Policy Management

Policy Front End Wireless User's Guide

Release 12.4
E89535-02
October 2019

Policy Management Policy Front End Wireless User's Guide, Release 12.4

E89535-02

Contents

4 About MRA Monitoring

About This Guide

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

How This Guide is Organized

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

- About This Guide contains general information about this guide, the organization of this guide, and how to get technical assistance.
- #unique_10 contains an overview of the guide, the Distributed Routing and Management Application (DRMA) protocol, and the Graphical User Interface (GUI).
- About Configuring a CMP System, MRA and MPE Devices describes how to configure the Configuration Management Platform CMP to manage the MRA, how to modify system settings and groupings, configuring role and scope, working with advanced MRA settings, and hiding the Gx application.
- #unique_12 describes associating network elements with an MRA, working with Stateful MRA servers, configuring MPE/MRA Pools and setting up Diameter Peer Tables, using Stateless Routing and Configuring for RADIUS.
- #unique_13 describes how to monitor cluster and server information, DRMA information, and event logs.

Scope and Audience

This guide is intended for service personnel who are responsible for configuring and monitoring MRAdevices in Policy Management systems.

Related Publications

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

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support

My Oracle Support is your initial point of contact for all product support and training needs. A representative at Customer Care Center can assist you with My Oracle Support registration.

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

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

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

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support 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.

List of Figures

List of Tables

1 Introduction

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

Multi-Protocol Routing Agent Devices

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

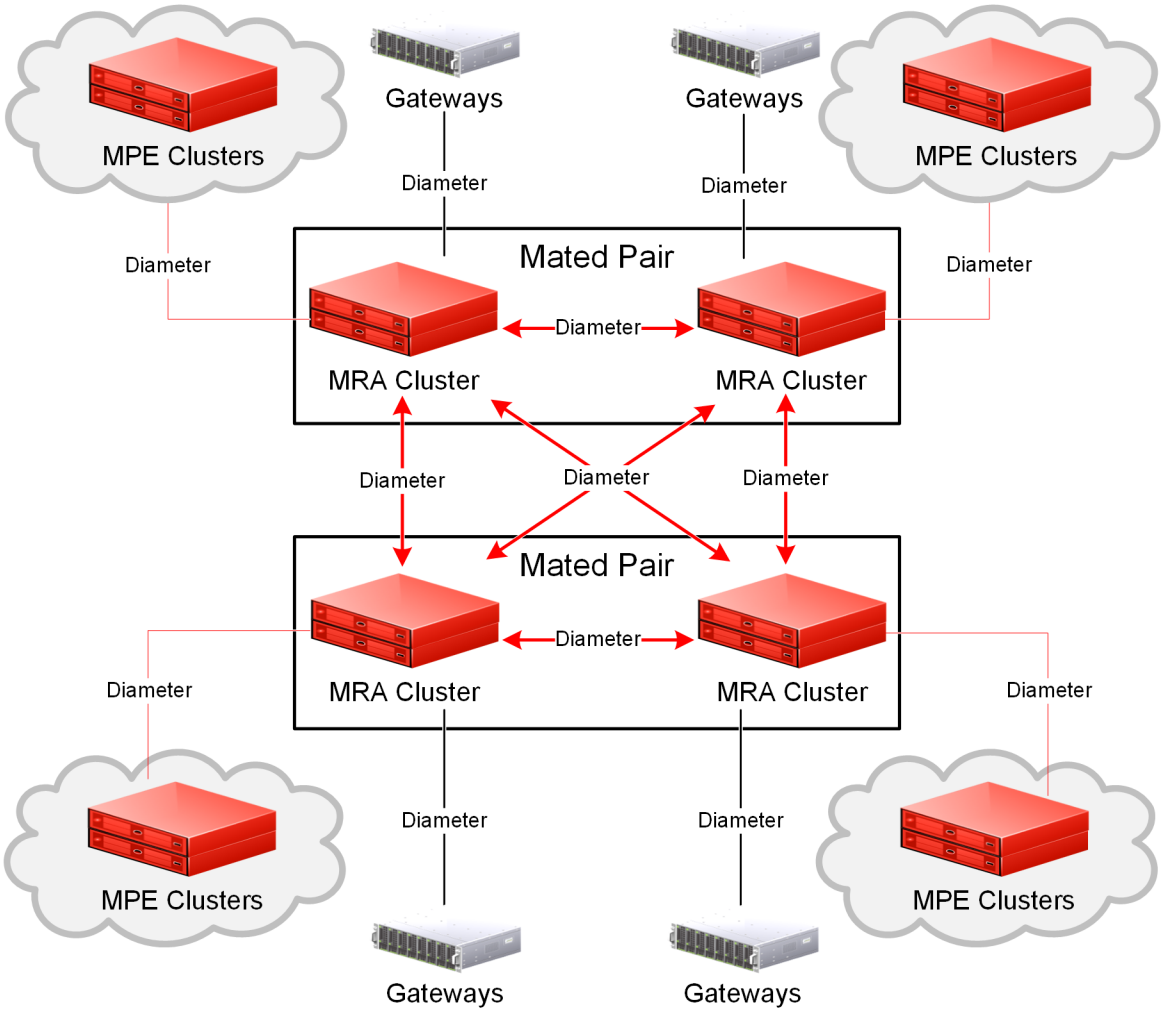
An MRA server correlates traffic between different sessions for a subscriber ensuring that all reference points reach the same MPE server when multiple and separately addressable MPE clusters are deployed.

An MRA server implements the proxy (PA1 variant) DRA functionality whereby all Diameter Policy and Charging Control (PCC) application messages are proxied through an MRA server.

When an MRA server 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 servers in the Policy Management network for a binding using the proprietary Distributed Routing and Management Application (DRMA) protocol. If another MRA server has the binding, the MRA server routes the request to it. If no other MRA server has a binding, the MRA server that received the request creates one.

An MRA server 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 1-1 Typical MRA Network



Distributed Routing and Management Application (DRMA) Protocol

The **DRMA** protocol is an Oracle proprietary **Diameter** based protocol that allows multiple MRA clusters in the network to communicate and share Diameter Routing Agent (**DRA**) binding information. **DRMA** ensures that all the **Diameter** sessions for a subscriber are served by the same MPE device. As a result, MRA devices can query one another for binding information by sending a **DRA**-Binding-Request (DBR) command and receiving a **DRA**-Binding-Answer (DBA) in response.

Backup MRAs, Associated MRAs, and Mated Pairs

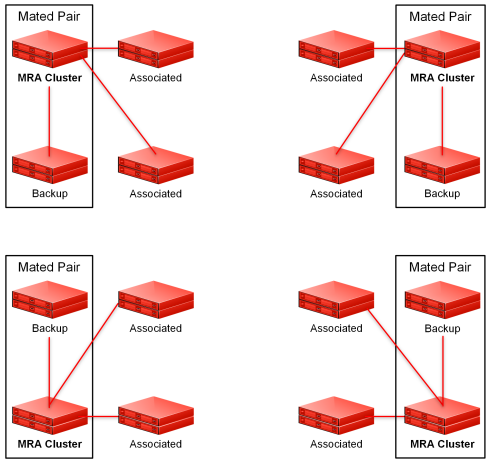
Each MRA exists as a cluster that consists of two servers, active and standby. Both servers in a cluster share a Virtual IP Address (VIP) that points to whichever server is active.

A backup MRA cluster shares a common pool of MPE servers with a primary MPE cluster. All of the MPE servers in the pool of a given MRA cluster will have backup connections to the backup MRA cluster. An MRA cluster and its backup are considered a mated pair.

An associated MRA cluster is one that is not the backup MRA cluster, but exists as part of a Diameter Route. (See Configuring Diameter Realm Based Peer Routes for more information on associated MRA servers.)

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 1-2 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 1-2 Backup and Associated MRA Clusters and Mated Pairs



2

About Configuring a CMP System, MRA and MPE Devices

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

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

About Configuration Management Platform's Role in Managing the MRA

The Multi-Protocol Routing Agent,MRA, is a standalone entity that uses the Oracle Communications Policy Management Configuration Management Platform (CMP) system. The CMP is used to manage all MRA functions. Before this can occur, the CMP must be configured to:

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

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

Creating an MRA Group

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

To create an MRA group:

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.

The MRA Administration page opens in the work area.

3. Click **Create Group**.

   The Create Group page opens.

4. Enter the name of the new MRA group.

   The name:

   - Can be up to 250 characters long
   - Must not contain spaces
   - Can contain the following characters:
     - Alphabetic characters
     - Numeric characters
     - Period
     - Hyphen (-)
     - Underscore(_)

5. Click **Save**.

The MRA group is created.

Deleting an MRA Group or Sub-group

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

> **Note:**
>
> Deleting an MRA group also deletes any associated sub-groups. However, any MRA cluster profiles associated with the deleted groups or sub-groups remain in the ALL group.

> **Note:**
>
> You cannot delete the **ALL** group.

To delete an MRA group or sub-group:

1. From the **MRA** section of the navigation pane, select **Configuration** which displays a list of the MRA groups; the initial group is **ALL**.
2. Select the MRA group or subgroup from the content tree.

   The contents of the selected MRA group are displayed.

3. Click **Delete** which opens a confirmation message.
4. Click **OK** to complete the procedure.

The MRA group or sub-group has been deleted.

Configuring the CMP System to Manage an MRA Cluster

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

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

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

1. From the **Help** navigation pane, select **About**.

   The About page opens, displaying the CMP software release number.
2. Click the **Mode** button.

   Consult with My Oracle Support for information about this button.

   The Mode Settings page opens.
3. On the bottom of the page, select **Manage MRAs**.
4. Click **OK** which closes the browser page and logs you out.
5. Refresh the browser page.

   The Welcome admin page is displayed.

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

Configuring MRA Protocol Options

MRA must be configured to work with protocols and capabilities, such as Subscriber Indexing, APN override, Diameter, S9, RADIUS, and others capabilities to function in your network. To configure protocol options on an MRA device:

1. From the **MRA** section of the navigation pane, select **Configuration**.
2. From the content tree, select the MRA device that requires protocol configuration.

   The MRA Administration page opens.
3. Select the **MRA** tab that displays the configuration options.
4. Click **Modify** and define options as necessary.

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

Table 2-1 MRA Protocol Configuration Options

Attribute	Description
Subscriber Indexing	**Note:** The indexing parameters used depend on what user IDs are needed for correlating various messages to ensure they all end up on the same MPE device for the same user. If you are unsure which indexing methods to configure, contact My Oracle Support (https://support.oracle.com).
Index by IPv4	Select if the MRA devices in the association should index by IPv4 address.
Index by IPv6	Select if the MRA devices in the association should index by IPv6 address.
Index by Username	Select if the MRA devices in the association should index by account ID.
Index by NAI	Select if the MRA devices in the association should index by network access ID.
Index by E.164 (MSISDN)	Select if the MRA devices in the association should index by E.164 phone number.
Index by IMSI	Select if the MRA devices in the association should index by IMSI number.
Index by Session ID	Select if the MRA devices in the association should index by session ID.

Table 2-1 (Cont.) MRA Protocol Configuration Options

Attribute	Description
Overrides by APN	Select to configure an alternate subscriber indexing by IP address, Username, NAI, E.164 (MSISDN) and IMSI for a specific access point name (APN). a. In the Overrides by APN section, click **Add**. b. Enter the APN name. **Note:** APN names are alphanumeric and have the following restrictions: • A 255 character limit • No spaces or special characters such as asterisks • Can contain hyphens (-) and periods (.) but must not begin or end with a hyphen or period Example name: `pdn1.examplecorp.com` c. Select one or more of the following: • **Index by IPv4** • **Index by IP-Domain-Id** • **Index by IPv6** • **Index by Username** • **Index by NAI** • **Index by E.164 (MSISDN)** • **Index by IMSI** • **Index by Session ID** d. click **Save** You can create APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.
Protocol Timer Profile	The timer profile to use.
S9	
Primary DEA	If one or more Diameter Edge Agents is defined, you can select the primary agent from the list. For information on defining a DEA, see Configuring Diameter Peers.
Secondary DEA	If multiple Diameter Edge Agents are defined, you can select the secondary agent from the list. If you select both primary and secondary DEAs, the MRA device establishes a connection to both DEAs. If the primary connection is down, the MRA device sends messages over the secondary connection; after the primary connection is back up, communication reverts back to it.

About Modifying, Grouping, or Deleting MRA devices

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

Defining an MRA Cluster Profile

In order to get accurate session analysis, log, error, and reporting information, you must define certain parameters of an MRA device to give a specific profile for each MRA cluster you are managing.

