50

2.9.8.2 Adding a Pending Transaction Limiting Configuration Set

Use this task to create a new Pending Transaction Limiting Configuration Sets.

The fields are described in Pending Transaction Limiting Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Pending Transaction Limiting Configuration Sets** on the SOAM or **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Pending Transaction Limiting Configuration Sets** on the NOAM.
2. Click **Insert**.
3. Enter a unique name for the Pending Transaction Limiting Configuration Set in the **Pending Transaction Limiting Configuration Set Name** field.
4. Select or enter the element values.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.8.3 Editing a Pending Transaction Limiting Configuration Set

Use this task to edit an existing Pending Transaction Limiting Configuration Set.

When the Pending Transaction Limiting Configuration Sets page opens, the fields are populated with the currently configured values.

The **Pending Transaction Limiting Configuration Set Name** cannot be edited.

The fields are described in Pending Transaction Limiting Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Pending Transaction Limiting Configuration Sets** on the SOAM or **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Pending Transaction Limiting Configuration Sets** on the NOAM.

2. Select the Pending Transaction Limiting Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.8.4 Deleting a Pending Transaction Limiting Configuration Set

Use this task to delete a Pending Transaction Limiting Configuration Set.

The Default Pending Transaction Limiting Configuration Set can be edited, but cannot be deleted.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Pending Transaction Limiting Configuration Sets** on the SOAM or **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Pending Transaction Limiting Configuration Sets** on the NOAM.
2. Select the Pending Transaction Limiting Configuration Set you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.9.9 Transaction Configuration Sets

A Transaction Configuration Set provides a mechanism to assign routing and transaction attributes (ART, PRT, PAT, and ROS) to Diameter request message based on Application ID and (Extended) Command Code.

You can perform these tasks on an Active System OAM (**SOAM**).

Configuration of Transaction Configuration Sets (TCS) that contain one or more Transaction Configuration Rules is supported. These Transaction Configuration Rules allow the assignment of routing and transaction attributes, for example Routing Option Set (ROS), Pending Answer Timer (PAT), Application Route Table (ART) and Peer Route Table (PRT) to Diameter messages based on Application ID and (Extended) Command Code.

The Transaction Configuration Set fields are described in Transaction Configuration Sets Elements.

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

- Filter the list of Transaction Configuration Sets to display only the desired Transaction Configuration Sets.
- Sort the list by column contents in ascending or descending order by clicking the column heading. The default order is by **Transaction Configuration Set Name** in ascending ASCII order.
- Click **Insert**.
  On the Transaction Configuration Sets [Insert] page, you can add a new Transaction Configuration Set. See Adding a Transaction Configuration Set.

  If the maximum number of Transaction Configuration Sets already exists in the system, an error message displays.
- Select a Transaction Configuration Set Name in the list and click **Edit**.

On the Transaction Configuration Sets [Edit] page, you can edit the selected Transaction Configuration Set. See Editing a Transaction Configuration Set.

If no row is selected, the **Edit** is disabled.

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

2.9.9.1 Transaction Configuration Sets Elements

Table 2-13 describes the fields on the Transaction Configuration Sets View, Edit, and Insert pages. Data input notes apply only to the Insert and Edit pages; the View page is read-only.

> **Note**
>
> If Application ID with an optional Command Code is selected, one of the other four routing attributes (ROS, PAT, ART, PRT) is mandatory.

Table 2-13 includes references to topics where you can define the attributes associated with the selected Transaction Configuration Sets.

Table 2-13 Transaction Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
* Transaction Configuration Set Name	Unique name of the Transaction Configuration Set.	Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
Transaction Configuration Rules	The rules associated with the Transaction Configuration Set Name	Format: Expandable or collapsible list of rules associated with the selected Transaction Configuration Set Name
Application ID	The Application ID in the Diameter message. In the view only screen, the Application ID hyperlinks to the **Diameter**, and then **Configuration**, and then **Application Ids (Filtered)**. **Note**: For more information about the configuration of Application Ids, see Using Application IDs to Identify Diameter Applications.	Format: List Range: List of configured Application IDs Default: not applicable

Table 2-13 (Cont.) Transaction Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
Command Code	The Command code in the Diameter message. In the view only screen, the Application ID hyperlinks to the **Diameter**, and then **Configuration**, and then **Commands Codes (Filtered)**. **Note**: For more information about the configuration of Commands Codes, see Diameter Command Codes.	Format: List Range: List of configured Command Codes Default: not applicable
Routing Option Set	The Routing Options Set associated with the Application ID and Command Code (if specified). In the view only screen, the Application ID hyperlinks to the **Diameter**, and then **Configuration**, and then **Routing Option Sets (Filtered)**. **Note**: For more information about the configuration of Routing Option Sets, see Diameter Routing Option Sets.	Format: List Range: List of configured Routing Option Sets Default: not applicable
Pending Answer Timer	The Pending Answer Time associated with Application ID and Command Code (if specified). In the view only screen, the Application ID hyperlinks to the **Diameter**, and then **Configuration**, and then **Pending Answer Timers (Filtered)**. **Note**: For more information about the configuration of Pending Answer Timers, see Diameter Pending Answer Timers.	Format: List Range: List of configured Pending Answer Timers Default: not applicable
Application Route Table	The Application Route Table associated with Application ID and Command Code (if specified). In the view only screen, the Application ID hyperlinks to the **Diameter**, and then **Configuration**, and then **Application Route Tables (Filtered)**. **Note**: For more information about the configuration of Application Route Tables, see Diameter Application Route Tables.	Format: List Range: List of configured Application Route Tables Default: not applicable

Table 2-13 (Cont.) Transaction Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
Peer Route Table	The Peer Route Table associated with Application ID and Command Code (if specified). In the view only screen, the Application ID hyperlinks to the **Diameter**, and then **Configuration**, and then **Peer Route Tables (Filtered)**. **Note**: For more information about the configuration of Peer Route Tables, see Diameter Peer Route Tables.	Format: List Range: List of configured Peer Route Tables Default: not applicable

2.9.9.2 Adding a Transaction Configuration Set

Use this task to create a new Transaction Configuration Set.

The fields are described in Transaction Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **TransactionConfiguration Sets**.
2. Click **Insert**.
3. Enter a unique name for the Configuration Set in the **Transaction Configuration Set Name** field.
4. Select or enter the element values.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.9.3 Editing a Transaction Configuration Set

Use this task to edit an existing Transaction Configuration Set.

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

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

The fields are described in Transaction Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Transaction Configuration Sets**.
2. Select the Transaction Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.9.4 Deleting a Transaction Configuration Set

Use this task to delete a Transaction Configuration Set.

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

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Transaction Configuration Sets**.
2. Select the Transaction Configuration Set you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.9.10 Traffic Throttle Point Configuration Sets

A TTP Configuration Set defines a set of configuration attributes for a TTP, and can be assigned to one or more TTPs.

You can modify any of the TTP Configuration Sets attributes while the TTP is enabled for service (Throttling Admin State is Enabled).

You can perform these tasks on an Active System OAM (**SOAM**).

You can perform the following actions for Traffic Throttle Point Configuration Sets:

- Filter the list of Traffic Throttle Point Configuration Sets to display only the desired Traffic Throttle Point Configuration Sets.
- Sort the list by column contents in ascending or descending order by clicking the column heading. The default order is by **Traffic Throttle Point Configuration Set Name** in ascending ASCII order.
- Click **Insert**.
  On the Traffic Throttle Point Configuration Sets [Insert] page, you can add a new Traffic Throttle Point Configuration Set. See Adding Traffic Throttle Point Configuration Sets.

  If the maximum number of Traffic Throttle Point Configuration Sets already exists in the system, an error message displays.
- Select a Traffic Throttle Point Configuration Set **Name** in the list. Click **Edit** to display the Traffic Throttle Point Configuration Sets [Edit] page and edit the selected Traffic Throttle Point Configuration Set.
  See Editing Traffic Throttle Point Configuration Sets.

  If no **Name** is selected, **Edit** is disabled.
- Select a Traffic Throttle Point Configuration Set **Name** in the list and click **Delete** to remove the selected Traffic Throttle Point Configuration Set.
  The default Traffic Throttle Point Configuration Set can be edited, but cannot be deleted.
  See Deleting Traffic Throttle Point Configuration Sets.

2.9.10.1 Traffic Throttle Point Configuration Sets Elements

Table 2-14 describes the fields on the Traffic Throttle Point 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 2-14 Traffic Throttle Point Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
* Name	A name of the TTP Configuration Set.	Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
* Abatement Recovery Rate (Percent)	Defines the rate of reduction in loss applied to a TTP when the loss time period has expired.	Format: numeric Range: 1 - 100 Default: 5
Override Message Priority Threshold	This attribute is only accessed during routing and changes to its value do not impact any pending transactions. When a pending transaction is rerouted or when a new transaction is processed, the new attribute value is used. When this parameter is set, messages whose priority is greater than or equal to this value are immune from diversion if the TTP's OTR is below its **Maximum ETR** attribute value. **Note**: If the TTP's OTR is greater or equal to the TTP's Maximum ETR, the only transaction exempt from diversion are NGN-PS transactions with priority=4 (and none of the TTP priority override transactions are exempt from TTP diversion). If the TTP's OTR is less than the TTP's Maximum ETR and you have enabled TTP priority override, then all TTP priority override transactions are also exempt from TTP diversion (as well as NGN-PS transactions).	Format: numeric Range: 1, 2 Default: none
Default Reduction Percentage	The default reduction percentage for a DOIC overload report if the value is not specified.	Format: numeric Range: 0 - 100 Default: 0
* Default Validity Duration	The default validity duration for a DOIC overload report if the value is not specified.	Format: numeric Range: 0 - 86400 Default: 30

Table 2-14 (Cont.) Traffic Throttle Point Configuration Sets Elements

Field (* indicates a required field)	Description	Data Input Notes
* Rate Convergence Time	The time it takes in milliseconds to converge on a per second rate. If the convergence time is less than 1000 milliseconds, the rate is extrapolated. If the convergence time is greater than 1000 milliseconds, the rate is averaged. The rate convergence time is the amount of time it takes for the measured rate to converge on the actual rate.	Format: numeric Range: 250, 500, 1000, 2000 Default: 1000

2.9.10.2 Adding Traffic Throttle Point Configuration Sets

Use this task to create a new Traffic Throttle Point Configuration Set.

The fields are described in Traffic Throttle Point Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Traffic Throttle Point Configuration Sets**.
2. Click **Insert**.
3. Enter a unique name for the **TTP** Configuration Set in the **Name** field.
4. Select or enter the element values.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.10.3 Editing Traffic Throttle Point Configuration Sets

Use this task to edit an existing Traffic Throttle Point Configuration Set.

When the Traffic Throttle Point Configuration Sets page opens, the fields are populated with the currently configured values.

The **Traffic Throttle Point Configuration Set Name** cannot be edited.

The fields are described in Traffic Throttle Point Configuration Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Traffic Throttle Point Configuration Sets**.
2. Select the Traffic Throttle Point Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

2.9.10.4 Deleting Traffic Throttle Point Configuration Sets

Use this task to delete Traffic Throttle Point Configuration Sets.

The default Traffic Throttle Point Configuration Set can be edited, but cannot be deleted.

1. Click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Traffic Throttle Point Configuration Sets**.
2. Select the Traffic Throttle Point Configuration Set you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.10 Diameter Local Nodes

A Local Node is a local Diameter node that is specified with a **realm** and an **FQDN**. When used in conjunction with RADIUS connections, it represents either a RADIUS client or a RADIUS server.

You can perform these tasks on an Active System OAM (**SOAM**).

The Local Node identifies:

- Local Node Name
- Realm
- SCTP Listen Port Number
- TCP Listen Port Number
- DTLS/SCTP Listen Port
- TLS/TCP Listen Port
- Radius UDP Server Ports
- Enable Radius UDP Client Ports
- Radius Client UDP Port Range Start
- Radius Client UDP Port Range End
- Verification Mode
- Certificate Type
- Certificate Name
- Connection Configuration Set
- CEX Configuration Set
- A list of IP addresses available for establishing Diameter transport connections
- Dess Enable
- CA Certificate
- Public Certificate
- Private Key
- Dess Algorithm

After it is configured, a Local Node can be assigned to connections for use in Diameter routing. Select one of the following connection transport configurations:

- SCTP

- DLTS over SCTP
- TCP
- TLS over TCP

For each connection you can select, TCP, SCTP, TLS/TCP or DTLS/SCTP as the security mechanism used to establish that connection to the peer. DTLS is available only for SCTP connections and TLS is available only for TCP connections.

> **Note**
>
> If you select TLS/DTLS, avoid using IPSec. Although IPsec is still supported, you must ensure that a connection does not implement both IPSec and TLS/DTLS, as this would have significant performance impacts.

TLS and DTLS are application layer security protocols that run over TCP and SCTP transport. TLS/DTLS provides tighter encryption via handshake mechanisms, and supports up to 1000 certificates for a node and across the network. TLS/DTLS requires pre-configured certificates/keys that are used during the handshake procedure after transport level connection is established, but before diameter capabilities are exchanged with the peers. The Local Node configuration uses imported certificates/keys and verification mode. If the handshake fails, the connection is not allowed to be established depending on the verification mode associated with the connection.

Note the following restrictions:

- If an attempt is made to edit a Connection and the specified Transport Protocol is DTLS, if the DTLS feature is not activated on the SOAM being used to edit the Connection, an error code is generated and the Connection information is not be updated in the configuration.
- Upon startup, the value of DtlsFeatureEnabled flag defined in DpiOption table is read, and depending on its value, the application does or does not send AUTH Extensions in SCTP_INIT and SCTP_INIT_ACK message while establishing SCTP or DTLS connections.

  > **Note**
  >
  > Any edits to DtlsFeatureEnabled flag defined in DpiOption table after startup do not take effect until the next diameter process restart.

- Client-side or server-side authentication for a TLS/DTLS connection is supported automatically when this is required by peer server or peer client.
- When TLS/DTLS is selected for a diameter-initiated connection, the TLS/DTLS parameters defined by the operator in the local node are applied. The application behavior is related to the local node **Verification Mode** selection.
- When TLS/DTLS is selected for a connection and TLS/DTLS cannot be established either due to a failed key exchange or because the peer does not support TLS/DTLS, the connection is not allowed.
- TLS/DTLS connections initiated by a Diameter peer are responded to. If TLS/DTLS cannot be established due to a failed key exchange, the connection is not allowed. A valid certificate and matching key are required, but you can set the **Verification Mode** to **None** to override this behavior.

- You cannot change the security mechanism selected for a connection while the connection is active.

> **Note**
>
> The algorithm types of CA Certificate, Public Certificate, and Private Key must match with the algorithm configured in Dess Algorithm field.

On the **Diameter**, and then **Configuration**, and then **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 for a Local Node.
- Click **Insert**.

  On the **Diameter**, and then **Configuration**, and then **Local Nodes [Insert]** page, you can add a new Local Node.

  The **Diameter**, and then **Configuration**, and then **Local Nodes [Insert]** page does 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**.

  On the **Diameter**, and then **Configuration**, and then **Local Nodes [Edit]** page, you can edit the selected Local Node.
- Select a Local Node in the list and click **Delete**. You can delete the selected Local Node.

2.10.1 Diameter Local Node Configuration Elements

The following table describes the fields on the Local Nodes View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages, the View page is read-only.

Table 2-15 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 to 32 characters Default: none

Table 2-15 (Cont.) Local Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* 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 Default: none
* FQDN	Unique Fully Qualified Domain Name; specifies exact location in the tree hierarchy of the DNS.	Format: a case-insensitive 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 Default: none
SCTP Listen Port	SCTP listen port number for the Local Node. This SCTP listen port must not be the same as a local initiator port of a connection. Initiator port ranges are divided into user-assigned and DCL (Diameter Transport Layer)-assigned sub-ranges. Note: DCL-assigned sub-ranges are configured through OAM and apply only to connections. DCL is the software layer of the stack that manages Diameter transport connections.	Format: numeric Range: 1024 to 49151 Default: 3868
TCP Listen Port	TCP listen port number for the Local Node. This TCP Listen Port must not be the same as a local initiator port for any connection. Initiator port ranges are divided into user-assigned and DCL (Diameter Transport Layer) -assigned sub-ranges. Note: DCL-assigned sub-ranges is implemented through OAM, and is restricted to connections only. DCL is the software layer of the stack which implements diameter transport connections.	Format: numeric Range: 1024 to 49151 Default: 3868

Table 2-15 (Cont.) Local Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
DTLS/SCTP Listen Port	The DTLS/SCTP listen port number for the Local Node. Datagram Transport Layer Security allows datagram based applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol.	Format: numeric Range: 1024 to 49151 Default: 5658
TLS/TCP Listen Port	The TLS/TCP listen port number for the Local Node. TLS (Transport Layer Security) is an application layer security protocol that runs over TCP transport.	Format: numeric Range: 1024 to 49151 Default: 5658
RADIUS UDP Server Ports	UDP port numbers used by Radius clients when sending Radius messages to the DSR. If no UDP port is specified here, this local node does not receive requests from Radius clients.	Format: numeric Range: 1024 to 49151 Default: none
Enable RADIUS UDP Client Ports	When checked, this local node can send Radius request messages to a Radius server using one of the UDP ports specified in the Radius client UDP port range.	Format: checkbox Range: none Default: unchecked
RADIUS Client UDP Port Range Start	The lowest UDP port number that can be used to send Radius request messages to a remote Radius server. **Note**: If this local node does not share any IP address with any other local node, this local node can use the default client port range start of 2000. However, if this local node shares any IP addresses with one or more local nodes, it can only use the default port range start of 2000 if none of the other local nodes (that share an IP with this local node) overlaps the port range specified for this local node.	Format: numeric Range: 1024 to 49151 Default: 2000 **Note**: Do not use port 5220 as it is already in use by another process.
RADIUS Client UDP Port Range End	The highest UDP port number that can be used to send Radius request messages to a remote Radius server. Note: If this local node does not share any IP address with any other local node, this local node can use the default client port range end of 2499. However, if this local node shares any IP addresses with one or more local nodes, this local node can only use the default port range end of 2499 if none of the other local nodes that share an IP with this local node overlaps the port range specified for this Local Node.	Format: numeric Range: 1024 to 49151 Default: 2499 **Note**: Do not use port 5220 as it is already in use by another process.

Table 2-15 (Cont.) Local Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Verification Mode:	The Certificate Verification Mode for the local node. If TLS/TCP or DTLS/SCTP Port is configured, this field sets the Verification Mode supported by the local node. Available certificate types for configuration.	Format: List Range: • Verify None • Verify Peer • Fail if No Peer Certificate • Verify client Once Default: Verify None
Certificate Type	Available certificate types for configuration. Note: Currently, available for TLS only. Note: This field is required if TLS/TCP or DTLS/SCTP Ports are being used.	Format: List Range: none Default: none
Certificate Name	A list of available X509 TLS security certificates. Note: This field is required if TLS/TCP or DTLS/SCTP Ports are being used.	Format: List Range: none Default: none
* Connection Configuration Set	Connection Configuration set for the local node.	Format: 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**, and then **Configuration**, and then **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: List Range: configured CEX Configuration Sets, Default CEX Configuration Set.

Table 2-15 (Cont.) Local Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* IP Addresses	IP address, or addresses, available for establishing Diameter transport Connections to the local node. User 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: • 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 that the IP address corresponds (for example, TSA# and TSA#-a for alternate IP Addresses where # is the Target Set number. TSAs can be present in either, but do not have to be present at all. If a TSA is selected and Initiator Connection Support is enabled, configuration of a listener to reside within responder port range is enforced. If a TSA is selected and Initiator Connection Support is not enabled and the provided port is out of range (1024 - 49151): – If existing local node [Edit], the operation is allowed with a warning – If new local node [Insert], the operation is denied with an error **Note**: See Adding a Connection for more information. If a combination of TSAs is selected one from a target set with Initiator Connection Support enabled and one without the listener configuration must reside within the responder port range. An error message appears if the connection is configured incorrectly. For the IPFE to differentiate between responder and initiator connections, it	Format: Lists Range: 1 to128 entries Default: none

Table 2-15 (Cont.) Local Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
	checks the destination port of the incoming packet. The IPFE processes the packet according to rules associated with the port range into which the destination port falls. To ensure unambiguous destination ports, diameter routing assigns non-overlapping port ranges.	
Dess Feature	When checked, DESS Feature is enabled.	Format: checkbox Range: none Default: unchecked
CA Certificate	Upload the file in **.pem** format to use in certificate verification.	Format: .pem file extension
Public Certificate	Upload the file in **.pem** format containing the client private key.	Format: .pem file extension
Private Key	Upload the file in **.pem** format containing the public certificate.	Format: .pem file extension
Dess Algorithm	The Dess Algorithm used for this Local Node in DESS Feature.	Format: List Range: • RSA_SHA_256 • EC_DSA_SHA_256 • DSA_SHA_256 Default: RSA_SHA_256

2.10.2 Adding a Local Node

Perform the following procedure to create a new Local Node.

1. Click **Diameter**,**Configuration**,**Local Nodes**.
2. Click **Insert**.
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. Enter an **SCTP Listen Port** number in the field.

   This is the port 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.
7. Enter a **TCP Listen Port** number in the field.

   This is the port 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.
8. Enter a **DTLS/SCTP Listen Port** number in the field.

   This is the port used by connections that use this Local Node to listen for **DTLS/SCTP** request messages. The default 5658 is the well-known IANA port for Diameter traffic.
9. Enter a **TLS/TCP Listen Port** number in the field.

This is the port used by connections that use this Local Node to listen for **TLS/TCP** request messages. The default 5658 is the well-known IANA port for Diameter traffic.

10. Make selections for RADIUS UDP ports and ranges.
11. Select a **Verification Mode** from the list.

    This is establishes the Certificate Verification Mode. If either TLS/TCP or DTLS/SCTP Port is configured, this sets the Verification Mode supported by the Local Node. The default Verify None.
12. Select a **Certificate Type** from the list.

    This establishes the Certificate Types available for configuration. This is mandatory if either of the **TLS/TCP** or **DTLS/SCTP** ports are being used.
13. Select a **Certificate Name** from the list of available X509 TLS Security Certificates.

    This is mandatory if either of the TLS/TCP or DTLS/SCTP ports are being used.
14. Select a **Connection Configuration Set** from the list. If you have not added additional Connection Configuration Sets, only the **Default** Connection Configuration Set is available.
15. Select a **CEX Configuration Set** for the Local Node from the list.

    If you have not added additional CEX Configuration Sets, only the **Default** CEX Configuration Set is available.
16. Select from 1 to 128 IP addresses from the **IP Addresses** list. See Diameter Local Node Configuration Elements for details about this element.
17. If DESS (Diameter End-to-End Security) feature user wants to enable, then check the DESS Feature field.
18. Upload the CA Certificate in `.pem` format only if DESS feature field is enabled.
19. Upload the Private Key in `.pem` format only if DESS feature field is enabled.
20. Upload the Public Certificate in `.pem` only if DESS feature field is enabled.
21. Select the DESS Alogorithm from the list.
22. Click **OK**, **Apply**, .

    For the RADIUS Client UDP Port Range End value, if this Local Node does not share any IP address with any other Local Node, this Local Node can use the default client port range end of 2499. However, if this Local Node shares any IP address(es) with one or more other Local Nodes, this Local Node can only use the default port range end of 2499 if none of the other Local Nodes (that share an IP with this Local Node) overlaps the port range specified for this Local Node. For the RADIUS Client UDP Port Range Start value, if this Local Node does not share any IP address with any other Local Node, this Local Node can use the default client port range start of 2000. However, if this Local Node shares any IP address(es) with one or more other Local Nodes, this Local Node can only use the default port range start of 2000 if none of the other Local Nodes (that share an IP with this Local Node) overlaps the port range specified for this Local Node.

2.10.3 Editing a Local Node

Use this task to edit a Local Node.

When the **Diameter**, and then **Configuration**, and then **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**)
  - **DTLS/SCTP Listen Port**
  - **TLS/TCP Listen Port**
  - **RADIUS UDP Server Ports**
  - **RADIUS UDP Client Ports**
  - **Enable RADIUS UDP Port Range Start**
  - **Enable RADIUS UDP Port Range End**
  - **Verification Mode**
  - **Certificate Type**
  - **Certificate Name**
  - **Connection Configuration Set**
  - **CEX Configuration Set**
- **IP Address** (cannot be removed if there is an Enabled connection, but a new **IP Address** can be added)

1. Click **Diameter**, and then **Configuration**, and then **Local Nodes**.
2. Select the Local Node you want to edit, then click **Edit**.
3. Update the relevant fields.

   For more information about each field, see Diameter Local Node Configuration Elements.

   The value for an entry in a list can be removed by selecting --Select-- in the list, or selecting the X at the end of the list (if an X is available).
4. Click **OK**, **Apply**, or **Cancel**.

2.10.4 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. Click **Diameter**, and then **Configuration**, and then **Local Nodes**.
2. Select the Local Node you want to delete.
3. Click **Delete.**

   A pop up window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.11 Diameter Peer Nodes

A Peer Node can represent either a Diameter Node or a RADIUS Node. When representing a Diameter Node, a **Peer** Node is an external Diameter client, server, or agent with which the application establishes direct transport connections. Qhwn representing a RADIUS Node, a Peer Node may be a single system or a cluster of systems and might have one or more transport connections.

You can perform these tasks on an Active System OAM (**SOAM**).

A Transaction ID is a unique end-to-end transaction ID created by DRL for each unique transaction received from an ingress Peer Node. This value is created when Peer Node routing commences and is stored in the Pending Transaction Record (PTR) for the lifetime of this end-to-end transaction. Its value does not change when the Request message is rerouted. You can apply transaction configuration sets that allow independent grouping of transaction configuration rules for varying use case needs.

If a Route List to route a Request message via a PRT search cannot be located and the message is not addressed to a Peer Node (via the Destination-Host AVP), an attempt is made to perform Implicit Realm Routing. Using the Destination-Realm AVP and Application-Id in the Request message, a matching entry in the system-wide Realm Route Table is sought. This identifies a Route List to use for routing the message. If a match is found, the Route List assigned to the (Realm, Application-Id) is used for routing the message. If a match is not found, transaction routing is abandoned.

Diameter Request messages can only be forwarded to Peer Nodes that support the Application to which the message is addressed (identified by the Application-ID field in the message). The List of Common Application IDs is acquired for elements that contain that connection (for example, Peer Nodes, Route Groups, and Route Lists). When a Connection is no longer a candidate for routing Request messages, the List of Common Application IDs for each Route List, Route Group, and Peer Node which contain this Connection are updated to reflect the potential loss of Application IDs supported by that Connection.

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**.
  On the **Diameter**, **Configuration**, **Peer Nodes [Insert]** page, you can add a new Peer Node.

  The **Diameter**, **Configuration**, and **Peer Nodes [Insert]** does not open if the maximum number of Peer Nodes per Network Element (16000) already exists in the system.
- Select a Peer Node in the list and click **Edit**.

  On the **Diameter**, **Configuration**, and **Peer Notes [Edit]** page, user can edit the selected Peer Node.

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

Redirect Notification Processing and Message Redirection

An egress Peer Node, acting as a Redirect Agent, can send an answer with a redirect notification. The result code in the answer can indicate either diameter redirect or diameter realm redirect. Upon receiving the redirect notification, the configuration dictates how to reroute the request (Redirected Request). If redirect notification is enabled, the redirected request can be started from ART or PRT.

Redirect notifications are processed as follows:

- Redirect notifications with no Redirect-Host-Usage AVP are processed.
- Redirect notifications with Redirect-Host-Usage equal to do not cache are processed.
- Redirect notifications with Redirect-Host-Usage not equal to do not cache are forwarded to the downstream peer.

The following original transaction attributes are carried with the redirected transaction:

- Copy of the original Request message received.
- Connection ID associated with the ingress Request message.
- Information about whether the transaction was initiated by a Peer Node or an application.
- Routing information received from the application.
- The number of times the Request message has been forwarded or rerouted and the Redirected Peer List.
- The message copy related flag, route list ID, or config set ID.
- TTR Event

> **Note**
>
> The Algorithm Types of CA Certificate and Public Certificate must match the algorithm configured in DESS (Diameter End-to-End Security) Algorithm field.

2.11.1 Diameter Peer Node Configuration Elements

The following table describes the fields on the Peer Node's Insert and Edit pages. Data input notes apply only to the Insert and Edit pages.

> **Note**
>
> Any request for a list of peer nodes does not include any dynamically created peer node instances.

When you select peer node from a peer route group, you can specify to exclude peer nodes that have high DOIC loss rate.

Table 2-16 Peer Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Peer Node Name	Unique name of the peer node.	Format: text Range: valid name
AAA Protocol	Specifies the AAA protocol for this peer node, which defines the peer node as diameter or RADIUS.	Format: list Range: diameter or RADIUS Default: NA
* Realm	Realm of the peer node.	Format: text Range: valid realm required
* FQDN	Unique Fully Qualified Domain Name (FQDN); specifies exact location in the tree hierarchy of the DNS.	Format: text Range: valid FQDN required
SCTP Listen Port	SCTP listen port number for the peer node. If the SCTP connection mode is set as **Responder Only**, the port is not considered a listen port and the value 3868 displays in the field.	Format: numeric Range: 1024 to 65535 Default: 3868
TCP Listen Port	TCP listen port number for the peer node. If the TCP connection mode is set as **Responder Only**, the port is not considered a listen port and the value 3868 displays in the field.	Format: numeric Range: 1024 to 65535 Default: 3868
DTLS/SCTP Listen Port	The DTLS/SCTP listen port number for the peer node. If the DTLS/SCTP connection mode is set as **Responder Only**, the port is not considered a listen port and the value 5658 displays in the field. Datagram Transport Layer Security (DTLS) allows datagram based applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol.	Format: numeric Range: 1024 to 65535 Default: 5658

Table 2-16 (Cont.) Peer Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
TLS/TCP Listen Port	The TLS/TCP listen port number for the peer node. If the TLS/TCP connection mode is set as **Responder Only**, the port is not considered a listen port and the value 5658 displays in the field. Transport Layer Security (TLS) is an application layer security protocol that run over TCP transport.	Format: numeric Range: 1024 to 65535 Default: 5658
RADIUS UDP Server Ports	UDP ports that serve (server port) as a destination port for messages from DA-MP to this peer node (representing a RADIUS server). When the peer node is representing a RADIUS server, this represents the UDP ports that can serve as a destination port for requests forwarded by DSR to the RADIUS server. A RADIUS client connection associated with the peer node must select one of these ports as a destination port during connection configuration to have DSR forward requests to the RADIUS server at the selected destination port.	Format: numeric Range: 1024 to 49151 Default: NA
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 Default: NA

Table 2-16 (Cont.) Peer Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Dynamic	Indicates whether or not the peer node was created dynamically (**YES**) or statically (**NO**). **NO** is assigned for all peer node instances, except for those created via dynamic peer discovery. If you attempt to edit a peer node whose dynamic attribute is yes, several of the GUI page attributes are rendered read-only. **Note**:This element does not display on the Peer Nodes [Insert] page.	Format: checkbox (read-only on the Peer Nodes [Edit] page) Range: checked, unchecked Default: unchecked
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**, and then **Configuration**, and then **Route List [Filtered]** page for the selected entry only.	Format: List Range: Configured Route Lists Default: none
Replace Dest Realm	If checked, the destination realm AVP of outgoing messages is overwritten with this peer node realm.	Format: checkbox Range: checked, unchecked Default: unchecked
Replace Dest Host	If checked, the destination host AVP of outgoing messages is overwritten with this peer node FQDN.	Format: checkbox Range: checked, unchecked Default: unchecked
Topology Hiding Status	If enabled, diameter topology hiding is applicable to this peer node. See Diameter Topology Hiding.	Format: list Range: Disabled, Enabled 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 to 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 to 4 Default: 4

Table 2-16 (Cont.) Peer Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Alternate Routing On Connection Failure	Indicates whether to perform alternate routing on alternate connections to the same peer before selecting the next eligible peer of a peer route group, when a connection failure occurs.	Format: options 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: options 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.	Format: options Range: Same Peer, Different Peer Default: different peer
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.	Format: options 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: list Range: Default, Configured Message Priority Configuration Sets Default: -select-
Transaction Configuration Set	A configuration managed object that allows independent grouping of transaction configuration rules for varying use case needs. For example, an ingress peer node can optionally use this configuration for routing and transaction parameters (ART/PRT/ROS/PAT) selection. Up to 100 of such containers are supported for grouping transaction configuration rules.	Format: list Range: Default, Configured Transaction Configuration Sets Default: not selected
Application Route Table	The application route table associated with this peer node. If application route table is set to is **Not Selected**, search default transaction configuration set and apply longest/strongest match. Use ART associated with best match, if any is found.	Format: list Range: Default, Configured Application Route Tables Default: not selected

Table 2-16 (Cont.) Peer Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Peer Route Table	The peer route table associated with the peer node. If peer route table is set to **Not Selected**, search default transaction configuration set and apply longest/strongest match. Use PRT associated with best match, if any is found.	Format: list Range: Default, Configured Peer Route Tables Default: not selected
Ingress Routing Option Set	The routing option set associated with this ingress peer node. If Ingress routing option set is set to **Not Selected**, search default Transaction Configuration Set and apply longest/strongest match. Use ROS associated with best match, if any is found.	Format: 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**, search default Transaction Configuration Set and apply longest/strongest match. Use PAT associated with best match, if any is found.	Format: list Range: Default, Configured Pending Answer Timers Default: not selected
Peer Node Group Name	A group of peer nodes that share common characteristics and attributes. This group is used by IPFE for peer node group aware connection distribution.	Format: unique string, case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 to 32 characters
AVP Removal List	The AVP removal list associated with this peer node.	See Diameter AVP Removal Lists .
Answer On Any Connection	Defines whether an Ingress Answer message on any connection from a Peer Node is supported or not. If enabled for a Peer Node, then DSR processes the Ingress Diameter Answer message received on any connection from the same upstream Peer to which the Egress Diameter Request message was sent. If disabled for a Peer Node, then DSR abandons the Diameter Answer message received on a different connection from the one on which the request was sent to the peer.	Format: checkbox Range: checked, unchecked Default: unchecked

Table 2-16 (Cont.) Peer Node Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Ignore Priority From Peer	If checked, Ignore priority from prior state can be changed only if DRMP or NGN-PS is enabled. If DRMP and NGN-PS both are **Disabled**, then Ignore priority from prior is not changed.	Format: checkbox Range: checked, unchecked Default: unchecked
Traffic Throttle Point	The number of TTPs associated with the peer node.	See Diameter Traffic Throttle Points.
Dess Feature	When checked, DESS Feature is enabled.	Format: checkbox Range: none Default: unchecked
CA Certificate	Upload the file in .pem format to use in certificate verification.	Format: .pem file extension
Public Certificate	Upload the file in .pem format containing the client private key.	Format: .pem file extension
Dess Algorithm	The Dess Algorithm used for this Peer Node in DESS Feature.	Format: List Range: • RSA_SHA_256 • EC_DSA_SHA_256 • DSA_SHA_256 Default: RSA_SHA_256
Action on Verification Failure	The action performed on verification failure.	Format: List Range: • SendError • SilentlyDiscardError Default: SendError

2.11.2 Adding a Peer Node

Perform the following procedure to create a new Peer Node:

1. Click **Diameter**, **Configuration**, and **Peer Nodes**.
2. Click **Insert**.
3. Enter a unique name for the Peer Node in the **Peer Node Name** field.
4. Make a selection for AAA Protocol.
5. Enter the **Realm**.
6. Enter a **FQDN**.
7. Enter a **SCTP Listen Port** number.

   If the SCTP connection mode is configured as **Initiator** or **Initiator & Responder**, then the port listens to SCTP connections. If the SCTP connection mode is set as **Responder Only**, the port is not considered a listen port and the value 3868 displays in the field.
8. Enter a **TCP Listen Port** number.

   If the TCP connection mode is configured as **Initiator** or **Initiator & Responder**, then the port listens to TCP connections. If the TCP connection mode is set as **Responder Only**, the port is not considered a listen port and the value 3868 displays in the field.

9. Enter a **DTLS/SCTP Listen Port** number.

   If the **DTLS/SCTP** connection mode is configured as **Initiator** or **Initiator & Responder**, then the port listens to **DTLS/SCTP** connections. If the **DTLS/SCTP** connection mode is set as **Responder Only**, the port is not considered a listen port and the value 5658 displays in the field.

10. Enter a **TLS/TCP Listen Port** number.

    If the **TLS/TCP** connection mode is configured as **Initiator** or **Initiator & Responder**, then the port listens to **TLS/TCP** connections. If the **TLS/TCP** connection mode is set as **Responder Only**, the port is not considered a listen port and the value 5658 displays in the field.

11. Enter a **RADIUS UDP Server Port**.

12. Enter an **IP Addresses**.

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

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

    To add another IP Address, click **Add** and enter the IP Address in the new text box. See Table 2-16 for limitations on the number of IP addresses you can add.

13. Select a **Alternate Implicit Route** from the list.

    This field is optional. This Route List is used for routing if a message does not match any of the configured Peer Routing Rules and implicit routes are exhausted.

14. To overwrite the Destination Realm of outgoing messages to the peer with the Peer Realm, click **Replace Dest Realm** checkbox (a checkmark appears in the box).

15. To overwrite the Destination Host of outgoing messages to the peer with the Peer Node's FQDN, click the **Replace Dest Host** checkbox.

16. In the **Minimum Connection Capacity** text box, enter the minimum number of Connections that must be Available for the Peer to be Available.

17. In the **Maximum Alternate Routing Attempts** text box, enter the maximum number of times that a Request can be rerouted to this Peer.

18. Select from the options in **Alternate Routing on Connection Failure** to indicate whether or not to perform alternate routing to the same or a different Peer when a Connection failure occurs.

19. Select from the options in **Alternate Routing on Answer Timeout** 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.

20. Select from the options in **Alternate Routing on Answer Result Code** to indicate whether or not to perform alternate routing to the same or a different Peer when a Reroute on Answer Result Code occurs.

21. Select from the options in **Message Priority Setting** to indicate the source of message priority for request messages arriving on Connections associated with the Peer Node.

22. If Message Priority Setting is set to **User Configured**, specify the **Message Priority Configuration Set** that is used to determine message priority.

23. Select a **Transaction Configuration Set** from the list.

    This allows independent grouping of transaction configuration rules for varying use case needs.

24. Select the **Application Route Table** for this Peer Node. See Selecting Peer Node Application Route Tables for selection criterion.
25. Select the **Peer Route Table** to specify which Peer Routing Rules are used when routing messages from the Peer Node. See Selecting Peer Node Peer Route Tables for selection criterion.
26. Select the **Ingress Routing Option Set** to specify which options are used for this ingress Peer Node. See Selecting Peer Node Ingress Routing Option Sets for selection criterion.
27. A Pending Transaction Timer limits the time DRL waits for an Answer response after forwarding a Request message to an upstream Peer Node. When this time-limit is exceeded, DRL abandons invoke message rerouting. Select the **Egress Pending Answer Timer** to specify how long diameter waits for a response from the Peer Node. When DRL selects a viable Connection for forwarding a Request message to an upstream Peer Node, it determines which Pending Answer Timer value to use based on the following precedence selection rules, highest to lowest priority. See Selecting Peer Node Egress Pending Answer Timers for selection criterion.
28. To support an Ingress Answer message on any connection from a Peer Node, click **Answer On Any Connection** checkbox (a checkmark appears in the box).
29. If ignore priority from Peer feature is to be provisioned, check the **Ignore Priority From Peer** checkbox (a checkmark appears in the box).
30. If DESS (Diameter End-to-End Security) feature user wants to enable, then check the Dess Feature field.
31. Upload the CA Certificate in `.pem` format only if Dess feature field is enabled.
32. Upload the Public Certificate in `.pem` only if Dess feature field is enabled.
33. Select the Dess Alogorithm from the list.
34. Select the **Action performed on Verification Failure**.
35. Click **OK** or **Apply**.

2.11.2.1 Selecting Peer Node Application Route Tables

Use this task to select Peer Node Application Route Tables.

1. Click **Diameter**, and then **Configuration**, and then **Peer Nodes**.
2. Select the **Application Route Table** for this Peer Node.

   Select the **Application Route Table** as per the following precedence selection criterion, highest to lowest priority.

   - This only applies when the Request message was received from a routing application. The ART is provided by the application via an Application-Data stack event parameter if it exists.
   - If the message is a Redirected Request, the ART provided by **System Options**, and then **Redirect Application Route Table** is used if it exists. As described here, when the message is a Redirected Request, the DRL selects the configured **System Options**, and then **Redirect Application Route Table**. If it is not configured, no ART is searched (ART processing skipped).
   - The ART provided by an Application Routing Rule with an action of Forward to ART if it exists.
   - Otherwise:

- If Transaction Configuration Set is selected on the ingress Peer Node from which the Diameter Request was received, use Transaction Configuration Set and apply longest/strongest match search criteria for Diameter Request message parameters comparison and if a match is found, the ART assigned to the Transaction Configuration Rule defined under this Transaction Configuration Set is applied if it exists.
- The ART assigned to the ingress Peer Node from which the Request message was received if it exists.
- Search Default TCS and apply longest/strongest match. Use ART associated with best match if any is found.
- Default ART.

2.11.2.2 Selecting Peer Node Peer Route Tables

Use this task to select Peer Node Peer Route Tables.

1. Click **Diameter**, and then **Configuration**, and then **Peer Nodes**.
2. Select the **Peer Route Table** to specify which Peer Routing Rules are used when routing messages from the Peer Node. Select the **Peer Route Table** as per the following precedence selection criterion, highest to lowest priority.
   - This only applies when the Request message was received from a routing application. The PRT provided by the application, if it exists, via an Application-Data stack event parameter.
   - Only applies when routing a Redirect Request. The **System Options**, and then **Redirect Peer Route Table** if it exists.
   - The PRT provided by an Application or Peer Routing Rule with an action of Forward to PRT if it exists.
   - If Transaction Configuration Set is selected on ingress Peer Node from which the Diameter Request was received, use Transaction Configuration Set and apply longest/strongest match search criteria for Diameter Request message parameters comparison and if a match is found, apply PRT assigned to the Transaction Configuration Rule defined under this Transaction Configuration Set if it exists.
   - The PRT assigned to the ingress Peer Node from which the Request message was received if it exists.
   - Search Default TCS and apply longest/strongest match. Use PRT associated with best match if any is found.
   - Default PRT.

2.11.2.3 Selecting Peer Node Ingress Routing Option Sets

Use this task to select Peer Node Ingress Routing Option Sets.

1. Click **Diameter**, and then **Configuration**, and then **Peer Nodes**.
2. Select the **Ingress Routing Option Set** to specify which options are used for this ingress Peer Node, as per the following precedence selection criterion, highest to lowest priority.
   - If Transaction Configuration Set is selected on ingress Peer Node from which the Diameter Request was received, use Transaction Configuration Set and apply longest/strongest match search criteria for Diameter Request message parameters comparison and if a match is found, apply ROS assigned to the Transaction Configuration Rule defined under this Transaction Configuration Set, if it exists.

- The ROS assigned to the ingress Peer Node from which the Request message was received, if it exists.
- Search Default TCS and apply longest/strongest match. Use ROS associated with best match, if any is found.
- Default ROS.

2.11.2.4 Selecting Peer Node Egress Pending Answer Timers

Use this task to select Peer Node Ingress Routing Option Sets.

1. Click **Diameter**, and then **Configuration**, and then **Peer Nodes**.
2. Select the **Egress Pending Answer Timer** to specify how long Diameter waits for a response from the Peer Node. When DRL selects a viable Connection for forwarding a Request message to an upstream Peer Node, it determines which Pending Answer Timer value to use based on the following precedence selection rules, highest to lowest priority. A Pending Transaction Timer limits the time that DRL waits for an Answer response after forwarding a Request message to an upstream Peer Node. When this time-limit is exceeded, DRL abandons Invoke Message Rerouting.
   - If Transaction Configuration Set is selected on ingress Peer Node from which the Diameter Request was received, use Transaction Configuration Set and apply longest/strongest match search criteria for Diameter Request message parameters comparison and if a match is found, apply PAT assigned to Transaction Configuration Rule defined under this Transaction Configuration Set, if it exists.
   - The Pending Answer Timer assigned to the Routing Option Set for the Ingress Peer, if it exists.
   - The Pending Answer Timer assigned to the egress Peer Node to which the Request message is forwarded, if it exists.
   - Default Pending Answer Timer.

   If Pending Answer Timer is set to **Not Selected**, the Egress Pending Answer Timer configured for the Application ID contained in the message is used.
   A Pending Answer Timer with a value > 10 seconds is considered a Long Timeout Pending Answer Timer. Long Timeout Pending Answer Timers are intended for Diameter Applications that can have long transaction times (for example: SLg). Because Requests assigned to Long Timeout Pending Answer Timers might hold internal resources (for example, PTRs, PDUs) for extended periods, this traffic uses a separate PTR Pool from standard Diameter traffic. It is expected that a very small percentage (< 2%) of overall traffic would be assigned to Long Timeout Pending Answer Timers, and users should configure the smallest timeout value acceptable based on the overall transaction path.
3. Click **OK**, **Apply**, or **Cancel**.

2.11.3 Editing a Peer Node

Use this task to edit a Peer Node.

When the **Diameter**, and then **Configuration**, and then **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
- 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**
  - **DTLS/SCTP Listen Port**
  - **TLS/TCP Listen Port**
  - **RADIUS UDP Server Ports**
  - **RADIUS UDP Client Ports**
  - **Enable RADIUS UDP Port Range Start**
  - **Enable RADIUS UDP Port Range End**
  - **AAA Protocol**

1. Click **Diameter**, and then **Configuration**, and then **Peer Nodes**.
2. Select the Peer Node you want to edit.
3. Click **Edit**.
4. Update the relevant fields.

   For more information about each field please see Diameter Peer Node Configuration Elements.
   An entry in a list can be removed by selecting --Select-- in the list, or selecting the X at the end of the list (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.

   Responder only connections associated with a Peer Node are not considered listen ports (SCTP, TCP, TLS, or DTLS).
5. Click **OK**, **Apply**, or **Cancel**.

   If you attempt to edit a Peer Node instance whose Dynamic attribute is **YES**, the following Peer Nodes attributes are rendered read-only:

   - **Realm**
   - **FQDN**
   - **SCTP Listen Port**
   - **TCP Listen Port**
   - **DTLS/SCTP Listen Port**
   - **TLS/TCP Listen Port**
   - **IP Addresses**
   - **Minimum Connection Capacity**

2.11.4 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

> **Note**
>
> You cannot delete dynamically created Peer Nodes.

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.

> **Note**
>
> The removal of Diameter Overload Indication Conveyance (**DOIC**) AVPs takes place at a peer node level.

1. Click **Diameter**, and then **Configuration**, and then **Peer Nodes**.
2. Select the Peer Node you want to delete.
3. Click **Delete**.
4. Click **OK** or **Cancel**.

2.12 Diameter Peer Node Groups

A Peer Node Group is a collection of peer nodes that cannot tolerate multiple failures within the collection. The participating peer nodes are configured in a **Peer Node Group** container to indicate that connections, which are initiated from peers in the group, are distributed across multiple DA-MPs of an IPFE Target Set. In order for the IPFE to be aware of Peer IP addresses, Peer Nodes in a Peer Node Group must be configured with one or more Peer IP addresses. Target sets can only be configured to support IPFE Initiator Connection support when its DA-MPs listening ports are within the new responder port range.

You can perform these tasks on an Active System OAM (SOAM).

The Peer Node Group Aware Least Load function spreads the connections from peer nodes; thus, reducing the negative impact if a single DA-MP fails. You can configure Peer Node Groups by using the GUI or through the Bulk Import and Export function. See the Bulk Import and Export information in the *Diameter Common User's Guide*.

> **Note**
>
> Peer Nodes can belong to one Peer Node Group at a time.

On the **Diameter**, and then **Configuration**, and then **Peer Node Groups** page, you can perform the following actions:

- Filter the list of Peer Node Groups to display only the desired Peer Node Groups.
- View the Peer Node Name associated with a Peer Node Group Name.

- Sort the list by a column in ascending or descending order by clicking the column heading. The default order is by **Peer Node Group Name** in ascending ASCII order.
- Click an entry shown in blue in a column to open the **Diameter**, and then **Configuration**, and then **<Component> [Filtered]** page and display that entry only.
- Click **Insert**.
  On the **Diameter**, and then **Configuration**, and then **Peer Node Groups [Insert]** page, you can add a new Peer Node Group.

  The **Diameter**, and then **Configuration**, and then **Peer Node Groups [Insert]** does not open if the maximum number of Peer Node Groups per Network Element (16000) already exist in the system.
- Select a Peer Node Group in the list and click **Edit**.

  On the **Diameter**, and then **Configuration**, and then **Peer Node Groups [Edit]** page, you can edit the selected Peer Node Group.
- Select a Peer Node Group in the list and click **Delete**. You can delete the selected Peer Node Group.

2.12.1 Diameter Peer Node Groups configuration elements

Table 2-17 describes the fields on the Peer Node Groups View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 2-17 Peer Node Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
*Peer Node Group Name	Unique name of the Peer Node Group. This is a group of Peer Nodes that share common characteristics and attributes. This group is used by IPFE for Peer Node Group Aware connection distribution. View - Each Peer Node Group entry displays a + sign and the number of Peer Nodes assigned to that Peer Node Group. Click the + sign to display the Peer Node names; the + sign changes to a - sign. Click the - sign to display the number again.	Format: string, case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters Default: none

Table 2-17 (Cont.) Peer Node Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Peer Node Name	A list of Peer Nodes (identified by their IP addresses), used by the IPFE for Peer Node Group Aware connection distribution. Connections from IP addresses in this list can be distributed across DA-MPs in a TSA to avoid having a single point of failure. **Note**: Peer Nodes that share an IP address must be in the same Peer Node Group. [Insert] and [Edit] - The field contains an **Add** button that can be clicked to create text boxes for Peer Node names. Each entry is numbered to indicate the number of Peer Node names that have been added.	Format: List that includes the names of all Peer Nodes hat have not been included in a different Peer Node Group yet Range: configured Peer Node names Default: -Select- The list of Peer Node Names are hyperlinks. Click on a hyperlink to view more detail on the selected Peer Node. **Note**: If the maximum number (2500) of Peer Node Groups has already been created, then an error displays.

