Oracle® Communications Policy Management

Policy Front End Wireless User's Guide

Release 11.5

E55089 Revision 01

November 2014

Oracle® Communications Policy Front End Wireless User's Guide, Release 11.5

Table of Contents

List of Figures

List of Tables

Chapter 1

About This Guide

Topics:

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

How This Guide is Organized

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

- *About This Guide* contains general information about this guide, the organization of this guide, and how to get technical assistance.
- *Introduction* contains an overview of the guide, the Distributed Routing and Management Application (DRMA) protocol, and the Graphical User Interface (GUI).
- *Configuring a CMP System and MRA, MPE Devices* describes how to configure the CMP to manage the MRA, how to associate an MPE to the MRA, and how to configure an MRA.
- *Monitoring the MRA* describes how to monitor cluster and blade information, DRMA information, and event logs.

Intended Audience

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

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*.)
WARNING	**Warning**: (This icon and text indicate the possibility of *equipment damage*.)
CAUTION	**Caution**: (This icon and text indicate the possibility of *service interruption*.)

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

Related Publications

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

Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As**.

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.

Policy Front End Overview

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

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

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

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

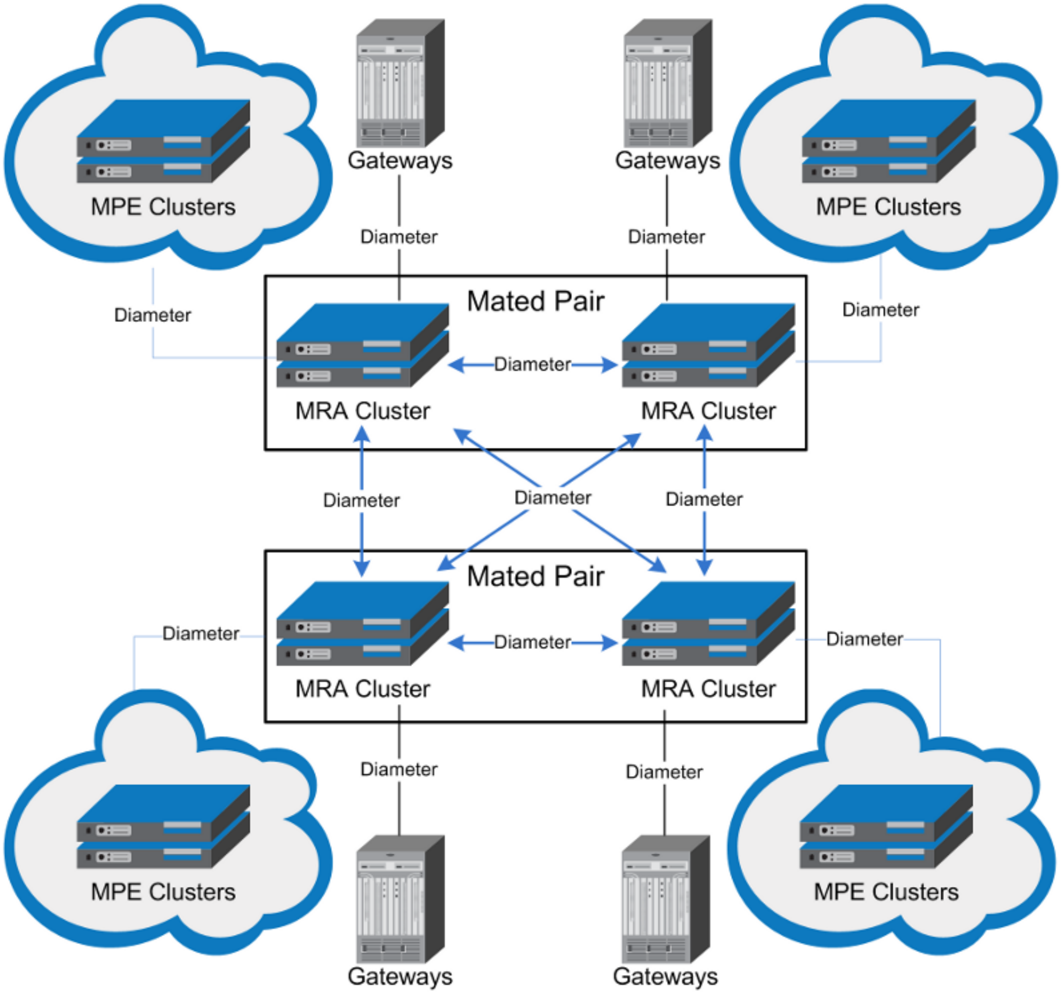


Figure 1: Typical Front End (MRA) Network

Distributed Routing and Management Application (DRMA) Protocol

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

Backup MRAs, Associated MRAs, and Mated Pairs

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

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

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

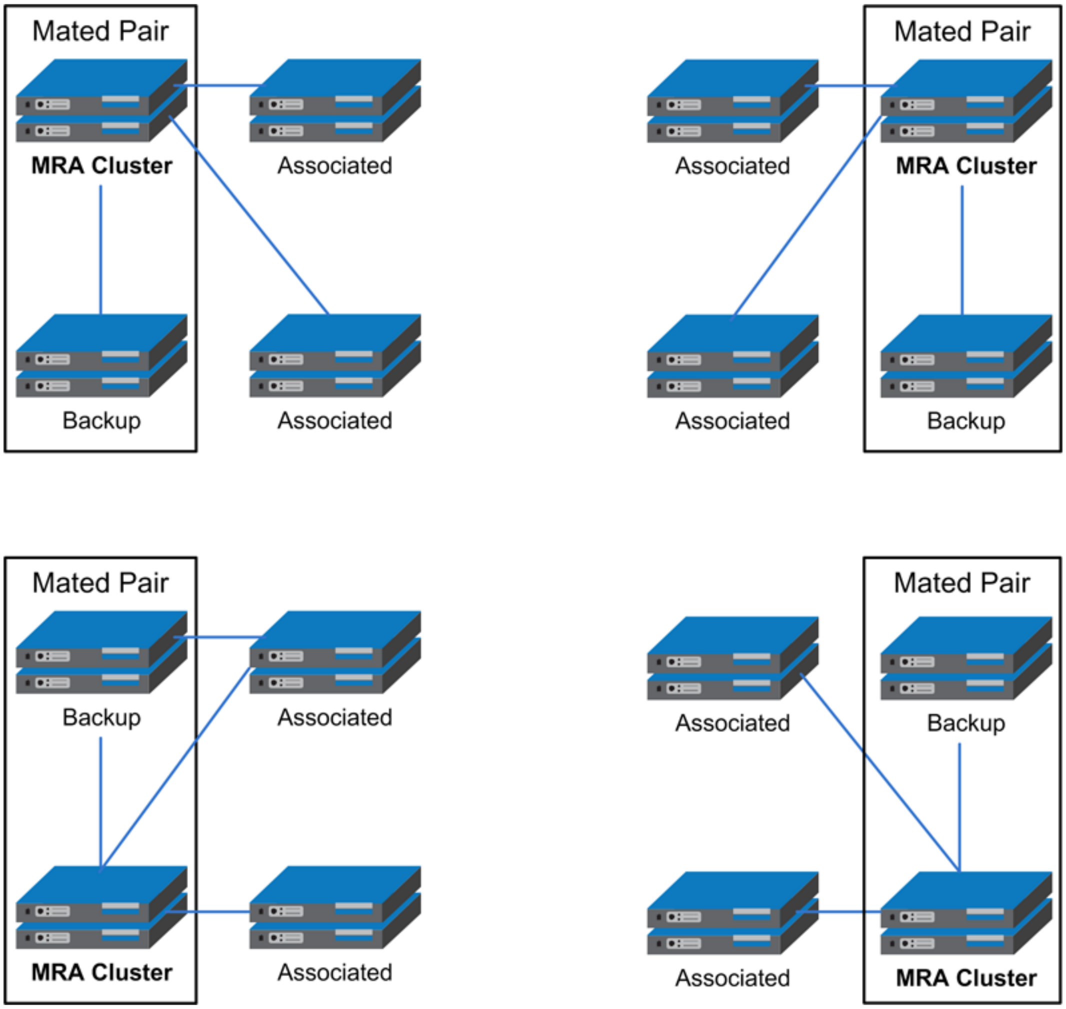
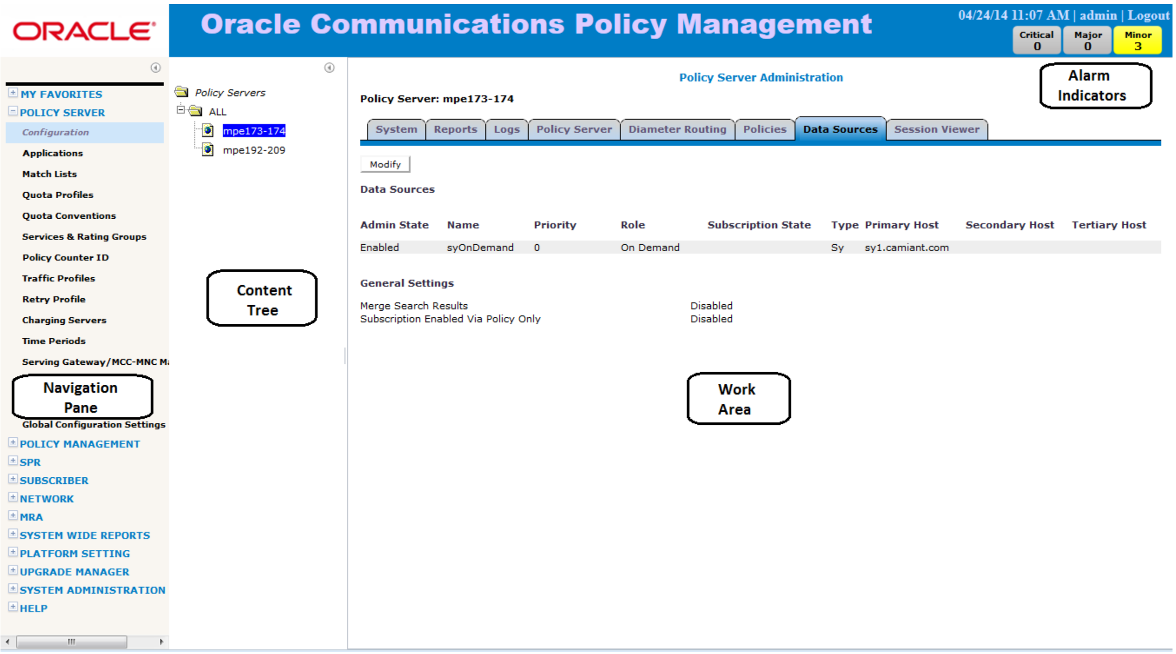


Figure 2: Backup and Associated MRA Clusters and Mated Pairs

GUI Overview

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



Policy Server: mpe173-174

Data Sources

Admin State	Name	Priority	Role	Subscription State	Type	Primary Host	Secondary Host	Tertiary Host
Enabled	syOnDemand	0	On Demand		Sy	sy1.camiant.com		

General Settings

Merge Search Results	Disabled
Subscription Enabled Via Policy Only	Disabled

Figure 3: Structure of the CMP GUI

- **Navigation Pane** — Provides access to the various available options configured within the CMP system.