To define an MRA cluster profile:

1. From the **MRA** section of the navigation pane select **Configuration**.

   The content tree displays a list of MRA groups; the initial group is **ALL**.

2. From the content tree, select the **ALL** group.

   The MRA Administration page opens in the work area.

3. Click **Create Multi-protocol Routing Agent**.

   The New MRA page opens.

4. Enter information for the MRA cluster:

   a. **Associated Cluster** (required): Select the MRA cluster from the list.

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

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

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

      Enter up to 250 characters.

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

      > **Note:**
      >
      > The default is a non-secure (HTTP) connection.

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

      The default is stateful routing.

5. Click **Save**.

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

Modifying an MRA Cluster Profile

As your network changes, is reconfigured, or adds new capabilities, such as Diameter and its associated interfaces, you must modify your existing MRA configuration to meet these needs.

To modify MRA cluster profile settings:

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.

2. Select the **MRA** cluster profile located in the content tree.

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

The MRA cluster profile settings are modified.

Removing an MRA Cluster Profile from an MRA Group

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

> **Note:**
>
> Removing an MRA cluster profile from an MRA group does not delete the MRA cluster profile from the ALL group, so it can be used again if needed. But removing an MRA cluster profile from the ALL group will delete it from all other groups in the system.

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

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

   The MRA cluster profile is removed from the group.

Reversing Georedundant Cluster Preference

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

To reverse a georedundant cluster preference:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the cluster you want to modify.

   The Topology Configuration page opens, displaying information about the cluster.
4. Click **Modify Cluster Settings**.

5. In the **Cluster Settings** section of the page:
   - To set the preference to reverse (where the active Site 1 becomes the inactive site and Site 2 becomes the active site), toggle to **Reverse**.
   - To set the preference to normal (where the active Site 2 becomes the inactive site and Site 1 becomes the active site), toggle to **Normal**.
6. Click **Save**.

The cluster preferences are reversed.

Changing Server Status to Forced Standby

You can change the status of a server in a cluster to forced standby. A server placed into forced standby status cannot become active. You would do this, for example, to an active server prior to performing maintenance on it. Oracle recommends this method to switch over from an active server or to resolve issues where more than one server in a cluster is active.

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

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

> **Caution:**
>
> If you set all servers in a cluster into forced standby status, you can trigger an outage.

To change a server to forced standby status:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the cluster you want to change.

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

The server status is changed to forced standby.

Setting Up a Non-CMP Cluster

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

- The server software is installed on all servers in the cluster.

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

To set up a non-CMP cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

   The **Cluster Configuration** page opens; the initial group is **All Clusters**.

2. From the work area, select **Add MPE/MRA/Mediation Cluster**.

   > **Note:**
   >
   > The list of available cluster types to add to the topology depends on the CMP modes configured. See the *CMP Wireless User's Guide* for more information.

   The Topology Configuration page opens.

3. In the **Cluster Settings** section of the page:

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

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 250 characters.

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

      Available options are:

      - MPE (default)
      - MRA
      - Mediation

      > **Note:**
      >
      > The list of available application types depends on the CMP modes configured. See the *CMP User's Guide* for more information.

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

      Available options are:

      - **C-Class** (default)—HP ProLiant BL460 Gen8 server
      - **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 Gen8
      - **Oracle RMS**—Oracle Server X5-2
      - **RMS** (rack-mounted server)—HP ProLiant DL380 Gen8 server
      - **VM** (virtual machine)
      - **VM(Automated)** (VM managed by NF Agent)
        See Setting Up a VM (Automated) Non-CMP Cluster for details on adding a VM (Automated) cluster.

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

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

The signaling VIP is the IP address a PCEF device uses to communicate with the cluster. A non-CMP cluster supports redundant communication channels, named SIG-A, SIG-B, or SIG-C for carriers who use redundant signaling channels.

The New Signaling VIP dialog appears.

i. Enter the **Signaling VIP** address and the **Mask**.
This is the IP address the CMP server uses to communicate with an external signaling network.

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

ii. Select the **Interface** from the list.
Available options are:

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

iii. Click **Save**.
The **Signaling VIP** address and **Mask** are saved.

f. Repeat the process for any remaining Signaling VIPs.

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

i. Enter the **OAM VLAN ID**.
The default value is 3.

ii. Enter the **SIG-A VLAN ID**.
The default value is 5.

iii. (Optional) Enter the **SIG-B VLAN ID**.
The default value is 6.

iv. (Optional) Enter the **SIG-C VLAN ID**.
The default value is 7.

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

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

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

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

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

The Add New IP dialog box appears.

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

The IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

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

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

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

The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

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

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

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

5. (Optional) Click **Add Server-B** and enter the information for the standby server of the cluster.

Server-B is defined for the cluster.

6. Click **Save**.

A confirmation message appears.

7. Click **OK**.

The cluster is defined. To set up another cluster, repeat the steps.
Figure 2-1 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.

Figure 2-1 Sample MRA Cluster Topology Configuration

Setting Up a Georedundant Non-CMP Cluster

> **Note:**
>
> Georedundancy requires that you configure the CMP system with **Manage Geo-Redundant** enabled. See the *CMP Wireless User's Guide* for more information.

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

- The server software is installed on all servers in the cluster.
- The servers have been configured with network time protocol (NTP), domain name server (DNS), IP Routing, and OAM IP addresses.

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

- MRA
- Mediation server

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

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

To set up a georedundant non-CMP cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

   The Cluster Configuration page opens; the initial group is **All Clusters**.

2. From the work area, select **Add MPE/MRA/Mediation Cluster**.

   The Topology Configuration page opens.

3. In the **Cluster Settings** section of the page:

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

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 35 characters.

   b. Select an **Appl Type**.

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

   c. Select the **Site Preference**.

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

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

      This is the number of redundant TCP/IP socket connections (streams) to carry replication traffic between sites. Up to 8 streams can be configured. The default value is `1` stream.

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

      This field only is visible if the system supports georedundancy:

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

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

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

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

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

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

Available options are:

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

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

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

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

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

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

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

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

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

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

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

Available options are:

- **C-Class** (default) – HP ProLiant BL460 Gen8 server
- **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 G8
- **Oracle RMS** – Oracle Server X5-2
- **RMS** (rack-mounted server) – HP ProLiant DL360 Gen8 or HP ProLiant DL380 Gen8 server
- **VM** (virtual machine)
- **VM(Automated)** (VM managed by NF Agent)
  See Setting Up a VM (Automated) Non-CMP Cluster for details on adding a VM (Automated) cluster.

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

The New OAM VIP dialog box appears.

i. Enter the **OAM VIP** address and the **Mask**.
This is the IP address the CMP server uses to communicate with a Policy Management cluster.

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

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

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

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

The New Signaling VIP dialog box appears.

i. Enter the **Signaling VIP** address and the **Mask**.
This is the IP address the CMP server uses to communicate with an external signaling network.

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

ii. Select the **Interface** from the list.
Available options are:

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

iii. Click **Save**.
The **Signaling VIP** address and **Mask** are saved.

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

i. Enter the **OAM VLAN ID**.
The default value is 3.

ii. Enter the **SIG-A VLAN ID**.
The default value is 5.

iii. (Optional) Enter the **SIG-B VLAN ID**.
The default value is 6.

iv. (Optional) Enter the **SIG-C VLAN ID**.
The default value is 7.

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

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

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

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

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

The Add New IP dialog box appears.

i. Enter the **IP** address in either IPv4 or IPv6 format.
This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

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

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

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

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

The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

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

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

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

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

The New Path dialog box appears.

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

i. Enter a **Static IP** address and **Mask**.

ii. Select the **Interface**:

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

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

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

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

The Add New IP dialog box appears.

i. Enter the **IP** address in either IPv4 or IPv6 format.
The IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

ii. Select the **IP Preference**: **IPv4** or **IPV6**.
The server will preferentially use the IP address of the specified format for communication.

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

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

The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

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

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

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

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

The New Path dialog box appears.

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

i. Enter a **Static IP** address and **Mask**.

ii. Select the **Interface**:

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

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

7. Click **Save**.

A confirmation message appears.

8. Click **OK**.

9. If you are setting up multiple clusters, repeat this procedure.

The cluster is defined.

Setting Up a VM (Automated) Non-CMP Cluster

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

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. If you do not see the Cluster Configuration page, click **All Clusters**.
3. From the work area, select **Add MPE/MRA/Mediation Cluster**.

   > **Note:**
   >
   > The list of available cluster types to add to the topology depends on the CMP modes configured. See the *CMP Wireless User's Guide* for more information.

   The Topology Configuration page opens.
4. In the **Cluster Settings** section of the page:
   a. (Required) Enter the **Name** for the cluster.

      Enter up to 250 characters, excluding quotation marks (") and commas (,).
   b. Select the **Appl Type** from the list.

      Available options are:

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

      > **Note:**
      >
      > The list of available application types depends on the CMP modes configured. See the *CMP Wireless User's Guide* for more information.

   c. Select **VM(Automated)** from the **HW Type** list.
   d. If needed, repeat the process for the second OAM VIP.
   e. (Optional) Click **Add New VIP**.You can enter up to six **Signaling VIPs** addresses (up to two for each SIG-A, SIG-B, and SIG-C).

      The signaling VIP is the IP address a PCEF device uses to communicate with the cluster. A non-CMP cluster supports redundant communication channels, named SIG-A, SIG-B, or SIG-C for carriers who use redundant signaling channels.

      The New Signaling VIP dialog box appears.

      i. Enter the **Signaling VIP** address and the **Mask**.
      This is the IP address the CMP server uses to communicate with an external signaling network.

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

ii. Select the **Interface** from the list.
Available options are:

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

iii. Click **Save**.
The **Signaling VIP** address and **Mask** are saved.

f. Repeat the process for any remaining Signaling VIPs.

5. Configure Server-A using VM (Automated). In the **Server-A** section of the page:

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

If the list is empty or your connection is not listed, it may need to be created. See Creating a VIM Connection for details about creating connections.

b. Verify that the VIM Connection Type is correct.

You cannot change this field. If the connection is not correct, select another VIM connection, or create a new one. See Creating a VIM Connection for details about creating a new connection.

c. If the server type is VMWare vCloud, configure the following fields:

i. Select the **Virtual Data Center** from the list of network ports or networks.

ii. Select the **Catalog** from the list.

iii. Select a **VM** (Virtual Machine) from the list.

iv. Enter a **vApp Name** site name is default, or it can be manually entered.
The vApp Name indicates what vApp to associate with the current Virtual Machine.

v. Enter the **NTP Server**.

d. If the server type is OpenStack API or OpenStack Heat, configure the following fields:

i. Select the **Image** from the list.

ii. Select the**Flavor** from the list.

iii. Select an **Availability Zone** from the list.

iv. Verify the Config Drive.
You cannot change this field.

v. Enter the **NTP Server**.

vi. Click **Add New** to add a DNS server.

vii. Click **Add New** to add a DNS search.

viii. Click **Manage** to add Security Groups.

e. Click **Add New IP** to add an **IP** address.

f. Select the **IP Preference** as either **IPv4** or **IPv6**.

g. Click **Add New IP** to add an **IP** address.

This is a fixed IP address for the VM device.

h. Enter the **HostName**.

i. Select to have the server in **Forced Standby**, see Changing Server Status to Forced Standby.

j. Click **Add New** to add a new **Static IP** address.

6. (Optional) Click **Add Server-B** and enter the information for the standby server of the cluster.

Server-B is defined for the cluster.

7. Click **Save**.

A confirmation message appears.

8. Click **OK**.

Configuring Diameter Peers

The MPE and MRAdevices support Diameter Rx, Gq, Ty, Gxx, Gx, S9, and Sd applications. For example, traffic control is supported using the Diameter Gx application. When a subscriber attaches to the network (for example, using a phone) via a GGSN (Gateway GPRS Support Node), the GGSN can establish a session with both the MPE and MRA devices using a Diameter Gx CCR (Credit Control Request) message. The MPE and MRA devices respond to the request with a Gx CCA (Credit Control Answer) message.
Use this procedure if you need to configure system devices (peers) to a diameter-based network.

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

1. Either in the **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.

The content tree displays a list of policy server or MRA groups.

2. From the content tree, select the MPE or MRA device.

The Administration page for that device opens in the work area.

3. Select the **Diameter Routing** tab.

The Diameter Routing configuration settings appear.

4. Click **Modify Peers** which opens the Modify the Diameter Peer Table.

5. Add a peer to the table using these steps.

a. Click **Add**.

