

Oracle® Communications
Diameter Signaling Router
Policy and Charging Application Configuration
Release 7.3
E67989, Revision 02

August 2016

ORACLE®

Copyright ©2012, 2016 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, then 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

My Oracle Support (MOS) (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>.

Table of Contents

LIST OF TABLES	4
LIST OF FIGURES.....	4
LIST OF PROCEDURES.....	4
1.0 INTRODUCTION	6
1.1 PURPOSE AND SCOPE	6
1.2 REFERENCES	6
1.3 GLOSSARY	6
1.4 GENERAL PROCEDURE STEP FORMAT.....	9
2.0 PCA CONFIGURATION OVERVIEW	11
2.1 REQUIRED CONFIGURATION DATA	11
2.2 PCA CONFIGURATION SUMMARY	13
3.0 PCA CONFIGURATION PREPARATION	14
3.1 HARDWARE PREPARATION.....	14
3.2 REQUIRED MATERIALS CHECK	14
3.3 SYSTEM TOPOLOGY CHECK	15
3.4 PCA / POLICY AND CHARGING SBR TOPOLOGY CHECK.....	18
3.5 DIAMETER NETWORK CHECK.....	22
3.5.1 <i>Diameter Network Check for Policy DRA.....</i>	<i>22</i>
3.5.2 <i>Diameter Network Check for Online Charging DRA</i>	<i>25</i>
3.6 PERFORM HEALTH CHECK.....	26
4.0 PCA CONFIGURATION.....	27
4.1 PLACE ASSOCIATIONS CONFIGURATION	28
4.1.1 <i>Policy and Charging Places</i>	<i>28</i>
4.1.2 <i>Policy and Charging Mated Sites Place Associations</i>	<i>29</i>
4.1.3 <i>Policy Binding Region Place Associations.....</i>	<i>29</i>
4.2 RESOURCE DOMAINS CONFIGURATION	31
4.2.1 <i>Policy and Charging DRA Resource Domain Configuration.....</i>	<i>31</i>
4.2.2 <i>Policy Session Resource Domain Configuration</i>	<i>32</i>
4.2.3 <i>Policy Binding Resource Domain Configuration</i>	<i>33</i>
4.3 DIAMETER CONFIGURATION PROCEDURES	35
4.3.1 <i>Diameter Configuration for Policy DRA.....</i>	<i>35</i>
4.3.2 <i>Diameter Configuration for Online Charging DRA</i>	<i>52</i>
4.4 PCA FUNCTION CONFIGURATION PROCEDURES.....	65
4.4.1 <i>Policy DRA Configuration</i>	<i>66</i>
4.4.2 <i>Online Charging DRA Configuration.....</i>	<i>75</i>
4.5 CONFIGURING ONLINE CHARGING FUNCTION ON A RUNNING DSR PCA SYSTEM	81
4.5.1 <i>Configuring new Online Charging DRA Sites.....</i>	<i>81</i>
4.5.2 <i>Configuring Online Charging DRA in existing Sites</i>	<i>81</i>
4.5.3 <i>Configuring Online Charging DRA in existing Sites with scaling</i>	<i>81</i>
4.6 CONFIGURING POLICY DRA FUNCTION ON A RUNNING DSR PCA SYSTEM.....	82
4.6.1 <i>Configuring Policy DRA</i>	<i>82</i>
4.7 UN-CONFIGURING POLICY DRA FUNCTION FROM A RUNNING DSR PCA SYSTEM.....	83
4.8 UN-CONFIGURING ONLINE CHARGING FUNCTION FROM A RUNNING DSR PCA SYSTEM	86
4.9 POST-CONFIGURATION PROCEDURES	87
4.9.1 <i>Enable Application</i>	<i>87</i>
4.9.2 <i>Enable SBR Databases</i>	<i>89</i>

Policy and Charging Application Configuration

4.9.3	Restart Process.....	90
4.9.4	Enable Connections.....	90
4.9.5	Perform Health Check.....	91
5.0	CAVEATS.....	93
6.0	CUSTOMER SERVICE SIGN OFF.....	94
	DISCREPANCY LIST	94
7.0	APPENDIX-A	95
7.1	PCA FEATURE ACTIVATION PROCEDURE.....	95
7.1.1	PCA Activation on an installed or upgraded system	95
7.1.2	PCA Activation on a newly added site.....	97
7.1.3	Restart Process.....	97
7.1.4	Post PCA Activation System Health Check	98
7.2	PCA FEATURE DEACTIVATION PROCEDURE	101
7.2.1	Pre PCA Deactivation Steps.....	101
7.2.2	PCA Deactivation Procedure	105
7.2.3	Site Specific PCA Deactivation Procedure	106
7.2.4	Post PCA Deactivation Steps	107
7.2.5	Post PCA Deactivation System Health Check	109
8.0	APPENDIX-B	112

List of Tables

Table 1. Acronyms	6
Table 2. Terminology	7

List of Figures

Figure 1: Example of a procedure step.....	10
Figure 2: Example – Mated Pair PCA / Policy and Charging SBR Topology	18

List of Procedures

Procedure 1: Required Materials Check	14
Procedure 2: System Topology Check	16
Procedure 3: Record Required Configuration Information.....	20
Procedure 4: Record Required P-DRA Diameter Configuration.....	23
Procedure 5: Record Required OC-DRA Diameter Configuration.....	25
Procedure 6: Perform Health Check (PCA configuration Preparation).....	26
Procedure 7: Policy and Charging Places configuration.....	28
Procedure 8: Policy and Charging Mated Sites Place Associations configuration	29
Procedure 9: Policy Binding Region Place Associations configuration	30
Procedure 10: Policy and Charging DRA Resource Domain configuration	31
Procedure 11: Policy Session Resource Domain configuration	32
Procedure 12: Policy Binding Resource Domain configuration	33
Procedure 13: Diameter configuration for Policy DRA.....	35
Procedure 14: Diameter configuration for Online Charging DRA	52
Procedure 15: Policy DRA configuration.....	66
Procedure 16: Online Charging DRA configuration	75

Policy and Charging Application Configuration

Procedure 17: New Online Charging DRA Site Configuration	81
Procedure 18: Online Charging DRA Configuration on a running DSR PCA System	81
Procedure 19: Online Charging DRA Configuration with scaling on a running DSR PCA System	81
Procedure 20: Policy DRA Configuration with scaling on a running DSR PCA System	82
Procedure 21: Un-configuring Policy DRA	83
Procedure 22: Un-configuring Online Charging DRA	86
Procedure 23: Enable Application	87
Procedure 24: Enable SBR Databases	89
Procedure 25: Restart Server	90
Procedure 26: Enable connections	90
Procedure 27: Perform Health Check	92
Procedure 28: Verify PCA Activation Pre-Requisites	95
Procedure 29: PCA Activation on the entire network	96
Procedure 30: PCA Activation on newly added site	97
Procedure 31: Restart Process	97
Procedure 32: Verification of application activation on NOAM Server	98
Procedure 33: Verification of application activation on SOAM Servers	100
Procedure 34: Verify and Deactivate GLA application	101
Procedure 35: Unconfigure PCA Functions (PDRA and OCDRA)	102
Procedure 36: Disable Diameter Connections	102
Procedure 37: Disable application	103
Procedure 38: Remove DSR configuration data	104
Procedure 39: PCA Application Deactivation	105
Procedure 40: PCA Application Deactivation on a particular site	106
Procedure 41: Move Policy and Charging SBR Servers to OOS State	107
Procedure 42: Remove Policy and Charging SBR Servers from Server Groups	107
Procedure 43: Delete Server Groups related to Policy and Charging SBR	108
Procedure 44: Remove Place configuration data	108
Procedure 45: Reboot the Servers	108
Procedure 46: Verification of application deactivation on NOAM Server	109
Procedure 47: Verification of application deactivation on SOAM Servers	110
Procedure 48: Restarting DA-MP servers on a running DSR system	112
Procedure 49: Rebooting DA-MP servers on a running DSR system	112

1.0 INTRODUCTION

1.1 PURPOSE AND SCOPE

This document defines the procedures required to configure the Policy and Charging Application (PCA) on a DSR system. This document contains information that is needed to configure and enable PCA which includes configuring:

- Resource Domains
- Place and Place Associations
- Diameter Stack, and
- SBR Databases

This document also provides the procedures to activate and deactivate PCA.

The audience for this document includes these Oracle CGBU Groups:

- Software Development
- Product Verification
- Documentation
- Customer Service:
 - Design Support
 - Oracle TAC
 - Professional Services

No additional software installation is required prior to executing this procedure. The standard installation procedure documented in Reference [1] and [2] have installed all of the required software. PCA also requires SBR function for which software is also included in standard installation described in Reference [2].

The scope of this document is limited to guiding the user on mandatory configurations required to run Policy and Charging Application. This document does not intend to train the user on deployment options. Redundency Level of PCA Sites and Diameter Routing should be planned prior to executing the configuration steps listed in this document. Such planning is outside the scope of this document.

1.2 REFERENCES

- [1] *DSR 7.3 Hardware and Software Installation Procedure 1/2, E53488-03*
- [2] *DSR 7.3 Software Installation and Configuration Part 2/2, E69409-02*
- [3] *IP Front End (IPFE) User's Guide, E73317-01*
- [4] *Policy Charging Application User's Guide, E73186-01*
- [5] *IDIH User's Guide, E69819-01*
- [6] *DSR Software Upgrade Guide, Release 7.3, E73343-01*
- [7] *Diameter User's Guide Release 7.3, E73184-01*
- [8] *DSR GLA Feature Activation Procedure, Release 7.3, E58659-04*

1.3 GLOSSARY

Table 1. Acronyms

ART	Application Route Table
BBERF	Bearer Binding and Event Reporting Function (Policy Client)
COMAGENT	Communication Agent
CTF	Charging Trigger Function (Online Charging Client)

DA-MP	Diameter Agent Message Processor
DB	Database
DPI	Diameter Plug-In
DSR	Diameter Signaling Router
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IP	Internet Protocol
IPFE	Internet Protocol Front End
MP	Message Processing or Message Processor
NE	Network Element
NO	Network OAM
NOAM	Network OAM
OAM	Operations, Administration and Maintenance
OC-DRA	Online Charging DIAMETER Routing Agent
OCS	Online Charging System (Online Charging Server)
P-DRA	Policy DIAMETER Routing Agent
PCA	Policy and Charging Application
PCEF	Policy and Charging Enforcement Function (Policy Client)
PCRF	Policy and Charging Rules Function (Policy Server)
PRT	Peer Route Table
SBR	Policy and Charging Subscriber Binding Repository
SO	System OAM
SOAM	System OAM
SSH	Secure Shell
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface

Table 2. Terminology

Term	Definition
PCA Application	The Policy and Charging Application hosts the Policy DRA and Online Charging DRA functionality for intelligent routing of policy and charging Diameter signaling. The PCA application is activated and deactivated using the PCA feature activation and deactivation scripts. The PCA application can be enabled and disabled per DA-MP server using the Main Menu: Diameter -> Maintenance -> Application Status GUI.
PCA Function	The PCA Application host two functions: Policy DRA and Online Charging DRA. The administrative state of these functions is controlled via the Main Menu: Policy and Charging Application -> Configuration -> General Options GUI – not by the Main Menu: Diameter -> Maintenance -> Application Status GUI. PCA Functions can be enabled and disabled independently of each other and without requiring feature deactivation or server restarts. PCA function enable and disable are system-wide in scope.
PCA Mated Sites	PCA Sites are said to be “mated” if they share an SBR Database for purposes of Site Redundancy.
PCA Site	The name of the Site where a DSR running the Policy and Charging Application is located. All of the DA-MP and SBR servers at a PCA Site must have the same Site Place name.

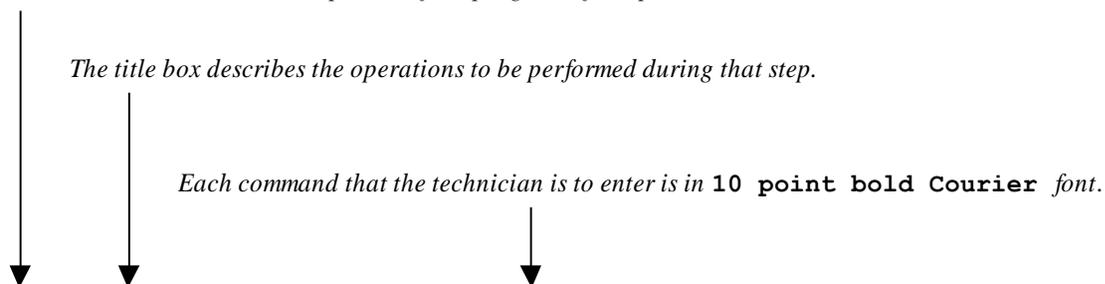
Term	Definition
Place	A Server can be assigned a "Place" that denotes its physical location. The Place type called "Site" is used to specify which DSR node a given server is located at. A Place is needed for each DSR node (DSR Site). The PCA application requires that all DA-MP servers and SBR servers be assigned to a "Site" Place.
Place Association	A container for Places (Sites) that have a relationship defined by the Place Association type. The PCA application defines two types of Place Associations: Policy Binding Region and Policy and Charging Mated Sites.
Policy and Charging Mated Sites Place Association	For a PCA network in which either the P-DRA function or the OC-DRA function are being used, a Policy and Charging Mated Sites Place Association is configured for each PCA Site or set of PCA Sites that will share an SBR Session Database. Typically there will be two Site Places in a Policy and Charging Mated Sites Place Association, but there could be one or three.
Policy and Charging DRA Resource Domain	A set of Server Groups having Function "DSR (multi-active cluster) that will be hosting the Policy and Charging DSR Application. One Policy and Charging DRA Resource Domain must be configured for each Policy and Charging Mated Sites Place Association.
Policy and Charging SBR Server Group	A Server Group with function set to "Policy and Charging SBR" – also known as an SBR Server Group. The SBR Binding Database and SBR Session Databases are hosted by one or more SBR Server Groups.
Policy Binding Region Place Association	For a PCA network in which the P-DRA function is being used, a Policy Binding Region Place Association is configured with all PCA Sites in the network.
Policy Binding Resource Domain	A set of SBR Server Groups that host the SBR Binding Database. See also Initial Resource Domain and Target Resource Domain.
Policy Session Resource Domain	A set of SBR Server Groups that host an instance of the SBR Session Database. See also Initial Resource Domain and Target Resource Domain.
Preferred Spare Server	A preference by a server in an SBR HA Policy to take on the role of spare server if other servers can successfully fulfill the active and standby roles. A preferred spare server can be promoted to standby if no other server is available for the standby role, or to active if no other servers are available for either active or standby roles.
Resource Domain	A container for Server Groups hosting a particular resource. See also Policy Binding Resource Domain and Policy Session Resource Domain.
Resource Provider	Resource Provider is a term used in the Communications Agent framework to refer literally to the provider of a software resource. A Resource Provider has a name, an identifier and an operational status. In the PCA application, an SBR Database consists of a number of resource providers equal to the number of Server Groups in the Resource Domain assigned to the database. Each resource provider hosts a portion of the logical database.
SBR Binding Database	The SBR Binding Database consists of Policy DRA binding records. The SBR Binding Database is hosted by Policy and Charging SBR Server Groups contained in a Policy Binding Resource Domain. The SBR Binding Database is accessible from all PCA Sites in the Policy Binding Region Place Association.
SBR Database	The PCA application supports two types of SBR Database: SBR Binding Database, used by the P-DRA function of PCA, and SBR Session Database, used by both P-DRA and OC-DRA functions of PCA. An SBR Database is hosted by Policy and Charging SBR Server Groups assigned to either a Policy Binding Resource Domain or a Policy Session Resource Domain.

Term	Definition
SBR HA Policy	The high availability policy that runs on an SBR Server group. The SBR HA Policy supports one active server, one standby server and 0 to 2 spare servers. When site redundancy is not needed, 1 active and 1 standby are deployed at the same site. If two-site redundancy is needed, 1 active and optionally 1 standby are deployed at one site and a spare is deployed at the mate site. If three-site redundancy is needed, 1 active and optionally 1 standby are deployed at one site, 1 spare is deployed at a mate site, and 1 spare is deployed at a second mate site.
SBR Session Database	An SBR Session Database consists of Policy DRA and/or Online Charging DRA session records. An SBR Session Database is hosted by Policy and Charging SBR Server Groups contained in a Policy Session Resource Domain. An SBR Session Database is accessible from all PCA Sites in a Policy and Charging Mated Sites Place Association. A PCA network can have many instances of an SBR Session Database.
Server Group	A container for servers having a common function. Example server group functions are Policy and Charging SBR, DSR Multi-Active Cluster, etc.
Site Redundancy	An HA arrangement in which one site can take over PCA functionality when one or two other PCA Mated Sites fail (e.g. due to flood, fire, etc.). See also, Two Site Redundancy and Three Site Redundancy.
Split Binding	A scenario when Diameter sessions for a given subscriber (identified by IMSI) originated from P-GW(s) having the same Access Point Name or routed to the same PCRF Pool exist on more than one PCRF that do not share state information.
Three Site Redundancy	An HA configuration in which SBR data is redundant across 3 typically geographically separate sites. In this configuration, SBR data integrity is preserved when at least one of the 3 sites remain operational.
Two Site Redundancy	An HA configuration in which SBR data is redundant across two typically geographically separate sites. In this configuration, SBR data integrity is preserved when one of the 2 sites remains operational.

1.4 GENERAL PROCEDURE STEP FORMAT

Figure 1 illustrates the general format of procedure steps as they appear in this document. Where it is necessary to explicitly identify the server on which a particular step is to be taken, the server name is given in the title box for the step (e.g. "ServerX" in Figure 1).

Each step has a checkbox for every command within the step that the technician should check to keep track of the progress of the procedure.



5 <input type="checkbox"/>	ServerX: Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. \$ <code>cu -l /dev/ttyS7</code>
-------------------------------	--	---

Figure 1: Example of a procedure step

2.0 PCA CONFIGURATION OVERVIEW

Before starting PCA configuration steps, PCA activation is required. Please refer to Appendix A in the document for activation details.

This section lists the required information needed to configure PCA. This includes topology configuration (e.g. Resource Domains, Places and Place Associations), Diameter and PCA specific configurations.

2.1 REQUIRED CONFIGURATION DATA

The following information needs to be collected by conducting a system/site survey. The user needs to plan the redundancy model required prior to system configuration.

- Please refer to the Diameter User's Guide^[7] for details of parameters required for configuring Diameter
- Please refer to the Policy Charging Application User's Guide^[4] for details of parameters required for configuration PCA Functions (Policy DRA, Online Charging DRA)

- A. A 3-tier DSR system installed using [1] and [2]
- B. Following Diameter configuration material
 1. List of supported Application Ids
 2. CEX Parameters
 3. Local and Peer Node(s) configuration parameters
 4. Diameter Connection parameters
 5. Routing configuration parameters
 - *Route Groups*
 - *Route Lists*
 - *Peer Route Tables*
 - *Application Route Tables*
 6. IDIH Configuration Parameters (Optional)
- C. Following PCA configuration material:
 1. Server Group configuration parameters
 2. Place configuration parameters
 3. Place Association configuration parameters
 4. Resource Domain configuration parameters
 5. SBR Databases
 6. Default Audit Options
 7. Access Point Names and the "Stale Session Timeout" for the APN
 8. Alarm Settings
 9. Congestion Settings

- D. Depending upon the PCA function, following configuration items
1. Policy DRA configuration parameters
 - PCRF Pools
 - PCRF Sub-Pools
 - Early Binding Options
 - Topology Hiding Options
 - Suspect Binding Removal Options
 - Session Integrity Option
 2. Online Charging DRA configuration parameters
 - OCS Realms/FQDNs and their session states
 - Realms that require Session State
 - CTFs that require Session State
 - Session State Scope
 - Session State Unavailable Action
 - OCS Pool Selection Mode.

2.2 PCA CONFIGURATION SUMMARY

An outline of the configurations required to run Policy and Charging Application on a DSR system is laid below.

- The information required to configure various components (for e.g. Diameter Common, Diameter Plugin and PCA is mentioned in Chapter 3.0.
 - Please use the references provided at the top of the procedures to gather details about the configuration parameters.
 - Please note that this document does not cover planning the site-redundancy levels or Diameter Routing.
 - The user needs to consult relevant Oracle contacts to discuss deployment and routing scenarios and figure out the deployment model most suitable for the given business needs. Once that is figured out, this document helps the user to feed the required configuration data into the DSR system to build the selected model.
- Policy and Charging Application feature needs to be activated prior to any configuration mentioned in this document. PCA activation instructions can be found in APPENDIX-A.
- If a new DSR system is being configured to run PCA, follow the configuration procedures in the following order:
 - Non Maintenance Window Procedures
 - Place Associations Configuration (Section 4.1)
 - Resource Domains Configuration (Section 4.2)
 - Diameter Configuration Procedures (Section 4.3)
 - PCA Function Configuration Procedures (Section 4.4)
 - Maintenance Window Procedures
 - Post-configuration Procedures (Section 4.9)
- If PCA is to be configured on an operational DSR system, follow the configuration procedures in the following order:
 - Non Maintenance Window Procedures
 - For Policy DRA Function – Configuring Policy DRA Function on a running DSR PCA System (Section 4.6)
 - For Online Charging DRA – Configuring Online Charging Function on a running DSR PCA System (Section 4.5)
 - Maintenance Window Procedures
 - Post-configuration Procedures (Section 4.9)

NOTE: Any site level configuration (steps that have **SOAM VIP** mentioned in the step name) must be repeated for each DSR site running PCA.

3.0 PCA CONFIGURATION PREPARATION

This section provides detailed procedures to prepare a system for PCA configuration.

3.1 HARDWARE PREPARATION

This document assumes that all necessary hardware has already been installed.

3.2 REQUIRED MATERIALS CHECK

This procedure verifies that all required materials needed for configuration have been collected and recorded.

Procedure 1: Required Materials Check

S T E P #	This procedure verifies that all required materials are present. Please refer to the Diameter User's Guide ^[7] for details of parameters required for configuring Diameter Please refer to the Policy Charging Application User's Guide ^[4] for details of parameters required for configuration PCA Functions (Policy DRA, Online Charging DRA) Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.	
	1 <input type="checkbox"/>	Verify that the configuration data has been collected

3.3 SYSTEM TOPOLOGY CHECK

This procedure is part of PCA configuration preparation and is used to verify the system topology of the DSR 7.3 network and servers.

Procedure 2: System Topology Check

S T E P #	<p>This procedure verifies System Topology.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>	
1 <input type="checkbox"/>	Verify Network Element Configuration data	<p>View the Network Elements configuration data; verify the data; save and print report:</p> <ol style="list-style-type: none"> 1. Log into the NOAM VIP GUI. 2. Select Configuration > Network Elements to view Network Elements Configuration screen. 3. Click Report at the bottom of the table to generate a report for all entries. 4. Verify the configuration data is correct for your network. 5. Save the report and/or print the report. Keep these copies for future reference.
2 <input type="checkbox"/>	Verify Services Configuration data	<p>View the Services configuration data; verify the data; save and print report:</p> <ol style="list-style-type: none"> 1. Select Configuration > Services to view Services screen. 2. Click Report at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for your network. 4. Save the report and/or print the report. Keep these copies for future reference.
3 <input type="checkbox"/>	Verify Place Configuration data	<p>View the Place configuration data; verify the data; save and print report:</p> <ol style="list-style-type: none"> 1. Select Configuration > Places to view Server Group screen. 2. Click Report at the bottom of the table to generate a report for all entries. 3. Verify that all DAMP servers that will be running the PCA application and all SBR MP Servers have a Site Place configured. 4. Save the report and/or print the report. Keep these copies for future reference.
4 <input type="checkbox"/>	Verify Server Group Configuration data	<p>View the Server Group configuration data; verify the data; save and print report:</p> <ol style="list-style-type: none"> 5. Select Configuration > Server Group to view Server Group screen. 6. Click Report at the bottom of the table to generate a report for all entries. 7. Verify that all Server Group(s) that have been identified to host the SBR Database(s) have the function "Policy and Charging SBR". 8. Save the report and/or print the report. Keep these copies for future reference.
5 <input type="checkbox"/>	Analyze and plan DA-MP restart sequence	<p>If the DSR system is running traffic other than PCA then all the DAMP servers must not be restarted/rebooted simultaneously. Doing so will cause a network/site wide outage. Instead a groups of DAMP servers must be selected and restarted one group at a time such that the servers that are operational when some are down can handle the additional traffic. Analyze system topology and plan for any DA-MPs which will be out-of-service during the PCA configuration sequence.</p> <ol style="list-style-type: none"> 1. Analyze system topology gathered in Step 1 and 2. 2. Determine exact sequence which DA-MP servers will be restarted (with the expected out-of-service periods). This sequence needs to be followed while executing APPENDIX-B
6 <input type="checkbox"/>	Verify Network Configuration data	<p>View the Network configuration data; verify the data; save and print report:</p> <ol style="list-style-type: none"> 1. Select Configuration > Network to view Network screen. 2. Click Report at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for your network. 4. Save the report and/or print the report. Keep these copies for future reference.
7 <input type="checkbox"/>	Verify Devices Configuration data	<p>View the Devices configuration data; verify the data; save and print report:</p> <ol style="list-style-type: none"> 1. Select Configuration > Network > Devices to view Devices screen. 2. Click Report All at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for your network.

		4. Save the report and/or print the report. Keep these copies for future reference.
--	--	---

3.4 PCA / POLICY AND CHARGING SBR TOPOLOGY CHECK

This procedure is part of PCA configuration preparation to identify the 3-tiered PCA topology for the deployed system. The following diagram depicts an example of a 2 site Mated-Pair PCA system. The topology configuration will depend on the customer’s choice of deployment options: standalone (no site-redundancy), mated pair (2 site-redundancy) or mated triplet (3 site-redundancy).

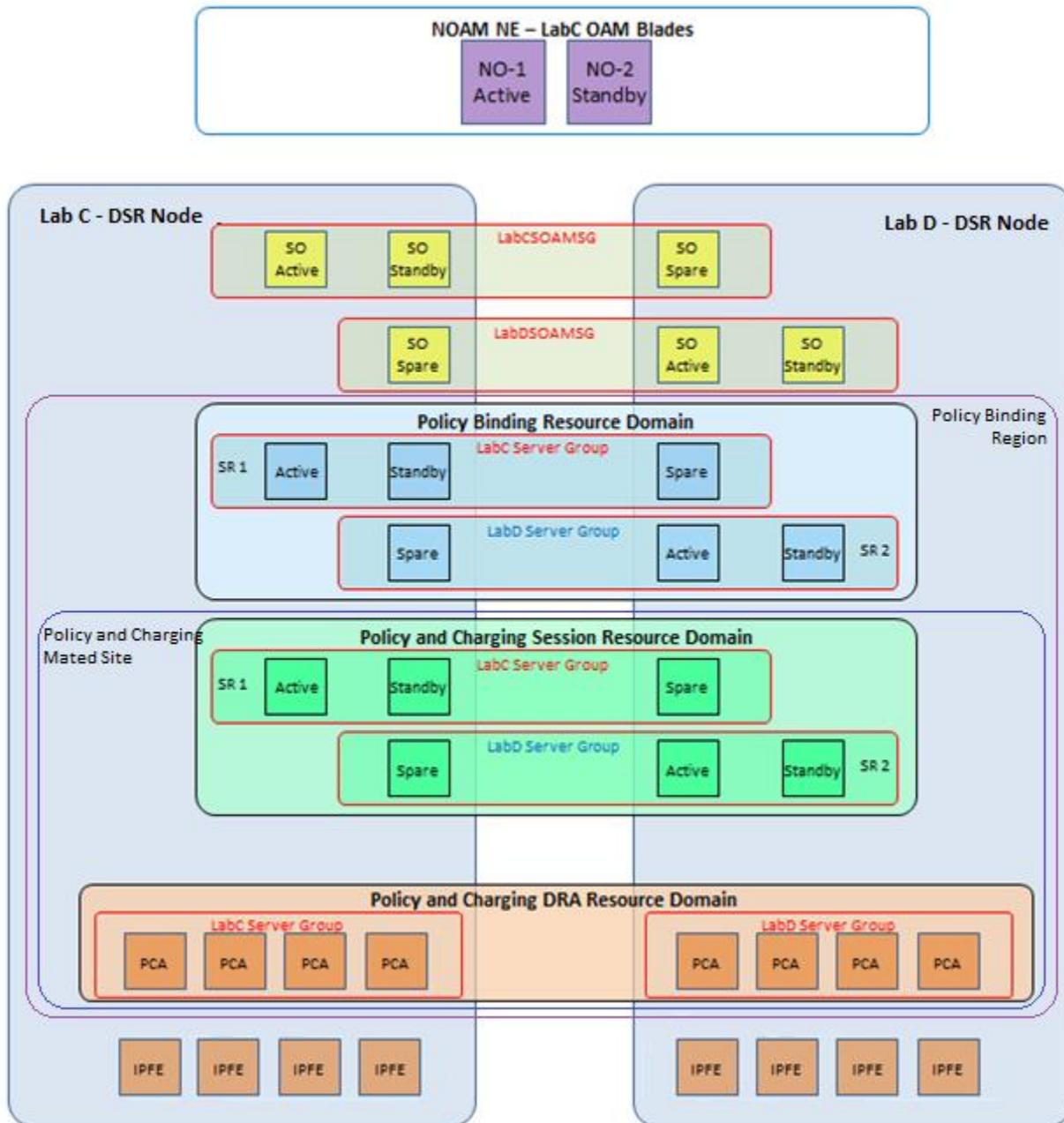


Figure 2: Example – Mated Pair PCA / Policy and Charging SBR Topology

Notes of Figure 2:

1. The standby SOAM and SBR servers shown in the diagram are optional and not needed if the user does not desire server-level redundancy.

2. The spare SOAM and SBR servers are not optional in a mated pair deployment.
3. The OAM servers can be virtualized. Please refer to [1] and [2] for installation procedures for virtualized OAM servers.
4. The IP Front End (IPFE) servers shown in the diagram are optional. Each DSR Node can have upto 4 IPFE Servers Groups (deployed as active-standby pairs) with one IPFE server in each Server Group. IPFE servers help in load distribution to DA-MP servers. Please refer to [3] for more information on IPFE servers.
5. Disaster Recovery NOAMs (DR-NOs) can be optionally setup to handle Disaster Recovery scenarios. Please refer to [2] for DR-NO installation procedures.
6. The Policy Binding Resource Domain can span across more than one mated site.
7. The Policy Binding Resource Domain can have upto 8 Server Groups.
8. Each Policy and Charging Session Resource Domain can have upto 8 Server Groups.

Procedure 3: Record Required Configuration Information

S T E P #	<p>This procedure gathers and records PCA Topology for the setup. This information must be gathered before configuring the PCA system.</p> <p>Please refer to the Policy Charging Application User's Guide^[4] for details of parameters required for configuration PCA Functions (Policy DRA, Online Charging DRA)</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>	
1 <input type="checkbox"/>	<p>Identify the Place and Place Association Information.</p>	<p>1. Identify and note the number of places and place names below – 2 in example, there might be upto 32 places.</p> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Number of Places:</p> <p>Place Names:</p> </div> <p>2. Identify the level of site redundancy to be deployed in the PCA system.</p> <p>a) In case site-redundancy is not required, the number of non-redundant PCA sites will be the same as the number of Places recorded above.</p> <p>b) In case a two-site redundancy model is chosen for some or all sites, Identify and note the number of PCA mated pairs – LabC and Lab D in example.</p> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Number of PCA Mated Pairs:</p> </div> <p>OR</p> <p>c) In case a three site redundancy model is chosen for some or all sites, Identify and note the number of PCA mated triplets</p> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Number of PCA Mated Triplets:</p> </div> <p>3. If Policy DRA function is being configured, then identify and note the places that are associated to the Place Association type – “Policy Binding Region”.</p> <p>Note: This step is required for Policy DRA functionality only.</p> <p>Policy Binding Region (Only 1 Binding Region since this is network wide) - LabC and Lab D are associated places (since these are the only 2 sites/places, there might be more depending on the number of sites/places).</p> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Number of Places in Binding Region:</p> </div> <p>4. Identify and note the places that are associated to the Place Association type “Policy and Charging Mated Sites”.</p> <p>NOTE: The Policy and Charging Mated Sites Place Association type is used for all levels of site redundancy chosen in item 2 above (no site redundancy, two-site redundancy, or 3-site redundancy). For example, if no site redundancy is chosen, you would configure a Policy and Charging Mated Sites Place Association for each Site Place (DSR node). If two-site redundancy is chosen and you have 3 pairs of DSR nodes, you would configure 3 Policy and Charging Mated Sites Place Associations - one for each pair.</p> <p>PCA Mated Sites – Identify and Log the site names for single sites, mated pairs or mated triplets</p>

		<p>PCA Mated Site 1: Lab C and Lab D</p> <p>PCA Mated Site 2:</p> <p>PCA Mated Site 3:</p> <p>PCA Mated Site 4:</p> <p>PCA Mated Site 5:</p> <p>PCA Mated Site 6:</p> <p>PCA Mated Site 7:</p> <p>Use additional space for recording more Mated Sites type Place Associations.</p>	
--	--	--	--

<p>2 <input type="checkbox"/></p>	<p>Identify and log the Resource Domain information.</p>	<p>1. Identify and log the number of 'Policy and Charging DRA' resource domains and their Server Groups – In this example it is 2 since there is only one mated pair. NOTE: Depending on the redundancy-model chosen there can be up to 3 Server Groups in one Policy and Charging DRA Resource Domain.</p> <div data-bbox="553 338 1052 705" style="border: 1px solid black; padding: 5px;"> <p>DRA RD1 - LabCDRASG DRA RD2 - LabDDRASG DRA RD3 - DRA RD4 - DRA RD5 - DRA RD6 - DRA RD7 - Use additional space for recording more Resource Domains.</p> </div> <p>2. Identify and log the 'Policy Binding' resource domain and its Server Groups. Note 1: This step is required for Policy DRA functionality only. Note 2: Depending on the capacity chosen there can be up to 8 Server Groups in one Policy Binding Resource Domain.</p> <div data-bbox="553 888 1052 951" style="border: 1px solid black; padding: 5px;"> <p>Policy Binding RD1 – LabCBindingSR1SG</p> </div> <p>3. Identify and log the number of 'Policy Session' resource domains and their Server Groups. Note: Depending on the capacity chosen there can be up to 8 Server Groups in one Policy Session Resource Domain.</p> <div data-bbox="553 1157 1052 1482" style="border: 1px solid black; padding: 5px;"> <p>Policy Session RD1 – LabCSessionSR1SG Policy Session RD2 – LabDSessionSR2SG Policy Session RD3 – LabCSessionSR3SG Policy Session RD4 – LabDSessionSR4SG Policy Session RD5 - Policy Session RD6 - Policy Session RD7 - Use additional space for recording more Resource Domains.</p> </div>
---------------------------------------	--	--

3.5 DIAMETER NETWORK CHECK

3.5.1 Diameter Network Check for Policy DRA

**NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION
 SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY**

Please refer to Section 2.1 for the information required to be logged.

