**Oracle® Diameter Signaling Router**

DSR Network Impact Report

Release 7.1

**DSR**-**7.1.0.0.0-71.24.0**

**E57811-05**

Dec 2015



Oracle Diameter Signaling Router DSR Network Impact Report, Release 7.1

Copyright © 2011-2015 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

**TABLE OF CONTENTS**

[1 Introduction 6](#_Toc436827291)

[***1.1*** ***Purpose/Scope*** 6](#_Toc436827292)

[***1.2*** ***Disclaimers*** 6](#_Toc436827293)

[2 Overview of DSR 7.1 Features 6](#_Toc436827294)

[**2.1** **DSR 7.1 New Features** 7](#_Toc436827295)

[**2.2** **DSR 7.1 Redirect** 7](#_Toc436827296)

[**2.3** **DSR 7.1 Enhanced Suspect Binding Cleanup** 9](#_Toc436827297)

[**2.4** **DSR 7.1 IPv6 support** 10](#_Toc436827298)

[**2.5** **DSR 7.1 SBR Reconfiguration** 10](#_Toc436827299)

[**2.6** **DSR 7.1 DSR Dashboard** 12](#_Toc436827300)

[**2.7** **DSR 7.1 Configuration and Performance** 13](#_Toc436827301)

[**2.8** **DSR 7.1 Upgrades** 14](#_Toc436827302)

[**2.9** **DSR 7.1 Network Integrated DIH (IDIH)** 16](#_Toc436827303)

[**2.10** **DSR 7.1 Routing Attributes by (Extended) Command Code** 17](#_Toc436827304)

[**2.11** **DSR Signaling Port Range Management and IPFE Initiator** 18](#_Toc436827305)

[**2.12** **DSR TLS/DTLS Support** 19](#_Toc436827306)

[**2.13** **Egress Throttling Enhancements** 20](#_Toc436827307)

[**2.14** **Mediation Enhancements** 21](#_Toc436827308)

[**2.15** **SDS Service Continuity** 22](#_Toc436827309)

[**2.16** **Hardware Changes** 23](#_Toc436827310)

[**2.16.3** **Software Changes** 23](#_Toc436827311)

[**2.17** **Firmware Changes** 24](#_Toc436827312)

[**2.18** **Upgrade Overview** 24](#_Toc436827313)

[**2.19** **Migration of DSR Data** 25](#_Toc436827314)

[3 Changes by Feature 26](#_Toc436827315)

[4 Administration (NOAM) 26](#_Toc436827316)

[**4.1** **Software Management -> Upgrade (Auto Upgrade)** 26](#_Toc436827317)

[5 Diameter Common (NOAM) 27](#_Toc436827318)

[**5.1** **Dashboard** 27](#_Toc436827319)

[**5.2** **Network Identifiers** 30](#_Toc436827320)

[6 Diameter (NOAM) 32](#_Toc436827321)

[**6.1** **Configuration - > Topology Hiding** 32](#_Toc436827322)

[**6.2** **Configuration - > Egress Throttle List** 36](#_Toc436827323)

[7 Policy and Charging (NOAM) 37](#_Toc436827324)

[**7.1** **Configuration** 37](#_Toc436827325)

[**7.2** **Configuration - > Policy DRA** 40](#_Toc436827326)

[**7.3** **Configuration - > Online Charging DRA** 41](#_Toc436827327)

[**7.4** **Maintenance** 44](#_Toc436827328)

[8 MAP-Diameter IWF (NOAM) 48](#_Toc436827329)

[8.1 Configuration 48](#_Toc436827330)

[8.1.1 MD-IWF Options 48](#_Toc436827331)

[8.1.2 Diameter Realm 49](#_Toc436827332)

[8.1.3 Diameter Identity GTA 50](#_Toc436827333)

[8.1.4 GTA Range to PC 51](#_Toc436827334)

[8.1.5 Map Exception 52](#_Toc436827335)

[8.1.6 CCNDC Mapping 53](#_Toc436827336)

[9 Diameter Common (SOAM) 54](#_Toc436827337)

[**9.1** **Dashboard** 54](#_Toc436827338)

[**9.2** **Network Identifiers -> MCC Ranges** 54](#_Toc436827339)

[**9.3** **MPs -> Profiles** 55](#_Toc436827340)

[**9.4** **MPs -> Profiles Assignments** 55](#_Toc436827341)

[10 Diameter (SOAM) 56](#_Toc436827342)

[**10.1** **Troubleshooting with IDIH** 56](#_Toc436827343)

[10.1.1 Configuration -> Traces 56](#_Toc436827344)

[10.1.2 Configuration -> Options 56](#_Toc436827345)

[10.1.3 Configuration -> Global Options 57](#_Toc436827346)

[10.1.4 Maintenance -> Traces 57](#_Toc436827347)

[**10.2** **AVP Dictionary** 58](#_Toc436827348)

[10.2.1 AVP Dictionary -> Base Dictionary 58](#_Toc436827349)

[10.2.2 AVP Dictionary -> Custom Dictionary 58](#_Toc436827350)

[10.2.3 AVP Dictionary -> All-AVP Dictionary 58](#_Toc436827351)

[10.2.4 AVP Dictionary -> Vendors Dictionary 59](#_Toc436827352)

[11 MEAL Inserts 60](#_Toc436827353)

[**11.1** **Alarm/Measurements/KPIs/MIBs Delta ( 7.1)** 60](#_Toc436827354)

[12 Reference List 60](#_Toc436827355)

**LIST OF TERMS**

ACL ………………………Access Control List

ASGU …………………….Automated Server Group Upgrade

AVP ………………………Attribute Value Pair

CLI ………………………..Command Line Interface

DNS ………………………Domain Name Server

GUI ……………………….Graphical User Interface

HSS .....................................Home Subscriber Server

iLO ………………………..Integrated Lights Out

IMI ......................................Internal Management Interface

IOT ………………………..Interoperability Tests

KPI ………………………..Key Performance Indicator

LTE ……………………….Long Term Evolution

MEAL..................................Measurements, Events, Alarms, and Logging

MME ……………………...Mobility Management Entity

MP.......................................Message Processor

MPS ………………………Messages per Second

NE ………………………...Network Element

NMS ………………………Network Management System

OAM……………………...Operations, Administration, Maintenance

OAM&P .............................Operations, Administration, Maintenance and Provisioning

OCF ………………………On-line Charging Function

OFCF ……………………..Off-line Charging Function

PDRA ……………………..Policy Diameter Relay Agent

PCRF ……………………..DSR Control and Charging Rules Function

P-CSCF................................Proxy-Call Session Control Function

PDU ………………………Protocol Data Unit

PM&C …………………….Platform, Management and Control

S-CSCF ...............................Session Call Session Control Function

SLF ……………………….Subscriber Locator Function

SPR……………………….Subscriber Profile Repository

TPD ……………………….ORACLE Platform Distribution

VIP ......................................Virtual IP Address

XMI......................................External Management Interface

XSI.......................................External Signaling Interface

1. **Introduction**
   1. ***Purpose/Scope***

Purpose of this Feature Guide document is to highlight the changes of the product that may have impact on the customer network operations, and should be considered by the customer during planning for this release.

The supported upgrade paths for DSR 7.1 are:

5.1 🡪 7.1

6.0 🡪 7.1

7.0 🡪 7.1

7.1.X 🡪 7.1

**Note: DSR 6.0 and 7.0 support the 3-tier network architecture only. Any deployments with 2-tier architecture must migrate to 3-tier before upgrade to DSR 6.0 or 7.0.**

* 1. ***Disclaimers***

This document summarizes Release 7.1 new and enhancement features as compared to Release 7.0, and the operations impacts of these features, at a high level. The Feature Requirements (FRS) documents remain the defining source for the expected behavior of these features.

*Note that feature implementations may chang**e slightly during product test.*

1. **Overview of DSR 7.1 Features**

This section provides an overview of the DSR 7.1 release features. Please see the following document:

**Oracle® Communications Diameter Signaling Router Release Notes**  
Release 7.1  
**E61925-01**

[E63474\_01.pdf](http://docs.oracle.com/cd/E63474_01/docs.71/E61925_rev_01.pdf" \o "DSR 7.1 Release Notes)

* 1. **DSR 7.1 New Features**

DSR 7.1 introduces the following new Features, which may be a new installed in DSR 7.1, or activated after upgrade to DSR 7.1, depending on customer need.

|  |
| --- |
| **Feature Name** |
|
| Diameter Redirect Notification Support |
| Enhanced Suspect Binding Cleanup |
| Full IPv6/IPv4 Dual-Stack  support for management interfaces |
| SBR Reconfiguration and Migration |
| DSR Dashboard |
| DSR Configuration and Performance |
| DSR Upgrades |
| Network Integrated DIH |
| Routing Attributes by (Extended) Command Code |
| DSR Signaling Port Range Management + IPFE initiator support |
| DSR TLS/DTLS Support |
| Egress Throttling Enhancements |
| Mediation Enhancements |
| SDS Service Continuity |

* 1. **DSR 7.1 Redirect**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| BUG 19088250 : Diameter Redirect Notification Support | This feature is intended to support Redirect Notification returned by a Redirect Agent which has determined that the request could not be satisfied locally, and the initiator of the request has to direct the request directly to the server, whose contact information has been added to the response from the Redirect Agent.  Currently DSR has a limited capability to support Redirect Notification coming from a Redirect Agent by using Reroute-on-Answer capability. However Redirection Notification support across this existing DSR capability is not a perfect setup.  Subsequent sections show some UC examples where different network elements can act as Redirect Agents in a diameter signaling network which can be solved with this new feature. The support of Redirect Agent mode is out of the scope of this feature . | Major feature |
| BUG 19570707 : Diameter Realm-Based Redirect Notification Support | The Diameter base protocol [RFC6733](http://tools.ietf.org/html/rfc6733) [1] specifies a redirection service provided by a Redirect Agent. The Redirect Notification Indication returned by the Redirect Agent is described in Section 6.1.8 and Sections 6.12 through 6.14 of [RFC6733](http://tools.ietf.org/html/rfc6733) [1]. As described in section 2, it provides one or more individual hosts to the message sender as the destination of the redirected message. In some circumstances, an operator may wish to redirect messages to an alternate domain without specifying individual hosts. For example an operator has offered a specific service but no longer wishes to do so.  The operator has arranged for an alternative domain to provide the service. To aid in the transition to the new arrangement, the original operator maintains a Redirect Diameter node ( Server or Proxy) to indicate to the message sender (Redirect Client, e.g. a DSR) the alternate domain to which the request should be sent.  Realm-Based Redirection Notification Support is required on the DSR as part of the need to fully support all type of Redirection Notification which are currently specified in [1] and [4]. | Major feature |
| BUG 19789230 : Mediation Support for Redirect | This feature is intended to ensure that request trigger points that are available for a normal Request shall also be available for a Redirected Request. | Major feature |
| BUG 19789031 : Transaction-based Redirect Notification Control | As part of Redirect Notification Support , this feature is intended to enhance OAM configurability for that feature by providing user with granular control on the activation of Redirect Notification Response processing on a per Ingress Transaction basis. The configuration of TCS shall be extended by adding new attributes in order to control Redirect Notification on a per TCS rule basis. | Major feature |

* 1. **DSR 7.1 Enhanced Suspect Binding Cleanup**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| Enhanced Suspect Binding Cleanup (PR# 238722) | This Feature Requirements Specification (FRS) identifies the requirements associated with Enhanced Suspect Binding Removal feature (PR #238722). While the feature’s original intent was to remove Gx sessions based on Rx failures, the feature is generically applicable to the session removal of any binding capable interfaces supported by the PDRA and the removal can be triggered off Diameter based failures on any of the PDRA supported interfaces. | Major feature enhancement |

* 1. **DSR 7.1 IPv6 support**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| DSR IPv6 support for Management Interfaces(PR 197780/BUG 19085083)  DSR IPv6 Integration with ComAgent (PR 240301/BUG 19117852)  SDS IPv6 Support for Management Interfaces (PR 240297/BUG 19117848)  SDS IPv6 Integration with ComAgent (PR 240299/BUG 19118471)  SDS IPv6 support for Provisioning Interfaces (PR 240300/BUG 19118472)  IPv6 support for IDIH (PR 240122/BUG 19117611 )  IDIH IPv6 Integration with ComAgent (PR 240123/BUG 19117612) | DSR currently supports IPv6 for Diameter Configuration/Signaling only. This feature requires that all remaining DSR network services and IP flows that are supported over routable IPv4 interfaces shall also be supported over IPv6 including Dual Stack support for signaling interfaces. | Major feature enhancement |

* 1. **DSR 7.1 SBR Reconfiguration**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| PR 219139 BUG19090983 Binding SBR Capacity Growth/Degrowth  PR 242117 BUG19120094 Session SBR Capacity Growth/Degrowth  PR 226985 BUG19100734 PCA per-mated pair sizing of SBR-S database  PR 219144 BUG19090988 PCA Remating Procedures  PR N/A BUG19270432 PCA Unmating Procedures | This feature is required to allow operational PCA deployments to change the configuration (location and size) of both SBR-B and SBR-S databases. Since this feature will be implemented after the 7.0 release, the term PCA will be used to describe the application that provides the Policy DRA, Online Charging DRA functionality. The functionality will also apply to the Gateway Location (GLA) application since it uses the same SBR architecture.  Many of the functions described are common to both the SBR-S and SBR-B, and in the case of the SBR-S, across both the P-DRA and the OC-DRA functionality. In general, when this document talks about SBR, it means that it applies to both the SBR-B and the SBR-S, and for both the OC-DRA and P-DRA functionality. If a requirement applies only to a SBR-B or SBR-S, then those terms will be used instead of SBR. | Major feature |

* 1. **DSR 7.1 DSR Dashboard**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| PR# 230281: DSR Dashboard  PR# 238365: Add Dashboard Metrics to DSR Maintenance Displays | DSR currently provides a rich set of operational maintenance tools for monitoring a DSR Node.  Separate KPI, alarm, and status monitoring tools exist. However, no top-down view of the overall status of a DSR Node or set of DSR Nodes exists.  Customers are asking for DSR operational tool(s) which allow(s) them to more easily identify the potential for or existence of a DSR Node or Diameter Network outage. This feature provides a “Dashboard” GUI display that can be accessed via the SOAM or NOAM GUI which provides the following high-level capabilities:   * Centralized View: Allows operators to view a high level summary of key operational metrics; * Identifies potential operational issues: Assists operators in identifying problems via visual enhancements such as colorization and highlighting; * Centralized Launch-Point: Allows operators to drill-down to the next level of status information to assist in pinpointing the source of a potential problem. | Major feature enhancement |

* 1. **DSR 7.1 Configuration and Performance**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| DSR Configuration and Performance for DSR Release 7.1 | This Feature Requirements Specification (FRS) documents the functions and requirements of DSR Configuration and Performance for DSR Release 7. This FRS contains incremental requirements to FRS FE007072, DSR 6.0 Configuration and Performance, as well as any incremental requirements from earlier releases. | Major feature enhancement |
| PR 235653 | DSR 7.1 Configuration and Performance - Configuration requirements are often not all collected into one place and it is left to the individual FRS writers to define their portions of the configuration. This document is a holistic approach to configuration, and configuration and related networking requirements for the entire DSR product are contained or referenced here. |  |
| PR 229035 | Multiple Applications Supported on DSR |  |
| PR 216741 | Charging Proxy (OCS) |  |
| PR 219142 | P-DRA 3-Site Redundancy |  |
| BUG 19326485 | DSR Support for 16,000 Diameter Connections |  |
| BUG 19326567 | 2000 Connections per DA-MP |  |
| BUG 19326523 | DSR Support for 16,000 Peer Nodes |  |

* 1. **DSR 7.1 Upgrades**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| Product Perspective of Upgrades | The ability to effectively upgrade the DSR application from one release to another is an important component in the overall lifecycle management of the DSR. This document details the upgrade paths and software release compatibility, as well as, requirements to address the continuous improvement of DSR upgrades.  Upgrades are often performed by Oracle consulting personnel, and are also performed by 3rd party contractors/distributors, as well as, directly by our customers. As the DSR product continues to scale and increasingly have more capabilities, it is becoming more important to:   * Increase the speed of upgrades * Decrease the number and length of upgrade maintenance windows required to complete an upgrade * Increase the accuracy and correctness of the upgrades * Make upgrades simpler and understandable | Major feature enhancement |
| PR 235654  BUG 19111838 | DSR 7.0 BASE Upgrade - This details all the upgrade paths needed for DSR release 7.0 and any general upgrade requirements for a DSR network. |  |
| BUG 19714835 | DSR 7.1 Upgrade - This details all the upgrade paths needed for DSR release 7.1 and any general upgrade requirements for a DSR network. |  |
| PR 228086  BUG 19102162 | Server group based automated upgrade - The complexity, manual nature and length of upgrades continue to be a problem for DSR networks. This feature is one of many features and procedural improvements for the continued improvement of DSR upgrades. This feature addresses:   * The complexity, error prone and manual steps currently required in upgrading a server group by automating the procedures. * Provides the configurable ability to reduce the time required to upgrade a server group by allowing parallel upgrade of more than one server within the server group. * Provides the configurable ability to reduce the upgrade time for a single DSR network element by allowing parallel upgrade of several server groups with a network element.   DSR is building upon a platform framework for server group upgrades. Please refer to: **Error! Reference source not found.** **Error! Reference source not found.** for more information. |  |

* 1. **DSR 7.1 Network Integrated DIH (IDIH)**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| FE007375  DSR Integrated DIH  Purpose and Scope of IDIH | This Feature Requirements Specification (FRS) documents the functions and requirements associated with the Network Integrated DIH (IDIH) feature. This feature allows traces to be defined and the results to be correlated and reviewed at a network level, spanning multiple DSR sites.  Each DSR site will continue to host a local IDIH instance which will gather and store trace data associated with the specific site. The network IDIH capability enables that data to be correlated and viewed across multiple sites.  This feature leverage the framework put in place by the Integrated DIH feature (PR-221026). | Major feature enhancement |
| N-IDIH Requirements  PR 232433 | The N-IDIH capability can gather and correlate trace data from other sites within a DSR network. The DSR network is defined to be the scope of an N-OAMP.  Note: The maximum number of sites is defined within the DSR Configuration and Performance FRS FE007142. There can be up to 32 sites within some DSR networks, although this number may be limited in the context of certain applications (PDRA only supports up to 16 sites). | Major feature enhancement |

* 1. **DSR 7.1 Routing Attributes by (Extended) Command Code**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| PR 232401 | This Feature Requirements Specification (FRS) documents the functions and requirements of ‘Routing Attributes by (Extended) Command Code’ feature (PR #232401) of Diameter Signaling Router (DSR). Initial scope of the feature request is limited to incorporating (E)CC defined Diameter Request transaction specific attributes in DSR ROS and PAT selection process. However, the solution presented in this document is extensible for other managed object selection.  The feature is required to support a pre-configured list of transaction attributes [Application Id, configured (E)CC <Command Code, and optional Diameter/3GPP AVP Code and AVP Data>]. At the writing of this FRS, any additional message attributes or combinations is out of scope. | Major feature enhancement |

* 1. **DSR Signaling Port Range Management and IPFE Initiator**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| PR 232202  BUG 19107427 | DSR Signaling Port Range Management: As of DSR 6.0, the DSR product has an overlapping port range (0-65535) for responder and initiator connections. Platform, OAM and signaling modules are all using the same port range for different types of connections for different services. There is likelihood of race conditions that can result in permanent socket binding failures.  Several customers also have requested for the ephemeral local port range to be brought in compliance with IANA recommended port range. This DSR enhancement defines a non-overlapping port range partitioning for application use across DSR system and leaves an IANA compliant ephemeral port range for platform or other services use. | Major feature enhancement |
| IPFE initiator Support  PR 220164  BUG 19092320  IPFE Initiator+Responder Support  PR 215682  BUG 19087317 | DSR releases prior to DSR 7.0, have IPFE support for ‘responder only’ connections. ‘initiator only’ and ‘initiator & responder’ connections are fixed DA-MP connections using static DA-MP IP addresses. Customers have provided feedback that initiator connections with static DA-MP IP addresses have operational, maintenance and service impacts synonymous with a mesh network and a single DSR view is required on the initiator side connectivity in the Diameter signaling network. | Major feature enhancement |
| BUG 20083083 | Port Number Flexibility - The IPFE Initiator feature (PR 220164 / BugDB ID# 19092320) has been implemented in DSR 7.0 using the Port Striping method. This implementation is somewhat restrictive in terms of the port numbers that a specific DA-MP/TSA combination that can be used if IPFE Initiator is enabled for the TSA. The requirement here is to provide more flexibility to use any port within a configurable range on any DA-MP within a TSA to initiate connections – for both Initiator Connections as well as Initiator+Responder Connections. | Major feature enhancement |

* 1. **DSR TLS/DTLS Support**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| PR 216749  DSR TLS/DTLS Support  FE007318  Purpose and Scope | Currently DSR optionally supports IP layer (IPsec) encryption per Diameter connection or association, and does not support transport layer security protocols (TLS/DTLS).  This Feature Requirements Specification (FRS) documents the requirements for the support of TLS for TCP connections and DTLS for SCTP associations in DSR as defined in Diameter Base Protocol Specification RFC6733.  RFC 6733 defines TLS/TCP and DTLS/SCTP as primary security mechanisms and IPsec as a secondary alternative:  *“The Diameter base protocol messages SHOULD be secured by using TLS/TCP (*[*RFC5246*](http://tools.ietf.org/html/rfc5246) *[2]) or DTLS/SCTP (*[*RFC6083*](http://tools.ietf.org/html/rfc6083) *[4]). Additional security mechanisms such as IPsec (*[*RFC4301*](http://tools.ietf.org/html/rfc4301) *[5]) MAY also be deployed to secure connections between peers. However, all Diameter base protocol implementations MUST support the use of TLS/TCP and DTLS/SCTP, and the Diameter protocol MUST NOT be used without one of TLS, DTLS, or IPsec”.* | Major feature enhancement |