2.12.2 Adding Peer Node Groups

Use this task to create new Peer Node Groups.

1. Click **Diameter**, and then **Configuration**, and then **Peer Node Groups**.
2. Click **Insert**.
3. Enter a unique name for the Peer Node Group Name in the **Peer Node Group Name** field.
4. Select a Peer Node Name from the **Peer Node Name** list.

   To add another Peer Node Name, click **Add** and select a Peer Node Name in the new text box.
5. Click **OK**, **Apply**, or **Cancel**.

   The following conditions exist:

   - You can only specify Peer Nodes whose Dynamic attribute is **NO** to be selected for inclusion in a Peer Node Group.
   - Peer Nodes created by the Dynamic Peer Discovery feature cannot be included by any Peer Node Group instance.
   - If you attempt to insert or update a Peer Node Group instance and the specified Peer Node whose Dynamic attribute value is **YES**.
   - Peer Route Groups are always statically configured; no statically configured instance can refer to a dependent GUI element that was added to the configuration as a result of Dynamic Peer Discovery.

2.12.3 Editing Peer Node Groups

Use this task to edit a Peer Node Group.

When the **Diameter**, and then **Configuration**, and then **Peer Node Groups [Edit]** screen opens, the fields are initially populated with the current values for the selected Peer Node Group.

1. Click **Diameter**, and then **Configuration**, and then **Peer Node Groups**.
2. Select the Peer Node Group you want to edit, and click **Edit**.

> **Note**
>
> The Peer Node Group Name field is read-only on this page.

3. Update the relevant fields.

   For more information about each field, see Table 2-17.
4. Click **OK**, **Apply**, or **Cancel**.

   The following conditions exist:

   - You can only specify Peer Nodes whose Dynamic attribute is **NO** to be selected for inclusion in a Peer Node Group.
   - Peer Nodes created by the Dynamic Peer Discovery feature cannot be included by any Peer Node Group instance.
   - Peer Route Groups are always statically configured; no statically configured instance can refer to a dependent GUI element that was added to the configuration as a result of Dynamic Peer Discovery.

2.12.4 Deleting Peer Node Groups

Use this task to delete a Peer Node Group.

> **Note**
>
> Deleting a Peer Node Group removes the references to the Peer Node Group from the Peer Node. It does not remove the Peer Nodes themselves.

Before you perform this task, remove all Peer Nodes from the group **Edit**.

1. Click **Diameter**, and then **Configuration**, and then **Peer Node Groups**.
2. Select the Peer Node Group you want to delete.
3. Click **Delete**.
4. Click **OK** or **Cancel** on the confirmation screen.

2.13 Diameter Peer Node Alarm Groups

A Peer Node Alarm Group is a group of peer nodes used to configure throttle and abatement threshold values for minor, major, and critical severity.

You can perform these tasks on an Active System OAM (SOAM).

You can configure Peer Node Alarm Groups by using the GUI function.

On the **Diameter**, and then **Configuration**, and then **Peer Node Alarm Groups** page, you can perform the following actions:

- Filter the list of Peer Node Alarm Groups to display only the desired Peer Node Alarm Groups.
- View the Peer Node Name associated with a Peer Node Alarm Group Name.
- Sort the list by a column in ascending or descending order by clicking the column heading. The default order is by **Peer Node Alarm Group Name** in ascending ASCII order.
- Click **Insert**.
  On the **Diameter**, and then **Configuration**, and then **Peer Node Alarm Groups [Insert]** page, you can add a new Peer Node Alarm Group.
- Select a Peer Node Alarm Group in the list and click **Edit**.

  On the **Diameter**, and then **Configuration**, and then **Peer Node Alarm Groups [Edit]** page, you can edit the selected Peer Node Alarm Group.
- Select a Peer Node Alarm Group in the list and click **Delete**. You can delete the selected Peer Node Alarm Group.

2.13.1 Diameter Peer Node Alarm Groups configuration elements

Table 2-18 describes the fields on the Peer Node Alarm Groups View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 2-18 Peer Node Alarm Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
*Peer Node Alarm Group Name	Unique name of the Peer Node Alarm Group. This is a group of Peer Nodes used by the Alarm Group feature if it is enabled on the **System Options**, and then **General Options**tab.	Format: string, case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters Default: none
*Peer Node Name	A list of Peer Nodes. [Insert] and [Edit] - The field contains an **Add** button that can be clicked to create text boxes for Peer Node names. Each entry is numbered to indicate the number of Peer Node names that have been added.	Format: List that includes the names of all Peer Nodes that have not been included in a different Peer Node Alarm Group yet Range: configured Peer Node names The list of Peer Node Names are hyperlinks. Click on a hyperlink to view more detail on the selected Peer Node. **Note**: If the maximum number (200) of Peer Nodes Groups has already been created, then an error displays.

Table 2-18 (Cont.) Peer Node Alarm Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
*Throttle Minor Threshold (%)	This percentage value indicates the number of peers failed out of total number of peers configured for that Peer Node Alarm Group. When the count of failed peers reaches the minor throttle level, a minor threshold alarm is raised. The following constraints apply to the value: • Throttle Minor Threshold > Abatement Minor Threshold • Throttle Minor Threshold < Throttle and Abatement Major Threshold • Throttle Minor Threshold < Throttle and Abatement Critical Threshold	Format: numeric Range: 2 - 96 Default: 25
*Abatement Minor Threshold (%)	This percentage value indicates the number of peers failed out of total number of peers configured for that Peer Node Alarm Group. When the count of failed peers falls under the minor abatement level, a minor threshold alarm is cleared. The following constraints apply to the value: • Abatement Minor Threshold < Throttle Minor Threshold • Abatement Minor Threshold < Throttle and Abatement Major Threshold • Abatement Minor Threshold < Throttle and Abatement Critical Threshold	Format: numeric Range: 1 - 95 Default: 20
*Throttle Major Threshold (%)	This percentage value indicates the number of peers failed out of total number of peers configured for that Peer Node Alarm Group. When the count of failed peers reaches the major throttle level, a major threshold alarm is raised. The following constraints apply to the value: • Throttle Major Threshold > Throttle and Abatement Minor Threshold • Throttle Major Threshold > Abatement Major Threshold • Throttle Major Threshold < Throttle and Abatement Critical Threshold	Format: numeric Range: 4 - 98 Default: 50

Table 2-18 (Cont.) Peer Node Alarm Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
*Abatement Major Threshold (%)	This percentage value indicates the number of peers failed out of total number of peers configured for that Peer Node Alarm Group. When the count of failed peers falls under the major abatement level, major threshold alarm is cleared. The following constraints apply to the value: • Abatement Major Threshold > Throttle and Abatement Minor Threshold • Abatement Major Threshold < Throttle Major Threshold • Abatement Major Threshold < Throttle and Abatement Critical Threshold	Format: numeric Range: 3 - 97 Default: 45
*Throttle Critical Threshold (%)	This percentage value indicates the number of peers failed out of total number of peers configured for that Peer Node Alarm Group. When the count of failed peers reaches the critical throttle level, critical threshold alarm is raised. The following constraints apply to the value: • Throttle Critical Threshold > Throttle and Abatement Minor Threshold • Throttle Critical Threshold > Throttle and Abatement Major Threshold • Throttle Critical Threshold > Abatement Critical Threshold	Format: numeric Range: 6 - 100 Default: 75
*Abatement Critical Threshold (%)	This percentage value indicates the number of peers failed out of total number of peers configured for that Peer Node Alarm Group. When the count of failed peers falls under the critical abatement level, critical threshold alarm is cleared. The following constraints apply to the value: • Abatement Critical Threshold > Throttle and Abatement Minor Threshold • Abatement Critical Threshold > Throttle and Abatement Major Threshold • Abatement Critical Threshold < Throttle Critical Threshold	Format: numeric Range: 5 - 99 Default: 70

2.13.2 Adding Peer Node Alarm Groups

Use this task to create new Peer Node Alarm Groups

1. Click **Diameter**, and then **Configuration**, and then **Peer Node Alarm Groups**.
2. Click **Insert**.
3. Enter a unique name for the Peer Node Group Alarm Name in the **Peer Node Group Alarm Name** field.
4. Select a Peer Node Name from the **Peer Node Name** list.

   To add another Peer Node Name, click **Add** and select a Peer Node Name in the new text box.
5. Enter the Minor Threshold Throttle and Abatement percentages, Major Threshold Throttle and Abatement percentages, and Critical Threshold Throttle and Abatement percentages.
6. Click **OK**, **Apply**, or **Cancel**.

2.13.3 Editing Peer Node Alarm Groups

Use this task to edit a Peer Node Alarm Group.

When the **Diameter**, and then **Configuration**, and then **Peer Node Alarm Groups [Edit]** screen opens, the fields are initially populated with the current values for the selected Peer Node Alarm Group.

1. Click **Diameter**, and then **Configuration**, and then **Peer Node Alarm Groups**.
2. Select the Peer Node Alarm Group you want to edit, and click **Edit**.

   > **Note**
   >
   > The Peer Node Alarm Group Name field is read-only on this page.
3. Update the relevant fields.

   For more information about each field, see Table 2-18.
4. Click **OK**, **Apply**, or **Cancel**.

2.13.4 Deleting Peer Node Alarm Groups

Use this task to delete a Peer Node Alarm Group.

> **Note**
>
> Deleting a Peer Node Alarm Group removes the references to the Peer Node Group from the Peer Node. It does not remove the Peer Nodes themselves.

1. Click **Diameter**, and then **Configuration**, and then **Peer Node Alarm Groups**.
2. Select the Peer Node Alarm Group you want to delete.
3. Click **Delete**.

4. Click **OK** or **Cancel** on the confirmation screen.

2.14 Connections

A connection provides the reliable transport connectivity between Diameter nodes.

You can perform these tasks on an Active System OAM (**SOAM**).

A connection:

- Can use the SCTP, TCP, TLS/TCP or DTLS/STCP 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**, and then **Configuration**, and then **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.
- Click **Insert**.

  On the **Diameter**, and then **Configuration**, and then **Connections [Insert]** page, you can add a new Connection.

  The **Diameter**, and then **Configuration**, and then **Connections [Insert]** does 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**.

  On the **Diameter**, and then **Configuration**, and then **Connections [Edit]** page, you can change the configuration of the selected Connection.

  If the selected Connection is not in the Disabled Admin State, the **Diameter**, and then **Configuration**, and then **Connections [Edit]** page does not open.

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

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

  See IPFE Connections and Capacity Validation for more information.

2.14.1 IPFE Connections and Capacity Validation

You can perform these tasks on an Active System OAM (**SOAM**).

IPFE Connections

IPFE supports the following connection types:

- Initiator only - indicates that Local Node only initiates the connection to the Peer Nodes.
- Responder only - indicates that Local Node only responds to the connection initiated from the Peer Node.
- Initiator & Responder - indicates that Local Node initiates the connection in addition to responding to connections initiated from the Peer Node.

> **Note**
>
> Only IPFE Diameter connections are supported at this time.

Fixed connections are configured with a static DA-MP IP address, where the connections are established on a specific DA-MP.

IPFE Initiator connections, the target set address, is the source address. It provides additional flexibility in assigning and using IP address efficiently in your configuration.

The default is Initiator & Responder provides additional flexibility and allows you to use any port within a configurable range on any DA-MP within a TSA to initiate connections.

IPFE connections are configured with a public TSA IP address and a static listening port, and IPFE Initiator connections are configured with a static initiator DA-MP and a public TSA IP address and a user-selected or automatically selected static initiator port.

The IPFE Initiator port range division depends on the connection type (fixed or floating IPFE) and the selection method (user-configured or system-selected).

> **Note**
>
> When overall connection counts are calculated, RADIUS connections are treated like fixed connections.

Port ranges for IPFE initiator connections are 1024-49151. You cannot configure a port range outside of this range; the GUI generates a message and corresponding explanation.

Port ranges for floating IPFE responder connections are 1024-49151.

> **Note**
>
> You cannot select a port value for IPFE responder, as diameter does not initiate these types of connections.

Port ranges for IPFE initiator and responder connections are 1024-49151 and are fully utilizable by initiator and responder connections. The port range management (port broker)

functionality manages ports, which avoids conflicts across Initiator and Responder connections. Only one initiator and responder connection per Diameter Peer Node is supported.

> **Note**
>
> Port Number flexibility combines the Responder and Initiator Port Ranges into one large port range. It also eliminates per DA-MP port ranges and port ranges set aside for user input or DCL.

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.

> **Note**
>
> All message types contribute to the ingress MPS rate of the connection; however, only routable request messages are subject to discard or reject actions.

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 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 an IPFE Initiator 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 IPFE Initiator Connection support to a new Target Set
- Converting a Fixed Connection to IPFE Initiator Connection support, or vice versa
- Assigning a different MP Profile to a configured DA-MP

An error displays, 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 displays 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 displays.

If a Responder Only connection is created without a Peer Node IP Address and **Transport FQDN** is selected, **Transport FQDN** is required even though it is not applicable.

The **Diameter**, and then **Configuration**, and then **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 Functions.

2.14.2 Diameter Connection Configuration Elements

Table 2-19 describes the fields on the Connections Edit and Insert pages. Data input notes only apply to the Insert and Edit pages.

> **Note**
>
> Any request for a list of connections does not include any dynamically-created connection instances.

When you select a connection route groups, you can specify to pass over connections that have too high of a DOIC loss rate.

If an element is not applicable to RADIUS connections (AAA protocol is RADIUS), the element is greyed out.

> **Note**
>
> If you attempt to add or edit RADIUS connections, you cannot set values for the Local Initiate Port, Alternate Local IP Address, IPFE Initiator DAMP, Alternate Peer IP Address, Transport FQDN, CEX Configuration Set, Transport Congestion Abatement Timeout, Remote Busy Usage, Remote Busy Abatement Timeout, Message Priority Setting, Message Priority Configuration Set, Suppress Connection Unavailable Alarm, Suppress Connection Attempts, and Test Mode fields.

> **Note**
>
> If you attempt to add or edit Diameter connections, you cannot set values for the Shared Secret Configuration Set, Message Authenticator Configuration Set, Status-Server Configuration Set, and UDP Port fields.

Table 2-19 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: field Range: 1 - 32 characters

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
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. If AAA protocol is selected as RADIUS, only UDP is offered. 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 • When the target set is configured to be TCP_AND_SCTP, then both TCP and SCTP connections are allowed. **Note**: Do not enable IPSEC if the connection is configured with TLS/TCP or DTLS/SCTP protocol; enabling both IPSEC and TLS/TCP or DTLS/SCTP is not recommended as this would have significant performance impact.	Format: options Range: SCTP, TCP, TLS/TCP, DTLS/SCTP, UDP Default: SCTP
* AAA Protocol	The AAA protocol for this connection, which defines the connection as diameter or RADIUS.	Format: List Range: Diameter, RADIUS Default: blank

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* 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**, and then **Configuration**, and then **Local Nodes [Filtered]** page, which shows only the selected entry. If two IP addresses are configured for the local node, it is recommended that an alternate IP Address be configured for the peer node. The peer's alternate IP address is used as a fallback for the initiation of the SCTP connection establishment if the peer's 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: List Range: all configured local nodes Default: blank

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Connection Mode	The connection can have one of the following connection modes: • Initiator Only - indicates the local node initiates the connection to the peer node. **Note**: If a initiator only connection is created and a TSA selected, check if IPFE initiator connection support is enabled on the target set. – If yes, allow IPFF initiator connection support. You must select from the DA-MP's port range if you want to explicitly configure the initiator port. – If no, IPFE initiator connection support is not allowed. • **Responder Only** - indicates the local node only responds to the connection initiated from the peer node. The local initiate port field is not available when the responder only is selected here. **Responder Only** connections associated with a Peer Node are not considered listen ports (SCTP, TCP, TLS, or DTLS). • **Initiator & Responder** - indicates the local node initiates a connection to the peer node and responds to connection initiations from the peer node. When configured with a TSA and as initiator & responder, the DA-MP uses the TSA as the source IP address for initiating connections and for all subsequent signaling traffic over that connection. • RADIUS Server - indicates that the DSR receives incoming RADIUS requests from a peer node that is a RADIUS client. • RADIUS Client - indicates that the DSR sends RADIUS requests to a peer node that is a RADIUS Server.	Format: List Range: diameter: initiator only, responder only, initiator & responder RADIUS: RADIUS server, RADIUS client Default: initiator & responder

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
	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 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	

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
	FQDN (from peer nodes configuration), peer Realm (from peer nodes configuration), transport protocol, local IP pair, local listen port (from local nodes configuration), Must Include application IDs in the CEX Configuration Set. • If the **Connection Mode** is **Initiator & Responder** and **Peer Node Identification** is **Transport FQDN** or **Peer Diameter Identity FQDN** for any connections to the peer, then the following combination must be unique for each connection to the peer: peer FQDN (from peer nodes configuration), peer Realm (from peer nodes configuration), transport protocol, local IP pair, local listen port (from local nodes configuration), Must Include application IDs in the CEX Configuration Set. • If the **Connection Mode** is **Initiator & Responder** and **Transport FQDN** is NOT specified in any connections to the peer, then the following combination must be unique for each connection the 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.	
Dynamic	Indicates whether or not the element was created dynamically (**YES**) or statically (**NO**). **NO** is assigned for all element instances, except for those created via Dynamic peer Discovery.	Format: checkbox (read-only on the element [Edit] page) Range: checked (the element was created as a result of Dynamic Discovery), unchecked Default: unchecked

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
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**. Initiator port ranges are divided into automatically assigned and DCL-assigned sub-ranges. Depending on the type of initiator connection, fixed or IPFE, there are two or more user/DCL sub-ranges. DCL (Diameter Transport Layer) is the software layer of the stack which implements diameter transport connections. If the connection remains fixed, a warning is generated if the configured port is out of range for an initiator connection type. If you convert the fixed initiator connection to an IPFE initiator connection, you must select from the DA-MP's port range if you want to explicitly configure the initiator port. See Connection Capacity Dashboard Functions for more information about fixed and IPFE initiator connections.	Format: numeric Range: 1024-49151 Default: Blank
UDP Port	For RADIUS Server connections, this is the UDP port on which the DSR expects to receive incoming RADIUS requests for this connection. For RADIUS Client connections, this is the UDP port at the destination peer node that receives the RADIUS request sent by the DSR.	Format: List Range: local (RADIUS server connections) or peer node (RADIUS client connections) UDP port numbers Default: blank
IP Owner	Identifies the DA-MP that owns this connection attribute. Each RCL instance ignores connection attributes that are not exclusively assigned to its local DA-MP.	Format: read-only Range: IP owner Default: blank

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Local IP Address	The IP address to be used as local node Address for this connection. A local node must be selected before the list becomes available, containing the IP Addresses corresponding to the selected local node. When configuring diameter TCP connections, only MP static IP addresses, TSAs and alternate TSAs can be selected as the local IP Address. If an IPFE alternate target set Address (selected from the local node's IP Address list) is assigned to the local IP Address of a diameter connection, then the alternate local IP Address selection is disabled. In this case, a Uni-homed connection is configured, but using the target set's alternate IP address as the only local IP Address for the connection. Uni-homed and multi-homes are applicable only to SCTP/Diameter connections; they are not applicable to RADIUS/UDP connections. When configuring RADIUS connections, only MP static IP addresses can be selected as local IP Address. Each IP address in the list has an identifying tag appended to it, as follows: • In Active/Standby DA-MP NEs, a DA-MP VIP is appended with (VIP). • In Multiple-Active DA-MP NEs, a static IP address owned by the DA-MP is appended with the Server Hostname of the DA-MP, for example, (DA-MP1). • IPFE target set Addresses are appended with the target set Name, for example, (TSA1). • For each IPFE connection listed on the View screen, the local IP Address field displays (TSA# or TSA#-a) after the IP address, where #	Format: List Range: all configured IP addresses for the selected local node Default: blank

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
	is the target set number and -a is an alternate TSA.	
Alternate Local IP Address	The IP address to be used as the alternate 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. **Note**: SCTP can be selected as a protocol only for diameter connections. IPFE target set Addresses are appended with the target set Name, for example, (TSA1). If an IPFE target set Address (selected from the local node's IP Address list) is assigned to the local IP Address of a diameter connection, then the only valid selection for the alternate local IP Address is the corresponding IPFE alternate target set Address (for example: if TSA1 is assigned to a local IP address of a diameter connection, then the only valid selection for the alternate local IP Address is TSA1-a. This address is used only for SCTP Multi-homing; it must be different from the selected local IP Address. An IPFE TSA and an alternate TSA cannot be identical. **Note**: SCTP can be selected as a protocol only for diameter connections.	Format: List Range: all configured IP addresses for the selected local node Default: blank

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
IPFE Initiator DAMP	The IPFE initiator DA-MP for this connection. When the addition of a new floating IPFE connection is being validated, OAM validates that the addition of the floating IPFE connection does not cause, for each DA-MP in the subject target set, the total number of connections allocated to the DA-MP, to exceed the DA-MP's total capacity. If the available capacity on one or more DA-MPs in the subject target set is less than zero and any DA-MP in the subject target set is included in more than one target set, OAM allows the floating IPFE connection to be added, but also issues a warning message. If the validation fails and the subject target set does not overlap any other target set, OAM computes the available capacity for the entire subject target set (by computing available capacity for each DA-MP and summing them). If the target set available capacity is less than zero, the validation fails and an error code is generated.	Format: List Range: available DA-MP IP addresses configured for the TSA selected for local IP Address Default: blank or IPFE initiator DA-MP
* 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**, and then **Configuration**, and then **Peer Nodes [Filtered]** page which shows only the selected entry.	Format: List Range: all configured peer nodes Default: blank

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Peer Node Identification	Specifies how the peer node's IP address(es) is derived when initiating a connection to the peer, and whether the peer node's IP address(es) is validated when responding to a connection from the peer. Transport FQDNs use the remote IP address(es) configured for this connection when initiating a connection to the peer, and to validate the peer node's IP address(es) when responding to a connection from the peer. Use the remote IP address(es) configured for this connection when initiating a connection to the peer and to validate the peer node's IP address(es) when responding to a connection from the peer. If no IP Address has been selected and no transport FQDN has been specified, then the only accepted choice is peer diameter identity FQDN. Use **None** for this connection when responding to a connection from the peer and do not validate the peer node's IP address(es). Use the DNS resolved FQDN address configured for the peer node associated with this connection when initiating a connection to the peer, and do not validate the peer node's IP address(es) when responding to a connection from the peer. 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 list is available. • If the peer node Identification is set to transport FQDN, then the peer IP Address list is not available and the transport FQDN field can be changed. • If the peer node Identification is set to peer diameter	Format: options Range: None, IP Address Default: IP Address

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
	Identity FQDN, then both the transport FQDN field and the peer IP Address list is not available.	
Peer IP Address	The IP Address to be used as the peer node address for this connection. A peer node must be selected before the list becomes available, containing the IP Addresses of the selected peer node.	Format: List Range: available IP addresses Default: blank
Alternate Peer IP Address	The IP Address to be used as the alternate peer node address for this connection. A peer 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 peer node. This address is used only for SCTP Multi-homing; it must be different from the selected peer IP Address.	Format: List Range: available IP addresses Default: blank
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. If a responder only connection is created without a peer node IP Address and **Transport FQDN** is selected, transport FQDN is required even though it is not applicable. In this case, an error code is generated (when using **Transport FQDN** with initiator connections.	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: List Range: all configured connection Configuration Sets, Default connection Configuration Set. Default: blank

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
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: List Range: all configured CEX Configuration Sets, "Default" CEX Configuration Set. Default: blank
* Capacity Configuration Set	Capacity Configuration Set associated with the connection. The Capacity Configuration Set defines reserved and maximum ingress message processing rates and alarms thresholds for this connection. The entries in the Capacity Configuration Set field are links to the Capacity Configuration Sets (Filtered) page, which displays only the selected entry. The addition of any connection having non-zero Reserved Ingress MPS is subject to capacity validation rules, which are discussed in the connection Capacity Validation content. See the MP Profiles information in *Diameter Common User's Guide*.	Format: List 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

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* 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: 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 the connection is considered BUSY from the last time a DIAMETER_TOO_BUSY response was received.	Format: numeric Range: 3 - 60 seconds Default: 5 seconds
Message Priority Setting	Defines the source of Message Priority for a Request message arriving on the connection. Possible settings are: • blank - 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: options Range: blank, Read from Request Message, User Configured Default: blank
Message Priority Configuration Set	The Message Priority Configuration set used if Message Priority Setting is User Configured	Format: List Range: all configured Message Priority Configuration Sets Default: blank

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
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: List Range: all configured Egress Message Throttling Configuration Sets Default: blank
Shared Secret Configuration Set	The Shared Secret Configuration Set used for this connection. (RADIUS only)	Format: List Range: all configured Shared Secret Configuration Sets Default: -Select-
Message Authenticator Configuration Set	The Message Authenticator Configuration Set used for this connection. (RADIUS only)	Format: List Range: all configured Message Authenticator Configuration Sets Default: -Select-
Message Conversion Configuration Set	The Message Conversion Configuration Set MO assigned to this RADIUS connection. (RADIUS only)	Format: list Range: blank Default: -Select-
Ingress Status-Server Configuration Set	The Ingress Status-Server Configuration Set used for this connection. (RADIUS only)	Format: List Range: all configured Ingress Status-Server Configuration Sets Default: -Select-
Suppress Connection Unavailable Alarm	If checked, this suppresses the connection attempts on the unavailable connections when a connection attribute is configured and turned ON for the connection object, then the connection unavailable alarm on those connections is not raised.	Format: checkbox Range: checked (YES) or unchecked (NO) Default: unchecked
Suppress Connection Attempts	If checked, suppresses the connection attempts when a diameter peer nodes status becomes available. This attribute is not applicable for responder only connection modes. It is only applicable for initiator only and initiator and responder connection modes. With any configuration edit action that results in connection mode to responder only mode, the attribute value is returned to the default value.	Format: checkbox Range: checked (YES) or unchecked (NO) Default: unchecked

Table 2-19 (Cont.) Connections Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Test Mode	If checked, the connection is in Test Mode.	Format: checkbox Range: checked (YES), not checked (NO) Default: not checked

2.14.3 Adding a Connection

Use this task to create a new Connection. The fields and configuration considerations are described in Diameter Connection Configuration Elements.

1. Click **Diameter**, and then **Configuration**, and then **Connections**.
2. Click **Insert**.

   The **Diameter**, and then **Configuration**, and then **Connections [Insert]** does 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.

   > **Note**
   >
   > You cannot configure routes for OAM from the Network routes screen of the DSR GUI.

3. Enter a unique name for the Connection in the **Connection Name** field.
4. Select a **AAA Protocol**.
5. Select an option 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.

6. Select a **Local Node** from the 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.

7. Select the **Connection Mode** from the list. See Diameter Connection Configuration Elements.

   Responder Only connections associated with a Peer Node are not considered listen ports (SCTP, TCP, TLS, or DTLS).

8. If you set up the Connection Mode for Initiator Only, you can optionally enter a **Local Initiate Port** number in the field.
9. Select the **Local IP Address** from the list.
10. If the Transport Protocol is set to SCTP, then select the **Alternate Local IP Address** of this Connection from the list.

11. Select a **IPFE Initiator DAMP** from the list.

    This step is only needed for IPFE Initiator connections.

12. Select a **Peer Node** from the list.

    Initiator port ranges are divided into user-assigned and DCL-assigned sub-ranges. Depending on the type of initiator connection, fixed or Floating IPFE, there are two or more user/DCL sub-ranges. 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.
    Diameter Transport Layer (DCL) is the software layer of the stack which implements diameter transport connections.

13. Select from the options in **Peer Node Identification** field.

14. If needed, select the Peer IP Address of this Connection from the **Peer IP Address** list.

15. If needed, select the Alternate Peer IP Address of this Connection from the **Alternate Peer IP Address** list.

16. If needed, enter a **Transport FQDN** for this Connection.

17. Select a **Connection Configuration Set** from the list.

18. If one is needed, select a **CEX Configuration Set** from the list .

19. If the Per Connection Ingress MPS Control feature is active in the system, select a **Capacity Configuration Set** from the list.

20. Specify the **Transport Congestion Abatement Timeout**.

21. Select a **Remote Busy Usage** setting from the list.

22. If you selected Enabled or Host Override for Remote Busy Usage, set the **Remote Busy Abatement Timeout** value.

23. Select from the options in **Message Priority Setting** field.

24. If you selected **User Configured** as the Message Priority Setting, select a **Message Priority Configuration Set** from the list.

25. Make selections from the **Egress Message Throttling Configuration Set**, **Shared Configuration Set**, **Message Authenticator Configuration Set**, and **Ingress Status-Server Configuration Set** lists.

26. Click the **Suppress Connection Unavailable Alarm** check box to suppress the Connection unavailable alarm.

27. Click the **Suppress Connection Attempts** check box to suppress the Connection attempts to a standby Peer Node, c

28. Click **Test Mode** check box to the test Connection.

29. Click **OK**, **Apply**, or **Cancel**.

30. Use the Enabling Connections procedure to enable the new connection.

    The following conditions exist:

    - Only Peer Nodes whose Dynamic attribute is **NO** can be selected for assignment to a connection.
    - Peer Nodes created by the Dynamic Peer Discovery feature cannot be assigned to any statically created connection.
    - CEX Configuration Sets created by the Dynamic Peer Discovery feature cannot be assigned to any statically created connection.

2.14.4 Editing a Connection

Use this task to edit an existing Connection.

1. Verify the Connection to be edited is in the Disabled Admin State. See how to disable a connection in Disabling Connections.
2. Click **Diameter**, and then **Configuration**, and then **Connections**.
3. Select the Connection you want to edit.
4. Click **Edit**.

   The edit page does not open if any of the following conditions exist:

   - The selected Connection no longer exists.
   - The Connection is not in the Disabled Admin state.
5. Update the relevant fields.

   See the Connection configuration elements description in Diameter Connection Configuration Elements. The **Connection Name** cannot be edited.

   > **Note**
   >
   > Uncheck the Test Mode checkbox to change from test connection to normal connection. You cannot reverse this action.

   Selecting the X at the end of a field clears the field. You can enter or select another value.
6. Click **OK**, **Apply**, or **Cancel**.

   The following conditions exist:

   - Any request for a list of Connections does not include any dynamically created Connection instances.
   - Dynamic Peer Discovery can insert a connection instance whose Dynamic attribute is set to **YES** only.
   - Dynamic Peer Discovery software can delete a Connection instance whose Dynamic attribute is set to **YES** only.
   - If you attempt to edit a Connection whose Dynamic attribute set to **NO**, the Edit page only allows Peer Nodes and CEX Configuration Sets whose own Dynamic attribute set to **NO** the assigned Connection.
   - If you attempt to edit a Connection whose Dynamic attribute set to **YES**, the Edit page only allows CEX Configuration Sets whose own Dynamic attribute set to **NO** the assigned Connection. A Connection whose Dynamic attribute set to **YES** or **NO** the assigned Connection.
   - If you attempt to edit a Connection whose Dynamic attribute set to **YES**, the selection options for Connection Mode does not include **Responder Only**.
7. Use the Enabling Connections procedure to enable the edited Connection.

2.14.5 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. Click **Diameter**, and then **Configuration**, and then **Connections**.
2. Select the Connection you want to delete.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click**OK**, **Apply**, or **Cancel**.

2.15 Diameter Connection Alarm Groups

A Connection Alarm Group is a group of connections used to configure throttle and abatement threshold values for minor, major, and critical severity.

You can perform these tasks on an Active System OAM (SOAM).

You can configure Connection Alarm Groups by using the GUI.

On the **Diameter**, and then **Configuration**, and then **Connection Alarm Groups** page, you can perform the following actions:

- Filter the list of Connection Alarm Groups to display only the desired Connection Alarm Groups.
- View the Connection Name associated with a Connection Alarm Group Name.
- Sort the list by a column in ascending or descending order by clicking the column heading. The default order is by **Connection Alarm Group Name** in ascending ASCII order.
- Click **Insert**.
  On the **Diameter**, and then **Configuration**, and then **Connection Alarm Groups [Insert]** page, you can add a new Connection Alarm Group.
- Select a Connection Alarm Group in the list and click **Edit**.

  On the **Diameter**, and then **Configuration**, and then **Connection Alarm Groups [Edit]** page, you can edit the selected Connection Alarm Group.
- Select a Connection Alarm Group in the list and click **Delete**. You can delete the selected Connection Alarm Group.

2.15.1 Diameter Connection Alarm Groups configuration elements

Table 2-20 describes the fields on the Connection Alarm Groups View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 2-20 Connection Alarm Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
*Connection Alarm Group Name	Unique name of the Connection Alarm Group. This is a group of Connections used by the Alarm Group feature if it is enabled on the **System Options**, and then **General Options** tab.	Format: string, case-sensitive; alphanumeric and underscore (_); cannot start with a digit and must contain at least one alpha Range: 1 - 32 characters Default: none
*Connection Name	A list of Connections. [Insert] and [Edit] - The field contains an **Add** button that can be clicked to create text boxes for Connection names. Each entry is numbered to indicate the number of Connection names that have been added.	Format: List that includes the names of all Connections that have not been included in a different Connection Alarm Group yet Range: configured Connection names The list of Connection Names are hyperlinks. Click on a hyperlink to view more detail on the selected Connection. **Note**: If the maximum number (200) of Connections has already been created, then an error displays.
*Throttle Minor Threshold (%)	This percentage value indicates the number of connections failed out of total number of connections configured for that Connection Alarm Group. When the count of failed connections reaches the minor throttle level, minor threshold alarm is raised. The following constraints apply to the value: • Throttle Minor Threshold > Abatement Minor Threshold • Throttle Minor Threshold < Throttle and Abatement Major Threshold • Throttle Minor Threshold < Throttle and Abatement Critical Threshold	Format: numeric Range: 2 - 96 Default: 25

Table 2-20 (Cont.) Connection Alarm Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
*Abatement Minor Threshold (%)	This percentage value indicates the number of connections failed out of total number of connections configured for that Connection Alarm Group. When the count of failed connections falls under the minor abatement level, minor threshold alarm is cleared. The following constraints apply to the value: • Abatement Minor Threshold < Throttle Minor Threshold • Abatement Minor Threshold < Throttle and Abatement Major Threshold • Abatement Minor Threshold < Throttle and Abatement Critical Threshold	Format: numeric Range: 1 - 95 Default: 20
*Throttle Major Threshold (%)	This percentage value indicates the number of connections failed out of total number of connections configured for that Connection Alarm Group. When the count of failed connections reaches the major throttle level, major threshold alarm is raised. The following constraints apply to the value: • Throttle Major Threshold > Throttle and Abatement Minor Threshold • Throttle Major Threshold > Abatement Major Threshold • Throttle Major Threshold < Throttle and Abatement Critical Threshold	Format: numeric Range: 4 - 98 Default: 50

Table 2-20 (Cont.) Connection Alarm Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
*Abatement Major Threshold (%)	This percentage value indicates the number of connections failed out of total number of connections configured for that Connection Alarm Group. When the count of failed connections falls under the major abatement level, major threshold alarm is cleared. The following constraints apply to the value: • Abatement Major Threshold > Throttle and Abatement Minor Threshold • Abatement Major Threshold < Throttle Major Threshold • Abatement Major Threshold < Throttle and Abatement Critical Threshold	Format: numeric Range: 3 - 97 Default: 45
*Throttle Critical Threshold (%)	This percentage value indicates the number of connections failed out of total number of connections configured for that Connection Alarm Group. When the count of failed connections reaches the critical throttle level, critical threshold alarm is raised. The following constraints apply to the value: • Throttle Critical Threshold > Throttle and Abatement Minor Threshold • Throttle Critical Threshold > Throttle and Abatement Major Threshold • Throttle Critical Threshold > Abatement Critical Threshold	Format: numeric Range: 6 - 100 Default: 75

Table 2-20 (Cont.) Connection Alarm Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
*Abatement Critical Threshold (%)	This percentage value indicates the number of connections failed out of total number of connections configured for that Connection Alarm Group. When the count of failed connections falls under the critical abatement level, critical threshold alarm is cleared. The following constraints apply to the value: • Abatement Critical Threshold > Throttle and Abatement Minor Threshold • Abatement Critical Threshold > Throttle and Abatement Major Threshold • Abatement Critical Threshold < Throttle Critical Threshold	Format: numeric Range: 5 - 99 Default: 70

2.15.2 Adding Connection Alarm Groups

Use this task to create new Connection Alarm Groups

1. Click **Diameter**, and then **Configuration**, and then **Connection Alarm Groups**.
2. Click **Insert**.
3. Enter a unique name for the Connection Group Alarm Name in the **Connection Group Alarm Name** field.
4. Select a Connection Name from the **Connection Name** list.

   To add another Connection Name, click **Add** and select a Connection Name in the new text box.
5. Enter the Minor Threshold Throttle and Abatement percentages, Major Threshold Throttle and Abatement percentages, and Critical Threshold Throttle and Abatement percentages.
6. Click **OK**, **Apply**, or **Cancel**.

2.15.3 Editing Connection Alarm Groups

Use this task to edit a Connection Alarm Group.

When the **Diameter**, and then **Configuration**, and then **Connection Alarm Groups [Edit]** screen opens, the fields are initially populated with the current values for the selected Connection Alarm Group.

1. Click **Diameter**, and then **Configuration**, and then **Connection Alarm Groups**.
2. Select the Connection Alarm Group you want to edit, and click **Edit**.

> **Note**
>
> The Connection Alarm Group Name field is read-only on this page.

3. Update the relevant fields.

   For more information about each field, see Table 2-20.

4. Click **OK**, **Apply**, or **Cancel**.

2.15.4 Deleting Connection Alarm Groups

Use this task to delete a Connection Alarm Group.

> **Note**
>
> Deleting a Connection Alarm Group removes the references to the Connection. It does not remove the Connections themselves.

1. Click **Diameter**, and then **Configuration**, and then **Connection Alarm Groups**.
2. Select the Connection Alarm Group you want to delete.
3. Click **Delete**.
4. Click **OK** or **Cancel** on the confirmation screen.

2.16 Diameter Route Groups

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.

> **Note**
>
> Connection Route Groups is not supported for RADIUS connections, but can be configured with all RADIUS or all Diameter Peer Nodes.

You can perform these tasks on an Active System OAM (**SOAM**).

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 is forwarded to Peer Node A and 60% of the messages is forwarded to Peer Node B.

Each Route Group can be assigned a maximum of 512 Connections. Route Groups are assigned to Route Lists.

> **Note**
>
> Route Groups created via Dynamic Peer Discovery cannot be assigned to any statically-created Route List.

On the **Diameter**, and then **Configuration**, and then **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.
- Click **Insert**.

  On the **Diameter**, and then **Configuration**, and then **Route Groups [Insert]** page, you can add a new Route Group.

  The **Diameter**, and then **Configuration**, and then **Route Groups [Insert]** does 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**.

  On the **Diameter**, and then **Configuration**, and then **Route Groups [Edit]** page, you can edit the selected Route Group.

  If the selected Route Group has been deleted by another user, the **Diameter**, and then **Configuration**, and then **Route Groups [Edit]** page does not open.
- Select a Route Group in the list and click **Delete**. You can delete the selected Route Group.

2.16.1 Diameter Route Group Configuration Elements

Route Group 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.

> **Note**
>
> Any request for a list of route groups does not include any dynamically created route group instances.

When you select a Peer Node from a Peer Route Group or Connections from a Connection Route Group, you can specify to pass over Connections that have too high of a DOIC loss rate.

Table 2-21 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 to 32 characters; cannot start with a digit and must contain at least one alpha.
Dynamic (View)	Indicates whether or not the route group was created dynamically (Yes) or statically (No).	Format: text Range: Yes, No Default: NA

Table 2-21 (Cont.) Route Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
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: options 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 **DiameterConfiguration{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 + sign to display the Peer Nodes or Connections; the + sign changes to a - sign. Click - sign to display the number again.
* Peer Node, Connection, and Provisioned Capacity	One entry defined for a Route Group.	Up to 512 entries can be configured for a Connection Route Group. Click **Add** to insert another entry for the Route Group.
Peer Node	A Peer Node associated with the Route Group. Each Route Group can be assigned up to 512 Peer Nodes. The Peer Node field is available when the Peer Route Group option is selected in the Type field. The Peer Node field is required.	Format: List Range: 1 to 512 configured Peer Nodes.
Connection	A connection associated with the Route Group. Each Route Group can be assigned up to 512 connections. The Connection field is available when the Connection Route Group option is selected in the Type field and a Peer Node is selected. The Connection field is required for Connection Route Groups.	Format: List Range: 1 to 512 configured Connections for the selected Peer Node.

Table 2-21 (Cont.) Route Groups Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Provisioned Capacity	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 and Connections in a Route Group proportional to the configured capacity for the Peer Node and Connection. A Peer Node and Connection with a higher capacity is assigned more traffic.	Format: numeric Range: 1 to 65535
Traffic Measurement	Traffic measurements can be enabled for up to 250 Route Groups including peer and connection route groups.	Format: options Range: Enabled, Disabled Default: Disabled

2.16.2 Adding a Route Group

Use this task to create a new Route Group.

1. Click **Diameter**, and then **Configuration**, and then **Route Groups**.
2. Click **Insert**.
3. Enter a unique name for the Route Group in the **Route Group Name** field.
4. Enable or disable traffic measurements in a route group by setting **Traffic Measurement**.
5. Select the **Type** option for the entries included in the Route Group (Peer Nodes or Connections).
6. 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** list.
   b. If the **Connection Route Group** option is selected for the **Type** field, then select a Connection assigned to the selected Peer Node from the **Connection** list.
   c. Enter the **Provisioned Capacity** for the selected Peer Node or Connection.
7. 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 6 for this next entry. Up to 512 entries can be provisioned for Connection Route Groups.
   - If you do not want to add another entry, continue with step 8.
8. Click **OK**, **Apply**, or **Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, then 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 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

The following conditions exist:

- You can only assign Peer Nodes whose Dynamic attribute is **NO** to a Route Group of either type (Peer Node or Connection). Peer Nodes created via Dynamic Peer Discovery cannot be assigned to any statically-created Route Group.
- Peer Nodes created by the Dynamic Peer Discovery cannot be assigned to any statically-created Route Group.
- You can only allow Connections whose Dynamic attribute is **NO** to a Route Group of type Connection Route Group.
- Connections created by the Dynamic Peer Discovery feature may not be assigned to any statically-created Connection Route Group.

2.16.3 Editing a Route Group

Use this task to make changes to a Route Group.

When the **Diameter**, and then **Configuration**, and then **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.

> **Note**
>
> When editing a Route Group, you can add only allow Peer Nodes whose Dynamic attribute is **NO** be selected for assignment to a Route Group of either type (Peer Node or Connection).

1. Click **Diameter**, and then **Configuration**, and then **Route Groups**.
2. Select the Route Group you want to edit.
3. Click **Edit**.

   The page is initially populated with the current configured values for the selected route group.

   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 list or by clicking the X at the end of the Provisioned Capacity list 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** 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 Diameter Route Group Configuration Elements.

5. Click **OK**, **Apply**, or **Cancel**.

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

   - If you attempt to add or edit a Route Group instance whose Dynamic attribute is **YES**.
   - If you attempt to insert or edit a static Route Group or Connection Route Group of either type (Peer or Connection), and one or more of the Peer Nodes supplied in the desired configuration has a Dynamic attribute a value of **YES**.
   - If you attempt to edit a static Route Group instance by changing its Dynamic attribute from NO to YES or vice-versa.
   - If you attempt to delete a Route Group instance whose Dynamic attribute is **YES**.
   - 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 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 following conditions exist:

   - When editing a Route Group, you can only add Connections whose Dynamic attribute is **NO** be selected for assignment to a Connection Route Group.
   - Connections created via Dynamic Peer Discovery cannot be assigned to any statically-created Connection Route Group.
   - A value of NO is assigned for the Dynamic attribute for all Route Group instances being inserted with the exception of instances added via Dynamic Peer Discovery.
   - Dynamic Peer Discovery can only delete a Route Group instance whose Dynamic attribute is **YES**.

2.16.4 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. Click **Diameter**, and then **Configuration**, and then **Route Groups**.
2. Select the Route Group you want to delete.
3. Click **Delete**.

   A popup window appears.

4. Click **OK** or**Cancel**.

   If **OK** is clicked and the selected Route Group is referenced by at least one Route List, then 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), then an error message appears and the Route Groups view is refreshed.

2.17 Diameter Route Lists

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 five Route Groups.

You can perform route lists tasks on an Active System OAM (**SOAM**).

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 5 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 directs the Diameter message to a Peer Node in the active Route Group.

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

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

On the **Diameter**, and then **Configuration**, and then **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).
- Click **Insert**.

  On the **Diameter**, and then **Configuration**, and then **Route Groups [Insert]** page, you can add a new Route List.

  The **Diameter**, and then **Configuration**, and then **Route Groups [Insert]** page does 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**.

On the **Diameter**, and then **Configuration**, and then **Route Lists [Edit]** page, you can edit the selected Route List.

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

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

2.17.1 Diameter Route List Configuration Elements

The Diameter Route List Configuration Elements describes the fields on the Route Lists View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages, the View page is read-only.

> **Note**
>
> Any request for a list of Routes does not include dynamically created route instances.

When user selects route groups from a route list, user can specify to exclude route groups with a DOIC loss rate that exceeds the threshold.

Table 2-22 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
Dynamic	Indicates whether or not the element was created dynamically (**YES**) or statically (**NO**). **NO** is assigned for all element instances, except for those created via Dynamic Peer Discovery.	Format: checkbox (read-only on the Element [Edit] page) Range: checked (the element was created as a result of Dynamic Discovery), unchecked Default: unchecked
* 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
Destination-Host	Destination-Host of this Route List.	Format: text Range: valid Destination-Host
Destination-Realm	Destination-Realm of this Route List.	Format: text Range: valid Destination-Realm
Origin-Host	Origin-Host of this Route List.	Format: text Range: valid Origin-Host
Origin-Realm	Origin-Realm of this Route List.	Format: text Range: valid Origin-Realm

Table 2-22 (Cont.) Route Lists Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* Route Group	Route Groups associated with the Route List. Up to five 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**, and then **Configuration**, and then **Route Groups [Filtered]**> page for the selected Route Group.	Format: List Range: available Route Groups
* Priority	The priority of the Route Group within the Route List. Priority is set from 1 (highest priority) to 5 (lowest priority).	Format: numeric Range: 1, 2, or 5
* Route Group	Route Groups associated with this Route List.	Format: List Range: 1 - 5 entries Default: NA
Site Name	Site Name whose TTG is to be selected to associate with the Route Group.	Format: List Range: Local Site Only Default: NA
Traffic Throttle Group	Traffic Throttle Group configured in the Site selected (all local TTGs if local site is selected and TTG marked as shared if remote site is selected).	Format: List Range: NA Default: NA
Maximum Loss Percent Threshold	Maximum Loss Percent Threshold for the combination of Route List, Route Group and Traffic Threshold Group	Format: List Range: 0 - 100 Default: NA

2.17.2 Adding a Route List

Perform the following procedure to create a new Route List:

> **Note**
>
> User must have at least one Route Group configured before you can create a Route List.

1. Click **Diameter**, **Configuration**, **Route Lists**.

2. Click **Insert**.
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. Enable or disable routing across alternate Route Groups in Route List by setting **Route Across Route Groups**.
6. Enter the Destination-Host.
7. Enter the Destination-Realm.
8. Enter the Origin-Host.
9. Enter the Origin-Realm.
10. Select one to five Route Groups from the **Route Group** lists. For each Route Group you specify, select a **Site Name**, **Traffic Throttle Group**, and **Maximum Loss Percent Threshold**.

    The **Site Name** list includes the local SOAM (assuming that at least one TTG has been configured).

    > **Note**
    >
    > **Traffic Throttle Group** is disabled until a **Site Name** is selected.

11. Click **OK**, **Apply**, or **Cancel**.

    If **OK** or **Apply** is clicked and any of the following conditions exist, one of the 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 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.

2.17.3 Editing a Route List

Use this task to make changes to existing Route Lists.

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

> **Note**
>
> If Dynamic (read-only checkbox) is checked, it means that the route list was created as a result of Dynamic Peer Discovery.

1. Click **Diameter**, and then **Configuration**, and then **Route Lists**.
2. Select the **Route List** you want to edit.
3. Click **Edit**.

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 Diameter Route List Configuration Elements.

5. Click **OK**, **Apply**, or **Cancel**.

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

   - If you attempt to edit a Route List instance whose Dynamic attribute is **YES**, a warning message displays, but the edit operation is allowed to proceed. Editing a dynamic route is allowed, but changes are lost to this Route List if the Realm to which the Route List is associated is dynamically re-discovered in the future.
   - If you attempt to delete a Route List instance whose Dynamic attribute is **YES**.
   - If you attempt to insert or edit a static Route List, one or more of the Route Groups supplied in the desired configuration has for its own Dynamic attribute a value of **YES**.
   - If youattempt to change one or more read-only attributes.

     > **Note**
     >
     > When editing a Route List instance whose Dynamic attribute is **YES**, all Route List attributes are treated as read-only except for Route Across Route Groups.

   - If you attempt to edit a static Route List instance by changing its Dynamic attribute from **NO** to **YES** or vice-versa.
   - If youattempt to add a Route List instance and the Dynamic attribute is **YES**. A Route List instanceDynamic attribute must be **YES** to be inserted using Dynamic Peer Discovery.
   - 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

2.17.4 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. Click **Diameter**, and then **Configuration**, and then **Route Lists**.
2. Select the **Route List** you want to delete.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

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

2.18 Diameter Peer Route Tables

A Peer Route Table is a set of prioritized Peer Routing Rules that DRL searches with the content of a Request message received from Diameter Nodes and applications to determine how to route the message to a Peer Node.

You can perform these tasks on an Active System OAM (**SOAM**).