Procedure 4: Record Required P-DRA Diameter Configuration

<p>S T E P #</p>	<p>This procedure gathers and records PCA – Policy DRA function Diameter Configuration.</p> <p>Please refer to the Diameter User’s Guide^[7] for details of parameters required for configuring Diameter</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>	
<p>1 <input type="checkbox"/></p>	<p>Identify the diameter network and properties.</p>	<ol style="list-style-type: none"> 1. Identify and log the hardware profile type for each of the DA-MP Servers (PCA) 2. Identify and log the number of policy clients (PCEFs, BBERFs and AFs) and policy servers (PCRFs) in the network. 3. Identify and log the diameter attributes for all the policy clients and policy servers in the network – FQDN, Realm, IP address. 4. Identify and log the type of diameter Transport Protocol needed for all the policy clients and policy Servers - TCP/SCTP 5. Identify and log the type of diameter connection mode needed for all the policy clients and policy server- Responder/Initiator/Responder-Initiator 6. Identify and log the 'Peer Node Identification' for all the policy clients and policy servers- IP Address/FQDN. 7. Identify and log the route groups and route lists needed for Policy Servers and Policy Clients. Routing configuration is required for Policy Clients if the Policy Servers send Diameter request messages to be routed to the Policy Clients. 8. Identify and log the Policy Server configuration needed – Both Gx and Rx on same Policy Server or are they on different servers. 9. Identify and log the number of peer route tables needed for the diameter configuration – e.g. one for Rx Policy Servers and One for Gx Policy Servers . 10. Identify and log the number of Application Route Table entries – one for Gx Application and one for Rx Application message processing. 11. Identify and log the TSA used for local nodes if IPFE is used.
<p>2 <input type="checkbox"/></p>	<p>Policy DRA Network configuration (NO scoped)</p>	<ol style="list-style-type: none"> 1. Identify and log the SBR Databases of Session and Binding types to be configured. 2. Identify and log the Access Point Names used and the “Stale Session Timeout” for the same. 3. Identify and log the PCRF Pools and the Sub-Pool Selection Rules. Note that PCRF Sub Pool Selection Rules are optional. 4. Identify and log the General Options parameters for the Policy DRA network – <ul style="list-style-type: none"> Default Stale Session Timeout Binding Audit Session Query Rate Audit Operation Rate 5. Identify and log the Network Wide Options parameters for the Policy DRA network – <ul style="list-style-type: none"> Early Binding Options Topology Hiding Options Suspect Binding Removal Options Session Integrity Options 6. Identify and log the Alarm Settings for “DSR Application ingress Message Rate”. 7. Identify and log the Congestion Alarm Thresholds and Message Throttling Rules
<p>3 <input type="checkbox"/></p>	<p>Policy DRA Site Configuration (SO scoped)</p>	<ol style="list-style-type: none"> 1. Identify and log the all the PCRFs handling the Policy Traffic for this site. 2. Identify and log the Binding Key Priority settings, i.e. the order in which subscriber keys (IMSI, MSISDN, IPv4, IPv6) will be used to correlate binding dependent session creation

		<p>messages and route them to final bound PCRFs.</p> <ol style="list-style-type: none"> 3. Identify and log the Policy Clients for which the topology hiding is needed. 4. Identify and log the PCRF Pool to PRT mapping configuration. 5. Identify and log the error code configuration for each of the 'Error Condition' in the table per the policy client team request/ inteoperability requirements for Policy Client Vendor. 6. Identify and log the Suspect Binding Removal Rules. 7. Identify and log the Site Options parameters.for this site.
--	--	---

3.5.2 Diameter Network Check for Online Charging DRA

NOTE: EXECUTE THIS PROCEDURE FOR ONLINE CHARGING DRA FUNCTION

SKIP THIS PROCEDURE IF POLICY DRA FUNCTION ONLY

Procedure 5: Record Required OC-DRA Diameter Configuration

S T E P #	<p>This procedure gathers and records PCA – Online Charging DRA function Diameter Configuration.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>	
1 <input type="checkbox"/>	Identify the diameter network and properties.	<ol style="list-style-type: none"> 1. Identify and log the hardware profile type for each of the DA-MP Servers (PCA) 2. Identify and log the number of Online Charging clients (CTFs) and Online Charging servers (OCSs) in the network. 3. Identify and log the diameter attributes for all the Online Charging clients and Online Charging servers in the network – FQDN, Realm, IP address. 4. Identify and log the type of diameter Transport Protocol needed for all the Online Charging clients and Online Charging servers - TCP/SCTP 5. Identify and log the type of diameter connection mode needed for all the Online Charging clients and Online Charging servers - Responder/Initiator/Responder-Initiator 6. Identify and log the 'Peer Node Identification' for all the Online Charging clients and Online Charging servers - IP Address/FQDN. 7. Identify and log the route groups and route lists needed for Online charging Servers. 8. Identify and log the number of peer route tables and peer route rules needed for the diameter configuration for Online charging Servers . 9. Identify and log the number of Application Route Table entries –for RBAR (regionalized routing configuration) and for PCA message processing. 10. Identify and log the TSA used for local nodes if IPFE is used.
2 <input type="checkbox"/>	Online Charging DRA Network configuration (NO scoped)	<ol style="list-style-type: none"> 1. Identify and log the SBR Database of Session type to be configured.NOTE: Skip this step if Session type SBR Database was added during Policy DRA Function configuration in 3.5.1 2. Identify and log the Access Point Names used and the “Stale Session Timeout” for the same. (Optional) 3. Identify and log the General Options parameters for the Online Charging DRA network – <ul style="list-style-type: none"> Default Stale Session Timeout Audit Operation Rate 4. Identify and log the Online Charging Network Realms to be configured for Session State maintenance. 5. Identify and log the Network Wide Options for the Online Charging DRA network – <ul style="list-style-type: none"> Session State Options OCS Selection Options 6. Identify and log the Alarm Settings for “DSR Application ingress Message Rate”. 7. Identify and log the Congestion Alarm Thresholds and Message Throttling Rules
3 <input type="checkbox"/>	Online Charging DRA Site Configuration (SO scoped)	<ol style="list-style-type: none"> 1. Identify and log the all the OCSs handling the Gy/Ro Traffic for this site. 2. Identify and log the all the CTFs to be configured for Session State maintenance. 3. Identify and Log the error code configuration for each of the 'Error Condition' in the table for the Gy/Ro interface.

3.6 PERFORM HEALTH CHECK

This procedure is part of PCA configuration preparation and is used to determine the health and status of the DSR 7.0 network and servers. This may be executed multiple times but must also be executed at least once within the time frame of 24-36 hours prior to the start of the maintenance window in which the PCA configuration will take place.

Procedure 6: Perform Health Check (PCA configuration Preparation)

S T E P #	This procedure performs a Health Check. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
	1	Verify Server status <input type="checkbox"/>
	Verify Server status: 1. Select Status & Manage > Server ; the Server Status screen is shown. 2. Verify all Server Status is Normal (Norm) for Application Status (Appl State), Alarms (Alm), Database (DB), Collection (Reporting Status), and Processes (Proc). 3. Do not proceed to PCA configuration if any of the following statuses is not Norm: DB, Reporting Status, Proc . If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the PCA configuration. Contact Engineering for assistance as necessary. 4. If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the PCA configuration. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the PCA configuration. The activation may be able to proceed in the presence of certain Major or Critical alarms. Contact Oracle Support for assistance as necessary.	
2	Log all current alarms <input type="checkbox"/>	Log all current alarms in the system: 1. Select Alarms & Events > View Active ; the Alarms & Events > View Active view is shown. 2. Click Report button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference. Note: the system should be alarm free unless the user is aware of the alarms and understands the impact. 4. Select Alarms & Events > View History and repeat steps 2 and 3.

4.0 PCA CONFIGURATION

Before PCA configuration, execute the site survey and the system health check specified in Section 3.0. This ensures that all the data is ready for PCA configuration. Performing the system health check determines which alarms are present in the system and if PCA configuration can proceed with alarms.

*** WARNING ***

If there are servers in the system which are not in Normal state, these servers should be brought to the Normal or the Application Disabled state before the PCA configuration process is started.

If alarms are present on the server, contact PCA Development to diagnose those alarms and determine whether they need to be addressed or if it is safe to proceed with the PCA configuration.

Please read the following notes on PCA configuration procedures:

- Command steps that require user entry are indicated with **white-on-black step numbers**.
- The shaded area within response steps must be verified in order to successfully complete that step.
- Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:
 - Session banner information such as *time* and *date*.
 - System-specific configuration information such as *hardware locations*, *IP addresses*, *Node names* and *hostnames*.
 - ANY information marked with “XXXX” or “YYYY” where appropriate, instructions are provided to determine what output should be expected in place of “XXXX or YYYY”
 - Aesthetic differences unrelated to functionality such as *browser attributes: window size, colors, and toolbars* and *button layouts*.
- After completing each step and at each point where data is recorded from the screen, the technician performing the PCA configuration must initial each step. A check box should be provided. For procedures which are executed multiple times, the check box can be skipped, but the technician must initial each iteration the step is executed. The space on either side of the step number can be used (margin on left side or column on right side).
- Captured data is required for future support reference.

NOTE: Refer to the data captured in Section 3.4 and Section 3.5 before proceeding with the configuration in below sections.

The maintenance operations performed in Section 4.9 should be performed in a maintenance window. Configuration of Policy and Charging Application can be done outside of the maintenance window.

4.1 PLACE ASSOCIATIONS CONFIGURATION

If all the required place associations are not already configured, then follow the procedures defined in this section, else skip this section.

The following type of Place Association is required for both functions (Policy DRA and Online Charging DRA) of PCA:

- Policy and Charging Mated Sites

The following type of Place Association is required for Policy DRA function ONLY:

- Policy Binding Region

4.1.1 Policy and Charging Places

NOTE: EXECUTE THIS PROCEDURE ONLY IF NEW MP SERVERS ARE TO BE CONFIGURED IN THE TOPOLOGY OTHER THAN THOSE CONFIGURED DURING INSTALLATION PROCEDURE FROM [1]

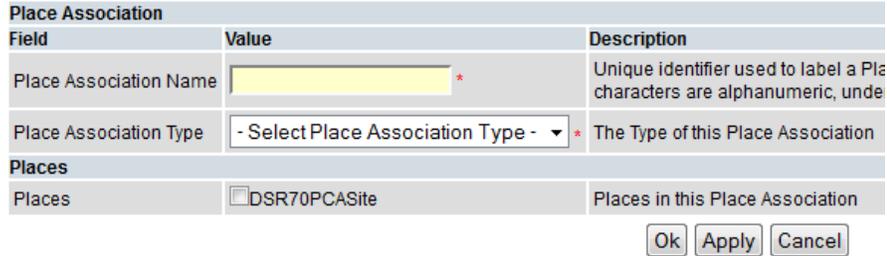
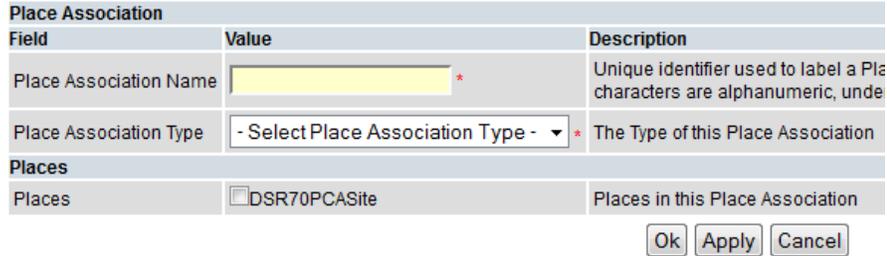
Procedure 7: Policy and Charging Places configuration

S T E P #	This procedure configures the Places.																						
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.																						
	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .																						
1	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".																					
2	NOAM VIP: Navigate to Places screen	Navigate to Main Menu -> Configuration -> Places Screen.																					
3	NOAM VIP: Add a new Place	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>  <p>Main Menu: Configuration -> Places [Insert]</p> <p>Info [v] Tue Nov 25 15:41:45</p> <p>Inserting a new Place</p> <table border="1"> <thead> <tr> <th>Place Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Place Name</td> <td>PlaceName</td> <td>Unique identifier used to label a Place. [Default = n/a. Range = A 1-32-character string. Valid characters are alphanumeric, underscore, dash, and space.]</td> </tr> <tr> <td>Parent</td> <td>NONE</td> <td>The Parent of this Place</td> </tr> <tr> <td>Place Type</td> <td>Site</td> <td>The Type of this Place</td> </tr> <tr> <td colspan="3">Servers</td> </tr> <tr> <td>GTXA_1111101_NO</td> <td><input type="checkbox"/> GTXA-NO1 <input type="checkbox"/> GTXA-NO2</td> <td>Available servers in GTXA_1111101_NO</td> </tr> <tr> <td>GTXA_1111101_SO</td> <td></td> <td>No servers available</td> </tr> </tbody> </table> <p style="text-align: right;">Ok Apply Cancel</p> <p>1. Enter the Place Name 2. Select "None" as the Parent 3. Select "Site" as the Place Type 4. Select all DAMP servers (running PCA) and all SBR servers that belong to this Place (DSR Site). 5. Click Ok.</p>	Place Field	Value	Description	Place Name	PlaceName	Unique identifier used to label a Place. [Default = n/a. Range = A 1-32-character string. Valid characters are alphanumeric, underscore, dash, and space.]	Parent	NONE	The Parent of this Place	Place Type	Site	The Type of this Place	Servers			GTXA_1111101_NO	<input type="checkbox"/> GTXA-NO1 <input type="checkbox"/> GTXA-NO2	Available servers in GTXA_1111101_NO	GTXA_1111101_SO		No servers available
Place Field	Value	Description																					
Place Name	PlaceName	Unique identifier used to label a Place. [Default = n/a. Range = A 1-32-character string. Valid characters are alphanumeric, underscore, dash, and space.]																					
Parent	NONE	The Parent of this Place																					
Place Type	Site	The Type of this Place																					
Servers																							
GTXA_1111101_NO	<input type="checkbox"/> GTXA-NO1 <input type="checkbox"/> GTXA-NO2	Available servers in GTXA_1111101_NO																					
GTXA_1111101_SO		No servers available																					
4	NOAM VIP: Add other Places.	Repeat Step 4 for all other Places that are to be added.																					



4.1.2 Policy and Charging Mated Sites Place Associations

Procedure 8: Policy and Charging Mated Sites Place Associations configuration

S T E P #	This procedure configures Place Association Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> . ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.	
	1	Establish GUI Session on the NOAM VIP <input type="checkbox"/>
	2	NOAM VIP: Navigate to Place Associations screen <input type="checkbox"/>
	3	NOAM VIP: Add Policy and Charging Mated Sites Place Association <input type="checkbox"/>
	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
	Navigate to Main Menu -> Configuration -> Place Associations Screen.	Navigate to Main Menu -> Configuration -> Place Associations Screen.
	Click on Insert in the lower left corner. You will see a screen similar to: Main Menu: Configuration -> Place Associations [Insert] 	Click on Insert in the lower left corner. You will see a screen similar to: Main Menu: Configuration -> Place Associations [Insert] 
	1. Enter the Place Association Name 2. Select "Policy and Charging Mated Sites" as the Place Association Type 3. Select the Places to associate with the Place Association. Please use the data recorded in Section 3.4. 4. Click Ok .	
4	NOAM VIP: Add other Policy and Charging Mated Sites Place Associations. <input type="checkbox"/>	Repeat Step 3 for all other Policy and Charging Mated Sites Place Associations that are to be added

4.1.3 Policy Binding Region Place Associations

NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION

SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY

Procedure 9: Policy Binding Region Place Associations configuration

S T E P #	<p>This procedure configures the Policy Binding Region Place Associations</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p> <p>ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.</p>																			
1 <input type="checkbox"/>	<p>Establish GUI Session on the NOAM VIP</p>	<p>Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".</p>																		
2 <input type="checkbox"/>	<p>NOAM VIP: Navigate to Place Associations screen</p>	<p>Navigate to Main Menu -> Configuration -> Place Associations Screen.</p>																		
3 <input type="checkbox"/>	<p>NOAM VIP: Add Policy Binding Region Place Association</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p style="text-align: center;">Main Menu: Configuration -> Place Associations [Insert]</p> <hr/> <p style="text-align: center;">Inserting a new Place Association</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e0e0e0;"> <th colspan="3">Place Association</th> </tr> <tr> <th style="width: 30%;">Field</th> <th style="width: 40%;">Value</th> <th style="width: 30%;">Description</th> </tr> </thead> <tbody> <tr> <td>Place Association Name</td> <td><input style="background-color: yellow;" type="text" value=""/> *</td> <td>Unique identifier used to label a Pla characters are alphanumeric, unde</td> </tr> <tr> <td>Place Association Type</td> <td>- Select Place Association Type - * <input type="button" value="v"/></td> <td>The Type of this Place Association</td> </tr> <tr style="background-color: #e0e0e0;"> <th colspan="3">Places</th> </tr> <tr> <td>Places</td> <td><input type="checkbox"/> DSR70PCASite</td> <td>Places in this Place Association</td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></p> <p>1. Enter the Place Association Name 2. Select "Policy Binding Region" as the Place Association Type 3. Select all the Places to associate with the Place Association. Select all the sites (Places) in the network.. 4. Click Ok.</p>	Place Association			Field	Value	Description	Place Association Name	<input style="background-color: yellow;" type="text" value=""/> *	Unique identifier used to label a Pla characters are alphanumeric, unde	Place Association Type	- Select Place Association Type - * <input type="button" value="v"/>	The Type of this Place Association	Places			Places	<input type="checkbox"/> DSR70PCASite	Places in this Place Association
Place Association																				
Field	Value	Description																		
Place Association Name	<input style="background-color: yellow;" type="text" value=""/> *	Unique identifier used to label a Pla characters are alphanumeric, unde																		
Place Association Type	- Select Place Association Type - * <input type="button" value="v"/>	The Type of this Place Association																		
Places																				
Places	<input type="checkbox"/> DSR70PCASite	Places in this Place Association																		

4.2 RESOURCE DOMAINS CONFIGURATION

If all the required resource domains are not already configured, then follow the procedures defined in this section, else skip this section.

The following Resource Domains are required for both functions (Policy DRA and Online Charging DRA) of PCA:

- Policy and Charging DRA
- Policy Session

The following Resource Domain is required for Policy DRA function ONLY:

- Policy Binding

4.2.1 Policy and Charging DRA Resource Domain Configuration

Procedure 10: Policy and Charging DRA Resource Domain configuration

S T E P #	<p>This procedure configures the Policy and Charging Resource Domain</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p> <p>ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.</p>																		
	1	<p>Establish GUI Session on the NOAM VIP</p> <p>Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".</p>																	
	2	<p>NOAM VIP: Navigate to Resource Domain Screen</p> <p>Navigate to Main Menu -> Configuration -> Resource Domains Screen.</p>																	
	3	<p>NOAM VIP: Add Policy and Charging DRA Resource Domain</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p style="text-align: center;">Main Menu: Configuration -> Resource Domains [Insert]</p> <hr/> <p style="text-align: center;">Inserting a new Resource Domain</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3">Resource Domain</th> </tr> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Resource Domain Name</td> <td><input style="width: 100%;" type="text" value=""/></td> <td>Unique identifier used to label a Resource Domain. Characters are alphanumeric and unique.</td> </tr> <tr> <td>Resource Domain Profile</td> <td>- Select Resource Domain Profile -</td> <td>The Profile of this Resource Domain</td> </tr> <tr> <th colspan="3">Server Groups</th> </tr> <tr> <td>Server Groups</td> <td> <input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG </td> <td>Server Groups associated with this Resource Domain</td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> <p>1. Enter the Resource Domain Name 2. Select "Policy and Charging DRA" as the Resource Domain Profile 3. Select the Server Groups to associate with the Resource Domain 4. Click Ok.</p> <p>NOTE: For Mated DSR sites, create one Policy and Charging DRA Resource Domain and add the</p>	Resource Domain			Field	Value	Description	Resource Domain Name	<input style="width: 100%;" type="text" value=""/>	Unique identifier used to label a Resource Domain. Characters are alphanumeric and unique.	Resource Domain Profile	- Select Resource Domain Profile -	The Profile of this Resource Domain	Server Groups			Server Groups	<input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG
Resource Domain																			
Field	Value	Description																	
Resource Domain Name	<input style="width: 100%;" type="text" value=""/>	Unique identifier used to label a Resource Domain. Characters are alphanumeric and unique.																	
Resource Domain Profile	- Select Resource Domain Profile -	The Profile of this Resource Domain																	
Server Groups																			
Server Groups	<input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG	Server Groups associated with this Resource Domain																	

		<p>DA-MP Server Groups from both sites into this Policy and Charging DRA Resource Domain. For Mated DSR Triplets, create one Policy and Charging DRA Resource Domain and add the DA-MP Server Groups from three sites into this Policy and Charging DRA Resource Domain. For non-mated pair DSRs and standalone DSR: Configure a Policy and Charging DRA Resource Domain per Site.</p>
4	<p>NOAM VIP: Add other Policy and Charging DRA Resource Domains.</p>	<p>Repeat Step 3 for all other Policy and Charging DRA Resource Domains that are to be added.</p>
5	<p>NOAM VIP: Restart the Servers</p>	<p>Navigate to Main Menu -> Status & Manage -> Server screen. Select the Servers just added to the Resource Domain and click 'Restart' button.</p>

4.2.2 Policy Session Resource Domain Configuration

Procedure 11: Policy Session Resource Domain configuration

<p>S T E P #</p>	<p>This procedure configures the Policy Session Resource Domain</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC. ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.</p>																		
	1	<p>Establish GUI Session on the NOAM VIP</p> <p>Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".</p>																	
	2	<p>NOAM VIP: Navigate to Resource Domain Screen</p> <p>Navigate to Main Menu -> Configuration -> Resource Domains Screen.</p>																	
3	<p>NOAM VIP: Add Session Resource Domain</p> <p>Click on Insert in the lower left corner. You will see a screen similar to:</p> <p style="text-align: center;">Main Menu: Configuration -> Resource Domains [Insert]</p> <hr/> <p style="text-align: center;">Inserting a new Resource Domain</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3">Resource Domain</th> </tr> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Resource Domain Name</td> <td><input style="width: 100%;" type="text" value=""/></td> <td>Unique identifier used to label a Res characters are alphanumeric and un</td> </tr> <tr> <td>Resource Domain Profile</td> <td><input type="text" value="- Select Resource Domain Profile -"/></td> <td>The Profile of this Resource Domain</td> </tr> <tr> <th colspan="3">Server Groups</th> </tr> <tr> <td>Server Groups</td> <td> <input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG </td> <td>Server Groups associated with this R</td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> <p>1. Enter the Resource Domain Name 2. Select "Policy Session" as the Resource Domain Profile 3. Select the Server Groups to associate with the Resource Domain 4. Click Ok.</p> <p>NOTE:</p>	Resource Domain			Field	Value	Description	Resource Domain Name	<input style="width: 100%;" type="text" value=""/>	Unique identifier used to label a Res characters are alphanumeric and un	Resource Domain Profile	<input type="text" value="- Select Resource Domain Profile -"/>	The Profile of this Resource Domain	Server Groups			Server Groups	<input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG	Server Groups associated with this R
Resource Domain																			
Field	Value	Description																	
Resource Domain Name	<input style="width: 100%;" type="text" value=""/>	Unique identifier used to label a Res characters are alphanumeric and un																	
Resource Domain Profile	<input type="text" value="- Select Resource Domain Profile -"/>	The Profile of this Resource Domain																	
Server Groups																			
Server Groups	<input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG	Server Groups associated with this R																	

		<p>For Mated DSR sites, create one Policy Session Resource Domain and add all the Policy and Charging SBR Server Groups from both sites that will be hosting the Session SBR Database for the Mated Pair into this Policy Session Resource Domain. For Mated DSR triplets, create one Policy Session Resource Domain and add all the Policy and Charging SBR Server Groups from three sites that will be hosting the Session SBR Database for the Mated triplet into this Policy Session Resource Domain. For non-mated pair DSRs and standalone DSR: Configure a Policy Session Resource Domain per site and add all the Policy and Charging SBR Server Groups in the site that will be hosting the Session SBR Database.</p>
4	<p>NOAM VIP: Add other Session Resource Domains.</p>	<p>Repeat Step 3 for all other Policy Session Resource Domains that are to be added.</p>

4.2.3 Policy Binding Resource Domain Configuration

The Policy Binding Resource Domain is only required for Policy DRA function of PCA. Skip this section if not configuring the Policy DRA function.

Procedure 12: Policy Binding Resource Domain configuration

<p>S T E P #</p>	<p>This procedure configures the Policy Binding Resource Domain</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC. ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.</p>																		
	1	<p>Establish GUI Session on the NOAM VIP</p> <p>Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".</p>																	
	2	<p>NOAM VIP: Navigate to Resource Domain Screen</p> <p>Navigate to Main Menu -> Configuration -> Resource Domains Screen.</p>																	
	3	<p>NOAM VIP: Add Policy and Charging DRA Resource Domain</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Configuration -> Resource Domains [Insert]</p> <hr/> <p>Inserting a new Resource Domain</p> <table border="1" data-bbox="521 1409 1406 1711"> <thead> <tr> <th colspan="3">Resource Domain</th> </tr> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Resource Domain Name</td> <td><input type="text"/></td> <td>Unique identifier used to label a Res characters are alphanumeric and un</td> </tr> <tr> <td>Resource Domain Profile</td> <td>- Select Resource Domain Profile -</td> <td>The Profile of this Resource Domain</td> </tr> <tr> <th colspan="3">Server Groups</th> </tr> <tr> <td>Server Groups</td> <td> <input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG </td> <td>Server Groups associated with this R</td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> <p>1. Enter the Resource Domain Name 2. Select "Policy Binding" as the Resource Domain Profile 3. Select the Server Groups to associate with the Resource Domain 4. Click Ok.</p>	Resource Domain			Field	Value	Description	Resource Domain Name	<input type="text"/>	Unique identifier used to label a Res characters are alphanumeric and un	Resource Domain Profile	- Select Resource Domain Profile -	The Profile of this Resource Domain	Server Groups			Server Groups	<input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG
Resource Domain																			
Field	Value	Description																	
Resource Domain Name	<input type="text"/>	Unique identifier used to label a Res characters are alphanumeric and un																	
Resource Domain Profile	- Select Resource Domain Profile -	The Profile of this Resource Domain																	
Server Groups																			
Server Groups	<input type="checkbox"/> C_BIND <input type="checkbox"/> C_MP <input type="checkbox"/> C_SESS <input type="checkbox"/> NOAM_SG <input type="checkbox"/> SOAM_SG	Server Groups associated with this R																	

	<p>NOTE: Create only one Policy Binding Resource Domain and add all the Policy and Charging SBR Server Groups from all sites that will be hosting the Binding SBR Database into this Policy Binding Resource Domain.</p>
--	--

4.3 DIAMETER CONFIGURATION PROCEDURES

4.3.1 Diameter Configuration for Policy DRA

Detailed steps are given in the procedures below. The procedures in this section mention the parts of Diameter configuration that are needed by Policy and Charging Application with some example sets of configuration. For extensive information on the fields and screens or for planning your Diameter configuration please refer to the Diameter User's Guide [7]

Procedure 13: Diameter configuration for Policy DRA

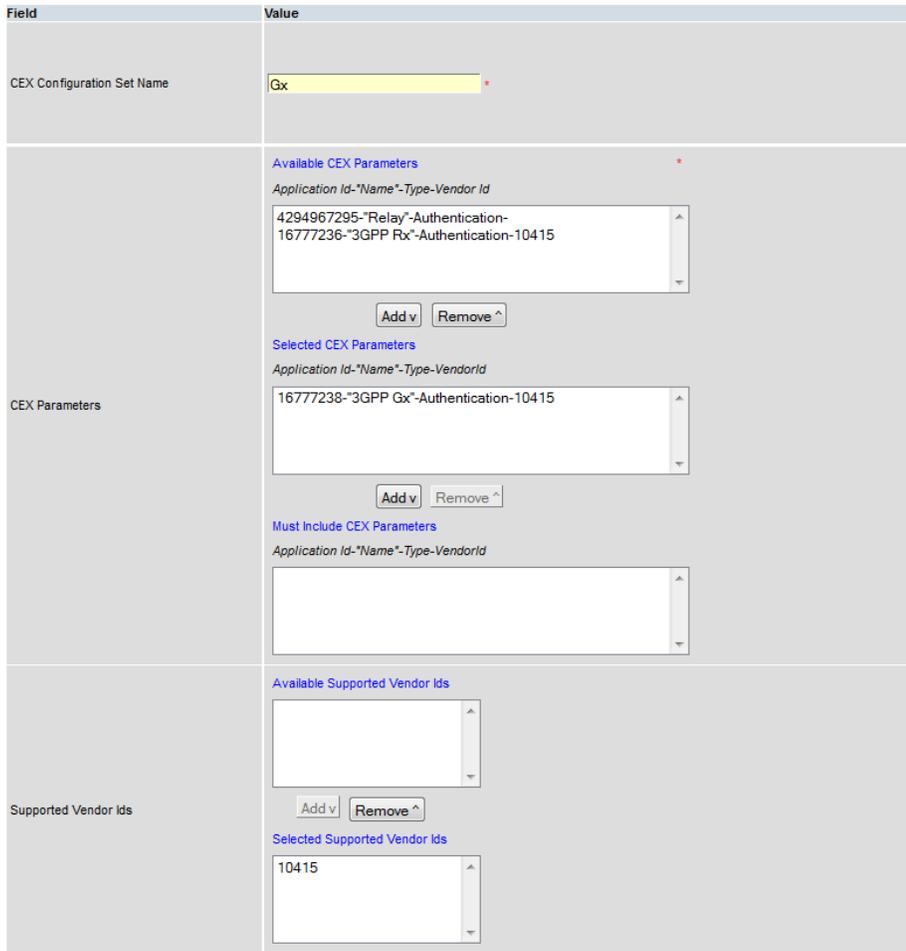
NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION

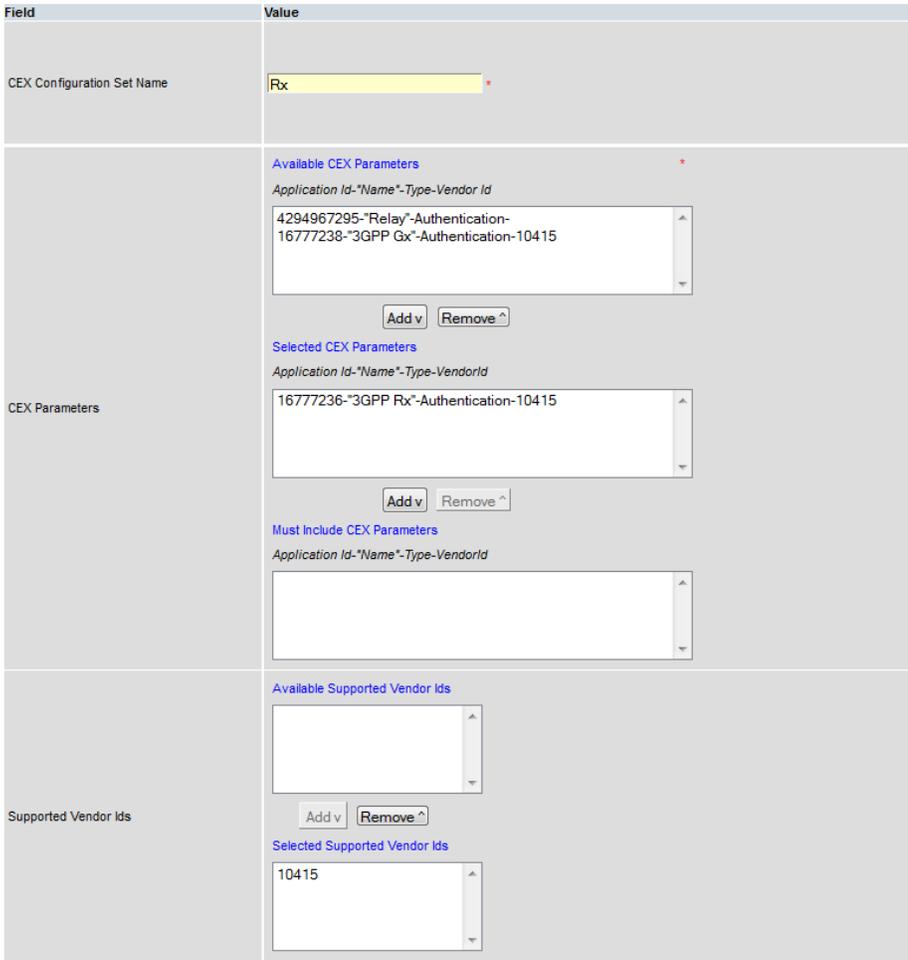
SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY

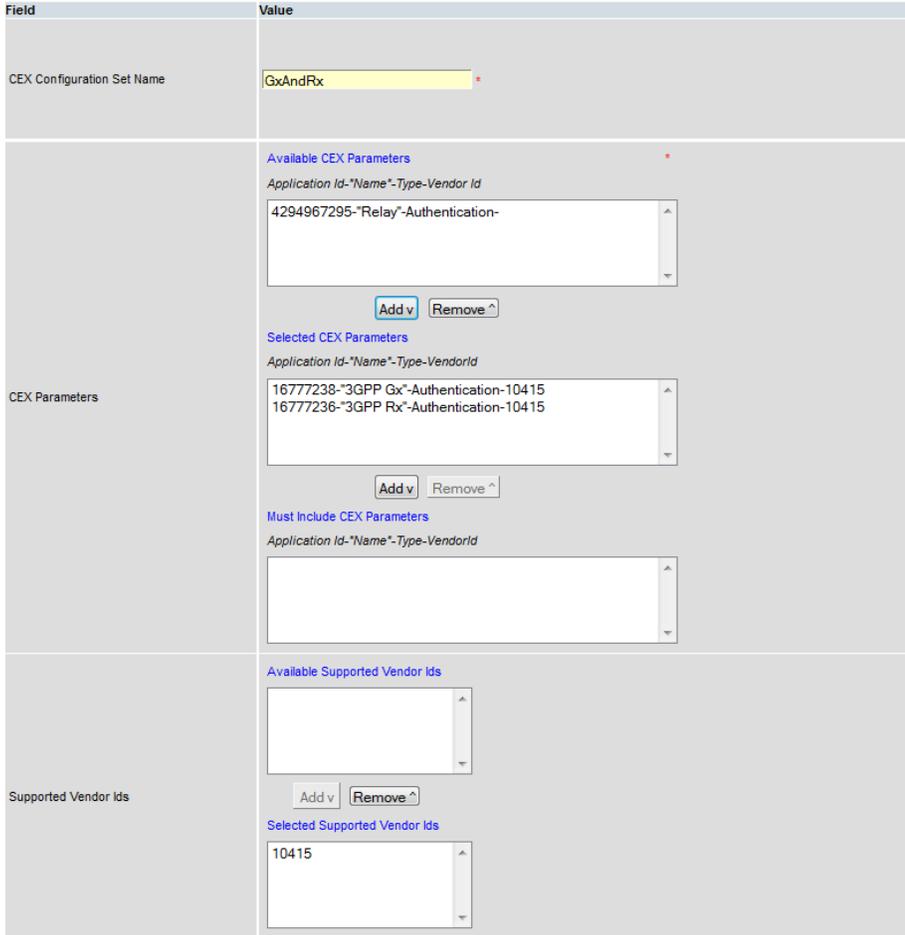
S T E P #	This procedure configures the Diameter stack. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .																					
	1	Establish GUI Session on the SOAM VIP Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".																				
	2	SOAM VIP: Navigate to Application Id Configuration Screen Navigate to Main Menu -> Diameter -> Configuration -> Application Ids																				
	3	SOAM VIP: Add Application Id for Gx Interface Click on Insert in the lower left corner. You will see a screen similar to: <p style="text-align: center;">Main Menu: Diameter -> Configuration -> Application Ids -> [Insert]</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Field</th> <th style="text-align: left;">Value</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><input style="width: 100%;" type="text" value=""/></td> <td>Application Id Name</td> </tr> <tr> <td>Application Id Value</td> <td> <input checked="" type="radio"/> - Select - <input type="radio"/> <input style="width: 100%;" type="text" value=""/> </td> <td>Application Id is used to ic [Default = n/a; Range = 1 - 16777216 - 4294967294]</td> </tr> <tr> <td>Application Route Table</td> <td>Default ▾</td> <td>Application Route Table as Used for routing Request when the downstream Pe</td> </tr> <tr> <td>Peer Route Table</td> <td>Default ▾</td> <td>Peer Route Table associa Used for routing Request Peer Node does not have</td> </tr> <tr> <td>Routing Option Set</td> <td>Default ▾</td> <td>Routing Option Set assoc Used when processing tr Peer Node does not have</td> </tr> <tr> <td>Pending Answer Timer</td> <td>Default ▾</td> <td>Pending Answer Timer as Used when processing tr Peer Node does not have</td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> <p>1. Select Application Id for Gx Interface "16777238 - 3GPP Gx" (This will automatically fill in the "Name" field, please make changes to the name as necessary). 2. Click Ok.</p> <p>NOTE: This Application-Id is also used for Gx-Prime interface.</p>	Field	Value	Description	Name	<input style="width: 100%;" type="text" value=""/>	Application Id Name	Application Id Value	<input checked="" type="radio"/> - Select - <input type="radio"/> <input style="width: 100%;" type="text" value=""/>	Application Id is used to ic [Default = n/a; Range = 1 - 16777216 - 4294967294]	Application Route Table	Default ▾	Application Route Table as Used for routing Request when the downstream Pe	Peer Route Table	Default ▾	Peer Route Table associa Used for routing Request Peer Node does not have	Routing Option Set	Default ▾	Routing Option Set assoc Used when processing tr Peer Node does not have	Pending Answer Timer	Default ▾
Field	Value	Description																				
Name	<input style="width: 100%;" type="text" value=""/>	Application Id Name																				
Application Id Value	<input checked="" type="radio"/> - Select - <input type="radio"/> <input style="width: 100%;" type="text" value=""/>	Application Id is used to ic [Default = n/a; Range = 1 - 16777216 - 4294967294]																				
Application Route Table	Default ▾	Application Route Table as Used for routing Request when the downstream Pe																				
Peer Route Table	Default ▾	Peer Route Table associa Used for routing Request Peer Node does not have																				
Routing Option Set	Default ▾	Routing Option Set assoc Used when processing tr Peer Node does not have																				
Pending Answer Timer	Default ▾	Pending Answer Timer as Used when processing tr Peer Node does not have																				