The Add Diameter Peer window opens.

b. Enter the following:

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

- **IP Address** (required)
  IP address in IPv4 or IPv6 format of the peer device.

  If not specified, the MPE device uses a DNS lookup to resolve the value in the Diameter Identity field into an IP address and try to connect.
- **Diameter Realm** (required)
  The domain of responsibility for the peer (for example, `Example.com`).
- **Diameter Identity** (required)
  Fully qualified domain name (FQDN) of the peer device (for example, `mpe33.Example.com`).
- **Protocol Timer Profie**
  Select from the list.
- **Initiate Connection**
  Select to initiate an S9 connection for this Diameter peer.
- **Transport**
  Select either **TCP** or **SCTP** (shown as Transport Info in the Diameter peer table). For TCP select **Connections** (range 1 through 8, default 1). For SCTP select **Max Incoming Streams** and **Max Outgoing Streams**(1 to 8 connections, default is 8) which will be shown as Connection Info in the Diameter peer table.
- **IP Port**
  Enter the IP Port number.
- **Watchdog Interval**
  Enter the watchdog interval in seconds. The default is 6 seconds.
- **Reconnect Delay**
  Enter the response time in seconds. The default is 3 seconds.
- **Response Timeout**
  Enter the response timeout interval is seconds. The default is 5 seconds.

c. Click **Save**.

6. Complete these steps to add, edit or delete additional Diameter Peers.
   - Cloning an entry in the table
     a. Select an entry in the table.
     b. Click **Clone**. The Clone window opens with the information for the entry.
     c. Make changes as required.
     d. Click **Save**. The entry is added to the table.
   - Editing an entry in the table
     a. Select the entry in the table.
     b. Click **Edit**. The Edit Response window opens, displaying the information for the entry.
     c. Make changes as required.
     d. Click **Save**. The entry is updated in the table.
   - Deleting a value from the table
     a. Select the entry in the table.
     b. Click **Delete**. A confirmation message displays.

c. Click **Delete** to remove the entry. The entry is removed from the table.

7. Click **Save**.

Creating a VIM Connection

To create a VIM connection:

1. From the **NF Management** section of the navigation pane, select **VIM Connections**.

   The VIM Connections page opens; the initial group is **VIM Connections**.

2. From the content tree, select the **VIM Connections** group.

   The VIM Connections page opens.

3. Click **Create VIM Connection**.

   The Create VIM Connections page opens.

4. Enter a **Name** for the VIM connection.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

   > **Note:**
   >
   > Once saved, the VIM Connection Name cannot be changed.

5. (Optional) Enter a **Description** for the VIM connection.

6. Select the **VIM Type** from the list.

   Available options include:

   - **OpenStack API**—Indicates the connection will use the OpenStack API
   - **OpenStack Heat** —Indicates the connection will use the OpenStack Heat API
   - **VMWare vCloud**—Indicates the connection will use the vCloud API

7. Enter the **Host** name.

   Enter an IP address or the FQDN of the VIM host.

8. Enter the **Port** number.

   This is the port to connect to the VIM host. Enter a number from 1 to 65535. A typical port number is 5000.

9. (For OpenStack VIM types) Select to use a **Secure Connection**.

   If enabled, the connection will use an HTTPS connection to encrypt the connection.

10. Enter the **Username**.

11. (For VMWare) Enter the **Organization**.

12. (For OpenStack VIM types) Enter the **Tenant** name.

13. Enter the **Password**.

    Select **Show Password** to view the password in clear text.

14. Click **Save**.

The CMP server saves the VIM connection to the database.

Role and Scope Configuration

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

Configuring an MRA Role

MRA configuration also provides the functionality for privilege control through Role Administration. The Role Administration page includes a section named **MRA Privileges** that contains a privilege setting options for the following privileges:

- Configuration:
- Bulk Operation:
- Configuration Template:

Each privilege has three options:

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

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

To configure an MRA role:

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

   The Role Administration page opens.
2. Click **Create Role**.
3. Enter the following information:
   a. **Name**:
   b. **Description/Location** (optional): Free-form text.
   c. **MRA Privileges**: There are three types of privileges for MRA configuration: Hide, Read-Only and Read-Write.
4. When you finish, click **Save**.

   Privileges are assigned to the role.

The MRA role is configured.

Configuring the Scope for an MRA

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

Use this procedure to define the scope for a user that manages MRA devices.
To configure a scope for an MRA:

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

   The Scope Administration page opens.
2. Click **Create Scope**.
3. Enter the following information:
   a. In **Name**, enter the name for the new scope.
   b. (Optional) In **Description/Location**, enter free-form text describing the scope.
   c. Select the MRA groups this scope can control.
4. Click **Save**.

The MRA scope is defined.

About Advanced Configuration Settings for the MRA

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 SigC in Devices Exposed to PCEF

The ability of an MRA sever to use SigC in VLAN 3 enables that MRA server to utilize internal signaling communication between an MPE server and itself. SigC configuration is used when the hardware selected for the MRA server is either C-Class, C-Class (Segregated Traffic), NETRA, or VMWare.

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

To configure SigC for use in VLAN 3:

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

   The content tree displays a list of MRA groups.
2. From the content tree, select an MRA device.

   The MRA Administration page opens.

3. From the MRA Administration page, select the **MRA** tab.

   The current MRA configuration settings are displayed.
4. Click **Advanced**.
5. Click **Modify** to edit the Service Overrides table.
6. In the Service Overrides section, click **Add**.
7. In the Add Configuration Key Value dialogue, enter the following information:
   a. Enter `DIAMETERDRA.SIGDeviceFilter` in the **Configuration Key** field.
   b. Enter `SIGC` in the **Value** field.
   c. (Optional) Enter information for this configuration in the **Comments** field.
8. Click **OK**.
9. Click **Save**.

You have configured the configured SigC for use in VLAN 3.

About Redirecting Traffic to Upgrade or Remove an MRA

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

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

Changing Redirect States

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

To change the redirect state of an MRA server:

1. In the **MRA** section of the navigation bar, click **Configuration**.
2. Select an MRA.

   The MRA Administration page displays information about the selected MRA.
3. Select the **MRA** tab.
4. Click **Advanced**.
5. Click **Modify** to edit the Service Overrides table.
6. In the Service Overrides section, click **Add**.

The Add Configuration Key Value dialogue opens.

7. Enter `DIAMETERDRA.RedirectState`.

   This service override indicates the redirect state of the MRA server.

8. Enter the redirect state in the **Value** field. The valid options are:

   Changing this variable to NORMAL will stop the release process.

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

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

9. (Optional) Enter information for this configuration in the **Comments** field.
10. Click **OK**.
11. Click **Save**.

The redirect state is changed.

Releasing Active Sessions

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

The release configurable variables are:

- DIAMETERDRA.Release.Enabled
  Indicates whether the binding release task is started. Valid values are `TRUE` or `FALSE`; the default is `FALSE`. Setting this to `FALSE` stops the release process.
- DIAMETERDRA.Release.MaxRARsRate
  The rate (in RARs/sec) at which the release task queues RAR messages to be sent; they will be evenly spread across the entire second. Valid values are a positive integer; default is `250`. Setting this to a negative integer stops the release process.
- DIAMETERDRA.Release.UnconditionallyRemoveSessions

Indicates if the release task removes the session information from the binding as soon as it is processed by the release task, or if it waits until it receives a CCR-T before updating the binding. Valid values are TRUE or FALSE; the default is FALSE.

- DIAMETERDRA.Release.ReleaseTaskDone
  Internal flag used by the release task to indicate if it has completed. Values are TRUE or FALSE; the default is FALSE

  .

- DIAMETERDRA.Release.OriginHost
  This value indicates the origin host to use when sending RARs initiated by the release task. Valid values are MPE or MRA; the default is MPE.

Determining a Mapping MRA (M-MRA)

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

Managing Configuration and Virtual Templates

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

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

About Configuring Templates

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

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

Creating a Configuration Template

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

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

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

To create a configuration template:

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

   The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates.**
2. From the content tree, select **Configuration Templates**.

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

   The New Configuration Template page opens.
4. Enter the **Name** of the template.

   > **Note:**
   >
   > This is an alphanumeric field that is limited to 255 characters. Single quotes, double quotes, spaces, commas, and backslash characters are not valid.
5. (Optional) To use an existing template as a base for the new template, select an existing template from the **Copy From** list.
6. (Optional) Enter a **Description / Location**.

   The text box is limited to 255 characters.
7. Click **Save**.

The new template appears in the list in the content pane.
After creating the template, proceed with configuring the template.

Modifying a Configuration Template

> **Note:**
>
> This procedure applies to both MPE and MRA servers.

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

To modify a configuration template:

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

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

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

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

3. Select the tab that contains the information you want to configure or modify and click **Modify**.

4. For an MRA server, edit the information:

   a. On the **MRA** tab, click **Modify**:

      - **Associations**
        Network Elements and/or Network Element Groups Associating Network Elements with an MRA Device for details.
      - **MPE Pools**
        See Configuring Diameter Realm Based Peer Routes for details.
      - **Subscriber Indexing**
        See Configuring MRA Protocol Options for details.
      - **Diameter**
        Provide the port and Realm (such as example.com), see Configuring MRA Protocol Options.
      - **S9**
        If you connecting to an external MRA, see Configuring MRA Protocol Options.
      - **Radius Configuration**
        If you are using a fixed mobile convergence and need Radius, see Configuring MRA Protocol Options.

   b. On the **MRA** tab, click **Advanced**:

      - **Expert Settings**
      - **Service Overrides**
      - **Load Shedding Configuration**

   c. On the **Diameter Routing** tab:

      - **Diameter Peers**: See Loading MPE/MRA Configuration Data when Adding Diameter Peer for details.
      - **Diameter Routes**: See Configuring Diameter Realm Based Peer Routes for details.

5. Click **Save**.

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

Changing the Template Priority

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

> **Note:**
>
> This procedure applies to both MPE and MRA servers.

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

   The content tree displays a list of **All Policy Servers** or **MRA** devices.
2. From the content tree, select the device.

   The Administration page opens with the device configuration.
3. Select the **System** tab.

   The device's system configuration settings display on the page.
4. Click **Modify**.

   The administration page becomes enabled for editing.
5. In the **Associated Templates** section, edit the **Priority** value to change the number to a higher or lower value.
6. Click **Update Order**.

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

Creating a Virtual Template

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

Because virtual templates are based on configuration templates, modifying a configuration template associated with a virtual template automatically modifies the virtual template. After the template is created, the template has the functionality that is specific to that instance (that is, MPE or MRA). After templates are created and associated, the templates can be viewed and managed from the **System** tab of the MPE or MRA device.

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

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

Use this procedure if you have virtual template capability.

To create a virtual template:

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

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

2. From the content tree, select **Virtual Templates**.

   The Virtual Template Administration page opens.

3. Click **Create Virtual Template**.

   The New Virtual Template page opens.

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

   > **Note:**
   >
   > This is an alphanumeric field that is limited to 255 characters. Single quotes, double quotes, spaces, commas, and backslash characters are not valid.

5. Select a template from the **Associated Configuration Template** list.
6. (Optional) Enter a **Description**.
7. Click **Save**.

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

About Overlaps

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

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

Associating Templates with a Device

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

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

To associate templates with an MPE or MRA device:

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

   The content tree displays a list of server groups; the initial group is **ALL**.

2. From the content tree, select the device.

The administration page opens in the work area.

3. Select the **System** tab.
4. Click **Modify**.

   The administration page becomes editable.
5. In the Associated Templates section, click **Add**.

   The Add Associated Templates dialog appears.
6. Select one or more templates from the list and click **Add**.

   The Associated Templates list updates to include the selected templates.
7. To order the **Priority** of the associated templates, change the values for each listed template.

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

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

Configuring Topology Hiding for the Gx Application

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

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

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

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

To configure topology hiding for the Gx application:

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA device.

   The MRA Administration page opens.
3. Select the **MRA** tab.

   The current MRA configuration settings are displayed.
4. Click **Modify**.

The Modify MRA page opens.

