Policy Management

Multi-Protocol Routing Agent User's Guide

910-6404-001 Revision A
June 2012

Table of Contents

List of Figures

List of Tables

Chapter 1

About This Guide

Topics:

This guide describes how to use Tekelec's Multi-Protocol Routing Agent (MRA).

How This Guide is Organized

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

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

Intended Audience

This guide is intended for the following trained and qualified service personnel who are responsible for operating Tekelec devices:

- System operators
- System administrators

Documentation Admonishments

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

Table 1: Admonishments

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

Conventions

Your view of the product may vary from the figures used as examples in this guide; the pages, tabs, fields, and functions that you see depend on your configuration or application.

The MPE device is the Tekelec policy server. The terms *policy server* and *MPE device* are synonymous.

The following conventions are used throughout this guide to emphasize certain information, such as user input, page options and output, and menu selections.

Italics — Indicates book titles and user input variables.

```
Monospace – Symbol program output
```

`Monospace bold –` Indicates user input.

```
Monospace italics – Indicates variables in commands.
```

Note: This icon indicates helpful suggestions or references to other documents.

CAUTION: This icon notifies you to proceed carefully to avoid damaging equipment or losing data.

Customer Care Center

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

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

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

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

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

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

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

TAC Regional Support Office Hours:

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

- **Caribbean and Latin America (CALA)**

  Phone:

  USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

  TAC Regional Support Office Hours (except Brazil):

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

  - **Argentina**

    Phone:

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

  - **Brazil**

    Phone:

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

    TAC Regional Support Office Hours:

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

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **Dominican Republic**

    Phone:

    1-888-367-8552

  - **Mexico**

    Phone:

    001-888-367-8552

  - **Peru**

    Phone:

    0800-53-087

  - **Puerto Rico**

    Phone:

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

  - **Venezuela**

    Phone:

0800-176-6497

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

  Regional Office Hours:

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

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

    +91 124 436 8552 or +91 124 436 8553

    TAC Regional Support Office Hours:

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

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

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

Emergency Response

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

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

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system

- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

Related Documentation

The following documents provide additional information for the configuration and use of Tekelec products:

- *TPD Troubleshooting*
- *SNMP User's Guide*
- *OSSI XML Interface Definitions Guide*
- *Policy Management Troubleshooting*
- *MPE / MRA Key Performance Indicators Application Note*

Locate Product Documentation on the Customer Support Site

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

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

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

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

Chapter 2

Introduction

Topics:

This chapter describes Tekelec's Multi-Protocol Routing Agent (MRA), which is used to scale the Policy Management infrastructure by distributing the PCRF load across multiple MPEs in the network.

MRA Overview

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

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

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

The MRA product can route requests across multiple MRA clusters within the Policy Management network. Up to four 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 up to 10 MPE clusters as a domain of responsibility. Each MRA cluster is a peer with the MPE clusters in its domain of responsibility. The following diagram shows a typical MRA configuration.

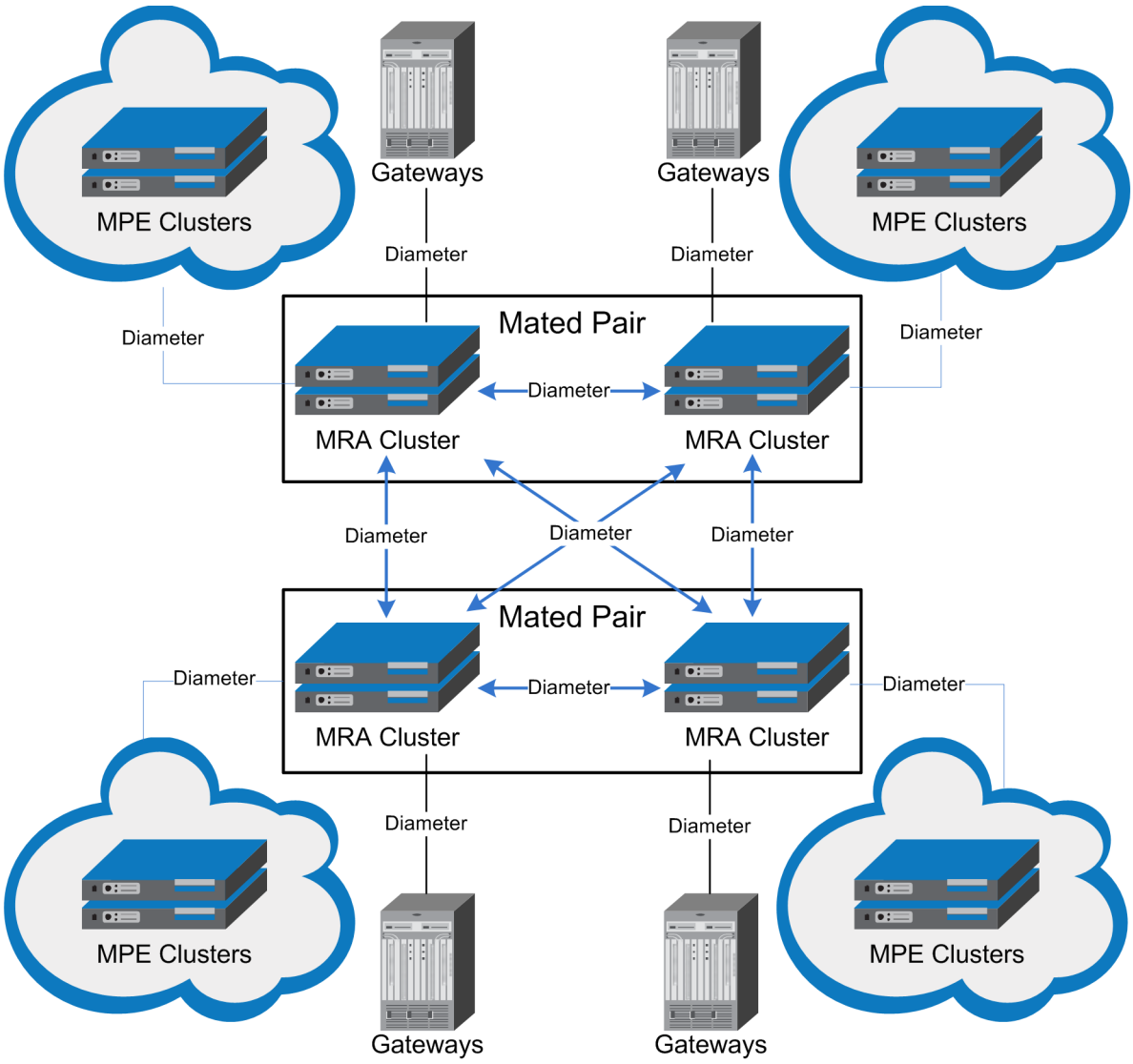


Figure 1: Typical MRA Network

Distributed Routing and Management Application (DRMA) Protocol

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

Backup MRAs, Associated MRAs, and Mated Pairs

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

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

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

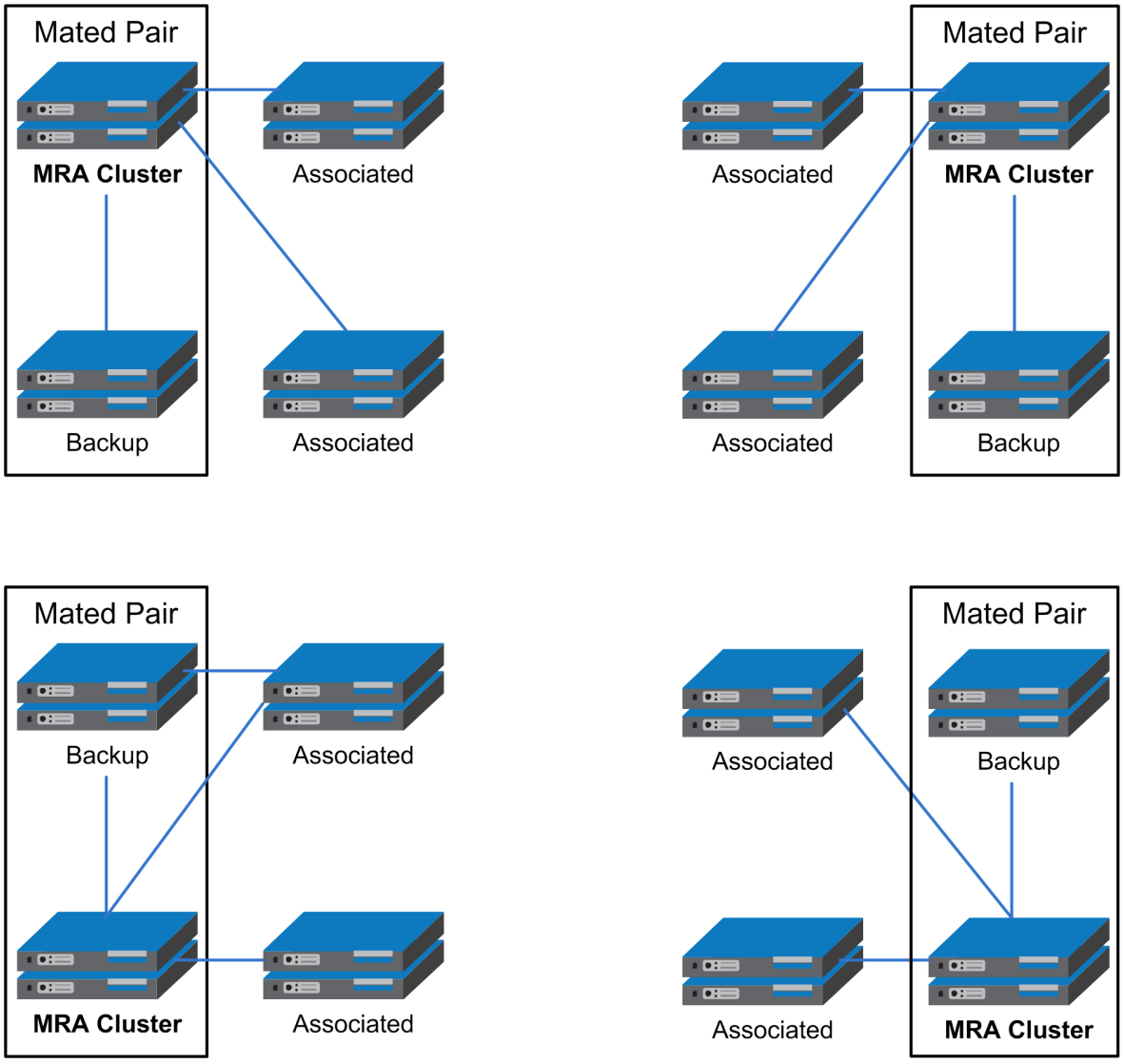


Figure 2: Backup and Associated MRAs and Mated Pairs

GUI Overview

The MRA uses an intuitive and highly portable Graphical User Interface (GUI) supporting industry-standard web technologies (SSL, HTTP, HTTPS, IPv4, IPv6, and XML). *Figure 3: GUI Components* shows the structure of the MRA GUI.

