EAGLE® XG Diameter Signaling Router

Policy DRA User Guide

910-6820-001 Revision A

July 2013

Tekelec

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter contains a brief description of the Policy Diameter Relay Agent (Policy DRA) feature. The contents include sections about the document scope, audience, and organization; how to find related publications; and how to contact Tekelec for assistance.

Purpose of this Documentation

This documentation:

- Gives a conceptual overview of the application's purpose, architecture, and functionality
- Describes the pages and fields on the application GUI (Graphical User Interface)
- Provides procedures for using the application interface
- Explains the organization of, and how to use, the documentation

The Policy DRA Application

The Policy Diameter Routing Agent (Policy DRA pr P-DRA) is a feature of the Tekelec Diameter Signaling Router (DSR) product, which is part of the Eagle XG product line of Tekelec signaling products. P-DRA solves Diameter routing problems that are specific to the policy management domain.

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

Policy DRA provides the following capabilities:

- Distribution of Gx, Gxx, and S9 Policy binding capable sessions across available PCRFs
- Binding of subscriber keys such as IMSI, MSISDN, and IP addresses to a selected PCRF when the initial Gx, Gxx, or S9 sessions are already established to that PCRF
- Network-wide correlation of subscriber sessions such that all Policy sessions for a given subscriber are routed to the same PCRF
- Use of multiple binding keys that identify a subscriber, so that sessions with these binding keys can still be routed to the PCRF assigned to the subscriber
- Efficient routing of Diameter messages such that any Policy Client in the network can signal to any PCRF in the network, and vice-versa, without requiring full-mesh Diameter connectivity
- Hiding of PCRF topology information from specified Policy Clients

The Policy DRA GUI pages allow performing configuration and maintenance tasks, editing System Options, and viewing elements for the Policy DRA Configuration and Maintenance components.

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

Document Organization

This document is organized into the following chapters:

- *Introduction* contains general information about the DSR documentation, the organization of this document, and how to get technical assistance.

- *The Policy DRA Application* describes the topology, architecture, components, and functions of the Policy DRA application and the Policy Session Binding Repository (Policy SBR).
- *Policy DRA Deployment* describes Policy DRA and Policy SBR deployment in a DSR system.
- *Policy DRA Configuration* describes configuration of Policy DRA application components.
- *Policy DRA Maintenance* describes Policy DRA Maintenance functions, and Diameter Maintenance functions that provide maintenance and status information for Policy DRA and the Policy SBR.

Scope and Audience

This document is intended for anyone responsible for configuring and using the EAGLE XG DSR Policy DRA application and Policy Session Binding Repository. Users of this manual must have a working knowledge of telecommunications and network installations.

Documentation Admonishments

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

Table 1: Admonishments

✋	**DANGER**: (This icon and text indicate the possibility of *personal injury*.)
⚡	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
⚠	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

Related Publications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Customer Care Center

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

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

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

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

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

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

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

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays
- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

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

  - **Argentina**

    Phone:

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

    Phone:

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

    TAC Regional Support Office Hours:

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

    Phone:

    1230-020-555-5468
  - **Colombia**

    Phone:

    01-800-912-0537
  - **Dominican Republic**

    Phone:

    1-888-367-8552

    - **Mexico**

      Phone:

      001-888-367-8552
    - **Peru**

      Phone:

      0800-53-087
    - **Puerto Rico**

      Phone:

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

      Phone:

      0800-176-6497

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

  Regional Office Hours:

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

    - **Signaling**

      Phone:

      +44 1784 467 804 (within UK)
    - **Software Solutions**

      Phone:

      +33 3 89 33 54 00

- **Asia**
    - **India**

      Phone:

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

      TAC Regional Support Office Hours:

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

      Phone:

      +65 6796 2288

      TAC Regional Support Office Hours:

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

Emergency Response

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

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

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

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

Locate Product Documentation on the Customer Support Site

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

1. Log into the *Tekelec Customer Support* site.

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

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

Chapter 2

The Policy DRA Application

Topics:

The Policy Diameter Routing Agent, or Policy DRA, is a feature of the Tekelec Diameter Signaling Router (DSR) product, which is part of the Eagle XG product line of Tekelec signaling products. Policy DRA runs as a DSR Application, to solve Diameter routing problems that are specific to the Policy Management domain.

Policy Session Binding Repository servers host the Policy Session and Policy Binding databases for use by the Policy DRA application.

Policy DRA Description

With the advent of LTE and high-speed wireless networks, operators and service providers need to efficiently manage subscriber resource usage across their entire network. To accomplish network-wide resource monitoring and control requires identification of subscriber resource usage using multiple keys (such as IMSI, MSISDN, and IP addresses) in a network with large numbers of Policy Enforcement Clients and Policy rules servers (PCRFs). Subscriber requests for access to network resources must be routed to a single PCRF in the network so that Policy decisions can be made with knowledge of all the resources being used by all of that subscriber's Policy sessions.

The Policy Diameter Relay Agent, or Policy DRA, is a feature of the Tekelec Diameter Signaling Router (DSR) product, which is part of the Eagle XG product line of Tekelec signaling products. Policy DRA runs as a DSR Application that interfaces with the Diameter Routing Function, to solve Diameter routing problems that are specific to the Policy and Charging Control (PCC) management domain as defined in 3GPP specifications.

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

In addition to managing a subscriber's resource usage across the network, network providers may have a need to perform Topology Hiding of the PCRF from some Policy Clients. Topology Hiding prevents the Policy Client from obtaining knowledge of the PCRF identity (host name or IP address), or knowledge of the number or location of PCRFs deployed in the network.

Policy DRA System Architecture

A Policy DRA DSR consists of the following architectural components:

- Policy Diameter Relay Agent (Policy DRA) application

  The Policy DRA application is a DSR application and makes use of the functions of the Diameter DSR Application Infrastructure (DAI), Diameter Routing Function, and Diameter Transport Function. The DAI and Diameter functions enable the Policy DRA application to:

  - Receive Diameter messages (Requests and Answers) from Diameter Peers for processing
  - Route Diameter messages (Requests and Answers) to Diameter Peers
  - Communicate Operational Status and other maintenance information to and from the Diameter Routing Function
  - Make use of the standard congestion handling procedures
  - Make use of the standard alarms, events, KPIs, and measurements functions

  Note: The Range Based Address Resolution (RBAR) DSR Application and the Policy DRA application can run together in the same DA-MP.

  Configured Application Routing Rules are used by the Diameter Routing Function to determine whether a received Diameter message will be routed to the Policy DRA application or routed to a Diameter Peer in the network. The Application Routing Rules are a prioritized list of user-configurable routing rules based upon the Diameter message Application ID, Command-Code, Destination-Realm/Host, and Origin-Realm/Host.

Peer Route Tables (PRT) are used to instruct the Diameter Routing Function on how the egress Diameter messages will be routed to the network. Each PRT is configured with a prioritized list of Peer Routing Rules that define routing to Peers based upon the content of the Diameter messages to be routed.

- Policy Session Binding Repository (Policy SBR)

  The Policy SBR provides a distributed scalable and High Available (HA) database function to the Policy DRA application for storing and managing the policy Session data and the subscriber-PCRF Binding data. A Session in the context of the Policy DRA application refers to a Diameter session over a policy interface (Gx/Gxx, Rx, S9) that the Policy DRA processes. A Binding refers to an association between a subscriber and a PCRF that is assigned to provide policy rules to that subscriber.

  The Policy SBR runs on different servers than those running the Diameter Agent Message Processor (DA-MP) and Policy DRA application. The Policy SBR servers communicate with Policy DRA using the services of the Communication Agent (ComAgent). Policy SBR servers also communicate with other Policy SBR servers for auditing to maintain database consistency.

  The Policy SBR servers contain the databases to store the session and binding data, and will respond to requests from P-DRA to add, delete, and update those database records. The Policy SBR is described in more detail in *The Policy DRA Database*.

  A Policy SBR can host a Session database, a Binding database, or both, depending on the Policy DRA deployment.

- Policy DRA and Policy SBR interface through the Communication Agent (ComAgent)

  The Policy DRA application uses the Communication Agent (ComAgent) for communication with the Policy Session Binding Repository (Policy SBR) for managing session and binding database operations. The ComAgent provides an interface and means to enable the Policy DRA MPs and the Policy SBR MPs to communicate with each other through reliable ComAgent routing services. The ComAgent Direct Routing service and HA service are directly employed by the Policy DRA and Policy SBR servers.

  The Policy SBR communicates with a Policy DRA server (as its local Policy DRA server) and other Policy SBR servers in the Policy DRA network through the ComAgent, to create, update, remove and audit the Binding and Session database records.

Figure 1: Policy and Charging Control Network with Policy DRA illustrates an example Policy and Charging Control (PCC) network with Policy DRA DSRs deployed.

- Policy DRA DSRs are deployed in mated pairs to support site redundancy. (The figure shows 8 Policy DRA nodes in 4 mated pairs.) Policy DRA can support up to 16 Policy DRA DSRs configured in 8 mated pairs.

  Policy DRA DSRs can be deployed without a mate DSR, which limits the level of signaling redundancy in the network.
- Each Policy DRA DSR is typically deployed at a separate geographic site.
- Policy DRA DSRs can be connected in a full mesh in order to provide the most efficient routing within the core network.
- Any Policy Client in the network can exchange Diameter signaling with any PCRF in the network.

  PCRFs and Policy Clients have primary connections to their local Policy DRA DSR and secondary connections to their mate Policy DRA DSR.

- A Policy Client can reach any PCRF in the network with a maximum of 3 Diameter hops with at most one WAN traversal between Policy DRA DSRs.

  If all 3 hops are used, they are: Policy Client to Policy DRA DSR, Policy DRA DSR to another Policy DRA DSR, and Policy DRA DSR to PCRF.

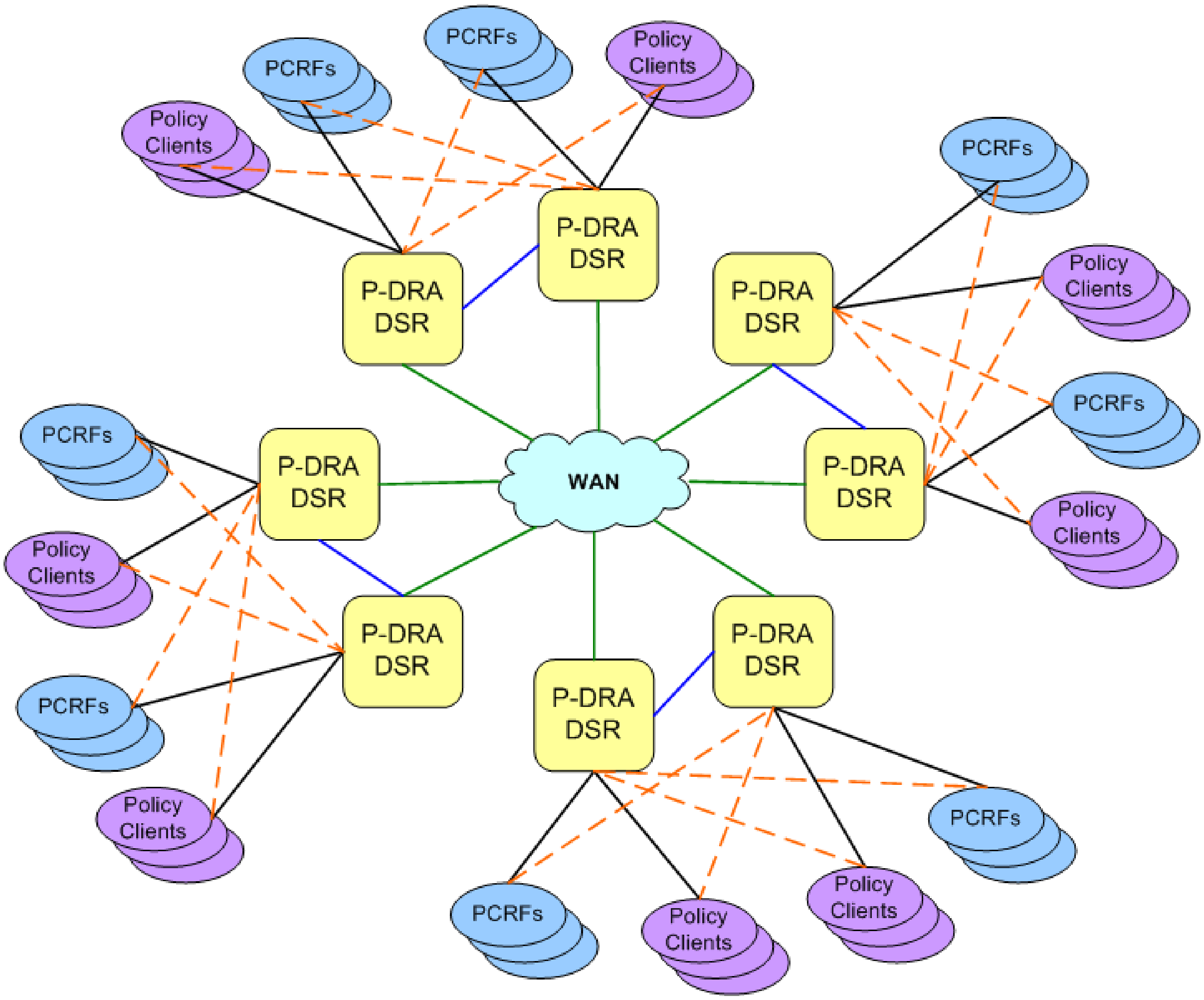


Figure 1: Policy and Charging Control Network with Policy DRA

High Level Policy DRA Description

A Policy DRA DSR consists of a number of Policy DRA DA-MPs , a number of Policy SBR servers, OAM servers, and (optionally) IP Front End (IPFE)servers.

The DSR product supports a 3-tiered DSR Topology, which is required for Policy DRA. (2-tiered DSR Topology is not supported for Policy DRA). The OAM functions are described in *3-Tiered DSR Topology*.

The Policy DRA DA-MPs are responsible for handling Diameter signaling and the Policy DRA functions. See *Policy DRA Functions*.

Policy SBR servers host the Policy Session and Policy Binding databases. These are special purpose MP blades that provide an off-board database for use by the Policy DRA application hosted on the Policy DRA DA-MPs. See *The Policy DRA Database*.

Each Policy DRA DSR hosts connections from Policy Clients and PCRFs. Policy Clients are devices (not provided by Tekelec) that request authorization for access to network resources on behalf of user equipment (such as mobile phones) from the PCRF. Policy Clients sit in the media stream and enforce Policy rules specified by the PCRF. Policy authorization requests and rules are carried in Diameter messages that are routed through Policy DRA. Policy DRA makes sure that all Policy authorization requests for a given subscriber are routed to the same PCRF.

Policy DRA DSRs can be deployed in mated pairs such that Policy session state is not lost even if an entire Policy DRA DSR fails or becomes inaccessible. When Policy DRA mated pairs are deployed, Policy Clients and PCRFs are typically cross-connected such that both Policy DRA DSRs have connections to all Policy Clients and all PCRFs at both mated sites.

The Policy DRA can be deployed for various network scenarios as a Policy routing agent, including the roaming scenarios. Policy DRAs can be located in Home Access and Visited Access networks. In addition to communicating to the Policy Clients and Policy servers using Gx/Gxx and Rx interfaces in their own network, the Policy DRAs can communicate to each other across the Visited and Home networks using the S9 interface for session binding. See deployment details in *Deployment Topology*.

Policy DRA Network is the term used to describe one or more sets of Policy DRA mated pairs that all share a common Binding database and NOAM server pair. All Policy Clients and PCRFs are reachable for Diameter signaling from any Policy DRA DSR in the Policy DRA network.

IP Front End (IPFE) provides traffic load balancing across connections in the system. IPFE is not mandatory, but is typically deployed with Policy DRA. Use of IPFE with Policy DRA is described in *IPFE*.

Policy DRA Major Functions

Policy DRA functions are described in *Policy DRA Functions*. The Policy DRA application provides the following major capabilities:

- Distribution of Gx, Gxx, and S9 Policy binding capable sessions across available PCRFs
- Binding of subscriber keys such as IMSI, MSISDN, and IP addresses to a selected PCRF when the initial Gx, Gxx, or S9 sessions are already established to that PCRF
- Network-wide session binding and correlation for all policy sessions related to a subscriber such that all policy sessions for a given subscriber are routed to the PCRF that is serving the subscriber.
- Hiding of PCRF topology information from specified Policy Clients

Policy DRA Configuration

Policy DRA configuration is described in *Policy DRA Configuration*. Making the Policy DRA application fully operational includes:

- DSR System Topology configuration, including hardware, firmware, and network elements, as described in 909-2228-001, *DSR 4.X HP C-Class Installation*
- Feature Activation for Policy DRA, and for IP Front End (IPFE) if used
- OAM configuration of MP Blade Servers and Server Groups, and Signaling Network components, Policy DRA Mated Pairs and Binding Regions, Resource Domains, Places, and Place Associations
- IPFE configuration if used
- Configuration of Diameter protocol components to support Policy DRA, including MP Profile Assignments, Peer Nodes, Route Groups, Route Lists, Peer Routing Rules, and Application Routing Rules
- Configuration of Policy DRA components on the NOAM and the SOAM, with elements for the Policy SBR database

- Post-configuration activities, including enabling the Policy DRA application and any configured Diameter Connections

3-Tiered DSR Topology

In 3-tiered DSR topology, the OAM server function is split into Network OAM (NOAM) servers and System OAM (SOAM) servers. A DSR NOAM Network Element with a pair of NOAM servers is connected to multiple DSR Signaling Network Elements in the network. Each NOAM Network Element is connected to up to 16 DSR Signaling Network Elements (configured as up to 8 mated pairs of SOAMs that interact directly with their respective DA-MPs).

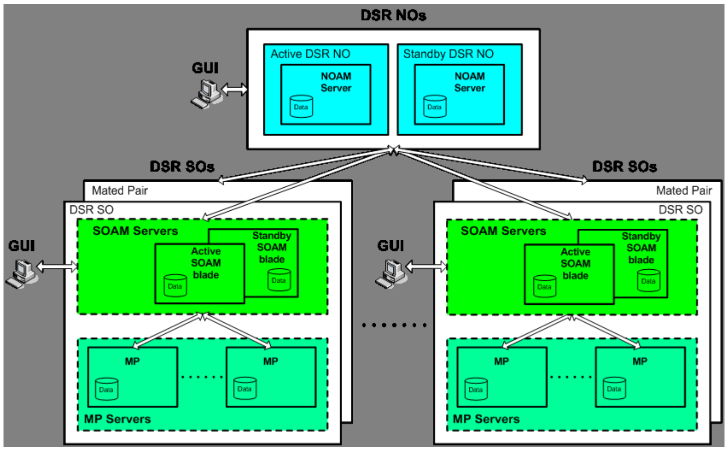


Figure 2: EAGLE XG DSR Diagram with 3-tiered Topology

The 3-tiered DSR topology does not alter existing DSR functions other than separating what can be configured or managed at what level (DSR NOAM or DSR SOAM).

The 3-tiered DSR topology architecture includes the following characteristics:

- Each DSR services signaling traffic to and from a collection of Diameter Clients, servers, and agents.
- Each DSR supports :
  - NOAM and SOAM servers in 3-tiered DSR topology, operating in active/standby mode.
  - At least two message processors (DA-MPs), operating in active/standby mode, or up to 16 DA-MPs in active/active mode.
- The DSR MPs provide the Diameter message handling function. The DSR MP supports connections to all of the DSR Peers.
- DSRs are deployed in mated pairs for purposes of geo-redundancy.

OAM Servers

The DSR Operations, Administration, and Maintenance (OAM) subsystem includes OAM servers (NOAMs and SOAMs for 3-tiered topology) and Message Processors (MPs). Each of these must be configured separately. (There is no provisioning data on OAM servers for DSR; the provisioning data used by the Full Address Based Resolution DSR Application is on the Subscriber Database Server, which has its own OAM servers.)

The 3-tiered DSR topology introduces the DSR SOAM server. The role of the DSR NOAM server takes on network scope instead of Network Element scope. The role of the DSR SOAM is managing a single DSR system (or DSR Signaling NE).

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

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

In 3-tiered DSR topology, GUI screens can be used to configure and manage:

- On a DSR NOAM, network topology data such as user accounts, network elements, servers, and server groups. Policy DRA maintenance functions and some configuration functions are available on the NOAM.
- On a DSR SOAM, Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists) and DSR Application data (for Policy DRA, RBAR, and other DSR applications)

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

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

The OAM servers provide the following services:

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

The Communication Agent

The Communication Agent (ComAgent) enables reliable communication between Policy DRA and Policy SBRs and among Policy SBRs in a scalable and high available Policy DRA network. *Figure 3: Communication between ComAgents, Policy DRA, and Policy SBR* depicts the communication paths between the Policy DRA, the Policy SBR, and their ComAgents, and the communication paths between the ComAgents.

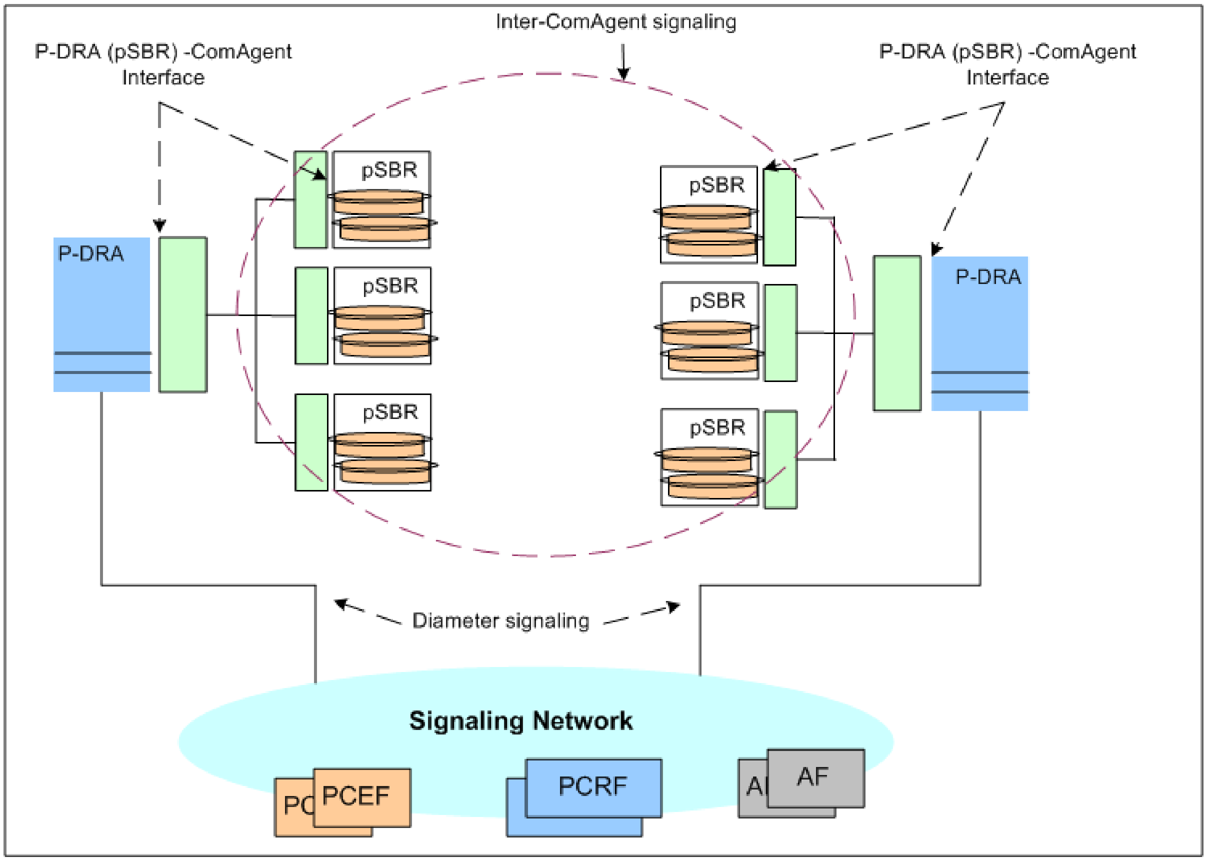


Figure 3: Communication between ComAgents, Policy DRA, and Policy SBR

The ComAgent Direct Routing service, HA service, and the MP Overload Management Framework are used by the Policy DRA and Policy SBR for communication and for Policy SBR congestion control. (See *Policy SBR Congestion* for information about the MP Overload Management Framework.)

ComAgent Direct Transfer Service

Through the ComAgent Direct Transfer Service, a DSR application can communicate directly to another DSR application. A sending application sets the destination to the IP-Address of the receiving application in a message and forwards the message to the ComAgent. The ComAgent locates a connection to a Peer ComAgent with the same IP-Address and sends the message to the Peer ComAgent, if the connection is In Service. The Peer ComAgent forwards the message to the receiving application.

The Policy DRA application and Policy SBR use the ComAgent Direct Transfer service when a Policy SBR sends Requests and responses to the Policy DRA.

ComAgent HA Service

The DSR High-Availability (HA) Framework provides the capability to allow an application to assign its various functions with identities that are called Resources. A function or Resource can be divided into pieces, each of which is called a Subresource. An application configures the HA Framework to manage its Resources and Subresources.

The HA Framework assigns states (Active, Standby, Spare, Observer, or Out-Of-Service) to each Subresource based upon the configuration and the health scores of participating DSR MPs.

- If a Resource or Subresource is Active on a given DSR MP, then the application on that MP is actively providing the function associated with the Resource or Sub-Resource.
- If a Resource or Subresource is Standby, Spare, Observer, or Out-of-Service, then the application on the MP is not actively providing the function. The application is waiting to be changed to Active if the current Active Resource or Subresource be changed from Active due to failures that reduce the other server's health score.

The Policy DRA application makes use of the Policy SBR database function by sending messages through the ComAgent to the Policy SBR that hosts the active slice of a Session or Binding Subresource. The Policy SBR does the same to other Policy SBRs in a similar manner.

The ComAgent HA Service, combined with the HA Framework, provides the Policy DRA application a means to track the placement of the Active Resources and Subresources and route messages reliably to the Active Policy SBR that may move from one Policy SBR MP to another while transactions are underway.

The ComAgent HA Service is used by Policy DRA to send messages to Active Policy SBRs for a given Resource and Subresource, and by Policy SBR to send messages to other Active Policy SBRs for a given Resource and Subresource.

When messages arrive from Policy DRA with Resource and Subresource ID, the ComAgent finds the Active Policy SBR MP for the Subresource specified in the message and uses the Resource ID and Subresource ID to route the message to the destination accordingly.

The Policy DRA Database

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

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

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

While technically both are part of the Policy DRA database, the Binding database and the Session database are referred to separately because they serve different purposes and have different scopes within the Policy DRA network.

Bindings

In the most generic sense, a Binding is a mapping between a subscriber and a PCRF assigned to handle Policy decisions for that subscriber. In 3GPP networks, however, there is more than one way to identify a subscriber.

Policy DRA supports four subscriber identifiers: IMSI, MSISDN, IPv4 IP Address, and IPv6 IP Address. Of these, IMSI and MSISDN are relatively permanent in that they do not change from call to call. IP addresses, on the other hand, are assigned by PCEFs to a subscriber's device for temporary use in accessing the Internet or other IP services.

Regardless of the type of subscriber identifier, the relationship of a subscriber to a PCRF assigned by the Policy DRA must be accessible from anywhere in the Policy DRA network. This means that the information in the Binding database must be accessible from all Policy DRA DSR sites. For example, a given IMSI, when bound, will appear in exactly one record in the Binding database, but will be accessible from any Policy DRA DSR in the Policy DRA network.

Sessions

A Session in this context represents a Diameter session for a Policy interface (Gx, Gxx, S9, or Rx). The Policy DRA application maintains session state, for the following reasons:

- Subscriber identifiers used for bindings are created and destroyed as a result of Diameter Requests sent in the context of a Diameter session. In other words, subscriber identifiers are created by binding capable session-initiating messages and removed by session-terminating messages.
- The binding of a subscriber to a PCRF must remain intact as long as the subscriber has at least one active binding capable Diameter session.
- If Topology Hiding is Enabled for a binding dependent session, the bound PCRF is stored in the session state because binding keys are not guaranteed to exist in all Requests within a Diameter session.

There are two broad categories of Policy sessions:

- **Binding capable sessions**

  A binding capable session is a Policy session that is allowed to cause a new binding to be created for a subscriber.

  Binding capable sessions are created by Gx, Gxx, or the S9 versions of Gx and Gxx Yes, the tars CCR-I messages. If a CCR-I message arrives for a Binding Capable Interface, Policy DRA checks for an existing binding for the IMSI in the message.

  - If a binding exists, the CCR-I is routed to the bound PCRF.
  - If no binding exists, a PCRF is selected and a binding is created for the subscriber IMSI.

  If additional subscriber identifiers, or Alternate Keys, are present in the CCR-I, Binding records are created for each Alternate Key present in the CCR-I. For example, a binding capable CCR-I may include a MSISDN and IPv4 and IPv6 addresses in addition to the IMSI. These Alternate Keys exist as long as the session exists.

- **Binding dependent sessions**

  A binding dependent session is a Policy session that cannot cause a binding to be created, and cannot be created unless a binding exists.

  Binding dependent sessions are created by Rx or the S9 version of Rx AAR messages. If an AAR message arrives for a `Binding Dependent Interface`, Policy DRA checks for an existing binding using a key in the AAR message.

  - If a binding is found, the AAR is routed to the bound PCRF.
  - If no binding is found, Policy DRA answers the AAR using an AAA with the error code configured for the “Binding Not Found” error condition.

  Binding dependent sessions can use Alternate Keys when locating a binding, but can neither create nor destroy Alternate Key Binding records.

  The Policy DRA generally does not need to save session state for binding dependent sessions. The exception is when the PCRF name is being topology hidden from the Policy Client. When Topology

Hiding applies, the bound PCRF name is stored in the session. Storage of the PCRF name is necessary for the following reasons:

- The Policy Client cannot learn the PCRF name from the AAA message because of the Topology Hiding.
- In-session messages (such as STR) are not guaranteed to include a subscriber identifier that could be used to look up the binding again.

The Binding Database

The Binding database consists of 4 tables: one Anchor Key table and three Alternate Key tables. Each binding table record maintains a list of one or more binding capable sessions that contain a reference to the binding key. These sessions are referred to using a Session Reference (SessionRef) instance, which is just a shorter means of identifying a session (shorter than a Diameter Session Id string).

The more permanent keys (IMSI and MSISDN) can be referenced by more than one binding capable session. These keys will not be removed until the last binding capable session that included the key is terminated.

The transient keys (IP Addresses), on the other hand, can be referenced only by a single binding capable session.

Anchor Key

Because binding capable sessions can originate from different places in the network at nearly the same time, it is necessary to serialize the Requests to prevent both from being assigned to different PCRFs. Serialization is accomplished by requiring that binding capable session origination messages (CCR-I) always contain an IMSI and that the IMSI is always used for creation of new bindings. Policy DRA supports only IMSI as the Anchor Key.

Alternate Keys

Alternate Keys provide different ways to identify a subscriber. Alternate Keys are created by binding capable sessions and used by binding dependent sessions. For example, a UE attached to a binding dependent interface like Rx may not have access to the subscriber's IMSI, but may have an IPv6 address that has been temporarily assigned to the subscriber. This IPv6 Alternate Key can be used to find the subscriber binding and the correct PCRF to route the Rx request to, only if that IPv6 Alternate Key record was previously created by a binding capable session.

Alternate Keys are optional. If all interfaces have access to the IMSI, or Anchor Key, there is no need to create or use Alternate Keys. Alternate Keys are created when they are present in the binding capable session creation message (CCR-I) and they are assigned a Policy DRA Binding Key Priority.

If a binding capable session initiation message includes multiple Alternate Keys that are also assigned with a Binding Key Priority, all of those Alternate Keys will be created when the binding capable session is established. When a binding dependent session creation message arrives, which Alternate Key will be used to find the binding depends to some degree on configuration.

Policy DRA allows the handling of Alternate Keys to be configured. The configuration defines which Alternate Keys should be used, and the Priority order in which to use them. (Assignment of Priorities must be consecutive, without skipping a number between two other numbers.)

Table 2: Example Binding Key Priority Configuration illustrates an example configuration of Alternate Keys. key types are assigned to the Priority values 1 through 4, where 1 is the highest Priority. If a

particular type of key is not used, that key need not be assigned to a Priority. In the example, IPv4 is not being used as an Alternate Key, meaning that even if a Framed-IP-Address is present in the binding capable session initiation message, no IPv4 key will be created.

Table 2: Example Binding Key Priority Configuration

Priority	Key
1	IMSI
2	IPv6
3	MSISDN
4	<Not Configured>

The Priority order defines the order in which Policy DRA looks for a given key type in a binding dependent session initiating message. In the example in *Table 2: Example Binding Key Priority Configuration*, Policy DRA will look for keys in the following order and AVP:

1. IMSI: Subscription-Id AVP with Subscription-Id-Type of END_USER_IMSI
2. IPv6 Address: Framed-IPv6-Prefix AVP (only high order 64 bits used)
3. MSISDN: Subscription-Id AVP with Subscription-Id-Type of END_USER_E164

The IMSI, as the Anchor Key, is the highest Priority key; the Priority cannot be changed. If a binding dependent session contains an IMSI, the IMSI will always be used to locate the binding, regardless of what other keys may be present in the Diameter message.

For each key found in the message and assigned a Binding Key Priority, Policy DRA will attempt to find a Binding record in the corresponding Binding database table. If a key is not present, Policy DRA will skip to the next highest Priority key type. Some keys can have more than one instance in a Diameter message, but only the first instance of a given key type will be used in the binding search.

- If no configured key is present in the Diameter message, an error response is returned to the originator.
- If keys are present in the Diameter message, but no corresponding binding is found, an error is returned to the originator.

The Session Database

The Session database consists of 2 tables: a Session table and a SessionRef table.

Session

The Session table is keyed by a Diameter Session-Id, a long string that is defined by Diameter to be “globally and eternally unique”. In addition, the Session table stores the values of any Alternate Keys defined by binding capable sessions. The relationship between Diameter sessions and Alternate Keys must be maintained so that the Alternate Keys can be removed when sessions defining those Alternate Keys are terminated.

The PCRF identifier to which a session is bound is stored in the Session record. This may be used to route in-session messages if Topology Hiding is enabled. In-session messages are not guaranteed to contain the same keys as session initiating messages.

Each Session record has a corresponding SessionRef record. The SessionRef provides a more compact means of uniquely identifying a Diameter Session-Id. This allows for a more compact Binding database. Session and SessionRef records are created and destroyed in unison.

Session Reference

SessionRef records are used to tie Binding records to Diameter sessions. This allows Policy DRA to know when a Binding record should be removed. IMSI and MSISDN records are removed when the last binding capable session that referenced them is removed. IP Address records are removed when the only binding capable session that referenced them is removed.

