

**Oracle® Communications
Policy Management**

Policy Front End Wireless User's Guide

Release 11.5.2

E65493 Revision 01

August 2015

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Chapter 1: About This Guide.....	9
How This Guide is Organized.....	10
Intended Audience.....	10
Documentation Admonishments.....	10
Related Publications.....	11
Locate Product Documentation on the Oracle Technology Network Site.....	11
Customer Training.....	12
My Oracle Support (MOS).....	12
Emergency Response.....	12
 Chapter 2: Introduction.....	 14
Policy Front End Overview.....	15
Distributed Routing and Management Application (DRMA) Protocol.....	16
Backup MRAs, Associated MRAs, and Mated Pairs.....	17
GUI Overview.....	18
 Chapter 3: Configuring a CMP System and MRA, MPE Devices.....	 20
Configuring the CMP to Manage the MRA.....	21
Creating an MRA Group.....	21
Deleting an MRA Group.....	21
Configuring the CMP System to Manage an MRA Cluster.....	22
Configuring Protocol Options for an MRA Device.....	22
Modifying MRA System Settings, Grouping or deleting MRA devices.....	24
Defining an MRA Cluster Profile.....	24
Modifying an MRA Cluster Profile.....	25
Deleting an MRA Cluster Profile from an MRA Group.....	25
Reversing Cluster Preference.....	26
Forcing a Server into Standby Status.....	26
Setting Up a Non-CMP Cluster.....	27
Role and Scope Configuration.....	38
Configuring an MRA Role.....	38
Configuring the Scope for an MRA.....	39
MRA Advanced Configuration Settings.....	40

Configuring MRA Session Clean Up Settings.....	41
Redirecting Traffic to Upgrade or Remove an MRA.....	43
Managing Configuration and Virtual Templates.....	45
Creating a Template.....	45
Creating Virtual Templates.....	49
Overlaps.....	49
Configuring Topology Hiding for the Gx Application.....	50

Chapter 4: Managing Network Elements, Backups and Diameter

Settings.....	51
Adding Associated MRAs.....	52
Configuring Protocol Options on an Associated MRA Device.....	53
Modifying Backup and Associated MRA devices.....	54
Associating Network Elements with an MRA Device.....	56
Defining a Network Element.....	57
Associating a DSR Network Element with an MRA.....	58
Creating a Network Element Group.....	59
Adding a Network Element to a Network Element Group.....	59
Managing Protocol Timer Profiles.....	60
About MPE/MRA Pools and Diameter Peer Tables.....	60
Configuring Diameter Realm Based Peer Routes.....	61
Associating a Diameter MPE Peer with an MRA.....	63
About Stateless Routing.....	65
Enabling Stateless Routing.....	65
Modifying the Stateless Migration Mode in an Existing MRA.....	66
Loading MPE/MRA Configuration Data when Adding Diameter Peer.....	67
Configuring for RADIUS.....	67

Chapter 5: Managing Subscriber Profile Repositories.....68

About Subscriber Profile Repositories.....	69
Configuring the CMP System to Manage SPR Subscriber Data.....	70
Configuring the SPR Connection.....	70
Modifying the SPR Connection.....	71
Finding a Subscriber Profile.....	71
Creating a Subscriber Profile.....	72
Managing Subscribers.....	73
Modifying a Subscriber Profile.....	73
Deleting a Subscriber Profile.....	73
Viewing Subscriber Entity States.....	74

Creating a Subscriber Entity State Property.....	74
Modifying a Subscriber Entity State Property.....	75
Deleting a Subscriber Entity State Property.....	75
Viewing Subscriber Quota Information.....	76
Adding a Subscriber Quota Category.....	77
Modifying a Subscriber Quota Category.....	78
Deleting a Subscriber Quota Category.....	78
Adding a Member to a Pooled Quota Group.....	79
Querying by Pool ID.....	79
Creating a Pool Quota Profile.....	80
Modifying a Pool Quota Profile.....	81
Deleting a Pool Quota Profile.....	81
Modifying a Pool Profile.....	81
Deleting a Pool Profile.....	82
Creating a Pool State.....	82
Modifying a Pool State.....	83
Deleting a Pool State.....	83
 Chapter 6: Monitoring the MRA.....	85
Displaying Cluster and Blade Information.....	86
Viewing Trace Logs.....	87
Trace Log Forwarding.....	87
KPI Dashboard.....	87
Mapping Reports Display to KPIs.....	88
The Subscriber Session Viewer.....	108
Viewing Session Data from the MPE.....	109
Viewing Session Data from the MRA.....	110
Deleting a Session from the Session Viewer Page.....	111
 Glossary.....	112

List of Figures

Figure 1: Typical Front End (MRA) Network.....	16
Figure 2: Backup and Associated MRA Clusters and Mated Pairs.....	18
Figure 3: Structure of the CMP Wireless GUI.....	19
Figure 4: Sample MRA Cluster Topology Configuration.....	29
Figure 5: Sample MPE Cluster Topology Configuration.....	35
Figure 6: Add Diameter Peer.....	36
Figure 7: New Role Page.....	38
Figure 8: Create Scope Page.....	40
Figure 9: Add Configuration Key Value Window.....	44
Figure 10: Original Template List.....	48
Figure 11: Reordered Template List.....	48
Figure 12: Select Network Elements.....	57
Figure 13: Add Network Element Page.....	60
Figure 14: Add Diameter MPE Peer Window.....	64
Figure 15: Enabling Stateless Routing.....	66
Figure 16: RADIUS Configuration Section.....	67
Figure 17: Cluster, Blade, and Diameter Information.....	86
Figure 18: MRA Trace Log.....	87
Figure 19: KPI Dashboard.....	88

List of Tables

Table 1: Admonishments.....	11
Table 2: MRA Protocol Configuration Options.....	22
Table 3: Session Clean Up Settings.....	41
Table 4: Topology Hiding Configuration Keys.....	50
Table 5: MRA Protocol Configuration Options.....	54
Table 6: Policy Statistics.....	89
Table 7: Quota Profile Statistics Details.....	89
Table 8: Diameter Application Function (AF) Statistics.....	89
Table 9: Diameter Policy Charging Enforcement Function (PCEF) Statistics.....	91
Table 10: Diameter Charging Function (CTF) Statistics.....	92
Table 11: Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics.....	93
Table 12: Diameter TDF Statistics.....	95
Table 13: Diameter Sh Statistics.....	96
Table 14: Diameter Distributed Routing and Management Application (DRMA) Statistics.....	97
Table 15: Diameter DRA Statistics.....	100
Table 16: Diameter Sy Statistics.....	100
Table 17: RADIUS Statistics.....	101
Table 18: Diameter Latency Statistics.....	103
Table 19: Diameter Event Trigger Statistics.....	104
Table 20: Diameter Protocol Error Statistics.....	104
Table 21: Diameter Connection Error Statistics.....	104
Table 22: LDAP Data Source Statistics.....	105

Table 23: Sh Data Source Statistics.....	106
Table 24: Sy Data Source Statistics.....	108
Table 25: KPI Interval Statistics.....	108

Chapter 1

About This Guide

Topics:

- *How This Guide is Organized.....10*
- *Intended Audience.....10*
- *Documentation Admonishments.....10*
- *Related Publications.....11*
- *Locate Product Documentation on the Oracle Technology Network Site.....11*
- *Customer Training.....12*
- *My Oracle Support (MOS).....12*
- *Emergency Response.....12*

This guide describes how to use the Policy Front End in the Policy Management system.

How This Guide is Organized

The information in this guide is presented in the following order:

- [About This Guide](#) contains general information about this guide, the organization of this guide, and how to get technical assistance.
- [Introduction](#) contains an overview of the guide, the Distributed Routing and Management Application (DRMA) protocol, and the Graphical User Interface (GUI).
- [Configuring a CMP System and MRA, MPE Devices](#) describes how to configure the CMP to manage the MRA, how to modify system settings and groupings, configuring role and scope, working with advanced MRA settings, and hiding the Gx application.
- [Managing Network Elements, Backups and Diameter Settings](#) describes associating network elements with an MRA, working with Stateful MRAs, configuring MPE /MRA Pools and setting up Diameter Peer Tables, using Stateless Routing and Configuring for RADIUS.
- [Managing Subscriber Profile Repositories](#)[Managing Subscribers](#) describes how to work with subscriber profiles, quotas, and pool.
- [Monitoring the MRA](#) describes how to monitor cluster and blade information, DRMA information, and event logs.

Intended Audience

This guide is intended for the following trained and qualified telecommunications and network installation personnel, such as system operators or system administrators, who are responsible for operating Policy Management devices such as:

- Multimedia Policy Engines (MPE)
- Multi-Protocol Routing Engine (MRA)
- Configuration Management Platform (CMP)

Documentation Admonishments

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

Table 1: Admonishments

Icon	Description
 DANGER	Danger: (This icon and text indicate the possibility of <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)
 TOPPLE	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage</i> .)

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See [Locate Product Documentation on the Oracle Technology Network Site](#) for more information.

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <http://www.adobe.com>.

1. Access the Oracle Technology Network site at <http://docs.oracle.com>.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
The Oracle Communications Documentation page appears with Tekelec shown near the top.
4. Click the **Oracle Communications Documentation for Tekelec Products** link.
5. Navigate to your Product and then the Release Number, and click the **View** link (the Download link will retrieve the entire documentation set).
A list of the entire documentation set for the selected product and release appears.

6. To download a file to your location, right-click the **PDF** link, select **Save target as**, and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

<http://education.oracle.com/communication>

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. 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 Oracle.

Chapter 2

Introduction

Topics:

- *Policy Front End Overview.....15*
- *Distributed Routing and Management Application (DRMA) Protocol.....16*
- *Backup MRAs, Associated MRAs, and Mated Pairs.....17*
- *GUI Overview.....18*

This chapter describes the Oracle Policy Front End product (referred to in this document as the Multi-Protocol Routing Agent [MRA]), which is used to scale the Policy Management infrastructure by distributing the PCRF load across multiple MPE devices in the network.

Policy Front End Overview

The Policy Front End product (referred to in this document as the Multi-Protocol Routing Agent [MRA]) is a product deployed in a Policy Management network that maintains bindings that link subscribers to Multimedia Policy Engine (MPE) devices. An MPE is a Policy Charging and Rules Function (PCRF) device. An MRA ensures that all of a subscriber's Diameter sessions established over the Gx, Gxx, Gx Lite, Rx and Sd reference points reach the same MPE device when multiple and separately addressable MPE clusters are deployed in a Diameter realm.

An MRA device implements the proxy (PA1 variant) DRA functionality defined in the 3GPP TS 29.203 [1] and 3GPP TS 29.213 [2] specifications, whereby all Diameter Policy and Charging Control (PCC) application messages are proxied through the MRA device.

When an MRA device receives a request for a subscriber for which it has a binding to an MPE device, it routes that request to an MPE device. If an MRA device does not have a binding, it queries other MRA devices in the Policy Management network, using the proprietary Distributed Routing and Management Application (DRMA) protocol, for a binding. If another MRA device has the binding, the MRA device routes the request to it. If no other MRA device has a binding, the MRA device that received the request creates one.

An MRA device can route requests across multiple MRA clusters within the Policy Management network. Multiple MRA clusters can be deployed in the same domain, (or realm), interconnected as Diameter peers. Each MRA cluster is responsible for a set, (or pool), of MPE clusters as a domain of responsibility. Each MRA cluster is a peer with the MPE clusters in its domain of responsibility. The following diagram shows a typical MRA configuration.

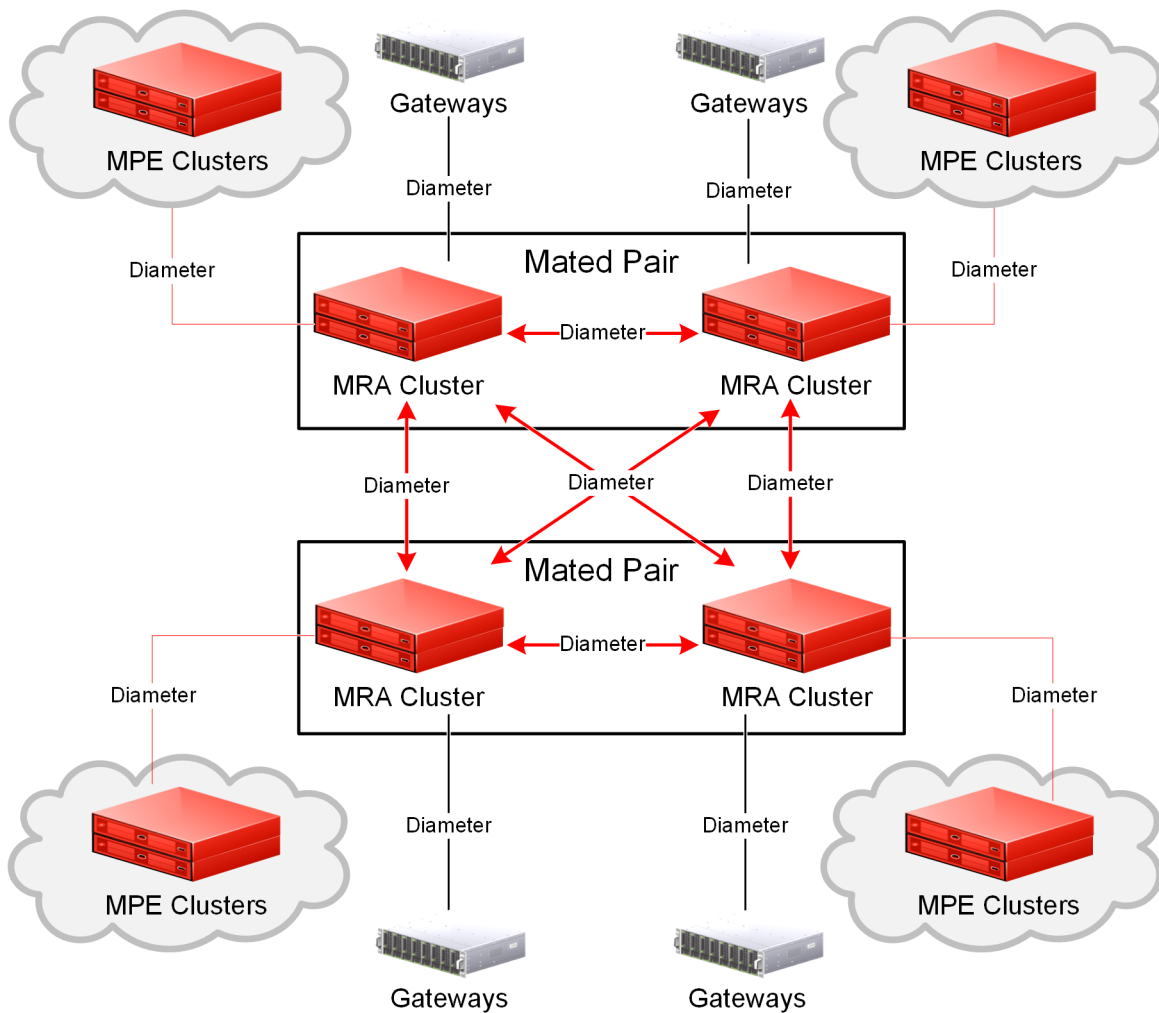


Figure 1: Typical Front End (MRA) Network

Distributed Routing and Management Application (DRMA) Protocol

The DRMA protocol is an Oracle proprietary Diameter based protocol that allows multiple MRA clusters in the network to communicate and share DRA binding information to ensure all the Diameter sessions for a subscriber are served by the same MPE device. An MRA device may query another MRA device for binding information by sending a DRA-Binding-Request (DBR) command and receiving a DRA-Binding-Answer (DBA) in response.

Backup MRAs, Associated MRAs, and Mated Pairs

A backup MRA cluster is one with which an MRA cluster shares the same pool of MPE devices. All of the MPE devices in the pool of a given MRA cluster will have backup connections to the backup MRA cluster. An MRA cluster and its backup are considered a mated pair.

An associated MRA cluster is one that is not the backup MRA cluster, but with which there is a connection and to which external binding look ups are done.

An MRA cluster can simultaneously be a backup to one MRA cluster and an associate of another. However, an MRA cluster cannot use the same MRA cluster as both a backup and an associate. [Figure 2: Backup and Associated MRA Clusters and Mated Pairs](#) shows a valid configuration of four MRA clusters, in two mated pairs, and how each cluster views its relationships with the other three. The four MRA clusters form a mesh network.

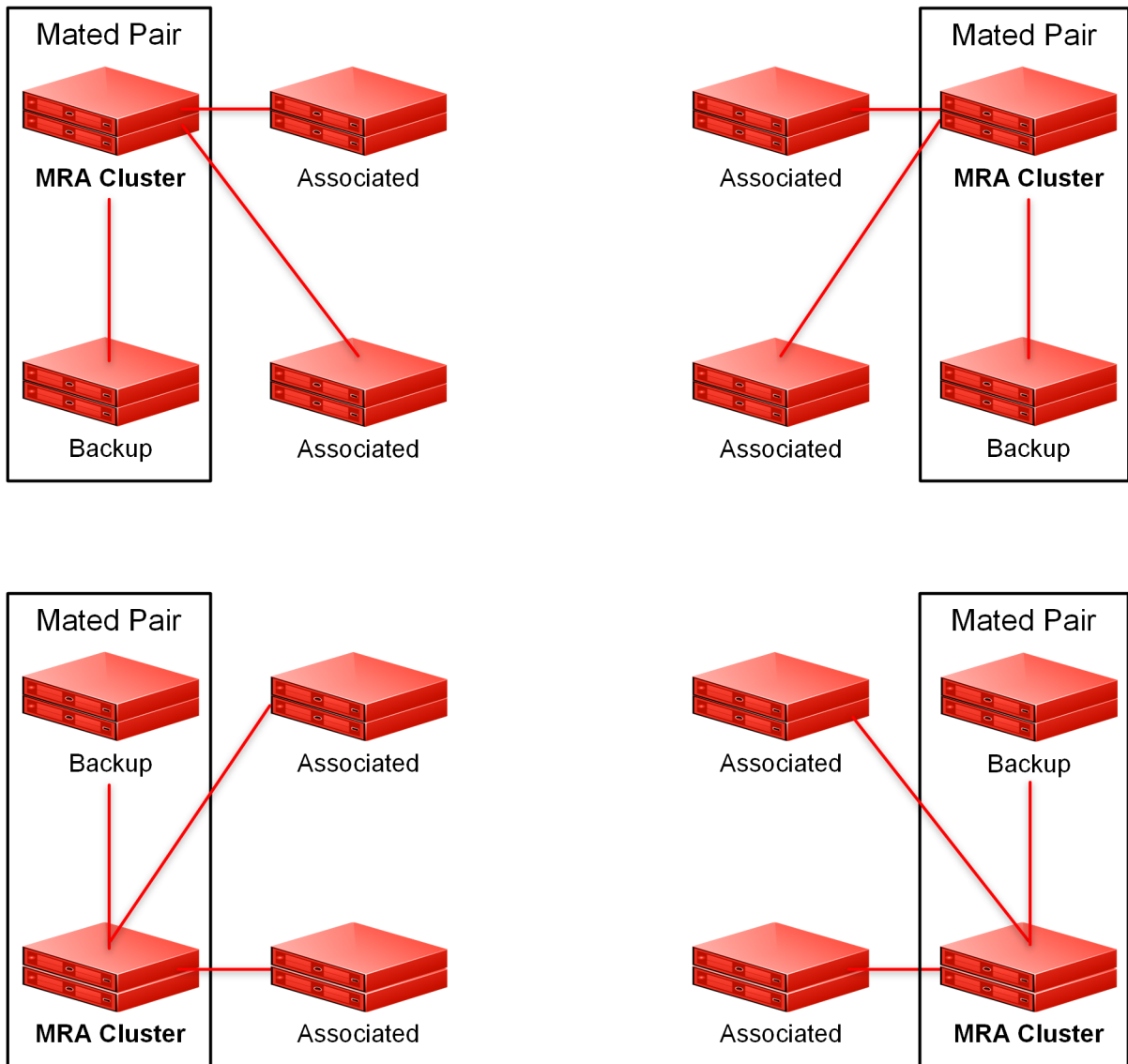


Figure 2: Backup and Associated MRA Clusters and Mated Pairs

GUI Overview

You interact with the CMP system through an intuitive and highly portable graphical user interface (GUI) supporting industry-standard web technologies (, HTTP, HTTPS, IPv4, IPv6, and XML). [Figure 3: Structure of the CMP Wireless GUI](#) shows the layout of the CMP GUI.