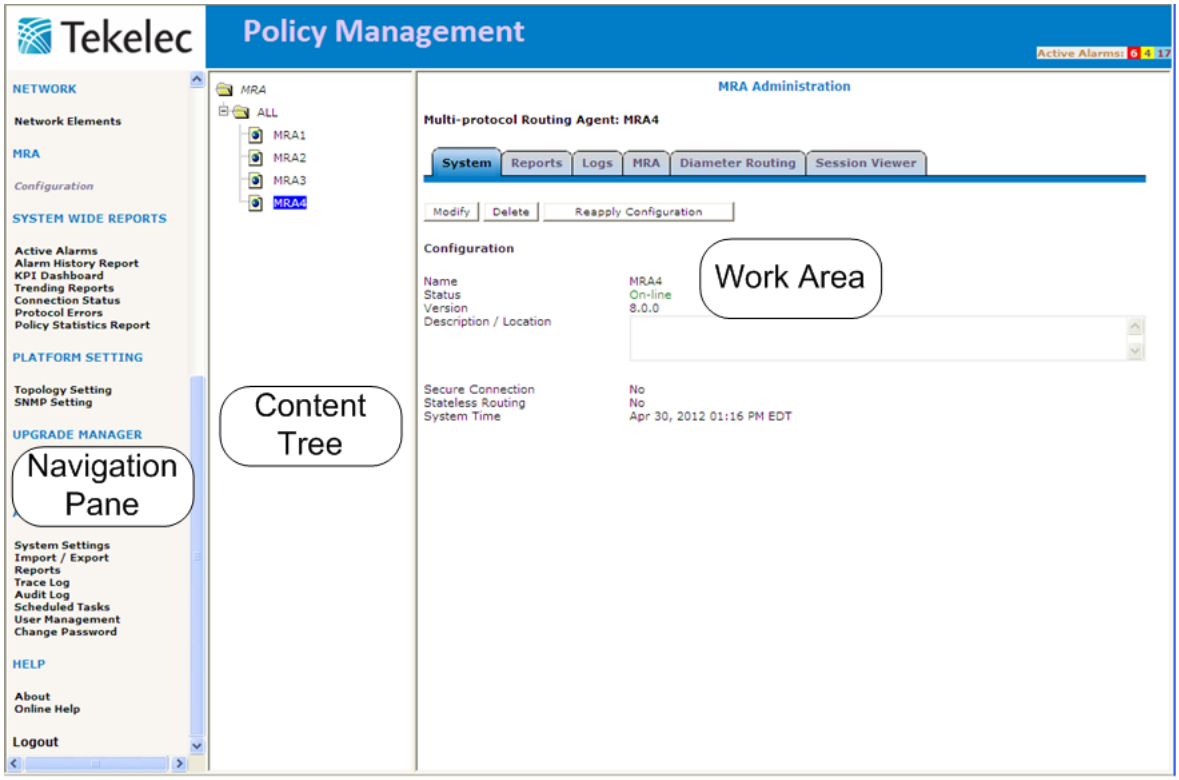


Figure 3: GUI Components

- **Navigation Pane** — Provides access to the various available options within the MRA Manager.
- **Content Tree** — Contains an expandable/collapsible listing of all the defined items for a given selection. For content trees that contain a group labeled **ALL**, you can create customized groups that display on the tree.

  The content tree section is not visible with all navigation selections.
- **Work Area** — Contains information that relates to choices in both the navigation pane and the content tree. This is the area in which you perform all work.

Specifications for Using the GUI

Tekelec recommends the following:

- **Web Browsers** —
  - Mozilla Firefox
  - Microsoft Internet Explorer 6 or higher, on Windows XP
- **Monitor** — 1024 x 768 or higher

GUI Icons

The MRA provides icons for removing, deleting, or changing the sequential order of items displayed in a list:

Remove icon — When visible in the work area, selecting the scissors icon removes an item from the group it is associated with. The item is still listed in the ALL group and any other group that it is currently associated with.

Delete icon — When visible in the work area, selecting the trash can icon deletes an item, removing it from the MPE device.

Note: Deleting an item from the**ALL** folder also deletes the item from any associated group. A delete verification window opens when this icon is selected.

Move icon — The up/down arrow icons are displayed when it is possible to change the sequential order of items in a list.

Chapter 3

CMP, MRA, and MPE Configuration

Topics:

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

This chapter describes how to:

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

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

Configuring the CMP to Manage the MRA

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

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

Configuring the CMP to Manage an MRA Cluster

The Multi-Protocol Routing Agent (MRA) is a standalone entity that supports Multimedia Policy Engine (MPE) devices. The CMP is used to manage all MRA functions. Before this can occur, the CMP operating mode must support managing MRA clusters.

To reconfigure the CMP operating mode, complete the following:

CAUTION: CMP operating modes should only be set in consultation with Tekelec Technical Support. Setting modes inappropriately could result in the loss of network element connectivity, policy function, OM statistical data, and cluster redundancy.

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

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

Defining an MRA Cluster Profile

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

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the ALL group.
   The MRA Administration page opens in the work area.
3. On the MRA Administration page, click **Create Multi-protocol Routing Agent**.
   The New MRA page opens.
4. Enter information as appropriate for the MRA cluster:
   a) **Associated Cluster** (required) — Select the MRA cluster from the pulldown list.
   b) **Name** (required) — Enter a name for the MRA cluster.

Enter up to 255 characters. The name can contain any alphanumeric characters except quotation marks (") and commas (,).

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

Enter up to 255 characters.

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

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

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

The default is stateful routing.

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

The MRA cluster profile is defined.

Setting Up an MRA Cluster

To define an MRA cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
The Topology Configuration page opens.
2. Click **Add MPE/MRA Cluster**.
The Cluster Settings Page opens.
3. Enter the following information (*Figure 4: Cluster Settings Page for MRA Cluster* shows an example):
   a) **Name** (required) — Name of the cluster. Enter up to 255 characters, excluding quotation marks (") and commas (,).
   b) **Appl Type** — Select **MRA**.
   c) **Site Preference** — Select **Normal** (the default) or **Reverse**.

   This field only appears on the page if the CMP system supports georedundancy.

   d) **Primary Site** — Select **Unspecified** (the default) or the name of a previously defined site. If you select **Unspecified** you create a non-georedundant site, and you cannot subsequently add a secondary site. You can assign multiple clusters to the same site.
   e) **HW Type** — Select **C-Class** (the default), **C-Class(Segregated Traffic)** (for a configuration in which Signaling and OAM networks are separated onto physically separate equipment), or **RMS** (for a rack-mounted server).
   f) **Network VLAN IDs** (appears if you selected **C-Class** or **C-Class(Segregated Traffic)**) — Enter the Operation, Administration, and Management (OAM), SIG-A, and SIG-B virtual LAN IDs, in the range 1–4095. The defaults are 3 for the OAM VIP and server IP, 5 for the SIG-A VIP, and 6 for the SIG-B VIP.

   The VLAN ID must be part of the device name. For example, if a VIP is on a VLAN with ID=230, the device name for this VIP must be "bond0.230." Enter a VLAN ID for each VIP.

   g) **OAM VIP** (required) — Enter the IPv4 address and mask of the OAM virtual IP (VIP) address. The OAM VIP is the IP address the CMP uses to communicate with the MRA cluster. Enter the address in the standard dot format, and the subnet mask in CIDR notation from 0–32.

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

h) **Signaling VIP 1** through **Signaling VIP 4** — Enter up to four IPv4 or IPv6 addresses and masks of the signaling virtual IP (VIP) addresses; for each, select **None**, **SIG-A**, or **SIG-B** to indicate whether the cluster will use an external signaling network. The Signaling VIP is the IP address a PCEF device uses to communicate with an MRA cluster. (To support redundant communication channels, an MRA cluster uses both **SIG-A** and **SIG-B**.) You must enter a Signaling VIP value if you specify either SIG-A or SIG-B. The IPv6 address subnetwork must be same as the configured IPv6 SIG-A or SIG-B VIP. If you enter an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. If you enter an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

4. Select **Server-A** and enter the following information for the first server of the cluster:
   a) **IP** (required) — The IPv4 address of the server. Enter the standard dot-formatted IPv4 address string.
   b) **HostName** (required) — The name of the server. This must exactly match the host name provisioned for this server (is, the output of the Linux command `uname -n`).
5. Once you define Server A, you can optionally click **Add Server-B** and enter the appropriate information for the second server of the cluster.
6. (Optional) **Secondary Site** — For a georedundant cluster, select the name of a previously defined site. The secondary site name must be different from the primary site name.

   This section only appears on the page if the CMP system supports georedundancy.
7. (Optional) For a georedundant cluster, click **Add Server-C** and enter the appropriate information for the spare server of the cluster.

   This section only appears on the page if the CMP system supports georedundancy. If you define a secondary site, you must define a spare server.
8. When you finish, click **Save** (or **Cancel** to discard your changes).

The MRA cluster is defined.

Once the topology is defined, use the Topology column, on the Reports tab, to determine if there are any topology mismatches.

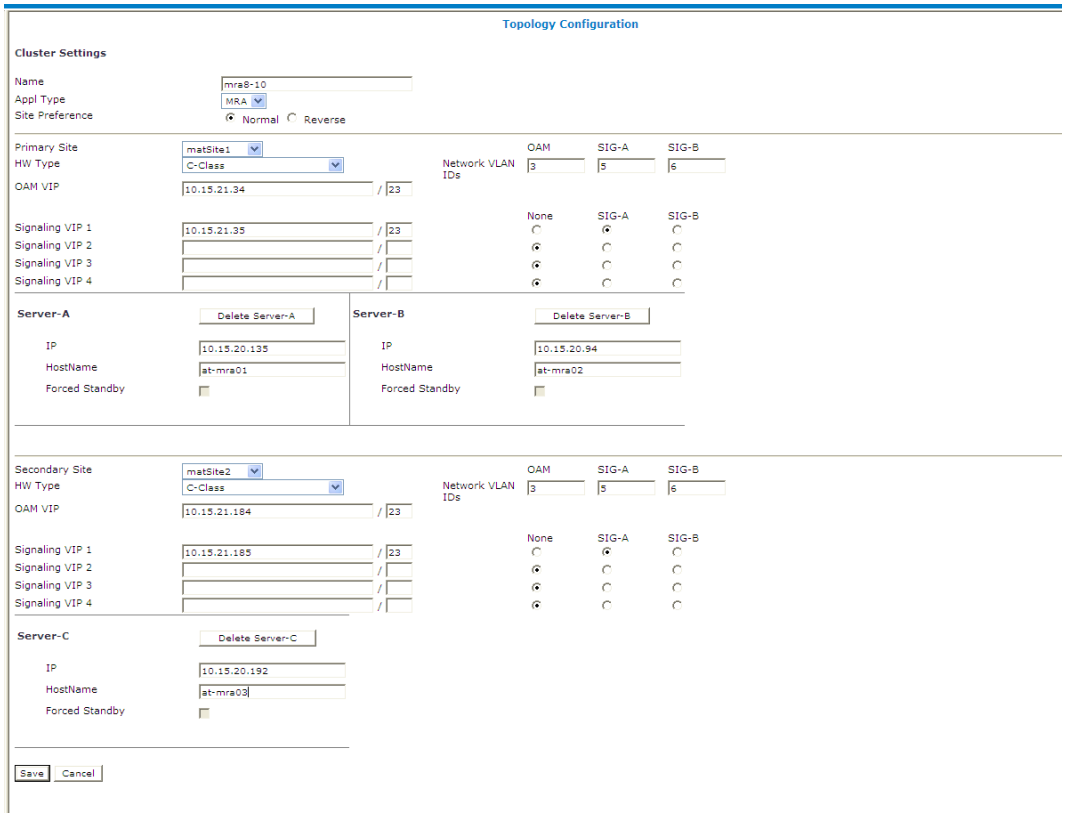


Figure 4: Cluster Settings Page for MRA Cluster

Modifying MRA System Settings, Grouping MRAs, or Deleting MRAs

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

Modifying an MRA Cluster Profile

To modify MRA cluster profile settings:

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

The MRA cluster profile settings are modified.

