Oracle® Communications Policy Management

Policy Front End Wireless User's Guide

Release 12.2

E66971 Revision 01

November 2016

Oracle Communications Policy Management Policy Front End Wireless User's Guide, Release 12.2

Table of Contents

List of Figures

List of Tables

Chapter

1

About This Guide

Topics:

This chapter contains an overview of this guide, describes how to obtain help, where to find related documentation, and provides other general information.

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).
- *About Configuring a CMP System, MRA and MPE Devices* describes how to configure the Configuration Management Platform 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.
- *About 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 a Subscriber Profile Repository* and *Managing Subscribers* describe how to work with subscriber profiles, quotas, and pool.
- *About MRA Monitoring* describes how to monitor cluster and blade information, DRMA information, and event logs.

Intended Audience

This guide is intended for service personnel who are responsible for operating Policy Management systems.

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 *personal injury*.)

Icon	Description
⚠ WARNING	Warning: (This icon and text indicate the possibility of *equipment damage*.)
⚠ CAUTION	Caution: (This icon and text indicate the possibility of *service interruption*.)
⚠ TOPPLE	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Specifications

For information about additional publications that are related to this document, refer to the Oracle Help Center site. See *Locate Product Documentation on the Oracle Help Center Site* for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) 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 Help Center site at *http://docs.oracle.com*.
2. Click **`Industries`**.
3. Under the Oracle Communications subheading, click the **`Oracle Communications documentation`** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings “Network Session Delivery and Control Infrastructure” or “Platforms.”
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **`PDF`** link, select **`Save target as`** (or similar command based on your browser), 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:

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.

Multi-Protocol Routing Agent Devices

The Multi-Protocol Routing Agent (MRA) (also known as the Policy Front End) is a product deployed in a Policy Management network that maintains bindings that link subscribers to Multimedia Policy Engine (MPE) devices.

An MRA device ensures that all of a subscriber's Diameter sessions established over the Gq, Ty, Gx, Gxx, Gx Lite, Sh, Sy, Rx, S9, 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 whereby all Diameter Policy and Charging Control (PCC) application messages are proxied through an 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 for a binding using the proprietary Distributed Routing and Management Application (DRMA) protocol. 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.

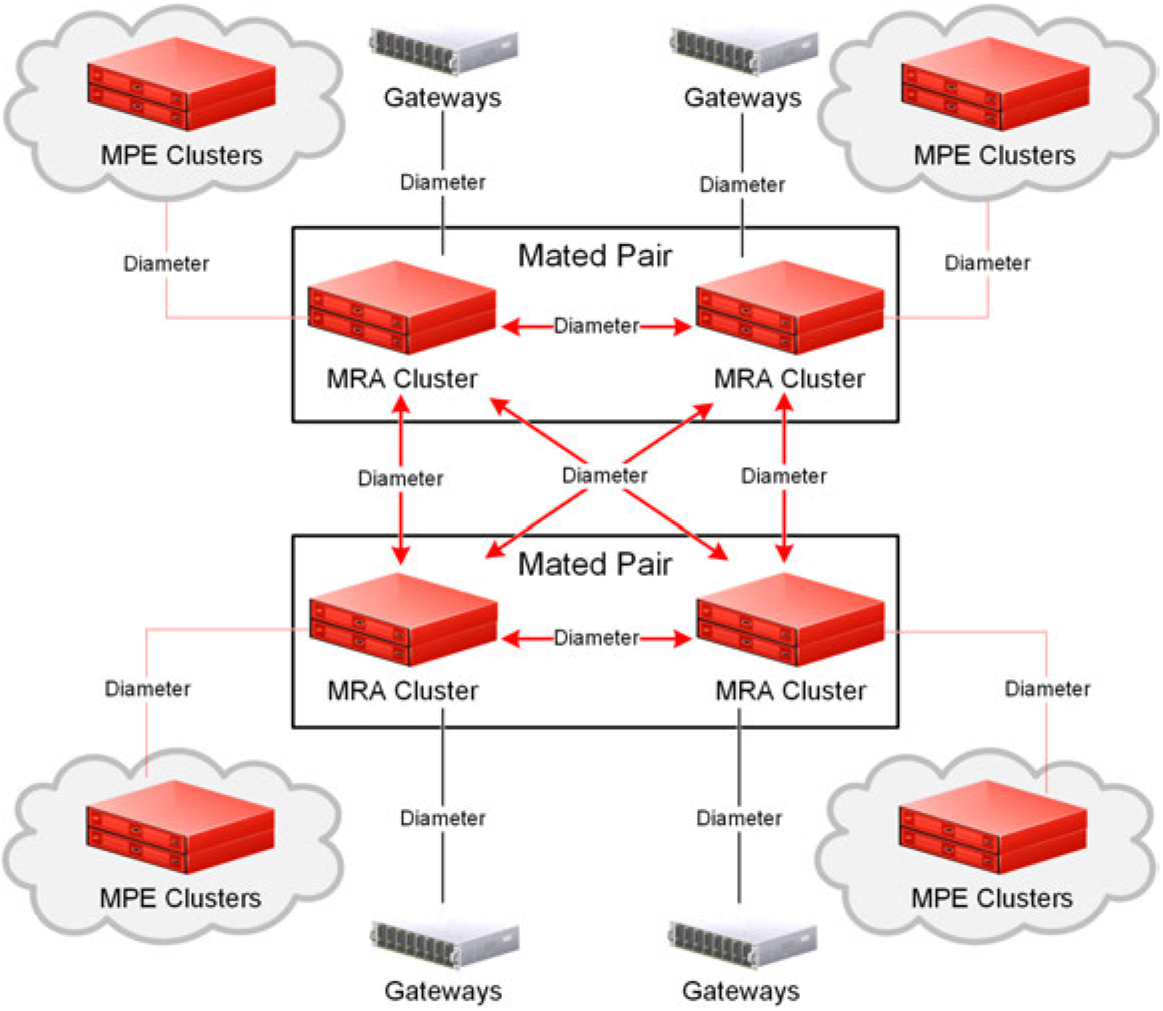


Figure 1: Typical MRA Network

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 Diameter Routing Agent (DRA) binding information. DRMA ensures that all the Diameter sessions for a subscriber are served by the same MPE device. As a result, MRA devices can query one another 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

Each MRA exists as a cluster that consists of two servers, active and standby. Both servers in a cluster share a Virtual IP Address (VIP) that points to which ever server is active.

A backup MRA cluster shares a common pool of MPE devices with a primary MPE cluster. 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 exists as part of a Diameter Route.

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.

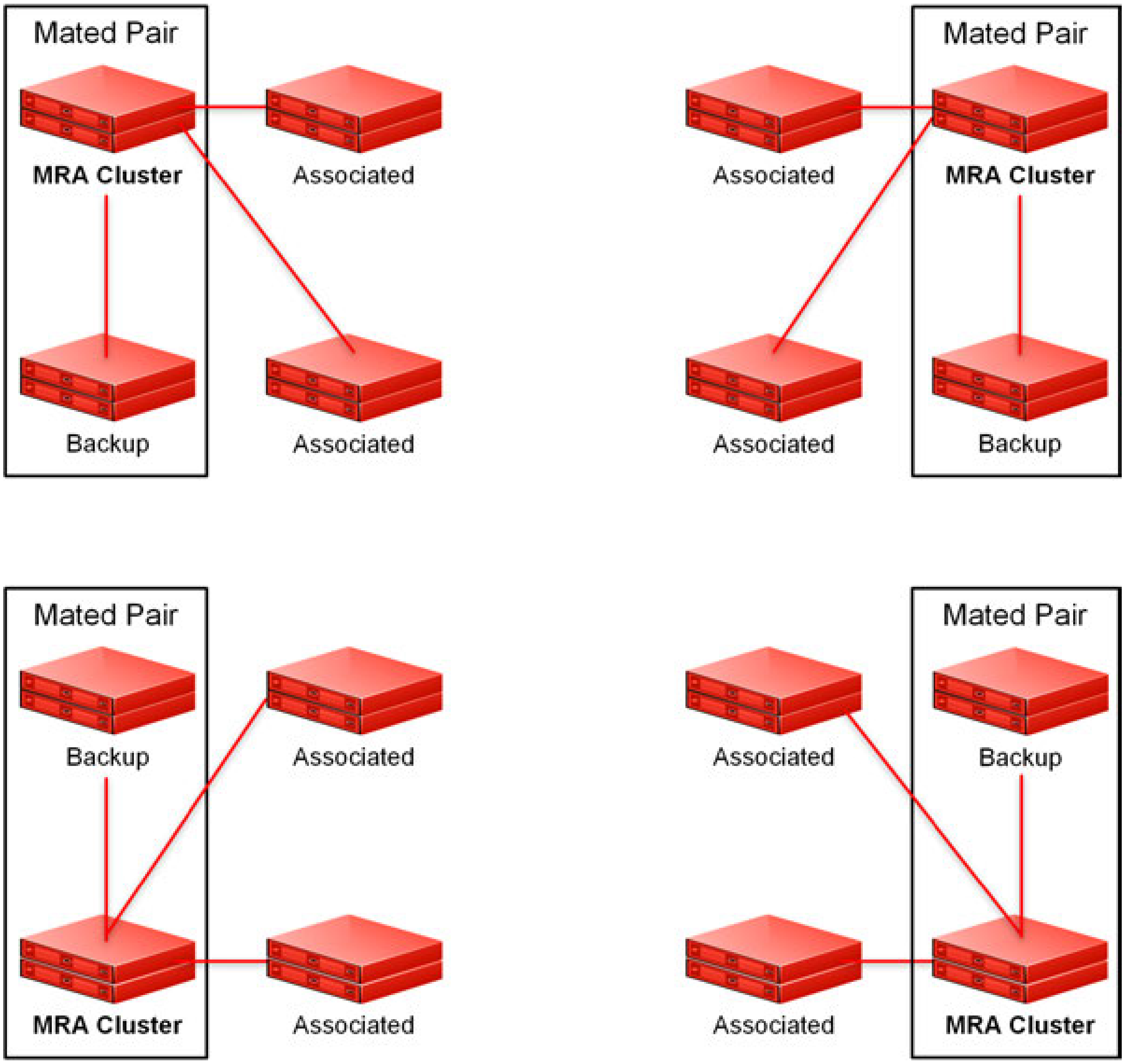
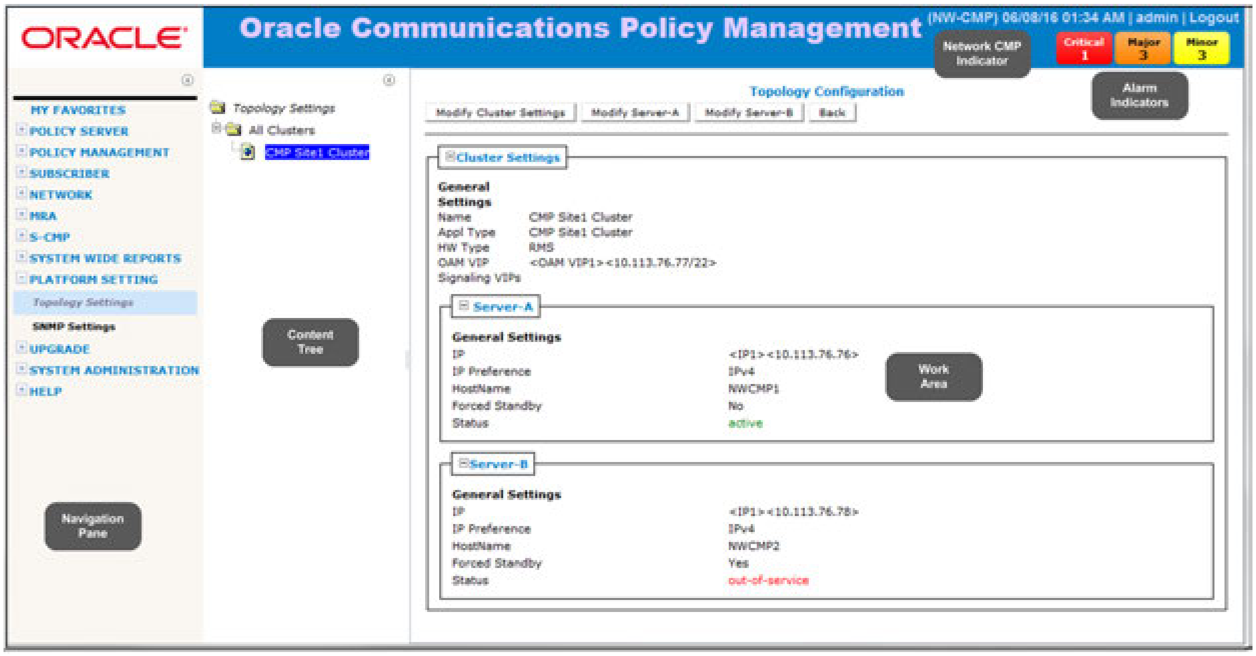


Figure 2: Backup and Associated MRA Clusters and Mated Pairs

GUI Overview

You interact with the CMP system through an intuitive and portable graphical user interface (GUI) supporting industry-standard web technologies (the SSL family of secure communication protocols, HTTP, HTTPS, IPv4, IPv6, and XML). *Figure 3: Layout of the CMP Window – Wireless Mode* shows the layout of the CMP GUI.



Cluster Settings

General Settings

Name	CMP Site1 Cluster
Appl Type	CMP Site1 Cluster
HW Type	RMS
OAM VIP	<OAM VIP1><10.113.76.77/22>
Signaling VIPs	

Server-A

General Settings

IP	<IP1><10.113.76.76>
IP Preference	IPv4
HostName	NWCMP1
Forced Standby	No
Status	active

Server-B

General Settings

IP	<IP1><10.113.76.78>
IP Preference	IPv4
HostName	NWCMP2
Forced Standby	Yes
Status	out-of-service

Figure 3: Layout of the CMP Window – Wireless Mode

The CMP system's window is divided into the following sections:

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 by 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.

Note: 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.

Network CMP 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

About Configuring a CMP System, MRA and MPE Devices

Topics:

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

Note: This document assumes that all CMP systems as well as MRA, and MPE devices are operational and available. 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*.

About Configuration Management Platform's Role in Managing the MRA

The Multi-Protocol Routing Agent,MRA, is a standalone entity that uses the Oracle Communications Policy Management Configuration Management Platform (CMP) system. 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

Note: This document assumes that all CMP systems as well as MRA, and MPE devices are operational and available. 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*.

Creating an MRA Group

You create an MRA group to manage various MRA functions (such as creating stateless sessions) on your wireless network.

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 MRA group.

   The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
5. Click **Save**.

The MRA group is created.

Deleting an MRA Group or Sub-group

An existing MRA groups as well as any associated sub-groups can be deleted from a system, for example if an MRA is to be replaced or upgraded.

Note: 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.

Note: 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** which displays a list of the 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** which opens a confirmation message.
4. Click **OK** to complete the procedure.

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 in either a wireless or wireline mode. The CMP system is used to manage all MRA functions. Before this can occur, the CMP operating mode, (Wireless or Wireline), must support managing MRA clusters.

Follow these steps to configure the CMP to the appropriate operating mode so that it can manage MRA devices:

⚠ CAUTION

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.

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. On the bottom of the page, select **Manage MRAs**.
4. Click **OK** which closes the browser page and logs you 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 MRA Protocol Options

MRA must be configured to work with protocols and capabilities, such as Subscriber Indexing, APN override, Diameter, S9, RADIUS, and others capabilities to function in your network.

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 that requires protocol configuration.
   The **MRA Administration** page opens.
3. Select the **MRA** tab that displays the configuration options.
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 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 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 configure an alternate subscriber indexing by IP address, Username, NAI, E.164 (MSISDN) and IMSI for a specific access point name (APN). **1.** In the **Overrides by APN** section, click **Add**. **2.** Enter the APN name. **Note:** APN names are alphanumeric and have the following restrictions: • A 255 character limit • No spaces or special characters such as asterisks • Can contain hyphens (-) and periods (.) but must not begin or end with a hyphen or period Example name: **`pdn1.examplecorp.com`** **3.** Select one or more of the following: • **Index by IPv4** • **Index by IP-Domain-Id** • **Index by IPv6** • **Index by Username** • **Index by NAI** • **Index by E.164 (MSISDN)**

Attribute	Description
	- **Index by IMSI** - **Index by Session ID** 4. click **Save** You can create APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.
Protocol Timer Profile	The timer profile to use.
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; after the primary connection is back up, communication reverts back to it.