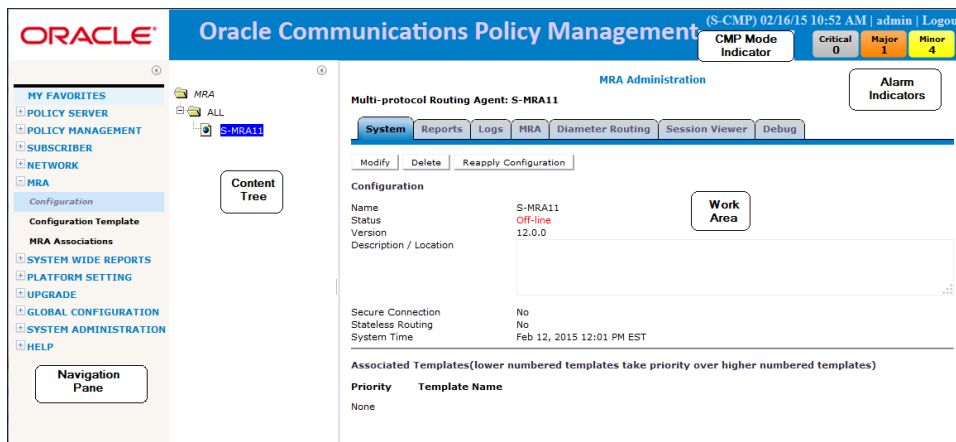


Figure 3: Structure of the CMP Wireless GUI

- Navigation Pane** Provides access to the various available options configured within the CMP system.
- You can bookmark options in the navigation pane by right-clicking the option and selecting **Add to Favorite**. Access the bookmarks clicking the **My Favorites** folder at the top of the navigation pane. Within the **My Favorites** folder, you can arrange or delete options by right-clicking the option and selecting **Move Up**, **Move Down**, or **Delete from Favorite**.
- You can collapse the navigation pane to make more room by clicking the button in the top right corner of the pane (⌵). Click the button again to expand the pane.
- Content Tree** Contains an expandable/collapsible listing of all the defined items for a given selection. For content trees that contain a group labeled **ALL**, you can create customized groups that display in the tree.
- The content tree section is not visible with all navigation selections.
- You can collapse the content tree to make more room by clicking the button in the top right corner of the pane (⌵). Click the button again to expand the tree. You can also resize the content tree relative to the work area.
- Work Area** Contains information that relates to choices in both the navigation pane and the content tree. This is the area where you perform all work.
- Alarm Indicators** Provides visual indicators that show the number of active alarms.
- CMP Mode Indicator** Indicates the current CMP mode. **NW-CMP** for Network mode or **S-CMP** for System mode. If there is not a mode indicated, the mode is **CMP**.

Chapter 3

Configuring a CMP System and MRA, MPE Devices

Topics:

- *Configuring the CMP to Manage the MRA.....21*
- *Modifying MRA System Settings, Grouping or deleting MRA devices.....24*
- *Role and Scope Configuration.....38*
- *MRA Advanced Configuration Settings.....40*
- *Managing Configuration and Virtual Templates.....45*
- *Configuring Topology Hiding for the Gx Application.....50*

An MRA is a standalone entity that uses the Oracle Communications Policy Management Configuration Management Platform (CMP) system and an Multimedia Policy Engine (MPE) device.

Note: This document assumes that all CMP systems as well as MRA, and MPE devices are operational. Also, the procedures used in this guide are MRA specific; for additional CMP system and MPE device configuration information, refer to the *CMP Wireless User's Guide* and *Policy Wizard Reference Guide*.

Configuring the CMP to Manage the MRA

The CMP is used to manage all MRA functions. Before this can occur, the CMP must be configured to:

- Access and manage the MRA
- Add the MRA to the CMP

Creating an MRA Group

To create an MRA group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **MRA Administration** page opens in the work area.
3. Click **Create Group**.
The **Create Group** page opens.
4. Enter the name of the new CMP group.
The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
5. When you finish, click **Save**.

The MRA group is created.

Deleting an MRA Group

Deleting an MRA group also deletes any associated sub-groups. However, any MRA cluster profiles associated with the deleted groups or sub-groups remain in the **ALL** group. You cannot delete the **ALL** group.

To delete an MRA group or sub-group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. Select the MRA group or subgroup from the content tree.
The contents of the selected MRA group are displayed.
3. Click **Delete**.
A confirmation message displays.
4. Click **OK** to delete the selected group.

The MRA group is deleted.

Configuring the CMP System to Manage an MRA Cluster

The Policy Front End (also known as the MRA) device is a standalone entity that supports MPE devices. The CMP system is used to manage all MRA functions. Before this can occur, the CMP operating mode must support managing MRA clusters.

To reconfigure the CMP operating mode, complete the following:



Caution: CMP operating modes should only be set in consultation with My Oracle Support. Setting modes inappropriately can result in the loss of network element connectivity, policy function, OM statistical data, and cluster redundancy.

CAUTION

1. From the **Help** navigation pane, select **About**.
The **About** page opens, displaying the CMP software release number.
2. Click the **Mode** button.
Consult with My Oracle Support for information on this button.
The **Mode Settings** page opens.
3. At the bottom of the page, select **Manage MRAs**.
4. Click **OK**.
The browser page closes and you are automatically logged out.
5. Refresh the browser page.
The **Welcome admin** page is displayed.

You are now ready to define an MRA cluster profile, specify network settings for the MRA cluster, and associate MPE devices with the MRA cluster.

Configuring Protocol Options for an MRA Device

To configure protocol options on an MRA device:

1. From the **MRA** section of the navigation pane, select **Configuration**.
2. From the content tree, select the MRA device.
The **MRA Administration** page opens.
3. On the **MRA Administration** page, select the **MRA** tab.
The current configuration options are displayed.
4. Click **Modify** and define options as necessary.
Table 2: MRA Protocol Configuration Options defines available options that pertain specifically to MRA devices. (The options may vary depending on the configuration mode of the system.)
5. When you finish, click **Save**.

Table 2: MRA Protocol Configuration Options

Attribute	Description
Subscriber Indexing	Note: The indexing parameters to use depend on what user IDs are needed for correlating various messages to ensure they all end up on the same MPE device for the same user. If you are unsure

Attribute	Description
	which indexing methods to configure, contact My Oracle Support (https://support.oracle.com).
Index by IPv4	Select if the MRA devices in the association should index by IPv4 address.
Index by IP-Domain-Id	Select if the MRA devices in the association should index by IP domain ID. The combination of framed IPv4 address and IP domain ID ensures a globally unique binding, even if the same IPv4 address is locally assigned in multiple networks.
Index by IPv6	Select if the MRA devices in the association should index by IPv6 address.
Index by Username	Select if the MRA devices in the association should index by account ID.
Index by NAI	Select if the MRA devices in the association should index by network access ID.
Index by E.164 (MSISDN)	Select if the MRA devices in the association should index by E.164 phone number.
Index by IMSI	Select if the MRA devices in the association should index by IMSI number.
Index by Session ID	Select if the MRA devices in the association should index by session ID.
Overrides by APN	Select to perform subscriber indexing for a specific IP address and a specific APN name. 1. In the Overrides by APN section, click Add. 2. Enter the APN name and click Save to enable Index by IPv4, Index by IP-Domain-Id, Index by IPv6, Index by Username, Index by NAI, Index by E.164 (MSISDN), Index by IMSI, or Index by Session ID. You can create APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.
Primary Indexing	Select from the list to set to the type of index that is expected for messages that create bindings, for example Gx CCR-I. Note: The type of index selected for primary indexing must also be selected either as an "Index by IMSI" or "Index by E.164" depending on the configuration.  Primary Index cannot be changed on a system that has already created bindings without suffering data loss.
Protocol Timer Profile	The timer profile to use.
Diameter	

Attribute	Description
Diameter Realm	Specifies the MRA device's domain of responsibility (for example, galactel.com).
Diameter Identity	Specifies the Diameter identity of the MRA device (for example, pgw1024.galactel.com).
S9	
Primary DEA	If one or more Diameter Edge Agents is defined, you can select the primary agent from the list. For information on defining a DEA, see Configuring Diameter Peers .
Secondary DEA	If multiple Diameter Edge Agents are defined, you can select the secondary agent from the list. If you select both primary and secondary DEAs, the MRA device establishes a connection to both DEAs. If the primary connection is down, the MRA device sends messages over the secondary connection; once the primary connection is back up, communication reverts back to it.
RADIUS Configuration	
RADIUS Enabled	When selected, the MRA device processes RADIUS messages; when deselected, RADIUS messages are ignored. The default is deselected.
Secret	Enter the default passphrase (a text string). This shared secret value is used when no shared secret is defined for a specific RADIUS network element. If you enter no passphrase, and either of the fields in the associated network elements are not set as well, then the MRA device ignores RADIUS requests and responses. The default is radius .

Modifying MRA System Settings, Grouping or deleting MRA devices

Once an MRA has been created you can change the system settings, group the MRA devices, or delete an MRA device from the CMP.

Defining an MRA Cluster Profile

You must define a profile for each MRA cluster you are managing. To define an MRA cluster profile:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **MRA Administration** page opens in the work area.
3. Click **Create Multi-protocol Routing Agent**.
The **New MRA** page opens.

4. Enter information as appropriate for the MRA cluster:
 - a) **Associated Cluster** (required) — Select the MRA cluster from the list.
 - b) **Name** (required) — Enter a name for the MRA cluster.
The name can be up to 250 characters long. The name can contain any alphanumeric characters except quotation marks (") and commas (,).
 - c) **Description/Location** (optional) — Free-form text.
Enter up to 250 characters.
 - d) **Secure Connection** — Select to enable a secure HTTP connection (HTTPS) instead of a normal connection (HTTP).
The default is a non-secure (HTTP) connection.
 - e) **Stateless Routing** — Select to enable stateless routing. In stateless routing, the MRA cluster only routes traffic; it does not process traffic.
The default is stateful routing.
5. When you finish, click **Save**.

The MRA cluster profile is defined. If you are setting up multiple MRA clusters, you must define multiple cluster profiles. Repeat the above steps to define additional profiles.

Modifying an MRA Cluster Profile

To modify MRA cluster profile settings:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the MRA cluster profile.
The **MRA Administration** page opens in the work area.
3. Select the **System** tab of the **MRA Administration** page
4. Click **Modify**.
The **Modify System Settings** page opens.
5. Modify MRA system settings.
6. When you finish, click **Save**.

The MRA cluster profile settings are modified.

Deleting an MRA Cluster Profile from an MRA Group

Removing an MRA cluster profile from an MRA group does not delete the MRA cluster profile from the **ALL** group, so it can be used again if needed. Removing an MRA cluster profile from the **ALL** group removes it from all other groups.

To delete an MRA cluster profile from an MRA group (other than **ALL**):

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the MRA group.
The **MRA Administration** page opens in the work area, displaying the contents of the selected MRA group.

3. Remove the MRA cluster profile using one of the following methods:
 - On the **MRA Administration** page, click the **Delete** icon, located to the right of the MRA cluster profile you want to remove.
 - From the content tree, select the MRA cluster profile; the **MRA Administration** page opens. On the **System** tab, click **Remove**.

The MRA cluster profile is removed from the group.

Reversing Cluster Preference

You can change the preference, or predilection, of the servers in a cluster to be active or spare. This setting is only available when the system has been configured for georedundancy.

To reverse cluster preference:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens.
2. Select the cluster from the content tree.
The **Topology Configuration** page opens, displaying information about the selected cluster.
3. Click **Modify Cluster Settings**.
The fields become editable.
4. In the **Cluster Settings** section of the page, toggle the **Site Preference** between **Normal** and **Reverse**.
5. Click **Save**.

The cluster preferences are reversed.

Forcing a Server into Standby Status

You can change the status of a server in a cluster to Forced Standby. A server placed into Forced Standby status is prevented from assuming the role Active. You would do this, for example, to the active server prior to performing maintenance on it.

When you place a server into forced standby status, the following happens:

- If the server is active, the server is demoted.
- The server will not assume the active role, regardless of its status or the roles of the other servers in the cluster.
- The server continues as part of its cluster, and reports its status as Forced-Standby.
- The server coordinates with the other servers in the cluster to take the role Standby or Spare.



CAUTION

Caution: If you force all servers in a cluster into Standby status, you can trigger a site outage.

To force a server into standby status:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Topology Configuration** page opens, displaying a cluster settings table listing information about the clusters defined in the topology.
2. In the cluster settings table, in the row listing the cluster containing the server you want to force into standby status, click **View**.

The **Topology Configuration** page displays information about the cluster.

3. Select the server. Click **Modify Server-A** or **Modify Server-B**, as appropriate.
4. Select **Forced Standby**.
5. Click **Save**.

The server is placed in standby status.

Setting Up a Non-CMP Cluster

A non-CMP cluster can be one of the following server types:

- MPE
- MRA

Before defining a non-CMP cluster, ensure the following:

- The server software is installed on all servers in the cluster
- The servers have been configured with network time protocol (NTP), domain name server (DNS), IP Routing, and OAM IP addresses
- The server IP connection is active
- The application is running on at least one server

Note: If you are creating a cluster in a georedundant system, see [Setting Up a Georedundant Cluster](#).

To define a cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens.
2. Click **Add MPE/MRA Cluster**.
The **Topology Configuration** page opens. Each section of the **Topology Configuration** page can be collapsed or expanded.
3. Define the general settings for the cluster in the General Settings section of the page.
 - a) **Name** (required) — Name of the cluster. Enter up to 250 characters, excluding quotation marks (") and commas (,).
 - b) **Appl Type** — Select the type of server:
 - MPE (default)
 - MRA
 - c) **HW Type** — Select the type of hardware:
 - C-Class (default)
 - C-Class (**Segregated Traffic**) (for a configuration where Signaling and other networks are separated onto physically separate equipment)
 - NETRA (for a Netra server)
 - RMS (for a rack-mounted server)
 - VM (for a virtual machine)
 - d) **OAM VIP** (optional) — The OAM VIP is the address the CMP cluster uses to communicate with the MPE or MRA cluster. Enter up to two OAM VIP addresses (one IPv4 and one IPv6) and their masks.

Enter the address in the standard dot format and the subnet mask in CIDR notation from 0–32 (IPv4), or standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128 (IPv6).

- e) **Signaling VIPs** (required) — The signaling VIP is the IP address a PCEF device uses to communicate with a cluster. Click **Add New VIP** to add a VIP to the system. A cluster supports the following redundant communication channels for carriers that use redundant signaling channels.
 - SIG-A
 - SIG-B

At least one signaling VIP is required.

You can enter up to four IPv4 or IPv6 addresses and masks of the signaling VIP addresses.

For each new VIP, enter the address and mask in the New Signaling VIP dialog and select an external signalling channel.

For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

4. Define the general network configuration for the C-Class, C-Class segregated, or Netra servers in the Network Configuration section of the page. This section is not available for RMS.
 - a) Enter the VLAN IDs, in the range 1–4095 for the following:
5. Define the settings for **Server-A** in the Server-A section of the page.
 - a) **IP** (required) — The IP address of the server. Up to two IP addresses can be entered (one IPv4 and one IPv6). Use the standard dot-formatted IP address string for an IPv4 address, and the standard 8-part colon-separated hexadecimal string format for an IPv6 address.
 - b) **IP Preference** — Specify the preferred IP version, either **IPv4** or **IPv6**. If IPv6 is selected, the server will prefer to use the IPv6 address for communication. If neither an IPv6 OAM IP nor a static IP address is defined, the IPv6 radio button cannot be selected here. Similarly, If neither an IPv4 OAM IP nor a static IP address is defined, the IPv4 radio button isn't accessible.
 - c) **HostName** — The name of the server. This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

Note: If the server has a configured server IP address, you can click **Load** to retrieve the remote server host name. If retrieval fails, you must enter the host name.

 - d) **Forced Standby** — Select to put the server into forced standby. (By default, Server A will be the initial active server of the cluster.)
6. (Optional) Click **Add Server-B** and enter the information for the standby server of the cluster. See step [Step 5](#) for information about the fields. Server-B is defined for the cluster.
7. When you finish, click **Save**.
The following message displays: The VLAN IDs on the page must match the VLAN IDs configured on the server. A mismatch will cause HA to fail. Please confirm that the VLAN IDs are correct before saving.
8. Click **OK**.
9. If you are setting up multiple clusters, repeat the steps.

The cluster is defined.

Figure 4: Sample MRA Cluster Topology Configuration shows the configuration for a georedundant (two-site) MRA cluster, using SIG-B for a replication network and OAM for the backup heartbeat network, with eight WAN replication streams.

Topology Settings

- All Clusters
 - CMP Site1 Cluster
 - Doc-Cluster-1
 - Doc-Cluster-2
 - Doc-MRA-Cluster-2
 - MPE09

General Settings

Name: MRA-112

Appl Type: MRA

HW Type: C-Class

OAM VIP:

Signaling VIPs:

Network Configuration

General Network

Name	VLAN ID
OAM	3
SIG-A	5
SIG-B	6

Server-A

Delete Server-A

General Settings

IP:

IP Preference: ☒ IPv4 ☐ IPv6

HostName:

Forced Standby: ☐

Server-B

Delete Server-B

General Settings

IP:

IP Preference: ☒ IPv4 ☐ IPv6

HostName:

Forced Standby: ☐

Save Cancel

Figure 4: Sample MRA Cluster Topology Configuration

Setting Up a Georedundant Cluster

This procedure contains the steps for setting up a non-CMP cluster:

- MPE
- MRA

Before defining a cluster, ensure the following:

- The server software is installed on all servers in the cluster
- The servers have been configured with network time protocol (NTP), domain name server (DNS), IP Routing, and OAM IP addresses
- The server IP connection is active
- The server application is running on at least one server

If your system is not set up for georedundancy, see [Setting Up a Non-CMP Cluster](#).

To define a cluster in a georedundant system:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**. The **Cluster Configuration** page opens.
2. From the content tree, select the **All Clusters** folder.

The defined clusters are listed.

3. Click **Add MPE/MRA Cluster**.

The **Topology Configuration** page opens. Each section of the **Topology Configuration** page can be collapsed or expanded.

4. Define the general settings for the cluster in the **Cluster Settings** section of the page:

- a) **Name** (required) — Name of the cluster. Enter up to 250 characters, excluding quotation marks (") and commas (,).
- b) **Appl Type** — Select the application type:
 - **MPE** (default)
 - **MRA**
- c) **Site Preference** — Select **Normal** (default) or **Reverse**.
- d) **DSCP Marking** — Select the type of Differentiated Services Code Point (DSCP) marking for replication traffic. The valid code points are **AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43** (assured forwarding), **CS1, CS2, CS3, CS4, CS5, CS6, CS7** (class selector), **EF** (expedited forwarding), or **PHB(None)** (default for no marking). For information on DSCP marking, see [Setting Up a Non-CMP Cluster](#).
- e) **Replication Stream Count** — Select the number of redundant TCP/IP socket connections (streams) to carry replication traffic between sites. Up to 8 streams can be configured. The default value is 1 stream.
- f) **Replication & Heartbeat** — Select a network to carry inter-site replication and heartbeat traffic. This field only appears if the system supports georedundancy:
 - **None** (default)
 - **OAM**
 - **SIG-A**
 - **SIG-B**
 - **REP**

A warning icon () indicates that you cannot select a network until you define a static IP address on all servers of both sites.

- g) **Backup Heartbeat** — Select a network to carry inter-site backup heartbeat traffic. This field only appears if the system supports georedundancy:
 - **None** (default)
 - **OAM**
 - **SIG-A**
 - **SIG-B**
 - **REP**

A warning icon () indicates that you cannot select a network until you define a static IP address on all servers of both sites.

5. Define the primary site settings in the **Primary Site Settings** section of the page:

- a) **Site Name** — Select **Unspecified** (default) or the name of a previously defined site. If you select **Unspecified**, you create a non-georedundant site, and cannot add a secondary site. You can assign multiple clusters to the same site.

Note: To import the hardware type and VLAN settings from the selected site, select **Use Site Configuration**. When this is selected the **HW Type** and **VALN IDs** become read only.

To edit the field, clear the **Use Site Configuration** checkbox. If **Unspecified** is selected for the site name, the **Use Site Configuration** option becomes unavailable.

b) **HW Type** — Select the hardware type:

- **C-Class** (default)
- **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment)
- **NETRA** (Netra server)
- **RMS** (rack-mounted server)
- **VM** (virtual machine)

c) **OAM VIP** (optional) — The OAM VIP is the address the CMP cluster uses to communicate with the cluster. Enter the address and mask of the OAM virtual IP (VIP) address.