Creating an MRA Group

To create an MRA group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The MRA Administration page opens in the work area.
3. On the MRA Administration page, click **Create Group**.
   The Create Group page opens.
4. Enter the name of the new MRA group.
5. When you finish, click **Save** (or **Cancel** to abandon your request).
   The new group appears in the content tree.

The MRA group is created.

Adding an MRA Cluster Profile to an MRA Group

Once an MRA group is created, you can add MRA cluster profiles to it. To add an MRA cluster profile to 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 desired MRA group.
   The MRA Administration page opens in the work area, displaying the contents of the selected MRA group.
3. On the MRA Administration page, click **Add Multi-protocol Routing Agent**.
   The Add Multi-protocol Routing Agent page opens.
4. Select the MRA cluster profile you want to add; use the Ctrl or Shift keys to select multiple MRA cluster profiles.
5. When you finish, click **Save** (or **Cancel** to abandon the request).

The MRA cluster profile is added to the MRA group.

Deleting an MRA Cluster Profile from an MRA Group

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

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

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the desired MRA group.
   The MRA Administration page opens in the work area, displaying the contents of the selected MRA group.
3. Remove the desired MRA cluster profile using one of the following methods:
   - On the MRA Administration page, click the Delete icon, located to the right of the MRA cluster profile you want to remove.
   - From the content tree, select the MRA cluster profile; the MRA Administration page opens. On the System tab, click **Remove**.

   The MRA cluster profile is removed from the group.

Deleting an MRA Group

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

To delete an MRA group or sub-group:

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

The MRA group is deleted.

Setting Up a Georedundant MRA Configuration

You can set up georedundant primary and secondary sites when configuring MRA servers.

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

To set up a georedundant configuration for a primary MRA site:

1. From the MRA section of the navigation pane, select **Configuration**.
   The MRA Administration page opens.
2. Select an MRA server.
3. On the MRA tab, click **Modify**.
   The Modify MRA page opens.
4. From the Configuration section of the page, configure the following fields:

   - **Backup MRA**: Select an MRA server.

     Note: The MRA server is configured as the backup. You can have more than one MRA configuration as a pair.

   - **Backup MRA IP Address**: Enter the connected backup MRA signaling address.
   - **Backup MRA Secondary IP Address**: Enter the georedundancy site 2 signaling address for the backup MRA server.
   - **Backup MRA Connect with SCTP**: Select to enable an SCTP connection to the backup MRA server. By default, TCP is used instead of SCTP.

   Note: Any live traffic is disrupted temporarily when a change is made.

5. **Associated MRA**: Select the associated MRA server(s) to be configured as the second backup pair.
6. **Subscriber Indexing**: Select how subscriber data is indexed.
7. When you finish, click **Save** (or **Cancel** to abandon the request).
   Your backup site is created.

Note: You cannot have more than two associated MRA servers with only one backup MRA. While adding an association, the CMP verifies the selected MRA to validate an existing reciprocal relationship. If it is not, you are prompted, "Please make sure MRA1 is also associated MRA2."

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

To configure and modify MRA associated network elements, define a backup MRA, define associated MRAs, or configure MRA Diameter settings, use the MRA tab.

The MRA tab displays the MRA device settings, the associated MPE pool, a list of network elements associated with the MRA, Diameter related configuration information, and settings to specify the backup MRA and associated MRAs. *Figure 5: MRA Tab* shows an example.

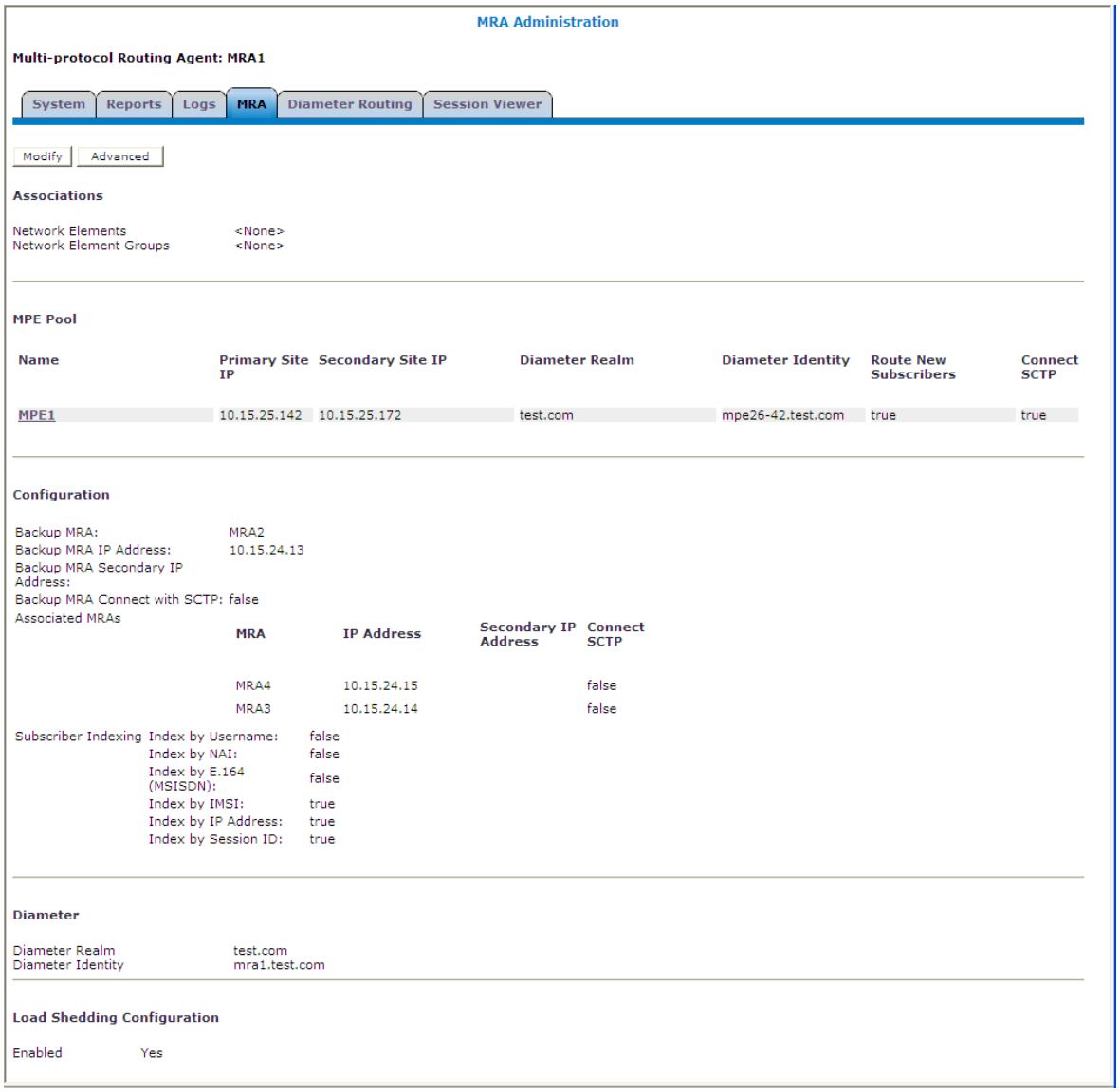


Figure 5: MRA Tab

Associating Network Elements with an MRA

Adding network elements to an MRA is similar to how network elements are added to an MPE: a list of supported network elements, which are pre-entered into the system (refer to the *CMP User's Guide* to add network elements), is available for selection.

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

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

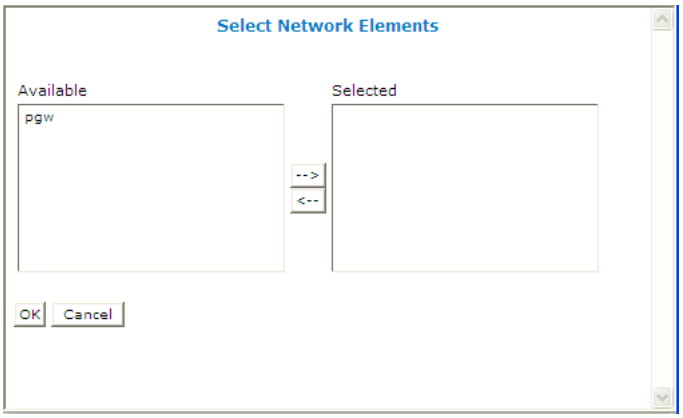


Figure 6: Select Network Elements

3. Select the desired network element and click **OK**.

The network element is added to the MRA.

Configuring the MRA/MPE Pool and Diameter Peer Routing Table

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

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

The MPE can function in the following roles:

1. The MPE is associated with an MRA and participates in an MRA's load balancing action.
2. The MPE is added as a simple Diameter peer for Diameter routing and it does not participate in the MRA's load balancing at all.
3. The MPE serves both roles.

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

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

Associating an MPE with an MRA

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

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

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

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

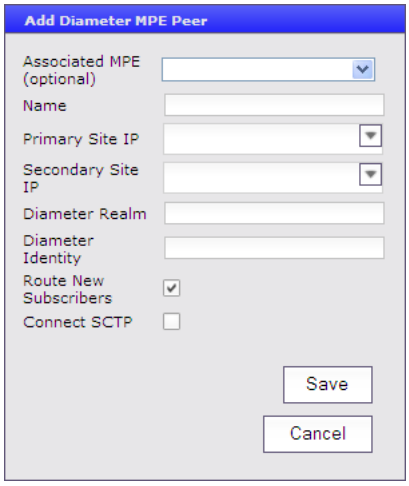


Figure 7: Adding a Diameter MPE Peer

The Add Diameter MPE Peer window opens.

3. Enter the following information:
   a) **Associated MPE** — Select the desired MPE device.
   b) **Name** —
   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** —
   f) **Diameter Identity** —
   g) **Route New Subscribers** —
   h) **Connect SCTP** —
4. When you finish, click **Save** (or **Cancel** to abandon your changes).

The Add Diameter MPE Peer window closes.

The MPE device is added to the MPE pool.

Cloning, Modifying, or Deleting an MPE

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

1. From within the MRA tab, click **Modify**.
2. Click on the desired MPE.
3. Click **Clone**, **Edit**, or **Delete** and enter the desired information or click on **Delete**.
4. If you are cloning or modifying an MPE, when you have finished, click **Save**.

Adding a Backup MRA

The backup MRA field, located within the MRA tab, provides a drop-down list with all qualified backup MRA candidates. All MRAs in this list should be managed by the same CMP.

To qualify as a backup MRA, an MRA cannot already serve as the backup MRA for another MRA. For example, if MRA-C has already been selected to back up MRA-B, MRA-C cannot be qualified as the backup MRA for any other MRAs. Also, if an MRA already exists as a Diameter peer in the Diameter peer routing table that MRA cannot be used as the backup MRA.