  You can bookmark options in the Navigation pane by right-clicking the option and selecting **Add to Favorite**. Bookmarked options can be accessed from the **My Favorites** folder at the top of the Navigation pane. Within the My Favorites folder, you can arrange or delete options by right-clicking the option and selecting **Move Up**, **Move Down**, or **Delete from Favorite**.

  You can collapse the navigation pane to make more room by clicking the button in the top right corner of the pane (◀). Click the button again to expand the pane.

- **Content Tree** — Contains an expandable/collapsible listing of all the defined items for a given selection. For content trees that contain a group labeled **ALL**, you can create customized groups that display in the tree.

  The content tree section is not visible with all navigation selections.

  You can collapse the content tree to make more room by clicking the button in the top right corner of the pane (◀). Click the button again to expand the tree. You can also resize the content tree relative to the work area.

- **Work Area** — Contains information that relates to choices in both the navigation pane and the content tree. This is the area where you perform all work.

- **Alarm Indicators —** Provides visual indicators that show the number of active alarms.

Chapter 3

Configuring a CMP System and MRA, MPE Devices

Topics:

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

This chapter describes how to:

- Configure a CMP system to manage an MRA
- Associate an MPE with an MRA
- Configure MRA backup and monitoring capabilities

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

Configuring the CMP to Manage the MRA

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

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

Configuring the CMP System to Manage an MRA Cluster

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

To reconfigure the CMP operating mode, complete the following:

CAUTION

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 version number.
2. Click the **Mode** button.

   Consult with My Oracle Support for information on this button.

   The **Mode Settings** page opens.
3. At the bottom of the page, select **Manage MRAs**.
4. Click **OK**.
   The browser page closes and you are automatically logged out.
5. Refresh the browser page.
   The **Welcome admin** page is displayed.

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

Defining an MRA Cluster Profile

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

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

b) **Name** (required) — Enter a name for the MRA cluster.

The name can be up to 250 characters long. The name can contain any alphanumeric characters except quotation marks (") and commas (,).

c) **Description/Location** (optional) — Free-form text.

Enter up to 250 characters.

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

The default is a non-secure (HTTP) connection.

e) **Stateless Routing** — Select to enable stateless routing. In stateless routing, the MRA cluster only routes traffic; it does not process traffic.

The default is stateful routing.

5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The MRA cluster profile is displayed in the **MRA Administration** page.

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

Modifying an MRA Cluster Profile

To modify MRA cluster profile settings:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the MRA cluster profile.
   The **MRA Administration** page opens in the work area.
3. On the **System** tab of the **MRA Administration** page, click **Modify**.
   The **Modify System Settings** page opens.
4. Modify MRA system settings as required.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The MRA cluster profile settings are modified.

Modifying MRA System Settings, Grouping or deleting MRA devices

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

Creating an MRA Group

To create an MRA group:

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

4. Enter the name of the new CMP group.

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

5. When you finish, click **Save** (or **Cancel** to abandon your request).
   The new group appears in the content tree.

The MRA group is created.

Setting Up an MRA Cluster

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens.
2. Click **Add MPE/MRA Cluster**.
   The **Topology Configuration** page opens. Each section of the **Topology Configuration** page can be collapsed or expanded.
3. Define the general settings for the cluster in the **General Settings** section of the page.
   a) **Name** (required) — Name of the cluster. Enter up to 250 characters, excluding quotation marks (") and commas (,).
   b) **Appl Type** — Select **MRA**.
   c) HW Type — Select **C-Class** (default), **C-Class(Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment), **NETRA**, or **RMS** (for a rack-mounted server).
   d) Enter the address in the standard dot format, and the subnet mask in CIDR notation from 0–32.

      Note: This address corresponds to the cluster address in Policy Management systems before V7.5.

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

      At least one signaling VIP is required.

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

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

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

4. Define the general network configuration for the C-Class, C-Class segregated, or NETRA servers in the **Network Configuration** section of the page. This section is not available for RMS.
   a) Enter the **OAM**, **SIG-A**, and **SIG-B** VLAN IDs, in the range 1–4095. The defaults are 3 for the OAM network and server IP, 5 for the SIG-A network, and 6 for the SIG-B network.

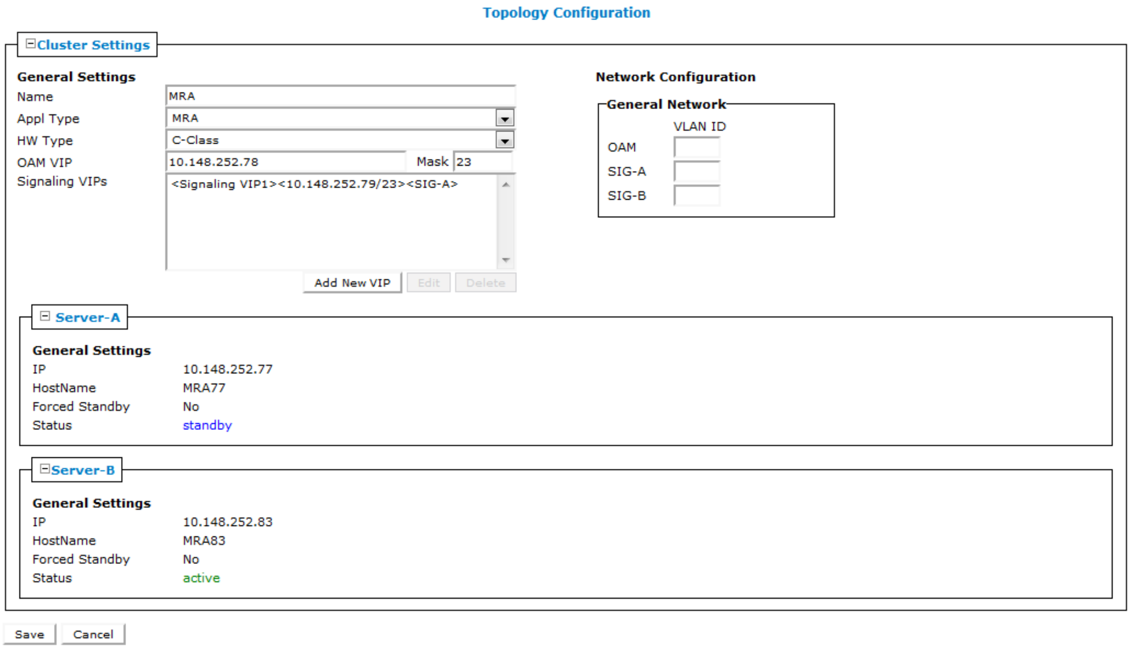
5. Define the settings for **Server-A** in the Server-A section of the page.
   a) **IP** (required) — The IPv4 address of the server. Enter the standard IP dot-formatted IPv4 address string.

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

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

6. (Optional) Click **Add Server-B** and enter the appropriate information for the standby server of the cluster. See step *Step 5* for information about the fields.
   Server-B is defined for the cluster.
7. When you finish, click **Save** (or **Cancel** to discard your changes).
   You are prompted, "The VLAN IDs on the page must match the VLAN IDs configured on the server. A mismatch will cause HA to fail. Please confirm that the VLAN IDs are correct before saving." Click **OK** (or **Cancel** to stop the save operation).
8. If you are setting up multiple clusters, repeat the steps.

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.



Topology Configuration

Cluster Settings

General Settings
Name: MRA
Appl Type: MRA
HW Type: C-Class
OAM VIP: 10.148.252.78 Mask 23
Signaling VIPs: <Signaling VIP1><10.148.252.79/23><SIG-A>

Network Configuration

General Network

	VLAN ID
OAM	
SIG-A	
SIG-B	

Server-A

General Settings
IP: 10.148.252.77
HostName: MRA77
Forced Standby: No
Status: standby

Server-B

General Settings
IP: 10.148.252.83
HostName: MRA83
Forced Standby: No
Status: active

Figure 4: Sample Cluster Topology Configuration

Configuring Protocol Options for an MRA Device

To configure protocol options on an MRA device:

1. From the **MRA** section of the navigation pane, select **Configuration**.
2. From the content tree, select the MRA device.
   The **MRA Administration** page opens.
3. On the **MRA Administration Administration** page, select the **MRA** tab.
   The current configuration options are displayed.
4. Click **Modify** and 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** (or **Cancel** to discard your changes).

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 method(s) to configure, contact My Oracle Support (*https://support.oracle.com*).
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.
Primary Indexing	Select from the pull-down list to set to the type of index that is expected for messages that create bindings, for example Gx CRR-I. **Note:** The type of index selected for primary indexing must also be selected either as an "Index by IMSI" or "Index by E.164" depending on the configuration. ⚠ CAUTION Primary Index cannot be changed on a system that has already created bindings without suffering data loss.
Index by IP Address	Select if the MRA devices in the association should index by IP address. You can select **Index by IPv4**, **Index by IPv6**, or both formats.
Overrides by APN	Select to perform subscriber indexing for a specific IP address and a specific APN name. In the **Overrides by APN** section, click **Add**. Enter the APN name and click **Save** to enable **Index by IPv4**, **Index by IPv6**, or both. You can create new APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.

Setting Up a Georedundant Cluster

Before defining a cluster, ensure the following:

- The MRA/ 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

If your system is not set up for georedundancy, see *Setting Up an MRA Cluster*.

To define a cluster in a georedundant system:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens.
2. From the content tree, select the **All Clusters** folder.
   The defined clusters are listed.
3. Click **Add MPE/MRA Cluster**.
   The **Topology Configuration** page opens. Each section of the **Topology Configuration** page can be collapsed or expanded.
4. Define the general settings for the cluster in the **Cluster Settings** section of the page:
   a) **Name** (required) — Name of the cluster. Enter up to 250 characters, excluding quotation marks (") and commas (,).
   b) **Appl Type** — Select the application type:

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

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

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

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

   g) **Backup Heartbeat** — Select a network to carry inter-site backup heartbeat traffic. This field only appears if the system supports georedundancy.

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

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

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

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

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

      - **C-Class** (default)
      - **C-Class(Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment)
      - **NETRA**
      - **RMS**

   c) **OAM VIP** (optional) — Enter the IPv4 address and mask of the OAM virtual IP (VIP) address. The OAM VIP is the address the CMP cluster uses to communicate with the cluster.

      Enter the address in the standard dot format, and the subnet mask in CIDR notation from 0–32.

      Note: This address corresponds to the cluster address in Policy Management systems before V7.5.

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

      At least one signaling VIP is required.

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

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

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

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

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

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

   a) **IP** (required) — The IPv4 address of the server. Enter the standard IP dot-formatted IPv4 address string.

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

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

d) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the New Path dialog, enter an IP address and mask, and select the network.

- **SIG-A**
- **SIG-B**
- **REP**
- **BKUP** (if the hardware type is **C-Class(Segregated Traffic)** or **NETRA**)

7. (Optional) Define Server-B in the **Server-B** section of the page. Click **Add Server-B** and enter the standby server information for the cluster:

a) **IP** (required) — The IPv4 address of the server. Enter the standard IP dot-formatted IPv4 address string.

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

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

d) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the New Path dialog, enter an IP address and mask, and select the network.

- **SIG-A**
- **SIG-B**
- **REP**
- **BKUP** (if the hardware type is NETRA)

8. Define the secondary site information in the **Secondary Site Settings** section of the page:

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

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

- **C-Class** (default)
- **C-Class(Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment)
- **NETRA**
- **RMS**

c) **OAM VIP** (optional) — Enter the IPv4 address and mask of the OAM virtual IP (VIP) address. The OAM VIP is the address the CMP cluster uses to communicate with the cluster.