For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

d) **Signaling VIPs** — The signaling VIP is the IP address a PCEF device uses to communicate with the cluster. A non-CMP cluster supports redundant communication channels, named SIG-A and SIG-B, for carriers who use redundant signaling channels.

At least one signaling VIP is required.

Click **Add New VIP** to add a VIP to the system. You can enter up to four IPv4 or IPv6 addresses and masks of the signaling VIP addresses.

For each new VIP, enter the address and mask in the New Signaling VIP dialog. Select **SIG-A** or **SIG-B** to indicate whether the cluster will use an external signaling network.

For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

e) **General Network VLAN ID** — This field appears if you selected **NETRA**, **C-Class**, or **C-Class (Segregated Traffic)**. Enter the **OAM**, **SIG-A**, and **SIG-B** VLAN IDs, in the range 1–4095. The defaults are 3 for the OAM network and server IP, 5 for the SIG-A network, and 6 for the SIG-B network.

f) **User Defined Network** — This field appears if you selected **C-Class** or **C-Class (Segregated Traffic)**. Enter the REP network VLAN ID, in the range 1–4095.

6. Define Server-A in the **Server-A** section of the page:

- a) **IP** (required) — The IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.
- b) **IP Preference** — Specify the preferred IP version, either **IPv4** or **IPv6**. If IPv6 is selected, the server will prefer to use the IPv6 address for communication. If neither an IPv6 OAM IP nor a static IP address is defined, the IPv6 radio button cannot be selected here. Similarly, If neither an IPv4 OAM IP nor a static IP address is defined, the IPv4 radio button isn't accessible.
- c) **HostName** — The name of the server. This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

Note: If the server has a configured server IP, you can click **Load** to retrieve the remote server host name. If the retrieve fails, you must enter the host name.

- d) **Forced Standby** — Select to put Server A into forced standby. (By default, Server A will be the initial active server of the cluster.)
 - e) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the New Path dialog, enter an IP address and mask, and select the network.
 - **SIG-A**
 - **SIG-B**
 - **REP**
 - **BKUP** (if the hardware type is **C-Class(Segregated Traffic)** or **NETRA**)
7. (Optional) Define Server-B in the **Server-B** section of the page. Click **Add Server-B** and enter the standby server information for the cluster:
- a) **IP** (required) — The IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.
 - b) **IP Preference** — Specify the preferred IP version, either **IPv4** or **IPv6**. If IPv6 is selected, the server will prefer to use the IPv6 address for communication. If neither an IPv6 OAM IP nor a static IP address is defined, the IPv6 radio button cannot be selected here. Similarly, if neither an IPv4 OAM IP nor a static IP address is defined, the IPv4 radio button is not accessible.
 - c) **HostName** — The name of the server. This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).
- Note:** If the server has a configured server IP address, you can click **Load** to retrieve the remote server hostname. If retrieval fails, you must enter the hostname.
- d) **Forced Standby** — Select to put Server A into forced standby. (By default, Server A will be the initial active server of the cluster.)
 - e) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the **New Path** dialog, enter an IP address and mask, and select the network:
 - **SIG-A**
 - **SIG-B**
 - **REP**
 - **BKUP** (if the hardware type is **NETRA**)
8. Define the secondary site information in the **Secondary Site Settings** section of the page:
- a) **Site Name** — Select **Unspecified** (default) or the name of a previously defined site. This site name must be different from the primary site name. If you select **Unspecified**, you create a non-georedundant site, and cannot add a secondary site. You can assign multiple clusters to the same site.
- Note:** To import the hardware type and VLAN settings from the from the selected site, select **Use Site Configuration**. When this is selected the **HW Type** and VLAN IDs become read only. To edit the field, clear the **Use Site Configuration** checkbox. If **Unspecified** is selected for the site name, the **Use Site Configuration** option becomes unavailable.
- b) **HW Type** — Select the hardware type:
 - **C-Class** (default)

- **C-Class(Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment)
 - **NETRA** (Netra server)
 - **RMS** (rack-mounted server)
 - **VM** (virtual machine)
- c) **OAM VIP** (optional) — Enter the address and mask of the OAM virtual IP (VIP) address. The OAM VIP is the address the CMP cluster uses to communicate with the cluster.
- For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.
- d) **Signaling VIPs** — The signaling VIP is the IP address a PCEF device uses to communicate with a cluster. Clusters support redundant communication channels, named SIG-A and SIG-B, for carriers that use redundant signaling channels.
- At least one signaling VIP is required.
- Click **Add New VIP** to add a VIP to the system. You can enter up to four IPv4 or IPv6 addresses and masks of the signaling VIP addresses.
- For each new VIP, enter the address and mask in the New Signaling VIP dialog. Select **SIG-A** or **SIG-B** to indicate whether the cluster will use an external signaling network.
- For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.
- e) **General Network VLAN ID** — This field appears if you selected **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**. Enter the **OAM**, **SIG-A**, and **SIG-B** VLAN IDs, in the range 1–4095. The defaults are 3 for the OAM network and server IP, 5 for the SIG-A network, and 6 for the SIG-B network.
- f) **User Defined Network** — This field appears if you selected **C-Class** or **C-Class(Segregated Traffic)**. Enter the REP network VLAN ID, in the range 1–4095.
9. Define Server-C in the **Server-C** section of the page. If you define a secondary site, you must define a spare server. Click **Add Server-C** and define the information for the spare server:
- a) **IP** (optional) — The IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.
- b) **IP Preference** — Specify the preferred IP version, either **IPv4** or **IPv6**. If IPv6 is selected, the server will prefer to use the IPv6 address for communication. If neither an IPv6 OAM IP nor a static IP address defined, the IPv6 radio button cannot be selected here. Similarly, If neither an IPv4 OAM IP nor a static IP address is defined, the IPv4 radio button isn't accessible.
- c) **HostName** — The name of the server. This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).
- Note:** If the server has a configured server IP address, you can click **Load** to retrieve the remote server hostname. If retrieval fails, you must enter the hostname.
- d) **Forced Standby** — Select **Forced Standby** to ensure that the server is in standby mode.
- e) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the New Path dialog, enter an IP address and mask, and select the network:

- SIG-A
- SIG-B
- REP

10. When you finish, click **Save**.

You are prompted, The VLAN IDs on the page must match the VLAN IDs configured on the server. A mismatch will cause HA to fail. Please confirm that the VLAN IDs are correct before saving..

11. Click **OK**.

12. If you are setting up multiple clusters, repeat the procedure.

The cluster is defined.

Figure 5: Sample MPE Cluster Topology Configuration shows the configuration for a georedundant (two-site) MPE cluster, using SIG-B for a replication network and OAM for the backup heartbeat network, with eight WAN replication streams.

Configuring a CMP System and MRA, MPE Devices

Topology Configuration

Cluster Settings

Cluster Settings

Name

Appl Type

Site Preference

DSCP Marking

Replication Stream Count

Replication & Heartbeat ☒

Backup Heartbeat ☒

None ☐

OAM ☒ SIG-A ☒ SIG-B ☒ REP ☒

Primary Site Settings

General Settings

Site Name

HW Type

OAM VIP

Signaling VIPs

Add New VIP Edit Delete

Use Site Configuration ☐

Network Configuration

General Network

VLAN ID

OAM

SIG-A

SIG-B

User Defined Network

VLAN ID

REP

Server-A

Delete Server-A

General Settings

IP

Add New IP Edit Delete

IP Preference ☐ IPv4 ☐ IPv6

HostName

Forced Standby ☐

Path Configuration

Static IP

Add New Edit Delete

Server-B

Delete Server-B

General Settings

IP

Add New IP Edit Delete

IP Preference ☐ IPv4 ☐ IPv6

HostName

Forced Standby ☐

Path Configuration

Static IP

Add New Edit Delete

Secondary Site Settings

General Settings

Site Name

HW Type

OAM VIP

Signaling VIPs

Add New VIP Edit Delete

Use Site Configuration ☐

Network Configuration

General Network

VLAN ID

OAM

SIG-A

SIG-B

User Defined Network

VLAN ID

REP

Server-C

Delete Server-C

General Settings

IP

Add New IP Edit Delete

IP Preference ☐ IPv4 ☐ IPv6

HostName

Forced Standby ☐

Path Configuration

Static IP

Add New Edit Delete

Figure 5: Sample MPE Cluster Topology Configuration

Configuring Diameter Peers

Policy Management MPE and MRA devices support Diameter Rx, Gq, Ty, Gxx, Gx, Gy, S9, and Sd applications. For example, traffic control is supported using the Diameter Gx application. When a subscriber attaches to the network (for example, using a phone) via a GGSN (Gateway GPRS Support Node), the GGSN can establish a session with both MPE and MRA devices using a Diameter Gx CCR (Credit Control Request) message. The MPE and MRA devices respond to the request with a Gx CCA (Credit Control Answer) message.

Complete these steps to configure Diameter peers for either an MPE or MRA device:

1. From the **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server or MRA groups.
2. From the content tree, select the MPE or MRA device.
The **Administration** page for that device opens in the work area.
3. Select the **Diameter Routing** tab.
The Diameter Routing configuration settings appear.
4. Click **Modify Peers**.
The **Modify the Diameter Peer Table** page opens.
5. Add a peer to the table.
 - a) Click **Add**.
The **Add Diameter Peer** window opens.

Figure 6: Add Diameter Peer

- b) Enter the following:
 - **Configured MRAs/MPEs (optional)** — If you are defining an existing Policy Management cluster as a Diameter peer, select it from this list; the other fields are populated.
 - **Name** (required) — Name of the peer device (which must be unique within the CMP database).

- **IP Address** (required) — IP address in IPv4 or IPv6 format of the peer device.
If not specified, the MPE device uses a DNS lookup to resolve the value in the Diameter Identity field into an IP address and try to connect.
- **Diameter Realm** (required) — The peer's domain of responsibility (for example, **galactel.com**).
- **Diameter Identity** (required) — Fully qualified domain name (FQDN) of the peer device (for example, **mpe33.galactel.com**).
- **Protocol Timer Profile** — Select from the list.
- **Initiate Connection** — Check mark to initiate an S9 connection for this Diameter peer. The default transport method is TCP, but can be changed to SCTP in the following **Transport** field. Turned on (check marked) by default.
- **Transport** — Select either **TCP** or **SCTP** (shown as Transport Info in the Diameter peer table). For TCP select **Connections** (range 1-8, default 1). For SCTP select **Max Incoming Streams** and **Max Outgoing Streams**(1-8 connections, default is 8) which will be shown as Connection Info in the Diameter peer table.
- **IP Port** — Enter the IP Port number.
- **Watchdog Interval** — Enter the watchdog interval in seconds. The default is 30 seconds.
- **Reconnect Delay** — Enter the response time in seconds. The default is 3 seconds.
- **Response Timeout** — Enter the response timeout interval in seconds. The default is 5 seconds.

c) When you finish, click **Save**.

6. Add, edit or delete additional Diameter Peers.

- Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.
 4. When you finish, click **Save**. The entry is added to the table
- Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. When you finish, click **Save**. The entry is updated in the table.
- Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.

7. When you finish, click **Save**.

Role and Scope Configuration

When configured in MRA mode, the CMP system defines default user accounts with roles and scopes that allow for control of MRA devices. If you want to define additional users to control MRA devices, you need to add appropriate roles and scopes.

Configuring an MRA Role

MRA configuration also provides the functionality for privilege control through Role Administration. The **Role Administration** page includes a section named **MRA Privileges** that contains a privilege setting option named **Configuration**. To access this option:

1. In the **System Administration** section of the navigation pane, click **User Management** and then click **Roles**.
The **Role Administration** page opens.
2. Click **Create Role**.

Role Administration

New Role

Name:

Description / Location:

Policy Server Privileges

Configuration	Hide
Application	Hide
Match Lists	Hide
Quotas	Hide
Traffic Profiles	Hide
Retry Profiles	Hide
Charging Server	Hide
Time Period	Hide
Monitoring Key	Hide
AVP Definition	Hide
Global Configuration Settings	Hide

Subscriber Privileges

Entitlement	Hide
Subscriber Tier	Hide
Quota Usage	Hide

SPR Privileges

Subscriber Data	Hide
-----------------	------

Network Privileges

Network Element	Hide
-----------------	------

MRA Privileges

Configuration	Hide
---------------	------

Figure 7: New Role Page

3. Enter the following information:
 - a) **Name** — The name for the new role.
 - b) **Description/Location** (optional) — Free-form text.
 - c) **MRA Privileges** — There are three types of privileges for MRA configuration: Hide, Read-Only and Read-Write.
 - **Hide** — No operation can be done on MRA configuration.
 - **Read-Only** — Only read operations can be done on MRA configuration (that is, settings can be viewed but not changed).
 - **Read-Write** — Both read and write operations can be done on MRA configuration (that is, settings can be viewed and changed).
4. When you finish, click **Save**.
Privileges are assigned to the role.

Configuring the Scope for an MRA

MRA configuration provides scope functionality which allows the administrator to configure scopes for MRA groups, which provides the context for a role. The default scope of Global contains all items defined within the CMP. Once a scope is defined, the administrator can apply it to a user. A user can only manage the MRA devices in the user defined scope. To configure a scope, complete the following:

1. In the **System Administration** section of the navigation pane, click **User Management** and then click **Scopes**.
The **Scope Administration** page opens.
2. Click **Create Scope**.

Scope Administration

New Scope

Name

Description / Location

Select the Policy Server Group(s) included in this scope:

Policy Server Groups

Select the Network Element Group(s) included in this scope:

Network Element Groups

Select the MRA Group(s) included in this scope:

MRA Groups

Figure 8: Create Scope Page

3. Enter the following information:
 - a) **Name** — The name for the new scope.
 - b) **Description/Location** (optional) — Free-form text.
 - c) Select the MRA group(s) this scope can control.
4. When you finish, click **Save**.
The scope is defined.

MRA Advanced Configuration Settings

The advanced configuration settings provide access to attributes that are not normally configured, including session cleanup settings, stateful MRA settings, and defining configuration keys.

Configuring MRA Session Clean Up Settings

Normally, a binding for a subscriber is maintained on only one MRA device. However, due to server or communication disruptions, it is possible for multiple MRA devices to create duplicate bindings. When a query returns duplicate bindings, the oldest is used.

The MRA device periodically runs a cleanup task to check for and remove stale and suspect bindings and sessions, which are defined as follows:

- A session is stale if its timestamp is greater than the Session Validity Time value for the MRA device.
- A binding is stale if its timestamp is greater than the Binding Validity Time value for the MRA device.
- A binding is suspect if it was created while one or more MRA devices were not reachable.

To customize stale session cleanup:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA device.
The **MRA Administration** page opens.
3. Select the **MRA** tab.
The current MRA configuration settings are displayed.
4. Click **Advanced**.
Session Clean Up settings are displayed and can be edited.

Table 3: Session Clean Up Settings

Attribute	Description
Check for Stale Sessions in Binding	Select to check for stale sessions in bindings during the cleanup cycle. If not selected, then the system only checks to see if the entire binding is stale. The default is selected (check for stale sessions).
Check for Stale Bindings	Select to check for stale bindings during the cleanup cycle. If not selected, then the system will not check if the binding is stale. If Check For Stale Sessions in Binding is selected, then the system still iterates through the enclosed session information to detect and clean up stale sessions. The default is deselected (do not check for stale bindings).
Check for Suspect Bindings	Select to check for suspect bindings during the cleanup cycle. If not selected, the system checks if the entire binding is stale. If Check for Stale Sessions In Binding is selected, stale sessions enclosed in the suspect binding are cleaned up as well. The default is selected (check for suspect bindings).
Session Cleanup Start Time	Defines the time of day when the cleanup task occurs. Specify either Start Time or Interval by clicking the associated radio button and entering or selecting a value. You can specify a time in 24-hour format from the drop-down menu. No default value is defined.

Binding Cleanup Interval (hour)	Defines the interval, in hours, at which the cleanup task runs. Specify either Start Time or Interval by clicking the associated radio button and entering or selecting a value from 0 to 24 hours. A value of 0 disables cleanup. The default is 24 hours. Note: Do not modify this setting without consulting Oracle Customer Service.
Max Duration For Binding Iteration (hour)	Defines the maximum duration, in hours, to iterate through the bindings. The default is 2 hours. The valid range is 1 to 2 hours. Note: Do not modify this setting without consulting Oracle Customer Service.
Binding Validity Time (hours)	Defines the number of hours after which the binding is declared stale. The default is 240 hours. The valid range is 1 to 240 hours.
Max Binding Cleanup Rate (bindings/sec)	Defines the rate, in bindings per second, at which the cleanup task attempts to clean stale bindings. The default is 50 sessions/sec. The valid range is 1 to 50 sessions/sec. Note: Do not modify this setting without consulting Oracle Customer Service.
Max Binding Iteration Rate (bindings/sec)	Defines the maximum rate, in bindings per second, at which the cleanup task iterates through the bindings database. The default is 1000 bindings/sec. The valid range is 1 to 1000 bindings/sec. Note: Do not modify this setting without consulting Oracle Customer Service.
Session Validity Time (hours)	Note: Do not modify this setting without consulting Oracle Customer Service.
Max Session Validity Time (hours)	Note: Do not modify this setting without consulting Oracle Customer Service.
Scheduler Granularity (sec)	Defines the adaptor scheduler's granularity in seconds. The default is 1 second. The valid range is 1-5 seconds.
Scheduler Thread Count	Defines the number of threads used by the cleanup scheduler to schedule jobs. The default is 2 threads. the valid range is 1 to 4 threads.
Cleanup Session Validity Time (hours)	Defines the number of hours after which a session in a binding is declared stale. The default is 120 hours. The valid range is 1 to 120 hours.

- Click **Save**.
The settings are applied to the MRA.

Redirecting Traffic to Upgrade or Remove an MRA

When the software for an MRA needs to be upgraded or an MRA needs to be removed from an MRA cluster, the traffic or potential traffic must be redirected to the other MRA within the cluster, and the current sessions released. To do this, traffic on clustered MRAs is redirected on to another MRA, allowing the traffic-free MRA to be replaced in the cluster or to have its software upgraded. During this process, the MRA that is to be replaced or updated is placed in a redirect state of ALWAYS, where it does not take on new subscribers but redirects them to the other MRA. Once all traffic has been removed or redirected, existing traffic is released from the MRA and it is shut down. Once the MRA is replaced or upgraded, the same process can be used on the other MRA, and then returned to the cluster.

Note: For detailed directions on performing a migration using the redirect states, please contact Oracle.

Changing Redirect States

To change the redirect state of an MRA device:

1. In the **MRA** section of the navigation bar, click **Configuration**.
2. Select an MRA.
The **MRA Administration** page displays information about the selected MRA.
3. Select the **MRA** tab.
4. Click **Advanced**.
5. In the **Other Advanced Configuration Settings** section, click the **Add** icon in the table.
The **Add Configuration Key Value** window opens ([Figure 9: Add Configuration Key Value Window](#)).

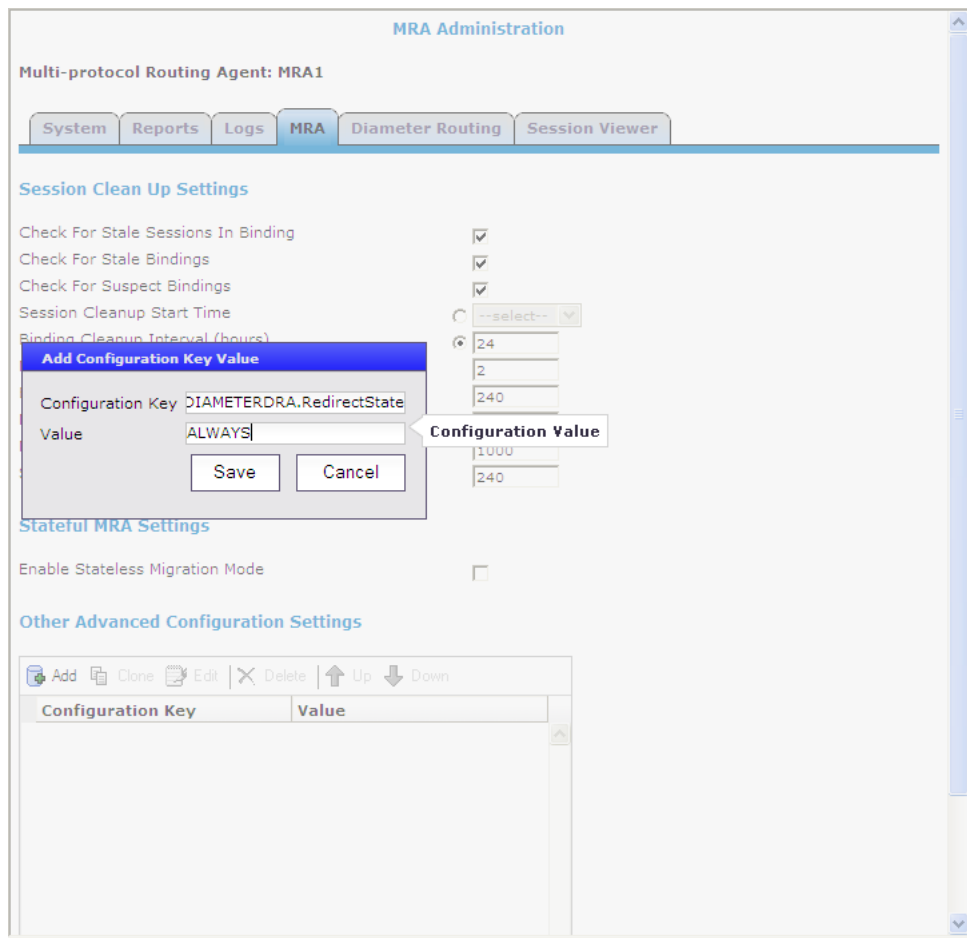


Figure 9: Add Configuration Key Value Window

6. Add the redirect configurable variable `DIAMETERDRA.RedirectState`, which indicates the redirect state of the MRA. Changing this variable to `NORMAL` will stop the release process. Valid values are:
 - **NORMAL** (default) — The MRA redirects CCR-I messages only when the DRMA link between the clustered MRAs is down and the subscriber does not have an existing binding on the MRA that first receives the CCR-I.
 - **ALWAYS** — The MRA always redirects CCR-I messages to the MRA it is clustered with for subscribers that do not have existing bindings, whether the DRMA link is active or not. An MRA in this state is not able to create new bindings.
 - **NEVER** — The MRA never redirects messages to the MRA it is clustered to, whether the DRMA link is active or not.