<p>4</p>	<p>SOAM VIP: Add Application Id for Rx Interface</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Diameter -> Configuration -> Application Ids -> [Insert]</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td><input type="text" value=""/></td> <td>Application Id Name</td> </tr> <tr> <td>Application Id Value</td> <td> <input checked="" type="radio"/> - Select - <input type="radio"/> <input type="text" value=""/> </td> <td>Application Id is used to ic [Default = n/a; Range = 1 - 16777216 - 4294967294]</td> </tr> <tr> <td>Application Route Table</td> <td>Default</td> <td>Application Route Table as Used for routing Requests when the downstream Pe</td> </tr> <tr> <td>Peer Route Table</td> <td>Default</td> <td>Peer Route Table associa Used for routing Requests Peer Node does not have</td> </tr> <tr> <td>Routing Option Set</td> <td>Default</td> <td>Routing Option Set assoc Used when processing tr; Peer Node does not have</td> </tr> <tr> <td>Pending Answer Timer</td> <td>Default</td> <td>Pending Answer Timer as Used when processing tr; Peer Node does not have</td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> <p>1. Select Application Id for Rx Interface "16777236 - 3GPP Rx" 2. Click Ok.</p>	Field	Value	Description	Name	<input type="text" value=""/>	Application Id Name	Application Id Value	<input checked="" type="radio"/> - Select - <input type="radio"/> <input type="text" value=""/>	Application Id is used to ic [Default = n/a; Range = 1 - 16777216 - 4294967294]	Application Route Table	Default	Application Route Table as Used for routing Requests when the downstream Pe	Peer Route Table	Default	Peer Route Table associa Used for routing Requests Peer Node does not have	Routing Option Set	Default	Routing Option Set assoc Used when processing tr; Peer Node does not have	Pending Answer Timer	Default	Pending Answer Timer as Used when processing tr; Peer Node does not have			
Field	Value	Description																								
Name	<input type="text" value=""/>	Application Id Name																								
Application Id Value	<input checked="" type="radio"/> - Select - <input type="radio"/> <input type="text" value=""/>	Application Id is used to ic [Default = n/a; Range = 1 - 16777216 - 4294967294]																								
Application Route Table	Default	Application Route Table as Used for routing Requests when the downstream Pe																								
Peer Route Table	Default	Peer Route Table associa Used for routing Requests Peer Node does not have																								
Routing Option Set	Default	Routing Option Set assoc Used when processing tr; Peer Node does not have																								
Pending Answer Timer	Default	Pending Answer Timer as Used when processing tr; Peer Node does not have																								
<p>5</p>	<p>SOAM VIP: Add Application Ids for any other required Interfaces for Policy DRA</p>	<p>Repeat Step 6 for all other Application Ids that are expected to be involved in the Diameter call-flows. For example, 16777266 (for 3GPP Gxx) etc.</p>																								
<p>6</p>	<p>SOAM VIP: Verify that all Application Ids have been configured successfully.</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Application Ids</p> <p>You should see a screen containing all the configured Application Ids.</p> <p>Main Menu: Diameter -> Configuration -> Application Ids</p> <p style="text-align: right;">Thu Aug 07 16:41</p> <table border="1"> <thead> <tr> <th>Application Id</th> <th>Name</th> <th>Application Route Table</th> <th>Peer Route Table</th> <th>Routing Option Set</th> <th>Pending Answer Timer</th> </tr> </thead> <tbody> <tr> <td>16777236</td> <td>3GPP Rx</td> <td>Default</td> <td>Default</td> <td>Default</td> <td>Default</td> </tr> <tr> <td>16777238</td> <td>3GPP Gx</td> <td>Default</td> <td>Default</td> <td>Default</td> <td>Default</td> </tr> <tr> <td>4294967295</td> <td>Relay</td> <td>Default</td> <td>Default</td> <td>Default</td> <td>Default</td> </tr> </tbody> </table>	Application Id	Name	Application Route Table	Peer Route Table	Routing Option Set	Pending Answer Timer	16777236	3GPP Rx	Default	Default	Default	Default	16777238	3GPP Gx	Default	Default	Default	Default	4294967295	Relay	Default	Default	Default	Default
Application Id	Name	Application Route Table	Peer Route Table	Routing Option Set	Pending Answer Timer																					
16777236	3GPP Rx	Default	Default	Default	Default																					
16777238	3GPP Gx	Default	Default	Default	Default																					
4294967295	Relay	Default	Default	Default	Default																					
<p>7</p>	<p>SOAM VIP: Navigate to CEX Parameters Screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> CEX Parameters</p>																								
<p>8</p>	<p>SOAM VIP: Add CEX Parameter for Gx Interface</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																								

	<p>Main Menu: Diameter -> Configuration -> CEX Parameters -> [Insert]</p> <hr/> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Application Id</td> <td>16777238 - 3GPP Gx *</td> <td>Application Id is used to identify a specific Diameter Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Standard / 16777216 - 4294967294 for Vendor specific Applic</td> </tr> <tr> <td>Application Id Type</td> <td><input checked="" type="radio"/> Authentication <input type="radio"/> Accounting</td> <td>Type of Application Id.</td> </tr> <tr> <td>Vendor Specific Application Id</td> <td><input checked="" type="checkbox"/></td> <td>If checked, Vendor Id and Application Id AVP will be grouped in Vendor specific Application Id AVP. [Default = Unchecked, Range = n/a]</td> </tr> <tr> <td>Vendor Id</td> <td>10415</td> <td>A vendor Id value for this Vendor Specific Application Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]</td> </tr> </tbody> </table> <p>Ok Apply Cancel</p> <ol style="list-style-type: none"> 1. Select Application Id Gx Interface "16777238" 2. Check the Vendor Specific Application Id button 3. Enter the Vendor Id "10415" 4. Click Ok. 	Field	Value	Description	Application Id	16777238 - 3GPP Gx *	Application Id is used to identify a specific Diameter Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Standard / 16777216 - 4294967294 for Vendor specific Applic	Application Id Type	<input checked="" type="radio"/> Authentication <input type="radio"/> Accounting	Type of Application Id.	Vendor Specific Application Id	<input checked="" type="checkbox"/>	If checked, Vendor Id and Application Id AVP will be grouped in Vendor specific Application Id AVP. [Default = Unchecked, Range = n/a]	Vendor Id	10415	A vendor Id value for this Vendor Specific Application Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]
Field	Value	Description														
Application Id	16777238 - 3GPP Gx *	Application Id is used to identify a specific Diameter Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Standard / 16777216 - 4294967294 for Vendor specific Applic														
Application Id Type	<input checked="" type="radio"/> Authentication <input type="radio"/> Accounting	Type of Application Id.														
Vendor Specific Application Id	<input checked="" type="checkbox"/>	If checked, Vendor Id and Application Id AVP will be grouped in Vendor specific Application Id AVP. [Default = Unchecked, Range = n/a]														
Vendor Id	10415	A vendor Id value for this Vendor Specific Application Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]														
<p>9 SOAM VIP: Add CEX Parameter for Rx Interface</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Diameter -> Configuration -> CEX Parameters -> [Insert]</p> <hr/> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Application Id</td> <td>16777236 - 3GPP Rx *</td> <td>Application Id is used to identify a specific Diameter Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Standard / 16777216 - 4294967294 for Vendor specific Applic</td> </tr> <tr> <td>Application Id Type</td> <td><input checked="" type="radio"/> Authentication <input type="radio"/> Accounting</td> <td>Type of Application Id.</td> </tr> <tr> <td>Vendor Specific Application Id</td> <td><input checked="" type="checkbox"/></td> <td>If checked, Vendor Id and Application Id AVP will be grouped in Vendor specific Application Id AVP. [Default = Unchecked, Range = n/a]</td> </tr> <tr> <td>Vendor Id</td> <td>10415</td> <td>A vendor Id value for this Vendor Specific Application Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]</td> </tr> </tbody> </table> <p>Ok Apply Cancel</p> <ol style="list-style-type: none"> 1. Select Application Id Rx Interface "16777236" 2. Check the Vendor Specific Application Id button 3. Enter the Vendor Id "10415" 4. Click Ok. 	Field	Value	Description	Application Id	16777236 - 3GPP Rx *	Application Id is used to identify a specific Diameter Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Standard / 16777216 - 4294967294 for Vendor specific Applic	Application Id Type	<input checked="" type="radio"/> Authentication <input type="radio"/> Accounting	Type of Application Id.	Vendor Specific Application Id	<input checked="" type="checkbox"/>	If checked, Vendor Id and Application Id AVP will be grouped in Vendor specific Application Id AVP. [Default = Unchecked, Range = n/a]	Vendor Id	10415	A vendor Id value for this Vendor Specific Application Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]
Field	Value	Description														
Application Id	16777236 - 3GPP Rx *	Application Id is used to identify a specific Diameter Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Standard / 16777216 - 4294967294 for Vendor specific Applic														
Application Id Type	<input checked="" type="radio"/> Authentication <input type="radio"/> Accounting	Type of Application Id.														
Vendor Specific Application Id	<input checked="" type="checkbox"/>	If checked, Vendor Id and Application Id AVP will be grouped in Vendor specific Application Id AVP. [Default = Unchecked, Range = n/a]														
Vendor Id	10415	A vendor Id value for this Vendor Specific Application Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]														
<p>10 SOAM VIP: Add CEX Parameters for any other required Interfaces</p>	<p>Repeat Step 9 for all other configured Application Ids. For example, 3GPP Gxx, etc.</p>															
<p>11 SOAM VIP: Verify that all CEX Parameters have been configured successfully.</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> CEX Parameters</p> <p>You should see a screen containing all the configured CEX parameters.</p>															

	<p>Main Menu: Diameter -> Configuration -> CEX Parameters</p> <p>Filter ▾</p> <table border="1"> <thead> <tr> <th>Application Id</th> <th>Application Id Type</th> <th>Vendor Id</th> </tr> </thead> <tbody> <tr> <td>16777236 - 3GPP Rx</td> <td>Authentication</td> <td>10415</td> </tr> <tr> <td>16777238 - 3GPP Gx</td> <td>Authentication</td> <td>10415</td> </tr> <tr> <td>4294967295 - Relay</td> <td>Authentication</td> <td>---</td> </tr> </tbody> </table>	Application Id	Application Id Type	Vendor Id	16777236 - 3GPP Rx	Authentication	10415	16777238 - 3GPP Gx	Authentication	10415	4294967295 - Relay	Authentication	---
Application Id	Application Id Type	Vendor Id											
16777236 - 3GPP Rx	Authentication	10415											
16777238 - 3GPP Gx	Authentication	10415											
4294967295 - Relay	Authentication	---											
<p>12 SOAM VIP: Navigate to CEX Configuration Sets screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets</p>												
<p>13 SOAM VIP: Configure the CEX Configuration set to be used for Connections with the PCEF nodes.</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]</p>  <p>1. Enter the CEX Configuration Set Name "Gx" 2. Select the 3GPP Gx Application Id "16777238" from Available Application Ids 3. Click Add just below the list 4. Select the Vendor Id "10415" from Available Supported Vendor Ids 5. Click Add just below that list 6. Click Ok.</p>												
<p>14 SOAM VIP: Configure the CEX Configuration</p>	<p>Click on Insert in the lower left corner.</p>												

<input type="checkbox"/>	<p>Set to be used for Connections with the AF nodes.</p>	<p>You will see a screen similar to:</p> <p>Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]</p>  <ol style="list-style-type: none"> 1. Enter the CEX Configuration Set Name "Rx" 2. Select the 3GPP Rx Application Id "16777236" from Available Application Ids 3. Click Add just below the list 4. Select the Vendor Id "10415" from Available Supported Vendor Ids 5. Click Add just below that list 6. Click Ok.
<p>15</p>	<p>SOAM VIP: Configure the CEX Configuration Set to be used for Connections with the PCRF nodes.</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>

	<p>Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]</p>  <ol style="list-style-type: none"> 1. Enter the CEX Configuration Set Name "GxAndRx" 2. Select the 3GPP Gx Application Id "16777238" and 3GPP Rx Application Id "16777236" from Available Application Ids 3. Click Add just below the list 4. Select the Vendor Id "10415" from Available Supported Vendor Ids 5. Click Add just below that list 6. Click Ok.
<p>16</p>	<p>SOAM VIP: Configure the CEX Configuration Set for any other combination of Application Ids.</p> <p>Repeat step 15 for any other combination of Application Ids that need to be shared in a CEX exchange with some other node, for example, BBERF etc.</p>
<p>17</p>	<p>SOAM VIP: Verify that all the required CEX Configuration Sets have been configured successfully.</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets</p> <p>You should see a screen containing all the configured CEX Configuration Sets.</p>

	<p>Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets</p> <p>Filter ▾</p> <table border="1"> <thead> <tr> <th>CEX Configuration Set Name</th> <th>CEX Parameters</th> <th>Supported Vendor Ids</th> </tr> </thead> <tbody> <tr> <td>Default</td> <td>1 App Id 4294967295-Relay</td> <td>~</td> </tr> <tr> <td>Gx</td> <td>1 App Id 16777238-3GPP Gx</td> <td>10415</td> </tr> <tr> <td>GxAndRx</td> <td>2 App Ids 16777236-3GPP Rx 16777238-3GPP Gx</td> <td>10415</td> </tr> <tr> <td>Rx</td> <td>1 App Id 16777236-3GPP Rx</td> <td>10415</td> </tr> </tbody> </table>	CEX Configuration Set Name	CEX Parameters	Supported Vendor Ids	Default	1 App Id 4294967295-Relay	~	Gx	1 App Id 16777238-3GPP Gx	10415	GxAndRx	2 App Ids 16777236-3GPP Rx 16777238-3GPP Gx	10415	Rx	1 App Id 16777236-3GPP Rx	10415												
CEX Configuration Set Name	CEX Parameters	Supported Vendor Ids																										
Default	1 App Id 4294967295-Relay	~																										
Gx	1 App Id 16777238-3GPP Gx	10415																										
GxAndRx	2 App Ids 16777236-3GPP Rx 16777238-3GPP Gx	10415																										
Rx	1 App Id 16777236-3GPP Rx	10415																										
<p>18</p> <p>SOAM VIP: Navigate to Local Nodes screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Local Nodes</p>																											
<p>19</p> <p>SOAM VIP: Configure the first Local Node (P-DRA)</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Diameter -> Configuration -> Local Nodes -> [Insert]</p> <p style="text-align: right;">Thu Feb</p> <hr/> <p>Adding a new node</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Local Node Name</td> <td>PDRA *</td> <td>Unique name of the Local Node. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one digit and must not start with a digit.]</td> </tr> <tr> <td>Realm</td> <td>tekelec.com *</td> <td>Realm of this Local Node. Realm is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ("-") and underscore ("_"), and must end with a letter, digit or underscore and must end with a digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = A valid Realm.]</td> </tr> <tr> <td>FQDN</td> <td>pdra.tekelec.com *</td> <td>Fully Qualified Domain Name of this Local Node. FQDN is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ("-") and underscore ("_"). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. [Default = n/a; Range = A valid FQDN.]</td> </tr> <tr> <td>SCTP Enabled</td> <td><input checked="" type="checkbox"/></td> <td>If checked, indicates that this Local Node listens for SCTP connections.</td> </tr> <tr> <td>SCTP Listen Port</td> <td>3868</td> <td>SCTP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]</td> </tr> <tr> <td>TCP Enabled</td> <td><input checked="" type="checkbox"/></td> <td>If checked, indicates that this Local Node listens for TCP connections.</td> </tr> <tr> <td>TCP Listen Port</td> <td>3868</td> <td>TCP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]</td> </tr> <tr> <td>Connection Configuration Set</td> <td>Default ▾ *</td> <td>Connection Configuration Set of this Local Node. [Default = n/a; Range = n/a]</td> </tr> </tbody> </table>	Field	Value	Description	Local Node Name	PDRA *	Unique name of the Local Node. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one digit and must not start with a digit.]	Realm	tekelec.com *	Realm of this Local Node. Realm is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ("-") and underscore ("_"), and must end with a letter, digit or underscore and must end with a digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = A valid Realm.]	FQDN	pdra.tekelec.com *	Fully Qualified Domain Name of this Local Node. FQDN is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ("-") and underscore ("_"). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. [Default = n/a; Range = A valid FQDN.]	SCTP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Local Node listens for SCTP connections.	SCTP Listen Port	3868	SCTP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]	TCP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Local Node listens for TCP connections.	TCP Listen Port	3868	TCP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]	Connection Configuration Set	Default ▾ *	Connection Configuration Set of this Local Node. [Default = n/a; Range = n/a]
Field	Value	Description																										
Local Node Name	PDRA *	Unique name of the Local Node. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one digit and must not start with a digit.]																										
Realm	tekelec.com *	Realm of this Local Node. Realm is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ("-") and underscore ("_"), and must end with a letter, digit or underscore and must end with a digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = A valid Realm.]																										
FQDN	pdra.tekelec.com *	Fully Qualified Domain Name of this Local Node. FQDN is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ("-") and underscore ("_"). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. [Default = n/a; Range = A valid FQDN.]																										
SCTP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Local Node listens for SCTP connections.																										
SCTP Listen Port	3868	SCTP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]																										
TCP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Local Node listens for TCP connections.																										
TCP Listen Port	3868	TCP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]																										
Connection Configuration Set	Default ▾ *	Connection Configuration Set of this Local Node. [Default = n/a; Range = n/a]																										

	<div style="border: 1px solid gray; padding: 5px;"> <p>CEX Configuration Set: GxAndRx *</p> <p>CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]</p> <hr/> <p>IP Addresses:</p> <ul style="list-style-type: none"> 10.240.71.118 X * 10.240.71.121(TSA) X - Select - X - Select - X - Select - X - Select - X - Select - X - Select - X <p>The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries]</p> <p style="text-align: right;">Ok Apply Cancel</p> <p>1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values) 2. Click Ok.</p> <p>NOTE: The drop down list of IP address should contain the XSI addresses configured on DSR MP Servers. If not found then Installation may be incomplete/incorrect, please contact ORACLE Customer Service for further assistance.</p> </div>
<p>20 <input type="checkbox"/> SOAM VIP: Configure other Local Nodes, if required.</p>	<p>Repeat Step 19 and configure more Local Nodes if required.</p>
<p>21 <input type="checkbox"/> SOAM VIP: Navigate to Peer Nodes screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Peer Nodes</p>
<p>22 <input type="checkbox"/> SOAM VIP: Configure the first PCEF node</p>	<p>Click on Insert in the lower left corner. You will see a screen similar to:</p>

Main Menu: Diameter -> Configuration -> Peer Nodes -> [Insert]

Adding a new Peer node

Field	Value	Description
Peer Node Name	PCEF1	Unique name of the Peer Node. [Default = n/a; Range = A 32-character string. Valid
Realm	oracle.com	Realm of this Peer Node. Realm is a case-insensitive, underscore ("_"). A label must start with a letter, digit be at most 63 characters long and a Realm must be [Default = n/a; Range = A valid Realm.]
FQDN	pcef1.oracle.com	Fully Qualified Domain Name of this Peer Node. FQ digits, dashes ("-") and underscore ("_"). A label must character. A label must be at most 63 characters long [Default = n/a; Range = A valid FQDN.]
SCTP Enabled	<input checked="" type="checkbox"/>	If checked, Indicates that this Peer Node listens for S
SCTP Listen Port	3868	SCTP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]
TCP Enabled	<input checked="" type="checkbox"/>	If checked, Indicates that this Peer Node listens for T
TCP Listen Port	3868	TCP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]
IP Addresses	001 10.240.147.22 <input type="button" value="Add"/>	The IP address list of this Peer Node. [Default = n/a; Range = 1 - 128 entries]
Alternate Implicit Route	- Select -	Route List to use for routing messages to this Peer
Replace Dest Realm	<input type="checkbox"/>	If checked, Indicates that the Destination-Realm AVP [Default = Unchecked; Range = n/a]
Replace Dest Host	<input type="checkbox"/>	If checked, Indicates that the Destination-Host AVP c [Default = Unchecked; Range = n/a]
Topology Hiding Status	Disabled	If Enabled, Indicates that the Topology Hiding will be [Default = Disabled; Range = Disabled, Enabled]
Minimum Connection Capacity	1	The minimum number of available connections to the Otherwise, if the number of available connections to 1 Connection Capacity', the peer is 'Degraded'. Similarly, if no connections are available to the peer, [Default = 1; Range = 1 - 64 connections]
Maximum Alternate Routing Attempts	4	The maximum number of times that a Request can b [Default = 4; Range = 1 - 4 times]
Alternate Routing on Connection Failure	<input checked="" type="radio"/> Different Peer	Whether or not to perform alternate routing on altern failure occurs. [Default = Different Peer]
Alternate Routing on Answer Timeout	<input checked="" type="radio"/> Different Peer	Whether or not to perform alternate routing on the s when a Answer Timeout occurs [Default = Different Peer]
Alternate Routing on Answer Result Code	<input checked="" type="radio"/> Different Peer	- Whether or not to perform alternate routing on alter Answer Result Code occurs. - For an Answer response received from a DAS Pee -> System Options -> Message Copy Options -> Di [Default = Different Peer]
Message Priority Setting	<input checked="" type="radio"/> None	Message Priority Setting supports the following cho None - Set Message Priority based on the Message Default Message Priority Configuration Set will be u Read From Request Message - Read Message Pri above User Configured - Apply User Configured Message [Default = None]
Message Priority Configuration Set	- Select -	The Message Priority Configuration Set used for The Message Priority Configuration Set defines
Application Route Table	Not Selected	Application Route Table of this Peer Node. If value is "Not Selected", the downstream Applic
Peer Route Table	Not Selected	Peer Route Table of this Peer Node. If value is "Not Selected", the downstream Applic
Ingress Routing Option Set	Not Selected	Routing Option Set of this Ingress Peer Node. If value is "Not Selected", the downstream Applic
Egress Pending Answer Timer	Not Selected	Pending Answer Timer of this egress Peer Node If value is "Not Selected", the downstream Applic
Peer Node Group Name		Peer Node Group Name this Peer Node assigne

3. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values)
Note:

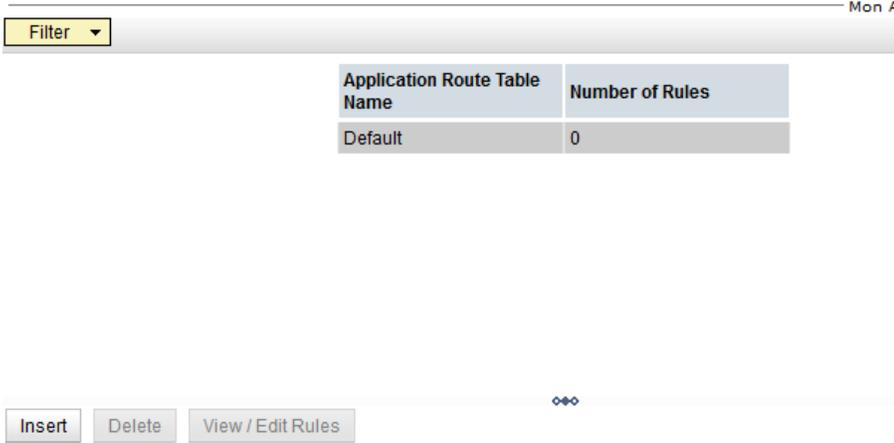
	<ul style="list-style-type: none"> - For Peer Nodes that are PCRFs, the “Replace Dest Host” and “Replace Dest Realm” check boxes MUST be checked. - “Topology Hiding Status” field is not applicable for PCA and should remain disabled. - The “Application Route Table” may apply for Peer Nodes that are Policy Clients. - The “Peer Route Table” field may be populated to route to Shared State PCRFs. - For more details on the fields and routing configuration please consult the Diameter User’s Guide ^[7] <p>2. Click Ok.</p>																																				
<p>23</p> <p>SOAM VIP: Configure other Peer Nodes</p>	<p>Repeat Step 22 to configure other peer nodes (PCEFs, AFs, BBERFs, PCRFs etc.) as required.</p>																																				
<p>24</p> <p>SOAM VIP: Navigate to Connections screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Connections</p>																																				
<p>25</p> <p>SOAM VIP: Configure the connection with PCEF Node</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <table border="1" data-bbox="516 699 1421 1375"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Connection Name</td> <td>PCRF1_Connection1</td> <td>A name that uniquely identifies the Connection. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric]</td> </tr> <tr> <td>AAA Protocol</td> <td>Diameter</td> <td>The AAA protocol for this Connection, which defines the Connection as Diameter [Default = N/A; Range = Diameter or RADIUS]</td> </tr> <tr> <td>Transport Protocol</td> <td> <input type="radio"/> SCTP <input checked="" type="radio"/> TCP <input type="radio"/> TLS/TCP <input type="radio"/> DTLS/SCTP <input type="radio"/> UDP </td> <td>The Transport Protocol used by this Connection. The protocol should be supported by both Local Node and Peer Node. Note: IPSEC should not be enabled if Connection is configured with TLS/TCP or significant performance impact.</td> </tr> <tr> <td>Connection Mode</td> <td>Initiator Only</td> <td>Initiator Only indicates that Local Node will only initiate the connection to the Peer Responder Only indicates that Local Node will only respond to the connection in Initiator & Responder indicates that Local Node will initiate connection in addition RADIUS Server indicates that the Local Node receives incoming RADIUS requests RADIUS Client indicates that the Local Node sends RADIUS requests to a Peer [Default = Initiator & Responder; Range = n/a]</td> </tr> <tr> <td>Local Node</td> <td>PCA</td> <td>The Local Node of this Connection.</td> </tr> <tr> <td>Local Initiate Port</td> <td></td> <td>The Local Initiator Port of this Connection. [Default = n/a; Range = 1024 - 49151]</td> </tr> <tr> <td>Primary Local IP Address</td> <td>10.240.71.108 (PDRAB3SiteA)</td> <td>The IP Address to be used as the Primary Local Node address for this Connection</td> </tr> <tr> <td>Secondary Local IP Address</td> <td>- Select -</td> <td>The IP Address to be used as the Secondary Local Node address for this Connection. This address is only used for SCTP multi-homing. This address must be different from the Primary Local IP Address.</td> </tr> <tr> <td>IPFE Initiator DAMP</td> <td>- Select -</td> <td>The DA-MP that will be used to initiate connections using the IPFE TSA address.</td> </tr> <tr> <td>Peer Node</td> <td>PCRF1</td> <td>The Peer Node of this Connection.</td> </tr> <tr> <td>Peer Node Identification</td> <td> <input type="radio"/> None <input checked="" type="radio"/> IP Address <input type="radio"/> Transport FQDN <input type="radio"/> Peer Diameter Identity FQDN </td> <td> Specifies how Node will derive the peer node’s IP address(es) when initiating a connection from the peer. None - Use option None for this connection when responding to a connection from the peer. IP Address - Use the remote IP address(es) configured for this Connection when responding to a connection from the peer. Transport FQDN - Use the DNS resolved Transport FQDN address configured for this Connection when responding to a connection from the peer. Peer Node FQDN - Use the DNS resolved FQDN address configured for the Peer Node when responding to a connection from the peer. </td> </tr> </tbody> </table>	Field	Value	Description	Connection Name	PCRF1_Connection1	A name that uniquely identifies the Connection. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric]	AAA Protocol	Diameter	The AAA protocol for this Connection, which defines the Connection as Diameter [Default = N/A; Range = Diameter or RADIUS]	Transport Protocol	<input type="radio"/> SCTP <input checked="" type="radio"/> TCP <input type="radio"/> TLS/TCP <input type="radio"/> DTLS/SCTP <input type="radio"/> UDP	The Transport Protocol used by this Connection. The protocol should be supported by both Local Node and Peer Node. Note: IPSEC should not be enabled if Connection is configured with TLS/TCP or significant performance impact.	Connection Mode	Initiator Only	Initiator Only indicates that Local Node will only initiate the connection to the Peer Responder Only indicates that Local Node will only respond to the connection in Initiator & Responder indicates that Local Node will initiate connection in addition RADIUS Server indicates that the Local Node receives incoming RADIUS requests RADIUS Client indicates that the Local Node sends RADIUS requests to a Peer [Default = Initiator & Responder; Range = n/a]	Local Node	PCA	The Local Node of this Connection.	Local Initiate Port		The Local Initiator Port of this Connection. [Default = n/a; Range = 1024 - 49151]	Primary Local IP Address	10.240.71.108 (PDRAB3SiteA)	The IP Address to be used as the Primary Local Node address for this Connection	Secondary Local IP Address	- Select -	The IP Address to be used as the Secondary Local Node address for this Connection. This address is only used for SCTP multi-homing. This address must be different from the Primary Local IP Address.	IPFE Initiator DAMP	- Select -	The DA-MP that will be used to initiate connections using the IPFE TSA address.	Peer Node	PCRF1	The Peer Node of this Connection.	Peer Node Identification	<input type="radio"/> None <input checked="" type="radio"/> IP Address <input type="radio"/> Transport FQDN <input type="radio"/> Peer Diameter Identity FQDN	Specifies how Node will derive the peer node’s IP address(es) when initiating a connection from the peer. None - Use option None for this connection when responding to a connection from the peer. IP Address - Use the remote IP address(es) configured for this Connection when responding to a connection from the peer. Transport FQDN - Use the DNS resolved Transport FQDN address configured for this Connection when responding to a connection from the peer. Peer Node FQDN - Use the DNS resolved FQDN address configured for the Peer Node when responding to a connection from the peer.
Field	Value	Description																																			
Connection Name	PCRF1_Connection1	A name that uniquely identifies the Connection. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric]																																			
AAA Protocol	Diameter	The AAA protocol for this Connection, which defines the Connection as Diameter [Default = N/A; Range = Diameter or RADIUS]																																			
Transport Protocol	<input type="radio"/> SCTP <input checked="" type="radio"/> TCP <input type="radio"/> TLS/TCP <input type="radio"/> DTLS/SCTP <input type="radio"/> UDP	The Transport Protocol used by this Connection. The protocol should be supported by both Local Node and Peer Node. Note: IPSEC should not be enabled if Connection is configured with TLS/TCP or significant performance impact.																																			
Connection Mode	Initiator Only	Initiator Only indicates that Local Node will only initiate the connection to the Peer Responder Only indicates that Local Node will only respond to the connection in Initiator & Responder indicates that Local Node will initiate connection in addition RADIUS Server indicates that the Local Node receives incoming RADIUS requests RADIUS Client indicates that the Local Node sends RADIUS requests to a Peer [Default = Initiator & Responder; Range = n/a]																																			
Local Node	PCA	The Local Node of this Connection.																																			
Local Initiate Port		The Local Initiator Port of this Connection. [Default = n/a; Range = 1024 - 49151]																																			
Primary Local IP Address	10.240.71.108 (PDRAB3SiteA)	The IP Address to be used as the Primary Local Node address for this Connection																																			
Secondary Local IP Address	- Select -	The IP Address to be used as the Secondary Local Node address for this Connection. This address is only used for SCTP multi-homing. This address must be different from the Primary Local IP Address.																																			
IPFE Initiator DAMP	- Select -	The DA-MP that will be used to initiate connections using the IPFE TSA address.																																			
Peer Node	PCRF1	The Peer Node of this Connection.																																			
Peer Node Identification	<input type="radio"/> None <input checked="" type="radio"/> IP Address <input type="radio"/> Transport FQDN <input type="radio"/> Peer Diameter Identity FQDN	Specifies how Node will derive the peer node’s IP address(es) when initiating a connection from the peer. None - Use option None for this connection when responding to a connection from the peer. IP Address - Use the remote IP address(es) configured for this Connection when responding to a connection from the peer. Transport FQDN - Use the DNS resolved Transport FQDN address configured for this Connection when responding to a connection from the peer. Peer Node FQDN - Use the DNS resolved FQDN address configured for the Peer Node when responding to a connection from the peer.																																			