Enter the address in the standard dot format, and the subnet mask in CIDR notation from 0–32.

Note: This address corresponds to the cluster address in Policy Management systems before V7.5.

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

At least one signaling VIP is required.

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

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

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

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

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

9. Define Server-C in the **Server-C** section of the page. If you define a secondary site, you must define a spare server. Click **Add Server-C** and define the information for the spare server:

a) **IP** (optional) — The IPv4 address of the server. Enter the standard IP dot-formatted IPv4 address string.

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

c) **Forced Standby** — Select **Forced Standby** to ensure that the server is in standby mode.

d) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the New Path dialog, enter an IP address and mask, and select the network:

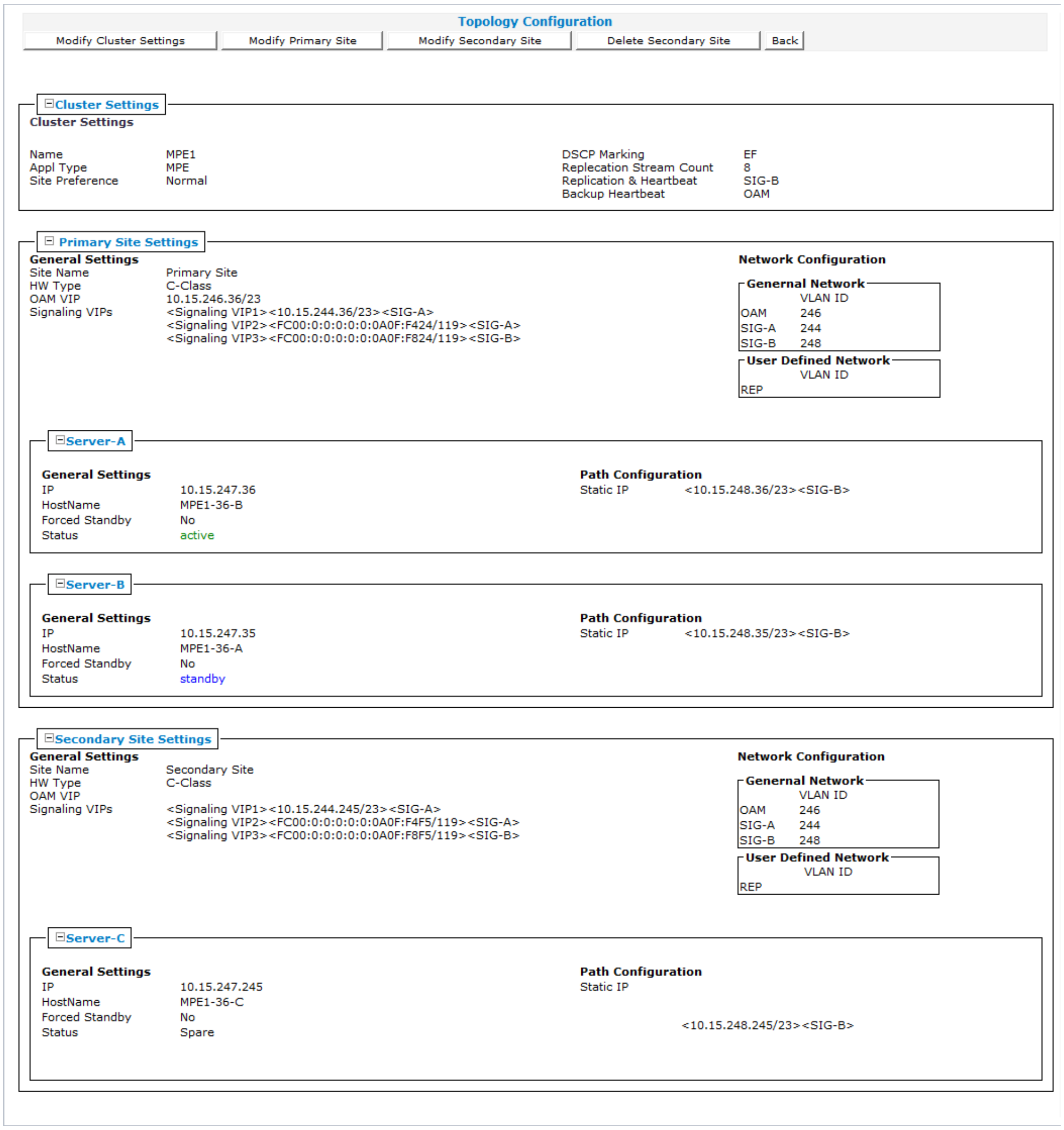
- **SIG-A**
- **SIG-B**
- **REP**

10. When you finish, click **Save** (or **Cancel** to discard your changes).
You are prompted, "The VLAN IDs on the page must match the VLAN IDs configured on the server. A mismatch will cause HA to fail. Please confirm that the VLAN IDs are correct before saving." Click **OK** (or **Cancel** to stop the save operation).

11. If you are setting up multiple clusters, repeat the above steps as often as necessary.

The MPE or MRA cluster is defined.

Setting Up a Georedundant Cluster shows the configuration for a georedundant (two-site) MPE cluster, using SIG-B for a replication network and OAM for the backup heartbeat network, with eight WAN replication streams.



⊟Cluster Settings

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

Genernal 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 Topology Configuration

Deleting an MRA Cluster Profile from an MRA Group

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

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

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the an MRA group.

The **MRA Administration** page opens in the work area, displaying the contents of the selected MRA group.

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

   The MRA cluster profile is removed from the group.

Deleting an MRA Group

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

To delete an MRA group or sub-group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is**ALL**.
2. Select the MRA group or subgroup from the content tree.
   The contents of the selected MRA group are displayed.
3. Click **Delete**.
   You are prompted: “Are you sure you want to delete this Group?”
4. Click **OK** to delete the selected group (or **Cancel** to abandon the request).

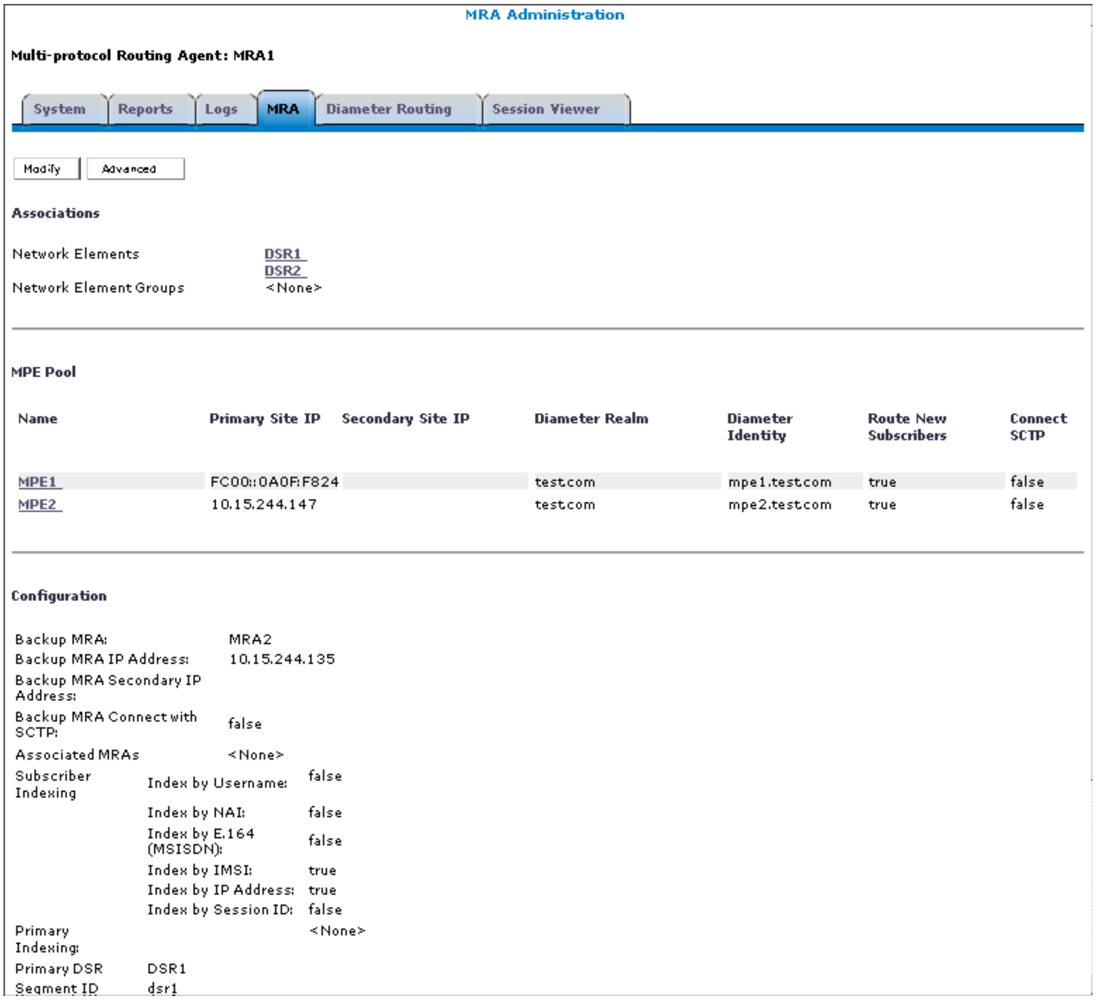
The MRA group is deleted.

Configuring and Modifying MRA Associated Network Elements, Backup MRAs, and MRA Diameter Settings

The **MRA** tab on the **MRA Configuration** page displays a list of network elements associated with the MRA device, the associated MPE pool, configuration settings for the MRA device, Diameter-related configuration information, and if load shedding is configured. *Figure 6: MRA Tab* shows an example.

Use the MRA tab to:

- Configure and modify MRA device associated network elements
- Define a backup MRA device
- Define associated MRA devices
- Associate MPE device with an MRA device and add to MPE pool
- Define georedundant MRA devices
- Configure subscriber indexing
- Associate a DSR network element with an MRA device
- Configure MRA Diameter settings
- Configure MRA RADIUS settings
- Configure load shedding



Multi-protocol Routing Agent: MRA1

Associations

Network Elements	DSR1 DSR2
Network Element Groups	<None>

MPE Pool

Name	Primary Site IP	Secondary Site IP	Diameter Realm	Diameter Identity	Route New Subscribers	Connect SCTP
MPE1	FC00::0A0F:F824		test.com	mpe1.test.com	true	false
MPE2	10.15.244.147		test.com	mpe2.test.com	true	false

Configuration

Backup MRA:	MRA2	
Backup MRA IP Address:	10.15.244.135	
Backup MRA Secondary IP Address:		
Backup MRA Connect with SCTP:	false	
Associated MRAs	<None>	
Subscriber Indexing	Index by Username:	false
	Index by NAI:	false
	Index by E.164 (MSISDN):	false
	Index by IMSI:	true
	Index by IP Address:	true
	Index by Session ID:	false
Primary Indexing:		<None>
Primary DSR	DSR1	
Segment ID	dsr1	

Figure 6: MRA Tab

Associating Network Elements with an MRA

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 (refer to the *CMP Wireless User's Guide* to add network elements), is available for selection.