5. In the **Subscriber Indexing** section, ensure that the **Index by Session ID** option is enabled if there are no other indexed subscriber keys available in update/terminate messages.
6. Click **Save**.
7. From the **MRA** tab, click **Advanced**.
8. Click **Modify** to edit the Service Overrides table.
9. In the Service Overrides section, click **Add**.
10. In the Add Configuration Key Value dialogue, enter the following information:
    a. Enter `DIAMETERDRA.TopologyHiding.Apps` in the **Configuration Key** field.
    b. Enter `Gx` in the **Value** field.
    c. (Optional) Enter information for this configuration in the **Comments** field.
11. Click **OK**.
12. In the Service Overrides section, click **Add**.
13. In the Add Configuration Key Value dialogue, enter the following information:
    a. Enter `DIAMETERDRA.TopologyHiding.Enabled` in the **Configuration Key** field.
    b. Enter `true` in the **Value** field.
    c. (Optional) Enter information for this configuration in the **Comments** field.
14. Add the following configuration keys to the Add Configuration Key Value window:
15. Click **OK**.
16. Click **Save**.

Topology hiding for the Gx application has been configured.

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.

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

To configure topology hiding for the Rx application:

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.

2. From the content tree, select an MRA device.

   The MRA Administration page opens.

3. Select the **MRA** tab.

   The current MRA configuration settings are displayed.

4. Click **Modify**.

   The Modify MRA page opens.

5. In the **Subscriber Indexing** section, ensure that the **Index by Session ID** option is enabled.

6. Click **Save**.

7. From the **MRA** tab, click **Advanced**.

8. Click **Modify** to edit the Service Overrides table.

9. In the Service Overrides section, click **Add**.

10. In the Add Configuration Key Value dialogue, enter the following information:

    a. Enter `DIAMETERDRA.TopologyHiding.Apps` in the **Configuration Key** field.

    b. Enter `Gx, Rx` in the **Value** field.

    c. (Optional) Enter information for this configuration in the **Comments** field.

11. Click **OK**.

12. In the Service Overrides section, click **Add**.

13. In the Add Configuration Key Value dialogue, enter the following information:

    a. Enter `DIAMETERDRA.TopologyHiding.Enabled` in the **Configuration Key** field.

    b. Enter `true` in the **Value** field.

    c. (Optional) Enter information for this configuration in the **Comments** field.

14. Click **OK**.

15. Click **Save**.

The topology hiding settings for the Rx application are configured.

3

About Network Elements, Backups, and Diameter Settings

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

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

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

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

Adding and Configuring Associated MRA servers

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

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

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

To add and configure an associated MRA server:

1. From the Navigation Panel select **MRA Associations**.

The MRA Association Administration page opens.

2. From the top of the MRA Associations tree, select **MRA Associations**.
3. Click **Create MRA Association**

   The Configuration screen opens.
4. Type in the **Name** of the MRA Association.
5. (Optional) Type in a **Description** of the MRA Association.
6. Select the **Type** of binding the Association will use (Algov1 or Legacy).
   - N-site v1 (default)
     Uses `Algorithm Verson 1` to distribute binding indexes across MRAs in a system.
   - Legacy
     Used after an MRA has been migrated and issues are encountered. Using this option deletes all mappings from the database and starts a rollback process that reverts the MRA servers back to the previous release.
7. From the Members section, click **Add**.
   a. Select an MRA server from the list of existing MRA servers.

      After the MRA has been selected, the **Default Primary IP Address** for that MRA is visible in the field.
   b. (Optional) If the Association is to be georedundant, select a **Default Secondary IP Address**.

      This is the IP Address other MRA servers in the Association will use when establishing Diameter Connections with this MRA.

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

   c. (Optional) Select a backup MRA from the list.

      > **Note:**
      >
      > The backup feature has a two-way capacity, for example, if MRA1 is selected to be the backup for MRA2, MRA2 will also function as a backup for MRA1 if something happens to MRA1.

   d. (Optional) Select a Protocol Timer Profile from the list. For more information, see Configuring MRA Protocol Options.
   e. Select either **TCP or SCTP** for transport protocol.

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

8. (Optional) If there is to be an Association Override, click **Add** in the Association Override section. .
   a. Select an MRA server from the list of existing MRA servers.

      After the MRA has been selected, the **Default Primary IP Address** for that MRA is visible in the field.

   b. (Optional) If the Association is to be georedundant, select a **Default Secondary IP Address**.

      This is the IP Address other MRA servers in the Association will use when establishing Diameter Connections with this MRA.

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

   c. (Optional) Select a backup MRA from the list.

      > **Note:**
      >
      > The backup feature has a two-way capacity, for example, if MRA1 is selected to be the backup for MRA2, MRA2 will also function as a backup for MRA1 if something happens to MRA1.

   d. (Optional) Select a Protocol Timer Profile from the list. For more information, see Configuring MRA Protocol Options.

   e. Select either **TCP or SCTP** for transport protocol.

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

   f. Click **Save** to save your configuration.
9. Click **Save**.
10. For Subscriber Indexing, select any or all of the following: (For more information, see *CMP Wireless User's Guide*.)
    - Index by IPv4
    - Index by IP-Domain-Id
    - Index by IPv6
    - Index by Username
    - Index by NAI
    - Index by E.164 (MSISDN)
    - Index by IMSI
    - Index by Session ID
    - Primary Indexing (IMSI or e.164/MSISDN)

> **Note:**
>
> Used for having all MRAs use the same subscriber indexing value after an upgrade.

11. (Optional) If there are to be overrides by APN, click **Add** in the Overrides by APN section.
    a. Enter the name of the APN (255 character limit, no spaces or special characters).

> **Note:**
>
> APN names are alphanumeric and have the following restrictions:
>
> - A 255 character limit
> - No spaces or special characters such as asterisks
> - Can contain hyphens (-) and periods (.) but must not begin or end with a hyphen or period
>
> Example name: pdn1.examplecorp.com

    b. select any or all of the following:
       - Index by IPv4
       - Index by IP-Domain-Id
       - Index by IPv6
       - Index by Username
       - Index by NAI
       - Index by E.164 (MSISDN)
       - Index by IMSI
       - Index by Session ID
    c. Click **Save**.
12. Click **Save**.

The MRA server is added and as associated MRA server.

Managing Client Mapping for an MRA Association

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

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

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

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

To configure client mapping for an MRA Association:

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

The MRA clusters are configured as associated MRA devices.

Modifying Backup and Associated MRA devices

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

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

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

To modify backup and associated MRA devices:

1. From the Navigation Panel select **MRA Associations**.Select **MRA Associations**from the within the screen, click **Modify**.

   The MRA Association Administration screen opens.
2. From the top of the MRA Associations tree, select the MRA association. The functions available from the table are as follows:
3. Click **Modify**.
   - To add an MRA to the table—Click **Add**; the Select MRA window opens. Select an MRA device. If this is a backup MRA, select **Is Backup**. Enter the **Primary IP Address**, and for a georedundant configuration, the **Secondary IP Address**.
   - To clone an MRA in the table—Select an MRA and click **Clone**; the Clone MRA window opens with the information for the MRA device. Make changes as required.

- To edit an MRA in the table—Select the MRA and click **Edit**; the Edit MRA window opens with the information for the MRA device. Make changes as required.
- To delete an MRA from the table—Select the MRA and click **Delete**. At the confirmation message, click **Delete**.

4. Click **Save**.

MRA Association Status Definitions

The Status column of an MRA server 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 indicates that the MRA server is not currently running any migration or sync tasks. If all MRA servers are in this state, a new MRA server can safely be added to the Association.
- `Syncing (xx%)`
  This indicates that the MRA server is currently running the sync task. If any MRA servers are in this state, a new MRA server cannot be safely added to the Association. If a new MRA server is added, data integrity cannot be guaranteed across the association. The percentage completion through the task will be displayed in parentheses.
- `Migrating (xx%)`
  This indicates that the MRA server is currently running the legacy migration task. If any MRA servers are in this state, a new MRA server cannot be safely added to the Association. The percentage completion through the task will be displayed in parentheses.
- `Migration Failed`
  This indicates that the last migration task which ran on the MRA server did not complete successfully. This likely means there were some connection failures between MRA servers during the task and the task should be manually rerun using the **Operations** menu.
- `Sync Failed`
  This indicates that the last sync task which ran on the MRA server did not complete successfully. This likely means there were some connection failures between MRA servers during the task and the task should be manually rerun using the **Operations** menu.
- `Migrated`
  This indicates that the last migration task which ran on the MRA server completed successfully. The MRA server is still running in a special migration mode, however. Use the **Complete Migration** operation to turn off migration mode on the MRA server and start using the n-site MRA server 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
  Manually starts a sync task on all MRA servers in the association.
- Cancel Sync
  Cancels a sync which is currently in progress.
- Manual Migration

Manually starts a migration task on all MRA servers in the association.

- Cancel Migration
  Cancels a migration which is currently in progress.
- Accept Migration
  Accepts the migration (after all MRA servers have finished running the migration task).

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

- Reset Counters
  Resets all counters on all MRA servers in the association.
- Reapply Configuration
  Reapplies the configuration to all MRA servers in the association.

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

Conditions Limiting Operation Options

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

Associating Network Elements with an MRA Device

Adding network elements to an MRA device is similar to how network elements are added to an MPE device: a list of supported network elements, which are pre-entered into the system is available for selection.

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

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

1. From within the **MRA** tab, click **Modify**.

   The MRA Administration Modify page opens.

2. In the Associations section of the MRA Administration Modify page, click **Manage**.

   The Select Network Elements window displays showing a list of available network elements.

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

4. (Optional) Add additional network elements to the **Selected** list.

5. Click **OK**.

The network element is added to the MRA.

Creating a Network Element

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

1. From the **Network** section of the navigation pane, select **Network Elements**.

   The content tree displays a list of network element groups; the initial group is **ALL**.

2. Click **Create Network Element**.

   The New Network Element page opens.

3. Enter information for the network element:

   a. (Required) **Name** — The name you assign to the network element.

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 250 characters.

   b. (Required) **Host Name/IP Address** — Registered domain name, or IP address in IPv4 or IPv6 format, assigned to the network element.

   c. **Backup Host Name** — Alternate address that is used if communication between the MPE device and the primary address for the network element fails.

   d. **Description/Location** — Free-form text.

      Enter up to 250 characters.

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

      The supported types are:

      - **PDSN**
        Packet Data Serving Node (with the sub-types **Generic PDSN** or **Starent**)
      - **HomeAgent**
        Customer equipment Home Agent (with the sub-types **Generic HomeAgent** or **Starent**)
      - **GGSN** (default)
        Gateway GPRS Support Node

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

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

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

   See Managing Protocol Timer Profiles for more information.

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

   When present, it contains the following options:

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

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

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

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

Associating a DSR Network Element with an MRA

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

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

To associate a DSR network element with an MRA:

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an **MRA** device.

   The MRA Administration page opens.
3. Select the **MRA** tab.

   The current MRA configuration settings are displayed.
4. Click **Modify**.

   The Modify MRA page opens.
5. Select a **Primary DSR** to associate with this MRA from the list.
6. Enter a string value into **Segment ID**, if needed. If the MRA receives a message with a Destination-Host equal to the Segment ID, the MRA removes the Destination-Host AVP from the message.
7. Click **Save**.

The specified DSR information is associated with this MRA device.

Creating a Network Element Group

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

To create a network element group:

1. From the **Network** section of the navigation pane, select **Network Elements**.

   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.

   The Network Element Administration page opens in the work area.
3. Click **Create Group**.

   The **Create Group** page opens.
4. Enter the name of the new network element group.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 250 characters.

5. Enter a text description and location of the network group.
6. Click **Save**.

You have created a network element group.

Adding a Network Element to a Network Element Group

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

1. From the **Network** section of the navigation pane, select **Network Elements**.

   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group.

   The Network Element Administration page opens in the work area, displaying the contents of the selected network element group.
3. Click **Add Network Element**.

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

   - If there are 25 or fewer network elements defined, the page displays the network elements not already part of the group.
   - If there are more than 25 network elements defined, the page does not display any elements. Instead, use the **Search Pattern** field to filter the list. Enter an asterisk (*) to generate a global search, or a search pattern to locate only those network elements whose name matches the pattern (for example, `star*`, `*pGw`, or `*-*`). When you have defined a search string, click **Filter**; the page displays the filtered list.
4. Select the network element you want to add. Use the Ctrl or Shift keys to select multiple network elements.

   You can also add previously defined groups of network elements by selecting those groups.
5. Click **Save**.

The network element is added to the network element group.

Managing Protocol Timer Profiles

This chapter describes how to define and manage protocol timer profiles within the CMP system.

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

About PCD Associations

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

Whenever a network element connects to an associated MRA device, the PCD establishes an MRA connection to the primary and secondary MRA devices that have a PCD association with

the network element. In the event of a site failure, the PCD can reroute messages from the network element to the secondary MRA device at the connection level with minimal impact on processing.