Because each Binding record must be associated with at least one valid Session record, a Binding record can be removed if it is not associated with any existing SessionRef. Removal of orphaned Binding records is one of the jobs of the Policy DRA database audit. See *Binding and Session Database Auditing* for more information about the database audit.

Subscriber Identification and Binding

Policy sessions can be established using multiple Diameter interfaces such as Gx, Gxx, Rx and S9. A session can be characterized as binding capable or binding dependent, depending on whether or not a binding can be created over it.

- Gx, Gxx and S9 interfaces are binding capable
- Rx and Rx over S9 interfaces are binding dependent

A session over a binding capable interface will be eligible to establish a binding to a PCRF, while a session over a binding dependent interface will rely on an existing binding to a PCRF but cannot create a new binding by itself.

In order for the Policy DRA to route all messages from a subscriber (perhaps through multiple interfaces and devices) to the same PCRF, the Policy DRA should be able to identify the subscriber by the information in the incoming Diameter Request messages. One subscriber can be associated with multiple Subscriber Ids depending on the access networks and device types used. The Subscriber Ids are also called Subscriber Keys or keys. Messages that can cause creation of a subscriber-PCRF binding are required to contain the subscriber's device IMSI, whuch can be used to uniquely identify the subscriber. IMSI is referred to as the subscriber Anchor Key in the Policy SBR Binding database.

Session initiating messages may also contain additional information to identify the subscriber. This information, which may include an MSISDN, an IPv4 address, or an IPv6 address prefix, is referred to as subscriber Alternate Keys. Database records with Alternate Keys are always established by binding capable sessions, and can be used to identify the subscriber in binding dependent sessions. For example, a Gx CCR-I message must contain the IMSI Anchor Key under normal circumstance, and may also contain an MSISDN, an IPv4 address, and an IPv6 address. After a binding is established between the subscriber and a PCRF, binding dependent sessions containing one or more of the subscriber keys can be routed to the PCRF using an Alternate Key.

In *Figure 4: Subscriber Key Usage*, a Gx CCR-I message created 3 subscriber keys: one Anchor Key and two Alternate Keys, all bound to a PCRF called PCRF5. When a binding dependent Rx session (AAR message) is created containing only IP addresses with no Anchor Key, the Policy DRA application looks up the IPv4 address of the subscriber and is able to relate it to the same PCRF because the Gx session had defined those IP addresses.

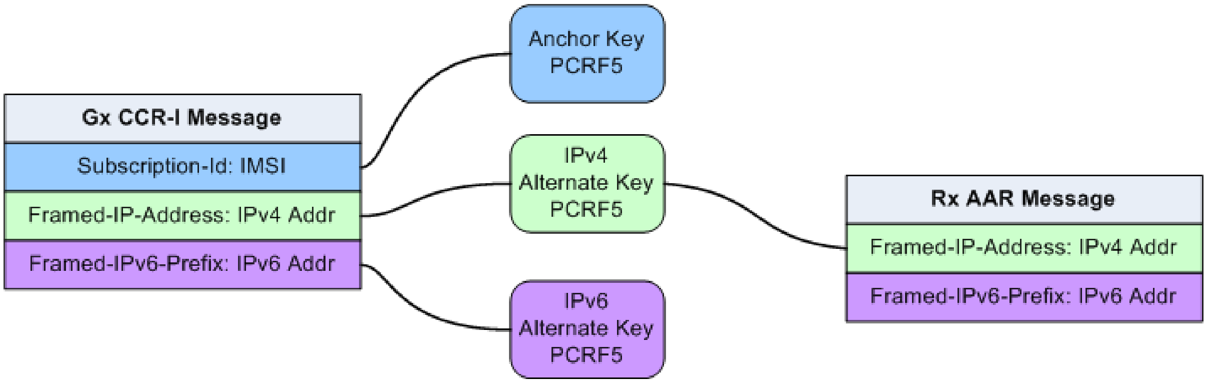

Gx CCR-I Message
Subscription-Id: IMSI
Framed-IP-Address: IPv4 Addr
Framed-IPv6-Prefix: IPv6 Addr
Anchor Key
PCRF5
IPv4
Alternate Key
PCRF5
IPv6
Alternate Key
PCRF5
Rx AAR Message
Framed-IP-Address: IPv4 Addr
Framed-IPv6-Prefix: IPv6 Addr

Figure 4: Subscriber Key Usage

Alternate Keys can be configured with a priority to improve the chances of finding the data in the Diameter message and the chances of finding the Alternate Key in the Binding database. *Table 3: Example Key Priority Configuration* illustrates an example Binding Key configuration with priorities assigned to each key. The Anchor Key is mandatory in the binding capable session creation message and is always at the top of the priority list.

Table 3: Example Key Priority Configuration

Priority	Key Type
1	IMSI
2	IPv4
3	MSISDN
4	IPv6
5	<Not configured>

The example configuration in *Table 3: Example Key Priority Configuration* will affect how the keys are searched in the Diameter message for binding dependent session initiating messages:

1. After the IMSI, the Framed-IP-Address AVP will be looked for first in the incoming Diameter Request message.
2. If the AVP is found, the Policy SBR database is searched for a binding with IPv4 address.
3. If the Framed-IP-Address AVP is not found, a Subscription-Id AVP containing an MSISDN will be looked for.
4. If the Subscription-Id AVP with an MSISDN is found, look for a binding with that MSISDN.
5. If a Subscription-Id AVP containing an MSISDN is not found, then no Alternate Keys are present in the message and no Alternate Key records will be created by the application.

Only the configured subscriber keys will be searched for. For example, an incoming Diameter message contains a MSISDN in the Subscription-ID AVP, but MSISDN is not configured in the priority configuration, the Policy DRA application will NOT look for MSISDN or use it in the Binding database.

Policy DRA Functions

The Policy DRA application performs the following major functions:

- Processing Diameter Request messages
- Querying subscriber binding status
- Selecting an available PCRF and routing the Diameter Requests to a selected PCRF
- Topology Hiding
- Processing Diameter Answer messages
- Managing subscriber Session and Binding databases

Diameter Request Message Processing

Diameter Request messages from Policy clients (PCEF, BBERF and AF) arrive at Policy DRA routed by the DSR Diameter Routing Function based on a prioritized list of Application Routing Rules. The Application Routing Rules are configured for the Policy DRA application based on the information in the Diameter Request message: Application ID, Command-Code, Destination-Realm and Host, and Origin-Realm and Host.

After receiving a Diameter Request, the Policy DRA retrieves and examines the relevant AVPs contained in the message. The AVPs relevant to the Policy DRA are those to be processed by the Policy DRA. The list of AVPs being processed by the Policy DRA is made available when the Policy DRA feature is activated. The AVPs not included in the list will not be looked at or processed by the Policy DRA. The Policy DRA-relevant AVPs vary depending on the Diameter interface on which a Diameter message is carried.

By retrieving and examining the contents of the relevant AVPs, the Policy DRA determines:

- The type of the Diameter Request: initiation, update, or termination
- The type of interface over which the Request message is carried and whether the session over this interface is binding capable or binding dependent.

  A session over a binding capable interface will be eligible to establish a binding to a PCRF, while a session over a binding dependent interface will rely on an existing binding to a PCRF but cannot create a new binding by itself.
- The subscriber's IDs from the appropriate AVPs (Subscription-ID AVP, Framed-IP-Address AVP, and Framed-IPv6-Prefix AVP)
- The Origin-Host and Realm AVPs, and Destination-Host and Realm AVPs.

The Policy DRA will use the information to query the Policy SBR database for binding and session status of the subscriber whose IDs are included in the Diameter Request message.

Emergency Session Handling

Under normal circumstance, an incoming Credit-Control Request message with Request Type as Initial (CCR-I) usually includes an AVP containing the subscriber's IMSI. However, a CCR-I might not have an IMSI included when emergency sessions occur for various reasons; for example, the subscriber's device has no SIM card in it.

The Policy DRA has capabilities to deal with these emergency sessions, by processing CCR-I messages that do not contain IMSI and any Alternate Keys. When a CCR-I arrives with no IMSI, the Policy DRA will still select a configured PCRF (see *Query Subscriber's Binding Status*) and route the Request message to that PCRF. If a CCA-I is received from the selected PCRF, Policy DRA will invoke the Policy SBR database to create a session and binding records based on any Alternate Keys included in the message. Policy DRA then forwards the CCA-I to the Policy Client that sent the CCR-I before, subject to Topology Hiding processing for that particular Policy Client.

Query Subscriber's Binding Status

After processing an incoming Diameter Request message, the Policy DRA may query the Policy SBR database for binding status based on the subscriber's IDs (keys) contained in the Request message. The query is done over the Policy DRA and Policy SBR interface through the associated ComAgents. A response to the request from the Active Policy SBR to the Policy DRA provides a result on whether or not the queried binding or session record exists in the database .

When a session initiation Request message is received over a binding capable interface (Gx, Gxx or S9), the Policy DRA will determine whether or not a binding exists for the Subscriber ID, an Anchor Key, included in the Request message. The Policy DRA queries the appropriate Policy SBR through ComAgent for the binding status for this session. Depending on the output from the interactions with the Policy SBRs, the Policy DRA may need to select an available PCRF to which the the Diameter Request message will be routed.

If the session initiation Request message is received from a binding dependent interface (such as Rx), the Policy DRA will check appropriate Policy SBRs to determine whether or not a binding record exists for this subscriber.

- If a binding record exists in the database, the PCRF bound to this subscriber can be located. The Policy DRA will use the PCRF's FQDN to route the Diameter Request message to it.
- If a binding record does not exist for this subscriber, the Policy DRA will check the Topology Hiding status for this Policy Client.
    - If Topology Hiding is NOT applicable, the Policy DRA will route the Request message based on the Destination-Host AVP, if present in the Request message, or send an Answer message with an error to the originator of the message, if the Destination-Host AVP is not present in the Request message.
    - If Topology Hiding is applicable for this message, the Policy DRA will look for a session for this subscriber.

      If such a session exists, the Policy DRA will route the Request message by using the PCRF information found in the session record.

      Otherwise, the Policy DRA will either route the Request message based on the Destination-Host AVP, if included in the AAR, or send an Answer message with an error to the originator of the message, if the Destination-Host AVP is not present in the Request message message.

PCRF Selection and Routing

PCRF selection involves distribution of subscriber bindings to PCRFs that are configured in advance. When a Diameter Request message arrives on a Gx, Gxx, or S9 interface aiming at generating a new session, the Policy DRA must determine if a binding already exists for the IMSI included in the Subscription-Id AVP of the Diameter message, and starts to select the PCRF then.

In *Figure 5: Policy DRA PCRF Selection Concepts*, four Policy DRA DSRs are located at four geographical sites. The Policy DRA DSRs at Sites 1 and 2 are configured to be mated, and the Policy DRA DSRs at Sites 3 and 4 are mated. Each site has a group of Policy clients (PCEFs in the figure) and a group of PCRFs connecting to the Policy DRA in the same site, the primary Policy DRA connection. The Policy clients and PCRFs also have a secondary connection to another Policy DRA DSR that is the mate of the local Policy DRA DSR. This relationship is illustrated by the solid blue lines shown at Site 1 and Site 2.

When PCRF selection occurs for a request arriving at Policy DRA DSR 1 at Site 1, only the PCRFs local to Policy DRA DSR 1 (PCRF 1 and PCRF 2 in *Figure 5: Policy DRA PCRF Selection Concepts*) are candidates for the new subscriber binding. If the Policy DRA at DSR1 knows that none of its local PCRFs are configured, the session initiating message is forwarded by Policy DRA to the mate Policy DRA DSR. The process of PCRF selection then occurs at the Site 2 Policy DRA DSR, with Policy DRA DSR 2 selecting from PCRF 3 and PCRF 4. If no PCRF is configured at Site 2 either, the binding attempt fails. Diameter loop prevention prohibits Policy DRA DSR 2 from routing the message to its mate because the message has already visited Policy DRA DSR 1.

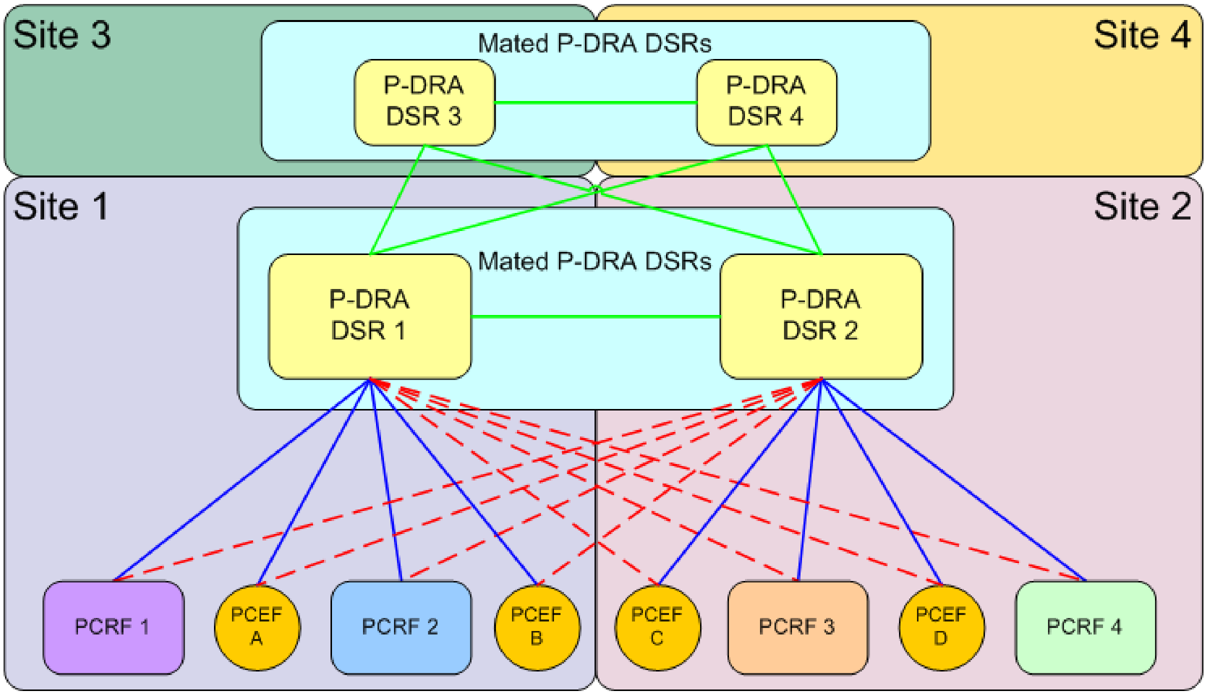


Figure 5: Policy DRA PCRF Selection Concepts

The Policy DRA application accomplishes the PCRF selection by performing a simple round-robin distribution across the configured PCRFs. After a binding is successfully established between the subscriber and the selected PCRF, all Diameter messages to that subscriber, either binding capable or binding dependent, must be routed to that specific PCRF regardless of where in the network those messages are initiated. This subscriber binding persists until the last binding capable session for that subscriber is terminated.

Topology Hiding Process

For security reasons, network operators require the Diameter Routing Agents to be able to hide the PCRF topology from selected Policy Clients. When a Policy Client is configured to have the PCRF topology hidden from it, all Diameter messages (Request or Answer) that are sent to it need to be processed by the Policy DRA for Topology Hiding. The Policy DRA will place some configured Origin-Host and Origin-Realm values into the messages instead of the PCRF's real Origin-Host and Origin-Realm values.

Topology Hiding configuration is done on each Policy DRA DSR using the Policy DRA GUI. The configuration enables users to set the Topology Hiding function to be Enabled or Disabled for the Policy DRA node. After being enabled, the Topology Hiding function can be further configured to apply for a specific Topology Hiding Scope, as summarized in *Table 4: Topology Hiding Scope Configuration*:

- The Policy Clients with specific FQDNs
- All of the Policy Clients with Foreign Realm
- All the Policy Clients with Foreign Realm and the local Policy Clients with specific FQDNs
- All Policy Clients

The Host Name used for hiding PCRF topology is also configured. If a Policy Client is configured to use Topology Hiding, the Origin Host and Realm of all messages sent to the Policy Client will be changed to the configured Host Name.

The Diameter messages to be topology hidden from certain Policy Clients can be initiated from either Policy Clients (by a CCR from a PCEF) or Policy servers (by an RAR from a PCRF), or initiated by the Policy DRA (by an RAR generated by the Policy DRA). The handling of the Diameter messages for Topology Hiding will be different depending on the specific scenarios. To determine whether or not Topology Hiding is applicable for a Policy Client:

- For messages initiated from Policy Clients, the Policy DRA will compare the Origin-Host and Origin-Realm values in the incoming messages to the configured values.
- For messages initiated from Policy servers or by the Policy DRA, the Policy DRA compares the Destination-Host and Destination-Realm values to the configured values.
- For messages initiated by the Policy DRA, the Policy DRA will compare the Destination-Host and Destination-Realm of the Policy Client with the configured values to determine whether or not the Topology Hiding is applicable to the Policy Client.

Table 4: Topology Hiding Scope Configuration

Topology Hiding System Setting	Topology Hiding Scope Setting	Result
Disabled	N/A	No Topology Hiding is performed
Enabled	Specific Hosts	Topology Hiding is performed for messages destined for the Policy Clients only if the Policy Clients' FQDNs are configured for Topology Hiding
	All Foreign Realms	Topology Hiding is performed for messages destined for the Policy Clients if the realms of the Policy Clients are different from the Realm of the PCRF that sends the messages
	All Foreign Realms + Specific Hosts	Superset of All Foreign Realms and Specific Hosts options
	All Messages	Topology Hiding is performed for all messages destined to all Policy Clients

Diameter Answer Message Processing

After the Policy DRA routes a Diameter Request message to a selected PCRF, and updates the Policy SBR on binding status, the Policy DRA could find itself in one of the following situations:

1. An Answer is received from a PCRF and a response is received from a Policy SBR
2. An Answer is received from a PCRF, but no response is received from a Policy SBR after a configured time interval
3. A response is received from a Policy SBR, but no Answer is received after a configured time interval

For situations 1 and 2, the Policy DRA always forwards the Answer messages to the corresponding Requests initiators through the Diameter Routing Function, with or without Topology Hiding processing depending on the Topology Hiding status of the Policy Client.

For situation 3, the Policy DRA generates Diameter Answer messages with proper Error Codes and routes the Answers to the Request initiators through the Diameter Routing Function, with or without Topology Hiding processing depending on the Topology Hiding status of the Policy Client.

Subscriber Session and Binding Database Management

The Policy DRA will invoke the Policy SBRs to perform relevant database operations after or in parallel with sending the Answer messages out. Which database operations to be performed depends on the Diameter interface type in the incoming Diameter Request, the Diameter Request message type (session initiation, session update, or session termination), and the results from the responses. The following operations can be performed:

- Finding, creating, or updating binding records
- Removing Suspect Binding records
- Creating or removing alternate key binding records
- Finding, creating, refreshing, or removing session records

Policy DRA Session Integrity

The Policy DRA application provides a capability called "Session Integrity" that addresses two potential problems:

1. **Session Audit Premature Removal of Sessions**

   Policy DRA uses the mechanism of the Session Audit (see *Binding and Session Database Auditing*), by which session-related resources can be freed in the event that the session is not torn down properly by Diameter signaling.

   Session state synchronization between Policy DRA and Policy Client for binding capable sessions prevents the Session Audit (see *Binding and Session Database Auditing*) from removing valid sessions that could be considered as “stale” .

   If the Policy DRA simply removed a binding capable session that it considered to be stale, any keys associated with that session would also be removed. This in turn would cause binding dependent Rx sessions that rely on those keys to fail. The Policy Client and PCRF have no idea that there is a problem with the binding capable session and therefore will not re-create it, causing the session and keys to be added back to the Policy DRA database.

   Instead of just removing a session that could be considered to be stale, Policy DRA queries the Policy Client. If the Policy Client responds indicating that the session is valid, Policy DRA waits for an interval of time before the session can be considered to be stale again. If the Policy Client responds indicating that the session is unknown, the Policy DRA will remove its session and free all resources associated with the session, including any keys that the session created.

2. **Incomplete Session Data**

In order to reduce Diameter signaling latency for policy signaling, Policy DRA attempts to relay Diameter messages before updating its various database tables. Provided that all database updates are created successfully and in a timely manner, this works very well. There are scenarios in which records cannot be successfully updated and the Policy Client and the PCRF are not aware of any problem. *Table 5: Policy DRA Error Scenarios for Session Integrity* describes specific scenarios where Policy DRA record creation failure can occur and the consequences of the failures for policy signaling.

In the case in which Policy DRA fails to create a binding record when a binding capable session is created, Policy DRA has already relayed the CCA-I message back to the PCEF (to reduce latency). The PCEF is unaware that one of the binding keys that it requested to be correlated with the subscriber's session does not exist in the Policy DRA. When a binding dependent Rx session attempts to use the failed binding key, the Rx session will fail because Policy DRA does not know which PCRF it should be routed to.

Incomplete or incorrect binding capable session data could persist for days because binding capable sessions can last as long as the UE (the subscriber's phone) is powered up and attached to the network. The PCEF that set up the binding capable session does not know that there is any problem with the correlation keys.

The solution for incomplete or incorrect data in the P-DRA is to compel the PCEF to tear down and reestablish the binding capable session in hopes that all P-DRA data updates will be created successfully on the next attempt. This is accomplished by P-DRA sending an RAR message containing a Session-Release-Cause AVP indicating that the session should be torn down.

Table 5: Policy DRA Error Scenarios for Session Integrity describes the specific scenarios in which the Policy DRA Session Integrity mechanism is required to remove a broken session. The first scenario is included to describe why Session Integrity does not apply to creation of an IMSI Anchor Key for a new binding.

Table 5: Policy DRA Error Scenarios for Session Integrity

Error Scenario	Policy DRA Behavior
Failed to create IMSI Anchor Key for new binding	Because the CCR-I has not yet been forwarded to the PCRF, this scenario can be handled by sending a failure Answer to the Policy Client in the CCA-I response. In this case, no session is ever established. The Policy Client will attempt to re-establish the binding capable session.
Failed to create binding capable session	By the time Policy DRA creates a session record, the CCA-I has already been relayed to the Policy Client. If the session record cannot be created, no Alternate Keys are created. Policy DRA must cause the Policy Client to terminate the binding capable session (and re-create it). If the session record is not created, and no Alternate Keys are created, a binding dependent session that needs to use those keys will fail.
Failed to create an alternate key	By the time Policy DRA creates an alternate key record, the CCA-I has already been relayed to the Policy Client. If the

	Alternate Key record cannot be created, Policy DRA must cause the Policy Client to terminate the binding capable session (and re-create it). If Alternate Keys are not created, a binding dependent session that needs to use those keys will fail.
Failed to update the binding after alternate routing of a new binding	By the time Policy DRA updates the binding with the new PCRF (the PCRF that actually originated the CCA-I), the CCA-I has already been relayed to the Policy Client. If the IMSI Anchor Key record cannot be updated, Policy DRA must cause the Policy Client to terminate the binding capable session (and re-create it). If the IMSI Anchor Key cannot be updated with the PCRF that sent the CCA-I, the binding will still point to the Suggested PCRF, while the original Policy Client will have a session with the answering PCRF. This could lead to a subscriber (IMSI) having sessions with 2 different PCRFs.

Note: Although Policy DRA maintains session state for binding dependent sessions when Topology Hiding applies to the Policy Client that created the session, the Policy DRA Session Integrity solution does not apply to binding dependent Rx sessions. The Rx RAR message differs from the Gx RAR message in that the Rx RAR message processing does not provide either a means to query a session or a means to cause a session to be released. If an Rx session is considered by Policy DRA to be stale, Policy DRA simply removes the session. If an Rx session is removed by Policy DRA audit or never successfully created, the next message in the Rx session will fail, causing the Policy Client to recreate the session.

Session Integrity Common Solution

The common solution for these two problems is based on the ability of Policy DRA to initiate binding capable Gx RAR Requests toward the Policy Client involved in the binding capable session. (Policy DRA does not relay an RAA received from a Policy Client to the PCRF associated with the session; the RAA is locally consumed by Policy DRA.)

Table 6: Session Integrity Conditions and Policy DRA Reaction describes the conditions that trigger the Policy DRA to send an RAR to the Policy Client. For each condition, the type of RAR is listed (Query or Release), and whether sending of the RAR is subject to throttling.

Table 6: Session Integrity Conditions and Policy DRA Reaction

Condition	RAR Type	Throttled	Comments
Session determined to be stale	Query	Y	See throttling description below.
Failed to create alternate key	Release	Y	Throttling is not needed in this case, but the error is detected on the Policy SBR server which already has the throttling mechanism for auditing and is therefore free for use.

Failed to create session record	Release	N	Quick teardown is desirable.
Failed to update binding when the answering PCRF differed from the Suggested PCRF	Release	N	Quick teardown is desirable.

When an RAR is not subject to throttling, the RAR is subject to transaction processing rules configured in the Diameter Routing Function.

When a query-type RAR is sent to ask the Policy Client if the session is valid, Policy DRA is looking for two result codes:

- An RAA response with a success result code indicates that the Policy Client still has the session. This causes Policy DRA to refresh the time the session can be idle before being considered as stale again.
- An RAA response with a result code of Unknown Session-Id indicates that the Policy Client no longer has the session. This causes the Policy DRA to remove the session and all of the session's keys.

An RAA response with any other result code is ignored.

Diameter Routing and Communication with Policy DRA

The Policy DRA, as a DSR Application, uses the DSR Application Infrastructure (DAI), which provides a mechanism for Diameter messages routing and for status updates between the Diameter Routing Function and the DAI.

Table 7: Communication between the Diameter Routing Function and the DAI describes two functions for communication between the Diameter Routing Function and the DAI.

Table 7: Communication between the Diameter Routing Function and the DAI

Function	Communication Direction	Description
Application Data	Policy DRA <-> Diameter Routing Function	Either a Request or an Answer with supporting information
Application Status	Policy DRA <->Diameter Routing Function	The Policy DRA Operational Status of Available, Degraded, or Unavailable

Request Routing

As shown in *Figure 6: Request Processing at the Diameter Routing Function and Policy DRA* , the Diameter Request messages are routed from the Diameter Routing Function to the Policy DRA based on the configured Application Routing Rule, and routed from the Policy DRA to the Diameter Routing Function, all using the Application-Data function. The Policy DRA will return the Request to the Diameter Routing Function for Peer Routing Rule processing and routing.

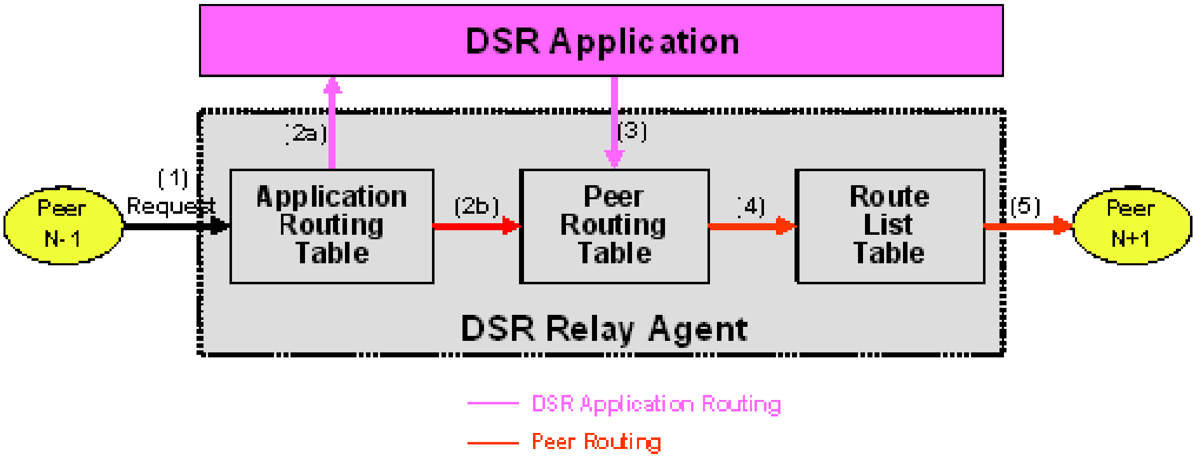


Figure 6: Request Processing at the Diameter Routing Function and Policy DRA

Answer Routing

When the Policy DRA forwards a Request message to the Diameter Routing Function for routing, it must inform the Diameter Routing Function how to process the corresponding Answer. It can inform the Diameter Routing Function either to route the Answer to the Policy DRA or to route the Answer to the downstream Peer without involving the Policy DRA. *Figure 7: Answer Processing at the Diameter Routing Function and Policy DRA* shows the case where an Answer is transmitted back to the Policy DRA. After the Policy DRA completes processing of the Answer, it will send it to the Diameter Routing Function for transmission to the Diameter Transport Function so that it can be routed to the downstream Peer.

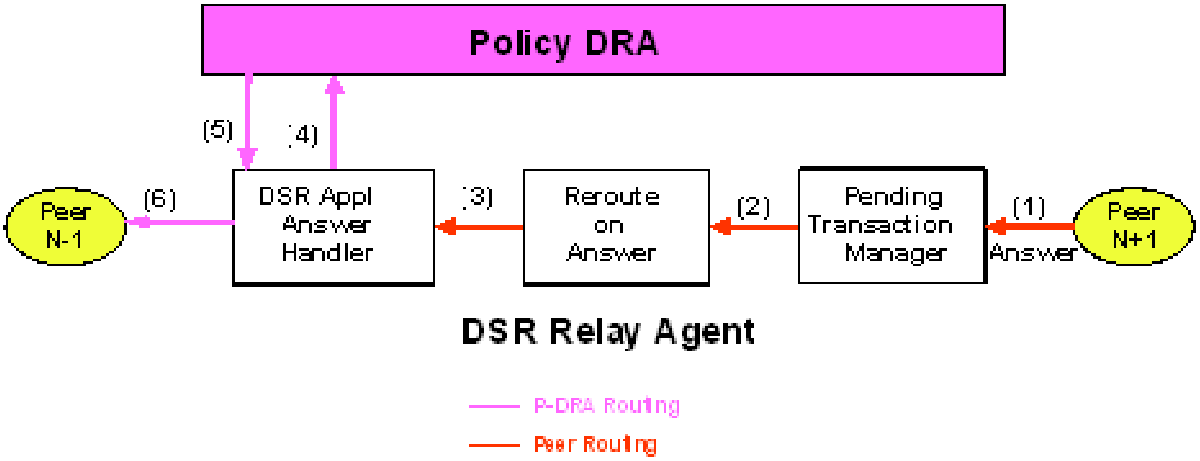


Figure 7: Answer Processing at the Diameter Routing Function and Policy DRA

Policy DRA Generated Answer

In some cases, the Policy DRA needs to generate an Answer message in response to an incoming Request. For example, the Policy DRA cannot find a PCRF to route the Request message to. *Figure 8: Policy DRA Generated Answer Routing* shows the Diameter Routing Function routing for this scenario.

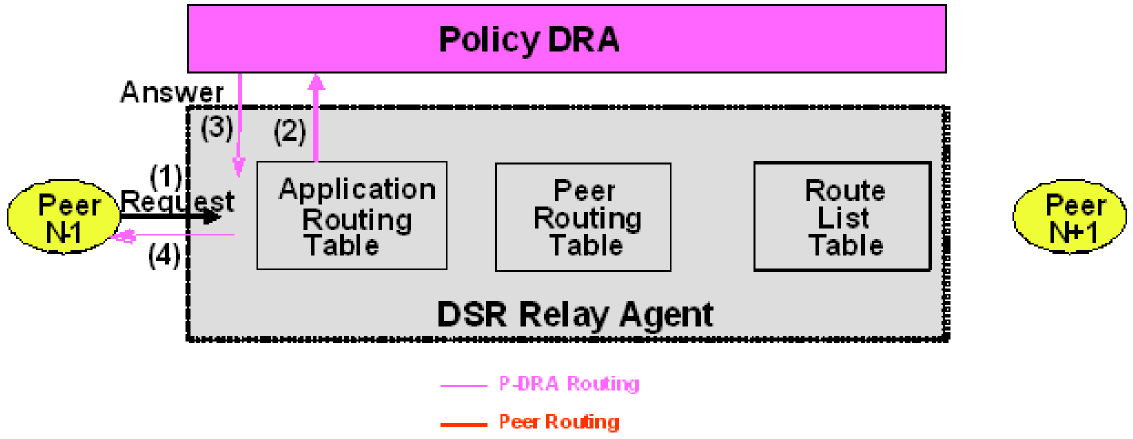


Figure 8: Policy DRA Generated Answer Routing

Policy DRA Generated Request

In some cases, the Policy DRA needs to generate Diameter Requests. *Figure 9: Policy DRA Generated Request Routing* shows the Diameter Routing Function routing for this scenario.

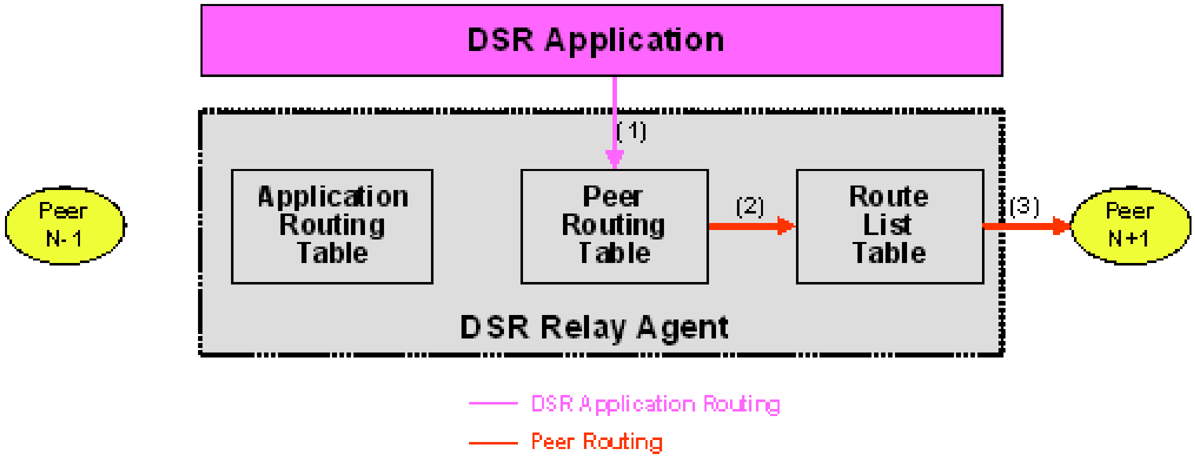


Figure 9: Policy DRA Generated Request Routing

Policy DRA Application Use Cases

The following typical Policy DRA application signaling use cases demonstrate the Policy DRA and Policy SBR capabilities to establish subscriber binding to some PCRF, and update and terminate the sessions when requested:

- **Binding and Session Creation and Session Termination over the Gx Interface** - A Policy Client requests to bind a subscriber for policy provisioning over a Gx interface. The Policy DRA creates the binding to a selected PCRF, generates the binding and session records in the Policy SBR database, updates the session as requested, and eventually terminate session as requested.
- **Subscriber Session Creation and Termination over the Rx Interface** - A Diameter Request is sent to the Policy DRA over the Rx interface for the same subscriber that has established a binding with

the PCRF over the Gx interface. The Policy DRA coordinates the sessions over the Gx and Rx interfaces and routes the Diameter messages to the same PCRF.