About Modifying, Grouping, or Deleting MRA devices

After an Multi-Protocol Routing Agent (MRA) has been created you can change the system settings, group the MRA devices, or delete an MRA device from the Configuration Management Platform (CMP).

Defining an MRA Cluster Profile

In order to get accurate session analysis, log, error, and reporting information, you must define certain parameters of an MRA device to give a specific 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 box.

Enter up to 250 characters.

d) **Secure Connection**: Select to enable a secure HTTP connection (HTTPS) instead of a normal connection (HTTP).

Note: 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. 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

As your network changes, is reconfigured, or adds new capabilities, such Diameter and it's associated interfaces, you will have to modify your existing MRA to meet these needs.

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. Select the **MRA** cluster profile located in the content tree.
3. Select the **System** tab located in the **MRA Administration** page.
4. Click **Modify** which opens the **Modify System Settings** page.
5. Modify those system settings that need modification.
6. When you finish, click **Save**.

Removing an MRA Cluster Profile from an MRA Group

As your network system changes, say from an upgrade or addition of a new protocol, the profiles on your existing MRAs may become outdated. In such instances, you can remove an MRA profile from an existing MRA.

Note: 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. But removing an MRA cluster profile from the **ALL** group will delete it from all other groups in the system.

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

1. From the MRA section of the navigation pane, select **Configuration**.
2. Select the MRA group which displays the contents of MRA group.
3. Remove the MRA cluster profile using one of the following methods:
   - Select **All** from the navigation pane. From the **MRA Administration** page, click the **Remove** icon (scissors), located to the right of the MRA cluster profile you want to remove.
   - From the content tree, select the MRA cluster profile which displays the **MRA Administration** page. On the **System** tab, click **Remove**.

The MRA cluster profile is removed from the group.

Reversing Georedundant Cluster Preference

If your system has been configured for georedundancy (**Manage Geo-Redundant MPE/MRA/BoD/MDFMDF** mode is enabled), there can be situations when you need to change the preference of the servers in a cluster to be active or spare.

To reverse a georedundant cluster preference:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.
   The **Cluster Configuration** page opens.
3. Click **View** for the cluster you want to modify.
   The **Topology Configuration** page opens, displaying information about the cluster.
4. Click **Modify Cluster Settings**.
5. In the **Cluster Settings** section of the page:
   - To set the preference to reverse (where the active Site 1 becomes the inactive site and Site 2 becomes the active site), toggle to **Reverse**.
   - To set the preference to normal (where the active Site 2 becomes the inactive site and Site 1 becomes the active site), toggle to **Normal**.
6. Click **Save**.

The cluster preferences are reversed.

Changing Server Status to Forced Standby

You can change the status of a server in a cluster to forced standby. A server placed into forced standby status cannot become active. You would do this, for example, to an active server prior to performing maintenance on it.

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

- 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 set all servers in a cluster into forced standby status, you can trigger a site outage.

To change a server to forced standby status:

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

3. Click **View** for the cluster you want to change.
   The **Topology Configuration** page opens, displaying information about the cluster.
4. Click **Modify Server-A** or **Modify Server-B** (whichever server needs the status change).
5. Select **Forced Standby**.
6. Click **Save**.

The server status is changed to forced standby.

Setting Up a Non-CMP Cluster

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

- The servers have been configured with network time protocol (NTP), domain name server (DNS), IP Routing, and OAM IP addresses.

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens; the initial group is **All Clusters**.
2. From the work area, select **Add MPE/MRA/Mediation Cluster**.

   Note: The list of available cluster types to add to the topology depends on the CMP modes configured.

   The **Topology Configuration** page opens.
3. In the **Cluster Settings** section of the page:
   a) (Required) Enter the **Name** for the cluster.
      Enter up to 250 characters, excluding quotation marks (") and commas (,).
   b) Select the **Appl Type** from the list.
      Available options are:

      - **MRA**
      - **Mediation**

      Note: The list of available application types depends on the CMP modes configured.

   c) Select the **HW Type** from the list.
      Available options are:

      - **C-Class** (default) – HP ProLiant BL460 Gen6/Gen8 server
      - **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 Gen6/Gen8
      - **NETRA** – Oracle Server X5-2 or Oracle Netra Server X5-2
      - **RMS** (rack-mounted server) – HP ProLiant DL360 Gen6 or HP ProLiant DL380 Gen8/Gen9 server
      - **VM** (virtual machine)
      - **VM(Automated)** (VM managed by NF Agent)

        See *Setting Up a VM (Automated) Non-CMP Cluster* for details on adding a VM (Automated) cluster.

   d) If needed, repeat the process for the second OAM VIP.

e) (Optional) To enter up to foursix **Signaling VIPs** addresses (up to two each for each of SIG-A, SIG-B, and SIG-C), click **Add New VIP**.

   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, SIG-B, or SIG-C for carriers who use redundant signaling channels.

   The **New Signaling VIP** dialog appears.

   1. Enter the **Signaling VIP** address and the **Mask**.

      This is the IP address the CMP server uses to communicate with an external signaling network.

      Note: Enter the IPv4 address in standard dot format and its subnet mask in CIDR notation from 0 to 32, or the IPv6 address in standard 8-part colon-separated hexadecimal string format and its subnet mask in CIDR notation from 0 to128.

   2. Select the **Interface** from the list.

      Available options are:

      - **SIG-A**
      - **SIG-B**
      - **SIG-C**

   3. Click **Save**.

      The **Signaling VIP** address and **Mask** are saved.

f) Repeat the process for any remaining Signaling VIPs.

g) If the hardware type is **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**, configure the **General Network** settings:

   1. Enter the **OAM VLAN ID**.

      The default value is **3**.

   2. Enter the **SIG-A VLAN ID**.

      The default value is **5**.

   3. (Optional) Enter the **SIG-B VLAN ID**.

      The default value is **6**.

   4. (Optional) Enter the **SIG-C VLAN ID**.

      The default value is **7**.

   Virtual LAN (VLAN) IDs are in the range of 1–4095.

h) If the hardware type is **C-Class** or **C-Class(Segregated Traffic)**, for the **User Defined Network**, enter the **REP VLAN ID**.

   Virtual LAN (VLAN) IDs are in the range of 1–4095.

4. To configure Server-A hardware, in the **Server-A** section of the page:

a) (Required) To enter the **IP** address, click **Add New IP**.

   The **Add New IP** dialog box appears.

1. Enter the **IP** address in either IPv4 or IPv6 format.

   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.

2. Select the **IP Preference**.

   Either **IPv4** or **IPV6**. If **IPv6** is selected, the server will preferentially use the IPv6 address for communication.

   Note: If neither an IPv6 OAM IP nor a static IP address is defined, **IPv6** cannot be selected. If neither an IPv4 OAM IP nor a static IP address is defined, **IPv4** cannot be selected.

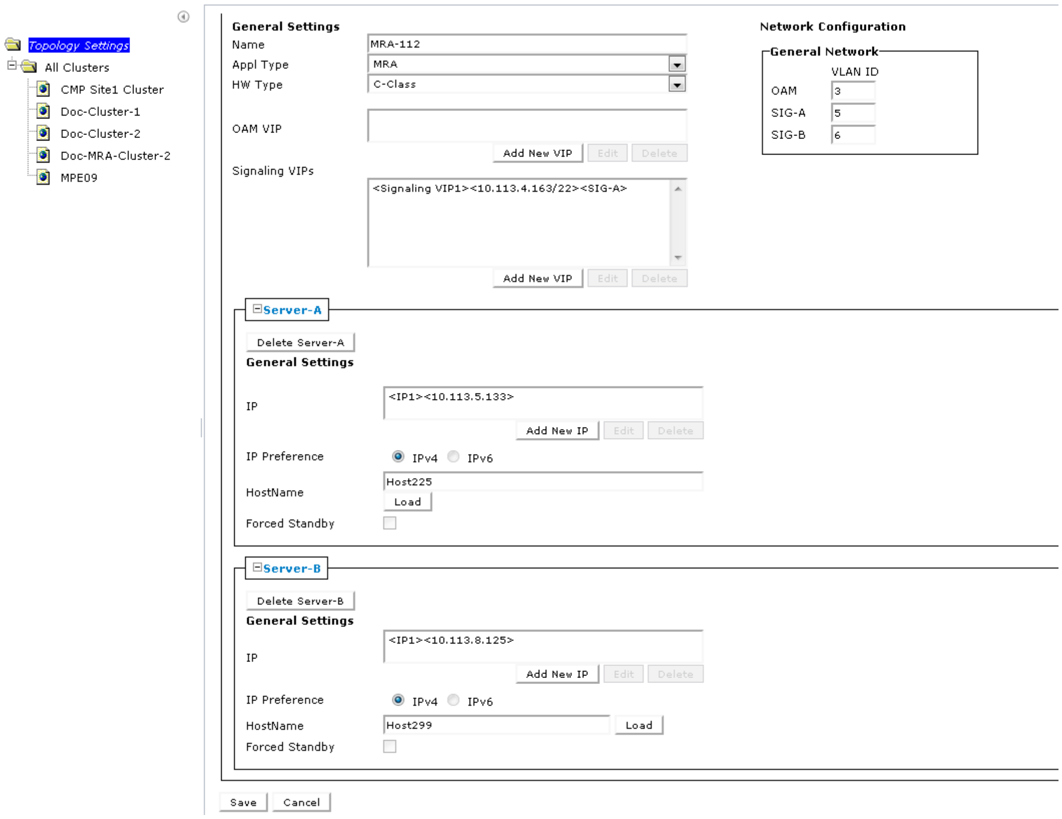
b) Enter the **HostName** of the server.
This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

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.

c) Select **Forced Standby** to put Server-A into forced standby status.
By default, Server-A will be the initial active server of the cluster.

5. (Optional) Click **Add Server-B** and enter the information for the standby server of the cluster.
   Server-B is defined for the cluster.
6. Click **Save**.
   A confirmation message appears.
7. Click **OK**.

Figure 4: Sample 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.



General Settings

Name: MRA-112

Appl Type: MRA

HW Type: C-Class

OAM VIP:

Signaling VIPs: <Signaling VIP1><10.113.4.163/22><SIG-A>

Network Configuration

General Network

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

Server-A

General Settings

IP: <IP1><10.113.5.133>

IP Preference: ● IPv4 ○ IPv6

HostName: Host225

Forced Standby: □

Server-B

General Settings

IP: <IP1><10.113.8.125>

IP Preference: ● IPv4 ○ IPv6

HostName: Host299

Forced Standby: □

Figure 4: Sample Cluster Topology Configuration

Setting Up a Georedundant Non-CMP Cluster

Note: Georedundancy requires the system to be configured with **Manage Geo-Redundant MPE/MRA/BoD/MDFMDF** enabled.

Before defining a cluster, ensure the following conditions are met:

- 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.

A georedundant non-CMP cluster is one of the following server types:

- MRA
- Mediation server

Note: The list of available server types depends on the CMP modes configured.

Note: If your system is not set up for georedundancy, see *Setting Up a Non-CMP Cluster*.

To setup a georedundant non-CMP cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens; the initial group is **All Clusters**.
2. From the work area, select **Add MPE/MRA/Mediation Cluster**.
   The **Topology Configuration** page opens.

3. In the **Cluster Settings** section of the page:
   a) (Required) Enter the **Name** for the site.

   Enter up to 35 alphanumeric characters; underscores (_) and hyphens (-) are allowed.

   b) Select an **Appl Type**.

   The available options are:

   - **MPE** (default)
   - **MRA**
   - **Mediation**

   Note: The list of available cluster types to add to the topology depends on the CMP modes configured.

   c) Select the **Site Preference**.

   Available options are **Normal** (default) or **Reverse**.

   d) Select the **Replication Stream Count**.

   This is 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.

   e) Select a **Replication & Heartbeat** network to carry inter-site replication and heartbeat traffic.

   This field only is visible if the system supports georedundancy:

   - **None** (default)
   - **OAM**
   - **SIG-A**
   - **SIG-B**
   - **SIG-C**
   - **REP**

   Note: When saving a configuration using **SIG-C**, a confirmation appears. Click **OK**. The **RMS** option for **HW Type** is removed until all configured Signaling C VIPs or **SIG-C** interfaces in static IP are removed.

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

   f) Select a **Backup Heartbeat** network to carry inter-site backup heartbeat traffic.

   Note: When saving a configuration using **SIG-C**, a confirmation message appears. Click **OK**. The **RMS** option for **HW Type** is removed until all configured Signaling C VIPs or **SIG-C** interfaces in static IP are removed.

   Note: This field only is visible if the system supports georedundancy.

   Available options are:

   - **None** (default)
   - **OAM**
   - **SIG-A**
   - **SIG-B**
   - **SIG-C**
   - **REP**

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

4. In the **Primary Site Settings** section of the page:

a) Select the **Site Name** from the list.

Select **Unspecified** (default) or the **Name** of a previously defined site. You can assign multiple clusters to the same site.

Note: If you select **Unspecified**, you create a non-georedundant site and cannot add a secondary site.

b) To import the **HW Type** and **VLAN ID** settings from the from the selected site, select **Use Site Configuration**.

When **Use Site Configuration** is selected, the **HW Type** and **VLAN ID** settings become read only.

To edit the fields, uncheck the **Use Site Configuration**.

Note: If **Unspecified** is selected for the site name, the **Use Site Configuration** option becomes unavailable.

c) Select the **HW Type** from the list.

Available options are:

- **C-Class** (default) – HP ProLiant BL460 Gen6/Gen8 server
- **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 G6/G8
- **NETRA** – or Oracle Netra Server X5-2 or Oracle Server X5-2
- **RMS** (rack-mounted server) – HP ProLiant DL360 Gen6/Gen8 or HP ProLiant DL380 Gen6/Gen8 server
- **VM** (virtual machine)
- **VM(Automated)** (VM managed by NF Agent)

See *Setting Up a VM (Automated) Non-CMP Cluster* for details on adding a VM (Automated) cluster.

d) (Required) To enter up to two **OAM VIP** (one IPv4 and one IPv6) addresses, click **Add New VIP**.

The **New OAM VIP** dialog box appears.

1. Enter the **OAM VIP** address and the **Mask**.

This is the IP address the CMP server uses to communicate with a Policy Management cluster.

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

2. Click **Save**

The **OAM VIP** address and **Mask** are saved. Repeat the process for the second OAM VIP.

e) (Optional) To enter up to foursix **Signaling VIPs** addresses (up to two each for each of SIG-A, SIG-B,and SIG-C), click **Add New VIP**.

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.

The **New Signaling VIP** dialog box appears.

1. Enter the **Signaling VIP** address and the **Mask**.

   This is the IP address the CMP server uses to communicate with an external signaling network.

   Note: Enter the IPv4 address in standard dot format and its subnet mask in CIDR notation from 0 to 32, or the IPv6 address in standard 8-part colon-separated hexadecimal string format and its subnet mask in CIDR notation from 0 to128.

2. Select the **Interface** from the list.

   Available options are:

   - **SIG-A**
   - **SIG-B**
   - **SIG-C**

3. Click **Save**.

   The **Signaling VIP** address and **Mask** are saved.

f) If the hardware type is **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**, configure the **General Network** settings:

1. Enter the **OAM VLAN ID**.

   The default value is **3**.

2. Enter the **SIG-A VLAN ID**.

   The default value is **5**.

3. (Optional) Enter the **SIG-B VLAN ID**.

   The default value is **6**.

4. (Optional) Enter the **SIG-C VLAN ID**.

   The default value is **7**.

Note: Virtual LAN (VLAN) IDs are in the range of 1–4095.

g) If the hardware type is **C-Class** or **C-Class(Segregated Traffic)**, for the **User Defined Network**, enter the **REP VLAN ID**.

Note: Virtual LAN (VLAN) IDs are in the range of 1–4095.

5. To configure Server-A, in the **Server-A** section of the page:

a) (Required) To enter the **IP** address, click **Add New IP**.

The **Add New IP** dialog box appears.

1. Enter the **IP** address in either IPv4 or IPv6 format.

This is 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.

2. Select the **IP Preference**: **IPv4** or **IPV6**.

   The server will preferentially use the IP address in the specified format for communication.

   - If neither an IPv6 OAM IP nor a static IP address is defined, **IPv6** cannot be selected.
   - If neither an IPv4 OAM IP nor a static IP address is defined, **IPv4** cannot be selected.

b) Enter the **HostName** 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.

c) Select **Forced Standby** to put Server-A into forced standby.