	<table border="1"> <tr> <td>Primary Peer IP Address</td> <td>10.240.90.192 ▼ ✕</td> <td>The IP Address to be used as the Primary Peer Node address for this Connection.</td> </tr> <tr> <td>Secondary Peer IP Address</td> <td>- Select - ▼</td> <td>The IP Address to be used as the Secondary Peer Node address for this Connection. This address is only used for SCTP multi-homing. This address must be different from the address c</td> </tr> <tr> <td>UDP Port</td> <td>- Select - ▼</td> <td>For RADIUS Server connections, this is the UDP port on which the DSR expects to receive incoming R destination Peer Node which will receive the RADIUS request sent by the DSR. [Default = n/a; Range = configured Local or Peer Node UDP port numbers]</td> </tr> <tr> <td>Transport FQDN</td> <td></td> <td>Fully Qualified Domain Name for this connection. FQDN is a case-insensitive string consisting of a list ("."). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscore must be at most 255 characters long. [Default = n/a; Range = A valid FQDN]</td> </tr> <tr> <td>Connection Configuration Set</td> <td>Default ▼ *</td> <td>The configuration set of this Connection.</td> </tr> <tr> <td>CEX Configuration Set</td> <td>GxAndRx ▼</td> <td>CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]</td> </tr> <tr> <td>Capacity Configuration Set</td> <td>Default ▼ *</td> <td>The Capacity Configuration Set used for this Connection. The Capacity Configuration Set defines reserved and maximum ingress message processing rates a [Default = Default; Range = A 32-character string. Valid characters are alphanumeric and underscore.</td> </tr> <tr> <td>Transport Congestion Abatement Timeout</td> <td>5 *</td> <td>Defines the time period (in seconds) spent by the connection in abating each congestion level during [Default = 5; Range = 3 - 60 secs]</td> </tr> <tr> <td>Remote Busy Usage</td> <td>Disabled ▼ *</td> <td>Defines which Request messages can be forwarded on this connection after receiving a DIAMETER_ "Disabled" - The Connection is not considered to be BUSY after receiving a DIAMETER_TOO_BUSY re "Enabled" - The Connection is considered to be BUSY after receiving a DIAMETER_TOO_BUSY respon Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled]</td> </tr> <tr> <td>Remote Busy Abatement Timeout</td> <td>5</td> <td>Defines the time period (in seconds) that a Connection will be considered BUSY from the last time a [Default = 5; Range = 3 - 60 secs]</td> </tr> <tr> <td>Message Priority Setting</td> <td> <input checked="" type="radio"/> None <input type="radio"/> Read From Request Message <input type="radio"/> User Configured </td> <td>Message Priority Setting supports the following choices None - Set Message Priority based on Peer Node Message Priority Setting Read From Request Message - Read Message Priority from Ingress Request. This option shall only b User Configured - Apply User Configured Message Priority Configuration Set [Default = None]</td> </tr> <tr> <td>Message Priority Configuration Set</td> <td>- Select - ▼</td> <td>The Message Priority Configuration Set used for this connection. The Message Priority Configuatiua Set defines the priority of the Request Messages.</td> </tr> <tr> <td>Egress Message Throttling Configuration Set</td> <td>- Select - ▼</td> <td>The Egress Message Throttling Configuration Set used for this connection.</td> </tr> <tr> <td>Shared Secret Configuration Set</td> <td>- Select - ▼</td> <td>The Shared Secret Configuration Set used for this Connection.</td> </tr> <tr> <td>Message Authenticator Configuration Set</td> <td>- Select - ▼</td> <td>The Message Authenticator Configuration Set used for this Connection.</td> </tr> <tr> <td>Ingress Status-Server Configuration Set</td> <td>- Select - ▼</td> <td>The Ingress Status-Server Configuration Set used for this Connection.</td> </tr> <tr> <td>Suppress Connection Unavailable Alarm</td> <td><input type="checkbox"/></td> <td>If checked, connection unavailable alarm will not be raised. [Default = unchecked; Range = n/a]</td> </tr> <tr> <td>Suppress Connection Attempts</td> <td><input type="checkbox"/></td> <td>If checked, the connection attempts to standby Peer Node will be suppressed once Peer Node's Oper [Default = unchecked; Range = n/a]</td> </tr> <tr> <td>Test Mode</td> <td><input type="checkbox"/></td> <td>If checked, indicates that connection is in test mode. [Default = unchecked; Range = n/a]</td> </tr> </table> <p>4. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). Note: Please refer to the Diameter User's Guide ^[7] for details on fields in this screen.</p> <p>5. Click Ok.</p> <p>NOTE: Make sure the IPFE configuration matches the protocol which is selected in this step.</p>	Primary Peer IP Address	10.240.90.192 ▼ ✕	The IP Address to be used as the Primary Peer Node address for this Connection.	Secondary Peer IP Address	- Select - ▼	The IP Address to be used as the Secondary Peer Node address for this Connection. This address is only used for SCTP multi-homing. This address must be different from the address c	UDP Port	- Select - ▼	For RADIUS Server connections, this is the UDP port on which the DSR expects to receive incoming R destination Peer Node which will receive the RADIUS request sent by the DSR. [Default = n/a; Range = configured Local or Peer Node UDP port numbers]	Transport FQDN		Fully Qualified Domain Name for this connection. FQDN is a case-insensitive string consisting of a list ("."). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscore must be at most 255 characters long. [Default = n/a; Range = A valid FQDN]	Connection Configuration Set	Default ▼ *	The configuration set of this Connection.	CEX Configuration Set	GxAndRx ▼	CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]	Capacity Configuration Set	Default ▼ *	The Capacity Configuration Set used for this Connection. The Capacity Configuration Set defines reserved and maximum ingress message processing rates a [Default = Default; Range = A 32-character string. Valid characters are alphanumeric and underscore.	Transport Congestion Abatement Timeout	5 *	Defines the time period (in seconds) spent by the connection in abating each congestion level during [Default = 5; Range = 3 - 60 secs]	Remote Busy Usage	Disabled ▼ *	Defines which Request messages can be forwarded on this connection after receiving a DIAMETER_ "Disabled" - The Connection is not considered to be BUSY after receiving a DIAMETER_TOO_BUSY re "Enabled" - The Connection is considered to be BUSY after receiving a DIAMETER_TOO_BUSY respon Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled]	Remote Busy Abatement Timeout	5	Defines the time period (in seconds) that a Connection will be considered BUSY from the last time a [Default = 5; Range = 3 - 60 secs]	Message Priority Setting	<input checked="" type="radio"/> None <input type="radio"/> Read From Request Message <input type="radio"/> User Configured	Message Priority Setting supports the following choices None - Set Message Priority based on Peer Node Message Priority Setting Read From Request Message - Read Message Priority from Ingress Request. This option shall only b User Configured - Apply User Configured Message Priority Configuration Set [Default = None]	Message Priority Configuration Set	- Select - ▼	The Message Priority Configuration Set used for this connection. The Message Priority Configuatiua Set defines the priority of the Request Messages.	Egress Message Throttling Configuration Set	- Select - ▼	The Egress Message Throttling Configuration Set used for this connection.	Shared Secret Configuration Set	- Select - ▼	The Shared Secret Configuration Set used for this Connection.	Message Authenticator Configuration Set	- Select - ▼	The Message Authenticator Configuration Set used for this Connection.	Ingress Status-Server Configuration Set	- Select - ▼	The Ingress Status-Server Configuration Set used for this Connection.	Suppress Connection Unavailable Alarm	<input type="checkbox"/>	If checked, connection unavailable alarm will not be raised. [Default = unchecked; Range = n/a]	Suppress Connection Attempts	<input type="checkbox"/>	If checked, the connection attempts to standby Peer Node will be suppressed once Peer Node's Oper [Default = unchecked; Range = n/a]	Test Mode	<input type="checkbox"/>	If checked, indicates that connection is in test mode. [Default = unchecked; Range = n/a]
Primary Peer IP Address	10.240.90.192 ▼ ✕	The IP Address to be used as the Primary Peer Node address for this Connection.																																																								
Secondary Peer IP Address	- Select - ▼	The IP Address to be used as the Secondary Peer Node address for this Connection. This address is only used for SCTP multi-homing. This address must be different from the address c																																																								
UDP Port	- Select - ▼	For RADIUS Server connections, this is the UDP port on which the DSR expects to receive incoming R destination Peer Node which will receive the RADIUS request sent by the DSR. [Default = n/a; Range = configured Local or Peer Node UDP port numbers]																																																								
Transport FQDN		Fully Qualified Domain Name for this connection. FQDN is a case-insensitive string consisting of a list ("."). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscore must be at most 255 characters long. [Default = n/a; Range = A valid FQDN]																																																								
Connection Configuration Set	Default ▼ *	The configuration set of this Connection.																																																								
CEX Configuration Set	GxAndRx ▼	CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]																																																								
Capacity Configuration Set	Default ▼ *	The Capacity Configuration Set used for this Connection. The Capacity Configuration Set defines reserved and maximum ingress message processing rates a [Default = Default; Range = A 32-character string. Valid characters are alphanumeric and underscore.																																																								
Transport Congestion Abatement Timeout	5 *	Defines the time period (in seconds) spent by the connection in abating each congestion level during [Default = 5; Range = 3 - 60 secs]																																																								
Remote Busy Usage	Disabled ▼ *	Defines which Request messages can be forwarded on this connection after receiving a DIAMETER_ "Disabled" - The Connection is not considered to be BUSY after receiving a DIAMETER_TOO_BUSY re "Enabled" - The Connection is considered to be BUSY after receiving a DIAMETER_TOO_BUSY respon Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled]																																																								
Remote Busy Abatement Timeout	5	Defines the time period (in seconds) that a Connection will be considered BUSY from the last time a [Default = 5; Range = 3 - 60 secs]																																																								
Message Priority Setting	<input checked="" type="radio"/> None <input type="radio"/> Read From Request Message <input type="radio"/> User Configured	Message Priority Setting supports the following choices None - Set Message Priority based on Peer Node Message Priority Setting Read From Request Message - Read Message Priority from Ingress Request. This option shall only b User Configured - Apply User Configured Message Priority Configuration Set [Default = None]																																																								
Message Priority Configuration Set	- Select - ▼	The Message Priority Configuration Set used for this connection. The Message Priority Configuatiua Set defines the priority of the Request Messages.																																																								
Egress Message Throttling Configuration Set	- Select - ▼	The Egress Message Throttling Configuration Set used for this connection.																																																								
Shared Secret Configuration Set	- Select - ▼	The Shared Secret Configuration Set used for this Connection.																																																								
Message Authenticator Configuration Set	- Select - ▼	The Message Authenticator Configuration Set used for this Connection.																																																								
Ingress Status-Server Configuration Set	- Select - ▼	The Ingress Status-Server Configuration Set used for this Connection.																																																								
Suppress Connection Unavailable Alarm	<input type="checkbox"/>	If checked, connection unavailable alarm will not be raised. [Default = unchecked; Range = n/a]																																																								
Suppress Connection Attempts	<input type="checkbox"/>	If checked, the connection attempts to standby Peer Node will be suppressed once Peer Node's Oper [Default = unchecked; Range = n/a]																																																								
Test Mode	<input type="checkbox"/>	If checked, indicates that connection is in test mode. [Default = unchecked; Range = n/a]																																																								
<p>26</p> <p>SOAM VIP: Configure all other connections with Peer nodes</p>	<p>Repeat Step 25 to configure all other required DIAMETER connections.</p>																																																									
<p>27</p> <p>SOAM VIP: Configure Route Groups</p>	<p>PCRF Pooling allows the user to set up routing to PCRFs in groups. APNs can be mapped to such groups of PCRFs (called PCRF Pools). Each PCRF Pool can be mapped to a PRT that points to a Route List that points to prioritized Route Groups.</p> <p>Primary and Alternate Route Groups can be set up within each PCRF Pool by creating separate Route Groups and assigning appropriate priority when configuring the Route List.</p> <p>Please refer to the Diameter User's Guide ^[7] for more information on Diameter Routing.</p>																																																									
<p>28</p> <p>SOAM VIP: Create a primary Route Group for the first PCRF Pool</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Route Groups</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																																																									

	<p>Main Menu: Diameter -> Configuration -> Route Groups -> [Insert]</p> <hr/> <p>Adding a new route group</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>De</th> </tr> </thead> <tbody> <tr> <td>Route Group Name</td> <td>PcrfRouteGroup *</td> <td>A [C ct M a</td> </tr> <tr> <td>Type</td> <td> <input checked="" type="radio"/> Peer Route Group <input type="radio"/> Connection Route Group </td> <td>A (F th</td> </tr> <tr> <td>Peer Node, Connection and Capacity</td> <td> <table border="1"> <thead> <tr> <th>Peer Node</th> <th>Connection</th> <th>Provisioned Capacity *</th> </tr> </thead> <tbody> <tr> <td>01 pcrf</td> <td></td> <td>1 X</td> </tr> </tbody> </table> <p>Add</p> </td> <td>P [C C [C P w T N R N [C</td> </tr> </tbody> </table> <p>Ok Apply Cancel</p> <ol style="list-style-type: none"> 1. Enter the Route Group name. 2. Select the Peer Node name (PCRF name). 3. If more PCRFs need to be added, click on "Add" and repeat step 2. 3. Enter the provisioned capacity as required. 4. Click Ok. 	Field	Value	De	Route Group Name	PcrfRouteGroup *	A [C ct M a	Type	<input checked="" type="radio"/> Peer Route Group <input type="radio"/> Connection Route Group	A (F th	Peer Node, Connection and Capacity	<table border="1"> <thead> <tr> <th>Peer Node</th> <th>Connection</th> <th>Provisioned Capacity *</th> </tr> </thead> <tbody> <tr> <td>01 pcrf</td> <td></td> <td>1 X</td> </tr> </tbody> </table> <p>Add</p>	Peer Node	Connection	Provisioned Capacity *	01 pcrf		1 X	P [C C [C P w T N R N [C
Field	Value	De																	
Route Group Name	PcrfRouteGroup *	A [C ct M a																	
Type	<input checked="" type="radio"/> Peer Route Group <input type="radio"/> Connection Route Group	A (F th																	
Peer Node, Connection and Capacity	<table border="1"> <thead> <tr> <th>Peer Node</th> <th>Connection</th> <th>Provisioned Capacity *</th> </tr> </thead> <tbody> <tr> <td>01 pcrf</td> <td></td> <td>1 X</td> </tr> </tbody> </table> <p>Add</p>	Peer Node	Connection	Provisioned Capacity *	01 pcrf		1 X	P [C C [C P w T N R N [C											
Peer Node	Connection	Provisioned Capacity *																	
01 pcrf		1 X																	
<p>29 SOAM VIP: Configure alternate Route Group(s) for the same PCRF Pool.</p>	<p>OPTIONAL</p> <p>If alternate Route Group(s) are planned, repeat step 28 for all such Route Groups.</p>																		
<p>30 SOAM VIP: Configure Route List for the first PCRF Pool.</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Route Lists</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																		

	<table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Route List Name</td> <td>Pool1_RL1 *</td> </tr> <tr> <td>Minimum Route Group Availability Weight</td> <td>1 *</td> </tr> <tr> <td>Route Across Route Groups</td> <td> <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled </td> </tr> <tr> <td rowspan="3">Route Group, Priority , Traffic Throttle Group and Maximum Loss Percent Threshold</td> <td> Route Group: RG1 Priority: 1 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add </td> </tr> <tr> <td> Route Group: RG2 Priority: 2 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add </td> </tr> <tr> <td> Route Group: Priority: <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add </td> </tr> </tbody> </table> <ol style="list-style-type: none"> 1. Enter the Route List name. 2. Set the Minimum Route Group Availability Weight as needed. 3. Select the Route Group(s) configured in the previous two steps and set their desired priorities. 4. Set any other parameters desired (for e.g. Maximum Loss Percent Threshold etc.) 5. Click Ok. 	Field	Value	Route List Name	Pool1_RL1 *	Minimum Route Group Availability Weight	1 *	Route Across Route Groups	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Route Group, Priority , Traffic Throttle Group and Maximum Loss Percent Threshold	Route Group: RG1 Priority: 1 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01		X	Route Group: RG2 Priority: 2 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01		X	Route Group: Priority: <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01		X
Field	Value																														
Route List Name	Pool1_RL1 *																														
Minimum Route Group Availability Weight	1 *																														
Route Across Route Groups	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled																														
Route Group, Priority , Traffic Throttle Group and Maximum Loss Percent Threshold	Route Group: RG1 Priority: 1 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01		X																								
	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold																												
	01		X																												
Route Group: RG2 Priority: 2 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01		X																									
Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold																													
01		X																													
Route Group: Priority: <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td>X</td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01		X																									
Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold																													
01		X																													
<p>31 SOAM VIP: Configure the Peer Routing Rules for the first PCRF Pool.</p>	<p>Configure the PRT such that DSR forwards messages based on the PCRF Pool selected by PCA.</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Peer Route Table</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Adding a new Peer Route Table</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Peer Route Table Name</td> <td>*</td> <td>Unique name of the Peer Route Table. [Default = n/a; Range = A 32-character string. Valid chara</td> </tr> </tbody> </table> <ol style="list-style-type: none"> 1. Enter the Peer Route Table name. 2. Click Ok. 	Field	Value	Description	Peer Route Table Name	*	Unique name of the Peer Route Table. [Default = n/a; Range = A 32-character string. Valid chara																								
Field	Value	Description																													
Peer Route Table Name	*	Unique name of the Peer Route Table. [Default = n/a; Range = A 32-character string. Valid chara																													
<p>32 SOAM VIP: Configure Routing Rules for the first PCRF Pool</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																														

	<table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rule Name</td> <td>Pool1_Rule1 *</td> <td>Unique name of the Rule. [Default = n/a; Range = A 32-c a digit]</td> </tr> <tr> <td>Peer Route Table</td> <td>Pool1_PRT *</td> <td>Peer Route Table associated</td> </tr> <tr> <td>Priority</td> <td>1 *</td> <td>Priority of this Rule. Low value means higher prior [Default = n/a; Range = 1 - 10]</td> </tr> <tr> <td>Conditions</td> <td> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Destination-Host</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Application-Id</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table> </td> <td> <p>Conditions associated with th Each condition has three part: In order for a Diameter mess; it must match the criteria of es Application-Id; [Default = n/a; Range = 0-429]</p> <p>Command Code: [Default = n/a; Range = 0-167]</p> <p>Destination-Realm and Origin Realm is a case-insensitive s where a label may contain lett A label must start with a letter, Underscores may be used on A label must be at most 63 ch [Default = n/a; Range = Sub sl</p> <p>Destination-Host and Origin+ FQDN is a case-insensitive sl where a label may contain lett A label must start with a letter, Underscores may be used on A label must be at most 63 ch [Default = n/a; Range = Sub sl</p> </td> </tr> <tr> <td>Action</td> <td> <input checked="" type="radio"/> Route to Peer <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer </td> <td>Action associated with this Ru Route to Peer will route mess Send Answer will abandon m Abandon With No Answer will</td> </tr> <tr> <td>Route List</td> <td>RL1</td> <td>Route List associated with this Ru Route List is required if Action is "R"</td> </tr> <tr> <td>Message Priority</td> <td>No Change</td> <td>The priority of the message to be s message only when the "Action" fie</td> </tr> <tr> <td>Message Copy Configuration Set</td> <td>- Select -</td> <td>Message Copy Configuration Set (Rule for copy to the DAS. [Default = n/a]</td> </tr> <tr> <td>Answer Result-Code Value</td> <td> <input type="radio"/> - Select - <input type="radio"/> </td> <td>Value to be placed in the Result-C Answer Result-Code Value is requ [Default = n/a; Range = 1000 - 599]</td> </tr> <tr> <td>Vendor Id</td> <td></td> <td>Vendor Id Value. Vendor Id will be placed in Vendor [Default = n/a; Range = 1 - 429496]</td> </tr> <tr> <td>Answer Error Message</td> <td></td> <td>String to be placed in the Error-Me; [Default = null string; Range = 0 to</td> </tr> </tbody> </table> <p>1. Enter the Rule name. 2. Set the Priority of the Rule as needed (preferably 1). 3. Select "Always True" for all Condition Parameters. You may base the PCRF Pool routing on some condition parameter in special use cases for example Origin-based routing. 3. Select the Route List configured in step 30. 4. Click Ok.</p>	Field	Value	Description	Rule Name	Pool1_Rule1 *	Unique name of the Rule. [Default = n/a; Range = A 32-c a digit]	Peer Route Table	Pool1_PRT *	Peer Route Table associated	Priority	1 *	Priority of this Rule. Low value means higher prior [Default = n/a; Range = 1 - 10]	Conditions	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Destination-Host</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Application-Id</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table>	Parameter	Operator	Value		Destination-Realm	Always True		AND	Destination-Host	Always True		AND	Application-Id	Always True	- Select -	AND	Command-Code	Always True	- Select -	AND	Origin-Realm	Always True		AND	Origin-Host	Always True			<p>Conditions associated with th Each condition has three part: In order for a Diameter mess; it must match the criteria of es Application-Id; [Default = n/a; Range = 0-429]</p> <p>Command Code: [Default = n/a; Range = 0-167]</p> <p>Destination-Realm and Origin Realm is a case-insensitive s where a label may contain lett A label must start with a letter, Underscores may be used on A label must be at most 63 ch [Default = n/a; Range = Sub sl</p> <p>Destination-Host and Origin+ FQDN is a case-insensitive sl where a label may contain lett A label must start with a letter, Underscores may be used on A label must be at most 63 ch [Default = n/a; Range = Sub sl</p>	Action	<input checked="" type="radio"/> Route to Peer <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer	Action associated with this Ru Route to Peer will route mess Send Answer will abandon m Abandon With No Answer will	Route List	RL1	Route List associated with this Ru Route List is required if Action is "R"	Message Priority	No Change	The priority of the message to be s message only when the "Action" fie	Message Copy Configuration Set	- Select -	Message Copy Configuration Set (Rule for copy to the DAS. [Default = n/a]	Answer Result-Code Value	<input type="radio"/> - Select - <input type="radio"/>	Value to be placed in the Result-C Answer Result-Code Value is requ [Default = n/a; Range = 1000 - 599]	Vendor Id		Vendor Id Value. Vendor Id will be placed in Vendor [Default = n/a; Range = 1 - 429496]	Answer Error Message		String to be placed in the Error-Me; [Default = null string; Range = 0 to
Field	Value	Description																																																															
Rule Name	Pool1_Rule1 *	Unique name of the Rule. [Default = n/a; Range = A 32-c a digit]																																																															
Peer Route Table	Pool1_PRT *	Peer Route Table associated																																																															
Priority	1 *	Priority of this Rule. Low value means higher prior [Default = n/a; Range = 1 - 10]																																																															
Conditions	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Destination-Host</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Application-Id</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table>	Parameter	Operator	Value		Destination-Realm	Always True		AND	Destination-Host	Always True		AND	Application-Id	Always True	- Select -	AND	Command-Code	Always True	- Select -	AND	Origin-Realm	Always True		AND	Origin-Host	Always True			<p>Conditions associated with th Each condition has three part: In order for a Diameter mess; it must match the criteria of es Application-Id; [Default = n/a; Range = 0-429]</p> <p>Command Code: [Default = n/a; Range = 0-167]</p> <p>Destination-Realm and Origin Realm is a case-insensitive s where a label may contain lett A label must start with a letter, Underscores may be used on A label must be at most 63 ch [Default = n/a; Range = Sub sl</p> <p>Destination-Host and Origin+ FQDN is a case-insensitive sl where a label may contain lett A label must start with a letter, Underscores may be used on A label must be at most 63 ch [Default = n/a; Range = Sub sl</p>																																			
Parameter	Operator	Value																																																															
Destination-Realm	Always True		AND																																																														
Destination-Host	Always True		AND																																																														
Application-Id	Always True	- Select -	AND																																																														
Command-Code	Always True	- Select -	AND																																																														
Origin-Realm	Always True		AND																																																														
Origin-Host	Always True																																																																
Action	<input checked="" type="radio"/> Route to Peer <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer	Action associated with this Ru Route to Peer will route mess Send Answer will abandon m Abandon With No Answer will																																																															
Route List	RL1	Route List associated with this Ru Route List is required if Action is "R"																																																															
Message Priority	No Change	The priority of the message to be s message only when the "Action" fie																																																															
Message Copy Configuration Set	- Select -	Message Copy Configuration Set (Rule for copy to the DAS. [Default = n/a]																																																															
Answer Result-Code Value	<input type="radio"/> - Select - <input type="radio"/>	Value to be placed in the Result-C Answer Result-Code Value is requ [Default = n/a; Range = 1000 - 599]																																																															
Vendor Id		Vendor Id Value. Vendor Id will be placed in Vendor [Default = n/a; Range = 1 - 429496]																																																															
Answer Error Message		String to be placed in the Error-Me; [Default = null string; Range = 0 to																																																															
<p>33</p> <p>SOAM VIP: Configure Routing for other PCRF Pools.</p>	<p>If more, PCRF Pools are planned in the Diameter network, repeat steps 28 through 32 for other PCRF Pools' Routing</p>																																																																
<p>34</p> <p>SOAM VIP: Configure Routing for in-session Diameter messages</p>	<p>OPTIONAL</p> <p>If required, configure the routing for messages where Destination Host is present in the Diameter messages (typically in-session messages).</p> <p>CAUTION In-session messages or session creation messages that follow a final subscriber binding, destined for a particular Destination Host (PCRF) can be routed to alternate PCRFs only when such PCRFs share state information. Doing so for PCRFs that do not share state information may result in call failures or split-bindings.</p>																																																																
<p>35</p> <p>SOAM VIP: Configure inter DSR Routing</p>	<p>OPTIONAL</p> <p>If Diameter messages need to be routed in between DSR sites (nodes), set up the routing as needed.</p> <p>This is likely in 3-site redundancy deployments because many PCEF's likely only support primary and secondary connections. In such deployments routing can be set up between the three sites.</p>																																																																

<p>36</p>	<p>SOAM VIP: Configure Routing for Gx RAR messages</p>	<p>OPTIONAL</p> <p>Configure the Routing Rules to route a Gx RAR message generated at one site that is destined for a PCEF connected to another site.</p> <p>This is likely in 3-site redundancy deployments because many PCEFs likely only support primary and secondary connections. In such deployments routing can be set up between the three sites.</p> <p>TIP: Destination-Host based routing can be set up to route the Gx RAR messages to the appropriate site's DSR.</p>
<p>37</p>	<p>SOAM VIP: Navigate to the Application Routing Rules screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Application Routing Rules</p> <p>You will see a screen similar to:</p> <p>Main Menu: Diameter -> Configuration -> Application Route Tables</p>  <p>1. Select the Default Application Route Table Name to which rules are to be added. 2. Click on View/Edit Rules button.</p>
<p>38</p>	<p>SOAM VIP: Configure the ART for Gx Interface messages</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>

Inserting Rule for Application Route Table: Default

Field	Value																													
Rule Name	GxRule	Un [Di sta																												
Application Route Table	Default	Ap																												
Priority	5	Pri Lov [Di																												
Conditions	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND Co [Di</td> </tr> <tr> <td>Destination-Host</td> <td>Always True</td> <td></td> <td>AND De</td> </tr> <tr> <td>Application-Id</td> <td>Equals</td> <td>16777238 - 3GPP Gx</td> <td>AND Re wh A t Un A t [Di</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND De FG wh A t Un A t [Di</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table>	Parameter	Operator	Value		Destination-Realm	Always True		AND Co [Di	Destination-Host	Always True		AND De	Application-Id	Equals	16777238 - 3GPP Gx	AND Re wh A t Un A t [Di	Command-Code	Always True	- Select -	AND	Origin-Realm	Always True		AND De FG wh A t Un A t [Di	Origin-Host	Always True			
	Parameter	Operator	Value																											
	Destination-Realm	Always True		AND Co [Di																										
	Destination-Host	Always True		AND De																										
	Application-Id	Equals	16777238 - 3GPP Gx	AND Re wh A t Un A t [Di																										
	Command-Code	Always True	- Select -	AND																										
	Origin-Realm	Always True		AND De FG wh A t Un A t [Di																										
Origin-Host	Always True																													
Action	<input checked="" type="radio"/> Route to Application <input type="radio"/> Forward To Egress Routing <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer	Ad Ro Fo Sel Ad																												
Answer Result-Code Value	<input type="radio"/> - Select - <input type="radio"/>	Val An [Di																												
Vendor Id		Ve Ve [Di																												
Answer Error Message		Str [Di																												
Application Name	PCA	Ap																												
Gx-Prime	<input type="checkbox"/>	If t																												

1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values).
 2. Click **Ok**.

39 SOAM VIP: Configure the ART for Rx Interface messages

Click on **Insert** in the lower left corner.
 You will see a screen similar to:

Inserting Rule for Application Route Table: Default

Field	Value																												
Rule Name	RxRule																												
Application Route Table	Default																												
Priority	5																												
Conditions	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Destination-Host</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Application-Id</td> <td>Equals</td> <td>16777236 - 3GPP Rx</td> <td>AND</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table>	Parameter	Operator	Value		Destination-Realm	Always True		AND	Destination-Host	Always True		AND	Application-Id	Equals	16777236 - 3GPP Rx	AND	Command-Code	Always True	- Select -	AND	Origin-Realm	Always True		AND	Origin-Host	Always True		
Parameter	Operator	Value																											
Destination-Realm	Always True		AND																										
Destination-Host	Always True		AND																										
Application-Id	Equals	16777236 - 3GPP Rx	AND																										
Command-Code	Always True	- Select -	AND																										
Origin-Realm	Always True		AND																										
Origin-Host	Always True																												
Action	<input checked="" type="radio"/> Route to Application <input type="radio"/> Forward To Egress Routing <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer																												
Answer Result-Code Value	<input type="radio"/> - Select - <input type="radio"/>																												
Vendor Id																													
Answer Error Message																													
Application Name	PCA																												
Gx-Prime	<input type="checkbox"/>																												

1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values).
 2. Click **Ok**.

40 **SOAM VIP:** Configure the ART for all other Interfaces

Repeat Step 38 for any other Application Id that needs to be routed to the PCA Application by Diameter Routing Layer.

4.3.2 Diameter Configuration for Online Charging DRA

Detailed steps are given in the procedure below.

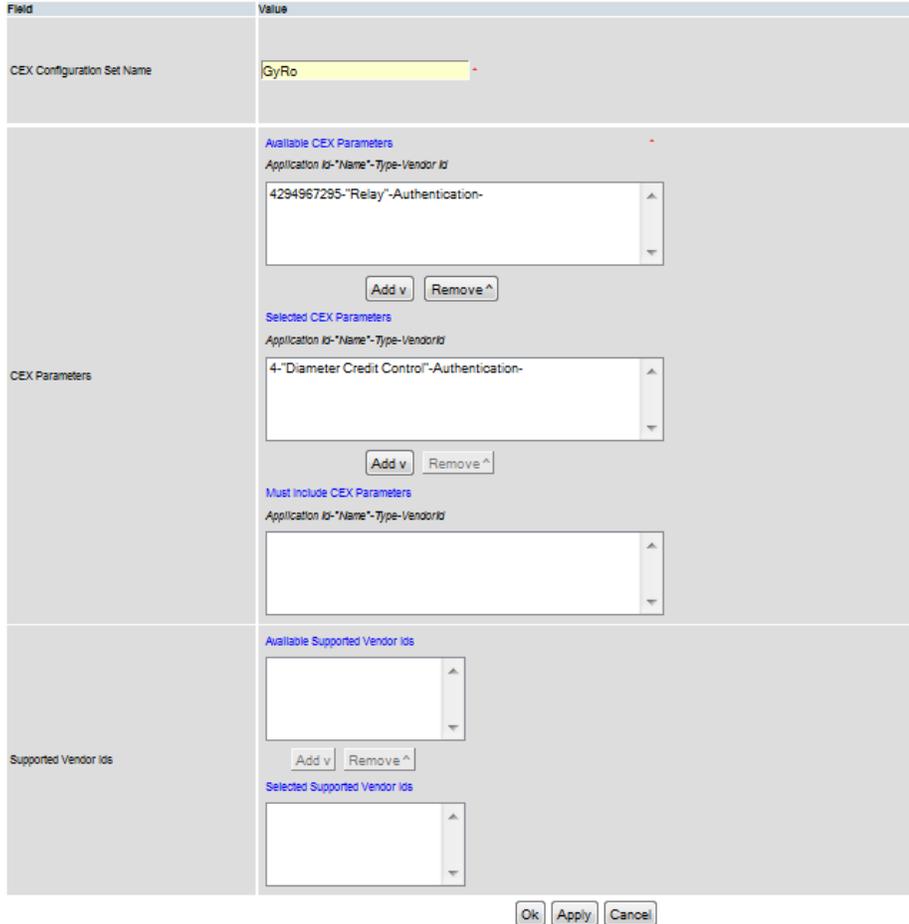
Procedure 14: Diameter configuration for Online Charging DRA

NOTE: EXECUTE THIS PROCEDURE FOR ONLINE CHARGING DRA FUNCTION

SKIP THIS PROCEDURE IF POLICY DRA FUNCTION ONLY

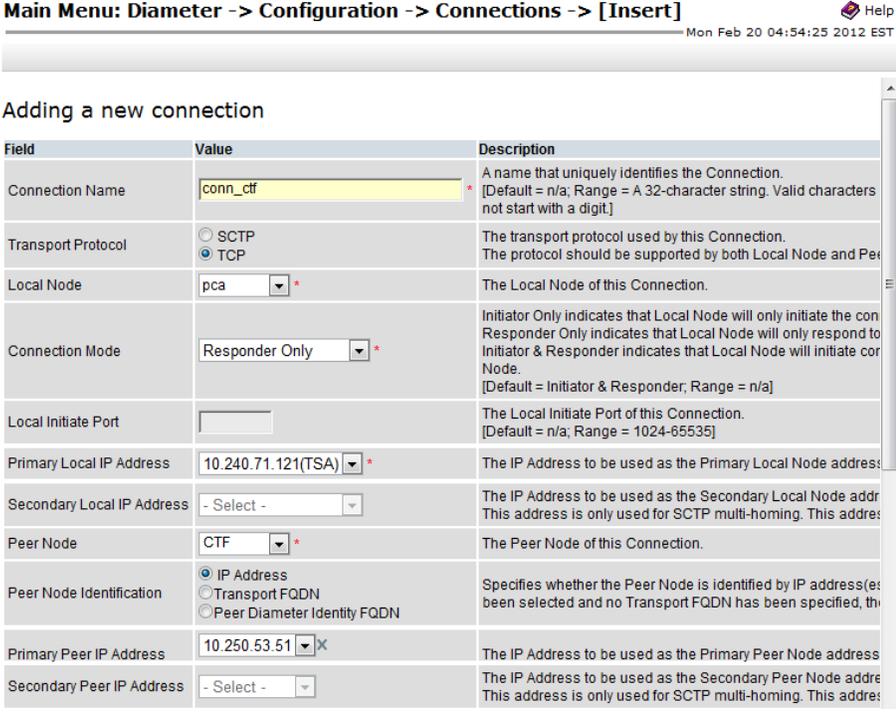
S T E P #	This procedure configures the Diameter stack. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .																						
	1	Establish GUI Session on the SOAM VIP Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".																					
	2	SOAM VIP: Navigate to Application Id Configuration Screen Navigate to Main Menu -> Diameter -> Configuration -> Application Ids																					
	3	SOAM VIP: Add Application Id for GyRo Interface Click on Insert in the lower left corner. You will see a screen similar to: <div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; margin: 0;">Main Menu: Diameter -> Configuration -> Application Ids -> [Insert]</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Field</th> <th style="text-align: left;">Value</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>Diameter Credit Control *</td> <td>Application Id Name</td> </tr> <tr> <td>Application Id Value</td> <td> <input checked="" type="radio"/> 4 - Diameter Credit Control <input type="radio"/> <input style="width: 100px;" type="text"/> </td> <td>Application Id is used to identify the peer node. [Default = n/a; Range = 1 - 16777216 - 4294967294 for Relay]</td> </tr> <tr> <td>Application Route Table</td> <td>Default ▾</td> <td>Application Route Table as Used for routing Requests when the downstream Peer Node does not have a Peer Route Table.</td> </tr> <tr> <td>Peer Route Table</td> <td>Default ▾</td> <td>Peer Route Table associated with the Peer Node. Used for routing Requests when the Peer Node does not have a Peer Route Table.</td> </tr> <tr> <td>Routing Option Set</td> <td>Default ▾</td> <td>Routing Option Set associated with the Peer Node. Used when processing traffic from the Peer Node downstream. Peer Node does not have a Peer Route Table.</td> </tr> <tr> <td>Pending Answer Timer</td> <td>Default ▾</td> <td>Pending Answer Timer associated with the Peer Node. Used when processing traffic from the Peer Node downstream. Peer Node does not have a Peer Route Table.</td> </tr> </tbody> </table> <p style="text-align: right; margin-top: 5px;"> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> </div> <p>1. Select Application Id for Diameter Credit Control "4". 2. Click Ok.</p>	Field	Value	Description	Name	Diameter Credit Control *	Application Id Name	Application Id Value	<input checked="" type="radio"/> 4 - Diameter Credit Control <input type="radio"/> <input style="width: 100px;" type="text"/>	Application Id is used to identify the peer node. [Default = n/a; Range = 1 - 16777216 - 4294967294 for Relay]	Application Route Table	Default ▾	Application Route Table as Used for routing Requests when the downstream Peer Node does not have a Peer Route Table.	Peer Route Table	Default ▾	Peer Route Table associated with the Peer Node. Used for routing Requests when the Peer Node does not have a Peer Route Table.	Routing Option Set	Default ▾	Routing Option Set associated with the Peer Node. Used when processing traffic from the Peer Node downstream. Peer Node does not have a Peer Route Table.	Pending Answer Timer	Default ▾	Pending Answer Timer associated with the Peer Node. Used when processing traffic from the Peer Node downstream. Peer Node does not have a Peer Route Table.
	Field	Value	Description																				
Name	Diameter Credit Control *	Application Id Name																					
Application Id Value	<input checked="" type="radio"/> 4 - Diameter Credit Control <input type="radio"/> <input style="width: 100px;" type="text"/>	Application Id is used to identify the peer node. [Default = n/a; Range = 1 - 16777216 - 4294967294 for Relay]																					
Application Route Table	Default ▾	Application Route Table as Used for routing Requests when the downstream Peer Node does not have a Peer Route Table.																					
Peer Route Table	Default ▾	Peer Route Table associated with the Peer Node. Used for routing Requests when the Peer Node does not have a Peer Route Table.																					
Routing Option Set	Default ▾	Routing Option Set associated with the Peer Node. Used when processing traffic from the Peer Node downstream. Peer Node does not have a Peer Route Table.																					
Pending Answer Timer	Default ▾	Pending Answer Timer associated with the Peer Node. Used when processing traffic from the Peer Node downstream. Peer Node does not have a Peer Route Table.																					
4	SOAM VIP: Navigate to CEX Parameters Screen Navigate to Main Menu -> Diameter -> Configuration -> CEX Parameters																						
5	SOAM VIP: Add CEX Parameter for GyRo Interface Click on Insert in the lower left corner. You will see a screen similar to:																						

	<p>Main Menu: Diameter -> Configuration -> CEX Parameters -> [Insert]</p> <hr/> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Application Id</td> <td>4 - Diameter Credit Control *</td> <td>Application Id is used to identify a specific D Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Sta 16777216 - 4294967294 for Vendor specific</td> </tr> <tr> <td>Application Id Type</td> <td><input checked="" type="radio"/> Authentication <input type="radio"/> Accounting</td> <td>Type of Application Id.</td> </tr> <tr> <td>Vendor Specific Application Id</td> <td><input type="checkbox"/></td> <td>If checked, Vendor Id and Application Id AVP grouped in Vendor specific Application Id A [Default = Unchecked, Range = n/a]</td> </tr> <tr> <td>Vendor Id</td> <td><input type="text"/></td> <td>A vendor Id value for this Vendor Specific Ap Vendor Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]</td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> <p>1. Select Application Id "4 – Diameter Credit Control". 2. Click Ok.</p>	Field	Value	Description	Application Id	4 - Diameter Credit Control *	Application Id is used to identify a specific D Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Sta 16777216 - 4294967294 for Vendor specific	Application Id Type	<input checked="" type="radio"/> Authentication <input type="radio"/> Accounting	Type of Application Id.	Vendor Specific Application Id	<input type="checkbox"/>	If checked, Vendor Id and Application Id AVP grouped in Vendor specific Application Id A [Default = Unchecked, Range = n/a]	Vendor Id	<input type="text"/>	A vendor Id value for this Vendor Specific Ap Vendor Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]
Field	Value	Description														
Application Id	4 - Diameter Credit Control *	Application Id is used to identify a specific D Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Sta 16777216 - 4294967294 for Vendor specific														
Application Id Type	<input checked="" type="radio"/> Authentication <input type="radio"/> Accounting	Type of Application Id.														
Vendor Specific Application Id	<input type="checkbox"/>	If checked, Vendor Id and Application Id AVP grouped in Vendor specific Application Id A [Default = Unchecked, Range = n/a]														
Vendor Id	<input type="text"/>	A vendor Id value for this Vendor Specific Ap Vendor Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295]														
<p>6 SOAM VIP: Navigate to CEX Configuration Sets screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets</p>															
<p>7 SOAM VIP: Configure the CEX Configuration set to be used for Connections with the CTF and OCS nodes.</p>	<p>Click on Insert in the lower left corner. You will see a screen similar to:</p>															