* 1. **Egress Throttling Enhancements**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| PR 168850  Egress Throttle Group Rate Limiting  PR 213271  Egress Throttle Group Pending Transaction Limiting | Egress Throttle Group Rate Limiting & Egress Throttle Group Pending Transaction Limiting - Prior to these features, DSR enforces egress message rate and pending transaction limits independently on each peer connection.  There is no support for egress throttling based on the aggregate egress message rate or aggregate pending transactions for a set of peers and/or peer connections. This presents limitations. | Major feature enhancement |
| PR 230706 | Coordinated Egress Throttling across multiple DSR  As described in preceding sections, with the SOAM Managed Egress throttling, all DSR signaling elements route Request traffic to the Server and execute egress throttling using single signaling NE scoped, SOAM configured thresholds. For the redundant DSR node deployments, the ETG limiting thresholds at each site is configured to a value less than or equal to ‘Capacity/Number of Redundant DSRs’. While configuring thresholds, operator must consider that the sum of the egress throttling at the DSRs must be less than or equal to the Server’s capacity in order to avoid risk of overloading the server. With this implementation, if a subset of the DSR signaling elements fail or lose connectivity to the Server, the remaining DSR(s) cannot fully utilize the Server’s capacity. In addition, operator manually and statically manages the capacity configuration across these DSR systems for handling traffic routing under normal and failure scenarios.  To address the capacity utilization and management limitations for redundant DSR deployments, The grouped DSR Signaling NEs (Signaling Nodes, Signaling Sites) will coordinate the egress traffic routing to the Server by sharing the ETG scoped metrics (egress traffic rate and pending transaction) of affected ETGs across multiple (up to 2 other) DSR signaling NEs. Following figure and subsequent examples describe the coordinated egress-throttling context for 2 DSR (mated DSR) example, the same can be extended for Coordinated Egress Throttling support up to 3 DSR (triplet DSR) signaling NEs. | Major feature enhancement |

* 1. **Mediation Enhancements**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| Summary | The enhancements proposed in this release fall into three categories. One of the enhancements (PR#19531528) is forwarding looking and are being proposed based on anticipated future needs while the second category of enhancements (PR#19531603, PR#19531614) allow for certain core DSR features that are targeted for future releases to be quickly addressed via the mediation framework. The last set of enhancements (PR#19531621, PR#19531631) cover utility functions for well-defined operations such as redirecting a request or for parsing a decorated NAI. These operations can be supported in the prior DSR releases via mediation but will involve multiple actions and could be error prone for an operator to define. Defining these as pre-defined functions will reduce such errors.  It should be noted that the last set of enhancements (PR#19531621, PR#19531631) are stretch objectives for this release and therefore optional. The corresponding sections will be deleted from this FRS if these enhancements are not included in this release. | Major feature enhancement |
| PR 19531528 | Grouped AVPs to depth of 8 - The Mediation framework currently allows for actions to be performed on AVPs that are 6 levels deep. This enhancement calls for increasing the depth to 8. |  |
| PR 19531603 | Peg Counter action - Operators have been asking for measurements based on message content and it has been a challenge to satisfy all the various operator needs in this regard. This enhancement will allow an operator to define up to 200 measurements based on message content. |  |
| PR 19531614 | Assert Alarm/Event action - Operators have also asked for the ability to Assert Alarms and Events based message content type and this enhancement will allow an operator to define a Critical, Major and Minor alarms each and a Info event based on message content. |  |
| PR19531621 | Redirect Request action - This enhancement calls for two closely related utility functions that can be used in mediation to re-direct a Request. These utility functions generate a Diameter 3006 or a 3011 response with the appropriate “redirect” AVPs when invoked. |  |
| PR 19531631 | Process Decorated NAI action - This enhancement calls for another utility function that can be used in mediation to Process the Decorated NAI if present in a request. This utility function parses the decorated NAI, if present, in the User-Name and modifies the User-Name and Destination-Realm AVPs. |  |

* 1. **SDS Service Continuity**

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| BUG 19129760  SDS Service Continuity | All SDS functionality needs to be maintained during software upgrades. |  |

* 1. **Hardware Changes**
     1. **Hardware Supported**

|  |  |
| --- | --- |
| **Hardware** | **Comment** |
| HP BL460 Gen6 | c-Class |
| HP BL620 Gen7 | c-Class |
| HP BL460c Gen8 | c-Class |
| **HP BL460c Gen9** | **c-Class** |
| HP DL360/380 Gen6 | Rack Mount Server |
| HP DL360/380 Gen8 | Rack Mount Server |
| **HP DL380 Gen9** | **Rack Mount Server** |
| Sun Netra X3-2 | Rack Mount Server |
| HP 6125, 6120 | Enclosure Switch |
| Cisco 3020 | Enclosure Switch |

Note: Gen9 and Gen 8 v2 hardware (with upgraded processors) are supported, when purchased by a customer.

Note: mixed Sun/HP deployments are not generally supported.

* + 1. **Hardware Upgrade**

No hardware upgrades are required with this release.

Deployment of certain Optional features may require additional hardware.

* + 1. **Software Changes**

Software change include a new release of the software Platform components, and new DSR release.

|  |  |
| --- | --- |
| Component | Release |
| TPD 64 Bit | 7.0.2.0.0-86.32.0 |
| COMCOL | 6.4-p252.11299\_tpd7.0.2.0.0\_86.32.0 |
| PM&C | 6.0.1.0.0-60.21.0 |
| TVOE | 3.0.2.0.0-86.28.0 |
| AppWorks | 6.0.29-6.0.1\_60.35.0 |

* + 1. **DSR Release 7.1**

DSR Release 7.1 inherits all functionality from DSR7.0 (And 6.0).

|  |  |
| --- | --- |
| Component | Release |
| DSR Release | 7.1 |

* + 1. **iDIH 7.1**

|  |  |
| --- | --- |
| Component | Release |
| Oracle | 7.1.0.0.0-71.24.3 |
| Mediation | 7.1.0.0.0-71.24.3 |
| Applications | 7.1.0.0.0-71.24.3 |

* + 1. **SDS Release Compatability**

DSR Release 7.1 is compatible with SDS Release 5.0 using IPV4 and SDS 7.1 using IPV4 and/or IPV6.

|  |  |  |
| --- | --- | --- |
| Component | Release | Internet Protocol |
| SDS | 5.0 | IPV4 |
| SDS | 7.1 | IPV6 |

* 1. **Firmware Changes**

Firmware release guidance is provided via DSR 7.1 Release Notice E61925 Rev 01 in conjuction with the current supported firmware release instructions located at the following link:

[*HPFupRleases*](https://beehiveonline.oracle.com/teamcollab/wiki/CGBU_Platform_Engineering_Firmware_Workspace:HpFupReleases)

* 1. **Upgrade Overview**

This section provides an overview of the Upgrade activities for Release 7.0.

* + 1. **Upgrade Path**

For this document, the path from DSR 5.1, 6.0, 7.0, or 7.1.x 🡪 7.1 is assumed.

* + 1. **Order of Upgrade**

1. Firmware Upgrade (if required)
2. Platform components
3. TVOE Upgrades
4. PM&C Upgrades
5. DSR Upgrade in the following sequence
6. NOAM / DR-NOAM
7. SOAM and site SOAM managed servers (site-at-a-time with mate site spare)
8. SBR MPs (site-at-a-time with mate site spares)
9. IPFE MPs
10. PDRA MPs
11. Configure for new DSR features
    * 1. **2-Tier OAM not Supported**

2-Tier OAM architecture is not supported in 7.1. Migration from 2-tier to 3-tier (if needed) must be done before upgrade to 7.1.

* + 1. **Active/Standby DA-MP servers supported**

Active/Standby DA-MP server architecture (1+1) continues to be supported in DSR 7.1.

Migration to Multi-active (N+0) DA-MP server architecture is recommended for all customers, and required for activating PDRA functionality.

* 1. **Migration of DSR Data**

As in prior releases, the existing DSR Data will be preserved during the upgrade.

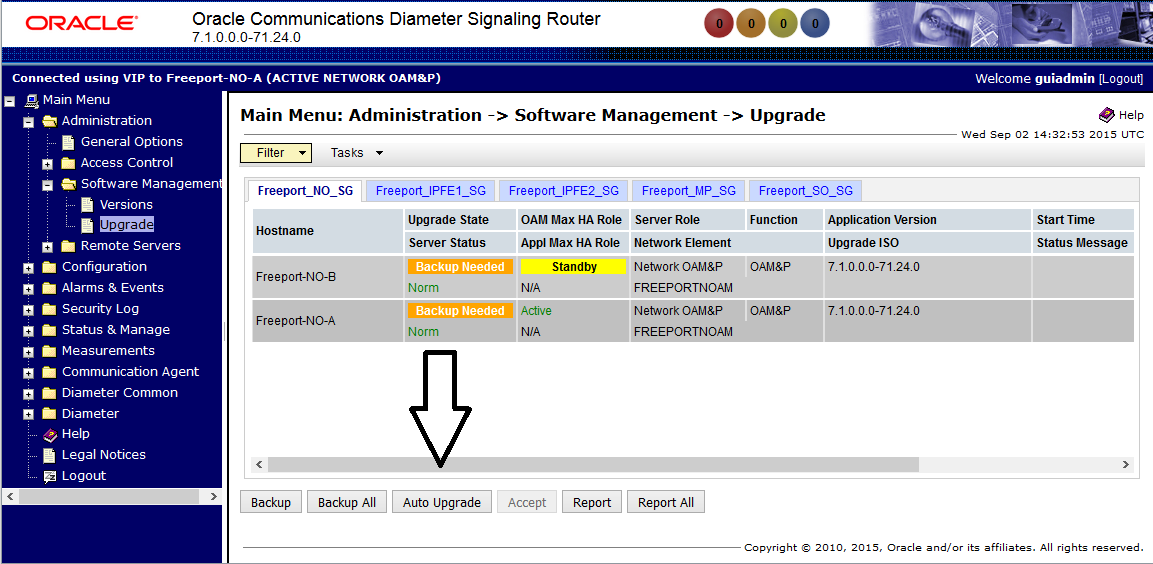
1. **Changes by Feature**

This section describes the OAM changes introduced to the 7.1 product (as compared to the 5.1) organized by feature.

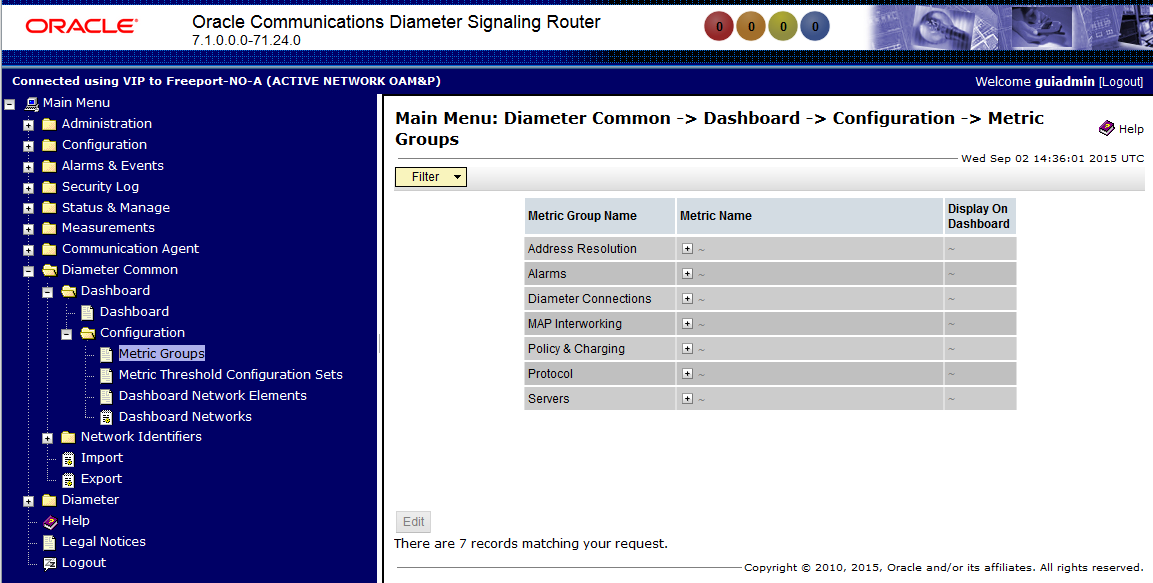
OAM changes include: User Interfaces (NO GUI, SO GUI), Measurements Reports, Alarms, and KPIs.

Note: this section covers OAM changes that will be visible after upgrade to the 7.1 release, and does not include changes that will be seen only as new Optional Features are Activated on the system (post-upgrade activity, and customer specific).

1. **Administration (NOAM)**
   1. **Software Management -> Upgrade (Auto Upgrade)**



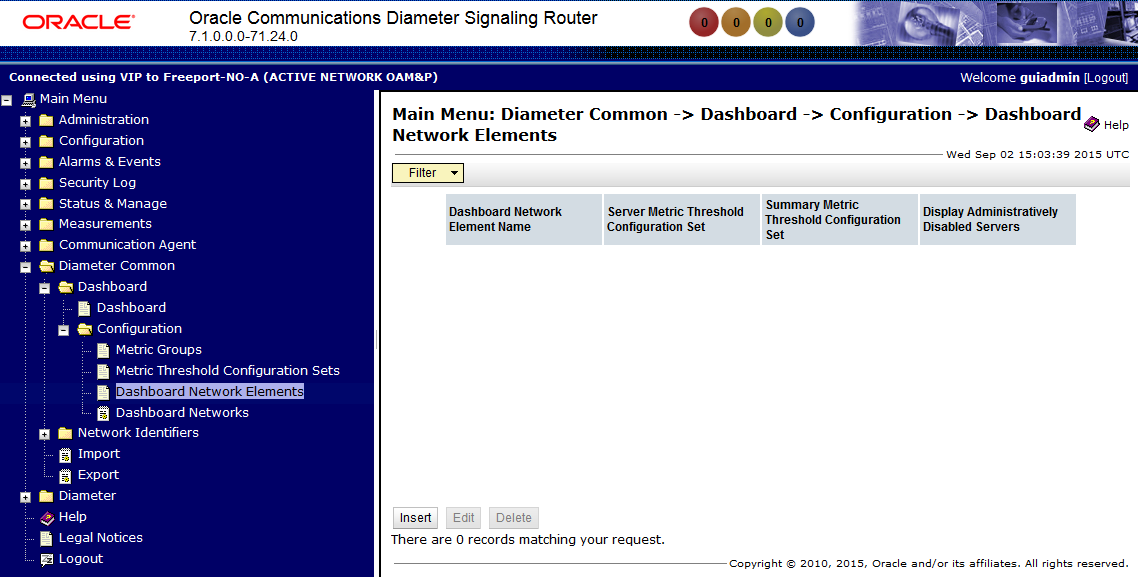
1. **Diameter Common (NOAM)**
   1. **Dashboard**
      1. **Configuration -> Metric Groups**



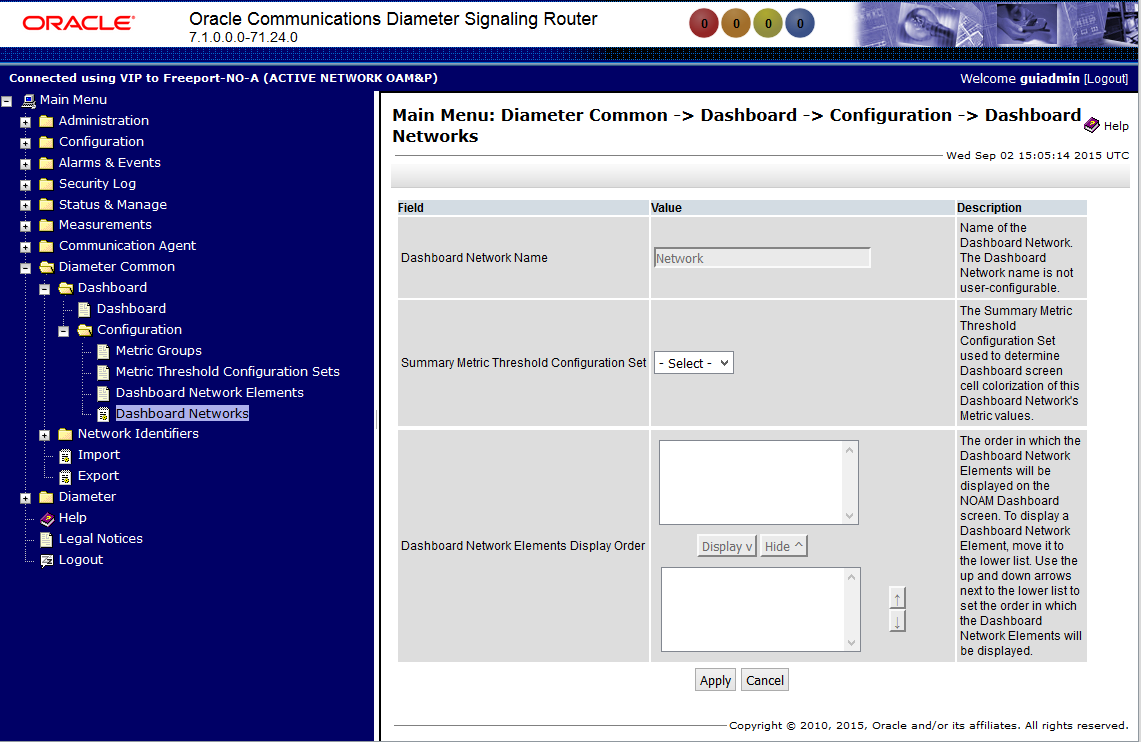
* + 1. **Configuration -> Metric Threshold Configuration Sets**



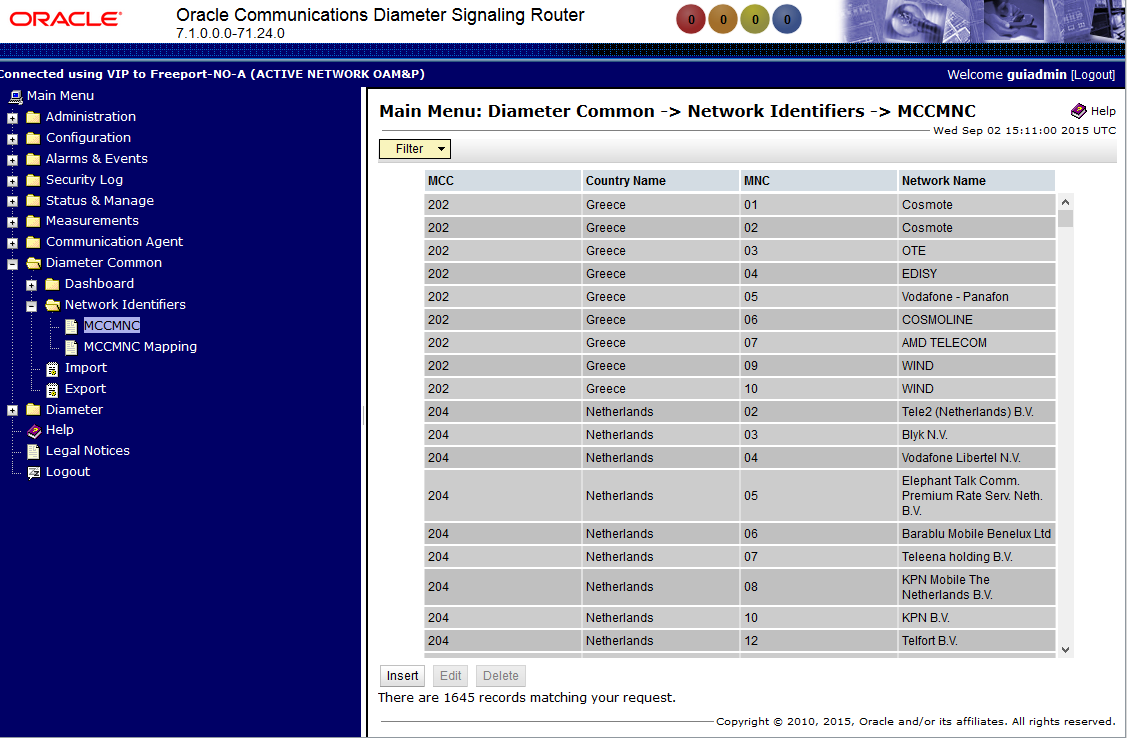
* + 1. **Configuration -> Dashboard Network Elements**



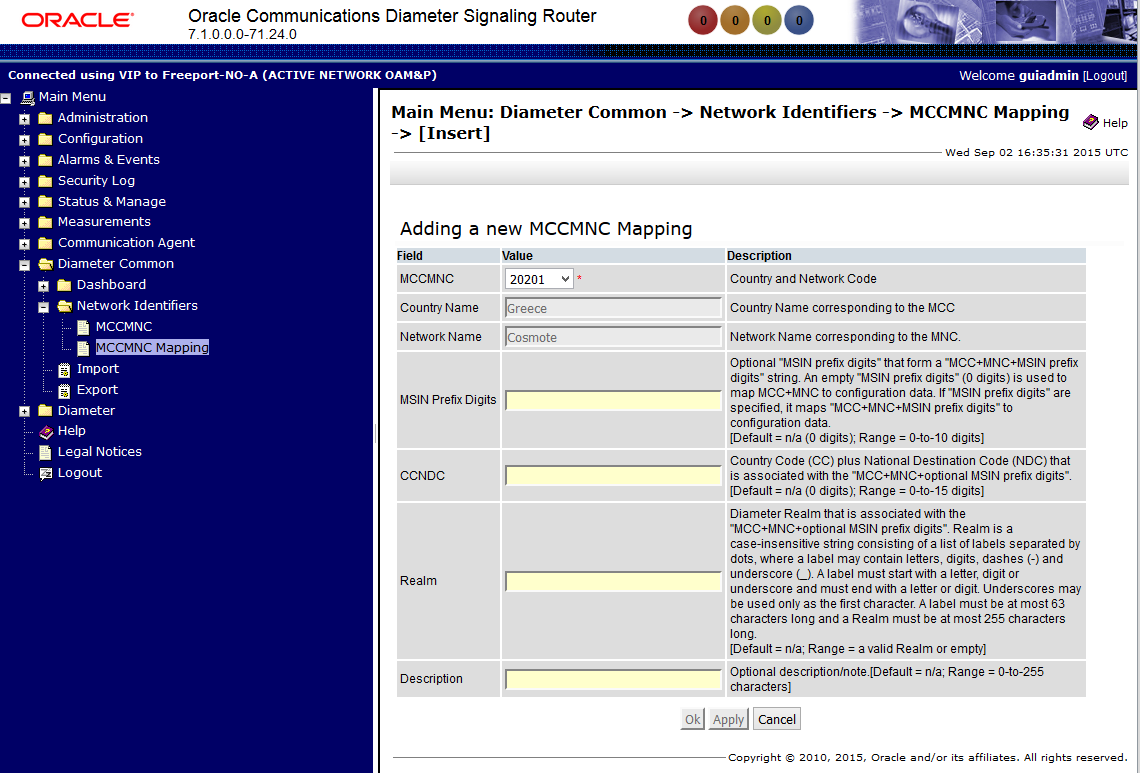
* + 1. **Configuration -> Dashboard Networks**