- **Policy DRA in Roaming Scenarios** - In addition to communicating to the Policy Clients and Policy servers through Gx/Gxx and Rx interfaces in their own networks, the Policy DRAs can communicate to each other across the Visited Access and Home Access networks through the S9 interface, for session binding purposes. See *Policy DRA in Roaming Scenarios*.

Ingress Routing

This section describes how Diameter Request and Answer messages are routed to Policy DRA.

Requests

Diameter Routing for Requests checks three conditions to determine whether to route a Request to a DSR Application:

1. Does the Request include a DSR-Application-Invoked AVP, indicating that the Request has already been processed and should not be processed again by a DSR Application?

   If this AVP is present, the Request will not be routed to any DSR Application. Otherwise, the next condition is checked.
2. Does the Request match an Application Routing Rule?

   If no rule is matched, the Request is not routed to any DSR Application. Otherwise, the next condition is checked.
3. If the Request matches an Application Routing Rule, is the DSR Application Operational Status for this DA-MP set to Available?

   If the DSR Application is not Available, then the “Unavailability action” is performed by Diameter. For Policy DRA, the Unavailability action is “Continue Routing”, which means to route the Request using PRT Peer Routing Rules.

   If the DSR Application is Available, then Diameter routes the Request to the DSR Application specified in the matching Application Routing Rule.

Ingress Requests are examined by Diameter to determine whether they should be routed to a DSR Application. The rules for deciding how to route ingress Requests are defined in Diameter Configuration Application Routing Rules. *Table 8: Policy DRA Application Routing Rule Configuration* describes the expected configuration of Application Routing Rules for Policy DRA. These rules will cause every Request that includes one of these values in the Application-Id in the Diameter Header to be routed to the Policy DRA application. Some of these rules can be omitted, depending on which interfaces are used for Policy DRA.

- The Rule Name can be any name that is chosen to identify the rule.
- The Priority is a value from 1 to 99, where 1 is the highest Priority. Rules with higher Priority will be evaluated for matching before rules with lower Priority. Rules that overlap (one rule is more specific than another) can use the Priority field to remove ambiguity about which rule should be chosen. ("Best Match" semantics is not supported for Application Routing Rules.)
- Conditions can include Destination-Realm, Destination-Host, Application-Id, Command Code, Origin-Realm, and Origin-Host. If more than one condition is specified, the conditions are logically ANDed together to determine if a rule is matched.
- The Application Name is always PDRA for the Policy DRA application. PDRA appears in the Application Name pulldown list only if the Policy DRA feature has been activated.

Table 8: Policy DRA Application Routing Rule Configuration

Rule Name	Priority	Conditions	Application Name
P-DRA Gx	1	AppId Equal 16777238 - 3GPP Gx	PDRA
P-DRA Rx	1	AppId Equal 16777236 - 3GPP Rx	PDRA
P-DRA S9	1	AppId Equal 16777267 - 3GPP S9	PDRA
P-DRA Gxx	1	AppId Equal 16777266 - 3GPP Gxx	PDRA

Answers

Diameter Answer messages can be routed to a DSR Application, or relayed by Diameter using Peer Routing Rules. *Table 9: Answer Processing by Policy DRA* lists all of the supported Answer messages and indicates which ones are processed by Policy DRA under what conditions.

If the Policy DRA application has requested to receive an Answer, but the Policy DRA application has Operational Status of Unavailable, the Diameter Routing Function will relay the Answer message directly to the remote Peer.

Note: Relaying an Answer while the Policy DRA application is Unavailable might result in exposing a PCRF name that was supposed to be topology hidden. This is because Diameter Routing does not support configuration of whether to relay or discard Answers when a DSR Application requested receipt of the Answer, but became Unavailable before the Answer was received.

Table 9: Answer Processing by Policy DRA

Answer	Requested by Policy DRA	Condition
CCA-I	Always	N/A
CCA-U	Conditional	CCA-U is processed by Policy DRA only if Policy DRA is configured to update the Session Last Touched Time on CCA-U in addition to RAA.
CCA-T	Always	N/A
RAA (Gx)	Always	N/A
AAA	Always	N/A
ASA	Never	N/A
RAA (Rx)	Always	N/A
STA	Always	N/A

Egress Routing

This section describes how Diameter Request messages are routed from Policy DRA. Diameter Request messages are routed from the Diameter Routing Function to the Policy DRA based on the configured

Application Routing Rule, and routed from the Policy DRA to the Diameter Routing Function. The Policy DRA will return the Request to the Diameter Routing Function for PRT processing and routing.

When the Policy DRA forwards a Request message to the Diameter Routing Function for routing, it must inform the Diameter Routing Function how to process the corresponding Answer. It can inform the Diameter Routing Function to either route the Answer to the Policy DRA or route the Answer to the downstream Peer without involving the Policy DRA. After the Policy DRA completes processing of the Answer, it will send it to the Diameter Routing Function for transmission to the Diameter Transport Function so that it can be routed to the downstream Peer. Egress Answer messages are always routed according to the Connection-Id and Diameter Hop-By-Hop-Id of the Request they are answering.

PCRF Selection for New Bindings

When a binding capable session initiation message (CCR-I) arrives for an IMSI that is not already bound to a PCRF, the Policy DRA application selects a PCRF from the list of adjacent PCRFs that are configured using the **Policy DRA -> Configuration -> PCRFs** GUI page This list of PCRFs generally contains only PCRFs that are local to the Site with the Policy DRA node. PCRFs that are local to the Policy DRA node's mate are generally not be included. The reason to include only local PCRFs is to avoid the extra latency associated with selection of a PCRF separated across a WAN from the Policy Client that initiated the session.

If the PCRF has different Hostnames for different 3GPP interfaces (Gx, Rx, Gxx, S9), only the binding capable Hostnames are configured in the **Policy DRA -> Configuration -> PCRFs** GUI.

Policy DRA distributes new bindings across the set of configured PCRFs. The distribution occurs independently on each DA-MP server; predicting the next PCRF that will be used is difficult on a Policy DRA node that has Policy Client connections to multiple DA-MP servers. In addition, the distribution is determined for each CCR-I received, causing the next PCRF to be updated even if the CCR-I is for a subscriber that already has a binding.

It is also possible to support more complicated PCRF selection by pushing the PCRF selection into Diameter Routing and out of the Policy DRA application. This can be accomplished by configuring a separate Peer Routing Table to be used for new binding creations using the **Policy DRA -> Configuration -> Site Options** GUI. The Peer Routing Rules can be configured to cause selection of different Route Lists. In this mode, Policy DRA can support weighted PCRF selection and different PCRF pools based on the origin of the Request.

PCRF Selection for Existing Bindings

A binding becomes finalized when a successful CCA-I is received from a PCRF for a given subscriber. At this point, all Policy sessions for that subscriber must be routed to that PCRF Peer Node, or a Peer Node that shares state with the bound Peer Node. The subscriber remains bound to this PCRF until all of the subscriber's binding capable sessions (Gx, Gxx, S9) are terminated.

The architecture for many PCRFs is such that a single Diameter host is not a single point of failure for a subscriber's Policy sessions. This is generally accomplished by designating a set of Diameter hosts that all share a common database and can therefore all access the subscriber's Policy data and Resource usage.

If the PCRF supports multiple Diameter hosts that share state, routing can be set up as follows:

- A Peer Routing Rule that matches the Destination-Host equal to the bound PCRF name
- A Route List that has a Primary and a Secondary Route Group
  - The Primary Route Group routes only to the bound PCRF

- The Secondary Route Group distributes across all PCRF Peers that share state with the bound PCRF.

Some PCRFs also have different Diameter hosts for different 3GPP interfaces. For example, they may have a hostname for Gx and a different hostname for Rx. This can be accommodated by creating two Peer Routing Rules as follows:

- A Peer Routing Rule that matches the Destination-Host equal to the bound PCRF name and Application-Id equal to Gx (16777238).
- A Peer Routing Rule that matches the Destination-Host equal to the bound PCRF name and Application-Id equal to Rx (16777236).

Routing In-Session Messages Without Topology Hiding

When the PCRF name is not topology hidden, the Policy Client is expected to learn the PCRF name from the Origin-Host and Origin-Realm of the Answer to the session initiation Request (CCA-I or AAA). This PCRF name is used as the Destination-Host and Destination-Realm of all subsequent in-session Requests originated by the Policy Client.

Policy Clients that are proxy-compatible (can learn the PCRF name) allow Policy DRA to host-route in-session Requests without the need for any Binding or Session database lookup. This behavior is desirable because it reduces the number of Policy SBR servers needed to support a given Diameter traffic load.

There are, however, Policy Clients that are not proxy-compatible. Many of these always omit the Destination-Host AVP from Requests, or include the Destination-Host AVP with the Policy DRA Diameter hostname. In order to support such Policy Clients, Policy DRA must be configured to add or replace the Destination-Host and Destination-Realm of all Requests with the PCRF that the subscriber is bound to. Policy Clients that are not proxy-compatible can also be accommodated by enabling Topology Hiding.

Routing In-Session Message with Topology Hiding

When topology hiding is enabled, the PCRF name is hidden from the applicable Policy Client. Refer to Policy DRA online help for Topology Hiding Scope options. If the PCRF name is hidden from the Policy Client, the Policy Client cannot use the PCRF as the Destination-Host and Destination-Realm in its in-session Requests. When Topology Hiding is in force for a Policy Client, Policy DRA must route in-session Requests to the bound PCRF by performing a Session record lookup and using the PCRF information stored in the Session record.

Use of topology hiding requires increased stack event processing and increased latency to look up the bound PCRF in the Session record. For these reasons, Topology Hiding should have the narrowest possible Scope. For example, if topology should be hidden from only a few Policy Clients, choose the per-Policy Client Topology Hiding Scope instead of choosing to hide topology from all Policy Clients.

Topology Hiding can also be used to “work around” a Policy Client that does not have the ability to learn the PCRF name (that is not proxy-compatible).

Naming Conventions and Hierarchical Routing

When Policy DRA is deployed in large networks with multiple Policy DRA mated pairs, the Diameter Routing configuration can be greatly simplified by employing some simple naming conventions. For example, naming all Policy Clients and PCRFs local to a particular Policy DRA node such that they start with a common prefix allows Peer Routing Rules like “Destination-Host Starts-With xxx”, where xxx is the Site prefix for that Policy DRA node. The “Starts-With” rule will point to a Route List that routes to the Policy DRA node where the equipment is located. Then if a new Policy Client or PCRF is added at a given Policy DRA node, routing changes are needed only at that node and that node’s mate, which have Peer Node entries and Diameter connections (that is, are adjacent) to the new Policy Client or PCRF. Policy DRA nodes that are non-adjacent do not require any routing updates.

Policy DRA Assumptions and Limitations

Policy DRA has the following assumptions and limitations:

Assumptions

- The Anchor Key that identifies all subscribers in the Policy DRA network is the IMSI.
- All Gx and Gxx session initiating Diameter messages will always include the IMSI. The only exception is emergency calls from devices with no SIM card (UICC-less).
- Messages sharing a common Diameter Session-Id will never arrive out of sequence.
- PCRF names and Policy Client names start with characters that can be used to identify which Policy DRA DSR hosts the primary connection to that equipment. This greatly simplifies routing configuration for the Policy DRA network. The network can be configured to work without such a naming convention, but routing setup and maintenance will be unnecessarily complex.

Limitations

- When a PCRF is selected for a new subscriber binding, a simple round-robin selection mechanism is employed. Policy DRA PCRF selection can be overridden by DSR routing configuration. When PCRF selection is overridden by DSR, weighted load distribution can also be used.
- Quota pooling is not supported. Quota pooling is a feature that would allow a number of subscribers to share a common pool of resources for Policy decisions. For example, a family plan where all members of the family share access to resources such as bandwidth. Policy DRA has no mechanism for identifying members of a quota pool such that their sessions could all be routed to the same PCRF.
- Policy data Binding records are guaranteed to survive only a single site failure.
- Policy DRA does not support the 3GPP mechanism to redirect Policy Clients to a PCRF.
- Policy DRA does not support growth of Policy SBR resources. A Policy DRA system can be configured at activation time to be as small as 3 servers, or as large as 8 Policy DRA mated pairs of 3 enclosures each, but once the number of Policy SBR(B) Server Groups per network and the number of Policy SBR(S) Server Groups per mated pair is chosen at feature activation time, neither growth nor de-growth is supported without first deactivating the feature. Feature deactivation requires a total network-wide outage for Policy DRA. (Additional mated pairs can, however, be added to grow the Policy DRA network provided that the new mated pairs have the same number of session Policy SBR Server Groups as the existing mated pairs.)
- Policy DRA supports only two of the Diameter Subscription-Id types: END_USER_IMSI (for IMSI) and END_USER_E164 (for MSISDN). Any other Subscription-Id type is ignored.
- Policy DRA evenly distributes new sessions across the Policy Session Policy SBR Server Groups at the mated pair, regardless of the physical location of the Active server. This results in ~50% of session accesses traversing the WAN between the mated pair sites.

Chapter 3

Policy DRA Deployment

Topics:

Policy DRA can be deployed in customer networks to solve Policy Diameter signaling routing issues.

A Policy DRA DSR consists of a number of Policy DRA DA-MPs, a number of Policy SBRs, OAM servers, and IPFE servers.

High Level Deployment Description

A Policy DRA DSR consists of a number of Policy DRA DA-MPs, a number of Policy SBRs, OAM servers, and optional IPFE servers.

The Policy DRA DA-MPs are responsible for handling Diameter signaling the Policy DRA application.

Policy SBRs are special purpose MP blades that provide an off-board database for use by the Policy DRA eature hosted on the Policy DRA DA-MPs. Policy SBRs host the Policy session and Policy Binding databases.

Each Policy DRA DSR hosts connections from Policy Clients and PCRFs. Policy Clients are devices (not provided by Tekelec) that request authorization for access to network resources on behalf of user equipment (such as mobile phones) from the PCRF. Policy Clients sit in the media stream and enforce Policy rules specified by the PCRF. Policy authorization requests and rules are carried in Diameter messages that are routed through Policy DRA. Policy DRA makes sure that all Policy authorization requests for a given subscriber are routed to the same PCRF.

Policy DRA DSRs can be deployed in mated pairs such that Policy session state is not lost even if an entire Policy DRA DSR fails or becomes inaccessible. When Policy DRA mated pairs are deployed, Policy Clients and PCRFs are typically cross-connected such that both Policy DRA DSRs have connections to all Policy Clients and all PCRFs at both mated sites.

“Policy DRA network” is the term used to describe a set of Policy DRA mated pairs and NOAM server pair. All Policy Clients and PCRFs are reachable for Diameter signaling from any Policy DRA DSR in the Policy DRA network.

Deployment Topology

This section describes the makeup of a Policy DRA network, regardless of its size. *Figure 10: Sites, Mated Pairs, and Region* illustrates an example Policy DRA network.

- A Policy DRA Network can have up to 8 mated pairs or 16 sites, or can be as small as a single site.
- The Policy DRA Binding Region provides the scope of the Policy Binding database. There is one instance of the Binding database in the entire Policy DRA network. Binding records are accessible from every Policy DRA DSR in the Region.

  The Binding database need not be confined to a single mated pair, but can be deployed across multiple Policy DRA DSRs. All Policy Binding Server Groups must be deployed before the Policy DRA network can be used.
- Mated Pair provides the scope for an instance of the Policy Session database.

  There is one instance of the Session database per Policy DRA Mated Pair. Session records are accessible from each Policy DRA DSR in the Mated Pair.
- Policy Clients and PCRFs have primary connections to their local Policy DRA and secondary connections to the mate of their local Policy DRA.
- Policy DRA DSRs are connected to each other on the External Signaling Network. Each Policy DRA Site must be reachable from every other Policy DRA Site in the Region for Diameter signaling.

- The External Signaling Network handles Stack Events, database replication, and Diameter signaling. All three are required for the Diameter signaling to function correctly and with the required level of redundancy. "Services" (configured using the **Configuration->Services** GUI page) can be used to enforce separation of different types of traffic.

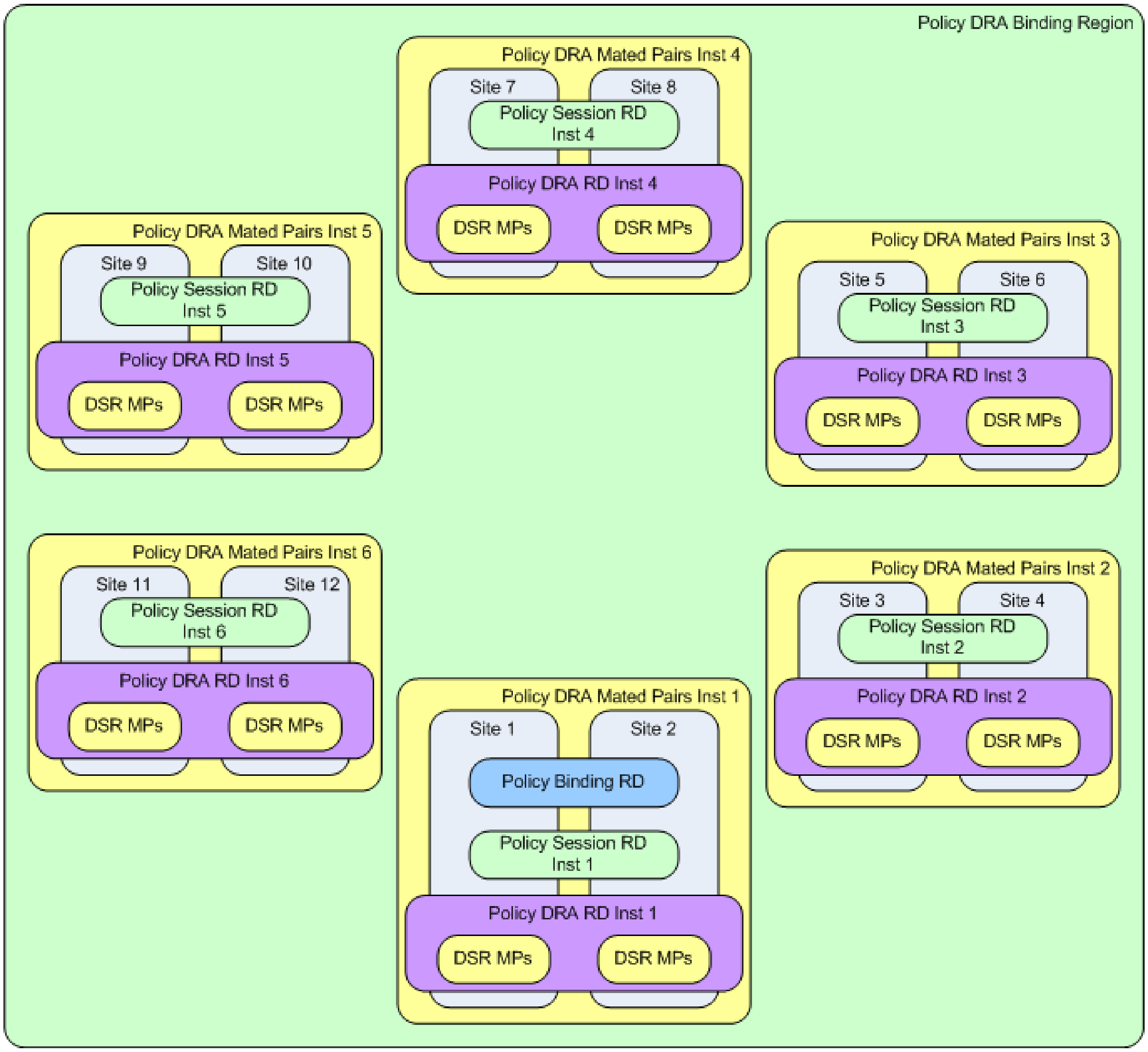


Figure 10: Sites, Mated Pairs, and Region

See *Policy DRA Scalability* for details on how the Policy DRA feature can scale from very small lab and trial systems to large multi-site deployments.

If the deployment includes more than one mated pair, all mated pairs that host the Binding database must be deployed before the Policy DRA network can be functional. Subsequent mated pairs can be deployed as needed, but will host only instances of the Session database.

Policy DRA in Roaming Scenarios

3GPP has defined two roaming scenarios with respect to Policy Control and Charging functions. The Policy DRA can be deployed for various network scenarios as a Policy routing agent, including the roaming scenarios.

In addition to communicating to the Policy Clients and Policy servers through Gx/Gxx and Rx interfaces in their own networks, the Policy DRAs can communicate to each other across the Visited Access and Home Access (or Home Routed Access) networks through the S9 interface, for session binding purposes.

Figure 11: Policy DRA in Roaming Scenarios illustrates an example Diameter network where the Policy DRAs are located in Home Access and Visited Access networks.

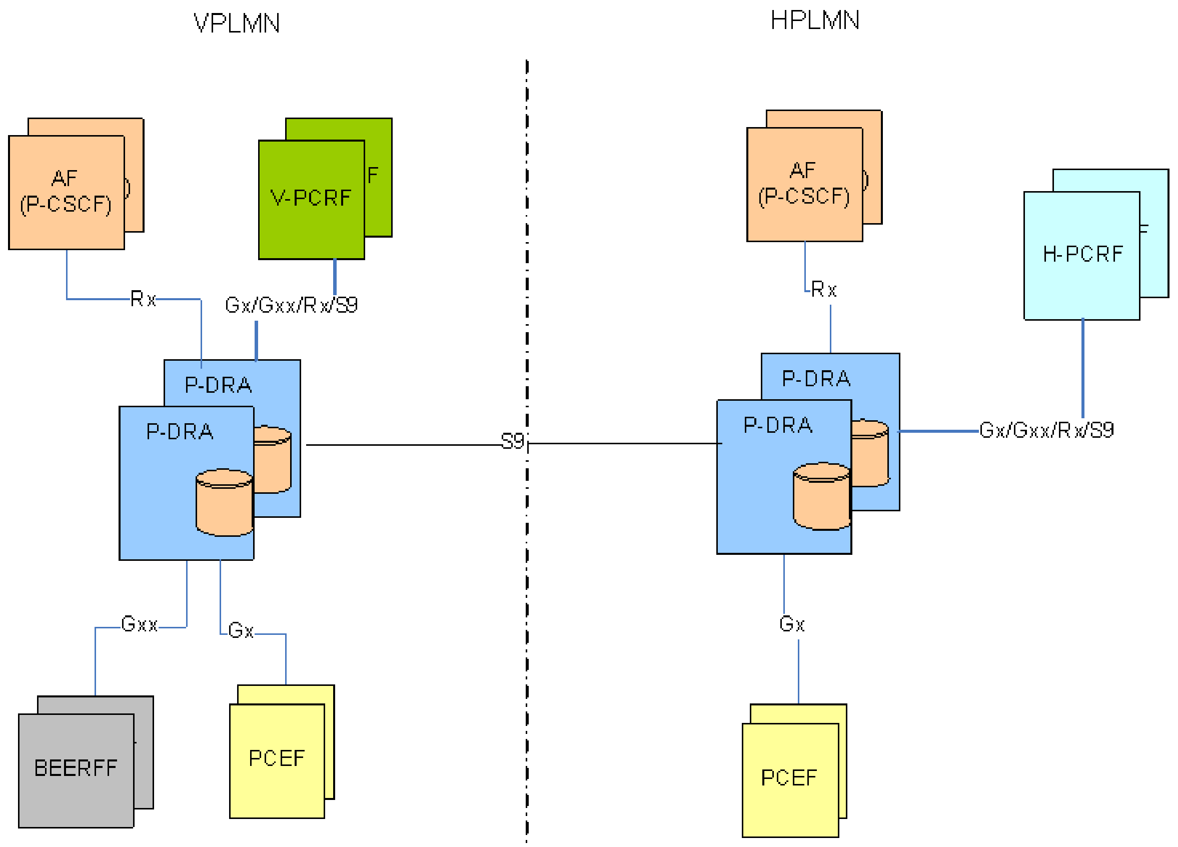


Figure 11: Policy DRA in Roaming Scenarios

The Visited Access (also known as Local Breakout) is one of the scenarios where UEs obtain access to the packet data network from the VPLMN where the PCEF is located.

The Home Routed Access is the roaming scenario in which the UEs obtain access to the Packet Data Network from the HPLMN where the PCEF is located.

The S9 reference point is defined in roaming scenarios between HPLMN and VPLMN over which two Diameter applications, S9 and Rx are used. The purpose of the S9 Diameter application is to install PCC or QoC rules from the HPLMN to the VPLMN and transport the events occurred in the VPLMN to the HPLMN.

The S9 protocol makes use of exactly the same commands and messages as the Gx/Gxx protocols, except that a V-PCRF in VPLMN will provide an emergency treatment for any incoming CC-Request (INITIAL_REQUEST) messages. This implies that the Policy DRA does not check the existence of the Called-Station-ID AVP if the IMSI is missing in a CC-Request (INITIAL_REQUEST) over the S9 interface.

Policy DRA Configurable Components

Figure 12: Policy DRA Component Relationships illustrates the relationships between the following key Policy DRA configurable components:

- Policy DRA Binding Region - consisting of all Policy DRA Sites
- Policy DRA Mated Pairs - consisting of pairs of Policy DRA Sites
- Policy DRA Sites
- Policy Session Resource Domains – one per Policy DRA Mated Site consisting of all Session Policy SBR Server Groups at the mated pair
- Policy Binding Resource Domain – one per Policy DRA Binding Region consisting of all Binding Policy SBR Server Groups
- Policy DRA Resource Domains – one per Policy DRA Mated Site consisting of all DSR (multi-active cluster) Server Groups at the mated pair.
- Policy SBR Server Groups – enough to handle the load in Stack Events per second
- Diameter Signaling Router (multi-active cluster) Server Groups – one per Policy DRA Site

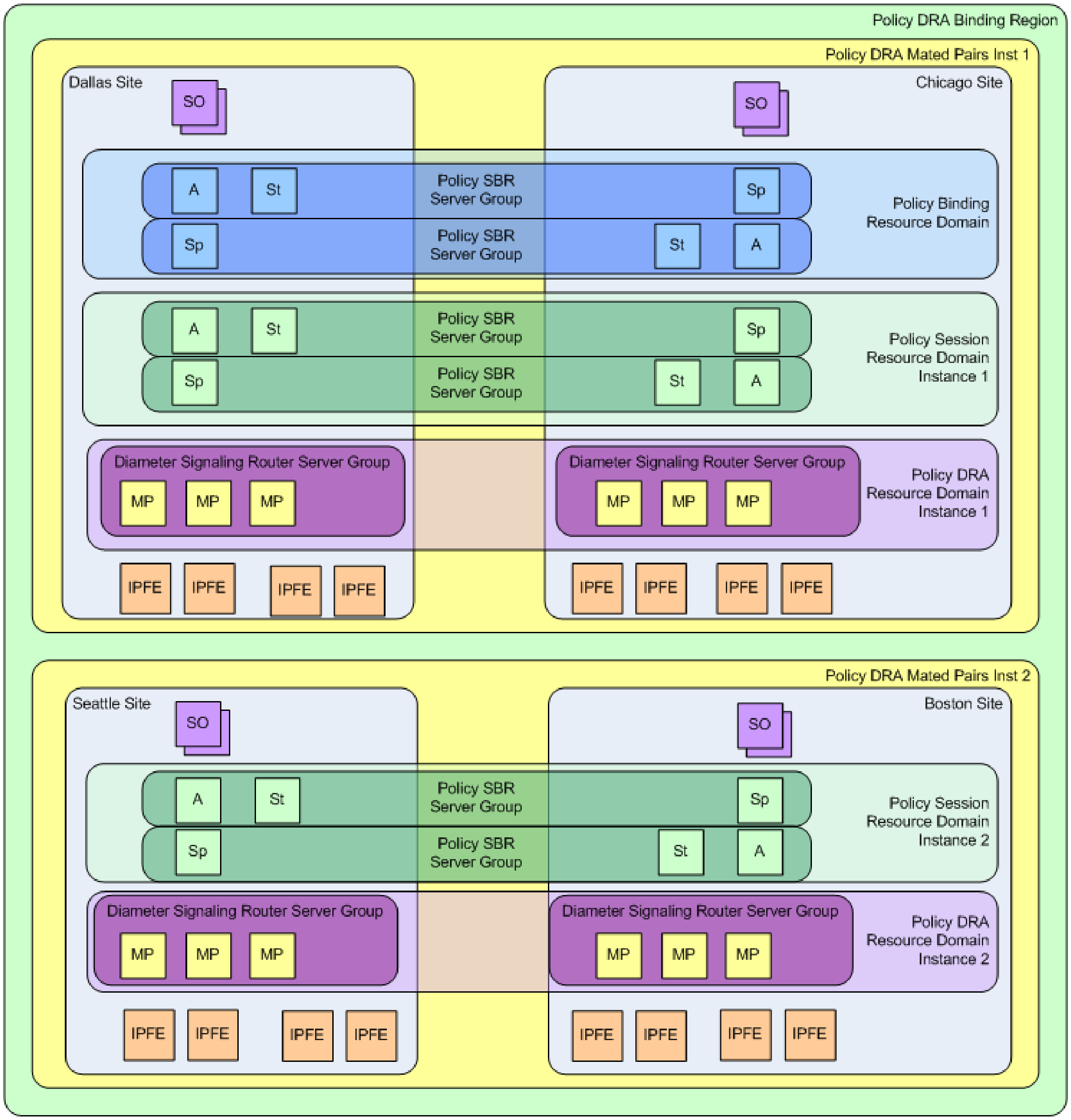

Policy DRA Binding Region
Policy DRA Mated Pairs Inst 1
Dallas Site
Chicago Site
SO
SO
A
St
Sp
Policy SBR Server Group
Sp
St
A
Policy SBR Server Group
Policy Binding Resource Domain
A
St
Sp
Policy SBR Server Group
Sp
St
A
Policy SBR Server Group
Policy Session Resource Domain Instance 1
Diameter Signaling Router Server Group
MP
MP
MP
Diameter Signaling Router Server Group
MP
MP
MP
Policy DRA Resource Domain Instance 1
IPFE
IPFE
IPFE
IPFE
IPFE
IPFE
IPFE
IPFE
Policy DRA Mated Pairs Inst 2
Seattle Site
Boston Site
SO
SO
A
St
Sp
Policy SBR Server Group
Sp
St
A
Policy SBR Server Group
Policy Session Resource Domain Instance 2
Diameter Signaling Router Server Group
MP
MP
MP
Diameter Signaling Router Server Group
MP
MP
MP
Policy DRA Resource Domain Instance 2
IPFE
IPFE
IPFE
IPFE
IPFE
IPFE
IPFE
IPFE

Figure 12: Policy DRA Component Relationships

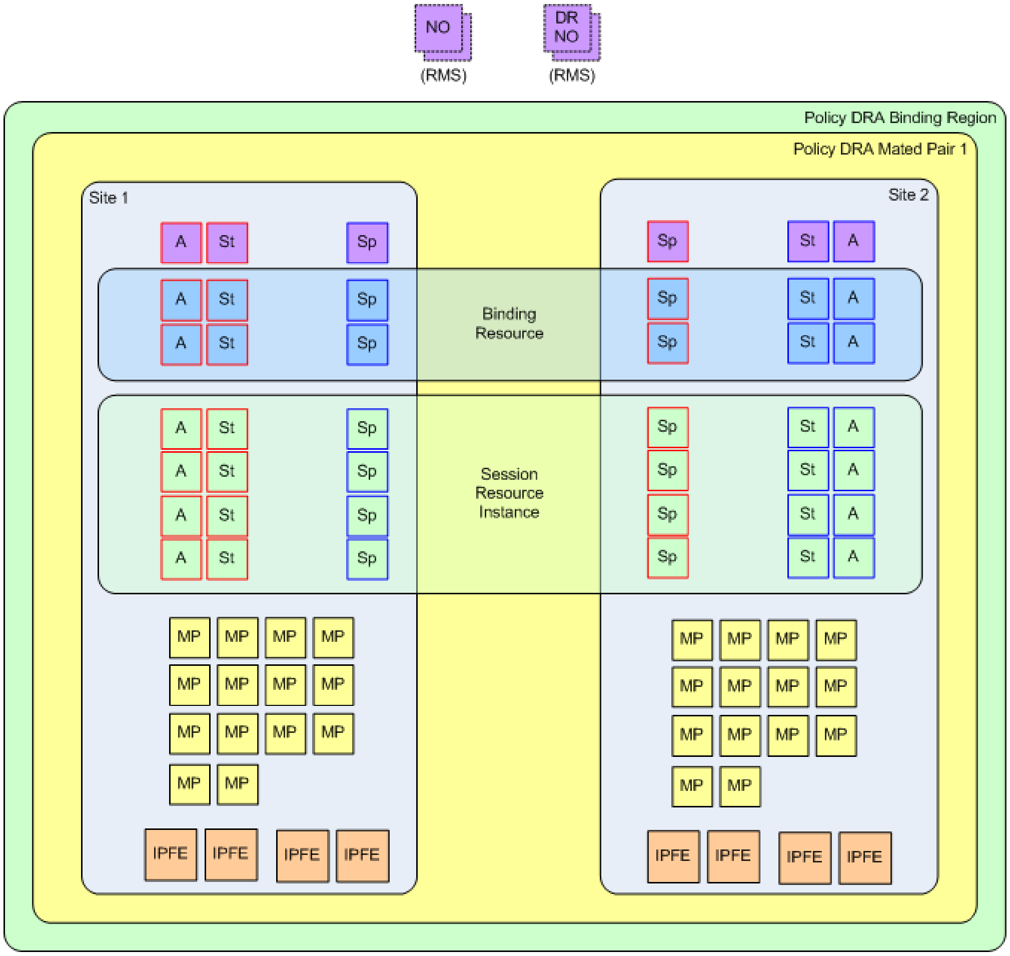
For multiple mated pair deployments, there are two different configurations for mated pairs:

- One mated pair that hosts the Policy Binding database and an instance of the Policy Session database
- N mated pairs that each host only an instance of the Policy Session database

Figure 13: Example Policy DRA Mated Pair - Hosting Binding Policy SBRs illustrates two Policy DRA DSR Sites configured as a Mated Pair that is hosting the Binding database:

- This Mated Pair hosts the Policy Binding database and an instance of the Policy Session database.
- The Policy Binding database is represented by a Policy Binding Resource Domain consisting of a number of Policy SBR Server Groups.