Users can assign Peer Route Table (PRT) to Diameter messages based on Application ID and (Extended) Command Codes by configuring Transaction Configuration Rule (TCR) with Application ID plus (E)CC as a key in Transaction Configuration Sets.

On the **Diameter**, and then **Configuration**, and then **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**.

  On the **Diameter**, and then **Configuration**, and then **Peer Route Tables [Insert]** page, you can add a new Peer Route Table.

  The **Diameter**, and then **Configuration**, and then **Peer Route Tables [Insert]** page does not open if

  – The maximum number of Peer Route Tables (500) already exists in the system.
- Select a Peer Route Table in the list and click **View/Edit Rules**.
  On the Viewing Rules for Peer Route Table page, you can select a Rule Name to work with.

  If the selected Peer Route Table has been deleted by another user, the Viewing Rules for Peer Route Table page does not open.
- Select a Peer Route Table in the list and click **Delete**. You can delete the selected Peer Route Table.

2.18.1 Diameter Peer Route Tables Elements

Table 2-23 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 2-23 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.	

2.18.2 Adding a Peer Route Table

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

1. Click **Diameter**, and then **Configuration**, and then **Peer Route Tables**.
2. Click **Insert**.
3. Enter a unique name for the Peer Route Table in the **Peer Route Table Name** field.
4. Click **OK**, **Apply**, or **Cancel**.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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 (500) 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 about required component configuration order, see Understanding the Diameter Configuration Sequence.

2.18.3 Deleting a Peer Route Table

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

> **Note**
>
> An Application 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 Route Table** is referenced by any Transaction Configuration Set
> - The selected default **Peer Route Table** is the Default **Peer Route Table**
> - The **Peer Route Table** is referenced by the DM-IWF Options configuration
> - If **OK** is clicked and the selected Application Route Table is currently referenced by any Transaction Configuration Set, the request is rejected and an error message displays.

1. Click **Diameter**, and then **Configuration**, and then **Peer Route Tables**.
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**, and then **Configuration**, and then **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 displays.

   If **OK** is clicked and the selected **Peer Route Table** is currently referenced by the DM-IWF Options configuration, the request is rejected and an error message displays.

2.18.4 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.

> **Note**
>
> When a Redirected Request is processed, if redirect PRT instance is not configured, the PRT instance used to Process the redirected Request is selected similar to an ingress request.

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 occurs. 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 is 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 has. (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 is directly routed to that Peer Node if it has an available Connection.

If there is not an available Connection or all routing attempts (per Peer Node configuration) to the implicit route are exhausted, the message is 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**, and then **Configuration**, and then **Route Lists [Filtered]** page for the selected entry.
- Click **Insert**.

  On the Inserting Rule for Peer Route Table: {Peer Route Table Name} page, 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 (50000) already exists for the Peer Route Table, the Inserting Rule for Peer Route Table: {Peer Route Table Name} page does not open and an error message displays.
- Select the **Rule Name** of a Peer Routing Rule in the list and click **Edit**.

  On the Editing Rule for Peer Route Table: {Peer Route Table Name} page, 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 does not open.
- Select the **Rule Name** of a Peer Routing Rule in the list and click **Delete** to remove the selected Peer Routing Rule. See Deleting a Peer Route Rule.

2.18.4.1 Peer Routing Rule Configuration Elements

Table 2-24 describes the fields on the Peer Routing Rules View, Edit, and Insert pages. Data input notes apply only to the Insert and Edit pages; the View page is read-only.

Table 2-24 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	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: List Range: For a description of operators, see Peer Routing Rule Operators.

Table 2-24 (Cont.) Peer Routing Rules Configuration Elements

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. The value field is disabled for the operators present, absent, and always true.	Format: text box or list Range: • 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. • Application-ID: available configured Application IDs. • Command-Code: available configured Command Codes. • Command-Code: list of configured Command Codes, including Extended Command-Code (ECC) immediately after their parent Command-Code. **Note**: An ECC is a Command Code that also takes into account the value of a specific AVP for that Command Code that gives the true command type (for

Table 2-24 (Cont.) Peer Routing Rules Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
		example, CCR-I, CCR-U, and so on). Range: One or more Parameters with Operator and Value for each Parameter Default for Application-ID and Command Code: -Select-
Action	The action that happens 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 containing the required result-code value to associated with this rule. • Abandon With No Answer discards the message routing and no answer is sent to the associated peer. **Note**: The answer is sent to any applications that requested an answer receive. • Forward To Peer Route Table forwards the message to the specified peer route table.	Format: options Range: Route to Peer, Send Answer, Abandon With No Answer, or Forward To Peer Route Table 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**, and then **Configuration**, and then **Route Lists [Filtered]** page for the selected entry. **Note**: You can only specify route lists whose dynamic attribute is **NO** to be selected for inclusion in a peer route rule. Also, you cannot include route lists created by the dynamic peer discovery feature cannot be included by any peer route rule instance.	Format: List Range: configured Route Lists Default: -Select-

Table 2-24 (Cont.) Peer Routing Rules Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Message Priority	The priority to assign to the message. The message priority is assigned only when action is set to route to peer.	Format: List Range: No Change, 0 - Max (Maximum Normal Request Priority as defined in System Options) Default: No Change
Message Copy Configuration Set	Message Copy Configuration Set (MCCS) used for copying the messages to the DAS. A valid MCCS marks the messages matched by this peer route rule for copy to the DAS.	Format: 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: options Range: • List of the available diameter answer codes • numeric 4 digit value Range: 1000 - 5999 Default: NA
Vendor ID	The Vendor ID to place in the vendor ID AVP of the answer message.	Format: numeric Range: 0 - 4294967295
Answer Error Message	Value returned in the Error-Message AVP of the answer message.	Format: text box Range: 0 - 64 characters Default: Null string
Target Peer Route Table	The table specified in action as forward to peer route table. In the view only screen, the peer route table links to the **Diameter**, and then **Configuration**, and then **Peer Route Tables (Filtered)**	View-only
* Peer Route Table	Peer route table associated with this rule.	View-only

2.18.4.2 Peer Routing Rule Operators

Table 2-25 describes the condition operators available for each parameter in a Peer Routing Rule.

Diameter Capacity Summary provides the maximum number of configurable rules (as defined in DpiCapacityConstraints table, MaxPrtRulesWithContainsPerPrt, MaxCondWithContainsPerPrr, and MaxCharPrtCondWithContains) with the Contains operator per PRT-Name.

> **Note**
>
> For runtime performance and resources efficiencies, only one condition with Contains operator in a rule is allowed.

Table 2-25 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
	Contains	content must contain 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
	Contains	content must contain 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-Real	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

Table 2-25 (Cont.) Peer Routing Rules Operators

Parameter	Operator	Meaning
	Ends With	content must end with the value specified
	Contains	content must contain 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
	Contains	content must contain the value specified
	Always True	content is not evaluated and the parameter's condition is always true

2.18.4.3 Adding a Peer Routing Rule

Use this task to create a new Peer Routing Rule in a Peer Route Table.

1. Click **Diameter**, and then **Configuration**, and then **Peer Route Tables**.
2. Select the Peer Route Table to which you want to add a Peer Routing Rule and click **View/ Insert Rules**.
3. Click **Insert**.
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** 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 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 is 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 option to use an existing Answer Result-Code, then select an Answer Result-Code in the list.
    - Select the option 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**, **Apply**, or **Cancel**

2.18.4.4 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. Click **Diameter**, and then **Configuration**, and then **Peer Route Tables**.
2. Select the Peer Route Table which contains the Peer Routing Rule you want to edit and click **View/Edit Rules**.
3. Select the Peer Routing Rule you want to edit, then click **Edit**.
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.

   The following condition exists:
   - Peer Route Rules are always statically configured; no statically configured instance can refer to a dependent GUI element that was added to the configuration as a result of Dynamic Peer Discovery.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then an error message appears:
   - If you attempt to insert or update a Peer Route Rule instance and the specified Route List whose Dynamic attribute value is **YES**.
   - 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)

2.18.4.5 Deleting a Peer Route Rule

Use this task to delete a Peer Routing Rule from a Peer Route Table.

1. Click **Diameter**, and then **Configuration**, and then **Peer Route Tables**.
2. Select the Peer Route Table that contains the Peer Routing Rule you want to delete and click **View/Edit Rules**.
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 displays and the Peer Routing Rules view refreshes.

2.19 Diameter Egress Throttle Groups

Egress Throttle Groups are used to monitor egress Request rate and pending transactions for multiple Peers and Connections across multiple DA-MPs. 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.

You can perform these tasks on an Active System OAM (**SOAM**).

Egress Throttle Group functions are described in detail in Egress Throttle Groups. Egress Throttle Groups control the following functions.

An Egress Throttle Group can be standalone, or it can be associated with an Egress Throttle List that spans multiple signaling routers. An Egress Throttle Group can be associated with only one Egress Throttle List. See Diameter Egress Throttle List.

- Egress Throttle Group Rate Limiting controls the total egress Request traffic that is routed to a configured group of Peers or Connections.
- Egress Throttle Group Pending Transaction Limiting controls the number of pending transactions that are allowed for a configured group of Peers or Connections.
- The Egress Throttle Group Rate Limiting and Egress Throttle Group Pending Transaction Limiting provide 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

- The Egress Throttling Control Scope.

On the **Diameter**, and then **Configuration**, and then **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. The default order is by **Egress Throttle Groups Name** in ascending ASCII order.
- Click **Insert**.

  On the **Diameter**, and then **Configuration**, and then **Egress Throttle Groups [Insert]** page, you can add new Egress Throttle Groups.

  The **Diameter**, and then **Configuration**, and then **Egress Throttle Groups [Insert]** page does not appear if the maximum number of Egress Throttle Groups (512 per NE) already exists in the system.
- Select an Egress Throttle Group in the list and click **Edit**.

  On the **Diameter**, and then **Configuration**, and then **Egress Throttle Groups [Edit]** page, you can edit the selected Egress Throttle Group.

  If the selected Egress Throttle Group has been deleted by another user, then the **Diameter**, and then **Configuration**, and then **Egress Throttle Groups [Edit]** page does not open.
- Select an Egress Throttle Group in the list and click **Delete** to delete the selected Egress Throttle Group.

2.19.1 Diameter Egress Throttle Groups Elements

Table 2-26 describes the fields on the **Diameter**, and then **Configuration**, and then **Egress Throttle Groups** page.

Table 2-26 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 contain at least one alpha and must not start with a digit. Range: 1 - 32 characters Default: NA
Rate Limiting configuration set	Available Rate Limiting configuration sets for this ETG.	Format: List Range: NA Default: NA
Pending Transaction Limiting Configuration Set	Available Pending Transaction Limiting configuration sets for this ETG.	Format: List Range: NA Default: NA

Table 2-26 (Cont.) Egress Throttle Groups Elements

Field (* indicates a required field)	Description	Data Input Notes
Egress Throttling Control Scope	The control scope used to determine if the ETG's aggregated data or the ETL's aggregated data is used for routing decisions. This determines if egress throttling is controlled by the configuration data for the ETG (ETG configuration sets) or (optionally) by the configuration data for an ETL that contains the ETG (ETL configuration sets). **Note**: The Egress Throttling Control Scope can be set to ETL only when the ETG has been added to an Egress Throttle List through the NOAM GUI. See Diameter Egress Throttle List.	Format: two options; one must be checked. Range: ETL or ETG Default: ETG checked
Peer Node	Peers associated with this Egress Throttle Group. **Note**: Click **Add** to add Peer Nodes.	Format: List Range: 0 - 128 Default: NA
Connection	Connection associated with this Egress Throttle Group. **Note**: Click **Add** to add Connections.	Format: List Range: 0 - 128 Default: NA

2.19.2 Adding Egress Throttle Groups

Use this task to create new Egress Throttle Groups.

Egress Throttle Groups fields are described in Diameter Egress Throttle Groups Elements.

1. Click **Diameter**, and then **Configuration**, and then **Egress Throttle Groups**.
2. Click **Insert**.
3. Enter a unique name for the Egress Throttle Group in the **Egress Throttle Group Name** field.
4. Select a **Rate Limiting configuration set**.
5. Select a **Pending Transaction Limiting Configuration Set**.
6. Select a **Egress Throttling Control Scope** option.
7. Select a **Peer Node** to associate with this ETG.
8. Select a **Connection** to associate with this ETG.
9. Click:
   - **OK** to save the changes and return to the **Diameter**, and then **Configuration**, and then **Egress Throttle Groups** page.
   - **Apply** to save the changes and remain on this page.

- **Cancel** to return to the **Diameter**, and then **Configuration**, and then **Egress Throttle Groups** page without saving any changes.

The following conditions exist:

- You can only insert Peer Nodes or Connections whose Dynamic attribute is **NO** for inclusion in an Egress Throttle Group.
- Peer Nodes or Connections created by the Dynamic Peer Discovery feature cannot be included by any Egress Throttle Group instance.

If **OK** or **Apply** is clicked and any of the following conditions exist, then 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 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.

2.19.3 Editing Egress Throttle Groups

Use this task to edit Egress Throttle Groups.

When the **Diameter**, and then **Configuration**, and then **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 irrespective of the Operational Status of the associated Peer Connections.

Use this GUI page to change configuration sets and set the **Egress Throttling Control Scope**.

Egress Throttle Groups fields are described in Diameter Egress Throttle Groups Elements.

1. Click **Diameter**, and then **Configuration**, and then **Egress Throttle Groups**.

2. Select the Egress Throttle Groups to be edited and click **Edit**.
3. Update the relevant fields.

   An entry in a list can be removed by selecting the entry in the list and clicking the **X** to the right of the list.
4. Click:
   - **OK** to save the changes and return to the **Diameter**, and then **Configuration**, and then **Egress Throttle Groups** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter**, and then **Configuration**, and then **Egress Throttle Groups** page without saving any changes.

   The following conditions exist:
   - You can only edit Peer Nodes or Connections whose Dynamic attribute is **NO** for inclusion in an Egress Throttle Group.
   - Peer Nodes or Connections created by the Dynamic Peer Discovery feature cannot be included by any Egress Throttle Group instance.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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.

2.19.4 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. Click **Diameter**, and then **Configuration**, and then **Egress Throttle Groups**.
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**, and then **Configuration**, and then **Egress Throttle Groups** page.

   If **OK** is clicked and the following condition exists, then 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.

- The Egress Throttle Group is configured in an Egress Throttle List. The Egress Throttle Group must be removed from the Egress Throttle List in the NOAM GUI before it can be deleted.

2.20 Diameter Reroute On Answer

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.

You can perform these tasks on an Active System OAM (**SOAM**).

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**, and then **Configuration**, and then **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**.

  On the **Diameter**, and then **Configuration**, and then **Reroute on Answer [Insert]** page, you can add a new entry.

  The **Diameter**, and then **Configuration**, and then **Reroute on Answer [Insert]** does 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.

2.20.1 Diameter Reroute On Answer Configuration Elements

Table 2-27 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 2-27 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

Table 2-27 (Cont.) Reroute On Answer Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
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: options, text box, and list Range: • first option: ALL • second option: list with available Application IDs Default: ALL

2.20.2 Adding a Reroute On Answer Entry

Use this task to create a new Reroute On Answer entry.

The fields are described in Diameter Reroute On Answer Configuration Elements.

1. Click **Diameter**, and then **Configuration**, and then **Reroute On Answer**.
2. Click **Insert**.
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 option and select the appropriate **Application ID** from the list.
5. Click:
   - **OK** to save the changes and return to the **Diameter**, and then **Configuration**, and then **Reroute on Answer** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter**, and then **Configuration**, and then **Reroute on Answer** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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

2.20.3 Deleting a Reroute On Answer

Use this task to delete a Reroute On Answer entry.

1. Click **Diameter**, and then **Configuration**, and then **Reroute On Answer**.
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**, and then **Configuration**, and then **Reroute on Answer** page.

   If **OK** is clicked and the selected entry no longer exists (it was deleted by another user), an error message displays and the Reroute on Answer page refreshes.

2.21 Diameter Application Route Tables

An **Application Route Table** contains one or more Application Routing Rules that can be used for routing Request messages to diameter applications.

You can perform these tasks on an Active System OAM (**SOAM**).

Users can assign Application Route Table (ART) to Diameter messages based on Application ID and (Extended) Command Codes by configuring Transaction Configuration Rule (TCR) with Application ID plus (E)CC as a key in Transaction Configuration Sets.

On the **Diameter**, and then **Configuration**, and then **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**.
  On the **Diameter**, and then **Configuration**, and then **Application Route Tables [Insert]** page, you can add a new **Application Route Table**.

  The **Diameter**, and then **Configuration**, and then **Application Route Tables [Insert]** page does not open if the maximum number of Application Route Tables (1500) 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**.
  On the **Diameter**, and then **Configuration**, and then **Application Route Tables [View/Edit Rules]** page, you can edit the selected Application Route Table Rules.

  If the selected Application Route Table has been deleted by another user, the **Diameter**, and then **Configuration**, and then **Application Route Tables [View/Edit Rules]** page does not open.

2.21.1 Diameter Application Route Tables Elements

Table 2-28 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 2-28 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
Number of Rules	The number of rules associated with this Application Route Table.	Format: numeric Range: NA

2.21.2 Adding an Application Route Table

Use this task to create a new **Application Route Table**. The fields are described in Diameter Application Route Tables Elements.

1. Click **Diameter**, and then **Configuration**, and then **Application Route Tables**.
2. Click **Insert**.
3. Enter a unique name for the Application Route Table in the **Application Route Table Name** field.
4. Click **OK**, **Apply**, or **Cancel**.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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** (1500) allowed in the system to be exceeded
   - Adding this Application Route Table would cause the maximum number of **Application Routing Rules** (50000) 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.

2.21.3 Deleting an Application Route Table

Use this task to delete an **Application Route Table**.

> **Note**
>
> An Application 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 Route Table** is referenced by any Transaction Configuration Set
> - The selected default **Peer Route Table** is the Default **Peer Route Table**
> - The **Peer Route Table** is referenced by the DM-IWF Options configuration
> - If **OK** is clicked and the selected Application Route Table is currently referenced by any Transaction Configuration Set, the request is rejected and an error message displays.

1. Click **Diameter**, and then **Configuration**, and then **Application Route Tables**.
2. Select the **Application Route Table** you want to delete.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

   If **OK** is clicked and the selected **Application Route Table** no longer exists (it was deleted by another user), then an error message appears.

   If **OK** is clicked and the selected **Application Route Table** is currently referenced by the DM-IWF Options configuration, then the request is rejected and an error message appears.

2.21.4 Application Routing Rules Configuration

An Application Routing Rule defines message routing to a diameter application based on message content matching the Application Routing Rule's conditions.

If the redirect ART instance is not configured, redirect processing skips ART evaluation for the redirected request, and it goes directly to PRT evaluation. If the redirect ART is configured, redirect processing searches for that ART and performs ART evaluation of the redirect request.

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 diameter application specified in the rule.

Application Routing Rules are assigned a priority in relation to other Application Routing Rules. A message is 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 has. (1 is highest priority and 1000 is lowest priority.)

One or more diameter 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 **Insert**.
  On the Inserting Rule for Application Route Table: {Application Route Table Name} page, 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 (50000) already exists in the system, then the Inserting Rule for Application Route Table: {Application Route Table Name} page does not appear and an error message displays.
- Select the **Rule Name** of an Application Routing Rule in the list and click **Edit**.
  On the Editing Rule for Application Route Table: {Application Route Table Name} page, 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 **Delete** to remove the selected Application Routing Rule. See Deleting an Application Routing Rule

2.21.4.1 Application Routing Rule Configuration Elements

Table 2-29 describes the fields on the Application Routing Rules View, Insert, and Edit pages. Data input notes apply only to the Insert and Edit pages.

Table 2-29 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 must contain at least one alpha (A-Z, a-z) Range: 1 - 32 characters
* Priority	Priority of the rule in relation to other rules. The lower the priority number, the higher a priority an application routing rule has. 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 - 1000

Table 2-29 (Cont.) Application Routing Rules Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
* 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: 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. The value field is disabled for the operators present, absent, and always true.	Format: text box or list • Destination-Realm and Origin-Realm • Destination-Host and Origin-Host • Application-ID • Command-Code **Note**: An ECC is a command code that also takes into account the value of a specific AVP for that command code that gives the true command type (for example, CCR-I, CCR-U, and so on). Range: One or more parameters with operator and value for each parameter Default for Application-ID and Command Code: -Select-
* Application Name	Application Name associated with this rule.	Format: List Range: All activated applications Default: -Select-

Table 2-29 (Cont.) Application Routing Rules Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Action	The action that happens if the diameter message matches the conditions set in the application routing rule: • Route to Application routes the message to the associated application. • Forward To Egress Routing forwards the message to PRT. • Send Answer abandons message routing and sends an answer response containing the required result-code value to associated application. • Abandon With No Answer discards the message routing and no answer is sent to the associated peer. • Forward to Application Route Table forwards the message to the specified ART. • Forward to Peer Route Table forwards the message to the specified PRT.	Format: options Range: Route to Application, Forward to Egress Routing, Send Answer, and Abandon With No Answer, Forward to Application Route Table, or Forward to Peer Route Table Default: Route to Application
Answer Result-Code Value	The value to be placed in the result-code AVP of the answer message. A diameter answer code is required if the action is set to send answer.	Format: options Range: 1000 - 5999 Default: none
Vendor ID	The value to be placed in the vendor ID AVP	Format: numeric Range: 0 - 4294967295 Default: none
Answer Error Message	String to be placed in the error-message AVP of the answer message	Format: text box Range: 0 - 64 Default: null, no Error-Message AVP in Answer message
Target Route Table	The value selected in the action element options Forward to Application Route Table or Forward to Peer Route Table. In the view only screen, the route table links to the **Diameter**, and then **Configuration**, and then **Application Route Tables (Filtered)** or **Diameter**, and then **Configuration**, and then **Peer Route Tables (Filtered)**.	View Only

Table 2-29 (Cont.) Application Routing Rules Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
Gx-Prime	If this rule matches a request, Policy DRA treats the request's diameter application as Gx-Prime.	Checkbox
* Application Route Table	Application Route Table associated with this rule.	View Only

2.21.4.2 Application Routing Rule Operators

Table 2-30 describes the **Conditions** operators available for each parameter in a Application Routing Rule.

Table 2-30 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
	Contains	content must contain 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
	Contains	content must contain 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

Table 2-30 (Cont.) Application Routing Rules Operators

Parameter	Operator	Meaning
	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
	Contains	content must contain 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
	Contains	content must contain the value specified
	Always True	content is not evaluated and the parameter's condition is always true

2.21.4.3 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. Click **Diameter**, and then **Configuration**, and then **Application Route Tables**.
2. Select an Application Route Table Name in the list.
3. Click **View/Edit Rules**.
4. Click **Insert**.

   If the maximum number of Application Routing Rules (50000) already exists in the system, the **Diameter**, and then **Configuration**, and then **Application Routing Rules [Insert]** page does 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 1000 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** 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 list, select the **Application Name** associated with this Rule.
9. Click **OK**, **Apply**, or **Cancel**

2.21.4.4 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. Click **Diameter**, and then **Configuration**, and then **Application Route Tables**.
2. Select an Application Route Table Name in the list.
3. Click **View/Edit Rules**.
4. Select a Rule to edit.
5. Click **Edit**.
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**, **Apply**, or **Cancel**.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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)

2.21.4.5 Deleting an Application Routing Rule

Use this task to delete an Application Routing Rule from a selected Application Route Table.

1. Click **Diameter**, and then **Configuration**, and then **Application Route Tables**.

   The **Diameter**, and then **Configuration**, and then **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 appears with a list of the Rules 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 displays and the Application Routing Rules view refreshes.

2.22 Diameter Routing Option Sets

A Routing Option Set is a collection of Routing Options that are used when a Request message is received. This functionality controls the number of times an application forwards the request message and the processing error delivery situations.

You can perform these tasks on an Active System OAM (SOAM).

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.

Users can assign Routing Option Set (ROS) to Diameter messages based on Application ID and (Extended) Command Codes by configuring Transaction Configuration Rule (TCR) with Application ID plus (E)CC as a key in Transaction Configuration Sets.

Select the Routing Option Set as per the precedence selection criterion as described in here, highest to lowest priority.

- If Transaction Configuration Set is selected on ingress Peer Node from which the Diameter Request was received, use Transaction Configuration Set and apply longest/strongest match search criteria for Diameter Request message parameters comparison and if a match is found, apply ROS assigned to the Transaction Configuration Rule defined under this Transaction Configuration Set, if it exists.
- The ROS assigned to the ingress Peer Node from which the Request message was received, if it exists.

- Search Default TCS and apply longest/strongest match. Use ROS associated with best match, if any is found.
- Default ROS.

On the **Diameter**, and then **Configuration**, and then **Route 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**.
  On the **Diameter**, and then **Configuration**, and then **Route Option Sets [Insert]** page, you can add a new Routing Option Set.

  The **Diameter**, and then **Configuration**, and then **Route Option Sets [Insert]** page does not open if the maximum number of Routing Option Sets (50) already exists in the system
- Select a **Routing Option Set** in the list and click **Edit**.
  On the **Diameter**, and then **Configuration**, and then **Route Option Sets [Edit]** page, you can edit the selected Routing Option Set.

  If the selected Routing Option Set has been deleted by another user, the **Diameter**, and then **Configuration**, and then **Route Option Sets [Edit]** page does 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.

2.22.1 Diameter Routing Option Sets Elements

Table 2-31 describes the fields on the Routing Option Sets View, Edit, and Insert pages. Data input notes apply only to the Insert and Edit pages; the View page is read-only.

Table 2-31 Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Routing Options Set Name	Unique name of the Routing Option Set.	Case-sensitive string: alphanumeric and underscore (_); must contain at least one alpha and cannot begin with a digit. Range: 1 - 32 characters
* Maximum Per Message Forwarding Allowed	Maximum number of times an application is allowed to forward a request message. If the maximum per message forwarding allowed value is set to 1, the transaction lifetime field is disabled. If the maximum per message forwarding allowed value is greater than 1, the transaction lifetime field is enabled.	Format: numeric Range: 1 - 16 Default: 1

Table 2-31 (Cont.) Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Transaction Lifetime	The total time diameter allows to forward a request, including initial and all subsequent routing attempts. This must be greater or equal to pending answer timer.	Format: numeric Range: 100 - 540000 Default: 1000
Pending Answer Timer	If the pending answer timer value is not selected, the egress peer node's associated pending answer timer, if it is defined, is used when processing transactions. A pending answer timer cannot be assigned to the default routing option set.	Format: List Range: Default, configured Pending Answer Timers Default: Not Selected.
* Resource Exhausted Action	Action taken when a request cannot be processed due to an internal resource being exhausted. If set to abandon with no answer the, resource exhausted answer result code, resource exhausted error message, and resource exhausted vendor ID fields are disabled. If set to send answer the, resource exhausted answer result code, resource exhausted error message, and resource exhausted vendor ID fields are enabled.	Format: List Range: Abandon with no Answer; Send Answer Default: Abandon with no Answer
Resource Exhausted Result-Code	Value to be placed in the result code AVP of the answer message. Answer result code value is required if action is send answer. If the resource exhausted action is set to abandon with no answer, the resource exhausted result code field is disabled.	Format: options • List of all standard set of Diameter Result Codes • text box; numeric 4 digit value Range: 1000 - 5999 Default: 3004_TOO_BUSY
Resource Exhausted Answer Error-Message	String to be placed in the error message AVP of the answer message for resource exhaustion. If the resource exhausted action is set to abandon with no answer, the resource exhausted error message is disabled.	Format: text box Range: 0 - 64 characters Default: Null string, no Error-Message AVP in Answer message

Table 2-31 (Cont.) Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Resource Exhausted Vendor-ID	Vendor ID value returned in an answer message when a message is not successfully routed due to resource exhausted vendor ID. If vendor ID is set to zero, then a result code AVP is sent. If vendor ID is greater than zero, then the grouped experimental result AVP is sent containing a vendor ID AVP (set to this value) and experimental result code set to the resource exhausted result code. If the resource exhausted action is set to abandon with no answer, the resource exhausted vendor ID field is disabled.	Format: numeric Range: 1 - 4294967295 Default: none
* No Peer Response Action	Action taken when the routing of a request is abandoned due to an answer timeout or transaction lifetime timeout. If the no peer response action is set to abandon with no answer, the no peer response answer result code, the no peer response error message, and the no peer response vendor ID fields are disabled. If the no peer response action is set to send answer, the no peer response answer result code, the no peer response error message, and the no peer response vendor ID fields are enabled.	Format: List Range: Abandon with no Answer; Send Answer Default: Send Answer
No Peer Response Result-Code	Value to be placed in the result code AVP of the answer message. Answer result code value is required if action is send answer. If the no peer response action is set to abandon with no answer, the no peer response answer result code field is disabled.	Format: options • List of all standard set of Diameter Result Codes • text box; numeric 4 digit value Range: 1000 - 5999 Default: 3002 _UNABLE_TO_DELIVER
No Peer Response Error-Message	String to be placed in the error message AVP of the answer message for no peer response. If the no peer response action is set to abandon with no answer, the no peer response answer error message field is disabled.	Format: text box Range: 0 - 64 characters Default: Null string, no Error-Message AVP in Answer message

Table 2-31 (Cont.) Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
No Peer Response Vendor-ID	Vendor ID value returned in an answer message when a message is not successfully routed due to no peer response. When specified, the answer generated is an experimental result code grouped AVP with the specified vendor ID value placed in the vendor ID AVP. If the no peer response action is set to abandon with no answer, the no peer response answer vendor ID field is disabled.	Format: numeric Range: 1 - 4294967295 Default: none
* Connection Failure Action	Action taken when the routing of a request is abandoned when the last egress connection selection fails. If the connection failure action is set to abandon with no answer, the connection failure answer result code, the connection failure answer error message, and the connection failure vendor ID fields are disabled. If the connection failure action is set to send answer, the connection failure answer result code, the connection failure answer error message, and the connection failure vendor ID fields are enabled.	Format: List Range: Abandon with no Answer; Send Answer Default: Send Answer
Connection Failure Result-Code	Value to be placed in the result code AVP of the answer message. Answer result code value is required if action is send answer. If the connection failure action is set to abandon with no answer, the connection failure answer result code field is disabled.	Format: options • List of all standard set of Diameter Result Codes • text box; numeric 4 digit value Range: 1000 - 5999 Default: 3002 UNABLE_TO_DELIVER
Connection Failure Answer Error-Message	String to be placed in the error message AVP of the answer message for connection failure. If the connection failure action is set to abandon with no answer, the connection failure answer error message field is disabled.	Format: text box Range: 0 - 64 characters Default: Null string, no Error-Message AVP in Answer message

Table 2-31 (Cont.) Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
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 is an experimental result code grouped AVP with the specified vendor ID value placed in the vendor ID AVP. If the connection failure action is set to abandon with no answer, the connection failure vendor ID field is disabled.	Format: numeric Range: 1 - 4294967295 Default: none
* Connection Congestion Action	Action taken when the routing of a request is abandoned because the last connection evaluated is congested. If the connection congestion action is set to abandon with no answer, the connection congestion result code, the connection congestion answer error message, and the connection congestion vendor ID fields are disabled. If the connection congestion action is set to send answer, the connection congestion answer result code Value, the connection congestion answer error message, and the connection congestion vendor Id fields are enabled.	Format: List Range: Abandon with no Answer; Send Answer Default: Send Answer
Connection Congestion 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. Answer result code value is required if action is send answer. If the connection congestion action is set to abandon with no answer, the connection congestion result code field is disabled.	Format: options • List of all standard set of Diameter Result Codes • text box; numeric 4 digit value Range: 1000 - 5999 Default: 3002 UNABLE_TO_DELIVER

Table 2-31 (Cont.) Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Connection Congestion Answer Error-Message	String to be placed in the error message AVP of the answer message for connection congestion. If the connection congestion action is set to abandon with no answer, the connection congestion answer error message field is disabled.	Format: text box Range: 0 - 64 characters Default: Null string, no Error-Message AVP in Answer message
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 is an experimental result code grouped AVP with the specified vendor ID value placed in the vendor ID AVP. If the connection congestion action is set to abandon with no answer, the connection congestion vendor ID field is disabled.	Format: numeric Range: 1 - 4294967295 Default: none
* Destination-Realm Not Served Action	Action taken when routing of a request is abandoned due to destination realm implicit routing failure to find a (Realm/Application-ID) match in the realm route table for routing the transaction. If the destination realm not served action is set to abandon with no answer, the destination realm not served result code, destination realm not served error message, and destination realm not served vendor ID fields are disabled. If the destination realm not served action is set to send answer, the destination realm not served result code, destination realm not served error message, and destination realm not served vendor ID fields are enabled.	Format: List Range: Send Answer, Abandon with no Answer Default: Send Answer

Table 2-31 (Cont.) Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Destination-Realm Not Served Result-Code	Value to be placed in the result code AVP of the answer message. Answer result code value is required if action is send answer. If the destination realm not served action is set to abandon with no answer, the destination realm not served result code field is disabled.	Format: options • List of all standard set of Diameter Result Codes • text box; numeric 4 digit value Range: 1000 - 5999 Default: 3003 REALM_NOT_SERVED
Destination-Realm Not Served Error-Message	String to be placed in the error message AVP of the answer message for destination realm not served. If the destination realm not served action is set to abandon with no answer, destination realm not served error message field is disabled.	Format: numeric Range: 0 - 64 characters Default: none
Destination-Realm Not Served Vendor-ID	Vendor ID value returned in an answer message when a message is not successfully routed due to destination realm not served. When specified, answer generated is experimental result code grouped AVP with vendor ID value specified placed in vendor ID AVP. If the destination realm not served action is set to abandon with no answer, destination realm not served vendor ID field is disabled.	Format: numeric Range: 1 - 4294967295 Default: none
* Peer Node Reported Congestion Action	Action taken when routing of a request is abandoned and the route evaluated is congested. If the peer node reported congestion action is set to abandon with no answer, the peer node reported congestion result code, the peer node reported congestion error message, and the peer node reported congestion vendor ID fields are disabled. If the peer node reported congestion action is set to send answer, the peer node reported congestion result code Value, the peer node reported congestion error message, and the peer node reported congestion vendor ID fields are enabled.	Format: List Range: Send Answer, Abandon with No Answer Default: Send Answer

Table 2-31 (Cont.) Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Peer Node Reported Congestion Result-Code	Value to be placed in the result code AVP of the answer message. Answer result code value is required if action is send answer. If the peer node reported congestion action is set to abandon with no answer, the peer node reported congestion result code field is disabled.	Format: options • List of all standard set of Diameter Result Codes • text box; numeric 4 digit value Range: 1000 - 5999 Default: 3002 UNABLE_TO_DELIVER
Peer Node Reported Congestion Answer Error-Message	String to be placed in the error message AVP of the answer message for peer node reported congestion. If the peer node reported congestion action is set to abandon with no answer, the peer node reported congestion error message field is disabled.	Format: numeric Range: 1 - 64 characters Default: null string, no Error-Message AVP in Answer message
Peer Node Reported Congestion Vendor-ID	Vendor ID value returned in an answer message when a message is not successfully routed due to peer node reported congestion. When specified, answer generated is experimental result code grouped AVP with vendor ID value specified placed in vendor ID AVP. If the peer node reported congestion action is set to abandon with no answer, the peer node reported congestion vendor ID field is disabled.	Format: numeric Range: 1 - 4294967295 Default: none

Table 2-31 (Cont.) Routing Option Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Nested ART/PRT Error Action	Action taken when routing of a request is abandoned due to a Nested Application Route Table/ Peer Route Table (ART/PRT) search results in a loop or maximum search depth exceeded. If the nested ART/PRT error action is set to abandon with no answer the, nested ART/PRT error result code, nested ART/PRT error message, and nested ART/PRT error vendor ID fields are disabled. If the nested ART/PRT error action is set to send answer, the nested ART/PRT error result code Value, the nested ART/PRT error message, and the nested ART/PRT error vendor ID fields are enabled.	Format: List Range: Send Answer, Abandon with No Answer Default: Send Answer
Nested ART/PRT Error Result Code	Value placed in the result code AVP of the answer message. Answer result code value is required if action is send answer. If the nested ART/PRT error action is set to abandon with no answer the, nested ART/PRT error result code field is disabled.	Format: options • List of all standard set of Diameter Result Codes • text box; numeric 4 digit value Range: 1000 - 5999 Default: 3002 UNABLE_TO_DELIVER
Nested ART/PRT Error Message	String to be placed in the error message AVP of the answer message for Nested Application route Table/Peer route Table (ART/PRT) Error. If the nested ART/PRT error action is set to abandon with no answer the, nested ART/PRT error message field is disabled.	Format: numeric Range: 1 - 64 characters Default: null string, no Error-Message AVP in Answer message
Nested ART/PRT Error Vendor ID	Vendor ID value returned in an answer message when a message is not successfully routed due to nested ART/PRT error. When specified, answer generated is experimental result code grouped AVP with vendor ID value specified placed in vendor ID AVP If the nested ART/PRT error action is set to abandon with no answer the, nested ART/PRT error vendor ID field is disabled.	Format: numeric Range: 1 - 4294967295 Default: none

2.22.2 Adding a Routing Option Set

Use this task to create a new Routing Option Set. The fields are described in Diameter Routing Option Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Routing Option Sets**.
2. Click **Insert**.
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**, **Apply**, or **Cancel**.

2.22.3 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. Click **Diameter**, and then **Configuration**, and then **Routing Option Sets**.
2. Select the **Routing Option Set** you want to edit.
3. Click **Edit**.

   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 Diameter Routing Option Sets Elements.
5. Click **OK**, **Apply**, or **Cancel**.

2.22.4 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 Transaction Configuration Set
> - The Routing Option Set is the Default Routing Option Set

1. Click **Diameter**, and then **Configuration**, and then **Routing Option Sets**.
2. Select the **Routing Option Set** you want to delete.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.23 Diameter Pending Answer Timers

A Pending Answer Timer sets the amount of time Diameter waits for an Answer after sending a Request to a Peer Node.

You can perform these tasks on an Active System OAM (SOAM).

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

Users can assign a Pending Answer Timer (PAT) to Diameter messages based on Application ID and (Extended) Command Codes by configuring Transaction Configuration Rule (TCR) with Application ID plus (E)CC as a key in Transaction Configuration Sets.

A Pending Answer Timer can be associated with:

- The Peer Node from which the request was received through Routing Option Set.
- The Peer Node that the Request is sent to
- The Transaction Configuration Set

Select the Pending Answer Timer using the following precedence selection criterion, highest to lowest priority:

- If Transaction Configuration Set is selected on ingress Peer Node from which the Diameter Request was received, use Transaction Configuration Set and apply longest/strongest match search criteria for Diameter Request message parameters comparison and if a match is found, apply PAT assigned to Transaction Configuration Rule defined under this Transaction Configuration Set, if it exists.
- The Pending Answer Timer assigned to the Routing Option Set for the Ingress Peer, if it exists.
- The Pending Answer Timer assigned to the egress Peer Node to which the Request message is forwarded, if it exists.
- Search Default TCS and apply longest/strongest match. Use PAT associated with best match, if any is found.
- 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 Diameter attempts 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:

- 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 Diameter attempts 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 may be extended by as much as 1 Pending Answer Timer interval in some cases.

A Routing Option Set referenced by a Transaction Configuration Set Rule in Transaction Configuration Set cannot have a Pending Answer Timer configured, because each Transaction Configuration Rule always has an associated Pending Answer Timer.

Diameter selection of the **Pending Answer Timer** and **Transaction Lifetime** values to use when routing Requests upstream operates as indicated in Table 2-32.

Table 2-32 Diameter Pending Answer Timer and Transaction Lifetime Selection

Transaction Configuration Set entry exists for Appl-ID and (Extended) Command Code in Request being processed and is associated with Ingress Peer Node	Pending Answer Timer specified in Ingress Peer Node Routing Option Set?	Egress Pending Answer Timer specified in Egress Peer Node?	Default Transaction Configuration Set entry exists for Appl-ID and (Extended) Command Code in Request being processed?	Resultant Pending Answer Timer value used
Yes	Yes	Yes	Yes	Pending Answer Timer from Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria.
Yes	No	Yes	No	Pending Answer Timer from Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria.
Yes	Yes	No	No	Pending Answer Timer from Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria.

Table 2-32 (Cont.) Diameter Pending Answer Timer and Transaction Lifetime Selection

Transaction Configuration Set entry exists for Appl-ID and (Extended) Command Code in Request being processed and is associated with Ingress Peer Node	Pending Answer Timer specified in Ingress Peer Node Routing Option Set?	Egress Pending Answer Timer specified in Egress Peer Node?	Default Transaction Configuration Set entry exists for Appl-ID and (Extended) Command Code in Request being processed?	Resultant Pending Answer Timer value used
Yes	Yes	Yes	No	Pending Answer Timer from Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria.
Yes	Yes	No	Yes	Pending Answer Timer from Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria.
Yes	No	Yes	No	Pending Answer Timer from Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria.
Yes	No	No	Yes	Pending Answer Timer from Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria.
Yes	No	Yes	Yes	Pending Answer Timer from Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria.

Table 2-32 (Cont.) Diameter Pending Answer Timer and Transaction Lifetime Selection

Transaction Configuration Set entry exists for Appl-ID and (Extended) Command Code in Request being processed and is associated with Ingress Peer Node	Pending Answer Timer specified in Ingress Peer Node Routing Option Set?	Egress Pending Answer Timer specified in Egress Peer Node?	Default Transaction Configuration Set entry exists for Appl-ID and (Extended) Command Code in Request being processed?	Resultant Pending Answer Timer value used
No	Yes	Yes	No	Pending Answer Timer in Ingress Peer Node Routing Option Set.
No	Yes	No	Yes	Pending Answer Timer in Ingress Peer Node Routing Option Set.
No	Yes	No	No	Pending Answer Timer in Ingress Peer Node Routing Option Set.
No	Yes	Yes	Yes	Pending Answer Timer in Ingress Peer Node Routing Option Set.
No	No	Yes	Yes	Egress Pending Answer Timer in Egress Peer Node.
No	No	Yes	No	Egress Pending Answer Timer in Egress Peer Node.
No	No	No	Yes	Pending Answer Timer from Default Transaction Configuration Set for Request's Appl-ID and (E)CC after applying longest/ strongest search criteria if match occur otherwise System Default Pending Answer Timer.
No	No	No	No	System Default Pending Answer Timer.

The **Diameter**, and then **Configuration**, and then **Pending Answer Timers**

On the **Diameter**, and then **Configuration**, and then **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**.

  On the **Diameter**, and then **Configuration**, and then **Pending Answer Timers [Insert]** page, you can add a new Pending Answer Timer.

  The **Diameter**, and then **Configuration**, and then **Pending Answer Timers [Insert]** page does not open if the maximum number of Pending Answer Timers (16) already exists in the system.
- Select a Pending Answer Timer in the list and click **Edit**.

  On the **Diameter**, and then **Configuration**, and then **Pending Answer Timers [Edit]** page, you can edit the selected Pending Answer Timer.

  If the selected Pending Answer Timer has been deleted by another user, the **Diameter**, and then **Configuration**, and then **Pending Answer Timers [Edit]** page does 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.

2.23.1 Diameter Pending Answer Timers Elements

Table 2-33 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 2-33 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 diameter waits for an Answer from a upstream peer after forwarding a request.	Format: numeric Range: 100 - 180000 ms Default: 1000 ms

2.23.2 Adding a Pending Answer Timer

Use this task to create a new Pending Answer Timer. The fields are described in Diameter Pending Answer Timers Elements.

1. Click **Diameter**, and then **Configuration**, and then **Pending Answer Timers**.
2. Click **Insert**.
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**, **Apply**, or **Cancel**.

2.23.3 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. Click **Diameter**, and then **Configuration**, and then **Pending Answer Timers**.
2. Select the **Pending Answer Timer** you want to edit.
3. Click **Edit**.

   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 Diameter Pending Answer Timers Elements.
5. Click **OK**, **Apply**, or **Cancel**.

2.23.4 Deleting a Pending Answer Timer

Use this task to delete a Pending Answer Timer.

> **Note**
>
> A Pending Answer Timer cannot be deleted if it is referenced by either a Peer Node or a Routing Option Set is referenced by Protected Networks. It also cannot be deleted if it is associated with any Routing Option Set.

1. Click **Diameter**, and then **Configuration**, and then **Pending Answer Timers**.
2. Select the **Pending Answer Timer** you want to delete.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.24 Diameter Traffic Throttle Points

A Traffic Throttle Point (**TTP**) is the logical entity that contains the information that is required to perform (Peer Node, Application ID) **ETR** throttling. It contains user-defined configuration attributes and dynamic throttling information received from upstream Peer Nodes via DOIC.

The RT-DB TTP table contains:

- User-defined TTP attributes
- DOIC throttling information received by way of DOIC AVPs
- Target ETR
- Diverted OTR

When the routing application selects a Peer Node or Connection from a Route Group (or selects a Peer Node for implicit Routing), it checks if a TTP exists for the selected Peer Node/

Connection and Application ID in the Request message. If an active TTP exists, ETR throttling can be applied.

When routing a Request message, which has an associated Active TTP with DOIC enabled, upstream Peer Nodes are notified that the node supports DOIC and provides a list of DOIC Abatement Algorithms. When an OC-Supported-Features AVP is sent in a Request message, it saves the TTP which triggered sending the DCA in the PTR. When an Answer response is received from a Peer Node and a non-NULL TTP is saved in the PTR, the application checks for DOIC AVPs that might contain a new overload report (**OLR**) or contain changes to an existing overload report being processed. Otherwise, the application does not check for DOIC AVPs in Answer responses. Any valid requests from the upstream Peer Node to reduce traffic are stored in the TTP and immediately applied.

A **TTP** is required to manage the DSR Diameter Overload Indication Conveyance (**DOIC**) relationship between the routing application and the reacting nodes. TTPs:

- Control HostID/AppID pair scope
- Manage configuration parameters
- Track rate information
- Track their administrative, operational and a throttling status

Information collected at the TTP level for DOIC throttling can be used to improve routing decisions.

You can perform these tasks on an Active System OAM (**SOAM**).

You can perform the following actions for Traffic Throttle Points:

- Filter the list of Traffic Throttle Points to display only the desired Traffic Throttle Points.
- Sort the list by column contents in ascending or descending order by clicking the column heading. The default order is by **Traffic Throttle Points Name** in ascending ASCII order.
- Click **Insert**.
  On the Traffic Throttle Points [Insert] page, you can add a new Traffic Throttle Point. See Adding Traffic Throttle Points.

  If the maximum number of Traffic Throttle Points already exists in the system, an error message displays.
- Select a Traffic Throttle Point **Name** in the list. Click **Edit** to display the Traffic Throttle Points [Edit] page and edit the selected Traffic Throttle Point.
  See Editing Traffic Throttle Points.

  If no **Name** is selected, **Edit** is disabled.
- Select a Traffic Throttle Point **Name** in the list and click **Delete** to remove the selected Traffic Throttle Point.
  See Deleting Traffic Throttle Points.

2.24.1 Diameter Traffic Throttle Point Elements

Table 2-34 describes the fields on the Traffic Throttle Points View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 2-34 Traffic Throttle Point Elements

Field (* indicates a required field)	Description	Data Input Notes
* Name	The name of the Traffic Throttle Point.	Format: case-sensitive; alphanumeric and underscore Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha Default: NA
* Peer Node	The Egress Peer associated with this Diameter Application ID and Traffic Throttle Point.	Format: List Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha Default: NA
* Application ID	The Diameter Application ID associated with this Traffic Throttle Point.	Format: List Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha Default: NA
TTP Configuration Set	The Traffic Throttle Point Configuration Set that is associated with this Traffic Throttle Point.	Format: List Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha Default: NA
* Max Loss Percent Threshold	The rate loss threshold where if the current percent loss is greater than or equal to this value, requests should not route to this Traffic Throttle Point and should be diverted or discarded instead.	Format: text box Range: 1 - 100 Default: 100%
Alternate Implicit Route	Optional Route List to use for routing messages to this Peer when implicit routing is invoked and the primary route to the Peer is unavailable.	Format: List Range: 1 - 100 Default: 100%
* Max ETR	The maximum allowed Egress Transaction Rate for this TTP.	Format: text box Range: 100 - 250000 Default: 6000

2.24.2 Adding Traffic Throttle Points

Use this task to create a new Traffic Throttle Point.

The fields are described in Diameter Traffic Throttle Point Elements.

1. Click **Diameter**, and then **Configuration**, and then **Traffic Throttle Points**.
2. Click **Insert**.
3. Enter a unique name for the Traffic Throttle Point in the **Name** field.
4. Select or enter the element values.
5. Click **OK**, **Apply**, or **Cancel**.

2.24.3 Editing Traffic Throttle Points

Use this task to edit an existing Traffic Throttle Point.

When the Traffic Throttle Pointts page opens, the fields are populated with the currently configured values.

The Traffic Throttle Point **Name** cannot be edited.

The fields are described in Diameter Traffic Throttle Point Elements.

1. Click **Diameter**, and then **Configuration**, and then **Traffic Throttle Points**.
2. Select the Traffic Throttle Point you want to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

2.24.4 Deleting Traffic Throttle Points

Use this task to delete Traffic Throttle Points.

The default Traffic Throttle Point can be edited, but cannot be deleted.

1. Click **Diameter**, and then **Configuration**, and then **Traffic Throttle Points**.
2. Select the Traffic Throttle Point you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.25 Diameter Traffic Throttle Groups

A Traffic Throttle Group (**TTG**) is a set of **TTP**s that share a common Application ID. A TTG is used for diverting transactions away from congested Route Groups (RGs). When a TTG is created and enabled for service, traffic loss is aggregated for the TTPs assigned to the TTG. Transactions are diverted away from congested RGs within a RL by assigning the TTG to a RG within a RL and assigning it a Maximum Loss Percentage Threshold. When the routing application selects a RG from a RL that is assigned an active TTG, it determines whether the TTG's Current Traffic Loss exceeds the RG's Maximum Loss Percentage Threshold. If the threshold is exceeded, that **RG** is bypassed for routing that transaction.