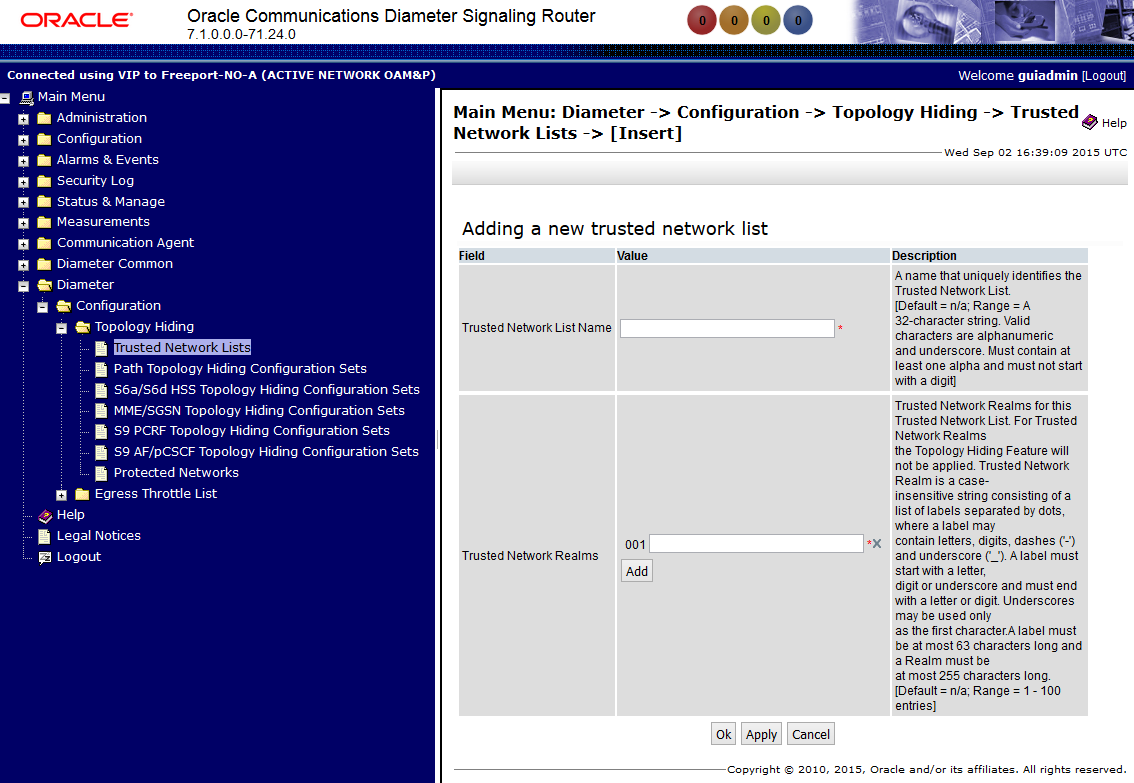
* 1. **Network Identifiers**
     1. **MCCMNC**



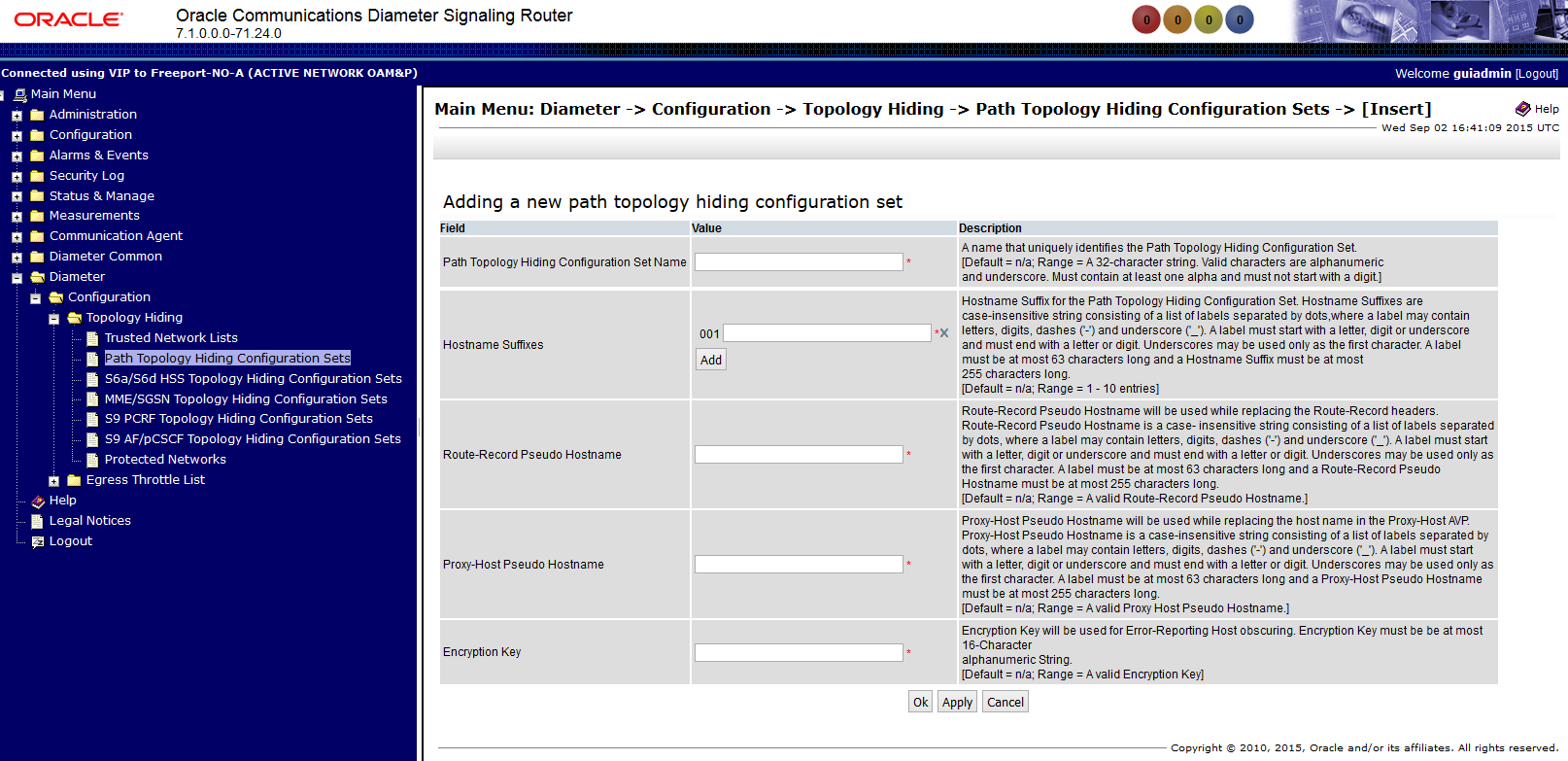
* + 1. **MCCMNC Mapping**

****

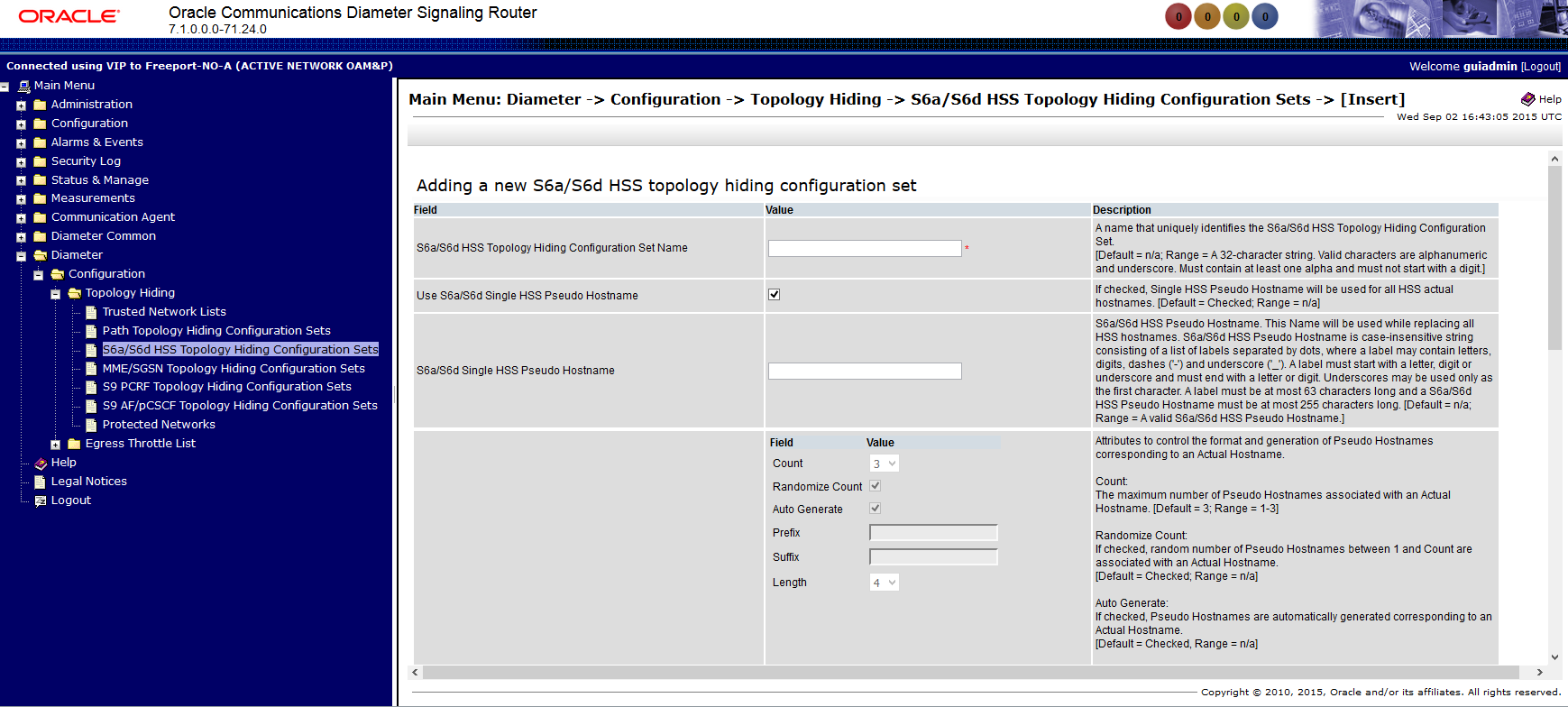
1. **Diameter (NOAM)**
   1. **Configuration - > Topology Hiding**
      1. **Trusted Network Lists**



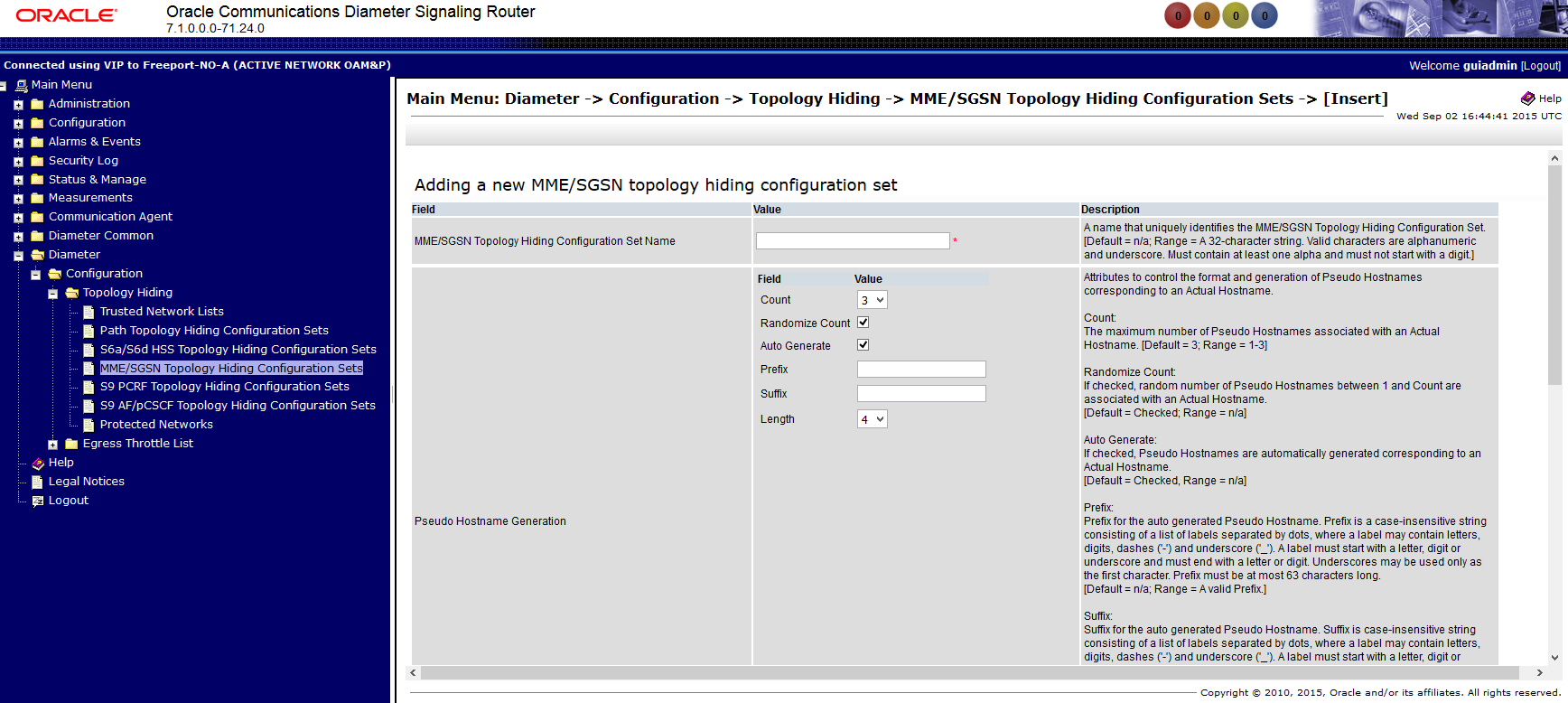
* + 1. **Path Topology Hiding Configuration Sets**



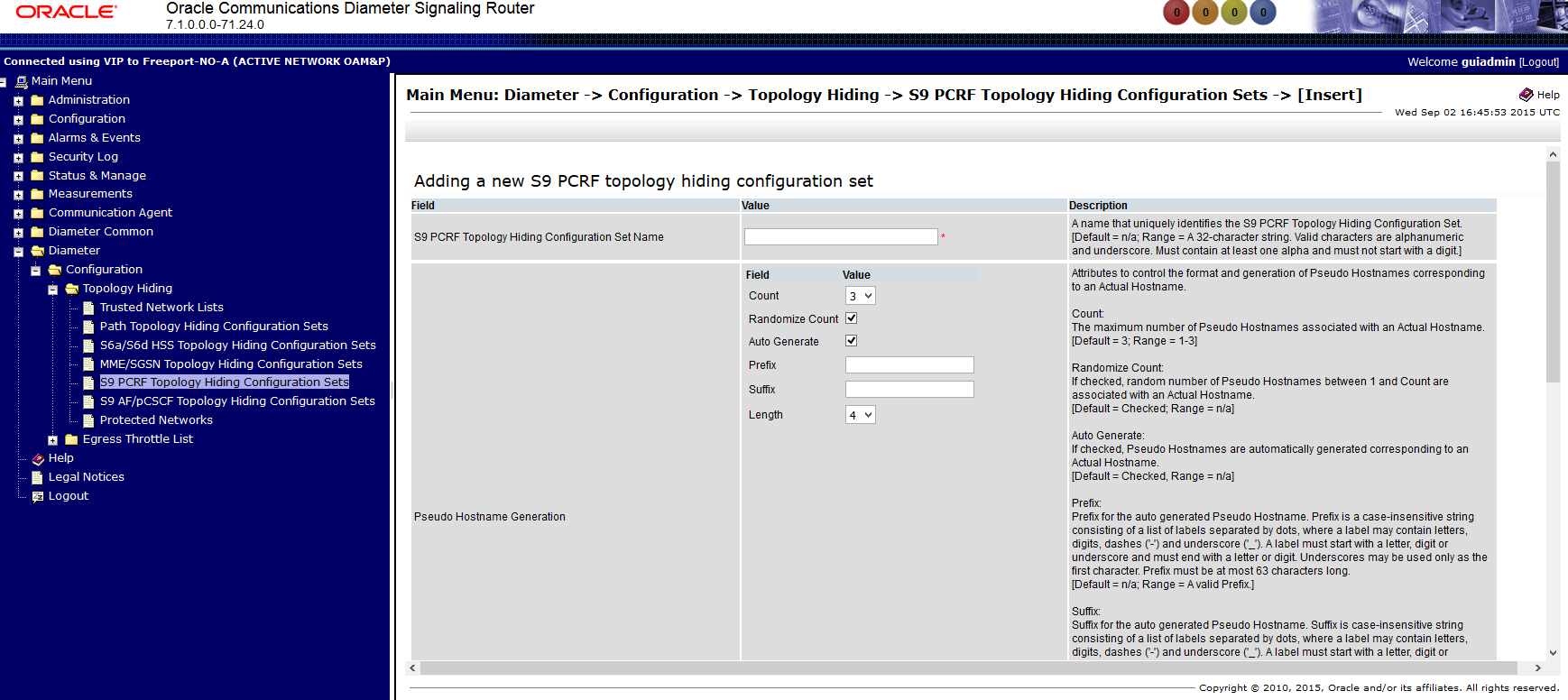
* + 1. **S6a/S6d HSS Topology Hiding Configuration Sets**



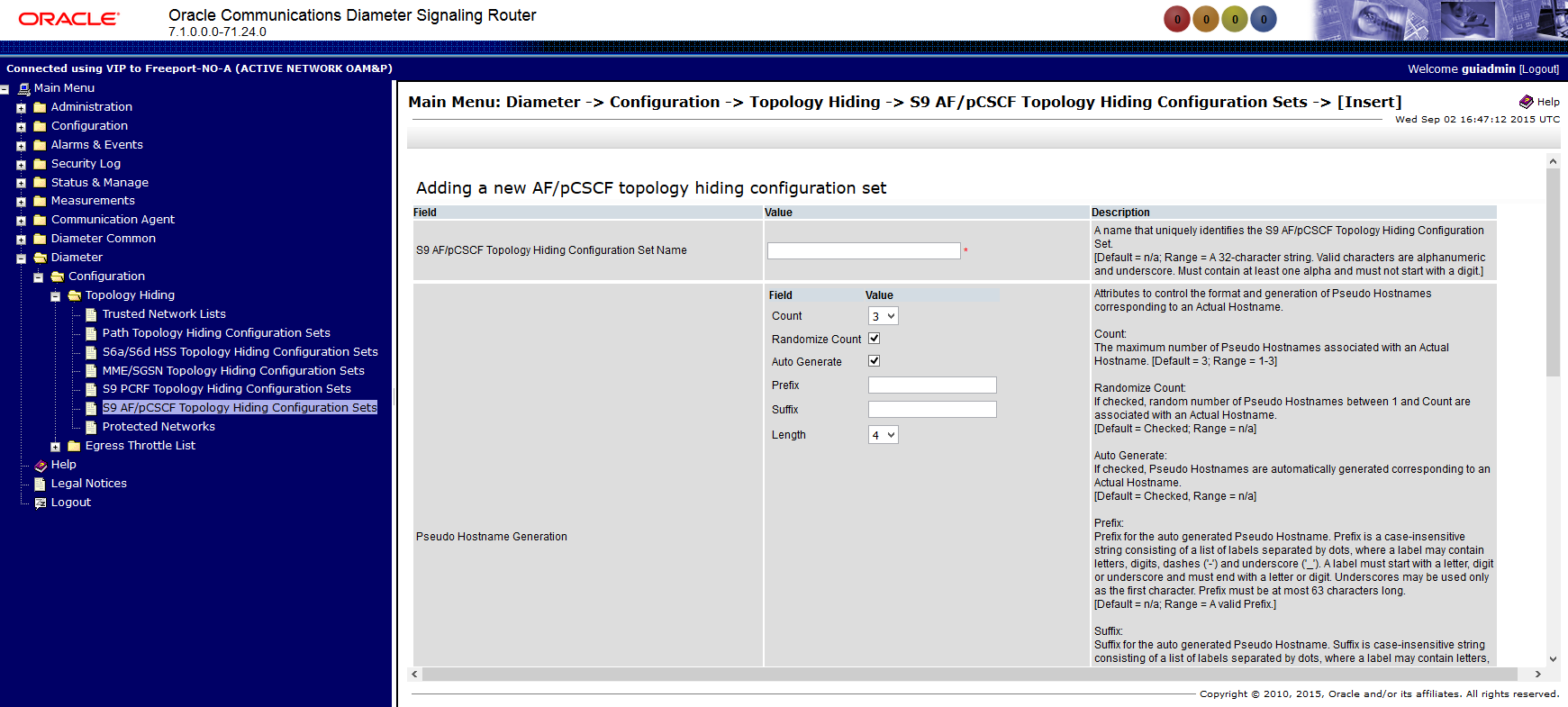
* + 1. **MME/SGSN Topology Hiding Configuration Sets**