Once the backup MRA is selected, the backup relationship is mutual, and the two MRAs back up each other. As a result, if the configuration of an MRA is changed, the CMP updates the backup with the corresponding configuration change (including an MPE pool change).

To configure a backup MRA, complete the following:

1. On the MRA tab, click **Modify**.
   The Modify MRA page opens.
2. In the Configuration section of the page, select a backup MRA from the **Backup MRA** drop-down list.
3. Enter the following information for the backup MRA:
   a) **Backup MRA IP Address** — An IP address, in IPv4 or IPv6 format, used to establish the Diameter connection from the MRA to its backup.

      The CMP does not validate if the specified IP address is correct, only that it is compliant with IPv4 or IPv6 address format.

   b) **Backup MRA Secondary IP Address** — An IP address, in IPv4 or IPv6 format, used to establish the Diameter connection from the MRA to the secondary backup.

      The CMP does not validate if the specified IP address is correct, only that it is compliant with IPv4 or IPv6 address format.

   c) **Backup MRA Connect with SCTP** —
4. When you finish, click **Save** (or **Cancel** to abandon your changes).
   The backup MRA is configured.

Adding Associated MRAs

Each MRA cluster can have a backup MRA and up to two associated MRA clusters.

To configure associated MRAs, complete the following:

1. From within the MRA tab, click **Modify**.
   The Modify MRA page opens.

2. In the Configuration section of the page, select one or two MRA clusters as associated MRAs.

   Do not select the existing backup MRA as an associated MRA; if you try, you will get an error message.

3. Enter an IP address for each selected MRA. The IP address is used to establish the Diameter connection from the MRA to the associated MRA.

   The CMP does not validate if the specified IP address is correct, only that it is in either IPv4 or IPv6 address format.

4. For a georedundant configuration only, enter the secondary IP address for each selected MRA. The IP address is used to establish the Diameter connection to the spare MRA server at the secondary site.

   The CMP does not validate if the specified IP address is correct, only that it is in either IPv4 or IPv6 address format.

5. When you finish, click **Save** (or **Cancel** to abandon your changes).
   If one of the selected MRAs doesn't have a reciprocal association relationship with the target MRA, you are prompted, "Please make sure MRA 1 is also associated with MRA 2". If this message appears, use the procedure in *Adding a Backup MRA* to establish the second associated MRA as the backup for the first associated MRA.

The selected MRA clusters are configured as associated MRAs.

Modifying Backup and Associated MRAs

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

To modify backup and associated MRAs:

1. From within the MRA tab, click **Modify**.
   The Modify MRA page opens.
2. The functions available from the table are as follows:

   - **To add an MRA to the table** — Click **Add**; the Select MRA window opens. Select an MRA. If this is a backup MRA, check **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 that MRA's information filled in. Make changes as required.
   - **To edit an MRA in the table** — Select the MRA and click **Edit**; the Edit MRA window opens with that MRA's information filled in. Make changes as required.
   - **To delete an MRA from the table** — Select the MRA and click **Delete**; you are prompted, "Are you sure you want to delete the selected MRA?" Click **Delete** to remove the MRA (or **Cancel** to cancel your request).

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

Configuring Diameter Routing

The Diameter Routing tab is used to configure the MRA so that the MPE will continue to be available for the MRA. In addition to the entries in the peer table, the MPEs in the MRA's MPE pool should also be available to participate in Diameter peer routing. So the entries in the Diameter Peer Table could

be added from either the Diameter routing page or from the MPE association page. However, the same MPE can only appear in either the peer table or the pool and can't appear in both.

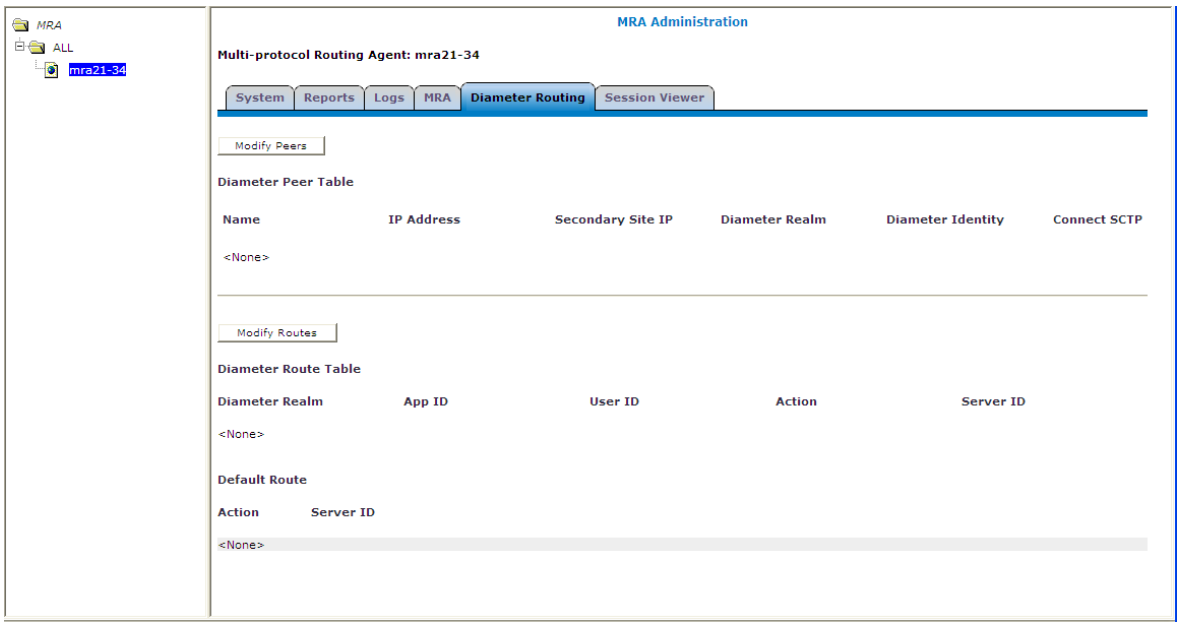


Figure 8: Diameter Routing Tab

To add a Diameter peer:

1. From the Diameter Routing tab, click **Modify Peers**.
   The Add Diameter Peer window opens.
2. Select a configured MRA or MPE from the drop-down list.
3. Enter the following:

   - **Name** — Enter the name of the peer device (which must be unique in the CMP database).
   - **Primary Site IP** — Enter the IP address, in IPv4 or IPv6 format, of the primary site.
   - **Secondary Site IP** — For georedundant configurations, enter the IP address, in IPv4 or IPv6 format, of the server at the secondary site.
   - **Diameter Realm** — Enter the peer's domain of responsibility (for example, `galactelEU.com`).
   - **Diameter Identity** — Enter a fully qualified domain name (FQDN) or the peer device (for example, `MRA10-24.galactel.com`).

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

Role and Scope Configuration

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

MRA Role Configuration

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

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

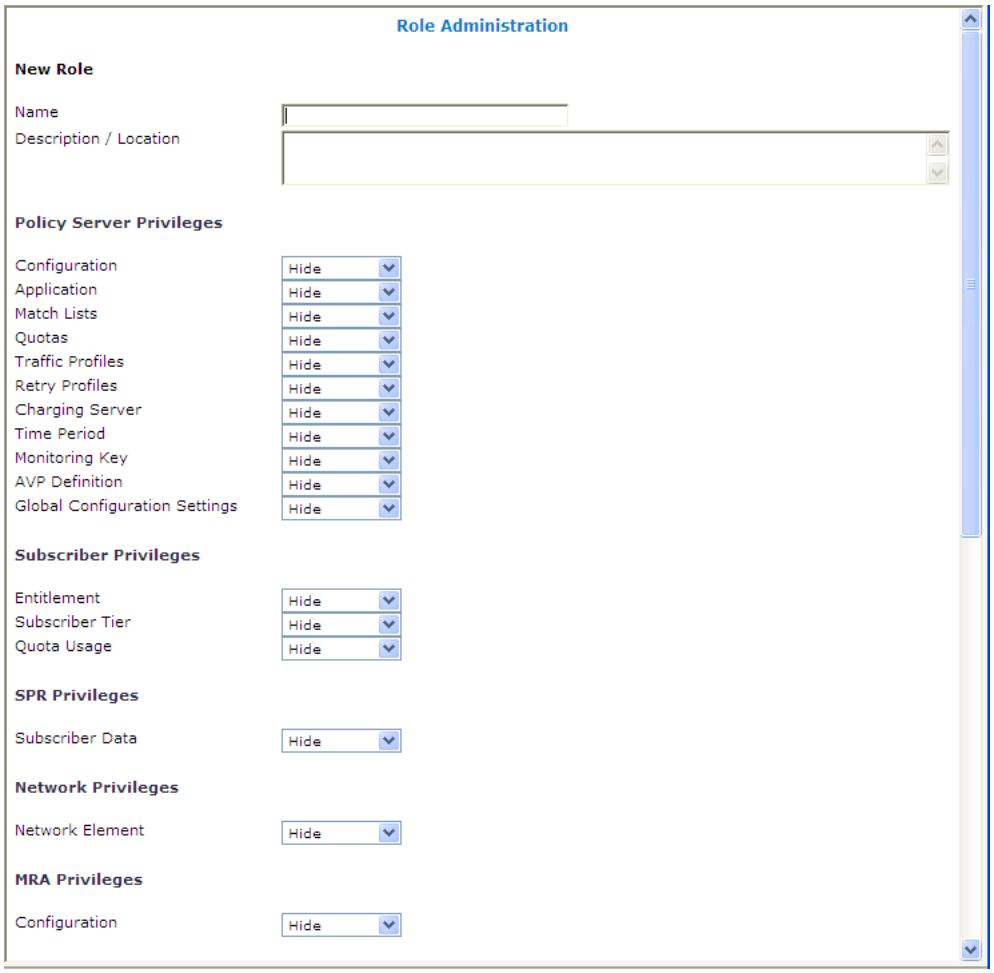


Figure 9: New Role Page

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

- **Hide** — No operation can be done on MRA configuration.

- **Read-Only** — Only read operations can be done on MRA configuration (that is, settings may be viewed but not changed).
- **Read-Write** — Both read and write operations can be done on MRA configuration (that is, settings may be viewed and changed).