To make routing decisions at the Route List level it is necessary to aggregate some of the individual TTP-level data into data that represents the entire Route Group. This summary data is a Traffic Throttling Group (**TTG**). Only one parameter is summarized in the TTG:

- The calculated Loss % of the TTG. This is the weighted (by Max ETR) average of the % loss in the available TTPs.

The routing application can use the congestion information in the TTGs to skip Route Groups in the Route List that do not meet threshold criteria for their congestion status. A typical use for skipping congested Route Groups is to prevent a routing application that cannot handle traffic due to congestion from sending that traffic to a mate routing application that is already equally overloaded.

> **Note**
>
> Only TTGs that are configured locally can be administratively enabled or disabled by an SOAM. A Shared TTG owned by another site must be disabled at the owning site.

You can perform these tasks on an Active System OAM (**SOAM**).

You can perform the following actions for Traffic Throttle Groups:

- Filter the list of Traffic Throttle Groups to display only the desired Traffic Throttle Groups.
- Sort the list by column contents in ascending or descending order by clicking the column heading. The default order is by Traffic Throttle Groups **Name** in ascending ASCII order.
- Click **Insert**.
  On the Traffic Throttle Groups [Insert] page, you can add a new Traffic Throttle Group. See Adding Traffic Throttle Groups.

  If the maximum number of Traffic Throttle Groups already exists in the system, an error message displays.
- Select a Traffic Throttle Group **Name** in the list. Click **Edit** to display the Traffic Throttle Groups [Edit] page and edit the selected Traffic Throttle Group.
  See Editing Traffic Throttle Groups.

  If no **Name** is selected, **Edit** is disabled.
- Select a Traffic Throttle Group **Name** in the list and click **Delete** to remove the selected Traffic Throttle Group.

2.25.1 Diameter Traffic Throttle Groups Elements

Table 2-35 describes the fields on the Traffic Throttle Groups View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 2-35 Traffic Throttle Groups Elements

Field (* indicates a required field)	Description	Data Input Notes
* Name	A name of the Traffic Throttle Group	Format: text box 1 - 32 characters; cannot start with a digit and must contain at least one alpha Default: NA
* TTP	TTPs associated with this TTG	Format: List Range: NA Default: NA
* Application ID	The Diameter Application ID associated with this Traffic Throttle Group	Format: List Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha Default: NA

2.25.2 Adding Traffic Throttle Groups

Use this task to create a new Traffic Throttle Group.

The fields are described in Diameter Traffic Throttle Groups Elements.

> **Note**
>
> When you select an Application Id to the Traffic Throttle Group, you are only allowed to select the TTP whose application ID matches the application ID that of Traffic Throttle Group.

1. Click **Diameter**, and then **Configuration**, and then **Traffic Throttle Groups**.
2. Click **Insert**.
3. Enter a unique name in the **Name** field.
4. Select or enter the element values.
5. Click **OK**, **Apply**, or **Cancel**.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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 **Name** is not unique; it already exists in the system.
   - The maximum number of TTGs has already been configured.

2.25.3 Editing Traffic Throttle Groups

Use this task to edit an existing Traffic Throttle Group.

When the Traffic Throttle Groups page opens, the fields are populated with the currently configured values.

The Traffic Throttle Point Groups **Name** cannot be edited.

The fields are described in Diameter Traffic Throttle Groups Elements.

1. Click **Diameter**, and then **Configuration**, and then **Traffic Throttle Groups**.
2. Select the Traffic Throttle Point Group to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

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

   - The selected Traffic Throttle Group no longer exists; it has been deleted by another user.
   - Any field is empty (no value was entered).
   - If you attempt to update a TTG and mark it as shared, but the NOAM is not accessible.

- If you attempt to mark the shared TTG to non-shared when it is already being used by a Route List configured on another DSR within this network.
- The value in any field is not valid or is out of range.

2.25.4 Deleting Traffic Throttle Groups

Use this task to delete Traffic Throttle Groups.

1. Click **Diameter**, and then **Configuration**, and then **Traffic Throttle Groups**.
2. Select the Traffic Throttle Group you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.26 Diameter AVP Removal Lists

The AVP Removal function allows you to specify which AVPs to remove. You can also exclude AVPs on a specific Peer by specifying which AVPs and in what type of message (request or answer).

You can perform these tasks on an Active System OAM (**SOAM**).

You can perform the following actions for AVP Removal Lists:

- Filter the list of AVP Removal Lists to display only the desired AVP Removal Lists.
- Sort the list by column contents in ascending or descending order by clicking the column heading. The default order is by **AVP Removal Lists** in ascending ASCII order.
- Click **Insert**.
  On the AVP Removal Lists [Insert] page, you can add a new AVP Removal List. See Adding AVP Removal Lists.

  If the maximum number of AVP Removal Lists already exists in the system, an error message displays.
- Select a AVP Removal List **Name** in the list. Click **Edit** to display the AVP Removal Lists [Edit] page and edit the selected AVP Removal List.
  See Editing AVP Removal Lists.

  If no **Name** is selected, **Edit** is disabled.
- Select a AVP Removal List **Name** in the list and click **Delete** to remove the selected AVP Removal List.
  The default AVP Removal List can be edited, but cannot be deleted. See Deleting AVP Removal Lists.

2.26.1 Diameter AVP Removal Lists Elements

Table 2-36 describes the fields on the **Diameter**, and then **AVP Removal Lists**, and then **View, Insert, and Edit** pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 2-36 AVP Removal Lists Elements

Field (* indicates a required field)	Description	Data Input Notes
* Name	A name of the AVP Removal List	Format: text box Range: 1 - 32 characters; cannot start with a digit and must contain at least one alpha Default: NA
* Direction	Defines whether the AVP removal occurs when the message is received from the peer node or whether the AVP removal occurs when the message, or both, is sent to the peer node	Format: List Range: Ingress Only, Egress Only, Egress & Ingress Default: Ingress Only
* Message Type	Defines the type of message that AVP removal is applied to	Format: List Range: Request Only, Answer Only, Answer & Request Default: Request Only
AVP Removal List	A list of one or more AVPs to be removed from messages	Format: multiple fields Range: A list of one or more AVPs to be removed from requests. Default: NA
AVP Code	The 32-bit AVP Code, combined with the Vendor-ID field, identifies the attribute uniquely	Format: text box Range: 32-bit Unsigned Integer Default: NA
AVP Name	User-defined name associated with the AVP Code	Format: text box Setting a value on this field is option; informational only.
Vendor ID	Vendors are allowed to add AVPs to the Diameter specification. Vendor-specific AVPs contains a Vendor-ID field	Format: text box Range: 32-bit Unsigned Integer Default: 0
Vendor Name	User-defined name associated with the Vendor-ID value	Format: text box Setting a value on this field is option; informational only.

2.26.2 Adding AVP Removal Lists

Use this task to create a new AVP Removal List.

The fields are described in Diameter AVP Removal Lists Elements.

1. Click **Diameter**, and then **Configuration**, and then **AVP Removal Lists**.
2. Click **Insert**.
3. Enter a unique name in the **Name** field.
4. Select or enter the element values.
5. Click **OK**, **Apply**, or **Cancel**.

If **OK** or **Apply** is clicked and any of the following conditions exist, then 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 AVP Removal Lists **Name** is not unique; it already exists in the system.

2.26.3 Editing AVP Removal Lists

Use this task to edit an existing AVP Removal List.

When the AVP Removal Lists page opens, the fields are populated with the currently configured values.

The **AVP Removal List Name** cannot be edited.

The fields are described in Diameter AVP Removal Lists Elements

1. Click **Diameter**, and then **Configuration**, and then **AVP Removal Lists**.
2. Select the AVP Removal List you want to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

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

   - The selected AVP Removal List 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.

2.26.4 Deleting AVP Removal Lists

Use this task to delete AVP Removal Lists.

1. Click **Diameter**, and then **Configuration**, and then **AVP Removal Lists**.
2. Select the AVP Removal List you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

   If **OK** is clicked and the selected AVP Removal List is referenced by any peer node, then an error message appears and the AVP Removal Lists are not deleted.

2.27 Diameter Rf Message Copy

vDSR maintains a new Rf message copy table. This table contains the list APNs that need message copy to the Diameter MPN Proxy Peer.

You can enable the Rf Message Copy feature only if the Message Copy feature is enabled. However, you can disable this feature any time.

Use the **Filter** button to display only the required APNs in the Rf Message Copy table. To arrange the APNs in an ascending order, click the APN column heading. This feature does not support the update task.

2.27.1 Adding a New Rf Message Copy

Perform the following procedure to add APNs to the Rf Message Copy table.

1. On the Oracle Communications Diameter Signaling Router GUI, click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Rf Message Copy**.
2. In the Table Description: Rf Message Copy area, click **Insert**.
3. In the Adding a new Rf Message Copy area, in the Value column, enter a value for the Access Point Name (APN).

   The value range is from 1-100 characters, and it is case-sensitive. The valid characters are alphabet (A-Z and a-z), digits (0-9), hyphen (-), and period (.). This string must start and end with an alphabetic character or a digit.
4. Click **Apply**.
5. Click one of the following buttons:
   - **Ok**: To update the configured APN value in the database and re-render the Rf Message Copy table with a new APN.
   - **Cancel**: To terminate the creation of a new APN instance.

2.27.2 Removing an Existing Rf Message Copy

1. On the Oracle Communications Diameter Signaling Router GUI, click **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Rf Message Copy**.
2. In the Table Description: Rf Message Copy area, select an APN that you want to remove from the APN column, and then click **Delete**.

   You can select only one APN at a time.

   The system removes the selected APN from the Rf Message Copy table.

2.28 Diameter Application Priority Options

This feature allows DSR to support Diameter Routing Message Priority (DRMP). DRMP allows Diameter to include DRMP Attribute-Value Pair (AVP) in Diameter messages to specify the relative priority of the Diameter message on a scale of 0 to 15 where priority value zero is specified as the highest priority and priority value 15 is the lowest priority.

When a Diameter node which supports DRMP receives a message containing a DRMP AVP, it is required to make any Diameter overload throttling decisions based upon the relative DRMP message priority. For example, lower priority messages are throttled before higher priority messages. The DRMP AVP can be appended to Request and Answer messages. A DRMP AVP appended to a Request message represents the priority of all messages associated with the end-to-end Diameter transaction. A Diameter endpoint node can optionally modify the priority of the Answer message for that transaction by appending a DRMP AVP.

Diameter Application Priority Options can be viewed and set on the **Diameter**, and then **Configuration**, and then **Application Priority Options** page.

You can perform these tasks on an active System OAM (**SOAM**).

On the **Diameter**, and then **Configuration**, and then **Application Priority Options** page, you can:

- Filter the list of Application Priority Options to display only the desired Applications.
- Sort the list by a column in ascending or descending order by clicking the column heading. The default order is by **Application Name** in ascending ASCII order.
- Click **Insert**.
  On the Application Priority Options [Insert] page, you can add a new Application. See Adding Application Priority Options.
- Select an Application in the list and click **Edit** to display the Application Priority Options [Edit] page and edit the options associated with the selected Application. See Editing Application Priority Options.
- Select an Application in the list and click **Delete** to remove the selected Application. See Deleting Application Priority Options.

2.28.1 Diameter Application Priority Options Elements

Table 2-37 describes the fields on the Application Priority Options page.

Table 2-37 Application Priority Options Elements

Field	Description	Data Input Notes
* Application Name	Diameter Application Name.	Format: field Range: none Default: 60000
* Application ID	Identifies a specific Diameter Application ID value associated with the Diameter Application Name.	Format: option Range: enabled, disabled Default: Disabled
NGN-PS 3GPP AVP Admin State	Defines if the NGN-PS feature is enabled for the selected Diameter Application.	Format: option Range: enabled, disabled Default: Disabled
NGN-PS DRMP AVP Admin State	Defines if a Diameter message can be tagged as invioable when DRMP AVP = 0 is received in a message	Format: option Range: enabled, disabled Default: Disabled
Request DRMP AVP Admin State	Defines if DRMP AVPS in normal Request messages are honored for this Application.	Format: option Range: enabled, disabled Default: Disabled
Answer DRMP AVP Admin State	Defines if DRMP AVPS in Answer messages associated with non-NGN-PS transactions are honored for this Application.	Format: option Range: enabled, disabled Default: Disabled

2.28.2 Adding Application Priority Options

Use this task to add a new application option to the priority list.

The fields are described in Diameter Application Priority Options Elements.

1. Click **Diameter**, and then **Configuration**, and then **Application Priority Options**.

2. Click **Insert**.
3. Select the **Application ID**.

   The Application Name corresponding with the Application ID is automatically populated.
4. Change any options for the Application.
5. Click **Apply** or **Cancel**.

2.28.3 Editing Application Priority Options

Use this task to edit an existing Application Priority Options.

When the Application Priority Options page opens, the fields are populated with the currently configured values.

You cannot edit greyed out fields on the Application Priority Options tabs.

The fields are described in Diameter Application Priority Options Elements.

1. Click **Diameter**, and then **Configuration**, and then **Application Priority Options**.
2. Select the Application row you want to edit.
3. Click **Edit**.
4. Change the options for the Application you selected.
5. Click **OK**, **Apply**, or **Cancel**.

2.28.4 Deleting Application Priority Options

Use this task to delete an Application from the priority options.

When the Application Priority Options page opens, the fields are populated with the currently configured values.

You cannot edit greyed out fields on the Application Priority Options tabs.

The fields are described in Diameter Application Priority Options Elements.

1. Click **Diameter**, and then **Configuration**, and then **Application Priority Options**.
2. Select the Application row you want to delete.
3. Click **Delete**.

   A window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.29 Diameter System Options

Diameter System Options can be viewed and set on the **Diameter**, and then **Configuration**, and then **System Options** page.

You can perform these tasks on an active System OAM (**SOAM**).

> **Note**
>
> See Next Generation Network Priority Service (NGN-PS) for an overview of NGN-PS.

On the **Diameter**, and then **Configuration**, and then **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**, **Radius UDP Options**, **Peer Discovery Options**, or **Priority Options** tab to access those options.

2.29.1 Diameter System Options Elements

The following table describes the fields on the System Options page:

Table 2-38 System Options Elements

Field (* indicates required field)	Description	Data Input Notes
	General Options	
Engineered Message Size Allowed	Engineered message size of a diameter message (in bytes) allowed by the application. This field is read-only; it cannot be changed.	Format: Field Range: none Default: 60000
Interval ICMP ping of all peer next-hops	If checked, an ICMP ping echo is sent to the next-hop of every remote peer every 2 minutes. This is useful for keeping switch address tables up-to-date.	Format: Checkbox Range: Checked (enabled), not checked (disabled) Default: Disabled
IPFE Connection Reserved Ingress MPS Scaling	Percentage of DA-MP engineered ingress MPS used by each DA-MP when validating the reserved ingress MPS for a newly received floating IPFE connection. A newly received floating IPFE connection is rejected if the total connection reserved ingress MPS for fixed and already established floating IPFE connections would exceed the DA-MP's engineered ingress MPS, scaled by this value. This field is view-only; it cannot be user-configured.	Format: Field Range: 30-100 percent Default: 50 percent

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
Redirect Answer Processing Enabled	If checked, redirect notification response processing is enabled. If unchecked, redirect notification response processing is disabled. If disabled, redirect notification responses are passed through to the downstream peer. Redirect notifications are processed as follows: • Redirect notifications with redirect-host-usage equal to do not cache are processed. • Redirect notifications with no redirect-host-usage AVP are processed. • Redirect notifications with redirect-host-usage not equal to do not cache are forwarded to the downstream peer.	Format: Checkbox Range: Checked (enabled), not checked (disabled) Default: none
Redirect Application Route Table	Application route table instance used to process a redirected request. **Note**: If not configured, ART processing is skipped, and if configured, the ART is searched with the content of the redirect request message, similar to an ingress request.	Format: List Range: none Default: none
Redirect Peer Route Table	Peer route table instance used to process a redirected request. **Note**: If not configured, the PRT selection process is identical to the ingress request.	Format: List Range: none Default: none
Encode FQDN In Lower Case	Determines whether or not FQDNs should be encoded as configured or in all lower-case.	Format: Options Range: Yes, No Default: Yes
* Excessive Reroute Onset Threshold	Excessive reroute alarm is raised when percentage of the total rerouted messages due to answer response and/or answer timeout to the total requests forwarded exceeds the onset threshold value.	Format: Field Range: 1-100 Default: 20

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
* Excessive Reroute Abatement Threshold	Excessive reroute alarm is cleared when percentage of the total rerouted messages due to answer response and/or answer timeout to the total requests forwarded is less than this abatement threshold for configured abatement time. The excessive reroute abatement threshold field value must be less than excessive reroute onset threshold field value.	Format: Field Range: 0-99 percent Default: 15 percent
Discard Policy	The order of priority and/or color-based traffic segments to consider when determining discard candidates for the application of treatment during Congestion processing.	Format: List Range: Color Within Priority, Priority Within Color, Priority Only Default: Priority Only
ETG Mode	Defines the type of message throttling supported when routing Request messages to connections associated with ETGs. Threshold - Threshold Mode is legacy mode, which configures the congestion level for ETGs and enforce the Requests based on congestion level of ETG. Limit - Limit Mode shapes the egress message rate according to the maximum message and pending transaction rate, the system discard policy, and the current mix of requests by message color and priority.	Format: List Range: Threshold, Limit Default: Threshold
Routing Thread Pool Utilization Enabled	If checked, Routing Thread Pool Utilization functionality is enabled, which calculates the CPU utilization of thread pools that runs mediation logic on routable messages. If unchecked, Routing Thread Pool Utilization functionality is disabled. A non-operational thread pool performance alarm is raised if DA-MP is not restarted after enabling the functionality.	Format: Checkbox Range: Checked (enabled), not checked (disabled) Default: none

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
Alarm Group Feature Enabled	If checked, Alarm Group Feature functionality is enabled for the Peer Nodes and Connections. Peers and Connections must be added respectively to the Peer Node Alarm Group and Connection Alarm Group for Alarm Group feature. Enabling of Alarm Group feature automatically disables the Alarm Aggregation feature for all Peer Nodes and Connections.	Format: Checkbox Range: Checked (enabled), not checked (disabled) Default: Disabled
Max number of retry within same Route Group	Total number of retry within same route group on answer timeout. DSR re-routes request to peer or connection within the same route group up to a specified number of times as defined in Max number of retry within same Route Group.	Range: 0-4 Default: 0
Interface and Result Code Level Measurement Enabled	If checked, Interface and Result Code Level Measurement Feature is enabled. All the Measurements present in the Interface Level Connection group will get pegged. If unchecked, Interface and Result Code Level Measurement Feature is disabled and thus measurements defined under Interface Level Connection group will not get pegged.	Default: Checked (Enabled) Range: Checked (enabled), Unchecked (disabled)
	Alarm Threshold Options	
* Available Alarm Budget	The engineered combined total supported alarms allowed for Fixed Connection, floating IPFE Connection, Peer Node, and Route List managed objects. The value displayed on the System Option screen is 3,000 minus the default values for each threshold field.	Format: Field Range: 0-3000 Default: 3000
* Fixed Connection Failure Major Aggregation Alarm Threshold	Major threshold for fixed connection failure alarm aggregation per DA-MP. The available alarm budget is decremented by this value multiplied by the number of configured DA-MPs.	Format: Field Range: 1 to Available Alarm Budget Default: 100
* Fixed Connection Failure Critical Aggregation Alarm Threshold	Critical threshold for fixed connection failure alarm aggregation per DA-MP. This value is not counted against the available alarm budget.	Format: Field Range: 0 to Available Alarm Budget Default: 200

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
* Floating IPFE Connection Failure Major Aggregation Alarm Threshold	Major threshold for aggregated floating IPFE connection alarms per NE. The available alarm budget is decrement by this value.	Format: Field Range: 1 to Available Alarm Budget Default: 100
* Floating IPFE Connection Failure Critical Aggregation Alarm Threshold	Critical threshold for aggregated floating IPFE connection alarms per NE. This value is not counted against the available alarm budget.	Format: Field 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: Field Range: 1 to Available Alarm Budget Default: 600
* 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: Field 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: Options Range: enabled, disabled Default: disabled
MP Congestion Level	The MP congestion at or above which the message copy function is disabled.	Format: Options Range: CL1, CL2 Default: CL1
Rf Message Copy Feature	Enables and disables the Rf Message Copy feature. You can enable this feature only if the Message Copy feature is enabled.	Format: Options Range: Enabled, Disabled Default: Disabled
MCCS For RF Message Copy	Provides a list of configured Message Copy Configuration Sets. Rf Message Copy uses the selected Message Copy Configuration Set. When the value is **mccs**, it uses the configurations of the Message Copy Configuration Sets table. The default value cannot be deleted.	Format: List Range: Default, Message Copy Configuration Sets] (mccs) Default: NA
	Radius UDP Options	
Client Socket Send Buffer Size	The socket sends buffer size for outgoing UDP messages sent to RADIUS servers	Format: Field Range: 8000 - 5000000 bytes Default: 126000
Client Socket Receive Buffer Size	The socket receives buffer size for incoming UDP messages received from RADIUS servers.	Format: Field Range: 8000 - 5000000 bytes Default: 126000

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
Server Socket Send Buffer Size	The socket sends buffer size for outgoing UDP messages sent to RADIUS clients.	Format: Field Range: 8000 - 5000000 bytes Default: 1000000
Server Socket Receive Buffer Size	The socket receive buffer size for incoming UDP messages received from RADIUS clients.	Format: Field Range: 8000 - 5000000 bytes Default: 1000000
Maximum Open RADIUS UDP Sockets per DA-MP	Maximum number of UDP Sockets that can be opened on a DA-MP for sending messages to RADIUS connections.	Format: Field Range: none Default: 2000
Server socket retry timer	The time internal used to retry opening a UDP socket which could not be opened.	Format: Field Range: none Default: 10000 ms
	Radius Routing Options	
AAA Route List	List of configured AAA Route Lists. Radius Routing Table can use the selected route list for routing.	Format: Field Range: Default, Configured Route Lists Default: NA
MPN Route List	List of configured MPN Route List. Radius Routing Table can use the selected route list for routing.	Format: Field Range: Default, Configured Route Lists Default: NA
UMF Route List	List of configured UMF Route List. Radius Routing Table can use the selected route list for routing.	Format: Field Range: Default, Configured Route Lists Default: NA
	Peer Discovery Options	
Realm Expiration Minor Alarm Set Time	Time, in hours before the expiration of a dynamically-discovered realm, at which a minor alarm is raised to indicate that the realm expiration is approaching. A value of zero means no minor alarm is raised to alert of the pending realm expiration.	Format: Field Range: 0 - 168 hours Default: 6
Realm Expiration Major Alarm Set Time	Time, in hours before the expiration of a dynamically-discovered realm, at which a major alarm is raised to indicate that the realm expiration is approaching. A value of zero means no major alarm is raised to alert of the pending realm expiration.	Format: Field Range: 0 - 167 hours Default: 1
	Priority Options	

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
16 Priority Admin State	Defines whether the DSR supports 15 or 5 message priorities. When set to **Disabled**, DSR supports 5 internal message priorities. When set to **Enabled**, the discard policy is set to Policing Mode.	Format: Options Range: enabled, disabled Default: disabled
NGN-PS Admin State	Defines whether the NGN-PS is enabled or not. When set to **Disabled**, DSR does not provide NGN-PS treatment to any messages.	Format: Options Range: enabled, disabled Default: disabled
Answer Priority Mode	Defines which method to be used for assigning priority to Answer messages. If Highest Priority, Answers will have highest priority (or 1 lower than Highest when 'NGN-PS Admin State' is set to Enabled. When this method is selected, DRMP AVPs in Answer messages are ignored. If Request Priority, Answers have the same priority as Requests.	Format: Options Range: Highest Priority, Request Priority Default: Highest Priority
Minimum Inviolable Priority	Defines the minimum priority considered to be inviolable from a message priority treatment perspective. A message with a priority greater than or equal to this attribute value is not subject to congestion controls. **Note**: This attribute is not user-configurable. Each DA-MP sets this value at start-up based upon the setting of the NGN-PS admin state attribute value as follows: • NGN-PS Admin State = Enabled: 4 • NGN-PS Admin State = Disabled: 3	Format: Textbox Range: P3, P4 Default: P3
Minimum Answer Priority	Defines the minimum priority assigned to ingress Answer messages. The priority is assigned based on the maximum value for this attribute and the priority of the original request message. **Note**: This attribute is not user-configurable.	Format: Textbox Range: P1 - P4 Default: P3

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
Maximum Normal Request Priority	Defines the maximum priority that can be assigned to an ingress normal (that is, non-NGN-PS) Request message. **Note**: This attribute is not user-configurable.	Format: Textbox Range: Default:
Maximum Priority-0 Allowed	Defines the maximum priority that will be converted to priority '0' when a message or stack event is sent from a 16 priority scheme system to a 5-priority scheme system. When **16 Priority Admin State** is to Enabled, this option can be changed.	Format: Textbox Range: 0 - 13 Default: 5
Maximum Priority-1 Allowed	Defines the maximum priority that will be converted to priority '1' when a message or stack event is sent from a 16 priority scheme system to a 5-priority scheme system. When **16 Priority Admin State** is to Enabled, this option can be changed.	Format: Textbox Range: 1 - 14 Default: 10
Maximum Priority-2 Allowed	Defines the maximum priority that will be converted to priority '2' when a message or stack event is sent from a 16 priority scheme system to a 5-priority scheme system. When **16 Priority Admin State** is to Enabled, this option can be changed.	Format: Textbox Range: 2 - 15 Default: 14
NGN-PS Maximum Message Rate Percent	Defines the maximum ingress NGN-PS message that is supported (a percentage of the DA-MP message rate). NGN-PS traffic in excess of this rate, is not considered to be inviolable.	Format: Field Range: 1 - 15 Default: 3
	NGN-PS Gx	
NGN-PS Gx Admin State	Defines whether the NGN-PS is enabled or not for Gx messages. When set to **Disabled**, DSR does not provide NGN-PS treatment to Gx messages. **Note**: This attribute is superseded by the **NGN-PS Admin State** attribute. If **NGN-PS Admin State** is set to **Disabled**, no Gx messages are provided NGN-PS treatment regardless of the setting of this attribute.	Format: Options Range: enabled, disabled Default: disabled

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
NGN-PS Gx ARP	Sets the priority level contained in Gx messages in ARP AVP that can be treated as NGN-PS messages. **Note**: You can configure a maximum of 5 priority levels.	Format: Field Range: 1-5 Default: none
NGN-PS Gx Advance Priority Type	Determines the Access Network priority provided to an NGN-PS Subscribed UE. This affects the tagging of Gx CCR messages for NGN-PS treatment.	Format: Options Range: None, Advance Priority SPR, and Advance Priority HSS Default: none
	NGN-PS Rx	
NGN-PS Rx Admin State	Defines whether the NGN-PS feature is enabled or not for Rx messages. When this attribute is set to **Disabled**, DSR does not provide NGN-PS treatment to Rx messages. **Note**: This attribute is superseded by the **NGN-PS Admin State** attribute. If **NGN-PS Admin State** is set to **Disabled**, no Rx messages are provided NGN-PS treatment regardless of the setting of this attribute.	Format: Options Range: enabled, disabled Default: disabled
NGN-PS Rx MPS AVP Value	A Rx AAR message is considered a NGN-PS message candidate if it contains a MPS-Identifier AVP whose value is identical to this string.	Format: Field Range: none Default: none
	NGN-PS Cx/Dx	
NGN-PS Cx/Dx Admin State	Defines whether the NGN-PS feature is enabled or not for Cx/Dx messages. When this attribute is set to **Disabled**, DSR does not provide NGN-PS treatment to Cx/Dx messages. **Note**: This attribute is superseded by the **NGN-PS Admin State** attribute. If **NGN-PS Admin State** is set to **Disabled**, no Cx/Dx messages are provided NGN-PS treatment regardless of the setting of this attribute.	Format: Options Range: enabled, disabled Default: disabled
	NGN-PS Dh/Sh	

Table 2-38 (Cont.) System Options Elements

Field (* indicates required field)	Description	Data Input Notes
NGN-PS Dh/Sh Admin State	Defines whether the NGN-PS feature is enabled or not for Dh/Sh messages. When this attribute is set to **Disabled**, DSR does not provide NGN-PS treatment to Dh/Sh messages. **Note**: This attribute is superseded by the **NGN-PS Admin State** attribute. If **NGN-PS Admin State** is set to **Disabled**, no Dh/Sh messages are provided NGN-PS treatment regardless of the setting of this attribute.	Format: options Range: enabled, disabled Default: disabled

2.29.2 Editing System Options

Use this task to edit an existing System Options.

When the System Options page opens, the fields are populated with the currently configured values.

You cannot edit greyed out fields cannot be edited on the System Options tabs.

The fields are described in Diameter System Options Elements.

1. Click **Diameter**, and then **Configuration**, and then **System Options**.
2. Select the System Options tab you want to edit.
3. Update the relevant fields.
4. Click **Apply** or **Cancel**.

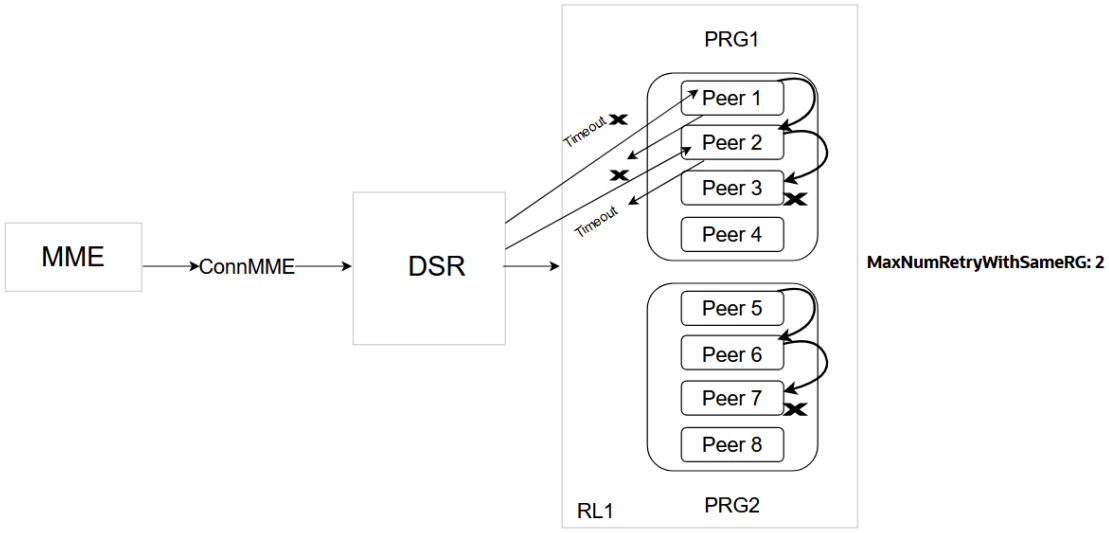
2.29.3 Timeout Based Redirection

When MME sends a request to DSR and the request gets timed out, based on the configured value in the **Pending Answer timeout interval** field on the DSR GUI, DSR forwards the request to the next available peer or connection within the selected route group. When the routing fails, rerouting continues until the predefined limit is reached, referred to as **Maximum Per Message Forwarding Allowed** or **Transaction Lifetime**, as configured in the **Routing Option Sets**.

With the timeout based redirection feature, DSR can re-route request to peer or connection within the same route group up to a specified number of times as defined in **Max number of retry within same Route Group**. When the count of reroutes attempts reaches the maximum limit, it re-routes the request to the next route group based on their priority.

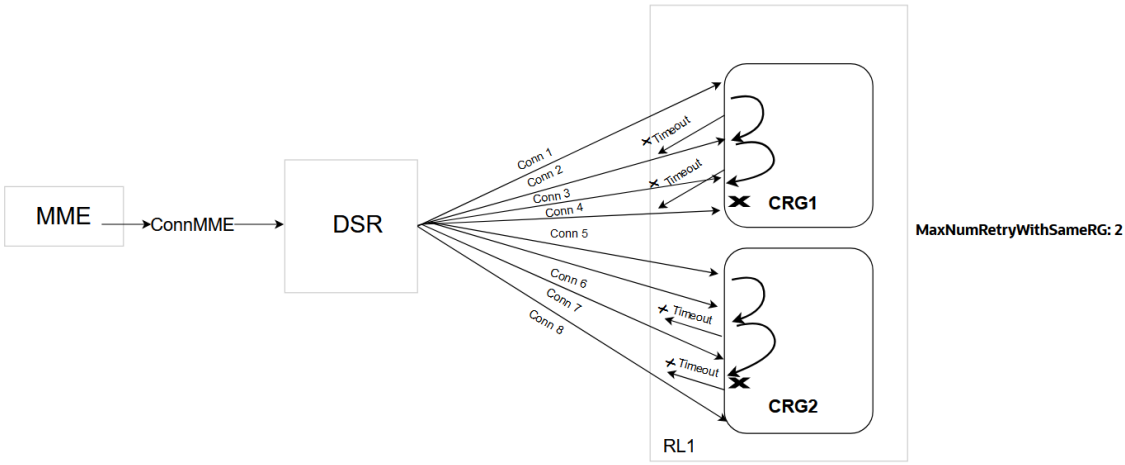
The following image describes the timeout based redirection in the peer route group:

Figure 2-1 Timeout Based Redirection Peer Group



The following image describes the timeout based redirection in the connection route group:

Figure 2-2 Timeout Based Redirection Connection Group



Perform the following procedure to configure the maximum number of retries within the same route group:

1. Log in to the DSR GUI using your login credentials.
2. From the **Main Menu**, click **Diameter**.
3. Click **Configuration**, and then click **System Options**.
4. In the **System Options** page, search for the option **Max number of retry within same Route Group** and edit the value.

The timeout can be set within a range of 0 to 4:

- 0: feature is disabled (range 0: implies that there is no limitation on the max attempts in the same route group).

- 1-4: feature is enabled (range 1-4: implies that the number of times the routing takes place based on the set limit in the same route group).

> **Note**
>
> The limit is not applicable for the last and single route group.

2.30 Diameter DNS Options

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

You can perform these tasks on an Active System OAM (**SOAM**).

To open the **Diameter**, and then **Configuration**, and then **DNS Options** page, select **Diameter**, and then **Configuration**, and then **DNS Options**.

The DNS Options fields are described in Diameter DNS Options Elements.

On the **Diameter**, and then **Configuration**, and then **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, then 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

2.30.1 Diameter DNS Options Elements

Table 2-39 describes the fields on the **Diameter**, and then **Configuration**, and then **DNS Options** page.

Table 2-39 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

2.30.2 Editing DNS Options

Use this task to edit an existing DNS Options.

The fields are described in Diameter DNS Options Elements.

1. Click **Diameter**, and then **Configuration**, and then **DNS Options**.
2. Update the relevant fields.
3. Click **Apply** or **Cancel**.

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

   - The selected Traffic Throttle Point 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.

2.31 Diameter Peer Discovery

Peer Discovery (also know as Dynamic Peer Discovery [**DPD**]) allows an application to discover remote hosts within user-defined Realms and configures all required GUI elements for successful routing of diameter traffic between the signalling router and those remote hosts. This configuration is dynamic, and no user input is required at the time the routing GUI elements are created.

You can perform these tasks on an Active System OAM (**SOAM**).

In general, Peer Discovery configuration order is as follows:

- Peer Node
- CEXCfgSet
- Connection
- Route Group
- Route List

> **Note**
>
> This order is not guaranteed; in some configurations, variations associated with a particular Application ID could alter this order.

For a Diameter router to route messages properly, target entity information is required. This includes the network entity IP address, the transport protocol and ports that it uses to communicate, and what Diameter application it supports. This information about a remote host is managed by the Peer Node configuration. See Diameter Peer Nodes.

After a Peer Node is defined, one or more IP connections must be defined so that packets can be routed between the diameter router and the Peer Node. **Connections** identify the parameters that define an IP connection, and the **CEX Configuration Set** defines the Diameter Application IDs that the diameter router is authorized to send and receive over the connection. When the diameter signalling router and a diameter peer initially establish an IP

connection between themselves, they negotiate the diameter services that can be carried on that IP connection. That negotiation involves the exchange of supported Diameter Application IDs.

For load balancing and redundancy purposes, multiple Peer Nodes that share certain characteristics can be grouped together into **Route Groups**. The diameter router uses the routing algorithms of the configured Route Groups and Route Lists when determining on which Connection to send a particular Diameter message.

Peer Discovery allows you to work with:

- Realms (see Realms)
- DNS Sets (see DNS Sets)
- Discovery Attributes (see Discovery Attributes)

2.31.1 Realms

The **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Realms** page displays the Realms GUI page.

See Realms Overview for more information.

On the **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Realms** page, you can perform the following actions:

- Filter the list of Realms to display only the desired Realms.
- Sort the list by a column, in ascending or descending order by clicking the column heading. The default order is by **Realm Name** in ascending ASCII order.
- Click **Insert**.
  On the Realms [Insert] page, you can add a new Realm. See Adding Realms.

  If the maximum number of Realms already exists in the system, an error message displays.
- Select a **Realm Name** in the list and click **Edit** to display the **Realms[Edit]** page and edit the selected Realm. See Editing Realms.
- Select a **Realm Name** and click **Delete** to remove the selected **Realm Name**. See Deleting Realms.

2.31.1.1 Realms Overview

A realm is an internet domain whose Fully-Qualified Domain Names (FQDNs) typically all share a domain designation. For example, example.com could be a Realm name, and the addressable hosts in the Realm would have names like host1.example.com, host2.subdomain1.example.com, and so on.

In the diameter signaling space, an operator creates a realm name, then assigns FQDNs to all of the computers that transact diameter traffic. The number of computers in the Diameter Realm depends on the number and type of diameter services the operator intends to support, as well as the expected volume of diameter traffic. Typically, load-sharing and redundancy are major factors governing the internal organization of a Diameter Realm.

The dynamic discovery of remote hosts is always undertaken within a single realm. Many realms can be discovered dynamically, but the discovery of one realm is a process independent of that for all other realms that are to be discovered.

Configuring Routing Information

Diameter signaling routers establish connections to Diameter Peers and route Diameter traffic to those Peers only after all of the necessary routing configuration changes are manually entered into the DSR. Specific configuration changes are user-initiated, either through the GUI or by importing configuration changes by way of Bulk Import/Export (BIE).See the Bulk Import and Export information in *Diameter Common User's Guide*. These configuration changes are static changes because once entered; they remain in place until you take action to modify or delete them.

DPD implies dynamic configuration changes. Instead of user-specified routing configuration changes, the diameter signaling router learns about remote hosts and dynamically makes the necessary routing configuration changes. The information discovered about remote hosts residing in any Diameter Realm has a defined lifetime, a Time To Live (**TTL**). Therefore, realm-specific routing configuration made dynamically to a diameter signaling router also has a defined lifetime, and under certain circumstances, this dynamic routing configuration is automatically destroyed, and the Realm can be re-discovered; all of this occurs without user interaction. Dynamic describes these diameter signaling router-initiated routing configuration changes that are created and destroyed over time.

You should understand the difference between static and dynamic configuration with respect to DPD.

- Static configuration is necessary to set up and execute DPD
- Dynamic configuration results from a Diameter Realm having been successfully discovered

DPD setup and execution requires static configuration. The name of the Realm to be discovered, the DNS server(s) that are used to get information about that Realm, and the necessary additional discovery attributes are all statically configured by a user to establish the input parameters governing the discovery of a particular Diameter Realm. Assuming the discovery algorithm is successful, at least one Peer Node and the Connection(s), CEX Configuration Set(s), Route Group(s), and Route List(s) required to properly route Diameter traffic to the Peer Node(s) are dynamically added to the routing configuration.

Creating Discoverable Realms

Any Diameter Realm that is to be discovered must first be made discoverable by a **DNS** administrator who has knowledge of the hosts within the Realm and the services they provide. The Realm's DNS administrator must set up a DNS zone file that contains all of the information about the Realm that the administrator wants to make public. The DNS zone file resides on any of the Realm's DNS servers that are expected to be queried about Realm services.

The routing application discovers the Realm by sending questions (DNS requests) to the Realm's DNS server or servers. Depending on the answers, the routing application dynamically updates the configuration. These answers are in the form of DNS Resource Records (RRs).

DPD relies on three DNS Resource Record types to obtain the information needed to dynamically configure a Realm. The three types are, in the hierarchical order in which they are requested:

- Name Authority Pointer (**NAPTR**) Record - is a general-purpose DNS record that has uses beyond Diameter
- Service Locator (**SRV**) Record - is another general-purpose DNS record that is used well beyond Diameter signaling
- Address (A or AAAA) Record - is a DNS containing an IP address that can be used to reach the host

Diameter Application IDs

Diameter Application IDs play a major role in the discovery of remote hosts. Diameter messages contain information specific to a particular telecommunications signaling function, and these are identified by Application ID. Nodes within a Diameter network are often set up to address certain signaling functions, but not others. So the Diameter Application ID(s) that are supported by a remote host are an important characteristic of that remote host. When configuring a Realm for discovery, you can specify up to ten Application IDs.

Supported Protocols

Realm discovery depends on information from remote hosts within the Realm. The routing application must discover what protocols can be used while communication with the host. Also important is the list of locally-supported protocols, which are protocols that are supported by the routing application, and thus could use when communicating with a remote host.

The full set of transport protocols that can be used when establishing Diameter connections is:

- TCP
- SCTP
- TLS
- DTLS

DNS Discovery

Realm discovery has two phases:

- DNS information for the Realm is retrieved and processed
  - A NAPTR record is selected
  - A single Diameter S-NAPTR record is selected for attempted resolution
  - If a Realm's DNS information does not include any NAPTR records, the DSR may still be able to learn something useful about the realm through the direct SRV query fallback mechanism.
- The routing application adds the needed configuration objects, based on the prioritized list of remote hosts, to enable proper routing of Diameter traffic to the remote hosts in the Realm. This only occurs after the routing application concludes that sufficient DNS information exists to route Diameter traffic to at least one remote host within the Realm. Converting discovered DNS information into a routing configuration can be a complex undertaking, and it depends entirely on the discovered remote hosts, how many IP addresses each host exposes, the protocol(s) each host supports, and the Application ID(s) each host supports. See Discovery Attributes, Diameter Route Lists, and Diameter Route Groups.

Realm Expiration

DNS is designed such that every piece of DNS information has a defined lifetime. After this time duration passes, the information is considered expired. In many cases, a particular piece of DNS information might not change at all over very long periods of time, but in some cases, the information can change, and users of that information are responsible for retrieving and acting on the updated values.

There are potentially dozens of individual DNS resource records that are processed when discovering a Realm, and each of those **RR**s has its own TTL value. The routing application distills those TTLs down to a single Realm Expiration date/time by taking the nearest-term TTL value from all of the DNS RRs it processes during the Realm's discovery. From the routing

application perspective, a Realm expires after enough time passes that the first relevant DNS record expires. After one piece of information becomes old, the entire Realm's discovered data is considered old. You can set or suppress the pending expiration alarms.

DPD implements a couple of user-configurable pending expiration alarms, in order to notify users that a Realm is approaching is expiration. The user configures each of these two alarms. The Realm Expiration Minor Alarm Set Time, in hours, indicates how many hours before Realm expiration a minor alarm should be raised. This value can be as large as 168 hours (one week) before Realm expiration. The Realm Expiration Major Alarm Set Time, also in hours, indicates how many hours before Realm expiration a major alarm should be raised. This value can be as large as 167 hours, and must always be at least one hour shorter than the Minor Alarm Set Time, if the Minor Alarm Set Time exists.

2.31.1.2 Peer Discovery Realms Elements

Table 2-40 describes fields on the Realms page.

If a Realm name is configured and listed on the View screen, this does not mean that it is subject to Diameter peer discovery. Configured Realms displayed on this screen are candidates for DPD, and the names shown on this screen become available on the Discovery Attributes page.

Table 2-40 Realms Elements

Field	Description	Data Input Notes
Realm Name	Name of the Realm	Format: Text box; case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-), and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores can be used only as the first character. A label can be at most 63 characters long and a Realm can be at most 255 characters long. Range: A valid realm Default: NA
Description	A description of the realm	Format: Text box; description of the realm Range: A valid string up to 255 characters Default: NA

2.31.1.3 Adding Realms

Use this task to create a new Peer Discovery Realm.

The fields are described in Peer Discovery Realms Elements.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Realms**.
2. Click **Insert**.
3. Enter a unique name in the **Realm Name** field.

4. Select or enter the element values.
5. Click **OK**, **Apply**, or **Cancel**.

   If **OK** or **Apply** is clicked and any of the following conditions exist, thenan 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 Realm **Name** is not unique; it already exists in the system.

2.31.1.4 Editing Realms

Use this task to edit an existing Peer Discovery Realm.

When the Realms page opens, the fields are populated with the currently configured values.

The **Realm Name** cannot be edited.

The fields are described in Peer Discovery Realms Elements.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Realms**.
2. Select the Realm Name to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

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

   - The selected Realm Name 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.

2.31.1.5 Deleting Realms

Use this task to delete Peer Discovery Realms.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Realms**.
2. Select the Realm Name you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.
4. Click **OK** or **Cancel**.

2.31.2 DNS Sets

The **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **DNS Sets** page displays the DNS Sets GUI page.

You can perform these tasks on an Active System OAM (**SOAM**).

On the **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **DNS Sets** page, you can perform the following actions:

- Filter the list of DNS Sets to display only the desired DNS Sets.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by **DNS Sets Name** in ascending ASCII order.
- Click **Insert**.
  On the DNS Sets [Insert] page, you can add a new DNS Sets. See Adding DNS Sets.

  If the maximum number of DNS Sets already exists in the system, an error message displays.
- Select a **DNS Sets Name** in the list and click **Edit** to display the **DNS Sets[Edit]** page and edit the selected Realm. See Editing DNS Sets.
- Select a **DNS Sets Name** and click **Delete** to remove the selected **DNS Sets Name**. See Deleting DNS Sets.

2.31.2.1 Peer Discovery DNS Sets Elements

Table 2-41 describes fields on the DNS Sets View, Insert, Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

This DNS Sets page shows all DNS Sets configured for potential Dynamic Peer Discovery.

> **Note**
>
> Although a DNS set is listed on the DNS Sets GUI page, this does not mean it is used for DPD. Configured DNS sets displayed on this page are candidates for DPD; the DNS sets listed here become available on the Discovery Attributes page. See Discovery Attributes.

Table 2-41 DNS Sets Elements

Field	Description	Data Input Notes
DNS Set Name	Name of the DNS 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 Default: NA
Primary DNS Server IP Address	IP address of the primary DNS server.	Format: valid IP address Range: 39 characters (The longest IPv6 address that can be formed is 8 octets of 4 characters (=32) plus seven colon delimiters (=7), for a total of 39 characters.
Secondary DNS Server IP Address	IP address of the secondary DNS server.	Format: valid IP address Range: 39 characters (The longest IPv6 address that can be formed is 8 octets of 4 characters (=32) plus seven colon delimiters (=7), for a total of 39 characters.
DNS Query Timeout (sec)	Specifies how long the application waits for a response from the DNS server.	Format: numeric value Range: 1 - 4 seconds Default: 2

Table 2-41 (Cont.) DNS Sets Elements

Field	Description	Data Input Notes
Number of Retries	Specifies how many times the application retires if the DNA query times out.	Format: numeric value Range: 1 - 3 seconds Default: 2

2.31.2.2 Adding DNS Sets

Use this task to create a new DNS Set.

The fields are described in Peer Discovery DNS Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **DNS Sets**.
2. Click **Insert**.
3. Enter a unique name in the **DNS Set Name** field.
4. Select or enter the element values.
5. Click:
   - **OK** to save the new DNS Set name and return to the DNS Sets page.

     > **Note**
     >
     > This assumes all validation checks pass.

   - **Apply** to save the new DNS Set name and remain on this page.

     > **Note**
     >
     > This assumes all validation checks pass.

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

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

   - Any validation checks fail.
   - Any required field is empty (no value was entered).
   - The value in any field is not valid or is out of range.
   - The DNS Set **Name** is not unique; it already exists in the system.
   - The maximum number of DNS Sets already exists in the system.
   - The secondary IP address duplicates the primary IP address.
   - The pair of IP addresses (primary/secondary) duplicates the pair already defined for another DNS Set.

> **Note**
>
> Exchanging the primary and secondary IP addresses does not constitute a unique DNS set.

2.31.2.3 Editing DNS Sets

Use this task to edit existing DNS Sets.

When the DNS Sets page opens, the fields are populated with the currently configured values.

The **DNS Set Name** cannot be edited.

The fields are described in Peer Discovery DNS Sets Elements.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **DNS Sets**.
2. Select the DNS Set Name to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

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

   - The selected DNS Set Name no longer exists; it has been deleted by another user.
   - The selected DNS Set Name is referenced by one or more administratively enabled Discovery Attributes.

     > **Note**
     >
     > You can edit an administratively disabled Discovery Attribute, because changing the DNS Set attributes has no impact on active Realm discovery.

   - Any validation checks fail.
   - Any required field is empty (no value was entered).
   - The value in any field is not valid or is out of range.
   - The DNS Set **Name** is not unique; it already exists in the system.
   - The maximum number of DNS Sets already exists in the system.
   - The secondary IP address duplicates the primary IP address.
   - The pair of IP addresses (primary/secondary) duplicates the pair already defined for another DNS Set.

     > **Note**
     >
     > Exchanging the primary and secondary IP addresses does not constitute a unique DNS set.

2.31.2.4 Deleting DNS Sets

Use this task to delete DNS Sets.

The default **DNS Set Name** can be edited, but cannot be deleted.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **DNS Sets**.
2. Select the DNS Set you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.

   > **Note**
   >
   > Deletion is only possible if all validation checks pass. If validation fails, an error code displays.

4. Click **OK** or **Cancel**.

2.31.3 Discovery Attributes

The **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Discovery Attributes** page displays the Discovery Attributes GUI page.

You can perform these tasks on an Active System OAM (**SOAM**).

On the **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Discovery Attributes** page, you can perform the following actions:

- Filter the list of Discovery Attributes.

  > **Note**
  >
  > You can filter up to four columns simultaneously by using the compound filter widget.