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

1. From within the **MRA** tab, click **Modify**.
   The **MRA Administration Modify** page opens.
2. In the **Associations** section of the **MRA Administration Modify** page, click **Manage**.
   A list of network elements is displayed. For example:

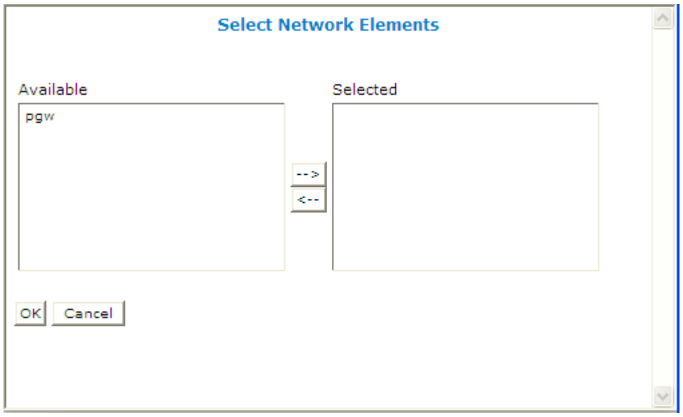


Figure 7: Select Network Elements

3. Select a network element in the **Available** list, click the right arrow to move the network element to the **Selected** list, and click **OK**.

The network element is added to the MRA.

Configuring the MRA/MPE Pool and Diameter Peer Routing Table

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:

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

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.

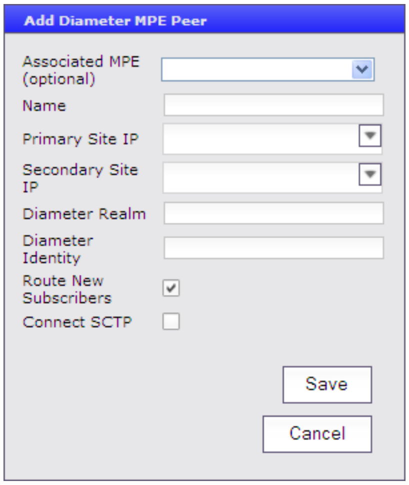
Associating an MPE with an MRA

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

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

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

1. From within the **MRA** tab, click **Modify**.
2. In the **MPE Pool** section, click **Add**.



Add Diameter MPE Peer

Associated MPE (optional)

Name

Primary Site IP

Secondary Site IP

Diameter Realm

Diameter Identity

Route New Subscribers ☑

Connect SCTP ☐

Figure 8: Adding a Diameter MPE Peer

The **Add Diameter MPE Peer** window opens.

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

      Note: An MPE device is selected from the list of MPEs managed by the CMP. If the MPE is *not* managed by this CMP, this should be left blank.

   b) **Name** — Name of the MPE device.
   c) **Primary Site IP** — Enter the IP address of the primary site.
   d) **Secondary Site IP** (for georedundant configurations only) — Enter the IP address of the secondary site.
   e) **Diameter Realm** — Enter the domain of responsibility for the peer (for example, galactelEU.com).
   f) **Diameter Identity** — Enter a fully qualified domain name (FQDN) or the peer device (for example, MRA10-24.galactel.com).
   g) **Route New Subscribers** — Select if the MPE should 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) **Connect SCTP** — Select if the MRA should connect to the MPE using SCTP (instead of TCP).
4. When you finish, click **Save** (or **Cancel** to abandon your changes).
   The **Add Diameter MPE Peer** window closes.
5. In the **Configuration** section of the page, select the identification system to use for **Primary Indexing**. This is the primary index for subscribers. This field should never be changed on a running system without contacting Oracle customer service.
6. 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**.

Adding Associated MRAs

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

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

To configure an associated MRA device, complete the following:

1. From the **Navigation Panel** select **MRA Associations**.
   The **MRA Association Administration** page opens.
2. From the top of the MRA Associations tree, select **MRA Associations**.
3. Click **Create MRA Association**
   The **Configuration** screen opens.
4. Type in the **Name** of the MRA Association.
5. (Optional) Type in a **Description** of the MRA Association.
6. From the **Members** section, click **Add**.
   The Add MRA Association Member pop-up appears.
7. From the **Add MRA Association Members** window, perform the following steps:
   a) Select an **MRA** from the list of existing MRAs.
      After the MRA has been selected, the **Default Primary IP Address** of that MRA appears in the field.
   b) (Optional) If the Association is to be georedundant, select a **Default Secondary IP Address**. This is the IP Address other MRAs in the Association will use when establishing Diameter Connections with this MRA.

      Note: A different IP Address will be used if there are any matching overrides configured.

   c) (Optional) Select a **Backup MRA** from the list.
   d) (Optional) Select **Connect SCTP** if other MRAs in the Association should connect to this MRA using SCTP instead of TCP.
   e) Click **Save** to save your configuration.
8. (Optional) If there is to be an **Association Override**, click **Add** in the **Association Override** section. Then repeat **substeps 7a-7e** and click **Save**.

9. For **Subscriber Indexing**, select any or all of the following:
   - **Index by Username**
   - **Index by NAI**
   - **Index by E.164 (MSISDN)**
   - **Index by IMSI**
   - **Index by Session ID**
   - **Primary Indexing**
   - **Default Index By IP Address**
10. (Optional) If there are to be **Overrides by APN** click **Add** in the section.
    a) Type in the name of the **APN**.
    b) Select **Index by IPv4, Index by IPv6** (either one or both).
    c) Click **Save** to save the APN configuration.
11. When you finish, click **Save** (or **Cancel** to abandon your changes).

The MRA clusters are configured as associated MRA devices.

Configuring Protocol Options on an Associated MRA Device

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

1. From the **MRA** section of the navigation pane, select **MRA Associations**.
   The content tree displays the list of Associated MRAs. The initial group is **ALL**.
2. From the content tree, select the MRA Association.
   The **MRA Association Administration** page opens.
3. On the **MRA Association Administration** page, click the **Modify**.
   The current configuration options are displayed.
4. From the **Subscriber Indexing** section define options as necessary.

   MRA Protocol Configuration Options defines available options that pertain specifically to MRA devices. (The options may vary depending on the configuration mode of the system.)
5. When you finish, click **Save** (or **Cancel** to discard your changes).

Table 3: 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 method(s) 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).

Attribute	Description
Index by Session ID	Select if the MRAs in the association should index by session ID.
Primary Indexing	Select from the pull-down list to set to the type of index that is expected for messages that create bindings, for example Gx CRR-I. **Note:** The type of index selected for primary indexing must also be selected either as an "Index by IMSI" or "Index by E.164" depending on the configuration. ⚠Primary Index cannot be changed on a system that has already created bindings without suffering data loss.
Index by IP Address	Select if the MRAs in the association should index by IP address. You can select **Index by IPv4**, **Index by IPv6**, or both formats.
Overrides by APN	Select to perform subscriber indexing for a specific IP address and a specific APN name. In the **Overrides by APN** section, click **Add**. Enter the APN name and click **Save** to enable **Index by IPv4**, **Index by IPv6**, or both. You can create new APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.

Modifying Backup and Associated MRA devices

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

To modify backup and associated MRA devices:

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

   When you finish, click **Save** (or **Cancel** to abandon your changes).

MRA Association Status Definitions

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

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

MRA Association Operations

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

These operations include:

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

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

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

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

Conditions Limiting Operation Options

- If the association type is set to **Legacy**, only Reset Counters and Reapply Configuration operations are available.

- If all of the MRAs in the association show **Migrated** or **Failed Migration** status, only Accept Migration operation is available.
- If at least one MRAs in the association shows**Migrating** status, only the Cancel operation is available.
- If at least one MRAs in the association shows**Syncing** status, only the Cancel Sync operation is available.
- If any of the MRAs in the association show **Syncing** or **Failed Sync** status, then only the Manual Migration operation is available.
- If any of the MRAs in the association show **Migrating**, **Migrated** or **Failed** status the Manual Sync operation will *not* be available.

Associating a DSR Network Element with an MRA

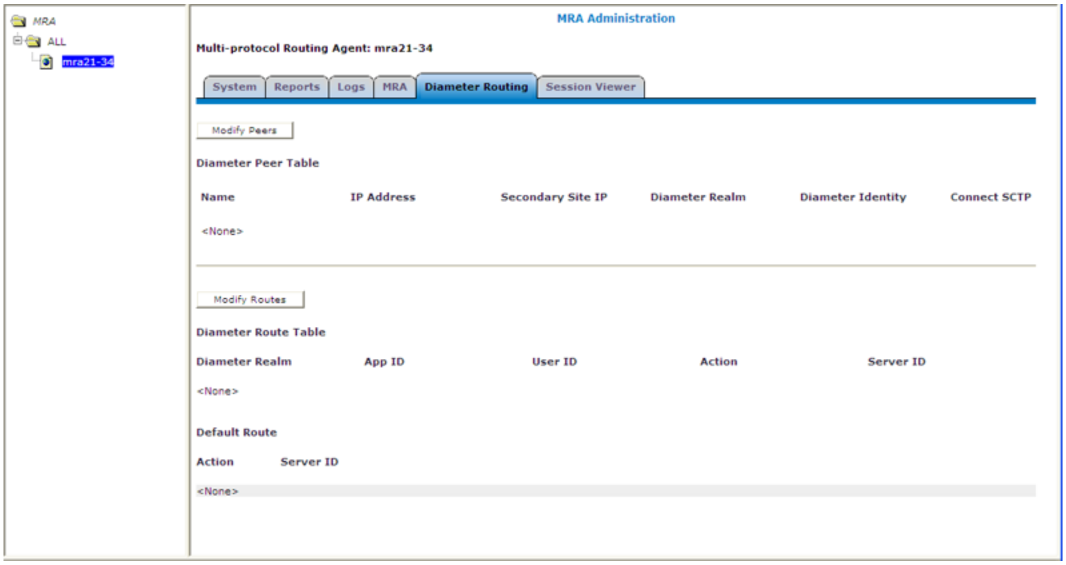
Use this procedure to associate a DSR with an MRA device. If the MRA device gets an MPE-initiated message and the MRA device has a DSR configured, the MRA device will forward the message to the Primary DSR. If the connection to the primary DSR is not available, the MRA device forwards the message to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

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA device.
   The **MRA Administration** page opens.
3. On the **MRA Administration** page, select the **MRA** tab.
   The current MRA configuration settings are displayed.
4. From within the **MRA** tab, click **Modify**.
   The **Modify MRA** page opens.
5. Select a **Primary DSR** to associate with this MRA from the pulldown menu.
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** (or **Cancel** to abandon your changes).

The specified DSR information is associated with this MRA device.

Configuring Diameter Routing

The **Diameter Routing** tab is used to configure the MRA so that the MPE will continue to be available for the MRA. In addition to the entries in the peer table, the MPE devices listed in the MPE pool for the MRA device should also be available to participate in Diameter peer routing. Therefore, the entries in the Diameter Peer Table can be added from either the Diameter routing page or from the MPE association page. However, the same MPE can only appear in either the peer table or the pool and cannot appear in both.