- The Policy Session database instance is represented by a Policy Session Resource Domain consisting of a number of Policy SBR Server Groups.
- Each Policy SBR Server Group consists of 3 servers using the Active/Standby/Spare redundancy model, allowing for Site redundancy.
- The number of Policy SBR Server Groups necessary to host the binding or Session database will be determined by Tekelec prior to feature activation based on expected Policy signaling needs.
- Each Site has an SOAM Server Group consisting of 3 servers using the Active/Standby/Spare redundancy model, allowing for Site redundancy.
- The Policy DRA network has an NOAM Server Group consisting of 2 servers using the Active/Standby redundancy model. If NOAM site redundancy is desired, another pair of Disaster Recovery NOAM servers can be deployed at a different Site.
- Each Site has a number of DA-MP servers sufficient to carry the desired Diameter signaling load.
- Each Site has two pairs of IPFE blades – one for use by Policy Clients and one for use by PCRFs. (IPFE is not required.)

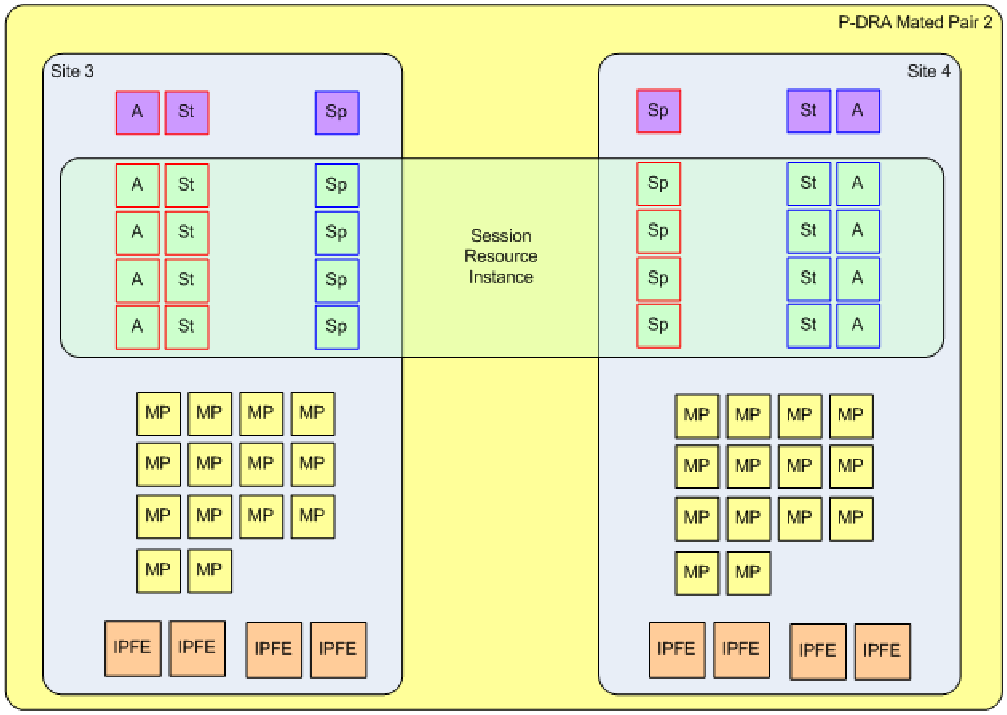


There is 1 Type 1 P-DRA Mated Pair per P-DRA Network
SOAM SGs are Act/Sby/Sp
Policy SBR SGs are Act/Sby/Sp
DSR SGs are N:K Act – 1 SG per Site
IPFE SGs are Act – 1 SG per IPFE server

Figure 13: Example Policy DRA Mated Pair - Hosting Binding Policy SBRs

Figure 14: Example Policy DRA Mated Pair - Not Hosting Binding Policy SBRs illustrates a possible configuration for additional mated pairs that do not host the Binding database:

- Each subsequent mated pair deployed after the set of mated pairs hosting the Binding database will host only an instance of the Session database (no Binding database).
- The number of DA-MPs can vary depending on the expected Diameter signaling load.



There are 5 Type 2 P-DRA Mated Pairs per P-DRA Network
SOAM SGs are Act/Sby/Sp
Policy SBR SGs are Act/Sby/Sp
DSR SGs are N:K Act – 1 SG per Site
IPFE SGs are Act – 1 SG per IPFE server

Figure 14: Example Policy DRA Mated Pair - Not Hosting Binding Policy SBRs

Figure 15: Policy Client, PCRF, and Site Relationships illustrates example relationships between Policy DRA DSR Sites and Policy Clients and PCRFs:

- Each Policy DRA DSR Site has a set of Policy Clients whose primary connection is directed to that Policy DRA.
- Each Policy DRA DSR Site has a set of PCRFs to which it distributes new bindings. Each PCRF at this Site has a primary connection to the Policy DRA DSR at that Site.
- Each Policy Client should have a secondary connection to the mate of the Policy DRA DSR for which it has a primary connection. (Without this “cross-connect”, Policy DRA site failure would leave the Policy Client with no access to any PCRF.)

- Each PCRF should have a secondary connection to the mate of the Policy DRA DSR for which it has a primary connection. (Without this "cross-connect", Policy DRA site failure would leave the PCRF inaccessible.)
- Each Mated Pair of Policy DRA DSRs shares an instance of the Policy Session database.
- All Policy DRA DSRs share the Policy Binding database, conceptually in the middle of the network.
- If Diameter signaling must be sent to a PCRF for which the Policy DRA DSR has no connection, the message must be routed to a Policy DRA DSR that does have a connection. This routing is configured using the DSR routing tables.

  See *Diameter Routing and Communication with Policy DRA* for more details about Diameter routing for Policy DRA .

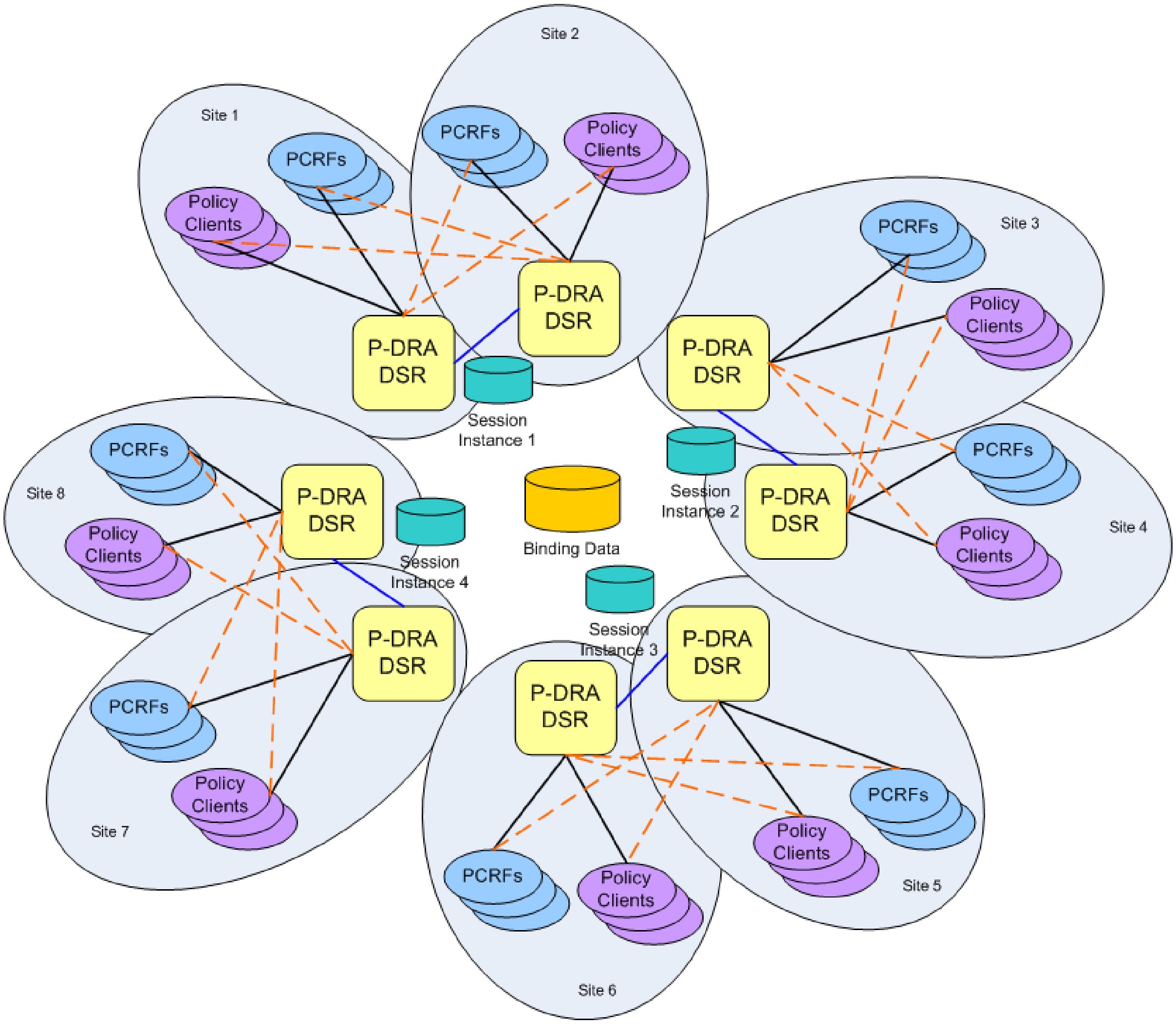


Figure 15: Policy Client, PCRF, and Site Relationships

Places

A "Place" allows servers or other Places to be associated with a physical location. The only Place type is "Site". A Site Place allows servers to be associated with a physical site.

An OAM GUI is used to configure Sites that correspond to physical locations where equipment resides. For example, Sites may be configured for Atlanta, Charlotte, and Chicago. Exactly one Place can be associated with a server when the server is configured

Place Associations

A “Place Association” allows Places to be grouped in ways that make sense for DSR Applications. A Place Association is a collection of one or more Places that have a common “Type”. A Place can be a member of more than one Place Association.

The Policy DRA application defines two Place Association Types:

- Policy DRA Binding Region

  As illustrated in *Figure 10: Sites, Mated Pairs, and Region*, the Policy DRA application defines a Region to include all Sites that are part of the Policy DRA network. This provides a scope for the Binding database, which is accessible to all Policy DRA Sites in the Policy DRA network.
- Policy DRA Mated Pair

  As illustrated in *Figure 10: Sites, Mated Pairs, and Region*, pairs of Policy DRA Sites are grouped together as Mated Pairs. Each Place Association with Type of Policy DRA Mated Pair includes exactly 2 sites. A Policy DRA Mated Pair has the following attributes:

  - Hosts an instance of the Policy DRA Session database
  - Hosts Policy Client Diameter connections for Policy Clients at both Sites in the Mated Pair
  - Hosts PCRF Diameter connections for PCRFs at both Sites in the Mated Pair

Server Groups

The Policy DRA application makes use of several different types of Server Groups, as defined in *Table 10: Server Group Functions*.

Table 10: Server Group Functions

Server Type	Server Group Function Name	Level
DA-MP servers	DSR (multi-active cluster)	MP
Policy SBR(S) and Policy SBR(B) servers	Policy SBR	MP
IPFE	IP Front End	MP
OAM server	DSR (acative/standby pair)	NOAM, SOAM

- Policy SBR Type

  Server Groups with the “Policy SBR” function type host either or both of the Policy Binding and Policy Session databases. The type of Policy database hosted by a given Server Group depends on the Resource Domain or Domains with which the Server Group is associated.

  Each Policy SBR Server Group consists of one, two, or three servers, depending on the type of deployment. *Table 11: Policy SBR Server Group Configuration and Data Redundance* describes the supported configurations for Policy SBR Server Groups. See *Redundancy* for details on Policy data redundancy.

Table 11: Policy SBR Server Group Configuration and Data Redundance

# of Servers	Redundancy	Typical Use
1	Active only. No Redundancy.	Labs and demos only.
2	Active/Standby. Server redundancy within a Site.	Single-site deployments or deplyments not requiring Site redundancy.
2	Active/Spare. Server redundancy across Sites.	Mated Pair deployments where the Standby server is eliminated at the primary Site (cost-saving). In this model, failure of the Active server at the primary Site will result in all Session access requests being routed across the WAN to the mate Site.
3	Active/Standby/Spare	Mated Pair deployments to avoid a single-server failure from causing Session access requests to be routed to the mate Site. This is the target for large deployments. New sessions are equally distributed across all Session Policy SBR Server Groups in the mated pair, meaning that ~50% of the Session accesses will be routed across the WAN.

Because only the active server in a Policy SBR Server Group is actually processing Stack Events, a Policy SBR Server Group can be engineered to run at 80% of maximum capacity. This holds for Site failure as well since the Spare server at the mate site will take over.

- DSR (multi-active cluster) Type

  For Policy DRA, all of the DA-MPs at a Site (even if there is only one) must be included in one Server Group with the DSR (multi-active cluster) function type. This eliminates the need to have all Policy Clients and PCRFs connected to every DA-MP.

  The DA-MPs in the Server Group will be treated as a cluster of active servers. There should be at least two DA- MPs in the Server Group in order to support in-service maintenance or upgrade. The DA- MPs in a Server Group should be engineered such that loss of a single server will not cause the remaining servers to go into overload.

  If the Policy DRA is being deployed in mated pairs, the DA- MPs at one site need to be configured to handle the entire load of the other site (in case of a site failure) without causing the surviving DA-MPs to go into overload – typically 40% of engineered capacity.

Resource Domains

A Resource Domain allows Server Groups to be grouped together and associated with a type of application resource. Each Resource Domain has a “Profile” that indicates the application usage of the resource domain. The Policy DRA application defines three Resource Domain Profiles: Policy Session, Policy Binding, and Policy DRA.

After Policy SBR Server Groups are configured to host the Session and Binding databases, those Server Groups can be added to Policy Binding and Policy Session Resource Domains. A Policy SBR Server Group must be associated with either a Policy Session or Policy Binding Resource Domain, or with both Policy Session and Policy Binding Resource Domains. The latter configuration is expected to be used only for small deployments.

DA- MPs are configured in a single Server Group per Policy DRA DSR with a Server Group function type of "DSR (multi-active cluster)". For a mated pair deployment, the two DSR (multi-active cluster) Server Groups containing all of the DA-MPs at the two sites must be included in a Policy DRA Resource Domain. For a non-mated deployment, the DSR (multi-active cluster) Server Group must be in its own Policy DRA Resource Domain.

Figure 16: Resource Domains illustrates the possible relationships between a single Policy SBR Server Group and the Policy Resource Domains. Although not shown in the figure, each Resource Domain will probably contain a number of Server Groups.

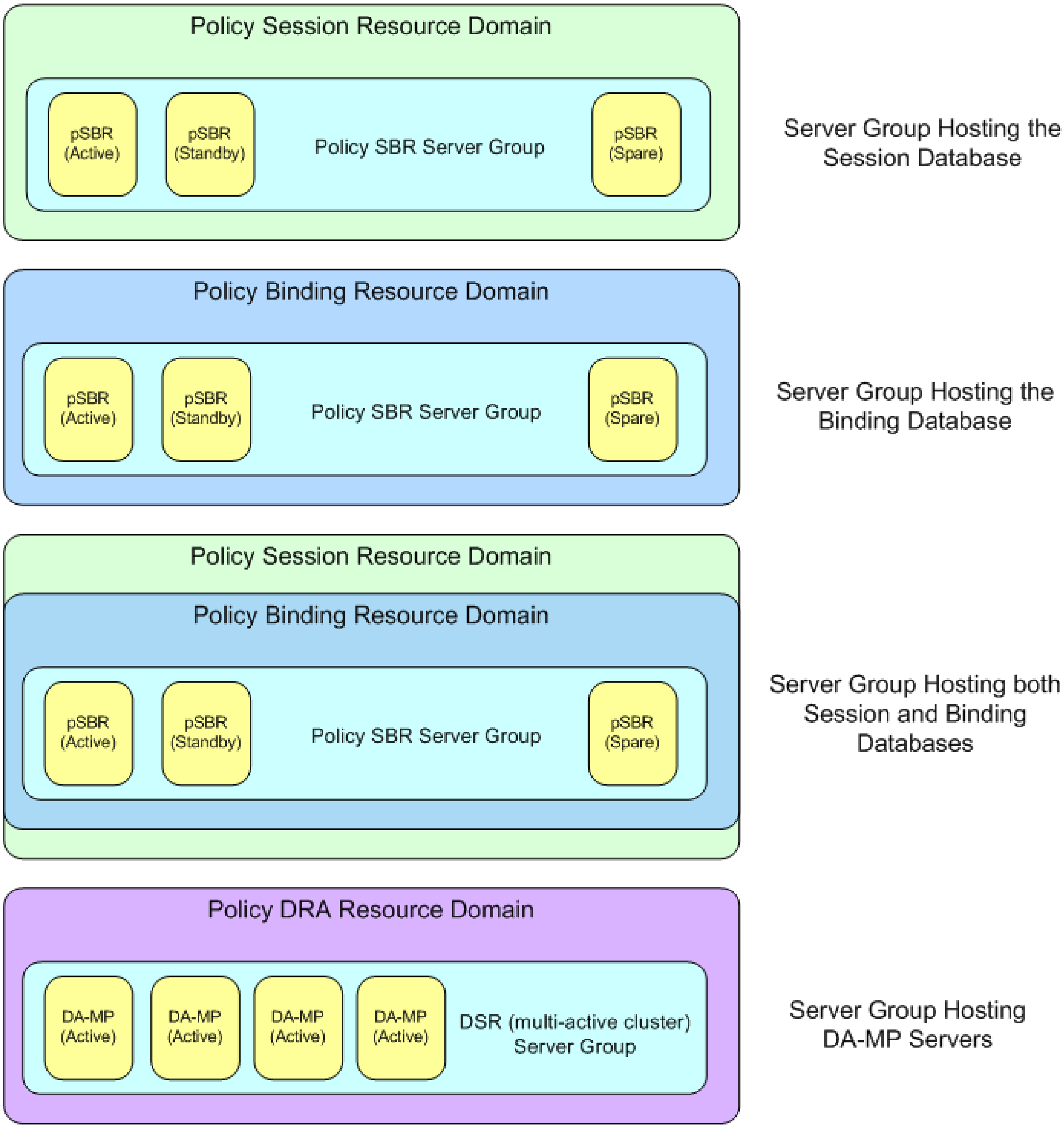

Policy Session Resource Domain
pSBR (Active)
pSBR (Standby)
Policy SBR Server Group
pSBR (Spare)
Server Group Hosting the Session Database
Policy Binding Resource Domain
pSBR (Active)
pSBR (Standby)
Policy SBR Server Group
pSBR (Spare)
Server Group Hosting the Binding Database
Policy Session Resource Domain
Policy Binding Resource Domain
pSBR (Active)
pSBR (Standby)
Policy SBR Server Group
pSBR (Spare)
Server Group Hosting both Session and Binding Databases
Policy DRA Resource Domain
DA-MP (Active)
DA-MP (Active)
DA-MP (Active)
DA-MP (Active)
DSR (multi-active cluster) Server Group
Server Group Hosting DA-MP Servers

Figure 16: Resource Domains

Policy Clients

Policy Clients act on behalf of the user equipment (UEs) to request Policy authorization and enforce Policy rules received from the PCRFs. Policy Clients send Policy requests to the Policy DRA, which ensures that the Policy request are sent to the PCRF in charge of Policy for the subscriber associated with the UE.

Policy DRA supports three different types of Policy Clients, referred to by 3GPP as AF, PCEF, and BBERF:

- The AF uses the Rx Diameter interface.
- The PCEF uses the Gx Diameter interface.
- The BBERF uses the Gxx Diameter interface.

How many connections a Policy Client might initiate towards the Policy DRA and how those connections are used are in customer control. The capabilities of the Policy Client, however, affect the functionality of the solution; as shown in *Table 12: Policy Client Connection Capability*.

Table 12: Policy Client Connection Capability

Number of Connections Supported by Policy Client (per Diameter host)	Effect on Solution Capability
1	• Site Redundancy cannot be taken advantage of. • Diameter signaling throughput is limited to the capacity of the connection. • Extra latency to reconnect in the event of a connection drop.
2	• Site Redundancy supported if secondary connection is configured to connect to Policy DRA mate site. • If both connections go to a single site and the Policy Client has the capability to use both connections simultaneously, Diameter signaling throughput may be doubled vs. only one connection. This configuration requires multiple Diameter connections to a single Diameter host – something that is not supported by RFC 3588, but which many vendors (including Tekelec) support to allow capacity beyond what a single connection can support. • Extra latency is avoided in the event of a single connection drop because the other connection can be used without waiting for reconnect and Capabilities Exchange.
>2	There are many scenarios possible, depending on the capabilities of the Policy Client. For example, there might be two connections to the primary Policy DRA (for capacity) and two to the mate Policy DRA (for Site redundancy).

Any Diameter Request can be sent to either Policy DRA in the mated pair, but to avoid possible race conditions between signaling and replication, messages in a Diameter session should be sent to the same Policy DRA Site when possible.

PCRFs

PCRFs are responsible for authorizing and making Policy decisions based on knowledge of subscriber resource usage and the capabilities allowed by the subscriber's account. In order to perform this function, all Policy requests for a given subscriber must be routed to the same PCRF.

Rather than provisioning a fixed relationship between a subscriber and a PCRF, the Policy DRA dynamically assigns subscribers to PCRFs using a load distribution algorithm, and maintains state about which subscribers are assigned to which PCRF. The relationship between a subscriber and a

PCRF can change any time the subscriber transitions from having no Diameter Policy sessions to having one or more Diameter Policy sessions. After a Policy session exists, however, all Policy sessions for that subscriber are routed to the assigned PCRF.

Policy DRA can interact with any 3GPP Release 9 compliant PCRF. Because these PCRFs come from different vendors, there are differences in how they are deployed in the network and how they "look" to the Policy DRA. The following PCRF configurations differ mainly in addressing and sharing of state across Diameter connections:

- A PCRF that shares state across different Diameter hostnames.
  - Each Diameter hostname can all support Gx, Gxx, S9, and Rx Diameter interfaces. This type of PCRF is supported by Policy DRA.
  - Each hostname has a different connection for each different interface type. This type of PCRF is supported by Policy DRA.
  - There is a different Diameter hostname for each connection for a specific Diameter interface. All of the Diameter hostnames share state. This type of PCRF is supported by Policy DRA.
  - There are different Diameter hostnames for different Policy Client vendors. Policy state is shared across the Diameter hostnames, but origin based routing is required to select a set of PCRFs for distribution of the initial binding depending on the Policy Client type. This type of PCRF is supported by Policy DRA, but requires use of Diameter Routing Function PCRF selection as described in *PCRF Selection for New Bindings*.
  - There is a different Diameter hostname for each connection. This type of PCRF is supported by Policy DRA, but requires use of Diameter Routing Function PCRF selection based on the vendor type of the Policy Client as described in *PCRF Selection for New Bindings*.
- A PCRF that has one Diameter hostname, but supports a number of connections to that hostname using different IP addresses.

  Each connection can support Gx, Gxx, S9, and Rx Diameter interfaces. This type of PCRF is supported by Policy DRA.

IPFE

In order to simplify network connectivity, Policy DRA will typically be deployed with one or two pairs of IPFEs per Policy DRA DSR site. IPFE is not mandatory, however; it is up to the customer whether it should be included.

The following deployment scenarios involving IPFE are possible:

- A single site Policy DRA in which the PCRFs are not capable of initiating connections to the Policy DRA. For example:
  - A Policy DRA DSR Site with a pair of IPFE blades, 8 DA-MP blades, and some Policy SBR blades
  - Four Policy Clients connected to two IPFE TSAs, with primary connections and secondary connections
  - The DA-MP blades are split into two groups that host connections to TSA1 and TSA2 respectively. This is necessary to ensure that a Policy Client's primary and secondary connections do not end up being connected to the same DA-MP.
  - One IPFE blade is primary for TSA1 and standby for TSA2; the other IPFE blade is primary for TSA2 and standby for TSA1.
  - Policy DRA MPs-to-PCRFs connectivity need not be fully meshed.

- An IPFE configuration in which Policy Clients are connected to a Policy DRA mated pair, but PCRFs are not capable of initiating connections to the Policy DRA. Each Policy Client has a primary connection to one Policy DRA site and a secondary connection to the mate site. For example:
  - Two Policy DRA DSR sites, each with a pair of IPFE blades and 4 DA-MP blades
  - Three Policy Clients with a primary connection to Policy DRA DSR Site 1 and secondary connections to Policy DRA DSR Site 2.
  - Three Policy Clients with a primary connection to Policy DRA DSR Site 2 and secondary connections to Policy DRA DSR Site 1.
  - Two PCRFs with primary connections to Policy DRA DSR Site1 and secondary connections to Policy DRA DSR Site 2.
  - Two PCRFs with primary connections to Policy DRA DSR Site2 and secondary connections to Policy DRA DSR Site 1.
  - One IPFE at Policy DRA DSR Site 1 is primary for TSA1. The other IPFE is standby for TSA1.
  - One IPFE at Policy DRA DSR Site 2 is primary for TSA2. The other IPFE is standby for TSA2.
- A single site Policy DRA in which a single IPFE pair is used for both Policy Clients and PCRFs. The use of IPFE for PCRFs is possible only if the PCRF can be configured to initiate connections towards the Policy DRA. Some customers refer to an IPFE used by PCRFs as an IP Back-End, or IPBE, although there is no difference between an IPBE and an IPFE from a software or configuration perspective. For example:
  - One pair of IPFE blades, each blade supporting two TSAs
  - Four Policy Clients connect to TSA1 with their secondary connection going to TSA3, or vice-versa.
  - The PCRFs connect to TSA2 with their secondary connection going to TSA4, or vice-versa.
  - Six Policy DRA MP servers, each capable of hosting connections from Policy Clients and PCRFs
  - One IPFE blade is primary for TSA1 and TSA2, and standby for TSA3 and TSA4.
  - The other IPFE blade is primary for TSA3 and TSA4, and standby for TSA1 and TSA2.
- A single site Policy DRA in which IPFE is used for both Policy Clients and PCRFs. In this case, two pairs of IPFE blades are deployed in order to support high Diameter signaling bandwidth. For example:
  - Two pairs of IPFEs, each supporting a two TSAs
  - The Policy Clients connect to either TSA1 or TSA2, with their secondary connection going to the other TSA.
  - The PCRFs connect to either TSA3 or TSA4, with their secondary connection going to the other TSA.
  - Eight Policy DRA DA-MPs, each capable of hosting connections from Policy Clients and PCRFs
  - One IPFE blade on the Policy Client side is primary for TSA1 and standby for TSA2. The other IPFE blade is primary for TSA2 and standby for TSA1.
  - One IPFE blade on the PCRF side is primary for TSA3 and standby for TSA4. The other IPFE blade is primary for TSA4 and standby for TSA3.
- A Policy DRA mated pair configured with an IPFE for Policy Clients and a separate IPFE for PCRFs. The Policy Clients and PCRFs have a primary connection to their local Policy DRA DSR and a secondary connection to the mate Policy DRA DSR. For example:
  - Two Policy DRA DSR sites, each with a two pairs of IPFE blades and 6 DA-MP blades
  - Three Policy Clients with a primary connection to Policy DRA DSR Site 1 and secondary connections to Policy DRA DSR Site 2.

- Three Policy Clients with a primary connection to Policy DRA DSR Site 2 and secondary connections to Policy DRA DSR Site 1.
- Two PCRFs with primary connections to Policy DRA DSR Site1 and secondary connections to Policy DRA DSR Site 2.
- Two PCRFs with primary connections to Policy DRA DSR Site2 and secondary connections to Policy DRA DSR Site 1.
- One IPFE on the Policy Client side at Policy DRA DSR Site 1 is primary for TSA1. The other IPFE is standby for TSA1.
- One IPFE on the Policy Client side at Policy DRA DSR Site 2 is primary for TSA3. The other IPFE is standby for TSA3.
- One IPFE on the PCRF side at Policy DRA DSR Site 1 is primary for TSA2. The other IPFE is standby for TSA2.
- One IPFE on the PCRF side at Policy DRA DSR Site 2 is primary for TSA4. The other IPFE is standby for TSA4.

Redundancy

Making the Policy DRA feature highly available is accomplished by deploying enough hardware to eliminate single points of failure. Except for lab and trial deployments, OAM servers and MP servers must be deployed such that a single failure or maintenance activity will not prevent the feature from performing its function.

The Policy DRA feature also supports site redundancy, which is the ability for the feature to continue functioning even when an entire site is lost to disaster or network isolation.

MP Server Redundancy

The following redundancy models are supported for MP servers, whether deployed as DA-MPs or Policy SBR MPs:

- DA-MP Multi-Active Cluster

  Policy DRA DA-MPs are deployed using an Active/Active redundancy model. This means that every DA-MP actively processes Diameter signaling. In order to avoid single points of failure, a minimum of two DA-MPs must be deployed (except for lab and trial deployments, where one DA-MP is acceptable). DA-MPs at a given site must be configured such that loss of a single DA-MP will not cause the remaining DA-MP servers to go into signaling overload.

- Policy SBR Active Only

  A Policy SBR (either Session or Binding) can be deployed in simplex redundancy mode only for labs or trials. Otherwise this configuration represents a single point of failure for the Policy SBR database being hosted by the Active-only Server Group. In this configuration, the Policy SBR Server Groups consist of a single Server.

- Policy SBR Active/Standby

  The Active/Standby redundancy model should be used for single site Policy DRA deployments, or for multi-site deployments when site redundancy is not important. In this configuration, the Policy SBR Server Groups consist of two servers. On system initialization, one of the two servers in each Policy SBR Server Group will be assigned the Active role and the other the Standby role.

These roles will not change unless a failure or maintenance action causes a switch-over. For Active/Standby Server Groups, switch-overs are non-revertive, meaning that recovery of a formerly Active server will not cause a second switch-over to revert the Active role to that server.

- Policy SBR Active/Spare

  The Active/Spare redundancy model can be used for mated pair deployments in which it is acceptable for traffic to move from one site to the mate site on failure of a single server. In this configuration, the Policy SBR Server Groups consist of two servers with one marked as “Preferred Spare”. On system initialization, the server not marked as Preferred Spare will be assigned the Active role and the other the Spare role. These roles will not change unless a failure or maintenance action causes a switch-over. For Active/Spare Server Groups, switch-overs are revertive, meaning that recovery of a formerly Active server will cause a second switch-over to revert the Active role to that server.
- Policy SBR Active/Standby/Spare

  The Active/Standby/Spare redundancy model should be used for Policy DRA mated pair deployments in which site redundancy is desired. In this configuration, each Policy SBR Server Group is configured with two servers at one site and the third at the mate site. The server at the mate site is designated in the Server Group configuration as “Preferred Spare”. On system initialization, one of the two servers that are located at the same site will be assigned the Active role and the other the Standby role. The server at the mate site will be assigned the Spare role (as was preferred). If the Active server can no longer perform its function due to failure or maintenance, the Standby Server will be promoted to Active. Only if both Active and Standby servers at a site are unable to perform their function will the Spare server at the mate site be promoted to Active. Active and Standby role changes within a site are non-revertive, but if the server at the mate site is Active and one of the other servers recovers, a switch-over will occur to revert the Active role back to the site with two servers.

Site Redundancy

Site redundancy is the ability to lose an entire site, for example due to a natural disaster or major network failure, without losing signaling or application state data. For Policy DRA this means no loss of Policy Binding or Policy Session data. In order to achieve site redundancy, the following configuration applies:

- Policy DRA is deployed on at least one mated pair of Policy DRA DSRs.
- Policy Clients and PCRFs are able to connect to both sites in the mated pair.
- Policy SBR Server Groups are set up to use the Active/Standby/Spare or Active/Spare redundancy model.
- System OAM (SOAM) Server Groups are set up to use the Active/Standby/Spare redundancy model.
- DA-MPs are recommended to be engineered at 40% capacity across the mated pair.

Data Redundancy

The Policy Session and Policy Binding databases are partitioned such that each Server Group in a Policy Session or Policy Binding Resource Domain hosts a portion of the data. Because each Server Group consists of redundant servers (Active/Standby, Active/Spare, or Active/Standby/Spare), the data owned by each Server Group is redundant within the Server Group.

Active, Standby, and Spare servers within a Policy SBR Server Group all maintain exact replicas of the data for the partition that the Server Group is responsible for. This data is kept in sync by using a form of signaling called replication. The synchronized tables on the Standby and Spare servers are continually audited and updated to match the master copy on the Active server.

Figure 17: Binding Table Partitioning Across Server Groups illustrates how a given Policy Binding table might be partitioned across four Policy SBR Server Groups in a Policy Binding Resource Domain.

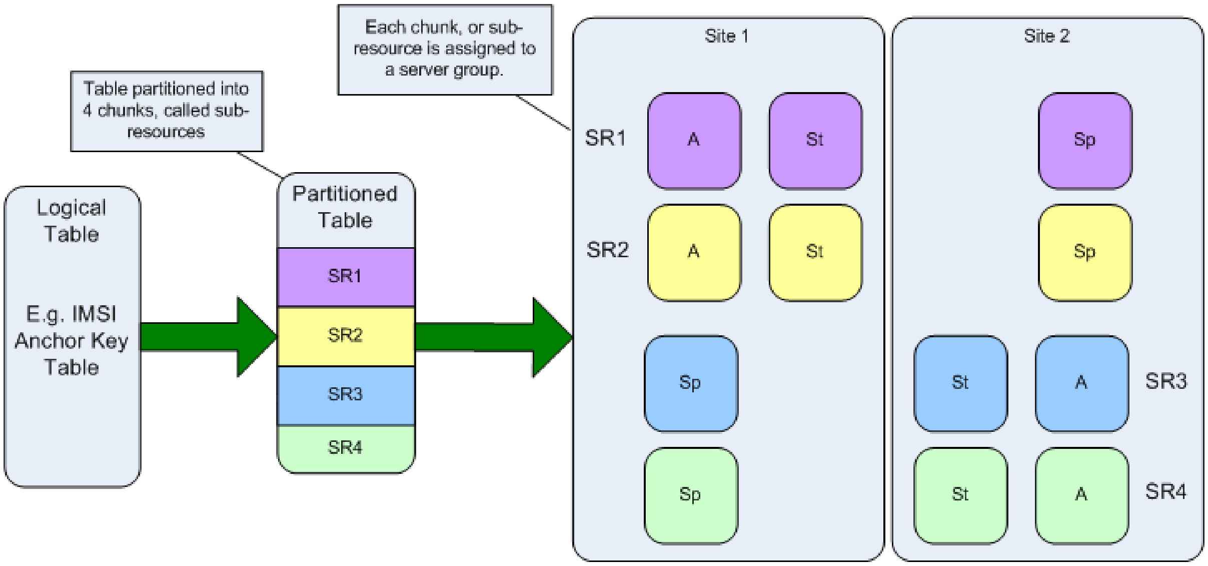


Table partitioned into 4 chunks, called sub-resources
Each chunk, or sub-resource is assigned to a server group.
Logical Table
E.g. IMSI Anchor Key Table
Partitioned Table
SR1
SR2
SR3
SR4
Site 1
Site 2
SR1
A
St
Sp
SR2
A
St
Sp
Sp
St
A
SR3
Sp
St
A
SR4

Figure 17: Binding Table Partitioning Across Server Groups

Figure 18: Multi-Table Resources illustrates how each Policy SBR Server Group hosts a partition of several tables. Only the Active Server within each Server Group can write to the database. The Standby and Spare servers replicate only actions (adds, changes, and deletes) performed by the Active server.