By default, Server-A will be the initial active server of the cluster.

d) In the **Path Configuration section**, to add a **Static IP**, click **Add New**.

The **New Path** dialog box appears.

Note: If an alternate replication path and secondary HA heartbeat path is used, a server **Static IP** address must be entered in this field.

1. Enter a **Static IP** address and **Mask**.
2. Select the **Interface**:

   - **SIG-A**
   - **SIG-B**
   - **SIG-C**
   - **REP**
   - **BKUP**

   Note: If the hardware type is **C-Class (Segregated Traffic)** or **NETRA**, the **BKUP** network is available.

6. (Optional) To configure Server-B, in the **Server-B** section of the page:

a) (Required) To enter the **IP** address, click **Add New IP**.

The **Add New IP** dialog box appears.

1. Enter the **IP** address in either IPv4 or IPv6 format.

   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.

2. Select the **IP Preference**: **IPv4** or **IPV6**.

   The server will preferentially use the IP address of the specified format for communication.

   - If neither an IPv6 OAM IP nor a static IP address is defined, **IPv6** cannot be selected.
   - If neither an IPv4 OAM IP nor a static IP address is defined, **IPv4** cannot be selected.

b) Enter the **HostName** of the server.

   This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

   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.

c) Select **Forced Standby** to put Server-B into forced standby.

   By default, Server-A will be the initial active server of the cluster.

d) In the **Path Configuration section**, to add a **Static IP**, click **Add New**.

   The **New Path** dialog box appears.

   Note: If an alternate replication path and secondary HA heartbeat path is used, a server **Static IP** address must be entered in this field.

   1. Enter a **Static IP** address and **Mask**.
   2. Select the **Interface**:

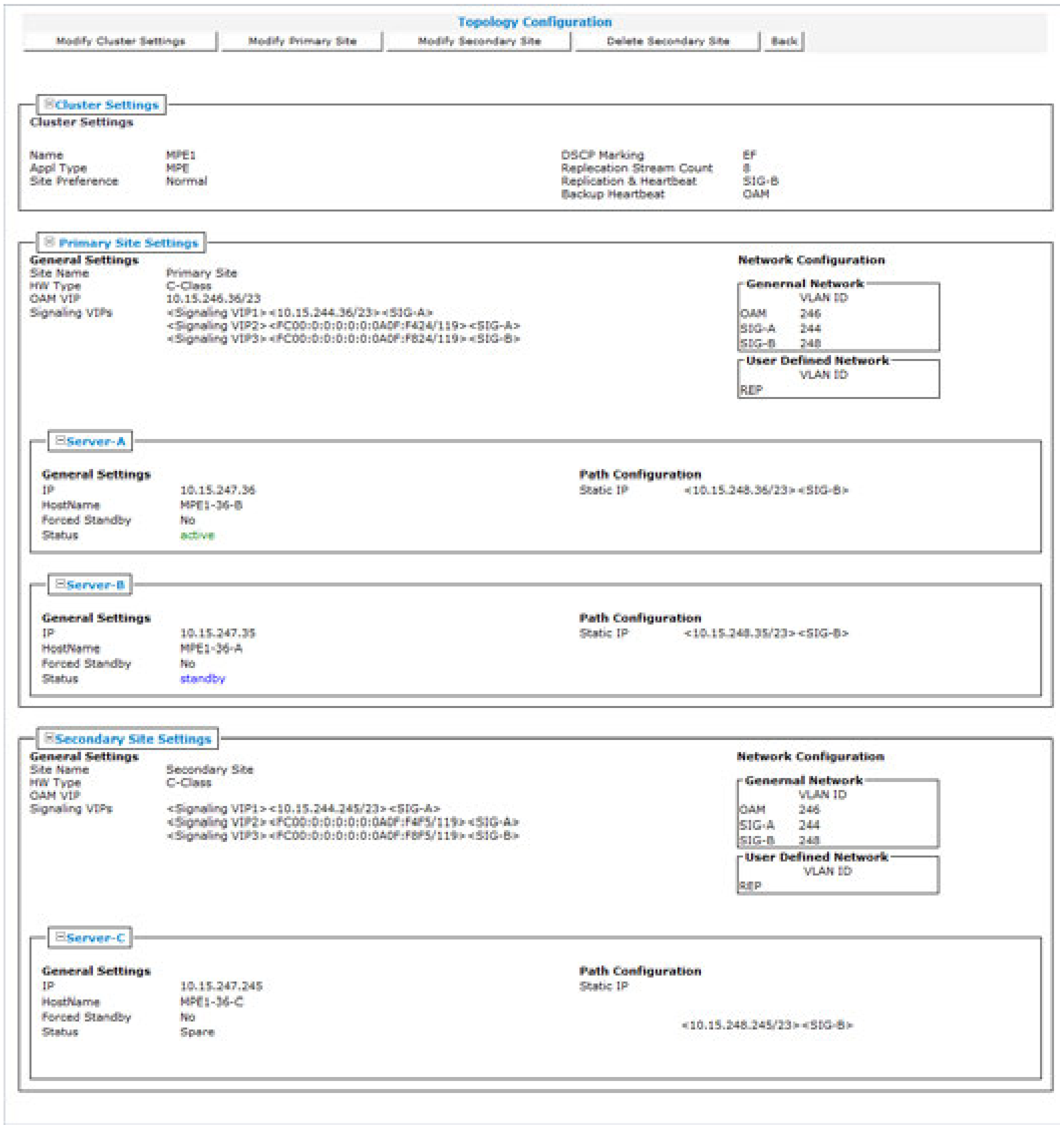
      - **SIG-A**
      - **SIG-B**
      - **SIG-C**
      - **REP**
      - **BKUP**

      Note: If the hardware type is **C-Class (Segregated Traffic)** or **NETRA**, the **BKUP** network is available.

7. Click **Save**.
   A confirmation message appears.
8. Click **OK**.
9. If you are setting up multiple clusters, repeat this procedure.

The cluster is defined.

Figure 5: Sample MPE Cluster Site 1 & 2 Configuration show the configuration for a georedundant (two-site) MPE cluster, using SIG-B for a replication network and OAM for the backup heartbeat network.



Cluster Settings

Name	MPE1	DSCP Marking	EF
Appl Type	MPE	Replecation Stream Count	8
Site Preference	Normal	Replication & Heartbeat	SIG-B
		Backup Heartbeat	OAM

Primary Site Settings

General Settings

Site Name	Primary Site
HW Type	C-Class
OAM VIP	10.15.246.36/23
Signaling VIPs	<Signaling VIP1><10.15.244.36/23><SIG-A> <Signaling VIP2><FC00:0:0:0:0:0:0A0F:F424/119><SIG-A> <Signaling VIP3><FC00:0:0:0:0:0:0A0F:F824/119><SIG-B>

Network Configuration

Genernal Network

	VLAN ID
OAM	246
SIG-A	244
SIG-B	248

User Defined Network

	VLAN ID
REP	

Server-A

General Settings

IP	10.15.247.36
HostName	MPE1-36-B
Forced Standby	No
Status	active

Path Configuration

Static IP <10.15.248.36/23><SIG-B>

Server-B

General Settings

IP	10.15.247.35
HostName	MPE1-36-A
Forced Standby	No
Status	standby

Path Configuration

Static IP <10.15.248.35/23><SIG-B>

Secondary Site Settings

General Settings

Site Name	Secondary Site
HW Type	C-Class
OAM VIP	
Signaling VIPs	<Signaling VIP1><10.15.244.245/23><SIG-A> <Signaling VIP2><FC00:0:0:0:0:0:0A0F:F4F5/119><SIG-A> <Signaling VIP3><FC00:0:0:0:0:0:0A0F:F8F5/119><SIG-B>

Network Configuration

Genermal Network

	VLAN ID
OAM	246
SIG-A	244
SIG-B	248

User Defined Network

	VLAN ID
REP	

Server-C

General Settings

IP	10.15.247.245
HostName	MPE1-36-C
Forced Standby	No
Status	Spare

Path Configuration

Static IP

<10.15.248.245/23><SIG-B>

Figure 5: Sample MPE Cluster Site 1 & 2 Configuration

Setting Up a VM (Automated) Non-CMP Cluster

Before defining a VM (Automated) non-CMP cluster, ensure the system is configured for virtualization and VIM Connections are defined.

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens; the initial group is **All Clusters**.
2. From the work area, select **Add MPE/MRA/Mediation Cluster**.

   Note: The list of available cluster types to add to the topology depends on the CMP modes configured.

   The **Topology Configuration** page opens.
3. In the **Cluster Settings** section of the page:

a) (Required) Enter the **Name** for the cluster.

   Enter up to 250 characters, excluding quotation marks (") and commas (,).

b) Select the **Appl Type** from the list.

   Available options are:

   - **MRA**
   - **Mediation**

   Note: The list of available application types depends on the CMP modes configured.

c) Select **VM(Automated)** from the **HW Type** list.

d) If needed, repeat the process for the second OAM VIP.

e) (Optional) To enter up to foursix **Signaling VIPs** addresses (up to two each for each of SIG-A, SIG-B, and SIG-C), click **Add New VIP**.

   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, SIG-B, or SIG-C for carriers who use redundant signaling channels.

   The **New Signaling VIP** dialog box appears.

   1. Enter the **Signaling VIP** address and the **Mask**.

      This is the IP address the CMP server uses to communicate with an external signaling network.

      Note: Enter the IPv4 address in standard dot format and its subnet mask in CIDR notation from 0 to 32, or the IPv6 address in standard 8-part colon-separated hexadecimal string format and its subnet mask in CIDR notation from 0 to128.

   2. Select the **Interface** from the list.

      Available options are:

      - **SIG-A**
      - **SIG-B**
      - **SIG-C**

   3. Click **Save**.

      The **Signaling VIP** address and **Mask** are saved.

f) Repeat the process for any remaining Signaling VIPs.

4. To configure Server-A using **VM(Automated)**, in the **Server-A** section of the page:

   a) Select the **VIM Connection** from the list.

      See *Creating a VIM Connection* for details.

   b) Enter the **Instance Name**.

      This is the same as a server name and allows reference to this particular device.

   c) Select the **Image** from the list.

      Refers to the software needed for creating the virtual machine.

   d) Select the **Flavor** from the list.

      Determines whether an MPE or MRA instance is created. This VM profile specifies the vCPU, RAM, vNIC, storage and location for the instance.

e) Select the **Availability Zone** from the list.
f) Select **Yes** to **Config Drive** (default value).
g) Enter the IP address for the **NTP Server**.
h) Click **Add New** to enter the IP address for the **DNS Server**.
i) Click **Add New** to enter the IP address for the **DNS Search**.
j) Click **Manage** to add or remove **Security Groups**.
k) Click **Add New IP** to add an **IP** address.

   This is a fixed IP address for the VM device.
l) Select the **IP Preference** as either **IPv4** or **IPv6**.
m) Enter the **HostName**.
n) Select to have the server in **Forced Standby**.
o) Click **Add New** to add a new **Static IP** address.

5. (Optional) Click **Add Server-B** and enter the information for the standby server of the cluster.
   Server-B is defined for the cluster.
6. Click **Save**.
   A confirmation message appears.
7. Click **OK**.

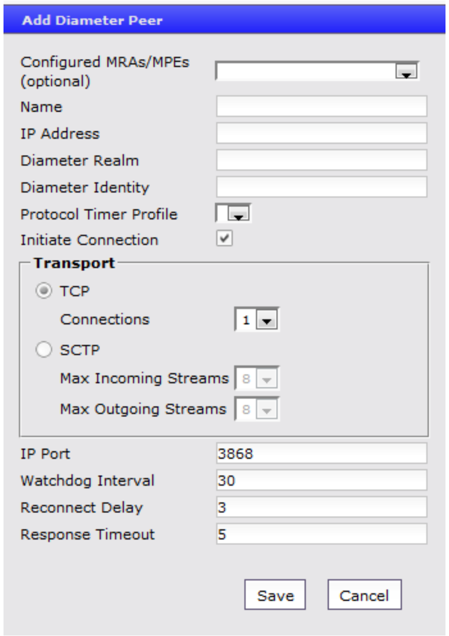
Configuring Diameter Peers

The MPE and MRAdevices support Diameter Rx, Gq, Ty, Gxx, Gx, 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 the 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.

Use this procedure if you need to configure system devices (peers) to a diameter-based network.

To configure Diameter peers for either an MPE or MRA device:

1. Either in 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** which opens the **Modify the Diameter Peer Table**.
5. Add a peer to the table using these steps.
   a) Click **Add**.
      The **Add Diameter Peer** window opens.



Add Diameter Peer

Configured MRAs/MPEs (optional)	
Name	
IP Address	
Diameter Realm	
Diameter Identity	
Protocol Timer Profile	
Initiate Connection	☑

Transport

● TCP

Connections	1

○ SCTP

Max Incoming Streams	8
Max Outgoing Streams	8

IP Port	3868
Watchdog Interval	30
Reconnect Delay	3
Response Timeout	5

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, **`Example.com`**).
- **Diameter Identity** (required) — Fully qualified domain name (FQDN) of the peer device (for example, **`mpe33.Example.com`**).
- **Protocol Timer Profie** — Select from the list.
- **Initiate Connection** — Select to initiate an S9 connection for this Diameter peer.
- **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 6 seconds.

  Note: If objects created prior release 12.1 have been imported, the interval for those objects remains at 30.

- **Reconnect Delay** — Enter the response time in seconds. The default is 3 seconds.
- **Response Timeout** — Enter the response timeout interval is seconds. The default is 5 seconds.

c) Click **Save**.

6. Complete these steps to 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. 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. 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. Click **Save**.

Creating a VIM Connection

To create a VIM connection:

1. From the **Platform Setting** section of the navigation pane, select **NF Management**.
   The **NF Management** page opens; the initial group is **NF Management**.
2. From the content tree, select the **NF Management** group.
   The **NF Management** page opens.
3. Click **Create VIM Connection**.
   The **Create VIM Connection** page opens.
4. Enter a **Name** for the VIM connection.
5. Enter a **Description** for the VIM connection.
6. Select the **VIM Type** from the list.

   Available options include:
   - OpenStack — Indicates the connection will use the OpenStack API
   - OpenStack HEAT — Indicates the connection will use the OpenStack HEAT API
7. Enter the **Host** name.
8. Enter the **Port** number.

   The default port number is 5000.
9. Select to use a **Secure Connection**.
   If enabled, the connection will use an HTTPS connection to encrypt the password.
10. Enter the **Username**

11. Enter the **Tenant** name.
12. Enter the **Password**.
13. Select **Show Password** to view the password in clear text.
14. Click **Save**.

The CMP server saves the VIM connection to the database.

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 options for the following privileges:

- Configuration:
- Bulk Operation:
- Configuration Template:

Each privilege has three options:

- **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).

Use this procedure if you need to create new role and configure the privileges for a role for MRA devices.

To configure a new role for an MRA device user:

1. In the **System Administration** section of the navigation pane, select **User Management** and then select **Roles**.
   The **Role Administration** page opens.
2. Click **Create Role**.
3. Enter the following information:
   a) **Name**:
   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.
4. When you finish, click **Save**.
   Privileges are assigned to the role.