- Sort by a column, in ascending or descending order, by clicking the column heading.
- Click **Insert**.
  On the **Discovery Attributes**, and then **[Insert]** page, you can add a new Discovery Attribute.

  If the maximum number of Discovery Attributes already exists in the system, an error message displays.
- Select an attribute in the list and click **Edit** to display the **Discovery Attributes[Edit]** page and edit the selected attribute. See Editing Discovery Attributes.
- Select an attribute and click **Delete** to remove the selected item. See Deleting Discovery Attributes.

2.31.3.1 Peer Discovery Attributes Elements

Table 2-42 describes fields on the Discovery Attributes View, Insert, Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

This Discovery Attributes page shows all Discovery Attributes configured for peer discovery.

Table 2-42 Discovery Attributes Elements

Field	Description	Data Input Notes
Realm Name	Name of the Realm where Diameter Peers are to be discovered.	Format: List Range: NA Default: NA
DNS Set	DNS server set used for Peer Discovery.	Format: List Default: -Select-
Local Node	Local Node used to connect to all Peers discovered within the Realm.	Format: List Range: NA Default: Initiator & Responder
Connection Mode	Specifies the connection mode used for Peer discovery.	Format: List Range: • Initiator Only indicates that all connections to discovered Peers are Initiator Only; the application attempts to initiate connection to these Peers. • Initiator and Responder indicates that all connections to discovered Peers are of the type Initiator and Responder; the application attempts to initiate connection to the discovered Peers as well as listen for connection attempts from these Peers. Default: Initiator & Responder
Local Protocol Preference Override	If checked, this indicates that the local protocol preferences specified for each Application ID take precedence over the protocol preferences discovered for each Peer in the Realm.	Format: checkbox Range: checked, unchecked Default: Unchecked
Applications	List of applications used for peer discovery.	
	CEX Parameters CEX parameters to be searched. You can specify up to ten parameters. . If no Vendor IDs are associated with the selected CEX parameter, **Additional Supported Vendor IDs** is empty. **Note**: Because each Realm can have one to ten CEX parameters, you must use the plus (+) symbol to expand the list. Sorting by any of the fields associated with the CEX parameter is not supported on the view page.	**CEX Parameters** Format: List Range: Configured CEX parameters Default: -Select-

Table 2-42 (Cont.) Discovery Attributes Elements

Field	Description	Data Input Notes
	Additional Supported Vendor IDs Vendor IDs, in addition to the one specified in the CEX parameter list, which can be paired with the Application ID.	**Additional Supported Vendor IDs** Format: Selection list Range: Vendor IDs configured for the Application ID Default: NA
	Protocol Preferences If zero, the associated protocol is not used for connections to a discovered Peer. Values 1 - 4 indicate the hierarchical local protocol preferences (1 is most preferred, 4 is least preferred). You can assign the same value to more than one protocol. **Note**: This selection is not required if the Local Protocol Preference Override checkbox is unchecked on the view page.	**Protocol Preferences** Format: Lists for TCP, SCTP, TLS, and DTLS) Range: 0 - 4 Default: -Select-
	Max Num Peers The maximum number of peers within the Realm that are created for the selection Application ID.	**Max Num Peers** Format: numeric Range: 1 - 3 Default: 2
	Max Num Connections The maximum number of peers within the Realm that are created spanning discovered Peers that support the associated Application ID.	**Max Num Connections** Format: numeric Range: 1 - 64 Default: 2
Local IP Address	Specifies the local IP address to be used as the Local Node address for all dynamic connections made to Peers in this Realm. **Note**: SCTP multi-homed connections to discovered Peers are not supported.	Format: List Range: Default:
IPFE Initiator DAMP	Specifies the DA-MP that initiates the dynamic connections. **Note**: This is mandatory if the Local IP Address is a Target Set address; otherwise it is not applicable.	Format: List Range: Default:

Table 2-42 (Cont.) Discovery Attributes Elements

Field	Description	Data Input Notes
Connection Configuration Set	Specifies the configuration set to be used when dynamic connections are made to Peers in this Realm.	Format: List Range: NA Default: Default
Capacity Configuration Set	Specifies the capacity configuration set to be used by all dynamic connections made to Peers in this Realm.	Format: List Range: NA Default: Default
Realm Prefix	Specifies the Realm prefix to be used as the first portion of the name of all configuration objects that are dynamically created by the application as a function of Realm discovery.	Format: text box; case sensitive; alphanumeric and underscore Range: 1 - 12 characters, cannot start with a digit and must contain at least one alpha Range: NA Default: Default

2.31.3.2 Adding Discovery Attributes

Use this task to create new Discovery Attributes.

The fields are described in Peer Discovery Realms Elements.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Discovery Attributes**.
2. Click **Insert**.
3. Specify a unique name in the **Realm Name** field.
4. Select or enter the element values.
5. Click:
   - **OK** to save the new Discovery Attributes and return to the Discovery Attributes page.

     > **Note**
     >
     > This assumes all validation checks pass.

   - **Apply** to save the new Discovery Attributes and remain on this page.

     > **Note**
     >
     > This assumes all validation checks pass.

   - **Cancel** to return to the Discovery Attributes page without saving any changes.

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

   - The **Connection Mode** for a Realm being discovered is Initiator & Responder, and the **Local Node** assigned to the Discovery Attributes instance does not have a Listen Port assigned to at least one protocol.

> **Note**
>
> In order for any dynamically-created Connection to act in the role of Responder, a Listen Port must be assigned for one or more protocols. If the Realm's **Connection Mode** is Initiator, then Listen Ports do not have to be supplied.

- The **Local Protocol Preference Override** value is Yes, and the preference value for all protocols associated with any configured Application Id is zero or is missing.
- Any validation checks fail.
- Any required field is empty (no value was entered).
- The value in any field is not valid or is out of range.
- Any required information is not unique; it already exists in the system.
- The maximum number of any of the discovery attributes already exists in the system.

2.31.3.3 Editing Discovery Attributes

Use this task to edit existing Discovery Attributes.

When the Discovery Attributes page opens, the fields are populated with the currently configured values.

The **Realm Name** cannot be edited.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Discovery Attributes**.
2. Select a row to edit.
3. Click **Edit**.
4. Update the relevant fields.
5. Click **OK**, **Apply**, or **Cancel**.

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

   - The selected element no longer exists; it has been deleted by another user.
   - The selected element is referenced by one or more administratively enabled Discovery Attributes.

   > **Note**
   >
   > You can edit an administratively disabled Discovery Attribute, because changing the DNS Set attributes has no impact on active Realm discovery.

   - Any validation checks fail.
   - Any required field is empty (no value was entered).
   - The value in any field is not valid or is out of range.
   - The **Realm Name** is not unique; it already exists in the system.

- The **Connection Mode** for a Realm being discovered is Initiator & Responder, and the **Local Node** assigned to the Discovery Attributes instance does not have a Listen Port assigned to at least one protocol.

> **Note**
>
> In order for any dynamically-created Connection to act in the role of Responder, a Listen Port must be assigned for one or more protocols. If the Realm's **Connection Mode** is Initiator, then Listen Ports do not have to be supplied.

- The **Local Protocol Preference Override** value is Yes, and the preference value for all protocols associated with any configured Application Id is zero or is missing.
- The maximum number of a selected element already exists in the system.

2.31.3.4 Deleting Discovery Attributes

Use this task to delete Discovery Attributes.

1. Click **Diameter**, and then **Configuration**, and then **Peer Discovery**, and then **Discovery Attributes**.
2. Select the row you want to delete.
3. Click **Delete.**

   A popup window appears to confirm the delete.

> **Note**
>
> Deletion is only possible if all validation checks pass. If validation fails, an error code displays.

4. Click **OK** or **Cancel**.

2.32 Concept Title

(Required) Enter introductory text here, including the definition and purpose of the concept.

Section Title

(Optional) Enter conceptual text here.

Example 2-1 Example Title

(Optional) Enter an example here.

3
Diameter Maintenance

The **Diameter**, and then **Maintenance** pages display status information for Route Lists, Route Groups, Peer Nodes, Connections, Egress Throttle Groups, diameter applications, and Diameter Agent Message Processors (DA-MPs).

On the **Diameter**, and then **Maintenance**, and then **Connections** page you can enable and disable Connections.

3.1 Diameter Maintenance Overview

The **Diameter**, and then **Maintenance** pages allow you to view the following information and perform the following actions:

- On the **Diameter**, and then **Maintenance** pages you can view status information for Route Lists, Route Groups, Peer Nodes, Connections, Egress Throttle Groups, diameter applications, and Diameter Agent Message Processors (DA-MPs).
- On the **Diameter**, and then **Maintenance**, and then **Connections** page you can enable and disable Connections.
- On the **Diameter**, and then **Maintenance**, and then **Applications** page you can enable and disable diameter applications.

3.2 Diameter Maintenance Route Lists

The **Diameter**, and then **Maintenance**, and then **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.

You can perform these tasks on an Active System OAM (**SOAM**).

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**, and then **Maintenance**, and then **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.

3.2.1 Diameter Route List Maintenance Elements

The following table describes fields on the Route Lists Maintenance page:

Table 3-1 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.
Destination-Host	Destination-Host of this route list.
Destination-Realm	Destination-Realm of this route list.
Origin-Host	Origin-Host of this route list.
Origin-Realm	Origin-Realm of this route list.
Route Group	Route groups assigned to the route list.
MP Server Hostname	Hostname of the Message Processor Server from which status is reported. • For a multiple active DA-MP configuration, the MP Leader always reports the route list status. • For an active or standby DA-MP configuration, the Active DA-MP reports the route list status.
Dynamic	Indicates whether or not the element is created dynamically (**Yes**) or statically (**No**). **No** is assigned for all element instances, except for those created through Dynamic Peer Discovery (DPD).
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. • Unknown: 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. • Unknown: status information is not available in the database.
Time of Last Update	Timestamp that displays the last time status information was updated.

3.3 Diameter Maintenance Route Groups

The **Diameter**, and then **Maintenance**, and then **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.

You can perform these tasks on an Active System OAM (**SOAM**).

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**, and then **Maintenance**, and then **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.

3.3.1 Diameter Route Group Maintenance Elements

Table 3-2 describes fields on the **Diameter**, and then **Maintenance Route Groups** page.

Table 3-2 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 statu • For an active/standby DA-MP configuration, the active DA-MP reports the route group statu
Dynamic	Indicates whether or not the element was created dynamically (**YES**) or statically (**NO**). **NO** is assigned for all element instances, except for those created via dynamic peer discovery.
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.

Table 3-2 (Cont.) Route Group Maintenance Elements

Field	Description
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 • Unavailable: the available capacity is zero • Unk: status information is not available in the database
Traffic Measurement	Traffic measurement can be enabled or disabled for a peer route group. Up to 250 route groups can be enabled (including peer and connection route groups). When enabled, this field measures how many request and answer messages are successfully forwarded and received to and from route groups.
Time of Last Update	Time stamp that shows the last time the status information was updated.

3.4 Diameter Maintenance Peer Nodes

The **Diameter**, and then **Maintenance**, and then **Peer Nodes** page provides the operational status of Peer Node connections, including a reason for the status.

You can perform these tasks on an Active System OAM (SOAM).

On the **Diameter**, and then **Maintenance**, and then **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.
- See the name of the Peer Node Alarm Group and any associated Alarm IDs raised by DA-MP for a Peer Node, if the Alarm Group feature has been enabled.

3.4.1 Diameter Peer Node Maintenance Elements

Table 3-3 describes fields on the Peer Nodes maintenance page.

Table 3-3 Peer Nodes Maintenance Elements

Field	Description
Peer Node Name	Name of the Peer Node.
MP Server Hostname	Hostname of MP server from which status is reported. For the Peer Node status: • For a Multiple Active DA-MP configuration, the MP Leader always reports the Peer Node status • For an Active/Standby DA-MP configuration, the Active DA-MP reports the Peer Node status For Connection status (when the Connection field is expanded): • Fixed (non-IPFE) Connections are always reported by the DA-MP that hosts the Fixed Connection • Owned IPFE Connections are always reported by the DA-MP that hosts the established IPFE Connection • Unowned IPFE Connections (ones that have been configured, but are currently not assigned to a DA-MP by IPFE) are reported by the MP Leader
Dynamic	Indicates whether or not the element was created dynamically (**YES**) or statically (**NO**). **NO** is assigned for all element instances, except for those created via Dynamic Peer Discovery.
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.
Peer Node Group Name	A group of Peer Nodes that share common characteristics and attributes. This group is used by IPFE for Peer Node Group Aware connection distribution.
Transaction Configuration Set Name	Unique name of the Transaction Configuration Set.
Peer Node Alarm Group Name	If the Alarm Group feature is enabled (on the **Diameter**, and then **Configuration**, and then **System Options (General Options tab)** page), this column displays the peer node alarm group name where the Peer Node is designated.
Alarm IDs	If the Alarm Group feature is enabled (on the **Diameter**, and then **Configuration**, and then **System Options (General Options tab)** page), this column displays the Alarm ID raised against the Peer Node. If more than one alarm is raised by the DA-MP for a Peer Node, then the values are separated by a comma.

3.5 Diameter Maintenance Connections

The **Diameter**, and then **Maintenance**, and then **Connections** page allows you to view information about existing connections, including the operational status of each connection.

You can perform these tasks on an Active System OAM (SOAM).

On the **Diameter**, and then **Maintenance**, and then **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 Printing and Saving Diagnostics Tool Reports.
- See the name of the Connection Alarm Group and any associated Alarm IDs raised by DA-MP for a Connection, if the Alarm Group feature has been enabled.

3.5.1 Diameter Connection Maintenance Elements

Table 3-4 describes fields on the Connections maintenance page.

Table 3-4 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
Dynamic	Indicates whether or not the element was created dynamically (**YES**) or statically (**NO**). **NO** is assigned for all element instances, except for those created via Dynamic Peer Discovery.

Table 3-4 (Cont.) Connections Maintenance Elements

Field	Description
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
Connection Type	Indicates the connection type (**Diameter** or (**RADIUS**).
Connection Mode	Specifies the connection mode used for Peer discovery. The Connection can have one of the following Connection Modes: **Initiator Only** Indicates that all connections to discovered Peers are Initiator Only; the application attempts to initiate connection to these Peers. **Initiator & Responder** Indicates that all connections to discovered Peers are of the type Initiator & Responder; the application attempts to initiate connection to the discovered Peers as well as listen for connection attempts from these Peers. **RADIUS Server** Indicates that RCL can only receive RADIUS Request messages and send RADIUS Response messages of the Connection. **RADIUS Client** Indicates that RCL can only send RADIUS Request messages and receives RADIUS Response messages of the Connection.
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 (0-98) • 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

Table 3-4 (Cont.) Connections Maintenance Elements

Field	Description
Local Node	Local Node associated with the Connection
Local Port	Specifies the local port used for Peer discovery.
IPFE Initiator DAMP	The IPFE Initiator DA-MP for this 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
Local Initiate Port	The Local Initiate Port 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. **Note**: For local nodes, CEAs are sent in response to erroneous CERs.
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. **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 in seconds that the Connection is 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
Egress Msgs Per Second	The most recent Egress Message Rate on the Connection

Table 3-4 (Cont.) Connections Maintenance Elements

Field	Description
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
Connection Alarm Group Name	If the Alarm Group feature is enabled (on the **Diameter**, and then **Configuration**, and then **System Options (General Options tab)** page), this column displays the connection alarm group name where the connection belongs.
Alarm IDs	If the Alarm Group feature is enabled (on the **Diameter**, and then **Configuration**, and then **System Options (General Options tab)** page), this column displays the Alarm ID raised against the Connection. If more than one alarm is raised by the DA-MP for a Connection, then the values are separated by a comma.

3.5.2 Enabling Connections

Use the following steps to enable one or more connections.

1. Click **Diameter**, and then **Maintenance**, and then **Connections**.
2. Select 1 - 20 connections to enable.

   To select multiple connections, press CTRL when selecting each connection. To select multiple contiguous connections, click the first connection you want, then press SHIFT and select the last connection you want. All the connections between are also selected.
3. Click **Enable**.
4. Click **OK** on the confirmation screen to enable the selected connections.

   If any of the selected connections no longer exist (they have been deleted by another user), an error message displays, but any selected connections that do exist are enabled.

3.5.3 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 are enabled. If no filter is applied, then all currently disabled connections are enabled.

1. Click **Diameter**, and then **Maintenance**, and then **Connections**.
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**.
4. Click **OK** on the confirmation screen to enable the connections.

   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.

3.5.4 Disabling Connections

Use the following steps to disable one or more connections.

1. Click **Diameter**, and then **Maintenance**, and then **Connections**.
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**.
4. Click **OK** on the confirmation screen to disable the selected connections.

   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.

3.5.5 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 are disabled. If no filter is applied, then all currently enabled connections are disabled.

1. Click **Diameter**, and then **Maintenance**, and then **Connections**.
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**.
4. Click **OK** on the confirmation screen to disable the connections.

   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.

3.5.6 Connections SCTP Statistics

The **Diameter**, and then **Maintenance**, and then **Connections**, and then **SCTP Statistics** page allows you to view statistics about paths within an SCTP connection.

Each line on the **Diameter**, and then **Maintenance**, and then **Connections**, and then **SCTP Statistics** page represents a path within an SCTP connection.

On the **Diameter**, and then **Maintenance**, and then **Connections**, and then **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**.

3.5.6.1 Diameter Connections SCTP Statistics Elements

Table 3-5 describes fields on the **Diameter**, and then **Maintenance**, and then **Connections**, and then **SCTP Statistics** page.

Table 3-5 Connections SCTP Statistics Elements

Field	Description
Duplicate TSNs Received	A duplicate TSNs received counter on a per SCTP connection basis.
Gap Acknowledgement Block Received	An acknowledgment blocks received counter on a per SCTP connection basis.
Retransmit Data Chunks Sent	A retransmit data chunks sent counter on a per SCTP connection basis.
Total Data Chunks Sent	A total data chunks sent counter on a per SCTP connection basis.
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, adjusted 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

3.5.7 Starting Diagnosis on a Test Connection

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

> **Note**
>
> This task is used primarily in lab environments to validate mediation rules, such as checking and debugging ART, PRT, and mediation flows for request messages.

In practice, a test request message is put on a test connection, and the user observes DSR processing in response to this message. The resulting report can be viewed on the GUI for analysis. The following rules apply to this task:

- Reroute is not supported
- Error Answers are not generated
- If an Answer is received, it is discarded; it is not routed to the originator

1. Click **Diameter**, and then **Maintenance**, and then **Connections**.
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**.
4. Click **OK** on the confirmation screen to begin the diagnosis on the selected test connection.

   The **PDU**s 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**, and then **Maintenance**, and then **Connections** page is refreshed.

3.5.8 Ending Diagnosis on a Test Connection

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

1. Click **Diameter**, and then **Maintenance**, and then **Connections**.
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**.
4. Click **OK** on the confirmation screen to stop the diagnosis on the selected test connection.

   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**, and then **Maintenance**, and then **Connections** page is refreshed.

3.6 Diameter Maintenance Egress Throttle Groups

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.

You can perform these tasks on an Active System OAM (SOAM).

Due to Egress Throttle Lists functionality, there is an additional maintenance parameter for Egress Throttle Groups, Control Scope. If the Egress Throttle Group does not belong to an Egress Throttle List, its Control Scope is ETG, which means that egress throttling is controlled by the ETG's configuration data. If the Egress Throttle Group is associated with an Egress Throttle List, its Control Scope can either be ETL, which means that egress throttling is controlled by the configuration data for the ETL that contains the ETG, or ETG, where egress throttling is controlled by the configuration data for the ETG. Under normal conditions the expected control scope for an ETG contained in an ETL would be ETL. A control scope of ETG for an ETG contained by an ETL can be used for maintenance transitions, such as when the ETG is being added or removed from the ETL.

Each function has an individual Control Scope State, as shown in Table 3-6.

Table 3-6 Egress Throttle Groups Control Scope States

Admin State	Description
ETL	Egress throttling for Rate Limiting and Pending Transaction Limiting is being controlled by the ETL's configuration data.
ETG	Egress throttling for Rate Limiting and Pending Transaction Limiting is being controlled by the ETG's configuration data.

Each function has an individual Administration State (Enable/Disable) and Operational Status, as shown in Table 3-7.

Table 3-7 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**, and then **Maintenance**, and then **Egress Throttle Groups** GUI page. Egress Throttle Groups use the Leader sourcing method for reporting of maintenance status. The Leader sourcing method is used because each DA-MP has identical status data; only the DA-MP Leader reports the maintenance status to the GUI. Table 3-8 shows the ETG operational status.

Table 3-8 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
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 throttles 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 throttles Request messages according to Congestion Level 2 (all Request messages with Priority 0 or 1 are throttled). As shown in Table 3-9.

Table 3-9 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**, and then **Maintenance**, and then **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 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**, and then **Maintenance**, and then **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.

3.6.1 Diameter Egress Throttle Groups Maintenance Elements

Table 3-10 describes fields on the Egress Throttle Groups maintenance page.

Table 3-10 Egress Throttle Groups Maintenance Elements

Field	Description
Egress Throttle Group Name	Name of the Egress Throttle Group.

Table 3-10 (Cont.) Egress Throttle Groups Maintenance Elements

Field	Description
Egress Throttle List Name	Name of optional Egress Throttle List that includes this Egress Throttle Group.
Egress Throttle Control Scope	Type of Egress Throttle Control Scope, either ETL for NOAM managed egress throttling or ETG for SOAM managed egress throttling
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
ETG Egress Request Rate	The egress request rate to the Peers and Connections that are members of the Egress Throttle Group.
ETL Egress Request Rate	The egress request rate to the Peers and Connections that are members of the ETL's component ETGs.
Pending Transaction Limiting Admin State	Pending Transaction Limiting Admin State can be Enabled or Disabled.

Table 3-10 (Cont.) Egress Throttle Groups Maintenance Elements

Field	Description
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 ETG Pending Transactions	The combined number of ETG Pending Transactions for the Peers and Connections of an ETG.
Number of ETL Pending Transactions	The combined number of Pending Transactions for the Peers and Connections of the ETL's ETGs.
Number of Active SMS Connections/Number of Required SDS Connections	The number of active SMS connections between the signaling routers with ETGs in the ETL/The number of required SMS connections between diameter signaling routers with ETGs in the ETL.
Time of Last Update	Displayed as yyyy-month name-date hr:min:sec UTC.

3.6.2 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. Click **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups**.
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, then 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.

3.6.3 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. Click **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups**.
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, then 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.

3.6.4 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. Click **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups**.
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, then 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.

3.6.5 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. Click **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups**.
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, then 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.

3.7 Diameter Maintenance Applications

The **Diameter**, and then **Maintenance**, and then **Applications** page allows you to view state and congestion information about existing diameter applications and can enable and disable diameter applications.

You can perform these tasks on an Active System OAM (SOAM).

If the MAP-Diameter InterWorking Function (IWF) is activated, you can view and configure items in the Map Internetworking folder. After activation, all selectable MAP-Diameter IWF related menu items are present on the SOAM and NOAM GUI, which allows full MAP-Diameter IWF configuration and provisioning. By default, MAP Interworking is not activated.

On the **Diameter**, and then **Maintenance**, and then **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 **Application Name** in ascending ASCII order.
- Change the Admin State of a selected 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.
- Enable and disable the DM-IWF and MD-IWF applications.

See *MAP-Diameter Interworking Function User's Guide* for additional information.

3.7.1 Diameter Applications Maintenance Elements

Table 3-11 describes fields on the Applications maintenance page.

Table 3-11 Applications Maintenance Elements

Field	Description
Application Name	Name of the application
MP Server Hostname	Hostname of the Message Processor server from which status is reported
Admin State	Admin State of the application (Enabled, Disabled). The Admin State persists over application restart and server reboot.
Operational Status	Operational Status of the application (Unavailable, Available, or Degraded)

Table 3-11 (Cont.) Applications Maintenance Elements

Field	Description
Operational Reason	Operational Reason that is filled in by the application and extracted from the database
Congestion Level	Congestion Level of the application (Normal, CL1, CL2, CL3)
Time of Last Update	Time stamp that shows when the application changed to the status shown in Operational State
If the run-time data for Operational Status, Operational Reason, Congestion Level, and Time of Last Status change is not present in the database, the data is displayed as Unknown.	

3.7.2 Enabling Applications

Use this task to enable one or more applications.

Applications are enabled only on the MP server shown in the rows you select.

1. Click **Diameter**, and then **Maintenance**, and then **Applications**.
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**.
4. Click
   - **OK** to enable the selected applications and bring the applications to the Available Operational State.
   - **Cancel** to return to the **Diameter**, and then **Maintenance**, and then **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**, and then **Maintenance**, and then **Applications** page is refreshed.

3.7.3 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. Click **Diameter**, and then **Maintenance**, and then **Applications**.
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**, and then **Maintenance**, and then **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**, and then **Maintenance**, and then **Applications** page is refreshed.

3.8 Diameter Maintenance DA-MPs

The **Diameter**, and then **Maintenance**, and then **DA-MPs** page allows you to view state and congestion information about Diameter Agent Message Processors.

On the **Diameter**, and then **Maintenance**, and then **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, then 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**, and then **Maintenance**, and then **DA-MPs** page, see Diameter DA-MPs maintenance elements.

For information about MP profiles, see *Diameter Common User's Guide*.

3.8.1 Diameter DA-MPs maintenance elements

Table 3-12 describes fields on the DA-MPs maintenance page.

Table 3-12 DA-MPs Maintenance Elements

Field	Description
Peer DA-MP Status Tab	
MP ID	The numeric identifier of the reporting DA-MP server
MP Server Hostname	The hostname of the reporting DA-MP server
# Peer MPs Available	The number of peer DA-MPs whose status is available
# Peer MPs Degraded	The number of peer DA-MPs whose status is degraded
# Peer MPs Unavailable	The number of peer DA-MPs whose status is unavailable
MP Leader	Indicates whether a DA-MP reports itself as MP Leader. The MP Leader provides status information to the OAM for Route Lists, Route Groups, and Peer Nodes, which are resources whose scope is beyond a single DA-MP.

Table 3-12 (Cont.) DA-MPs Maintenance Elements

Field	Description
Note: If a configured DA-MP is not alive, the above fields 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	The number of configured Connections whose IP Address is one of the fixed IP addresses assigned to the DA-MP.
# Fixed Connections Established	The number of Connections whose operation status is available and IP Address is one of the fixed IP addresses assigned to the DA-MP.
# Floating IPFE Connections Configured	The number of configured floating IPFE connections on a DA-MP in the TSA(s).
# Floating IPFE Connections Established	The number of floating IPFE connections owned by the DA-MP whose operation status is available.
Used/Free Connection Capacity	The used connection capacity sums the number of fixed connections configured and the number of floating IPFE connections established. The free connection capacity subtracts the used value from the max connections value in the MP profile of the reported DA-MP.
Used/Free Reserved MPS Capacity	The used reserved MPS capacity sums the reserved ingress MPS capacity set in the capacity configuration sets table for all fixed connections configured for the DA-MP and all floating IPFE connection currently established on the DA-MP. The free reserved MPS capacity subtracts the used value from the engineered ingress message rate value of the DA-MP in the MP Profile.
Current Total Connection Max Ingress MPS	The sum of the Maximum Ingress MPS settings for all fixed and floating IPFE connections currently established on the DA-MP.
Note: If a configured DA-MP is not alive, the above fields 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, 98 • Unavailable - CPL = 99
CPL	Connection Priority Level (0,1, 2, 3, 98, 99) of the configured peer DA-MP. This overall value takes into account the following status: • Operational Status of the ComAgent connection between the reporting DA-MP and the peer DA-MP • Congestion level of the peer DA-MP • Status of the process running on the peer DA-MP

Table 3-12 (Cont.) DA-MPs Maintenance Elements

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

3.9 Diameter Maintenance Peer Discovery

Peer Discovery (also know as Dynamic Peer Discovery [**DPD**]) allows an application to discover remote hosts within user-defined Realms and configures all required GUI elements for successful routing of diameter traffic between the signalling router and those remote hosts. This configuration is dynamic, and no user input is required at the time the routing configuration elements are created.

The **Diameter**, and then **Maintenance**, and then **Peer Discovery** page allows you to view Peer Discovery information.

You can perform these tasks on an Active System OAM (**SOAM**).

On the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page, you can perform the following actions:

- Filter the list of Realm Names to display only the desired names.
- Sort the list by column, in ascending or descending order, by clicking the column heading. The default order is by **Realm Name** in ascending **ASCII** order.
- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.
- Enable and disable Peer Discovery.
- Refresh and Extend Peer Discovery.
- Refresh the GUI page.

3.9.1 Diameter Peer Discovery Maintenance Elements

Table 3-13 describes fields on the Peer Discovery maintenance page.

Table 3-13 Peer Discovery Maintenance Elements

Field	Description
Realm Name	Name of the Realm assigned to the Discovery Attribute instance. **Note**: Any given Realm can only be configured for a single Mode (Initiator Only or Initiator & Responder), so each configured Realm name should appear just once in the list on the Peer Discovery Maintenance screen.
Mode	The connection mode used for each Discovery Attribute instance.
Expires	The date and time (in the locally-configured time zone) at which the Realm discovery expires, for any Realm whose Operational Status is Discovered or Expired; or the string "---" for any Realm whose Operational Status is anything other than Discovered or Expired.
Admin State	The current administrative state for each configured Discovery Attributes instance.
Operational Status	The current operational status for each configured Discovery Attributes instance.
Operational Reason	The current operational reason string for each configured Discovery Attributes instance
Configured Peers	The current number of Peer Nodes that are part of the DSR configuration due to the dynamic peer discovery for the Realm.
Configured Connections	The current number of Connections that are part of the DSR configuration due to the dynamic peer discovery for the Realm.
Application ID	The number of Application IDs, from the Discovery Attributes instance configuration, for which at least one Peer Node has been successfully identified.
Route List	Displays a ~ in the field corresponding to the parent Realm row. **Note**: For every Application ID for which at least one Peer Node is configured, a single Route List is listed. But the same Route List can be associated with more than one Application ID, if the same set of Peer Nodes supports multiple Application IDs.

3.9.2 Enabling Peer Discovery

Use this task to enable one or more Peer Discovery instances.

1. Click **Diameter**, and then **Maintenance**, and then **Peer Discovery**.
2. Select an instance to enable.

   To select multiple instances, press the CTRL key when selecting each instance. To select multiple contiguous instances, click the first instance you want, then press the SHIFT key and select the last instance you want. All the instances between are also selected.
3. Click **Enable**.

   A popup window appears.

4. Click
   - **OK** to enable the selected instances.
   - **Cancel** to return to the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page without enabling the applications.

   If **OK** is clicked and an instance no longer exists in the system (it was deleted by another user), an error message is displayed and the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page is refreshed.

3.9.3 Disabling Peer Discovery

Use this task to disable one or more Peer Discovery instances.

1. Click **Diameter**, and then **Maintenance**, and then **Peer Discovery**.
2. Select a Peer Discovery instance to disable.

   To select multiple instances, press the CTRL key when selecting each instance. To select multiple contiguous instances, click the first instance you want, then press the SHIFT key and select the last instance you want. All the instances between are also selected.
3. Click **Disable**.

   A confirmation box appears.
4. Click
   - **OK** to disable the selected instances.
   - **Cancel** to return to the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page without disabling the applications.

   If **OK** is clicked and an instance no longer exists in the system (it was deleted by another user), an error message is displayed and the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page is refreshed.

3.9.4 Refreshing Peer Discovery

Use this task to refresh Peer Discovery instances.

1. Click **Diameter**, and then **Maintenance**, and then **Peer Discovery**.
2. Select a Peer Discovery instance to refresh.

   To select multiple instances, press the CTRL key when selecting each instance. To select multiple contiguous instances, click the first instance you want, then press the SHIFT key and select the last instance you want. All the instances between are also selected.
3. Click **Refresh**.

   A confirmation box appears.
4. Click
   - **OK** to refresh (begin a new discovery sequence) the selected instances.

> **Note**
>
> After the software begins the new discovery sequence, the Admin State transitions from Rediscover to Enabled. You might or might not not see the Rediscover state on the **DiameterMaintenancePeer Discovery** page, depending on how long the transition takes and where it occurs within the screen refresh cycle.

- **Cancel** to return to the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page without refreshing the Peer Discovery instances.

If **OK** is clicked and an instance no longer exists in the system (it was deleted by another user), an error message is displayed and the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page is refreshed.

3.9.5 Extending Peer Discovery

Use this task to extend Peer Discovery instances.

1. Click **Diameter**, and then **Maintenance**, and then **Peer Discovery**.
2. Select a Peer Discovery instance to extend.

   To select multiple instances, press the CTRL key when selecting each instance. To select multiple contiguous instances, click the first instance you want, then press the SHIFT key and select the last instance you want. All the instances between are also selected.
3. Click **Extend**.

   A confirmation box appears.
4. Click

   - **OK** to extend a new discovery sequence for the selected instances (associated with an expired Realm). This adds one week to the Realm's expiration time.
   - **Cancel** to return to the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page without extending the Peer Discovery instances.

   If **OK** is clicked and an instance no longer exists in the system (it was deleted by another user), an error message is displayed and the **Diameter**, and then **Maintenance**, and then **Peer Discovery** page is refreshed.

> **Note**
>
> Configured Discovery Attributes instances cannot be edited unless they are administratively disabled.

3.10 Diameter Maintenance Traffic Throttle Points

A TTP has two administrative states that let you enable/disable TTP throttling. The Throttling Admin State is used to disable all throttling (both static and dynamic). When enabled, it automatically enables Static ETR throttling and might or might not perform Dynamic ETR throttling/DOIC as that is determined by the TTP's Dynamic Throttling Admin State.

> **Note**
>
> The TTP's Dynamic Throttling Admin State is not used to determine the TTP's Operational Status value.

The **Diameter**, and then **Maintenance**, and then **Traffic Throttle Points** page allows you to view information about and change the administrative state of TTP.

You can perform these tasks on an Active System OAM (**SOAM**).

You can perform the following actions for Traffic Throttle Points:

- Filter the list of Traffic Throttle Points (individually or multiples).
- Sort the list by column contents, in ascending or descending order, by clicking the column heading. The default order is by **TTP** in ascending ASCII order.
- Select a Traffic Throttle Point **Name** in the list.

You cannot change the TTP maintenance screen to change the Dynamic Throttling state to **Disabled** to **Enabled** when Throttling state is **Disabled**.

You can change the TTP maintenance screen to change the Dynamic Throttling state from **Enabled** to **Disabled** when Throttling state is **Enabled**.

TTP Throttling Admin State

When you change a TTP's Throttling Admin State is to Enabled:

- The routing instance starts sharing OTR data associated with the TTP with other DA-MP's within the DSR Node.
- If the TTP's Dynamic Throttling Admin State is set to Enabled and the TTP's Peer Node Operational Status is Available, the routing application starts sending a DCA to the Peer Node in all Request messages associated with this TTP and processes DOIC AVPs received from the Peer Node.
- TTP's Operational Status/Reason are updated.

When you change a TTP's Throttling Admin State to Disabled:

- Stop any Maximum ETR Throttling associated with this TTP.
- Ignore the TTP's Maximum Loss Percent Threshold during routing decisions.
- Stop sharing OTR data associated with the TTP with other DA-MP's within the DSR Node.
- Abandon all dynamic throttling (functional equivalent to TTP's Dynamic Throttling State being set to Disabled.
- The Current Loss Percent for all TTGs associated with this TTP are recalulated.
- TTP's Operational Status/Reason are updated.

TTP Dynamic Throttling Admin State

The routing application ignores any changes to the TTP's Dynamic Throttling Admin State when the TTP's Throttling Admin State is set to Disabled. When a TTP's Throttling Admin State is set to Enabled, the routing application process changes to the TTP's Dynamic Throttling Admin State as follows:

- TTP's Dynamic Throttling Admin State changed from Disabled to Enabled.
- TTP's Dynamic Throttling Admin State changed from Enabled to Disabled.

3.10.1 Diameter Traffic Throttle Points Maintenance Elements

Table 3-14 describes the fields on the Traffic Throttle Points maintenance page.

Table 3-14 Traffic Throttle Points Maintenance Elements

Field	Description
Name	A name of the Traffic Throttle Point.
Throttling Admin State	The static throttling administrative state.
Dynamic Throttling Admin State	The dynamic throttling administrative state from the associated Peer Node.
Operational Status	Operational status for TTP ETR throttling.
Operational Reason	Operational reason for each TTP. This provides additional information for each Operational Status regarding the condition is preventing the Operational Status from being available.
Abatement Algorithm	Abatement algorithm that is currently being applied as a result of receiving an OLR associated with the TTP (TTP's Operational Reason = Peer Overload).
Current Loss Percentage (%)	Loss rate (Reduction Percentage) currently being applied to the traffic routed to a TTP based upon an OLR received from a DOIC node. This value is non-zero during TTP Overload Recovery. This field is updated when a new OLR is processed, when a modify OLR changes this value and each time the DOIC Overload Recovery timer expires.
Validity Duration	DOIC Validity Duration value (in seconds) if an OLR is received from a DOIC node.
Offered Transactions per Second	The rate of transactions which are being routed to the TTP before diversion is applied.
Max Egress Transactions per Second Allowed	The maximum number of egress transactions allowed per second.
Percent of Actions Diverted (%)	The percentage of transactions which are being routed to the TTP which are being diverted or abandoned.
Target Egress Transactions per Second Allowed	The target number of egress transactions which are allowed per second.
Time until Loss=0 (sec)	The time of day when the Current Loss Percent is restored to 0%.
Time of Last Update	Time of most recent update.

3.11 Diameter Maintenance Traffic Throttle Groups

The **Diameter**, and then **Maintenance**, and then **Traffic Throttle Groups** page allows you to view information about and change the administrative state of **TTG**.

You can perform these tasks on an Active System OAM (**SOAM**).

You can perform the following actions for Traffic Throttle Groups:

- Filter the list of Traffic Throttle Groups (individually or multiples).

- Sort the list by column contents, in ascending or descending order, by clicking the column heading. The default order is by **TTG** in ascending ASCII order.
- Select a Traffic Throttle Group **Name** in the list.

3.11.1 Diameter Traffic Throttle Groups Elements

Table 3-15 describes the fields on the Traffic Throttle Groups maintenance page.

Table 3-15 Traffic Throttle Group Maintenance Elements

Field	Description
Name	The internal identifier for the TTG attribute that this TTG Status record is associated with.
Administrative Status	The administrative status of the Traffic Throttle Group. **Note**: This column displays a tilde character (~) for rows associated with Remote TTGs.
Site Name	Name of the site to which this TTG is owned and controlled.
Current Loss Percentage	A weighted value for the TTPs assigned to the TTG. This field is updated when a new OLR is processed by a TTP assigned to the TTG, and each time an OLR expires for a TTP assigned to the TTG. **Note**: This calculation is only made for TTGs assigned to the local DSR Node. This value is shared with other DSR Nodes.
Time of Last Update	Time of most recent update.

3.11.2 Enabling Traffic Throttle Groups

Use the following steps to enable one or more TTGs.

> **Note**
>
> When a TTG's **Administrative State** is Disabled, the TTG's **Current Loss Percent** value is ignored when making routing decisions.

1. Click **Diameter**, and then **Maintenance**, and then **Traffic Throttle Groups**. The **Administrative State** defines whether the TTG is active and can be applied to routing.
2. Select one or more TTGs to enable.

   If you select one or more rows in the TTG maintenance screen that are associated with remote TTGs, **Enable** and **Disable** are greyed out (disabled).

   To select multiple TTGs, press the CTRL key when selecting each TTG. To select multiple contiguous TTGs, click the first connection you want, then press the SHIFT key and select the last TTG you want. All the TTGs between are also selected.
3. Click **Enable**. Enable is greyed out for TTGs associated with remote TTGs. You must deselect all shared TTGs in order to enable the locally configured TTGs.

   A confirmation box appears.

4. Click **OK** on the confirmation screen to enable the selected (eligible) TTGs.

   If any of the selected TTGs no longer exist (they have been deleted by another user), an error message is displayed, but any selected TTGs that do exist are enabled.

   If you attempt to delete a TTG where the **Administrative State** is **Enabled**, an error message is displayed.

3.11.3 Enabling All Traffic Throttle Groups

Use the following steps to enable TTGs that are displayed as result of the application of a filter. The list includes TTGs configured at the local SOAM, as well as Shared TTGs configured at other SOAM server groups that are referred to by one or more Route Lists configured at the local SOAM. If a filter is applied, then all TTGs that meet the filter requirements and that are currently disabled are enabled. If no filter is applied, then all currently disabled TTGs are enabled.

> **Note**
>
> When a TTG's **Administrative State** is Disabled, the TTG's **Current Loss Percent** value is ignored when making routing decisions.

To enable and disable individual and multiple TTGs, shared TTGs must be included.

> **Note**
>
> Shared TTGs cannot be enabled or disabled on another DSR (the GUI page buttons are inactive for prohibited actions).

If you select one or more rows that are associated with remote TTGs, **Enable** and **Disable** are greyed out. **Enable** and **Disable** are active only when the selected row or rows are associated with locally-defined TTGs.

> **Note**
>
> **Enable All** and **DisableAll** are active regardless of the selected row state. If you select **Enable All** or **DisableAll**, then a window prompts you to enable or disable all locally configured TTGs, and a message indicates TTGs configured at other sites are not enabled or disabled.

1. Click **Diameter**, and then **Maintenance**, and then **Traffic Throttle Groups**. The **Administrative State** defines whether the TTG is active and can be applied to routing.
2. Optionally, click **Filter** and add up to four filters to limit the number of TTGs displayed. Click **Go** to apply the filter.
3. Click **Enable All**.

   A confirmation box appears to prompt you to enable or disable all locally configured TTGs, and a note displays to indicate TTGs configured at other sites are not enabled/disabled.
4. Click **OK**.

   The TTGs are enabled.

If any of the selected TTGs no longer exist (they have been deleted by another user), an error message is displayed, but any selected TTGs that do exist are enabled.

3.11.4 Disabling Traffic Throttle Groups

Use the following steps to disable one or more TTGs.

> **Note**
>
> When a TTG's **Administrative State** is Disabled, the TTG's **Current Loss Percent** value is ignored when making routing decisions.

1. Click **Diameter**, and then **Maintenance**, and then **Traffic Throttle Groups**. The **Administrative State** defines whether the TTG is active and can be applied to routing.
2. Select one or more TTGs to disable.

   If you select one or more rows in the TTG maintenance screen that are associated with remote TTGs, **Enable** and **Disable** are greyed out (disabled).

   To select multiple connections, press the CTRL key when selecting each TTG. To select multiple contiguous TTGs, click the first TTG you want, then press the SHIFT key and select the last TTG you want. All the TTGs between are also selected.
3. Click **Disable**. Disable is greyed out for TTGs associated with remote TTGs. You must deselect all shared TTGs in order to enable the locally configured TTGs.
4. Click **OK** on the confirmation screen to disable the selected (eligible) TTGs.

   If any of the selected TTGs no longer exist (they have been deleted by another user), an error message is displayed, but any selected TTGs that do exist are disabled.

3.11.5 Disabling All Traffic Throttle Groups

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 are disabled. If no filter is applied, then all currently enabled connections are disabled.

> **Note**
>
> When a TTG's **Administrative State** is Disabled, the TTG's **Current Loss Percent** value is ignored when making routing decisions.

To enable and disable individual and multiple TTGs, shared TTGs must be included.

> **Note**
>
> Shared TTGs cannot be enabled or disabled on another DSR (the GUI page buttons are inactive for prohibited actions).

If you select one or more rows that are associated with remote TTGs, **Enable** and **Disable** are greyed out. **Enable** and **Disable** are active only when the selected row or rows are associated with locally-defined TTGs.

> **Note**
>
> **Enable All** and **DisableAll** are active regardless of the selected row state. If you select **Enable All** or **DisableAll**, then a window prompts you to enable or disable all locally configured TTGs, and a message indicates TTGs configured at other sites are not enabled or disabled.

1. Click **Diameter**, and then **Maintenance**, and then **Trafffic Throttle Groups**. The **Administrative State** defines whether the TTG is active and can be applied to routing.
2. Optionally, click **Filter** and add up to four filters to limit the number of TTGs displayed. Click **Go** to apply the filter.
3. Click **Disable All**.

   A confirmation box appears to prompt you to enable or disable all locally configured TTGs, and a note is displayed to indicate that TTGs configured at other sites are not enabled/disabled.
4. Click **OK**.

   The TTGs are disabled.
   If any of the selected TTGs no longer exist (they have been deleted by another user), an error message is displayed, but any selected TTGs that do exist are disabled.

4 Diameter Reports

You can perform these tasks on an Active System OAM (**SOAM**).

The Diameter Reports pages provide access to the following reports:

- Diagnostics Tool reports
- MP Statistics (SCTP) reports

4.1 Overview

The Diameter Reports GUI pages provide access to the following reports:

- Diagnostics Tool reports
  The 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 Diameter Maintenance Connections). At various tracepoints, the 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.

> **Note**
>
> Report generation time depends on a number of factors and may vary based on the number of records (that is, data size), CPU utilization during report generation, number of measurements/alarms/events, and number of reports selected. Decrease the number of selected reports if reporting tasks are not being completed in the desired time.

4.2 Diameter Diagnostics Tool

The 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 **Diagnose Start** is clicked on the **Diameter**, and then **Maintenance**, and then **Connections** page, TestMode messages are sent on a test connection that is selected, in Test Mode, and not Disabled.

At various trace points, the 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 **Diagnose Start** is clicked. The test can be stopped by clicking **Diagnose Stop** on the Maintenance Connection page.

Use this task to generate Diagnostics Tool reports from the test logs.

1. Click **Diameter**, and then **Reports**, and then **Diagnostics Tool**.
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 includes all available Diagnostics Tool data.
   - If one or more records are selected, the report includes data for the selected test runs.
3. Click **Report**.

   On the **Diameter**, and then **Reports**, and then **Diagnostics Tool [Report]** page, you can save and print the generated report.

4.2.1 Diagnostic Tool Reports

Use this task to view, print, and save reports that are generated from Diagnostics Tool test logs.

When **Report** is clicked on the **Diameter**, and then **Reports**, and then **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>`.

```
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
.....................................................................
..
```

4.2.2 Printing and Saving Diagnostics Tool Reports

1. To print the report, click **Print**.

   A dialog box opens allowing you to choose the printer to be used for printing the report.
2. To save the report, click **Save**.

   A dialog box opens allowing you to choose the location in which to save the report.

4.3 Diameter MP Statistics (SCTP)

The **Diameter**, and then **Reports**, and then **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 **Update** 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. Click **Diameter**, and then **Reports**, and then **MP Statistics (SCTP)**.
2. Select the Scope of the report from the **Scope** list.
   - To be able to select individual MPs, select **Server**.
   - To select all MPs in a Network Element, select **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 are 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 **AddAll**.
   - 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.

4.3.1 MP Statistics (SCTP) Report Elements

Table 4-1 describes the fields for selecting MPs and the contents of the columns on the **Diameter**, and then **Reports**, and then **MP Statistics (SCTP)** page.

Table 4-1 MP Statistics (SCTP) Report Elements

Field	Description	Data Input Notes
	MP Selection	
Scope	Select Network Element or Server. All of the selected MPs have the same Scope.	Format: 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	
Checksum Error	Number of SCTP Checksum Errors detected	

5

Troubleshooting with IDIH

The **Diameter**, and then **Troubleshooting with IDIH** pages allow you to manage the Integrated Diameter Intelligence (**IDIH**) feature.

The IDIH feature allows you to capture detailed information about selected DIAMETER transactions, and transmit this information to IDIH for further analysis. The integration of troubleshooting capabilities provides a way to troubleshoot issues that might be identified with the Diameter traffic that transits the diameter routing program. These troubleshooting capabilities can supplement other network monitoring functions provided by the **OSS** and network support centers to help to identify the cause of signaling issues associated with connections, peer signaling nodes, or individual subscribers.

Use IDIH **Diameter**, and then **Troubleshooting with IDIH** pages to perform IDIH configuration and maintenance tasks. See *IDIH User's Guide*.

6
Diameter AVP Dictionary

The AVP Dictionary function provides the ability to work with Attribute-Value Pairs (AVPs) that are used by the Diameter Routing Function in making decisions for routing messages to and from applications and for the Diameter Message Copy feature.

You can perform these tasks on an Active System OAM (**SOAM**).

6.1 AVP Flags

Table 6-1 describes the AVP flags on the AVP GUI pages.

Table 6-1 AVP Flags Definitions

Field	Description	Data Notes
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 recipient of the message.	Format: 3 buttons for each flag Range: Must, Must Not, May be set for each flag

6.2 Base Dictionary

The **Diameter**, and then **AVP Dictionary**, and then **Base Dictionary** page allows you to view or clone the 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 cloning function allows you to edit the base AVP and puts the modified AVP in Custom Dictionary. The AVPs in Custom Dictionary shall supersede Base Dictionary AVPs.

The AVP Attribute Name, AVP Code, AVP Flag settings, Vendor ID, Data Type, and Protocol 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, then the list of Grouped AVPs appears in the dictionary. A grouped AVP's **Data** field is specified as a sequence of AVPs. Each of those AVPs can, in turn have the **Data** field specified as a sequence of AVPs. This pattern of embedding AVPs inside AVPs can occur multiple times.

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

> **Note**
>
> 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.

> **Note**
>
> AVP depth refers to the position of an AVP inside the Diameter message. All AVPs following the header of the Diameter message are called Base AVPs, and the Base AVP position is counted as 1. An AVP embedded immediately inside the Base AVP has a depth of 2. An AVP embedded immediately inside an AVP with a depth of 2 has a depth of 3 and so on. See *Diameter Mediation User's Guide*.

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

On the **Diameter**, and then **AVP Dictionary**, and then **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 **Clone AVP**.
  The detailed definition for the selected AVP is displayed. Update the fields as needed. Click **OK** or **Apply** to save the custom AVP definition.
- Select an AVP definition in the list and click **View**.
  The detailed definition for the selected AVP is displayed. The fields are described in Diameter Base Dictionary Elements.