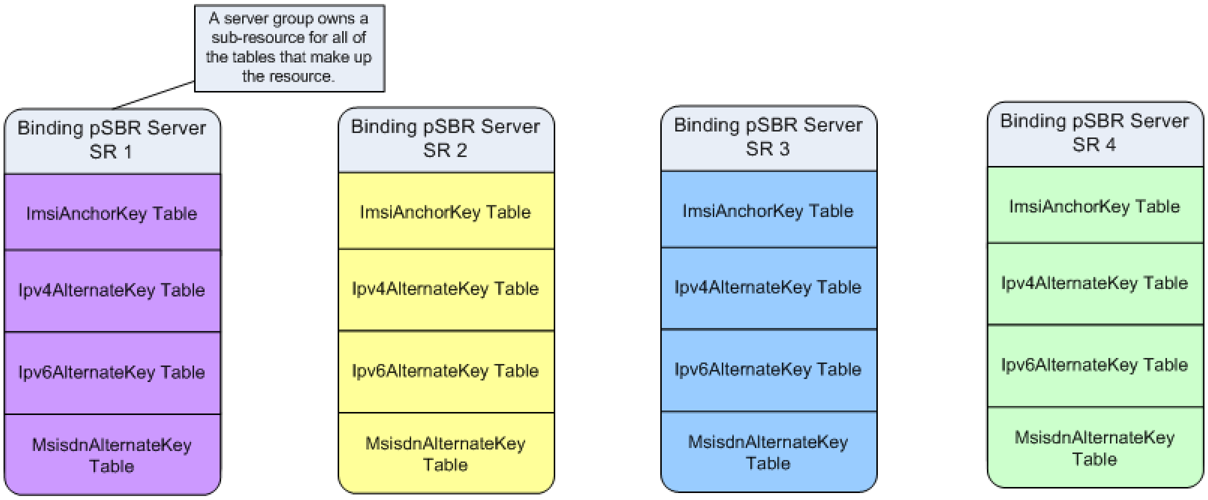


Figure 18: Multi-Table Resources

OAM Server Redundancy

The Policy DRA application can be deployed with varying degrees of redundancy on the NOAM and SOAM servers. Like the Policy SBR servers, the OAM servers can be configured to support site redundancy if desired.

Regardless of whether site redundancy is supported, the OAM servers must be deployed on redundant servers at a given site.

- Active/Standby NOAM and Active/Standby DR NOAM

  The NOAM servers are deployed using the active/standby redundancy model at one of the sites in the Policy DRA network. If site redundancy is desired, an optional pair of Disaster Recovery (DR) NOAM servers can be deployed at a different site. The DR NOAM servers are used only if manually brought into service following loss of the site where the original NOAM pair was located.
- Active/Standby/Spare SOAM

  If site redundancy is desired for Policy DRA mated pairs, the SOAM servers at each of the mate DSRs should be deployed using the Active/Standby/Spare redundancy model. In this configuration, two SOAM servers are deployed at one site and a third server is deployed at the mate site. The third server is configured as “Preferred Spare” in the SOAM Server Group. In the event of a site failure, the Policy SBR Servers running at the surviving site of the mated pair will report measurements, events, and alarms to the SOAM server at that site. Without the Spare SOAM server, the Spare Policy SBR servers would have no parent OAM server and would not be able to report measurements, events, and alarms.

Policy SBR servers in a given Policy SBR Server Group must be set up such that they belong to the Signaling Network Element of the site that has two of the three servers. This will allow all three servers in the Server Group to merge their measurements, events, and alarms to the same SOAM Server Group.

Figure 19: Data Merging - Normal Case illustrates how measurements, alarms, and events are merged. MP servers merge to the Active SOAM server for the signaling network element they belong to. The Active SOAM server then replicates the data to its Standby and Spare servers.

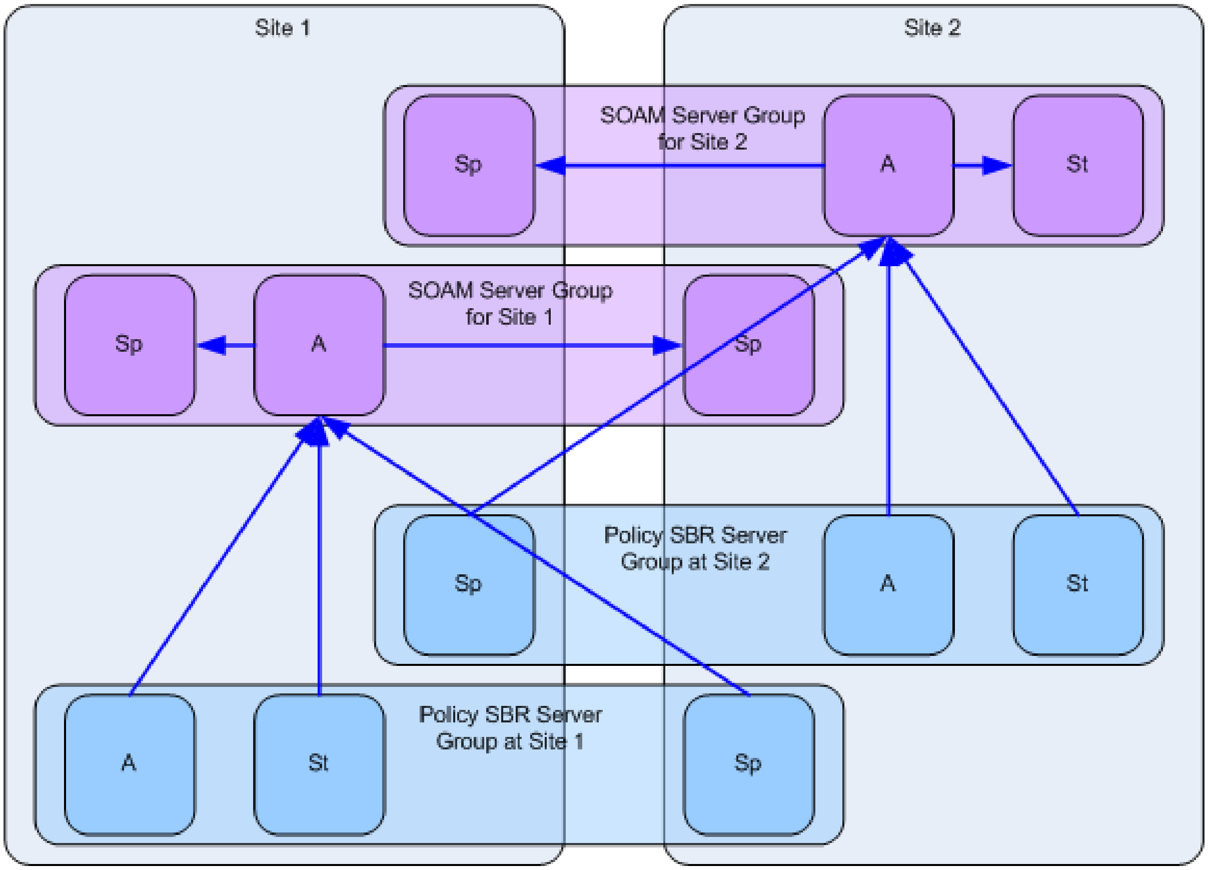


Figure 19: Data Merging - Normal Case

Figure 20: Data merging - Redundant Site Failure illustrates how a site failure affects merging of alarms, events, and measurements. When Site 2 fails, the servers at Site 1 that were marked as Preferred Spare are promoted to Active. The MP server that is now Active for the Policy SBR Server Group for Site 2 will start merging its data to the SOAM server that is now Active for the SOAM Server Group for Site 2.

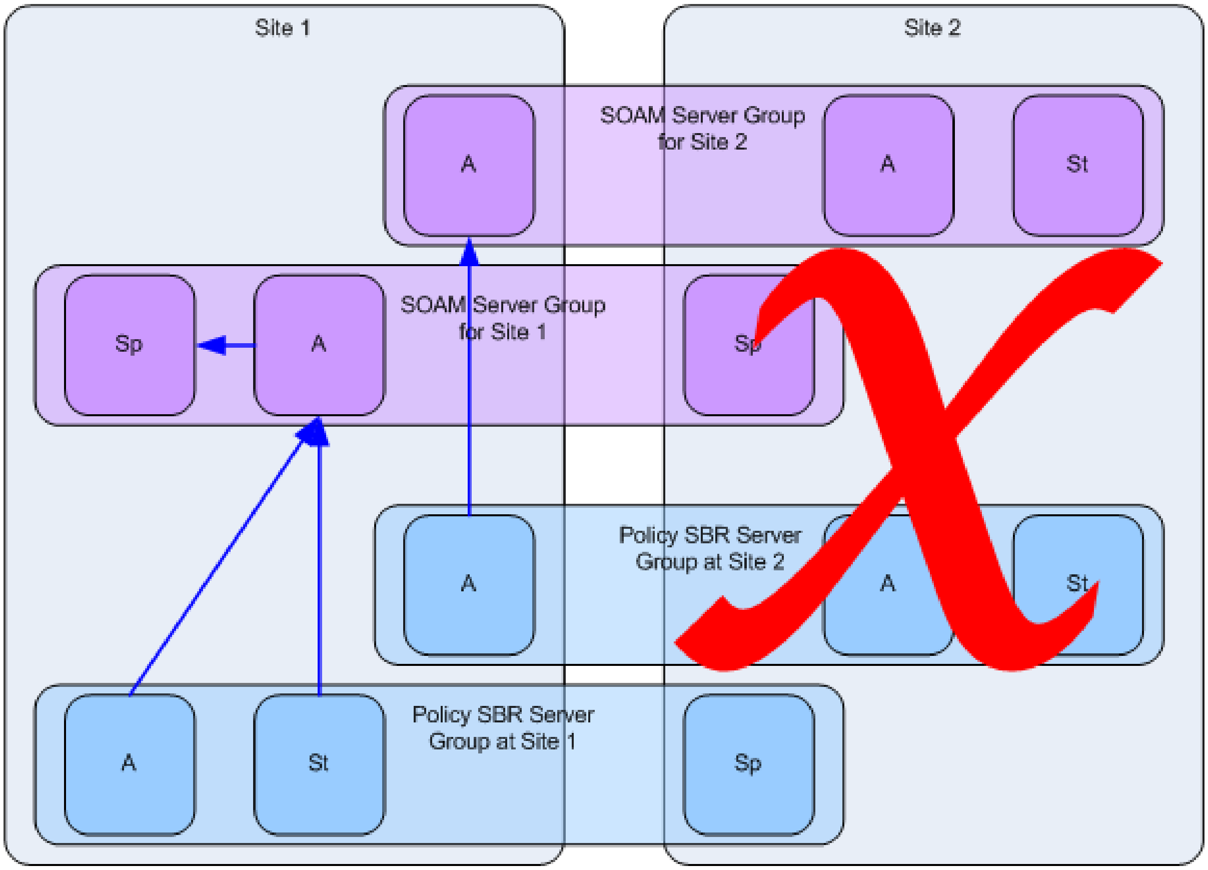

Site 1
Site 2
SOAM Server Group for Site 2
A
A
St
SOAM Server Group for Site 1
Sp
A
Sp
Policy SBR Server Group at Site 2
A
A
St
Policy SBR Server Group at Site 1
A
St
Sp

Figure 20: Data merging - Redundant Site Failure

Policy DRA Scalability

The Policy DRA feature is highly scalable. In addition to scaling up to support large customer networks, Policy DRA can scale down to support small customers, lab trials, and demos. This section describes supported configurations that illustrate how the Policy DRA feature scales.

For large systems, Policy DRA can scale up as follows:

- Eight mated pairs of Policy DRA DSRs (16 sites)
- Three enclosures per Policy DRA DSR site using half-height blades

  Each enclosure has 16 half-height slots.
- Two pairs of IPFE blades per Policy DRA DSR
- Sixteen DA-MP blades per Policy DRA DSR

Figure 10: Sites, Mated Pairs, and Region illustrates a sample Policy DRA network consisting of 6 mated pairs, or 12 sites with components that must be configured as follows:

- An instance of a Site (Place with type Site) is created for each physical location of a Policy DRA DSR.

- All MP servers (both Policy SBRs and DA-MPs) are assigned to the Site where they are physically located.
- An instance of a Policy DRA Mated Pair (Place Association with type Policy DRA Mated Pair) is created for each pair of sites that are mates.
- A pre-determined number of Policy Binding Server Groups are created on the Policy DRA DSR nodes that are initially deployed.
  - Each Policy Binding Server Group, if configured for site redundancy, must have at least one Server at the home site and one Server at the mate site.
  - Policy Binding Server Groups can exist on more than 2 sites, but the Policy DRA network is not operational until all sites hosting Policy Binding Server Groups are operational.
- A Policy Binding Resource Domain is created including all Policy Binding Server Groups.
- A pre-determined number of Policy Session Server Groups are created at each mated pair.

  Each Policy Session Server Group, if configured for site redundancy, must have at least one server at the home site and one server at the mate site.
- A Policy Session Resource Domain is created for each mated pair including the Policy Session Server Groups at the two mated sites.
- A DSR (multi-active cluster) Server Group is created for each Site, containing all of the DA-MP servers at the Site.
- A Policy DRA Resource Domain is created including the DSR Server Group at each of the mated Sites.
- A Policy DRA Binding Region (Place Association with type Policy DRA Binding Region) is created containing all Sites.

The Mated Pair of Policy DRA DSR sites illustrated in Figure 5 could support approximately 336,000 Diameter MPS with site redundancy (with DA-MPs engineered at 40%).

The single site Policy DRA DSR illustrated in Figure 6 could support approximately 384,000 Diameter MPS (with DA-MPs engineered at 80%).

MP Growth

The Policy DRA feature supports addition of DA-MPs as needed to support Diameter traffic. Each Policy DRA DA-MP can support 12,000 MPS when engineered to run at 40% to support site redundancy. If site redundancy is not needed, Policy DRA DA-MPs can be engineered at 80%, thereby supporting 24,000 MPS.

The DSR supports up to 16 DA-MPs per DSR site.

Database Growth

The Policy DRA feature does not support growth of the Policy Session or Policy Binding databases after feature activation.

Note: The percentages of different types of Policy Diameter messages in the overall Policy Diameter traffic load is referred to as the call model.

This has the following implications:

- The number of Server Groups that will host the Policy Session database for each mated pair (or single site if no mated pair is planned) must be determined prior to feature activation.

The number of Policy Session Server Groups required depends on the expected Diameter traffic rate in MPS for Policy signaling and the ratio of Diameter MPS to Session stack events determined by the call model.

- The number of Policy Binding database Server Groups for the entire planned Policy DRA network must be determined prior to feature activation.

  The number of Policy Binding Server Groups required depends on the number of Policy subscribers and the expected Diameter traffic rate in MPS for Policy signaling and the ratio of Diameter MPS to Binding stack events determined by the call model.
- After the number of Policy Binding and Policy Session Server Groups has been configured at Policy DRA feature activation time, these numbers cannot be changed without deactivating the feature.

  Deactivation of the Policy DRA feature results in an outage for all Policy signaling that traverses all Policy DRA DSRs in the Policy DRA network.

Mated Pair Growth

A mate Policy DRA DSR can be added to a single-site Policy DRA DSR.

A mated pair of Policy DRA DSRs can be added to a Policy DRA network.

Adding a Mate Policy DRA DSR to an Existing Policy DRA DSR

Because Policy SBR growth is not supported, a Policy DRA DSR deployed without a mate must host all of the Policy SBR Server Groups that are planned for deployment across the mated pair when the mate is added. This requires planning ahead for the eventual mate.

Note: Policy SBR Server Groups with only one server represent a single point of failure for a portion of the Policy SBR database.

A Policy DRA DSR site could be configured as follows for eventually adding a mate:

- Site A has two SOAM Server Groups configured: the red one on the top left for use by Site A and the blue one on the top right for use by Site B.
  - The Site A SOAM Server Group is set up with two Servers in Active/Standby configuration.
  - The Site B SOAM Server Group is set up with one Server configured as Preferred Spare. Because there are no other Servers in this Server Group, the Server will become active.
- Site A has four Policy SBR(B) Server Groups configured: the two red ones on the left for use by Site A and the two blue ones on the right for use by Site B.
  - The Site A Policy SBR(B) Server Groups are set up with two Servers in Active/Standby configuration. These Server Groups have the Site A SOAM Server Group as parent.
  - The Site B Policy SBR(B) Server Groups are set up with one Server configured as Preferred Spare. These Server Groups have the Site B SOAM Server Group as parent. Because there are no other Servers in these Server Groups, the single Server will become active.
- Site A has eight Policy SBR(S) Server Groups configured: the four red ones on the left for use by Site A and the four blue ones on the right for use by Site B.
  - The Site A Policy SBR(S) Server Groups are set up with two servers in Active/Standby configuration. These Server Groups have the Site A SOAM Server Group as parent.

- The Site B Policy SBR(S) Server Groups are set up with one Server configured as Preferred Spare. These Server Groups have the Site B SOAM Server Group as parent. Because there are no other Servers in these Server Groups, the single Server will become active.

Adding a Mated Pair of Policy DRA DSRs

Policy DRA network capacity can be expanded by adding mated pairs of Policy DRA DSRs. Policy DRA mated pairs added after the Policy DRA network is up and running cannot include additional Policy Binding Policy SBR Servers.

The number of Policy Session Policy SBR Servers must be the same for each of the new Policy DRA mates, and must be determined at Policy DRA feature activation. Every Policy DRA mated pair must have the same number of Policy Session Policy SBR Server Groups. After the number is selected the value cannot change until a software upgrade becomes available that supports Policy SBR growth.

While Policy SBR growth (adding Policy SBR Server Groups) is not supported, Policy DRA MP servers can be added as needed (up to a maximum of 16 DA-MPs) to support the desired level of Diameter signaling traffic.

Small System Support

In order to support small customers and lab and trial deployments, the Policy DRA feature can scale down to run on a small hardware footprint. This section describes the smallest supported Policy DRA DSR deployments.

A lab or trial system may not be required to support in-service maintenance, or have any hardware redundancy whatsoever. In the smallest supported lab/trial Policy DRA DSR, IPFE is not included because it does not make sense to distribute ingress connections when there is only one DA-MP server.

The NOAM and SOAM servers are also running in simplex mode, meaning that no redundancy exists. In addition, the NOAM and SOAM are virtualized on a single physical server to save hardware. The Policy SBR Server is also running in simplex mode and is configured to host both the Policy Binding and Policy Session databases. A single DA-MP hosts all Diameter signaling. Signaling is not affected if one or both of the (virtual) OAM servers happens to fail.

The configuration of the smallest viable commercially deployable Policy DRA DSR has enough hardware redundancy to support in-service maintenance:

- Two DA-MPs are required to survive server failures and maintenance. These DA-MPs should be engineered at 40% load since in a failure or maintenance situation, one Server will have to handle the load for both.
- The Policy SBR Server pair uses the Active/Standby redundancy model in order to support failures and maintenance.
- The Policy SBR Server pair hosts both the Policy Binding and Policy Session databases.
- The NOAM/SOAM Server pair uses the Active/Standby redundancy model in order to support failures and maintenance.
- Both NOAM and SOAM are virtualized onto a single pair of physical servers. The NOAM instance is Active on one server and Standby on the other. The SOAM instance is Active on one server and Standby on the other.

The smallest supported Mated Pair of Policy DRA DSRs, illustrated in *Figure 21: Smallest Supported Policy DRA Mated Pair*, has the following characteristics:

- The NOAM servers are deployed at Site 1 using Active/Standby redundancy.

- The Site 1 SOAM servers are deployed at Site 1, virtualized on the same servers with the NOAM servers. They, however, use the Active/Standby/Spare redundancy model, with the Spare server deployed at Site 2 and virtualized on the same server with one of the Site 2 SOAM servers.
- The Site 2 SOAM servers are deployed at Site 2 using the Active/Standby/Spare redundancy model. The Spare Site 2 SOAM server is virtualized at Site 1 on one of the servers already hosting an NOAM and a Site 1 SOAM server.
- A single combined Session and Binding Policy SBR triplet is deployed with two servers at Site 1 and one server at Site 2.
- Two DA-MPs are deployed at each site to support server redundancy at each site.

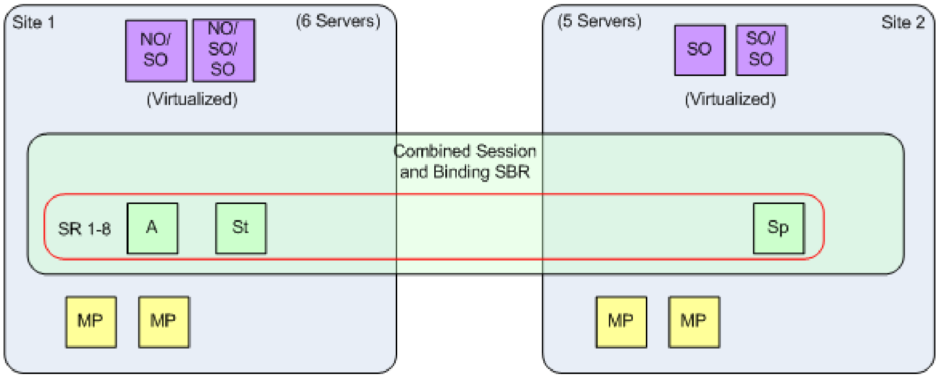


Figure 21: Smallest Supported Policy DRA Mated Pair

IP Networking

The flexibility of the Eagle XG DSR product iresults in many possible configurations for IP networking. This section focuses on IP network configurations that separate OAM functions from signaling functions such that signaling can continue to function normally if the OAM network is somehow disabled.

IP traffic is divided into categories called “Services”. For each Service, a network can be specified for both intra- and inter- Network Element IP traffic. *Table 13: IP Traffic-to-Service Mapping* illustrates a possible Services configuration for eparating signaling traffic from OAM traffic. In *Table 13: IP Traffic-to-Service Mapping*, there are two physical networks, one for OAM traffic and one for signaling traffic. The signaling network is divided into two VLANs for separation of Diameter signaling from C-level replication and stack event signaling.

The OAM network is divided into intra-NE and inter-NE networks. Both signaling and OAM networks include a secondary path for HA heart-beating. (The secondary path for HA heart-beating was added to improve robustness for HA heart-beating going across WANs.) The primary path for HA heart-beating is always the same as the network used for replication.

Table 13: IP Traffic-to-Service Mapping

Traffic Type	Service Name	Intra-NE Network	Inter-NE Network
Signaling Traffic			
Diameter signaling	Signaling	Signaling VLAN 5	Signaling VLAN 5

Traffic Type	Service Name	Intra-NE Network	Inter-NE Network
Stack events sent between DA-MPs, between DA-MPs and Policy SBRs, and between Policy SBRs	ComAgent	Signaling VLAN 4	Signaling VLAN 4
Replication of data among DA-MPs	Replication_MP	Signaling VLAN 4	Signaling VLAN 4
Replication of data among Policy SBRs	Replication_MP	Signaling VLAN 4	Signaling VLAN 4
HA Heartbeating among Policy SBRs (Primary Path)	Replication_MP	Signaling VLAN 4	Signaling VLAN 4
HA Heartbeating among DA-MPs (Primary Path)	Replication_MP	Signaling VLAN 4	Signaling VLAN 4
HA Heartbeating among Policy SBRs (Secondary Path)	HA_MP_Secondary	OAM VLAN 3	OAM VLAN 3
HA Heartbeating among DA-MPs (Secondary Path)	HA_MP_Secondary	OAM VLAN 3	OAM VLAN 3
OAM Traffic			
Replication of configuration data from NOAMs to SOAMs and from SOAMs to MPs	Replication	IMI	OAM VLAN 3
Merging of measurements, events, and alarms from MPs to SOAMs and from SOAMs to NOAMs	Replication	IMI	OAM VLAN 3
SNMP traps	Replication	IMI	OAM VLAN 3
SOAP Signaling	OAM	IMI	OAM VLAN 3
File Transfers to/from the File Management Area	OAM	IMI	
HA Heartbeating among OAM servers (Primary Path)	Replication	IMI	OAM VLAN 3
HA Heartbeating among OAM servers (Secondary Path)	HA_Secondary	Signaling VLAN 4	Signaling VLAN 4

Chapter 4

Policy DRA Configuration

Topics:

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

Policy DRA Configuration Overview

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

The Policy DRA application must be activated in the system before Policy DRA configuration can be performed.

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

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

  OAM configuration is performed on the NOAM.

  As shown in *Figure 22: GUI Structure for 3-tiered DSR Topology with Policy DRA*, network-wide Policy DRA configuration is performed on the NOAM.
- A pair or triplet of SOAM servers at each site running in active/standby, or active/standby/spare redundancy

  Diameter protocol configuration is done on the SOAM.

  Most of the OAM configuration components are viewable on the SOAM.

  Most DSR Application configuration is done on the SOAM.

  As shown in *Figure 22: GUI Structure for 3-tiered DSR Topology with Policy DRA*, site-specific configuration for Policy DRA is performed on the SOAM; some network-wide Policy DRA configuration components are viewable on the SOAM.
- A set of MP servers, which can host signaling protocol stacks (for example, DA-MPs), or in-memory database servers (for example, Policy Session Binding Repository [SBR])

An optional pair of Disaster Recovery NOAMs can be configured to manually take over in the event of loss of both the active and standby NOAMs

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

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

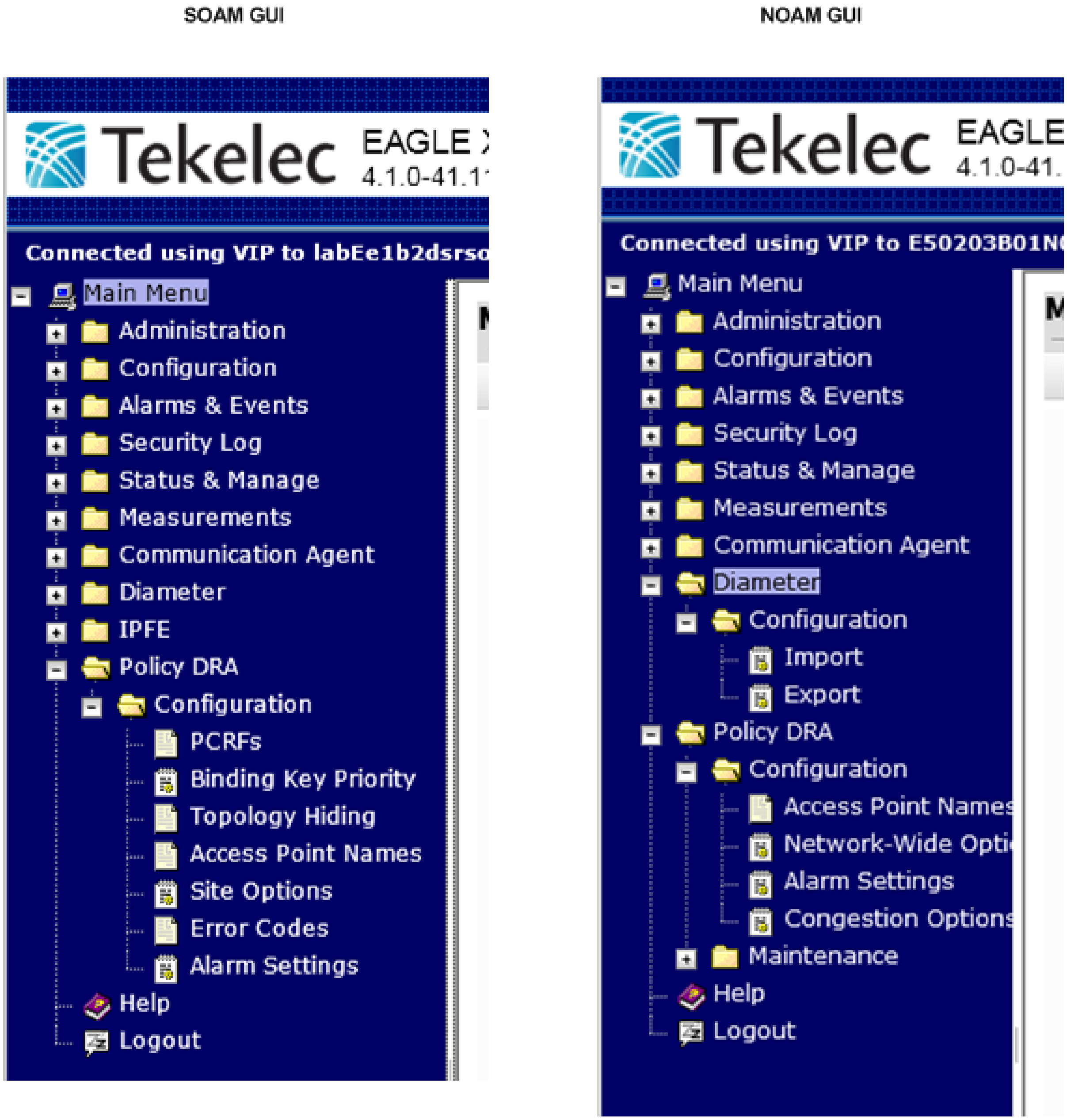


Figure 22: GUI Structure for 3-tiered DSR Topology with Policy DRA

NOAM and SOAM Configuration

Configuration data is divided into two categories depending on the scope of the data:

- Network-wide data is configured at the NOAM and is called A-scope data.
- Per-site data is configured at the SOAM for a given site and is called B-scope data.

In general, topology data like creation of sites, assignment of servers to sites, creation of server groups, and so on is A-scope data. DSR data configuration is generally site-scoped, or B-scope data.

Some Policy DRA data must be configured at the A-scope level and some data must be configured at the B-scope level.

Policy related data configured at the NOAM include:

- Assignment of Servers to Site Places
- Assignment of Servers to Policy SBR Server Groups
- Assignment of Policy SBR Server Groups to Policy Session and/or Policy Binding Resource Domains
- Assignment of DSR Multi-active Cluster Server Groups to Policy DRA Resource Domains
- Assignment of Site Places to Policy DRA Mated Sites Place Associations
- Assignment of Site Places to Policy DRA Binding Region Place Associations

Policy DRA-specific data configured at the NOAM include:

- Alarm Thresholds for:
  - Policy DRA Application Ingress Message Rate
  - Policy Session Database Capacity
  - Policy Binding Database Capacity
- Access Point Names (APN)
- Maximum Session Inactivity Time per APN

Policy DRA-specific data configured at the SOAM include:

- PCRFs local to the site
- Binding Key Priority for the site
- Topology Hiding configuration for the site
- Error response configuration for the site

Pre-Configuration Activities

Before Policy DRA configuration can be performed, the following activities need to be performed in the system:

- Verify that the Policy DRA application is activated in the system. (This is usually performed as part of the installation or upgrade activities.)

  Policy DRA appears in the left-hand GUI menu on the NOAM and the SOAM after the application is activated.
- Verify that the following NOAM configuration is complete for Policy DRA:
  - Places

    Select **Configuration ➤ Places**.

    Click **Report** to generate a report about the configured Places.

    Click **Print** to print the report, or **Save** to save the report as a text file.
  - Place Associations

    Select **Configuration ➤ Place Associations**.

    Click **Report** to generate a report about the configured Place Associations

Click **Print** to print the report, or **Save** to save the report as a text file.

- Resource Domains

  Select **Configuration ➤ Resource Domains**.

  Click **Report** to generate a report about the configured Resource Domains

  Click **Print** to print the report, or **Save** to save the report as a text file.

  Note: A Resource Domain cannot be deleted that is part of a Policy Binding or Policy Session profile, unless the P-DRA feature is deactivated. Resource Domains that are part of Policy DRA profiles can be deleted when the Policy DRA application is activated.

- Gather component information that is required for Diameter and Policy DRA configuration, including component item naming conventions and names, IP addresses, hostnames, and numbers of items to be configured.

  Naming Conventions and Hierarchical Routing illustrates the use of a naming convention.
- Configure Diameter Configuration components that are required for Policy DRA configuration. See *Diameter Configuration for Policy DRA*.

Diameter Configuration for Policy DRA

The Policy DRA application requires configuration of several Diameter Configuration components before the Policy DRA configuration can be performed.

All Diameter Configuration components are configured using the SOAM GUI.

Use the explanations and procedures in the Diameter Configuration online help and the *Diameter and Mediation User Guide* to complete the configuration of the Diameter Configuration components for the system, including the following Diameter Configuration components for use with the Policy DRA application.

1. **MP Profiles**

   Select **Diameter ➤ DA-MPs ➤ Profile Assignments**, and verify that the correct Session MP Profiles have been assigned for Policy DRA DA-MPs. If assignments need to be made or changed,

   - Use the **Diameter > Configuration > DA-MPs > Profile Assignments** page to assign an **MP Profile** for each configured Policy DRA DA-MP shown in the **DA-MP** list.
   - From the pulldown list, select the MP Profile that is for the correct blade type and for a Session application (such as **G6 Session** or **G8 Session**).

2. **Application Ids**

   Use the **Diameter > Configuration > Application Ids [Insert]** page to define an Application Id for each Diameter interface that will be used by Policy DRA in the system.

   Policy DRA supports the following values that can be selected in the **Application Id Value** pulldown list:

   - 16777236 – 3GPP Rx
   - 16777238 – 3GPP Gx
   - 16777266 – 3GPP Gxx
   - 16777267 – 3GPP S9
   - 4294967295 – Relay

Policy DRA always attempts to route using Peer Route Tables. The Peer Route Table can be configured here for each Application Id, or can be configured for Peer Nodes. If neither is configured, the Default Peer Route Table will be used. See *Policy DRA Routing of Diameter Messages*.