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

Creating PCD Associations for a Network Element

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

To create a PCD association for a network element:

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

   The content tree displays the **MRA Associations** group.

2. From the content tree, select the MRA association for which you want to create a PCD association.

   The MRA Association Administration page opens in the work area, displaying the details of the selected MRA association.

3. Click **Modify**.

   The **Configuration** page opens in the work area.

4. In the Client Mapping table, click **Add**.

   The Add Client Mapping window opens.

5. Add a client mapping by doing the following:

   a. From the **Network Element** list, select the network element for which you want to create a PCD association.

   b. From the **Primary MRA** list, select the MRA device that you want to handle connection-level routing for the network element. The selected MRA device must be part of the MRA association.

   c. From the **Secondary MRA** list, select the MRA device that is configured as a backup for the primary MRA device. The selected MRA device must be part of the MRA association and must be configured as a backup of the primary MRA device.

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

   d. Click **Save**.

   The client mapping is displayed in the Client Mapping table.

6. Click **Save**.

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

Modifying PCD Associations for a Network Element

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

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

   The content tree displays the **MRA Associations** group.

2. From the content tree, select the MRA association for which you want to create a PCD association.

   The MRA Association Administration page opens in the work area, displaying the details of the selected MRA association.

3. Click **Modify**.

   The **Configuration** page opens in the work area.

4. In the Client Mapping table, select the PCD association you want to modify.

5. Click **Edit**.

   The Edit Client Mapping window opens.

6. Modify the client mapping information.

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

7. Click **Save**.

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

Cloning PCD Associations for a Network Element

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

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

   The content tree displays the **MRA Associations** group.

2. From the content tree, select the MRA association for which you want to create a PCD association.

   The MRA Association Administration page opens in the work area, displaying the details of the selected MRA association.

3. Click **Modify**.

   The **Configuration** page opens in the work area.

4. In the Client Mapping table, select the PCD association you want to clone.

5. Click **Clone**.

   The Clone window opens.

6. Select the **Network Element** for the Primary and Secondary MRA servers.

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

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

7. Click **Save**.

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

Deleting PCD Associations for a Network Element

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

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

   The content tree displays the **MRA Associations** group.

2. From the content tree, select the MRA association for which you want to delete a PCD association.

   The MRA Association Administration page opens in the work area, displaying the details of the selected MRA association.

3. Click **Modify**.

   The **Configuration** page opens in the work area.

4. In the Client Mapping table, select the PCD association you want to delete.

5. Click **Delete**.

   The Delete Client Mapping window opens.

6. Click **Delete**.

   The client mapping is no longer displayed in the Client Mapping table.

7. Click **Save**.

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

About Stateful Routing

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

About Stateful MRA servers

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

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

About MPE/MRA Pools and Diameter Peer Tables

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

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

The MPE can function in the following roles:

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

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

Configuring Diameter Realm Based Peer Routes

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

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

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

To configure the Diameter realm based peer routes:

1. From the Policy Management device (either **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.

   The content tree displays a list of policy server groups.

2. From the content tree, select the **Policy Server** or **MRA** that needs diameter routing.

   The Policy Server Administration or MRA Administration page opens in the work area.

3. Select the **Diameter Routing** tab.

   The Diameter Routing configuration settings display.

4. Click **Modify Routes**.

   The Modify the Diameter Route Table page opens.

5. Add a route to the table

   a. Click **Add**.

      The Add Diameter Route (Realm Based Route) window opens.

   b. Configure the route using the following fields.

      - **Diameter Realm**
        For example, `Example.com`.
      - **Application ID**
        Select **Rx** (default), **Gq**, **Ty**, **Gx**, **Gxx**, **Sd**, **Sy**, **Gy**, **S9**, **Vzr**, or **All**.

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

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

        See Examples of Java Regular Expressions for MRA Routes for more information about using regular expressions for MRA routes.
      - **Action**
        Select **PROXY** (stateful route, default), **RELAY** (stateless route), or **LOCAL** (process on this device).
      - **Server ID**
        Select a destination peer from the list.

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

c. Click **Save**.

6. (Optional) Add, delete, modify, or order entries.
   - Cloning an entry in the table
     a. Select an entry in the table.
     b. Click **Clone**. The Clone window opens with the information for the entry.
     c. Make changes as required.
     d. Click **Save**. The entry is added to the table.
   - Editing an entry in the table
     a. Select the entry in the table.
     b. Click **Edit**. The Edit Response window opens, displaying the information for the entry.
     c. Make changes as required.
     d. Click **Save**. The entry is updated in the table.
   - Deleting a value from the table
     a. Select the entry in the table.
     b. Click **Delete**. A confirmation message displays.
     c. Click **Delete** to remove the entry. The entry is removed from the table.
   - Ordering the list.
     If you define multiple entries, they are searched in the order displayed in this list. To change the order:
     a. Select an entry.
     b. Click **Up** or **Down**. The search order is changed.
7. Define the default route:
   a. Click **Edit** in the **Default Route** section.
   b. Select the default action: **PROXY**, **RELAY**, or **LOCAL**.
   c. Select the peer server ID.
   d. Click **Save**.
8. To delete the default route, click **Delete**.
9. Click **Save**.

The Diameter realm based peer routes are configured.

Examples of Java Regular Expressions for MRA Routes

The following sample regular expressions are for MRA Routes.

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

Configuring Diameter Host Based Peer Routes

Host based diameter routes are when messages are intended for a specific destination-host or a list of destination-hosts and must be routed to an intermediary peer because the destination-host cannot be reached.
Use this procedure if you have a very wide network where direction Destination-Host connections must be routed through an intermediary peer.

To configure the Diameter host based peer routes table:

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

   The content tree displays a list of policy server/MRA groups.

2. From the content tree, select the MRA server.

   The MRA Administration page opens in the work area.

3. Select the **Diameter Routing** tab.

   The Diameter Routing configuration settings are displayed for that server or device.

4. Click **Modify Routes**.

   The Modify the Diameter Route Table page opens.

5. Click **Add** and select **Host Based Route**.

   The Add Host Based Route window opens.

6. Enter a name for the destination host.

7. Add destination host identities.

   a. Enter the number of host identities in the **Value** field.

   > **Note:**
   >
   > You can use the wildcards * (match any number of characters) and ? (match only one character).

   b. (Optional) Select **Evaluate as a Regular Expression**.

   When selected, enabled the matching of route criteria using regular expression syntax, opposed to the previously supported matching wildcards. (See Examples of Java Regular Expressions for MRA Routes for examples of using JAVA Regular Expressions.)

   c. Click **Add**

   This adds the host identities to the field.

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

   d. (Optional) Repeat to add additional destination host identities.

   e. Select the **Origin**.

The default is ANY. Enables a message to be routed based on the origin-host of the message. For example, if **MPE** is selected, then it is an MPE originated message (meaning that any messages that originated from any managed MPE are applied to this route).

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

8. Define the filter.
   a. Select the **Application ID**.

      The default is **Rx**.

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

   b. Select the **User ID type**.

      ANY is the default.

   c. Enter the user ID to be routed (for example, an NAI or E.164 number) in the **Value** field. Separate user IDs using a comma (,); use an asterisk (*) as a wildcard character.

   d. Click **Add** to add to the list.

      > **Note:**
      >
      > To remove one or more user ID from the list, select the ID and click **Delete**.

   e. (Optional) Repeat to add additional destination host identities.

   f. Click **Save**.

9. Define the next hop.
   a. Select the action.

   b. Select the server.

10. Click **Save**.

11. Define the default route:
    a. Click **Edit** in the **Default Route** section.

    b. Select the default action. (**PROXY**, **RELAY**, or **LOCAL**)

    c. Select the peer server ID.

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

d. Click **Save**.

> **Note:**
>
> To delete the default route, click **Delete** next to the route.

12. Click **Save**.

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

Associating an MRA with a Diameter MPE Peer

An MRA load shares sessions among MPE servers listed in its pool.

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

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

1. From the **MRA** section of the navigation pane, select **Configuration**.
2. Select the **MRA** to associated with an MPE device.
3. Select the **MRA** tab, click **Modify**.
4. In the **MPE Pool** section, click **Add** to open the Add Diameter MPE Peer window.
5. Enter the following information:
   a. **Associated MPE**: Select an MPE device.
   b. **Name**: Name of the MPE device.
   c. **Primary Site IP**: Enter the IP address of the primary site.
   d. **Secondary Site IP** (for georedundant configurations only): Enter the IP address of the secondary site.
   e. **Diameter Realm**: Enter the domain of responsibility for the peer (for example, `Example.com`).
   f. **Diameter Identity**: Enter a fully qualified domain name (FQDN) or the peer device (for example, `MRA10-24.Example.com`).
   g. **Route New Subscribers**: Select if the MPE no new sessions will be routed requests for new subscribers (that is, no existing binding). If it is unselected, the MPE no new sessions will be routed to this MPE.
   h. In the **Transport** section, select:
   - Select **TCP** and the number of **Connections**. The default number of connections is 1.
   - Select **SCTP** and the number of **Connections** (incoming and outgoing streams) to be used. The default is 8.
6. When you finish, click **Save**.

The Add Diameter MPE Peer window closes.

7. (Optional) In the **Diameter** section enter the following information:
   a. **Diameter Realm**, (for example, Example.com).
   b. **Diameter Identity**, (for example mra143-58.Example.com).
8. In the **S9** section select the following information:
   a. Select a **Primary agent**, (for example E_MPE-Example), from the **Primary DEA** list.
   b. (Optional if this is a georedundant device) Select a **Secondary agent** from the **Secondary DEA** list.
9. Click **Save**.

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

Cloning, Modifying, or Deleting an MPE

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

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

About Diameter Routing

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

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

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

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

- A diameter connection failure

- A diameter connection watchdog failure

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

- Certain types of error codes, that can be configured, are received in response messages
- A response timeout that can be configured

You can configure diameter routing using these four components:

- Endpoints
- Connections
- Peers
- Peer Groups

Diameter Routing: Creating an Endpoint

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

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

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

> **Note:**
>
> CMP must be configured for Wireless-C or Diameter Routing Enh to use Diameter Routing.

Complete these steps to create an Endpoints:

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

     > **Note:**
     >
     > If **Local** is selected, you must choose an **Associated MRA**.

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

- **Primary Site IP Address**—Enter the IP address, in IPv4 or IPv6 format, of the primary site.

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

- **Secondary Site IP Address**—For georedundant configurations, enter the IP address, in IPv4 or IPv6 format, of the server at the secondary site.

> **Note:**
>
> An error message will notify you if the IP address of the local peer is invalid. The secondary IP address is hidden if the connection type is TCP.

> **Note:**
>
> The secondary IP will be hidden if the connection Type is TCP.

- **Port**—Enter the port number (integer, for example 6000).
- **Description**—(Optional) Enter a description of the Endpoint.

5. Click **Save**.

The Endpoint is created.

Diameter Routing: Creating Connections

Connections provide routing lists to all MRA servers in the system.

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

> **Note:**
>
> The CMP system must be configured for Wireless-C to use Diameter Routing.

Complete these steps to add a Connection:

1. From the **MRA** section of the navigation pane, select **Diameter Routing**.
2. From the **Diameter Routing** tab, select **Connections**.
3. Click **Create Connection** to open the Configuration screen.

4. Enter the following information:
   - **Name**: Enter the name of the connection (which must be unique in the CMP database).
   - **Protocol**: Enter either **SCTP** or **TCP** depending on the type of connection being created.
   - **Client Endpoint**: Enter the name of either the local or remote endpoint that will be used.
   - **Server Endpoint**: Enter the name of either the local or remote endpoint that will be used.
   - (If local endpoints have been chosen)**Associated MRA**: Enter the name of MRA used in the endpoints.
   - **Connections**: The name of the connections to be used.
   - **Description**: (Optional) Enter a description of the Connection.
5. Click **Save** to save the changes and send the information to all the MRA servers in the system.

Diameter Routing: Creating Peers

A peer defines the relationship between several connections.

Create peers to define your connections to your MRA devices.

> **Note:**
>
> The CMP system must be configured for Wireless-C to use Diameter Routing.

To create a peer.

1. From the navigation pane, select the **MRA** and then **Diameter Routing**
2. From the **Diameter Routing** tree, select **Peer**.
3. Click **Create Peer** to open the Configuration table.
4. Enter the **Diameter Identity**.
5. (Optional) Enter the **Description/Location**
6. Select a **Mode** .
7. Select an **Associated MRA**
8. Enter any **Connections** used.
9. Click **Save**.

The peer is created.