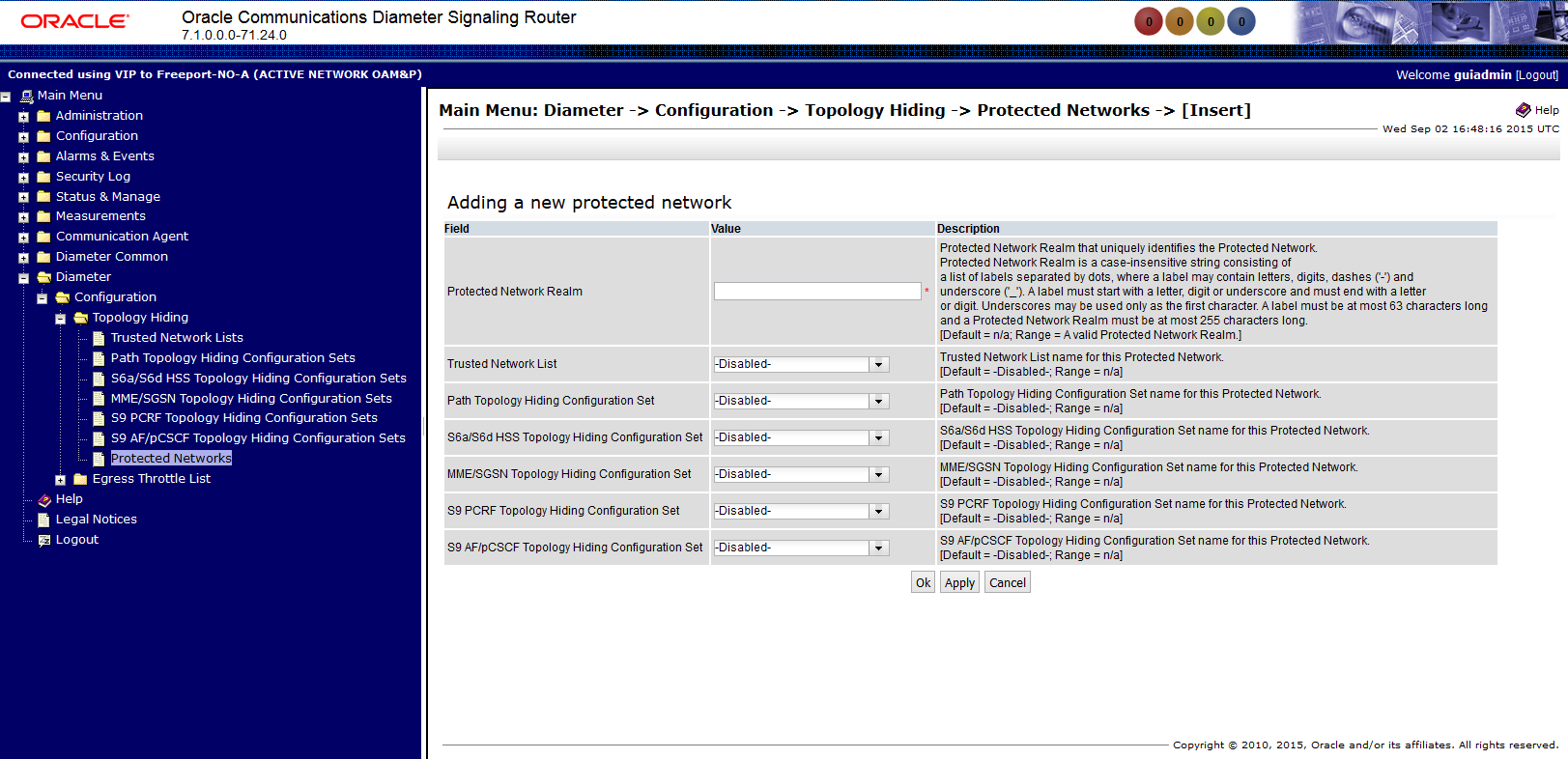
* + 1. **S9 PCRF Topology Hiding Configuration Sets**



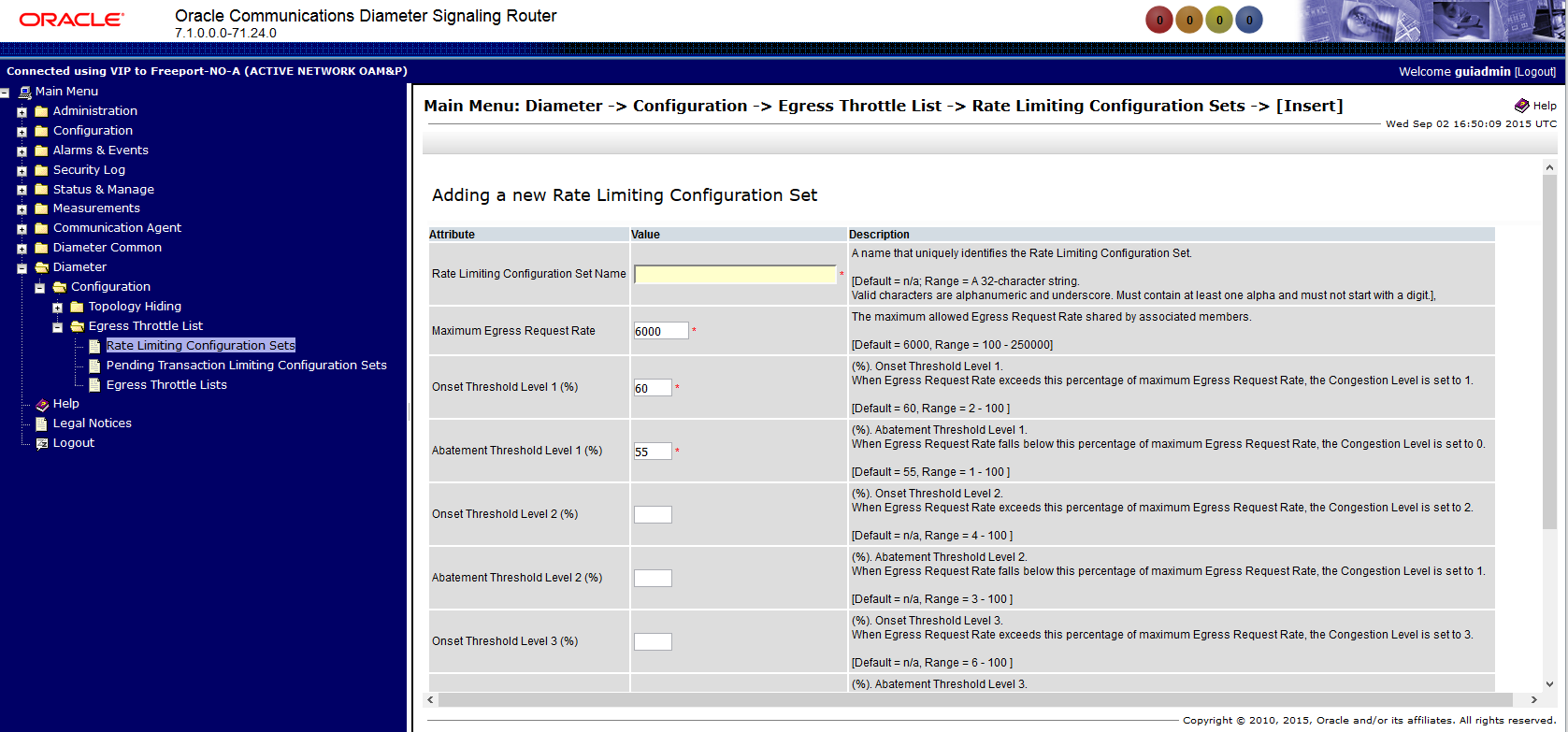
* + 1. **S9 AF/pCSCF Topology Hiding Configuration Sets**



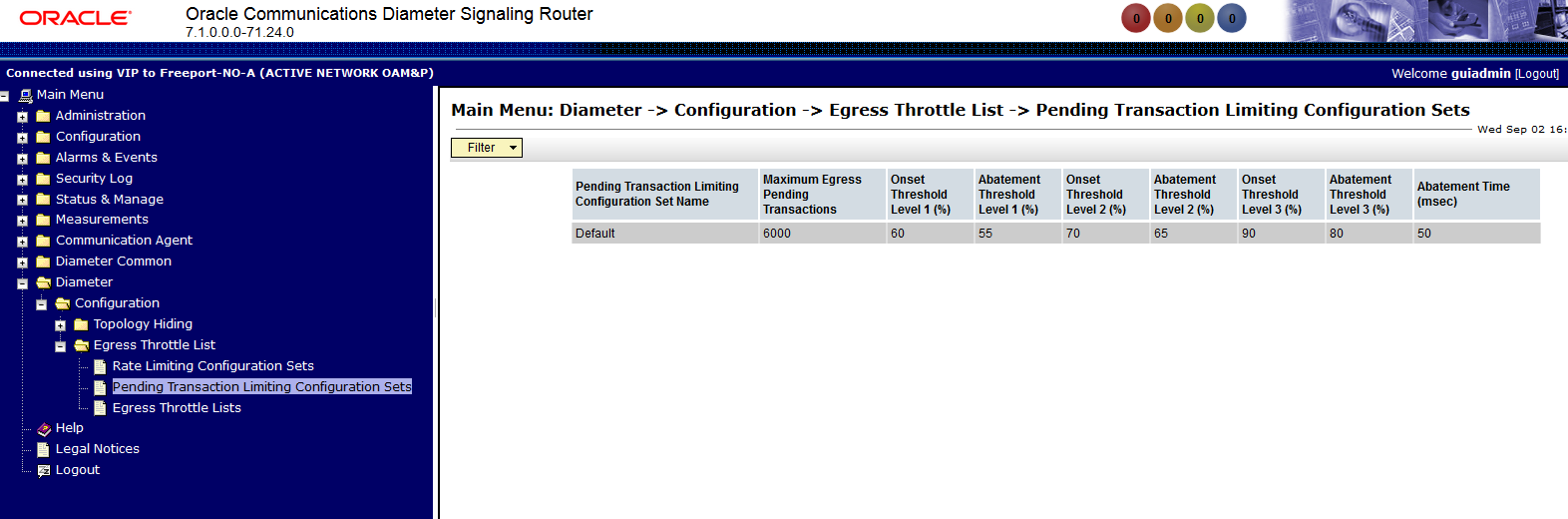
* + 1. **Protected Networks**



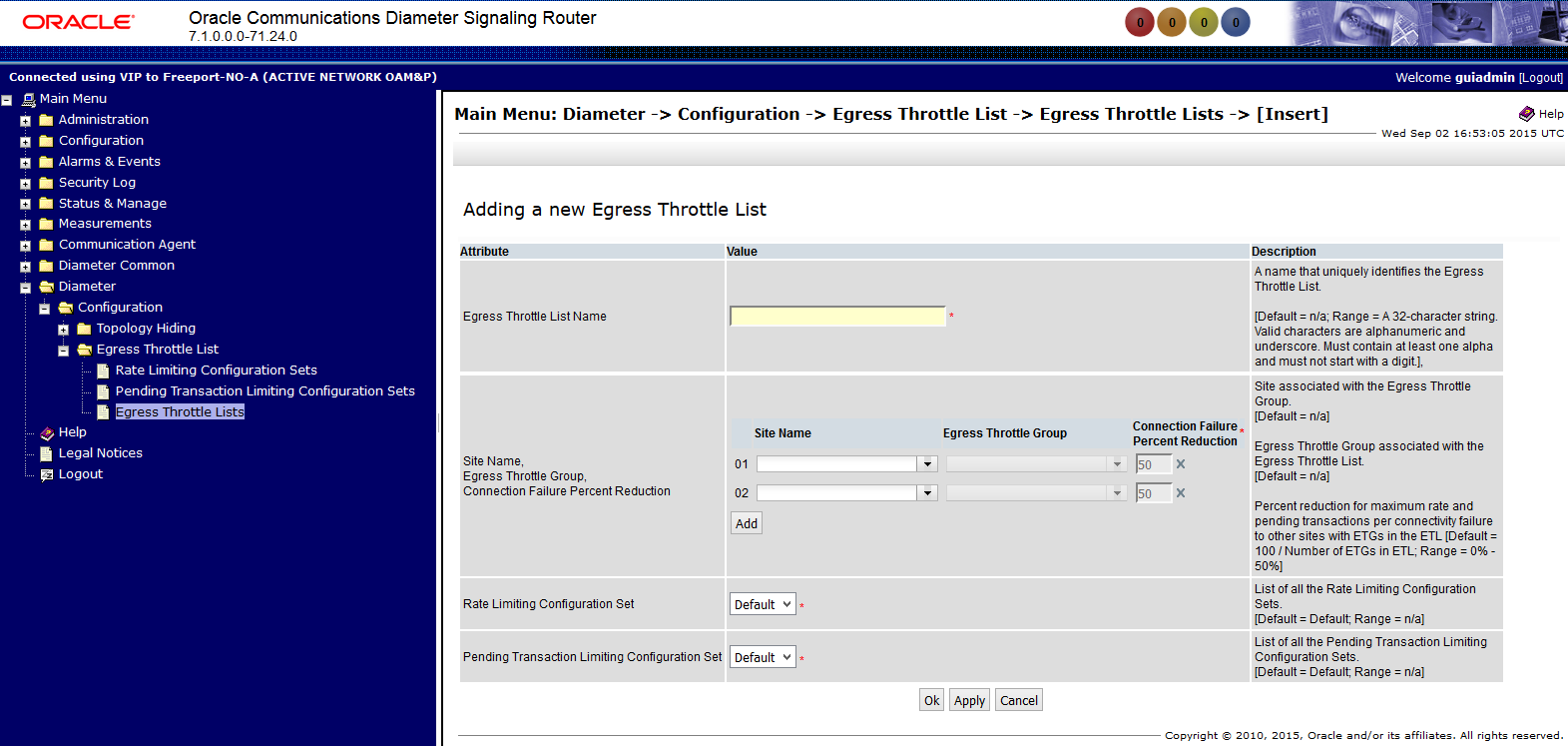
* 1. **Configuration - > Egress Throttle List**
     1. **Rate Limiting Configuration Sets**



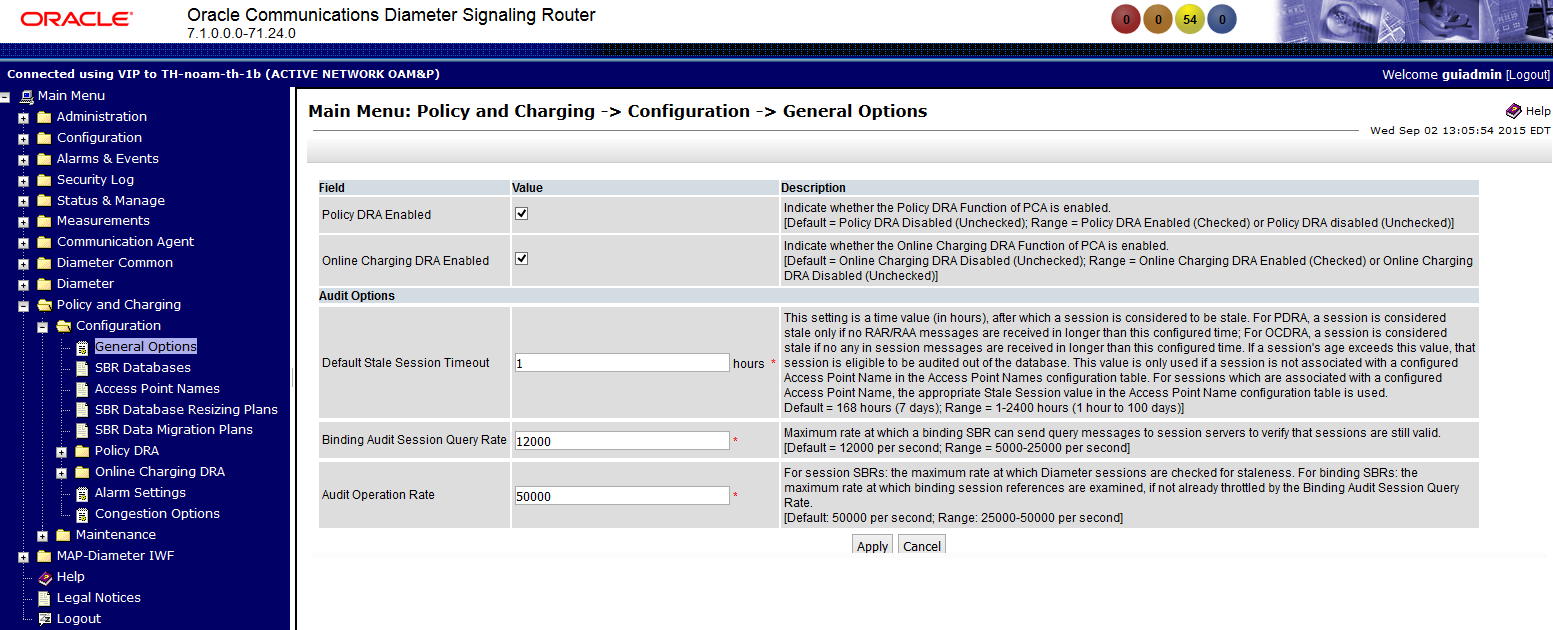
* + 1. **Pending Transaction Limiting Configuration Sets**



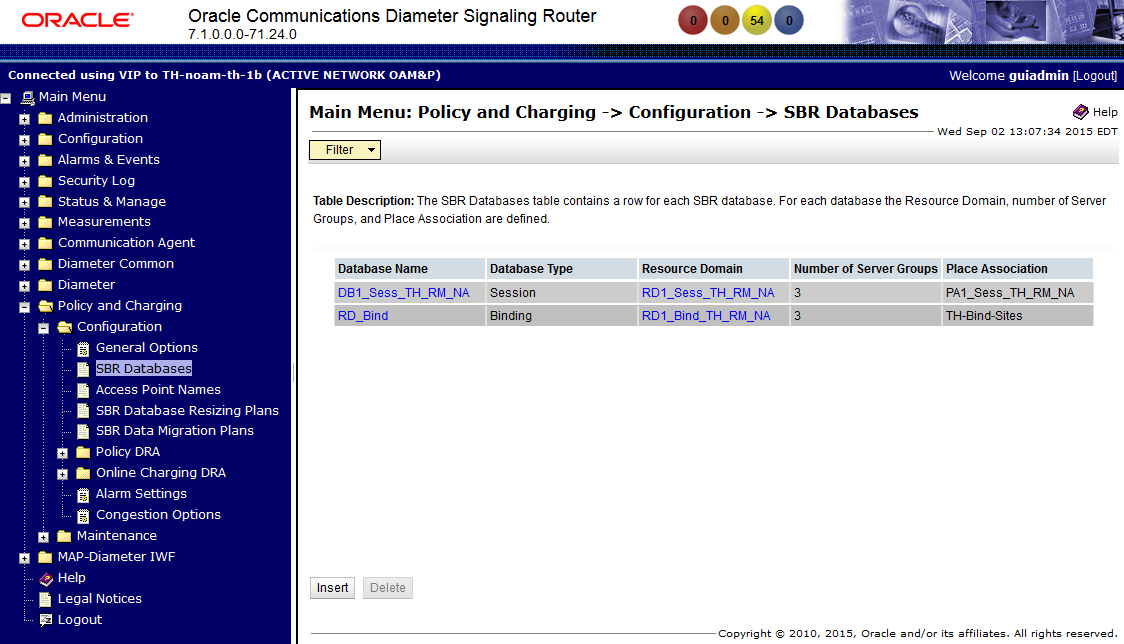
* + 1. **Egress Throttle Lists**



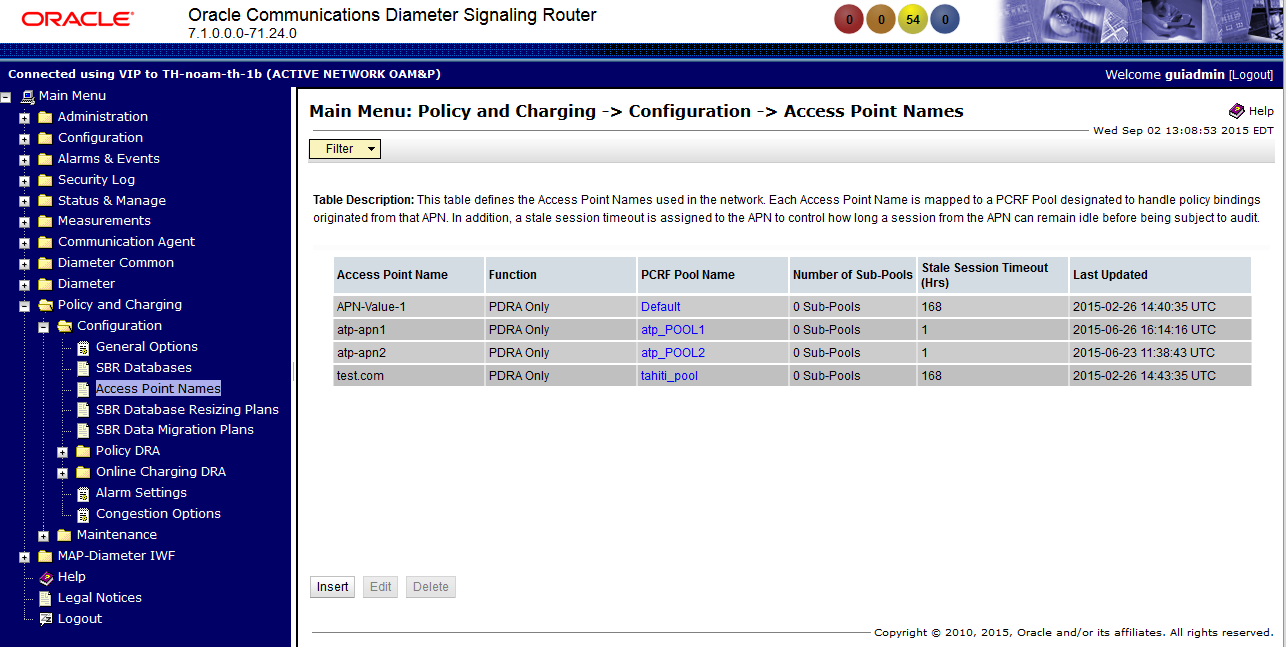
1. **Policy and Charging (NOAM)**
   1. **Configuration**
      1. **General Options**