	<p>Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]</p>  <ol style="list-style-type: none"> 1. Enter the CEX Configuration Set Name "GyRo". 2. Select the Diameter Credit Control Application Id from Available CEX Parameters box 3. Click Add just below the list. 4. Click Ok. 									
<p>8</p> <p>SOAM VIP: Verify that all the required CEX Configuration Sets have been configured successfully.</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets</p> <p>You should see a screen containing all the configured CEX Configuration Sets.</p> <p>Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets Mon Aug 11</p>  <table border="1"> <thead> <tr> <th>CEX Configuration Set Name</th> <th>CEX Parameters</th> <th>Supported Vendor Ids</th> </tr> </thead> <tbody> <tr> <td>Default</td> <td><input type="checkbox"/> 1 App Id 4294967295-Relay</td> <td>~</td> </tr> <tr> <td>GyRo</td> <td><input type="checkbox"/> 1 App Id 4-Diameter Credit Control</td> <td>~</td> </tr> </tbody> </table>	CEX Configuration Set Name	CEX Parameters	Supported Vendor Ids	Default	<input type="checkbox"/> 1 App Id 4294967295-Relay	~	GyRo	<input type="checkbox"/> 1 App Id 4-Diameter Credit Control	~
CEX Configuration Set Name	CEX Parameters	Supported Vendor Ids								
Default	<input type="checkbox"/> 1 App Id 4294967295-Relay	~								
GyRo	<input type="checkbox"/> 1 App Id 4-Diameter Credit Control	~								
<p>9</p> <p>SOAM VIP: Navigate to Local Nodes screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Local Nodes</p>									
<p>10</p> <p>SOAM VIP: Configure the first Local Node</p>	<p>Click on Insert in the lower left corner.</p>									

<p>(OC-DRA)</p>	<p>You will see a screen similar to:</p> <p>Main Menu: Diameter -> Configuration -> Local Nodes -> [Insert]</p> <p>Thu Feb</p> <p>Adding a new node</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Local Node Name</td> <td>pca</td> <td>Unique name of the Local Node. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one character and must not start with a digit.]</td> </tr> <tr> <td>Realm</td> <td>oracle.com</td> <td>Realm of this Local Node. Realm is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ('-') and underscore ('_'). Each label must start with a letter, digit or underscore and must end with a letter, digit or underscore. Underscores may be used only as the first character of a label. A label must be at most 63 characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = A valid Realm.]</td> </tr> <tr> <td>FQDN</td> <td>pca.oracle.com</td> <td>Fully Qualified Domain Name of this Local Node. FQDN is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character of a label. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. [Default = n/a; Range = A valid FQDN.]</td> </tr> <tr> <td>SCTP Enabled</td> <td><input checked="" type="checkbox"/></td> <td>If checked, indicates that this Local Node listens for SCTP connections.</td> </tr> <tr> <td>SCTP Listen Port</td> <td>3868</td> <td>SCTP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]</td> </tr> <tr> <td>TCP Enabled</td> <td><input checked="" type="checkbox"/></td> <td>If checked, indicates that this Local Node listens for TCP connections.</td> </tr> <tr> <td>TCP Listen Port</td> <td>3868</td> <td>TCP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]</td> </tr> <tr> <td>Connection Configuration Set</td> <td>Default</td> <td>Connection Configuration Set of this Local Node. [Default = n/a; Range = n/a]</td> </tr> <tr> <td>CEX Configuration Set</td> <td>GyRo</td> <td>CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]</td> </tr> <tr> <td>IP Addresses</td> <td> 10.240.71.118 X 10.240.71.121(TSA) X - Select - X </td> <td>The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries]</td> </tr> </tbody> </table> <p>Ok Apply Cancel</p>	Field	Value	Description	Local Node Name	pca	Unique name of the Local Node. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one character and must not start with a digit.]	Realm	oracle.com	Realm of this Local Node. Realm is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ('-') and underscore ('_'). Each label must start with a letter, digit or underscore and must end with a letter, digit or underscore. Underscores may be used only as the first character of a label. A label must be at most 63 characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = A valid Realm.]	FQDN	pca.oracle.com	Fully Qualified Domain Name of this Local Node. FQDN is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character of a label. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. [Default = n/a; Range = A valid FQDN.]	SCTP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Local Node listens for SCTP connections.	SCTP Listen Port	3868	SCTP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]	TCP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Local Node listens for TCP connections.	TCP Listen Port	3868	TCP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]	Connection Configuration Set	Default	Connection Configuration Set of this Local Node. [Default = n/a; Range = n/a]	CEX Configuration Set	GyRo	CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]	IP Addresses	10.240.71.118 X 10.240.71.121(TSA) X - Select - X	The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries]
Field	Value	Description																																
Local Node Name	pca	Unique name of the Local Node. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one character and must not start with a digit.]																																
Realm	oracle.com	Realm of this Local Node. Realm is a case-insensitive string consisting of a list of labels separated by dots, where each label may contain letters, digits, dashes ('-') and underscore ('_'). Each label must start with a letter, digit or underscore and must end with a letter, digit or underscore. Underscores may be used only as the first character of a label. A label must be at most 63 characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = A valid Realm.]																																
FQDN	pca.oracle.com	Fully Qualified Domain Name of this Local Node. FQDN is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character of a label. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. [Default = n/a; Range = A valid FQDN.]																																
SCTP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Local Node listens for SCTP connections.																																
SCTP Listen Port	3868	SCTP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]																																
TCP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Local Node listens for TCP connections.																																
TCP Listen Port	3868	TCP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]																																
Connection Configuration Set	Default	Connection Configuration Set of this Local Node. [Default = n/a; Range = n/a]																																
CEX Configuration Set	GyRo	CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]																																
IP Addresses	10.240.71.118 X 10.240.71.121(TSA) X - Select - X	The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries]																																
<p>11 SOAM VIP: Configure other Local Nodes, if required.</p>	<p>1 . Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). Please refer to the Diameter User's Guide ^[7] for details on the fields in this screen.</p> <p>2. Click Ok.</p> <p>NOTE: The drop down list of IP address should contain the XSI addresses configured on DSR MP Servers. If not found then Installation may be incomplete/incorrect, please contact Oracle Customer Service for further assistance.</p> <p>Repeat Step 10 and configure more Local Nodes if required.</p>																																	

12	<p>SOAM VIP: Navigate to Peer Nodes screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Peer Nodes</p>																																																												
13	<p>SOAM VIP: Configure the first CTF node</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <div style="border: 1px solid gray; padding: 5px;"> <p>Main Menu: Diameter -> Configuration -> Peer Nodes -> [Insert] Help</p> <p style="text-align: right;">Wed Jul 04 06:42:01 2012 UTC</p> <hr/> <p>Adding a new Peer node</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">Field</th> <th style="width: 45%;">Value</th> <th style="width: 40%;">Description</th> </tr> </thead> <tbody> <tr> <td>Peer Node Name</td> <td>CTF *</td> <td>Unique name of the Peer Node. [Default = n/a; Range = A 32-character string. Valid characters are letters, digits, dashes ('-'), and dots ('.'). A label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 63 characters long.</td> </tr> <tr> <td>Realm</td> <td>oracle.com *</td> <td>Realm of this Peer Node. Realm is a case-insensitive string of characters separated by dots, where a label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 63 characters long.</td> </tr> <tr> <td>FQDN</td> <td>ctf.oracle.com *</td> <td>Fully Qualified Domain Name of this Peer Node. FQDN is a string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 255 characters long.</td> </tr> <tr> <td>SCTP Enabled</td> <td><input checked="" type="checkbox"/></td> <td>If checked, indicates that this Peer Node listens for SCTP connections.</td> </tr> <tr> <td>SCTP Listen Port</td> <td>3868</td> <td>SCTP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]</td> </tr> <tr> <td>TCP Enabled</td> <td><input checked="" type="checkbox"/></td> <td>If checked, indicates that this Peer Node listens for TCP connections.</td> </tr> <tr> <td>TCP Listen Port</td> <td>3868</td> <td>TCP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]</td> </tr> <tr> <td>IP Addresses</td> <td>01 10.250.53.53 <input type="button" value="Add"/></td> <td>The IP address list of this Peer Node. [Default = n/a; Range = 1 - 128 entries]</td> </tr> <tr> <td>Alternate Implicit Route</td> <td>- Select - X</td> <td>Route List to use for routing messages to this Peer if all other routes fail.</td> </tr> <tr> <td>Replace Dest Realm</td> <td><input type="checkbox"/></td> <td>If checked, indicates that the Destination-Realm AVP of outgoing messages is replaced with this Peer Node Realm. [Default = Unchecked; Range = n/a]</td> </tr> <tr> <td>Replace Dest Host</td> <td><input type="checkbox"/></td> <td>If checked, indicates that the Destination-Host AVP of outgoing messages is replaced with this Peer Node Fully Qualified Domain Name. [Default = Unchecked; Range = n/a]</td> </tr> <tr> <td>Minimum Connection Capacity</td> <td>1 *</td> <td>The minimum number of connections that must be available for this Peer Node. Otherwise, the Peer is 'Degraded' if connections less than this value are available. [Default = 1; Range = 1 - 64 connections]</td> </tr> <tr> <td>Maximum Alternate Routing Attempts</td> <td>4 *</td> <td>The maximum number of times that a Request can be retransmitted to an alternate peer is selected. [Default = 4; Range = 1 - 4 times]</td> </tr> <tr> <td>Alternate Routing on Connection Failure</td> <td><input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer</td> <td>Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when a connection to the selected peer fails. [Default = Different Peer]</td> </tr> <tr> <td>Alternate Routing on Answer Timeout</td> <td><input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer <input type="radio"/> Same Connection</td> <td>Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when an Answer timeout occurs. [Default = Different Peer]</td> </tr> <tr> <td>Alternate Routing on Answer Result Code</td> <td><input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer</td> <td>- Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when an Answer Result Code is determined by the Diameter -> Copy Options -> DAS Answer Result Code parameter. [Default = Different Peer]</td> </tr> <tr> <td>Peer Route Table</td> <td>Default</td> <td>The Peer Route Table to be associated with this Peer Node.</td> </tr> <tr> <td>Routing Option Set</td> <td>Default</td> <td>The Routing Option Set to be associated with this Peer Node.</td> </tr> <tr> <td>Pending Answer Timer</td> <td>Default</td> <td>The Pending Answer Timer to be associated with this Peer Node.</td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></p> </div> <p>6. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values).</p> <p>Note:</p> <ul style="list-style-type: none"> - For Peer Nodes that are OCSs, the "Replace Dest Host" and "Replace Dest Realm" 	Field	Value	Description	Peer Node Name	CTF *	Unique name of the Peer Node. [Default = n/a; Range = A 32-character string. Valid characters are letters, digits, dashes ('-'), and dots ('.'). A label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 63 characters long.	Realm	oracle.com *	Realm of this Peer Node. Realm is a case-insensitive string of characters separated by dots, where a label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 63 characters long.	FQDN	ctf.oracle.com *	Fully Qualified Domain Name of this Peer Node. FQDN is a string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 255 characters long.	SCTP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Peer Node listens for SCTP connections.	SCTP Listen Port	3868	SCTP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]	TCP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Peer Node listens for TCP connections.	TCP Listen Port	3868	TCP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]	IP Addresses	01 10.250.53.53 <input type="button" value="Add"/>	The IP address list of this Peer Node. [Default = n/a; Range = 1 - 128 entries]	Alternate Implicit Route	- Select - X	Route List to use for routing messages to this Peer if all other routes fail.	Replace Dest Realm	<input type="checkbox"/>	If checked, indicates that the Destination-Realm AVP of outgoing messages is replaced with this Peer Node Realm. [Default = Unchecked; Range = n/a]	Replace Dest Host	<input type="checkbox"/>	If checked, indicates that the Destination-Host AVP of outgoing messages is replaced with this Peer Node Fully Qualified Domain Name. [Default = Unchecked; Range = n/a]	Minimum Connection Capacity	1 *	The minimum number of connections that must be available for this Peer Node. Otherwise, the Peer is 'Degraded' if connections less than this value are available. [Default = 1; Range = 1 - 64 connections]	Maximum Alternate Routing Attempts	4 *	The maximum number of times that a Request can be retransmitted to an alternate peer is selected. [Default = 4; Range = 1 - 4 times]	Alternate Routing on Connection Failure	<input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer	Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when a connection to the selected peer fails. [Default = Different Peer]	Alternate Routing on Answer Timeout	<input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer <input type="radio"/> Same Connection	Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when an Answer timeout occurs. [Default = Different Peer]	Alternate Routing on Answer Result Code	<input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer	- Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when an Answer Result Code is determined by the Diameter -> Copy Options -> DAS Answer Result Code parameter. [Default = Different Peer]	Peer Route Table	Default	The Peer Route Table to be associated with this Peer Node.	Routing Option Set	Default	The Routing Option Set to be associated with this Peer Node.	Pending Answer Timer	Default	The Pending Answer Timer to be associated with this Peer Node.
Field	Value	Description																																																												
Peer Node Name	CTF *	Unique name of the Peer Node. [Default = n/a; Range = A 32-character string. Valid characters are letters, digits, dashes ('-'), and dots ('.'). A label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 63 characters long.																																																												
Realm	oracle.com *	Realm of this Peer Node. Realm is a case-insensitive string of characters separated by dots, where a label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 63 characters long.																																																												
FQDN	ctf.oracle.com *	Fully Qualified Domain Name of this Peer Node. FQDN is a string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), a letter, digit or underscore and must end with a letter or digit as the first character. A label must be at most 255 characters long.																																																												
SCTP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Peer Node listens for SCTP connections.																																																												
SCTP Listen Port	3868	SCTP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]																																																												
TCP Enabled	<input checked="" type="checkbox"/>	If checked, indicates that this Peer Node listens for TCP connections.																																																												
TCP Listen Port	3868	TCP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]																																																												
IP Addresses	01 10.250.53.53 <input type="button" value="Add"/>	The IP address list of this Peer Node. [Default = n/a; Range = 1 - 128 entries]																																																												
Alternate Implicit Route	- Select - X	Route List to use for routing messages to this Peer if all other routes fail.																																																												
Replace Dest Realm	<input type="checkbox"/>	If checked, indicates that the Destination-Realm AVP of outgoing messages is replaced with this Peer Node Realm. [Default = Unchecked; Range = n/a]																																																												
Replace Dest Host	<input type="checkbox"/>	If checked, indicates that the Destination-Host AVP of outgoing messages is replaced with this Peer Node Fully Qualified Domain Name. [Default = Unchecked; Range = n/a]																																																												
Minimum Connection Capacity	1 *	The minimum number of connections that must be available for this Peer Node. Otherwise, the Peer is 'Degraded' if connections less than this value are available. [Default = 1; Range = 1 - 64 connections]																																																												
Maximum Alternate Routing Attempts	4 *	The maximum number of times that a Request can be retransmitted to an alternate peer is selected. [Default = 4; Range = 1 - 4 times]																																																												
Alternate Routing on Connection Failure	<input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer	Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when a connection to the selected peer fails. [Default = Different Peer]																																																												
Alternate Routing on Answer Timeout	<input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer <input type="radio"/> Same Connection	Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when an Answer timeout occurs. [Default = Different Peer]																																																												
Alternate Routing on Answer Result Code	<input type="radio"/> Same Peer <input checked="" type="radio"/> Different Peer	- Whether or not to perform alternate routing on alternate peers when selecting the next eligible peer of a Peer Route Group when an Answer Result Code is determined by the Diameter -> Copy Options -> DAS Answer Result Code parameter. [Default = Different Peer]																																																												
Peer Route Table	Default	The Peer Route Table to be associated with this Peer Node.																																																												
Routing Option Set	Default	The Routing Option Set to be associated with this Peer Node.																																																												
Pending Answer Timer	Default	The Pending Answer Timer to be associated with this Peer Node.																																																												

	<p>check boxes MUST be checked.</p> <ul style="list-style-type: none"> - "Topology Hiding Status" field is not applicable for PCA and should remain disabled. - The "Application Route Table" may apply for Peer Nodes that are CTFs. - The "Peer Route Table" field may be populated to route to Shared State OCSs. - For mode details on the fields and routing configuration please consult the Diameter User's Guide ^[7] <p>7. Click Ok.</p>
<p>14 SOAM VIP: Configure other Peer Nodes</p>	<p>Repeat Step 13 to configure other CTF and OCS peer nodes as required.</p>
<p>15 SOAM VIP: Navigate to Connections screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Connections</p>
<p>16 SOAM VIP: Configure the connection with CTF Node</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> 

	<table border="1"> <tr> <td>Transport FQDN</td> <td><input type="text"/></td> <td>Fully Qualified Domain Name for this connection. FQDN is a c label may contain letters, digits, dashes (-) and underscore (_), letter or digit. Underscores may be used only as the first chara 255 characters long. [Default = n/a; Range = A valid FQDN]</td> </tr> <tr> <td>Connection Configuration Set</td> <td>Default ▾ +</td> <td>The configuration set of this Connection.</td> </tr> <tr> <td>CEX Configuration Set</td> <td>GyRo ▾</td> <td>CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]</td> </tr> <tr> <td>Capacity Configuration Set</td> <td>Default ▾ +</td> <td>The Capacity Configuration Set used for this Connection. The Capacity Configuration Set defines reserved and maximum connection. [Default = Default; Range = A 32-character string. Valid charac must not start with a digit.]</td> </tr> <tr> <td>Remote Busy Usage</td> <td>Disabled ▾ +</td> <td>Defines which Request messages can be forwarded on this c connection's Peer. 'Disabled' - The Connection is not considered to be BUSY after continue to be forwarded to (or rerouted to) this connection. 'Enabled' - The Connection is considered to be BUSY after rec forwarded to (or rerouted to) this connection until the Remote E 'Host Override' - The Connection is considered to be BUSY after whose Destination-Host AVP value is the same as the connec Remote Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled, Host Overrid</td> </tr> <tr> <td>Remote Busy Abatement Timeout</td> <td><input type="text"/></td> <td>Defines the time period (in seconds) that a Connection will be received. [Default = 3; Range = 3 - 60 secs]</td> </tr> <tr> <td>Test Mode</td> <td><input type="checkbox"/></td> <td>If checked, indicates that connection is in test mode. [Default = unchecked; Range = n/a]</td> </tr> </table>	Transport FQDN	<input type="text"/>	Fully Qualified Domain Name for this connection. FQDN is a c label may contain letters, digits, dashes (-) and underscore (_), letter or digit. Underscores may be used only as the first chara 255 characters long. [Default = n/a; Range = A valid FQDN]	Connection Configuration Set	Default ▾ +	The configuration set of this Connection.	CEX Configuration Set	GyRo ▾	CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]	Capacity Configuration Set	Default ▾ +	The Capacity Configuration Set used for this Connection. The Capacity Configuration Set defines reserved and maximum connection. [Default = Default; Range = A 32-character string. Valid charac must not start with a digit.]	Remote Busy Usage	Disabled ▾ +	Defines which Request messages can be forwarded on this c connection's Peer. 'Disabled' - The Connection is not considered to be BUSY after continue to be forwarded to (or rerouted to) this connection. 'Enabled' - The Connection is considered to be BUSY after rec forwarded to (or rerouted to) this connection until the Remote E 'Host Override' - The Connection is considered to be BUSY after whose Destination-Host AVP value is the same as the connec Remote Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled, Host Overrid	Remote Busy Abatement Timeout	<input type="text"/>	Defines the time period (in seconds) that a Connection will be received. [Default = 3; Range = 3 - 60 secs]	Test Mode	<input type="checkbox"/>	If checked, indicates that connection is in test mode. [Default = unchecked; Range = n/a]
Transport FQDN	<input type="text"/>	Fully Qualified Domain Name for this connection. FQDN is a c label may contain letters, digits, dashes (-) and underscore (_), letter or digit. Underscores may be used only as the first chara 255 characters long. [Default = n/a; Range = A valid FQDN]																				
Connection Configuration Set	Default ▾ +	The configuration set of this Connection.																				
CEX Configuration Set	GyRo ▾	CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]																				
Capacity Configuration Set	Default ▾ +	The Capacity Configuration Set used for this Connection. The Capacity Configuration Set defines reserved and maximum connection. [Default = Default; Range = A 32-character string. Valid charac must not start with a digit.]																				
Remote Busy Usage	Disabled ▾ +	Defines which Request messages can be forwarded on this c connection's Peer. 'Disabled' - The Connection is not considered to be BUSY after continue to be forwarded to (or rerouted to) this connection. 'Enabled' - The Connection is considered to be BUSY after rec forwarded to (or rerouted to) this connection until the Remote E 'Host Override' - The Connection is considered to be BUSY after whose Destination-Host AVP value is the same as the connec Remote Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled, Host Overrid																				
Remote Busy Abatement Timeout	<input type="text"/>	Defines the time period (in seconds) that a Connection will be received. [Default = 3; Range = 3 - 60 secs]																				
Test Mode	<input type="checkbox"/>	If checked, indicates that connection is in test mode. [Default = unchecked; Range = n/a]																				
	<p>8. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). Note: Please refer to the Diameter User's Guide^[7] for details on fields in this screen</p> <p>9. Click Ok.</p> <p>NOTE: Make sure the IPFE configuration matches the Transport Protocol which is selected in this step.</p>																					
<p>17 SOAM VIP: Configure all other connection with Peer nodes</p>	<p>Repeat Step 16 to configure all other required connections.</p>																					
<p>18 SOAM VIP: Configure Route Groups</p>	<p>If Online Charging DRA is configured to run in Single Pool Mode, Destination Host will not be populated in the CCR-Initiate Diameter message. The user needs to configure Routing Rules based on Origin-Host or route all new session creation messages to a single Pool of OCSs. In either case, primary and alternate routing groups may be configured and prioritized.</p> <p>If Online Charging DRA is configured to run in Multiple Pool Mode, Destination Host will be present in the Diameter CCR-Initiate message. Destination-Host based routing rules may be configured in this case.</p> <p>The Routing configuration shown below takes an example of Multiple Pool Mode OCS Selection.</p>																					
<p>19 SOAM VIP: Configure the Primary Route Group for the first OCS Pool.</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Route Groups</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																					

	<p>Main Menu: Diameter -> Configuration -> Route Groups -> [Insert] Help Tue Feb 28 03:04:11 2012 EST</p> <p>Adding a new route group</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Route Group Name</td> <td>ocsRouteGroup</td> <td>A name that uniquely identifies the Route Group. (Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit)</td> </tr> <tr> <td>Type</td> <td><input checked="" type="radio"/> Peer Route Group <input type="radio"/> Connection Route Group</td> <td>A Route Group can be provisioned as a set of Peers (PRG) or Connections (C) that have the same priority within a Route List.</td> </tr> <tr> <td rowspan="2">Peer Node, Connection and Capacity</td> <td>Peer Node</td> <td>Peer Nodes associated with this Route Group. (Default = n/a; Range = 1 - 64 entries)</td> </tr> <tr> <td>Connection</td> <td>Connections associated with this Route Group. (Default = n/a; Range = 1 - 64 entries)</td> </tr> <tr> <td></td> <td>Provisioned Capacity</td> <td>Provisioned Capacity of the Peer Node/Connection within this Route Group. Traffic is distributed to available Peer Nodes/Connections within a Route Group proportional to the Peer Node's/Connection's provisioned capacity. (Default = n/a; Range = 1 - 64000)</td> </tr> </tbody> </table> <p>01 OCS -Select- 1 X Add</p> <p>Ok Apply Cancel</p> <ol style="list-style-type: none"> 1. Enter the Route Group name. 2. Select the Peer Node name (OCS name). 3. If more OCSs need to be added to this Route Group click on Add and repeat step 2. 4. Enter the provisioned capacity as 1. 5. Click Ok. 	Field	Value	Description	Route Group Name	ocsRouteGroup	A name that uniquely identifies the Route Group. (Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit)	Type	<input checked="" type="radio"/> Peer Route Group <input type="radio"/> Connection Route Group	A Route Group can be provisioned as a set of Peers (PRG) or Connections (C) that have the same priority within a Route List.	Peer Node, Connection and Capacity	Peer Node	Peer Nodes associated with this Route Group. (Default = n/a; Range = 1 - 64 entries)	Connection	Connections associated with this Route Group. (Default = n/a; Range = 1 - 64 entries)		Provisioned Capacity	Provisioned Capacity of the Peer Node/Connection within this Route Group. Traffic is distributed to available Peer Nodes/Connections within a Route Group proportional to the Peer Node's/Connection's provisioned capacity. (Default = n/a; Range = 1 - 64000)
Field	Value	Description																
Route Group Name	ocsRouteGroup	A name that uniquely identifies the Route Group. (Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit)																
Type	<input checked="" type="radio"/> Peer Route Group <input type="radio"/> Connection Route Group	A Route Group can be provisioned as a set of Peers (PRG) or Connections (C) that have the same priority within a Route List.																
Peer Node, Connection and Capacity	Peer Node	Peer Nodes associated with this Route Group. (Default = n/a; Range = 1 - 64 entries)																
	Connection	Connections associated with this Route Group. (Default = n/a; Range = 1 - 64 entries)																
	Provisioned Capacity	Provisioned Capacity of the Peer Node/Connection within this Route Group. Traffic is distributed to available Peer Nodes/Connections within a Route Group proportional to the Peer Node's/Connection's provisioned capacity. (Default = n/a; Range = 1 - 64000)																
<p>20 SOAM VIP: Configure the Alternate Route Group(s) for the same OCS Pool.</p>	<p>OPTIONAL</p> <p>If alternate Route Group(s) are planned, repeat step 19 for all such Route Groups.</p>																	
<p>21 SOAM VIP: Configure the Route List for the first OCS Pool</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Route Lists</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																	

	<table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Route List Name</td> <td>Pool1_RL1 *</td> </tr> <tr> <td>Minimum Route Group Availability Weight</td> <td>1 *</td> </tr> <tr> <td>Route Across Route Groups</td> <td> <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled </td> </tr> <tr> <td rowspan="3">Route Group, Priority , Traffic Throttle Group and Maximum Loss Percent Threshold</td> <td> Route Group: RG1 * Priority: 1 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add </td> </tr> <tr> <td> Route Group: RG2 Priority: 2 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add </td> </tr> <tr> <td> Route Group: Priority: <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add </td> </tr> </tbody> </table> <ol style="list-style-type: none"> 1. Enter the Route List name. 2. Set the Minimum Route Group Availability Weight as needed. 3. Select the Route Group(s) configured in the previous two steps and set their desired priorities. 4. Set any other parameters desired (for e.g. Maximum Loss Percent Threshold etc.) 5. Click Ok. 	Field	Value	Route List Name	Pool1_RL1 *	Minimum Route Group Availability Weight	1 *	Route Across Route Groups	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Route Group, Priority , Traffic Throttle Group and Maximum Loss Percent Threshold	Route Group: RG1 * Priority: 1 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01			Route Group: RG2 Priority: 2 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01			Route Group: Priority: <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01		
Field	Value																														
Route List Name	Pool1_RL1 *																														
Minimum Route Group Availability Weight	1 *																														
Route Across Route Groups	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled																														
Route Group, Priority , Traffic Throttle Group and Maximum Loss Percent Threshold	Route Group: RG1 * Priority: 1 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01																										
	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold																												
	01																														
Route Group: RG2 Priority: 2 <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01																											
Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold																													
01																															
Route Group: Priority: <table border="1"> <thead> <tr> <th>Site Name</th> <th>Traffic Throttle Group</th> <th>Maximum Loss Percent Threshold</th> </tr> </thead> <tbody> <tr> <td>01</td> <td></td> <td></td> </tr> </tbody> </table> Add	Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold	01																											
Site Name	Traffic Throttle Group	Maximum Loss Percent Threshold																													
01																															
<p>22 SOAM VIP: Configure Routing Rules for the first OCS Pool</p>	<p>Configure the Default PRT such that DSR forwards messages based on the OCS Pool selected by PCA.</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Peer Route Table</p> <p>Select the Default Peer Route Table and Click Edit</p> <p>You will see a screen similar to:</p>																														

	<table border="1"> <tr> <td>Rule Name</td> <td>Pool1_Rule1 *</td> <td>Unique name of the Rule. [Default = n/a; Range = A 32-c a digit]</td> </tr> <tr> <td>Peer Route Table</td> <td>Pool1_PRT *</td> <td>Peer Route Table associated</td> </tr> <tr> <td>Priority</td> <td>1 *</td> <td>Priority of this Rule. Low value means higher priority [Default = n/a; Range = 1 - 10]</td> </tr> <tr> <td>Conditions</td> <td> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Destination-Host</td> <td>Equals</td> <td>ocs1.oracle.com</td> <td>AND</td> </tr> <tr> <td>Application-Id</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table> </td> <td> <p>Conditions associated with this Rule. Each condition has three parts. In order for a Diameter message to match the criteria of this rule, it must match the criteria of every condition. [Default = n/a; Range = 0-429]</p> <p>Command Code: [Default = n/a; Range = 0-167]</p> <p>Destination-Realm and Origin-Host is a case-insensitive string where a label may contain letters, digits, hyphens, and underscores. A label must start with a letter, and a label must be at most 63 characters long. [Default = n/a; Range = Sub string]</p> <p>Destination-Host and Origin-Host is a case-insensitive string where a label may contain letters, digits, hyphens, and underscores. A label must start with a letter, and a label must be at most 63 characters long. [Default = n/a; Range = Sub string]</p> </td> </tr> <tr> <td>Action</td> <td> <input checked="" type="radio"/> Route to Peer <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer </td> <td>Action associated with this Rule. Route to Peer will route message. Send Answer will abandon message. Abandon With No Answer will abandon message.</td> </tr> <tr> <td>Route List</td> <td>RL1</td> <td>Route List associated with this Rule. Route List is required if Action is 'Route to Peer'.</td> </tr> <tr> <td>Message Priority</td> <td>No Change</td> <td>The priority of the message to be sent. Message priority only when the 'Action' field is 'Route to Peer'.</td> </tr> <tr> <td>Message Copy Configuration Set</td> <td>- Select -</td> <td>Message Copy Configuration Set (Rule) for copy to the DAS. [Default = n/a]</td> </tr> <tr> <td>Answer Result-Code Value</td> <td>- Select -</td> <td>Value to be placed in the Result-Code field of the Answer. Answer Result-Code Value is required. [Default = n/a; Range = 1000 - 599]</td> </tr> <tr> <td>Vendor Id</td> <td></td> <td>Vendor Id Value. Vendor Id will be placed in Vendor-Id field. [Default = n/a; Range = 1 - 429496]</td> </tr> <tr> <td>Answer Error Message</td> <td></td> <td>String to be placed in the Error-Message field. [Default = null string; Range = 0 to 255]</td> </tr> </table> <p>1. Enter the Rule name. 2. Set the Priority of the Rule as needed (preferably 1). 3. Select the Operator as "Equals" for Destination-Host Condition Parameter and enter the Destination-Host (FQDN) that will be populated by RBAR or any other DSR Application for the first OCS Pool. 3. Select "Always True" for the remaining Condition Parameters. You may base the OCS Pool routing on some condition parameters in special use cases for example Origin-based routing. 3. Select the Route List configured in step 21. 4. Click Ok.</p>	Rule Name	Pool1_Rule1 *	Unique name of the Rule. [Default = n/a; Range = A 32-c a digit]	Peer Route Table	Pool1_PRT *	Peer Route Table associated	Priority	1 *	Priority of this Rule. Low value means higher priority [Default = n/a; Range = 1 - 10]	Conditions	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Destination-Host</td> <td>Equals</td> <td>ocs1.oracle.com</td> <td>AND</td> </tr> <tr> <td>Application-Id</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table>	Parameter	Operator	Value		Destination-Realm	Always True		AND	Destination-Host	Equals	ocs1.oracle.com	AND	Application-Id	Always True	- Select -	AND	Command-Code	Always True	- Select -	AND	Origin-Realm	Always True		AND	Origin-Host	Always True			<p>Conditions associated with this Rule. Each condition has three parts. In order for a Diameter message to match the criteria of this rule, it must match the criteria of every condition. [Default = n/a; Range = 0-429]</p> <p>Command Code: [Default = n/a; Range = 0-167]</p> <p>Destination-Realm and Origin-Host is a case-insensitive string where a label may contain letters, digits, hyphens, and underscores. A label must start with a letter, and a label must be at most 63 characters long. [Default = n/a; Range = Sub string]</p> <p>Destination-Host and Origin-Host is a case-insensitive string where a label may contain letters, digits, hyphens, and underscores. A label must start with a letter, and a label must be at most 63 characters long. [Default = n/a; Range = Sub string]</p>	Action	<input checked="" type="radio"/> Route to Peer <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer	Action associated with this Rule. Route to Peer will route message. Send Answer will abandon message. Abandon With No Answer will abandon message.	Route List	RL1	Route List associated with this Rule. Route List is required if Action is 'Route to Peer'.	Message Priority	No Change	The priority of the message to be sent. Message priority only when the 'Action' field is 'Route to Peer'.	Message Copy Configuration Set	- Select -	Message Copy Configuration Set (Rule) for copy to the DAS. [Default = n/a]	Answer Result-Code Value	- Select -	Value to be placed in the Result-Code field of the Answer. Answer Result-Code Value is required. [Default = n/a; Range = 1000 - 599]	Vendor Id		Vendor Id Value. Vendor Id will be placed in Vendor-Id field. [Default = n/a; Range = 1 - 429496]	Answer Error Message		String to be placed in the Error-Message field. [Default = null string; Range = 0 to 255]
Rule Name	Pool1_Rule1 *	Unique name of the Rule. [Default = n/a; Range = A 32-c a digit]																																																												
Peer Route Table	Pool1_PRT *	Peer Route Table associated																																																												
Priority	1 *	Priority of this Rule. Low value means higher priority [Default = n/a; Range = 1 - 10]																																																												
Conditions	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Destination-Host</td> <td>Equals</td> <td>ocs1.oracle.com</td> <td>AND</td> </tr> <tr> <td>Application-Id</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table>	Parameter	Operator	Value		Destination-Realm	Always True		AND	Destination-Host	Equals	ocs1.oracle.com	AND	Application-Id	Always True	- Select -	AND	Command-Code	Always True	- Select -	AND	Origin-Realm	Always True		AND	Origin-Host	Always True			<p>Conditions associated with this Rule. Each condition has three parts. In order for a Diameter message to match the criteria of this rule, it must match the criteria of every condition. [Default = n/a; Range = 0-429]</p> <p>Command Code: [Default = n/a; Range = 0-167]</p> <p>Destination-Realm and Origin-Host is a case-insensitive string where a label may contain letters, digits, hyphens, and underscores. A label must start with a letter, and a label must be at most 63 characters long. [Default = n/a; Range = Sub string]</p> <p>Destination-Host and Origin-Host is a case-insensitive string where a label may contain letters, digits, hyphens, and underscores. A label must start with a letter, and a label must be at most 63 characters long. [Default = n/a; Range = Sub string]</p>																																
Parameter	Operator	Value																																																												
Destination-Realm	Always True		AND																																																											
Destination-Host	Equals	ocs1.oracle.com	AND																																																											
Application-Id	Always True	- Select -	AND																																																											
Command-Code	Always True	- Select -	AND																																																											
Origin-Realm	Always True		AND																																																											
Origin-Host	Always True																																																													
Action	<input checked="" type="radio"/> Route to Peer <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer	Action associated with this Rule. Route to Peer will route message. Send Answer will abandon message. Abandon With No Answer will abandon message.																																																												
Route List	RL1	Route List associated with this Rule. Route List is required if Action is 'Route to Peer'.																																																												
Message Priority	No Change	The priority of the message to be sent. Message priority only when the 'Action' field is 'Route to Peer'.																																																												
Message Copy Configuration Set	- Select -	Message Copy Configuration Set (Rule) for copy to the DAS. [Default = n/a]																																																												
Answer Result-Code Value	- Select -	Value to be placed in the Result-Code field of the Answer. Answer Result-Code Value is required. [Default = n/a; Range = 1000 - 599]																																																												
Vendor Id		Vendor Id Value. Vendor Id will be placed in Vendor-Id field. [Default = n/a; Range = 1 - 429496]																																																												
Answer Error Message		String to be placed in the Error-Message field. [Default = null string; Range = 0 to 255]																																																												
<p>23</p>	<p>SOAM VIP: Configure Routing for other OCS Pools.</p>	<p>If more, OCS Pools are planned in the Diameter network, repeat steps 19 through 22 for other OCS Pools' Routing</p>																																																												
<p>24</p>	<p>SOAM VIP: Configure inter DSR Routing</p>	<p>OPTIONAL</p> <p>If Diameter messages need to be routed in between DSR sites (nodes), set up the routing as needed.</p> <p>This is likely in 3-site redundancy deployments because many CTFs likely only support primary and secondary connections. In such deployments routing can be set up between the three sites.</p>																																																												
<p>25</p>	<p>SOAM VIP: Configure PRT rules for all other OCSs</p>	<p>Repeat from step 28 for all other OCSs connected to this DSR. This Routing configuration will ensure that whenever PCA requests DSR to route to a particular OCS based on PRT, DSR will route to it if the OCS is available, however, if not, it will route the message to any other available OCS.</p>																																																												
<p>26</p>	<p>SOAM VIP: Navigate to the Application Routing Rules screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Application Routing Rules</p> <p>You will see a screen similar to:</p>																																																												

	<p>Main Menu: Diameter -> Configuration -> Application Route Tables Mon 8</p> <p>Filter ▾</p> <table border="1"><thead><tr><th>Application Route Table Name</th><th>Number of Rules</th></tr></thead><tbody><tr><td>Default</td><td>0</td></tr></tbody></table> <p style="text-align: center;">◆◆</p> <p>Insert Delete View / Edit Rules</p> <p>1. Select the Default Application Route Table Name to which rules are to be added. 2. Click on View/Edit Rules button.</p>	Application Route Table Name	Number of Rules	Default	0
Application Route Table Name	Number of Rules				
Default	0				
<p>27 SOAM VIP: Configure the ART for GyRo Interface messages</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>				

Inserting Rule for Application Route Table: Default																													
Field	Value																												
Rule Name	GyRoRule *																												
Application Route Table	Default *																												
Priority	1 *																												
Conditions	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Destination-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Destination-Host</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Application-Id</td> <td>Equals</td> <td>4 - Diameter Credit Control</td> <td>AND</td> </tr> <tr> <td>Command-Code</td> <td>Always True</td> <td>- Select -</td> <td>AND</td> </tr> <tr> <td>Origin-Realm</td> <td>Always True</td> <td></td> <td>AND</td> </tr> <tr> <td>Origin-Host</td> <td>Always True</td> <td></td> <td></td> </tr> </tbody> </table>	Parameter	Operator	Value		Destination-Realm	Always True		AND	Destination-Host	Always True		AND	Application-Id	Equals	4 - Diameter Credit Control	AND	Command-Code	Always True	- Select -	AND	Origin-Realm	Always True		AND	Origin-Host	Always True		
Parameter	Operator	Value																											
Destination-Realm	Always True		AND																										
Destination-Host	Always True		AND																										
Application-Id	Equals	4 - Diameter Credit Control	AND																										
Command-Code	Always True	- Select -	AND																										
Origin-Realm	Always True		AND																										
Origin-Host	Always True																												
Action	<input checked="" type="radio"/> Route to Application <input type="radio"/> Forward To Egress Routing <input type="radio"/> Send Answer <input type="radio"/> Abandon With No Answer																												
Answer Result-Code Value	<input type="radio"/> - Select - <input type="radio"/>																												
Vendor Id																													
Answer Error Message																													
Application Name	PCA																												
Gx-Prime	<input type="checkbox"/>																												
<input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>																													
1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). 2. Click Ok .																													
28 SOAM VIP: Configure the ART for all other Interfaces	Repeat Step 26 for any other Application Id that needs to be routed to the PCA Application by Diameter Routing Layer.																												