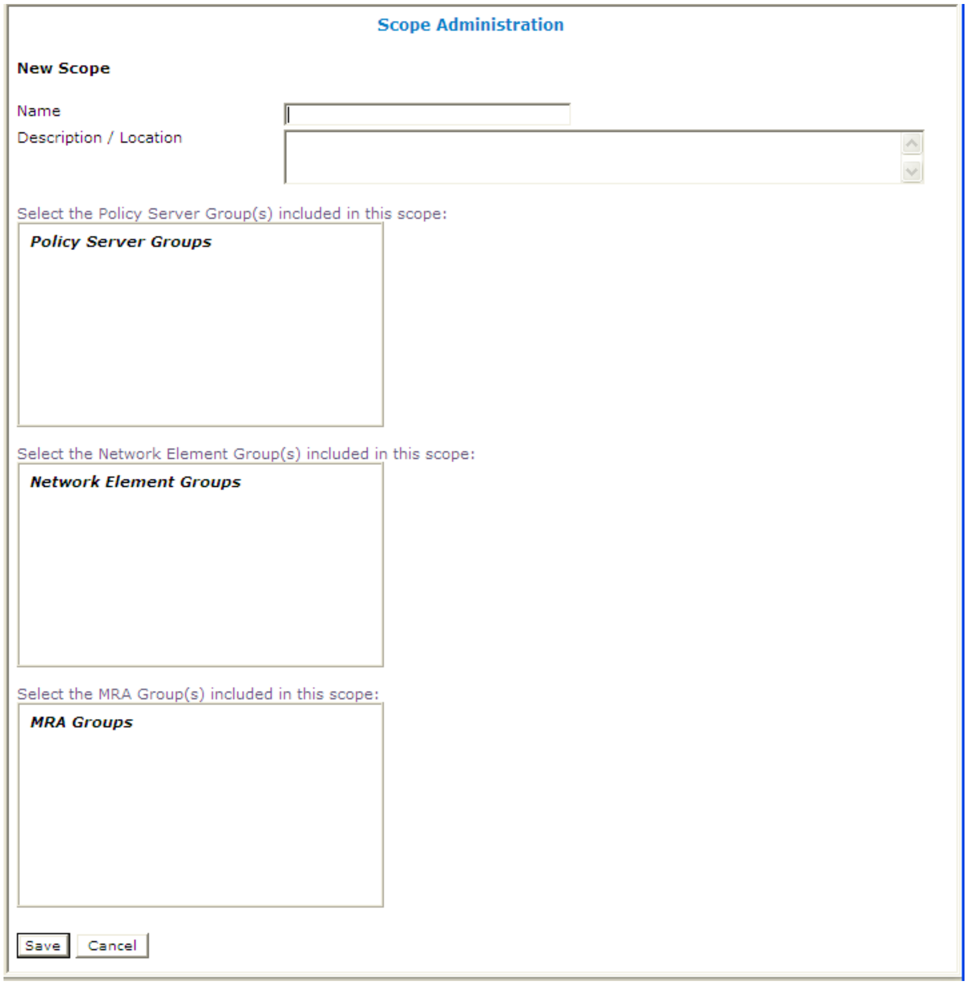
Configuring the Scope for an MRA

MRA configuration provides scope functionality which allows the administrator to configure scopes for MRA groups, that provides the context for a role. The default scope of **Global** contains all items defined within the CMP. After 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.

Use this procedure to define the scope for a user that manages MRA devices.

To configure a scope for a user managing an MRA:

1. In the **System Administration** section of the navigation pane, select **User Management** and then select **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:

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

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

Figure 7: 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. Click **Save**.

The scope is defined.

About 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.

Use this procedure to remove stale or suspect bindings on an MRA.

To configure an MRA to clean up sessions:

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 device that needs duplicate bindings and/or sessions removed.
   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.

5. When you finish, click **Save**.
   The settings are applied to the MRA.

Configuring SigC in Devices Exposed to PCEF

An MRAs capacity to use SigC in VLAN 3 enables that MRA to utilize internal signaling communication between an MPE and and itself. SigC configuration is used when an MRA's hardware is selected as either C-Class, or C-Class (Segregated Traffic), NETRA, or VMWare.

Note: To configure a device for SigC, the MRA topology must be configured for either C-Class, or C-Class (Segregated Traffic), NETRA, or VMWare. See *Setting Up a Non-CMP Cluster*

Use this procedure to set up an appropriately configured MRA to utilize SigC in VLAN 3.

To set the configuration key for SigC in VLAN 3:

1. From the MRA section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups.
2. From the content tree, select an MRA device.
   The **MRA Administration** page opens.
3. From the **MRA Administration** page, select the **MRA** tab.
   The current MRA configuration settings are displayed.
4. Click **Advanced**.
5. Click **Add** in the **Other Advanced Configuration Settings** section.

   Note: You can also **Clone, Edit, Delete** existing configuration key records, as well as scroll up and down the list.

6. In the **Add Configuration Key Value** screen enter the following information:
   - Enter **DIAMETERDRA.SIGDeviceFilter**in the Configuration Key field.
   - Enter either **SIGA** or **SIGB** in the Value field.
   - Enter **Comments** (or leave blank) for this configuration in the Change Log field.
7. When you finish, click **Save**.

About 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 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. When all traffic has been removed or redirected, existing traffic is released from the MRA and it is shut down. After the MRA is replaced or upgraded, the same process can be used on the other MRA, and then returned to the cluster.

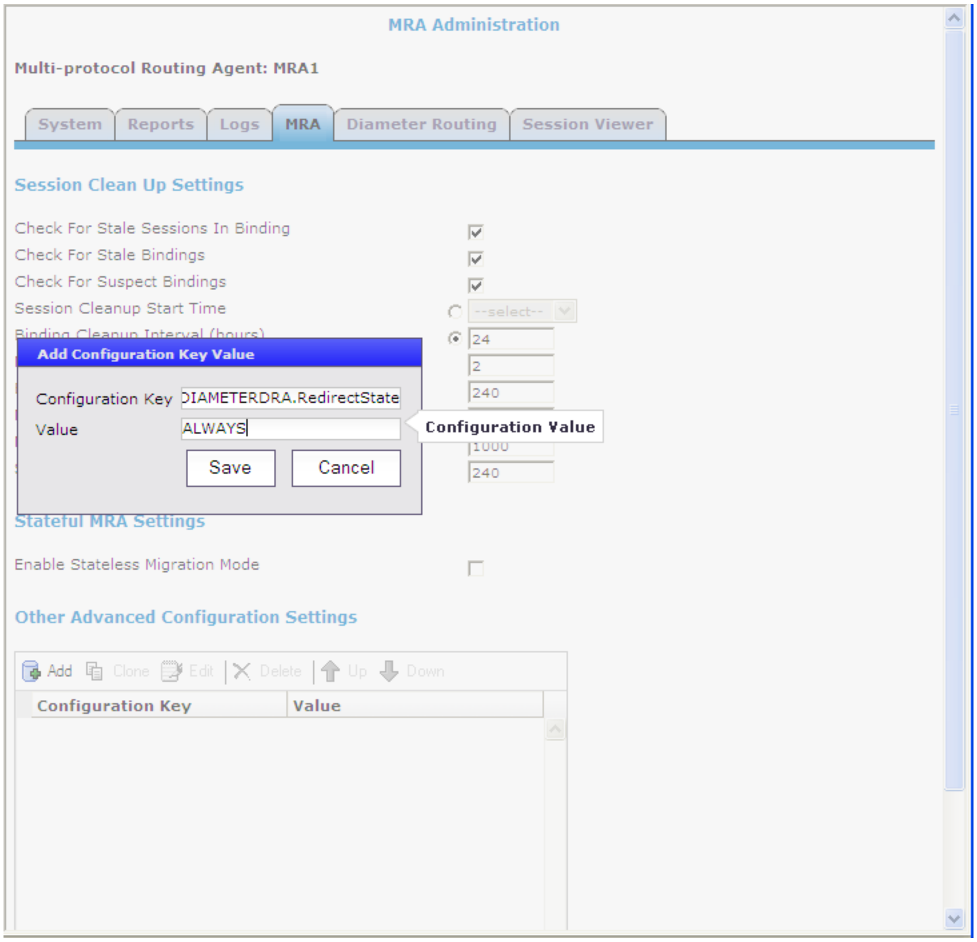
Note: For detailed directions on performing a migration using the redirect states, please contact Oracle.

Changing Redirect States

Use this procedure to redirect states when you need to perform a software upgrade on an MRA or remove an MRA.

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** screen opens (*Figure 8: Add Configuration Key Value Window*).



MRA Administration

Multi-protocol Routing Agent: MRA1

Session Clean Up Settings

Check For Stale Sessions In Binding ☑

Check For Stale Bindings ☑

Check For Suspect Bindings ☑

Session Cleanup Start Time ○ --select--

Binding Cleanup Interval (hours) ● 24

2

240

1000

240

Add Configuration Key Value

Configuration Key DIAMETERDRA.RedirectState

Value ALWAYS

Stateful MRA Settings

Enable Stateless Migration Mode □

Other Advanced Configuration Settings

Configuration Key	Value

Figure 8: 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 when the binding no longer has any associated sessions, the session 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**.

Determining a Mapping MRA (M-MRA)

The DRADRMA.MultiSiteOptimization configuration determines the algorithm used to distribute binding indexes across MRAs in a system. The default value is N-Site v1. To disable this functionality, the configuration needs to be set to Legacy.

Managing Configuration and Virtual Templates

Configuration and Virtual Templates provide a more efficient means of normalizing common configurations between multiple MPE or MRA instances. Any given device can be associated with no template, one, or many templates. In addition, users can add, remove, clone, and prioritize 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 devices with another template.

About Configuring Templates

Because an MPE or an MRA device exist independently of one another, you can create both virtual and configuration templates in two locations in the CMP interface. You can create templates either in the **MRA** or the **Policy Server** section of the navigation pane.

After a template is created, the template has the functionality that is specific to that instance (that is, either MPE or MRA instance). After templates are created and associated with a device, the templates can be viewed and managed from the **System** tab of the MPE or MRA device.

Note: MPE Pools cannot be configured in an MRA device.

Creating a Configuration Template

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

Note: MPE Pools cannot be configured in an MRA device.

Note: You must create a configuration template before creating a virtual template because a virtual template references, and is dependent on, a configuration template.

Use this procedure if you want to make a template that you will use many times.

To create a configuration template:

1. From the **MRA** section of the navigation pane, select **Configuration Template**.
   The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates.**
2. From the content tree, select **Configuration Templates**.
   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) To use an existing template as a base for the new template, select an existing template from the **Copy From** list.
6. (Optional) Enter a **Description / Location**.

   The text box is limited to 255 characters.

7. Click **Save**.

The new template appears in the list in the content pane.

After creating the template, proceed with configuring the template.

Modifying a Configuration Template

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

Use this procedure if you need to modify an existing template to comply with new requirements or conditions.

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 Templates** and **Configuration Templates.**
2. From the content tree, select the **Configuration Template** for modification.

The **Configuration Template Administration** page opens with the template configuration settings.

3. Select the tab that contains the information you want to configure or modify and click **Modify**.
4. For an MRA device, edit the information:
   - **MRA** tab – **Modify** button:
     - **Associations** – See *Associating Network Elements with an MRA Device* for details.
     - **MPE Pools** – See *Configuring Diameter Realm Based Peer Routes* for details.

       Note: MPE Pools cannot be configured or modified in an MRA template.
     - **Subscriber Indexing** – See *Configuring MRA Protocol Options* for details.
     - **Diameter** settings – See *Associating Network Elements with an MRA Device* for details.
     - **S9**
     - **Radius Configuration**
   - **MRA** tab –**Advanced** button:
     - **Expert Settings**
     - **Service Overrides**
     - **Load Shedding Configuration**
   - **Diameter Routing** tab
     - **Diameter Peers** – See *Loading MPE/MRA Configuration Data when Adding Diameter Peer* for details.
     - **Diameter Routes** – See *Configuring Diameter Realm Based Peer Routes* for details.
5. Click **Save**.

The configuration template is modified. The modified template is applied to all associated MRA or MPE devices.

Changing the Template Priority

You would reorder templates in a list 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 is listed in the **Associated Templates** section of the **Modify System Settings** screen.

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

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of **All Policy Servers** or **MRA** devices.
2. From the content tree, select the device.
   The Administration page opens with the device configuration.
3. Select the **System** tab.
   The device's system configuration settings display on the page.
4. Click **Modify**.
   The administration page becomes enabled for editing.
5. In the **Associated Templates** section, edit the **Priority** value to change the number to a higher or lower value.
6. Click **Update Order**.

The priority order of the **Associated Templates** is changed.

Creating a Virtual Template

Because an MPE or an MRA device can exist independently of one another, you can create both virtual and configuration templates in two locations in the CMP interface. Depending on your needs, the CMP interface enables you to create templates either in the **MRA** or the **Policy Server** 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 template is created, the template has the functionality that is specific to that instance (that is, either MPE or MRA). After templates are created and associated, the templates can be viewed and managed from the **System** tab of the MPE or MRA device.

Note: You must create a configuration template before creating a virtual template because a virtual template references, and is dependent on, a configuration template.

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

Use this procedure if you have virtual template capability.

To create a virtual 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 Templates** and **Configuration Templates.**
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** list.
6. (Optional) Enter a **Description**.
7. Click **Save**.

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

About Overlaps

Overlaps occur when both a template and an MPE or an MRA server 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 MPE or MRA server. The result is that when the template and MPE or MRA server are associated, the index of the user name becomes an overlapped field. When an overlap occurs, a prompt appears stating, `The server configuration has overlaps with the associated template(s).` You 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.

Associating Templates with a Device

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

You would use this procedure if you had a number of devices that required the same instance.

To associate templates with an MPE or MRA device:

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of server groups; the initial group is **ALL**.
2. From the content tree, select the device.
   The administration page opens in the work area.
3. Select the **System** tab.
4. Click **Modify**.
   The administration page becomes editable.
5. In the Associated Templates section, click **Add**.
   The **Add Associated Templates** dialog appears.
6. Select one or more templates from the list and click **Add**.
   The Associated Templates list updates to include the selected templates.
7. To order the **Priority** of the associated templates, change the values for each listed template.

   Note: Lower numbered templates have higher priority than higher numbered templates. This means that settings configured with a lower value priority template can override the settings of a higher value priority template.

8. Click **Save**.

The specified templates' configurations are applied to the specified device.

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.

Use this procedure when you want to improve internal security by hiding internal IP addresses and domain names in a Diameter-enabled network.

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. From 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 8: 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.

Configuring Topology Hiding for the Rx Application

When topology hiding is enabled, Rx AAR, ASR, STR, RAR, AAA, ASA, STA and RAA 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 Rx AAR-U, STR 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.

Complete these steps 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.
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 8: Add Configuration Key Value Window*).

   Note: Rx can only be indexed by the session id when hiding is enabled. As a result, when in the topology hiding mode, the index session id will always be enabled. All relative information in Binding Information can be queried.

   Add the following configuration keys to the **Add Configuration Key Value** window:

   Table 5: Topology Hiding Configuration Keys

Configuration Key	Value
DIAMETERDRA.TopologyHiding.Apps	**Gx, Rx**
DIAMETERDRA.TopologyHiding.Enabled	**true**

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

Chapter 4

About Network Elements, Backups, and Diameter Settings

Topics:

The Multi-Protocol Routing Agent, (**MRA** tab), on the **MRA Configuration** page displays a list of:

- Network elements associated with the MRA device
- Associated MPE pool
- Configuration settings for the MRA device
- Diameter-related configuration information
- Load shedding configuration

Note: This document assumes that all CMP systems as well as MRA, and MPE devices are operational and available. 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*.

Note: If any MRA, or MPE devices are unavailable during backup MRA implementation the Remote Diversion function does not work and the error message `DIAMETER_TOO_BUSY` message occurs. See *Policy Management Troubleshooting Reference* for more information.

Adding and Configuring Associated MRA devices

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 a 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.

Use this procedure if you are setting up protection from server failure in a georedundant system.

To configure an associated MRA device:

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 Verson 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 that reverts the MRA devices back to the previous release.
7. From the **Members** section, click **Add**.
   The **Add MRA Association Member** screen opens.
8. From the **Add MRA Association Member** screen, perform the following steps:
   a) Select an MRA device from the list of existing MRA devices.
   After the MRA has been selected, the **Default Primary IP Address** for that MRA is visible in the field.
   b) (Optional) If the Association is to be georedundant, select a **Default Secondary IP Address**. This is the IP Address other MRA devices 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 a Subscriber Profile Repository*.
   e) Select either **TCP or SCTP** for transport protocol.

If other MRA devices 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 MRA Protocol Options*.)

- **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.

a) Type in the name of the **APN** (255 character limit, no spaces or special characters).

Note: APN names are alphanumeric and have the following restrictions:

- A 255 character limit
- No spaces or special characters such as asterisks
- Can contain hyphens (-) and periods (.) but must not begin or end with a hyphen or period

Example name: pdn1.examplecorp.com

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.

Managing Client Mapping for an MRA Association

Configure the **Client Mapping** option when using Policy Connection Director (PCD) Associations.

Note: You can only configure client mapping after an association has been created. After the association has been created, select the association that will have client mapping, and click **Modify**. See*About PCD Associations*.

Note: Only those MRAs which are part of that MRA are shown in the primary and secondary MRA lists.

Once a client mapping is created, it can be modified, deleted, or cloned by selecting that client mapping record and clicking on the appropriate choice (edit, clone, delete).

To configure client mapping for an MRA Association:

1. In the **Client Mapping** section, click **Add**.
2. Select the **Network Element**.
3. Select the **Primary MRA**.
4. Select the **Secondary MRA**.
5. Click **Save**.