Multi-protocol Routing Agent: mra21-34

Diameter Peer Table

Name	IP Address	Secondary Site IP	Diameter Realm	Diameter Identity	Connect SCTP
<None>					

Diameter Route Table

Diameter Realm	App ID	User ID	Action	Server ID
<None>				

Default Route

Action	Server ID
<None>	

Figure 9: Diameter Routing Tab

To add a Diameter peer:

1. From the **Diameter Routing** tab, click **Modify Peers**.
   The **Add Diameter Peer** window opens.
2. Select a configured MRA or MPE from the drop-down list.
3. Enter the following:
   - **Name** — Enter the name of the peer device (which must be unique in the CMP database).
   - **Primary Site IP** — Enter the IP address, in IPv4 or IPv6 format, of the primary site.
   - **Secondary Site IP** — For georedundant configurations, enter the IP address, in IPv4 or IPv6 format, of the server at the secondary site.
   - **Diameter Realm** — Enter the domain of responsibility for the peer (for example, **`galactelEU.com`**).
   - **Diameter Identity** — Enter a fully qualified domain name (FQDN) or the peer device (for example, **`MRA10-24.galactel.com`**).

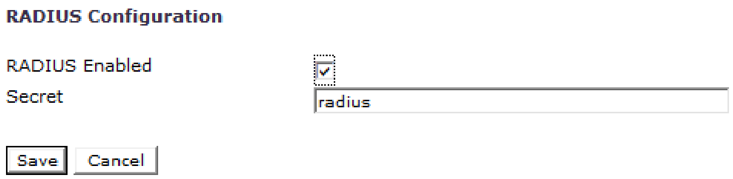
   When you finish, click **Save** (or **Cancel** to discard your changes).

Configuring for RADIUS

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

Complete these steps to configure an existing MRA for RADIUS.

1. From the **MRA Tree**, select the **MRA** to be configured for RADIUS.
2. Select the **MRA Tab**.
3. Click **Modify**.
4. Scroll to the **RADIUS Configuration** section and enter the following:


RADIUS Configuration

RADIUS Enabled ☑

Secret radius

Figure 10: RADIUS Configuration Section

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

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

Configuring Load Shedding

Use this procedure to enable or disable load shedding on the specified MRA. Load shedding is used to reduce latency and to keep the MRA stable and reliable in overload situations. When enabled, certain requests are rejected by the MRA when it becomes too heavily loaded to process them.

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. On the **MRA Administration** page, select the **MRA** tab.
   The current MRA configuration settings are displayed.
4. From within the **MRA** tab, click **Advanced**.
   The **Advanced MRA Settings** page opens.
5. In the **Enable Load Shedding** section, check mark to turn load shedding on for this MRA device, or remove the check mark by clicking the box to turn load shedding off. See *Configuring Load Shedding Rules for an MRA* for more information on load shedding rules.
6. Click **Save** (or **Cancel** to abandon your changes).

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 once more processing requests.

Configuring Load Shedding Rules for an MRA

You can configure load shedding rules to determine how an MRA device reacts to a processing backlog. This state is called "busyness." By default there are three levels of busyness, from Level 1, the least busy, to Level 3, the most busy. With each successive level, the MRA device becomes more aggressive in rejecting or discarding messages in an attempt to prevent the main queue from become full. At any level of busyness, requests 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. The *Default MRA Device Busyness Levels* table shows the default load-shedding rules for both an MRA or MPE device.

Table 4: Default MRA Device Busyness Levels

Busyness Level	Rule Name	Actions
Level 1 MPE and MRA	DefaultRule1	Reject Gx CCR-I messages with DIAMETER_TOO_BUSY
	DefaultRule2	Reject Gxx CCR-I messages with DIAMETER_TOO_BUSY
	DefaultRule3	Reject Gy CCR-I messages with DIAMETER_TOO_BUSY
Level 2 MPE Only	DefaultRule4	Reject Gx CCR-I messages with DIAMETER_TOO_BUSY
	DefaultRule5	Reject Gxx CCR-I messages with DIAMETER_TOO_BUSY
	DefaultRule6	Reject Gy CCR-I messages with DIAMETER_TOO_BUSY
	DefaultRule7	Reject Rx AAR-I messages with DIAMETER_TOO_BUSY
Level 3 MPE Only	DefaultRule8	Reject Gx CCR-I messages with DIAMETER_TOO_BUSY
	DefaultRule9	Reject Gxx CCR-I messages with DIAMETER_TOO_BUSY
	DefaultRule10	Reject Gy CCR-I messages with DIAMETER_TOO_BUSY
	DefaultRule11	Reject Rx AAR-I messages with DIAMETER_TOO_BUSY
	DefaultRule12	Reject Sh PNR messages with DIAMETER_TOO_BUSY
	DefaultRule13	Reject Sy SNR messages with DIAMETER_TOO_BUSY

Use the **Load Shedding Configuration** section of the **Advanced Configuration** page to edit, reorder, or add new rules at each of the three levels of busyness for an MPE device based on the amount of backlog. To reach a configured level of busyness:

- The backlog of outstanding messages in a node crosses a pre-defined threshold for the level.
- The backlog has been above the busyness level threshold for a minimum amount of time.

At each level, the MPE device can be configured to take one of the following actions (referred to as rules) until the busyness level clears:

- Reject new messages with a specific result code (the default is DIAMETER_TOO_BUSY).
- Drop the message.

Note: Configuration keys must also be used in configuring load shedding options. Contact MOS for assistance.

Configure the load shedding rules as follows:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the MRA device to be enabled for load shedding.
   The **Policy Server Administration** page opens.
3. Select the **MRA** tab.
   The MRA Administration page is displayed.
4. Click **Advanced**.

   Advanced configuration settings are displayed and can be edited.

5. On the **Load Shedding Configuration** section of the page, **Enabled** is selected by default.
6. Configure the rules for the busyness levels:
   a) Click the arrow next to the level to expand the level.
   b) Click **Add**.
      The **Add Load Shedding Rule** dialog appears.
   c) Enter the values for the load shedding rule:
      - **Name** — Name of the rule.
      - **Application** — Select the application the rule applies to. You can select **Gx**, **Gy**, **Gxx**, **Rx**, **Sh**, or **Sy**.
      - **Message** — Type of message the rule applies to (which depends on the application chosen).
      - **Request Types** (available depending on the message selected) — Select the Request-Type attribute-value pairs (AVPs) that the message must contain. You can select **Initial**, **Update**, and/or **Terminate**. These fields can only be selected when a Gx application and a CCR message are configured.
      - **APNs** — Enter a CSV list of one or more access point names that the message must contain.
      - **Action** — Select the action to be taken if the criteria are met for the busyness level. You can select **Drop** (drop the message); **Answer With** (select a code from the drop-down list), or **Answer With Code** (enter a code) and **Vendor ID** (enter a vendor ID).

   d) Click **Save** (or **Cancel** to discard your changes).
      The rule is displayed in the table.
7. Once a rule is defined, you can optionally clone, edit, or delete it by selecting it and clicking the appropriate button.
8. When finished making changes, click **Save** (or **Cancel** to discard your changes).

The settings are applied to the selected MPE device.

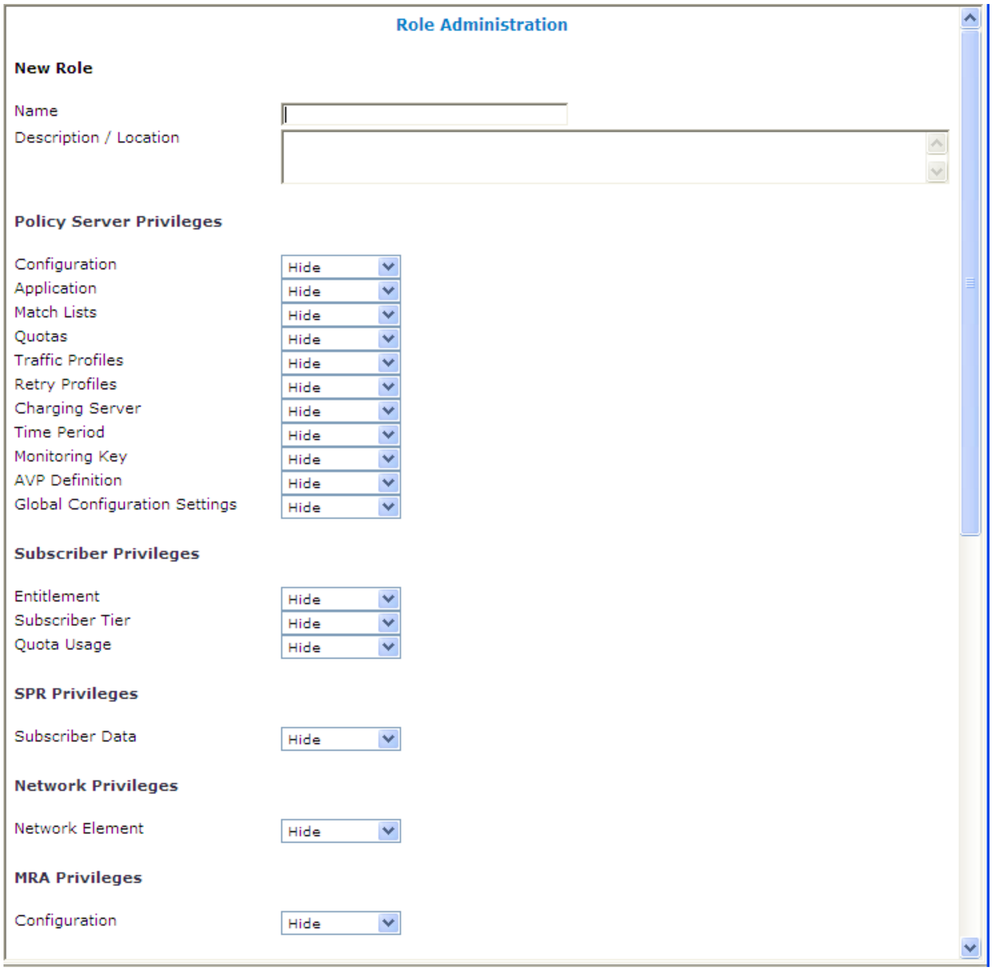
Role and Scope Configuration

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.

MRA Role Configuration

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

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



Role Administration

New Role

Name	
Description / Location	

Policy Server Privileges

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

Subscriber Privileges

Entitlement	Hide
Subscriber Tier	Hide
Quota Usage	Hide

SPR Privileges

Subscriber Data	Hide

Network Privileges

Network Element	Hide

MRA Privileges

Configuration	Hide

Figure 11: New Role Page

3. Enter the following information:
   a) **Name** — The name for the new role.
   b) **Description/Location** (optional) — Free-form text.
   c) **MRA Privileges** — There are three types of privileges for MRA configuration: Hide, Read-Only and Read-Write.

   - **Hide** — No operation can be done on MRA configuration.
   - **Read-Only** — Only read operations can be done on MRA configuration (that is, settings can be viewed but not changed).
   - **Read-Write** — Both read and write operations can be done on MRA configuration (that is, settings can be viewed and changed).