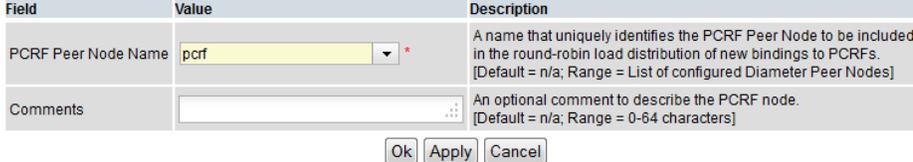
4.4 PCA FUNCTION CONFIGURATION PROCEDURES

This section provides the detailed procedure steps of the PCA configuration execution.

4.4.1 Policy DRA Configuration

Detailed steps are given in the procedure below.

Procedure 15: Policy DRA configuration

S T E P #	<p>This procedure configures the Policy DRA function of PCA application. For details on the fields of various configuration screens please refer to the Policy Charging User's Guide ^[4].</p> <p>PRE-REQUISITE: Procedure 13 must be executed before this procedure.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>										
	1	<p>Establish GUI Session on the SOAM VIP</p> <p>Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".</p>									
	2	<p>SOAM VIP: Navigate to PCRFs screen</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRFs</p>									
	3	<p>SOAM VIP: Configure the first PCRF node.</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRFs -> [Insert] </p> <p>Adding a new PCRF</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>PCRF Peer Node Name</td> <td>pcrf</td> <td>A name that uniquely identifies the PCRF Peer Node to be included in the round-robin load distribution of new bindings to PCRFs. [Default = n/a; Range = List of configured Diameter Peer Nodes]</td> </tr> <tr> <td>Comments</td> <td></td> <td>An optional comment to describe the PCRF node. [Default = n/a; Range = 0-64 characters]</td> </tr> </tbody> </table> <p style="text-align: center;">Ok Apply Cancel</p> <p>1. Select the PCRF name from the drop down 2. Click Ok.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Field	Value	Description	PCRF Peer Node Name	pcrf	A name that uniquely identifies the PCRF Peer Node to be included in the round-robin load distribution of new bindings to PCRFs. [Default = n/a; Range = List of configured Diameter Peer Nodes]	Comments		An optional comment to describe the PCRF node. [Default = n/a; Range = 0-64 characters]
	Field	Value	Description								
PCRF Peer Node Name	pcrf	A name that uniquely identifies the PCRF Peer Node to be included in the round-robin load distribution of new bindings to PCRFs. [Default = n/a; Range = List of configured Diameter Peer Nodes]									
Comments		An optional comment to describe the PCRF node. [Default = n/a; Range = 0-64 characters]									
4	<p>SOAM VIP: Configure all other PCRF nodes.</p> <p>Repeat Step 3 to configure all the PCRF nodes.</p>										
5	<p>SOAM VIP: Navigate to Binding Key Priority screen</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Binding Key Priority</p> <p>You will see a screen similar to:</p>										

	<p>Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Binding Key Priority</p> <p style="text-align: right;">Mon Aug 18 14:18:44 2014</p> <p>Table Description: The Binding Key Priority table defines search priorities for binding keys that can be used to locate a subscriber binding for Binding Dependent sessions of Gx-Prime and Rx diameter interfaces. The priority determines the order used to find a binding for subsequent sessions. The alternative binding keys must be assigned below in order to be used to locate subscriber bindings. If any alternative binding key not assigned a priority, they will not be used to locate subscriber bindings, even if the key is present in the Diameter message.</p> <table border="1"> <thead> <tr> <th>Priority</th> <th>Binding Key Type</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>IPv6 Address ▾ *</td> </tr> <tr> <td>2</td> <td>IPv4 Address ▾</td> </tr> <tr> <td>3</td> <td>- Select - ▾</td> </tr> <tr> <td>4</td> <td>- Select - ▾</td> </tr> </tbody> </table> <p style="text-align: right;">Apply Cancel</p>	Priority	Binding Key Type	1	IPv6 Address ▾ *	2	IPv4 Address ▾	3	- Select - ▾	4	- Select - ▾
Priority	Binding Key Type										
1	IPv6 Address ▾ *										
2	IPv4 Address ▾										
3	- Select - ▾										
4	- Select - ▾										
<p>6</p> <p>SOAM VIP: Configure the Binding Key Priorities</p>	<p>1. Select the Binding Keys priority as appropriate</p> <p>2. Click Apply.</p>										
<p>7</p> <p>NOAM VIP: Navigate to Topology Hiding screen</p>	<p>OPTIONAL</p> <p>If Topology Hiding feature is required execute Steps 7 through 11. Else skip to Step 12</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options</p> <div data-bbox="516 890 1416 1297"> <p>Topology Hiding Options</p> <table border="1"> <tr> <td>Enable Topology Hiding</td> <td><input checked="" type="checkbox"/></td> <td>Enable or disable topology hiding using the check box. Once enabled or disabled here, the Topology Hiding is enabled or disabled at all SOAMs under this NOAM. [Default = Disabled (unchecked); Range = Enabled (checked), Disabled (unchecked)]</td> </tr> <tr> <td>Topology Hiding Scope</td> <td>- Select - ▾</td> <td>This sets the scope of messages where topology hiding will be applied. Select 'All Messages' to perform topology hiding for all messages destined to policy clients. Select 'All Foreign Realms' to perform topology hiding for messages destined to the policy clients whose realms are different from the realm of the PCRF to be bound. Select 'Specific Clients' to perform topology hiding for the policy clients that are configured in one of SOAM GUI Main Menu: Policy and Charging->Configuration->Policy DRA->Policy Clients screen. Select 'All Foreign Realms + Specific Clients' to perform topology hiding if either condition ('All Foreign Realms' or 'Specific Clients') is met. [Default = n/a; Range = All Messages, All Foreign Realms, Specific Clients, All Foreign Realms + Specific Clients]</td> </tr> <tr> <td>Default Topology Hiding Virtual Name</td> <td>FQDN: _____ Realm: _____</td> <td>FQDN: This FQDN is used as a default value in the Origin-Host AVP for answer messages routed from a PCRF to a policy client, or in the Destination-Host AVP for request messages routed from a PCRF to a policy client, only if Topology Hiding Virtual Name FQDN is not configured at a SOAM relevant to the policy client and PCRF. Realm: This Realm is used as a default value in the Origin-Realm AVP for answer messages routed from a PCRF to a policy client, or in the Destination-Realm AVP for request messages routed from a PCRF to a policy client, only if Topology Hiding Virtual Name Realm is not configured at a SOAM relevant to the policy client and PCRF. [Default = n/a; Range = FQDN and Realm: a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as</td> </tr> </table> </div> <p>In the Topology Hiding Options section:</p> <ol style="list-style-type: none"> 1. Check the Enable Topology Hiding checkbox. 2. Select the Topology Hiding Scope from the dropdown. 3. Enter the default Virtual FQDN and Realm to be used in Topology Hidden messages. These are default values that can be overridden by site configuration. 4. Click Ok. <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Enable Topology Hiding	<input checked="" type="checkbox"/>	Enable or disable topology hiding using the check box. Once enabled or disabled here, the Topology Hiding is enabled or disabled at all SOAMs under this NOAM. [Default = Disabled (unchecked); Range = Enabled (checked), Disabled (unchecked)]	Topology Hiding Scope	- Select - ▾	This sets the scope of messages where topology hiding will be applied. Select 'All Messages' to perform topology hiding for all messages destined to policy clients. Select 'All Foreign Realms' to perform topology hiding for messages destined to the policy clients whose realms are different from the realm of the PCRF to be bound. Select 'Specific Clients' to perform topology hiding for the policy clients that are configured in one of SOAM GUI Main Menu: Policy and Charging->Configuration->Policy DRA->Policy Clients screen. Select 'All Foreign Realms + Specific Clients' to perform topology hiding if either condition ('All Foreign Realms' or 'Specific Clients') is met. [Default = n/a; Range = All Messages, All Foreign Realms, Specific Clients, All Foreign Realms + Specific Clients]	Default Topology Hiding Virtual Name	FQDN: _____ Realm: _____	FQDN: This FQDN is used as a default value in the Origin-Host AVP for answer messages routed from a PCRF to a policy client, or in the Destination-Host AVP for request messages routed from a PCRF to a policy client, only if Topology Hiding Virtual Name FQDN is not configured at a SOAM relevant to the policy client and PCRF. Realm: This Realm is used as a default value in the Origin-Realm AVP for answer messages routed from a PCRF to a policy client, or in the Destination-Realm AVP for request messages routed from a PCRF to a policy client, only if Topology Hiding Virtual Name Realm is not configured at a SOAM relevant to the policy client and PCRF. [Default = n/a; Range = FQDN and Realm: a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as	
Enable Topology Hiding	<input checked="" type="checkbox"/>	Enable or disable topology hiding using the check box. Once enabled or disabled here, the Topology Hiding is enabled or disabled at all SOAMs under this NOAM. [Default = Disabled (unchecked); Range = Enabled (checked), Disabled (unchecked)]									
Topology Hiding Scope	- Select - ▾	This sets the scope of messages where topology hiding will be applied. Select 'All Messages' to perform topology hiding for all messages destined to policy clients. Select 'All Foreign Realms' to perform topology hiding for messages destined to the policy clients whose realms are different from the realm of the PCRF to be bound. Select 'Specific Clients' to perform topology hiding for the policy clients that are configured in one of SOAM GUI Main Menu: Policy and Charging->Configuration->Policy DRA->Policy Clients screen. Select 'All Foreign Realms + Specific Clients' to perform topology hiding if either condition ('All Foreign Realms' or 'Specific Clients') is met. [Default = n/a; Range = All Messages, All Foreign Realms, Specific Clients, All Foreign Realms + Specific Clients]									
Default Topology Hiding Virtual Name	FQDN: _____ Realm: _____	FQDN: This FQDN is used as a default value in the Origin-Host AVP for answer messages routed from a PCRF to a policy client, or in the Destination-Host AVP for request messages routed from a PCRF to a policy client, only if Topology Hiding Virtual Name FQDN is not configured at a SOAM relevant to the policy client and PCRF. Realm: This Realm is used as a default value in the Origin-Realm AVP for answer messages routed from a PCRF to a policy client, or in the Destination-Realm AVP for request messages routed from a PCRF to a policy client, only if Topology Hiding Virtual Name Realm is not configured at a SOAM relevant to the policy client and PCRF. [Default = n/a; Range = FQDN and Realm: a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as									
<p>8</p> <p>SOAM VIP: Configure the Peer node for which PCRF identity needs to be hidden</p>	<p>OPTIONAL</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Policy Clients</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>										

		<p>Adding a new Policy Client</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Policy Client Peer Node Name</td> <td><input type="text"/></td> <td>A name that uniquely identifies the Policy Client Peer Node from which PCRF names should be hidden. While configured in SOAM GUI, the Policy Client Peer Node Name is written to NOAM and is available globally within the NOAM topology. [Default = n/a; Range = List of configured Diameter Peer Nodes]</td> </tr> <tr> <td>Topology Hiding Enabled</td> <td><input checked="" type="checkbox"/></td> <td>A read-only check box with default 'checked' to indicate the Topology Hiding for the policy client peer node being enabled. It is the only option currently supported. [Default = Enabled (checked); Range = n/a (Read-Only)]</td> </tr> <tr> <td>Comments</td> <td><input type="text"/></td> <td>An optional comment to describe the Policy Client Peer Node. [Default = n/a; Range: 0-64 characters]</td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></p> <p>1. Select the (policy client) node name from the list for which the PCRF identity needs to be hidden</p> <p>2. Click Ok.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Field	Value	Description	Policy Client Peer Node Name	<input type="text"/>	A name that uniquely identifies the Policy Client Peer Node from which PCRF names should be hidden. While configured in SOAM GUI, the Policy Client Peer Node Name is written to NOAM and is available globally within the NOAM topology. [Default = n/a; Range = List of configured Diameter Peer Nodes]	Topology Hiding Enabled	<input checked="" type="checkbox"/>	A read-only check box with default 'checked' to indicate the Topology Hiding for the policy client peer node being enabled. It is the only option currently supported. [Default = Enabled (checked); Range = n/a (Read-Only)]	Comments	<input type="text"/>	An optional comment to describe the Policy Client Peer Node. [Default = n/a; Range: 0-64 characters]						
Field	Value	Description																		
Policy Client Peer Node Name	<input type="text"/>	A name that uniquely identifies the Policy Client Peer Node from which PCRF names should be hidden. While configured in SOAM GUI, the Policy Client Peer Node Name is written to NOAM and is available globally within the NOAM topology. [Default = n/a; Range = List of configured Diameter Peer Nodes]																		
Topology Hiding Enabled	<input checked="" type="checkbox"/>	A read-only check box with default 'checked' to indicate the Topology Hiding for the policy client peer node being enabled. It is the only option currently supported. [Default = Enabled (checked); Range = n/a (Read-Only)]																		
Comments	<input type="text"/>	An optional comment to describe the Policy Client Peer Node. [Default = n/a; Range: 0-64 characters]																		
9	<p>SOAM VIP: Configure other Peer nodes for which PCRF identity needs to be hidden</p>	<p>OPTIONAL</p> <p>Repeat Step 8 for all (policy client) nodes for which the PCRF identity needs to be hidden.</p>																		
10	<p>SOAM VIP: Navigate to PCA Site Options screen</p>	<p>OPTIONAL</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Site Options</p>																		
11	<p>SOAM VIP: Configure the Topology Hiding Virtual FQDN and Realm.</p>	<p>OPTIONAL</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Topology Hiding Virtual Name</td> <td>FQDN: <input type="text"/> Realm: <input type="text"/></td> <td>FQDN: This value is used to populate the Diameter Origin-Host AVP for answer messages routed from a PCRF to a policy client, or the Diameter Destination-Host AVP for request messages routed from a PCRF to a policy client. If no value is configured here when Topology Hiding is enabled, the FQDN value of the Default Topology Hiding Virtual Name configured in NOAM GUI, Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options will be used. Realm: This value is used to populate the Origin-Realm AVP for answer messages routed from a PCRF to a policy client, or the Diameter Destination-Realm AVP for request messages routed from a PCRF to a policy client. If no value is configured here when Topology Hiding is enabled, the Realm value of the Default Topology Hiding Virtual Name configured in NOAM GUI, Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options will be used. [Default = n/a; Range = FQDN and Realm: a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long.]</td> </tr> <tr> <td>Peer Route Table Name</td> <td><input type="text" value="Not Selected"/></td> <td>The name of the Peer Route Table to be used for routing new binding requests. This entry is no longer used once PCRF Pooling is Enabled. [Default = Not Selected; Range = List of configured Diameter Peer Route Tables.]</td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p> <p>1. Enter the virtual/pseudo host FQDN and Realm to be used for this site. These values override the Virtual FQDN and Realm values configured in Step 7.</p> <p>2. Click Apply.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Field	Value	Description	Topology Hiding Virtual Name	FQDN: <input type="text"/> Realm: <input type="text"/>	FQDN: This value is used to populate the Diameter Origin-Host AVP for answer messages routed from a PCRF to a policy client, or the Diameter Destination-Host AVP for request messages routed from a PCRF to a policy client. If no value is configured here when Topology Hiding is enabled, the FQDN value of the Default Topology Hiding Virtual Name configured in NOAM GUI, Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options will be used. Realm: This value is used to populate the Origin-Realm AVP for answer messages routed from a PCRF to a policy client, or the Diameter Destination-Realm AVP for request messages routed from a PCRF to a policy client. If no value is configured here when Topology Hiding is enabled, the Realm value of the Default Topology Hiding Virtual Name configured in NOAM GUI, Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options will be used. [Default = n/a; Range = FQDN and Realm: a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long.]	Peer Route Table Name	<input type="text" value="Not Selected"/>	The name of the Peer Route Table to be used for routing new binding requests. This entry is no longer used once PCRF Pooling is Enabled. [Default = Not Selected; Range = List of configured Diameter Peer Route Tables.]									
Field	Value	Description																		
Topology Hiding Virtual Name	FQDN: <input type="text"/> Realm: <input type="text"/>	FQDN: This value is used to populate the Diameter Origin-Host AVP for answer messages routed from a PCRF to a policy client, or the Diameter Destination-Host AVP for request messages routed from a PCRF to a policy client. If no value is configured here when Topology Hiding is enabled, the FQDN value of the Default Topology Hiding Virtual Name configured in NOAM GUI, Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options will be used. Realm: This value is used to populate the Origin-Realm AVP for answer messages routed from a PCRF to a policy client, or the Diameter Destination-Realm AVP for request messages routed from a PCRF to a policy client. If no value is configured here when Topology Hiding is enabled, the Realm value of the Default Topology Hiding Virtual Name configured in NOAM GUI, Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options will be used. [Default = n/a; Range = FQDN and Realm: a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes ('-') and underscore ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long.]																		
Peer Route Table Name	<input type="text" value="Not Selected"/>	The name of the Peer Route Table to be used for routing new binding requests. This entry is no longer used once PCRF Pooling is Enabled. [Default = Not Selected; Range = List of configured Diameter Peer Route Tables.]																		
12	<p>NOAM VIP: Configure SBR Databases</p>	<p>Navigate to Main Menu -> SBR -> Configuration -> SBR Databases</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Adding a new SBR Database</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Database Name</td> <td><input type="text" value="BindingSbrDb"/></td> <td>A name that uniquely identifies the SBR Database. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscores contain at least one alpha and must not start with a digit.]</td> </tr> <tr> <td>Database Type</td> <td><input type="text" value="Binding"/></td> <td>The type of SBR Database. Select 'Binding' for a Policy Binding database, or 'Session' for a Policy DRA or Online Charging Session database. [Default = n/a; Range = 'Binding' or 'Session']</td> </tr> <tr> <td>Resource Domain</td> <td><input type="text" value="BindingRd_2SG"/></td> <td>The Policy and Charging Session or Policy Binding Resource Domain that contains the SBR configured for use by this database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching the selected Database Type already been assigned to a Database.]</td> </tr> <tr> <td>Number of Server Groups</td> <td><input type="text" value="2"/></td> <td>The number of SBR Server Groups required to host this database. Enter or change the number of Server Groups necessary to support the desired capacity of the selected Resource Domain already contains Server Groups, the number of Server Group Resource Domain is displayed in the field, but can be overridden as desired. [Default = n/a; Range = 1 to 8]</td> </tr> <tr> <td>Place Association</td> <td><input type="text" value="BindingRegion"/></td> <td>The Policy Binding Region or Policy and Charging Mated Sites Place Association that contain will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching the selected Database Type already been assigned to a Database.]</td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>	Field	Value	Description	Database Name	<input type="text" value="BindingSbrDb"/>	A name that uniquely identifies the SBR Database. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscores contain at least one alpha and must not start with a digit.]	Database Type	<input type="text" value="Binding"/>	The type of SBR Database. Select 'Binding' for a Policy Binding database, or 'Session' for a Policy DRA or Online Charging Session database. [Default = n/a; Range = 'Binding' or 'Session']	Resource Domain	<input type="text" value="BindingRd_2SG"/>	The Policy and Charging Session or Policy Binding Resource Domain that contains the SBR configured for use by this database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching the selected Database Type already been assigned to a Database.]	Number of Server Groups	<input type="text" value="2"/>	The number of SBR Server Groups required to host this database. Enter or change the number of Server Groups necessary to support the desired capacity of the selected Resource Domain already contains Server Groups, the number of Server Group Resource Domain is displayed in the field, but can be overridden as desired. [Default = n/a; Range = 1 to 8]	Place Association	<input type="text" value="BindingRegion"/>	The Policy Binding Region or Policy and Charging Mated Sites Place Association that contain will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching the selected Database Type already been assigned to a Database.]
Field	Value	Description																		
Database Name	<input type="text" value="BindingSbrDb"/>	A name that uniquely identifies the SBR Database. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscores contain at least one alpha and must not start with a digit.]																		
Database Type	<input type="text" value="Binding"/>	The type of SBR Database. Select 'Binding' for a Policy Binding database, or 'Session' for a Policy DRA or Online Charging Session database. [Default = n/a; Range = 'Binding' or 'Session']																		
Resource Domain	<input type="text" value="BindingRd_2SG"/>	The Policy and Charging Session or Policy Binding Resource Domain that contains the SBR configured for use by this database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching the selected Database Type already been assigned to a Database.]																		
Number of Server Groups	<input type="text" value="2"/>	The number of SBR Server Groups required to host this database. Enter or change the number of Server Groups necessary to support the desired capacity of the selected Resource Domain already contains Server Groups, the number of Server Group Resource Domain is displayed in the field, but can be overridden as desired. [Default = n/a; Range = 1 to 8]																		
Place Association	<input type="text" value="BindingRegion"/>	The Policy Binding Region or Policy and Charging Mated Sites Place Association that contain will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching the selected Database Type already been assigned to a Database.]																		

		<ol style="list-style-type: none"> 1. Enter Database Name 2. Select Database Type. 3. Select Resource Domain. <i>This will populate Number of Server Groups field with the number of server groups currently present in the selected Resource Domain.</i> 4. If needed, update Number of Server Groups value. <i>Note that Resource Domain will then have to be updated to match this count.</i> 5. Select Place Association. 6. Click Ok <p>NOTE: This is a sample set of configuration data, the actual configuration may differ.</p> <p>For Policy DRA Function one Session Type SBR Database per standalone-site/mated-pair/mated-triplet and one Binding Type SBR Database for the network must be configured.</p>												
<p>13</p> <p>NOAM VIP: Configure PCRF Pools</p>		<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pools</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pools -> [Insert] <small>Mon Aug 18 19:12:4</small></p> <hr/> <p>Adding a new PCRF Pool</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>PCRF Pool Name</td> <td>PcrfPool01</td> <td>A name that uniquely identifies the PCRF Pool. A PCRF Pool names a set of PCRFs that should be used for policy requests for specified APN. The mapping from APN to PCRF Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> Access Point Names. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric underscore. Must contain at least one alpha and must not start with a digit.]</td> </tr> <tr> <td>Sub-Pool</td> <td><input type="checkbox"/></td> <td>Check this box if the PCRF Pool is to be used as a Sub-Pool. A Sub-Pool is used if policy requests from specified origin-hosts should be routed to a different set of the PCRFs from those in the PCRF Pool selected by the APN. Sub-Pool Selection Rules are configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules. [Default = No (Unchecked); Range = Yes (Checked for Sub-Pool), No (Unchecked for Pool)]</td> </tr> <tr> <td>Comments</td> <td><input type="text"/></td> <td>An optional comment to describe the PCRF Pool or Sub-Pool. [Default = n/a; Range = 0-64 characters]</td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></p> <ol style="list-style-type: none"> 1. Enter PCRF Pool name 2. Click Ok <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Field	Value	Description	PCRF Pool Name	PcrfPool01	A name that uniquely identifies the PCRF Pool. A PCRF Pool names a set of PCRFs that should be used for policy requests for specified APN. The mapping from APN to PCRF Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> Access Point Names. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric underscore. Must contain at least one alpha and must not start with a digit.]	Sub-Pool	<input type="checkbox"/>	Check this box if the PCRF Pool is to be used as a Sub-Pool. A Sub-Pool is used if policy requests from specified origin-hosts should be routed to a different set of the PCRFs from those in the PCRF Pool selected by the APN. Sub-Pool Selection Rules are configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules. [Default = No (Unchecked); Range = Yes (Checked for Sub-Pool), No (Unchecked for Pool)]	Comments	<input type="text"/>	An optional comment to describe the PCRF Pool or Sub-Pool. [Default = n/a; Range = 0-64 characters]
Field	Value	Description												
PCRF Pool Name	PcrfPool01	A name that uniquely identifies the PCRF Pool. A PCRF Pool names a set of PCRFs that should be used for policy requests for specified APN. The mapping from APN to PCRF Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> Access Point Names. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric underscore. Must contain at least one alpha and must not start with a digit.]												
Sub-Pool	<input type="checkbox"/>	Check this box if the PCRF Pool is to be used as a Sub-Pool. A Sub-Pool is used if policy requests from specified origin-hosts should be routed to a different set of the PCRFs from those in the PCRF Pool selected by the APN. Sub-Pool Selection Rules are configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules. [Default = No (Unchecked); Range = Yes (Checked for Sub-Pool), No (Unchecked for Pool)]												
Comments	<input type="text"/>	An optional comment to describe the PCRF Pool or Sub-Pool. [Default = n/a; Range = 0-64 characters]												
<p>14</p> <p>NOAM VIP: Configure PCRF Sub Pool</p>		<p>OPTIONAL</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pools</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>												

15
NOAM VIP: Configure PCRF Sub Pool Selection Rule

Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pools -> [Insert]

Mon Aug 18 19:13:23

Adding a new PCRF Pool

Field	Value	Description
PCRF Pool Name	<input type="text" value="PcrSubPool01"/>	A name that uniquely identifies the PCRF Pool. A PCRF Pool names a set of PCRFs that should be used for policy requests from specified APN. The mapping from APN to PCRF Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> Access Point Names. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit]
Sub-Pool	<input checked="" type="checkbox"/>	Check this box if the PCRF Pool is to be used as a Sub-Pool. A Sub-Pool is used if policy requests from specified origin-hosts should be routed to a different set of the PCRFs from those in the PCRF Pool selected by the APN. Sub-Pool Selection Rules are configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules. [Default = No (Unchecked); Range = Yes (Checked for Sub-Pool), No (Unchecked for Pool)]
Comments	<input type="text"/>	An optional comment to describe the PCRF Pool or Sub-Pool. [Default = n/a; Range = 0-64 characters]

1. Enter PCRF Sub Pool name
2. Check the Sub-Pool box
3. Click **Ok**.

NOTE: this is a sample set of configuration data, the actual configuration may differ.

OPTIONAL

Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pools Selection Rules**

Click on **Insert** in the lower left corner.

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules -> [Insert]

Mon Aug 18 19:13:23

Adding a new PCRF Sub-Pool Selection Rule

Field	Value	Description						
PCRF Sub-Pool Selection Rule Name	<input type="text" value="SubPoolSelectionRule01"/>	A name that uniquely identifies the PCRF Sub-Pool Selection Rule. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit]						
Priority	<input type="text" value="50"/>	Priority of this Rule. Low value means higher priority. [Default = 50; Range = 1 - 99]						
PCRF Pool Name	<input type="text" value="PcrPool01"/>	The name of the PCRF Pool for which a Sub-Pool Selection Rule is being defined. [Default = n/a; Range = Configured PCRF Pools that have not been specified as PCRF Sub-Pool Selection Rule Names]						
Conditions	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Origin-Host</td> <td>Starts With</td> <td><input type="text" value="attservice01"/></td> </tr> </tbody> </table>	Parameter	Operator	Value	Origin-Host	Starts With	<input type="text" value="attservice01"/>	Condition associated with this Rule. Origin-Host FQDN is a case-insensitive string consisting of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscores and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and an FQDN must be at most 255 characters long. [Default = n/a; Range = Substring or complete string of a valid FQDN]
Parameter	Operator	Value						
Origin-Host	Starts With	<input type="text" value="attservice01"/>						
PCRF Sub-Pool Name	<input type="text" value="PcrSubPool01"/>	PCRF Sub-Pool that is to be used for Gx and G'x session initiation request messages matching this Rule. [Default = n/a; Range = Choice of configured PCRF Pools]						
Last Updated	<input type="text"/>	This read-only field displays the date and time this rule was created, or the last time the rule was changed, whichever is most recent. This field records the time and date of changes that affect routing of binding capable session initiation requests. This date and time can be compared against binding creation times when troubleshooting using Policy and Charging Maintenance -> Policy Database Query.						