The MRA clusters are configured as associated MRA devices.

Configuring Protocol Options on an Associated MRA Device

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 6: 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.

Attribute	Description
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 configure an alternate subscriber indexing by IP address, Username, NAI, E.164 (MSISDN) and IMSI for a specific access point name (APN). 1. In the **Overrides by APN** section, click **Add**. **Note:** APN names are alphanumeric and have the following restrictions: • A 255 character limit • No spaces or special characters such as asterisks • Can contain hyphens (-) and periods (.) but must not begin or end with a hyphen or period Example name: pdn1.examplecorp.com 2. Enable **Index by IPv4**, **Index by IPv6**, or both. 3. click **Save** You can create APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.

Modifying Backup and Associated MRA devices

After you define the backup and associated MRA devices, the devices 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.

Note: If any MRA, or MPE devices are unavailable during backup MRA implementation, the Remote Diversion function does not work and the error message `DIAMETER_TOO_BUSY` message occurs. See *Policy Management Troubleshooting Reference* for more information.

Use these procedures as the requirements or the configuration of your georedundant system change.

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 the MRA association. 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.

Click **Save**.

MRA Association Status Definitions

The **Status** column of an MRA device 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 device is not currently running any migration or sync tasks. If all MRA devices are in this state, a new MRA device can safely be added to the Association.
- **Syncing (xx%)** - This status means the MRA device is currently running the sync task. If any MRA devices are in this state, a new MRA device cannot be safely added to the Association. If a new MRA device is added, data integrity cannot be guaranteed across the association. The percentage completion through the task will be displayed in parentheses.
- **Migrating (xx%)** - This status means the MRA device is currently running the legacy migration task. If any MRA devices are in this state, a new MRA device 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 device did not complete successfully. This likely means there were some connection failures between MRA devices 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 device did not complete successfully. This likely means there were some connection failures between MRA devices 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 device completed successfully. The MRA device is still running in a special migration mode, however. Use the **Complete Migration** operation to turn off migration mode on the MRA device and start using the n-site MRA device 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 MRA devices 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 MRA devices in the Association.
- **Cancel Migration** - To cancel a migration which is currently in progress.
- **Accept Migration** - To accept the migration (after all MRA devices have finished running the migration task).

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

- **Reset Counters** - Reset all counters for all MRA devices in the association.

- **Reapply Configuration** - Reapply configuration for all MRA devices in the association.

Note: If at least one MRA device 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 do not 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 MRA devices in the association show **Migrated** or **Failed Migration** status, only Accept Migration operation is available.
- If at least one MRA devices in the association shows**Migrating** status, only the Cancel operation is available.
- If at least one MRA devices in the association shows**Syncing** status, only the Cancel Sync operation is available.
- If any of the MRA devices in the association show **Syncing** or **Failed Sync** status, then only the Manual Migration operation is available.
- If any of the MRA devices 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 is available for selection.

Use this procedure when you need to add new or upgraded MRA to your Diameter-enabled system and then associate a network element (for example PCEF) to that MRA.

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 available network elements.

   For example:

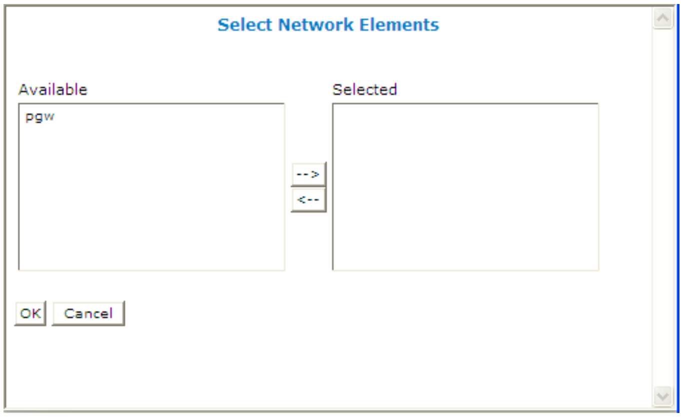


Figure 9: Select Network Elements

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.

Creating a Network Element

You must create a network element for each device associated with any of the MPE devices within the network. To create 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. Click **Create Network Element**.
   The **New Network Element** page opens.
3. Enter information for the network element:
   a) (Required) **Name** — The name you assign to the network element.

      Enter up to 250 alphanumeric characters. The name can include underscores (_), hyphens (-), colons (:), and periods (.)

   b) (Required) **Host Name/IP Address** — 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 primary address for the network element fails.
   d) **Description/Location** — Free-form text.

      Enter up to 250 characters.

   e) (Required) **Type** — Select the type of network element.

      The supported types are:

      - **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

- **HSGW** — HRPD Serving Gateway
- **PGW** — Packet Data Network Gateway
- **SGW** — Serving Gateway
- **AF** — Application Function
- **DRA** — Diameter Routing Agent
- **DPI** — Deep Packet Inspection device
- **NAS** — Network Access Server device

Note: For more information on managing network elements, see *Policy Configuration Management Platform Wireless User's Guide*.

f) **Protocol Timer Profile** — The timer profile that sets timeout values for messages in applications/interfaces.

See *Managing the Protocol Timer Profiles* for more information.

g) **Capability** — This field is valid for some network element types.

When present, it contains the following options:

- **TDF-Solicit** — DPI accepts Sd session establishment requests from the MPE device.
- **Time-Tariff** — PGW and DPI network element types support Time-Tariff functionality.
- **Usage-Report-26** — GGSN, PGW, SGW, and DPI network element types are compatible with usage_report event trigger value 26.

h) **Capacity** — The bandwidth allocated to this network element.

4. In **Policy Servers associated with this Network Element**, select one or more policy servers (MPE devices) to associate with this network element.
5. In **MRAs associated with this Network Element**, select one or more Multi-Protocol Routing Agent (MRA devices) to associated with this network elements.
6. In **Network Element Groups which contain this Network Element**, select one or more groups (see *Adding a Network Element to a Network Element Group*).
7. Click **Save**.

You have created the definition for a network element and the network element is listed on the **Network Element Administration** page.

Note: After saving the new network element, the CMP server automatically discovers all associated subnets. The CMP supports automatically provisioning to the associated MPE-R and MPE-S devices.

Associating a DSR Network Element with an MRA

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.

If your system is using DSR for your Diameter routing, use this procedure to associate a DSR network element with an MRA device.

To associate a DSR network element with an MRA:

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

Network element groups exist in a distributed network to perform specific duties.

Use this procedure if you are creating a network element group to perform specific functions in your distributed network. After you create a network group, you can then create network elements to associate with devices such as an MPE or MRA.

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 and location of the network group.
6. Click **Save**.

You have created a network element group.

Adding a Network Element to a Network Element Group

After a network element group is created, you can add individual network elements to the group.

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.
   - If there are more than 25 network elements defined, the page does not display any elements. 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.

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

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

5. Click **Save**.

The network element is added to the selected group, and a message indicates the change.

Managing the Protocol Timer Profiles

This chapter 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 PCD Associations

The Policy Connection Director (PCD) enables multiple MRA devices to handle connection-level routing as well as Diameter-level and binding-level routing. The PCD is not an independent entity; you configure an MRA device to have PCD functionality by creating a PCD association for one or more network elements associated with the MRA device.

Whenever a network element connects to an associated MRA device, the PCD establishes an MRA connection to the primary and secondary MRA devices that have a PCD association with the network element. In the event of a site failure, the PCD can reroute messages from the network element to the secondary MRA device at the connection level with minimal impact on processing.

The PCD enables individual MRA devices in a georedundant deployment to operate at greater capacity by reducing the processing impact of site-failover.

Creating PCD Associations for a Network Element

You can only configure a Policy Connection Director (PCD) association within an existing MRA association and for an existing network element. For information about creating an MRA association, see *Adding and Configuring Associated MRA devices*. For information about creating network elements, see *Creating a Network Element*.

To create a PCD association for a network element:

1. From the **MRA** section of the navigation pane, select **MRA Associations**.
   The content tree displays the **MRA Associations** group.
2. From the content tree, select the MRA association for which you want to create a PCD association. The **MRA Association Administration** page opens in the work area, displaying the details of the selected MRA association.
3. Click **Modify**.
   The **Configuration** page opens in the work area.
4. In the **Client Mapping** table, click **Add**.
   The **Add Client Mapping** window opens.
5. Add a client mapping by doing the following:
   a) From the **Network Element** list, select the network element for which you want to create a PCD association.
   b) From the **Primary MRA** list, select the MRA device that you want to handle connection-level routing for the network element. The selected MRA device must be part of the MRA association.
   c) From the **Secondary MRA** list, select the MRA device that is configured as a backup for the primary MRA device. The selected MRA device must be part of the MRA association and must be configured as a backup of the primary MRA device.

      Note: An MRA device cannot be selected as both a primary and secondary MRA device for a network element.

   d) Click **Save**.

   The client mapping is displayed in the **Client Mapping** table.
6. Click **Save**.

The PCD association to the MRA devices is created for the network element.

Modifying PCD Associations for a Network Element

To modify a Policy Connection Director (PCD) association for a network element:

1. From the **MRA** section of the navigation pane, select **MRA Associations**.
   The content tree displays the **MRA Associations** group.
2. From the content tree, select the MRA association for which you want to create a PCD association. The **MRA Association Administration** page opens in the work area, displaying the details of the selected MRA association.
3. Click **Modify**.
   The **Configuration** page opens in the work area.
4. In the **Client Mapping** table, select the PCD association you want to modify.
5. Click **Edit**.
   The **Edit Client Mapping** window opens.
6. Modify the client mapping information.

   For a description of the fields contained in this window, see *Creating PCD Associations for a Network Element*.

7. Click **Save**.

The PCD association to the MRA devices is modified for the network element.

Cloning PCD Associations for a Network Element

To clone a Policy Connection Director (PCD) association for a network element:

1. From the **MRA** section of the navigation pane, select **MRA Associations**.
   The content tree displays the **MRA Associations** group.
2. From the content tree, select the MRA association for which you want to create a PCD association.
   The **MRA Association Administration** page opens in the work area, displaying the details of the selected MRA association.
3. Click **Modify**.
   The **Configuration** page opens in the work area.
4. In the **Client Mapping** table, select the PCD association you want to clone.
5. Click **Clone**.
   The **Clone** window opens.
6. Select the **Network Element** for the Primary and Secondary MRAs.

   Note: The Network Element must be unique for each Primary and Secondary MRA pairing.

   For a description of the fields contained in this window, see *Creating PCD Associations for a Network Element*.
7. Click **Save**.

The PCD association to the MRA devices is modified for the network element.

Deleting PCD Associations for a Network Element

To delete a Policy Connection Director (PCD) association for a network element:

1. From the **MRA** section of the navigation pane, select **MRA Associations**.
   The content tree displays the **MRA Associations** group.
2. From the content tree, select the MRA association for which you want to delete a PCD association.
   The **MRA Association Administration** page opens in the work area, displaying the details of the selected MRA association.
3. Click **Modify**.
   The **Configuration** page opens in the work area.
4. In the **Client Mapping** table, select the PCD association you want to delete.
5. Click **Delete**.
   The **Delete Client Mapping** window opens.
6. Click **Delete**.
   The client mapping is no longer displayed in the **Client Mapping** table.
7. Click **Save**.

The PCD association to the MRA devices is deleted for the network element.

About Stateful Routing

Stateful routing enables a server, (MPE or MRA), to keep the information on each and every session as long as that session lasts. This type of routing enables you to control the information on a transaction. The trade off for this control is speed and space. Speed is compromised by how many transactions per second (tps) the server can handle in a given time interval and space is limited by the amount of RAM needed to control the number of sessions that can be in-progress at any given time. For example, a server running stateful routing can process 200K TPS is still limited in that all sessions have to stop when the RAM is full.

About Stateful MRAs

Stateful MRA devices let you view the session and track its destination prior to sending multiple sessions to the same MPE device. An MRA is placed into migration mode in order to render a stateful MRA.

Messages can be based on the destination-host or host-based routing. If no destination-host route is provided in a message and a host-based route is configured with a host identity, then the route will not be a match. The message will continue to be processed further by the other routes that have been configured in the **Diameter Route Table**. See *Configuring Diameter Host Based Peer Routes* for more information.

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.

Use this procedure if you have an extensive peer network or a network that includes multiple realms, user IDs or applications.

To configure the Diameter realm based peer routes:

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 display.
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 (Realm Based Route)** window opens.

   b) Configure the route using the following fields.

      - **Diameter Realm** — For example, `Example.com`.
      - **Application ID** — Select **Rx** (default), **Gq**, **Ty**, **Gx**, , **Gxx**, **Sd**, , **Sy**, **Gy**, **S9**, **Vzr**, 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 (,); use a period followed by an asterisk (.*) 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) 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. 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. 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) Click **Save**.
8. To delete the default route, click **Delete**.
9. Click **Save**.

The Diameter realm based peer routes are configured.

Examples of JAVA Regular Expressions for MRA Routes

The following sample regular expressions are 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)`

Configuring Diameter Host Based Peer Routes

Host based diameter routes are used in cases where messages are intended for a specific Destination-Host, (or a list of Destination-Hosts), and need to be routed to an intermediary peer because the Destination-Host cannot be reached directly.

Note: The routing table can be used with a stateful MRA by creating a route with an action of LOCAL. In order to use routes in tandem with a stateful MRA, a route with an action of LOCAL must be created.

Use this procedure if you have a very wide network where direction Destination-Host connections must be routed through an intermediary peer.

To configure the Diameter host based route table:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server/MRA groups.
2. From the content tree, select the **MRA** device.
   The **MRA Administration** page opens in the work area.
3. Select the **Diameter Routing** tab.
   The Diameter Routing configuration settings are displayed for that server or device.
4. Click **Modify Routes**.
   The **Modify the Diameter Route Table** page opens.
5. Add a route to the table:
   a) Click the **Add** button and select **Host Based Route**.

      the **Add Host Based Route** window opens.
   b) Configure the route using the following fields.

      - **Name** — The name for the Destination Host.
      - **Type** — This column lists whether the route is "realm-based" or "host-based."
      - **Host Identities** — This option enables you to manually type in any number of host identities.

        Note: The wildcards ***** (match any number of characters) and **?** (match only one character) can be used. This is a alphanumeric field with a 255 character limit.

      - (Optional) **Evaluate as a Regular Expression** — The check box allows the matching of route criteria using regular expression syntax, opposed to the previously supported matching wildcards. (See *Examples of JAVA Regular Expressions for MRA Routes* for examples of using JAVA Regular Expressions.)
      - **Add** — This adds the host identities to the field.

        Note: Clicking **Delete** deletes a selected host identity.

      - **Origin (Default "Any")** — Enables a message to be routed based on the message's Origin-Host. For example, if **MPE** is selected, then it is an MPE originated message (meaning that any messages that originated from any managed MPE are applied to this route).

        Note: If topology hiding is enabled, the message is processed based on the original Origin-Host in the routing table, since topology hiding processing takes place after the routing table.

- **Application ID** — Select **Rx** (default), **Gq**, **Ty**, **Gx**, **Gy**, **Gxx**,**Sh**, **Sd**, **Sy**, **S9**, **Vzr**, 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 (,); use an asterisk (*) 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**.
- **Action** — Select **PROXY** (stateful route, the 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) Clone, 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. 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. 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**)

   and peer server ID. When you finish, click **Save**.

8. To delete the default route, click **Delete**.

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

The Diameter routes are configured with the Realm/Host Identities column displaying the Realm or Host name for the configured route.

Associating an MRA with a Diameter MPE Peer

An MRA load shares sessions among MPEs listed in its pool.

Use this procedure to add an MPE to the pool of devices that the MRA shares the session load among them.

To associate an MRA device with an MPEand add it to the MPE pool:

1. From the **MRA** section of the navigation pane, select **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.
5. Enter the following information:
   a) **Associated MPE**: Select an MPE device.

      Note: If the desired MPE is managed by the same CMP, select the desired MPE from the drop-down box. All of the following fields will auto fill. An MPE device is selected from the list of MPEs managed by the CMP.

      Note: If the desired MPE is not managed by the same CMP, leave this drop-down box unselected and fill in the fields below.