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

MRA Scope Configuration

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

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

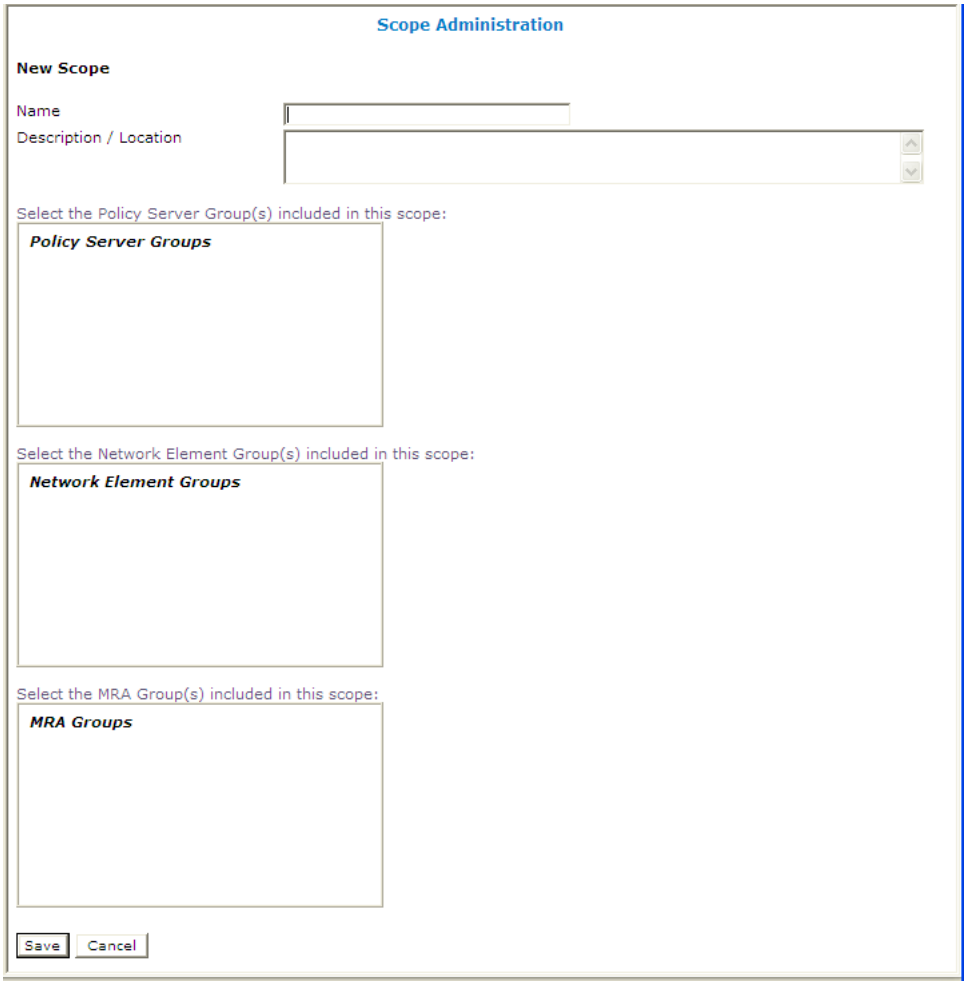


Figure 10: Create Scope Page

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

Configuring Stateless Routing

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

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

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

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

Enabling Stateless Routing

To enable stateless routing, from within the MRA creation page or within the System Tab page for the MRA, select **Stateless Routing** (*Figure 11: Enabling Stateless Routing* shows an example).

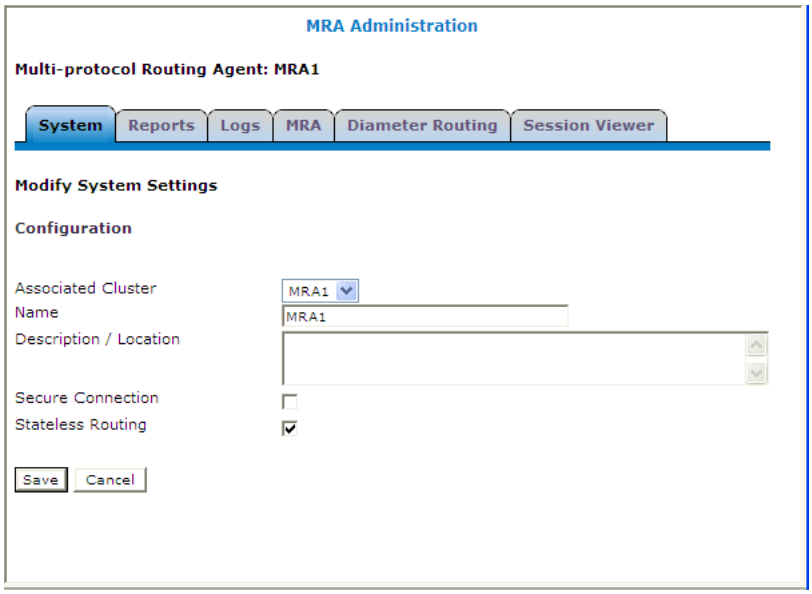


Figure 11: Enabling Stateless Routing

Enabling and Disabling Migration Mode

Enabling the migration mode setting permits the MRA device to use static routes to transition to a stateful mode. You can also disable the migration mode setting.

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 desired 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 desire to enable the migration mode).
   The stateless migration mode is enabled.
6. Click **Save** (or **Cancel** to abandon your change).

The MRA device is put into migration mode.

Loading MPE/MRA Configuration Data when Adding Diameter Peer

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

Configuring Diameter Routes

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

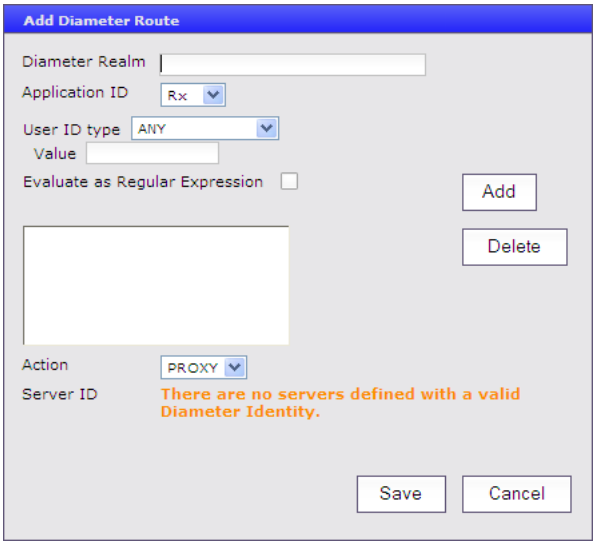
To configure the Diameter route table:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups.
2. From the content tree, select the desired policy server.
   The Policy Server Administration page opens in the work area.
3. On the Policy Server Administration page, select the **Diameter Routing** tab.
   The Diameter Routing configuration settings are displayed.
4. Click **Modify Routes**.

   The Modify the Diameter Route Table page opens.

   The functions available from this table are as follows:

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



The fields are as follows:

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

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

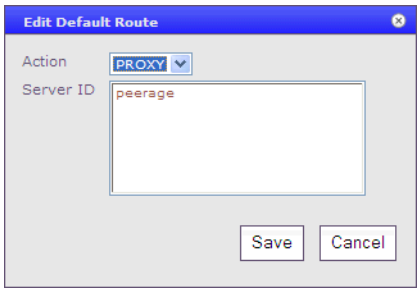
- **User ID type** — Select **ANY** (the default), **E.164(MSISDN)**, **IMSI**, **IP**, **NAI**, **PRIVATE**, **SIP_URI**, or **USERNAME**.
- **Value** — Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); use an asterisk (*) as a wildcard character.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

  Note: If desired, you can define a server with a Diameter identity.

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

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

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



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

The Diameter routes are configured.

MRA Advanced Configuration Settings

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

Configuring MRA Session Clean Up Settings

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

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

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

To customize stale session cleanup:

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

Table 2: Session Clean Up Settings

Attribute	Description
Check for Stale Sessions in Binding	Select to check for stale sessions in bindings during the cleanup cycle. If not selected, then the system only checks to see if the entire binding is stale. The default is selected (check for stale sessions).
Check for Stale Bindings	Select to check for stale bindings during the cleanup cycle. If not selected, then the system will not check if the binding is stale. If **Check For Stale Sessions in Binding** is selected, then the system still iterates through the enclosed session information to detect and clean up stale sessions. The default is deselected (do not check for stale bindings).
Check for Suspect Bindings	Select to check for suspect bindings during the cleanup cycle. If not selected, the system checks if the entire binding is stale. If **Check for Stale Sessions In Binding** is selected, stale sessions enclosed in the suspect binding are cleaned up as well. The default is selected (check for suspect bindings).
Session Cleanup Start Time	Defines the time of day when the cleanup task occurs. Specify either **Start Time** or **Interval** by clicking the associated radio button and entering or selecting a value. You can specify a time in 24-hour format from the drop-down menu. No default value is defined.
Binding Cleanup Interval (hour)	Defines the interval, in hours, at which the cleanup task runs. Specify either **Start Time** or **Interval** by clicking the associated radio button and entering or selecting a value from 0 to 24 hours. A value of 0 disables cleanup. The default is 24 hours. **Note:** Do not modify this setting without consulting Tekelec Customer Service.
Max Duration For Binding Iteration (hour)	Defines the maximum duration, in hours, to iterate through the bindings. The default is 2 hours. The valid range is 1 to 2 hours. **Note:** Do not modify this setting without consulting Tekelec Customer Service.
Binding Validity Time (hours)	Defines the number of hours after which the binding is declared stale. The default is 240 hours. The valid range is 1 to 240 hours.
Max Binding Cleanup Rate (bindings/sec)	Defines the rate, in bindings per second, at which the cleanup task attempts to clean stale bindings. The default is 50 sessions/sec. The valid range is 1 to 50 sessions/sec. **Note:** Do not modify this setting without consulting Tekelec Customer Service.

Max Binding Iteration Rate (bindings/sec)	Defines the maximum rate, in bindings per second, at which the cleanup task iterates through the bindings database. The default is 1000 bindings/sec. The valid range is 1 to 1000 bindings/sec. **Note:** Do not modify this setting without consulting Tekelec Customer Service.
Max Iteration Burst Size	Define the number of iterations which can be processed before the rate is limited. This is the Token Bucket size. The default is 1000 iterations. The valid range is 1 to 1000 iterations. **Note:** Do not modify this setting without consulting Tekelec Customer Service.
Scheduler Granularity (sec)	Defines the adaptor scheduler's granularity in seconds. The default is 1 second. The valid range is 1-5 seconds.
Scheduler Thread Count	Defines the number of threads used by the cleanup scheduler to schedule jobs. The default is 2 threads. the valid range is 1 to 4 threads.
Cleanup Session Validity Time (hours)	Defines the number of hours after which a session in a binding is declared stale. the default is 120 hours. The valid range is 1 to 120 hours.

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

Working with Stateful MRAs

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

Enabling and Disabling Migration Mode

Enabling the migration mode setting permits the MRA device to use static routes to transition to a stateful mode. You can also disable the migration mode setting.

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 desired 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 desire to enable the migration mode).
   The stateless migration mode is enabled.
6. Click **Save** (or **Cancel** to abandon your change).

The MRA device is put into migration mode.

Redirecting Traffic to Upgrade or Remove an MRA

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

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

Changing Redirect States

To change the redirect state of an MRA device:

1. In the MRA section of the navigation bar, click **Configuration**.
2. Select the desired MRA. The MRA Administration page displays information about the selected MRA.
3. On the **MRA** tab, click **Advanced**.
4. In the **Other Advanced Configuration Settings** section, click the **Add** icon in the table. The Add Configuration Key Value window opens (*Figure 12: Add Configuration Key Value Window*).