3. **CEX Parameters**

   Use the **Diameter > Configuration > CEX Parameters [Insert]** page to define the Capability Exchange parameters for each Application Id that was configured for use by Policy DRA:

   For each Application Id, select or enter:

   - **Application Id Type** – Authentication
   - **Vendor Specific Application Id**, if the Application Id and Vendor Id will be grouped in a Vendor-specific Application Id AVP
   - **Vendor Id** – if **Vendor Specific Application Id** is selected

     The Vendor ID 10415 is defined in 3GPP as follows:

     - Gx: 16777238 with Vendor-Id of 10415 (Defined in 3GPP 29.212)
     - Gxx: 16777266 with Vendor-Id of 10415 (Defined in 3GPP 29.212)
     - Rx: 16777236 with Vendor-Id of 10415 (Defined in 3GPP 29.214)
     - S9: 16777267 with Vendor-Id of 10415 (Defined in 3GPP 29.215)

4. **CEX Configuration Sets**

   Use the **Diameter > Configuration > Configuration Sets > CEX Configuration Sets [Insert]** page to select the configured CEX parameters to use in:

   - A CEX Configuration Set to be used for connections with the PCEF nodes (Gx)
   - A CEX Configuration Set to be used for connections with the AF nodes (Rx)
   - A CEX Configuration Set to be used connections with the PCRF nodes (Gx and Rx)
   - CEX Configuration Sets to be used with any other types of nodes, such as BBERF (Gxx)
   - A CEX Configuration Set named Default is provided for the Relay Application Id; it can be edited if needed.

5. **Local Nodes** (Policy DRA DA-MPs)

   Use the **Diameter > Configuration > Local Nodes [Insert]** page to configure the Policy DRA DA-MPs as Local Nodes in the system.

   The pulldown list of **IP Addresses** contains the XSI addresses configured on DSR MP Servers.

6. **Peer Nodes**

   Use the **Diameter > Configuration > Peer Nodes [Insert]** page to configure PCEFs, AFs, BBERFs, and any other types of nodes as Peer Nodes to the Policy DRA DA-MPs in the system. (Policy DRA DA-MPS can also be Peer Nodes to each other at different sites.)

   See *Policy DRA Routing of Diameter Messages* for details on routing of messages for Policy DRA.

7. **Connections**

   Use the **Diameter > Configuration > Peer Nodes [Insert]** page to configure connections between the Policy DRA DA-MPS and the Peer Nodes.

   Any IPFE Target Set Address (TSA) that is used to configure a connection must use the same **Transport Protocol** (SCTP or TCP) that is selected to configure the connection.

8. **Route Groups**

Use the **Diameter > Configuration > Route Groups [Insert]** page to configure Route Groups for use with Policy DRA Peers.

For priority-based initial CCR-I routing, configure N+1 Route Groups where N is the number of PCRFs in the system. The first N Route Groups contain one corresponding PCRF Peer Node in each one, and the last Route Group contains all PCRFs.

The goal is to setup a routing configuration such that if there is no route available to the suggested PCRF in an initial (binding capable) session Request, Diameter automatically sends the Request messages to any other available PCRF.

Define a Route Group for each PCRF; enter the **Route Group Name**, select the **Peer Node** name (PCRF name) and enter the **Provisioned Capacity** as **1**.

Define a last Route Group for all PCRFs; enter the **Route Group Name**, then add a **Peer Node, Connection and Capacity** entry for every PCRF. Select the **Peer Node** (PCRF) and enter the **Provisioned Capacity** as **1** for each PCRF entry.

9. **Route Lists**

   Use the **Diameter > Configuration > Route Lists [Insert]** page to configure Route Lists for use with the configured Route Groups.

   For priority-based initial session binding, configure N Route Lists where N is the number of PCRFs in the system.

   All Route Lists must contain at least two Route Groups, one for a single PCRF and one for all PCRFs.

   Assign **Priority** value **1** to each Route Group for a single PCRF; assign **Priority** value **2** to the Route Group containing all the PCRFs.

   Enter **1** for the **Minimum Route Group Availability Weight** in all of the Route Lists.

10. **Peer Route Table** and **Peer Routing Rules**

    Use the **Diameter > Configuration > Peer Route Tables [Insert]** page to configure new Peer Route Tables if needed, and the **Viewing Rules for Peer Route Table** page to configure Peer Routing Rules, such that DSR forwards messages based on the PCRF preference.

    Peer Routing Rules can be added to the Default Peer Route Table (PRT) or to new Peer Route Tables.

    See *Policy DRA Routing of Diameter Messages* for details on PRT routing of Policy DRA messages.

    The routing configuration will ensure that whenever Policy DRA requests Diameter to route to a particular PCRF based on the PRT:

    - If the PCRF is available, Diameter will route to it.
    - If the PCRF is not available, Diameter will route the message to any other available PCRF.

11. **Application Routing Rules**

    Use the **Diameter > Configuration > Application Routing Rules** page to configure an Application Routing Rule for each Diameter interface (such as Gx or Rx) that is configured in an Application Id, to be used for Diameter routing of messages to the Policy DRA application. Policy DRA must receive all Policy Diameter Requests.

    For each rule, enter or select:

    - **Rule Name** for a configured Application Id (Diameter interface)
    - **Priority**

- In **Conditions**, for **Application Id** select from the pulldown lists the **Equals** Operator and the **Application Id** configured for Policy DRA.
- **Application Name - PDRA**

Policy DRA Routing of Diameter Messages

Policy DRA routes Diameter messages depending on the following criteria:

- Answer message or Request message
- New session Request or in-session Request
- New binding or existing binding new session Request

Peer Routing

Policy DRA always attempts to route using Peer Route Tables. The Diameter Routing Function attempts to use Peer Route Tables in the following predefined precedence:

1. Peer Route Table configured for the originating Peer Node (Diameter->Configuration->Peer Nodes)

   If a match is found, the specified Peer Route Table is used.
2. Peer Route Table configured for the Diameter Application-ID of the policy session initiation request being routed (Diameter->Configuration->Application Ids)

   If the ingress Peer Node is configured as "Not Selected", that entry is skipped and the Application Ids configuration is checked.
3. Default Peer Route Table

   If no match is found in the Application-Ids configuration, the Default Peer Route Table is used.
4. Destination-Host Routing

   If no Peer Routing Rule matches in the Default Peer Route Table, Policy DRA will attempt to route the Request using Destination-Host routing (for example, to a connection or Alternate Implicit Route List associated with the destination Peer Node).

Routing of Session Initiation Requests for New Bindings

Policy DRA allows a Peer Route Table to be configured for use when a new binding is created. This Peer Route Table can specify Peer Routing Rules to:

- Allow new bindings to be routed, for example, based on the Origin-Host or Origin-Realm of the PCEF
- Cause new bindings to be load-shared across all local PCRFs.

The Peer Route Table to use for new bindings is specified in the **Policy DRA->Configuration->Site Options** GUI page on the SOAM at each site.

If the Peer Route Table for new bindings is set to "Not Selected", the Diameter Routing Function uses the precedence described in *Peer Routing*.

Routing of Session Initiation Requests for Existing Bindings

Sessions for subscribers that are already bound to a PCRF must be routed to the bound PCRF, or to a PCRF that shares state with the bound PCRF if the PCRF supports sharing of policy state. For existing bindings, no Peer Route Table is configured in the Policy DRA application Site Options. Instead, the Diameter Routing Function uses the precedence described in *Peer Routing*.

Routing of Requests from PCRF to a Policy Client

In order to route Requests initiated by the PCRF, routing must be configured such that Requests from any PCRF can be routed to any Policy Client in the network. This type of routing is used to route RAR and ASR requests. For Requests from PCRFs to Policy Clients, no Peer Route Table is configured in the Policy DRA application Site Options. Instead, the Diameter Routing Function uses the precedence described in *Peer Routing*.

Routing of In-Session Requests

In-session Requests are Requests within a Diameter session other than the Request that established the Diameter session. CCR-U, CCR-T, and STR are all examples of in-session Requests. In-session Requests are routed using the predefined precedence of Peer Route Tables described in *Peer Routing*.

Routing of Answer Messages

All Diameter Answer messages are routed over the same path on which the Request was routed, using hop-by-hop routing. No routing configuration is necessary to route Answer messages.

Policy DRA Configuration on the NOAM and the SOAM

This section describes the **Policy DRA > Configuration** GUI pages on the NOAM and the SOAM.

Access Point Names

An Access Point Name (APN) is a unique Packet Data network identifier. The Policy DRA uses configured Access Point Names to validate APN entries received in Diameter signaling, and to apply appropriate Stale Session Timeout values during database audits.

A session is considered stale only if no RAR/RAA messages are received in a length of time longer than the configured Stale Session Timeout time. If a session's age exceeds this value, that session is eligible to be audited out of the database. The Stale Session Timeout value is used for sessions associated with an Access Point Name. For sessions which are not associated with any configured Access Point Names, the Default Stale Session Timeout value configured on the **Policy > DRA > Configuration >Network-Wide Options** page is used.

Note: Access Point Names are configurable only on Active NOAM servers, and are viewable on SOAM and NOAM servers.

The fields are described in *Access Point Names elements*.

On the **Policy DRA > Configuration > Access Point Names** page on the Active NOAM, you can perform the following actions:

- Filter the list of Access Point Names, to display only the desired Access Point Names.
- Sort the list entries in ascending or descending order by Access Point Names or by Stale Session Timeout, by clicking the column heading. By default, the list is sorted by Access Point Names in ascending numerical order.
- Click the **Insert** button.

The **Policy DRA > Configuration > Access Point Names [Insert]** page opens. You can add a new Access Point Name. See *Inserting Access Point Names*. If the maximum number of Access Point Names (200) already exists in the system, the **Policy DRA > Configuration > Access Point Names [Insert]** page will not open, and an error message is displayed.

- Select an Access Point Name in the list, and click the **Edit** button.

  The **Policy DRA > Configuration > Access Point Names [Edit]** page opens. You can edit the selected Access Point Name. See *Editing Access Point Names*.
- Select an Access Point Name in the list, and click the **Delete** button to remove the selected Access Point Name. See *Deleting an Access Point Name*.

On the **Policy DRA > Configuration > Access Point Names** page on the SOAM, you can view the configured Access Point Names, and perform the following actions:

- Filter the list of Access Point Names, to display only the desired Access Point Names.
- Sort the list entries in ascending or descending order by Access Point Names or by Stale Session Timeout, by clicking the column heading. By default, the list is sorted by Access Point Names in ascending numerical order.

Access Point Names elements

Table 14: Access Point Names elements describes the elements on the **Policy DRA > Configuration> Access Point Names** page. Data Input Notes apply to the Insert and Edit pages; the View page is read-only.

Table 14: Access Point Names elements

Elements (* indicates required field)	**Description**	**Data Input Notes**
* Access Point Name	The unique network identifier of a Packet Data Access Point.	Format: Text box. Valid characters are A-Z, a-z, 0-9, dash (-), and period (.). The string must begin and end with an alphabetic or numeric character. Range: 1-100 characters
Stale Session Timeout (Hrs)	The time value (in hours) after which a session is considered to be stale. A session is considered stale only if no RAR/RAA messages are received in longer than the configured time. This value is used for sessions associated with this Access Point Name. For sessions that are not associated with any configured Access Point Names, the Default Stale Session Timeout value configured on the NOAM **Policy DRA >**	Format: Text box. Value must be numeric. Range: 1-2400 Default: 168 hours (7 days)

Elements (* indicates required field)	Description	Data Input Notes
	Configuration > Network-Wide Options page is used. If a session's age exceeds this value, that session is eligible to be audited out of the database.	

Viewing Access Point Names

Use this task to view all configured Access Point Names on the NOAM or SOAM.

Select **Policy DRA ➤ Configuration ➤ Access Point Names**.

The **Policy DRA > Configuration > Access Point Names** page appears with a list of configured Access Point Names.

The fields are described in *Access Point Names elements*.

Inserting Access Point Names

Use this task to insert Access Point Names.

Note: Access Point Names are configurable only on Active NOAM servers, and are viewable on NOAM and SOAM servers.

The fields are described in *Access Point Names elements*.

1. Select **Policy DRA ➤ Configuration ➤ Access Point Names**.

   The **Policy DRA > Configuration > Access Point Names** page appears.
2. Click **Insert**.

   The **Policy DRA > Configuration > Access Point Names [Insert]** page appears.
3. Enter a unique Access Point Name in the Access Point Name **Value** field.
4. If a value other than the default Stale Session Timeout value is desired, enter the desired length of time in hours in the Stale Session Timeout (Hrs) **Value** field.
5. Click:

   - **OK** to save the new Access Point Name and return to the **Policy DRA > Configuration > Access Point Names** page.
   - **Apply** to save the new Access Point Name and remain on this page.
   - **Cancel** to return to the **Policy DRA > Configuration > Access Point Names** page without saving any changes.

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

   - The entered Access Point Name is not unique (already exists).
   - Any fields contain a value that contains invalid characters or is out of the allowed range
   - Any required field is empty (not entered)
   - Adding the new Access Point Name would cause the maximum number of Access Point Names (200) to be exceeded

Editing Access Point Names

Use this task to edit Access Point Stale Session Timeout values.

Note: The Access Point Name **Value** cannot be edited.

Note: Access Point Names are configurable only on Active NOAM servers, and are viewable on NOAM and SOAM servers.

The fields are described in *Access Point Names elements*.

1. Select **Policy DRA** ➤ **Configuration** ➤ **Access Point Names**.

   The **Policy DRA Configuration Access Point Names** page appears.
2. Click **Edit**.

   The **Policy DRA > Configuration > Access Point Names [Edit]** page appears.
3. Enter the desired length of time in hours in the Stale Session Timeout (Hrs) **Value** field.
4. Click:

   - **OK** to save the changes and return to the **Policy DRA > Configuration > Access Point Names** page.
   - **Apply** to save the edited Access Point Name and remain on this page.
   - **Cancel** to return to the **Policy DRA > Configuration > Access Point Names** page without saving any changes.

   If **OK** or **Apply** is clicked and the following condition exists, an error message appears:

   - The edited Access Point Name no longer exists (for example, it has been deleted by another user), and no changes are made to the database.

Deleting an Access Point Name

Use this task to delete an Access Point Name.

Note: Access Point Names are configurable only on Active NOAM servers, and are viewable on NOAM and SOAM servers.

1. Select **Policy DRA** ➤ **Configuration** ➤ **Access Point Names**.

   The **Policy DRA > Configuration > Access Point Names** page appears.
2. Select the **Access Point Name** to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.
4. Click:

   - **OK** to delete the Access Point Name.
   - Click **Cancel** to cancel the delete function and return to the **Policy DRA > Configuration > Access Point Names** page.

   If **OK** is clicked and the selected Access Point Name no longer exists (it was deleted by another user), an error message is displayed. The Access Point Names view is refreshed and the deleted Access Point Name no longer appears on the page.

Network-Wide Options

On the **Policy DRA > Configuration > Network-Wide Options** page on an Active NOAM, the following **Network-Wide Options** can be configured:

- **General Options**
    - Indicate whether to relay or discard an Answer message when the Policy DRA is Unavailable (for answers).
    - Indicate whether to use the Local Host Origin-Host and Origin-Realm or the PCRF Origin-Host and Origin-Realm as the Origin-Host and Origin-Realm in RAR messages that are constructed and sent by Policy DRA to the Policy Clients.
- **Audit Options**
    - Change the **Default Stale Session Timeout** value to a value other than the default value in the field.

      This setting is a length of time in hours after which a session is considered to be stale. A session is considered stale only if no RAR/RAA messages are received in a length of time longer than this configured time. If a session's age exceeds this value, that session is eligible to be audited out of the database.

      This value is used only if a session is not associated with a configured Access Point Name. For sessions that are associated with a configured Access Point Name, the **Stale Session Timeout** value configured for the Access Point Name is used.
    - Change the **Maximum Audit Frequency** default value to a different number of records per second for auditing the Policy SBR database.

The fields are described in *Network-Wide Options elements*.

Network-Wide Options elements

Table 15: Network-Wide Options elements describes the elements on the **Policy DRA > Configuration > Network-Wide Options** page on the NOAM.

Table 15: Network-Wide Options elements

Fields (* indicates a required field)	Description	Data Input Notes
General Options		
Policy DRA Unavailable (for answers)	A choice to relay or discard an Answer message when Policy DRA is Unavailable.	Format: Radio buttons Range: Relay or Discard Default: Relay
Origin-Host and Origin-Realm for Policy	A radio button choice to control the selected option's Origin-Host and Origin-Realm use as the Origin-Host and Origin-Realm in the RAR	Format: Radio buttons Range: Local Host or PCRF

Fields (* indicates a required field)	Description	Data Input Notes
DRA generated RAR messages	messages built and sent by Policy DRA to Policy Clients.	Default: Local Host
Audit Options		
* Default Stale Session Timeout	The time (in hours) after which a session is considered to be stale. A session is considered stale only if no RAR/RAA messages are received in longer than the configured time. If a session's age exceeds this value, that session is eligible to be audited out of the database. This value is used only if a session is not associated with a configured Access Point Name. For sessions that are associated with a configured Access Point Name, the **Stale Session Timeout** value configured for the Access Point Name is used.	Format: Text box Range: 1-2400 hours (1 hour to 100 days) Default: 168 hours (7 days)
* Maximum Audit Frequency	The maximum records per seconds for auditing the Policy SBR database.	Format: Text box Range: 1000-25000 Default: 12000

Viewing Network-Wide Options

Use this task to view configured Network-Wide Options on the NOAM.

Select **Policy DRA** ➤ **Configuration** ➤ **Network-Wide Options**.

The **Policy DRA > Configuration > Network-Wide Options** page appears with a list of configured Network-Wide Options.

The fields are described in *Network-Wide Options elements*.

Setting Network-Wide Options

Use this task to set Network-Wide Options on the NOAM.

The fields are described in *Network-Wide Options elements*.

The following Policy DRA configuration options apply to the entire Policy DRA Network:

- Policy DRA Unavailable (for answers)
- Default Stale Session Timeout (in hours)
- Origin-Host and Origin-Realm for Policy DRA generated RAR messages

1. Select **Policy DRA** ➤ **Configuration** ➤ **Network-Wide Options**.

   The **Policy DRA Network-Wide Options** page appears.

2. The **Relay** or **Discard** radio button setting is an engineered system value (uneditable) that controls the network option for the Policy DRA Unavailable (for answers) field.
3. Enter a number in the Default Stale Session Timeout **Value** field.
4. Select the **Local Host** or **PCRF** radio button.

   This sets the Origin-Host and Origin-Realm that will be used in the RAR messages constructed and sent by Policy DRA to policy clients.
5. Click:
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to discard changes and remain on the **Policy DRA > Configuration > Network-Wide Options** page.

   If **Apply** is clicked and the following condition exists, an error message appears:
   - The entered Default Stale Session Timeout value contains invalid characters, is out of the allowed range, or the field is empty.

Alarm Settings

Note: Alarm Settings are configurable only on Active NOAM servers, and are viewable on NOAM and SOAM servers.

On the **Policy DRA > Configuration > Alarm Settings** page on an SOAM, you can view the configured Alarm Thresholds and Suppress indications.

Each alarm can be configured with Minor, Major, and Critical threshold percentages.

The fields are described in *Alarm Settings elements*.

On the **Policy DRA > Configuration > Alarm Settings** page on the NOAM, you can change the Alarm Thresholds and the Suppress indications for the following alarms:

- DSR Application Ingress Message Rate

  The DSR Application Ingress Message Rate alarm is raised when the average Policy DRA ingress messages rate exceeds the configured Alarm Threshold. The thresholds are based on the engineered system value for Ingress Message Capacity.
- Policy SBR Sessions Threshold Exceeded

  The Policy SBR Sessions Threshold Exceeded alarm percent full is based on the number of Session records compared to an engineered maximum that varies according to the number of session Policy SBR Server Groups per mated pair chosen during Policy DRA feature activation.

  The Policy SBR Sessions Threshold Exceeded alarm is raised when number of concurrent Policy SBR sessions exceeds the configured threshold.
- Policy SBR Bindings Threshold Exceeded

  The Policy SBR Bindings Threshold Exceeded alarm measures the number of IMSI Anchor Key records against an engineered maximum value that varies according to the number of binding Policy SBR Server Groups specified at Policy DRA feature activation.

  The Policy SBR Bindings Threshold Exceeded alarm works similarly to the session capacity alarm except that the scope of the binding capacity alarm is network-wide.

Alarm Settings elements

Table 16: Alarm Settings elements describes the elements on the **Policy DRA > Configuration > Alarm Settings** page. The elements can be configured and viewed on the NOAM, and only viewed on the SOAM. Data Input Notes apply to the Insert and Edit pages; the View page is read-only.

The page contains three sets of input fields for the following alarms:

- DSR Application Ingress Message Rate
- Policy SBR Sessions Threshold Exceeded
- Policy SBR Bindings Threshold Exceeded

The element labels are the same for each input field set, but some serve different purposes and have different values. These distinctions are noted in the table.

Table 16: Alarm Settings elements

Elements (* indicates required field)	Description	Data Input Notes
	DSR Application Ingress Message Rate	
* Alarm Name	This alarm is raised when average Policy DRA ingress messages rate exceeds the configured threshold. The thresholds are based on the engineered system value for Ingress Message Capacity.	Format: Non-editable text box Range: DSR Application Ingress Message Rate
* Critical Alarm Threshold (Percent)	The Policy DRA ingress message rate threshold for this alarm to be raised as Critical. The threshold is a percentage of the Ingress Capacity Capability.	Format: Text box Range: 100-200 Default: 160
Suppress Critical	Controls whether this alarm is raised as Critical.	Format: Check box Range: Unchecked (No) or Checked (Yes) Default: Unchecked (No)
* Major Alarm Threshold (Percent)	The Policy DRA ingress message rate threshold for this alarm to be raised as Major. The threshold is a percentage of the Ingress Capacity Capability.	Format: Text box Range: 100-200 Default: 140
Suppress Major	Controls whether this alarm is raised as Major.	Format: Check box Range: Unchecked (No) or Checked (Yes) Default: Unchecked (No)

Elements (* indicates required field)	Description	Data Input Notes
* Minor Alarm Threshold (Percent)	The Policy DRA ingress message rate threshold for this alarm to be raised as Minor. The threshold is a percentage of the Ingress Capacity Capability.	Format: Text box Range: 100-200 Default: 110
Suppress Minor	Controls whether this alarm is raised as Minor.	Format: Check box Range: Unchecked (No) or Checked (Yes) Default: Unchecked (No)
	Policy SBR Sessions Threshold Exceeded	
* Alarm Name	This alarm is raised when the number of concurrent Policy SBR sessions exceeds the configured threshold.	Format: Non-editable text box Range: Policy SBR Sessions Threshold Exceeded
* Critical Alarm Threshold (Percent)	The concurrent sessions threshold for this alarm to be raised as Critical. The threshold is a percentage of the Maximum Policy SBR Sessions.	Format: Text box Range: 1-99 Default: 95
Suppress Critical	Controls whether this alarm is raised as Critical.	Format: Check box Range: Unchecked (No) or Checked (Yes) Default: Unchecked (No)
* Major Alarm Threshold (Percent)	The concurrent sessions threshold for this alarm to be raised as Major. The threshold is a percentage of the Maximum Policy SBR Sessions.	Format: Text box Range: 1-99 Default: 90
Suppress Major	Controls whether this alarm is raised as Major.	Format: Check box Range: Unchecked (No) or Checked (Yes) Default: Unchecked (No)
* Minor Alarm Threshold (Percent)	The concurrent sessions threshold for this alarm to be raised as Minor. The threshold is a percentage of the Maximum Policy SBR Sessions.	Format: Text box Range: 1-99 Default: 80

Elements (* indicates required field)	Description	Data Input Notes
Suppress Minor	Controls whether this alarm is raised as Minor.	Format: Check box Range: Unchecked (No) or Checked (Yes) Default: Unchecked (No)
Policy SBR Bindings Threshold Exceeded		
* Alarm Name	This alarm is raised when the number of concurrent Policy SBR bindings exceeds the configured threshold.	Format: Non-editable text box Range: Policy SBR Bindings Threshold Exceeded
* Critical Alarm Threshold (Percent)	The concurrent bindings threshold for this alarm to be raised as Critical. The threshold is a percentage of the Maximum Policy SBR Bindings.	Format: Text box Range: 1-99 Default: 95
Suppress Critical	Controls whether this alarm is raised as Critical.	Format: Check box Range: Unchecked (No) or Checked (Yes) Default: Unchecked (No)
* Major Alarm Threshold (Percent)	The concurrent bindings threshold for this alarm to be raised as Major. The threshold is a percentage of the Maximum Policy SBR Bindings.	Format: Text box Range: 1-99 Default: 90
Suppress Major	Controls whether this alarm is raised as Major.	Format: Check box Range: Unchecked (No) or Checked (Yes) Default: Unchecked (No)
* Minor Alarm Threshold (Percent)	Te concurrent bindings threshold for this alarm to be raised as Minor. The threshold is a percentage of the Maximum Policy SBR Bindings.	Format: Text box Range: 1-99 Default: 80
Suppress Minor	Controls whether this alarm is raised as Minor.	Format: Check box Range: Unchecked (No) or Checked (Yes)

Elements (* indicates required field)	Description	Data Input Notes
		Default: Unchecked (No)

Viewing Alarm Settings

Use this task to view configured Alarm-Settings on either the NOAM or SOAM.

Select **Policy DRA** ➤ **Configuration** ➤ **Alarm Settings**.

The **Policy DRA** > **Configuration** > **Alarm Settings** page appears with a list of configured Alarm Settings.

The fields are described in *Alarm Settings elements*.

Defining Alarm Settings

Use this task to define Alarm Settings on an Active NOAM.

Note: Alarm Settings are configurable only on Active NOAM servers, and are viewable on NOAM and SOAM servers.

The fields are described in *Alarm Settings elements*.

1. Select **Policy DRA** ➤ **Configuration** ➤ **Alarm Settings**.

   The **Policy DRA** > **Configuration** > **Alarm Settings** page appears.
2. Enter values in the editable fields to define the alarm settings.
3. Click:

   - **Apply** to save the changes and remain on this page.
   - **Cancel** to discard the changes and remain on the **Policy DRA** > **Configuration** > **Alarm Settings** page.

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

   - The entered values contain the wrong data type or is out of the allowed range.
   - The value entered for **Critical Alarm Threshold (Percent)** is less than or equal to the value entered for **Major Alarm Threshold (Percent)**.
   - The value entered for **Major Alarm Threshold (Percent)** is less than or equal to the value entered for **Minor Alarm Threshold (Percent)**.

Congestion Options

Congestion Options are configurable on Active NOAM servers.

The following Congestion Options can be configured:

- Alarm Thresholds, which are used to:
  - Set the percentage of the Policy DRA ingress message rate capacity at which an alarm is raised with Critical, Major, or Minor severity.

- Set the percentage of the Policy DRA ingress message rate capacity at which a Critical, Major, or Minor severity alarm is cleared.

  The percentages control the onset and abatement of the corresponding Congestion Levels.

  Default thresholds are based n the engineered system value for Ingress Policy DRA Request Message Capacity.

- Message Throttling Rules, which determine the percentage of Session Creation, Update, and Terminate Request messages that are discarded when Congestion Levels 1, 2, and 3 exist.

The fields are described in *Congestion Options elements*.

Congestion Options elements

Table 17: Congestion Options elements describes the elements on the **Policy DRA > Configuration > Congestion Options** page. The elements can be configured and viewed on the NOAM.

The page contains two sets of input fields:

- Alarm Thresholds
- Message Throttling Rules

Table 17: Congestion Options elements

Fields (* indicates required field)	Description	Data Input Notes
	Alarm Thresholds	
Alarm Name	The Policy DRA Server in Congestion alarm is raised hen average Policy DRA ingress request messages rate exceeds the configured threshold. The thresholds are based on the engineered system value for Ingress Pdra Request Message Capacity.	Format: Non-editable text box Range: Policy DRA Server in Congestion
* Critical Alarm Onset Threshold	Percentage of Policy DRA Ingress Request Message Rate capacity at which this alarm gets raised with Critical severity. This implies that the system is at Congestion Level 3.	Format: Text box Range: 100-200 Default: 160
* Critical Alarm Abatement Threshold	Percentage of Policy DRA Ingress Request Message Rate capacity at which this alarm with Critical severity is cleared. This implies that the system has come out of Congestion Level 3.	Format: Text box Range: 100-200 Default: 150
* Major Alarm Onset Threshold	Percentage of Policy DRA Ingress Request Message Rate capacity at which this alarm gets raised with Critical severity. This implies that the system is at Congestion Level 2.	Format: Text box Range: 100-200 Default: 140

Fields (* indicates required field)	Description	Data Input Notes
* Major Alarm Abatement Threshold	Percentage of Policy DRA Ingress Request Message Rate capacity at which this alarm with Critical severity is cleared. This implies that the system has come out of Congestion Level 2.	Format: Text box Range: 100-200 Default: 130
* Minor Alarm Onset Threshold	Percentage of Policy DRA Ingress Request Message Rate capacity at which this alarm gets raised with Critical severity. This implies that the system is at Congestion Level 1.	Format: Text box Range: 100-200 Default: 110
* Minor Alarm Abatement Threshold	Percentage of Policy DRA Ingress Request Message Rate capacity at which this alarm with Critical severity is cleared. This implies that the system has come out of Congestion Level 1.	Format: Text box Range: 100-200 Default: 100
Mesage Throttling Rules Tabs for Congestion Level 1, Congestion Level 2, and Congestion Level 3		
* Discard Session Creation Requests	Percentage of Request messages that result in new session creation, to be discarded when this congestion level exists.	Format: Text box Range: 0-100 Default: Level 1 - 25 Level 2 - 50 Level 3 - 100
* Discard Session Update Requests	Percentage of Request messages that result in updating existing sessions, to be discarded when this congestion level exists.	Format: Text box Range: 0-100 Default: Level 1 - 0 Level 2 - 25 Level 3 - 50
* Discard Session Terminate Requests	Percentage of Request messages that result in terminating existing sessions, to be discarded when this congestion level exists.	Format: Text box Range: 0-100 Default: Level 1 - 0 Level 2 - 0 Level 3 - 0

Viewing Congestion Options

Use this task to view configured Congestion Options on the NOAM.

Select **Policy DRA** ➤ **Configuration** ➤ **Congestion Options**.

The **Policy DRA** > **Configuration** > **Congestion Options** page appears with a list of configured Congestion Options.

The fields are described in *Congestion Options elements*.

Setting Congestion Options

Use this task to set the following Congestion Options on the Active NOAM:

- **Alarm Thresholds** for the **Policy DRA Server in Congestion** onset and abatement alarm for Critical, Major, and Minor severities
- **Message Throttling Rules** for discarding Session Creation, Update, and Terminate Requests for Congestion Levels 1, 2, and 3

1. Select **Policy DRA** ➤ **Configuration** ➤ **Congestion Options**.

   The **Policy DRA** > **Configuration** > **Congestion Options** page appears.
2. Enter changes for the **Alarm Thresholds.**
3. Enter changes for the **Message Throttling Rules**.
4. Click:

   - **Apply** to save the Congestion Options changes and refresh the page to show the changes.
   - **Cancel** to discard the changes and refresh the page.

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

   - Any fields contain a value that contains invalid characters or is out of the allowed range.
   - Any required field is empty (not entered).
   - A **Major Alarm Onset Threshold** value is greater than the corresponding **Critical Alarm Onset Threshold.**
   - A **Minor Alarm Onset Threshold** value is greater than the corresponding **Major Alarm Onset Threshold.**
   - An **Alarm Abatement Threshold** value is greater than the corresponding **Alarm Onset Threshold** of a particular severity.

PCRFs

The **Policy DRA** > **Configuration** > **PCRFs** page contains the list of PCRF Peer Nodes that are to be used when a new subscriber binding is created at this site. New bindings created at this Policy DRA DSR are distributed evenly among the configured PCRFs.

PCRFs are responsible for authorizing and making policy decisions based on knowledge of subscriber resource usage and the capabilities allowed by the subscriber's account. All policy requests for a given subscriber must be routed to the same PCRF. The Policy DRA dynamically assigns subscribers to PCRFs using a load distribution algorithm, and maintains state about which subscribers are assigned to which PCRF. The relationship between a subscriber and a PCRF can change any time the subscriber transitions from having no Diameter policy sessions to having one or more Diameter policy sessions. After a policy session exists, all policy sessions for that subscriber are routed to the assigned PCRF.

The fields are described in *PCRFs elements*.

Note: For details about configuring Peer Nodes, refer to the *Diameter and Mediation User Guide* and Diameter online help.

On the **Policy DRA > Configuration > PCRFs** page on the SOAM, you can perform the following actions:

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

  The **Policy DRA > Configuration > PCRFs [Insert]** page opens. You can add a PCRF. See *Inserting PCRFs*. If the maximum number of PCRFs (2500) already exists in the system, the **Policy DRA > Configuration > PCRFs [Insert]** page will not open, and an error message is displayed.

- Select a PCRF in the list, and click the **Edit** button.

  The **Policy DRA > Configuration > PCRFs [Edit]** page opens. You can edit the selected PCRF. See *Editing PCRFs*.

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

PCRFs elements

Table 18: PCRFs page elements describes the elements on the **Policy DRA > Configuration PCRFs** page. Data Input Notes apply to the Insert and Edit pages; the View page is read-only.

Table 18: PCRFs page elements

Fields (* indicates required field)	Description	Data Input Notes
* PCRF Peer Node Name	The name of a configured Diameter Peer Node that identifies the PCRF Peer Node to be included in the round-robin load distribution of new bindings to PCRFs. Selecting a PCRF Peer Node name (blue hyperlink) displays the **Diameter > Configuration > Peer Nodes (Filtered)** page where Diameter Peer Nodes are filtered by the PCRF Peer Node Name.	Format: List Range: Configured Diameter Peer Nodes **Note:** The PCRF Peer Node Name cannot be changed on the [Edit] page.
Comment	An optional comment to describe the PCRF Peer Node.	Format: Text box Range:0-64 characters

Viewing PCRFs

Use this task to view all configured PCRFs on the SOAM.

Select **Policy DRA** ➤ **Configuration** ➤ **PCRFs**.

The **Policy DRA** > **Configuration** > **PCRFs** page appears with a list of configured PCRF Peer Nodes.

The fields are described in *PCRFs elements*.

Inserting PCRFs

Use this task to insert (create new) PCRFs.

The fields are described in *PCRFs elements*.

1. On the Active SOAM, select **Policy DRA** ➤ **Configuration** ➤ **PCRFs**.

   The **Policy DRA** > **Configuration** > **PCRFs** page appears.
2. Click **Insert**.

   The **Policy DRA** > **Configuration** > **PCRFs [Insert]** page opens.
3. Enter a unique PCRF Peer Node Name in the **PCRF Peer Node Name** field.

   This name uniquely identifies the PCRF Peer Node to be included in the round-robin load distribution of new bindings to PCRFs.
4. Enter an optional comment in the **Comments** field.
5. Click:

   - **OK** to save the new PCRF and return to the **Policy DRA** > **Configuration** > **PCRFs** page.
   - **Apply** to save the new PCRF and remain on this page.
   - **Cancel** to return to the **Policy DRA** > **Configuration** > **PCRFs** page without saving any changes.