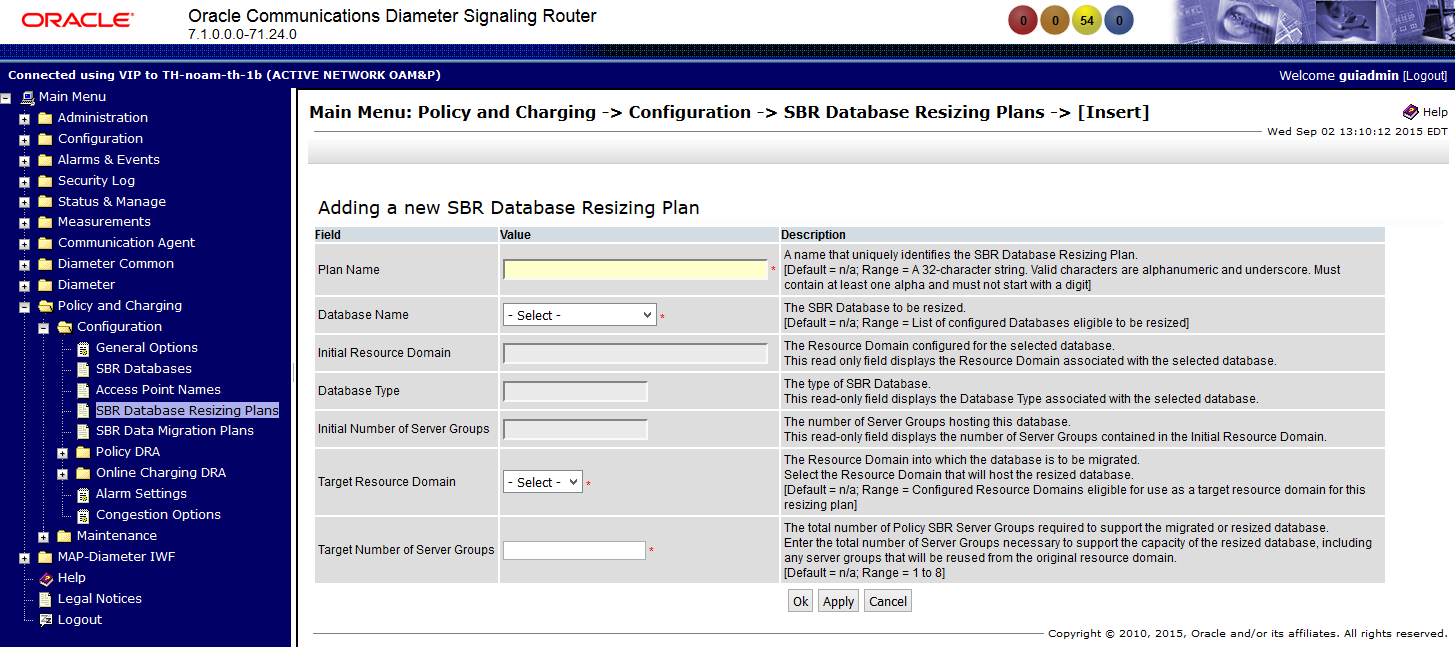
* + 1. **SBR Databases**



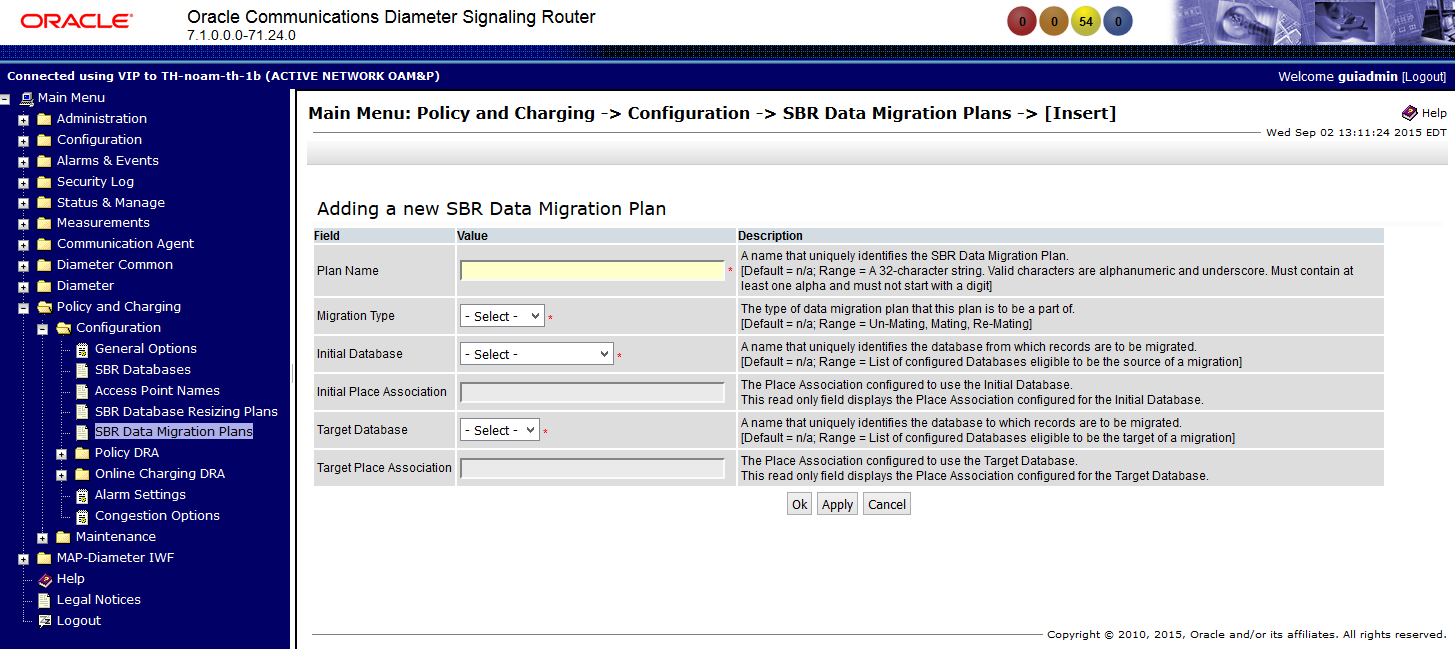
* + 1. **Access Point Names**



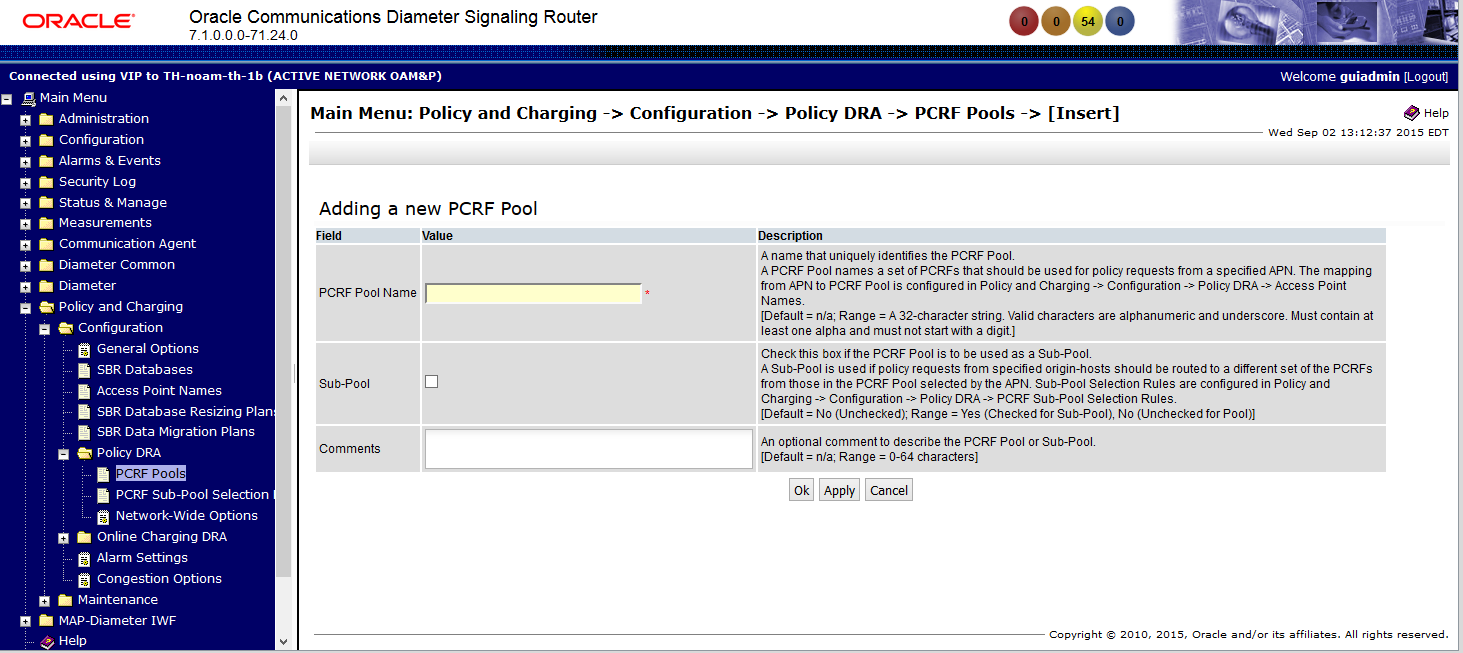
* + 1. **SBR Database Resizing Plans**



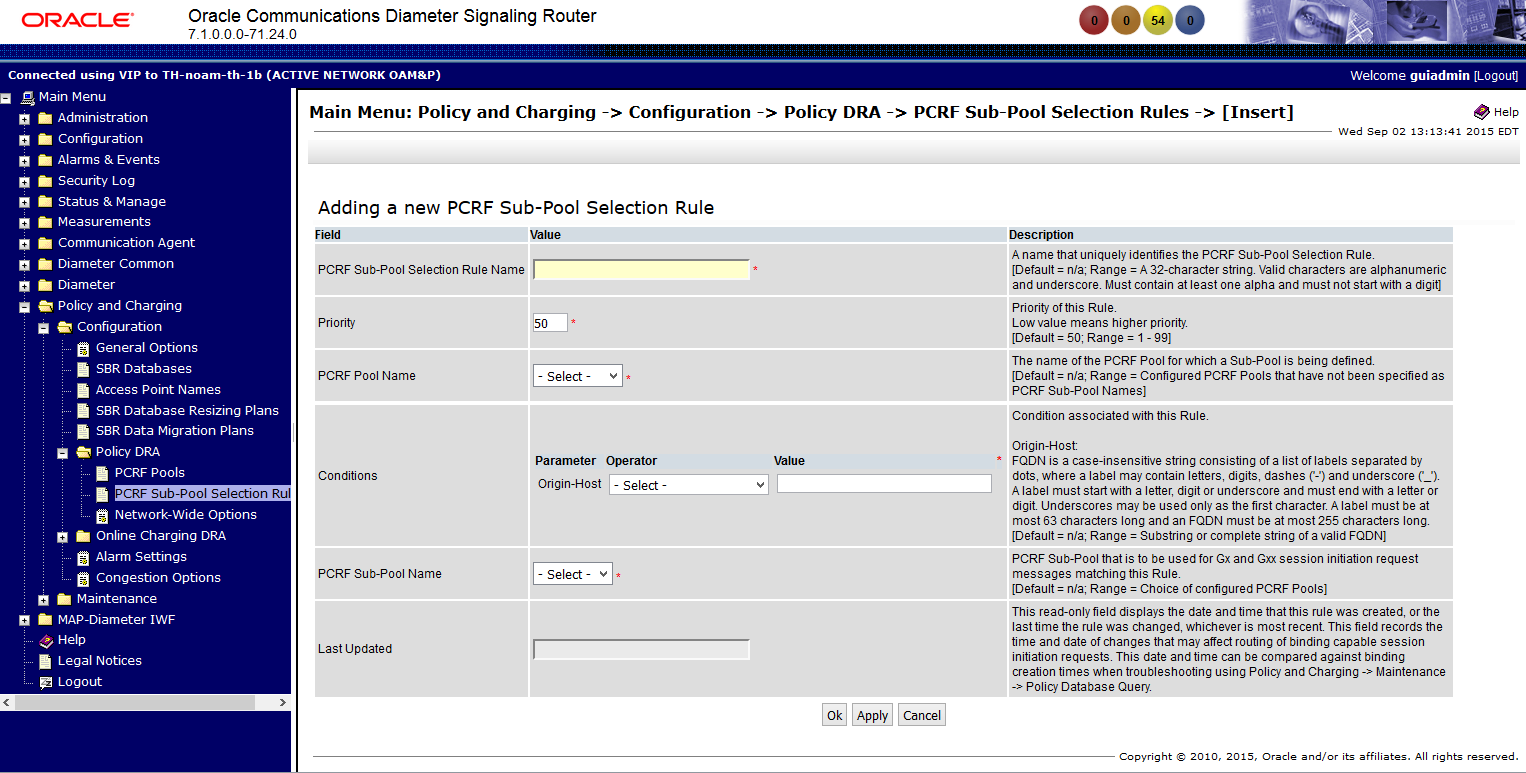
* + 1. **SBR Data Migration Plans**



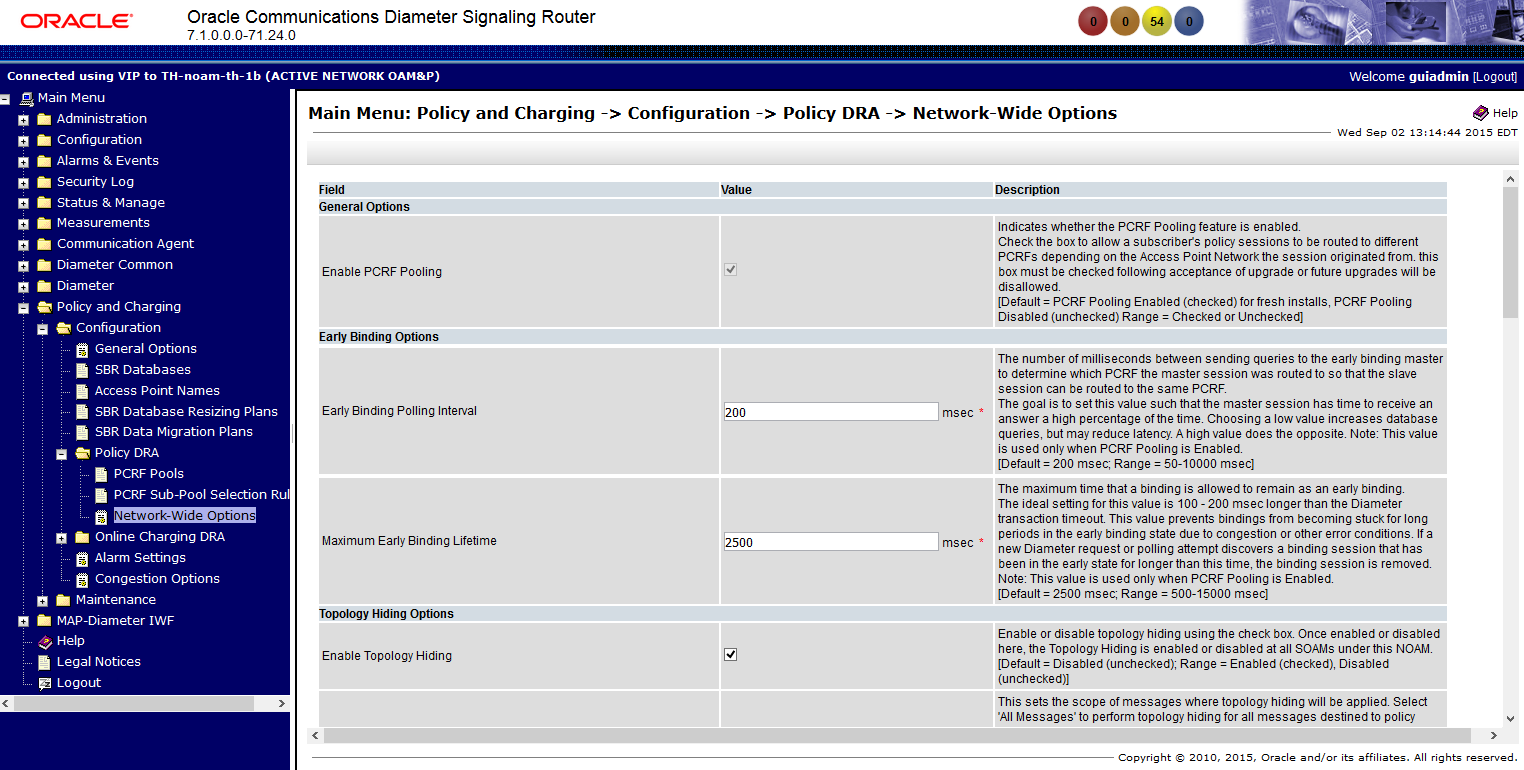
* 1. **Configuration - > Policy DRA**
     1. **PCRF Pools**



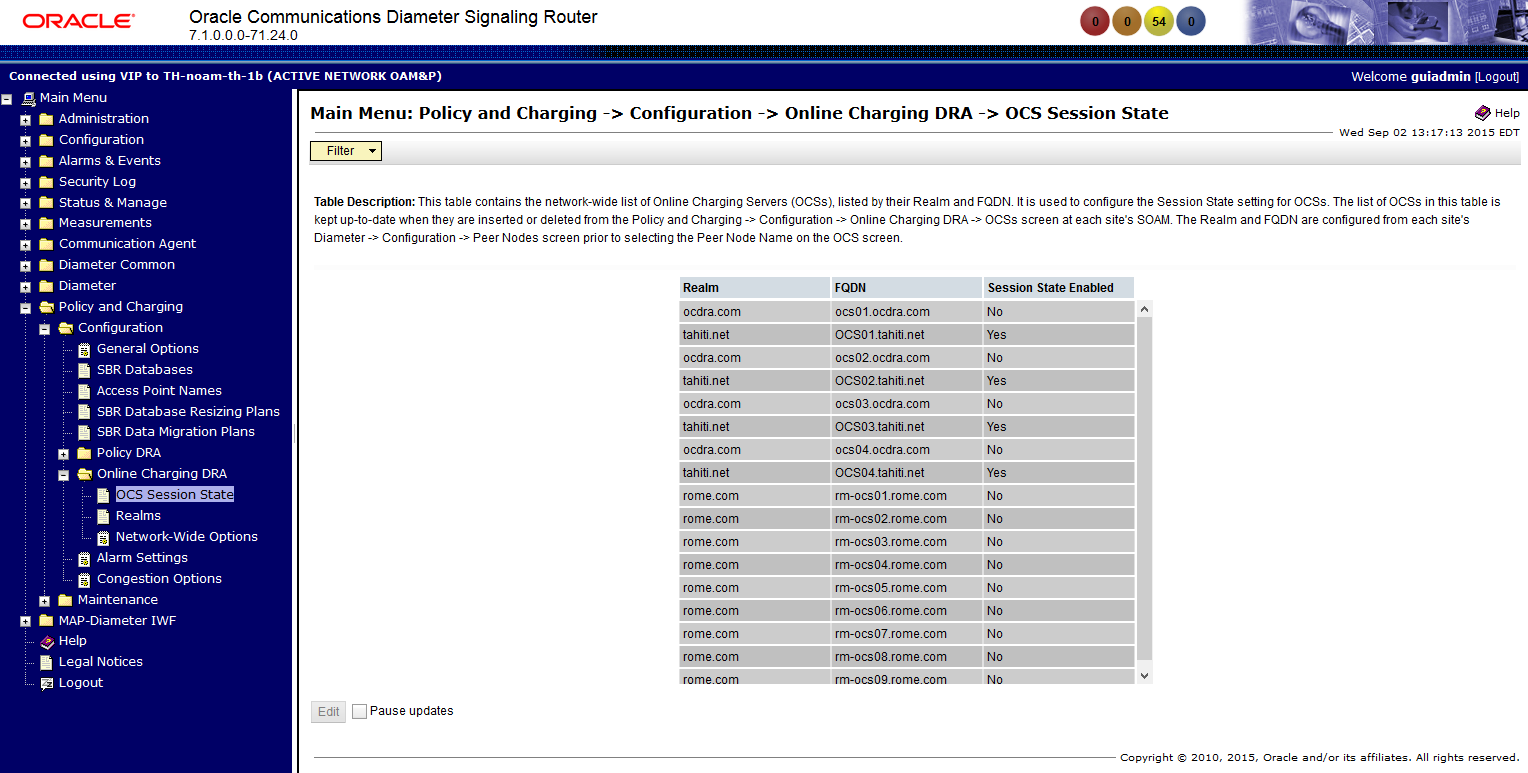
* + 1. **PCRF Sub-Pool Selection Rules**



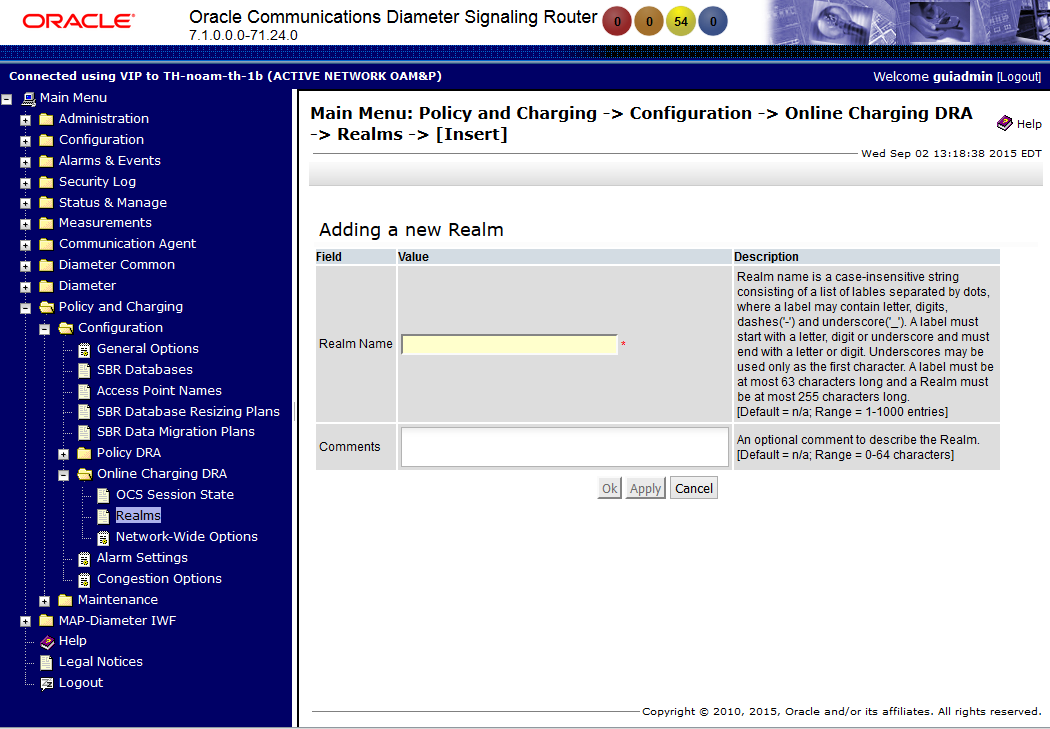
* + 1. **Network-Wide Options**



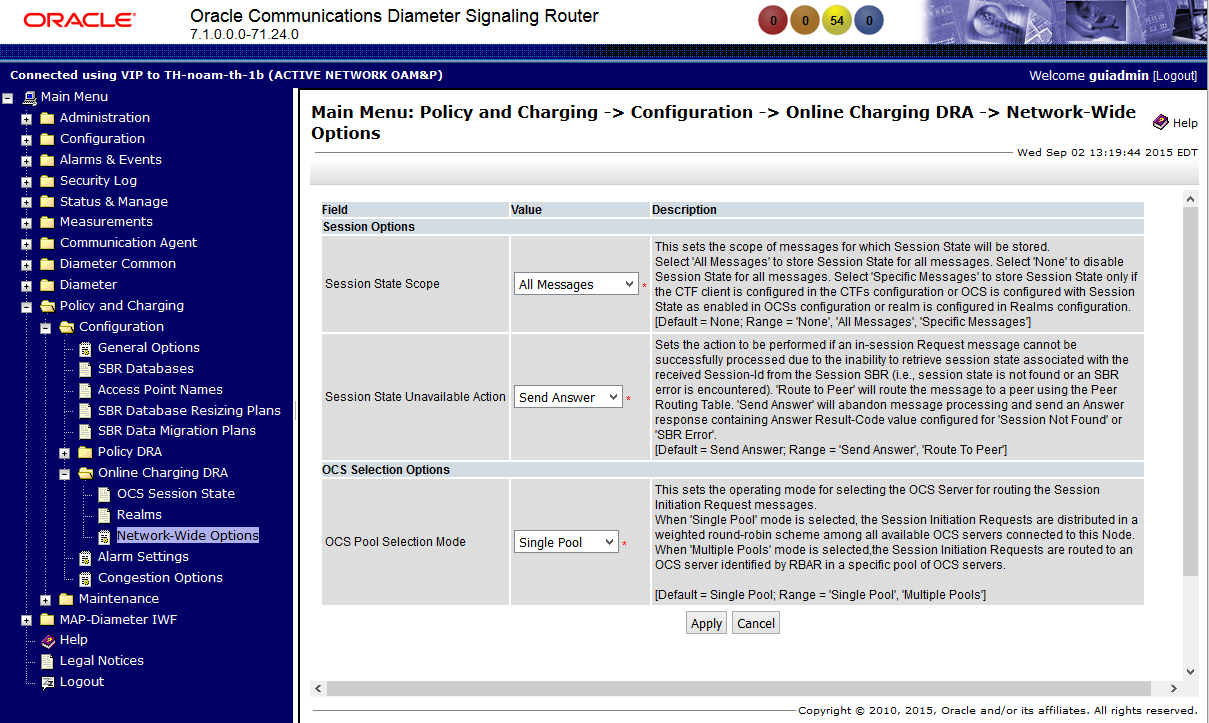
* 1. **Configuration - > Online Charging DRA**
     1. **OCS Session State**