4. When you finish, click **Save** (or **Cancel** to discard your changes).
   Privileges are assigned to the role.

MRA Scope Configuration

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

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

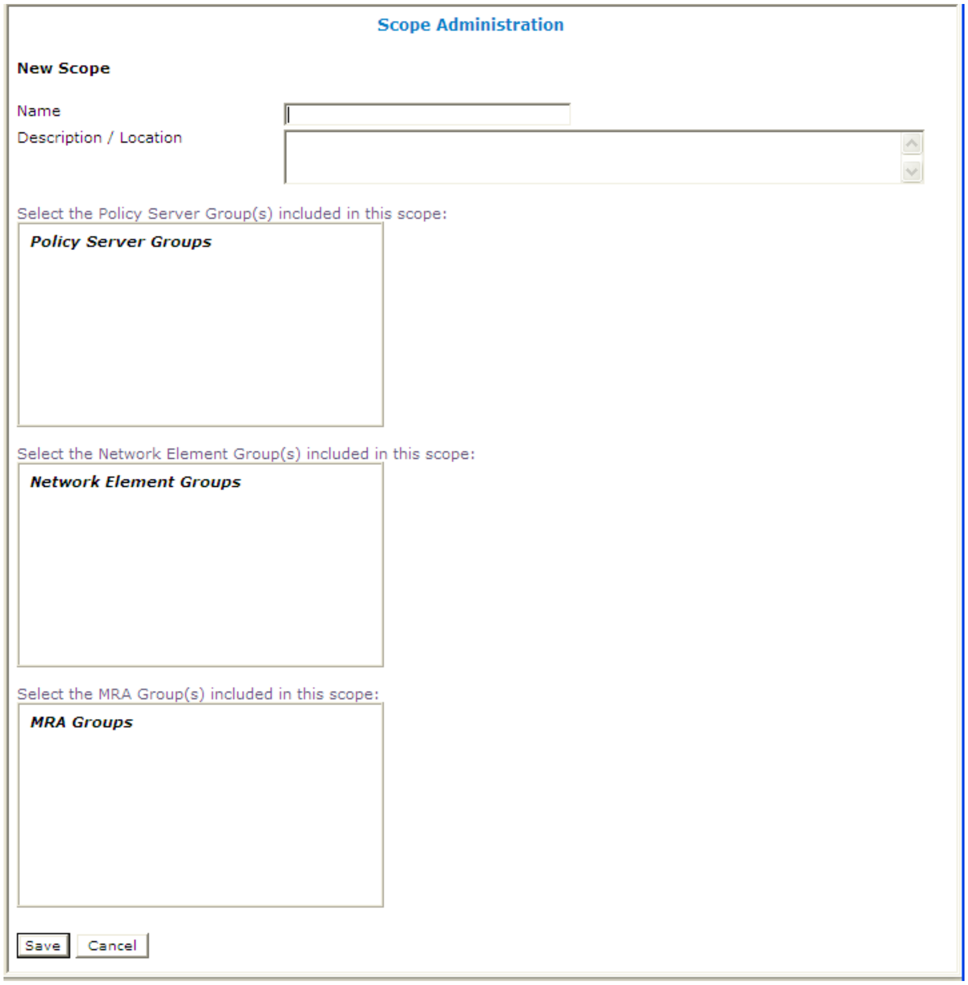

Scope Administration
New Scope
Name
Description / Location
Select the Policy Server Group(s) included in this scope:
Policy Server Groups
Select the Network Element Group(s) included in this scope:
Network Element Groups
Select the MRA Group(s) included in this scope:
MRA Groups
Save
Cancel

Figure 12: Create Scope Page

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

The scope is defined.

Configuring Stateless Routing

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

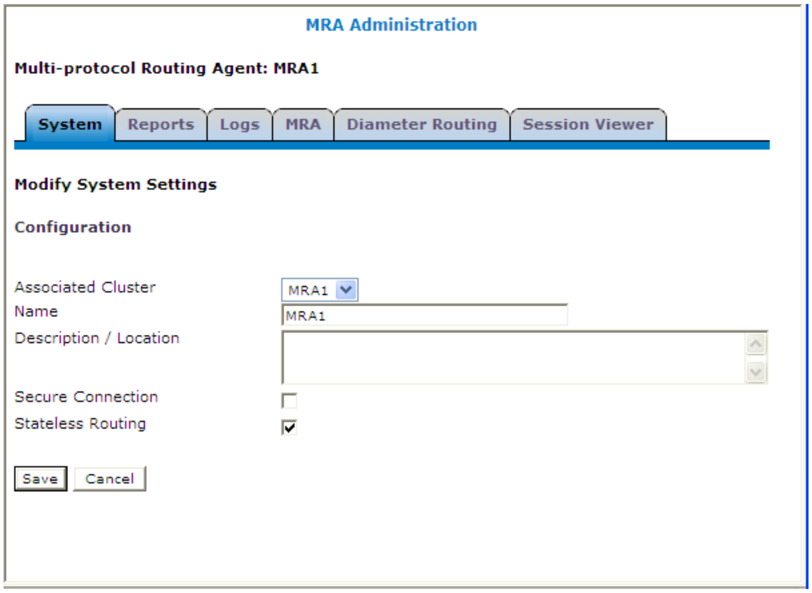
Using stateless routing, the MRA establishes a diameter connection with every peer that is defined in the Diameter Peer Table, where a peer consists of a name, IP address, diameter realm, diameter identity, and port. A route consists of a diameter realm, application ID, user ID, action, and server ID.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

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

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

Enabling Stateless Routing

To hide configuration relevant to a stateful MRA device in the CMP display, select **Stateless Routing** (*Figure 13: Enabling Stateless Routing* shows an example).



Multi-protocol Routing Agent: MRA1

Modify System Settings

Configuration

Associated Cluster: MRA1

Name: MRA1

Description / Location:

Secure Connection: □

Stateless Routing: ☑

Figure 13: Enabling Stateless Routing

Modifying the Stateless Migration Mode in an Existing MRA

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

To enable and disable the migration mode setting:

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

The MRA device is put into migration mode.

Loading MPE/MRA Configuration Data when Adding Diameter Peer

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

Configuring Diameter 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.

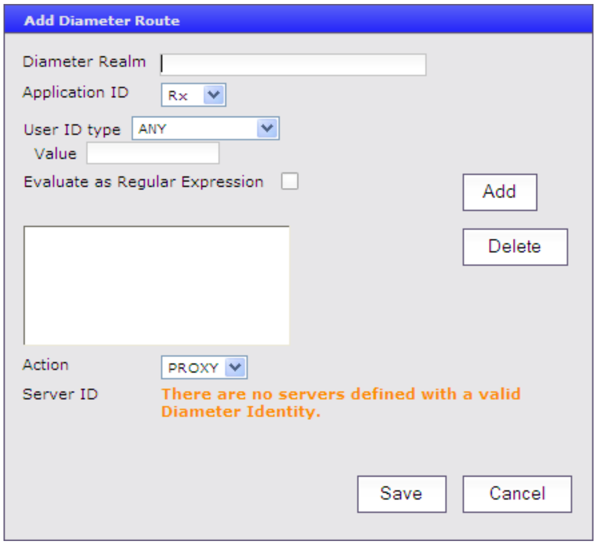
To configure the **Diameter route** table:

1. From the **Policy Server** 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.
   The **Policy Server Administration** page opens in the work area.
3. On the **Policy Server Administration** page, select the **Diameter Routing** tab.
   The Diameter Routing configuration settings are displayed.
4. Click **Modify Routes**.

   The **Modify the Diameter Route Table** page opens.

   The functions available from this table are as follows:

   - **To add a route to the table** — Click **Add**; the **Add Diameter Route** window opens:



Diameter Realm

Application ID: Rx

User ID type: ANY

Value

Evaluate as Regular Expression □

Action: PROXY

Server ID: There are no servers defined with a valid Diameter Identity.

The fields are as follows:

- **Diameter Realm** — For example, **`galactel.com`**.
- **Application ID** — Select **Rx** (the default), **Gq**, **Ty**, **Gx**, **Gy**, **Gxx**, **Sh**, **Sy**, or **All**.

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

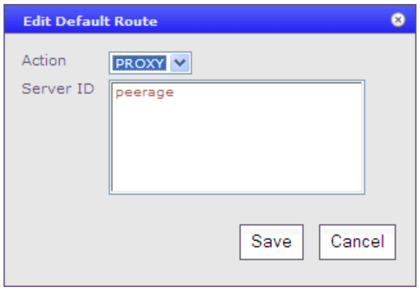
- **User ID type** — Select **ANY** (the default), **E.164(MSISDN)**, **IMSI**, **IP**, **NAI**, **PRIVATE**, **SIP_URI**, or **USERNAME**.
- **Value** — Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); use an asterisk (*) as a wildcard character.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

When you finish, click **Save** (or **Cancel** to abandon your changes).

- **To change the order of a route in the table** — Select an existing route in the table and click **Up** or **Down**. The order of routes is changed.
- **To clone a route in the table** — Select an existing route in the table and click **Clone**; the **Clone Diameter Route** window opens with that route's information filled in. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
- **To edit a route in the table** — Select an existing route in the table and click **Edit**; the **Edit Diameter Route** window opens with that route's information. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
- **To delete a route from the table** — Select one or more existing routes and click **Delete**; you are prompted, "Are you sure you want to delete the selected Diameter Route(s)?" Click **Delete** (or **Cancel** to cancel your request). The route entry is removed.

5. To define the default route, click **Edit** in the **Default Route** section.
   The Edit Default Route window opens:

   Action: PROXY

   Server ID: peerage

   Enter the default action (**PROXY**, **RELAY**, or **LOCAL**) and peer server ID. When you finish, click **Save** (or **Cancel** to discard your changes).

6. To delete the default route, click **Delete**.
7. When you finish, click **Save** (or **Cancel** to discard your changes).

The Diameter routes are configured.

MRA Advanced Configuration Settings

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

Configuring MRA Session Clean Up Settings

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

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

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

To customize stale session cleanup:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA device.
   The **MRA Administration** page opens.
3. On the **MRA Administration** page, 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 5: 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.
Max Iteration Burst Size	Define the number of iterations which can be processed before the rate is limited. This is the Token Bucket size. The default is 1000 iterations. The valid range is 1 to 1000 iterations. **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. Click **Save** (or **Cancel** to discard changes).
   The settings are applied to the MRA.

Working with Stateful MRAs

Stateful MRAs 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.

See *Configuring Stateless Routing* for more information.