6.2.1 Diameter Base Dictionary Elements

Table 6-2 describes the fields on the **AVP Dictionary**, and then **Base Dictionary** (View-only) page.

Table 6-2 Base Dictionary Elements

Field (*indicates a required 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
Flags	Setting indicator for AVP Flags: V, M, P, r3, r4, r5, r6, r7 **Note**: Flags V, M, and P are supported; r3, r4, r5, r6 and r7 are reserved for future use. See AVP Flags for flag definitions.	Format: 3 buttons for each flag Range: Must, Must Not, May be set for each flag
* Vendor-ID	Vendor-ID	Format: List Range: all configured Vendors
* 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: 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: 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

6.2.2 Cloning AVP Entries

Use the following task to clone AVP entries.

The cloning function allows you to edit the base AVP and puts the modified AVP in Custom Dictionary. The AVPs in Custom Dictionary supersede Base Dictionary AVPs.

> **Note**
>
> Templates or rules might already use an existing version of the AVP. If you clone an AVP that is referred from a template or rule, you can only add a new sub-AVP to the grouped AVP; no other changes are allowed. If the AVP is not used by any template or rule, you can make other modifications.

The cloning function is available from the following pages:

- **Diameter**, and then **AVP Dictionary**, and then **Base Dictionary**
- **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**
- **Diameter**, and then **AVP Dictionary**, and then **All-AVP Dictionary**

To clone an existing AVP from the **Diameter**, and then **AVP Dictionary**, and then **Base Dictionary**, **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**, or **Diameter**, and then **AVP Dictionary**, and then **All-AVP Dictionary** page:

1. Select an AVP entry from the list.
2. Click **Clone AVP**.

   The **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary [Insert]** page displays the attributes that are configured for the selected AVP dictionary entry.
3. Make changes to the AVP elements and click **OK** to implement the changes and return to the previous page, or click **Apply** to implement the changes and remain on the current page.

   The cloned AVP is inserted into the AVP Dictionary list.

6.3 Custom Dictionary

The **Diameter**, and then **AVP Dictionary**, and then **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, Data Type, and Protocol must be specified in the AVP definition.

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

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

The values for AVP definitions are described in Diameter Custom Dictionary Elements.

The **Diameter**, and then **AVP Dictionary**, and then **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, then the Custom Dictionary definition is used when the AVP is selected in Rule Template Actions and Conditions.
- Clone AVPs.

On the **Diameter**, and then **AVP Dictionary**, and then **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 **Insert**.
  You can add a new AVP and its values.

  If the maximum number of AVPs (1024) already exist in the system, then the **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary [Insert]** page does not open and an error message displays.
- Select an AVP definition in the list and click **Edit**.
  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 **Delete** to remove the selected AVP definition from the dictionary.
- Select an AVP definition in the list and click **Clone AVP** to clone the selected AVP definition.

6.3.1 Diameter Custom Dictionary Elements

Table 6-3 describes the fields on the **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary** view, [Insert], and [Edit] pages.

Table 6-3 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
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. **Note**: Flags V, M and P are supported; r3, r4, r5, r6 and r7 are reserved for future use. See AVP Flags for flag definitions.	Format: 3 buttons for each flag Range: Must, Must Not, May for each flag
Vendor-ID	Vendor-ID The field is required.	Format: List Range: all configured Vendors

Table 6-3 (Cont.) Custom Dictionary Elements

Field	Description	Data Input Notes
Data Type	AVP Data Format The field is required.	Format: List Range: all available AVP data formats
Include AVP in the group (insert and edit pages only)	Include an AVP into the Grouped AVP This field is active when the selected Data Type is Grouped. To include another AVP in the Grouped AVP, click **Add AVP**. A new row for AVP selection appears. To remove an AVP from the Grouped AVP, click **Delete AVP**.	Format: 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

6.3.2 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 Diameter Custom Dictionary Elements.

1. Click **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**.

   The **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary** page does not open if the maximum number of AVPs (1024) have already been created in the dictionary.

2. Click **Insert**.

   The **Diameter**, and then **AVP Dictionary**, and then **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**, and then **AVP Dictionary**, and then **Custom Dictionary** page.
   - **Apply** to save the changes and remain on the **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary [Insert]** page.
   - **Cancel** to return to the **Diameter**, and then **AVP Dictionary**, and then **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.

6.3.3 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 Diameter Custom Dictionary Elements.

1. Click **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**.
2. In the list, select the entry to be changed and click **Edit**.
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**, and then **AVP Dictionary**, and then **Custom Dictionary** page.
   - **Apply** to save the changes and remain on the **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary [Edit]** page.

     Cancel to return to the **Diameter**, and then **AVP Dictionary**, and then **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 is used until the restart is done.

6.3.4 Deleting an AVP Dictionary Entry

Use the following procedure to delete an AVP entry from the Custom Dictionary.

> **Note**
>
> The removal of Diameter Overload Indication Conveyance (DOIC) AVPs takes place at a peer node level.

1. Click **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**.
2. Select the **Attribute Name** of the AVP entry to be deleted.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the AVP and return to the **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary** page.
   - **Cancel** to return to the**Diameter**, and then **AVP Dictionary**, and then **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.

6.3.5 Cloning AVP Entries

Use the following task to clone AVP entries.

The cloning function allows you to edit the base AVP and puts the modified AVP in Custom Dictionary. The AVPs in Custom Dictionary supersede Base Dictionary AVPs.

> **Note**
>
> Templates or rules might already use an existing version of the AVP. If you clone an AVP that is referred from a template or rule, you can only add a new sub-AVP to the grouped AVP; no other changes are allowed. If the AVP is not used by any template or rule, you can make other modifications.

The cloning function is available from the following pages:

- **Diameter**, and then **AVP Dictionary**, and then **Base Dictionary**
- **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**
- **Diameter**, and then **AVP Dictionary**, and then **All-AVP Dictionary**

To clone an existing AVP from the **Diameter**, and then **AVP Dictionary**, and then **Base Dictionary**, **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**, or **Diameter**, and then **AVP Dictionary**, and then **All-AVP Dictionary** page:

1. Select an AVP entry from the list.
2. Click **Clone AVP**.

   The **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary [Insert]** page displays the attributes that are configured for the selected AVP dictionary entry.
3. Make changes to the AVP elements and click **OK** to implement the changes and return to the previous page, or click **Apply** to implement the changes and remain on the current page.

   The cloned AVP is inserted into the AVP Dictionary list.

6.4 All-AVP Dictionary

The **Diameter**, and then **AVP Dictionary**, and then **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**, and then **AVP Dictionary**, and then **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 **View**.

  The detailed definition for the selected AVP is displayed (the definition cannot be changed on this page). The definition elements are described in Diameter All-AVP Dictionary Elements.
- Clone AVPs.

6.4.1 Diameter All-AVP Dictionary Elements

Table 6-4 describes the fields on the **Diameter**, and then **AVP Dictionary**, and then **All-AVP Dictionary** and [View] pages.

Table 6-4 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
Dictionary	Indicates where the AVP resides.	Range: Base or custom
AVP Code	AVP Code	Format: numeric Range: 0 - 4294967295
Flags	AVP Flags V, M, P, r3, r4, r5, r6, r7 **Note**: Flags V, M, and P are supported; r3, r4, r5, r6 and r7 are reserved for future use. See AVP Flags for flag definitions.	Format: 3 buttons for each flag Range: Must, Must Not, May for each flag
Vendor-ID	Vendor-ID	Format: List Range: all configured Vendors
Include AVP in the group (view page only)	Include an AVP into the Grouped AVP This field is active when the selected Data Type is Grouped.	Format: 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

6.4.2 Cloning AVP Entries

Use the following task to clone AVP entries.

The cloning function allows you to edit the base AVP and puts the modified AVP in Custom Dictionary. The AVPs in Custom Dictionary supersede Base Dictionary AVPs.

> **Note**
>
> Templates or rules might already use an existing version of the AVP. If you clone an AVP that is referred from a template or rule, you can only add a new sub-AVP to the grouped AVP; no other changes are allowed. If the AVP is not used by any template or rule, you can make other modifications.

The cloning function is available from the following pages:

- **Diameter**, and then **AVP Dictionary**, and then **Base Dictionary**
- **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**
- **Diameter**, and then **AVP Dictionary**, and then **All-AVP Dictionary**

To clone an existing AVP from the **Diameter**, and then **AVP Dictionary**, and then **Base Dictionary**, **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary**, or **Diameter**, and then **AVP Dictionary**, and then **All-AVP Dictionary** page:

1. Select an AVP entry from the list.
2. Click **Clone AVP**.

   The **Diameter**, and then **AVP Dictionary**, and then **Custom Dictionary [Insert]** page displays the attributes that are configured for the selected AVP dictionary entry.
3. Make changes to the AVP elements and click **OK** to implement the changes and return to the previous page, or click **Apply** to implement the changes and remain on the current page.

   The cloned AVP is inserted into the AVP Dictionary list.

6.5 Vendors

The **Diameter**, and then **AVP Dictionary**, and then **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. See Custom Dictionary.

On the **Diameter**, and then **AVP Dictionary**, and then **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 **Insert**.
  You can add a new Vendor. See Adding a Vendor.

If the maximum number of Vendors (128) already exist in the system, the **Diameter**, and then **AVP Dictionary**, and then **Vendors [Insert]** page does not open and an error message is displayed.

- Select a Vendor row in the list and click **Edit**.
  You can edit the Vendor Name for the selected Vendor. See Editing a Vendor Name.

  The **Diameter**, and then **AVP Dictionary**, and then **Vendors [Edit]** page does 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 **Delete** 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.

6.5.1 Diameter Vendors Elements

Table 6-5 describes the fields on the **Diameter**, and then **AVP Dictionary**, and then **Vendors** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 6-5 Vendors Elements

Field	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

6.5.2 Adding a Vendor

The following procedure can be used to configure a new Vendor.

The fields are described in Diameter Vendors Elements.

1. Click **Diameter**, and then **AVP Dictionary**, and then **Vendors**.
2. Click **Insert**.

   If the maximum number of Vendors (128) has already been configured in the system, then the **Diameter**, and then **AVP Dictionary**, and then **Vendors [Insert]** page does not open and an error message appears.
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**, and then **AVP Dictionary**, and then **Vendors** page.
   - **Apply** to save the changes and remain on the **Diameter**, and then **AVP Dictionary**, and then **Vendors [Insert]** page.

- **Cancel** to return to the **Diameter**, and then **AVP Dictionary**, and then **Vendors [Insert]** page without saving any changes.

If **OK** or **Apply** is clicked and any of the following conditions exist, then 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

6.5.3 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 Diameter Vendors Elements.

1. Click **Diameter**, and then **AVP Dictionary**, and then **Vendors**.
2. Select the Vendor Name to be changed.
3. Click **Edit**.
4. Change the Vendor Name of the selected Vendor.
5. Click:
   - **OK** to save the changes and return to the **Diameter**, and then **AVP Dictionary**, and then **Vendors** page
   - **Apply** to save the changes and remain on the **Diameter**, and then **AVP Dictionary**, and then **Vendors [Edit]** page.
   - **Cancel** to return to the **Diameter**, and then **AVP Dictionary**, and then **Vendors** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then an error message appears:
   - The Vendor Name is not unique
   - The Vendor Name contains characters that are not valid

6.5.4 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. Click **Diameter**, and then **AVP Dictionary**, and then **Vendors**.
2. Select the row that contains the Vendor to be deleted.
3. Click **Delete**.

   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**, and then **AVP Dictionary**, and then **Vendors** page.

If the Vendor is used in any AVP definitions in the dictionary, then the Vendor is not deleted and an error message appears.

7

Mediation

The **Diameter**, and then **Mediation** pages allow you to manage the Mediation feature.

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 that are applied to modify the message contents. 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.

Use **Diameter**, and then **Mediation** pages to perform Mediation configuration and maintenance tasks. See *Diameter Mediation User 's Guide*.

8 Diameter Shared Traffic Throttle Groups

> **Note**
>
> Shared Traffic Throttle Groups configuration components must be viewed from the NOAM.

The Shared Traffic Throttle Groups GUI page shows all TTGs defined as shared across the diameter routing network. TTGs can be shared between DSR Nodes in the same network managed by a NOAM. Thus, each TTG is uniquely identified by its DSR Node.

The following components can be viewed for Shared Traffic Throttle Groups:

- Shared Traffic Throttle Group Name
- Site Name

8.1 Diameter Shared Traffic Throttle Groups Elements

Table 8-1 describes the fields on the **Diameter**, and then **Configuration**, and then **Shared Traffic Throttle Groups** page.
Any TTG configured at the local SOAM, and marked as shared is listed on the NOAM and available for assignment to a Route List, Route Group, TTG association at any SOAM in the diameter routing network.

This view-only GUI page is refreshed automatically.

> **Note**
>
> You control the **View** attribute for Shared Traffic Throttle Groups on the NOAM.

Table 8-1 Shared Traffic Throttle Groups elements

Field (* indicates a required field)	Description
* Shared Traffic Throttle Group Name	A name that uniquely identifies the Shared Traffic Throttle Group.
Site Name	A name that uniquely identifies the Shared Traffic Throttle Groups site.

8.2 Adding Shared Traffic Throttle Groups

To add (designate) a shared traffic throttle group on the SOAM, select **Diameter**, and then **Configuration**, and then **Traffic Throttle Groups**.

Use this page to work with shared throttle groups. The fields are described in Adding Traffic Throttle Groups.

8.3 Editing Shared Traffic Throttle Groups

To edit a shared traffic throttle groups on the SOAM, select **Diameter**, and then **Configuration**, and then **Traffic Throttle Groups**.

Use this page to work with shared throttle groups. The fields are described in Editing Traffic Throttle Groups.

8.4 Deleting Shared Traffic Throttle Groups

To delete a shared traffic throttle group on the SOAM, select **Diameter**, and then **Configuration**, and then **Traffic Throttle Groups**.

The **Diameter**, and then **Configuration**, and then **Traffic Throttle Groups** page appears with a list of configured traffic throttle groups. Use this page to delete shared throttle groups. The fields are described in Deleting Traffic Throttle Groups.

9

Diameter Topology Hiding

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
- S9 PCRF Topology Hiding Configuration Sets
- S9 AF/pCSCF Topology Hiding Configuration Sets
- Protected Networks

You can perform these tasks on an Active Network OAM&P (NOAM).

9.1 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 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 trustor non-trust relationship is always viewed from the perspective of a Protected Network. For example, if Networks N1 and N2 are Protected Networks, it's 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 is not protected from N2, but the topology information of N2 is protected from N1.
- Trusted Network - A network that a particular Protected Network trusts; no information from that Protected Network is 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 is hidden or modified when forwarded to an Untrusted Network.

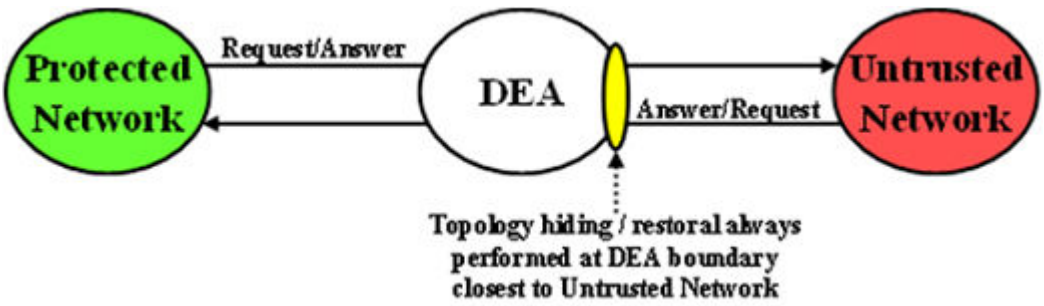
Topology Hiding involves hiding topology-related information in messages sent from a Protected Network to an Untrusted Network, as well as restoring the topology-related information in messages from an Untrusted Network. The restoral process can occur during the same Diameter transaction or can occur 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 where 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 9-1.

Figure 9-1 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.

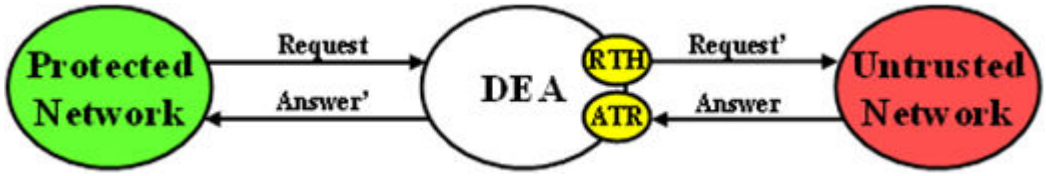
For Protected-to-Untrusted Network Diameter transactions, any topology-sensitive information in the Protected-to-Untrusted Network Request message is hidden just before forwarding the Request message to a Peer Node that serves as a gateway to the Untrusted Network. (The adjacent Peer Node may be a member 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 9-2.

Figure 9-2 Diameter Topology Hiding Trigger Points: Protected-to-Untrusted Transactions

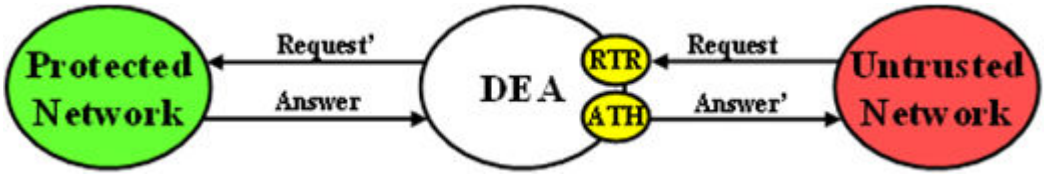


For Untrusted-to-Protected Network Diameter transactions, any topology-hidden information embedded in the Untrusted-to-Protected Network Request message may be a candidate for topology information restoral. The Trigger Point for evaluating whether topology-related information in a Request message should 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 9-3.

Figure 9-3 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 before Mediation
- Information restoral Trigger Points: immediately after Mediation

The Diameter Routing Function has the ability to edit messages just before forwarding them to Peer Nodes. Any Diameter Routing Function message editing must be performed before any TH treatment. For example, an 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 before 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 9-1 summaries the topology information hiding and restoral procedures that are supported at each TH Trigger Point.

Table 9-1 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.
		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.

Table 9-1 (Cont.) Topology Information Hiding and Restoral Procedures

Trigger	TH Type	AVP	Information Hiding/ Restoral Procedure
	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
	PCRF	Origin-Host	Replace the AVP value with one of the pseudo-host names assigned to the actual PCRF in S9 PCRF TH Configuration Set for S9 messages and for Rx messages if S9 AF/pCSCF TH Configuration Set is not assigned to the Protected network.
		Session-Id	Replace the host portion of this AVP with one of the pseudo-host names assigned to the actual AF/pCSCF in S9 PCRF TH Configuration Set for S9 messages and for Rx messages if S9 AF/ pCSCF TH Configuration Set is not assigned to the Protected network.
	AF/pCSCF	Origin-Host	Replace the AVP value with one of the pseudo-host names assigned to the actual AF/pCSCF in S9 AF/pCSCF ThH Configuration Set for Rx messages.
		Session-Id	Replace the host portion of this AVP with one of the pseudo-host names assigned to the actual AF/pCSCF in S9 AF/ pCSCF Th Configuration Set for Rx messages.

Table 9-1 (Cont.) Topology Information Hiding and Restoral Procedures

Trigger	TH Type	AVP	Information Hiding/ Restoral Procedure
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 before RTR.
	HSS	None; HSS Pseudo Hostname to Actual Hostname restoral is performed by a HSS Address Resolution application like FABR or RBAR.	not applicable
	MME/SGSN	Destination-Host	Replace the MME/SGSN Pseudo Hostname with the MME/SGSN's Actual Hostname.
	PCRF	Destination-Host	Replace the PCRF pseudo-host name with the PCRF's actual-host name.
		Session-Id	Replace the host portion of this AVP with actual PCRF host name.
	AF/pCSCF	Destination-Host	Replace the AF/pCSCF pseudo-host name with the AF/pCSCF actual-host name.
		Session-Id	Replace the host portion of this AVP with actual AF/pCSCF host name.
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.

Table 9-1 (Cont.) Topology Information Hiding and Restoral Procedures

Trigger	TH Type	AVP	Information Hiding/ Restoral Procedure
	HSS	Origin-Host	Replace the HSS host name with the single HSS Pseudo Hostname assigned to the Protected Network.
	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).
	PCRF	Origin-Host	Replace the AVP value with one of the pseudo-host names assigned to the actual PCRF in S9 PCRF TH Configuration Set for S9 messages and for Rx messages if S9 AF/p CSCF TH Configuration Set is not assigned to the Protected network.
		Session-Id	Replace the hostname received in the Request Session-ID AVP that is saved in the PTR.
	AF/pCSCF	Origin-Host	Replace the AVP value with one of the pseudo-host names assigned to the actual AF/pCSCF in S9 AF/pCSCF TH Configuration Set for Rx Messages.
		Session-Id	Replace the hostname received in the Request Session-ID AVP that is saved in the PTR.
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.

Table 9-1 (Cont.) Topology Information Hiding and Restoral Procedures

Trigger	TH Type	AVP	Information Hiding/ Restoral Procedure
	PCRF	Session-Id	Restore the PCRF's host name received in the Request Session-Id AVP that is stored in the PTR.
	AF/pCSCF	Session-Id	Restore the AF/pCSCF'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:

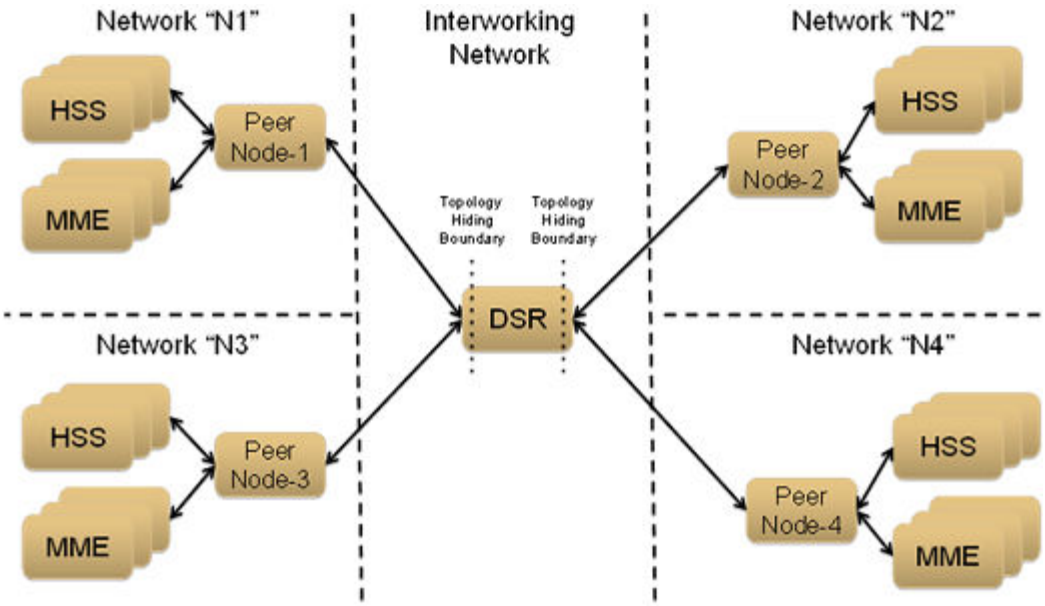
- Is the message that was just received (or about to be sent) a potential Topology Hiding and Restoral candidate?
- If the message is a potential candidate, is this a message between a Protected Network and an Untrusted Network?

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 9-4:

- 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 9-4 TH Network Deployment 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 9-2 and Table 9-3 are configured:

Table 9-2 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 9-3 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 9-4.

Table 9-4 Network Trust Relationship Matrix

Protected Network	Relationship with Peer Network			
	N1	N2	N3	N4
N1	Trusted	Not Trusted	Trusted	Not Trusted
N2	N2	Not 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 9-5 would be used:

Table 9-5 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 9-5, the TH type-independent criteria for determining whether a message is a potential candidate for Topology Hiding/Restoral are defined in Table 9-6.

Table 9-6 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 Destination-Realm is a Protected Network X, AND Origin-Realm is an Untrusted Network to Protected Network X

Table 9-6 (Cont.) General Criteria for Determining Whether a Message is a TH Candidate

TH Trigger	Message	Message Path	General Topology Hiding/Restoral Candidate Criteria
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 before 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.

Table 9-6 (Cont.) General Criteria for Determining Whether a Message is a TH Candidate

TH Trigger	Message	Message Path	General Topology Hiding/Restoral Candidate Criteria
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 9-6 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, MME/SGSN, S0 PCRF, and S9 AF/pCSCF 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 9-7:

Table 9-7 Protected Network Configuration Example

Protected Network Name	Protected Network Realm Name	Trusted Network List Name	Path TH	S6a/S6d HSS TH	MME/ SGSN TH	S9 PCRF TH	S9 AF/ pCSCF TH
N1	n1.com	Trusted Networks-1	Path Config Set-1	S6a/S6d HSS Config Set-1	MME/ SGSN Config Set-1	NULL	NULL
N2	n2.com	Trusted Networks-2	Path Config Set-2	S6a/S6d HSS Config Set-1	MME/ SGSN Config Set-1	NULL	NULL

Table 9-7 (Cont.) Protected Network Configuration Example

Protected Network Name	Protected Network Realm Name	Trusted Network List Name	Path TH	S6a/S6d HSS TH	MME/ SGSN TH	S9 PCRF TH	S9 AF/ pCSCF TH
N3	n3.com	Trusted Networks-3	Path Config Set-3	NULL	NULL	S9 PCRF Config Set-1	S9 AF/ pCSCF onfig Set-1
N4	n4.com	Trusted Networks-4	Path Config Set-4	NULL	NULL	S9 PCRF Config Set-2	S9 AF/ pCSCF onfig Set-2

In the example, if a message associated with Protected Network N3 is a candidate for topology hiding/restoral, then the Diameter Routing Function invokes 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 9-8 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 9-8 Topology Hiding AVPs and Hiding Methods

		Information Hiding Method	
Diameter Applications	AVP Name	Pseudo-Host Name Replacement	Encryption
S6a, S6d, S9, Rx	Session-Id	X	
S6a, S6d, S9, Rx	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 is 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, it is recommended that you contact your My Oracle Support. You need the Encryption Key configured in the **Diameter**, and then **Configuration**, and then **Topology**, and then **Path Topology Configuration Set** GUI page.

Assumptions

Diameter Topology Hiding has the following assumptions:

- 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.

9.1.1 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:

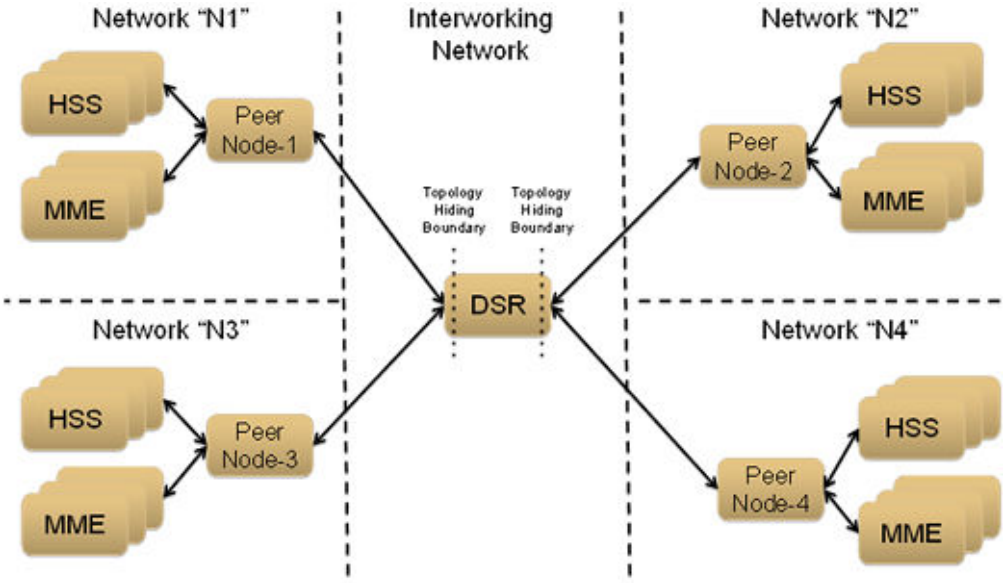
- Is the message that was just received (or about to be sent) a potential Topology Hiding and Restoral candidate?
- If the message is a potential candidate, is this a message between a Protected Network and an Untrusted Network?

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 9-5:

- **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 9-5 TH Network Deployment 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 9-9 and Table 9-10 are configured:

Table 9-9 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 9-10 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 9-11.

Table 9-11 Network Trust Relationship Matrix

Protected Network	Relationship with Peer Network			
	N1	N2	N3	N4
N1	Trusted	Not Trusted	Trusted	Not Trusted
N2	N2	Not 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 9-12 would be used:

Table 9-12 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 9-5, the TH type-independent criteria for determining whether a message is a potential candidate for Topology Hiding/Restoral are defined in Table 9-13.

Table 9-13 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 Destination-Realm is a Protected Network X, AND Origin-Realm is an Untrusted Network to Protected Network X

Table 9-13 (Cont.) General Criteria for Determining Whether a Message is a TH Candidate

TH Trigger	Message	Message Path	General Topology Hiding/Restoral Candidate Criteria
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 before 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.

Table 9-13 (Cont.) General Criteria for Determining Whether a Message is a TH Candidate

TH Trigger	Message	Message Path	General Topology Hiding/Restoral Candidate Criteria
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 9-13 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, MME/SGSN, S0 PCRF, and S9 AF/pCSCF 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 9-14:

Table 9-14 Protected Network Configuration Example

Protected Network Name	Protected Network Realm Name	Trusted Network List Name	Path TH	S6a/S6d HSS TH	MME/ SGSN TH	S9 PCRF TH	S9 AF/ pCSCF TH
N1	n1.com	Trusted Networks-1	Path Config Set-1	S6a/S6d HSS Config Set-1	MME/ SGSN Config Set-1	NULL	NULL
N2	n2.com	Trusted Networks-2	Path Config Set-2	S6a/S6d HSS Config Set-1	MME/ SGSN Config Set-1	NULL	NULL

Table 9-14 (Cont.) Protected Network Configuration Example

Protected Network Name	Protected Network Realm Name	Trusted Network List Name	Path TH	S6a/S6d HSS TH	MME/ SGSN TH	S9 PCRF TH	S9 AF/ pCSCF TH
N3	n3.com	Trusted Networks-3	Path Config Set-3	NULL	NULL	S9 PCRF Config Set-1	S9 AF/ pCSCF onfig Set-1
N4	n4.com	Trusted Networks-4	Path Config Set-4	NULL	NULL	S9 PCRF Config Set-2	S9 AF/ pCSCF onfig Set-2

In the example, if a message associated with Protected Network N3 is a candidate for topology hiding/restoral, then the Diameter Routing Function invokes only the Path Topology Hiding Configuration Set rules for that message.

The TH type-specific Hiding/Restoral rules are defined in Topology Hiding Types.

9.1.2 Topology Hiding Supported AVPs

Table 9-15 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 9-15 Topology Hiding AVPs and Hiding Methods

		Information Hiding Method	
Diameter Applications	AVP Name	Pseudo-Host Name Replacement	Encryption
S6a, S6d, S9, Rx	Session-Id	X	
S6a, S6d, S9, Rx	Origin-Host	X	
Any	Route-Record	X	
Any	Proxy-Host	X	
Any	Error-Reporting-Host		X

9.1.3 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 is 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, it is recommended that you contact your My Oracle Support. You need the Encryption Key configured in the **Diameter**, and then **Configuration**, and then **Topology**, and then **Path Topology Configuration Set** GUI page.

9.1.4 Diameter Topology Hiding 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.

9.1.5 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**HSS
    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.

- S9 PCRF Topology Hiding
  S9 PCRF Topology Hiding is concerned with hiding the host names of PCRF's in a Protected Network, as well as the number of PCRFs from Untrusted Networks.

  > **Note**
  >
  > S9 PCRF topology hiding is only applied to the S9 and Rx command codes.

- S9 AF/pCSCF Topology Hiding
  S9 AF/pCSCF Topology Hiding is only applied to the Rx command codes when Visited Access Roaming Architecture is used and AF/pCSCF is communicating to H-PCRF in Proxy Mode. It allows the operator to hide the host names of AF/pCSCF's in a Protected Network as well as the number of AF/pCSCF's from Untrusted Networks.

- 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.

9.1.5.1 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 9-6
- 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 9-6.

Figure 9-6 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 are not 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 is 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 9-6
- 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 9-7.

Figure 9-7 Route-Record Hiding - Answer Message

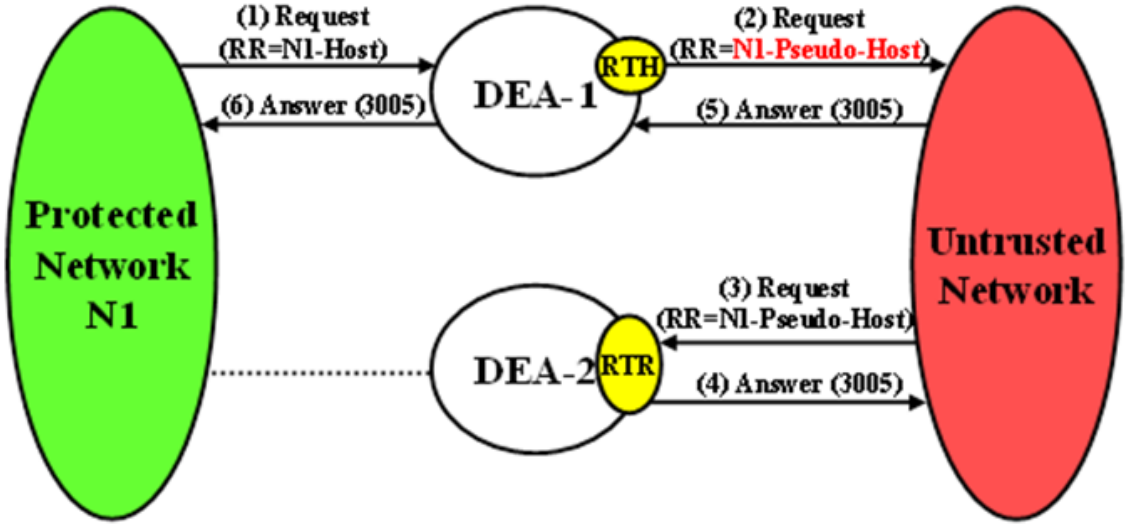
Route-Record AVP Hiding and Inter-Network Message Loop Detection

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 9-8. If an inter-network message loop is not detected by a DEA, the loop is not 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 is distributed to all DEAs controlled by the NOAM. This allows inter-network ingress message loop detection to be supported by any DEA.

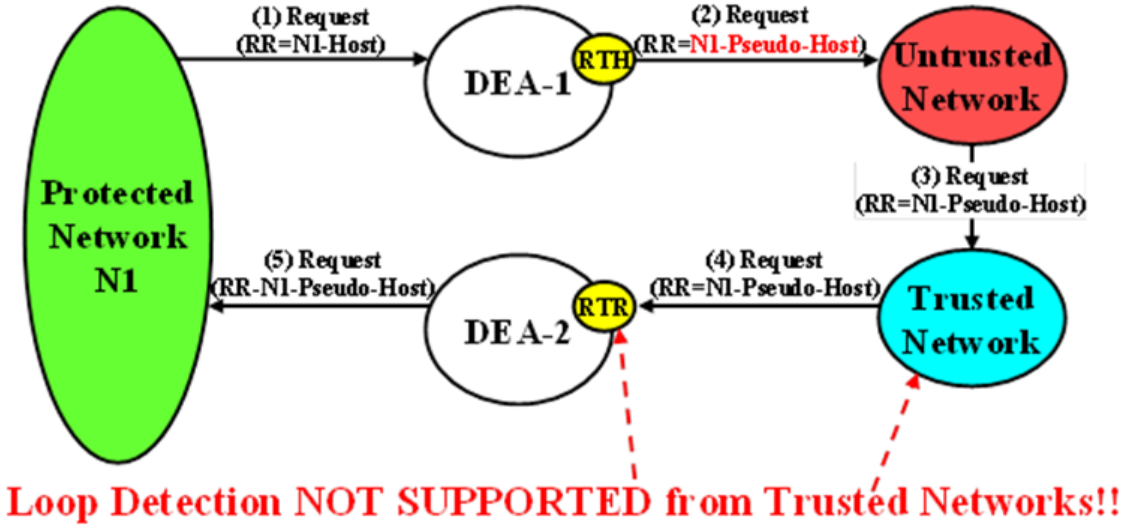
Inter-network ingress message loop detection is supported at the RTR Trigger Point. A typical message loop path between two DEAs with Path Topology Hiding enabled is illustrated in Figure 9-8.

Figure 9-8 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 9-9. This type of message loop detection is NOT supported.

Figure 9-9 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 9-6
- 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 is 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 unique Pseudo Hostname.

The Path Topology Hiding Configuration Set assigned to the Protected Network has the following elements that are used for Proxy-Host AVP Hiding:

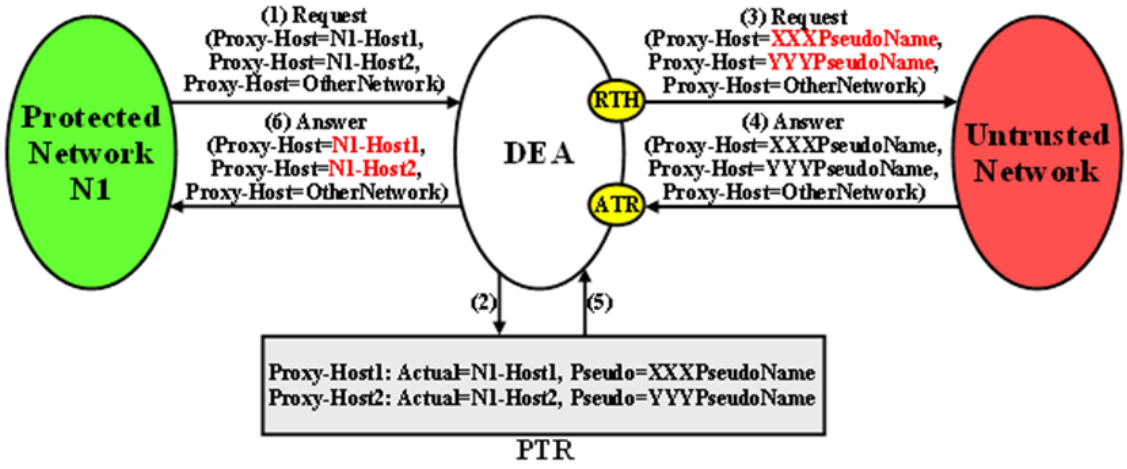
- Hostname Suffixes - A list of Protected Network Hostname Suffixes that are used to specify which Hostnames to hide when messages are forwarded to Untrusted Networks. Any Proxy-Host AVPs with a Hostname not matching an entry in this Hostname Suffixes list is not hidden.
- Proxy-Host Pseudo Hostname Suffix - To hide the number of Proxy Agents in the Protected Network, a random Proxy-Host pseudo-host name of the format <prefix><suffix> is 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 9-6
- 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 9-10.

Figure 9-10 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 is performed. The Diameter Routing Function replaces 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 is 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 9-6
- 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 9-11.

Figure 9-11 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 is not 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.

9.1.5.2 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 sends 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 internal nodes (Diameter Routing Function and applications) as these Answer responses are based upon the original Request message content and thus do not contain Pseudo Hostnames.

If a single S6a/S6d pseudo-hostname per S6a/S6d HSS TH Configuration Set is used, then that pseudo-hostname is used for hiding actual S6a/S6d host name. If multiple pseudo-names per actual host-name are used, then contents of User-Name AVP are used to select pseudo-host. In S6a/S6d, subscriber's IMSI is carried in the User-Name AVP. The content of the User-Name AVP content may be one of the following forms:

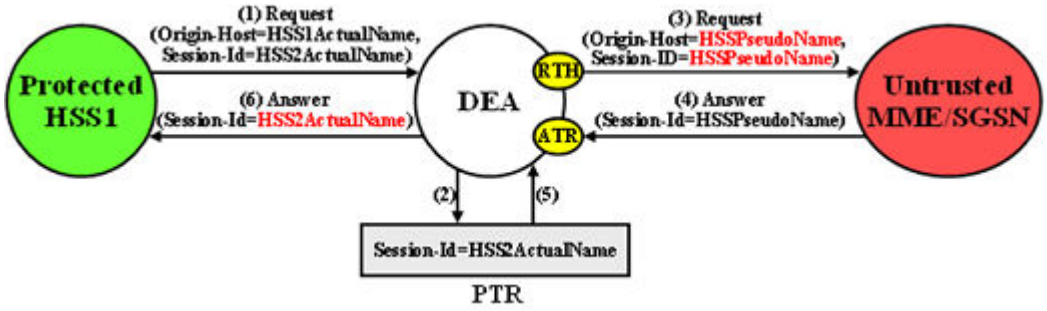
- IMSI
- IMSI@realm

It is not necessary to extract the IMSI portion from the User-Name AVP value. The User-Name AVP value content is the same in all transactions associated with subscriber. Therefore, the algorithm for mapping actual S6a/S6d HSS host name to one of the pseudo-names assigned to the S6a/S6d HSS is as follows:

- Pseudo-Host Name Selected = Function (User-Name AVP Content) MODULO (Number of Pseudo-Host Names assigned to this S6a/S6d HSS Host Name)

An example of a Protected-HSS to Untrusted-MME/SGSN Diameter transaction is shown in Figure 9-12.

Figure 9-12 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 9-6
- 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 is 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 Destination-Host AVP contains an S6a/S6d HSS pseudo-host name. If a single pseudo-name is assigned in S6a/S6d HSS TH Configuration Set, then no restoral of the Destination-Host is done by TH (instead the operator can deploy host Resolution Application such as RBAR/FABR). If a single pseudo-name is not assigned per S6a/S6d HSS Configuration Set and instead a unique pseudo-name is assigned per actual S6a/S6d HSS name, then the pseudo-host name must be replaced with the S6a/S6d HSS actual-host name at TH trigger point RTR.

  An Untrusted-MME/SGSN to Protected-HSS Request message may not contain an S6a/S6d HSS pseudo-host name. If the Destination-Host AVP value does not match an entry in the TH Pseudo-Host Name, then no host name conversion is required and the Request message is routed as normal. The Destination-Host name conversion is performed to prevent the following problems:

  - Certain S6a/S6d HSSs do not accept messages that do not contain its actual host name
  - Diameter outing problems associated with pseudo-host names. For example, DRL Implicit Routing currently only works with actual host names (for example, the FQDN assigned to the Peer Node and used for the Capabilities Exchange procedure [CER/CEA])
- The S6a/S6d HSS-initiated Answer response contains an actual S6a/S6d HSS host name in the Origin-Host AVP. This must be hidden with the S6a/S6d HSS pseudo-host name assigned to the Protected Network at TH trigger point ATH.

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 9-6
- 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

Restoral of a Protected-HSS's actual-host name in the Untrusted-MME/SGSN to Protected-HSS Request message is not performed by topology hiding if a single pseudo-name is used in S6a/S6d HSS TH Configuration Set assigned to a protected network. Instead, this replacement function is required of a HSS Address Resolution application such as FABR or RBAR applications.

HSS
An example of an Untrusted-MME/SGSN to Protected-HSS Diameter transaction is shown in Figure 9-13 and when pseudo-name per S6a/S6d HSS host name in S6a/S6d HSS TH Configuration Set.

Figure 9-13 S6a/S6d HSS TH Untrusted-MME/SGSN to Protected-HSS Transaction

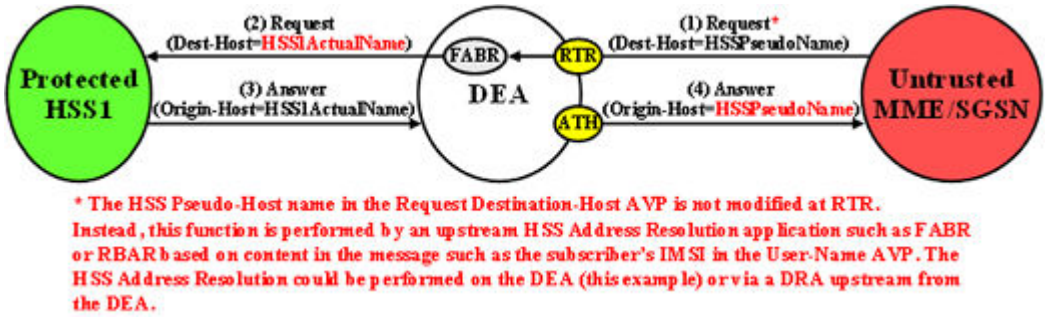
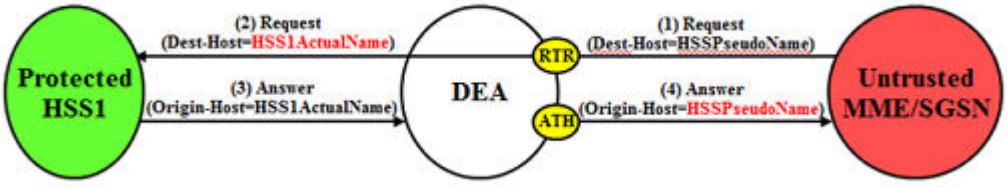


Figure 9-14 S6a/S6d HSS TH Untrusted-MME/SGSN to Protected-HSS Transaction



Restoral of a Protected-HSS's actual-host name in the Untrusted-MME/SGSN to Protected-HSS Request message is performed by topology hiding if a unique pseudo-name is assigned per S6a/S6d HSS host name in S6a/S6d HSS TH Configuration Set.

For Untrusted-HSS to Protected-MME/SGSN transactions, S6a/S6d HSS topology hiding is only invoked on Request messages which meet the following criteria:

- Message was a candidate for topology hiding as defined by topology trigger point RTR
- S6a/S6d HSS TH is enabled for the Protected Network (S6a/S6d HSS 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
- The Destination-Host AVP contains an S6a/S6d HSS pseudo-host name that is assigned to the Protected Network as determined from the internal S6a/S6d HSS TH Pseudo-Host Name

9.1.5.3 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.

To hide the number of MME/SGSNs in a network, each MME/SGSN is 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 9-16 shows an example of MME/SGSN TH Host Names configuration for a Protected Network with a maximum of 3 randomly created Pseudo Hostnames.

Table 9-16 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 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:

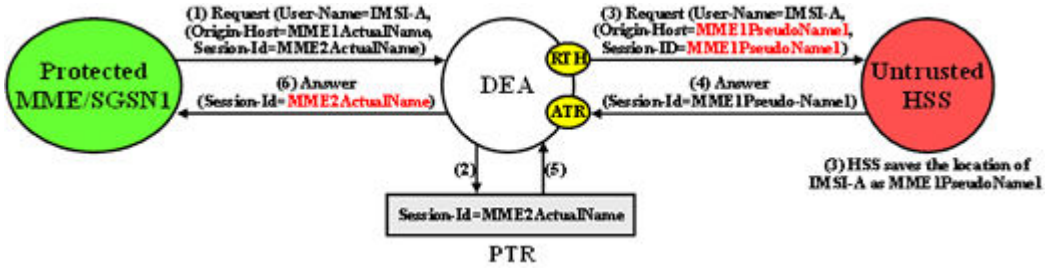
- The AVPs containing an MME/SGSN's Actual Hostname in Request messages must be hidden with one of the Pseudo Hostnames assigned to the MME/SGSN at TH Trigger Point RTH.
- The HSS saves the subscriber's location using the Origin-Host AVP contents containing a Pseudo Hostname. In subsequent HSS-to-MME/SGSN transactions, the MME/SGSN is 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 thinks the subscriber has moved to another MME/SGSN and unnecessarily changes 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 diameter internal nodes (the Diameter Routing Function and 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 9-15.

Figure 9-15 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 is 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 9-6
- 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:

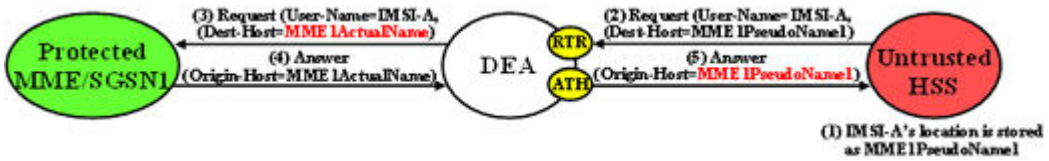
- The Destination-Host AVP contains a MME/SGSN Pseudo Hostname that must be replaced with the MME/SGSN's Actual Hostname at TH Trigger Point RTR. Pseudo-to-Actual Hostname mapping is performed using the list of created MME/SGSN TH Hostnames described in MME/SGSN Topology Hiding. It is acceptable that 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 is routed normally. Destination-Hostname conversion is performed to prevent the following problems:
- Certain MME/SGSNs do not accept messages that do not contain its Actual Hostname.
- Diameter 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]).

> **Note**
>
> For local nodes, CEAs are sent in response to erroneous CERs.

- 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 9-16.

Figure 9-16 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 9-6
- 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 9-6
- 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.

9.1.5.4 S9 PCRF Topology Hiding

S9 PCRF Topology Hiding is concerned with hiding the identities of a Protected Network's PCRFs, as well as the number of PCRFs in the network, when it exchanges messages with Untrusted Networks. A PCRF's identity 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 (and S9 AF/pCSCF Topology Hiding) is associated with the Diameter S9 and Rx application message set.

S9 PCRF topology hiding is concerned with all S9 messages and Rx messages when AF/pCSCF is deployed in client/server mode. If the PCRF is deployed in client/server mode for Rx messages, then S9 AF/pCSCF TH Configuration Set should not be enable for the protected network.

> **Note**
>
> All S9 messages initiated by hPCRF or vPCRF have S9 PCRF Topology Hiding applied (if enabled). If S9 AF/pCSCF TH is not enabled, then all Rx messages initiated by hPCRF or vPCRF have S9 PCRF Topology Hiding applied (if enabled). If S9 AF/pCSCF TH is enabled (i.e., if vPCRF is proxying AF/pCSCF messages to hPCRF), then only AAA/STA/RAR and ASR Rx messages have PCRF TH applied.