Note: In all redirect states, the MRA devices continue to handle DRMA traffic and process traffic normally for subscribers with existing bindings.

Releasing Active Sessions

Release configuration settings allow the MRA to release active subscribers and remove their bindings. These settings allow a task to be started that iterates through the bindings in the database and sends RARs for each session contained in each binding. These RARs indicate a session release cause, triggering the PGW/HSGW to terminate the corresponding sessions. Upon receiving a message to terminate the session, the MRA removes the session from the binding, and once the binding no longer has any sessions associated with it, it is removed. Any new sessions are redirected to the active MRA.

The release configurable variables are:

- **DIAMETERDRA.Release.Enabled:** Indicates whether the binding release task is started. Valid values are **TRUE** or **FALSE**; the default is **FALSE**. Setting this to **FALSE** stops the release process.
- **DIAMETERDRA.Release.MaxRARsRate:** The rate (in RARs/sec) at which the release task queues RAR messages to be sent; they will be evenly spread across the entire second. Valid values are a positive integer; default is **250**. Setting this to a negative integer stops the release process.
- **DIAMETERDRA.Release.UnconditionallyRemoveSessions:** Indicates if the release task removes the session information from the binding as soon as it is processed by the release task, or if it waits until it receives a CCR-T before updating the binding. Valid values are **TRUE** or **FALSE**; the default is **FALSE**.
- **DIAMETERDRA.Release.ReleaseTaskDone:** Internal flag used by the release task to indicate if it has completed. Values are **TRUE** or **FALSE**; the default is **FALSE**.
- **DIAMETERDRA.Release.OriginHost:** This value indicates the origin host to use when sending RARs initiated by the release task. Valid values are **MPE** or **MRA**; the default is **MPE**.

Managing Configuration and Virtual Templates

Configuration and Virtual templates allow for a more efficient means of normalizing common configurations between multiple MPE/MRA instances. Any given MPE/MRA can be associated with no template, one or many templates. In addition, users can add, remove, clone and reorder templates.

Virtual templates are similar to symbolic links in Linux. Virtual templates are particularly efficient when users want to replace a template that has been associated to multiple MPE or MRA with another template.

Creating a Template

Since an MPE or an MRA can exist independently of one another, there are two locations in the CMP interface where both virtual and configuration templates can be created. Template creation actions are found either in the **MRA** or the **Policy Server** section of the navigation pane. After the template is created, the template has the functionality that is specific to their instance (MPE or MRA).

Note: This procedure applies to both MPE or MRA devices.

Note: You must create a Configuration Template before a Virtual Template because a Virtual Template references, and is dependent on, a Configuration Template.

To create a configuration template:

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**.

The content tree displays a list of **All Templates** including Virtual and Configuration.

2. From the content tree, select **Configuration Template**.
The **Configuration Template Administration** page opens.

3. Click **Create Template**.
The **New Configuration Template** page opens.

4. Enter the **Name** of the template.

Note: This is an alphanumeric field that is limited to 255 characters. Single quotes, double quotes, space, comma, and backslash characters are not valid.

5. (Optional) Select a template from the **Copy From** list
6. (Optional) Enter a **Description / Location** (limited to 255 characters).
7. When you finish, click **Save**.

The settings are saved for the template and applied to all associated MPE or MRA devices.

Modifying a Template

Since an MPE or MRA device can exist independently of one another, there are two locations in the Policy Management interface where , both virtual and configuration, templates can be managed. Template creation actions are found either in the **Policy Server** or the **MRA** section of the navigation pane. After the template is created, the template has the functionality specific to their instance (MPE or MRA devices). After templates are created and associated, the templates can be viewed and managed from the **System** tab of the MPE or MRA device.

Note: This procedure applies to both MPE or MRA devices.

To modify a configuration template:

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**.
The content tree displays a list of all templates including Virtual and Configuration.
2. From the content tree, select the configuration template for modification.
The **Configuration Template Administration** page opens with the template.
3. Click **Modify**. From the **MRA** and **Diameter Routing** tabs, you can configure the following:
 - From the **MRA** section you have the following tabs and options:
 - **Template** tab
 - **Name**
 - **Description**
 - **MRA** tab - **Modify** button
 - **Associations** or
 - **MPE Pools**
 - **Subscriber Indexing**
 - **Diameter** settings
 - **S9**
 - **Radius Configuration**
 - **MRA** tab - **Advanced** button
 - **Expert Settings**

- Service Overrides
- Load Shedding Configuration
- Diameter Routing tab
 - Diameter Peers
 - Diameter Routes
- From the **Policy Server** section you have the following tabs and options:
 - Template tab
 - Name
 - Description
 - Logs tab
 - Modify Policy Log Settings
 - Policy Syslog Forwarding Configuration
 - Policy Server tab - **Modify** button
 - Associations
 - Subscriber Indexing
 - Configuration
 - Diameter settings
 - User Profile Lookup Retry on Session Updates
 - Diameter AF Default Profiles
 - Default Charging Servers
 - SMS Relay Configuration
 - SMPP Configuration
 - Primary SMSC configuration
 - Secondary SMSC configuration
 - SMTP Configuration
 - Analytics
 - Policy Server tab - **Advanced** button
 - Expert Settings
 - Service Overrides
 - MPE Load Shedding Configuration
 - Diameter Routing tab
 - Diameter Peers
 - Diameter Routes
 - Policies tab
 - Deployed Policies
 - Data Sources tab
 - Data Sources
 - General Settings

- **Sh Settings**

4. When you finish, click **Save**.

The settings are saved for the template, and applied to all associated MRA or MPE devices.

Reordering Templates

Since an MPE or an MRA can exist independently of one another, there are two locations in the Policy Management interface where templates can be created. Template creation actions are found either in the **Policy Server** or the **MRA** section of the navigation pane. Templates have the functionality specific to their instance (MPE or MRA). After a template is created and associated, the template can be viewed in the **System** tab of the **Configuration** for the MPE or MRA device.

Note: This procedure applies to both MPE or MRA devices.

Reordering templates in a list allows a user to prioritize templates according to configuration values applied to a given MRA or MPE instance. For example, different configurations will provide different prioritizations depending on the order (the lower the number the higher the prioritization) as it appears in the **Associated Templates** section of the **Modify System Settings** screen.

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**. The content tree displays a list of all templates including Virtual and Configuration.
2. From the content tree, select the configuration template for modification. The **Configuration Template Administration** page opens with the template.
3. Click **Modify**.
4. Edit the numbers in the priority field.
5. Click **Update Order**. The associated templates are reordered.

Associated Templates(lower numbered templates take priority over higher numbered templates)

Total: 2 Add Undo Redo Update Order

Priority	Template Name
1	MRADocTest4
2	MRADocTest3

Save Cancel

Figure 10: Original Template List

Associated Templates(lower numbered templates take priority over higher numbered templates)

Total: 2 Add Undo Redo Update Order

Priority	Template Name
1	MRADocTest3
2	MRADocTest4

Save Cancel

Figure 11: Reordered Template List

Creating Virtual Templates

Since an MPE or MRA can exist independently of one another, there are two locations in the Policy Management interface where, both virtual and configuration, templates can be created. Templates can be created and managed either in the **Policy Server** or **MRA** section of the navigation pane. Because Virtual templates are based on Configuration Templates, modifying a Configuration Template associated with a Virtual Template automatically modifies the Virtual Template. After the templates are created, the templates have the functionality specific to their instance (MPE or MRA).

Note: This procedure applies to both MPE or MRA devices.

Complete these steps to create a configuration template.

1. From the **MRA** or **Policy Server** section of the Navigation pane, select **Configuration Templates**. The content tree displays a list of all templates including Virtual and Configuration.

Note: You must create a Configuration Template before a Virtual Template because a Virtual Template references, and is dependent on, a Configuration Template.

2. From the content tree, select **Virtual Templates**.
The **Virtual Template Administration** page opens.
3. Click **Create Virtual Template**.
The **New Virtual Template** page opens.
4. Enter the **Name** of the template.

Note: This is an alphanumeric field that is limited to 255 characters. Single quotes, double quotes, space, comma, and backslash characters are not valid.

5. Select a template from the **Associated Configuration Template** pull-down menu.
6. (Optional) Enter a **Description**.
7. When you finish, click **Save**.

The settings are saved for the template, and applied to all associated MRA or MPE devices.

Overlaps

Overlaps occur when both a template and an MRA or MPE are assigned an identical value for the same attribute or field. For example, the index of a user name is true in template A, and the index of a user name is also true in an MRA or MPE. The result is that when the template and MRA or MPE are associated, the index of the user name becomes an overlapped field. When an overlap occurs, a prompt opens stating, The server configuration has overlaps with the associated template(s) . The user can take one of two actions:

- Remove the overlaps and use the settings from the template.
- Keep the overlaps and use the settings from the server.

Configuring Topology Hiding for the Gx Application

When topology hiding is enabled, Gx CCA and RAR messages forwarded by the MRA to the network are modified to include the MRA Origin-Host instead of the MPE Origin-Host. Route-Record in RARs are not removed.

If a Gx CCR-U/T message does not contain a Destination-Host, or contains a Destination-Host set to the MRA identity, a binding lookup is performed based on the available and indexed keys to find the corresponding MPE device. The message is then forwarded to the MPE device with no Destination-Host. If the message contains a Destination-Host set to an identity other than the MRA, the message is routed based on the Destination-Host only.

When the Origin-Host is replaced on a forwarded message, the original Origin-Host is logged at the end of a message when logging the message details.

To configure topology hiding:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA device.
The **MRA Administration** page opens.
3. Select the **MRA** tab.
The current MRA configuration settings are displayed.
4. Click **Modify**.
The **Modify MRA** page opens.
5. In the **Subscriber Indexing** section, ensure that the **Index by Session ID** option is enabled if there are no other indexed subscriber keys available in update/terminate messages.
6. Click **Save**.
7. On the **MRA** tab, click **Advanced**.
8. In the **Other Advanced Configuration Settings** section, click the **Add** icon in the table. The **Add Configuration Key Value** window opens (see [Figure 9: Add Configuration Key Value Window](#)).
Add the following configuration keys to the **Add Configuration Key Value** window:

Table 4: Topology Hiding Configuration Keys

Configuration Key	Value
DIAMETERDRA.TopologyHiding.Apps	Gx
DIAMETERDRA.TopologyHiding.Enabled	true

9. Click **Save**.
The topology hiding settings are applied to the MRA.

Chapter 4

Managing Network Elements, Backups and Diameter Settings

Topics:

- [Adding Associated MRAs.....52](#)
- [Associating Network Elements with an MRA Device.....56](#)
- [About MPE/MRA Pools and Diameter Peer Tables.....60](#)
- [About Stateless Routing.....65](#)
- [Configuring for RADIUS.....67](#)

The **MRA** tab on the **MRA Configuration** page displays a list of network elements associated with the MRA device, the associated MPE pool, configuration settings for the MRA device, Diameter-related configuration information, and if load shedding is configured.

Note: This document assumes that all CMP systems as well as MRA, and MPE devices are operational. Also, the procedures used in this guide are MRA specific; for additional CMP system and MPE device configuration information, refer to the *CMP Wireless User's Guide* and *Policy Wizard Reference Guide*.

Adding Associated MRAs

Each MRA cluster can have a backup MRA and multiple associated MRA clusters. In addition, if your system is configured for georedundancy, you have the option to configure an georedundant MRA with a secondary site (Default Secondary IP Address).

If the system is set for georedundancy, a primary site contains the preferred site or connection, and a secondary site contains a non-preferred (optional) spare server. The spare server, though located elsewhere, is still part of the cluster, and prepared to take over if an active server and its secondary backup fails. You must associate a primary and secondary site with a cluster.

To configure an associated MRA device, complete the following:

1. From the **Navigation Panel** select **MRA Associations**.
The **MRA Association Administration** page opens.
2. From the top of the MRA Associations tree, select **MRA Associations**.
3. Click **Create MRA Association**
The **Configuration** screen opens.
4. Type in the **Name** of the MRA Association.
5. (Optional) Type in a **Description** of the MRA Association.
6. Select the **Type** of binding the Association will use (Algov1 or Legacy).
 - Algov1 - (Default) Uses **Algorithm Version 1** to distribute binding indexes across MRAs in a system.
 - Legacy - Used after an MRA has been migrated and issues are encountered. Using this option deletes all mappings from the database and starts a "rollback" process. "revert" MRAs back
7. From the **Members** section, click **Add**.
The Add MRA Association Member pop-up appears.
8. From the **Add MRA Association Member** window, perform the following steps:
 - a) Select an **MRA** from the list of existing MRAs.
After the MRA has been selected, the **Default Primary IP Address** of that MRA appears in the field.
 - b) (Optional) If the Association is to be georedundant, select a **Default Secondary IP Address**.
This is the IP Address other MRAs in the Association will use when establishing Diameter Connections with this MRA.
Note: A different IP Address will be used if there are any matching overrides configured.
 - c) (Optional) Select a **Backup MRA** from the list.
Note: The backup feature has a "two-way" capacity, for example, if MRA1 is selected to be the backup for MRA2, MRA2 will also function as a backup for MRA1 if something happens to MRA1.
 - d) (Optional) Select a **Protocol Timer Profile** from the list. For more information, see *Managing Subscriber Profile Repositories*.
 - e) Select either **TCP** or **SCTP** for transport protocol.

If other MRAs in the Association should connect to this MRA using SCTP instead of TCP, select **Connect SCTP** and then select **Max Incoming Streams** and **Max Outgoing Streams** (the default is "8" streams for both incoming and outgoing streams).

- f) Click **Save** to save your configuration.
9. (Optional) If there is to be an **Association Override**, click **Add** in the **Association Override** section. Then repeat **substeps 7a-7e** and click **Save**.
10. For **Subscriber Indexing**, select any or all of the following: (For more information, see *Configuring Protocol Options for an MRA Device*.)
- **Index by Username**
 - **Index by NAI**
 - **Index by E.164 (MSISDN)**
 - **Index by IMSI**
 - **Index by Session ID**
 - **Primary Indexing** (IMSI or e.164/MSISDN)
- Note:** Used for having all MRAs use the same subscriber indexing value after an upgrade.
11. (Optional) If there are to be **Overrides by APN** click **Add** in the section. Fill in or select the following parameters as needed.
- a) Type in the name of the **APN** (255 character limit, no spaces or special characters).
 - b) **Index by IPv4**,
 - c) **Index by IPv6**
 - d) **Index by Username**
 - e) **Index by NAI**.
 - f) **Index by E.164 (MSISDN)**
 - g) **Index by IMSI**
 - h) Click **Save** to save the APN configuration.

12. When you finish, click **Save**.

The MRA clusters are configured as associated MRA devices.

Configuring Protocol Options on an Associated MRA Device

Follow these steps to configure protocol options on an Associated MRA device:

1. From the **MRA** section of the navigation pane, select **MRA Associations**.
The content tree displays the list of Associated MRAs. The initial group is **ALL**.
2. From the content tree, select the MRA Association.
The **MRA Association Administration** page opens.
3. On the **MRA Association Administration** page, click the **Modify**.
The current configuration options are displayed.
4. From the **Subscriber Indexing** section define options as necessary.
MRA Protocol Configuration Options defines available options that pertain specifically to MRA devices. (The options may vary depending on the configuration mode of the system.)
5. When you finish, click **Save**.

Table 5: MRA Protocol Configuration Options

Attribute	Description
Subscriber Indexing	Note: The indexing parameters to use depend on what user ids are needed for correlating various messages to ensure they all end up on the same MPE for the same user. If you are unsure which indexing methods to configure, contact My Oracle Support. (https://support.oracle.com)
Index by Username	Select if the MRAs in the association should index by account ID.
Index by NAI	Select if the MRAs in the association should index by network access ID.
Index by E.164 (MSISDN)	Select if the MRAs in the association should index by E.164 phone number.
Index by IMSI	Select if the MRAs in the association should index by IMSI number).
Index by Session ID	Select if the MRAs in the association should index by session ID.
Primary Indexing	Select from the pull-down list to set to the type of index that is expected for messages that create bindings, for example Gx CRR-I. Note: The type of index selected for primary indexing must also be selected either as an "Index by IMSI" or "Index by E.164" depending on the configuration.  CAUTION: Primary Index cannot be changed on a system that has already created bindings without suffering data loss. CAUTION
Index by IP Address	Select if the MRAs in the association should index by IP address. You can select Index by IPv4 , Index by IPv6 , or both formats.
Overrides by APN	Select to perform subscriber indexing for a specific IP address and a specific APN name. In the Overrides by APN section, click Add . Enter the APN name and click Save to enable Index by IPv4 , Index by IPv6 , or both. You can create new APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.

Modifying Backup and Associated MRA devices

Once you have defined backup and associated MRA devices, they are listed in an Associated MRA table. The table indicates whether an MRA is a backup, the primary IP address, and, in a georedundant configuration, the secondary IP address. Using this table you can add, modify, or delete MRA devices from the list.

To modify backup and associated MRA devices:

1. From the **Navigation Panel** select **MRA Associations**. Select **MRA Associations** from the within the screen, click **Modify**.
The **MRA Association Administration** screen opens.
2. From the top of the MRA Associations tree, select **MRA Association** that will be modified. The functions available from the table are as follows:
3. Click **Modify**.
 - **To add an MRA to the table** — Click **Add**; the **Select MRA** window opens. Select an MRA device. If this is a backup MRA, select **Is Backup**. Enter the **Primary IP Address**, and for a georedundant configuration, the **Secondary IP Address**.
 - **To clone an MRA in the table** — Select an MRA and click **Clone**; the **Clone MRA** window opens with the information for the MRA device. Make changes as required.
 - **To edit an MRA in the table** — Select the MRA and click **Edit**; the **Edit MRA** window opens with the information for the MRA device. Make changes as required.
 - **To delete an MRA from the table** — Select the MRA and click **Delete**; you are prompted, Are you sure you want to delete the selected MRA? Click **Delete** to remove the MRA.

When you finish, click **Save**.

MRA Association Status Definitions

The **Status** column of an MRA shows current status on any sync or migration tasks that have run or are running. A status can be one of the following:

- **OK** - This status means the MRA is not currently running any migration or sync tasks. If all MRAs are in this state, a new MRA can safely be added to the Association.
- **Syncing (xx%)** - This status means the MRA is currently running the sync task. If any MRAs are in this state, a new MRA cannot be safely added to the Association. If a new MRA is added, data integrity can't be guaranteed across the association. The percentage completion through the task will be displayed in parentheses.
- **Migrating (xx%)** - This status means the MRA is currently running the legacy migration task. If any MRAs are in this state, a new MRA cannot be safely added to the Association. The percentage completion through the task will be displayed in parentheses.
- **Migration Failed** - This status means the last migration task which ran on the MRA did not complete successfully. This likely means there were some connection failures between MRAs during the task and the task should be manually rerun using the Operations menu.
- **Sync Failed** - This means the last sync task which ran on the MRA did not complete successfully. This likely means there were some connection failures between MRAs during the task and the task should be manually rerun using the Operations menu.
- **Migrated** - This status means the last migration task which ran on the MRA completed successfully. The MRA is still running in a special migration mode, however. Use the operation "Complete Migration" to turn off migration mode on the MRA and start using the n-site MRA optimizations. Complete Migration can also be used when in a Migration Failed state if the number of failures is low and running another full migration is not needed.