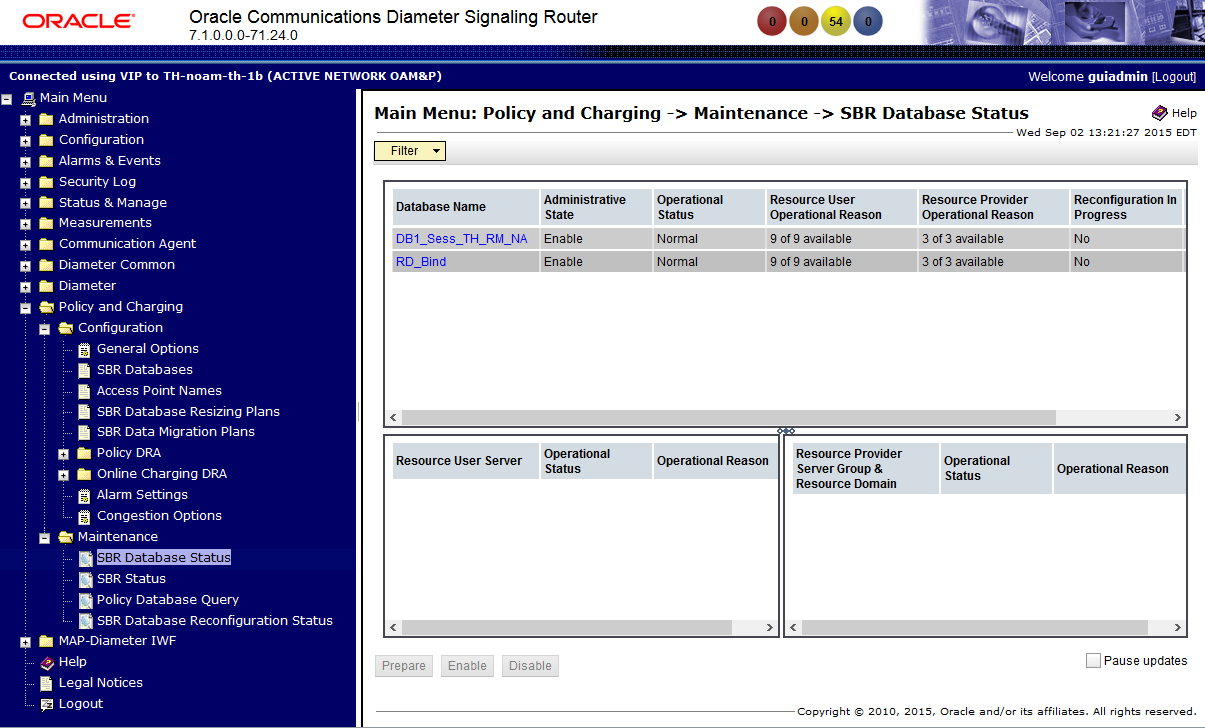
* + 1. **Realms**



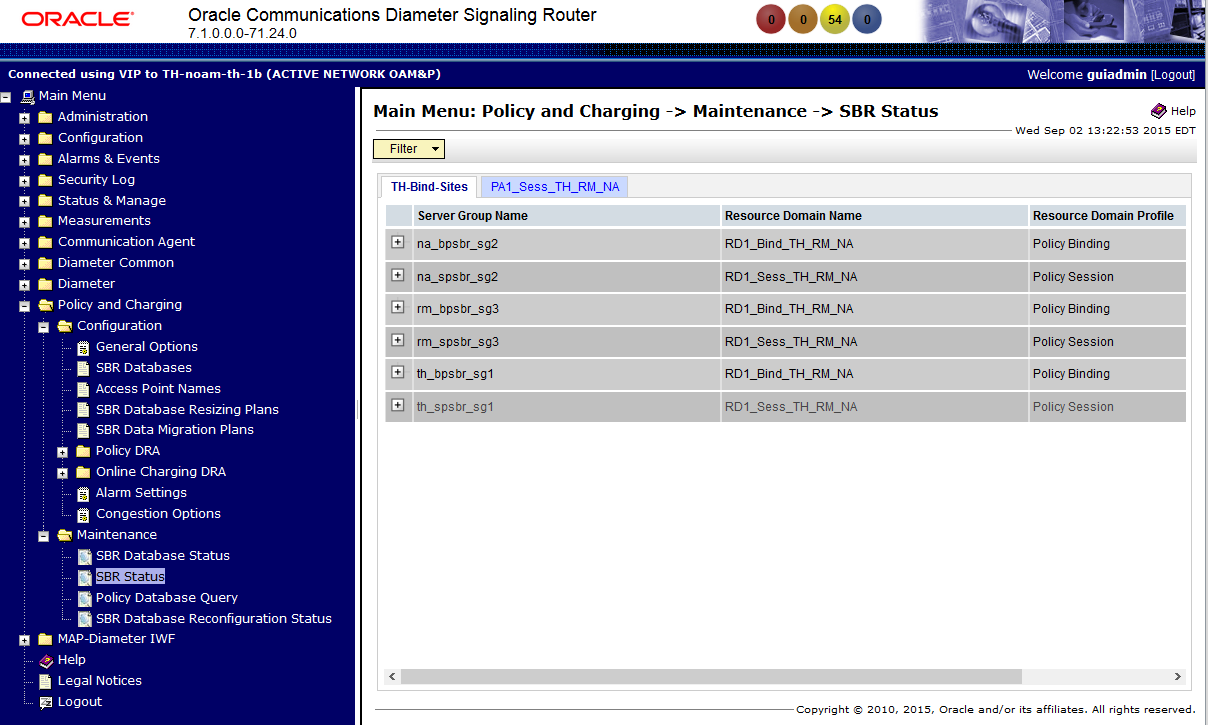
* + 1. **Network-Wide Options**



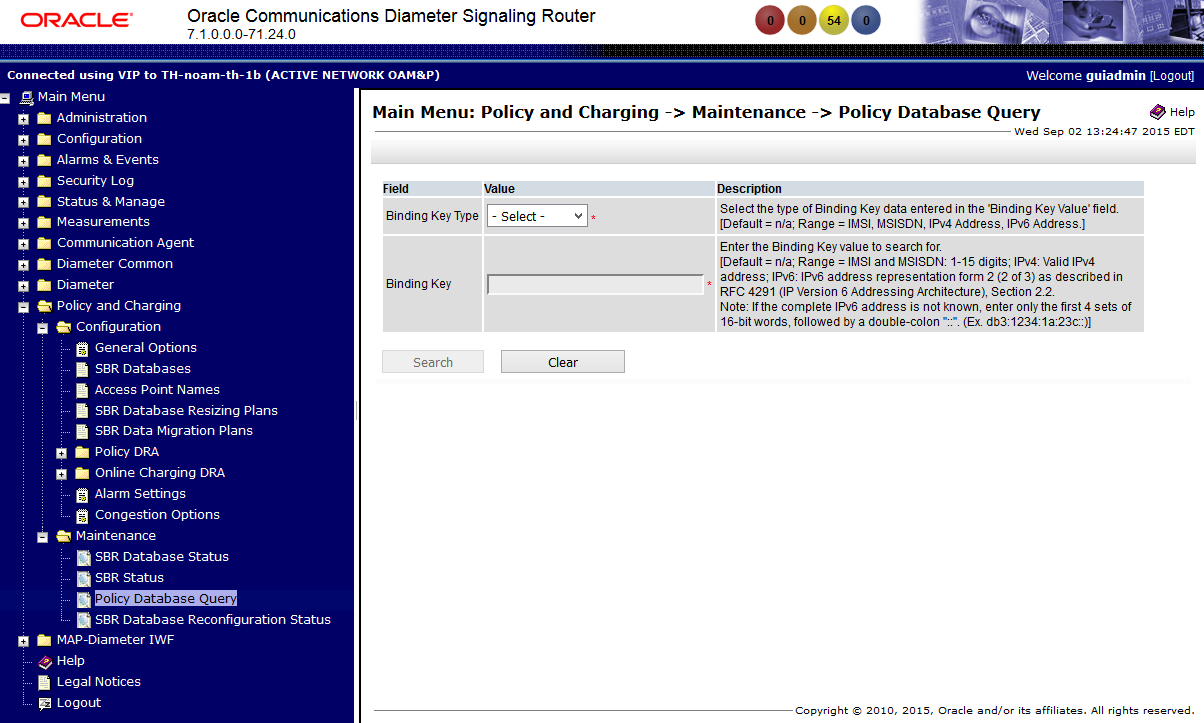
* 1. **Maintenance**
     1. **SBR Database Status**



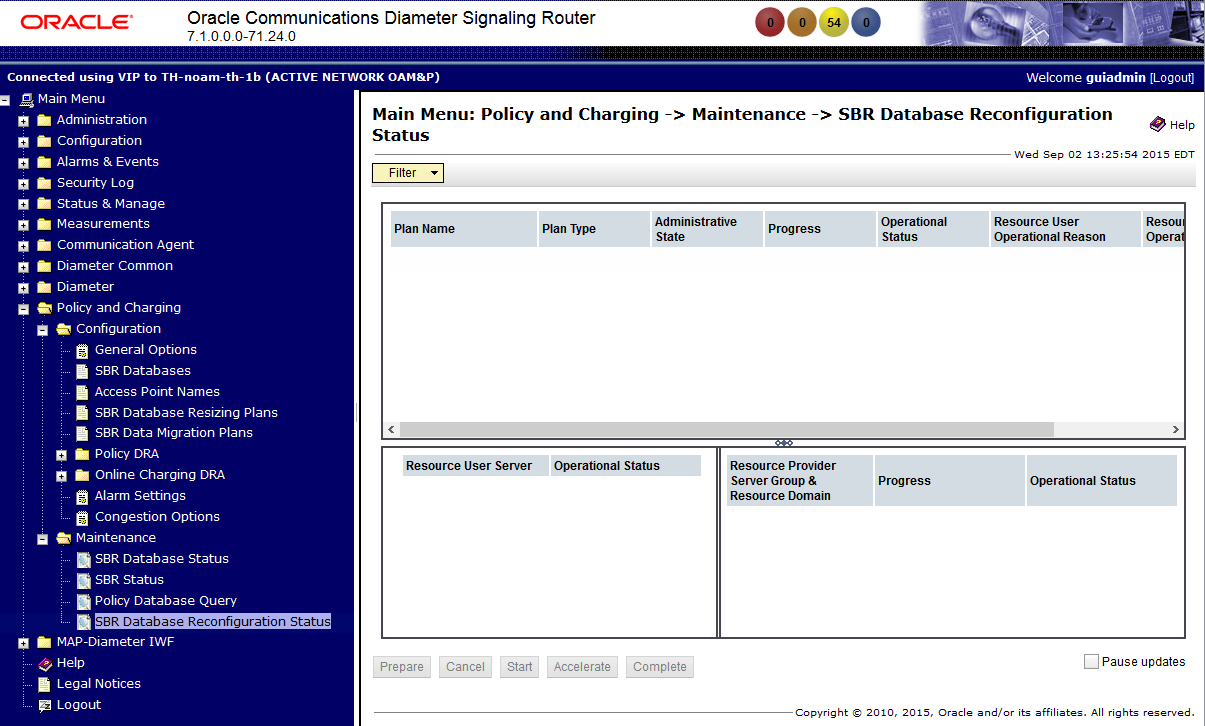
* + 1. **SBR Status**



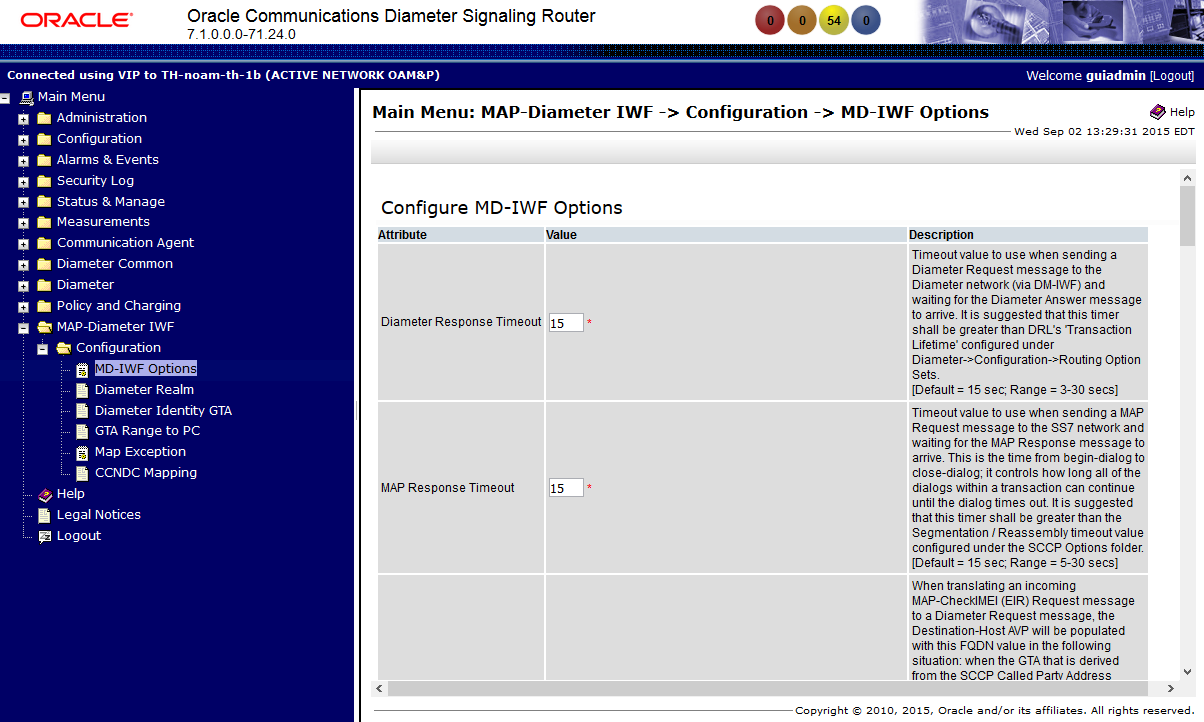
* + 1. **Policy Database Query**



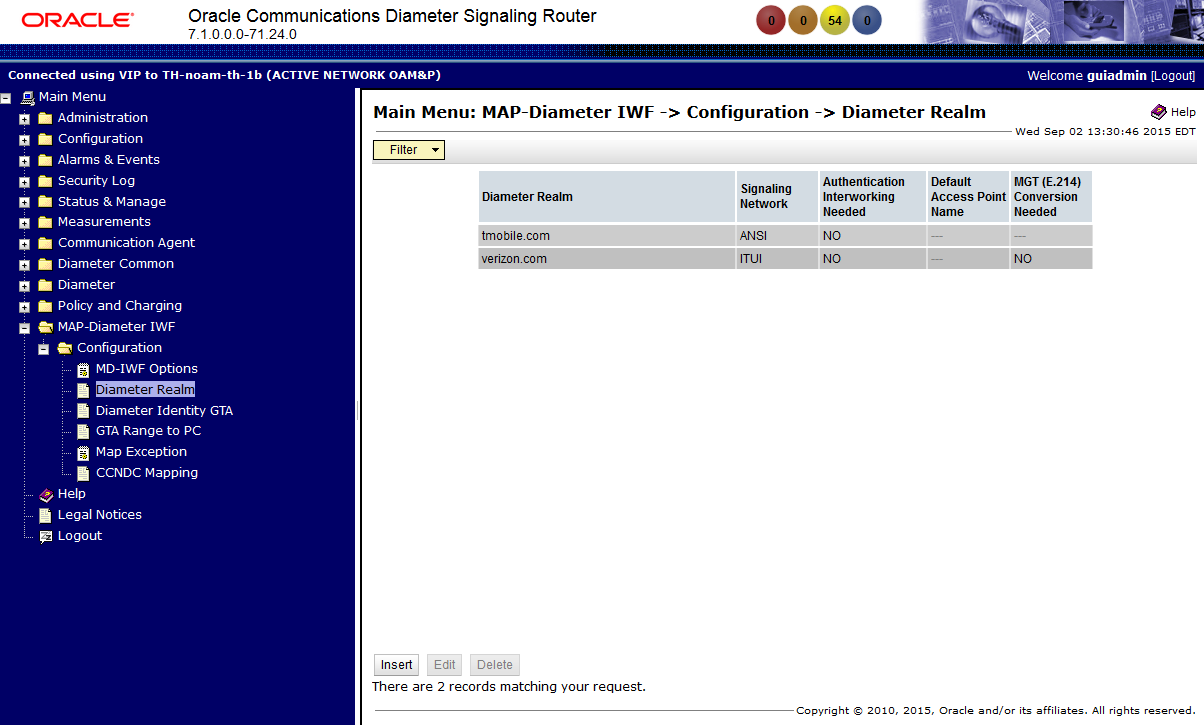
* + 1. **SBR Database Reconfiguration Status**



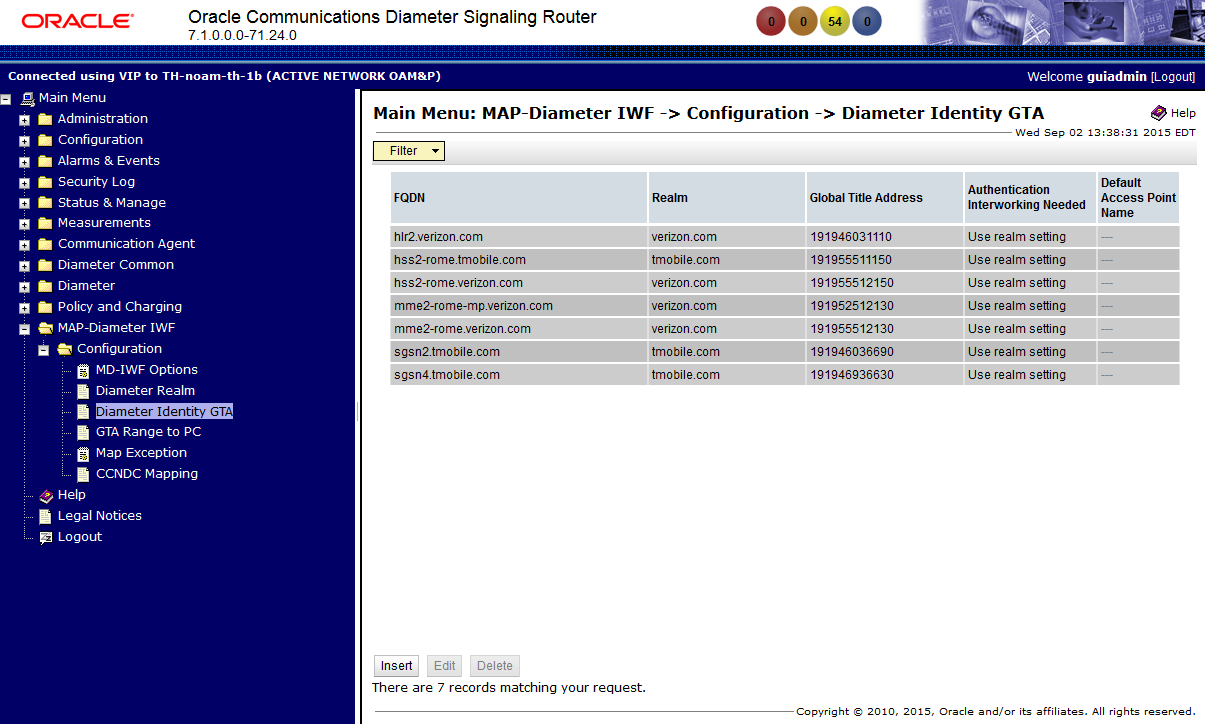
1. **MAP-Diameter IWF (NOAM)**
   1. **Configuration**
      1. **MD-IWF Options**