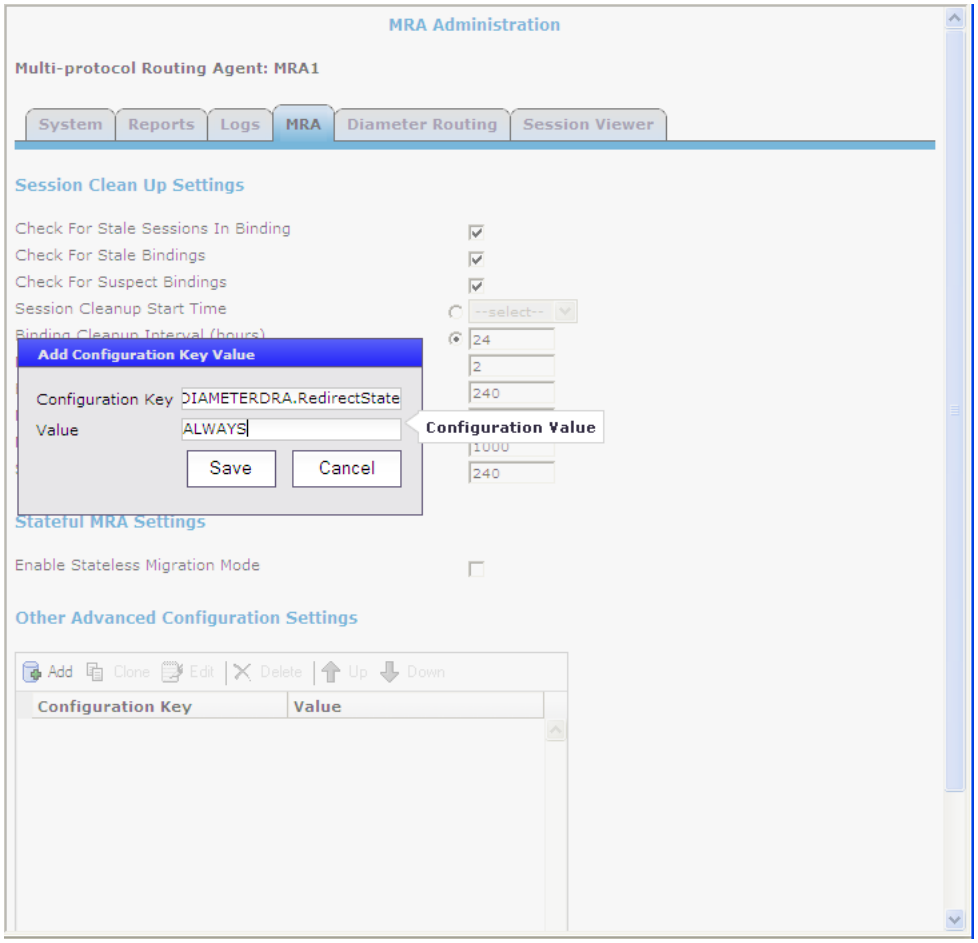


Figure 12: Add Configuration Key Value Window

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

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

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

Releasing Active Sessions

Release configuration settings allow the MRA to release active subscribers and remove their bindings. These settings allow a task to be started that iterates through the bindings in the database and sends RARs for each session contained in each binding. These RARs indicate a session release cause, triggering

the PGW/HSGW to terminate the corresponding sessions. Upon receiving a message to terminate the session, the MRA removes the session from the binding, and once the binding no longer has any sessions associated with it, it is removed as well. Any new sessions will be redirected to the other, 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.

Reversing Cluster Preference

You can change the preference, or predilection, of the servers in a cluster to be active or spare.

To reverse cluster preference:

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

The cluster preferences are reversed.

Forcing a Server into Standby Status

You can change the status of an active or spare server in a cluster to Standby. You would do this, for example, to the active server prior to performing maintenance on it.

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

- If the server is active, it demotes itself.

- The server will not assume the active role, regardless of the status or roles of the other servers in the cluster.
- The server continues as part of its cluster, and reports its status as "Forced-Standby."

To force a server into standby status:

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

The server is placed in standby status.

Chapter 4

Monitoring the MRA

Topics:

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

- Cluster and blade information
- DRMA information
- Event logs

Displaying Cluster and Blade Information

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

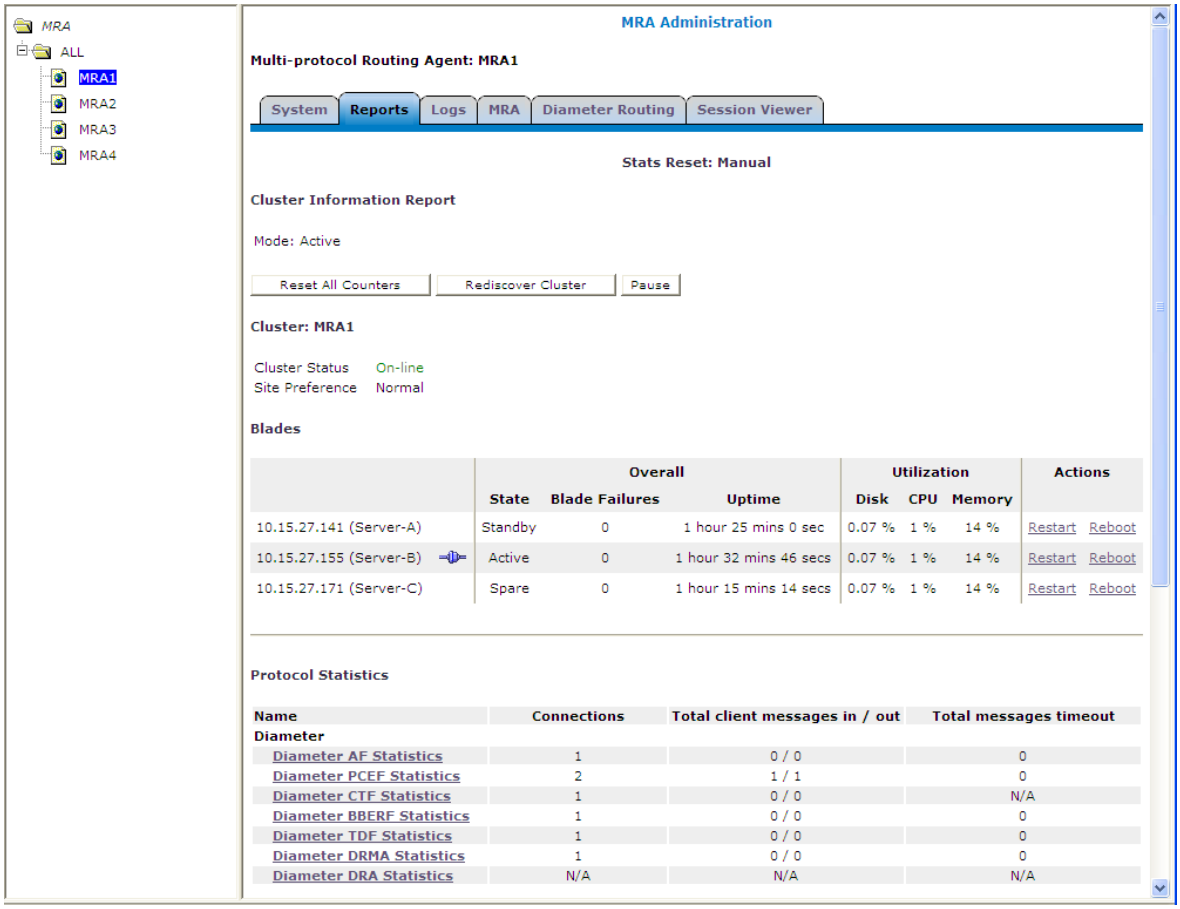


Figure 13: Cluster, Blade, and Diameter Information

The following is a list of Diameter statistics:

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

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

Viewing Trace Logs

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

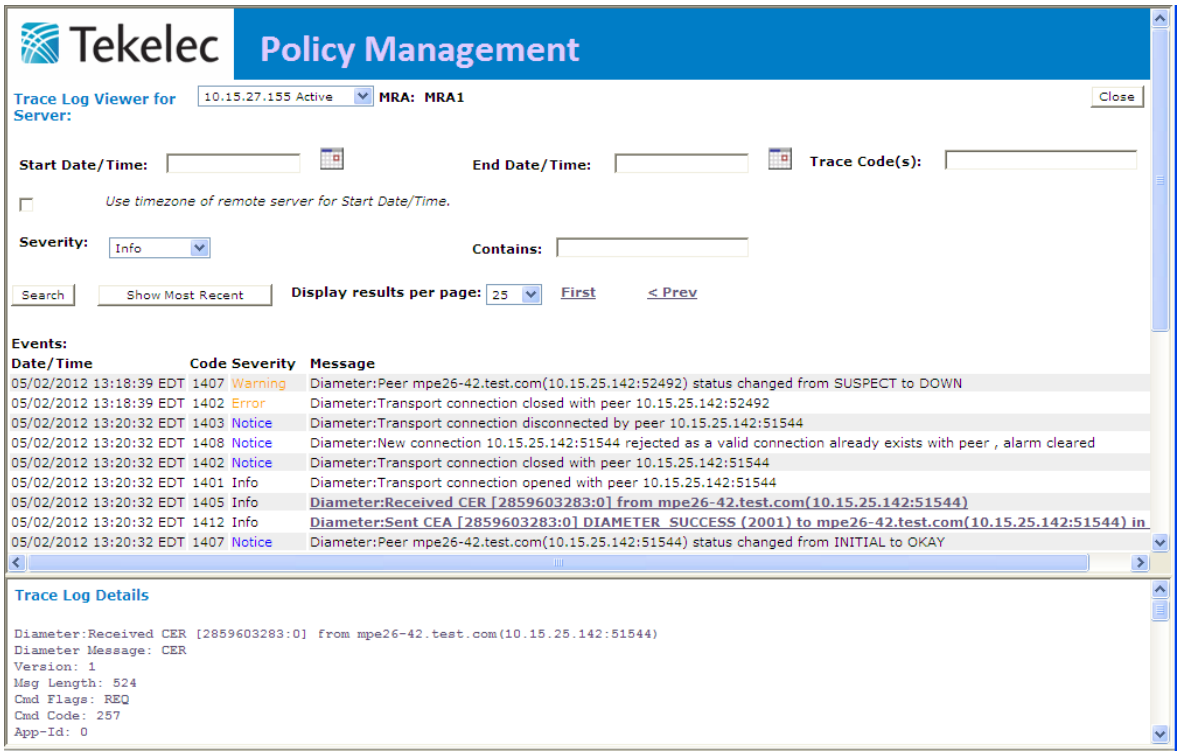


Figure 14: MRA Trace Log

KPI Dashboard

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

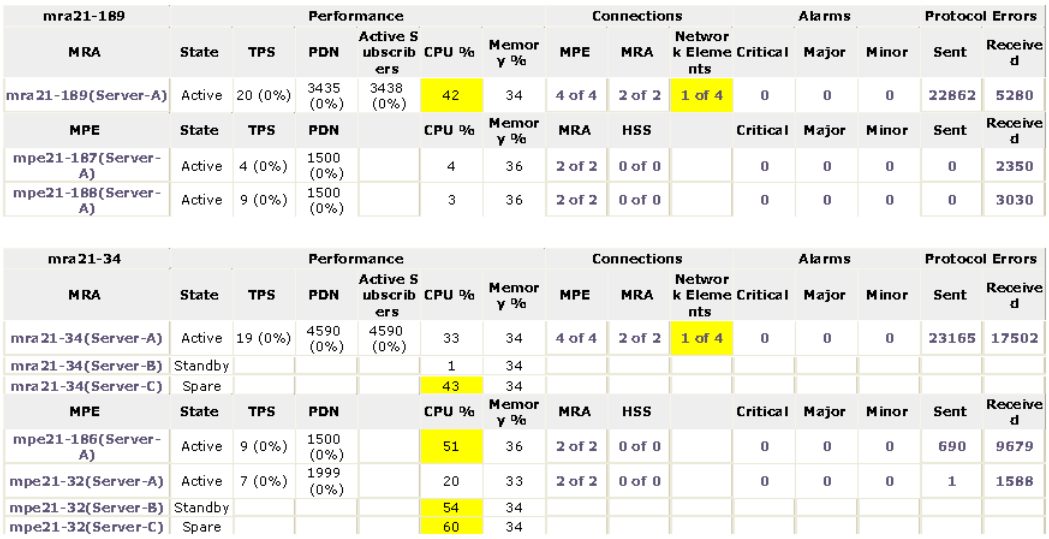
- Offered load (transaction rate)
- System capacity (counters for active sessions)
- Inter-system connectivity
- Physical resource utilization (memory, CPU)
- System status

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

The KPI dashboard displays the indicators for all the systems on a single page, with each MRA's KPIs in a separate table. Each row within a table represents a single system (either an MRA blade or an MPE blade that is being managed by that MRA). The table cells are rendered using a color scheme to highlight areas of concern that is well adapted by the telecommunication industry. The table contents

are periodically refreshed. The color changing thresholds are user configurable. The refresh rate is set to 10 seconds and is not configurable.