PCRF identities are hidden by replacing the actual host name portion of the Origin-Host and Session-ID AVPs with a PCRF pseudo-host name. The Origin-Hose and Session-ID AVPs may have different PCRF host names. A unique pseudo- name must be created for each PCRF in a Protected Network. When the vPCRF initiates a transaction to the hPCRF, the hPCRF saves the vPCRF's identity for use in subsequent hPCRF-to-vPCRF transactions. This vPCRF pseudo-host name must not only be unique, but the DEA must be able to convert the vPCRF's pseudo-name to an actual vPCRF host name for these subsequent hPCRF to vPCRF transactions.

To hide the number of PCRFs in a network, each PCRF is assigned either a random or fixed number of pseudo-host names (the maximum is defined by an S9 PCRF TH Configuration Set attribute called Maximum Pseudo-Host Names per PCRF). The GUI creates the randomized PCRF pseudo-host names and assign them to actual pseudo-host names to be used by DRL. The TH Host Names allows DRL to map a Protected-PCRF actual-host name to a set of PCRF pseudo-host names as well as map a PCRF pseudo-host named received from an Untrusted Network to a Protected-PCRF actual-host name.

Protected-vPCRF to Untrusted-hPCRF Transactions

When vPCRF is in a Protected Network, S9 Diameter sessions are initiated by vPCRF in a Protected Network on behalf of an inbound roamer to request PCC or QoS rules to the hPCRF.

When AF/pCSCF and PCRF are in a Protected Network and AF/pCSCF uses vPCRF in client/server mode to communicate Rx messages initiated by vAF/pCSCF to hPCRF in an Untrusted network, then S9 PCRF TH is used to hide PCRF host names to an Untrusted Network.

For Protected-vPCRF to Untrusted-hPCRF S9 Diameter transactions, S9 PCRF TH is concerned with the following topology information hiding and restoral issues:

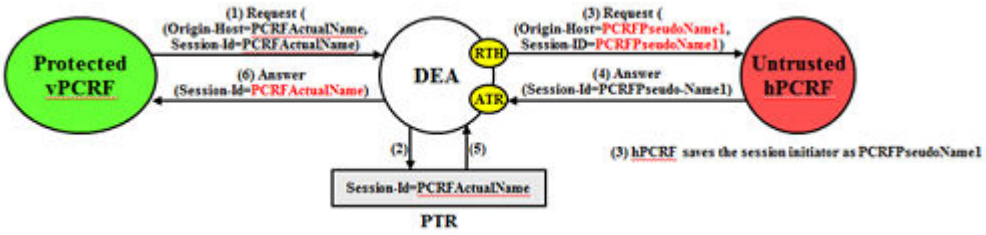
- The AVPs containing a PCRF's actual-host name in Request messages must be hidden with one of the pseudo-host names assigned to the PCRF at TH trigger point RTH
- The Untrusted network's PCRF (hPCRF in this case) saves the subscriber's location using the Origin-Host AVP contents containing a pseudo-host name. This has the following impact:
  - In subsequent hPCRF-vPCRF transactions(e.g RAR/ASR), the vPCRF may be addressed by one of its pseudo-host names requiring a pseudo-to-actual name restoral
  - All vPCRF-to-hPCRF transactions associated with a particular session must use the same vPCRF pseudo-host name. The Session is identified by Session-ID AVP, a mandatory AVP in all S9/Rx messages.

  > **Note**
  >
  > Although the Origin-Host and Session-ID AVPs both have actual PCRF host names, they may be different. Because S9/Rx is a session based application , actual PCRF host names must be restored in subsequent hPCRF-vPCRF transactions. Hence both Origin-Host and Session-ID AVPs must be selected from Actual Host Names in S9 PCRF TH.

- The hPCRF sends an Answer response to the transaction with the Session-ID received in the Request (also containing a PCRF pseudo-host name). Because the Session-ID value returned in the Answer must match the Request, the PCRF pseudo-host name in the Session-ID AVP must be replaced with its corresponding value received in the Request message. This value is restored at TH trigger point ATR. This requires saving the host name portion of the Session-ID AVP value in the PTR. This host name restoral procedure is not required for Answers initiated by internal nodes as these Answer responses are based upon the original Request message content

An example of a Protected-vPCRF to Untrusted-hPCRF Diameter transaction is shown in Figure 9-17.

Figure 9-17 Protected-vPCRF to Untrusted-hPCRF Transaction



To ensure all S9/Rx messages for the same session are modified using the same pseudo-name, the Session-ID AVP can be used as a key to select a Pseudo Host Name for an Actual Host Name.

Untrusted-hPCRF to Protected-vPCRF Transactions

For Protected-vPCRF to Untrusted-hPCRF S9/Rx transactions, PCRF topology hiding is only required on Request messages which meet the following criteria:

- The message was a candidate for topology hiding as defined by topology trigger point RTH and
- S9 PCRF TH is enabled for the Protected network (S9 PCRF TH Configuration Set is assigned to the Protected Network) and
- The Request message is a member of the S9 message and was initiated by a PCRF or
- The Request message is a member of the Rx message set and was initiated by a PCRF and S9 AF/pCSCF TH is not enabled and
- The Origin-Host and/or Session-ID AVPs in the Request contain an actual PCRF host name assigned to the Protected Network via the S9 PCRF Configuration Set.

For Protected-vPCRF to Untrusted-hPCRF transactions, PCRF topology information restoral is only performed on Answer messages which meet the following criteria:

- At topology trigger point ATR, the PCRF TH ATR flag in the PTR associated with the Answer message is set to Enabled.

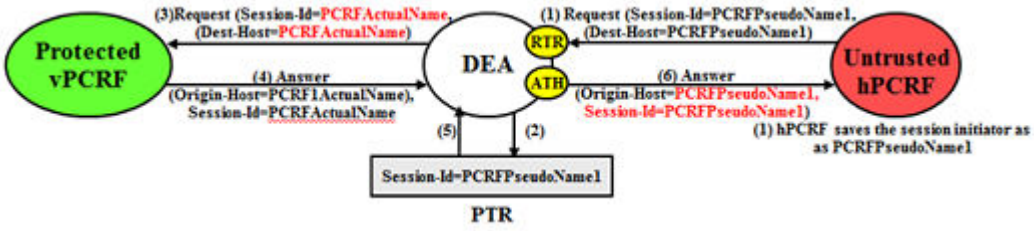
When an Untrusted-hPCRF initiates a transaction to a Protected-vPCRF, it is most likely addressed to one of the vPCRF pseduo-host names that the hPCRF saved in a previous vPCRF-to-hPCRF transaction for which S9 PCRF TH was applied. For Untrusted-hPCRF to Protected-vPCRF Diameter transactions (RAR, ASR, and so on), S9 PCRF TG is concerned with the following topology information hiding and restoral issues:

- The Destination-Host AVP contains a vPCRF pseudo-host name. This pseudo-host name must be replaced with the vPCRF's actual-host name at TH trigger point RTR. Pseudo-to-actual host name mapping is performed using the internal TH Host Names. It's perfectly acceptable that an Untrusted-hPCRF to Protected-vPCRF Request message does not contain a PCRF pseudo-host name. If the Destination-Host AVP value does not match an entry in the TH Pseudo-Host Name, then no host name conversion is required and the Request message is routed as normal. Destination-Host name conversion is performed to prevent the following problems:
  - Certain vPCRFs do not accept messages that do not contain its actual host name
  - Diameter routing problems associated with pseudo-host names. For example, DRL Implicit Routing currently only works with actual host names (for example, the FQDN assigned to the Peer Node and used for the Capabilities Exchange procedure [CER/CEA]).

- The host portion of Session-ID AVP containing a PCRF pseudo-host name must be replaced back with vPCRF's actual host name at TH trigger point RTR. Pseudo-to-actual host name mapping is performed using the internal TH Host Names.
- An Origin-Host AVP containing a vPCRF's actual-host name in the Answer response from the Protected-vPCRF must be hidden with one of the pseudo-host names assigned to that PCRF. This procedure is done at TH trigger point ATH.
- Session-ID AVP containing a vPCRF's actual-host name in the Answer response from the Protected-vPCRF must be hidden with one of the pseudo-host names assigned to that PCRF. This is done at TH trigger point ATH.

An example of an Untrusted-hPCRF to Protected-vPCRF Diameter transaction is shown in Figure 9-18.

Figure 9-18 Untrusted-hPCRF to Protected-vPCRF Diameter Transaction



For Untrusted-hPCRF to Protected-vPCRF transactions, S9 PCRF TH is only invoked on Request messages at topology trigger point RTR which meet the following criteria:

- The message was a candidate for topology hiding as defined by topology trigger point RTR and
- S9 PCRF TH is enabled for the Protected Network (S9 PCRF TH Configuration Set is assigned to the Protected Network) and
- The Request message is a member of the S9 message set and was initiated by a PCRF or
- The Request message is a member of Rx message set and was initiated by a PCRF and S9 AF/pCSCF TH is not enabled and
- The Destination-Host AVP or host portion of Session-ID AVP contains a PCRF pseudo-host name that is assigned to the Protected Network as determined from the internal Pseudo-Host Name

For Untrusted-hPCRF to Protected-vPCRF transactions, S9 PCRF HSS topology hiding is only invoked on Answer messages at topology trigger point ATH which meet the following criteria:

- Message was a candidate for topology hiding as defined by topology trigger point ATH
- S9 PCRF TH is enabled for the Protected Network (S9 PCRF TH Configuration Set is assigned to the Protected Network)
- The Answer message is a member of the S9 message set and was initiated by a PCRF or
- The Answer message is a member of Rx message set and was initiated by a PCRF and S9 AF/pCSCF TH is not enabled and
- The Origin-Host AVP or host portion of Session-ID AVP contains an actual PCRF host name that is assigned to the Protected Network via the S9 PCRF TH Configuration Set

Protected-hPCRF to Untrusted-vPCRF Transactions

When an hPCRF is in Protected Network, S9 Diameter sessions are initiated by a vPCRF in an Untrusted Network on behalf of an outbound roamer to request PCC or QoS rules to the hPCRF. hPCRF can send RAR in the session initiated by vPCRF.

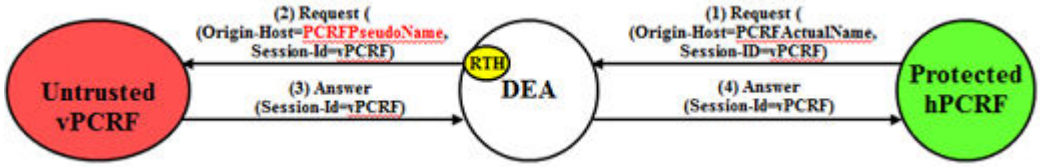
When AF/pCSCF and PCRF is in an Untrusted network and AF/pCSCF uses vPCRF in client/server mode to communicate Rx messages initiated by vAF/pCSCF to hPCRF in a Protected Network, then S9 PCRF TH is used to hide PCRF host names from an Untrusted Network. hPCRF can send RAR or ASR messages in the session intiated vPCRF.

For Protected-hPCRF to Untrusted-vPCRF S9 Diameter transactions, S9 PCRF TH is concerned with the following topology information hiding and restoral issues:

- S9 Sessions are initiated from untrusted network using CCR and Rx Sessions are initiated from untrusted network using AAR. Hence the host portion of Session-ID AVP contains the host of the untrusted network, which does not need to be hidden.
- The Origin-Host AVP containing an PCRF's actual-host name in Request messages must be hidden with one of the pseudo-host names assigned to the PCRF at TH trigger point RTH.

An example of a Protected-hPCRF to Untrusted-vPCRF Diameter transaction is shown in Figure 9-19.

Figure 9-19 Protected-hPCRF to Untrusted-vPCRF Transaction



To ensure all S9/Rx messages for same session are modified using same pseudo-name , Session-ID AVP can be used as key to select a Pseudo Host Name for an Actual Host Name.

For Protected-hPCRF to Untrusted-vPCRF S9/Rx transactions, PCRF topology hiding is only required on Request messages which meet the following criteria:

- The message was a candidate for topology hiding as defined by topology trigger point RTH and
- S9 PCRF TH is enabled for the Protected Network (S9 PCRF TH Configuration Set is assigned to the Protected Network) and
- The Request message is a member of the S9/Rx message set and was initiated by a PCRF and
- The Origin-Host AVP in the Request contain an actual PCRF host name assigned to the Protected Network via the S9 PCRF TH Configuration Set

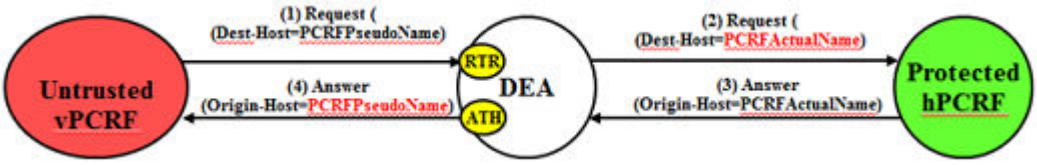
Untrusted-vPCRF to Protected-hPCRF Transactions

When an Untrusted-vPCRF initiates a transaction to a Protected-hPCRF, it is most likely addressed to one of the hPCRF pseudo-host names that the vPCRF saved in a previous hPCRF-to-vPCRF transaction for which PCRF TH was applied. For Untrusted-vPCRF to Protected-hPCRF Diameter transactions (CCR, AAR/STR, and so on), PCRF TH is concerned with the following topology information hiding and restoral issues:

- The Destination-Host AVP contains a PCRF pseudo-host name. This pseudo-host name must be replaced with the hPCRF's actual-host name at TH trigger point RTR. Pseudo-to-actual host name mapping is performed using the internal TH Host Names table. It's perfectly acceptable that an Untrusted-vPCRF to Protected-hPCRF Request message does not contain a PCRF pseudo-host name. If the Destination-Host AVP value does not match an Pseudo-Host Name entry in the TH Host Names, then no host name conversion is required and the Request message is routed as normal. Destination-Host name conversion is performed to prevent the following problems:
  - Certain hPCRFs do not accept messages that do not contain its actual host name
  - Diameter routing problems associated with pseudo-host names. For example, DRL Implicit Routing currently only works with actual host names (i.e., the FQDN assigned to the Peer Node and used for the Capabilities Exchange procedure (CER/CEA))
- An Origin-Host AVP containing an vPCRF's actual-host name in the Answer response from the Protected-hPCRF must be hidden with one of the pseudo-host names assigned to that PCRF . This is done at TH trigger point ATH.

An example of an Untrusted-vPCRF to Protected-hPCRF Diameter transaction is shown in Figure 9-20.

Figure 9-20 Untrusted-vPCRF to Protected-hPCRF Transaction



For Untrusted-vPCRF to Protected-hPCRF transactions, S9 PCRF HSS topology hiding is only invoked on Request messages at topology trigger point RTR which meet the following criteria:

- Message was a candidate for topology hiding as defined by topology trigger point RTR and
- S9 PCRF TH is enabled for the Protected Network (S9 PCRF TH Configuration Set is assigned to the Protected Network) and
- The Request message is a member of the S9 message set and was initiated by a PCRF as determined and
- The Request message is a member of Rx message set and was initiated by a PCRF and S9 AF/pCSCF TH is not enabled and
- The Destination-Host AVP contains a PCRF pseudo-host name that is assigned to the Protected Network as determined from the internal Pseudo-Host Name

For Untrusted-vPCRF to Protected-hPCRF transactions, S9 PCRF HSS topology hiding is only invoked on Answer messages at topology trigger point ATH which meet the following criteria:

- Message was a candidate for topology hiding as defined by topology trigger point ATH
- S9 PCRF TH is enabled for the Protected Network (S9 PCRF TH Configuration Set is assigned to the Protected Network)
- The Answer message is a member of the S9 message set and was initiated by a PCRF
- The Origin-Host AVP contains an actual PCRF host name that is assigned to the Protected Network via the S9 PCRF TH Configuration Set

9.1.5.5 S9 AF/pCSCF Topology Hiding

S9 AF/pCSCF Topology Hiding is concerned with hiding the identities of a Protected Network's AF/pCSCFs, as well as the number of AF/pCSCFs in the network, when it exchanges messages with Untrusted Networks. An AF/pCSCF identity is embedded in the Origins-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 Rx application message set.

S9 AF/pCSCF topology hiding is concerned with Rx messages when AF/pCSCF is deployed in proxy mode. If PCRF is deployed in client/server mode for Rx messages, then S9 AF/pCSCF TH Configuration Set should be enabled for the protected network. If S9 AF/pCSCF TH is enabled (for example, if vPCRF is proxying AF/pCSCF messages to hPCRF), then only AAR/STR and RAA/ASA have S9 PCRF TH applied.

AF/pCSCF identities are hidden by replacing the actual host name portion of the Origin-Host and Session-ID AVPs with AF/pCSCF pseudo-host name. The Origin-Host and Session-ID AVPs may have different AF/pCSCF host names. A unique pseudo name must be created for each AF/pCSCF in a Protected Network. When the vAF/pCSCF initiates a transaction to the hPCRF, the hPCRF saves the vAF/pCSCF's identity for use in subsequent hPCRF-to-vAF/pCSCF transactions. This vAF/pCSCF's pseudo-host name must not only be unique, but the DEA must be able to convert the vAF/pCSCF's pseudo-name to an actual vAF/pCSCF host name for these subsequent hPCRF to vAF/pCSCF transactions.

To hide the number of AF/pCSCFs in a network, each AF/pCSCF is assigned either a random or fixed number of pseudo-host names (the maximum is defined by an S9 AF/pCSCF TH Configuration Set attribute called Maximum Pseudo-Host Names per AF/pCSCF). This procedure of creating randomized AF/pCSCF pseudo-host names and assigning them to actual pseudo-host names is performed by the GUI and used by DRL. The TH Host Names MO allows DRL to map a Protected-AF/pCSCF actual-host name to a set of AF/pCSCF pseudo-host names and map an AF/pCSCF pseudo-host name received from an Untrusted network to a Protected-AF/pCSCF actual-host name.

Protected-vAF/pCSCF to Untrusted-hPCRF Transactions

When AF/pCSCF and PCRF are in a Protected Network and AF/pCSCF uses vPCRF in proxy mode to communicate Rx messages initiated by vAF/pCSCF to hPCRF in Untrusted Network, then S9 AF/pCSCF TH is used to hide AF/pCSCF host names to Untrusted Network.

For Protected-vAF/pCSCF to Untrusted-hPCRF Rx Diameter transactions, S9 AF/pCSCF TH is concerned with the following topology information and restoral issues:

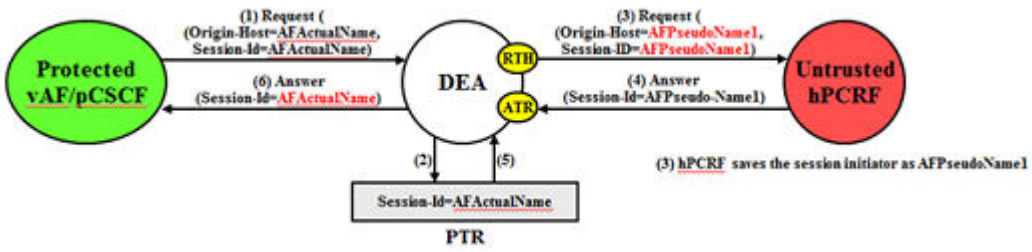
- The AVPs containing an AF/pCSCF's actual-host name in Request message must be hidden with one of the pseudo-host names assigned to the AF/pCSCF at TH trigger point RTH
- The Untrusted Network's PCRF (hPCRF in this case) saves the subscriber's location using the Origin-Host AVP contents containing a pseudo-host name. This action has the following impact:
  - In subsequent hPCRF-vAF/pCSCF transactions (for example, RAR/ASR), the vAF/pCSCFis addressed by on of its pseudo-host names requiring a pseudo-to-actual name restoral
  - All vAF/pCSCF-to-hPCRF transactions associated with a particular session must use the same vAF/pCSCF pseudo-host name. The Session is identified by Session-ID AVP, a mandatory AVP in all S9/RX messages.

> **Note**
>
> Although the Origin-Host and Session-ID AVPs both have actual AF/pCSCF host names, the may be different. Because Rx is a session based application, actual AF/pCSCF host names must be restored in subsequent hPCRF-vAF/pCSCF transactions. Hence the Origin-Host and Session-ID AVPs must be selected from the Actual Host Names TH Host Names.

- The hPCRF sends an Answer response to the transaction with the Session-ID received in the Request (containing an AF/pCSCF pseudo-host name). Because the Session-ID value returned in the Answer must match the Request, the AF/pCSCF pseudo-host name in the Session-ID AVP must be replaced with its corresponding value received in the Request message. This value is restored at TH trigger point ATR. This requires saving the host name portion of the Session-ID AVP value in the PTR. This host name restoral procedure is not required for Answers initiated by internal nodes as these Answer responses are based upon the original Request message content.

An example of a Protected-vAF/pCSCF to Untrusted-hPCRF Diameter transaction is shown in Figure 9-21.

Figure 9-21 Protected vAF/pCSCF to Untrusted-hPCRF Transaction



To ensure all Rx messages for the same session are modified using the same pseudo-name, Session-ID AVP can be used as a key to select a Pseudo Host Name for an Actual Host Name.

For Protected-vAF/pCSCF to Untrusted-hPCRF Rx transactions, S9 Af/pCSCF topology hiding is only required on Request messages at topology hiding point RTH which meet the following criteria:

- The message was a candidate for topology hiding as defined by topology trigger point RTH and
- S9 AF/pCSCF TH is enabled for the Protected Network (S9 PCRF TH Configuration Set is assigned to the Protected Network) and
- The Request message is a member of the Rx message set and was initiated by an AF/pCSCF and
- The Origin-Host and/or Session-ID AVPs in the Request contain an actual AF/pCSCF host name assigned to the Protected Network via the S9 AF/pCSCF TH Configuration Set.

For Protected-vAF/pCSCF to Untrusted-hPCRF transactions, AF/pCSCF topology information restoral is only performed on Answer messages which meet the following criterion:

- At TH Trigger Point ATR, the AF/pCSCF TH ATR flag in the PTR associated with the Answer message is set to Enabled.

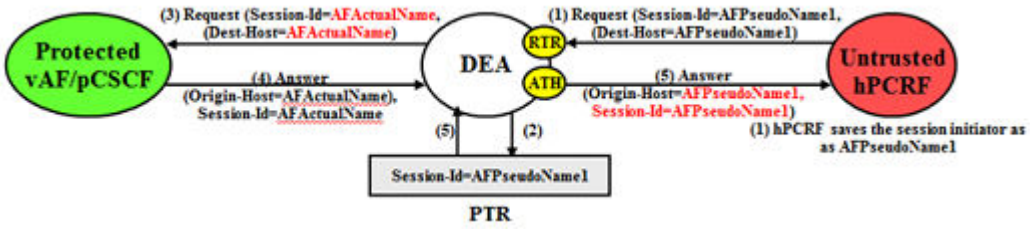
Untrusted-hPCRF to Protected-vAf/pCSCF Transactions

When an Untrusted-hPCRF initiates a transaction to a Protected-vAF/pCSCF, it is most likely addressed to one of the vAF/pCSCF pseudo-host names that the hPCRF saved in a previous vAF/pCSCF-to-hPCRF transaction for which S9 AF/pCSCF TH was applied. For Untrusted-hPCRF to Protected-vAF/pCSCF Diameter transactions (RAR, ASR, and so on), S9 AF/pCSCF TH is concerned with the following topology information hiding and resotral issues:

- The Destination-Host AVP contains a vAF/pCSCF pseudo-host name. This pseudo-host name must be replaced with the vAF/pCSCF's actual-host name at TH trigger point RTR. It's perfectly acceptable that an Untrusted-hPCRF to Protected-vAF/pCSCF Request message does not contain a vAF/pCSCF pseudo-host name. If the Destination-Host AVP value does not match a Pseudo-Host entry in the TH Host Name table , then no host name conversion is required and the Request message is routed as normal. Destination-Host name conversion is performed to prevent the following problems:
  - Certain vAF/pCSCFs do not accept messages that do not contain its actual host name
  - Diameter routing problems associated with pseudo-host names. For example, DRL Implicit Routing currently only works with actual host names (for example, the FQDN assigned to the Peer Node and used for the Capabilities Exchange procedure (CER/CEA)).
  - The host portion of Session-ID AVP containing a vAF/pCSCF pseudo-host name must be replaced back with vAF/pCSCF's actual host name at TH trigger point RTR
  - An Origin-Host AVP containing an vAF/pCSCF's actual-host name in the Answer response from the Protected- vAF/pCSCF must be hidden with one of the pseudo-host names assigned to that vAF/pCSCF. This is done at TH trigger point ATH.
  - Session-ID AVP containing an vAF/pCSCF's actual-host name in the Answer response from the Protected-vAF/pCSCF must be hidden with one of the pseudo-host names assigned to that vAF/pCSCF. This is done at TH trigger point ATH.

An example of an Untrusted-hPCRF to Protected- vAF/pCSCF Diameter transaction is shown in Figure 9-22.

Figure 9-22 Untrusted-hPCRF to Protected-vAF/pCSCF Transaction



For Untrusted-hPCRF to Protected-vAF/pCSCF transactions, S9 AF/pCSCF TH is only invoked on Request messages at topology trigger point RTR which meet the following criteria:

- Message was a candidate for topology hiding as defined by topology trigger point RTR and
- S9 AF/pCSCF TH is enabled for the Protected Network (S9 AF/pCSCF TH Configuration Set is assigned to the Protected Network) and
- The Request message is a member of the Rx message set and was initiated by a AF/pCSCF and

- The Destination-Host AVP or host portion of Session-ID AVP contains a AF/pCSCF pseudo-host name that is assigned to the Protected Network as determined from the internal AF/pCSCF TH Pseudo-Host Name
- Message was a candidate for topology hiding as defined by topology trigger point ATH
- S9 AF/pCSCF TH is enabled for the Protected Network (S9 AF/pCSCF TH Configuration Set is assigned to the Protected Network)
- The Answer message is a member of the Rx message set and was initiated by a AF/pCSCF
- The Origin-Host AVP or host portion of Session-ID AVP contains an actual AF/pCSCF host name that is assigned to the Protected Network via the S9 AF/pCSCF TH Configuration Set

Protected-hPCRF to Untrusted-vAF/pCSCF Transactions

When AF/pCSCF and PCRF are in untrusted network and AF/pCSCF uses vPCRF in proxy to communicate Rx messages initiated by vAF/pCSCF to hPCRF in protected network, then S9 PCRF TH is used to hide PCRF host names to untrusted network.

Untrusted-vAF/pCSCF to Protected-hPCRF Transactions

When AF/pCSCF and PCRF are in untrusted network and AF/pCSCF uses vPCRF in proxy to communicate Rx messages initiated by hPCRF in protected network to vAF/pCSCF, then S9 PCRF TH is used to hide PCRF host names to untrusted network.

9.2 Trusted Networks Lists

A Trusted Network List is a list of Realms identifying networks where Topology Hiding is NOT 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**, and then **Configuration**, and then **Topology Hiding**, and then **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 **Insert**.

  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**, and then **Configuration**, and then **Topology Hiding**, and then **Trusted Networks Lists** page does not open and an error message is displayed.
- Select a **Trusted Networks List Name** in the list and click **Edit**.

  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 **Delete** to remove the selected Trusted Networks List. See Deleting a Trusted Network List.

9.2.1 Diameter Trusted Network Lists Elements

Table 9-17 describes the fields on the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Trusted Networks Lists** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 9-17 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 is not applied. Click **Add** 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

9.2.2 Adding a Trusted Network List

Use this task on the NOAM to create a new Trusted Network List. The fields are described in Diameter Trusted Network Lists Elements.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding > Trusted Network Lists**.
2. Click **Insert**.
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**, and then **Configuration**, and then **Topology Hiding**, and then **Trusted Networks Lists** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Trusted Networks Lists** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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

9.2.3 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. Click **Diameter**, and then **Configuration**, and then **Topology Hiding > Trusted Network Lists**.
2. Select the **Trusted Network List** you want to edit.
3. Click **Edit**.

   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 Diameter Trusted Network Lists Elements.
5. Click:
   - **OK** to save the data and return to the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Trusted Networks Lists** page .
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Trusted Networks Lists** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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)

9.2.4 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 it is referenced by either a Peer Node or a Routing Option Set is referenced by Protected Networks. It also cannot be deleted if it is associated with any Routing Option Set.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Trusted Networks Lists**.
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**, and then **Configuration**, and then **Topology Hiding**, and then **Trusted Networks 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.

9.3 Path Topology Hiding Configuration Sets

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 Diameter Topology Hiding 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.
- Proxy-Host Pseudo Hostname – Proxy-Host Pseudo Hostname is used while replacing the host name in the Proxy-Host AVP.
- Encryption Key – Encryption key used for Error-Reporting-Host obscuring.

On the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **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 **Insert**.
  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, then the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Path Topology Hiding Configuration Sets [Insert]** page does not open and an error message is displayed.
- Select a Path Topology Hiding Configuration Set Name in the list and click **Edit**.

You can edit the selected Path Topology Hiding Configuration Set. See Editing a Path Topology Hiding Configuration Set.

If at least one Protected Network references the Path Topology Hiding Configuration Set, then the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Path Topology Hiding Configuration Sets [Edit]** page does not open.

- Select a Path Topology Hiding Configuration Set Name in the list and click **Delete** 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, then the Configuration Set is not deleted.

9.3.1 Diameter Topology Hiding Path Topology Hiding Configuration Set Elements

Table 9-18 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 9-18 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 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.

Table 9-18 (Cont.) Path Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* 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 Range: up to 16 characters; valid Encryption Key

9.3.2 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 Diameter Topology Hiding Path Topology Hiding Configuration Set Elements.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Path Topology Hiding Configuration Sets**.
2. Click **Insert**.

> **Note**
>
> If the maximum number of Configuration Sets allowed in the system (500) has been configured, then the Path Topology Hiding Configration Sets page does 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, then 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.

9.3.3 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. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Path Topology Hiding Configuration Sets**.
2. Select the Path Topology Hiding Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.

   For information about each field, see Diameter Topology Hiding 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, then 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.

9.3.4 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. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Path Topology Hiding Configuration Sets**.
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.

9.4 S6a/S6d HSS Topology Hiding Configuration Sets

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**HSS.

The fields are described in Diameter 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.
- Use S6a/S6d Single HSS Pseudo Hostname - If checked, then Single HSS Pseudo Hostname are used for all HSS actual hostnames.

  > **Note**
  >
  > When the **Use S6a/S6d Single HSS Pseudo Host Name**HSS field is configured, all HSS TH Configuration Set fields associated with multiple pseudo-host names must not be configured

- S6a/S6d Single HSS Pseudo Hostname - S6a/S6d HSS Pseudo Hostname
- Pseudo Hostname Generation - Attributes to control the format and generation of Pseudo Hostnames corresponding to an Actual Hostname.

> **Note**
>
> In order to support multiple pseudo hostnames for each HSS real hostname, each S6a/S6d TH Configuration set includes the following attributes:
>
> – 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 S6a/S6d HSS Topology Hiding Configuration Set.
- S6a/S6d HSS 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 S6a/S6d HSS Topology Hiding Configuration Set.
- S6a/S6d HSS Actual Hostname Not Found Answer Result-Code Value - Value to be placed in the Result-Code AVP of the Answer message.
- S6a/S6d HSS Actual Hostname Not Found Vendor ID - Vendor ID is placed in Vendor ID AVP.
- S6a/S6d HSS Actual Hostname Not Found Answer Error Message - String to be placed in the Error-Message AVP of the Answer message.

On the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S6a/S6d HSS Topology Hiding Configuration Sets**HSS 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**HSS in ascending ASCII order.
- Click **Insert**.
  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, then the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S6a/S6d HSS Topology Hiding Configuration Sets [Insert]** page does not open and an error message is displayed.
- Select a S6a/S6d HSS Topology Hiding Configuration Set Name in the list and click **Edit**. 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 **Delete** 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, then the Configuration Set is not deleted.

9.4.1 Diameter S6a/S6d HSS Topology Hiding Configuration Set Elements

Table 9-19 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 9-19 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

Table 9-19 (Cont.) S6a/S6d HSS Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Use S6a/S6d Single HSS Pseudo Hostname	If checked, Single HSS Pseudo Hostname are used for all HSS actual hostnames.	Default: Checked Range: n/a

Note

When the **Use S6a/S6d Single HSS Pseudo Host Name**HSS field is configured, all HSS TH Configuration Set fields associated with multiple pseudo-host names must not be configured

Table 9-19 (Cont.) S6a/S6d HSS Topology Hiding Configuration Sets Elements

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

Table 9-19 (Cont.) S6a/S6d HSS Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
Pseudo Hostname Generation	Attributes to control the format and generation of Pseudo Hostnames corresponding to an Actual Hostname. **Note** In order to support multiple pseudo hostnames for each HSS real hostname, each S6a/S6d TH Configuration set includes the following attributes: • **Count** - The maximum number of Pseudo Hostnames associated with an Actual Hostname. • **Randomize Count** - If checked, random number of Pseudo Hostnames between 1 and Count are associated with an Actual Hostname. • **Auto Generate** - If checked, Pseudo Hostnames are automatically generated	Count: • Default = 3 • Range = 1 - 3 Randomize Count: • Default = Checked • Range = n/a Auto Generate: • Default = Checked • Range = n/a Prefix: • Default = n/a • Range = A valid Prefix Suffix: • Default = n/a • Range = A valid Suffix Length: • Default = 4 • Range = 4 - 5

Table 9-19 (Cont.) S6a/S6d HSS Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
	corresponding to an Actual Hostname. • **Prefix** - Prefix for the auto generated Pseudo Hostname. Prefix is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. Prefix must be at most 63 characters long. • **Suffix** - Suffix for the auto generated Pseudo Hostname. Suffix is 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. Suffix must be at most 63 characters long. • **Length** - Length of the random number used in the auto generated Pseudo Hostname.	
* Hostnames	List of Actual Hostnames and their Pseudo Hostnames in this S6a/S6d HSS 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 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.
S6a/S6d HSS 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 S6a/S6d HSS Topology Hiding Configuration Set.	Default: Send Answer Range: n/a

Table 9-19 (Cont.) S6a/S6d HSS Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
S6a/S6d HSS Actual Hostname Not Found Answer Result-Code Value	Value to be placed in the Result-Code AVP of the Answer message. S6a/S6d HSS Actual Hostname Not Found Answer Result-Code Value is required if action is Send Answer.	Default: 3002 Range: 1000 - 5999
S6a/S6d HSS Actual Hostname Not Found Vendor ID	Vendor ID is placed in Vendor ID AVP	Default: n/a Range: 1 - 4294967295
S6a/S6d HSS Actual Hostname Not Found Answer Error Message	String to be placed in the Error-Message AVP of the Answer message	Default: null string, no Error-Message AVP in Answer message Range: 0 - 64 characters

9.4.2 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 Diameter S6a/S6d HSS Topology Hiding Configuration Set Elements.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S6a/S6d HSS Topology Hiding Configuration Sets**.

   > **Note**
   >
   > If the maximum number of Configuration Sets allowed in the system (500) has been configured, then the S6a/S6d HSS Topology Hiding Configuration SetsHSS page does not open.

2. Click **Insert**.
3. Enter a unique name for the Configuration Set in the **S6a/S6d HSS Topology Hiding Configuration Set Name** field.
4. Check or uncheck the box for the **Use S6a/S6d Single HSS Pseudo Hostname** field to indicate whether or not a Single HSS Pseudo Hostname is used for all HSS actual hostnames.
5. Enter a unique name to be used when replacing the S6a/S6d HSS Hostname in the **S6a/S6d Single HSS Pseudo Hostname** field.
6. Set the **Count**, **Randomize Count**, **Auto Generate**, **Prefix**, **Suffix**, and **Length** attributes associated with **Pseudo Hostname Generation**.
7. Add **Hostnames** to serve as Actual Hostnames and their Pseudo Hostnames in the S6a/S6d HSS Topology Hiding Configuration Set.
8. Select an **S6a/S6d HSS Actual Hostname Not Found Action** to be performed when the Orig-Host in the Diameter message is not configured as Actual Hostname in this S6a/S6d HSS Topology Hiding Configuration Set in the field.
9. Enter an **S6a/S6d HSS Actual Hostname Not Found Answer Result-Code Value** to be placed in the Result-Code AVP of the Answer message.

10. Enter an **S6a/S6d HSS Actual Hostname Not Found Vendor ID** to be placed in Vendor Id AVP.
11. Enter an **S6a/S6d HSS Actual Hostname Not Found Answer Error Message** to be placed in the Error-Message AVP of the Answer message.
12. 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, then 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.

9.4.3 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. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S6a/S6d HSS Topology Hiding Configuration Sets**.
2. Select the S6a/S6d HSS Topology Hiding Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.

   For information about each field, see Diameter 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, then 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.

9.4.4 Deleting an S6a/S6d HSS Topology Hiding Configuration Set

Use this task to delete an S6a/S6d HSS Topology Hiding Configuration Set.

> **Note**
>
> An S9 AF/pCSCF Topology Hiding Configuration Set that is used in a Protected Network cannot be deleted.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S6a/S6d HSS Topology Hiding Configuration Sets**.
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.

9.5 MME/SGSN Topology Hiding Configuration Sets

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 Diameter 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**, and then **Configuration**, and then **Topology Hiding**, and then **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 **Insert**.
  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**, and then **Configuration**, and then **Topology Hiding**, and then **MME/SGSN Topology Hiding Configuration Sets [Insert]** page does not open, and an error message displays.
- Select a MME/SGSN Topology Hiding Configuration Set Name in the list and click **Edit**.
  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 **Delete** 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, then the Configuration Set is not deleted.

9.5.1 Diameter MME/SGSN Topology Hiding Configuration Set Elements

Table 9-20 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 9-20 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:	

Table 9-20 (Cont.) MME/SGSN Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
	Count - The maximum number of Pseudo Hostnames associated with an Actual Hostname.	Format: 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 contai 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: List Range: 4, 5 Default: 4

Table 9-20 (Cont.) MME/SGSN Topology Hiding Configuration Sets Elements

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 **Add** 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: options 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: options with values as a text box and a 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
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.

9.5.2 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 Diameter MME/SGSN Topology Hiding Configuration Set Elements.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **MME/SGSN Topology Hiding Configuration Sets**.
2. Click **Insert**.

> **Note**
>
> If the maximum number of Configuration Sets allowed in the system (500) has been configured, then the MME/SGSN Topology Hiding Configuration Sets page does 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, then 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.

9.5.3 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. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **MME/SGSN Topology Hiding Configuration Sets**.
2. Select the MME/SGSN Topology Hiding Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.

   For information about each field, see Diameter 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, then 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.

9.5.4 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. Click **Diameter**, and then **Configuration**, and then **Toplogy Hiding**, and then **MME/SGSN Toplogy Hiding Configuration Sets**.
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.

9.6 S9 PCRF Topology Hiding Configuration Sets

S9 PCRF Topology Hiding Configuration Sets provide information that is used to perform S9 PCRF Topology Hiding for a Protected Network's PCRFs, as well as the number of PCRFs in the network, when it exchanges messages with Untrusted Networks. A PCRF's identity is embedded in the Origin-Host and Session-ID AVPs sent in Request messages and the Origin-Host AVP sent in Answer messages.

The fields are described in Diameter S9 PCRF Topology Hiding Configuration Set Elements.

Each S9 PCRF Topology Hiding Configuration Set contains the following information:

- S9 PCRF 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 S9 PCRF Topology Hiding Configuration Set.
- S9 PCRF 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 S9 PCRF Topology Hiding Configuration Set.
- S9 PCRF Actual Hostname Not Found Answer Result-Code Value - Value to be placed in the Result-Code AVP of the Answer message.
- S9 PCRF Actual Hostname Not Found Vendor ID - Vendor ID is placed in Vendor ID AVP.
- S9 PCRF Actual Hostname Not Found Answer Error Message - String to be placed in the Error-Message AVP of the Answer message.

On the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 PCRF Topology Hiding Configuration Sets** page, you can perform the following actions:

- Filter the list of S9 PCRF Topology Hiding Configuration Sets to display only the desired S9 PCRF 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 **S9 PCRF Topology Hiding Configuration Set Name** in ascending ASCII order.
- Click **Insert**.
  On the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 PCRF Topology Hiding Configuration Sets [Insert]** page, you can add a new S9 PCRF Topology Hiding Configuration Set and its elements. Adding an S9 PCRF Topology Hiding Configuration Set describes the fields on the S9 PCRF Topology Hiding Configuration Sets

  If the maximum number of S9 PCRF Topology Hiding Configuration Sets (500) already exists in the system, then the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 PCRF Topology Hiding Configuration Sets [Insert]** page does not open and an error message is displayed.
- Select a S9 PCRF Topology Hiding Configuration Set Name in the list and click **Edit**.
  On the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 PCRF Topology Hiding Configuration Sets [Edit]** page, you can edit the selected S9 PCRF Configuration Set. See Editing an S9 PCRF Topology Hiding Configuration Set.
- Select a S9 PCRF Topology Hiding Configuration Set Name in the list and click **Delete** to remove the selected S9 PCRF Topology Hiding Configuration Set. See Deleting an S9 PCRF Topology Hiding Configuration Set.
  If the selected S9 PCRF Topology Hiding Configuration Set is used in a Protected Network, then the Configuration Set is not deleted.

9.6.1 Diameter S9 PCRF Topology Hiding Configuration Set Elements

Table 9-21 describes the fields on the S9 PCRF 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 9-21 S9 PCRF Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* S9 PCRF Topology Hiding Configuration Set Name	A name that uniquely identifies the S9 PCRF 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

Table 9-21 (Cont.) S9 PCRF Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
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** - If checked, random number of Pseudo Hostnames between 1 and Count are associated with an Actual Hostname. • **Auto Generate** - If checked, Pseudo Hostnames are automatically generated corresponding to an Actual Hostname. • **Prefix** - Prefix for the auto generated Pseudo Hostname. Prefix is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. Prefix must be at most 63 characters long. • **Suffix** - Suffix for the auto generated Pseudo Hostname. Suffix is 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. Suffix must be at most 63 characters long. • **Length** - Length of the random number used in the auto generated Pseudo Hostname.	Count: • Default = 3 • Range = 1 - 3 Randomize Count: • Default = Checked • Range = n/a Auto Generate: • Default = Checked • Range = n/a Prefix: • Default = n/a • Range = A valid Prefix Suffix: • Default = n/a • Range = A valid Suffix Length: • Default = 4 • Range = 4 - 5

Table 9-21 (Cont.) S9 PCRF Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Hostnames	List of Actual Hostnames and their Pseudo Hostnames in this S9 PCRF 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 must end with a letter or digit. Underscores can be used only as the first character. Label - up to 63 characters; S9 PCRF Pseudo Hostname - up to 255 characters.
S9 PCRF 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 S9 PCRF Topology Hiding Configuration Set.	Default: Send Answer Range: n/a
S9 PCRF Actual Hostname Not Found Answer Result-Code Value	Value to be placed in the Result-Code AVP of the Answer message. S9 PCRF Actual Hostname Not Found Answer Result-Code Value is required if action is Send Answer.	Default: 3002 Range: 1000 - 5999
S9 PCRF Actual Hostname Not Found Vendor ID	Vendor ID is placed in Vendor ID AVP	Default: n/a Range: 1 - 4294967295
S9 PCRF Actual Hostname Not Found Answer Error Message	String to be placed in the Error-Message AVP of the Answer message	Default: null string, no Error-Message AVP in Answer message Range: 0 - 64 characters

9.6.2 Adding an S9 PCRF Topology Hiding Configuration Set

Use this task to create a new S9 PCRF Topology Hiding Configuration Set.

For more information about the fields, see Diameter S9 PCRF Topology Hiding Configuration Set Elements.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 PCRF Topology Hiding Configuration Sets**.

   > **Note**
   >
   > If the maximum number of Configuration sets allowed in the system (500) has been configured, then the S9 PCRF Topology Hiding Configuration Sets page does not open.

2. Click **Insert**.
3. Enter a unique name for the Configuration Set in the **S9 PCRF Topology Hiding Configuration Set Name** field.

4. Select/Enter desired values for the **Pseudo Hostname Generation** field.
5. Select a unique name to be used when replacing the S9 PCRF Hostname in the **Hostnames** field.
6. In the **S9 PCRF Actual Hostname Not Found Action** field, select the action to be taken if the Actual Hostname is not found.
7. In the **S9 PCRF Actual Hostname Not Found Answer Result-Code Value** field, enter a value to be placed in the Result-Code AVP of the Answer message.
8. In the **S9 PCRF Actual Hostname Not Found Vendor Id** field, enter a Vender Id to be place in the Vendor id AVP.
9. In the **S9 PCRF Actual Hostname Not Found Answer Error Message** field, enter a string to be placed in the Error-Message AVP of the Answer message.
10. Click:
    - **OK** to save the changes and return to the S9 PCRF Topology Hiding Configuration Sets page.
    - **Apply** to save the changes and remain on this page.
    - **Cancel** to return to the S9 PCRF Topology Hiding Configuration Sets page without saving any changes.

    If **OK** or **Apply** is clicked and any of the following conditions exist, then 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 **S9 PCRF Topology Hiding Configuration Set Name** is not unique; it already exists in the system.

9.6.3 Editing an S9 PCRF Topology Hiding Configuration Set

Use this task to edit an existing S9 PCRF Topology Hiding Configuration Set.

When the S9 PCRF Topology Hiding Configuration Sets page opens, the fields are populated with the currently configured values.

The **S9 PCRF Topology Hiding Configuration Set Name** cannot be edited.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 PCRF Topology Hiding Configuration Sets**.

> **Note**
>
> If the maximum number of Configuration Sets allowed in the system (500) has been configured, then the MME/SGSN Topology Hiding Configuration Sets page does not open.

2. Click **Edit**.
3. Enter a unique name for the Configuration Set in the **S9 PCRF Topology Hiding Configuration Set Name** field.
4. Select/Enter desired values for the **Pseudo Hostname Generation** field.
5. Select a unique name to be used when replacing the S9 PCRF Hostname in the **Hostnames** field.

6. In the **S9 PCRF Actual Hostname Not Found Action** field, select the action to be taken if the Actual Hostname is not found.
7. In the **S9 PCRF Actual Hostname Not Found Answer Result-Code Value** field, enter a value to be placed in the Result-Code AVP of the Answer message.
8. In the **S9 PCRF Actual Hostname Not Found Vendor Id** field, enter a Vender ID to be placed in the Vendor ID AVP.
9. In the **S9 PCRF Actual Hostname Not Found Answer Error Message** field, enter a string to be placed in the Error-Message AVP of the Answer message.
10. Click:
    - **OK** to save the changes and return to the S9 PCRF Topology Hiding Configuration Sets page.
    - **Apply** to save the changes and remain on this page.
    - **Cancel** to return to the S9 PCRF Topology Hiding Configuration Sets page without saving any changes.

    If **OK** or **Apply** is clicked and any of the following conditions exist, then 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 **S9 PCRF Topology Hiding Configuration Set Name** is not unique; it already exists in the system.

9.6.4 Deleting an S9 PCRF Topology Hiding Configuration Set

Use this task to delete an S9 PCRF Topology Hiding Configuration Set.

> **Note**
>
> An S9 AF/pCSCF Topology Hiding Configuration Set that is used in a Protected Network cannot be deleted.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 PCRF Topology Hiding Configuration Sets**.
2. Select the S9 PCRF 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 S9 PCRF Topology Hiding Configuration Set.
    - **Cancel** to cancel the delete function and return to the S9 PCRF Topology Hiding Configuration Sets page.

9.7 S9 AF/pCSCF Topology Hiding Configuration Sets

S9 AF/pCSCF Topology Hiding Configuration Sets provide information that is used to perform S9 AF/pCSCF Topology Hiding for a Protected Network's PCRFs, as well as the number of PCRFs in the network, when it exchanges messages with Untrusted Networks. A PCRF's

identity is embedded in the Origin-Host and Session-ID AVPs sent in Request messages and the Origin-Host AVP sent in Answer messages.

The fields are described in Diameter S9 AF/pCSCF Topology Hiding Configuration Set Elements.

Each S9 AF/pCSCF Topology Hiding Configuration Set contains the following information:

- S9 AF/pCSCF 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 S9 PCRF Topology Hiding Configuration Set.
- S9 AF/pCSCF 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 S9 AF/pCSCF Topology Hiding Configuration Set.
- S9 AF/pCSCF Actual Hostname Not Found Answer Result-Code Value - Value to be placed in the Result-Code AVP of the Answer message.
- S9 AF/pCSCF Actual Hostname Not Found Vendor ID - Vendor ID is placed in Vendor ID AVP.
- S9 AF/pCSCF Actual Hostname Not Found Answer Error Message - String to be placed in the Error-Message AVP of the Answer message.

On the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 AF/pCSCF Topology Hiding Configuration Sets** page, you can perform the following actions:

- Filter the list of S9 AF/pCSCF Topology Hiding Configuration Sets to display only the desired S9 AF/pCSCF 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 **S9 AF/pCSCF Topology Hiding Configuration Set Name** in ascending ASCII order.
- Click **Insert**.
  You can add a new S9 AF/pCSCF Topology Hiding Configuration Set and its elements. See Adding an S9 AF/pCSCF Topology Hiding Configuration Set.

  If the maximum number of S9 AF/pCSCF Topology Hiding Configuration Sets (500) already exists in the system, then the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 AF/pCSCF Topology Hiding Configuration Sets [Insert]** page does not open and an error message displays.
- Select a S9 AF/pCSCF Topology Hiding Configuration Set Name in the list and click **Edit**.

You can edit the selected S9 AF/pCSCF Configuration Set. See Editing an S9 AF/pCSCF Topology Hiding Configuration Set.

- Select a S9 AF/pCSCF Topology Hiding Configuration Set Name in the list and click **Delete** to remove the selected S9 AF/pCSCF Topology Hiding Configuration Set. See Deleting an S9 AF/pCSCF Topology Hiding Configuration Set.
  If the selected S9 AF/pCSCF Topology Hiding Configuration Set is used in a Protected Network, then the Configuration Set is not deleted.