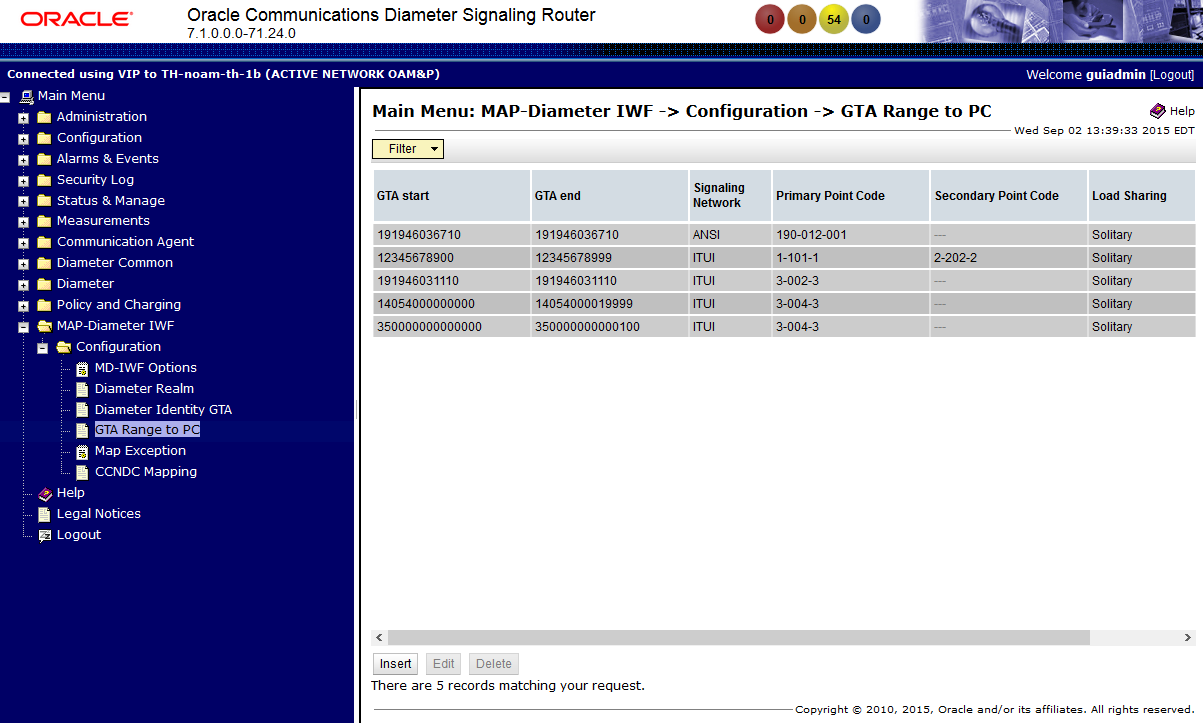
* + 1. **Diameter Realm**



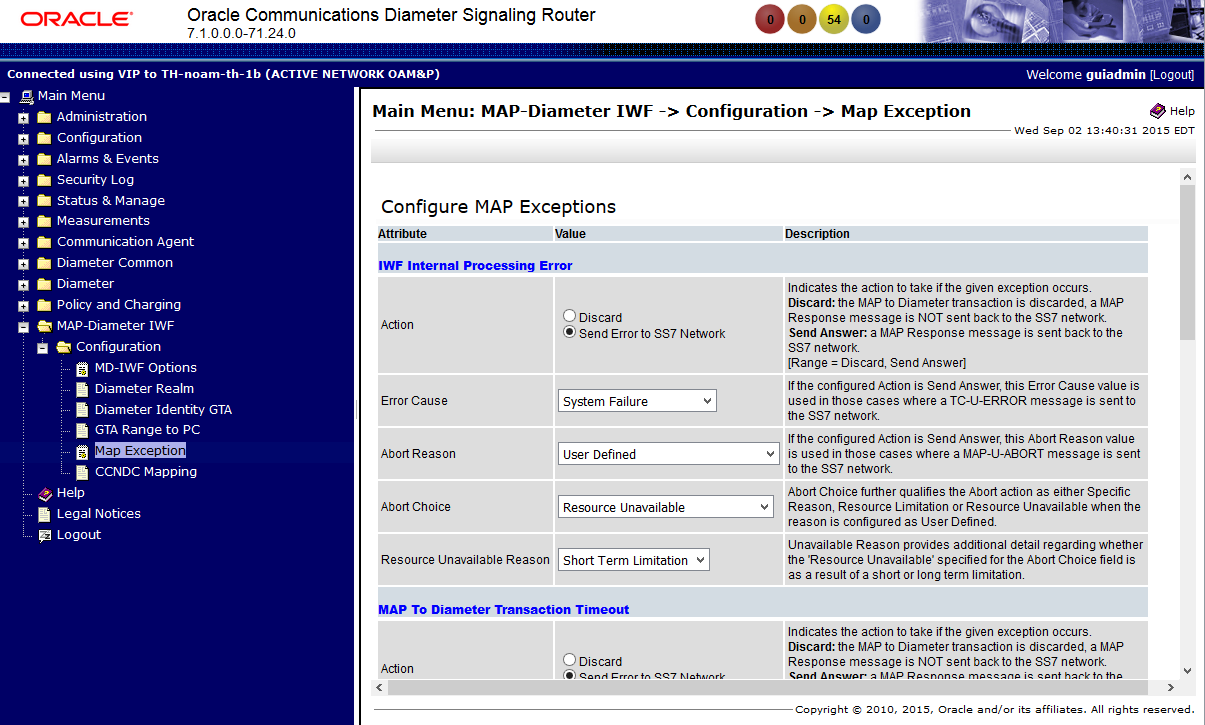
* + 1. **Diameter Identity GTA**



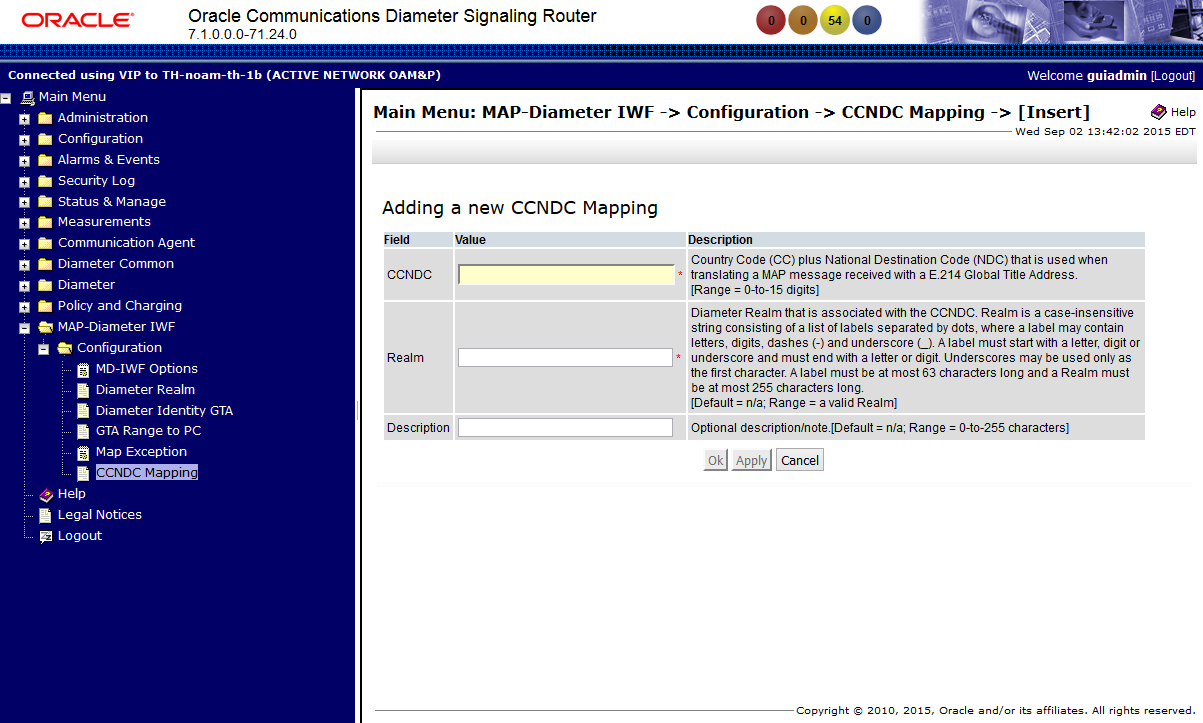
* + 1. **GTA Range to PC**



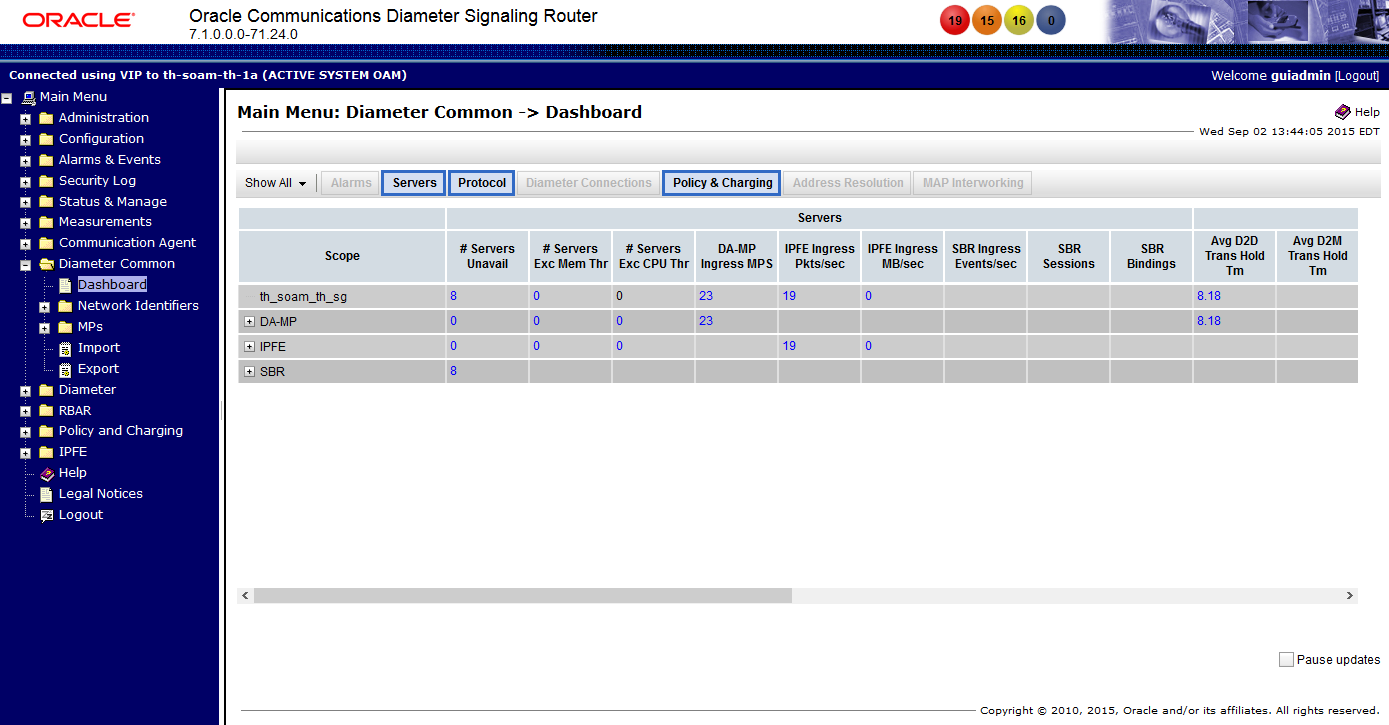
* + 1. **Map Exception**



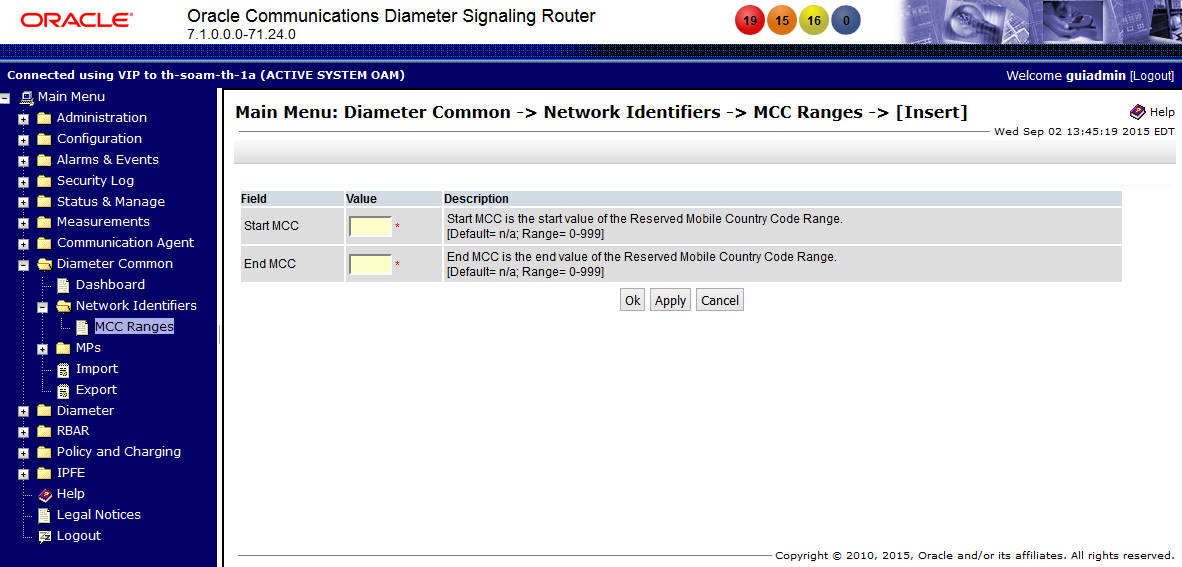
* + 1. **CCNDC Mapping**



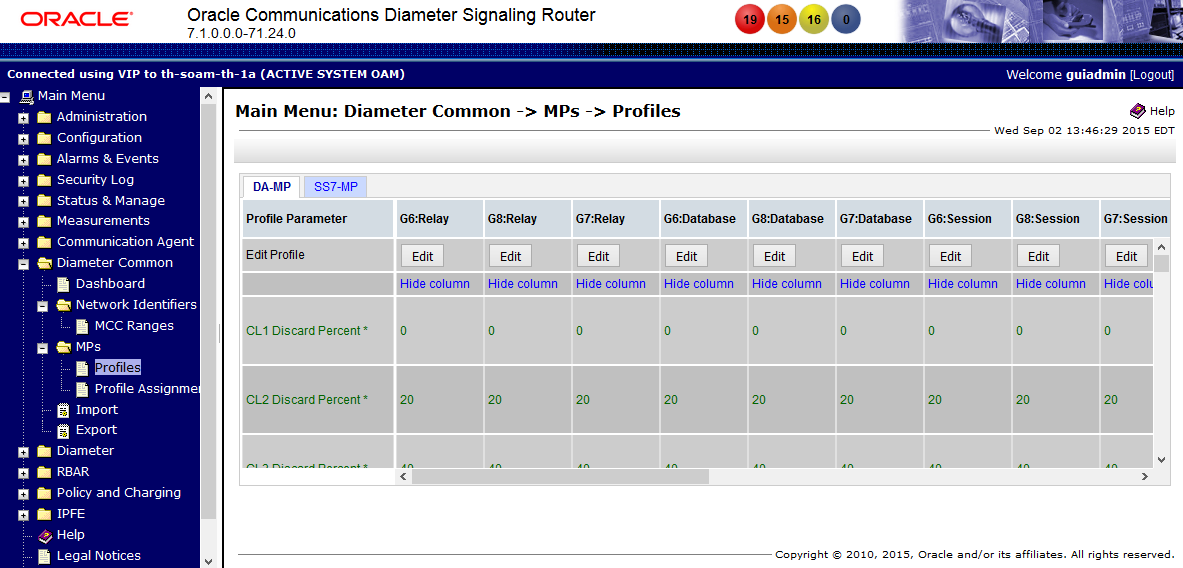
1. **Diameter Common (SOAM)**
   1. **Dashboard**



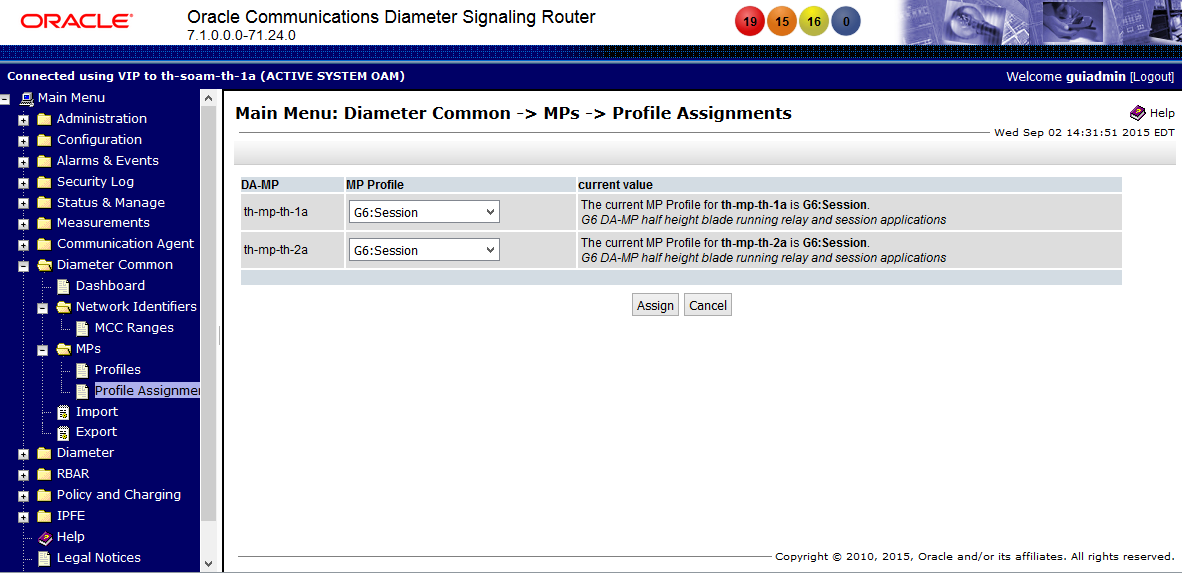
* 1. **Network Identifiers -> MCC Ranges**