Diameter Routing: Creating Peer Groups

> **Note:**
>
> You must first create endpoints, connections, and peers before creating peer groups.

A peer group defines a complete routing rule by specifying the relationship between several connection groups.

> **Note:**
>
> The CMP system must be configured for Wireless-C to use Diameter Routing.

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

To create a peer group:

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

     > **Note:**
     >
     > Only one peer group can be created if the connection type is DRA.

   - Select **Direct Link** if one or more Peer Groups are to be used.
8. Select an **Associated MRA**.
9. Select if the Peer Group is **Enabled**. Enable a Peer Group if Direct Link is the connection type.
10. Select **Peers** if peers are to be used.

> **Note:**
>
> If DRA connection type is used, only one peer can be selected.

11. Click **Save**.

The peer group is created.

About Stateless Routing

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

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

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

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

Enabling Stateless Routing

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

To enable a stateless routing:

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

   The content tree displays a list of MRA groups; the initial group is**ALL**.
2. Select the MRA from the content tree.

   The MRA Administration page displays the configuration for the MRA.
3. Select the **System** tab.

   The Modify System Settings page opens.
4. Click **Modify**.
5. Select **Stateless Routing**.

Stateless routing is enabled.

Modifying the Stateless Migration Mode in an Existing MRA

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

To enable and disable the migration mode setting:

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. Select the MRA device from the content tree.

   The MRA Administration page opens, displaying information about the selected MRA device.
3. Select the **MRA** tab.
4. Click **Advanced**.
5. In the **Stateful MRA Settings** section of the page, select **Enable Stateless Migration Mode** (or leave the box unchecked if you do not want to enable the migration mode).

   The stateless migration mode is enabled.
6. Click **Save**.

The MRA device is put into migration mode.

Loading MPE/MRA Configuration Data when Adding Diameter Peer

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

Configuring for RADIUS

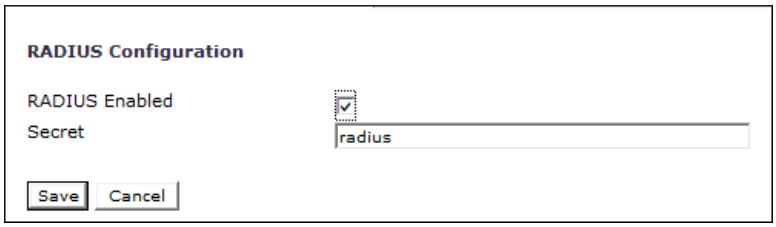
For an MRA server to utilize RADIUS, the system must be RADIUS enabled (see *CMP Wireless User's Guide*) and the MPE server associated with the MRA server must be configured for RADIUS (see *CMP Wireless User's Guide*).

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

To configure an MRA for RADIUS:

1. From the **MRA** section of the navigation pane, select **Configure**.
2. From the list, select the **MRA** to be configured.
3. Select the **MRA** tab.
4. Click **Modify**.
5. Scroll to the **RADIUS Configuration** section and enter the following:
   a. Select **RADIUS Enabled**.
   b. In the **Secret** field, enter the default pass phrase.

Figure 3-1 RADIUS Configuration Section



6. Click **Save**.

About Load Shedding Overload Control for Diameter

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

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

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

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

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

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

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

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

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

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

Configuring Load Shedding for an MRA Device

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

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

To configure load shedding for an MRA:

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

   The content tree displays a list of MRA device groups; the initial group is **ALL**.
2. From the content tree, select the **MRA** that needs load shedding capabilities.

   The MRA Administration page opens.
3. Select the **MRA** tab.

   The current MRA device configuration settings are displayed.

4. Click **Advanced**.

   The Advanced MRA Settings page opens.

5. Click **Modify**.

   The advanced configuration settings can be edited.

6. In the **MRA Load Shedding Configuration** section of the page, select the enabled state.

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

   See MRA Default Load Shedding Rules for more information on load shedding rules.

7. (Optional) Set the **Level Action** for a busyness level.

   a. Click the **right arrow** to expand the level.

   b. Select one of the following **default Level Actions**:

      - **Drop** all messages.
      - **Answer With** appropriate code from the drop-down list.
      - **Answer With Code** enter the appropriate `code` and `Vendor ID`.

8. Add rules for the busyness level.

   a. Click **Add**.

   b. Select the **Catagory**.

   c. Enter the **Values** for the load shedding rules for the appropriate busyness levels:

      - (Required) The **Name**
        Name of the rule.
      - In the Filter section select:
        - **Application**
          The application the rules apply to.
        - **Message**
          The type of message the rule applies to (which depends on the application chosen).
      - Select the **Request Type** (available only when the CCR message type is selected)
        - Initial
        - Update
        - Terminate
      - Enter the **APNs**
        This is a CSV list of one or more access point names that the massage must contain.
      - In the Action section select the action to be taken if the criteria are met for the load-shedding rule.

9. Repeat steps 6 through 8 to add rules In the MPE Load Shedding Configuration section.

> **Note:**
>
> MPEs can use all four busyness levels.

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

10. Click **Save**.

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

Cloning Load Shedding Rules

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

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

To clone a load shedding rule:

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.

2. From the content tree, select theMRA that needs load shedding capabilities.

   The MRA Administration page opens.

3. Select the **MRA** tab.

   The current MRA configuration settings are displayed.

4. Click **Advanced**.

   The Advanced MRA Settings page opens.

5. Click **Modify**.

6. Select the section (**MRA Load Shedding Configuration** or **MPE Load Shedding Configuration**) and select the rule to be cloned.

7. Click  (clone icon) on the toolbar.

8. Enter a new **Name** for the rule.

9. Select an action.

10. Click **OK** to save the changes.

    The new rule displays in the list above the rule that was cloned.

Modifying Load Shedding Rules

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

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

To modify a load shedding rule:

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the MRA that needs load shedding capabilities.

   The MRA Administration page opens.
3. From the MRA Administration page, select the **MRA** tab.

   The current MRA configuration settings are displayed.
4. Click **Advanced**.

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

   The rule is modified.

Re-ordering Load Shedding Rules

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

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

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

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

   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the MRA that needs load shedding capabilities.

   The MRA Administration page opens.
3. From the MRA Administration page, select the **MRA** tab.

   The current MRA configuration settings are displayed.
4. Click **Advanced**.

   The Advanced MRA Settings page opens.
5. Click **Modify**.
6. Select the section (**MRA Load Shedding Configuration** or **MPE Load Shedding Configuration**) to change.
7. Select the **rule** to be re-ordered in the list.
8. Click the (up arrow) or (down arrow) on the toolbar to place the rule in the desired position in the list.

MRA Default Load Shedding Rules

You can configure load shedding rules to determine how a device reacts to a processing backlog. This state is called busyness. Levels of busyness can be configured to accept, reject, or drop select messages at each level. An MRA has two busyness levels. At each level of busyness, requests that have been queued longer than a configurable time are discarded without further processing, since the originator would have abandoned that request.

On the MRA Advanced Configuration page, there is a default action for each Busyness Level. The default level action is Accept for Level 1, which means to process the message by bypassing load shedding rules. Level actions are configurable.

The following tables show the default load-shedding rules for an MRA.

> **Note:**
>
> The default rules shown in your system may differ than those listed here depending on how your system is configured.

Table 3-1 MRA Busyness Level 1

Rule Name	Actions
DefaultRule1	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule2	Reject Gxx CCR messages with DIAMETER_TOO_BUSY
DefaultRule6	Accept Gx CCR messages with DRMP priority 0

Table 3-2 MRA Busyness Level 2

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

4

About MRA Monitoring

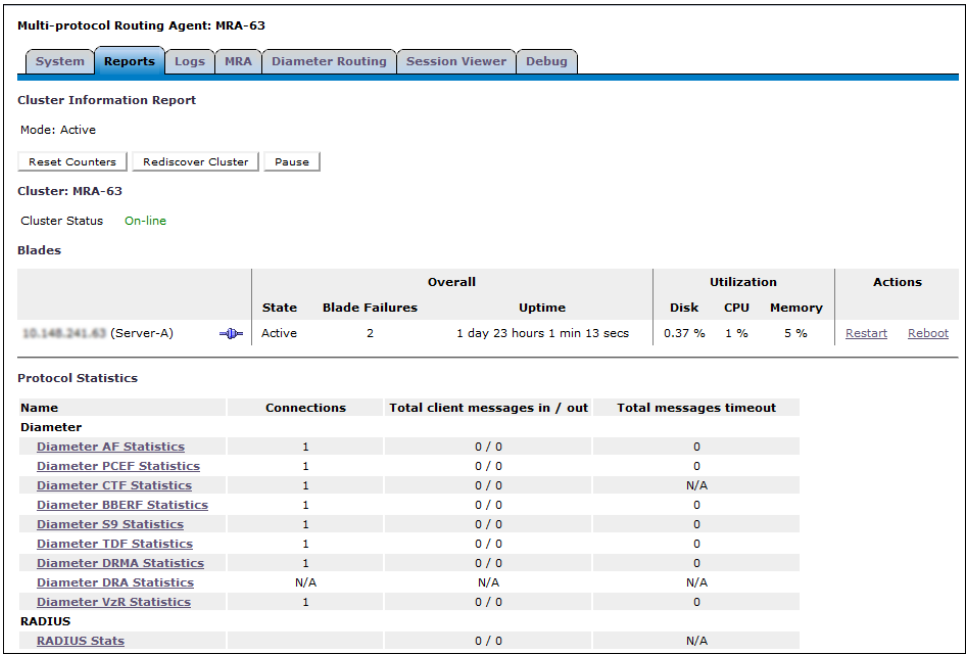
Monitoring a Multi-Protocol Routing Agent, (MRA), device is similar to monitoring Multimedia Policy Engine, (MPE), devices. The MRA uses the Reports page, the Logs page, and the Debug page to provide the MRA status information. Specifically:

- Cluster and server information
- DRMA information
- Event logs

About Displaying Cluster and Blade Information

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

Figure 4-1 Cluster, Blade, and Diameter Information



The following is a list of Diameter statistics in the Protocol Statistics section of the report:

- Diameter AF (Application Function) Statistics
- Diameter PCEF (Policy and Charging Enforcement Function) Statistics
- Diameter CTF (Charging Trigger Function) Statistics

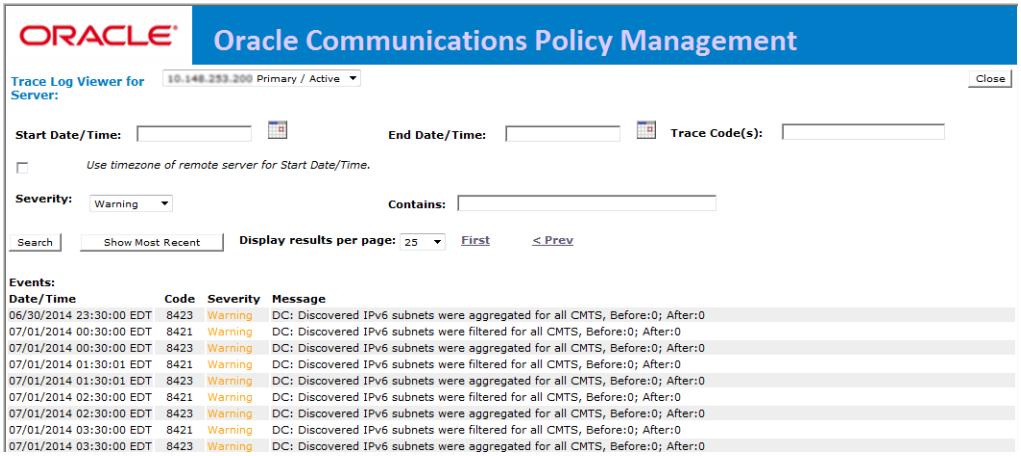
- Diameter BBERF (Bearer Binding and Event Reporting) Statistics
- Diameter S9 Statistics
- Diameter TDF (Traffic Detection Function) Statistics
- Diameter DRMA (Distributed Routing and Management Application) Statistics
- Diameter DRA (Distributed Routing Application) Statistics
- Diameter VzR Statistics

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.