   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, `Example.com`).
   f) **Diameter Identity**: Enter a fully qualified domain name (FQDN) or the peer device (for example, `MRA10-24.Example.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**, (for example, Example.com).
   b) **Diameter Identity**, (for example mra143-58.Example.com).
8. In the **S9** section select the following information:
   a) Select a **Primary agent**, (for example E_MPE-Example), from the **Primary DEA** list.

b) (Optional if this is a georedundant device) Select a **Secondary agent** from the **Secondary DEA** list.

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 Diameter Routing

The **Diameter Routing** feature enables an MRA to communicate to PCEF/AFs via multiple P-DRAs in active-standby or load-balancing mode, and re-route failed request to other available P-DRA.

Another function of diameter routing is to enable an MRA to support the PCEF directly connecting to it-self with multiple diameter connections. These direct-connect nodes are independent in general.

Note: The term independent means that there is no AS/LB mode that defines their relationship, but the relationship of AS/LB is still applicable in the diameter connection level in direct-connect network element.

For an MRA device to initiate a diameter request in load-balancing mode, the MRA device is responsible for the P-DRA selection that is based on load-balancing arithmetic. Ensuring robustness and reliability of the diameter signaling network, the MRA device needs to provide a best effort to select an alternate connection or node to rout messages when a message failure is detected. An MRA device is responsible for re-routing requests to an alternate P-DRA connection if these two transport failures are encountered:

- A diameter connection failure
- A diameter connection watchdog failure

In addition, an MRA device is also responsible for re-routing requests to an alternate P-DRA node if the following response failures are encountered:

- Certain types of error codes, that cannot be configured, are received in response messages
- A response timeout that can be configured

You can configure diameter routing using these four components:

- Endpoints
- Connections
- Peers
- Peer Groups

Diameter Routing: Creating a Endpoint

Endpoints contain all the remote and local peers and display their basic information such as Endpoint Type, Connection Type, Address and Port.

Note: Multiple IP address can be configured for an Endpoint.

Use this procedure if you need to create multiple IP addresses on a remote or local peer.

Complete these steps to add Endpoints:

1. From the **MRA** section of the navigation pane, select **Diameter Routing**.
2. From the **Diameter Routing** tree, select **Endpoints**.
3. Click **Create Endpoint** to open the **Configuration** screen.
4. Enter the following:
   - **Name —** Enter the name of the endpoint (which must be unique in the CMP database).
   - **Connection Protocol** -- Enter either **SCTP** or **TCP** depending on the type of node being used.
   - **Type** -- Select either **Local** or **Remote** depending on type of connection being used.

     Note: Both of the primary IP and the secondary IPs must be the sigA or sigB of the MRA defined in topology when the connection type is **Local** .

     Note: If **Local** is selected, then choose **Associated MRA**.
   - **Primary Site IP —** Enter the IP address, in IPv4 or IPv6 format, of the primary site.

     Note: An error prompt will notify you if the IP of local peer is invalid.
   - **Secondary Site IP** — For georedundant configurations, enter the IP address, in IPv4 or IPv6 format, of the server at the secondary site.

     Note: An error prompt will notify you if the IP of local peer is invalid.

     Note: The secondary IP will be hidden if the connection Type is TCP.
   - **Port —** Enter the port number (integer, for example 6000).
   - **Description —** (Optional) Enter a description of the Endpoint.
5. When you finish, click **Save**.

Diameter Routing: Creating Connections

Connections provide routing lists to all MRAs in the system.

If you have multiple MRAs, use this procedure to use connections to create routing lists for your MRA through creating

Complete these steps to add a Connection:

1. From the **MRA** section of the navigation pane, select **Diameter Routing**.
2. From the **Diameter Routing** tree, select **Connections**.
3. Click **Create Connection** to open the **Configuration** screen.
4. Enter the following information:
   - **Name —** Enter the name of the connection (which must be unique in the CMP database).

- **Connection Protocol** -- Enter either **SCTP** or **TCP** depending on the type of connection being created.
- **Client Peer —** Enter the name of either the local or remote **Endpoint** that will be used.
- **Server Peer —** Enter the name of either the local or remote **Endpoint** that will be used.
- **Description —** (Optional) Enter a description of the Connection.

5. When you finish, click **Save** to save the changes and send the information to all the MRAs in the system.

Diameter Routing: Creating Peers

A Peer defines the relationship between several connections.

Create Peers to define your connections to your MRA devices.

Complete these steps to create a Peer.

1. From the navigation pane, select the **MRA Configuration**
2. From the content tree, select the **MRA** that needs diameter peers.
3. From the **MRA Administration** screen, select the **Diameter Routing** tab.
4. From the **Diameter Routing** tree, select **Peer**.
5. Click **Modify Peers** to open the **Modify the Diameter Peer Table**.
6. Click **Add** to open the **Add Diameter Peer** window.
7. Enter or select the following parameters:
   a) (Optional) Select an MPE device.

      Note: Or leave blank if you are using an external MPE device.

   b) Enter the **Name**.
   c) Select a **Primary Site IP** address.
   d) (If configuring for georedundancy) Select a **Secondary Site IP** address.
   e) Enter a **Diameter Realm** .
   f) Enter a **Diameter Identity** .
   g) Select a **Protocol Timer Profile** .
   h) Select a **Transport protocol** (TCP or SCTP).
   i) Enter a **IP Port**, **Watchdog Interval**, **Reconnect Delay**, and **Response Timeout** (or accept the defaults).
   j) Enter
8. Click **Save**.

Diameter Routing: Creating Peer Groups

A Peer Group defines a complete routing rule by specifying the relationship between several connection groups.

If you need to define routing rules between several connection groups, use this procedure.

Complete these steps to add a Peer Group:

1. From the **MRA** section of the navigation pane, select **Diameter Routing**.

2. From the **Diameter Routing** tree, select **Peer Groups**.
3. Click **Create Peer Group** to open the **Configuration** screen.
4. Enter the **Name**
   When you finish, click **Save**.
5. (Optional) Enter the **Description / Location** for the Peer Group.
6. Select the **Peer Group Mode**.
   - Do not select a **Peer Group Mode** if the selected mode groups are independent of each other.
   - Select either **Active Standby** or **Load Balancing** depending on what is needed in the routing scenario.
7. Select the **Connect Type**
   - Select **DSR** if only one peer group is to be used.

     Note: Only one peer group can be created if the connection type is DRA.
   - Select **Direct Link** if one or more Peer Groups are to be used.
8. Select if the Peer Group is **Enabled**. Enable a Peer Group if Direct Link is the connection type.
9. Select the **Peers** to be used.

   Note: If DSR connection type is used, only one Peer can be selected.
10. Click **Save** to save changes.

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.

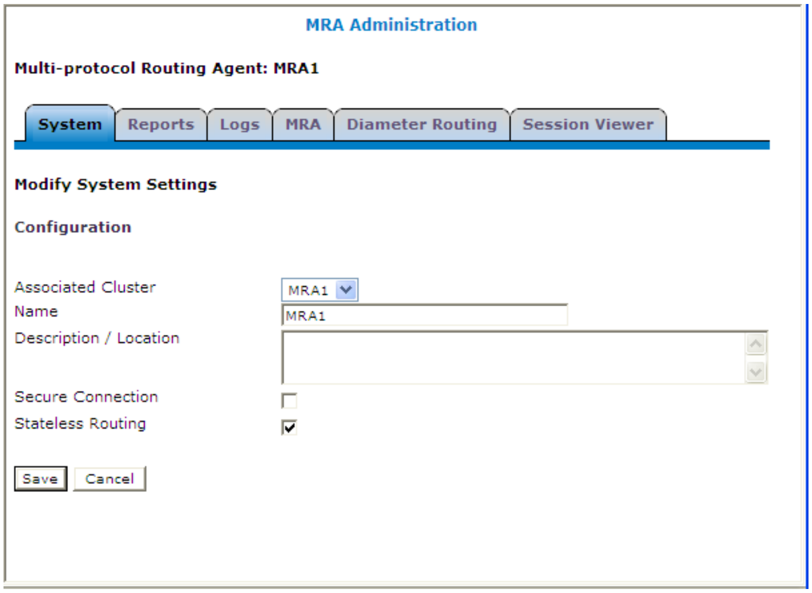
Enabling Stateless Routing

Use this procedure to be able to manage more sessions within a time period.

To enable a stateful MRA device to run as statelessly:

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 10: Enabling Stateless Routing* shows an example).

The stateful MRA configuration is hidden.



Multi-protocol Routing Agent: MRA1

Modify System Settings

Configuration

Associated Cluster: MRA1
Name: MRA1
Description / Location:
Secure Connection: □
Stateless Routing: ☑

Figure 10: 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.

Use this procedure when you want to use static routes in your transition to stateless migration

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, select a peer from the list on the **Diameter Routing** tab. After the peer is selected, the peer configuration fields are automatically populated.

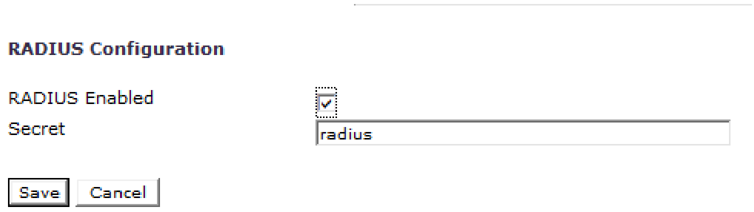
Configuring for RADIUS

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

Use this procedure if the both the MPE and MRA are to be configured for RADIUS instead of Diameter.

To configure an existing MRA for RADIUS:

1. From the **MRA** section of the navigation pane, select **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: radius

Figure 11: RADIUS Configuration Section

- Select **RADIUS Enabled**.
- **Secret**: Enter name of the **Default Passphrase**.

6. Click **Save** when you have completed the steps.

About Load Shedding Overload Control for Diameter

Load shedding is used to reduce latency and to keep an MRA device stable and reliable in overload situations. When enabled, certain requests are rejected by an MRA device when it becomes too heavily loaded to process them. You can access Load Shedding Configuration controls from the MRA and MPE Advanced Configuration pages where you can configure rules for rejecting messages during overload conditions. Multiple congestion levels are defined which can be configured to accept, reject or drop selected messages at each level.

An MRA attempts to successfully process a message whenever possible in one of the following ways:

- Local Diversion -- Selects a new MPE device in the MPE pool to handle a new connection for a subscriber who is bound to a busyMPE device.
- Remote Diversion -- Selects an MRA device to handle a new connection for a subscriber who is bound to a busy MPE device. That MRA device creates a binding for the subscriber pointing to one of the MPE devices in the MPE pool.

Note: If any MRA, or MPE devices are unavailable during backup MRA implementation the Remote Diversion function does not work and the error message `DIAMETER_TOO_BUSY` message occurs. See *Policy Management Troubleshooting Reference* for more information.

Both MPE and MRA devices handle message overload by utilizing congestion (busyness) levels. An MRA device utilizes two congestion levels (Level 1 and 2) while an MPE device utilizes four congestion levels (Levels 1-4). At each level you can create rules to match the message types that are received. In addition, you can configure a "default action" that is taken if none of the rules configured for the level match a message. For example, for Level 1, the default Level Action is Accept, which means to bypass load shedding rules. (For more information on actions, see step 8 in *Configuring Load Shedding for an MRA Device*.)

Note: When Local or Remote Diversion is not possible, the default result code is DIAMETER_TOO_BUSY. The NO_CAPACITY result code indicates an MRA device has a binding, but the MPE device it points to is currently overloaded, and the MRA device cannot perform local diversion to handle the request. The default result code is configurable.

An MRA device proactively rejects all messages destined for an overloaded MPE at all congestion levels. For example, if an MPE is configured to reject CCR-U messages at Level 2, the MRA device rejects the CCR-U message with DIAMETER_UNABLE_TO_COMPLY instead of forwarding it to an MPE device.

An MRA device subscribes to its pool of MPE devices for load notifications by issuing an LSR message after connection is established. It also subscribes to MPE devices in the backup MRA pool and to all other MRA devices in its association. MRA devices communicate their status using Load Notification (LNR) messages that include a Diversion-Status AVP to indicate whether that MRA device is available.

The Diversion-Status AVP indicates whether an MRA is available for diverting traffic to its MPE devices (Remote Diversion). The diversion status is set to DIVERTABLE if none of the MPE devices in an MPE pool are overloaded. The status is set to NOT_DIVERTABLE if at least one MPE device in the MPE pool is overloaded.

When you configure the admission rules for an MRA device to reject messages on behalf of an overloaded MPE device, there can still be times when the MPE device responds to a message with DIAMETER_TOO_BUSY. In these cases, before forwarding the answer message, the MRA device runs the original request through the MPE admission rules and updates the result code in the message with the result code found in the rules.

MRA Default Load Shedding Rules

You can configure load shedding rules to determine how an MRA device reacts to a processing backlog. (Refer to *Configuring Load Shedding for an MRA Device*.) This state is called "busyness." Levels of busyness can be configured to accept, reject, or drop select messages at each level. An MRA has two busyness levels. At any level of busyness, request that have been queued longer than a configurable time are silently discarded without further processing, since the originator would have already given up on that request.

On the MRA **MRA Advanced Configuration** page, there is a default Level Action for each busyness level. The default level action is **Accept** for Level 1, which means to process the message by bypassing load shedding instead of rejecting it. (The other actions are **Drop** which means to drop the message and do not process it.**Answer With** or **Answer With Code**, which means select an appropriate code to answer the message or manually enter the code to answer the message. The last action **Vendor ID** means to manually enter a specific ID for answering the message.

Level actions are configurable. The *Table 7: MRA Busyness Level 1 Rules* and *Table 8: MRA Busyness Level 2 Rules* tables show the default load-shedding rules for an MRA device.

The default action for Level 1 is Accept.

Table 7: MRA Busyness Level 1 Rules

Rule Name	Actions
DefaultRule1	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule2	Reject Gxx CCR messages with DIAMETER_TOO_BUSY

The default action for Level 4 is Drop, which applies to all messages other than the Drma messages that are accepted by default.

Note: The DRMA rule configuration is only displayed when the Diameter-based protocol is in use.

Table 8: MRA Busyness Level 2 Rules

Rule Name	Actions
DefaultRule3	Accept Drma LNR with ACCEPT
DefaultRule4	Accept Drma LNR with ACCEPT
DefaultRule5	Accept Drma LNR with ACCEPT

Configuring Load Shedding for an MRA Device

Use this procedure to enable or disable load shedding on the specified MRA device. Load shedding can help reduce or prevent congestion at theMPE. It could cause the MRA to go into congestion. If the MRA goes into congestion before any MPE does, turning off load shedding could reduce or even solve the problem.

Note: You can also configure an MPE device from an MRA device that controls that device. (See Step 9.)

To configure load shedding for an MRA:

1. From the MRA section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA device groups; the initial group is **ALL**.
2. From the content tree, select the **MRA** that needs load shedding capabilities.
   The **MRA Administration** page opens.
3. Select the **MRA** tab.
   The current MRA device configuration settings are displayed.
4. Click **Advanced**.
   The **Advanced MRA Settings** page opens.
5. Click **Modify**.
   The advanced configuration settings can be edited.
6. In the **MRA Load Shedding Configuration** section of the page, select the enabled state.

   - **true** (default)—Enables load shedding.
   - **false**—Disables load shedding.
   - **undefined**— The value for this field is taken from the associated Configuration Template. If there is not a configuration template associated, then the default value is used.

   See *MRA Default Load Shedding Rules* for more information on load shedding rules.
7. (Optional) Set the **Level Action** for a busyness level.
   a) Click the **right arrow** to expand the level.
   b) Select one of the following **default Level Actions**:

      - **Drop** all messages.
      - **Answer With** appropriate code from the drop-down list.
      - **Answer With Code** enter the appropriate `code` and `Vendor ID`.
8. Add a **rule(s)** for the busyness level.
   a) Click **Add**.
   b) Select the **Catagory**.
   c) Enter the **Values** for the load shedding rule(s) for the appropriate busyness level(s):

      - (Required) The **Name**— Name of the rule.
      - In the **Filter** section select:
        - **Application** — The application the rules apply to. You can select: **Sd, Gx, Gxx, or Rx**.
        - **Message** — The type of message the rule applies to (which depends on the application chosen).
      - Select the **Request Type** (available only when the CCR message type is selected) — Initial, Update, Terminate.
      - Enter a **APNs** — `CSV` list of one or more access point names that the massage must contain.
      - In the **Action** section select the action to be taken if the criteria are met for the load-shedding rule.
9. Repeat steps 6 -8 to add rules In the **MPE Load Shedding Configuration** section.

   Note: MPEs can use all four busyness levels.