MRA Association Operations

There are various operations that can be performed on MRA Associations.

These operations include:

- **Manual Sync** - To be able to manually start a sync task on all MRAs in the Association.
- **Cancel Sync** - To cancel a sync which is currently in progress.
- **Manual Migration** - To be able to manually start a migration task on all MRAs in the Association.
- **Cancel Migration** - To cancel a migration which is currently in progress.
- **Accept Migration** - To accept the migration (after all MRAs have finished running the migration task).

Note: This operation will disable the migration mode on the MRAs so that they will fully transition into using the N-site feature. All MRAs in the Association must either be in **Migrated** or **Failed Migration** status.

- **Reset Counters** - Reset all counters for all MRAs in the association.
- **Reapply Configuration** - Reapply configuration for all MRAs in the association.

Note: If at least one MRA in the Association has a software version less than the version where this feature is introduced, the CMP will display a warning that clusters are in a mixed version, and the Operations drop down will be disabled. This is to prevent running operations on servers which don't have the required software to support those operations.

Conditions Limiting Operation Options

- If the association type is set to **Legacy**, only Reset Counters and Reapply Configuration operations are available.
- If all of the MRAs in the association show **Migrated** or **Failed Migration** status, only Accept Migration operation is available.
- If at least one MRAs in the association shows **Migrating** status, only the Cancel operation is available.
- If at least one MRAs in the association shows **Syncing** status, only the Cancel Sync operation is available.
- If any of the MRAs in the association show **Syncing** or **Failed Sync** status, then only the Manual Migration operation is available.
- If any of the MRAs in the association show **Migrating**, **Migrated** or **Failed** status the Manual Sync operation will not be available.

Associating Network Elements with an MRA Device

Adding network elements to an MRA device is similar to how network elements are added to an MPE device: a list of supported network elements, which are pre-entered into the system (see [Defining a Network Element](#) to add network elements), is available for selection.

To add a network element to an MRA, complete the following:

1. From within the **MRA** tab, click **Modify**.
The **MRA Administration Modify** page opens.
2. In the Associations section of the **MRA Administration Modify** page, click **Manage**.
The Select Network Elements window displays showing a list of network elements.

For example:

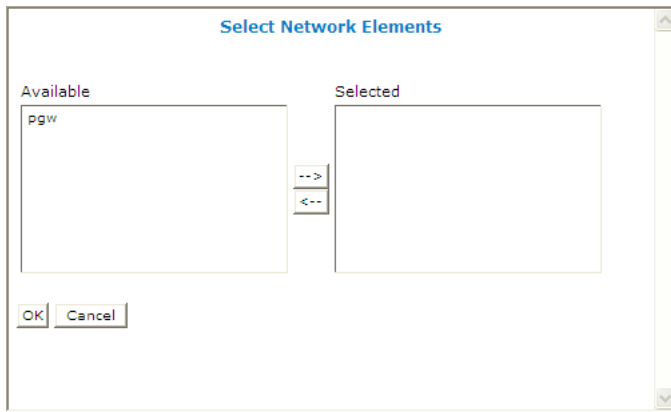


Figure 12: Select Network Elements

3. Select a network element in the **Available** list, click the right arrow to move the network element to the **Selected** list.
4. (Optional) Add additional network elements to the **Selected** list.
5. Click **OK**.

The network element is added to the MRA.

Defining a Network Element

You must define a network element for each device associated with any of the MPE devices within the network. To define a network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group in which you want to define the network element.
(See [Creating a Network Element Group](#) for information on creating network element groups.)
The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, click **Create Network Element**.
The **New Network Element** page opens.
4. Enter information for the network element:
 - a) **Name** (required) — The name you assign to the network element.
Enter up to 250 alphanumeric characters. The name can include underscores (_), hyphens (-), colons (:), and periods (.).
 - b) **Host Name/IP Address** (required) — Registered domain name, or IP address in IPv4 or IPv6 format, assigned to the network element.
 - c) **Backup Host Name** — Alternate address that is used if communication between the MPE device and the network element's primary address fails.
 - d) **Description/Location** — Free-form text.
Enter up to 250 characters.
 - e) **Type** (required) — Select the type of network element.
The supported types are:

Note: This list varies depending on the configuration of the CMP system.

- **PDSN** — Packet Data Serving Node (with the sub-types **Generic PDSN** or **Starent**)
 - **HomeAgent** — Customer equipment Home Agent (with the sub-types **Generic HomeAgent** or **Starent**)
 - **GGSN** (default) — Gateway GPRS Support Node
 - **Radius-BNG** — RADIUS broadband network gateway
 - **HSGW** — HRPD Serving Gateway
 - **PGW** — Packet Data Network Gateway
 - **SGW** — Serving Gateway
 - **DPI** — Deep Packet Inspection device
 - **DSR** — Diameter Signaling Router device
 - **NAS** — Network Access Server device
- f) **Protocol Timer Profile**—select a protocol timer profile. For information on creating protocol timers, see [Managing Protocol Timer Profiles](#).
- g) **Capacity** — The bandwidth allocated to this network element. Not applicable.
- h) **Links to other Network Elements** — Specifies the links to other network elements.
5. Select one or more policy servers (MPE devices) to associate with this network element.
6. Select one or more MRA devices to associate with this network element.
7. To add a network element to a network element group, select the group (see [Adding a Network Element to a Network Element Group](#)).
8. When you finish, click **Save**.

You have created the definition for a network element.

Associating a DSR Network Element with an MRA

Use this procedure to associate a DSR with an MRA device. If the MRA device gets an MPE-initiated message and the MRA device has a DSR configured, the MRA device will forward the message to the Primary DSR. If the connection to the primary DSR is not available, the MRA device forwards the message to another DSR (if configured). Note that the primary DSR Network Element (NE) should be configured in the Associated NEs list first.

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA device.
The **MRA Administration** page opens.
3. Select the **MRA** tab.
The current MRA configuration settings are displayed.
4. Click **Modify**.
The **Modify MRA** page opens.
5. Select a **Primary DSR** to associate with this MRA from the list.
6. Enter a string value into **Segment ID**, if needed. If the MRA receives a message with a Destination-Host equal to the Segment ID, the MRA removes the Destination-Host AVP from the message.
7. Click **Save**.

The specified DSR information is associated with this MRA device.

Creating a Network Element Group

To create a network element group:

1. From the **Network** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **Network Element Administration** page opens in the work area.
3. Click **Create Group**.
The **Create Group** page opens.
4. Enter the **Name** of the new network element group.
The name can be up to 250 characters long and must not contain quotation marks (") or commas (.).
5. Enter a text **Description/Location** of the network group.
6. When you finish, click **Save**.

You have created a network element group.

Adding a Network Element to a Network Element Group

Once a network element group is created, you can add individual network elements to it. To add a network element to a network element group:

1. From the **Network** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group.
The **Network Element Administration** page opens in the work area, displaying the contents of the selected network element group.
3. Click **Add Network Element**.

The **Add Network Elements** page opens. The page supports both small and large networks, as follows:

- If there are 25 or fewer network elements defined, the page displays the network elements not already part of the group. (*Figure 13: Add Network Element Page* shows an example.)
- If there are more than 25 network elements defined, the page does not display any of them. Instead, use the **Search Pattern** field to filter the list. Enter an asterisk (*) to generate a global search, or a search pattern to locate only those network elements whose name matches the pattern (for example, **star***, ***pGw**, or *** - ***). When you have defined a search string, click **Filter**; the page displays the filtered list.

The screenshot shows a web-based interface titled "Network Element Administration". It contains a section "Add Network Elements" with the instruction "Select the Network Elements to add to this Group." Below this is a search bar with a "Search Pattern:" label, a text input field containing an asterisk (*), and two buttons: "Filter" and "Select All".

Below the search bar is a list titled "Add Network Elements" containing a sub-header "Network Elements" and a list of items: ggsn1, pgw1, hsgw1, tdf1, tdf2, and tdf3. Each item has a checkbox to its left. A vertical scrollbar is on the right side of this list.

Below the first list is a second section titled "Add Network Elements from Network Element Groups" with the instruction "Press Ctrl and click check box can make recursive change". It contains a sub-header "Network Element Groups" and a list with one item: TransAlpine, which also has a checkbox to its left.

At the bottom of the interface are two buttons: "Save" and "Cancel".

Figure 13: Add Network Element Page

4. Select the network element you want to add. Press the Ctrl or Shift key to select multiple network elements.

You can also add previously defined groups of network elements by selecting those groups.

5. When you finish, click **Save**.

The network element is added to the selected group and a message indicates the change. For example, 2 Network Elements were added to this group.

Managing Protocol Timer Profiles

Managing Protocol Timer Profiles describes how to define and manage protocol timer profiles within the CMP system.

A protocol timer profile configures the Diameter response timeout values for specific applications and the different message types within an application.

About MPE/MRA Pools and Diameter Peer Tables

Note: Each MRA cluster can support a pool of 10 MPE clusters.

The MPE can have dual roles within the MRA. It can be associated with a MRA as an element in the MPE pool of the MRA so that it participates in the load balancing operation of the MRA and it can serve as a Diameter peer for Diameter routing.

The MPE can function in the following roles:

- The MPE is associated with an MRA and participates in the load balancing action of the MRA.
- The MPE is added as a simple Diameter peer for Diameter routing and it does not participate in the load balancing of the MRA.
- The MPE can serve both roles but not simultaneously.

If there are explicit Diameter routes, the routes take precedence over the load balancing action of the MRA. To allow maximum flexibility, you can associate an MPE with an MRA to cover roles 1 and 3. When you associate an MPE with the MRA, the MPE automatically becomes a Diameter routing peer available in the Diameter routing table. In addition, you can add a new MPE as a simple Diameter peer to cover role 2. In this case, the MPE only serves as a simple Diameter peer and does not participate in the load balancing operation at all.

Note: An MPE cannot be present in both the MPE pool and Diameter routing table at the same time. If you try to do this, an error message is returned indicating that an MPE entry already exists in either the MPE pool or the Diameter peer routing table. If an MPE is in the peer table and you want to add it to the MPE pool, you need to delete it from the peer table first and then add it to the MPE pool. Also, if you try to remove an MPE from the MPE pool and the MPE is also in the Diameter peer routing table, a warning message is displayed informing you that the selected MPE cannot be removed until it is first deleted from the Diameter peer routing table.

Configuring Diameter Realm Based Peer Routes

By default, Diameter messages are processed locally. In a network with multiple Policy Management devices, messages can be routed, by realm, application, or user ID, for processing by peers or other realms.

Note: Diameter messages can be routed in either an MPE or MRA the steps listed below can be used for either device.

To configure the Diameter route table:

1. From the Policy Management device (either **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups.
2. From the content tree, select the **Policy Server** or **MRA** that needs diameter routing.
The **Policy Server Administration** or **MRA Administration** page opens in the work area.
3. Select the **Diameter Routing** tab.
The Diameter Routing configuration settings appear.
4. Click **Modify Routes**.
The **Modify the Diameter Route Table** page opens.
5. Add a route to the table
 - a) Click **Add**.
The **Add Diameter Route** window opens.
 - b) Configure the route using the following fields.
 - **Diameter Realm** — For example, **galactel.com**.

- **Application ID** — Select **Rx** (default), **Gq**, **Ty**, **Gx**, **Gy**, **Gxx**, **Sh**, **Sy**, or **All**.

Note: You can include only one application per route rule. For multiple applications, create multiple rules.

- **User ID type** — Select **ANY** (default), **E.164(MSISDN)**, **IMSI**, **IP**, **NAI**, **PRIVATE**, **SIP_URI**, or **USERNAME**.
- **Value** — Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); as a wildcard character. To add the user ID to the list, click **Add**; to remove one or more user IDs from the list, select them and click **Delete**.
- **Evaluate as Regular Expression** — The check box allows the matching of route criteria using regular expression syntax, opposed to the previously supported matching wildcards.

Note: Regular expressions are specifically JAVA expressions and using any other language expression will result in a failed status. See [Examples of JAVA Regular Expressions for MRA Routes](#) for more information about using regular expressions for MRA routes.

- **Action** — Select **PROXY** (stateful route, default), **RELAY** (stateless route), or **LOCAL** (process on this device).
- **Server ID** — Select a destination peer from the list.

Note: You can define a server with a Diameter identity.

c) When you finish, click **Save**.

6. (Optional) Add, delete, modify, or order entries.

- Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.
 4. When you finish, click **Save**. The entry is added to the table
- Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. When you finish, click **Save**. The entry is updated in the table.
- Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.
- Ordering the list.

If you define multiple entries, they are searched in the order displayed in this list. To change the order:

1. Select an entry.
2. Click  **Up** or  **Down**. The search order is changed.

7. Define the default route:
 - a) Click **Edit** in the **Default Route** section.
 - b) Select the default action: **PROXY**, **RELAY**, or **LOCAL**.
 - c) Select the peer server ID.
 - d) When you finish, click **Save**.
8. To delete the default route, click **Delete**.
9. When you finish, click **Save**.

The Diameter routes are configured.

Examples of JAVA Regular Expressions for MRA Routes

Sample Regular Expressions for MRA Routes

- For E164 numbers ending in 00 to 24: #E164:1234.*?(?:0\d|1\d|2[0-4])
- For E164 numbers ending in 25 to 49: #E164:1234.*?(?:2[5-9]|3\d|4\d)
- For E164 numbers ending in 50 to 74: #E164:1234.*?(?:5\d|6\d|7[0-4])
- For E164 numbers ending in 75 to 99: #E164:1234.*?(?:7[5-9]|8\d|9\d)

Associating a Diameter MPE Peer with an MRA

When adding an MPE device to the MPE Pool, the IP Address must be from the application network and not from the management network.

Note: When specifying an associated MPE device, it is not necessary that the MPE device is under the same CMP. The CMP does not verify if it is an MPE device and if it is online or not.

To associate an MPE device with an MRA and add it to the MPE pool, complete the following steps:

1. Select **MRA > Configuration**.
2. Select the **MRA** to associated with an MPE device.
3. Select the **MRA** tab, click **Modify**.
4. In the **MPE Pool** section, click **Add** to open the **Add Diameter MPE Peer** window.

Add Diameter MPE Peer

Associated MPE (optional)

Name

Primary Site IP

Secondary Site IP

Diameter Realm

Diameter Identity

Protocol Timer Profile

Route New Subscribers ☒

Transport

☒ TCP

Connections

☐ SCTP

Max Incoming Streams

Max Outgoing Streams

Save Cancel

Figure 14: Add Diameter MPE Peer Window

5. Enter the following information:
 - a) **Associated MPE** — Select an MPE device.

Note: An MPE device is selected from the list of MPEs managed by the CMP. If the MPE is not managed by this CMP, this should be left blank.
 - b) **Name** — Name of the MPE device.
 - c) **Primary Site IP** — Enter the IP address of the primary site.
 - d) **Secondary Site IP** (for georedundant configurations only) — Enter the IP address of the secondary site.
 - e) **Diameter Realm** — Enter the domain of responsibility for the peer (for example, **galacteleu.com**).
 - f) **Diameter Identity** — Enter a fully qualified domain name (FQDN) or the peer device (for example, **MRA10-24.galactel.com**).
 - g) **Route New Subscribers** — Select if the MPE no new sessions will be routed requests for new subscribers (that is, no existing binding). If it is unselected, the MPE no new sessions will be routed to this MPE.
 - h) In the **Transport** section, select:
 - Select **TCP** and the number of **Connections**. The default number of connections is 1.
 - Select **SCTP** and the number of **Connections** (incoming and outgoing streams) to be used. The default is 8.
6. When you finish, click **Save**.

The **Add Diameter MPE Peer** window closes.
7. (Optional) In the **Diameter** section enter the following information:
 - a) **Diameter Realm**.
 - b) **Diameter Identity**.
8. In the **S9** section select the following information:
 - a) **Primary DEA**.

b) **Secondary DEA.**

9. Click **Save**.

The MPE device is added to the MPE pool. If you are setting up multiple MRA clusters, repeat the above steps for each MRA in each cluster.

Cloning, Modifying, or Deleting an MPE

To clone, modify, or delete an MPE from the MPE pool of an MRA, complete the following steps:

1. From the **MRA** tab, click **Modify**.
2. In the **MPE Pool** section of the page, select the MPE.
3. Click **Clone**, **Edit**, or **Delete**.
 - a) If deleting, click **Delete**.
 - b) If cloning or modifying, enter the required information and click **Save**.

About Stateless Routing

Stateless routing allows the MRA to route diameter messages to MPE devices or other devices, without the need to maintain state. Typically, the MRA selects an MPE device for a user, and continues to use the same MPE for the user by maintaining session state. Using stateless routing, static routes are configured ahead of time, so the state does not need to be maintained.

Using stateless routing, the MRA establishes a diameter connection with every peer that is defined in the Diameter Peer Table, where a peer consists of a name, IP address, diameter realm, diameter identity, and port. A route consists of a diameter realm, application ID, user ID, action, and server ID. The Action can be either proxy or relay.

Stateless routing uses routing based on FramedIPAddress and FramedIPv6Prefix, with wildcard pattern matching. The IP address must be configured in either dotted decimal notation for IPv4 or expanded notation for IPv6 excluding the prefix length.

The MRA processes routes in the order of their configured priority, which is based on the order in which they were configured in the route. If the destination of a route is unreachable, the route with the next highest priority is used. If no available routes are found, the MRA returns a **DIAMETER_UNABLE_TO_DELIVER** error message. If a destination is currently up when the route is chosen but the forwarded request times out, the MRA returns a **DIAMETER_UNABLE_TO_DELIVER** error message and does not try the next route.

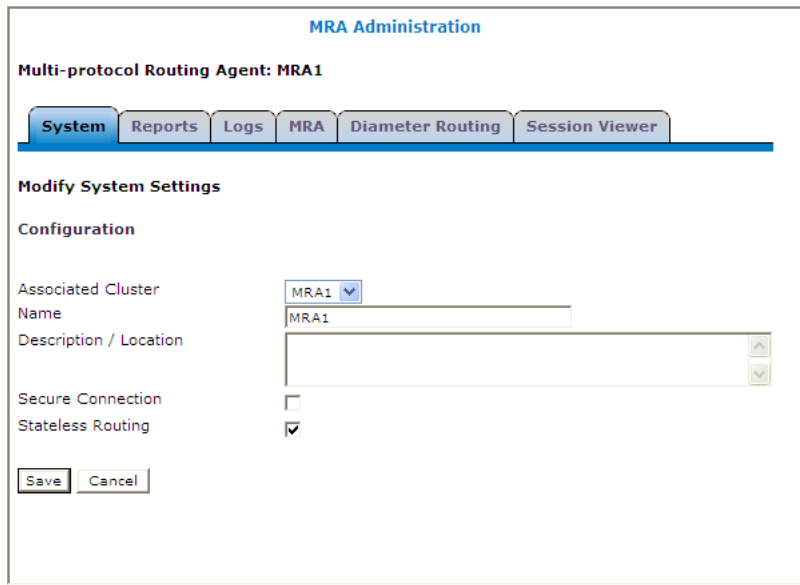
Enabling Stateless Routing

To hide configuration relevant to a stateful MRA device in the CMP display, perform the following procedure.

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. Select the MRA from the content tree.
The **MRA Administration** page displays the configuration for the MRA.

3. Select the **System** tab.
The **Modify System Settings** page opens.
4. Select **Stateless Routing** ([Figure 15: Enabling Stateless Routing](#) shows an example).

The stateful MRA configuration is hidden.



The screenshot shows the 'MRA Administration' interface. At the top, it says 'Multi-protocol Routing Agent: MRA1'. Below this is a navigation bar with tabs: 'System' (selected), 'Reports', 'Logs', 'MRA', 'Diameter Routing', and 'Session Viewer'. The main section is titled 'Modify System Settings' and contains a 'Configuration' section. In this section, 'Associated Cluster' is set to 'MRA1' via a dropdown. 'Name' is 'MRA1' in a text field. 'Description / Location' is an empty text area. 'Secure Connection' is unchecked. 'Stateless Routing' is checked. At the bottom are 'Save' and 'Cancel' buttons.

Figure 15: Enabling Stateless Routing

Modifying the Stateless Migration Mode in an Existing MRA

When modifying an existing MRA, you can enable or disable the **Enable Stateless Migration Mode** which enables the MRA device to use static routes to transition to a stateless migration mode.