Redirecting Traffic to Upgrade or Remove an MRA

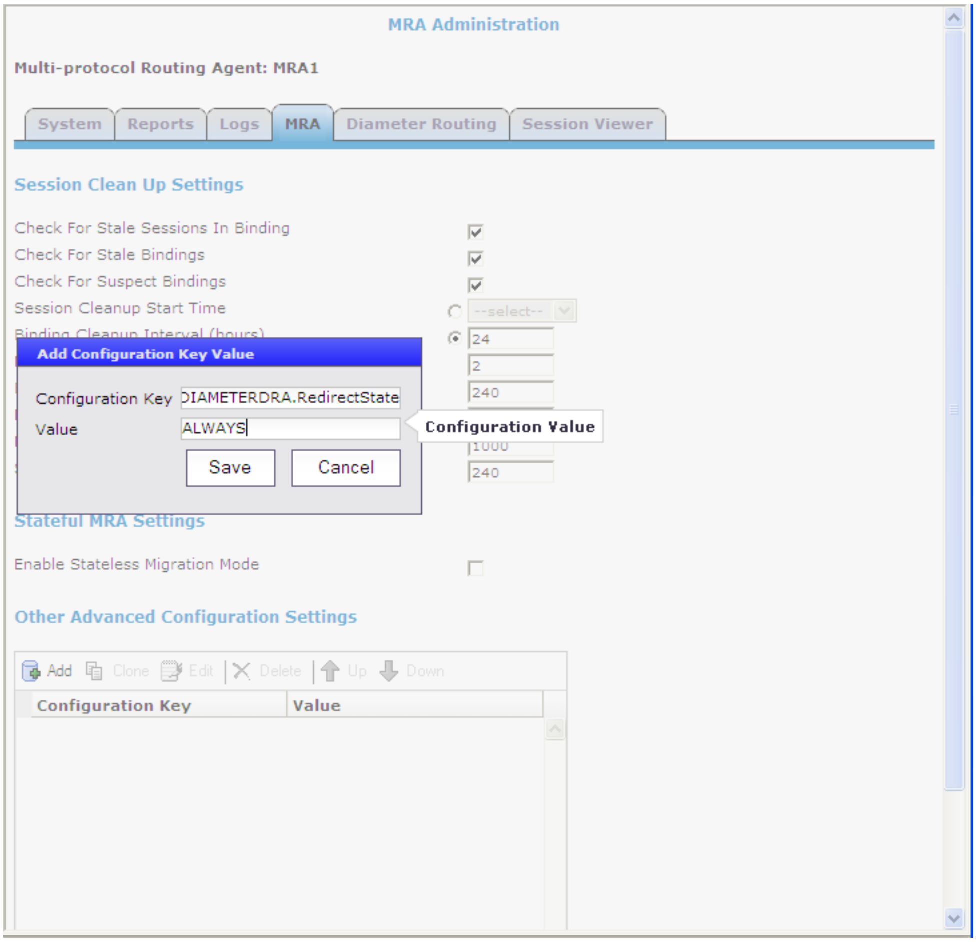
When the software for an MRA needs to be upgraded or an MRA needs to be removed from an MRA cluster, the traffic or potential traffic must be redirected to the other MRA within the cluster, and the current sessions released. To do this, traffic on clustered MRAs is redirected on to another MRA, allowing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

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

Changing Redirect States

To change the redirect state of an MRA device:

1. In the **MRA** section of the navigation bar, click **Configuration**.
2. Select an MRA. The **MRA Administration** page displays information about the selected MRA.
3. On the **MRA** tab, click **Advanced**.
4. In the **Other Advanced Configuration Settings** section, click the **Add** icon in the table. The **Add Configuration Key Value** window opens (*Figure 14: 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

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 14: Add Configuration Key Value Window

The redirect configurable variable is DIAMETERDRA.RedirectState, which indicates the redirect state of the MRA. Changing this variable to NORMAL will stop the release process. Valid values are:

- **NORMAL** (the default) — The MRA redirects CCR-I messages only when the DRMA link between the clustered MRAs is down and the subscriber does not have an existing binding on the MRA that first receives the CCR-I.
- **ALWAYS** — The MRA always redirects CCR-I messages to the MRA it is clustered with for subscribers that do not have existing bindings, whether the DRMA link is active or not. An MRA in this state is not able to create new bindings.
- **NEVER** — The MRA never redirects messages to the MRA it is clustered to, whether the DRMA link is active or not.

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

Releasing Active Sessions

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

The release configurable variables are:

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

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 Algov1 (Algorithm version1). To disable this functionality, the configuration needs to be set to Legacy.

Reversing Cluster Preference

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

To reverse cluster preference:

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

The cluster preferences are reversed.

Forcing a Server into Standby Status

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

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

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

CAUTION

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

To force a server into standby status:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Topology Configuration** page opens, displaying a cluster settings table listing information about the clusters defined in the topology.
2. In the cluster settings table, in the row listing the cluster containing the server you want to force into standby status, click **View**.
   The **Topology Configuration** page displays information about the cluster.
3. Select the server. Click **Modify Server-A** or **Modify Server-B**, as appropriate.
4. Select **Forced Standby**.
5. Click **Save** (or **Cancel** to abandon your request).
   The page closes.

The server is placed in standby status.

Configuring Topology Hiding for the Gx Application

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

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

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

To configure topology hiding:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA device.
   The **MRA Administration** page opens.
3. On the **MRA Administration** page, select the **MRA** tab.
   The current MRA configuration settings are displayed.
4. On the **MRA** tab, 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** (or **Cancel** to discard changes).
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 14: Add Configuration Key Value Window*). Add the following configuration keys to the **Add Configuration Key Value** window:

   Table 6: Topology Hiding Configuration Keys

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

9. Click **Save** (or **Cancel** to discard changes).
   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.

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. On the **MRA Administration** page, select the **MRA** tab.

The current MRA configuration settings are displayed.

4. On the **MRA** tab, 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** (or **Cancel** to discard changes).
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 14: 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 quired.

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

   Table 7: Topology Hiding Configuration Keys

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

9. Click **Save** (or **Cancel** to discard changes).
   The topology hiding settings are applied to the MRA.

Chapter 4

Monitoring the MRA

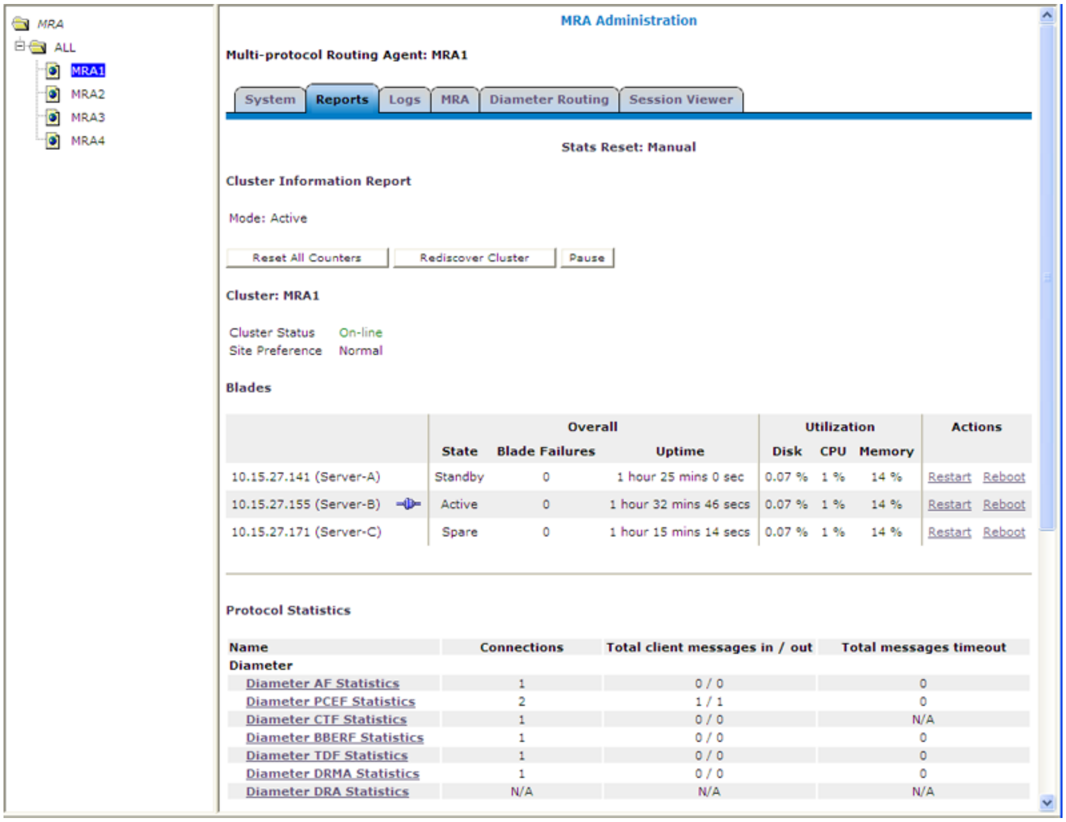
Topics:

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

- Cluster and blade information
- DRMA information
- Event logs

Displaying Cluster and Blade Information

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



MRA Administration

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 15: Cluster, Blade, and Diameter Information

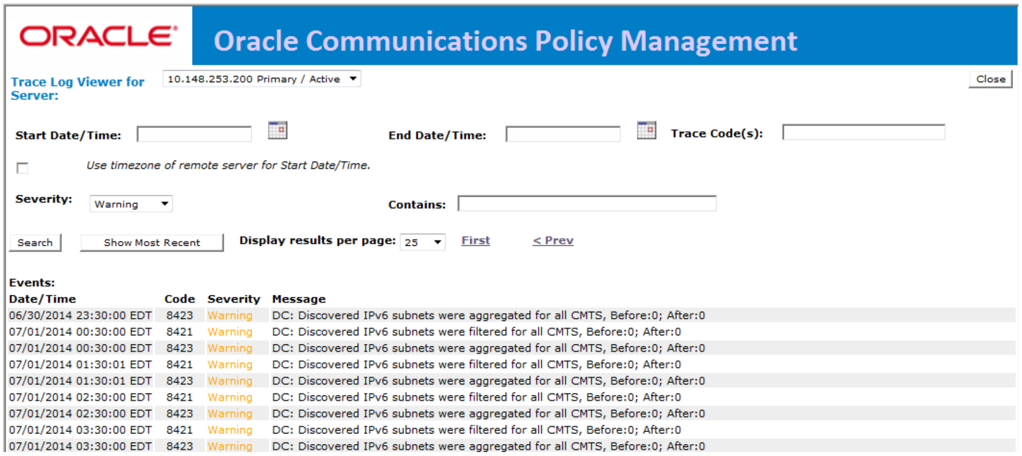
The following is a list of Diameter statistics:

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

For a detailed breakdown of a statistic, click the statistic. For descriptions of the statistics available for display, refer to *Mapping Reports Display to KPIs*.

Viewing Trace Logs

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



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 16: MRA Trace Log

KPI Dashboard

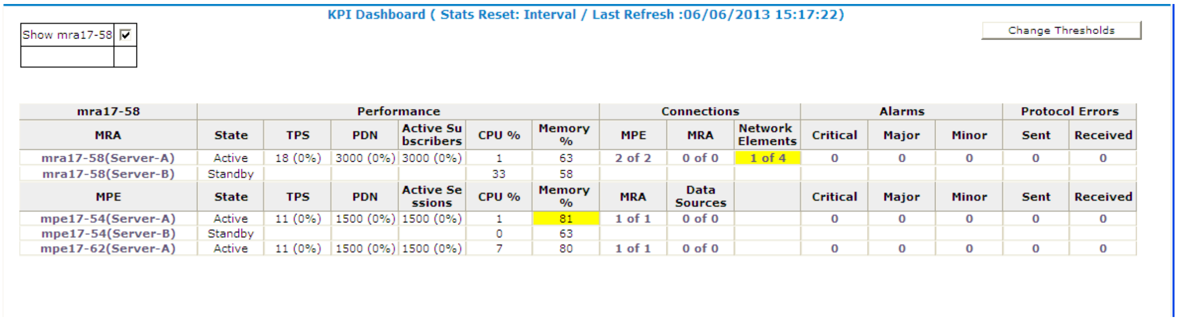
The KPI dashboard provides a multi-site, system-level, summary of performance and operational health indicators in the CMP web based GUI. The display includes indicators for:

- 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 ☑

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 17: KPI Dashboard

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

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

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

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

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

Mapping Reports Display to KPIs

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

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

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

Table 8: 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:			
Policy TDF session	Y	N	
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 9: 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 10: Diameter Application Function (AF) Statistics

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

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

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

Table 11: Diameter Policy Charging Enforcement Function (PCEF) Statistics

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

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

Table 12: Diameter Charging Function (CTF) Statistics

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

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

Table 13: Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics

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

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

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

Table 14: Diameter TDF Statistics

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

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

Table 15: Diameter Sh Statistics

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

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

Table 16: Diameter Distributed Routing and Management Application (DRMA) Statistics

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

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

Display	MPE	MRA	Name
DBR-S messages timeout	N	Y	
DBA-S success messages received/sent	N	Y	
DBA-S failure messages received/sent	N	Y	
RUR messages received/sent	Y	Y	RURRecv Count\ RURSend Count
RUR messages timeout	Y	Y	RURTimeout Count
RUA success messages received/sent	Y	Y	RUARecv Success Count\ RUASend Success Count
RUA failure messages received/sent	Y	Y	RUARecv Failure Count\ RUASend Failure Count
LNR messages received/sent	Y	Y	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			
SQA messages received/sent			
SQA messages timeout			
Session found received/sent			
Session not found received/sent			
Diameter DRMA connections			

Note: Diameter DRA statistics apply only to MRA devices.