9.7.1 Diameter S9 AF/pCSCF Topology Hiding Configuration Set Elements

Table 9-22 describes the fields on the S9 AF/pCSCF 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 9-22 S9 AF/pCSCF Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* S9 AF/pCSCF Topology Hiding Configuration Set Name	A name that uniquely identifies the S9 AF/pCSCF 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

Table 9-22 (Cont.) S9 AF/pCSCF Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
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** - If checked, random number of Pseudo Hostnames between 1 and Count are associated with an Actual Hostname. • **Auto Generate** - If checked, Pseudo Hostnames are automatically generated corresponding to an Actual Hostname. • **Prefix** - Prefix for the auto generated Pseudo Hostname. Prefix is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. Prefix must be at most 63 characters long. • **Suffix** - Suffix for the auto generated Pseudo Hostname. Suffix is 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. Suffix must be at most 63 characters long. • **Length** - Length of the random number used in the auto generated Pseudo Hostname.	Count: • Default = 3 • Range = 1 - 3 Randomize Count: • Default = Checked • Range = n/a Auto Generate: • Default = Checked • Range = n/a Prefix: • Default = n/a • Range = A valid Prefix Suffix: • Default = n/a • Range = A valid Suffix Length: • Default = 4 • Range = 4 - 5

Table 9-22 (Cont.) S9 AF/pCSCF Topology Hiding Configuration Sets Elements

Field (* indicates required field)	Description	Data Input Notes
* Hostnames	List of Actual Hostnames and their Pseudo Hostnames in this S9 AF/pCSCF 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 must end with a letter or digit. Underscores can be used only as the first character. Label - up to 63 characters; S9 AF/pCSCF Pseudo Hostname - up to 255 characters.
S9 AF/pCSCF 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 S9 AF/pCSCF Topology Hiding Configuration Set.	Default: Send Answer Range: N/A
S9 Af/pCSCF Actual Hostname Not Found Answer Result-Code Value	Value to be placed in the Result-Code AVP of the Answer message. S9 AF/pCSCF Actual Hostname Not Found Answer Result-Code Value is required if action is Send Answer.	Default: 3002 Range: 1000 - 5999
S9 AF/pCSCF Actual Hostname Not Found Vendor ID	Vendor ID is placed in Vendor ID AVP.	Default: n/a Range: 1 - 4294967295
S9 AF/pCSCF Actual Hostname Not Found Answer Error Message	String to be placed in the Error-Message AVP of the Answer message.	Default: null string, no Error-Message AVP in Answer message Range: 0 - 64 characters

9.7.2 Adding an S9 AF/pCSCF Topology Hiding Configuration Set

Use this task to create a new S9 AF/pCSCF Topology Hiding Configuration Set.

For more information about the fields, see Diameter S9 AF/pCSCF Topology Hiding Configuration Set Elements.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 AF/pCSCF Topology Hiding Configuration Sets**.

> **Note**
>
> If the maximum number of Configuration Sets allowed in the system (500) has been configured, then the S9 AF/PCRF Topology Hiding Configuration Sets page does not open.

2. Click **Insert**.

3. Enter a unique name for the Configuration Set in the **S9 AF/pCSCF Topology Hiding Configuration Set Name** field.
4. Enter a unique name to be used when replacing the S9 AF/pCSCF Hostname in the **S9 AF/pCSCF Pseudo Hostname** field.
5. Click:
   - **OK** to save the changes and return to the S9 AF/pCSCF Topology Hiding Configuration Sets page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the S9 AF/pCSCF Topology Hiding Configuration Sets page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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 **S9 AF/pCSCF Topology Hiding Configuration Set Name** is not unique; it already exists in the system.

9.7.3 Editing an S9 AF/pCSCF Topology Hiding Configuration Set

Use this task to edit an existing S9 AF/pCSCF Topology Hiding Configuration Set.

When the S9 AF/pCSCF Topology Hiding Configuration Sets page opens, the fields are populated with the currently configured values.

The **S9 AF/pCSCF Topology Hiding Configuration Set Name** cannot be edited.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 AF/pCSCF Topology Hiding Configuration Sets**.
2. Select the S9 AF/pCSCF Topology Hiding Configuration Set you want to edit.
3. Click **Edit**.
4. Update the relevant fields.

   For information about each field, see Diameter S9 AF/pCSCF Topology Hiding Configuration Set Elements.
5. Click:
   - **OK** to save the data and return to the S9 AF/pCSCF Topology Hiding Configuration Sets page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the S9 AF/pCSCF Topology Hiding Configuration Sets page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then an error message appears:
   - The selected S9 AF/pCSCF 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.

9.7.4 Deleting an S9 AF/pCSCF Topology Hiding Configuration Set

Use this task to delete an S9 AF/pCSCF Topology Hiding Configuration Set.

> **Note**
>
> An S9 AF/pCSCF Topology Hiding Configuration Set that is used in a Protected Network cannot be deleted.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **S9 AF/pCSCF Topology Hiding Configuration Sets**.
2. Select the S9 AF/pCSCF 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 S9 AF/pCSCF Topology Hiding Configuration Set.
   - **Cancel** to cancel the delete function and return to the S9 AF/pCSCF Topology Hiding Configuration Sets page.

9.8 Protected Networks

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 Diameter 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.
- S9 PCRF Topology Hiding Configuration Set - S9 PCRF Topology Hiding Configuration Set name for this 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.
- S9 AF/pCSCF Topology Hiding Configuration Set - S9 AF/pCSCF Topology Hiding Configuration Set name for this Protected Network

On the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **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**, and then **Configuration**, and then **Topology Hiding [Filtered]** view page for that entry only.
- Click **Insert**.

  You can add a new Protected Network.

  The **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Protected Networks [Insert]** does 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**.

  You can edit the selected Protected Network
- Select a Protected Network in the list and click **Delete**. You can delete the selected Protected Network.

9.8.1 Diameter Protected Network Configuration Elements

Table 9-23 describes the fields on the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **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 9-23 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: 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: List Range: -Disabled-; configured Path Topology Configuration Sets Default: Disabled
S6a/S6d HSS Topology Hiding Configuration Set	S6a/S6d Topology Hiding Configuration Set name for this Protected Network.	Format: List Range: -Disabled-; configured S6a/S6d HSS Topology Configuration Sets Default: Disabled

Table 9-23 (Cont.) Protected Network Configuration Elements

Field (* indicates required field)	Description	Data Input Notes
MME/SGSN Topology Hiding Configuration Set	MME/SGSN Topology Hiding Configuration Set name for this Protected Network.	Format: List Range: -Disabled-; configured MME/SGSN Topology Configuration Sets Default: Disabled
S9 PCRF Topology Hiding Configuration Set	S9 PCRF Topology Hiding Configuration Set name for this Protected Network	Format: List Range: -Disabled-; configured S9 PCRF Topology Configuration Sets Default: Disabled
S9 AF/pCSCF Topology Hiding Configuration Set	S9 AF/pCSCF Topology Hiding Configuration Set name for this Protected Network	Format: List Range: -Disabled-; configured S9 AF/pCSCF Topology Configuration Sets Default: Disabled

9.8.2 Adding a Protected Network

Use this task on the NOAM to create a new Protected Network.

The fields are described in Diameter Protected Network Configuration Elements.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Protected Networks**.
2. Click **Insert**.
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
   - S9 PCRF Topology Hiding Configuration Set
   - S9 AF/pCSCF Topology Hiding Configuration Set
6. Click **OK**, **Apply**, or **Cancel**.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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

9.8.3 Editing a Protected Network

Use this task to make changes to existing Protected Networks.

The **Protected Network Realm** cannot be changed.

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Protected Networks**.
2. Select the **Protected Network** you want to edit.
3. Click **Edit**.

   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 Diameter Protected Network Configuration Elements
5. Click:
   - **OK** to save the changes and return to the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Protected Networks** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Protected Networks** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then 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)

9.8.4 Deleting a Protected Network

Use this task on the NOAM to delete a Protected Network

1. Click **Diameter**, and then **Configuration**, and then **Topology Hiding**, and then **Protected Networks**.
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.

10 Diameter Egress Throttle List

The following components can be configured for Egress Throttle List:

- Rate Limiting Configuration Sets
- Pending Transaction Limiting Configuration Sets
- Egress Throttle Lists

> **Note**
>
> Egress Throttle List configuration components must be managed from the NOAM.

10.1 Egress Throttle List Overview

Egress Throttle Lists are collections of two or three Egress Throttle Groups, where each of those Egress Throttle Groups is configured on a different diameter routing systems. Egress Throttle Lists are used to implement Coordinated Egress Throttling across Multiple diameter routing systems. Egress Throttle Lists aggregate Egress Message Rate and Pending Transaction data from the component Egress Throttle Groups and use the aggregated metrics to throttle Requests to the component ETGs' peer nodes and connections.

Egress Throttle Lists have a similar data structure to Egress Throttle Groups. Both can track Egress Message Rate and Pending Transactions independently. Both have the same set of Onset and Abatement Thresholds for EMR and EPT, which are calculated from associated ETL Rate and Pending Transaction Limiting Configuration Sets.

The primary difference between Egress Throttle Lists and Egress Throttle Groups is that ETLs are provisioned at the NOAM level, while ETGs are provisioned at the SOAM level. Egress Throttle Groups are enabled and disabled with a maintenance GUI on the SOAM, but Egress Throttle Lists do not have an associated maintenance screen in a GUI. Egress Throttle Lists are enabled and disabled on a diameter signaling router by provisioning and maintenance actions against the component ETGs.

ETL Message Rate Limiting is controlled by the settings for the component ETGs, as described in Rate Limiting Configuration Sets and Diameter Maintenance Egress Throttle Groups. ETL Pending Transaction Limiting is controlled by the settings for the component ETGs, as described in Pending Transaction Limiting Configuration Sets and Diameter Maintenance Egress Throttle Groups.

Egress Throttle List Maintenance

Egress Throttle Lists perform two functions: rate limiting and pending transaction limiting. Each of the functions is independent of one another and can be optionally configured and controlled separately. Egress Throttle Lists does not have an associated GUI maintenance page to control whether Egress Message Rate Limiting and Egress Pending Transaction Rate Limiting are enabled or disabled. EMR and EPT Limiting for the ETL are controlled by maintenance changes to the ETL's component ETGs.

Because an Egress Throttle List is composed of Egress Throttle Groups provisioned on different routers, an Egress Throttle List instance on an MP has additional state data that an Egress Throttle Group does not have. This data is the number of SMS-controlled ComAgent connections between the local diameter router server and the other diameter router servers with Egress Throttle Groups in the Egress Throttle List. If the local diameter router server is connected to all other diameter router servers with ETGs in the ETL, the Egress Message Rate and Pending Transaction thresholds are based on values calculated from the associated ETL Rate and Pending Transaction Limiting Configuration Sets. But if the local diameter router server is not connected to all diameter router servers with ETGs in the ETL, the Egress Message Rate and Pending Transaction thresholds are reduced according to the Per SMS Connection Failure Percent Reduction parameter provisioned against the ETL on the local diameter signaling router.

The following is an example of the reduced EMR and EPT thresholds due to a connectivity failure with another diameter router server that has an ETG contained in an ETL. Assume that the ETL contains two ETGs in two different diameter router servers. The maximum rate for the ETL is 10,000 messages per second, and the maximum number of pending transactions is 12,000. The per-connection percent reduction value for each ETG is 50, which means that the maximum values of EMR and EPT should be reduced 50 percent if a diameter server router cannot connect to the other diameter signaling router to exchange aggregated data for the ETL. In this example, if one of the diameter signaling router cannot connect with the other, it uses 5,000 messages per second for the maximum EMR for the ETL, and it uses 6,000 transactions as the maximum EPT. The rate and pending transaction onset and abatement thresholds are calculated from these reduced maximums for as long as the diameter signaling router is not able to connect to the other diameter signaling router.

10.2 Rate Limiting Configuration Sets on the NOAM

Rate Limiting Configuration Sets configuration provides the mechanism to enter data needed by Egress Throttle Lists to perform egress throttling by egress message rate.

Rate Limiting Configuration Sets are inserted and edited on the NOAM via the **Main Menu: Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Rate Limiting Confuguration Sets** page. For details about the SOAM functionality, see Rate Limiting Configuration Sets.

The Rate Limiting Configuration Set fields are described in Rate Limiting Configuration Sets Elements.

On the Rate Limiting Configuration Sets page, you can perform the following actions:

- Filter the list of Rate Limiting Configuration Sets to display only the desired Rate Limiting Configuration Sets.
- Sort the list by column contents, in ascending or descending order, by clicking the column heading. The default order is by **Rate Limiting Configuration Set Name** in ascending ASCII order.
- Click **Insert**.
  You can add a new Rate Limiting Configuration Set. See Adding a Rate Limiting Configuration Set.

  If the maximum number of Rate Limiting Configuration Sets already exists in the system, an error message is displayed.
- Select a **Rate Limiting Configuration Set Name** in the list and click **Edit**.
  You can edit the selected Rate Limiting Configuration Set. See Editing a Rate Limiting Configuration Set.

  If no row is selected, **Edit** is disabled.

- Select a **Rate Limiting Configuration Set Name** in the list and click **Delete** to remove the selected Rate Limiting Configuration Set.
  The Default Rate Limiting Configuration Set can be edited, but cannot be deleted. See Deleting a Rate Limiting Configuration Set.

10.3 Pending Transaction Limiting Configuration Sets on the NOAM

Pending Transaction Limiting Configuration Sets configuration provides the mechanism to enter configuration data needed by Egress Throttle Groups to determine when to start throttling for pending transactions. For details about the SOAM functionality, see Pending Transaction Limiting Configuration Sets.

Pending Transaction Limiting Configuration Sets are inserted and edited on the NOAM via the **Main Menu: Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Pending Transaction Limiting Configuration Sets** page.

An ETL is always associated with an Pending Transaction Limiting Configuration Set that provides the following data for performing Pending Transaction Throttling based on pending transactions:

- Maximum pending transactions
- Onset and Abatement Thresholds:
  - Percentages of the maximums
  - Used with Message Priority to determine which requests to throttle
- Abatement time

You must change the Egress Throttling Control Scope of the Egress Throttle Group to ETL and enable Pending Transaction Limiting on the Egress Throttle Group before Egress Pending Transaction Limiting can be started on Egress Throttle Lists.

The Pending Transaction Limiting Configuration Sets fields are described in Pending Transaction Limiting Configuration Sets Elements.

On the Pending Transaction Limiting Configuration Sets page, you can perform the following actions:

- Filter the list of Pending Transaction Limiting Configuration Sets to display only the desired Pending Transaction Limiting Configuration Sets.
- Sort the list by column contents, in ascending or descending order, by clicking the column heading. The default order is by **Pending Transaction Limiting Configuration Sets** in ascending ASCII order.
- Click **Insert**.
  You can add a new Pending Transaction Limiting Configuration Sets. See Adding a Pending Transaction Limiting Configuration Set.

  If the maximum number of Pending Transaction Limiting Configuration Sets already exists in the system, an error message is displayed.
- Select a Pending Transaction Limiting Configuration Set Name in the list and click **Edit**.
  You can edit the selected Pending Transaction Limiting Configuration Set. See Editing a Pending Transaction Limiting Configuration Set.

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

- Select a **Pending Transaction Limiting Configuration Set Name** in the list and click **Delete** to remove the selected Pending Transaction Limiting Configuration Set.
  The Default Pending Transaction Limiting Configuration Set can be edited, but cannot be deleted. See Deleting a Pending Transaction Limiting Configuration Set.

10.4 Egress Throttle Lists on the NOAM

Egress Throttle Lists is used to manage coordinated Egress Throttling across multiple diameter signaling routers by adding Egress Throttle Groups to an Egress Throttle List. ETLs have congestion level states similar to Egress Throttle Groups, but they span multiple diameter signaling routers.

For Coordinated Egress Throttling across Multiple diameter signalling routers, all of the Egress Throttle Groups that belong to an Egress Throttle List must belong to the same network.

Egress Throttle Lists control the following functions:

- Defines the Egress Throttle List name.
- Identifies the site name, Egress Throttle Group, and the Connection Failure Percent Reduction.
- Establishes the Rate Limiting Configuration Set and the Pending Transaction Limiting Configuration Set.

10.4.1 Diameter Egress Throttle Lists Elements

Table 10-1 describes the fields on the **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists** page.

Table 10-1 Egress Throttle Lists Elements

Field (* indicates a required field)	Description	Data Input Notes
*Egress Throttle List Name	A name that uniquely identifies the Egress Throttle List.	Format: text box; alphanumeric and underscore; must contain at least one alpha and must not start with a digit. Range: 1 - 32 characters Default: NA
Site Name	The Site Name to associate to the Egress Throttle List Name.	Format: List. Default: NA
Egress Throttle Group	The Egress Throttle Group to associate to the Egress Throttle List Name.	Format: List. Range: NA Default: NA
Connection Failure Percent Reduction	The Connection Failure Percent Reduction to associate to the Egress Throttle List Name.	Format: List. Range: NA Range: Percent reduction for maximum rate and pending transactions per connectivity failure to other sites with ETGs in the ETL. 0% - 50% Default: 100

Table 10-1 (Cont.) Egress Throttle Lists Elements

Field (* indicates a required field)	Description	Data Input Notes
Rate Limiting Configuration Set	List of all of the Rate Limiting Configuration Sets.	Format: List. Range: NA Default: NA
Pending Transaction Limiting Configuration Set	List of all of the available Pending Transaction Limiting Configuration Sets.	Format: List. Range: NA Default: NA

10.4.2 Adding Egress Throttle Lists

Use this task to create new Egress Throttle Lists.

Egress Throttle Lists fields are described in Diameter Egress Throttle Lists Elements.

1. Click **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists.**.
2. Click **Insert**.
3. Enter a unique name for the Egress Throttle List in the **Egress Throttle List Name** field.
4. Select a **Site Name**.
5. Select a **Egress Throttle Group**.
6. Set a **Connection Failure Percent Reduction** value.
7. Select a **Rate Limiting Configuration Set**.
8. Select a **Pending Transaction Limiting Configuration Set**.
9. Click:
   - **OK** to save the changes and return to the **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, then an error message appears:
   - The maximum number of Egress Throttle Lists have already been created.
   - There is no Egress Throttle Group in the network element corresponding to the Egress Throttle List to be added.
   - Any required fields are left empty.
   - An Egress Throttle List is configured with duplicate Peers or Connections.
   - An Egress Throttle List is configured with a Egress Throttle Group already configured as a member in any Egress Throttle List.

10.4.3 Editing Egress Throttle Lists

Use this task to edit Egress Throttle Lists.

When the **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists [Edit]** page opens, the columns are initially populated with the current configuration of the selected Egress Throttle List.

The existing **Egress Throttle List Name** cannot be changed.

Changes can be made to an Egress Throttle List 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 List configuration irrespective of the Operational Status of the associated Peer Connections.

Egress Throttle Lists fields are described in Diameter Egress Throttle Lists Elements.

1. Click **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists**.
2. Select the Egress Throttle List to be edited, then click **Edit**.
3. Update the relevant fields.

   An entry in a list can be removed by selecting the entry in the list and clicking the **X** to the right of the list.
4. Click:
   - **OK** to save the changes and return to the **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists** page without saving any changes.

10.4.4 Deleting Egress Throttle Lists

Use this task to delete Egress Throttle Lists.

1. Click **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists**
2. Select the Egress Throttle List to be deleted.
3. Click **Delete**.

   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the Egress Throttle List.
   - **Cancel** to cancel the delete function and return to the **Diameter**, and then **Configuration**, and then **Egress Throttle List**, and then **Egress Throttle Lists** page.

   If **OK** is clicked and the following condition exists, then an error message appears:
   - If the ETL contains one or more ETGs that have their Egress Throttling Control Scope set to ETL. To delete the ETL, the Egress Throttling Control Scope for all of the ETGs in that ETL must be set to ETG.

11

Diameter Message Copy

The Diameter Message Copy function provides the ability to forward a copy of a Diameter Request message, and optionally the Answer message, routed through diameter routing to a Diameter Application Server (a DAS Peer). Diameter Message Copy can be triggered by a configuration or can be dictated by a routing application.

11.1 Diameter Message Copy Overview

Diameter Message Copy copies both Diameter Request and Answer messages as directed by one or more Trigger Points within the node. The Trigger Points can be any processing functions acting on the messages, including Diameter Mediation, diameter 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.

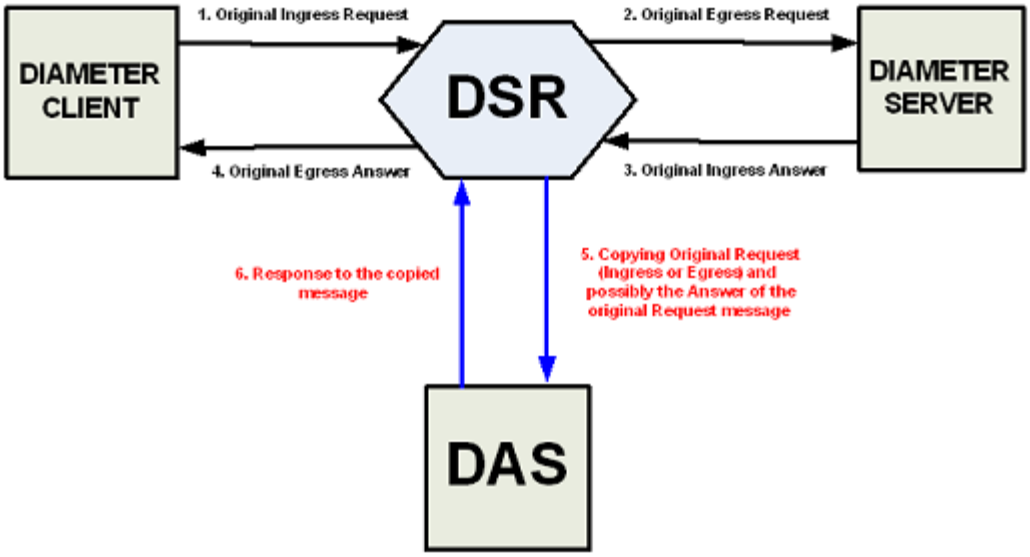
A copy of certain Diameter Request messages that transit a routing network can be used for such functions as bookkeeping and verification or for offering additional services. The criteria or triggering condition to copy a Request to a DAS Peer can be simple or complex, and might be based on the presence 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, 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 11-1 depicts this message flow overview:

Figure 11-1 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 diameter application determines the Requests to be copied to a DAS.

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 diameter application. When a Request message received, 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 Node (Ingress Request Message) or the final processed Request message routed out of the Node (Egress Request Message). The Trigger Point can determine whether the response Answer message received (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 is used (with its specified Route List).

The copy rules and trigger actions could be implemented as described in the following examples:

- 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 *Diameter Mediation User's Guide* for information about rule templates.

11.2 Diameter Message Copy

Diameter Message Copy 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 diameter 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, Diameter Message Copy 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 diameter processing, the Diameter Message header and data portions can get modified; a function like Mediation, a local diameter 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, and 2) after all the modifications are made 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 is useful at the DAS while processing the copied data. Diameter Message Copy supports copying the Ingress Answer messages along with the Request messages (Ingress or Egress); the Answer message alone cannot be copied to a DAS. Diameter Message Copy 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.

Diameter Message Copy 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 diameter 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 successfully copied Diameter Request is 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. 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 are 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.

> **Note**
>
> The DASs are expected to be direct Peers. Message Copy cannot be supported to DASs connected through other diameter applications, 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 diameter tries to route the original Diameter Request message to Peer in a Route List and the Answer is not received, diameter 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, are sent to the DAS Peer to avoid flooding the DAS Peer due to failure recovery and rerouting on the signaling side.

Diameter Message Copy 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 Diameter Message Copy only once on the original Diameter Request messages. The Message Copy triggering is not 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 resends 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 is 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).

> **Note**
>
> 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 needs 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 specific MsgCopyAnswer AVP. Table 11-1 describes the AVP format.

Table 11-1 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 removed 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. This is shown in Table 11-2.

Table 11-2 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

Rerouting of the Copied Messages to DAS is different from rerouting of the original Request messages. A Copied Message is 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 number of 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 number of retry attempts and the Pending Answer Timer configured for the Peers limits the Total Transaction Lifetime of the Copied Message.

Diameter routing Message Copy congestion

You can manually enable or disable Diameter Message Copy on a system-wide basis.

> **Note**
>
> The discussion in this section assumes that Diameter Message Copy is enabled.

The Diameter Routing Function can automatically disable Diameter Message Copy if the DA-MP reaches a specific level of congestion. The congestion level at which Diameter Message Copy is disabled is configurable on the **Diameter**, and then **Configuration**, and then **System Options**, and then **Message Copy Options** GUI page.

If the local DA-MP enters a congestion level based on the value of the configured MP Congestion Level for Message Copy, Diameter Message Copy on that DA-MP is disabled automatically as a load-shedding mechanism. Messages that are waiting for the copy action (those that have been marked and are awaiting an original Answer from a Diameter Peer) are not copied. Messages that have already been copied to the DAS and are waiting for a response from the DAS to complete the transaction are 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); thus, their transactions are 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 the time a message is marked for copy and is actually copied, the local DA-MP's status can change. Therefore, Diameter Message Copy is 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 is raised at this time.

Diameter Message Copy is 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 is 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 Diameter Message Copy.

If Diameter Message Copy processing capacity reaches 100% congestion, further Message Copy actions cannot be completed. To process the messages, Diameter Message Copy is not

disabled; but an alarm is raised to indicate 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.

Up to 100 Message Copy Configuration Sets are supported. 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 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. Requests matching the advertised Application-ID inly 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 DASs are expected to be direct Peers. Message Copy is not supported to DASs connected through other diameter applications, relays, and proxy servers.

Message Copy Request Type
The original Request significantly altered as it traverses the routing network. Depending on the function provided by the DAS, the DAS might be interested in seeing the Request before or after the modifications made. 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 before any manipulation. The Original Egress Request is the Request as sent to the upstream Peer. The default is Original Ingress Request.

Ingress Answer Included
In some cases, DAS must query the contents of the original Answer received for the Request message in order to accomplish the function. When the Ingress Answer Included element is set to **YES**, Diameter Message Copy 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 might influence the Message Copy action. For example, a DAS might 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, Diameter Message Copy 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 diameter routing function receives an Answer from the upstream Peer. The default is to copy on 2xxx only.
The Diameter Message Copy is not performed if the Answer is generated or if the original Request times out.
Alternate routing is not attempted 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
DASs 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 copied message is transmitted again 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 transmitted again 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 copied message is transmitted again for the 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 are no retransmission attempts.

Diameter Configuration for Message Copy

The following Diameter Configuration components must be configured if Diameter Message Copy is 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 is used to trigger Message Copy.
  - Set the **Message Copy Feature** element to Enabled in **Diameter**, and then **Configuration**, and then **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 is used to trigger Message Copy for Mediation.
  - Set the **Message Copy Feature** element to Enabled in **Diameter**, and then **Configuration**, and then **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). Diameter Message Copy 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. Diameter Message Copy validates the transaction using the MCCS and copies the message to the DAS.

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. Mediation Rule Templates are described in the *Diameter Mediation User's Guide* and associated online help.

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 Diameter Message Copy to copy the message to a DAS. The Message Copy Configuration Set specifies a configured Route List for the DAS. See Message Copy Configuration Sets.

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 before being 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.

12

Diameter Capacity and Congestion Controls

The diameter routing function 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.

12.1 Introduction

> **Note**
>
> RADIUS design dictates that most of the per-connection and per-MP features apply in a similar way to both RADIUS and Diameter connections.

The diameter routing function provides the following features and functions for capacity and congestion control:

- DA-MP Overload Control
- Per-Connection Ingress MPS Control
- User Configurable Message Priority (not supported for RADIUS)
- Remote BUSY Congestion (not supported for RADIUS)
- 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:
  - 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 diameter 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 (not supported for RADIUS), Egress Transport Congestion (not supported for RADIUS), 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/RADIUS Connections or Peers, or both, across multiple DA-MPs on a Network Element.

12.2 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.

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, 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. See the MP Profiles information in *Diameter Common User's Guide*.

  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 MPs menu vary depending on the type of server used for the DA-MP.

  The following elements can be user-configured from the **Diameter Common**, and then **MPs** menu 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 polices 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 polices 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 polices 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 discards when the DA-MP is in danger of congestion.

- 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

12.3 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 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 PCIMC feature:

- Is always available in the system.
- Is applied in the diameter transport function, which is used by all diameter 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.

Per-Connection Ingress Message Coloring

In addition to enforcing ingress message rate limits on a per-connection basis, PCIMC colors ingress messages based on the reserved and average ingress message rates. message color can be used at other traffic shedding points, such as DA-MP Overload Control.

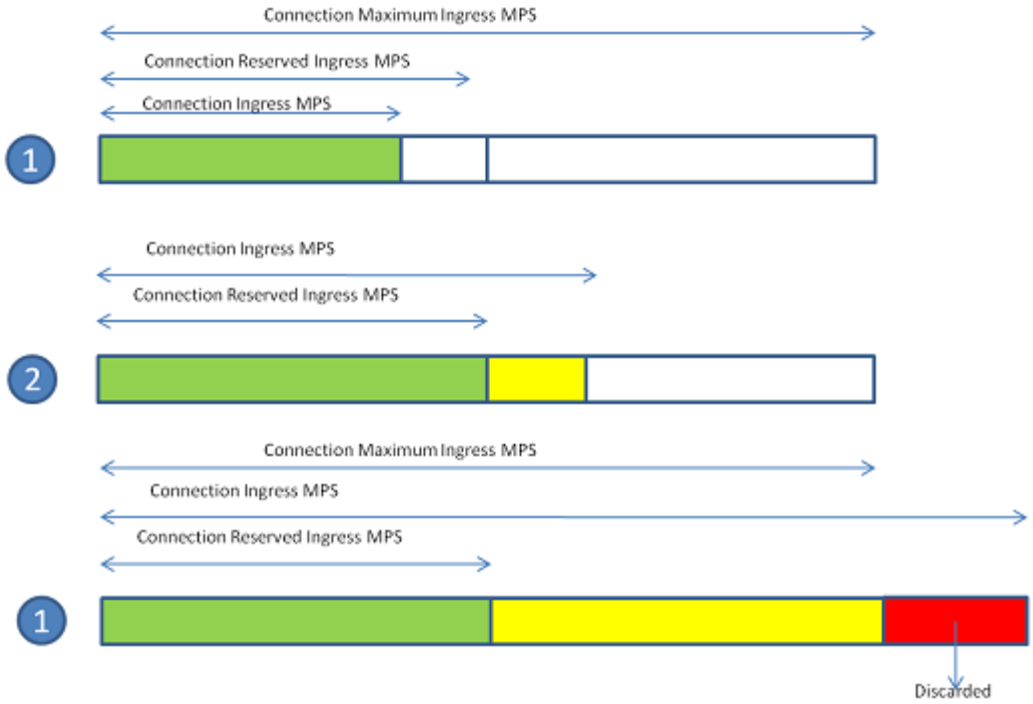
Traffic from under-utilized connections is marked green by per-connection ingress message controls, while traffic from over-utilized connections is marked yellow. Traffic discarded by PCIMC due to capacity exhaustion (per-connection or shared) is marked red and is not considered for any subsequent processing.

The following items describe the numbered items in Figure 12-1:

- 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 up to reserved ingress MPS are colored green and above that are colored green.
- When the connection's ingress MPS rate is above its configured maximum ingress MPS, the messages in excess of maximum ingress MPS are dropped, unless NGN-PS feature is enabled.
- When NGN-PS feature is enabled, then messages in excess of maximum ingress MPS are dropped, except NGN-PS messages.

> **Note**
>
> If the connection's reserved ingress MPS is 0, all the messages processed by the connection are colored yellow.

Figure 12-1 Per-Connection Message Coloring



Message Discard Policy

The Message Discard Policy function considers the priority of the message while discarding the message.

Each peer connection tracks the priority of the ingress message and discards the messages that exceed the maximum ingress MPS configured for the connection.

The request messages are discarded based on the configured resource exhausted action that is set as abandon the request with no answer or send answer. For a description of Resource Exhausted Action see Diameter Routing Option Sets.

Per MP Server Capacity Management

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 configured ingress message rate capacity limits:

- Engineered Ingress MPS is the maximum ingress message rate that a DA-MP supports 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 for the MP Profile assigned to the DA-MP.
- MP Engineered Maximum Ingress MPS is a configurable ingress MPS limit that dictates the maximum rate at which the DA-MP attempts 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 can be 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 do 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 a MP server can exceed the MP engineered ingress MPS to 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 majoralarm is triggered.
  The ingress MPS major alarm threshold must be greater than the ingress MPS minor alarm threshold.
- Ingress MPS Alarm Abatement Time defines the minimum time that a connection's ingress message rate must remain less than or equal to the respective Abatement threshold before the alarm clears or its severity reduced from major to minor.
- Convergence Time - Defines the time it takes in milliseconds to converge to a per second rate that is used to calculate the ingress MPS of the connection.

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
- Ingress MPS Alarm Abatement Time - 2000ms
- Convergence Time - 1000ms

Maintenance and Monitoring for Per-Connection Ingress MPS Control

The PCIMC 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 PCIMC feature uses the following GUI information:

- **Diameter**, and then **Configuration**, and then **Connections** specifies which capacity configuration set the connection uses.
- The **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Capacity Configuration Sets** pages provide elements for configuring capacity configuration sets.
- **Diameter**, and then **Maintenance**, and then **Connections** reports KPI 10500 for average ingress MPS for each diameter connection (ingress messages 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.

Connection Alarm

The PCIMC 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 MPS rate exceeds the configured ingress MPS minor alarm threshold value for the connection. The minor alarm is cleared when the MPS rate falls 5% below the ingress MPS minor alarm threshold value configured for the connection.

The major alarm is asserted when the 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 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 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.

12.4 Remote Congestion Controls

> **Note**
>
> Remote Busy congestion and egress transport congestion are not supported for RADIUS.

The following features provide remote congestion controls:

Remote BUSY Congestion
Addresses Remote Congestion detection
The 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-98 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 Peer Connection
User-Configurable Connection Pending Transaction Limiting (UC-CPTL) provides a configurable pending transaction limit for each 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.

Routing Based on Congestion Level

Features such as Remote BUSY Congestion, Egress Transport Congestion, and Per Connection Egress Throttling Control are used 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

Up to five Congestion Levels (CL-0, CL-1, CL-2, CL-3, and CL-98) are supported, with CL-0 indicating no congestion to CL-98 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, CL-3, and CL-98
- 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.

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, 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 12-1 summarizes this behavior.

Table 12-1 CLs, CPLs, and Message Treatment

Connection CPL Value	Message Priorities Allowed	Message Priorities Not Allowed	Comment
98	None	All	Requests nor Answers can be sent on the Connection
3	3	0, 1, 2	Allow only Answers to be sent on the Connection
2	3, 2	0, 1	Allow only Answers and Pri=2 Requests to be sent on the Connection
1	3, 2, 1	0	Allow only Answers and Pri=2,1 Requests to be sent on the Connection
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-98). Therefore, the concept of Connection Priority Level (CPL) is used 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 12-2 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, X98)

- This composite CPL value is then used by the Diameter Routing Function as shown in Table 12-1.

Table 12-2 Mapping Congestion Levels to CPL Values

Attribute	Value	CPL Value
X1: Diameter Connection Operational Status	Available	0
	Degraded	1 - 3, 98
	Unavailable	99
X2: Diameter Connection Remote BUSY Congestion	CL-0 through CL-3	0-3
X3: Diameter Connection Egress Transport Congestion	CL-0, CL-1, CL-2, CL-3, and CL-98	0, 1, 2, 3, and 98
X98: Diameter Connection Egress Message Throttling	CL-0 through CL -3	0 - 3

Capacity and Ranges

Table 12-3 specifies the capacity and ranges for Remote BUSY and Egress Message Rate.

Table 12-3 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 DA-MP
Remote BUSY processing	2000	Remote BUSY processing on up to 2000 simultaneous Diameter connections on a single DA-MP
Remote BUSY processing	1000	Remote BUSY processing on up to 16000 simultaneous Diameter connections on a single DA-MP
Egress Transport Congestion processing	1000	Egress Transport Congestion processing on up to 1000 simultaneous Diameter connections on a single DA-MP
Egress Transport Congestion processing	2000	Egress Transport Congestion processing on up to 2000 simultaneous Diameter connections on a single DA-MP
Egress Transport Congestion processing	1000	Egress Transport Congestion processing on up to 16000 simultaneous Diameter connections on a single DA-MP
Egress Message Throttling	500	Egress Message Throttling on up to 500 simultaneous Diameter connections on a single DA-MP
Egress Message Throttling	500	Egress Message Throttling on up to 500 simultaneous Diameter connections on a single DA
Egress Message Throttling	500	Egress Message Throttling on up to 500 simultaneous Diameter connections on a single DA

Table 12-3 (Cont.) Remote BUSY and EMR Capacity Ranges

Item	Maximum	Description
Egress Message Throttling Configuration Sets	50	Up to 50

12.4.1 User Configurable Message Priority

> **Note**
>
> User Configurable Message Priority is not supported for RADIUS.

User Configurable Message Priority provides the following functions to set the Priority of messages that are handled 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 that are to be marked with a Message Priority.
- A method for the Message Priority determined by the first diameter signaling router to handle a Request to be communicated to any other diameter signaling router that also handles the Request.
  Message Priority is determined based in part on the Connection on which the Request arrives at the first diameter signaling router to handle the Request. A second diameter signaling router 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 is never 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 upon entrance based on the following:

- 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 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 diameter routes, Request Message Priority might need to be assigned on one diameter signaling router and used by any and all diameter signaling routers 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-Diameter nodes.

Egress Request routing and Answer forwarding 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 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 router-to- router 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 12-4 indicates 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 12-4 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 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

12.4.2 Remote BUSY Congestion

> **Note**
>
> Remote BUSY Congestion is not supported for RADIUS.

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 Connections Peer FQDN.

The status is set to BUSY only for the Connection of a Peer on which DIAMETER TOO BUSY is received. The other Connections between the diameter signaling router and the Peer might or might 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 Peer Node, then the DIAMETER_TOO_BUSY is ignored.

Message traffic reduction is managed through the use of four 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 is 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-98 are mapped to Connection Priority Level (CPL) values 0, 1, 2, 3, 98 respectively.

Diameter Configuration for Remote BUSY Congestion

The Remote BUSY Congestion feature is configured using the following elements on the **Diameter**, and then **Configuration**, and then **Connections** page:

- Remote Busy Usage: Enabled, Disabled
- Remote Busy Abatement Timeout - time period (in seconds) that a Connection is 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.

12.4.3 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-98.

The Connection Congestion Levels CL-0, CL-1, CL-2, CL-3, and CL-98 are mapped to Connection Priority Level (CPL) values 0, 1, 2, 3, 98 respectively, as shown in Table 12-5.

Table 12-5 Mapping Congestion Levels to CPL Values

Attribute	Value	CPL Value
Diameter Connection Operational Status	Available	0
	Available Degraded	1 - 3, 98
	Unavailable	99
Diameter Connection Remote BUSY Congestion	CL-0 through CL-3	0 - 3
Diameter Connection Egress Transport Congestion	CL-0, CL-1, CL-2, CL-3, and CL-98	0, 1, 2, 3, and 98
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-98. 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 is 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-98 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-98 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 98.
- 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.
  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 remains 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 for other reasons, and is not 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 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).

12.4.4 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, signalling 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 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 12-6. 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, an EMR configured with **Convergence Time**, and an Abatement Time) provide a high degree of user control over the characteristics of transitions between Congestion Levels due to throttling.

- Up to 128 Egress Message Throttling Configuration Sets are supported.
- Up to 500 Peer Connections can have egress message throttling enabled in a single 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 and 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 depending on configuration and message priorities.
  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.

  > **Note**
  >
  > The Max EMR is not the maximum volume that can be served, but it is the volume on which the Congestion Level percentages are calculated.

- 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 is updated as indicated in Table 12-6. The offered rate is the value computed for EMRs configured with **Convergence Time**.

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 15 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 12-6 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.

- Convergence Time - The rate convergence time is the amount of time it takes for the measured rate to converge on the actual rate.
  For example, if the actual rate jumps from 0 MPS to 1000 MPS and the Rate Convergence Time is 5 seconds, then it takes that long for the measured rate to converge on the actual rate, and that long for the measured rate to be reported as follows:
  - T(0) = 0 MPS
  - T(1) = 200 MPS
  - T(2) = 400 MPS
  - T(3) = 600 MPS
  - T(4) = 800 MPS
  - T(5) = 1000 MPS

  The EMR is calculated every 100ms by subtracting the oldest traffic count from the newest traffic count, and averaging the difference over the elapsed time between them.

- Abatement Time - amount of time that a throttled Connection's adjusted 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 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**, and then **Configuration**, and then **System Options** GUI page.
  Disabling Egress Message Throttling has the same effect as un-assigning the Egress Message Throttling Configuration Set for all the Connections 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).

12.4.5 User Configurable Connection Pending Transaction Limiting

User-Configurable Connection Pending Transaction Limiting (UC-CPTL) provides a configurable pending transaction limit for each 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.

Peer Nodes have different requirements for the maximum number of pending transactions that are required. For example:

- Diameter-to-Server Connections typically carry higher traffic volumes than Diameter-to-Client Connections due to aggregation of traffic from many client Connections to few server Connections.
- A high percentage of the traffic on Diameter-to-Server Connections requires Pending Transaction Records, because Requests are the majority of the egress traffic on these Connections.
- A low percentage of the traffic on Diameter-to-Client Connections requires Pending Transaction Records, because Answers are the majority of the egress traffic on these Connections.
- Diameter-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 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 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

A configurable Pending Transactions Per Connection option is provided for each 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.

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, then any pending transactions on the Connection that are above the new limit continue to be processed and the new Pending Transactions Per Connection value are applied only for new transactions that are initiated after the change.

12.5 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 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 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-RCL) (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
  - Convergence Time 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

A maximum of 5 congestion levels (CL-0 to CL-3 and CL-98) is supported, which indicates the Congestion Level of a resource. CL0 indicates the resource has no congestion, and CL-98 indicates 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 has 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.

2. 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 is throttled. Requests with Message Priority less than Congestion Level is not 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 12-7.

Table 12-7 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
4 NGN-PS as Request Message Priority	Congestion Level 0, 1, 2, and 3

When the EMR for an Egress Throttle Group reaches the Egress Throttle Group Maximum Egress Request Rate or the Egress Throttle Group's Pending Transactions reaches the Egress Throttle Group's Maximum Egress Pending Requests, no Requests are 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 is updated as indicated in Table 12-8.

Table 12-8 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
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 Convergence Time and the Abatement Time provide a high degree of user control over the characteristics of transitions between Congestion Levels due to throttling.

- Convergence Time - The rate convergence time is the amount of time it takes for the measured rate to converge on the actual rate.
  For example, if the actual rate jumps from 0 MPS to 1000 MPS and the Rate Convergence Time is 5 seconds, it takes that long for the measured rate to converge on the actual rate, and the that long for the measured rate is reported as follows:
  - T(0) = 0 MPS
  - T(1) = 200 MPS
  - T(2) = 400 MPS
  - T(3) = 600 MPS
  - T(4) = 800 MPS
  - T(5) = 1000 MPS

  The EMR is calculated every 15ms by subtracting the difference between current traffic count and traffic count convergence time ago.
- EMR Abatement Time - Amount of time that a throttled connection's adjusted 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**, and then **Maintenance**, and then **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 is 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 is updated as indicated in Table 12-9.

Table 12-9 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

Table 12-9 (Cont.) ETG Pending Transaction Congestion Levels Based on Threshold

Onset and Abatement Thresholds	ETG Pending Transaction Congestion Level (ETG-PCL) Impact
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.

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.

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 is used for Pending Transaction Limiting calculation.

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**, and then **Configuration**, and then **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**, and then **Maintenance**, and then **Egress Throttle Groups** GUI page.

Egress Throttle Groups configuration procedures are provided in Diameter Egress Throttle Groups.

Egress Throttle Groups maintenance information and procedures are provided in Diameter Maintenance Egress Throttle Groups.

A.1 SCTP Parameter Configuration

The following table provides the parameter configuration for SCTP.

Table 10 SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
RTO.initial	Retransmit Initial Timeout (ms)	The expected average network round-trip time in milliseconds. This value is used to initialize the round trip time when an association is started, before the round trip time has been measured. It helps SCTP determine when to retransmit chunks. **Note** The parameter with the local node's connection configuration set is used by the peer initiated (responder) connection.	3000	120	10 to 5000	Same as RTO.min suggestion
RTO.min	Retransmit Minimum Timeout (ms)	The minimum amount of time to wait for an acknowledgment of a sent message. This value prevents the retransmit timeout from becoming too short in networks with very low round-trip times.	1000	120	10 to 5000	greater of (1.2 * average RTT) or (10 ms + average RTT)

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
RTO.max	Retransmit Maximum Timeout (ms)	The maximum amount of time to wait for an acknowledgment of a sent message. This value sets an upper limit on the exponential back-off algorithm used by SCTP for retransmission timing. Once this time is reached, retransmits are sent at a constant rate until an acknowledgment is received or the maximum number of attempts is reached.	60000	120	10 to 10000	**Note** Keep 3 * RMINI less than 1/6 of upper layer timeout, so t

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
						per layer timeout.
	Retransmit Maximum Timeout for INIT (ms)	The maximum amount of time to wait for an initialization to be acknowledged. This value overrides the Retransmit Maximum Timeout for initialization, limiting the initial setup time. A value of 0 means the Retransmit Maximum Timeout is used for initialization as well. **Note** The parameter with the local node's connection configuration set is used by the peer-initiated (responder) connection.		120	10 to 10000	Same as RTO.max suggestion.

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
Path.Max.Retrans	Number of Retransmits Triggering Path Failure	The number of consecutive unsuccessful retransmits that will cause a path of the SCTP association to be marked as failed. This value specifies how many retransmission attempts should be made to each destination before marking that destination as failed. It must be less than the "Number of Retransmits Triggering Association Failure" value.	5	3	1 to 10	3
Association.Max.Retrans	Number of Retransmits Triggering Association Failure	The number of consecutive retransmits that will cause an SCTP association to be marked as failed. This value specifies how many retransmission attempts should be made to all destinations for an SCTP association before it is considered failed. It should not exceed the total retransmit attempts for all destinations within the association.	10	5	1 to 20	6 (to test the behaviour of re-tx for multi-homed association)

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
Max.Init. Retransmits	Number of Retransmits Triggering Init Failure	The number of consecutive retransmits for initialization and COOKIE-ECHO chunks that will cause an SCTP connection to be marked as failed. This value specifies how many retransmission attempts should be made to the primary SCTP address before considering the connection failed. **Note** The parameter with the local node's connection configuration set is used by the peer-initiated (responder) connection.	8	8	1 to 20	8
Acknowledgement timer	SACK Delay (ms)	The number of milliseconds to wait after receiving a data chunk before sending a Selective Acknowledgment. A non-zero value allows the application to bundle data chunks with the Selective Acknowledgment in the same SCTP datagram, reducing network packet count. Setting the delay to zero disables this wait, sending Selective Acknowledgments as quickly as possible.	User Configurable not to exceed 500 ms	10	1 to 200	10ms or ½ RTO, whichever is less

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
HB.interval	SCTP Heartbeat Interval (ms)	The number of milliseconds between sending SCTP Heartbeat messages to a peer. Heartbeats are sent only if no user data has been sent during the Heartbeat Interval. Setting the interval to 0 disables heartbeats (not recommended).	30000	1000	0, 100 to 300000	1000
NA	Socket Send Buffer Size (bytes)	The socket send buffer size for outgoing SCTP messages must be at least the product of the bandwidth and round-trip delay for the association. **Note** The parameter with the local node's connection configuration is used by the peer-initiated (responder) connection.	NA	1000000	8000 to 5000000	The traffic pattern on the association must be analyzed. The send buffer size should be at least the product of the bandwidth and round-trip delay for the association.

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
NA	Socket Receive Buffer Size (bytes)	The socket receive buffer size for incoming SCTP messages must be at least the product of the bandwidth and round-trip delay for the association. **Note** The parameter with the local node's connection configuration is used by the peer-initiated (responder) connection.	NA	1000000	8000 to 5000000	The traffic pattern on the association must be analyzed. The receive buffer size should be at least the product of the bandwidth and round-trip delay for the association.
Max.Burst	Maximum Burst	Specifies the maximum number of packets that can be sent in a burst by this association.	4	4	1 to 4	4

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
NA	Max Number of Inbound Stream	Maximum number of inbound SCTP streams supported locally by the SCTP connection. **Note** The parameter with the local node's connection configuration is used by the peer-initiated (responder) connection.	NA	8	1 to 16	Align with peer configuration

Table 10 (Cont.) SCTP parameter configuration

RFC Name	DSR SCTP Parameter Name	Description	RFC Recommended Default Value	Oracle Default Value	Oracle Ranges	Oracle Suggestions
NA	Max Number of Outbound Streams	Maximum number of outbound SCTP streams supported locally by the SCTP connection. **Note** The parameter with the local Node's connection configuration is used by the peer-initiated (responder) connection.	NA	8	1 to 16	Align with peer configuration
NA	Datagram Bundling Enabled	If checked, datagram bundling is enabled for the SCTP connection.	NA	checked	checked, unchecked	Checked
NA	Maximum Segment Size	The maximum size for any outgoing SCTP data chunk. If a message is larger, SCTP fragments it into the specified size.		0	0, 64 to 1460	Set to 0 if ICMP (Internet Control Message Protocol) is not blocked in the connection's IP path. If ICMP is blocked, set the Maximum Segment Size based on the path MTU supported by the end-to-end IP transport.
	Ordered Delivery	If checked, ordered delivery of the SCTP data chunk is performed. Otherwise, unordered delivery of the SCTP data chunk is performed.		unchecked	checked, unchecked	unchecked