		<ol style="list-style-type: none"> 1. Enter the Rule name 2. Select PCRF Pool Name and PCRF Sub-Pool Name 3. Enter the Condition as shown 4. Click Ok. <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>									
<p>16</p>	<p>SOAM VIP: Navigate to PCRF Pool To PRT Mapping screen</p>	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping</p> <p>You will see a screen similar to:</p> <p>Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping</p> <p style="text-align: right;">Mon Aug 18 15:38:33 2016</p> <p>Filter ▾</p> <p>Table Description: The PCRF Pool To PRT Mapping table displays the list of PCRF Pools or Sub-Pool configured at the NOAMP and each to be mapped to a Peer Routing Table to be used when a new binding is created for the PCRF Pool. The PCRF Pool or Sub-Pool used for a given subscriber binding attempt is determined based on Access point Name to PCRF Pool mappings, or by rules configured in NOAMP in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules.</p> <table border="1"> <thead> <tr> <th>PCRF Pool Name</th> <th>Peer Route Table Name</th> </tr> </thead> <tbody> <tr> <td>Default</td> <td>Default</td> </tr> <tr> <td>PcrfPool01</td> <td>Not Selected</td> </tr> <tr> <td>PcrfSubPool01</td> <td>Not Selected</td> </tr> </tbody> </table>	PCRF Pool Name	Peer Route Table Name	Default	Default	PcrfPool01	Not Selected	PcrfSubPool01	Not Selected	
PCRF Pool Name	Peer Route Table Name										
Default	Default										
PcrfPool01	Not Selected										
PcrfSubPool01	Not Selected										
<p>17</p>	<p>SOAM VIP: Configure the PCRF Pool To PRT Mapping</p>	<p>Select the row with 'Not Selected' under Peer Route Table Name and click 'Edit'</p> <p>You will see a screen similar to:</p> <p>Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping -> [Edit]</p> <p style="text-align: right;">Mon Aug 18 15:39:33 2016</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>PCRF Pool Name</td> <td>PcrfPool01</td> <td>A name that uniquely identifies the PCRF Pool. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]</td> </tr> <tr> <td>Peer Route Table Name</td> <td>PcrfPoolPRT</td> <td>The name of the Peer Route Table that is used to route new bindings for this PCRF Pool. [Default = Not Selected; Range = All Peer Route Tables configured at this site.]</td> </tr> </tbody> </table> <p style="text-align: center;">Ok Apply Cancel</p> <ol style="list-style-type: none"> 1. Select appropriate Peer Route Table Name form the drop box. 2. Click Ok. <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Field	Value	Description	PCRF Pool Name	PcrfPool01	A name that uniquely identifies the PCRF Pool. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]	Peer Route Table Name	PcrfPoolPRT	The name of the Peer Route Table that is used to route new bindings for this PCRF Pool. [Default = Not Selected; Range = All Peer Route Tables configured at this site.]
Field	Value	Description									
PCRF Pool Name	PcrfPool01	A name that uniquely identifies the PCRF Pool. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]									
Peer Route Table Name	PcrfPoolPRT	The name of the Peer Route Table that is used to route new bindings for this PCRF Pool. [Default = Not Selected; Range = All Peer Route Tables configured at this site.]									
<p>18</p>	<p>SOAM VIP: Configure other PCRF Pool To PRT Mapping</p>	<p>Repeat Step 17 for all other PCRF Pool Names where the Peer Route Table Name is displayed as 'Not Selected'.</p>									
<p>19</p>	<p>SOAM VIP: Navigate to the Error Codes screen</p>	<p>OPTIONAL</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Error Codes</p> <p>You will see a screen similar to:</p>									

		<p>Main Menu: Policy and Charging -> Configuration -> Error Codes</p> <p style="text-align: right;">Help Mon Aug 18 15:46:20 2014 EDT</p> <p>Table Description: The Error Codes table defines the result codes to be returned for various Policy and Charging error conditions. Each error condition will return the result code configured for each interface. Setting an experimental result code requires a corresponding Vendor ID. The default result code is 3002-DIAMETER_UNABLE_TO_DELIVER. The Vendor ID "-" means the result code is not vendor-specific.</p> <table border="1"> <thead> <tr> <th>Error Condition</th> <th>Gx/Gxx Result Code</th> <th>Gx/Gxx Vendor ID</th> <th>Rx Result Code</th> <th>Rx Vendor ID</th> <th>S9 Result Code</th> <th>S9 Vendor ID</th> <th>Gx-Prime Result Code</th> <th>Gx-Prime Vendor ID</th> <th>GyRo Result Code</th> <th>GyRo Vendor ID</th> </tr> </thead> <tbody> <tr> <td>PCA Unavailable Or Degraded</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> </tr> <tr> <td>PCA Functionality Unavailable or Disabled</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> </tr> <tr> <td>Binding Not Found</td> <td>n/a</td> <td>n/a</td> <td>3002</td> <td>---</td> <td>n/a</td> <td>n/a</td> <td>3002</td> <td>---</td> <td>n/a</td> <td>n/a</td> </tr> <tr> <td>Unable To Route</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> </tr> <tr> <td>SBR Error</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>5012</td> <td>---</td> </tr> <tr> <td>No Usable Keys In Binding Dependent Message</td> <td>n/a</td> <td>n/a</td> <td>3002</td> <td>---</td> <td>n/a</td> <td>n/a</td> <td>3002</td> <td>---</td> <td>n/a</td> <td>n/a</td> </tr> <tr> <td>Session Not Found</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>3002</td> <td>---</td> <td>5002</td> <td>---</td> </tr> <tr> <td>Missing Or Unconfigured APN</td> <td>3002</td> <td>---</td> <td>n/a</td> <td>n/a</td> <td>3002</td> <td>---</td> <td>n/a</td> <td>n/a</td> <td>n/a</td> <td>n/a</td> </tr> </tbody> </table>	Error Condition	Gx/Gxx Result Code	Gx/Gxx Vendor ID	Rx Result Code	Rx Vendor ID	S9 Result Code	S9 Vendor ID	Gx-Prime Result Code	Gx-Prime Vendor ID	GyRo Result Code	GyRo Vendor ID	PCA Unavailable Or Degraded	3002	---	3002	---	3002	---	3002	---	3002	---	PCA Functionality Unavailable or Disabled	3002	---	3002	---	3002	---	3002	---	3002	---	Binding Not Found	n/a	n/a	3002	---	n/a	n/a	3002	---	n/a	n/a	Unable To Route	3002	---	3002	---	3002	---	3002	---	3002	---	SBR Error	3002	---	3002	---	3002	---	3002	---	5012	---	No Usable Keys In Binding Dependent Message	n/a	n/a	3002	---	n/a	n/a	3002	---	n/a	n/a	Session Not Found	3002	---	3002	---	3002	---	3002	---	5002	---	Missing Or Unconfigured APN	3002	---	n/a	n/a	3002	---	n/a	n/a	n/a	n/a
Error Condition	Gx/Gxx Result Code	Gx/Gxx Vendor ID	Rx Result Code	Rx Vendor ID	S9 Result Code	S9 Vendor ID	Gx-Prime Result Code	Gx-Prime Vendor ID	GyRo Result Code	GyRo Vendor ID																																																																																											
PCA Unavailable Or Degraded	3002	---	3002	---	3002	---	3002	---	3002	---																																																																																											
PCA Functionality Unavailable or Disabled	3002	---	3002	---	3002	---	3002	---	3002	---																																																																																											
Binding Not Found	n/a	n/a	3002	---	n/a	n/a	3002	---	n/a	n/a																																																																																											
Unable To Route	3002	---	3002	---	3002	---	3002	---	3002	---																																																																																											
SBR Error	3002	---	3002	---	3002	---	3002	---	5012	---																																																																																											
No Usable Keys In Binding Dependent Message	n/a	n/a	3002	---	n/a	n/a	3002	---	n/a	n/a																																																																																											
Session Not Found	3002	---	3002	---	3002	---	3002	---	5002	---																																																																																											
Missing Or Unconfigured APN	3002	---	n/a	n/a	3002	---	n/a	n/a	n/a	n/a																																																																																											
<p>20</p>	<p>SOAM VIP: Configure the Error Codes</p>	<p>OPTIONAL</p> <p>Select the row to edit and click on 'Edit' button</p> <p>You will see a screen similar to:</p> <p>Main Menu: Policy and Charging -> Configuration -> Error Codes -> [Edit]</p> <p style="text-align: right;">Mon Aug 18 15:49:15</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Error Condition</td> <td>Unable To Route</td> <td>This error condition applies to session creation messages for all Diameter interfaces. These error codes will be returned if a binding is found (or created) and the Policy DRA is unable to route the message to the PCRf.</td> </tr> <tr> <td>Gx/Gxx Result Code</td> <td>3002</td> <td>Result code to be returned on the Gx and Gxx interfaces. [Default = 3002; Range = 1-9999]</td> </tr> <tr> <td>Gx/Gxx Vendor ID</td> <td></td> <td>Vendor ID which corresponds with the experimental code for the Gx and Gxx interfaces. [Default = n/a; Range = 1-4294967295]</td> </tr> <tr> <td>Rx Result Code</td> <td>3002</td> <td>Result code to be returned on the Rx interface. [Default = 3002; Range = 1-9999]</td> </tr> <tr> <td>Rx Vendor ID</td> <td></td> <td>Vendor ID which corresponds with the experimental code for the Rx interface. [Default = n/a; Range = 1-4294967295]</td> </tr> <tr> <td>S9 Result Code</td> <td>3002</td> <td>Result code to be returned on the S9 interface. [Default = 3002; Range = 1-9999]</td> </tr> <tr> <td>S9 Vendor ID</td> <td></td> <td>Vendor ID which corresponds with the experimental code for the S9 interface. [Default = n/a; Range = 1-4294967295]</td> </tr> <tr> <td>Gx-Prime Result Code</td> <td>3002</td> <td>Result code to be returned on the Gx-Prime interface. [Default = 3002; Range = 1-9999]</td> </tr> <tr> <td>Gx-Prime Vendor ID</td> <td></td> <td>Vendor ID which corresponds with the experimental code for the Gx-Prime interface. [Default = n/a; Range = 1-4294967295]</td> </tr> <tr> <td>GyRo Result Code</td> <td>3002</td> <td>Result code to be returned on the GyRo interface. [Default = 3002; Range = 1-9999]</td> </tr> <tr> <td>GyRo Vendor ID</td> <td></td> <td>Vendor ID which corresponds with the experimental code for the GyRo interface. [Default = n/a; Range = 1-4294967295]</td> </tr> </tbody> </table> <p style="text-align: center;">Ok Apply Cancel</p> <p>1. Enter the Result Code and Vendor ID values as appropriate</p> <p>2. Click Ok.</p>	Field	Value	Description	Error Condition	Unable To Route	This error condition applies to session creation messages for all Diameter interfaces. These error codes will be returned if a binding is found (or created) and the Policy DRA is unable to route the message to the PCRf.	Gx/Gxx Result Code	3002	Result code to be returned on the Gx and Gxx interfaces. [Default = 3002; Range = 1-9999]	Gx/Gxx Vendor ID		Vendor ID which corresponds with the experimental code for the Gx and Gxx interfaces. [Default = n/a; Range = 1-4294967295]	Rx Result Code	3002	Result code to be returned on the Rx interface. [Default = 3002; Range = 1-9999]	Rx Vendor ID		Vendor ID which corresponds with the experimental code for the Rx interface. [Default = n/a; Range = 1-4294967295]	S9 Result Code	3002	Result code to be returned on the S9 interface. [Default = 3002; Range = 1-9999]	S9 Vendor ID		Vendor ID which corresponds with the experimental code for the S9 interface. [Default = n/a; Range = 1-4294967295]	Gx-Prime Result Code	3002	Result code to be returned on the Gx-Prime interface. [Default = 3002; Range = 1-9999]	Gx-Prime Vendor ID		Vendor ID which corresponds with the experimental code for the Gx-Prime interface. [Default = n/a; Range = 1-4294967295]	GyRo Result Code	3002	Result code to be returned on the GyRo interface. [Default = 3002; Range = 1-9999]	GyRo Vendor ID		Vendor ID which corresponds with the experimental code for the GyRo interface. [Default = n/a; Range = 1-4294967295]																																																															
Field	Value	Description																																																																																																			
Error Condition	Unable To Route	This error condition applies to session creation messages for all Diameter interfaces. These error codes will be returned if a binding is found (or created) and the Policy DRA is unable to route the message to the PCRf.																																																																																																			
Gx/Gxx Result Code	3002	Result code to be returned on the Gx and Gxx interfaces. [Default = 3002; Range = 1-9999]																																																																																																			
Gx/Gxx Vendor ID		Vendor ID which corresponds with the experimental code for the Gx and Gxx interfaces. [Default = n/a; Range = 1-4294967295]																																																																																																			
Rx Result Code	3002	Result code to be returned on the Rx interface. [Default = 3002; Range = 1-9999]																																																																																																			
Rx Vendor ID		Vendor ID which corresponds with the experimental code for the Rx interface. [Default = n/a; Range = 1-4294967295]																																																																																																			
S9 Result Code	3002	Result code to be returned on the S9 interface. [Default = 3002; Range = 1-9999]																																																																																																			
S9 Vendor ID		Vendor ID which corresponds with the experimental code for the S9 interface. [Default = n/a; Range = 1-4294967295]																																																																																																			
Gx-Prime Result Code	3002	Result code to be returned on the Gx-Prime interface. [Default = 3002; Range = 1-9999]																																																																																																			
Gx-Prime Vendor ID		Vendor ID which corresponds with the experimental code for the Gx-Prime interface. [Default = n/a; Range = 1-4294967295]																																																																																																			
GyRo Result Code	3002	Result code to be returned on the GyRo interface. [Default = 3002; Range = 1-9999]																																																																																																			
GyRo Vendor ID		Vendor ID which corresponds with the experimental code for the GyRo interface. [Default = n/a; Range = 1-4294967295]																																																																																																			
<p>21</p>	<p>SOAM VIP: Navigate to Suspect Binding Removal Rules screen</p>	<p>OPTIONAL</p> <p>Execute Steps 21 through 23 if additional Suspect Binding Removal Rules are required.</p> <p>Note: A default Suspect Binding Removal rule for Gx CCA-I messages is created by default.</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Suspect Binding Removal Rules</p>																																																																																																			
<p>22</p>	<p>SOAM VIP: Configure the Suspect Binding Removal Rule for Diameter Interfaces and messages that are needed.</p>	<p>OPTIONAL</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																																																																																																			

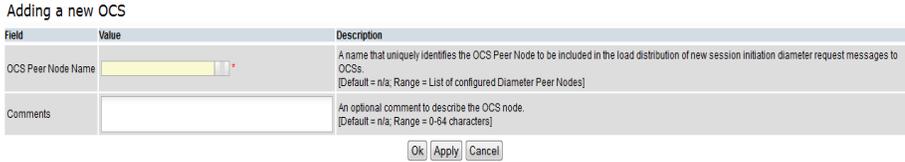
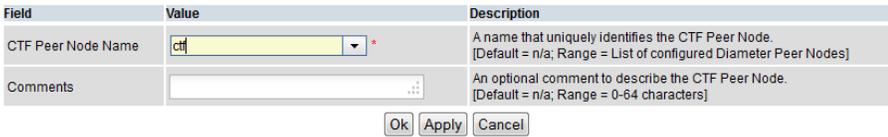
<p>Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Suspect Binding Removal Rules -> [Insert] Help Wed Apr 29 14:55:29 2015 EDT</p> <p>Inserting a new Suspect Binding Removal Rule</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rule Name</td> <td><input type="text"/></td> <td>A name that uniquely identifies the Suspect Binding Removal Rule. [Default = n/a, Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]</td> </tr> <tr> <td>Application Name</td> <td>- Select -</td> <td>The Diameter Application Name and Id to which this Suspect Binding Removal Rule applies. Session initiation answer messages including this Application-Id are candidates to match this rule. [Default = n/a, Range = Supported P-DRA Application-Ids]</td> </tr> <tr> <td>Command Code</td> <td>- Select -</td> <td>The Diameter Command Code or Extended Command Code name and value to which this Suspect Binding Removal Rule applies. Session initiation answer messages including this Command Code are candidates to match this rule. [Default = n/a, Range = Supported P-DRA session initiation answer messages]</td> </tr> <tr> <td>Error Scenario Category</td> <td>- Select -</td> <td>The error category to which the Suspect Binding Removal Rule applies. Category 'Unable to Route' is for when no session initiation answer is received from the PCRF (possibly because the request could not be routed). If 'Unable To Route' is chosen, the (Experimental) Result Code sent to the policy client is the one configured in Policy and Charging -> Configuration -> Error Codes screen for the specific interface. Category 'External Result' is for when a specified session initiation error answer is received from the PCRF. If 'External Result' is chosen, a Result Code must be specified, otherwise no Result Code is necessary. [Default = n/a, Range = External Result, Unable to Route]</td> </tr> <tr> <td>Result Code</td> <td><input type="text"/></td> <td>The session initiation error answer (Experimental) Result Code to which this Suspect Binding Removal Rule applies if the Error Scenario Category is 'External Result'. This field is not applicable when Error Scenario Category is set to 'Unable to Route'. [Default = n/a, Range = 1-9999]</td> </tr> <tr> <td>Vendor ID</td> <td><input type="text"/></td> <td>If a Result Code is entered in the Result Code field above, and that Result Code is an experimental result code, enter the Vendor-Id in this field. Otherwise leave this field set to blank. [Default = n/a, Range = 1-4294967295]</td> </tr> <tr> <td>Remove Suspect Binding Immediately</td> <td><input type="checkbox"/></td> <td>Check this box if a single occurrence of this rule match means that the binding should be removed. Uncheck this box if multiple occurrences of this rule match are required before the binding should be removed. Note: If this box is unchecked, the 'Suspect Binding Removal Events Threshold' field in Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options at the HCAI controls how many Suspect Binding Removal Events must occur before a Session-Release RAR will be sent to the policy client to request removal of the binding. [Default = No (Unchecked); Range = Yes (Checked), No (Unchecked)]</td> </tr> <tr> <td>Comments</td> <td><input type="text"/></td> <td>An optional comment to describe this suspect binding removal rule. [Default = n/a, Range = 0 - 64 characters]</td> </tr> </tbody> </table> <p style="text-align: right;">OK Apply Cancel</p>		Field	Value	Description	Rule Name	<input type="text"/>	A name that uniquely identifies the Suspect Binding Removal Rule. [Default = n/a, Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]	Application Name	- Select -	The Diameter Application Name and Id to which this Suspect Binding Removal Rule applies. Session initiation answer messages including this Application-Id are candidates to match this rule. [Default = n/a, Range = Supported P-DRA Application-Ids]	Command Code	- Select -	The Diameter Command Code or Extended Command Code name and value to which this Suspect Binding Removal Rule applies. Session initiation answer messages including this Command Code are candidates to match this rule. [Default = n/a, Range = Supported P-DRA session initiation answer messages]	Error Scenario Category	- Select -	The error category to which the Suspect Binding Removal Rule applies. Category 'Unable to Route' is for when no session initiation answer is received from the PCRF (possibly because the request could not be routed). If 'Unable To Route' is chosen, the (Experimental) Result Code sent to the policy client is the one configured in Policy and Charging -> Configuration -> Error Codes screen for the specific interface. Category 'External Result' is for when a specified session initiation error answer is received from the PCRF. If 'External Result' is chosen, a Result Code must be specified, otherwise no Result Code is necessary. [Default = n/a, Range = External Result, Unable to Route]	Result Code	<input type="text"/>	The session initiation error answer (Experimental) Result Code to which this Suspect Binding Removal Rule applies if the Error Scenario Category is 'External Result'. This field is not applicable when Error Scenario Category is set to 'Unable to Route'. [Default = n/a, Range = 1-9999]	Vendor ID	<input type="text"/>	If a Result Code is entered in the Result Code field above, and that Result Code is an experimental result code, enter the Vendor-Id in this field. Otherwise leave this field set to blank. [Default = n/a, Range = 1-4294967295]	Remove Suspect Binding Immediately	<input type="checkbox"/>	Check this box if a single occurrence of this rule match means that the binding should be removed. Uncheck this box if multiple occurrences of this rule match are required before the binding should be removed. Note: If this box is unchecked, the 'Suspect Binding Removal Events Threshold' field in Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options at the HCAI controls how many Suspect Binding Removal Events must occur before a Session-Release RAR will be sent to the policy client to request removal of the binding. [Default = No (Unchecked); Range = Yes (Checked), No (Unchecked)]	Comments	<input type="text"/>	An optional comment to describe this suspect binding removal rule. [Default = n/a, Range = 0 - 64 characters]
Field	Value	Description																										
Rule Name	<input type="text"/>	A name that uniquely identifies the Suspect Binding Removal Rule. [Default = n/a, Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]																										
Application Name	- Select -	The Diameter Application Name and Id to which this Suspect Binding Removal Rule applies. Session initiation answer messages including this Application-Id are candidates to match this rule. [Default = n/a, Range = Supported P-DRA Application-Ids]																										
Command Code	- Select -	The Diameter Command Code or Extended Command Code name and value to which this Suspect Binding Removal Rule applies. Session initiation answer messages including this Command Code are candidates to match this rule. [Default = n/a, Range = Supported P-DRA session initiation answer messages]																										
Error Scenario Category	- Select -	The error category to which the Suspect Binding Removal Rule applies. Category 'Unable to Route' is for when no session initiation answer is received from the PCRF (possibly because the request could not be routed). If 'Unable To Route' is chosen, the (Experimental) Result Code sent to the policy client is the one configured in Policy and Charging -> Configuration -> Error Codes screen for the specific interface. Category 'External Result' is for when a specified session initiation error answer is received from the PCRF. If 'External Result' is chosen, a Result Code must be specified, otherwise no Result Code is necessary. [Default = n/a, Range = External Result, Unable to Route]																										
Result Code	<input type="text"/>	The session initiation error answer (Experimental) Result Code to which this Suspect Binding Removal Rule applies if the Error Scenario Category is 'External Result'. This field is not applicable when Error Scenario Category is set to 'Unable to Route'. [Default = n/a, Range = 1-9999]																										
Vendor ID	<input type="text"/>	If a Result Code is entered in the Result Code field above, and that Result Code is an experimental result code, enter the Vendor-Id in this field. Otherwise leave this field set to blank. [Default = n/a, Range = 1-4294967295]																										
Remove Suspect Binding Immediately	<input type="checkbox"/>	Check this box if a single occurrence of this rule match means that the binding should be removed. Uncheck this box if multiple occurrences of this rule match are required before the binding should be removed. Note: If this box is unchecked, the 'Suspect Binding Removal Events Threshold' field in Policy and Charging -> Configuration -> Policy DRA -> Network-Wide Options at the HCAI controls how many Suspect Binding Removal Events must occur before a Session-Release RAR will be sent to the policy client to request removal of the binding. [Default = No (Unchecked); Range = Yes (Checked), No (Unchecked)]																										
Comments	<input type="text"/>	An optional comment to describe this suspect binding removal rule. [Default = n/a, Range = 0 - 64 characters]																										
23	<p>SOAM VIP: Configure additional Suspect Binding Removal Rules.</p>	<p>OPTIONAL</p> <p>Repeat Step 22 for all Suspect Binding Rules that are needed.</p> <p>Note: Steps 21 through 23 may need to be repeated for each active SOAM.</p>																										
25	<p>NOAM VIP: Configure Access Point Names</p>	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Access Point Names</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																										

	<p>Main Menu: Policy and Charging -> Configuration -> Access Point Names -> [Insert]</p> <p style="text-align: right;">Fri May 13 09:14:11</p> <hr/> <p>Adding a new Access Point Name</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Access Point Name</td> <td><input type="text"/></td> <td>This network identifier of the Packet Data Network access point. [Default = n/a, Range = 1-100 characters. Valid characters are alphabetic characters (A-Z and a-z), digits (0-9), hyphen (-), and period (.). Must begin and end with an alphabetic character or a digit.]</td> </tr> <tr> <td>Function</td> <td> <input checked="" type="radio"/> PDRA Only <input type="radio"/> OGDRA Only <input type="radio"/> PDRA and OGDRA </td> <td>The PCA function which uses this Access Point. PCRF Pool is required to be configured for PDRA only. [Default = PDRA Only, Range = PDRA Only, OGDRA Only or PDRA and OGDRA]</td> </tr> <tr> <td>PCRF Pool Name</td> <td>Default</td> <td>The PCRF Pool to which new bindings initiated from the Access Point Network are to be routed. [Default = Default PCRF Pool, Range = Configured PCRF Pools]</td> </tr> <tr> <td>Number of Sub-Pools</td> <td>1</td> <td>This read-only field displays the number of PCRF Sub-Pools associated with the selected PCRF Pool. The mapping between PCRF Pool and PCRF Sub-Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules.</td> </tr> <tr> <td>Maximum Allowed Sessions per IMSI</td> <td>2</td> <td>This setting is the maximum number of bound sessions allowed per IMSI for this APN. [Default = 2, Range = 1-10]</td> </tr> <tr> <td>Per IMSI Session Exceeded Treatment</td> <td> <input checked="" type="radio"/> Route <input type="radio"/> Reject </td> <td>This setting defines the treatment of new binding capable session initiation attempts when the maximum number of bound sessions for an IMSI for this APN is exceeded. If 'Route' is selected, the CCR-I message will be routed and the oldest bound session will be replaced. If 'Reject' is selected, the CCR-I message will be rejected using the Diameter response code configured for SRR Error. [Default = Route, Range = Route, Reject]</td> </tr> <tr> <td>State Session Timeout (Hrs)</td> <td>168</td> <td>This setting is a time value (in hours), after which a session is considered to be stale. For PDRA, a session is considered stale only if no RAR/RAA messages are received in longer than this configured time. For OGDRA, a session is considered stale if no any in session messages are received in longer than this configured time. If a session's age exceeds this value, that session is eligible to be audited out of the database. This value is used for sessions associated with this Access Point Name. For sessions which are not associated with any configured Access Point Names, the Default State Session Timeout value in the Policy and Charging Configuration General Options table is used. [Default = 168 hours (7 days), Range = 1-2400 hours (1 hour to 100 days)]</td> </tr> <tr> <td>Last Updated</td> <td><input type="text"/></td> <td>This read-only field displays the date and time that this APN was created, or the last time the PCRF Pool Name was changed, whichever is most recent. This field records the time and date of changes that may affect routing of binding capable session initiation requests. This date and time can be compared against binding creation times when troubleshooting using Policy and Charging -> Maintenance -> Policy Database Query.</td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></p> <ol style="list-style-type: none"> 1. Enter the field values as required 2. Click Ok. <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Field	Value	Description	Access Point Name	<input type="text"/>	This network identifier of the Packet Data Network access point. [Default = n/a, Range = 1-100 characters. Valid characters are alphabetic characters (A-Z and a-z), digits (0-9), hyphen (-), and period (.). Must begin and end with an alphabetic character or a digit.]	Function	<input checked="" type="radio"/> PDRA Only <input type="radio"/> OGDRA Only <input type="radio"/> PDRA and OGDRA	The PCA function which uses this Access Point. PCRF Pool is required to be configured for PDRA only. [Default = PDRA Only, Range = PDRA Only, OGDRA Only or PDRA and OGDRA]	PCRF Pool Name	Default	The PCRF Pool to which new bindings initiated from the Access Point Network are to be routed. [Default = Default PCRF Pool, Range = Configured PCRF Pools]	Number of Sub-Pools	1	This read-only field displays the number of PCRF Sub-Pools associated with the selected PCRF Pool. The mapping between PCRF Pool and PCRF Sub-Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules.	Maximum Allowed Sessions per IMSI	2	This setting is the maximum number of bound sessions allowed per IMSI for this APN. [Default = 2, Range = 1-10]	Per IMSI Session Exceeded Treatment	<input checked="" type="radio"/> Route <input type="radio"/> Reject	This setting defines the treatment of new binding capable session initiation attempts when the maximum number of bound sessions for an IMSI for this APN is exceeded. If 'Route' is selected, the CCR-I message will be routed and the oldest bound session will be replaced. If 'Reject' is selected, the CCR-I message will be rejected using the Diameter response code configured for SRR Error. [Default = Route, Range = Route, Reject]	State Session Timeout (Hrs)	168	This setting is a time value (in hours), after which a session is considered to be stale. For PDRA, a session is considered stale only if no RAR/RAA messages are received in longer than this configured time. For OGDRA, a session is considered stale if no any in session messages are received in longer than this configured time. If a session's age exceeds this value, that session is eligible to be audited out of the database. This value is used for sessions associated with this Access Point Name. For sessions which are not associated with any configured Access Point Names, the Default State Session Timeout value in the Policy and Charging Configuration General Options table is used. [Default = 168 hours (7 days), Range = 1-2400 hours (1 hour to 100 days)]	Last Updated	<input type="text"/>	This read-only field displays the date and time that this APN was created, or the last time the PCRF Pool Name was changed, whichever is most recent. This field records the time and date of changes that may affect routing of binding capable session initiation requests. This date and time can be compared against binding creation times when troubleshooting using Policy and Charging -> Maintenance -> Policy Database Query.
Field	Value	Description																										
Access Point Name	<input type="text"/>	This network identifier of the Packet Data Network access point. [Default = n/a, Range = 1-100 characters. Valid characters are alphabetic characters (A-Z and a-z), digits (0-9), hyphen (-), and period (.). Must begin and end with an alphabetic character or a digit.]																										
Function	<input checked="" type="radio"/> PDRA Only <input type="radio"/> OGDRA Only <input type="radio"/> PDRA and OGDRA	The PCA function which uses this Access Point. PCRF Pool is required to be configured for PDRA only. [Default = PDRA Only, Range = PDRA Only, OGDRA Only or PDRA and OGDRA]																										
PCRF Pool Name	Default	The PCRF Pool to which new bindings initiated from the Access Point Network are to be routed. [Default = Default PCRF Pool, Range = Configured PCRF Pools]																										
Number of Sub-Pools	1	This read-only field displays the number of PCRF Sub-Pools associated with the selected PCRF Pool. The mapping between PCRF Pool and PCRF Sub-Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules.																										
Maximum Allowed Sessions per IMSI	2	This setting is the maximum number of bound sessions allowed per IMSI for this APN. [Default = 2, Range = 1-10]																										
Per IMSI Session Exceeded Treatment	<input checked="" type="radio"/> Route <input type="radio"/> Reject	This setting defines the treatment of new binding capable session initiation attempts when the maximum number of bound sessions for an IMSI for this APN is exceeded. If 'Route' is selected, the CCR-I message will be routed and the oldest bound session will be replaced. If 'Reject' is selected, the CCR-I message will be rejected using the Diameter response code configured for SRR Error. [Default = Route, Range = Route, Reject]																										
State Session Timeout (Hrs)	168	This setting is a time value (in hours), after which a session is considered to be stale. For PDRA, a session is considered stale only if no RAR/RAA messages are received in longer than this configured time. For OGDRA, a session is considered stale if no any in session messages are received in longer than this configured time. If a session's age exceeds this value, that session is eligible to be audited out of the database. This value is used for sessions associated with this Access Point Name. For sessions which are not associated with any configured Access Point Names, the Default State Session Timeout value in the Policy and Charging Configuration General Options table is used. [Default = 168 hours (7 days), Range = 1-2400 hours (1 hour to 100 days)]																										
Last Updated	<input type="text"/>	This read-only field displays the date and time that this APN was created, or the last time the PCRF Pool Name was changed, whichever is most recent. This field records the time and date of changes that may affect routing of binding capable session initiation requests. This date and time can be compared against binding creation times when troubleshooting using Policy and Charging -> Maintenance -> Policy Database Query.																										
<p>24</p> <p>NOAM VIP: Enable the Policy DRA function</p>	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> General Options Screen.</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Policy DRA Enabled</td> <td><input checked="" type="checkbox"/></td> <td>Indicate whether the Policy DRA Function of PCA is enabled. [Default = Policy DRA Disabled (Unchecked), Range = Policy DRA Enabled (Checked) or Policy DRA disabled (Unchecked)]</td> </tr> <tr> <td>Online Charging DRA Enabled</td> <td><input type="checkbox"/></td> <td>Indicate whether the Online Charging DRA Function of PCA is enabled. [Default = Online Charging DRA Disabled (Unchecked), Range = Online Charging DRA Enabled (Checked) or Online Charging DRA Disabled (Unchecked)]</td> </tr> </tbody> </table> <ol style="list-style-type: none"> 1. Check the Policy DRA Enabled box 2. Click Apply. 	Field	Value	Description	Policy DRA Enabled	<input checked="" type="checkbox"/>	Indicate whether the Policy DRA Function of PCA is enabled. [Default = Policy DRA Disabled (Unchecked), Range = Policy DRA Enabled (Checked) or Policy DRA disabled (Unchecked)]	Online Charging DRA Enabled	<input type="checkbox"/>	Indicate whether the Online Charging DRA Function of PCA is enabled. [Default = Online Charging DRA Disabled (Unchecked), Range = Online Charging DRA Enabled (Checked) or Online Charging DRA Disabled (Unchecked)]																		
Field	Value	Description																										
Policy DRA Enabled	<input checked="" type="checkbox"/>	Indicate whether the Policy DRA Function of PCA is enabled. [Default = Policy DRA Disabled (Unchecked), Range = Policy DRA Enabled (Checked) or Policy DRA disabled (Unchecked)]																										
Online Charging DRA Enabled	<input type="checkbox"/>	Indicate whether the Online Charging DRA Function of PCA is enabled. [Default = Online Charging DRA Disabled (Unchecked), Range = Online Charging DRA Enabled (Checked) or Online Charging DRA Disabled (Unchecked)]																										

4.4.2 Online Charging DRA Configuration

Detailed steps are given in the procedure below.

Procedure 16: Online Charging DRA configuration

S T E P #	<p>This procedure configures the Online Charging DRA function of PCA application. For details on the fields of various configuration screens please refer to the Policy Charging User’s Guide [4].</p> <p>PREREQUISITE: Procedure 14 must be executed before this procedure.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>	
	1	<p>Establish GUI Session on the SOAM VIP</p> <p>Establish a GUI session on the SOAM by using the XMI VIP address. Login as user “guiadmin”.</p>
	2	<p>SOAM VIP: Navigate to OCSs screen</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> OCSs</p>
	3	<p>SOAM VIP: Configure the first OCS node.</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Policy and Charging -> Configuration -> Online Charging DRA -> OCSs -> [Insert]</p>  <p>1. Select the OCS name from the drop down 2. Click Ok.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>
	4	<p>SOAM VIP: Configure all other OCS nodes.</p> <p>Repeat Step 3 to configure all the OCS nodes.</p>
	5	<p>SOAM VIP: Navigate to CTFs screen</p> <p>If Session State needs to be maintained for Online Charging client, then</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> CTFs</p>
6	<p>SOAM VIP: Configure the first CTF node.</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Policy and Charging -> Configuration -> Online Charging DRA -> CTFs -> [Insert]</p> 	

		<p>1. Select the CTF name from the drop down</p> <p>2. Click Ok.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>																		
<p>7</p>	<p>SOAM VIP: Configure all other CTF nodes.</p>	<p>Repeat Step 6 to configure all the CTF nodes for which the Session State needs to be maintained.</p>																		
<p>8</p>	<p>NOAM VIP: Configure SBR Databases</p>	<p>Navigate to Main Menu -> SBR -> Configuration -> SBR Databases</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <div data-bbox="516 604 1409 1081" style="border: 1px solid gray; padding: 5px;"> <p>Adding a new SBR Database</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Database Name</td> <td>SessionSbrDb</td> <td>A name that uniquely identifies the SBR Database. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and contain at least one alpha and must not start with a digit]</td> </tr> <tr> <td>Database Type</td> <td>Session</td> <td>The type of SBR Database. Select 'Binding' for a Policy Binding database, or 'Session' for a Policy DRA or Online Session database. [Default = n/a; Range = 'Binding' or 'Session']</td> </tr> <tr> <td>Resource Domain</td> <td>SessionRd_Mated</td> <td>The Policy and Charging Session or Policy Binding Resource Domain that contains the database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching the selected Database already been assigned to a Database]</td> </tr> <tr> <td>Number of Server Groups</td> <td>2</td> <td>The number of SBR Server Groups required to host this database. Enter or change the number of Server Groups necessary to support the desired capacity of the selected Resource Domain already contains Server Groups, the number of Server Groups in the Resource Domain is displayed in the field, but can be overridden as desired. [Default = n/a; Range = 1 to 8]</td> </tr> <tr> <td>Place Association</td> <td>MatedSites</td> <td>The Policy Binding Region or Policy and Charging Mated Sites Place Association that will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching the selected Database already been assigned to a Database]</td> </tr> </tbody> </table> <p style="text-align: right;">Ok Apply Cancel</p> </div> <p>1. Enter Database Name</p> <p>2. Select Database Type (Session).</p> <p>3. Select Resource Domain. <i>This will populate Number of Server Groups field with the number of server groups currently present in the selected Resource Domain.</i></p> <p>4. If needed, update Number of Server Groups value. <i>Note that Resource Domain will then have to be updated to match this count.</i></p> <p>5. Select Place Association.</p> <p>6. Click Ok</p> <p>NOTE: This is a sample set of configuration data, the actual configuration may differ.</p> <p>For Online Charging DRA Function, Session Type SBR Database per standalone-site/mated-pair/mated-triplet MUST be configured.</p>	Field	Value	Description	Database Name	SessionSbrDb	A name that uniquely identifies the SBR Database. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and contain at least one alpha and must not start with a digit]	Database Type	Session	The type of SBR Database. Select 'Binding' for a Policy Binding database, or 'Session' for a Policy DRA or Online Session database. [Default = n/a; Range = 'Binding' or 'Session']	Resource Domain	SessionRd_Mated	The Policy and Charging Session or Policy Binding Resource Domain that contains the database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching the selected Database already been assigned to a Database]	Number of Server Groups	2	The number of SBR Server Groups required to host this database. Enter or change the number of Server Groups necessary to support the desired capacity of the selected Resource Domain already contains Server Groups, the number of Server Groups in the Resource Domain is displayed in the field, but can be overridden as desired. [Default = n/a; Range = 1 to 8]	Place Association	MatedSites	The Policy Binding Region or Policy and Charging Mated Sites Place Association that will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching the selected Database already been assigned to a Database]
Field	Value	Description																		
Database Name	SessionSbrDb	A name that uniquely identifies the SBR Database. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and contain at least one alpha and must not start with a digit]																		
Database Type	Session	The type of SBR Database. Select 'Binding' for a Policy Binding database, or 'Session' for a Policy DRA or Online Session database. [Default = n/a; Range = 'Binding' or 'Session']																		
Resource Domain	SessionRd_Mated	The Policy and Charging Session or Policy Binding Resource Domain that contains the database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching the selected Database already been assigned to a Database]																		
Number of Server Groups	2	The number of SBR Server Groups required to host this database. Enter or change the number of Server Groups necessary to support the desired capacity of the selected Resource Domain already contains Server Groups, the number of Server Groups in the Resource Domain is displayed in the field, but can be overridden as desired. [Default = n/a; Range = 1 to 8]																		
Place Association	MatedSites	The Policy Binding Region or Policy and Charging Mated Sites Place Association that will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching the selected Database already been assigned to a Database]																		
<p>9</p>	<p>NOAM VIP: Configure Access Point Names</p>	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Access Point Names</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																		

Main Menu: Policy and Charging -> Configuration -> Access Point Names -> [Insert] Mon Aug 18 20

Adding a new Access Point Name

Field	Value	Description
Access Point Name	ocsservice.att.com	The network identifier of the Packet Data Network access point. [Default = n/a; Range = 1-100 characters. Valid characters are alphabetic characters (A-Z a-z), digits (0-9), hyphen (-), and period (.). Must begin and end with an alphabetic character.]
PCRF Pool Name	Default	The PCRF Pool to which new bindings initiated from the Access Point Network are to be routed. [Default = Default PCRF Pool; Range = Configured PCRF Pools]
Number of Sub-Pools	0	This read-only field displays the number of PCRF Sub-Pools associated with the selected PCRF Pool. The mapping between PCRF Pool and PCRF Sub-Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules.
State Session Timeout (Hrs)	168	This setting is a time value (in hours), after which a session is considered to be stale. A session is considered stale only if no RAR/RAA messages are received in longer than this configuration time. If a session's age exceeds this value, that session is eligible to be audited out of the database. This value is used for sessions associated with this Access Point Name. For sessions which are not associated with any configured Access Point Names, the Default Session Timeout value in the Policy DRA Configuration Network-Wide Options table is used. [Default = 168 hours (7 days); Range = 1-2400 hours (1 hour to 100 days)]
Last Updated		This read-only field displays the date and time that this APN was created, or the last time the PCRF Pool Name was changed, whichever is most recent. This field records the time and changes that may affect routing of binding capable session initiation requests. This date and time can be compared against binding creation times when troubleshooting using Policy -> Charging -> Maintenance -> Policy Database Query.

[Ok] [Apply] [Cancel]

1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values)
2. Click **Ok**.

NOTE: this is a sample set of configuration data, the actual configuration may differ.

10 **NOAM VIP: Navigate to OCS Session State screen**

OPTIONAL

Execute Step 10, 11, 12 if any OCS is required to have Session State Configured.

Navigate to **Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> OCS Session State**

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Online Charging DRA -> OCS Session State Mon Nov 24 13:41:01 2014 EST

Filter

Table Description: This table contains the network-wide list of Online Charging Servers (OCSs), listed by their Realm and FQDN. It is used to configure the Session State setting for OCSs. The list of OCSs in this table is kept up-to-date when they are inserted or deleted from the Policy and Charging -> Configuration -> Online Charging DRA -> OCSs screen at each site's SOAM. The Realm and FQDN are configured from each site's Diameter -> Configuration -> Peer Nodes screen prior to selecting the Peer Node Name on the OCS screen.