To enable and disable the migration mode setting:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. Select the MRA device from the content tree.
The **MRA Administration** page opens, displaying information about the selected MRA device.
3. Select the **MRA** tab.
4. Click **Advanced**.
5. In the **Stateful MRA Settings** section of the page, select **Enable Stateless Migration Mode** (or leave the box unchecked if you do not want to enable the migration mode).
The stateless migration mode is enabled.
6. Click **Save**.

The MRA device is put into migration mode.

Loading MPE/MRA Configuration Data when Adding Diameter Peer

When adding a diameter peer one must be selected from the list contained within the Diameter Routing tab. Once selected, the peer configuration fields are automatically populated.

Configuring for RADIUS

For an MRA to utilize RADIUS, the system must be RADIUS enabled (see *CMP Wireless User's Guide*) and the MPE for the MRA must be configured for RADIUS (see *CMP Wireless User's Guide*).

Complete these steps to configure an existing MRA for RADIUS.

1. From the navigation section, select **MRA > Configure**.
2. From the list, select the **MRA** to be configured.
3. Select the **MRA Tab**.
4. Click **Modify**.
5. Scroll to the **RADIUS Configuration** section and enter the following:



RADIUS Configuration

RADIUS Enabled ☒

Secret

Figure 16: RADIUS Configuration Section

- Select **RADIUS Enabled**.
 - **Secret** — Enter name of the **Default Passphrase**.
6. Click **Save** when you have completed the steps.

Chapter 5

Managing Subscriber Profile Repositories

Topics:

- [About Subscriber Profile Repositories.....69](#)
- [Configuring the CMP System to Manage SPR Subscriber Data.....70](#)
- [Configuring the SPR Connection.....70](#)
- [Modifying the SPR Connection.....71](#)
- [Finding a Subscriber Profile.....71](#)
- [Creating a Subscriber Profile.....72](#)
- [Modifying a Subscriber Profile.....73](#)
- [Deleting a Subscriber Profile.....73](#)
- [Viewing Subscriber Entity States.....74](#)
- [Creating a Subscriber Entity State Property.....74](#)
- [Modifying a Subscriber Entity State Property...75](#)
- [Deleting a Subscriber Entity State Property.....75](#)
- [Viewing Subscriber Quota Information.....76](#)
- [Adding a Subscriber Quota Category.....77](#)
- [Modifying a Subscriber Quota Category.....78](#)
- [Deleting a Subscriber Quota Category.....78](#)
- [Adding a Member to a Pooled Quota Group.....79](#)
- [Querying by Pool ID.....79](#)
- [Creating a Pool Quota Profile.....80](#)
- [Modifying a Pool Quota Profile.....81](#)
- [Deleting a Pool Quota Profile.....81](#)
- [Modifying a Pool Profile.....81](#)
- [Deleting a Pool Profile.....82](#)
- [Creating a Pool State.....82](#)
- [Modifying a Pool State.....83](#)
- [Deleting a Pool State.....83](#)

Managing Subscriber Profile Repositories describes how to define and manage an optional Subscriber Profile Repository (SPR) using the CMP system.

An SPR is a system for storing and managing subscriber-specific policy control data as defined in the 3GPP standard.

Note: For information on operating Oracle Communications Enhanced Subscriber Profile Repository devices, refer to the *Enhanced Subscriber Profile Repository User's Guide*.

About Subscriber Profile Repositories

A Subscriber Profile Repository (SPR) is a system for storing and managing subscriber-specific policy control data as defined under the 3GPP standard.

An SPR can be deployed in environments where the MPE device needs access to a separate repository for subscriber data. The SPR acts as a centralized repository for this data so that multiple MPE devices can access and share the data. This data may include profile data (pre-provisioned information that describes the capabilities of each subscriber), quota data (information that represents the subscriber's use of managed resources), or other subscriber-specific data.

The following SPR systems can be used in the CMP system:

- The Oracle Communications Subscriber Database Management (SDM) product includes interfaces for provisioning subscriber information, as well as managing, changing, and accessing this information. These interfaces include an application programming interface (API) for XML provisioning of subscriber profile data, as well as an interactive user interface through the CMP system using a proprietary RESTful API interface.

The SDM is built upon an existing software base and technology. It not only manages static provisioned subscriber data, but also dynamic intra- and inter-session data from MPE devices—for example, when it is critical to store inter-session quota data centrally so that it can be retrieved upon the next subscriber attachment, wherever that attachment occurs within the network. Intra-session data such as mappings from IP addresses to MSISDNs becomes important as well, especially when managing enforcement points such as DPI devices and optimization gateways where MSISDN/IMSI data is not available. With this the SDM provides both a storage and notification platform for policy operations, as well as a platform for operator provisioning.

For detailed information on the SDM, see the Subscriber Data Management documentation.

- The Oracle Communications User Data Repository (UDR) is a highly-scalable, consolidated database back end for subscriber and profile data. UDR utilizes multiple application front ends with the database. UDR supports the Oracle Communications Enhanced Subscriber Profile Repository (ESPR) application, a function used for the storage and management of subscriber policy control and pool data. XML-REST and XML-SOAP interfaces are used by ESPR for creating, retrieving, modifying, and deleting subscriber and pool data.

For detailed information on the UDR, see the User Data Repository documentation.

- A customer-specified SPR.

See the SPR documentation for more information.

To use an SPR with CMP, you must perform the following actions:

- [Configuring the CMP System to Manage SPR Subscriber Data](#)
- [Configuring the SPR Connection](#)

You can also modify an SPR connection. See [Modifying the SPR Connection](#) for details.

Configuring the CMP System to Manage SPR Subscriber Data

The CMP system can manage SPR subscriber data. Before this can occur, the CMP operating mode must support managing SPR clusters.



Caution: CMP operating modes should only be set in consultation with My Oracle Support. Setting modes inappropriately can result in the loss of network element connectivity, policy function, OM statistical data, and cluster redundancy.

CAUTION

To reconfigure the CMP operating mode:

1. From the **Help** section of the navigation pane, select **About**.
The **About** page opens, displaying the CMP software release number.
2. Click the **Change Mode** button.
Consult with My Oracle Support for information on this button.
The **Mode Settings** page opens.
3. In the Mode section, select the mode **Diameter 3GPP**, **Diameter 3GPP2**, or **PCC Extensions**, as appropriate.
4. At the bottom of the page, select **Manage SPR Subscriber Data**.
5. Click **OK**.
The browser page closes and you are automatically logged out.
6. Refresh the browser page.
The **Welcome** page appears.

You are now ready to define an SPR cluster profile and manage SPR subscriber profile and pooled quota data.

Configuring the SPR Connection

You must define the operation mode and connection details for the SPR database before you can look up subscriber information from the CMP system.

To configure the CMP connection to an SPR database:

1. From the **SPR** section of the navigation pane, select **Configuration**.
The **SPR Connection Configuration** page opens in the work area, displaying connection information.
2. On the **SPR Connection Configuration** page, click **Modify**.
The **Configuration** page opens.
3. Enter information as appropriate for the SPR system:
 - a) **SPR Operation Mode** (required) — Select from the list:
 - **SDM RESTful API** (default)
 - b) **Remote Port** — Enter the port (a number from 1 to 65535) to listen on for SPR traffic.
The default port is 8787.
 - c) **Secure Connection** — Select to establish a secure connection.

- d) **Enable Custom Fields for Data Entry**—Select to show the custom fields on the **Service**, **User Session Policy**, and **User Location** tabs.
 - e) **SDM Profile Fields**—Defines the custom fields for the SDM profile.
Enter the field name in the field and click **Add**. To remove a field from the list, select the field and click **Delete**.
 - f) **SDM Pool Fields**—Defines the custom fields for the SDM pool.
Enter the field name in the field and click **Add**. To remove a field from the list, select the field and click **Delete**.
4. When you finish, click **Save**.
The connection definition is added to the CMP database.
The SPR connection is configured.

Modifying the SPR Connection

To modify the SPR connection:

1. From the **SPR** section of the navigation pane, select **Configuration**.
The **SPR Connection Configuration** page opens in the work area, displaying connection information.
2. Click **Modify**.
The **Configuration** page opens.
3. Modify the configuration information.
See [Configuring the SPR Connection](#) for information on the fields on this page.
4. When you finish, click **Save**.
The SPR connection configuration is modified.

Finding a Subscriber Profile

Once you have defined SPR devices, you can search them for a subscriber profile.

To find a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select the **Data Source Primary Diameter Identity**.
This is the list of defined SPR devices. You can select any SPR device configured for the Policy Management network. Devices are identified by both their primary identity and MPE device name.
3. Select the **Key Type**:
 - **E.164 (MSISDN)** (default) — search by Mobile Station International Subscriber Directory Number. This is a number of up to 15 digits.
 - **IMSI** — search by International Mobile Subscriber Identity. This is a number of up to 15 digits.
 - **NAI** — search by Network Access Identifier.
 - **Pool ID** — search by quota pool identifier.

4. **Key String** — enter a search string in the format appropriate for the selected key type. The string must match exactly; partial or wildcard searching is not supported.
5. Click **Search**.
The **Subscriber Profile** page opens, displaying information about the subscriber.

Note: If no matching subscriber profile is found, the page displays the message `No matching user is found`.
6. When you finish, click **Back to Search Page**.
The **Subscriber Profile Administration** page opens.

Creating a Subscriber Profile

If an SPR database is configured to use the RESTful API interface, you can manually create a subscriber profile.

To create a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Click **Create Subscriber Profile**.
The **New Subscriber Profile** page opens in the work area.
3. Enter the following information:
 - a) Select the **Data Source Primary Diameter Identity**.
You can select any SPR device configured for the Policy Management network.
 - b) In the **Key Fields** section, enter one format:
 - **NAI** — Network Access Identifier. You must enter a valid user name, optionally followed by a valid realm name. A valid user name consists of the characters `&*+0-9?a-z_A-Z{|!#$%'^/= `| ~-`, optionally separated by a period (.). A valid realm name consists of the characters `0-9a-zA-Z-` separated by one or more period (.), but the minus sign (-) cannot be first, last, or adjacent to a period.
 - **E.164 (MSISDN)** — Mobile Station International Subscriber Directory Number. Enter up to 15 Unicode digits, optionally preceded by a plus sign (+).
 - **IMSI** — International Mobile Subscriber Identity. Enter up to 15 Unicode digits.
 - c) Optionally, in the **Subscriber Information** section, enter the following:
 - **Account ID** — Free-form string that identifies the account for the subscriber. You can enter up to 255 characters.
 - **Billing Day** — The day of the month on which the subscriber's associated quota is reset. If you enter 0 or leave this field blank, then the default global value configured for this MPE device is used instead.
 - **Tier** — The subscriber's tier. Enter a tier name defined in the CMP database; or, if you click **Manage**, a window opens from which you can select a tier name. In order to add a tier, you must enter the tier name prior to clicking **Manage**. See *Managing Subscribers Managing Subscriber in the CMP Wireless User's Guide* for information on managing tiers.
 - **Entitlements** — The subscriber's entitlements. Enter the entitlement names; or, if you click **Manage**, a window opens from which you can enter or select entitlement names defined in

the CMP database. See [Managing Subscribers](#) *Managing Subscriber in the CMP Wireless User's Guide* for information on managing entitlements.

Note: Entitlements are defined external to the CMP system.

- **Custom** — Free-form strings representing custom subscriber fields. You can enter up to 255 characters per field. By default, five fields are available, but if the subscriber profile has more than five custom fields defined, the page displays them. Click **Add** to create additional fields as needed.

4. When you finish, click **Save**.

The subscriber profile is defined.

Managing Subscribers

Managing Subscribers describes how to create and manage subscriber tiers and quota usage within the CMP system.

Note: The actual options you see depend on whether or not your CMP system is configured to operate with a (SPR). For information about the Oracle Communications Subscriber Database Management product, see the SDM documentation. For information about the Oracle Communications User Data Repository product, see the UDR documentation.

Modifying a Subscriber Profile

To modify a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to modify.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Click **Modify**.
The **Subscriber Profile Administration** page opens.
4. Modify subscriber profile information as required.
For a description of the fields contained on this page, see [Creating a Subscriber Profile](#).
5. When you finish, click **Save**.

The subscriber profile is modified.

Deleting a Subscriber Profile

Using the RESTful API operation mode, you can delete a subscriber profile. See [Configuring the SPR Connection](#) for information on setting the operation mode.

To delete a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to delete.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Click **Delete**.
A confirmation message displays.
4. Click **OK** to delete the subscriber profile.
The subscriber profile is deleted.

Viewing Subscriber Entity States

To view the entity states associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to view.
Profile information appears. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Click the **State** tab.
Entity state information appears.
4. When you finish, click **Back to Search Page**.
You have viewed the subscriber entity states.

Creating a Subscriber Entity State Property

To create a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to modify.
Profile information appears. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **State** tab.
Entity state information appears.
4. Click **Create**.
The **Create Property** page opens.
5. Enter the following information:
 - a) **Name** — The name assigned to the property.
The name cannot be blank and must be unique within this list of properties.
 - b) **Value** — The property value.
The value cannot be blank.

6. Click **Save**.
The profile information page opens and displays the message **Properties created successfully**.
7. To create additional properties, repeat steps 4 through 6.
If you exceed 100 states, you are prompted whether you want to add more. Click **Yes** to continue, or **No** to stop.
8. When you finish, click **Back to Search Page**.
The page displays the message **Properties created successfully**.
The subscriber entity state property is defined.

Modifying a Subscriber Entity State Property

You can modify the value (but not the name) of a subscriber profile entity state property. To modify a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to modify.
Profile information appears. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **State** tab.
Entity state information appears.
4. In the list of entity state properties, click the property you want to modify.
The **Modify Property** page opens.
5. Modify the property value as required.
The value cannot be blank.
6. When you finish, click **Save**.
The subscriber entity state property value is modified.

Deleting a Subscriber Entity State Property

To delete a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to modify.
Profile information appears. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **State** tab.
Entity state information appears.
4. In the list of entity state properties:
 - Use the check boxes to select the property or properties you want to delete.

- To select all properties, click **All**.
 - To deselect all properties, click **None**.
5. Click **Delete**.
A confirmation message displays.
 6. Click **OK**.
The property or properties are removed from the list.
- The subscriber entity state properties are deleted.

Viewing Subscriber Quota Information

To view the quotas associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile.
Profile information appears. (See [Finding a Subscriber Profile](#) for information on locating a subscriber profile.)
3. Select the **Quota** tab.
The **Subscriber Profile Quota Usage** page appears. The table provides the following information:
 - **Name** — Quota name defined in the CMP system.
 - **Time Usage** — Usage counter, in seconds, to track time-based resource consumption.
 - **Time Limit** — Time limit, in seconds, defined in the named quota.
 - **Total Volume Usage** — Usage counter, in bytes, to track volume-based resource consumption.
 - **Total Volume Limit** — Volume limit, in bytes, defined in the named quota.
 - **Upstream Volume Usage** — Usage counter, in bytes, to track upstream bandwidth volume-based resource consumption. Also known as Input Volume.
 - **Upstream Volume Limit** — Upstream volume limit, in bytes, defined in the named quota.
 - **Downstream Volume Usage** — Usage counter, in bytes, to track downstream bandwidth volume-based resource consumption. Also known as Output Volume.
 - **Downstream Volume Limit** — Downstream volume limit, in bytes, defined in the named quota.
 - **Service Specific Event** — Usage counter to track service-specific resource consumption.
 - **Service Specific Event Limit** — Resource consumption limit defined in the named quota.
 - **Next Reset Time** — The time after which the usage counters need to be reset.
 - **CID** — A unique identifier, assigned by the CMP system. Top-ups and rollovers have the CID of their associated plan.
 - **Type** — Defines whether the data is for a quota (plan), pass, rollover, top-up, or default rollover.
 - **Quota State** — An internal identifier, which defines whether the option selected in the **Type** field is active or expired.
 - **RefInstanceId** — The CID of the plan.
4. When you finish, click **Back to Search Page**.
You have viewed the subscriber quota information.

Adding a Subscriber Quota Category

To add a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to view.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Quota** tab.
The **Quota Usage** information appears in the work area.
4. Click **Create**.
The **Quota Usage** page opens. If you exceed 10 quotas, you are prompted whether to add more. Click **Yes** to continue, or **No** to stop.
5. Enter the following information:
 - a) **CID** — A unique identifier assigned by the CMP system. Rollovers and top-ups have the CID of their associated plan.
Note: This information is assigned by the system, and you should not change it.
 - b) **Name** (required) — Select the name of a quota. You cannot add the same quota twice for a subscriber. See the *Policy Wizard Reference* for information on creating quotas.
 - c) **Type** — Select the type of quota defined in the CMP system. You can select **quota** (plan), **pass**, **rollover**, **top-up**, or **default rollover**.
 - d) **Time (seconds)** — Enter a value, in seconds, to track time consumption.
The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - e) **Total Volume (bytes)** — Enter a value, in bytes, to track bandwidth volume consumption.
The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - f) **Upstream Volume (bytes)** — Enter a value, in bytes, to track upstream bandwidth volume consumption.
The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - g) **Downstream Volume (bytes)** — Enter a value, in bytes, to track downstream bandwidth volume consumption.
The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - h) **Service Specific Event** — Enter a value representing service-specific resource consumption.
The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - i) **Next Reset Time** (required) — Enter a date and time after which the quotas need to be reset, in the format *yyyy-mm-ddThh:mm:ss[Z]* (for example, **2011-11-01T00:00:01-5:00**).
Alternatively, click  (calendar) and select a date, enter a time, and optionally select a UTC offset (time zone). When you finish, click **OK**.
 - j) **Quota State** — This field is an internal identifier and should not be defined by the user.
 - k) **RefInstanceID** — The CID of the associated plan. This field only applies to a top-up type quota.
Note: This field is an internal identifier, and you should not change it.
6. When you finish, click **Save**.
The subscriber quota is defined.

Modifying a Subscriber Quota Category

To modify a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to view.
Profile information appears. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Quota** tab.
The **Subscriber Profile Quota Usage** page appears.
4. Click the **Name** of the quota you want to modify.
The **Quota Usage** page opens, displaying information about the quota.
5. Modify the subscriber quota information as required.
For a description of the fields contained on this page, see [Adding a Subscriber Quota Category](#).
6. When you finish, click **Save**.

The subscriber quota category is modified.

Deleting a Subscriber Quota Category

To delete a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to modify.
Profile information appears. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Quota** tab.
The **Subscriber Profile Quota Usage** page appears.
4. In the list of quotas:
 - Use the check boxes to select the quota or quotas you want to delete.
 - To select all quotas, click **All**.
 - To deselect all quotas, click **None**.
5. Click **Delete**.
A confirmation message displays.
6. Click **OK**.
The quota or quotas are removed from the list.

The subscriber quota categories are deleted.

Adding a Member to a Pooled Quota Group

You can add a member and associate a subscriber when creating a pooled quota group. You can include up to 20 subscribers in a pooled quota group.

To add a member to a pooled quota group:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select **Create Pooled Quota Group**.
The **New Pooled Quota Group Profile** page opens.
3. In the **Data Source Primary Diameter Identity** section of the page, select one of the configured ProfileV3 or ProfileV4 data sources.
4. In the **Pool Quota Group Key Fields** section of the page, enter the **Pool ID**.
The pool ID must be a numeric value that is greater than 0 and can have a maximum of 22 decimals.
5. (Optional) In the **Pool Information** section of the page, enter the following:
 - a) **Billing Day** — The billing day of the subscriber pool. This field is used only for monthly billing.
 - b) **Tier** — Enter the name of a tier defined in the CMP database or click **Manage** to select a tier.
 - c) **Entitlements** — Click **Manage** and select one or more entitlement names defined in the CMP database.
 - d) **Custom 1, Custom 2, Custom 3, Custom 4, Custom 5** — Enter name value fields. You can refer to them in policies.
 - e) **Custom N** — If you click **Add**, you can add additional custom fields.
6. (Optional) In the **Membership Information** section of the page, to add a member or associate a subscriber to the pooled quota group:
 - a) **Key Type** — The type of subscriber identifier type. You can select one of the following:
 - **E.164 (MSISDN)** — Mobile Station International Subscriber Directory Number.
 - **IMSI** — International Mobile Subscriber Identity.
 - **NAI** — Network Access Identifier.
 - b) **Key String** — Enter the key string for the subscriber.
Note: When associating a subscriber, you must enter the subscriber **Key String**.
 - c) Click **Add** to add the subscriber to the pooled quota group.
7. When you finish, click **Save**.