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

   - The entered PCRF is not unique (already exists).
   - Any fields contain a value that contains invalid characters or is out of the allowed range.
   - Any required field is empty (not entered).
   - Adding the new PCRF would cause the maximum number of PCRFs (2500) to be exceeded.

Editing PCRFs

Use this task to edit PCRF Comments.

Note: The PCRF Peer Node Name cannot be edited.

1. On the Active SOAM, select **Policy DRA** ➤ **Configuration** ➤ **PCRFs**.

   The **Policy DRA** > **Configuration** > **PCRFs** page appears. The page displays a list of the configured PCRF Peer Nodes that are used when a new subscriber binding is created.
2. Click in the **Comments** field of the row to select the PCRF to edit.

DO NOT click the blue PCRF Peer Node Name (unless you want to see the configuration of the Peer Node). The blue color indicates a hyper-link that opens the **Diameter > Configuration > Peer Nodes [Filtered]** page to display the configuration information for the Peer Node.

3. Edit the **Comments** field for the selected PCRF.

   The PCRF Peer Node name cannot be changed.
4. Click:
   - **OK** to save the change and return to the **Policy DRA > Configuration > PCRFs** page.
   - **Apply** to save the change and remain on this page.
   - **Cancel** to return to the **Policy DRA > Configuration > PCRFs** page without saving any changes.

   If **Apply** or **OK** is clicked and the selected **PCRF Peer Node Name** entry no longer exists (was deleted by another user), an error message appears.

Deleting a PCRF

Use the following procedure to delete a PCRF.

1. Select **Policy DRA** ➤ **Configuration** ➤ **PCRFs**.

   The **Policy DRA > Configuration > PCRFs** page appears.
2. Select the **PCRF** to be deleted.
3. Click the **Delete** button.

   A popup window appears to confirm the delete.
4. Click:
   - **OK** to delete the PCRF.
   - **Cancel** to cancel the delete function and return to the **Policy DRA > Configuration > PCRFs** page.

   If **OK** is clicked and the selected PCRF no longer exists (it was deleted by another user), an error message is displayed and the PCRFs page is refreshed. The row that was selected is no longer displayed in the list.

Binding Key Priority

The Binding Key Priority defines search priorities for Alternative Keys that can be used to locate a subscriber binding.

The Binding Key Priority controls:

- Which keys are stored for binding correlation
- The order in which keys are searched for purposes of binding correlation

The priority determines the order used to find a binding for subsequent sessions. Alternative Keys with an assigned priority will be created with the binding if they are present in the session initiation message that created the binding. The Alternative Keys must be assigned a priority in order to be used to locate subscriber bindings. If any Alternative Keys are not assigned a priority, they will not be used to locate subscriber bindings even if the Alternative Key is present in the session initiation message.

The fields are described in *Binding Key Priority elements*.

On the **Policy DRA > Configuration > Binding Key Priority** page on the Active SOAM, you can change the Binding Key Type for Binding Key Priority 2, 3, and 4.

Note: Priority 1 for Binding Key Type IMSI is the highest priority and cannot be modified.

Binding Key Priority elements

Table 19: Binding Key Priority elements describes the elements on the **Policy DRA > Configuration > Binding Key Priority** page.

Table 19: Binding Key Priority elements

Field (* indicates a requried field)	Description	Data Input Notes
* Binding Key Type	The Binding Key Type which is assigned to a Binding Key Priority. **Note:** The first row is Priority 1 and the corresponding Binding Key Type is IMSI. This row is read-only.	Format: Pulldown list Range: MSISDN, IPv4, or IPv6 for Priority 2, 3, and 4 Default: -Select- (No Binding Key Type selected)

Viewing Binding Key Priority

Use this task to view configured Binding Key Priority settings on the SOAM.

Select **Policy DRA ➤ Configuration ➤ Binding Key Priority**.

The **Policy DRA > Configuration > Binding Key Priority** page appears with a list of configured Binding Key Priority settings.

The fields are described in *Binding Key Priority elements*.

Setting Binding Key Priority

Use this task to set Binding Key Priority values.

The fields are described in *Binding Key Priority elements*.

1. On the Active SOAM, select **Policy DRA ➤ Configuration ➤ Binding Key Priority**. The **Policy DRA > Configuration > Binding Key Priority** page appears.
2. Make Binding Key Type selections for Priority 2 - 4 as needed. Priority 1 is non-editable (it is the Anchor Key and is always IMSI).
3. Click:

   - **Apply** to save the selected Binding Key Type values and remain on this page.
   - **Cancel** to remain on the **Policy DRA > Configuration > Binding Key Priority** page without saving any changes.

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

- A Binding Key Priority Type is selected for more than one Priority
- Binding Key Types are not selected for consecutive Priority values

Topology Hiding

Use the **Policy DRA > Configuration > Topology Hiding** page to define the list of Policy Client Peer Nodes from which the PCRF name is to be hidden. This page can be used only if Topology Hiding is **Enabled** and the **Topology Hiding Scope** option is either **Specific Hosts** or **All Foreign Realms + Specific Hosts** on the **Policy DRA > Configuration > Site Options** page. See *Site Options*.

The fields are described in *Topology Hiding elements*.

On the **Policy DRA > Configuration > Topology Hiding** page, you can:

- Filter the list of Policy Client Peer Node Names, to display only the desired Policy Client Peer Node Names.
- Sort the list entries in ascending or descending order by Policy Client Peer Node Names or by Comments, by clicking the column heading. By default, the list is sorted by Policy Client Peer Node Names in ascending numerical order.
- Click the **Insert** button.

  The **Policy DRA > Configuration > Topology Hiding [Insert]** page opens. You can add a Policy Client Peer Node Name and Comment. See *Adding a new Policy Client for Topology Hiding*. If the maximum number of Policy Client Peer Nodes (1000) already exists in the system, the **Policy DRA > Configuration > Topology Hiding [Insert]** page will not open, and an error message is displayed.
- Select the **Comment** cell in the row for a Policy Client Peer Node Name in the list, and click the **Edit** button. (Clicking the blue **Policy Client Peer Node Nam**e will open the filtered **Diameter > Configuration > Peer Nodes** page for the Peer Node.)

  The **Policy DRA > Configuration > Topology Hiding [Edit]** page opens. You can edit the **Comment** for the selected **Policy Client Peer Node Name**. (The Policy Client Peer Node Name cannot be changed.)
- Select the **Comment** in the row for a Policy Client Peer Node Name in the list, and click the **Delete** button to remove the selected **Policy Client Peer Node Name**. See *Deleting a Topology Hiding Policy Client Peer Node*.

Topology Hiding elements

Table 20: Topology Hiding elements describes the elements on the **Policy DRA > Configuration > Topology Hiding** page. Data Input Notes apply to the Insert and Edit pages; the View page is read-only.

Table 20: Topology Hiding elements

Elements	Description	Data Input Notes
Policy Client Peer Node Name	The name of a configured Diameter Peer Node that identifies a Policy Client Peer Node. Selecting a Policy Client Peer Node name (blue hyperlink) displays the **Diameter > Configuration > Peer Nodes (Filtered)** page where Diameter	Format: Pulldown list **Note:** The Policy Client Peer Node Name cannot be changed on the [Edit] page.

Elements	Description	Data Input Notes
	Peer Nodes are filtered by the Policy Client Peer Node Name.	Range: Configured Diameter Peer Nodes
Comments	An optional comment that describes the Policy Client Peer Node.	Format: Text box Range 0-64 characters

Viewing Topology Hiding

Use this task to view all configured Topology Hiding settings on the SOAM.

Select **Policy DRA** ➤ **Configuration** ➤ **Topology Hiding**.

The **Policy DRA > Configuration > Topology Hiding** page appears.

The fields are described in *Topology Hiding elements*.

Adding a new Policy Client for Topology Hiding

Use this task to add a new Policy Client for Topology Hiding.

Note: Topology Hiding is performed only if it is Enabled and the Topology Hiding **Scope** option is defined as **Specific Host**s or **All Foreign Realms + Specific Hosts** in the Policy DRA > Configuration > **Site Options** page.

The fields are described in *Topology Hiding elements*.

1. On the Active SOAM, select **Policy DRA** ➤ **Configuration** ➤ **Topology Hiding**.

   The **Policy DRA > Configuration > Topology Hiding** page appears.
2. Click **Insert**.

   The **Policy DRA > Configuration > Topology Hiding [Insert]** page appears.
3. Select a Policy Client Peer Node Name from the **Value** pulldown list.
4. Enter an optional comment in the **Comments** field.
5. Click:

   - **OK** to save the changes and return to the **Policy DRA > Configuration > Topology Hiding** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the Policy DRA **Policy DRA > Configuration > Topology Hiding** page without saving any changes.

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

   - The entered comment exceeds 64 characters in length or contains something other than 7-bit ASCII characters.
   - The **Policy Client Peer Node Name** is missing.
   - The selected **Policy Peer Node Name** is already configured in the system.
   - Any fields contain invalid input (for example, the wrong type of data was entered or a value is out of range).

- The maximum number (1000) of **Topology Hiding** records has already been configured.

Editing Topology Hiding

Use this task to edit a Policy Client for Topology Hiding.

Note: Topology Hiding is performed only if it is also activated and the Topology Hiding **Scope** option is defined as **Specific Hosts** or **All Foreign Realms + Specific Hosts** in the Policy DRA > Configuration > **Site Options** page.

The fields are described in *Topology Hiding elements*.

1. On the Active SOAM, select **Policy DRA** ➤ **Configuration** ➤ **Topology Hiding**.

   The **Policy DRA > Configuration > Topology Hiding** page appears.
2. Click **Edit**.

   The **Policy DRA > Configuration > Topology Hiding [Edit]** page appears.

   A read-only value is displayed in the Policy Client Peer Node Name **Value** field.
3. Edit or enter an optional comment in the **Comments** field.
4. Click:

   - **OK** to save the edited Comment and return to the **Policy DRA > Configuration > Topology Hiding** page.
   - **Apply** to save the edited Comment and remain on this page.
   - **Cancel** to return to the **Policy DRA > Configuration > Topology Hiding** page without saving any changes.

   If **OK** or **Apply** is clicked and the following condition exists, an error message appears:

   - The selected Policy Client Code Name no longer exists (for example, it has been deleted by another user), and no changes are made to the database.

Deleting a Topology Hiding Policy Client Peer Node

Use the following procedure to delete a Topology Hiding Policy Client Peer Node.

1. Select **Policy DRA** ➤ **Configuration** ➤ **Topology Hiding**.

   The **Policy DRA > Configuration > Topology Hiding** page appears.
2. Select the Comment in the line for a Policy Client Peer Node Name to be deleted. (Clicking the blue Policy Client Peer Node Name will open the filtered **Diameter > Configuration > Peer Nodes** page for the Peer Node.)
3. Click the **Delete** button.

   A popup window appears to confirm the delete.
4. Click:

   - **OK** to delete the Policy Client Peer Node Name.
   - Click **Cancel** to cancel the delete function and return to the **Policy DRA > Configuration > Topology Hiding** page.

If **OK** is clicked and the selected Policy Client Peer Node no longer exists (it was deleted by another user), an error message is displayed and the **Policy DRA > Configuration > Topology Hiding** page is refreshed. The row that was selected is no longer displayed in the list.

Site Options

The Policy DRA Site Options apply independently to each Policy DRA site. The following Site Options can be configured on **P-DRA > Configuration > Site Options page on** the active SOAM server:

- Policy DRA Mate DSR Name - the name of the configured Diameter Peer Node that is the Mate DSR node to which binding capable session initialization messages are routed if no local PCRFs are configured.
- Topology Hiding Options - Enable/Disable, Scope, FQDN, and Realm. See *Site Options elements*
- Peer Route Table Name - The name of the configured Diameter Peer Route Table that contains the Peer Routing Rules to be used for routing new binding Requests.
- Ingress Message Capacity (read only) - Ingress message capacity for a single MP server; the value is the same as the **Engineered Ingress MPS** value in the Session **MP Profile** assigned for the blade type on which the Policy DRA application is running

The fields are described in *Site Options elements*.

Site Options elements

Table 21: Site Options elements describes the elements on the SOAM **Policy DRA > Configuration > Site Options** page. Data Input Notes apply to the Insert and Edit pages; the View page is read-only.

Table 21: Site Options elements

Field (* indicates field is required)	Descriptions	Data Input Notes
* Policy DRA Mate DSR Name	The name of the configured Diameter Peer Node that is the Mate DSR node to which binding capable session initialization messages are routed if no local PCRFs are configured.	Format: Pulldown list Range: Configured Diameter Peer Nodes Default: No Mate
Topology Hiding Options	**Enabled** Check or uncheck the box to **Enable** (checked) or **Disable** (unchecked) Topology Hiding. When the box is checked, select the **Scope** and enter **FQDN** and **Realm** that apply for Topology Hiding.	Format: Check box Range: Checked (Enabled), Unchecked (Disabled) Default: Unchecked (Disabled)

Field (* indicates field is required)	Descriptions	Data Input Notes
	Scope The scope of messages where Topology Hiding will be applied.	Format: Pulldown list Range: • All Messages -Perform Topology Hiding for all messages destined for Policy Clients. • All Foreign Realms - Perform Topology Hiding if the Realm of the Policy Client is different from the Realm of the PCRF that originated the message. • Specific Hosts - Perform Topology Hiding only if the Policy Client is configured on the **Policy DRA > Configuration > Topology Hiding** page. • All Foreign Realms +Specific Hosts - Perform Topology Hiding if either the 'All Foreign Realms' or 'Specific Hosts' condition is met.
	FQDN Value used to populate the Diameter Origin-Host AVP for Answer messages routed from a PCRF to a Policy Client, or the Diameter Destination-Host AVP for Request messages routed from a PCRF to a Policy Client.	Format: Text box Range: 1 - 255 characters. Valid characters are letters, digits, dots (.), and hyphens (-). At least one alpha character is required.
	Realm Value used to populate the Origin-Realm AVP for Answer messages routed from a PCRF to a policy client, or the Diameter Destination-Realm AVP for Request messages routed from a PCRF to a Policy Client.	Format: Text box Range: 1 - 255 characters. Valid characters are letters, digits, dots (.), and hyphens (-). At least one alpha character is required.

Field (* indicates field is required)	Descriptions	Data Input Notes
Peer Route Table Name	The name of the Diameter Peer Route Table to be used for routing new binding requests. The Default PRT is always available, but must be selected from the list to be used.	Format: Pulldown list Range: Not Selected, Default, configured Diameter Peer Route Tables Default: Not Selected

Table 22: Topology Hiding Scope Configuration shows the available Topology Hiding settings and corresponding results.

Note: Topology Hiding must be performed at the originating P-DRA.

Table 22: Topology Hiding Scope Configuration

Topology Hiding System Setting	Topology Hiding Scope Setting	Result
Disabled	N/A	No Topology Hiding is performed
Enabled	Specific Hosts	Topology Hiding is performed for messages for the Policy Clients only if the Policy Clients' FQDNs are configured for Topology Hiding.
	All Foreign Realms	Topology Hiding is performed for messages for the Policy Clients if the Realms of the Policy Clients are different from the Realm of the PCRF that sends the messages.
	All Foreign Realms + Specific Hosts	Superset of All Foreign Realms
	All	Topology Hiding is performed for all messages to all Policy Clients

Viewing Site Options

Use this task to view all configured Site Options on an SOAM.

Select **Policy DRA** ➤ **Configuration** ➤ **Site Options**.

The **Policy DRA > Configuration > Site Options** page appears with a list of configured Site Options.

The fields are described in *Site Options elements*.

Setting Site Options

Use this task to set Site Options on the Active SOAM server.

The fields are described in *Site Options elements*.

Note: The **Ingress Message Capacity** field is read-only; it cannot be changed.

1. Select **Policy DRA** ➤ **Configuration** ➤ **Site Options**.

   The **Policy DRA** > **Configuration** > **Site Options** page appears.
2. Select a mate DSR Peer Node from the **Policy DRA Mate DSR Peer Node Name** pulldown list.

   This defines the Peer Node to which binding capable session initiating messages are routed if no local PCRFs are configured.
3. Check the Topology Hiding Options **Enabled** check box to enable or disable Topology Hiding.

   Note: If Enabled, select the **Scope**, **FDQN** and **Realm** to apply topology hiding.
4. If the Topology Hiding Options **Enabled** box is checked, enter or select the **Scope**, **FDQN**, and **Realm** values to apply for Topology Hiding.
5. Select a Peer Route Table from the **Peer Route Table Name** pulldown list.
   This identifies the Peer Route Table that contains the Peer Routing Rules that are used for routing new binding Requests.
6. Click:

   - **Apply** to save the changes and refresh this page.
   - **Cancel** to discard the changes and remain on the **Policy DRA** > **Configuration** > **Site Options** page.

   If **Apply** is clicked and any entered value contains the wrong data type or is out of the allowed range, an error message appears.

Error Codes

For each Policy DRA Site, the Diameter Error Result Code value to send to the Request initiator for policy related errors can be configured according to which condition applies. Each condition can be mapped to a different Result Code for each supported interface. Result Codes can be Diameter IANA defined or experimental.

Table 23: Policy DRA Error Conditions

Error Conditions	Description	Applies to
P-DRA Unavailable Or Degraded	Returned if 1) The Policy DRA application Operational Status=Unavailable due to disabling the application on the **Diameter > Maintenance > Applications** GUI page (Admin State=Disabled), or 2) The Policy DRA application is in a Degraded stat due to congestion	Gx, Gxx, Rx, S9 messages

Error Conditions	Description	Applies to
Binding Not Found	Returned if an Rx session is created or updated with an AAR message and the Binding Key in the Rx message cannot be found in the database	Rx sessions only
Binding Found, But Unable To Route	Returned if a binding is found or created and the Policy DRA is unable to route the message to the PCRF	Gx, Gxx, Rx, S9 session creation messages (CCR-I and AAR)
Policy SBR Error	Returned if the Policy DRA receives an unexpected error while executing a database operation such as a lookup, insertion, or deletion of records	Gx, Gxx, Rx, S9 messages
No Usable Keys In Binding Dependent Message	Returned if an AAR message does not contain any keys that match the keys configured in the **Policy DRA > Configuration > Binding Key Priority** GUI page	Rx sessions only
Session Not Found	Returned if the Policy DRA is unable to find a session record matching the in-session message	In-session Gx, Gxx, Rx, S9 messages, only when Topology Hiding applies to the message

On the **Policy DRA > Configuration > Error Codes** page on the SOAM, you can perform the following action:

- Select an **Error Condition** in the list, and click the **Edit** button.

  The **Policy DRA > Configuration > Error Codes [Edit]** page opens. You can edit the selected Error Code. See *Editing Error Codes*.

The fields are described in *Error Codes elements*.

Error Codes elements

Table 25: Error Codes elements describes the elements on the **Policy DRA > Configuration > Error Codes** pages. Data Input Notes apply to the [Edit] page; the View page is read-only.

The Error Codes define the Result Codes to be returned for various Policy DRA Error Conditions. Each Error Condition will return the Result Code configured for each applicable Diameter interface.

Table 24: Interfaces Supported for Each Error Code indicates the Diameter interfaces that are supported for each Error Code.

The default Result Code is 3002-DIAMETER_UNABLE_TO_DELIVER.

Table 24: Interfaces Supported for Each Error Code

Error Code	Result Code	Experimental Code	Vendor ID
Policy DRA Unavailable Or Degraded	Gx/Gxx, Rx, S9	Gx/Gxx, Rx, S9	Gx/Gxx, Rx, S9

Error Code	Result Code	Experimental Code	Vendor ID
Binding Not Found	Rx	Rx	Rx
Binding Found, But Unable To Route	Gx/Gxx, Rx, S9	Gx/Gxx, Rx, S9	Gx/Gxx, Rx, S9
Policy SBR Error	Gx/Gxx, Rx, S9	Gx/Gxx, Rx, S9	Gx/Gxx, Rx, S9
No Usable Keys In Binding Dependent Message	Rx	Rx	Rx
Session Not Found	Gx/Gxx, Rx, S9	Gx/Gxx, Rx, S9	Gx/Gxx, Rx, S9

Table 25: Error Codes elements

Fields (* indicates required field)	Description	Data Input Notes
Error Condition	The name of the selected Policy DRA Error Condition.	View only; cannot be edited
* Gx/Gxx Result Code	The Result Code to be returned on the Gx and Gxx interfaces.	Format: Text box Range: 1-9999 Default: 3002
Gx/Gxx Experimental Code	Defines the Gx/Gxx Result Code as experimental. Experimental codes require a corresponding Vendor ID.	Format: Check box Range: Yes (checked), (No) unchecked Default: No (unchecked)
Gx/Gxx Vendor ID	The Vendor ID that corresponds with the Experimental Code for the Gx and Gxx interfaces. The Vendor ID '---' means the RFC standard error code will be sent.	Format: Text box Range: 1-4294967295
* Rx Result Code	The Result Code to be returned to the Rx interface.	Format: Text box Range: 1-9999 Default: 3002
Rx Experimental Code	Defines the Rx Result Code as experimental. Experimental Codes require a corresponding Vendor ID.	Format: Check box Range: Yes (checked), (No) unchecked Default: No (unchecked)

Fields (* indicates required field)	Description	Data Input Notes
Rx Vendor ID	The Vendor ID that corresponds with the Experimental Code for the Rx interface. The Vendor ID '---' means the RFC standard error code will be sent.	Format: Text box Range: 1-4294967295
* S9 Result Code	The Result Code to be returned to the S9 interface.	Format: Text box Range: 1-9999 Default: 3002
S9 Experimental Code	Defines the S9 Result Code as experimental. Experimental Codes require a corresponding Vendor ID.	Format: Check box Range: Yes (checked), (No) unchecked Default: No (unchecked)
S9 Vendor ID	The Vendor ID that corresponds with the Experimental Code for the S9 interface. The Vendor ID '---' means the RFC standard error code will be sent.	Format: Text box Range: 1-4294967295

Viewing Error Codes

Use this task to view configured Error Codes on the SOAM.

Select **Policy DRA ➤ Configuration ➤ Error Codes**.

The **Policy DRA > Configuration > Error Codes** page appears with a list of configured Error Codes. The fields are described in *Error Codes elements*.

Editing Error Codes

Use this task to edit Error Codes on the Active SOAM.

The fields are described in *Error Codes elements*.

1. Select **Policy DRA ➤ Configuration ➤ Error Codes**.

   The **Policy DRA > Configuration > Error Codes** page appears
2. Select the **Error Condition** that you want to edit.
3. Click **Edit**.

   The **Policy DRA > Configuration > Error Codes [Edit]** page opens

   The fields that appear on the **Policy DRA > Configuration > Error Codes [Edit]** page are dependent on the Error Condition that was selected.
4. Edit the fields to define the selected Error Condition.
5. Click:

- **Ok** to save the changes and return to the **Policy DRA > Configuration > Error Codes** page
- **Apply** to save the changes and remain on this page
- **Cancel** to discard the changes and return to the **Policy DRA > Configuration > Error Codes** page

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

- Any required field value is missing (not entered or selected)
- Any fields contain invalid input (for example, the wrong type of data was entered or a value is out of range).

Post-Configuration Activities

After Policy DRA configuration is complete, the following activities need to be performed to make the Policy DRA application fully operational in the system:

- Enable the Policy DRA application
- Enable Diameter Connections with Peer Nodes
- Status Verification

Enable the Policy DRA Application

Use this task to enable the Policy DRA application. For each Active SOAM,

1. Select **Diameter ➤ Maintenance ➤ Applications**.

   The **Diameter > Maintenance > Applications** page appears.
2. Under **DSR Application Name**, select each **PDRA** row.

   To select more than one row, press and hold **Ctrl** while you click each row.
3. Click **Enable**.
4. Verify the application status on the page.

   The **Admin State**, **Operational Status**, **Operational Reason**, and **Congestion Level** in each of the selected rows should change respectively to **Enabled**, **Available**, **Normal**, **Normal**.

Enable Connections

Use the following task to enable one or more connections to Peer Nodes.

1. At the Active SOAM, select **Diameter ➤ Maintenance ➤ Connections**.
   The **Diameter > Maintenance > Connections** page appears.
2. Select 1 - 20 connections to enable.

   To select multiple connections, press and hold the Ctrl key while you select each connection.

   To select multiple contiguous connections, click the first connection you want, press and hold the Shift key, and select the last connection you want. All the connections between are also selected.
3. Click **Enable**.

A confirmation box appears.

4. Click **OK**.
   The selected connections are enabled.

   If any of the selected connections no longer exist (they have been deleted by another user), an error message is displayed, but any selected connections that do exist are enabled.

5. Verify Connection status on the page.

   Verify that the **Admin State** of all connections changes to Enabled and the Operational Reason shows Connecting for connections to PCRF nodes and Listening for connections to other nodes (such as policy clients - PCEF, AF, and others). nodes.

   For connections of type Responder Only (Policy Client nodes), the **Operational Status** and **Operational Reason** will be "Unk" if IPFE TSA connections are used.

Status Verification

Use the following task to verify Policy DRA and Policy SBR status after configuration is complete.

1. Verify Communication Agent (ComAgent) HA Services Status.
   a) At the Active NOAM, select **Communication Agent ➤ Maintenance ➤ Connection Status**.
   b) Verify that **Resource Routing Status** is **Available** for all listed **User/Provider** entries.
2. Verify the ComAgent Automatic Connection Status.
   a) At the Active NOAM, select **Communication Agent ➤ Maintenance ➤ Ha Services Status**
   b) Verify that **Automatic Connection Count** is **X of Y In Service**, where Y >= X and X = Y indicate successful Automatic Connection setup.
3. Verify Policy SBR Status.
   a) At the Active NOAM, select **Policy DRA ➤ Maintenance ➤ Policy SBR Status**.
   b) Verify that the server **Resource HA Role** is **Active/Standby/Spare** and **Congestion Level** is **Normal** for all Servers in each Server Group in the Binding Region and Mated Site tab entries.

DSR Bulk Export

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

Exported CSV Files

Each exported CSV file contains one or more records for the configuration data that was selected for the Export operation.

CSV file formats and procedures for using Bulk Export operations are in the Diameter Configuration Bulk Import Help and in the *Diameter and Mediation User Guide*.

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

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

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

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

- All exportable configuration data in the system
- All exportable configuration data from the selected Export Application
- Exportable configuration data from a selected configuration component for the selected Export Application

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

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

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

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

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

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

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

Export Operations

Exported files can be written to the File Management Directory in the Status & Manage File Management area (see the **Status &Manage Files** page) or to the Export Server Directory.

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

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

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

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

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

Export Results

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

DSR Bulk Import

The DSR Bulk Import operations use configuration data in ASCII Comma-Separated Values (CSV) files (.csv), to insert new data into, update existing data in, or delete existing data from the Diameter Configuration or DSR Applications (FABR, RBAR, P-DRA, and CPA/SBR) Configuration data in the system.

Import CSV Files

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

CSV file formats and procedures for using Bulk Import operations are in the Diameter Configuration Import Help and in the *Diameter and Mediation User Guide*.

CAUTION

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

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

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

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

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

For files that are exported to the Export Server Directory,

- If a remote Export Server has been configured (see the **Administration Export Server** page), the files in the Export Server Directory are automatically transferred to the configured remote Export Server and are deleted from the Export Server Directory. The transferred files do not appear in the list on the local system **Status & Manage Files** page or in the list on the **Diameter Configuration Import** page.
- If a remote Export Server has not been configured, the files in the Export Server Directory appear in the list on the **Status & Manage Tasks Active Tasks** page, and also appear in the list on the local system **Status & Manage Files** page.

For files that are exported to the File Management Directory,

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

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

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

Import Operations

CAUTION

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

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

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

The following Import operations can be performed:

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

- Insert new configuration data into the system

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

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

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

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

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

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

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

  Delete operations – Using an exported file without editing it will remove from the system all of the configuration data entries in the exported records. If you do not want to delete all of the configuration data entries that are in the file records, edit the file and remove the records for the entries that are NOT to be deleted. Records for configuration data entries that do not exist in the system will be flagged as errors for a Delete operation. For example, if you want to delete 20 of 100 configured connections, edit the file and remove the records for the 80 connections that you do not want to delete.
- Files that were created using the DSR Bulk Export operation and are transferred to another system for importing configuration data on that other system may not need to be edited. Exceptions might be system-specific information such as IP addresses and DA-MP profiles.
- Manually created files can be created so that they contain only the configuration data that is needed for the desired Import operation.

  The files can be edited later for use with a different Import operation.

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

Not all of the Import operations are valid for all types of configuration data. *Table 26: Valid Import Operations* indicates the valid operations for the listed types of configuration data.

Table 26: Valid Import Operations

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

Configuration Data	Insert	Update	Delete
Address Resolution	X	X	X
System Options		X	
Fabr			
Applications	X	X	X
Exceptions		X	
Default Destinations	X	X	X
Address Resolution	X	X	X
System Options		X	
Cpa			
System Options		X	
Message Copy		X	
Sbr (for CPA)			
SBR		X	
SBR Subresource Mapping	Cannot be imported or exported		
Pdra			
PCRFs	X	X	X
Binding Key Priority		X	
Topology Hiding	X	X	X
Site Options		X	
Error Codes		X	
Alarm Settings		X	
Access Point Names	X	X	X
Network-Wide Options		X	
Congestion Options		X	

Import Operation Results

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

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

  For example, `ImportExportStatus/<import file name>.log`
  The Bulk Import operation can be configured with the **Abort On First Error** check box to:

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

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

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

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

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

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

Chapter 5

Policy DRA Maintenance

Topics:

This chapter describes or indicates where to find the following information that can be used for the Policy DRA application and Policy SBR:

- Maintenance and status information that is maintained by the Policy DRA Configuration and Maintenance components and displayed on the **Policy DRA > Maintenance** pages.
- Maintenance and status data that is maintained by Diameter for Diameter Configuration components, DSR Applications, and DA-MPs and displayed on the **Diameter Maintenance** GUI pages.
- Descriptions of Policy DRA and Policy SBR alarms, KPIs, and measurements
- Auditing of the Session and Binding databases
- Policy DRA and Policy SBR overload management
- Database Backup and Restore of Policy DRA configuration data

Introduction

This chapter describes:

- *Policy DRA Maintenance Pages* describes maintenance and status data that is maintained by the Policy DRA application and by Policy DRA DA-MPs.

  On the **P-DRA > Maintenance** pages you can:

  - View Policy SBR Status
  - Define and execute a Binding Key Query
- *Diameter Maintenance and Status Data for Components, DSR Applications, and DA-MPs* describes maintenance and status information that is maintained by the Diameter Routing Function and the Diameter Transport Function for the Diameter Configuration components that are used to make egress Request message routing decisions.

  The **Diameter > Maintenance** pages include status information for:

  - Peer Nodes
  - Connections
  - DSR Applications (including Policy DRA)
  - DA-MPs
- *Alarms, KPIs, and Measurements*describes Policy DRA-specific database alarms, and indicates the location of descriptions of Policy DRA and Policy SBR alarms, KPIs, and measurements.
- *Binding and Session Database Auditing* describes the auditing of the Session and Binding databases.
- *Overload Management* describes overload controls and load shedding and for Policy DRA and Policy SBR.
- *Backup and Restore for Policy DRA Configuration Data* describes the OAM database backup and restore of Policy DRA configuration data.

Policy DRA Maintenance Pages

The Policy DRA > Maintenance GUI pages on the NOAM display Policy SBR status information and provide access to the Binding :Key Query tool.

Policy SBR Status

The **Policy DRA > Maintenance > Policy SBR Status** page displays a collapsed or expanded detailed report for Policy SBR. The data is displayed within Server Groups by configured Place Associations. Each line on the page represents a Server Group.

Fields are described in *Policy SBR Status elements*.

Policy SBR Status elements

Table 27: Policy SBR Status elements describes the elements on the **Policy SBR Status** page, which displays Policy SBR Server Status data within Server Groups that are assigned to each type of Place Association.

Each tab name was configured on the **Configuration > Place Associations** GUI page.

Table 27: Policy SBR Status elements

Elements	Description	Data Input Notes
One <Binding Region> tab	A list of all configured Server Groups that are assigned to the Binding Region Place Association. The Resource Domain Name and the Resource Domain Profile of each Server Group is shown. The Resource HA Role of the Server, the server's Congestion Level, and a list of Sub Resources Hosted by the server are shown for each Server in the expanded list.	The page is view-only. The Server Group in each row under the tab can be expanded or collapsed by clicking on the + symbol, to list the Servers that are assigned to that Server Group.
A tab for each Policy DRA Mated Site in the system	Each tab displays a list of all configured Server Groups that are assigned to that Mated Pair Place Association. The Resource Domain Name and the Resource Domain Profile of each Server Group are shown. The Resource HA Role of the Server, the server's Congestion Level, and a list of Sub Resources Hosted by the server are shown for each Server in the expanded list.	

Binding Key Query

Use the **Policy DRA > Maintenance > Binding Key Query** page to enter a value for an individual query for a specified binding key. The tool queries the Binding database to determine if the binding key exists.

- If the binding key exists, a report is generated that includes the PCRF that the key is bound to and information about which Diameter session or sessions are associated with that binding key.

  The returned session information includes all other binding keys that were included in the session, the session creation time, and the session last touched time.
- If the queried binding key does not exist, an error message is displayed..

Note: The Binding Key Query tool can be used only with Gx sessions. It is not applicable to Rx sessions.

The fields are described in *Binding Key Query elements*.

To use the Binding Key Query tool,

1. On the Active NOAM, select **Policy DRA** ➤ **Maintenance** ➤ **Binding Key Query**.
2. Select the **Binding Key Type** in the pulldown list.
3. Enter the **Binding Key** value to search for.
4. Click **Search**.

   The report appears on the page.

To enter another query, click **Clear**, and select and enter the values for the new search.

Binding Key Query elements

Table 28: Binding Key Query elements describes the elements on the **Policy DRA > Maintenance > Binding Key Query** page.

Table 28: Binding Key Query elements

Elements (* indicates a required field)	Description	Data Input Notes
* Binding Key Type	The binding key type for the search.	Format: Pulldown list Range: IMSI, MSISDN, IPv4 Address, IPv6 Address
* Binding Key	The binding key string to search for.	Format: Text box. Valid characters are letters (a-z, A-Z), digits (0-9), dots (.), colons (:), and hyphens (-). Range: 1-256 characters. • IMSI (1-15 digits) • MSISDN (1-15 digits) • Valid IPv4 Address • IPv6 Address (Address representation type 2 as described in RFC 4291 Section 2.2.) **Note:** If the complete IPv6 Address is not known, enter only the first 4 sets of 16-bit words, followed by a double-colon; for example, .db3:1234:1a:23c::

Alarms, KPIs, and Measurements

This section describes the type of alarm, KPI, and measurements information that is available for Policy DRA and Policy SBR, and how to access the information in the DSR GUI.