See the *CMP Wireless User's Guide* for more information.

10. Click **Save**.

The specified Load Shedding setting is saved for this MRA device. When load shedding is enabled, if the busy threshold is exceeded, an alarm is generated to notify you that the MRA is in a busy state. When either the clear threshold or the busy time limit is met, another alarm is generated to notify you that the MRA is processing requests.

Cloning Load Shedding Rules

After a load shedding rule is created, it can be cloned, modified or deleted. In addition, rules can be re-ordered in order to meet different needs.

Cloning load shedding rules enables you to use the same rule multiple times without having to create it over again.

To clone a load shedding rule:

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 that needs load shedding capabilities.
   The **MRA Administration** page opens.
3. From the **MRA Administration** page, select the **MRA** tab.
   The current MRA configuration settings are displayed.
4. Click **Advanced**.
   The **Advanced MRA Settings** page opens.
5. Click **Modify**.
6. Select the section (**MRA Load Shedding Configuration** or **MPE Load Shedding Configuration**) and select the rule to be cloned.
7. Click the **Clone** button on the toolbar.
8. Add a new **Name** for the rule.
9. Select an **Action**.
10. Click **OK** to save the changes.
    The new rule appears in the list above the rule that was cloned.

Modifying Load Shedding Rules

After a load shedding rule is created, it can be cloned, modified or deleted. In addition, rules can be re-ordered in order to meet different needs.

Use this procedure if a load shedding rule needs to be modified.

To modify a load shedding rule:

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 that needs load shedding capabilities.
   The **MRA Administration** page opens.
3. From the **MRA Administration** page, select the **MRA** tab.
   The current MRA configuration settings are displayed.

4. Click **Advanced**.
   The **Advanced MRA Settings** page opens.
5. Click **Modify**.
6. Select the section (**MRA Load Shedding Configuration** or **MPE Load Shedding Configuration** and select the rule to be modified.
7. Click the **Edit** button on the toolbar.
8. Make the appropriate changes.
9. Click **OK** to save the changes.
   The rule is modified.

Re-ordering Load Shedding Rules

After creating a load shedding rule, you can be clone, modify or delete rules. In addition, you can re-order rules to meet different your needs.

Re-ordering load shedding rules puts a different priority on them, so if you need to shift priorities in your load shedding rules, use this procedure.

Complete these steps to change the order of load shedding rules.

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 that needs load shedding capabilities.
   The **MRA Administration** page opens.
3. From the **MRA Administration** page, select the **MRA** tab.
   The current MRA configuration settings are displayed.
4. Click **Advanced**.
   The **Advanced MRA Settings** page opens.
5. Click **Modify**.
6. Select the section (**MRA Load Shedding Configuration** or **MPE Load Shedding Configuration**) that needs to be changed.
7. Select the **rule** to be re-ordered in the list.
8. Click the **Up** or **Down** arrows on the toolbar to place the rule in the desired position in the list.

MRA Default Load Shedding Rules

You can configure load shedding rules to determine how an MRA device reacts to a processing backlog. (Refer to *Configuring Load Shedding for an MRA Device*.) This state is called “busyness.” Levels of busyness can be configured to accept, reject, or drop select messages at each level. An MRA has two busyness levels. At any level of busyness, request that have been queued longer than a configurable time are silently discarded without further processing, since the originator would have already given up on that request.

On the MRA **MRA Advanced Configuration** page, there is a default Level Action for each busyness level. The default level action is **Accept** for Level 1, which means to process the message by bypassing load shedding instead of rejecting it. (The other actions are **Drop** which means to drop the message and do not process it.**Answer With** or **Answer With Code**, which means select an appropriate code to answer the message or manually enter the code to answer the message. The last action **Vendor ID** means to manually enter a specific ID for answering the message.

Level actions are configurable. The *Table 9: MRA Busyness Level 1 Rules* and *Table 10: MRA Busyness Level 2 Rules* tables show the default load-shedding rules for an MRA device.

The default action for Level 1 is Accept.

Table 9: MRA Busyness Level 1 Rules

Rule Name	Actions
DefaultRule1	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule2	Reject Gxx CCR messages with DIAMETER_TOO_BUSY

The default action for Level 4 is Drop, which applies to all messages other than the Drma messages that are accepted by default.

Note: The DRMA rule configuration is only displayed when the Diameter-based protocol is in use.

Table 10: MRA Busyness Level 2 Rules

Rule Name	Actions
DefaultRule3	Accept Drma LNR with ACCEPT
DefaultRule4	Accept Drma LNR with ACCEPT
DefaultRule5	Accept Drma LNR with ACCEPT

Chapter 5

Managing a Subscriber Profile Repository

Topics:

This chapter 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 can 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 for XML provisioning of subscriber profile data, as well as an interactive user interface through the Configuration Management Platform system using a proprietary RESTful API interface.

  The SDM system 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 Subscriber Database Management system provides both a storage and notification platform for policy operations, as well as a platform for provisioning.

  For detailed information on the Subscriber Database Management system, 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. User Data Repository 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 Enhanced Subscriber Profile Repository 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 Subscriber Profile Repository documentation for more information.

To use an SPR with the CMP system, 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

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.

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 opens.

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 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. 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. Click **Save**.

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. Click **Save**.

The SPR connection configuration is modified.

Finding a Subscriber Profile

After the SPR devices are defined, 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. 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 quota for the subscriber 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 tier for the subscriber. 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 entitlements for the subscriber. 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.
- **User Billing Type** — The type of billing. Enter a value of 0 (online charging) or 1 (offline charging). The default value is 1.
- **User Notify MSISDN** — The mobile number used to send messages or reminders to users. Enter a character string of 1 - 15 characters in length.
- **User Status** — The quota status for the user. This value determines whether the user is within quota. Enter a value between 1 and 100. A value of 1 means the user is within the quota. A value of 2 means the user is outside the quota. A value of 3 means the user exceeds the value of the top-up. Values of 4 - 50 are used for united expansion in Group Company. Values of 51 - 100 are used for expansion in companies in each province.

  If the user status has a value of 2 or 3, the value is reset to the default (0) on the date configured by the **Billing Day** field.

4. Click **Save**.

The subscriber profile is created.

Managing Subscribers

This chapter describes how to create and manage subscriber tiers and quota usage within the Configuration Management Platform system.

Note: The actual options you see depend on whether or not your Configuration Management Platform system is configured to operate with a Subscriber Profile Repository. For information about the Oracle Communications Subscriber Database Management product, see the Subscriber Database Management documentation. For information about the Oracle Communications User Data Repository product, see the User Data Repository 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. Select 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. 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 Associated with a Subscriber

To view the subscriber 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.
   That subscriber profile information is shown. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Click the **State** tab.
   Entity state information is shown.
4. 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. Select the subscriber profile you want to modify.

That profile information is shown. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)

3. Select the **State** tab.
   The entity state information is shown.
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. 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. Select the subscriber profile you want to modify.
   The profile information is shown. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the **State** tab.
   The entity state information is shown.
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. 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.
   The profile information is shown. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the **State** tab.
   The entity state information is shown.
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 Associated with a Subscriber

To view the subscriber quotas information 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.
   The profile information is shown. (See *Finding a Subscriber Profile* for information on locating a subscriber profile.)
3. Select the **Quota** tab.
   The **Subscriber Profile Quota Usage** page opens. 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. 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 is shown in the work area.
4. Click **Create**.
   The **Quota Usage** page opens.
5. If there are more than 10 quotas, a message displays prompting you to add more. Click **Yes**.
6. 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-dd*T*hh*:*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). 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.

7. 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.
   The profile information is shown. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the **Quota** tab.
   The **Subscriber Profile Quota Usage** page opens.
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. 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.
   The profile information is shown. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the **Quota** tab.
   The **Subscriber Profile Quota Usage** page opens.

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 Basic Pooled Quota Group

You can use pooled quota groups to create a shared pool profile for multiple subscribers. A basic pool can include up to 25 subscribers as pooled quota group members. You can add members or modify the membership list from the CMP when the pool is a basic pool.

Note: The **Modify Membership** button is hidden when the pool is an enterprise pool. Pooling information for enterprise pools, including pool membership, is provisioned from the SPR.

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. Use the **Search** function to find the desired pool quota group.
   a) 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.

   b) Select **Pool ID** as the **Key Type**.
   c) In the **Key String** field, enter the Pool ID of the desired pool quota group.

      The Pool ID must match exactly; partial or wildcard searching is not supported.

   d) Click **Search**.

   The **Pool Profile** page opens.
3. On the **Pool Profile** tab, click **Modify Membership Information**.
   The **Pool Profile Configuration** page opens.
4. In the **Membership Information** section of the page, enter the following:
   a) **Key Type —** The type of subscriber identifier. 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.

A confirmation message is displayed.

Note: Click **Cancel** to return to the **Pool Profile** page.

5. 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:
      - **quota** (plan)
      - **pass**
      - **top-up**
      - **roll-over**
      - **roll-over-def**

Note: 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. 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. 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. 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 create 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, **`ProfileV3`** or **`ProfileV4`**.
7. 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. 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

About MRA Monitoring

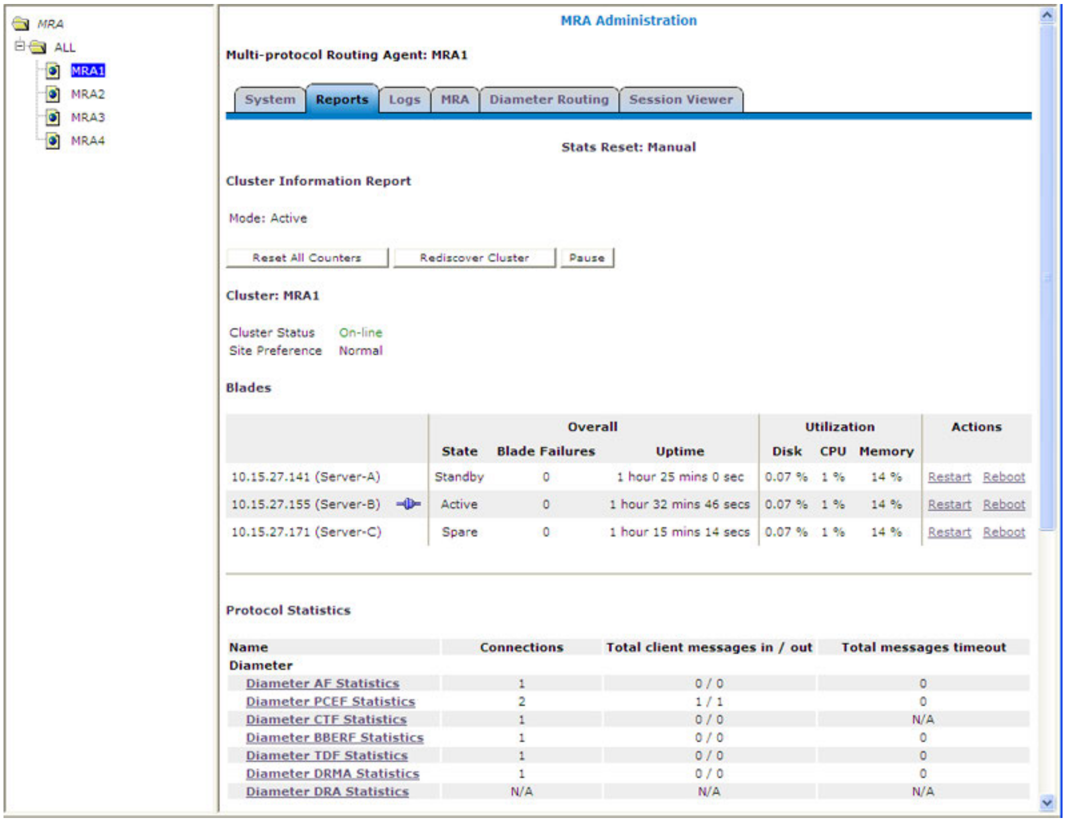
Topics:

Monitoring a Multi-Protocol Routing Agent, (MRA), device is similar to monitoring Multimedia Policy Engine, (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

About 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.



Multi-protocol Routing Agent: MRA1

Stats Reset: Manual

Cluster Information Report

Mode: Active

Cluster: MRA1

Cluster Status On-line
Site Preference Normal

Blades

	Overall			Utilization			Actions	
	State	Blade Failures	Uptime	Disk	CPU	Memory		
10.15.27.141 (Server-A)	Standby	0	1 hour 25 mins 0 sec	0.07 %	1 %	14 %	Restart	Reboot
10.15.27.155 (Server-B)	Active	0	1 hour 32 mins 46 secs	0.07 %	1 %	14 %	Restart	Reboot
10.15.27.171 (Server-C)	Spare	0	1 hour 15 mins 14 secs	0.07 %	1 %	14 %	Restart	Reboot

Protocol Statistics

Name	Connections	Total client messages in / out	Total messages timeout
Diameter			
Diameter AF Statistics	1	0 / 0	0
Diameter PCEF Statistics	2	1 / 1	0
Diameter CTF Statistics	1	0 / 0	N/A
Diameter BBERF Statistics	1	0 / 0	0
Diameter TDF Statistics	1	0 / 0	0
Diameter DRMA Statistics	1	0 / 0	0
Diameter DRA Statistics	N/A	N/A	N/A

Figure 12: Cluster, Blade, and Diameter Information

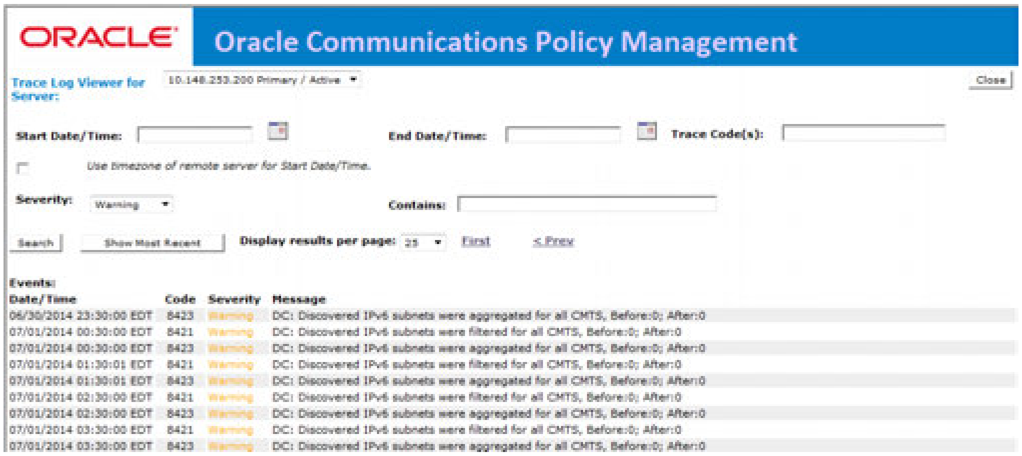
The following is a list of Diameter statistics:

- 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 *About the Mapping Reports KPI Display*.

About the Trace Log Page

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.


ORACLE
Oracle Communications Policy Management
Trace Log Viewer for Server:
10.148.253.200 Primary / Active
Close
Start Date/Time:
End Date/Time:
Trace Code(s):
□ Use timezone of remote server for Start Date/Time.
Severity:
Warning
Contains:
Search
Show Most Recent
Display results per page:
25
First
< Prev

Events:

Date/Time	Code	Severity	Message
06/30/2014 23:30:00 EDT	8423	Warning	DC: Discovered IPv6 subnets were aggregated for all CMTS, Before:0; After:0
07/01/2014 00:30:00 EDT	8421	Warning	DC: Discovered IPv6 subnets were filtered for all CMTS, Before:0; After:0
07/01/2014 00:30:00 EDT	8423	Warning	DC: Discovered IPv6 subnets were aggregated for all CMTS, Before:0; After:0
07/01/2014 01:30:01 EDT	8421	Warning	DC: Discovered IPv6 subnets were filtered for all CMTS, Before:0; After:0
07/01/2014 01:30:01 EDT	8423	Warning	DC: Discovered IPv6 subnets were aggregated for all CMTS, Before:0; After:0
07/01/2014 02:30:00 EDT	8421	Warning	DC: Discovered IPv6 subnets were filtered for all CMTS, Before:0; After:0
07/01/2014 02:30:00 EDT	8423	Warning	DC: Discovered IPv6 subnets were aggregated for all CMTS, Before:0; After:0
07/01/2014 03:30:00 EDT	8421	Warning	DC: Discovered IPv6 subnets were filtered for all CMTS, Before:0; After:0
07/01/2014 03:30:00 EDT	8423	Warning	DC: Discovered IPv6 subnets were aggregated for all CMTS, Before:0; After:0

Figure 13: MRA Trace Log Page

About 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.