The member is added to the pooled quota group.

Querying by Pool ID

You can query a new quota by specifying the Pool ID Key Type and Key String value.

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.

2. Select **Pool ID** in the **Key Type** list, enter a **Key String** and click **Search**.
The **Pool Group Quota Profile** page opens with the search results. The following tabs appear:
 - **Pool Profile**
 - **Pool Quota**
 - **Pool State**
3. You can select the **Modify**, **Delete**, or **Back to Search Page** options.

Creating a Pool Quota Profile

The CMP system uses a pool quota profile for tracking and displaying usage threshold events.

To create a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens.
4. Click **Pool Quota Profile**.
The **Quota Usage** section displays.
5. Click **Create**.
6. Enter the following:
 - a) **Name** — Select the name of the pool state.
 - b) **Type** — Select the quota being assigned to the pool. You can select **quota (plan)**, **pass**, **top-up**, **roll-over**, or **roll-over-def**.
If you select **roll-over-def**, rollover units are consumed before top-up units unless the highest priority top-up expires in the next 24 hours.
 - c) **Time** (seconds) — The amount of time attributed to the quota in seconds.
 - d) **Total Volume** (bytes) — The amount of volume attributed to a length of time.
 - e) **Upstream Volume** (bytes) — Traffic from the handset (or other device) to the network.
 - f) **Downstream Volume** (bytes) — Traffic directed to the handset or other device.
 - g) **Service Specific Event** — Tracks text information.
 - h) **Next Reset Time** — The reset date and time of the subscriber or pool quota usage.
Note: This is typically the billing day, although for a daily quota the usage is normally reset at midnight or shortly thereafter.
7. When you finish, click **Save**.
The pool quota profile is created.

Modifying a Pool Quota Profile

To make changes to the subscriber information or membership information, modify the pool quota profile.

To modify a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens with **Pool Profile** as the default.
4. Click **Pool Quota Profile**.
The **Pool Quota Profile** view displays.
5. Select the profile that you want to modify.
6. Modify any of the fields.
Note: The **Name** field cannot be changed.
7. When you finish, click **Save**.

The pool quota profile is modified.

Deleting a Pool Quota Profile

To delete a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
The **Data Source Primary Diameter Identity** and **Key Type** are selected.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens.
4. Click **Pool Quota Profile**.
The **Quota Usage** section displays.
5. Select the name of the profile you want to delete and click **Delete**.
A confirmation message displays.
6. Click **OK**.
The selected properties are deleted.

Modifying a Pool Profile

You can modify a pool profile to make changes to the subscriber information or membership information.

To modify a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of the **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens with Pool Profile as the default.
4. Click **Modify**.
The **Subscriber Profile Configuration** page opens.
5. Modify any of the field information.
6. When you finish, click **Save**.

The pool profile is modified.

Deleting a Pool Profile

To delete a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens with **Pool Profile** as the default.
4. Click **Delete**.
A confirmation message displays.
5. Click **OK**.

The pool profile is deleted.

Creating a Pool State

When using an Sh ProfileV3 or ProfileV4 data source, you can define a pool state.

To create a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Subscriber Profile** page opens.
4. Select the **Pool State** tab.
The **Pool Profile** page opens.
5. Click **Create**.

The Create Property section displays.

6. Enter the following:

- **Name** — The name of the pool state.
- **Value** — The value can be any string, for example, **Profile V3** or **V4**.

7. When you finish, click **Save**.

The pool state is created. The Pool Entity State Properties section displays the **Pool Quota Group Key Fields** and the **Pool ID**.

Modifying a Pool State

If you want to make changes to the subscriber information or membership information, you can modify the pool state.

To modify a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Subscriber Profile** page opens.
4. Select the **Pool State** tab.
The **Pool Entity State Properties** section displays.
5. Click the **Name** of the pool state that you want to modify.
The **Modify Property** section displays.
6. The **Name** and **Value** fields are displayed but you can only modify the **Value** field.
7. Modify the **Value** field.
8. When you finish, click **Save**.

The system saves the modified pool state.

Deleting a Pool State

To delete a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Subscriber Profile** page opens.
4. Select the **Pool State** tab.
The **Pool Entity State Properties** section is displayed.

5. Select a check box for one or more properties to delete and click **Delete**.
The specified properties are deleted.

Chapter 6

Monitoring the MRA

Topics:

- [*Displaying Cluster and Blade Information.....86*](#)
- [*KPI Dashboard.....87*](#)
- [*Mapping Reports Display to KPIs.....88*](#)
- [*The Subscriber Session Viewer.....108*](#)

Monitoring MRA is similar to monitoring the MPE devices. The MRA uses the Reports page, the Logs page, and the Debug page to provide the MRA status information. Specifically:

- Cluster and blade information
- DRMA information
- Event logs

Displaying Cluster and Blade Information

The report page is used to display the cluster and blade status, in addition to the Diameter protocol related statistics. The following figure shows cluster, blade information, and the Diameter statistics.

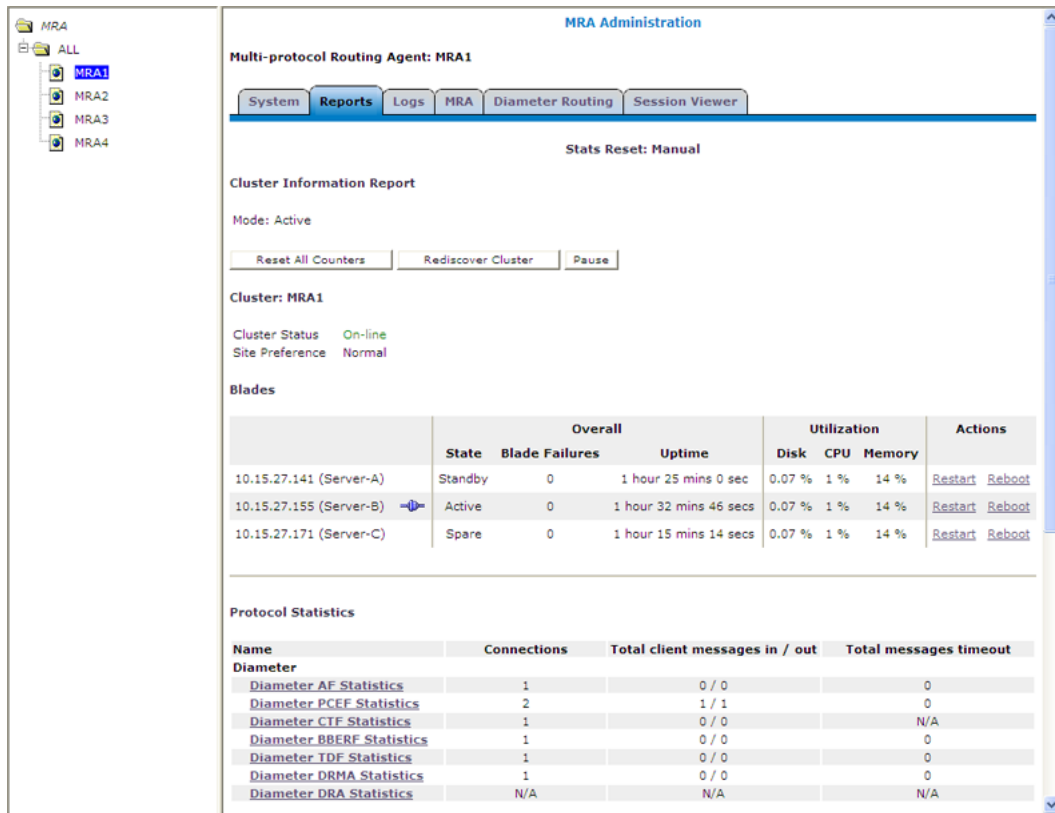


Figure 17: Cluster, Blade, and Diameter Information

The following is a list of Diameter statistics:

- Diameter AF (Application Function) Statistics
- Diameter PCEF (Policy and Charging Enforcement Function) Statistics
- Diameter CTF (Charging Trigger Function) Statistics
- Diameter BBERF (Bearer Binding and Event Reporting) Statistics
- Diameter TDF (Traffic Detection Function) Statistics
- Diameter DRMA (Distributed Routing and Management Application) Statistics
- Diameter DRA (Distributed Routing Application) Statistics

For a detailed breakdown of a statistic, click the statistic. For descriptions of the statistics available for display, refer to [Mapping Reports Display to KPIs](#).

Viewing Trace Logs

The trace logs page displays MRA related messages. The page also has functionality to configure these logs and provides a log viewer to search and browse the log entries.

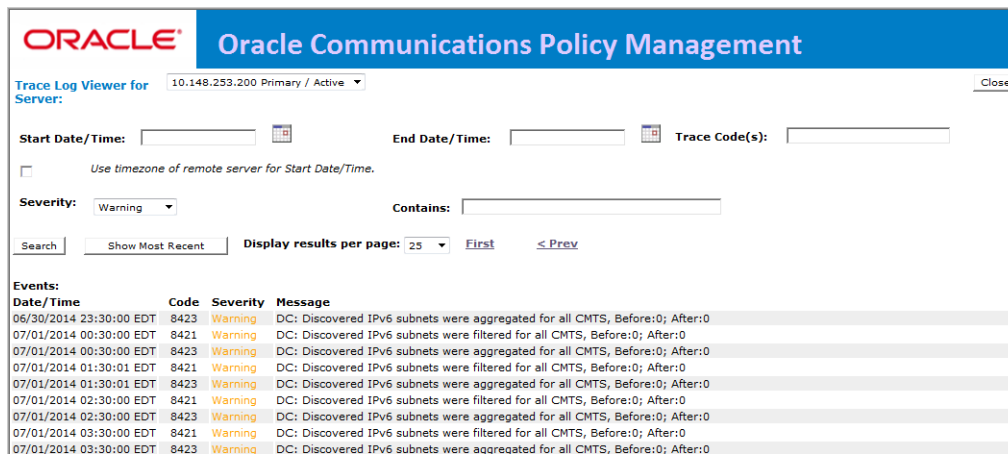


Figure 18: MRA Trace Log

Trace Log Forwarding

The CMP cable mode only system provides log forwarding configuration for all products that have trace logs: MPE, MRA, MA, BoD, and the CMP itself. Refer to *Configuring Log Settings* in the *Configuration Management Platform Cable User's Guide* for additional information.

KPI Dashboard

The KPI dashboard provides a multi-site, system-level, summary of performance and operational health indicators in the CMP web based GUI. The display includes indicators for:

- Offered load (transaction rate)
- System capacity (counters for active sessions)
- Inter-system connectivity
- Physical resource utilization (memory, CPU)
- System status

To display the KPI dashboard, from the main menu click KPI Dashboard. The dashboard opens in the work area.

The KPI dashboard displays the indicators for all the systems on a single page, with the KPIS for each MRA in a separate table. Each row within a table represents a single system (either an MRA blade or an MPE blade that is being managed by that MRA). The table cells are rendered using a color scheme to highlight areas of concern that is well adapted by the telecommunication industry. The table contents are periodically refreshed. The color changing thresholds are user configurable. The refresh rate is set to 10 seconds and is not configurable.

The following figure is an example illustrating the dashboard's contents.

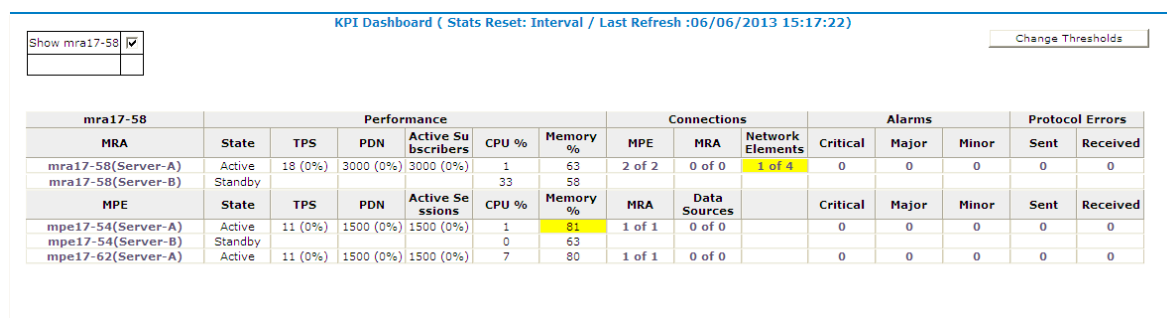


Figure 19: KPI Dashboard

The top left corner lists each MRA with a checkbox that allows you to enable/disable the table for that MRA. In the top right corner there is a **Change Thresholds** button that allows you to change threshold settings used to determine cell coloring (discussed below).

Each MRA or MPE system has two rows in the table. The first row displays data for the primary (active) blade in the cluster. The second row displays data for the secondary (backup) blade in the cluster. Several of the KPI columns are not populated for the secondary blade (since the blade is not active). The only columns that contain data are: Status, CPU%, and Memory%.

If a monitored system is unreachable, or if the data is unavailable for some reason, then the status is set to "Off-line" and the values in all the associated columns is cleared. In this situation, the entire row is displayed with the error color (red). If a monitored system does not support KPI retrieval then the status is set to "N/A" and the values in all the associated columns is cleared. No coloring is applied.

The columns that display "TPS" (on the MPE - the number of Diameter Requests (per second) received from the Clients) and "PDN Connections" information is displayed in the form X (Y%) where X represents the actual numeric value and Y represents the % of rated system capacity that is consumed.

The columns that display connection counts is displayed in the form "X of Y" where X is the current number of connections and Y is the configured number of connections. When X and Y are not the same, the column uses the warning color to indicate a connectivity issue, unless X is 0, in which case the error color is displayed.

Mapping Reports Display to KPIs

From the KPI Dashboard, you can click any MPE or MRA system shown to open the **Reports** page. From there, a variety of statistics and measurements can be viewed. In the following tables, these statistics are mapped to their names as they appear in OSSI XML output.

For more information on the OSSI XML interface, see the *OSSI XML Interface Definitions Reference Guide*.

¹ On the MPE - the number of Diameter Requests (per second) received from the Clients). On the MRA - The number of Diameter Requests per second received from either MRA and the number of Diameter Requests per second sent to the HSS.

Table 6: Policy Statistics

Display	MPE	MRA	Name
Peg Count	Y	N	Policy Count
Evaluated	Y	N	Evaluated Count
Executed	Y	N	Executed Count
Ignored	Y	N	Ignored Count
Policy Details Stats:			
Name	Y	N	Policy Name
Evaluated	Y	N	Eval Count
Executed	Y	N	Trigger Count
Ignored	Y	N	Ignore Count
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	(Data for each installed rule)

Table 7: Quota Profile Statistics Details

Display	MPE	MRA	Name
Peg Count	Y	N	Quota Count
Activated	Y	N	Quota Activated Count
Volume Threshold Reached	Y	N	Quota Volume Threshold Reached Count
Time Threshold Reached	Y	N	Quota Time Threshold Reached Count
Event Threshold Reached	Y	N	Quota Event Threshold Reached Count

Table 8: Diameter Application Function (AF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count

Display	MPE	MRA	Name
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
AAR messages received/sent	Y	Y	AAR Recv Count\AAR Send Count
AAR Initial messages received/sent	Y	Y	AAR Initial Recv Count\AAR Initial Send Count
AAR Modification messages received/sent	Y	Y	AAR Modification Recv Count\AAR Modification Send Count
AAA success messages received/sent	Y	Y	AAA Recv Success Count\AAA Send Success Count
AAA failure messages received/sent	Y	Y	AAA Recv Failure Count\AAA Send Failure Count
AAR messages timeout	Y	Y	AAR Timeout Count
ASR messages received/sent	Y	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	Y	Y	ASR Timeout Count
ASA success messages received/sent	Y	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages received/sent	Y	Y	ASA Recv Failure Count\ASA Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages received/sent	Y	Y	STR Recv Count\STR Send Count
STR messages timeout	Y	Y	STR Timeout Count
STA success messages received/sent	Y	Y	STA Recv Success Count\STA Send Success Count
STA failure messages received/sent	Y	Y	STA Recv Failure Count\STA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
Cleanup ASA received	Y	Y	ASA Received Count
Cleanup ASR sent	Y	Y	ASR Sent Count

Display	MPE	MRA	Name
Current number of active sponsored sessions	Y	N	Current Sponsored Session Count
Max sponsored active sessions	Y	N	Max Sponsored Session Count
Current number of active sponsors	Y	N	Current Sponsor Count
Max number of sponsors	Y	N	Max Sponsor Count
Current number of active service providers	Y	N	Current Service Provider Count
Max number of service providers	Y	N	Max Service Provider Count
Diameter AF Peer Stats (in Diameter AF Stats window)	N	Y	
ID	Y	Y	
IP Address: Port			
Currently active connections			
Currently active sessions			
Connect Time	N	Y	Connect Time
Disconnect Time	N	Y	Disconnect Time

Table 9: Diameter Policy Charging Enforcement Function (PCEF) Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count (SCTP or TCP)
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count
CCR messages received/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages received/sent	Y	Y	CCR-I Recv Count\CCR-I Send Count
CCR-I messages timeout	Y	Y	CCR-I Timeout Count
CCA-I success messages received/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count

Display	MPE	MRA	Name
CCA-I failure messages received/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count

Table 10: Diameter Charging Function (CTF) Statistics

Display	MPE	MRA	Name
Connections	N	Y	Conn Count
Currently OK peers	N	Y	Peer Okay Count
Currently down/suspect/reopened peers	N	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	N	Y	Msg In Count\Msg Out Count
CCR messages sent/received	N	Y	CCR Recv Count\CCR Send Count
CCA success messages recd/sent	N	Y	CCA Recv Success Count\CCA Send Success Count

Display	MPE	MRA	Name
CCA failure messages recd/sent	N	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages sent/received	N	Y	CCR-I Recv Count\CCR-I Send Count
CCA-I success messages recd/sent	N	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages recd/sent	N	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages sent/received	N	Y	CCR-U Recv Count\CCR-U Send Count
CCA-U success messages recd/sent	N	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages recd/sent	N	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages sent/received	N	Y	CCR-T Recv Count\CCR-T Send Count
CCA-T success messages recd/sent	N	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages recd/sent	N	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages sent/received	N	Y	RAR Recv Count\RAR Send Count
RAA success messages recd/sent	N	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd/sent	N	Y	RAA Recv Failure Count\RAA Send Failure Count
ASR messages sent/received	N	Y	ASR Recv Count\ASR Send Count
ASA success messages recd/sent	N	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages recd/sent	N	Y	ASA Recv Failure Count\ASA Send Failure Count
Currently active sessions	N	Y	Active Session Count
Max active sessions	N	Y	Max Active Session Count

Table 11: Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count

Display	MPE	MRA	Name
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
CCR messages received/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages received/sent	Y	Y	CCR-I Recv Count\CCR-I Send Count
CCR-I messages timeout	Y	Y	CCR-I Timeout Count
CCA-I success messages received/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages received/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Currently active sessions	Y	N	Curr Session Count

Display	MPE	MRA	Name
Max active sessions	Y	N	Max Active Session Count
Diameter BBERF connections	Y	Y	

Table 12: Diameter TDF Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
CCR messages received/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count

Display	MPE	MRA	Name
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
TSR messages received/sent	Y	Y	
TSA success messages received/sent	Y	Y	
TSA failure messages received/sent	Y	Y	
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count
Diameter TDF connections	Y	Y	

Table 13: Diameter Sh Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count
Messages retried	Y	N	
UDR messages received/sent	Y	N	UDR Messages Received Count\UDR Messages Sent Count
UDR messages timeout	Y	N	UDRTimeout Count
UDR messages retried	Y	N	
UDA success messages received/sent	Y	N	UDA Success Messages Received Count\UDA Success Messages Sent Count
UDA failure messages received/sent	Y	N	UDA Failure Messages Received Count\UDA Failure Messages Sent Count
PNR messages received/sent	Y	N	PNR Messages Received Count\PNR Messages Sent Count
PNA success messages received/sent	Y	N	PNA Success Messages Received Count\PNA Success Messages Sent Count
PNA failure messages received/sent	Y	N	PNA Failure Messages Received Count\PNA Failure Messages Sent Count

Display	MPE	MRA	Name
PUR messages received/sent	Y	N	PUR Messages Received Count\PUR Messages Sent Count
PUR messages timeout	Y	N	PURTimeout Count
PUR messages retried	Y	N	
PUA success messages received/sent	Y	N	PUA Success Messages Received Count\PUA Success Messages Sent Count
PUA failure messages received/sent	Y	N	PUA Failure Messages Received Count\PUA Failure Messages Sent Count
SNR messages received/sent	Y	N	SNR Messages Received Count\SNR Messages Sent Count
SNR messages timeout	Y	N	SNRTimeout Count
SNR messages retried	Y	N	
SNA success messages received/sent	Y	N	SNA Success Messages Received Count\SNA Success Messages Sent Count
SNA failure messages received/send	Y	N	SNA Failure Messages Received Count\SNA Failure Messages Sent Count
Currently active sessions	Y	N	Active Sessions Count
Max active sessions	Y	N	Maximum Active Sessions Count
Diameter Sh connections			