About the Trace Log Page

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

Figure 4-2 MRA Trace Log Page



About the KPI Dashboard

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

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

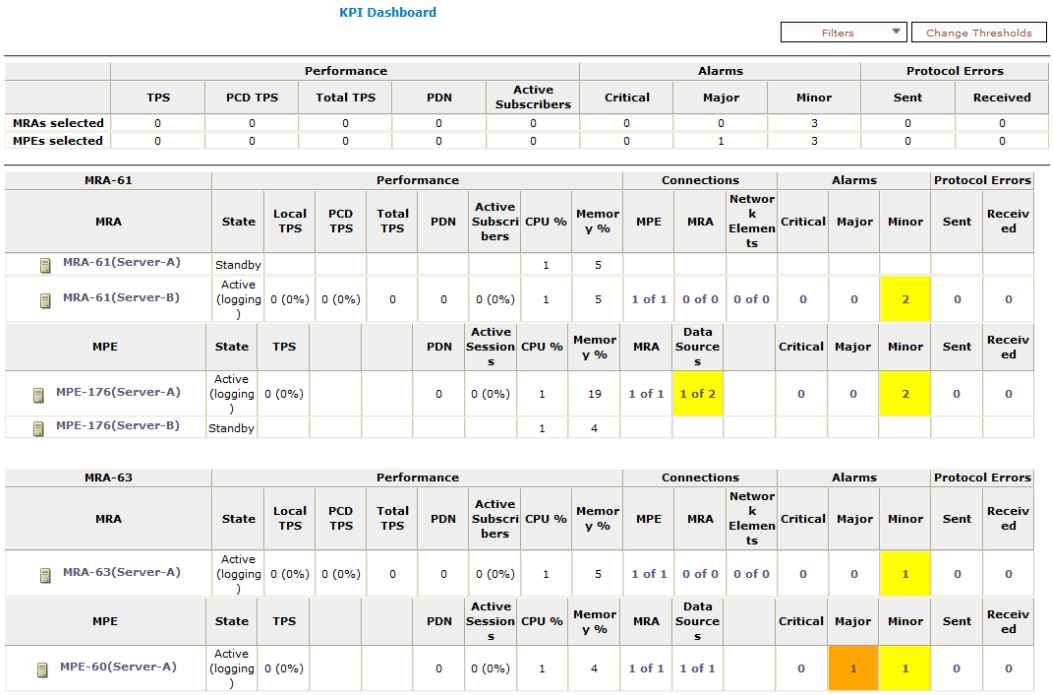
To display the KPI dashboard, from the main menu click KPI Dashboard. The dashboard opens in the work area.

The KPI dashboard displays the indicators for all the systems on a single page, with the KPIs for each MRA in a separate table. Each row within a table represents a single system (either an MRA server or an MPE server 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 contents of the KPI dashboard.

Figure 4-3 KPI Dashboard


KPI Dashboard

Filters | Change Thresholds

	Performance					Alarms			Protocol Errors	
	TPS	PCD TPS	Total TPS	PDN	Active Subscribers	Critical	Major	Minor	Sent	Received
MRAs selected	0	0	0	0	0	0	0	3	0	0
MPEs selected	0	0	0	0	0	0	1	3	0	0

MRA-61	Performance								Connections			Alarms			Protocol Errors	
MRA	State	Local TPS	PCD TPS	Total TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
MRA-61(Server-A)	Standby						1	5								
MRA-61(Server-B)	Active (logging)	0 (0%)	0 (0%)	0	0	0 (0%)	1	5	1 of 1	0 of 0	0 of 0	0	0	2	0	0

MPE	State	TPS			PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
MPE-176(Server-A)	Active (logging)	0 (0%)			0	0 (0%)	1	19	1 of 1	1 of 2		0	0	2	0	0
MPE-176(Server-B)	Standby						1	4								

MRA-63	Performance								Connections			Alarms			Protocol Errors	
MRA	State	Local TPS	PCD TPS	Total TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
MRA-63(Server-A)	Active (logging)	0 (0%)	0 (0%)	0	0	0 (0%)	1	5	1 of 1	0 of 0	0 of 0	0	0	1	0	0

MPE	State	TPS			PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
MPE-60(Server-A)	Active (logging)	0 (0%)			0	0 (0%)	1	4	1 of 1	1 of 1		0	1	1	0	0

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 (see Changing KPI Color Threshold Levels).

Each MRA or MPE system has two rows in the table. The first row displays data for the primary (active) server in the cluster. The second row displays data for the secondary (backup) server in the cluster. Several of the KPI columns are not populated for the secondary server (since the server 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 then the status is set to `Off-line` and the values in all the associated columns are 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 are cleared and no coloring is applied.

The columns that display `TPS Connections` [1] and PDN [2] information are displayed in two forms:

[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

[2] The columns that display connection counts are 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.

- Numerically
  The number of Diameter Requests (per second) received from the clients

  .
- Graphically
  Where X represents the actual numeric value and Y represents the % of rated system capacity that is consumed.

About Color Threshold Configuration

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

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

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

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

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

Changing KPI Color Threshold Levels

Occasionally, you might want lower the level of a parameter, such as **CPU%**, to make sure that there you have adequate warning if a device is getting too much traffic or usage.

To change the KPI color threshold levels:

1. From the **System Wide Reports** section of the navigation pane, select **KPI Dashboard**.
2. Click **Change Thresholds**.

   The KPI Dashboard Configuration dialog opens.
3. Select the **Percentage Field** for a parameter.
4. Enter the percentage.
5. Repeat for all parameter levels that need to change.
6. Click **Save**.

The KPI color threshold is changed.

Resetting the KPI Threshold Levels

Resetting the KPI thresholds changes the levels back to their default values.

> **Note:**
>
> You cannot reset just one parameter. Clicking **Reset** changes all parameters that have been changed.

To reset the threshold levels of the KPI Dashboard:

1. From the **System Wide Reports** section of the navigation pane, select **KPI Dashboard**.
2. From the KPI Dashboard, click **Change Thresholds**.

   The KPI Dashboard Configuration dialog opens.
3. Click **Reset**.
4. Click **Save**.

The KPI threshold levels are reset.

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.

- Table 4-22

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

Table 4-1 Policy Statistics

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

Table 4-2 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 4-3 Diameter Application Function (AF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count \Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
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

Table 4-3 (Cont.) Diameter Application Function (AF) Statistics

Display	MPE	MRA	Name
AAR messages timeout	Y	Y	AAR Timeout Count
ASR messages received/sent	Y	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	Y	Y	ASR Timeout Count
ASA success messages received/sent	Y	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages received/sent	Y	Y	ASA Recv Failure Count\ASA Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages received/sent	Y	Y	STR Recv Count\STR Send Count
STR messages timeout	Y	Y	STR Timeout Count
STA success messages received/sent	Y	Y	STA Recv Success Count\STA Send Success Count
STA failure messages received/sent	Y	Y	STA Recv Failure Count\STA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
Cleanup ASA received	Y	Y	ASA Received Count
Cleanup ASR sent	Y	Y	ASR Sent Count
Current number of active sponsored sessions	Y	N	Current Sponsored Session Count
Max sponsored active sessions	Y	N	Max Sponsored Session Count
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
Currently active emergency sessions	Y	N	Current Emergency Session Count
Max active emergency sessions	Y	N	Max Active Emergency Session Count

Table 4-4 Diameter AF Peer Stats (in Diameter AF Stats window)

Display	MPE	MRA	Name
ID	Y	Y	
IP Address: Port			
Currently active connections			
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
Connect Time	N	Y	Connect Time
Disconnect Time	N	Y	Disconnect Time

Table 4-5 Diameter Policy Charging Enforcement Function (PCEF) Statistics

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

Table 4-6 Diameter Charging Function (CTF) Statistics

Display	MPE	MRA	Name
Connections	N	Y	Conn Count

Table 4-6 (Cont.) Diameter Charging Function (CTF) Statistics

Display	MPE	MRA	Name
Currently OK peers	N	Y	Peer Okay Count
Currently down/suspect/reopened peers	N	Y	Peer Down Count\Peer Suspect Count \Peer Reopen Count
Total messages in/out	N	Y	Msg In Count\Msg Out Count
CCR messages sent/received	N	Y	CCR Recv Count\CCR Send Count
CCA success messages recd/sent	N	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	N	Y	CCA Recv Failure Count\CCA Send Failure Count
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 4-7 Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count \Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count

Table 4-7 (Cont.) Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics

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

Table 4-8 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

Table 4-8 (Cont.) Diameter TDF Statistics

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

Table 4-9 Diameter Sh / Sh Peer Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count \Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count
Messages retried due to error response	Y	N	
Messages retried due to response timeout	Y	N	
UDR messages received/sent	Y	N	UDR Messages Received Count\UDR Messages Sent Count

Table 4-9 (Cont.) Diameter Sh / Sh Peer Statistics

Display	MPE	MRA	Name
UDR messages timeout	Y	N	UDR Timeout Count
UDR messages retried due to error response	Y	N	
UDR messages retried due to response timeout	Y	N	
UDR messages retried due to error response	Y	N	
UDR messages retried due to response timeout	Y	N	
UDR messages from session updates	Y	N	
UDA success messages received/ sent	Y	N	UDA Success Messages Received Count\UDA Success Messages Sent Count
UDA failure messages received/ sent	Y	N	UDA Failure Messages Received Count\UDA Failure Messages Sent Count
PNR messages received/sent	Y	N	PNR Messages Received Count\PNR Messages Sent Count
PNA success messages received/ sent	Y	N	PNA Success Messages Received Count\PNA Success Messages Sent Count
PNA failure messages received/sent	Y	N	PNA Failure Messages Received Count\PNA Failure Messages Sent Count
PUR messages received/sent	Y	N	PUR Messages Received Count\PUR Messages Sent Count
PUR messages timeout	Y	N	PURTimeout Count
PUR messages retried due to error response	Y	N	
PUR messages retried due to response timeout	Y	N	
PUA success messages received/ sent	Y	N	PUA Success Messages Received Count\PUA Success Messages Sent Count
PUA failure messages received/sent	Y	N	PUA Failure Messages Received Count\PUA Failure Messages Sent Count
SNR messages received/sent	Y	N	SNR Messages Received Count\SNR Messages Sent Count
SNR messages timeout	Y	N	SNRTimeout Count
SNR messages retried due to error response	Y	N	
SNR messages retried due to response timeout	Y	N	
SNA success messages received/ sent	Y	N	SNA Success Messages Received Count\SNA Success Messages Sent Count

Table 4-9 (Cont.) Diameter Sh / Sh Peer Statistics

Display	MPE	MRA	Name
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 4-10 Diameter S9 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
CCR messages received/sent	Y	N	CCR Messages Received Count\CCR Messages Sent Count
CCR messages timeout	Y	N	CCRTimeout Count
CCA success messages received/ sent	Y	N	CCA Success Messages Received Count\CCA Success Messages Sent Count
CCA failure messages received/sent	Y	N	CCA Failure Messages Received Count\CCA Failure Messages Sent Count
CCR-I messages received/sent	Y	N	CCR-I Messages Received Count \CCR-I Messages Sent Count
CCR-I messages timeout	Y	N	CCRTimeout Count
CCA-I success messages received/ sent	Y	N	CCA-I Success Messages Received Count\CCA-I Success Messages Sent Count
CCA-I failure messages received/ sent	Y	N	CCA-I Failure Messages Received Count\CCA-I Failure Messages Sent Count
CCR-U messages received/sent	Y	N	CCR-U Messages Received Count \CCR-U Messages Sent Count
CCR-U messages timeout	Y	N	CCRUTimeout Count
CCA-U success messages received/ sent	Y	N	CCA-U Success Messages Received Count\CCA-U Success Messages Sent Count
CCA-U failure messages received/ sent	Y	N	CCA-U Failure Messages Received Count\CCA-U Failure Messages Sent Count
CCR-T messages received/sent	Y	N	CCR-T Messages Received Count \CCR-T Messages Sent Count
CCR-T messages timeout	Y	N	CCRTTimeout Count
CCA-T success messages received/ sent	Y	N	CCA-T Success Messages Received Count\CCA-T Success Messages Sent Count

Table 4-10 (Cont.) Diameter S9 Statistics

Display	MPE	MRA	Name
CCA-T failure messages received/ sent	Y	N	CCA-T Failure Messages Received Count\CCA-T Failure Messages Sent Count
RAR messages received/sent	Y	N	RAR Messages Received Count\RAR Messages Sent Count
RAR messages timeout	Y	N	RARTimeout Count
RAA success messages received/ sent	Y	N	RAA Success Messages Received Count\RAA Success Messages Sent Count
RAA failure messages received/ sent	Y	N	RAA Failure Messages Received Count\RAA Failure Messages Sent Count
Currently active inbound sessions	Y	N	Active Inbound Sessions Count
Max active inbound sessions	Y	N	Maximum Active Inbound Sessions Count
Currently active outbound sessions	Y	N	Active Outbound Sessions Count
Max active outbound sessions	Y	N	Maximum Active Outbound Sessions Count

Table 4-11 Diameter Distributed Routing and Management Application (DRMA) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently okay peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count \Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
DBR messages received/sent	N	Y	DBRRecv Count\DBRSend Count
DBR messages timeout	N	Y	DBRTimeout Count
DBA success messages received/ sent	N	Y	DBARecv Success Count\DBASend Success Count
DBA failure messages received/ sent	N	Y	DBARecv Failure Count\DBASend Failure Count
DBA message received/sent– binding found	N	Y	Binding Found Recv Count\Binding Found Send Count
DBA messages received/sent – binding not found	N	Y	Binding Not Found Recv Count \Binding Not Found Send Count
DBA messages received/sent – PCRF down	N	Y	Binding Found Pcrf Down Recd Count\ Binding Found Pcrf Down Send Count
DBA messages received/sent – all PCRFs down	N	Y	All Pcrfs Down Recv Count\ All Pcrfs Down Send Count
DBR-Q messages received/sent	N	Y	
DBR-Q messages timeout	N	Y	
DBA-Q success messages received/ sent	N	Y	

Table 4-11 (Cont.) Diameter Distributed Routing and Management Application (DRMA) Statistics

Display	MPE	MRA	Name
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	
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			

Table 4-11 (Cont.) Diameter Distributed Routing and Management Application (DRMA) Statistics

Display	MPE	MRA	Name
SQA messages received/sent			
SQA messages timeout			
Session found received/sent			
Session not found received/sent			
Diameter DRMA connections			

> **Note:**
>
> The statistics listed in Table 4-12 apply only to MRA devices.