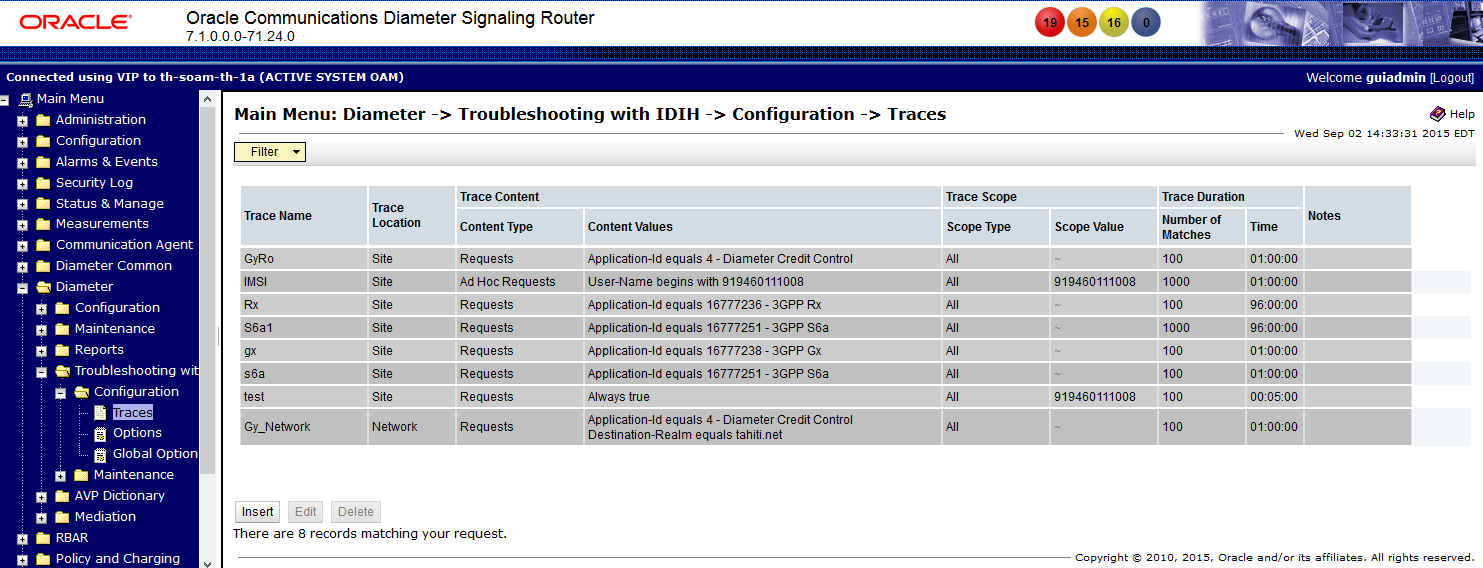
* 1. **MPs -> Profiles**



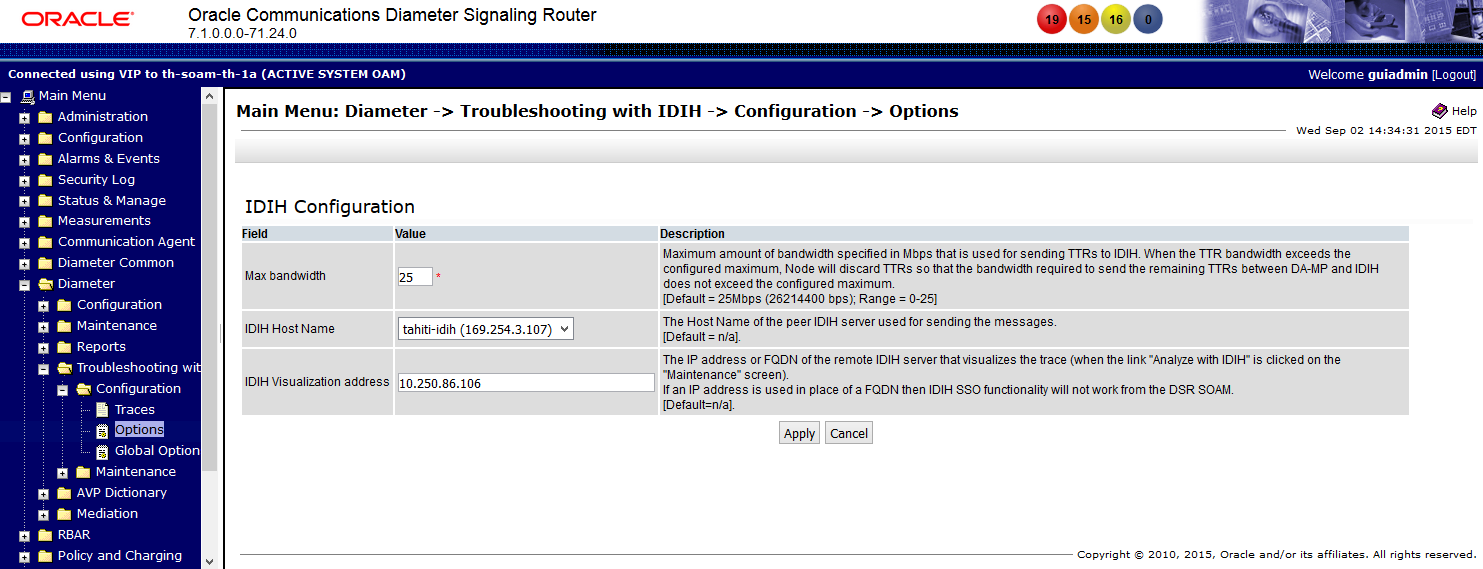
* 1. **MPs -> Profiles Assignments**



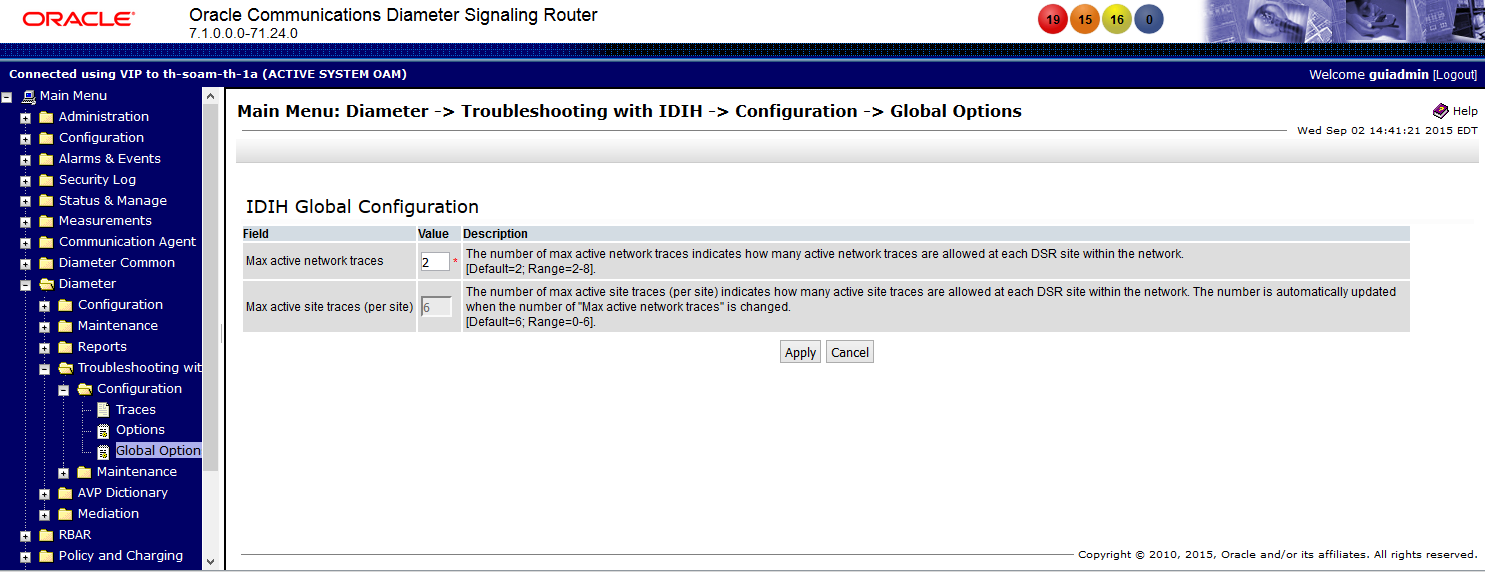
1. **Diameter (SOAM)**
   1. **Troubleshooting with IDIH**
      1. **Configuration -> Traces**



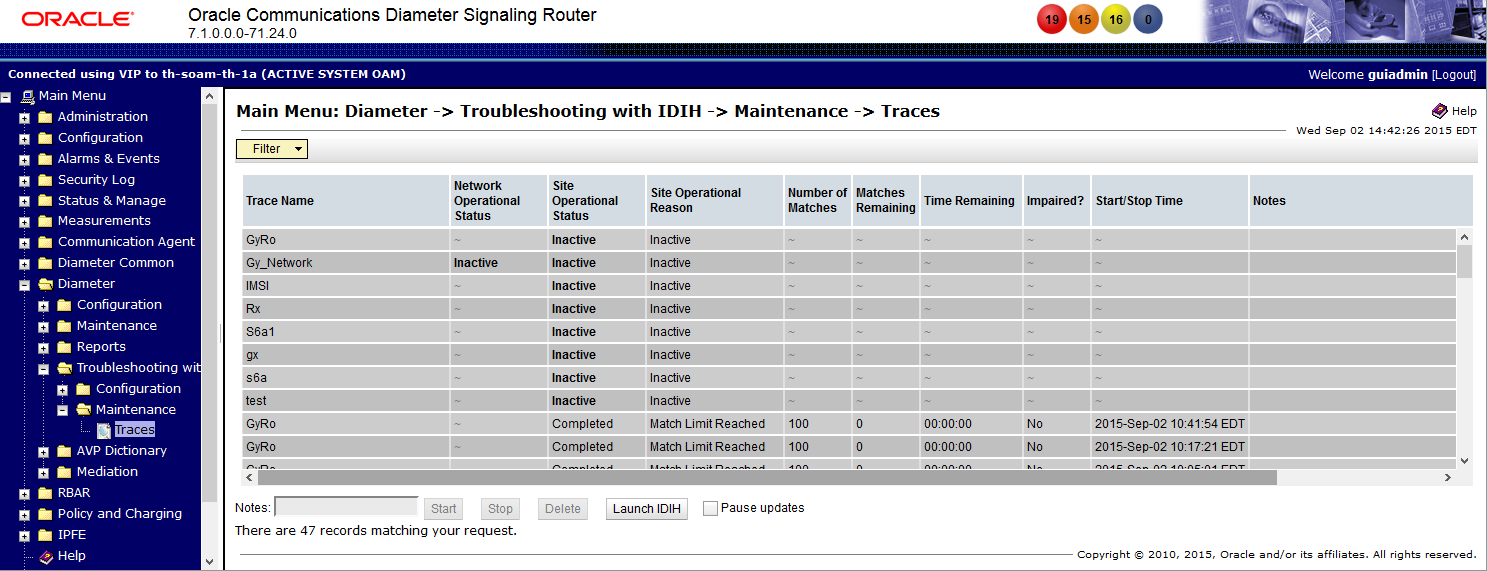
* + 1. **Configuration -> Options**



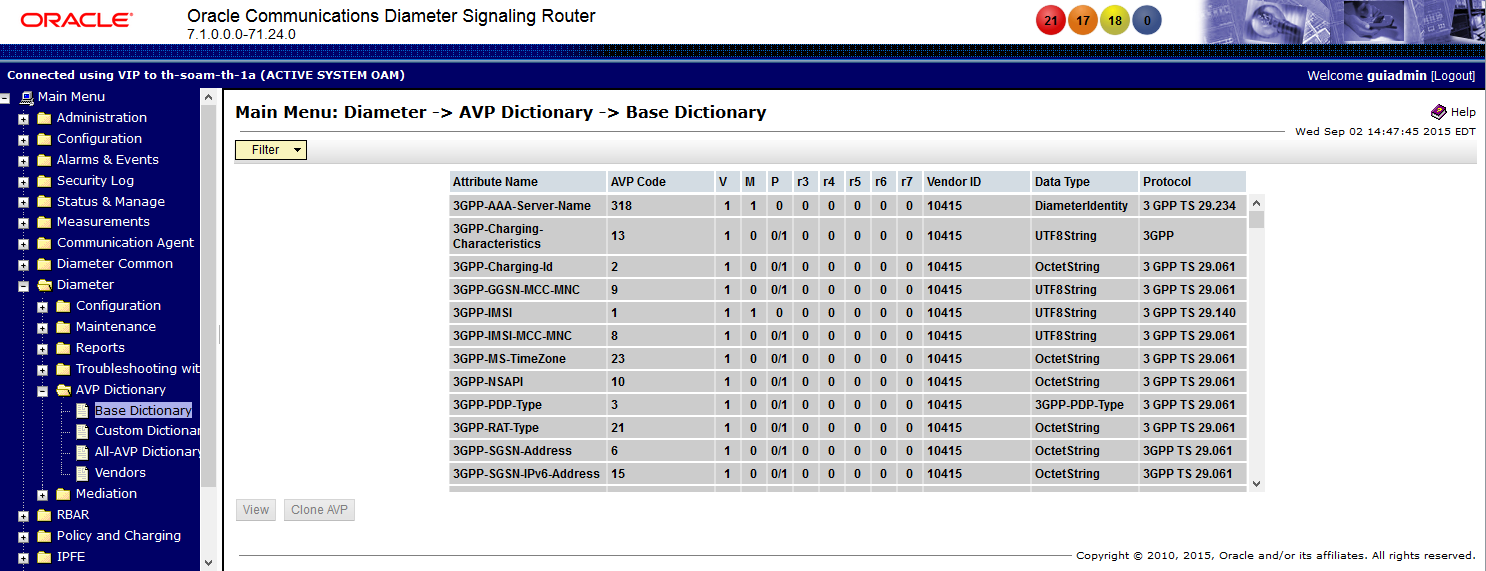
* + 1. **Configuration -> Global Options**



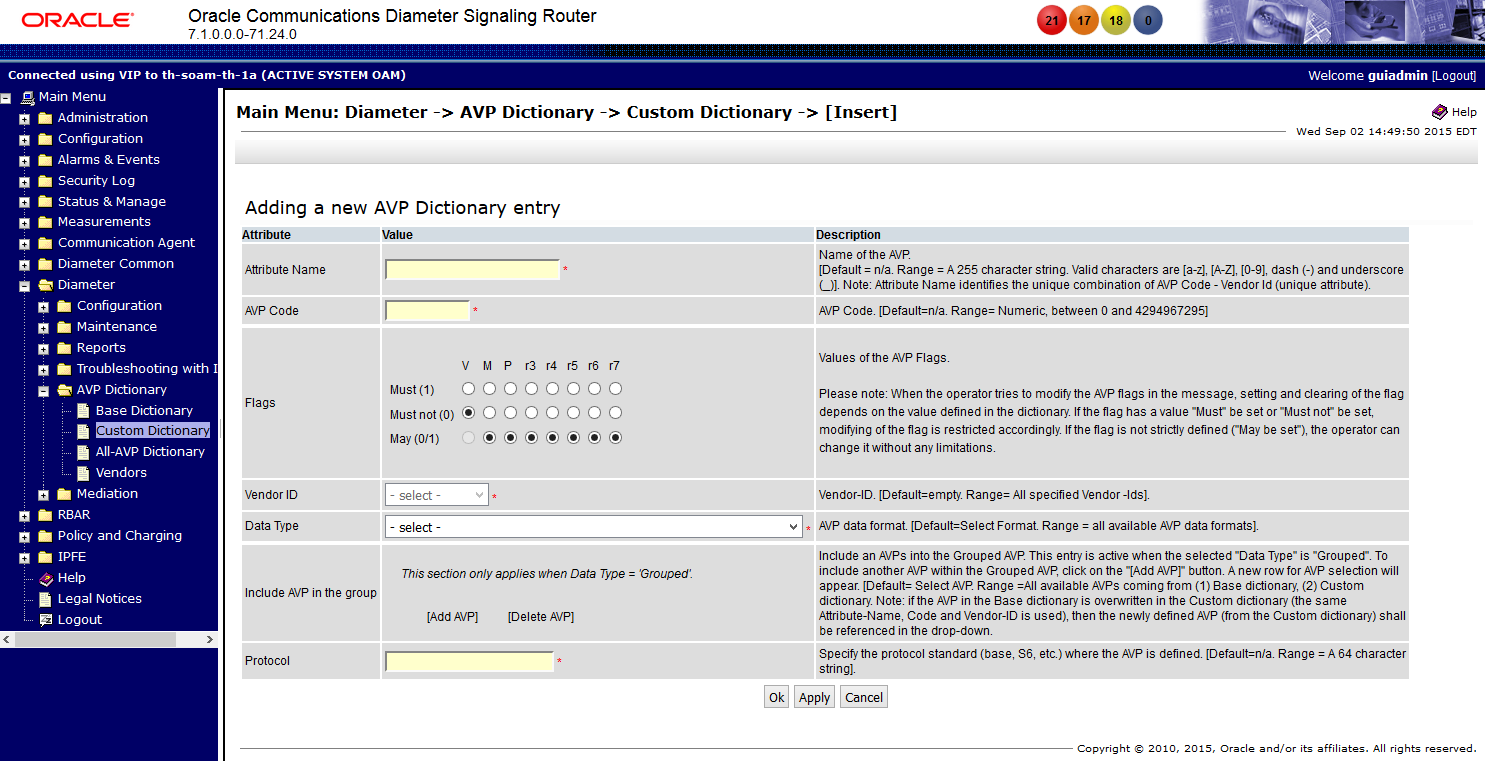
* + 1. **Maintenance -> Traces**



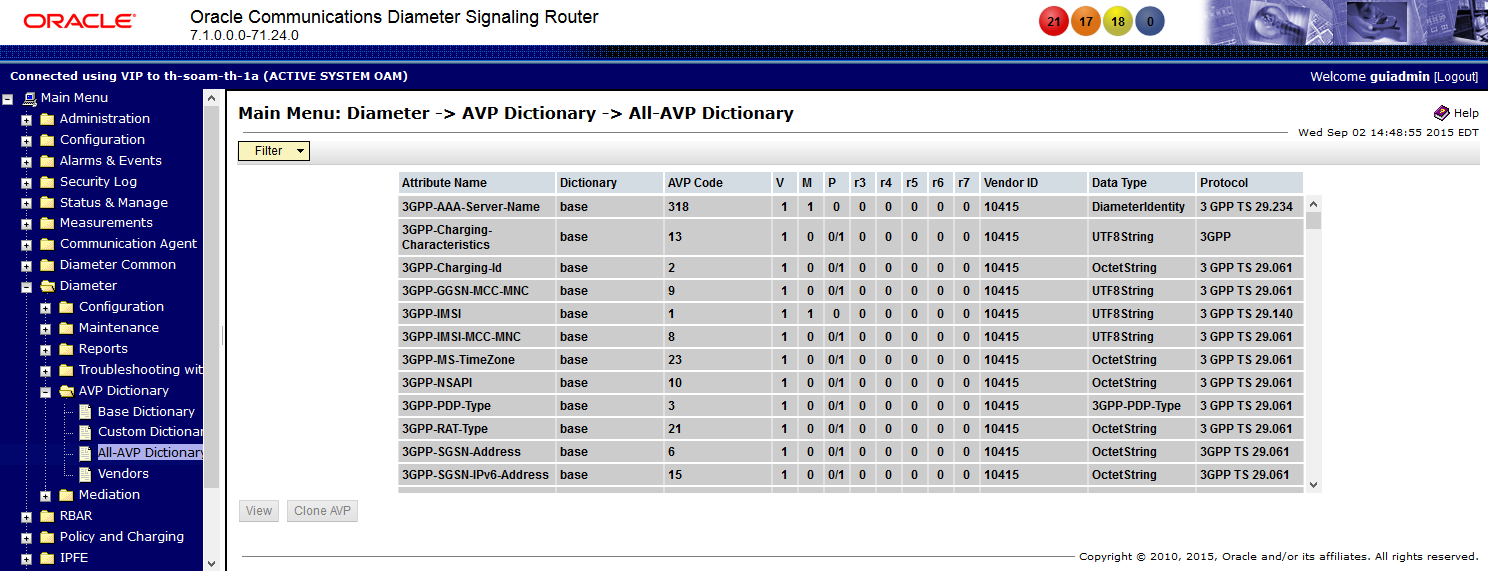
* 1. **AVP Dictionary**
     1. **AVP Dictionary -> Base Dictionary**



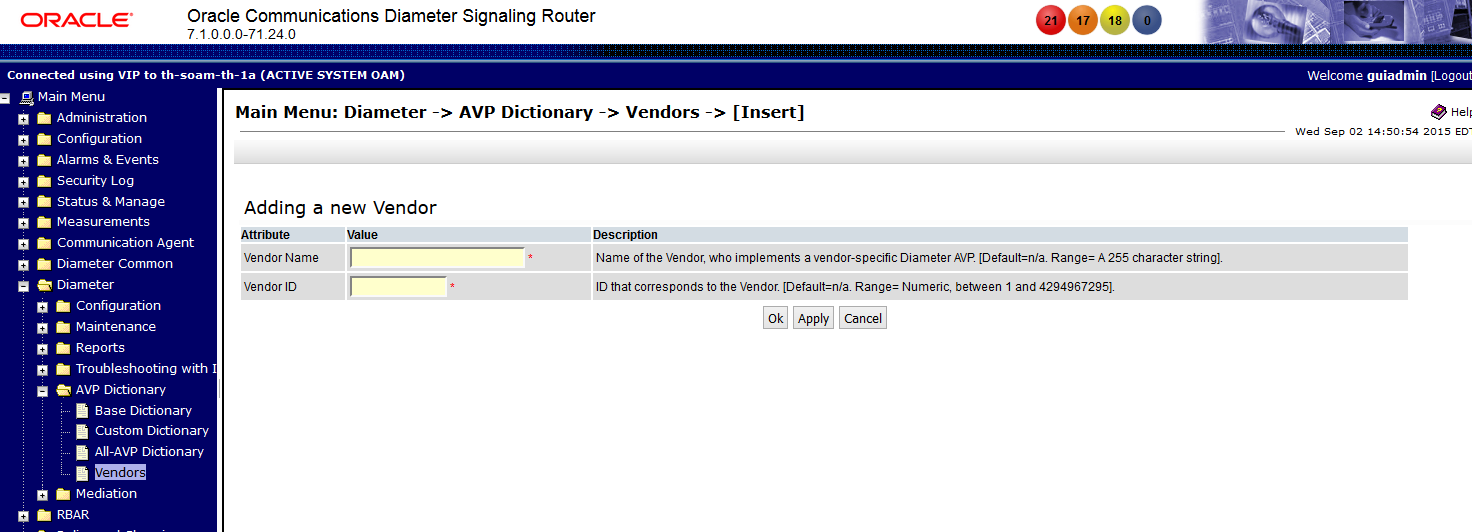
* + 1. **AVP Dictionary -> Custom Dictionary**



* + 1. **AVP Dictionary -> All-AVP Dictionary**



* + 1. **AVP Dictionary -> Vendors Dictionary**



1. **MEAL Inserts**

This section will summarize the changes to Alarms, Measurements and KPIs. In the following inserts pertain to 7.1 and deltas with 5.0, 6.0, and 7.0 Alarms, Measurements, KPIs, and MIBs.

(Includes 5.0 to 7.1 deltas)

(Includes 6.0 to 7.1 deltas)

(Includes 7.0 to 7.1 deltas)

dsr-7.1.0.0.0-71.24.1

* 1. **Alarm/Measurements/KPIs/MIBs Delta ( 7.1)**

**  **

The attached spreadsheets contain a column “Change Type” to indicate the following types of changes:

Added (Green color background)

Deleted (Red color background)

Changed ( Orange color background)

Unchanged (white color background)

Alarms, Measurements, KPI’s and MIB Notifications for new Optional features are not listed. Please see the documentation for these new features.

Scope: An alarm with B scope is reported at the SOAM and NOAM. An alarm with A scope is reported at the NOAM only.

1. **Reference List**

**DSR 7.1 User Guides for DSR (see customer documentation)**

[**http://docs.oracle.com/cd/E63474\_01/index.htm**](http://docs.oracle.com/cd/E63474_01/index.htm)

**Diameter Signaling Router (DSR) 7.1 Core Document Set**

*DSR 7.1 Release NoticePDF*

*DSR 7.1 Licensing Information User ManualPDF*

*Planning, Installation, Upgrade, and Disaster Recovery*

*DSR Hardware and Software Installation Procedure 1/2PDF*

*DSR Software Installation and Configuration Procedure 2/2PDF*

*DSR 7.1 Software Upgrade GuidePDF*

*Three-tier Disaster Recovery GuidePDF*

*RMS Productization Installation GuidePDF*

*RMS Productization Disaster Recovery GuidePDF*

*PCA ConfigurationPDF*

*GLA Feature Activation ProcedurePDF*

*CPA Feature Activation ProcedurePDF*

*Mediation Feature Activation ProcedurePDF*

*FABR Feature Activation ProcedurePDF*

*RBAR Feature Activation ProcedurePDF*

*MAP-Diameter Feature Activation ProcedurePDF*

*DSR Network Impact ReportWord*

*Diameter Signaling Router 7.1 Core Document Set*

*Operation, Administration, and Maintenance (OAM) GuidePDF*

*Communication Agent User's GuidePDF*

*Roadmap to Hardware Documentation (Gen8)PDF*

*Policy and Charging Application User's GuidePDF*

*Diameter User's GuidePDF*

*Mediation User's GuidePDF*

*Range Based Address Resolution (RBAR) User's GuidePDF*

*Full Address Based Resolution (FABR) User's GuidePDF*

*Charging Proxy Application (CPA) and Offline Charging Solution User's GuidePDF*

*IP Front End (IPFE) User's GuidePDF*

*DSR Alarms and KPIs ReferencePDF*

*Diameter Measurements ReferencePDF*

*Diameter Common User's GuidePDF*

*Diameter Administrator's GuidePDF*

*MAP-Diameter IWF User's GuidePDF*

*SS7/SIGTRAN User's GuidePDF*

*Transport Manager User's GuidePDF*

*Gateway Location Application (GLA) User's GuidePDF*

*Related Publications ReferencePDF*

**Integrated Diameter Intelligence Hub (IDIH) 7.1 Document Set**

IDIH User's GuidePDF

IDIH Audit Viewer Administrator's Guide PDF

IDIH Alarm Forwarding Administrator's GuidePDF

IDIH Operations, Administration and Maintenance Administrator’s GuidePDF

IDIH ProTrace User's Guide PDF

IDIH System Alarms User's GuidePDF

IDIH Log Viewer User's GuidePDF