Table 14: Diameter Distributed Routing and Management Application (DRMA) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently okay peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
DBR messages received/sent	N	Y	DBRRecv Count\DBRSend Count
DBR messages timeout	N	Y	DBRTimeout Count
DBA success messages received/sent	N	Y	DBARecv Success Count\DBASend Success Count

Display	MPE	MRA	Name
DBA failure messages received/sent	N	Y	DBARecv Failure Count\DBASend Failure Count
DBA message received/sent-binding found	N	Y	Binding Found Recv Count\Binding Found Send Count
DBA messages received/sent – binding not found	N	Y	Binding Not Found Recv Count\Binding Not Found Send Count
DBA messages received/sent – PCRF down	N	Y	Binding Found Pcrf Down Recd Count\ Binding Found Pcrf Down Send Count
DBA messages received/sent – all PCRFs down	N	Y	All Pcrfs Down Recv Count\ All Pcrfs Down Send Count
DBR-Q messages received/sent	N	Y	
DBR-Q messages timeout	N	Y	
DBA-Q success messages received/sent	N	Y	
DBA-Q failure messages received/sent	N	Y	
DBR-QC messages received/sent	N	Y	
DBR-QC messages timeout	N	Y	
DBA-QC success messages received/sent	N	Y	
DBA-QC failure messages received/sent	N	Y	
DBR-U messages received/sent	N	Y	
DBR-U messages timeout	N	Y	
DBA-U success messages received/sent	N	Y	
DBA-U failure messages received/sent	N	Y	
DBR-T messages received/sent	N	Y	
DBR-T messages timeout	N	Y	
DBA-T success messages received/sent	N	Y	
DBA-T failure messages received/sent	N	Y	
DBR-S messages received/sent	N	Y	

Display	MPE	MRA	Name
DBR-S messages timeout	N	Y	
DBA-S success messages received/sent	N	Y	
DBA-S failure messages received/sent	N	Y	
RUR messages received/sent	Y	Y	RURRecv Count\ RURSend Count
RUR messages timeout	Y	Y	RURTimeout Count
RUA success messages received/sent	Y	Y	RUARecv Success Count\ RUASend Success Count
RUA failure messages received/sent	Y	Y	RUARecv Failure Count\ RUASend Failure Count
LNR messages received/sent	Y	Y	LNRRRecv Count\ LNRSend Count
LNR messages timeout	Y	Y	LNRTIMEOUT Count
LNA success messages received/sent	Y	Y	LNARECV Success Count\ LNASend Success Count
LNA failure messages received/sent	Y	Y	LNARECV Failure Count\ LNASend Failure Count
LSR messages received/sent	Y	Y	LSRRecv Count\ LSRSend Count
LSR messages timeout	Y	Y	LSRTIMEOUT Count
LSA success messages received/sent	Y	Y	LSARECV Success Count\ LSASend Success Count
LSA failure messages received/sent	Y	Y	LSARECV Failure Count\ LSASend Failure Count
SQR messages received/sent			
SQR messages timeout			
SQA messages received/sent			
SQA messages timeout			
Session found received/sent			
Session not found received/sent			
Diameter DRMA connections			

Note: The statistics listed in apply only to MRA devices.

Table 15: Diameter DRA Statistics

Display	MPE	MRA	Name
Currently active bindings	N	Y	DRABinding Count
Max active bindings	N	Y	Max DRABinding Count
Total bindings	N	Y	DRATotal Binding Count
Suspect bindings	N	Y	Suspect Binding Count
Detected duplicate bindings	N	Y	Detected Duplicate Binding Count
Released duplicate bindings	N	Y	Released Duplicate Binding Count
Diameter Release Task Statistics	N	Y	
Bindings Processed	N	Y	Release Bindings Processed
Bindings Released	N	Y	Release Bindings Removed
RAR messages sent	N	Y	Release RARs Sent
RAR messages timed out	N	Y	Release RARs Timed Out
RAA success messages recd	N	Y	Release RAAs Received Success
RAA failure messages recd	N	Y	Release RAAs Received Failure
CCR-T messages processed	N	Y	Release CCRTs Received

Table 16: Diameter Sy Statistics

Display	MPE	MRA	Name
Connections	Y	N	Current Connections Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Messages In Count\Messages Out Count
SLR messages received/sent	Y	N	SLR Messages Received Count\SLR Messages Sent Count
SLR messages timeout	Y	N	SLRTimeout Count
SLA success messages received/sent	Y	N	SLA Success Messages Received Count\SLA Success Messages Sent Count
SLA failure messages received/sent	Y	N	SLA Failure Messages Received Count\SLA Failure Messages Sent Count

Display	MPE	MRA	Name
SNR messages received/sent	Y	N	SNR Messages Received Count\SMR Messages Sent Count
SNA success messages received/sent	Y	N	SNA Success Messages Received Count\SNA Success Messages Sent Count
SNA failure messages received/sent	Y	N	SNA Failure Messages Received Count\SNA Failure Messages Sent Count
STR messages received/sent	Y	N	STR Messages Received Count\STR Messages Sent Count
STR messages timeout	Y	N	STRTimeout Count
STA success messages received/sent	Y	N	STA Success Messages Received Count\STA Success Messages Sent Count
STA failure messages received/sent	Y	N	STA Failure Messages Received Count\STA Failure Messages Sent Count
Currently active sessions	Y	N	Active Sessions Count
Max active sessions	Y	N	Maximum Active Sessions Count
Diameter Sy connections			

Table 17: RADIUS Statistics

Display	MPE	MRA	Name
Connections	Y	Y	
Total messages in/out	Y	Y	Messages In Count\ Messages Out Count
Total RADIUS messages received	Y	Y	
Total RADIUS messages send		Y	
Messages successfully decoded	Y	Y	
Messages dropped	Y	Y	
Total errors received	Y	Y	
Total errors sent	Y	Y	
Accounting Start sent	Y	Y	
Accounting Start received	Y	Y	Accounting Start Count
Accounting Stop sent	Y	Y	

Display	MPE	MRA	Name
Accounting Stop received	Y	Y	Accounting Stop Count
Accounting Stop received for unknown reason	Y	Y	
Accounting On sent	Y	Y	
Accounting On received	Y	Y	
Accounting Off sent	Y	Y	
Accounting Off received	Y	Y	
Accounting Response sent	Y	Y	Accounting Response Count
Accounting Response received	Y	Y	
Duplicates detected	Y	Y	Duplicated Message Count
Unknown/Unsupported messages received	Y	Y	
Interim Update Received	Y	Y	Accounting Update Count
Interim Update Received for unknown reason	Y	Y	
Currently active sessions	Y	Y	
Max active sessions	Y	Y	
Messages with Authenticator field mismatch	Y	Y	
Last RADIUS message received time	Y	Y	
COA-request sent	Y	Y	CoA Request Count
COA-request received	Y	Y	
COA-ACK sent	Y	Y	CoA Ack Count
COA-ACK received	Y	Y	CoA Success Count
COA-NAK sent	Y	Y	
COA-NAK received	Y	Y	CoA Nck Count
Parsed under 100m(icro)s	Y	Y	
Parsed under 200m(icro)s	Y	Y	
Parsed under 500m(icro)s	Y	Y	
Parsed under 1m(illi)s	Y	Y	
Parsed over 1m(illi)s	Y	Y	
Total Parse Time	Y	Y	

Display	MPE	MRA	Name
Average Parse Time	Y	Y	
Maximum Parse Time	Y	Y	
Unknown BNG. Message dropped	Y	Y	Unknown Gateway Request Count
Unknown BNG. Account Start dropped	Y	Y	
Unknown BNG. Account Stop dropped	Y	Y	
Unknown BNG. Interim Update dropped	Y	Y	
Stale sessions deleted	Y	Y	
Stale sessions deleted due to missed Interim Update	Y	Y	
Stale sessions deleted on Account-On or Account-Off	Y	Y	
Invalid subscriber key. Message dropped	Y	Y	
Invalid subscriber identifier specified. Message dropped	Y	Y	Unknown Subscriber Request Count

Table 18: Diameter Latency Statistics shows information for these Diameter Statistics:

- Application Function (AF)
- Policy and Charging Enforcement Function (PCEF)
- Bearer Binding and Event Reporting (BBERF)
- Traffic Detection Function (TDF)
- Diameter Sh protocol
- Distributed Routing and Management Application (DRMA)
- Diameter Sy protocol

Table 18: Diameter Latency Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Active Connection Count
Max Processing Time recd/sent (ms)	Y	Y	Max Trans In Time\ Max Trans Out Time
Avg Processing Time recd/sent (ms)	Y	Y	Avg Trans In Time\ Avg Trans Out Time
Processing Time recd/sent <time frame> (ms)	Y	Y	Processing Time [0-20] ms Processing Time [20-40] ms

Display	MPE	MRA	Name
			Processing Time [40-60] ms Processing Time [60-80] ms Processing Time [80-100] ms Processing Time [100-120] ms Processing Time [120-140] ms Processing Time [140-160] ms Processing Time [160-180] ms Processing Time [180-200] ms Processing Time [>200] ms

Table 19: Diameter Event Trigger Statistics

Display	MPE	MRA	Name
Diameter Event Trigger Stats by Code	Y	N	
Diameter Event Trigger Stats by Application:			
Diameter PCEF Application Event Trigger	Y	N	
Diameter BBERF Application Event Trigger	Y	N	

Table 20: Diameter Protocol Error Statistics

Display	MPE	MRA	Name
Total errors received	Y	Y	In Error Count
Total errors sent	Y	Y	Out Error Count
Last time for total error received	Y	Y	Last Error In Time
Last time for total error sent	Y	Y	Last Error Out Time
Diameter Protocol Errors on each error codes	Y	Y	(see specific errors listed in GUI)

Table 21: Diameter Connection Error Statistics

Display	MPE	MRA	Name
Total errors received	Y	Y	In Error Count
Total errors sent	Y	Y	Out Error Count
Last time for total error received	Y	Y	Last Error In Time

Display	MPE	MRA	Name
Last time for total error sent	Y	Y	Last Error Out Time
Diameter Protocol Errors on each error codes	Y	Y	(see specific errors listed in GUI)

Table 22: LDAP Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count
Number of searches that failed because of errors	Y	N	Search Err Count
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Average time spent on successful searches (ms)	Y	N	Search Avg Hit Time
Average time spent on unsuccessful searches (ms)	Y	N	Search Avg Miss Time
Number of successful updates	Y	N	Update Hit Count
Number of unsuccessful updates	Y	N	Update Miss Count
Number of updates that failed because of errors	Y	N	Update Err Count
Time spent on successful updates (ms)	Y	N	Update Total Hit Time
Time spent on unsuccessful updates (ms)	Y	N	Update Total Miss Time
Max Time spent on successful update (ms)	Y	N	Update Max Hit Time
Max Time spent on unsuccessful update (ms)	Y	N	Update Max Miss Time
Average time spent on successful update (ms)	Y	N	Update Avg Hit Time
Average time spent on unsuccessful updates (ms)	Y	N	Update Avg Miss Time

Table 23: Sh Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count
Number of searches that failed because of errors	Y	N	Search Err Count
Number of search errors that triggered the retry	Y	N	
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Average time spent on successful searches (ms)	Y	N	Search Avg Hit Time
Average time spent on unsuccessful searches (ms)	Y	N	Search Avg Miss Time
Number of successful updates	Y	N	Update Hit Count
Number of unsuccessful updates	Y	N	Update Miss Count
Number of updates that failed because of errors	Y	N	Update Err Count
Number of update errors that triggered the retry	Y	N	
Time spent on successful updates (ms)	Y	N	Update Total Hit Time
Time spent on unsuccessful updates (ms)	Y	N	Update Total Miss Time
Max Time spent on successful update (ms)	Y	N	Update Max Hit Time
Max Time spent on unsuccessful update (ms)	Y	N	Update Max Miss Time
Average time spent on successful updates (ms)	Y	N	Update Avg Hit Time
Average time spent on unsuccessful updates (ms)	Y	N	Update Avg Miss Time
Number of successful subscriptions	Y	N	Subscription Hit Count
Number of unsuccessful subscriptions	Y	N	Subscription Miss Count

Display	MPE	MRA	Name
Number of subscriptions that failed because of errors	Y	N	Subscription Err Count
Number of subscription errors that triggered the retry	Y	N	
Time spent on successful subscriptions (ms)	Y	N	Subscription Total Hit Time
Time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Total Miss Time
Max Time spent on successful subscriptions (ms)	Y	N	Subscription Max Hit Time
Max Time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Max Miss Time
Average time spent on successful subscriptions (ms)	Y	N	Subscription Avg Hit Time
Average time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Avg Miss Time
Number of successful unsubscriptions	Y	N	Unsubscription Hit Count
Number of unsuccessful unsubscriptions	Y	N	Unsubscription Miss Count
Number of unsubscriptions that failed because of errors	Y	N	Unsubscription Err Count
Number of unsubscription errors that triggered the retry	Y	N	
Time spent on successful unsubscriptions (ms)	Y	N	Unsubscription Total Hit Time
Time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Total Miss Time
Max Time spent on successful unsubscription (ms)	Y	N	Unsubscription Max Hit Time
Max Time spent on unsuccessful unsubscription (ms)	Y	N	Unsubscription Max Miss Time
Average time spent on successful unsubscriptions (ms)	Y	N	Unsubscription Avg Hit Time
Average time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Avg Miss Time

Table 24: Sy Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count
Number of searches that failed because of errors	Y	N	Search Err Count
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Average time spent on successful searches (ms)	Y	N	Search Avg Hit Time
Average time spent on unsuccessful searches (ms)	Y	N	Search Avg Miss Time

Table 25: KPI Interval Statistics

Display	MPE	MRA	Name
Interval Start Time	Y	Y	Interval Start Time
Configured Length (Seconds)	Y	Y	Configured Length (Seconds)
Actual Length (Seconds)	Y	Y	Actual Length (Seconds)
Is Complete	Y	Y	Is Complete
Interval MaxTransactions Per Second	Y	Y	Interval Max Transactions Per Second
Interval MaxMRABinding Count	Y	Y	Interval Max MRABinding Count
Interval MaxSessionCount	Y	Y	Interval Max Session Count
Interval MaxPDNConnectionCount	Y	Y	Interval Max PDNConnection Count

The Subscriber Session Viewer

The Session Viewer displays detailed session information for a specific subscriber. This information is contained on the **Session Viewer** tab, located under the configuration page for both MRA and MPE devices. You can view the same subscriber session from an MRA device or its associated MPE device.

Within the session viewer, you can enter query parameters to render session data for a specific subscriber. For example:

MRA Administration

Multi-protocol Routing Agent: MRA1

System Reports Logs MRA Diameter Routing **Session Viewer**

Session Viewer:

Identifier type: IMSI Identifier name: 310410000000017 Search

Subscriber Binding Data:

UserId(s)	ServerId	IsSuspect	Delete Binding
-----	-----	-----	
IMSI:310410000000017	mpe26-42.test.com	false	
IP:2001:db8:85a3:9837:0:0:0:0			
IP:10.3.3.33			
SESSID:pgw1.test.com;1336073844;13			
Associated MPE mpe26-42.test.com			

Viewing Session Data from the MPE

You can view the same subscriber session from an MRA device or its associated MPE device. To view session data from the MPE:

1. From the Policy Server section of the navigation pane, select **Configuration**.
2. Select the MPE device from the content tree.
3. On the **Session Viewer** tab, select the identifier type (**NAI**, **E.164(MSISDN)**, **IMSI**, **IPv4Address**, or **IPv6Address**), enter the identifier name, and click **Search**. Information about the subscriber session(s) is displayed.

Policy Server Administration

Policy Server: mpe230-127

[System](#)
[Reports](#)
[Logs](#)
[Policy Server](#)
[Diameter Routing](#)
[Policies](#)
[Data Sources](#)
[Session Viewer](#)

Session Viewer:

Identifier type: Identifier name:

Subscriber Session Data:

2 session(s) has been found.

User: IMSI:56575657885 key: 270002
 Account ID:null

User IDs:
 IMSI:56575657885
 Pool ID:null
 Usagekey:IMSI:56575657885

[Read more...](#)

SessionId: pgw.tekelec.com;1408989258;1

AppId: 16777238
 AppName: Gx [REL9, REL8]
 PeerId: pgw.tekelec.com
 DestinationHost: pgw.tekelec.com
 DestinationRealm: tekelec.com
[Read more...](#)

The MRA device is listed by peer ID.

If no session data is available, the CMP returns the following message:

There are no sessions available for the subscriber.

Viewing Session Data from the MRA

You can view the same subscriber session from an MRA device or its associated MPE device. To view session data from the MRA device:

1. From the MRA section of the navigation pane, select **Configuration**.
2. Select the MRA device from the content tree.
3. On the **Session Viewer** tab, select the Identifier Type (NAI, E.164(MSISDN), IMSI, IPv4Address, or IPv6Address), enter the **Identifier name**, and click **Search**. Information about the subscriber binding data is displayed; for example:

MRA Administration

Multi-protocol Routing Agent: MRA1

[System](#)
[Reports](#)
[Logs](#)
[MRA](#)
[Diameter Routing](#)
[Session Viewer](#)

Session Viewer:

Identifier type: IMSI Identifier name:

Subscriber Binding Data:

UserId(s)	ServerId	IsSuspect	Delete Binding
-----	-----	-----	
IMSI:310410000000017	mpe26-42.test.com	false	
IP:2001:db8:85a3:9837:0:0:0:0			
IP:10.3.3.33			
SESSID:pgw1.test.com;1336073844;13			
Associated MPE mpe26-42.test.com			

The MPE device that is handling sessions for the subscriber is listed by its server ID.

If no session data is available, the CMP returns, "There are no bindings available for the subscriber."

Deleting a Session from the Session Viewer Page

The Session Viewer page includes a **Delete** button that lets you delete the session (or binding data) that is being displayed. After you have clicked **Delete** and confirmed the delete operation, the CMP sends the delete request to the MRAgent/MIAgent and returns to the Session Viewer data page, displaying the delete result and the remaining session data.



Caution: This is an administrative action that deletes the associated record in the database and should only be used for obsolete sessions. If the session is in fact active it will not trigger any signaling to associated gateways or other external network elements.

B

BBERF	Bearer Binding and Event Reporting Function: A type of Policy Client used to control access to the bearer network (AN).
-------	---

C

CID	Connection ID
CPU	Central Processing Unit
CTF	Charging Trigger Function

D

Diameter	Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty. Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment.
DNS	Domain Name Services Domain Name System

D

A system for converting Internet host and domain names into IP addresses.

E

E.164

The international public telecommunication numbering plan developed by the International Telecommunication Union.

F

FQDN

Fully Qualified Domain Name

The complete domain name for a specific computer on the Internet (i.e., www.oracle.com).

A domain name that specifies its exact location in the tree hierarchy of the DNS.

G

GPRS

General Packet Radio Service

A mobile data service for users of GSM mobile phones.

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.

H

HSS

Home Subscriber Server

A central database for subscriber information.

HTTP

Hypertext Transfer Protocol

I

IMSI	International Mobile Subscriber Identity International Mobile Station Identity A unique internal network ID identifying a mobile subscriber.
IPv4	Identifies an Internet Protocol version 4 address composed of 4 bytes in a dotted decimal format (for example, nnn.nn.nnn.nn).
IPv6	Identifies an Internet Protocol version 6 address composed of 8 groups of colon-separated 4 hexadecimal digits.
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

K

KPI	Key Performance Indicator
-----	---------------------------

M

MPE	Multimedia Policy Engine A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization.
-----	---

M

MRA Multi-Protocol Routing Agent - Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server devices.

O

OM Operational Measurement

P

PCC Policy and Charging Control

PDN Packet Data Network
A digital network technology that divides a message into packets for transmission.

R

RADIUS Remote Authentication Dial-In User Service
A client/server protocol and associated software that enables remote access servers to communicate with a central server to authorize their access to the requested service. The MPE device functions with RADIUS servers to authenticate messages received from remote gateways. See also Diameter.

realm A fundamental element in Diameter is the realm, which is loosely referred to as domain. Realm IDs are owned by service providers and are used by Diameter nodes for message routing.

X

X

XML

eXtensible Markup Language

A version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.