Table 4-12 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 4-13 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

Table 4-13 (Cont.) Diameter Sy Statistics

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

Table 4-14 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	
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	

Table 4-14 (Cont.) RADIUS Statistics

Display	MPE	MRA	Name
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	
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 4-15 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 4-15 Diameter Latency Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Active Connection Count
Max Processing Time recd/sent (ms)	Y	Y	Max Trans In Time\ Max Trans Out Time
Avg Processing Time recd/sent (ms)	Y	Y	Avg Trans In Time\ Avg Trans Out Time
Processing Time recd/sent <time frame> (ms)	Y	Y	Processing Time [0-20] ms
			Processing Time [20-40] ms
			Processing Time [40-60] ms
			Processing Time [60-80] ms
			Processing Time [80-100] ms
			Processing Time [100-120] ms
			Processing Time [120-140] ms
			Processing Time [140-160] ms
			Processing Time [160-180] ms
			Processing Time [180-200] ms
			Processing Time [>200] ms

Table 4-16 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 4-17 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

Table 4-17 (Cont.) Diameter Protocol Error Statistics

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 4-18 Diameter Connection Error Statistics

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

Table 4-19 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 4-20 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
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

Table 4-20 (Cont.) Sh Data Source Statistics

Display	MPE	MRA	Name
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 4-21 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 4-22 KPI Interval Statistics

Display	MPE	MRA	Name
Interval Start Time	Y	Y	Interval Start Time
Configured Length (Seconds)	Y	Y	Configured Length (Seconds)

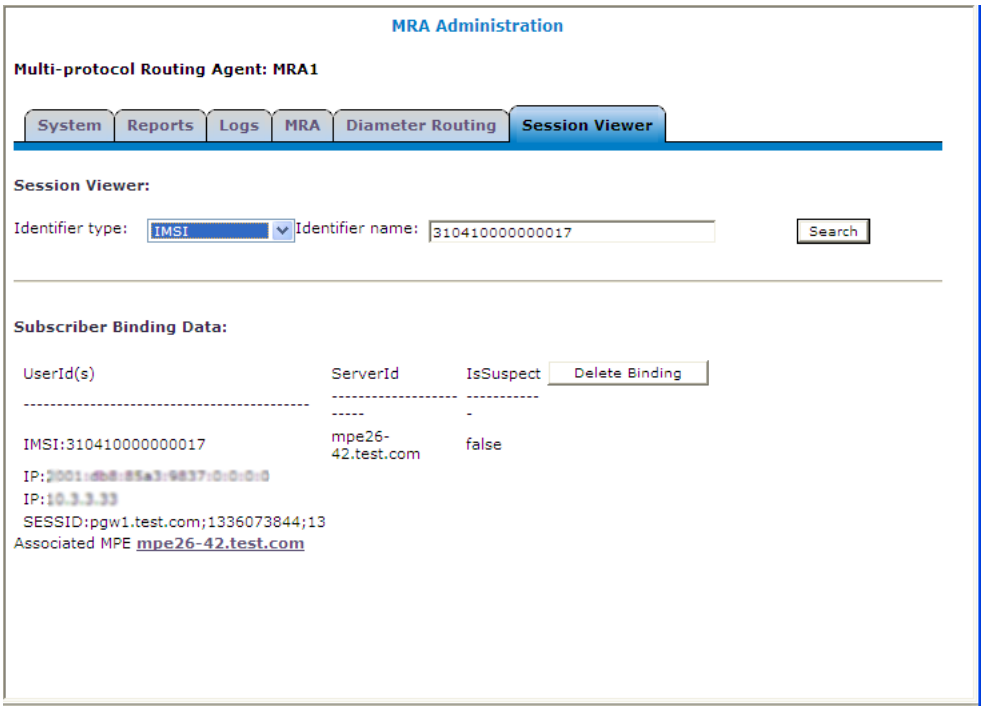
Table 4-22 (Cont.) KPI Interval Statistics

Display	MPE	MRA	Name
Actual Length (Seconds)	Y	Y	Actual Length (Seconds)
Is Complete	Y	Y	Is Complete
Interval MaxTransactionsPerSecond	Y	Y	For MPE, maximum transactions per second for the previous interval For MRA, maximum local transactions per second for the previous interval
Interval MaxPCDTransactionsPerSecond	N	Y	Maximum PCD transactions per second for the previous interval
Interval MaxMRATotalTransactionsPerSecond	N	Y	Maximum MRA total transactions per second for the previous interval
Interval MaxMRABinding Count	N	Y	Maximum MRA bindings for the previous interval
Interval MaxPDNConnectionCount	N	Y	Maximum PDN connections for the previous interval
Interval MaxSessionCount	Y	Y	Maximum session count for the previous interval

About the Subscriber Session Viewer

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

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

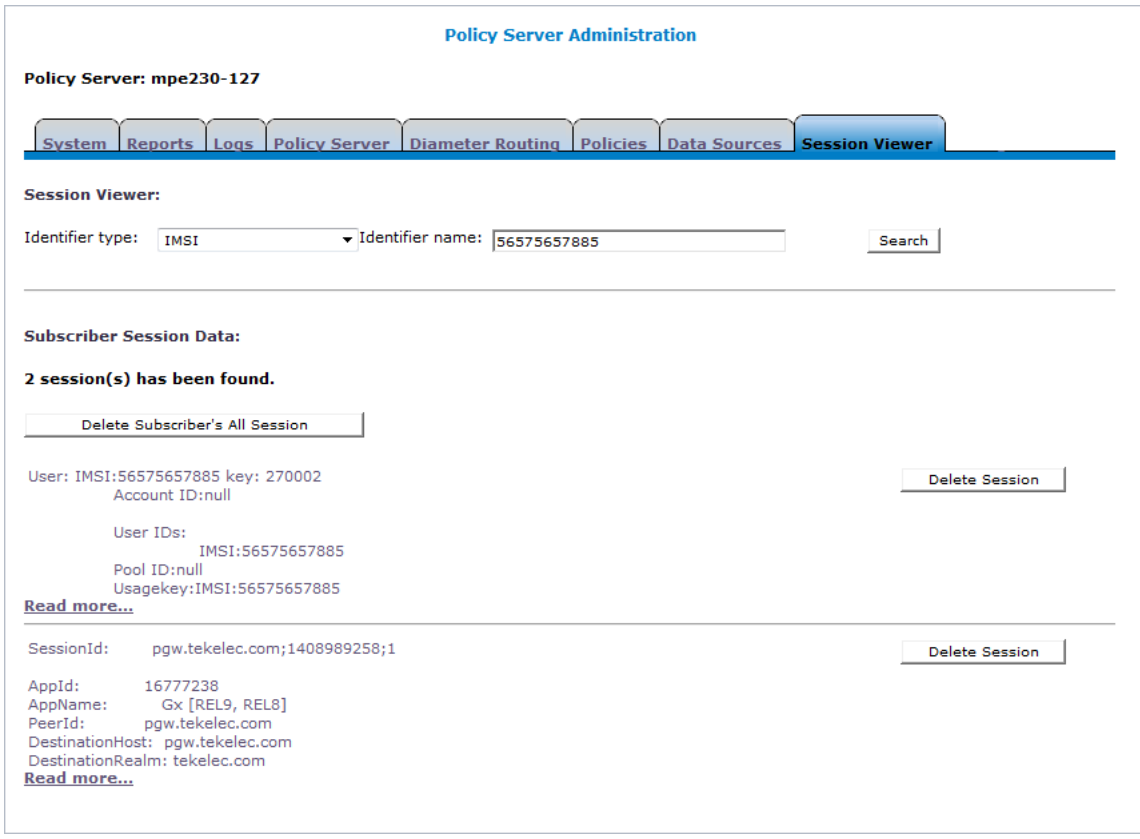


Viewing Session Data from the MPE

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

To view session data from the MPE device:

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



The MRA device is listed by peer ID.

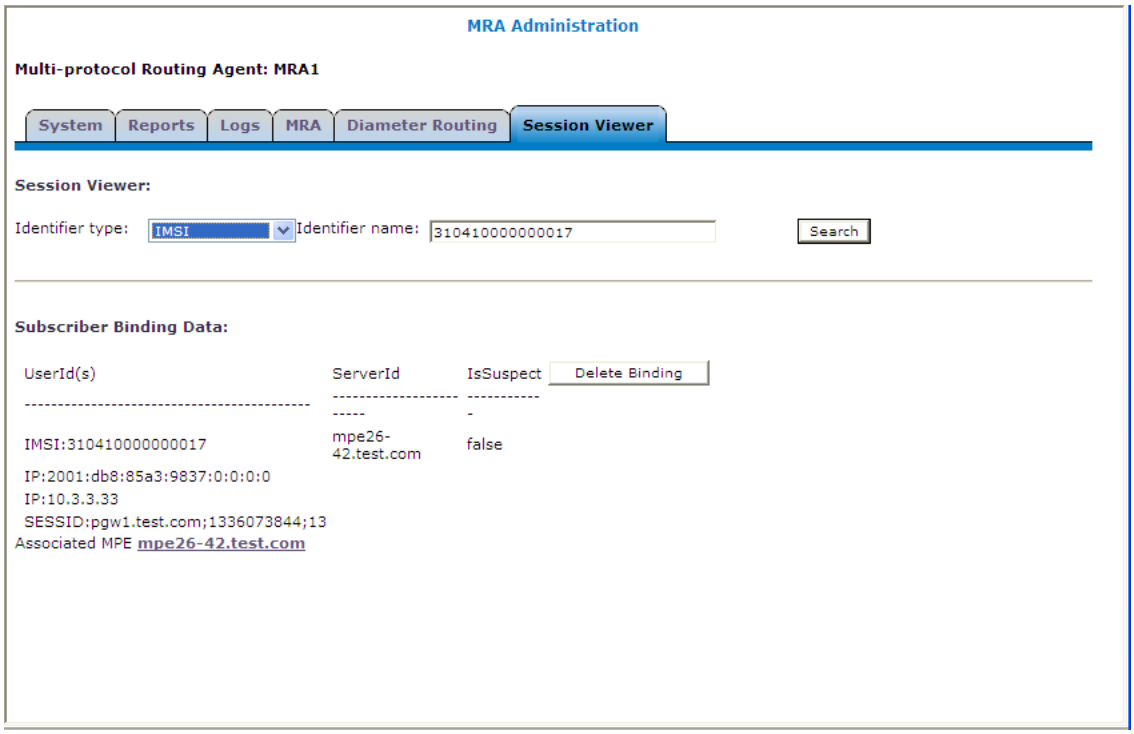
If no session data is available, the CMP returns the following message:

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. From the content tree, select the MRA device.
3. On the **Session Viewer** tab, select the Identifier Type, enter the **Identifier name**, and click **Search**. Information about the subscriber binding data is displayed; for example:



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 system sends the delete request to the MRAgent/MIAgent and returns to the Session Viewer page, displaying the delete result and the remaining session data.

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