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



mra21-189			Performance				Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra21-189(Server-A)	Active	20 (0%)	3435 (0%)	3438 (0%)	42	34	4 of 4	2 of 2	1 of 4	0	0	0	22862	5280
MPE	State	TPS	PDN		CPU %	Memory %	MRA	HSS		Critical	Major	Minor	Sent	Received
mpe21-187(Server-A)	Active	4 (0%)	1500 (0%)		4	36	2 of 2	0 of 0		0	0	0	0	2350
mpe21-188(Server-A)	Active	9 (0%)	1500 (0%)		3	36	2 of 2	0 of 0		0	0	0	0	3030

mra21-34			Performance				Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra21-34(Server-A)	Active	19 (0%)	4590 (0%)	4590 (0%)	33	34	4 of 4	2 of 2	1 of 4	0	0	0	23165	17502
mra21-34(Server-B)	Standby				1	34								
mra21-34(Server-C)	Spare				43	34								
MPE	State	TPS	PDN		CPU %	Memory %	MRA	HSS		Critical	Major	Minor	Sent	Received
mpe21-186(Server-A)	Active	9 (0%)	1500 (0%)		51	36	2 of 2	0 of 0		0	0	0	690	9679
mpe21-32(Server-A)	Active	7 (0%)	1999 (0%)		20	33	2 of 2	0 of 0		0	0	0	1	1588
mpe21-32(Server-B)	Standby				54	34								
mpe21-32(Server-C)	Spare				60	34								

Figure 15: KPI Dashboard

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

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

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

The columns that display "TPS"[1] (on the MPE - the number of Diameter Requests (per second) received from the Clients) and "PDN Connections" information is displayed in the form X (Y%) where X represents the actual numeric value and Y represents the % of rated system capacity that is consumed.

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

[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 the number of Diameter Requests per second sent to the HSS.

Mapping Reports Display to KPIs

From the KPI Dashboard, you can click on any MPE or MRA 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 the name as it appears in OSSI XML output.

Table 3: Diameter Application Function (AF) Stats

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 sent/received	Y	Y	AAR Recv Count\AAR Send Count
AAR initial messages recd /sent	Y	Y	AAR Initial Recv Count\AAR Initial Send Count
AAR modification messages recd/sent	Y	Y	AAR Modification Recv Count\AAR Modification Send Count
AAA success messages recd/sent	Y	Y	AAA Recv Success Count\AAA Send Success Count
AAA failure messages recd/sent	Y	Y	AAA Recv Failure Count\AAA Send Failure Count
AAR messages timeout	Y	Y	AAR Timeout Count
ASR messages recd/sent	Y	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	Y	Y	ASR Timeout Count
ASA success messages recd/sent	Y	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages recd/sent	Y	Y	ASA Recv Failure Count\ASA Send Failure Count
RAR messages recd/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages recd/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd /sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages recd/sent	Y	Y	STR Recv Count\STR Send Count

Display	MPE	MRA	Name
STR messages timeout	Y	Y	STR Timeout Count
STA success messages recd /sent	Y	Y	STA Recv Success Count\STA Send Success Count
STA failure messages recd/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
Diameter AF Peer Stats (in Diameter AF Stats window)	N	Y	
Connect Time	N	Y	Connect Time
Disconnect Time	N	Y	Disconnect Time
Connection Type			
IP Address: Port			
Total messages in/out	N	Y	Msg In Count\Msg Out Count
Total error messages in/out			
AAR messages sent/received	N	Y	AAR Recv Count\AAR Send Count
AAR initial messages recd/sent	N	Y	AAR Initial Recv Count\AAR Initial Send Count
AAR modification messages recd/sent	N	Y	AAR Modification Recv Count\AAR Modification Send Count
AAA success messages recd/sent	N	Y	AAA Recv Success Count\AAA Send Success Count
AAA failure messages recd/sent	N	Y	AAA Recv Failure Count\AAA Send Failure Count
AAR messages timeout	N	Y	AAR Timeout Count
ASR messages recd/sent	N	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	N	Y	ASR Timeout 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
RAR messages recd/sent	N	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	N	Y	RAR Timeout Count

Display	MPE	MRA	Name
RAA success messages recd/sent	N	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages rec/sent	N	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages recd/sent	N	Y	STR Recv Count\STR Send Count
STR messages timeout	N	Y	STR Timeout Count
STA success messages rec/sent	N	Y	STA Recv Success Count\STA Send Success Count
STA failure messages recd/sent	N	Y	STA Recv Failure Count\STA Send Failure Count

Table 4: 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/reopned 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 recd/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages recd/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages recd/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 recd/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages recd/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages recd/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 recd/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count

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

Table 5: Diameter Charging Function (CTF) Statistics

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

Display	MPE	MRA	Name
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 6: 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
CCR messages sent/received	Y	Y	CCR Recv Count\CCR Send Count

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

Table 7: 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 sent/received	Y	Y	CCR Recv Count\CCR Send Count
CCR messages Timeout	Y	Y	CCR-Timeout Count
CCA success messages recd/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-U messages sent/received	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages Timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages recd/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages recd/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages sent/received	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages Timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages recd/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages recd/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages sent/received	Y	Y	RAR Recv Count\RAR Send Count
RAR messages Timeout	Y	Y	RAR Timeout Count
RAA success messages recd/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
TSR messages sent/received	Y	Y	
TSA success messages recd/sent	Y	Y	
TSA failure messages recd/sent	Y	Y	

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

Table 8: Diameter Distributed Routing and Management Application (DRMA) 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
DBR messages recd/sent	Y	Y	DBRRecv Count\DBRSend Count
DBR messages timeout	Y	Y	DBRTimeout Count
DBA success messages recd/sent	Y	Y	DBARecv Success Count\DBASend Success Count
DBA failure messages recd/sent	Y	Y	DBARecv Failure Count\DBASend Failure Count
DBA messages recd/sent – binding found	Y	Y	Binding Found Recv Count\Binding Found Send Count
DBA messages recd/sent – binding not found	Y	Y	Binding Not Found Recv Count\Binding Not Found Send Count
DBA messages recd/sent – PCRF down	Y	Y	Binding Found Pcrf Down Recd Count\ Binding Found Pcrf Down Send Count
DBA messages recd/sent – all PCRFs down	Y	Y	All Pcrfs Down Recv Count\ All Pcrfs Down Send Count
RUR messages recd/sent	Y	Y	RURRecv Count\ RURSend Count
RUR messages timeout	Y	Y	RURTimeout Count
RUA success messages recd/sent	Y	Y	RUARecv Success Count\ RUASend Success Count
RUA failure messages recd/sent	Y	Y	RUARecv Failure Count\ RUASend Failure Count
LNR messages recd/sent	Y	Y	LNRRecv Count\ LNRSend Count
LNR messages timeout	Y	Y	LNRTimeout Count

Display	MPE	MRA	Name
LNA success messages recd/sent	Y	Y	LNARecv Success Count\ LNASend Success Count
LNA failure messages recd/sent	Y	Y	LNARecv Failure Count\ LNASend Failure Count
LSR messages recd/sent	Y	Y	LSRRecv Count\ LSRSend Count
LSR messages timeout	Y	Y	LSRTimeout Count
LSA success messages recd/sent	Y	Y	LSARecv Success Count\ LSASend Success Count
LSA failure messages recd/send	Y	Y	LSARecv Failure Count\ LSASend Failure Count

Table 9: 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 10: Diameter Latency Statistics shows information for these Diameter Statistics:

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

- Distributed Routing and Management Application (DRMA)

Table 10: 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 11: Diameter Event Trigger Statistics

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

Table 12: Diameter Protocol Error Statistics

Display	MPE	MRA	Name
Total errors recd	Y	Y	In Error Count

Display	MPE	MRA	Name
Total errors sent	Y	Y	Out Error Count
Last time for total error recd	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 13: Diameter Connection Error Statistics

Display	MPE	MRA	Name
Total errors recd	Y	Y	In Error Count
Total errors sent	Y	Y	Out Error Count
Last time for total error recd	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 14: KPI Interval Statistics

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

Table 15: Policy Statistics

Display	MPE	MRA	Name
Peg Count	Y	N	
Evaluated	Y	N	

Display	MPE	MRA	Name
Executed	Y	N	
Ignored	Y	N	
Policy Details Stats:			
Policy TDF session	Y	N	
Name	Y	N	
Evaluated	Y	N	Eval Count
Executed	Y	N	Trigger Count
Ignored	Y	N	
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	
Policy ADC-Rule-Install	Y	N	
Name	Y	N	
Evaluated	Y	N	
Executed	Y	N	
Ignored	Y	N	
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	
Policy write state on session create	Y	N	
Name	Y	N	

Display	MPE	MRA	Name
Evaluated	Y	N	
Executed	Y	N	
Ignored	Y	N	
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	
Policy write state on session termination	Y	N	
Name	Y	N	
Evaluated	Y	N	
Executed	Y	N	
Ignored	Y	N	
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	

Table 16: Quota Profile Statistics Details

Display	MPE	MRA	Name
Peg Count	Y	N	
Application	Y	N	
Session	Y	N	
Total	Y	N	

Table 17: Diameter Sh Statistics

Display	MPE	MRA	Name
UDR messages recd/sent	Y	N	UDR Recv Count\UDR Send Count
UDR messages timeout	Y	N	UDR Timeout Count
UDA success messages recd/sent	Y	N	UDA Recv Success Count\UDA Send Success Count
UDA failure messages recd/sent	Y	N	UDA Recv Failure Count\UDA Send Failure Count
PNR messages recd/sent	Y	N	PNR Recv Count\PNR Send Count
PNA success messages recd/sent	Y	N	PNA Recv Success Count\PNA Send Success Count
PNA failure messages recd/sent	Y	N	PNA Recv Failure Count\PNA Send Failure Count
PUR messages recd/sent	Y	N	PUR Recv Count\PUR Send Count
PUR messages timeout	Y	N	PUR Timeout Count
PUA success messages recd/sent	Y	N	PUA Recv Success Count\PUA Send Success Count
PUA failure messages recd/sent	Y	N	PUA Recv Failure Count\PUA Send Failure Count
SNR messages recd/sent	Y	N	SNR Recv Count\SNR Send Count
SNR messages timeout	Y	N	SNR Timeout Count
SNA success messages recd/sent	Y	N	SNA Recv Success Count\SNA Send Success Count
SNA failure messages recd/sent	Y	N	SNA Recv Failure Count\SNA Send Failure Count
Currently active sessions Y N Active Session Count			
Max active sessions	Y	N	Max Active Session Count
Diameter Sh connections	Y	N	Connect Count