About the KPI Dashboard

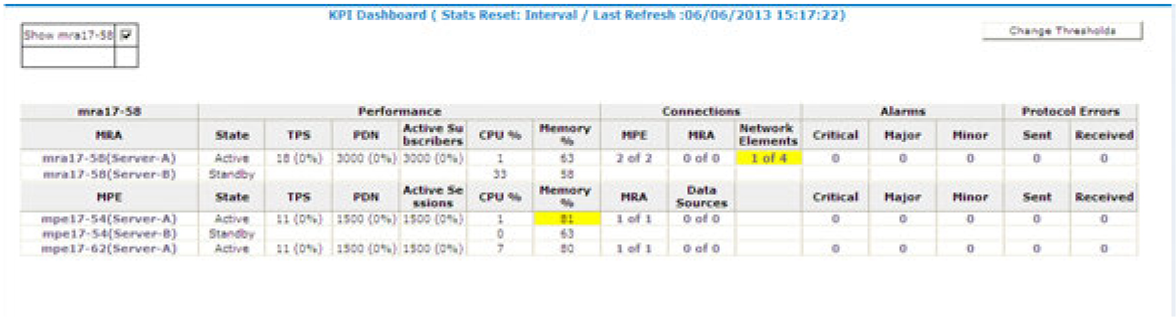
The KPI dashboard provides a multi-site, system-level, summary of performance and operational health indicators in the CMP web based GUI. The display includes indicators for:

- 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.



KPI Dashboard (Stats Reset: Interval / Last Refresh :06/06/2013 15:17:22)

Show mra17-58 ☑

Change Thresholds

mra17-58	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra17-58(Server-A)	Active	18 (0%)	3000 (0%)	3000 (0%)	1	63	2 of 2	0 of 0	1 of 4	0	0	0	0	0
mra17-58(Server-B)	Standby				33	58								
MPE	State	TPS	PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
mpe17-54(Server-A)	Active	11 (0%)	1500 (0%)	1500 (0%)	1	81	1 of 1	0 of 0		0	0	0	0	0
mpe17-54(Server-B)	Standby				0	63								
mpe17-62(Server-A)	Active	11 (0%)	1500 (0%)	1500 (0%)	7	80	1 of 1	0 of 0		0	0	0	0	0

Figure 14: 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.

About Color Threshold Configuration

The **KPI Dashboard Configuration** dialog appears when you click the **Change Thresholds** button located in the top right corner of the KPI Dashboard.

The dialog shows the current settings for the specified parameters. You can modify the values and click **Save** to put the new values into effect. The values are saved so the next time the dashboard is opened it uses the new values.

Note: Saving the thresholds affects other users that may be viewing the dashboard at the same time.

Cancel	Closes the dialog without any changes to the KPI dashboard display.

[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.

Reset	Restores the values to their defaults. The **TPS** and **Session** limits for the Policy Management device are set to the officially supported rates for the current software release.

Changing KPI Color Threshold Levels

You use this feature to change the levels for specific parameters. There can be times that you want lower the level of a parameter, such as CPU% to make sure that there you have adequate warning if a device is getting too much traffic or usage.

To change the threshold level of a KPI:

1. From the **System Wide Reports** section of the navigation pane, select **KPI Dashboard**.
2. From the **KPI Dashboard** screen, click on **Change Thresholds** button (located in the top right corner).
   The KPI Dashboard Configuration window opens.
3. Select the **Percentage Field** for the parameter that is to be modified (warning or error).
4. Type in the new **Percentage**.
5. Repeat step #4 for any other parameter levels that need to be changed.
6. When you finish, click **Save**.

Resetting the KPI Threshold Levels

You use this function to reset the KPI thresholds back to their default levels.

Note: You cannot reset just one parameter. Clicking the **Reset** button will change all parameters that have been previously changed.

To reset the threshold levels of the KPI Dashboard:

1. From the **System Wide Reports** section of the navigation pane, select **KPI Dashboard**.
2. From the **KPI Dashboard** screen, click on **Change Thresholds** button (located in the top right corner).
   The KPI Dashboard Configuration window opens.
3. Click the **Reset** button on the bottom left of the window.
4. When you finish, click **Save**.

About the Mapping Reports KPI Display

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 are listed in the OSSI XML output.

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

Table 11: 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 12: 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 13: Diameter Application Function (AF) 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

Display	MPE	MRA	Name
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
Current number of active sponsored sessions	Y	N	Current Sponsored Session Count
Max sponsored active sessions	Y	N	Max Sponsored Session Count

Display	MPE	MRA	Name
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 14: 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
CCA-I failure messages received/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count

Display	MPE	MRA	Name
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 15: 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
CCA failure messages recd/sent	N	Y	CCA Recv Failure Count\CCA Send Failure Count

Display	MPE	MRA	Name
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 16: 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
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count

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

Table 17: 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
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	

Display	MPE	MRA	Name
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count
Diameter TDF connections	Y	Y	

Table 18: Diameter Sh / Sh Peer 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 due to error response	Y	N	
Messages retried due to response timeout	Y	N	
UDR messages received/sent	Y	N	UDR Messages Received Count\UDR Messages Sent Count
UDR messages timeout	Y	N	UDR Timeout Count
UDR messages retried due to error response	Y	N	
UDR messages retried due to response timeout	Y	N	
UDR messages retried due to error response	Y	N	
UDR messages retried due to response timeout	Y	N	
UDR messages from session updates	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

Display	MPE	MRA	Name
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
PUR messages received/sent	Y	N	PUR Messages Received Count\PUR Messages Sent Count
PUR messages timeout	Y	N	PURTimeout Count
PUR messages retried due to error response	Y	N	
PUR messages retried due to response timeout	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 due to error response	Y	N	
SNR messages retried due to response timeout	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 19: 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
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	

Display	MPE	MRA	Name
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	
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	LNRRecv 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			

Display	MPE	MRA	Name
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 20: 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 21: 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

Display	MPE	MRA	Name
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
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 22: 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	

Display	MPE	MRA	Name
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	
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	

Display	MPE	MRA	Name
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	
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 23: 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 23: 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 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 24: 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 25: 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

Display	MPE	MRA	Name
Diameter Protocol Errors on each error codes	Y	Y	(see specific errors listed in GUI)

Table 26: 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
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 27: 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

Display	MPE	MRA	Name
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 28: 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

Display	MPE	MRA	Name
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
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

Display	MPE	MRA	Name
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 29: 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

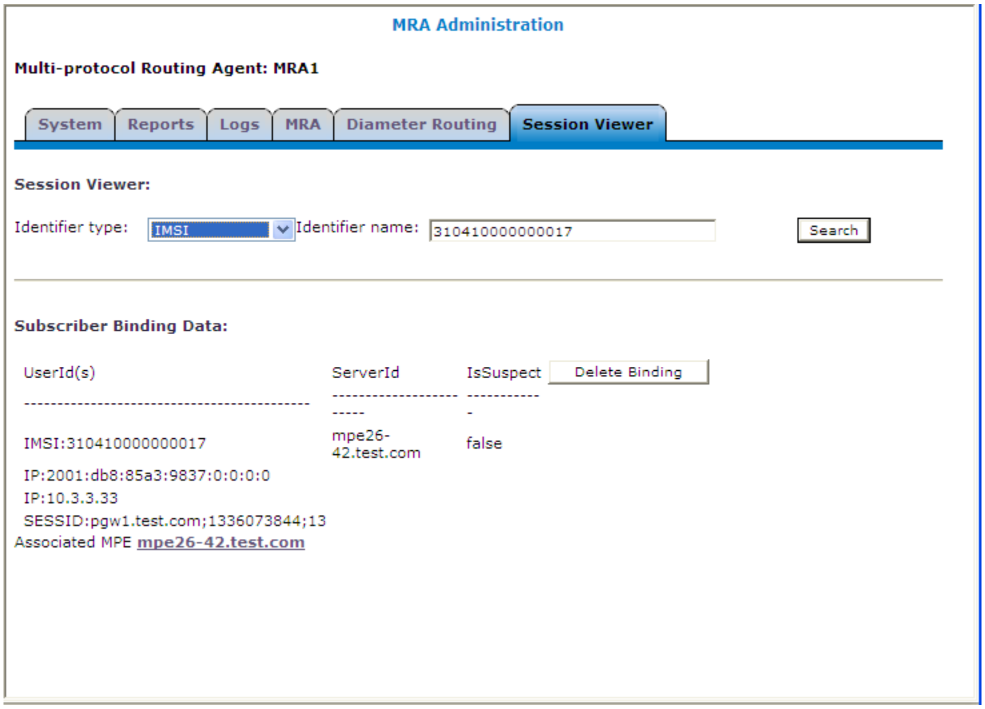
Table 30: KPI Interval Statistics

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

About 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:



Multi-protocol Routing Agent: MRA1

Session Viewer:

Identifier type: IMSI Identifier name: 310410000000017

Subscriber Binding Data:

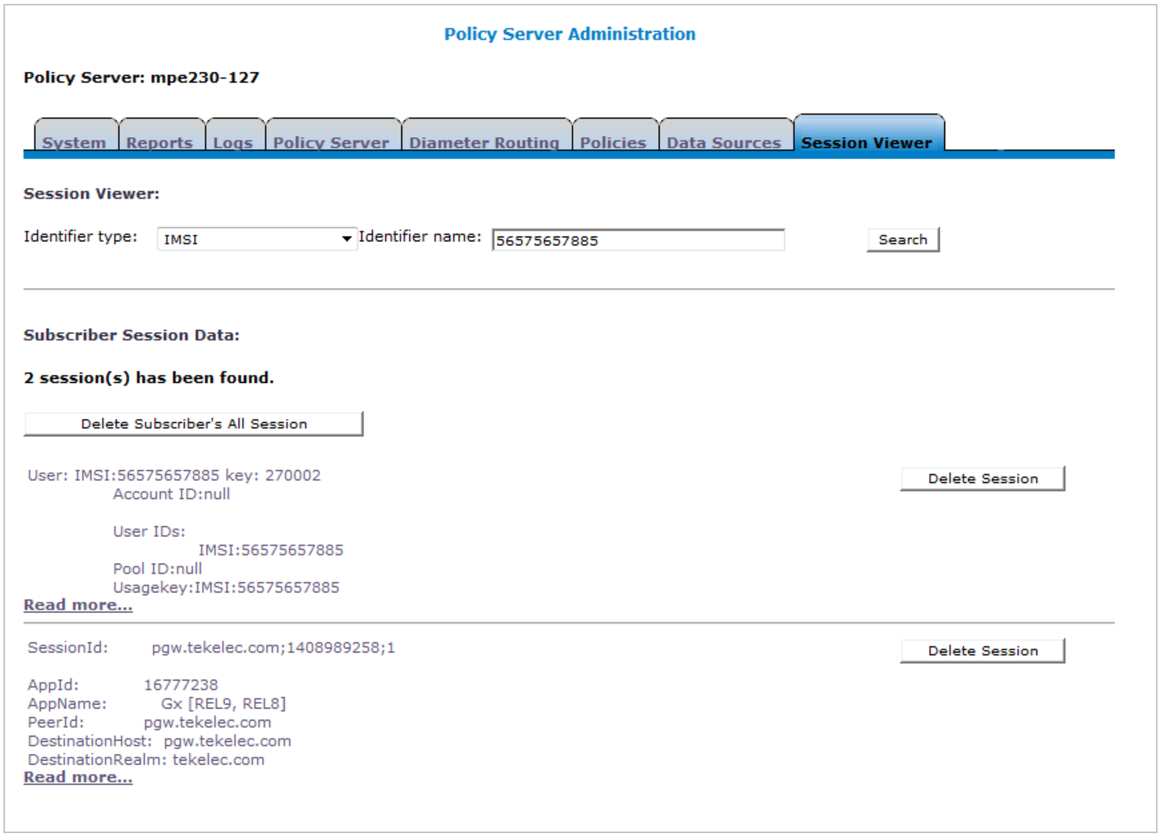
UserId(s)	ServerId	IsSuspect
IMSI:310410000000017 IP:2001:db8:85a3:9837:0:0:0:0 IP:10.3.3.33 SESSID:pgw1.test.com;1336073844;13	mpe26-42.test.com	false

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

Session Viewer:

Identifier type: IMSI Identifier name: 56575657885

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
```

```
SessionId:      pgw.tekelec.com;1408989258;1

AppId:          16777238
AppName:          Gx [REL9, REL8]
PeerId:         pgw.tekelec.com
DestinationHost:  pgw.tekelec.com
DestinationRealm: tekelec.com
```

The MRA device is listed by peer ID.

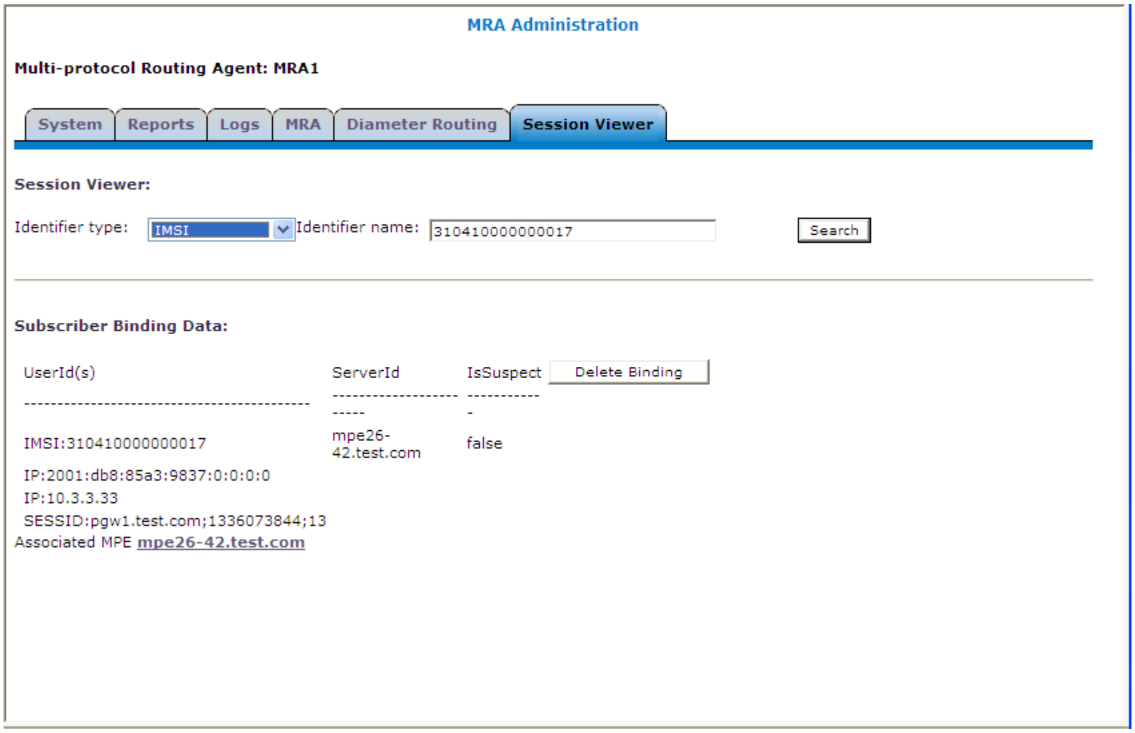
If no session data is available, the CMP returns the following message:

> 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:



Multi-protocol Routing Agent: MRA1

Session Viewer:

Identifier type: IMSI Identifier name: 310410000000017

Subscriber Binding Data:

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

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

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.

Glossary

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.

DRMA

Distributed Routing and Management Application

A Tekelec proprietary protocol used for communicating routing information between Policy Management systems.

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 (for example, 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 provides you with a graphic means for manipulating screen data rather than being limited to character based commands.

H

	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	Internet Protocol version 4 Identifies an Internet Protocol version 4 address composed of 4 bytes in a dotted decimal format (for example, nnn.nn.nnn.nn).
IPv6	Internet Protocol version 6 Identifies an Internet Protocol version 6 address composed of 8 groups of colon-separated 4 hexadecimal digits.
	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

M

engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization.

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

Policy rules that define the conditions and actions used by a carrier network to control how subscribers and applications are treated and how network resources are allocated and used.

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

R

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.

T

TDF

Traffic Detection Function

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.