Table 17: 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 18: Diameter Sy Statistics

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

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

Table 19: RADIUS Statistics

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

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

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

Table 20: 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 20: Diameter Latency Statistics

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

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

Table 21: 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 22: Diameter Protocol Error Statistics

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

Table 23: Diameter Connection Error Statistics

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

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

Table 24: LDAP Data Source Statistics

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

Table 25: Sh Data Source Statistics

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

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

Table 26: 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

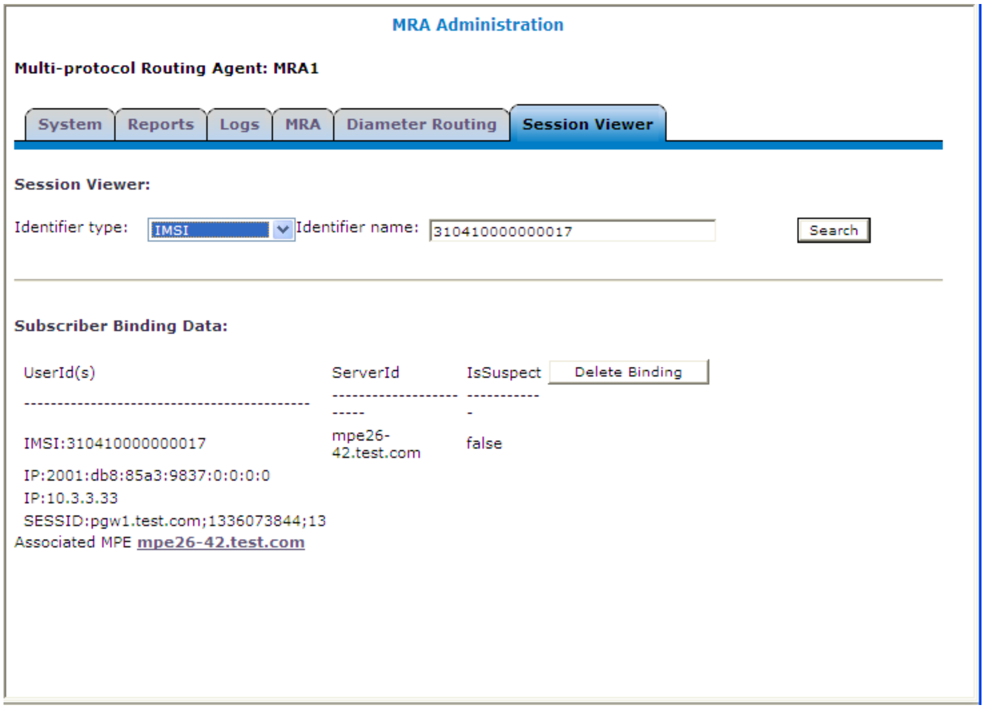
Table 27: KPI Interval Statistics

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

The Subscriber Session Viewer

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

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



MRA Administration

Multi-protocol Routing Agent: MRA1

Session Viewer:

Identifier type: IMSI Identifier name: 310410000000017

Subscriber Binding Data:

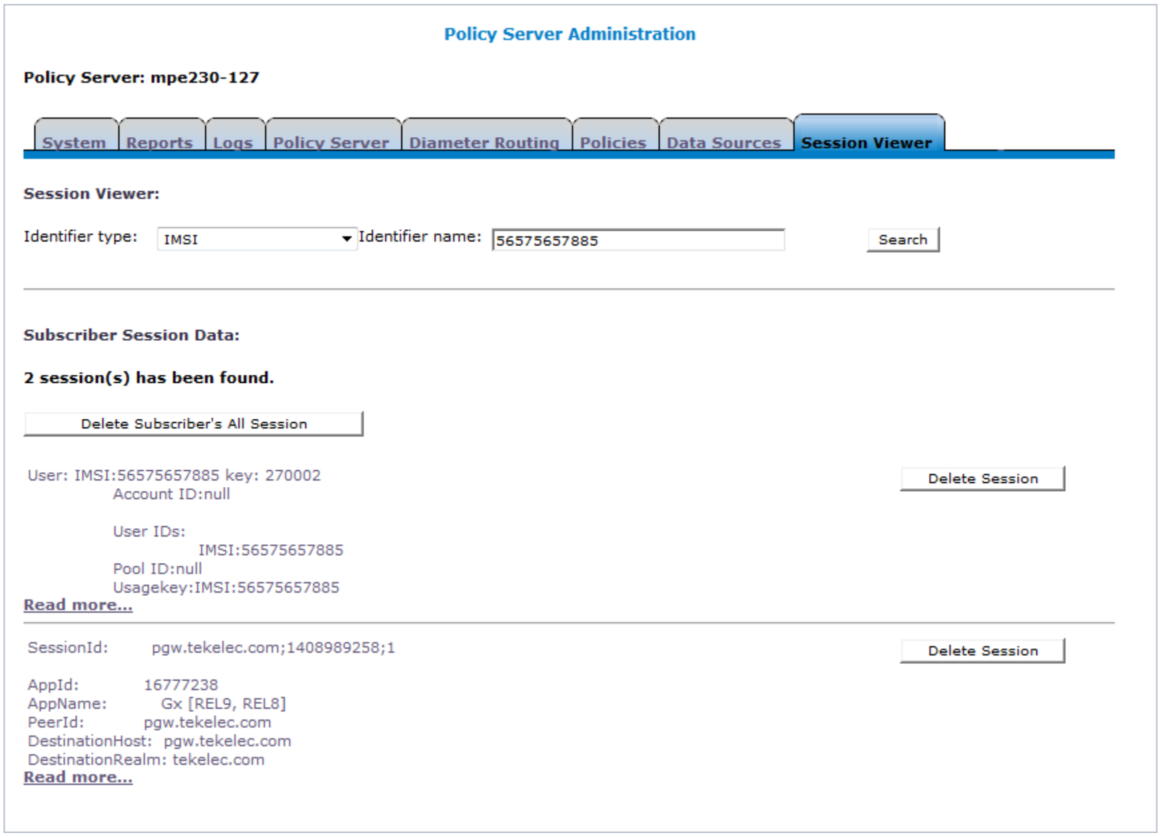
UserId(s)	ServerId	IsSuspect
IMSI:310410000000017 IP:2001:db8:85a3:9837:0:0:0:0 IP:10.3.3.33 SESSID:pgw1.test.com;1336073844;13	mpe26-42.test.com	false

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
Read more...
```

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

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

The MRA device is listed by peer ID.

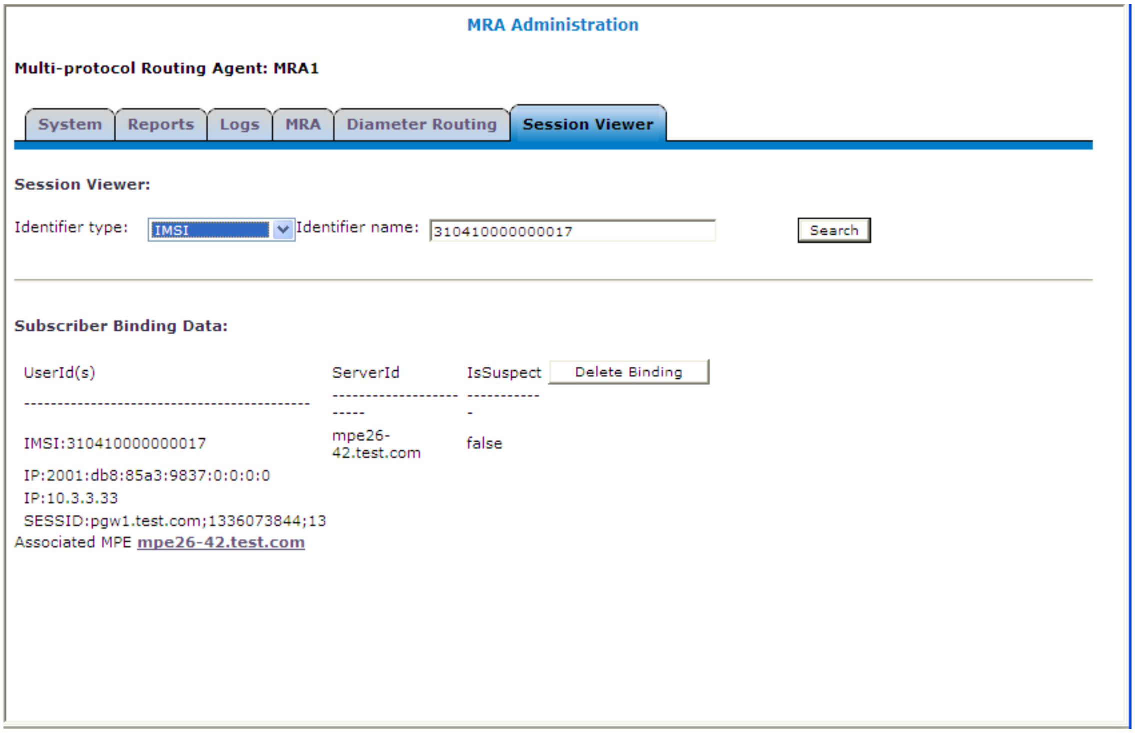
If no session data is available, the CMP returns the following message:

> There are no sessions available for the subscriber.

Viewing Session Data from the MRA

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

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



MRA Administration

Multi-protocol Routing Agent: MRA1

Session Viewer:

Identifier type: IMSI Identifier name: 310410000000017

Subscriber Binding Data:

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

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

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

Deleting a Session from the Session Viewer Page

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

CAUTION

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

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.

E

E.164

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

G

GUI

Graphical User Interface

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HSS

Home Subscriber Server

A central database for subscriber information.

HTTP

Hypertext Transfer Protocol

I

IMSI

International Mobile Subscriber Identity

A unique internal network ID identifying a mobile subscriber.

International Mobile Station Identity

IPv4

Internet Protocol version 4

IPv6

Internet Protocol version 6

K

KPI

Key Performance Indicator

M

MPE

Multimedia Policy Engine

A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a

M

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

MRA

Multi-Protocol Routing Agent

Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server devices.

P

PCC

Policy and Charging Control

PDN

Packet Data Network

A digital network technology that divides a message into packets for transmission.

R

RADIUS

Remote Authentication Dial-In User Service

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

realm

A fundamental element in Diameter is the realm, which is loosely referred to as domain. Realm IDs are owned by service

R

providers and are used by Diameter nodes for message routing.

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.