Table 18: Sh Data Source Stats

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count

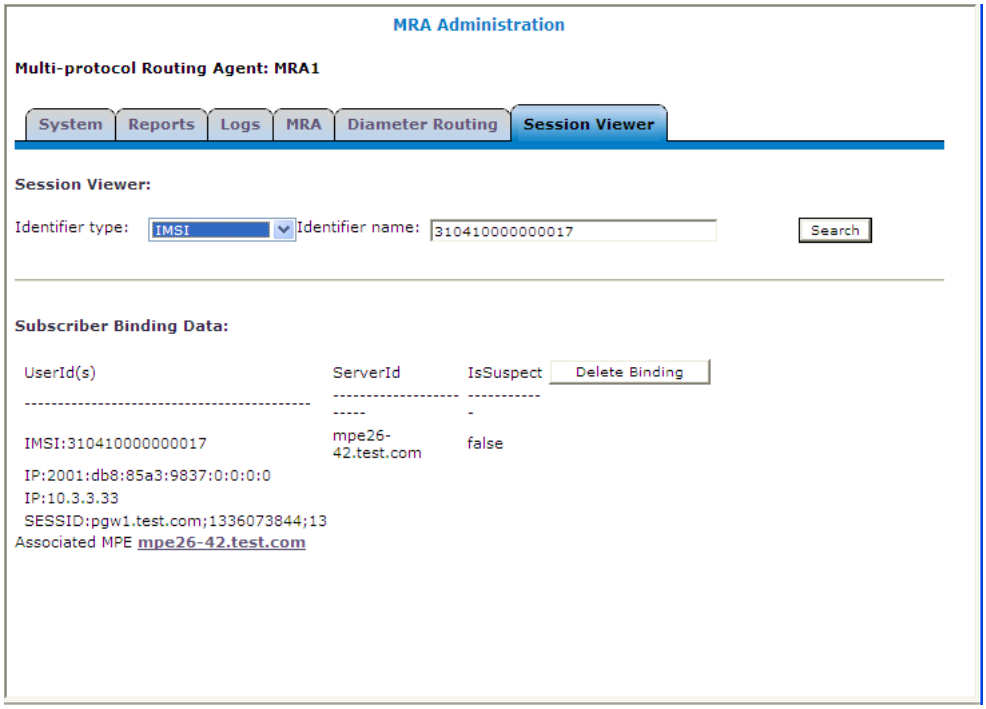
Display	MPE	MRA	Name
Number of searches that failed because of errors	Y	N	Search Err Count
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Avg Time spent on successful search (ms)	Y	N	Search Avg Hit Time
Avg Time spent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

Display	MPE	MRA	Name
Max Time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Max Miss Time
Avg Time spent on successful subscriptions (ms)	Y	N	Subscription Avg Hit Time
Avg 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
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 unsubscriptions (ms)	Y	N	Unsubscription Max Hit Time
Max Time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Max Miss Time
Avg Time spent on successful unsubscriptions (ms)	Y	N	Unsubscription Avg Hit Time
Avg Time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Avg Miss Time

The Subscriber Session Viewer

The Session Viewer displays detailed session information for a specific subscriber. This information is contained within 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.

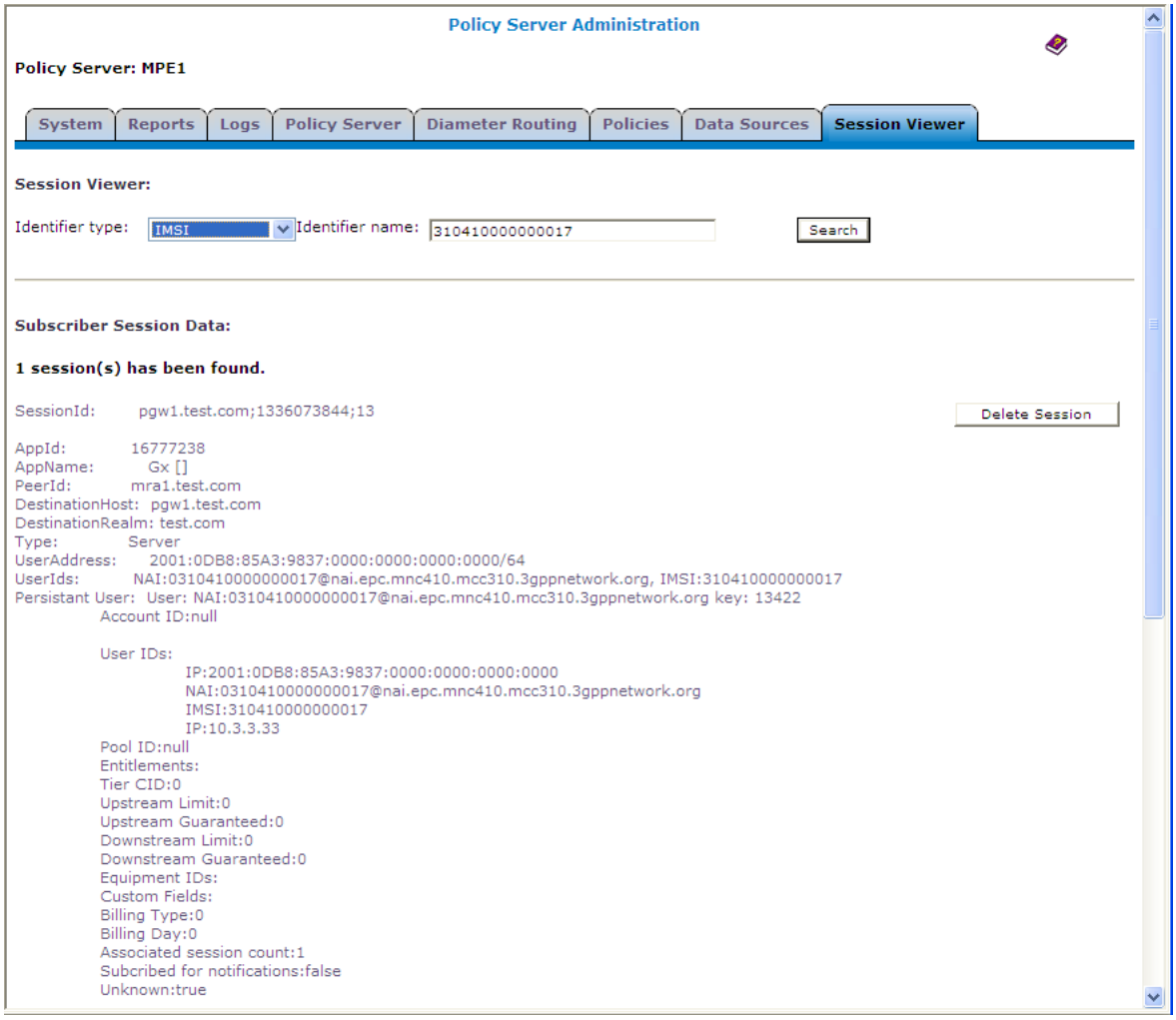
Within the session viewer, you can enter query parameters to render session data for a specific subscriber. For example:



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:

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



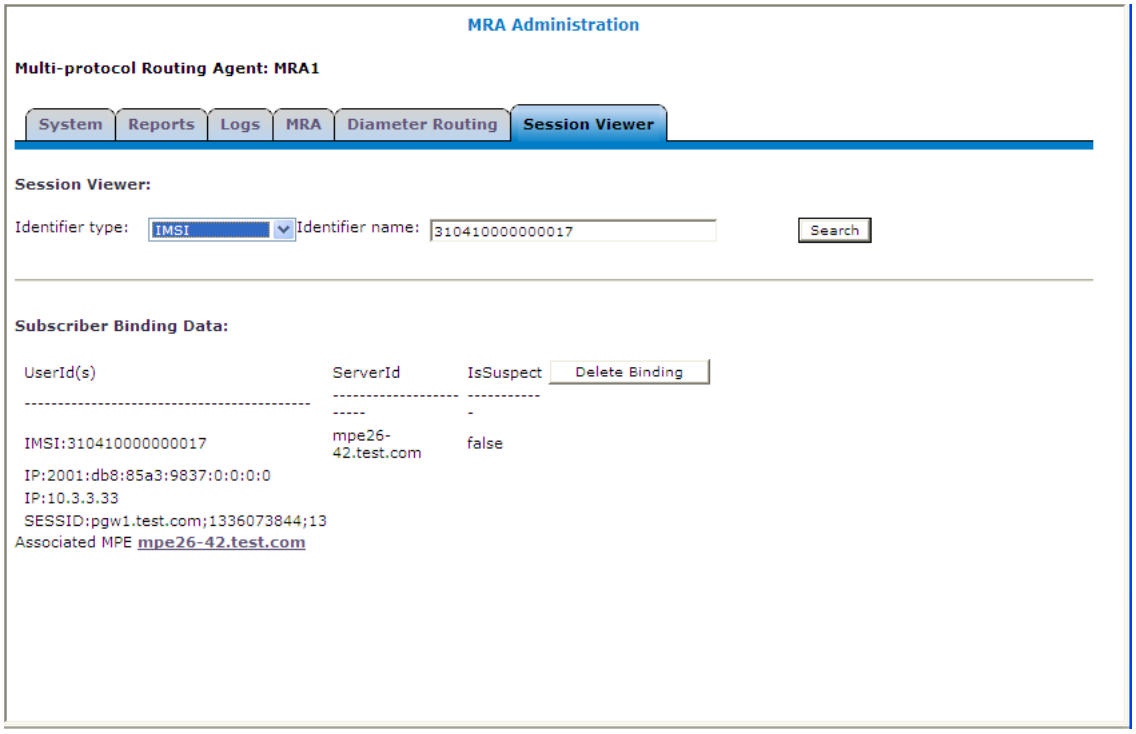
The MRA device is listed by its peer ID.

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

Viewing Session Data from the MRA

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

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



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

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

Deleting a Session from the Session Viewer Page

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

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

Glossary

C

CPU	Central Processing Unit
CTF	Charging Trigger Function

D

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

G

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

H

HSS	Home Subscriber Server A central database for subscriber information.

K

K

KPI	Key Performance Indicators

P

PCC	Policy and Charging Control
PDN	Packet Data Network A digital network technology that divides a message into packets for transmission. Public Data Network A data network that uses the X.25 protocol to provide the connectivity.
policy server	A network element that interfaces with an application and makes policy decisions, such as authorization, entitlements, bandwidth, and QoS, based on the application's requirements and operator rule sets. The Camiant policy server is the Multimedia Policy Engine (MPE).

R

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

S

SSL	Secure Socket Layer

X

XML	eXtensible Markup Language A version of the Standard Generalized Markup Language (SGML) that allows Web developers

X

to create customized tags for additional functionality.