Policy DRA and Policy SBR Alarms and Events

Policy DRA application and Policy SBR alarms and events are described in the *Alarms, KPIs, and Measurements Reference* and the DSR Alarms, KPIs, and Measurements online help.

Active alarms and events and alarm and event history can be displayed on the **Alarms & Events > View Active** and **Alarms & Events > View History** GUI pages.

Database Alarms

The Policy DRA application supports two Policy SBR alarms related to database capacity:

- A **Binding Capacity alarm**: "Policy SBR Bindings Threshold Exceeded"

  The Binding Capacity alarm scope is network-wide. The Binding Capacity alarm is raised and cleared based on the percentage full of the Binding database.

  The assertion threshold values are specified as percentages and can be configured at any time using the **Policy DRA > Configuration > Alarm Settings** GUI page on the active NOAM. Each alarm severity can be suppressed if desired by checking a box on the **Policy DRA > Configuration > Alarm Settings** GUI page.

  The Binding Capacity alarm measures the number of binding (IMSI) records against an engineered maximum value that varies according to the number of Binding Policy SBR Server Groups that are specified at feature activation.

  Because no single Binding Policy SBR server holds the entire Binding database (except in the case of small systems with only one Binding Policy SBR Server Group), each Binding Policy SBR reports the size of its portion of the database to the NOAM server. A mechanism on the NOAM aggregates the reported database size records such that only the records from active servers in each Server Group are counted. This summation is then converted into a percent-full of the maximum database size and compared against the assertion and abatement thresholds, causing alarms to be raised and cleared accordingly.

  Alarm abatement occurs at 5% below the assertion threshold for each alarm severity. For example, if the minor alarm threshold is configured as 70%, a minor alarm will clear only after the database size drops below 65% full.

- A **Session Capacity alarm**: "Policy SBR Sessions Threshold Exceeded"

  The Session Capacity alarm is scoped to a mated pair of Policy DRA DSRs because each mated pair has its own instance of the Session database. The Session Capacity alarm is raised and cleared based on the percentage full of an instance of the Session database.

  The assertion threshold values are specified as percentages and can be configured any time, using the **Policy DRA > Configuration > Alarm Settings** GUI page on the active NOAM. Each alarm severity can be suppressed if desired by checking a box on the **Policy DRA > Configuration > Alarm Settings** GUI page.

  The Session Capacity alarm percent full is based on the number of Session records compared to an engineered maximum, which varies according to the number of Session Policy SBR Server Groups per mated pair that are chosen at Policy DRA feature activation.

  Because no single Session Policy SBR server holds the entire Session database (except in the case of small systems with only one Session Policy SBR Server Group), each session Policy SBR reports the size of its portion of the database to the NOAM server. A mechanism on the NOAM aggregates the reported database size records such that only the records from active servers in each Server

Group in an instance of the Session database are counted. This summation is then converted into a percent-full of the maximum database size and compared against the assertion and abatement thresholds, causing alarms to be raised and cleared accordingly.

Alarm abatement occurs at 5% below the assertion threshold for each alarm severity. For example, if the minor alarm threshold is configured as 70%, a minor alarm will clear only after the database size drops below 65% full.

If a Policy SBR Session Capacity alarm is asserted, the “instance” field of the alarm is set to the name of the Policy DRA Mated Pair **Place Association** that identifies the Policy DRA mated pair.

DSR Application Ingress Message Rate Alarm

The number of ingress messages (both Requests from PCEF and Answers from PCRF) per second received by Policy DRA is counted as input to Policy DRA ingress message processing capacity. The capacity is an engineering system value for the number of ingress messages per second processed by Policy DRA for a single MP server.

Thresholds (in percentages) associated with the Policy DRA ingress message capacity can be configured on the **Policy DRA > Configuration > Alarm Settings** GUI page on the active NOAM.

If the ingress message rate received at Policy DRA exceeds the configured percentage of the maximum capacity, ths alarm is raised at the appropriate severity (Minor, Major, Critical).

Ths alarm is cleared when the Ingress Message rate drops below the configured percentage of the ingress message capacity for the alarm severity (Minor, Major, Critical).

Policy SBR Audit Report Event 22716

To limit the effects of stale Binding and Session records, all Policy DRA MPs that own an active part of the database continually audit each table to detect and remove stale records.

In order to have some visibility into what the audit is doing, the audit generates Event 22716 with audit statistics at the end of each pass of a table. The format of the report varies depending on which table the audit statistics are being reported for. The audit reports for each table type are formatted as described in *Table 30: Audit Report Formats*.

Policy DRA and Policy SBR KPIs

Key Performance Indicators, or KPIs, provide a means to convey performance information to the user in near real-time. All the KPIs for Policy DRA and Policy SBR are displayed on the **Status & Manage > KPIs** GUI page. Selecting the tab for a server and either **P-DRA** or **pSBR** under the tab displays the KPI information for the selected server.

The Policy DRA and Policy SBR KPIs are described in the *DSR Alarms, KPIs, and Measurements Reference* and the DSR Alarms, KPIs, and Measurements online help.

Policy DRA and Policy SBR Measurements

Measurements for Policy DRA and Policy SBR are collected and reported in various measurement groups.

A measurement report and a measurement group can be associated with a one-to-one relationship. A measurements report can be generated with report criteria selected on the **Measurements -> Reports** GUI page.

The *DSR Alarms, KPIs, and Measurements* online help and PDF explain the report selection criteria, and describe each measurement in each measurement group.

Binding and Session Database Auditing

In the vast majority of cases Binding and Session database records are successfully removed as a result of signaling to terminate Diameter sessions. There are, however, instances in which signaling incorrectly removed a session and did not remove a database record that should have been removed. The following cases can result in stale Binding or Session records:

- No Diameter session termination message is received when the UE no longer wants the session.
- IP signaling network issues prevent communication between MPs that would have resulted in one or more records being deleted.
- Policy SBR congestion could cause stack events to be discarded that would have resulted in removal of a Binding or Session record.

To limit the effects of stale Binding and Session records, all Policy SBRs that own an active part of the database continually audit each table to detect and remove stale records. The audit is constrained by both minimum and maximum audit rates. The actual rate varies based on how busy the Policy SBR server is. Audit has no impact on the engineered rate of signaling.

Table 29: Effects of Stale Binding and Session Records describes the possible effects of a stale record, according to the type of stale record.

Table 29: Effects of Stale Binding and Session Records

Record Type	Effect of a Stale Record
IMSI	A stale IMSI anchor key record will cause all sessions for that IMSI to be handled by whatever PCRF was assigned to the IMSI when the IMSI anchor key record was created. Having one or more subscribers tied indefinitely to a given PCRF may hinder the Policy DRA load distribution algorithm from keeping PCRFs evenly loaded.
MSISDN	A stale MSISDN alternate key record will cause all binding dependent sessions that rely on the MSISDN for subscriber identity to be routed to the PCRF that was assigned to the MSISDN record when it was created. If some binding capable sessions include MSISDN and some do not, it is possible that a subscriber's sessions could be routed to two different PCRFs (one used by the stale MSISDN record, and one used by a new IMSI anchor key record). This situation is expected to be rare and is further mitigated by the Policy DRA software overwriting MSISDN records if the same MSISDN is later assigned to a different PCRF.

Record Type	Effect of a Stale Record
IPv4	A stale IPv4 alternate key record could result in mis-routing of a Diameter session containing an IP address that was reassigned (such as by a DHCP server) to another subscriber. This situation is mitigated by the Policy DRA software overwriting IPv4 Address records if the same IP address is later assigned to a different PCRF.
IPv6	A stale IPv6 Alternate key record could result in mis-routing of a Diameter session containing an IP address that was reassigned (such as by a DHCP server) to another subscriber. This situation is mitigated by the Policy DRA software overwriting IPv6 Address records if the same IP address is later assigned to a different PCRF.
Session	The main problem caused by a stale Session record is that removal of a binding capable session is what triggers removal of Binding records. If a stale Session record exists, the associated and correspondingly stale Binding records probably also exist.
SessionRef	SessionRef records are written in lock-step with Session records such that if one fails, the other is removed. As a result, if a SessionRef record is stale, the corresponding Session record is probably also stale. Because Binding database records contain SessionRef instances, a stale SessionRef record prevents those Binding records from being removed when they should be. Binding records are removed only if they are not associated with a valid SessionRef.

Binding table audits are confined to confirming with the Session Policy SBR that the session still exists. If the session exists, the record is considered valid and the audit makes no changes. If the session does not exist, however, the record is considered to be an orphan and is removed by the audit.

Session table audits work entirely based on valid session lifetime. When a session is created, it is given a lifetime for which the session will be considered to be valid regardless of any signaling activity. Each time an RAA is processed, the lifetime is renewed for a session. The duration of the lifetime defaults to 7 days, but can be configured in one of two ways:

- The default duration can be configured using the NOAM **Policy DRA > Configuration > Network-Wide Options** GUI page.
- A session lifetime can be configured per Access Point Name using the NOAM **Policy DRA > Configuration > Access Point Names** GUI page.

If the session initiating message (CCR-I) contains a Called-Station-Id AVP (an Access Point Name) and the Access Point Name is configured in the Access Point Names GUI, the session will use the value associated with that Access Point Name for the session lifetime value. If the session initiating message contains no Called-Station-Id Access Point Name, or contains a Called-Station-Id Access Point Name that is not configured in the Access Point Names GUI, the default session lifetime from Network-Wide Options will be used.

If the audit discovers a session record for which the current time minus the last touched time (either when the session was created, or when the last RAA was processed, whichever is more recent) exceeds the applicable session lifetime, the record is considered to be stale. Stale records are scheduled for Policy DRA initiated RAR messages to query the policy client that created the session to ask if the session is still valid.

Generally, Policy SBR servers are engineered to run at 80% of maximum capacity. The audit is pre-configured to run within the 20% of remaining capacity. Audit will yield to signaling. Audit can use the upper 20% only if signaling does not need it.

The maximum audit rate is configurable (with a default of 12,000) so that the audit maximum rate can be tuned according to the customer's traffic levels. For example, if the Policy SBR servers are using only 50% capacity for signaling, a higher rate could be made available to audit.

If the Policy SBR signaling load plus the audit load cause a Policy SBR server to exceed 100% capacity, that Policy SBR server will report congestion, which will cause an automatic suspension of auditing. Audit will continue to be suspended until no Policy SBR server is reporting congestion. Any Policy SBR on which audit is suspended will have minor alarm 22715 to report the suspension. The alarm is cleared only when congestion abates.

A Policy SBR server determines that it is in congestion by examining the rate of incoming stack events.

- Local congestion refers to congestion at the Policy SBR server that is walking through Binding or Session table records.
- Remote congestion refers to congestion at one of the Session Policy SBR servers that a Binding Policy SBR server is querying for the existence of session data (using sessionRef).

A Binding Policy SBR server will suspend audit processing if the server on which it is running is congested (local congestion), or if any of the Session Policy SBR servers to which it is connected through ComAgent connections have reported congestion (remote congestion). Audit processing will remain suspended until both local congestion and all instances of remote congestion have abated.

A Session Policy SBR server will suspend audit processing if the server on which it is running is congested (local congestion). The Session Policy SBR does not have to worry about remote congestion because it does not rely on binding data to perform its auditing function. Recall that session records are removed by audit if they are determined to be stale and the policy client that created the session indicates that the session is no longer needed (or if the session integrity feature has exhausted all attempts to communicate with a policy client that created a session). Session auditing will remain suspended until the local congestion abates.

When a Policy SBR server starts up (i.e. Policy SBR process starts), or when a Policy SBR's audit resumes from being suspended, the audit rate ramps up using an exponential slow-start algorithm. The audit rate starts at 1500 records per second and is doubled every 10 seconds until the configured maximum audit rate is reached.

In addition to the overall rate of record auditing described above, the frequency at which a given table audit can be started is also controlled. This is necessary to avoid needless frequent auditing of the same records when tables are small and can be audited quickly. A given table on a Policy SBR server will be audited no more frequently than once every 10 minutes.

In order to have some visibility into what the audit is doing, the audit generates Event 22716 " Policy SBR Audit Statistics Report" with audit statistics at the end of each pass of a table. The format of the report varies depending on which table the audit statistics are being reported for. The audit reports for each table type are formatted as described in *Table 30: Audit Report Formats*.

Table 30: Audit Report Formats

Data Type	Audit Report Format
IMSI Binding Records	Policy SBR Table Audit Pass Statistics Table: ImsiAnchorKey Records Visited: N Session References Audited: N Session References Removed: N Records Removed: N Audit Pass Duration: N seconds Suspended Duration: N seconds
IPv4 Alternate Key Binding Records	Policy SBR Table Audit Pass Statistics Table: Ipv4AlternateKey Records Visited: N Records Removed: N Audit Pass Duration: N seconds Suspended Duration: N seconds
IPv6 Alternate Key Binding Records	Policy SBR Table Audit Pass Statistics Table: Ipv6AlternateKey Records Visited: N Records Removed: N Audit Pass Duration: N seconds Suspended Duration: N seconds
MSISDN Alternate Key Binding Records	Policy SBR Table Audit Pass Statistics Table: MsisdnAlternateKey Records Visited: N Session References Audited: N Session References Removed: N Records Removed: N Audit Pass Duration: N seconds Suspended Duration: N seconds
Sessions Records	Policy SBR Table Audit Pass Statistics

	Table: Session Records Visited: N Records Requiring a Policy Client Query: N Records Removed due to Policy Client Query Results: N Stale Binding Dependent Records Removed: N Audit Pass Duration: N seconds Suspended Duration: N seconds
Session Reference Records	Policy SBR Table Audit Pass Statistics Table: SessionRef Records Visited: N Records Removed: N Audit Pass Duration: N seconds Suspended Duration: N seconds

Overload Management

The Policy DRA application provides mechanisms to manage the overload and congestion that can occur on the Policy DRA and Policy SBR. The Policy DRA might receive ingress messages at a rate higher than the engineered capacity. The internal queues on the Policy DRA might experience higher utilization level than configured. The same might happen on the Policy SBR servers, directly or indirectly resulting from the overloaded traffic from the network or from the Policy DRA.

Overload Controls

The Policy SBRs that implement the Session and Binding databases must protect themselves from becoming so overloaded that they cease to perform their function. There are two parts to achieving this goal:

- Detecting the overload condition and severity
- Shedding work to reduce load.

Policy DRA DA-MP Overload Control

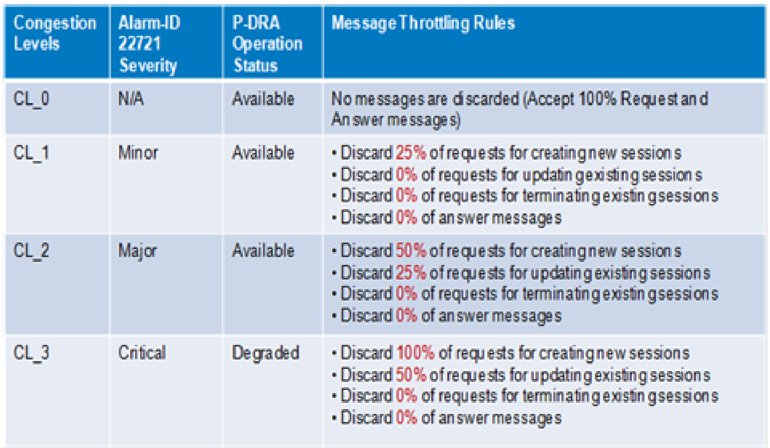
The number of ingress messages (both Requests and Answers) per second received by Policy DRA is counted as input to Policy DRA ingress message processing capacity. The capacity is an engineering number of ingress messages per second processed by Policy DRA. The number of Request messages received at Policy DRA per second is also measured separately.

Policy DRA defines alarms on the queue utilization levels based on configured threshold values. Thresholds (in percentage) are configured in association with the Policy DRA ingress message capacity. If the ingress message rate received at Policy DRA exceeds the configured percentage of the maximum capacity, alarms will be raised. Policy DRA ingress Request capacity can be engineering configured to provide the value based on which thresholds (in percentage) are configured. See *Alarm Settings*.

The Policy DRA congestion is then defined by the ingress Request messages capacity and the configured threshold values. Policy DRA will be considered in congestion if the ingress Request rate at Policy DRA exceeds the configured percentages (thresholds) of Policy DRA ingress Request capacity.

Three Policy DRA congestion levels (CL_1, CL_2 and CL_3) are defined, each of them is associated with onset and abatement threshold values. The onset and abatement values are configurable (see *Congestion Options*). When Policy DRA is in congestion, a Policy DRA congestion alarm will be raised at the severity (Minor, Major or Critical) corresponding to the congestion level (CL_1, CL_2 or CL_3).

When congestion is detected, Policy DRA will perform overload control by throttling a portion of incoming messages to keep Policy DRA from being severely impacted. The type and percentage of the messages to be throttled will be configurable through the Policy DRA GUI as displayed in *Figure 23: Policy DRA Default Overload Control Thresholds*:



Congestion Levels	Alarm-ID 22721 Severity	P-DRA Operation Status	Message Throttling Rules
CL_0	N/A	Available	No messages are discarded (Accept 100% Request and Answer messages)
CL_1	Minor	Available	• Discard 25% of requests for creating new sessions • Discard 0% of requests for updating existing sessions • Discard 0% of requests for terminating existing sessions • Discard 0% of answer messages
CL_2	Major	Available	• Discard 50% of requests for creating new sessions • Discard 25% of requests for updating existing sessions • Discard 0% of requests for terminating existing sessions • Discard 0% of answer messages
CL_3	Critical	Degraded	• Discard 100% of requests for creating new sessions • Discard 50% of requests for updating existing sessions • Discard 0% of requests for terminating existing sessions • Discard 0% of answer messages

Figure 23: Policy DRA Default Overload Control Thresholds

The Policy DRA's internal congestion state contributes to Policy DRA's Operational Status directly, along with its Admin state and Shutdown state. Consequently, the congestion state of the Policy DRA impacts the Diameter Routing Function message transferring decision. Depending on the Policy DRA's Operational Status (Unavailable, Degraded, Available), the Diameter Routing Function will forward all the ingress messages to the Policy DRA when the Policy DRA's Operational Status is Available, or discard some or all of the ingress messages when the Operational Status is Degraded or Unavailable. *Table 31: Diameter Routing Function Message Handling Based on Policy DRA Operational Status* describes the Diameter Routing Function handling of the messages to the Policy DRA.

Table 31: Diameter Routing Function Message Handling Based on Policy DRA Operational Status

Policy DRA Operational Status	Diameter Routing Function Message Handling
Available	Forward all Request and Answer messages to Policy DRA
Degraded	Forward all Answer messages only to Policy DRA
Unavailable	Discard all messages intended for Policy DRA

Policy SBR Congestion

Policy SBR relies on ComAgent for resource monitoring and overload control. The ComAgent Resource Monitoring and Overload Framework monitors local MP's resource utilizations, defines MP congestion based on one or multiple resource utilizations, communicates the MP congestion levels to Peers, and reports local MP congestion level to the local application (Policy SBR).

Messages called "stack events" are used for communication to and from ComAgent.

ComAgent defines MP congestion levels based on a CPU utilization metric and ingress stack event rate (number of stack events received per second at local ComAgent), whichever is higher than the pre-defined congestion threshold, and broadcasts the MP congestion state to all its Peers. ComAgent provides APIs that the local Policy SBR can call for receiving congestion level notifications.

Policy SBR congestion is measured based on the Policy SBR CPU utilization level. There are four Policy SBR congestion levels: CL0 (normal), CL1 (Minor), CL2 (Major) and CL3 (Critical). There are related Onset and Abatement threshold values, and Abatement time delays.

The Policy SBR congestion state (CPU utilization) is managed and controlled by the ComAgents on both Policy DRA and Policy SBR MPs based on the ComAgent MP Overload Management Framework. Messages to a Policy SBR from a Policy DRA are handled based on the congestion state of the Policy SBR. A Policy SBR congestion alarm will be raised when MP congestion notification is received from ComAgent. The appropriate alarm severity information will be included in the notification. The alarm will be cleared if the congestion level is changed to Normal, also indicated in the notification from ComAgent.

In order to manage the overload situation on a Policy SBR, all stack event messages are associated with pre-defined priorities. Before a stack event message is sent, its priority will be compared with the congestion level of the Policy SBR to which the stack event is sent. If the priority is higher than or equal to the Policy SBR current congestion level, the message will be forwarded. Otherwise, it will be discarded.

The stack events may also be routed from a Policy SBR to another Policy SBR in some scenarios. The congestion control in this case should be conducted based on the congestion state of the receiving Policy SBR, i.e. the ComAgent on the sending Policy SBR is responsible to compare the stack event priority with the congestion level of the receiving Policy SBR and make the routing decision accordingly.

Load Shedding

After the Policy SBR has determined that it is in overload (CL1 – CL3), it informs ComAgent that its resources and sub-resources are in congestion. ComAgent then broadcasts this information to all of the resource users for the specified resources and sub-resources. The resource users now begin to shed load by sending only certain requests for database updates. The resource users determine which database requests to discard based on the current congestion level of the resource provider.

Database requests are delivered to Policy SBRs using ComAgent stack events. Each stack event has a priority. The resource user software (on either DA-MPs or Policy SBRs) sets the stack event priority for every Stack Event it sends, depending on the type of stack event and the circumstances under which the Stack Event is being used. For example, the same stack event may be used for signaling and for audit, but may have a different priority in each circumstance. The Stack Event priority is compared with the congestion level of the server that is the target of the stack event to determine whether stack event should be sent, as shown in *Table 32: Stack Event Load Shedding*.

Table 32: Stack Event Load Shedding

Congestion Level	Description
CL0	The resource provider is not congested. No load shedding occurs. Send all Stack Events.
CL1	Minor congestion. Auditing is suspended. Send all Stack Events not related to auditing.
CL2	Major congestion. No new bindings or sessions are created. Existing bindings and sessions are unaffected. Send only Stack Events related to existing sessions.
CL3	Critical congestion. Send only Stack Events already started and Stack Events that remove sessions or bindings.

Shutdown

DA-MP- The Policy DRA application running on DA-MPs supports the DSR Application Infrastructure graceful shutdown with 5 seconds grace period. This means that when Policy DRA is Disabled (using the **Diameter->Maintenance->Applications** GUI page), the application will transition to the Degraded Operational Status for 5 seconds to allow in-flight messages to be processed without accepting any new Requests before transitioning to the Unavailable Operational Status. In the Unavailable status, neither Requests nor Answers are processed by the Policy DRA application.

Policy SBR - Because Policy SBR servers use the Active/Standby/Spare redundancy model, and ComAgent supports reliable transactions, there is no need for a graceful shutdown mode. Shutdown of a Policy SBR server will cause a failover to another server in the same Server Group. (The exception is if the Server Group only has one server, as might be the case in a small demo system.)

The Policy DRA Operational Status (Unavailable, Degraded and Available) is determined by its Admin State, Congestion Level, and the Shutdown State. The Policy DRA application calculates and maintains its own operational status and reports it to the Diameter Routing Function.

When the Policy DRA application is not processing requests (in Operational Status of Degraded or Unavailable), the Diameter Routing Function will attempt to route new Requests using the rules in the Peer Routing Tables. If the Request has no Destination-Host AVP, as would be the case for session-initiating Requests, the routing will fail and the Diameter Routing Function will respond with a 3002 DIAMETER_UNABLE_TO_DELIVER Answer.

When a Server is "Stopped" using the Stop function on the **Status & Manage -> Server** GUI page, Diameter will terminate all Diameter connections by sending a DPR and waiting for the DPA. If all DPAs have not been received within 15 seconds, Diameter begins termination of its layers and queues. If Diameter is still not shut down after another 15 seconds, the process is abruptly terminated.

To properly shut down a Policy DRA DA-MP server,

1. Go to the Diameter -> Maintenance -> Applications GUI page and Disable the Policy DRA application.

   The Operational Status of the application will transition to Unavailable

2. Go to the **Status & Manage -> Server** page and Stop the Server's application processes.

   After 30 seconds maintenance can proceed as necessary.

Table 33: Policy DRA Operational Status shows an example of the Policy DRA Operational Status determination where the Shutdown mode is Graceful Shutdown. The Shut down and Shutting down in the Operational Reason column indicate the states where the (Graceful) shutdown process has been completed (Shut down) and is in progress (Shutting down) respectively. While the Graceful Shutdown is in progress, the Policy DRA continues to process the messages in its queue for a time interval that is engineering configurable.

Table 33: Policy DRA Operational Status

Admin State	Congestion Level	Shutdown State	Operational Status	Operational Reason
N/A	N/A	N/A	Unavailable	Not initialized
Disabled	0 ,1, 2, 3	False	Unavailable	Shut down
Disabled	0 ,1, 2, 3	True	Degraded	Shutting down
Enabled	0 1 2	N/A	Available	Normal Available with CL_1 Available with CL_2
Enabled	3	N/A	Degraded	Congested with CL_3

Policy SBR - Because Policy SBR servers use the Active/Standby/Spare redundancy model, and ComAgent supports reliable transactions, there is no need for a graceful shutdown mode. Shutdown of a Policy SBR server will cause a failover to another server in the same Server Group. (The exception is if the Server Group only has one server, as might be the case in a small demo system.)

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

Maintenance and status data is maintained and displayed on the following Diameter > Maintenance GUI pages for Diameter Configuration components, DSR Applications including Policy DRA, and DA-MPs including those that run the Policy DRA application:

- **Route Lists Maintenance** - The **Diameter > Maintenance > Route Lists** page displays information about the Route Groups assigned to Route Lists. Route List maintenance and status data is maintained and merged to the OAMs. The data is derived from the current Operational Status of Route Groups assigned to a given Route List. The Operational **Status** of each Route List determines whether the Route List can be used for egress routing of Request messages.
- **Route Groups Maintenance** - The **Diameter > Maintenance > Route Groups** page displays the configured and available capacity for Route Groups and displays information about Peer Nodes or Connections assigned to a Route Group.

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

- **Peer Nodes Maintenance** - The **Diameter > Maintenance > Peer Nodes** page provides the Operational Status of Peer Node connections, including a Reason for the status.
- **Connections Maintenance** - The **Diameter > Maintenance > Connections** page displays information about existing connections, including the Operational Status of each connection.

  The **Diameter > Maintenance > Connections > SCTP Statistics** page displays statistics about paths within an SCTP connection. Each line on the page represents a path within an SCTP connection.
- **Applications Maintenance** - The **Diameter > Maintenance > Applications** page displays status, state, and congestion information about activated DSR Applications. The data is refreshed every 10 seconds.

  On the **Diameter > Maintenance > Applications** page, you can change the Admin State of the selected DSR Application to Enabled or Disabled.
- **DA-MPs Maintenance** - The **Diameter > Maintenance > DA-MPs** page provides state and congestion information about Diameter Agent Message Processors.

  On the **Diameter > Maintenance > DA-MPs** page,

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

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

Diameter Maintenance is described in more detail in the *Diameter and Mediation User Guide* and in the Diameter Help.

Backup and Restore for Policy DRA Configuration Data

Because Policy DRA is required to run on a 3-tier OAM topology where some data is mastered at the NOAM and some data is mastered at SOAMs at each site, backup and restore must be performed on the NOAM and on the SOAMs at each site.

Only configured data is backed up and restored. Dynamic data such as policy sessions and policy bindings that is mastered on Policy SBR MP servers is not backed up or restored.

The Policy DRA feature uses the capabilities of the Backup and Restore functions provided by the OAM **Status & Manage >Database** GUI page, as described in the "Database Backups and Restores" chapter of the *DSR Administration Guide*.

Glossary

#

2-tiered DSR Topology

A DSR architecture consisting of a management (NOAM) layer and a message processor (MP) layer. The scope of management for is a single DSR Signaling Network Element.

3-tiered DSR Topology

A DSR architecture consisting of a centralized management layer with network wide scope (NOAM), a network element (also called system) management (SOAM) layer, and message processors (MPs).

3GPP

3rd Generation Partnership Project. The standards body for wireless communications.

A

AAA

Authentication, Authorization, and Accounting (Rx Diameter command)

AAR

Authentication, Authorization Request (Rx Diameter command)

AF

Application Function (such as P-CSCF)

Alternate Key

A subscriber key other than the anchor subscriber key; for example, IP addresses or MSISDNs. Binding capable interfaces can include alternate subscriber keys. Binding dependent interfaces (Rx) cannot add alternate subscriber keys, but

A

they can use them to find a binding.

Anchor Key

The main identifier used in the P-DRA network to identify a subscriber. The Anchor Key must be an IMSI and must be present in all binding capable interfaces (Gx, Gxx, and S9).

APN

Access Point Name

The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.

Application ID

Each Diameter application is uniquely identified by an assigned Application ID that is a mandatory 32-bit field in all Diameter messages. Every Diameter Application (standard-base or vendor-specific) must have a unique Application ID assigned by IANA. Application ID ranges are Standards-based and Vendor-specific.

Each Diameter application is uniquely identified by an IANA assigned Application ID that is a mandatory 32-bit field in all Diameter messages. The Application ID is commonly used for screening and routing messages between Diameter Nodes. Diameter Relay Nodes advertise the reserved Application ID 42946967295 (0xffffffff) when connecting to Peers during the Diameter Capabilities Exchange procedure. Peer-to-Peer Diameter messages such as CER/CEA use the reserved Application ID “0”.

A

Application Routing Rule	A set of conditions that control message routing to a DSR application based on message content.
ASA	Abort-Session-Answer

B

BBERF	Bearer Binding and Event Reporting Function: A type of Policy Client used to control access to the bearer network (AN).
Binding Capable Interface	Gx and Gxx interfaces are capable of creating a binding if no binding exists for a subscriber. The CCR-I message must include the anchor subscriber key and may include alternate subscriber keys.
Binding database	Policy SBR database that holds network-wide subscriber binding information. Maps subscriber keys to the PCRF that hosts the subscriber’s policy rules. A given binding record is maintained by 3 servers in the network: an Active server, a Standby server, and a Spare server.

C

CCA-I	Credit Control Answer – Initial
CCA-T	Credit Control Answer - Terminate
CCA-U	Credit Control Answer - Update
CCR-I	CCR Initial

C

CEX Configuration Set

A mechanism for assigning Application IDs and supported Vendor IDs to a Local Node or to a Connection.

D

DA-MP

Diameter Agent Message Processor

A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application such as CPA can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.

Diameter Client

A device at the edge of the network that performs access control.

Diameter Relay Agent

Diameter agent that forwards requests and responses to other Diameter nodes based on routing-related AVPs (e.g., Destination-Realm) and routing table entries. Since relays do not make policy decisions, they do not examine or alter non-routing AVPs. As a result, relays never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are capable of handling any Diameter application or message type.

DRA

Destination Routing Address

DSR

Diameter Signaling Router

A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers.

D

A DSR Network Element may consist of one or more Diameter nodes.

E

EMS

Element Management System

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

G

GUI

Graphical User Interface

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

Gx

The Diameter credit control based interface between a PCRF and a PCEF as defined by 3GPP. The interface is used to convey session information from the PCEF to the PCRF, and in reply the PCRF provides rule information for the PCEF to enforce.

Gxx

Short for Gxa and Gxc. The Diameter credit control based interface between a BBERF and a PCRF, as defined by 3GPP.

I

IMI

Internal Management Interface

I

IMSI

International Mobile Subscriber Identity

IPFE

IP Front End

A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.

M

MEAL

Measurements, Events, Alarms, and Logs

MSISDN

Mobile Station International Subscriber Directory Number

The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.

N

NE

Network Element

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

NMS

Network Management System

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

N

(for example, data analysis and fault recovery applications).

NOAM

Network Operations, Administration, and Maintenance

O

OAM

Operations, Administration, and Maintenance

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

P

PCEF

Policy and Charging Enforcement Function

Maintains rules regarding a subscriber’s use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.

PCRF

Policy and Charging Rules Function

The ability to dynamically control access, services, network capacity, and charges in a network.

Peer

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

Peer Route Table

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

P

Peer Routing Table

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

Place

An OAM configured component that defines physical locations. The Site Place groups the servers at a physical location. Each server is associated with exactly one Site Place.

Place Association

An OAM configured component used by P-DRA to group Site Places into Policy DRA Mated Pairs and Policy DRA Binding Regions.

Policy DRA

Policy Diameter Relay Agent. A scalable, geo-diverse DSR application that creates a binding between a subscriber and a PCRF, and routes all policy messages for a given subscriber to the PCRF that currently hosts that subscriber's policy rules. Policy DRA is capable of performing Topology Hiding to hide the PCRF from the Policy Client.

Policy DRA Binding Region

A type of Place Association that defines the scope of an instance of the P-DRA Binding database. In the context of the P-DRA network, a region is all of the sites in the P-DRA network. P-DRA supports only one instance of the Policy Binding Region, meaning that there is only one Binding database for the entire P-DRA Network.

Policy DRA Mated Pair

A type of Place Association. In the context of a P-DRA network, a Mated Pair is two P-DRA DSRs that

P

	are paired for redundancy such that if one site fails, the other site can take over the failed site's entire load. A Mated Pair sets the scope of an instance of the Policy Session database.
Policy SBR	Policy Session Binding Repository
PRT	Peer Route Table or Peer Routing Table

R

RAA	Re-Authorization Answer (Gx or Rx Diameter command)
RAR	Re-Authorization Request (Gx or Rx Diameter command)
Resource Domain	A list of Server Groups that support a logical resource.

S

S9	The S9 Diameter interface includes Rx, Gx, and Gxx messages, but when these messages are used between a visited PCRF and the home PCRF, the interfaces are collectively referred to as S9. Defined by 3GPP 29.215 as the interface between a visited PCRF and a home PCRF. There is no difference in processing of Rx over S9 versus. Rx not over S9. The S9 interface is binding capable for Gx and Gxx only. Rx over S9 is binding dependent.
SBR	For DSR, Session Binding Repository

S

	A highly available, distributed database for storing Diameter session binding data.
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SOAM	System Operations, Administration, and Maintenance
STA	Session-Termination-Answer Session Termination Answer (Rx Diameter command)
Subscriber Key	One of several possible keys that can be used to uniquely identify a subscriber. Subscriber Keys are delivered in the Subscriber-Id Diameter AVP of a CCR-I message. One of the Subscriber Keys is designated as an Anchor Key.
Suggested PCRF	PCRF that will be used for the binding unless an error causes alternate routing. Avoids the need to update the binding if the suggested PCRF successfully answers the CCR-I.
Suspect Binding	A Policy DRA IMSI Anchor Key binding record is considered to be

S

“suspect” if the last attempt to route a CCR-I message to the bound PCRF failed with a 3002 Error Code response. The concept of Suspect Binding allows bindings to be removed after a short period of time (called the Suspect Binding Interval) from a PCRF that has become unreachable.

T

TSA

Target Set Address

An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.

U

UE

User Equipment

V

VIP

Virtual IP Address

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

V-PCRF

Visited PCRF

X

XMI

External Management Interface

XSI

External Signaling IP Address

XSI

External Signaling Interface