Realm	FQDN	Session State Enabled
east-gtba.com	OCS1-GTAX-east-gtba.com	No

11 **NOAM VIP: Configure the Session State for an OCS.**

OPTIONAL

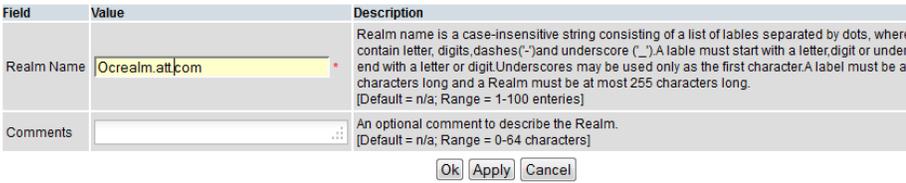
Select an OCS by highlighting the line, click on edit in the lower left corner.

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Online Charging DRA -> OCS Session State -> [Edit] Mon Nov 24 13:45:01 2014 EST

Field	Value	Description
Realm	east-gtba.com	Realm of this Peer Node. Realm is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = A valid Realm]
FQDN	OCS1-GTAX-east-gtba.com	Fully Qualified Domain Name of this Peer Node. FQDN is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-) and underscore (_). A label must start with a letter, digit or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long. [Default = n/a; Range = A valid FQDN]
OCS Session State Enabled	<input type="checkbox"/>	Setting to enable Session State for OCSs. Check this box if the sessions are to be maintained for this OCS. The Sessions shall be maintained if the Session State Scope is set to 'All Messages' in Policy and Charging -> Configuration -> Online Charging DRA -> Network-Wide Options configuration or if Session State Scope is set to 'Specific Messages' and this Session State Enabled setting is checked. [Default = No (unchecked) - Do not maintain session states; Range = Yes (checked) - Maintain session states, or No (unchecked) - Do not maintain session states.]

[Ok] [Apply] [Cancel]

		<p>1. Check OCS Session State Enabled checkbox to turn on the Session State for this OCS; Or uncheck OCS Session State Enabled checkbox to turn off the Session State for this OCS.</p> <p>2. Click Ok.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>									
<p>12</p>	<p>NOAM VIP: Configure the Session State for all other OCSs.</p>	<p>OPTIONAL</p> <p>Repeat Step 11 to configure all the OCSs.</p>									
<p>13</p>	<p>NOAM VIP: Navigate to Realms screen</p>	<p>OPTIONAL</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> Realms</p>									
<p>14</p>	<p>NOAM VIP: Configure the first Realm.</p>	<p>OPTIONAL</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Policy and Charging -> Configuration -> Online Charging DRA -> Realms -> [Insert]</p>  <p>Adding a new Realm</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Realm Name</td> <td>Ocrealm.att.com</td> <td>Realm name is a case-insensitive string consisting of a list of labels separated by dots, where contain letter, digits,dashes("-")and underscore ("_").A lable must start with a letter,digit or unders end with a letter or digit.Underscores may be used only as the first character.A lable must be at characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = 1-100 enteries]</td> </tr> <tr> <td>Comments</td> <td></td> <td>An optional comment to describe the Realm. [Default = n/a; Range = 0-64 characters]</td> </tr> </tbody> </table> <p>Ok Apply Cancel</p> <p>1. Enter the realm name</p> <p>2. Click Ok.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Field	Value	Description	Realm Name	Ocrealm.att.com	Realm name is a case-insensitive string consisting of a list of labels separated by dots, where contain letter, digits,dashes("-")and underscore ("_").A lable must start with a letter,digit or unders end with a letter or digit.Underscores may be used only as the first character.A lable must be at characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = 1-100 enteries]	Comments		An optional comment to describe the Realm. [Default = n/a; Range = 0-64 characters]
Field	Value	Description									
Realm Name	Ocrealm.att.com	Realm name is a case-insensitive string consisting of a list of labels separated by dots, where contain letter, digits,dashes("-")and underscore ("_").A lable must start with a letter,digit or unders end with a letter or digit.Underscores may be used only as the first character.A lable must be at characters long and a Realm must be at most 255 characters long. [Default = n/a; Range = 1-100 enteries]									
Comments		An optional comment to describe the Realm. [Default = n/a; Range = 0-64 characters]									
<p>15</p>	<p>NOAM VIP: Configure all other Realm names.</p>	<p>OPTIONAL</p> <p>Repeat Step 14 to configure all the realms.</p>									
<p>16</p>	<p>NOAM VIP: Navigate to Network-Wide Options screen</p>	<p>OPTIONAL</p> <p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> Network-Wide Options</p>									
<p>17</p>	<p>NOAM VIP: Configure the options</p>										

18

SOAM VIP: Navigate to the Error Codes screen

18

Thu May 21 06:04:26

Field	Value	Description
Session Options		
Session State Scope	None	This sets the scope of messages for which Session State will be stored. Select 'All Messages' to store Session State for all messages. Select 'None' to disable Session State for all messages. Select 'Specific Messages' to store Session State only if the CTF client is configured in the CTFs configuration or OCS is configured with Session State as enabled in OCSs configuration or realm is configured in Realms configuration. [Default = None; Range = 'None', 'All Messages', 'Specific Messages']
Session State Unavailable Action	Send Answer	Sets the action to be performed if an in-session Request message cannot be successfully processed due to the inability to retrieve session state associated with the received Session-Id from the Session SBR (i.e., session state is not found or an SBR error is encountered). 'Route to Peer' will route the message to a peer using the Peer Routing Table. 'Send Answer' will abandon message processing and send an Answer response containing Answer Result-Code value configured for 'Session Not Found' or 'SBR Error'. [Default = Send Answer; Range = 'Send Answer', 'Route to Peer']
OCS Selection Options		
OCS Pool Selection Mode	Single Pool	This sets the operating mode for selecting the OCS Server for routing the Session Initiation Request messages. When 'Single Pool' mode is selected, the Session Initiation Requests are distributed in a weighted round-robin scheme among all available OCS servers connected to this Node. When 'Multiple Pools' mode is selected, the Session Initiation Requests are routed to an OCS server identified by RBAR in a specific pool of OCS servers. [Default = Single Pool; Range = 'Single Pool', 'Multiple Pools']

Apply Cancel

- Select the appropriate values for the available options. Please refer to the Policy Charging Application User's Guide ^[4] for details on the fields.
- Click **Apply**.

Mon Aug 18 15:46:20 2014 EDT

Main Menu: Policy and Charging -> Configuration -> Error Codes

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Error Codes

Table Description: The Error Codes table defines the result codes to be returned for various Policy and Charging error conditions. Each error condition will return the result code configured for each interface. Setting an experimental result code requires a corresponding Vendor ID. The default result code is 3002-DIAMETER_UNABLE_TO_DELIVER. The Vendor ID '-' means the result code is not vendor-specific.

Error Condition	Gx/Gxx Result Code	Gx/Gxx Vendor ID	Rx Result Code	Rx Vendor ID	S9 Result Code	S9 Vendor ID	Gx-Prime Result Code	Gx-Prime Vendor ID	Gy/Ro Result Code	Gy/Ro Vendor ID
PCA Unavailable Or Degraded	3002	---	3002	---	3002	---	3002	---	3002	---
PCA Functionality Unavailable or Disabled	3002	---	3002	---	3002	---	3002	---	3002	---
Binding Not Found	n/a	n/a	3002	---	n/a	n/a	3002	---	n/a	n/a
Unable To Route	3002	---	3002	---	3002	---	3002	---	3002	---
SBR Error	3002	---	3002	---	3002	---	3002	---	5012	---
No Usable Keys In Binding Dependent Message	n/a	n/a	3002	---	n/a	n/a	3002	---	n/a	n/a
Session Not Found	3002	---	3002	---	3002	---	3002	---	5002	---
Missing Or Unconfigured APN	3002	---	n/a	n/a	3002	---	n/a	n/a	n/a	n/a

19

SOAM VIP: Configure the Error Codes

19

Select the row to edit and click on 'Edit' button

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Error Codes -> [Edit]
Mon Aug 18 15:49:5

Field	Value	Description
Error Condition	Unable To Route *	This error condition applies to session creation messages for all Diameter interfaces. These error codes will be returned if a binding is found (or created) and the Policy DRA is unable to route the message to the PCRF.
Gx/Gxx Result Code	3002 *	Result code to be returned on the Gx and Gxx interfaces. [Default = 3002; Range = 1-9999]
Gx/Gxx Vendor ID		Vendor ID which corresponds with the experimental code for the Gx and Gxx interfaces. [Default = n/a; Range = 1-4294967295]
Rx Result Code	3002 *	Result code to be returned on the Rx interface. [Default = 3002; Range = 1-9999]
Rx Vendor ID		Vendor ID which corresponds with the experimental code for the Rx interface. [Default = n/a; Range = 1-4294967295]
S9 Result Code	3002 *	Result code to be returned on the S9 interface. [Default = 3002; Range = 1-9999]
S9 Vendor ID		Vendor ID which corresponds with the experimental code for the S9 interface. [Default = n/a; Range = 1-4294967295]
Gx-Prime Result Code	3002 *	Result code to be returned on the Gx-Prime interface. [Default = 3002; Range = 1-9999]
Gx-Prime Vendor ID		Vendor ID which corresponds with the experimental code for the Gx-Prime interface. [Default = n/a; Range = 1-4294967295]
GyRo Result Code	3002 *	Result code to be returned on the GyRo interface. [Default = 3002; Range = 1-9999]
GyRo Vendor ID		Vendor ID which corresponds with the experimental code for the GyRo interface. [Default = n/a; Range = 1-4294967295]

1. Enter the GyRo Result Code and GyRo Vendor ID values as appropriate
2. Click **Ok**.

20

NOAM VIP: Enable the Online Charging DRA function

Navigate to **Main Menu -> Policy and Charging -> Configuration -> General Options** Screen.

Field	Value	Description
Policy DRA Enabled	<input type="checkbox"/>	Indicate whether the Policy DRA Function is Enabled (Checked) or Disabled (Unchecked) [Default = Policy DRA Disabled (Unchecked)]
Online Charging DRA Enabled	<input checked="" type="checkbox"/>	Indicate whether the Online Charging DRA Function is Enabled (Checked) or Disabled (Unchecked) [Default = Online Charging DRA Disabled (Unchecked)]

1. Check the Online Charging DRA Enabled box
2. Click **Apply**.

4.5 CONFIGURING ONLINE CHARGING FUNCTION ON A RUNNING DSR PCA SYSTEM

4.5.1 Configuring new Online Charging DRA Sites

Detailed steps are given in the procedure below.

Procedure 17: New Online Charging DRA Site Configuration

S T E P #	This procedure configures a site for OC-DRA function in a DSR PCA network	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
1 <input type="checkbox"/>	Configure new PCA OC-DRA site	Execute the procedures defined in [1] and [2] to add new site(s) in the DSR network and configure the PCA Online Charging Function by executing Procedure 16.

4.5.2 Configuring Online Charging DRA in existing Sites

Detailed steps are given in the procedure below.

Procedure 18: Online Charging DRA Configuration on a running DSR PCA System

S T E P #	This procedure configures OC-DRA function in a DSR PCA network without any hardware changes	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
1 <input type="checkbox"/>	Configure and enable OC-DRA	Execute Procedure 16 to configure OC-DRA functionality.

4.5.3 Configuring Online Charging DRA in existing Sites with scaling

Detailed steps are given in the procedure below.

Procedure 19: Online Charging DRA Configuration with scaling on a running DSR PCA System

S T E P #	This procedure performs scaling of OC-DRA function on a running PCA system	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
1 <input type="checkbox"/>	Call ORACLE Customer Service	If the need arises to scale OC-DRA on a running PCA system, please call ORACLE Customer Service for assistance.

4.6 CONFIGURING POLICY DRA FUNCTION ON A RUNNING DSR PCA SYSTEM

This section provides the procedures to configure the Policy DRA function in an already configured and running DSR network with PCA application and Online Charging DRA function enabled.

4.6.1 Configuring Policy DRA

Detailed steps are given in the procedure below.

Procedure 20: Policy DRA Configuration with scaling on a running DSR PCA System

S T E P #	This procedure performs scaling of P-DRA function on a running PCA system	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
1 <input type="checkbox"/>	Call ORACLE Customer Service	If the need arises to scale P-DRA on a running PCA system, please call ORACLE Customer Service for assistance.

4.7 UN-CONFIGURING POLICY DRA FUNCTION FROM A RUNNING DSR PCA SYSTEM

Detailed steps are given in the procedure below.

Procedure 21: Un-configuring Policy DRA

S T E P #	<p>This procedure un-configures the Policy DRA function of PCA application.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>										
1 <input type="checkbox"/>	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".									
2 <input type="checkbox"/>	NOAM VIP: Disable the Policy DRA function	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> General Options Screen.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Field</th> <th style="text-align: left;">Value</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td>Policy DRA Enabled</td> <td style="text-align: center;"><input type="checkbox"/></td> <td>Indicate whether the Policy DRA is enabled (Checked) or Policy DRA disabled (Unchecked) [Default = Policy DRA Disabled (Policy DRA disabled (Unchecked))]</td> </tr> <tr> <td>Online Charging DRA Enabled</td> <td style="text-align: center;"><input type="checkbox"/></td> <td>Indicate whether the Online Charging DRA Function is enabled (Checked) or Online Charging DRA Disabled (Unchecked) [Default = Online Charging DRA Disabled (Unchecked)]</td> </tr> </tbody> </table> <p>Audit Options</p> <ol style="list-style-type: none"> Uncheck the Policy DRA Enabled box Click Apply. <p>CAUTION Executing this step will irretrievably delete all the subscriber binding and Policy session records from the SBR Databases.</p>	Field	Value	Description	Policy DRA Enabled	<input type="checkbox"/>	Indicate whether the Policy DRA is enabled (Checked) or Policy DRA disabled (Unchecked) [Default = Policy DRA Disabled (Policy DRA disabled (Unchecked))]	Online Charging DRA Enabled	<input type="checkbox"/>	Indicate whether the Online Charging DRA Function is enabled (Checked) or Online Charging DRA Disabled (Unchecked) [Default = Online Charging DRA Disabled (Unchecked)]
Field	Value	Description									
Policy DRA Enabled	<input type="checkbox"/>	Indicate whether the Policy DRA is enabled (Checked) or Policy DRA disabled (Unchecked) [Default = Policy DRA Disabled (Policy DRA disabled (Unchecked))]									
Online Charging DRA Enabled	<input type="checkbox"/>	Indicate whether the Online Charging DRA Function is enabled (Checked) or Online Charging DRA Disabled (Unchecked) [Default = Online Charging DRA Disabled (Unchecked)]									
3 <input type="checkbox"/>	NOAM VIP: Disable the Policy DRA specific Binding SBR Database	<p>Main Menu -> SBR -> Maintenance -> SBR Database Status</p> <p>Select the SBR Database of type 'Binding' and Disable it.</p>									
4 <input type="checkbox"/>	NOAM VIP: Disable the Policy DRA Session SBR Database	<p>If the Online Charging DRA Function is not enabled, disable all the Session Database(s). Navigate to Main Menu -> SBR -> Maintenance -> SBR Database Status</p> <p>One by one select the SBR Database of type 'Session' and Disable it.</p>									
5 <input type="checkbox"/>	NOAM VIP: Delete the Policy DRA specific Binding SBR Database	<p>Main Menu -> SBR -> Configuration -> SBR Databases</p> <p>Delete the SBR Database of type 'Binding' from this screen.</p>									
6 <input type="checkbox"/>	NOAM VIP: Delete the Policy DRA Session SBR Databases	<p>If the Online Charging DRA Function is not enabled, disable all the Session Database(s). Navigate to Main Menu -> SBR -> Configuration -> SBR Databases</p> <p>Delete the SBR Databases of type 'Session' from this screen.</p>									
7 <input type="checkbox"/>	NOAM VIP: Delete the Policy DRA specific APNs	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE APN CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -></p>									

		<p>Access Point Names</p> <p>Delete the Policy DRA specific configuration data from this screen.</p>
8	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
9	SOAM VIP: De-reference all the PRTs from PCRF Pools	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF POOL CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping</p> <p>Edit all the PCRF Pool Name entries and set the Peer Route Table Name to 'Not Selected'.</p>
10	SOAM VIP: Delete all the PCRFs	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRFs</p> <p>Delete the complete configuration data from this screen.</p>
11	SOAM VIP: Delete all the Policy Clients configuration	<p>Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Policy Clients</p> <p>Delete the complete configuration data from this screen.</p>
12	SOAM VIP: Un-configure the Site Options	<p>Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Site Options</p> <p>Uncheck the 'Enabled' box against 'Topology Hiding Options'.</p>
13	SOAM VIP: Restore default values of Error Codes (OPTIONAL)	<p>Main Menu -> Policy and Charging -> Configuration -> Error Codes</p> <p>Edit all Error Conditions and set the Result Code as 3002 for all Policy DRA application interfaces (Gx/Gxx, Rx, S9, Gx-Prime etc.).</p>
14	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Steps 4 to 9 on All Active SOAM servers.
13	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
16	NOAM VIP: Delete all the Sub-Pool Selection Rules	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF POOL CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules</p> <p>Delete the complete configuration data from this screen.</p>
17	NOAM VIP: Delete all the PCRF Pools	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF POOL CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pools</p>

	Delete the complete configuration data from this screen.
--	--

4.8 UN-CONFIGURING ONLINE CHARGING FUNCTION FROM A RUNNING DSR PCA SYSTEM

Detailed steps are given in the procedure below.

Procedure 22: Un-configuring Online Charging DRA

S T E P #	<p>This procedure un-configures the Online Charging DRA function of PCA application.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>										
1 <input type="checkbox"/>	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".									
2 <input type="checkbox"/>	NOAM VIP: Disable the Online Charging DRA function	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> General Options Screen.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Field</th> <th style="text-align: left;">Value</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td>Policy DRA Enabled</td> <td style="text-align: center;"><input type="checkbox"/></td> <td>Indicate whether the Policy DRA [Default = Policy DRA Disabled (DRA disabled (Unchecked))]</td> </tr> <tr> <td>Online Charging DRA Enabled</td> <td style="text-align: center;"><input type="checkbox"/></td> <td>Indicate whether the Online Cha [Default = Online Charging DRA Enabled (Checked) or Online Ch</td> </tr> </tbody> </table> <p>Audit Options</p> <ol style="list-style-type: none"> Uncheck the Online Charging DRA Enabled box Click Apply. 	Field	Value	Description	Policy DRA Enabled	<input type="checkbox"/>	Indicate whether the Policy DRA [Default = Policy DRA Disabled (DRA disabled (Unchecked))]	Online Charging DRA Enabled	<input type="checkbox"/>	Indicate whether the Online Cha [Default = Online Charging DRA Enabled (Checked) or Online Ch
Field	Value	Description									
Policy DRA Enabled	<input type="checkbox"/>	Indicate whether the Policy DRA [Default = Policy DRA Disabled (DRA disabled (Unchecked))]									
Online Charging DRA Enabled	<input type="checkbox"/>	Indicate whether the Online Cha [Default = Online Charging DRA Enabled (Checked) or Online Ch									
3 <input type="checkbox"/>	NOAM VIP: Disable the Online Charging DRA Session SBR Database	<p>If the Policy DRA Function is not enabled, disable all the Session Database(s). Navigate to Main Menu -> SBR -> Maintenance -> SBR Database Status</p> <p>One by one select the SBR Database of type 'Session' and Disable it.</p>									
4 <input type="checkbox"/>	NOAM VIP: Delete the Online Charging DRA Session SBR Databases	<p>If the Policy DRA Function is not enabled, delete all the Session Database(s). Navigate to Main Menu -> SBR -> Configuration -> SBR Databases</p> <p>Delete the SBR Databases of type 'Session' from this screen.</p>									
5 <input type="checkbox"/>	NOAM VIP: Delete all configured Realms	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE ONLINE CHARGING REALMS CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> Realms</p> <p>Delete the complete configuration data from this screen.</p>									
6 <input type="checkbox"/>	NOAM VIP: Delete the Online Charging specific APNs	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE APN CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -> Access Point Names</p> <p>Delete the Online charging specific configuration data from this screen.</p>									

7 <input type="checkbox"/>	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
8 <input type="checkbox"/>	SOAM VIP: Delete the Online Charging Servers	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE OCS CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> OCSs</p> <p>Delete the complete configuration data from this screen.</p>
9 <input type="checkbox"/>	SOAM VIP: Delete the Online charging Clients	<p>NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE CTF CONFIGURATION DATA AFTER RE-ENABLE.</p> <p>Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> CTFs</p> <p>Delete the complete configuration data from this screen.</p>
10 <input type="checkbox"/>	SOAM VIP: Restore default values of Error Codes (OPTIONAL)	<p>Main Menu -> Policy and Charging -> Configuration -> Error Codes</p> <ol style="list-style-type: none"> Edit the Error Condition 'SBR Error' and set the Gy/Ro Result Code as 5012. Edit the Error Condition 'Session Not found' and set the Gy/Ro Result Code as 5002. Edit all other Error Conditions and set the Gy/Ro Result Code as 3002.
11 <input type="checkbox"/>	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Steps 5 to 7 on All Active SOAM servers.

4.9 POST-CONFIGURATION PROCEDURES

4.9.1 Enable Application

Detailed steps are given in the procedure below.

Procedure 23: Enable Application

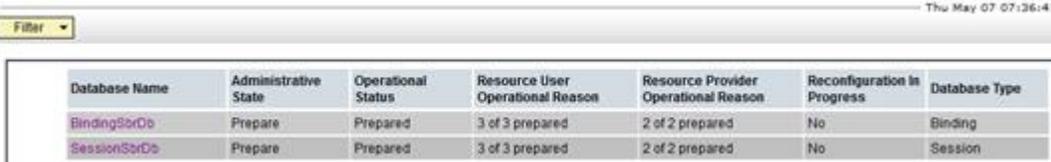
S T E P #	<p>This procedure enables the PCA application on the DA-MP servers.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>	
1 <input type="checkbox"/>	Establish GUI Session on the active SOAM VIP	Establish a GUI session on the Active SOAM server by using the XMI VIP address. Login as user "guiadmin".
2 <input type="checkbox"/>	SOAM VIP: Navigate to	Navigate to Main Menu -> Diameter -> Maintenance -> Applications

	Applications screen																						
3	SOAM VIP: Enable the PCA application	Select the PCA row(s) and Click Enable .																					
4	SOAM VIP: Verify that the PCA application has been Enabled.	Navigate to Main Menu -> Diameter -> Maintenance -> Applications Verify that the Application status has changed to Enabled-Available-Normal-Normal. <table border="1" data-bbox="402 552 1458 682"> <thead> <tr> <th>Application Name</th> <th>MP Server Hostname</th> <th>Admin State</th> <th>Operational Status</th> <th>Operational Reason</th> <th>Congestion Level</th> <th>Time of Last Update</th> </tr> </thead> <tbody> <tr> <td>PCA</td> <td>th-mp-th-2a</td> <td>Enabled</td> <td>Available</td> <td>Normal</td> <td>Normal</td> <td>2015-Mar-26 07:42:22 EDT</td> </tr> <tr> <td>PCA</td> <td>th-mp-th-1a</td> <td>Enabled</td> <td>Available</td> <td>Normal</td> <td>Normal</td> <td>2015-Mar-26 13:00:46 EDT</td> </tr> </tbody> </table> <p>NOTE: It may take some time (15-30 seconds) to initialize and change state.</p>	Application Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Congestion Level	Time of Last Update	PCA	th-mp-th-2a	Enabled	Available	Normal	Normal	2015-Mar-26 07:42:22 EDT	PCA	th-mp-th-1a	Enabled	Available	Normal	Normal	2015-Mar-26 13:00:46 EDT
Application Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Congestion Level	Time of Last Update																	
PCA	th-mp-th-2a	Enabled	Available	Normal	Normal	2015-Mar-26 07:42:22 EDT																	
PCA	th-mp-th-1a	Enabled	Available	Normal	Normal	2015-Mar-26 13:00:46 EDT																	
5	SOAM VIP: Enable PCA application on All Active SOAM servers	Repeat Steps 1 to 4 on All Active SOAM servers.																					

4.9.2 Enable SBR Databases

Detailed steps are given in the procedure below.

Procedure 24: Enable SBR Databases

S T E P #	<p>This procedure enables the SBR Databases.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>	
1 <input type="checkbox"/>	<p>Establish GUI Session on the active NOAMP VIP</p>	<p>Establish a GUI session on the Active NOAMP servers by using the XMI VIP address. Login as user "guiadmin".</p>
2 <input type="checkbox"/>	<p>NOAMP VIP: Navigate to SBR Database Status screen</p>	<p>Navigate to Main Menu -> SBR -> Maintenance -> SBR Database Status</p>
3 <input type="checkbox"/>	<p>NOAMP VIP: Prepare the SBR Database</p>	<p>Select the SBR Database and Click Prepare.</p> <p>NOTE: This step enables status monitoring of the database by all servers that will communicate with the database. In the Prepare state, the PCA application is not yet allowed to use the database.</p>
4 <input type="checkbox"/>	<p>NOAMP VIP: Verify that the SBR Database has been prepared.</p>	<p>Navigate to Main Menu -> SBR -> Maintenance -> SBR Database Status</p> <p>Verify that the SBR Database status has changed to Prepare – Prepared – N of N prepared – N of N prepared</p>  <p>NOTE: It may take some time (5-6 seconds) to change state.</p> <p>CAUTION: If the state does not change to "N of N prepared" it is recommended to fix the problems that are causing part or all of the database resource users and/or providers to not transit to prepared state. If the SBR Database is enabled while it is still in "Preparing" state calls may fail because users of the database do not have access to part or all the it.</p>
5 <input type="checkbox"/>	<p>NOAMP VIP: Enabled the SBR Database</p>	<p>Select the SBR Database and Click Enable.</p> <p>NOTE: Enabling the database allows the PCA application to begin reading and writing the database.</p>
6 <input type="checkbox"/>	<p>NOAMP VIP: Verify that the SBR Database has been enabled.</p>	<p>Navigate to Main Menu -> SBR -> Maintenance -> SBR Database Status</p> <p>Verify that the SBR Database status has changed to Enable – Normal – N of N available – N of N available</p>

7	NOAMP VIP: Enable PCA application on All Active SOAM servers	Thu May 07 07:37:41																			
		<div style="border: 1px solid gray; padding: 5px;"> <p>Filter ▾</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Database Name</th> <th>Administrative State</th> <th>Operational Status</th> <th>Resource User Operational Reason</th> <th>Resource Provider Operational Reason</th> <th>Reconfiguration In Progress</th> <th>Database Type</th> </tr> </thead> <tbody> <tr> <td>BindingSbrDb</td> <td>Enable</td> <td>Normal</td> <td>3 of 3 available</td> <td>2 of 2 available</td> <td>No</td> <td>Binding</td> </tr> <tr> <td>SessionSbrDb</td> <td>Enable</td> <td>Normal</td> <td>3 of 3 available</td> <td>2 of 2 available</td> <td>No</td> <td>Session</td> </tr> </tbody> </table> </div> <p>NOTE: It may take some time (5-6 seconds) to change state.</p>	Database Name	Administrative State	Operational Status	Resource User Operational Reason	Resource Provider Operational Reason	Reconfiguration In Progress	Database Type	BindingSbrDb	Enable	Normal	3 of 3 available	2 of 2 available	No	Binding	SessionSbrDb	Enable	Normal	3 of 3 available	2 of 2 available
Database Name	Administrative State	Operational Status	Resource User Operational Reason	Resource Provider Operational Reason	Reconfiguration In Progress	Database Type															
BindingSbrDb	Enable	Normal	3 of 3 available	2 of 2 available	No	Binding															
SessionSbrDb	Enable	Normal	3 of 3 available	2 of 2 available	No	Session															
		<p>Repeat Steps 1 to 6 for all SBR Databases which are to be enabled.</p> <p>NOTE: If all the verifications for SBR Database Status are successful, then proceed with the next step else STOP! And call ORACLE Customer Service for further assistance.</p>																			

4.9.3 Restart Process

Detailed steps are given in the procedure below.

Procedure 25: Restart Server

STEP #	<p>This procedure restarts the DSR and Policy and Charging SBR process.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>	
1	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2	NOAM VIP: Restart Process on DSR MP and Policy and Charging SBR Servers	<p>Navigate to Main Menu -> Status & Manage -> Server</p> <p>Select the MP servers with Function "DSR (multi-active cluster)" that are or will be handling PCA traffic and all MP servers with Function "Policy and Charging SBR" then Click Restart.</p> <p>NOTE: The Function of an MP Server is the same as the Function assigned to its Server Group in Main Menu -> Configuration -> Server Groups</p> <p>CAUTION:</p> <p>If the DSR system is processing traffic other than PCA then DO NOT restart all DA-MP servers simultaneously. Doing so will cause a network-wide outage. Please follow the procedure listed in APPENDIX-B to restart the DA-MP servers in a controlled order to minimize traffic loss.</p>

4.9.4 Enable Connections

Detailed steps are given in the procedure below.

Procedure 26: Enable connections

STEP	<p>This procedure enables the Diameter connection with Peer nodes.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p>
------	---

E P #	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.																																																									
1	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".																																																								
2	SOAM VIP: Navigate to Connections screen	Navigate to Main Menu -> Diameter -> Maintenance -> Connections																																																								
3	SOAM VIP: Enable all connections	Select all Connection rows for newly added PCA Peers Nodes and Click Enable .																																																								
4	SOAM VIP: Verify that the connections have been Enabled.	<p>Navigate to Main Menu -> Diameter -> Maintenance -> Connections</p> <p>Verify that the Admin state of all connections change to "Enabled" and the Operational Reason shows "Connecting" for connections to PCRF nodes and "Listening" for connections to other (policy client e.g. PCEF, AF etc.) nodes.</p> <p>Main Menu: Diameter -> Maintenance -> Connections Help</p> <p style="text-align: right;">Thu Feb 16 09:39:46 2012 EST</p> <p>Filter ▾</p> <table border="1"> <thead> <tr> <th>Connection Name</th> <th>MP Server Hostname</th> <th>Admin State</th> <th>Operational Status</th> <th>Operational Reason</th> <th>Connection Mode</th> <th>Local Node</th> <th>Peer No</th> </tr> </thead> <tbody> <tr> <td>conn_af</td> <td>blade14</td> <td>Enabled</td> <td>Unavailable</td> <td>Listening</td> <td>Responder Only</td> <td>PDRA</td> <td>AF</td> </tr> <tr> <td>conn_pcef1</td> <td>blade14</td> <td>Enabled</td> <td>Unavailable</td> <td>Listening</td> <td>Responder Only</td> <td>PDRA</td> <td>PCEF1</td> </tr> <tr> <td>conn_pcef2</td> <td>blade14</td> <td>Enabled</td> <td>Unavailable</td> <td>Listening</td> <td>Responder Only</td> <td>PDRA</td> <td>PCEF2</td> </tr> <tr> <td>conn_pcrf1</td> <td>blade14</td> <td>Enabled</td> <td>Unavailable</td> <td>Connecting</td> <td>Initiator Only</td> <td>PDRA</td> <td>PCRF1</td> </tr> <tr> <td>conn_pcrf2</td> <td>blade14</td> <td>Enabled</td> <td>Unavailable</td> <td>Connecting</td> <td>Initiator Only</td> <td>PDRA</td> <td>PCRF2</td> </tr> </tbody> </table> <p>NOTE 1:</p> <p>For connections of type "Responder Only" (client nodes), the Operational Status and Reason will be "Unk" if using TSA.</p> <table border="1"> <tbody> <tr> <td>conn_af1</td> <td></td> <td>Enabled</td> <td>Unk</td> <td>Unk</td> <td>Responder Only</td> <td>PDRA</td> <td>AF1</td> </tr> </tbody> </table> <p>NOTE 2:</p> <p>It may take some time (15-30 seconds) to initialize and change state. Responder Only connections will remain in Listening Operational Status until the peer node initiates the connection</p>	Connection Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Connection Mode	Local Node	Peer No	conn_af	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	AF	conn_pcef1	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	PCEF1	conn_pcef2	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	PCEF2	conn_pcrf1	blade14	Enabled	Unavailable	Connecting	Initiator Only	PDRA	PCRF1	conn_pcrf2	blade14	Enabled	Unavailable	Connecting	Initiator Only	PDRA	PCRF2	conn_af1		Enabled	Unk	Unk	Responder Only	PDRA	AF1
Connection Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Connection Mode	Local Node	Peer No																																																			
conn_af	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	AF																																																			
conn_pcef1	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	PCEF1																																																			
conn_pcef2	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	PCEF2																																																			
conn_pcrf1	blade14	Enabled	Unavailable	Connecting	Initiator Only	PDRA	PCRF1																																																			
conn_pcrf2	blade14	Enabled	Unavailable	Connecting	Initiator Only	PDRA	PCRF2																																																			
conn_af1		Enabled	Unk	Unk	Responder Only	PDRA	AF1																																																			

4.9.5 Perform Health Check

Execute this Procedure to verify the sanity of the system.

Procedure 27: Perform Health Check

S T E P #	<p>This procedure performs a Health Check.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>	
1 <input type="checkbox"/>	<p>Verify SBR Database Status</p>	<ol style="list-style-type: none"> 1. Log into the NOAM GUI using the XMI VIP address. 2. Navigate to Main Menu: SBR -> Maintenance -> SBR Database Status 3. Verify that the status for all the SBR Database rows have the following values Administrative State = Enabled Operational Status = Normal Resource User Operational Reason = X of X available Resource Provider Operational Reason = Y of Y available <p>If all the verifications are successful, then proceed with next step else STOP! And call ORACLE Customer Service for further assistance.</p>
2 <input type="checkbox"/>	<p>Verify the Policy and Charging SBR Status</p>	<ol style="list-style-type: none"> 1. Log into the NOAM GUI using the XMI VIP address. 2. Navigate to Main Menu: SBR -> Maintenance -> SBR Status 3. Verify that the server "Resource HA Role" is shown as "Active/Standby/Spare" and 'Congestion Level' is 'Normal' for all the "Binding Region" and 'Mated Site" tabs. <p>The Resource HA Role of Standby applies if there is server level redundancy configured in the DSR system. The Resource HA Role of Spare applies if there is site level redundancy configured in the DSR system.</p> <p>If all the verifications are successful, then proceed with signaling call flow execution else STOP! And call ORACLE Customer Service for further assistance.</p>
3 <input type="checkbox"/>	<p>Verify there are no PCA Alarms raised</p>	<ol style="list-style-type: none"> 1. Log into the NOAM GUI using the XMI VIP address. 2. Navigate to Main Menu: Alarms & Events -> View Active 3. Verify that there are no Alarms raised with Product PCA/SBR. <p>If all the verifications are successful, then proceed with signaling call flow execution else STOP! And call ORACLE Customer Service for further assistance.</p>

5.0 CAVEATS

7.0 APPENDIX-A

7.1 PCA FEATURE ACTIVATION PROCEDURE

This section provides the detailed procedure steps of the PCA activation.

The procedures in this section need to be executed in the following order:

- For PCA activation on the entire network
 - Section 7.1.1 PCA Activation on an installed or upgraded system
 - Section 7.1.3 Restart Process
 - Section 7.1.4 Post PCA Activation System Health Check
- For PCA activation on a newly added site
 - Section 7.1.2 PCA Activation on a newly added site
 - Section 7.1.3 Restart Process
 - Section 7.1.4.2 System health check after Application Activation on SOAM servers

7.1.1 PCA Activation on an installed or upgraded system

Detailed steps are given in the procedure below.

Procedure 28: Verify PCA Activation Pre-Requisites

S T E P #	<p>This procedure ensures that pre-requisites for activating PCA on an installed or upgraded system have been fulfilled.</p> <p>This Procedure does not require a Maintenance Window</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p> <p>NOTE: - PLEASE COMPLETE THE TOPOLOGY CONFIGURATION OF ALL THE REQUIRED SOAM SERVERS BEFORE CONTINUING THIS STEP. SEE [1] AND [2] FOR STEPS.</p>																													
1	<p>NOAM VIP: Check the software version on all servers.</p>	<p>Navigate to Main Menu: Administration -> Software Management -> Upgrade</p> <p>Verify that the Upgrade ISO column shows the correct release number for all servers in the DSR network.</p> <p>NOTE: All servers in the network must be on the same DSR release when activating PCA.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>NO_SG</th> <th>BSBR_SG_SiteA</th> <th>DAMP_SG_SiteA</th> <th>DAMP_SG_SiteB</th> <th>SO_SG_SiteA</th> <th>SO_SG_SiteB</th> <th>SSBR_SG_SiteA</th> </tr> </thead> <tbody> <tr> <td>Hostname</td> <td>Upgrade State</td> <td>OAM Max HA Role</td> <td>Server Role</td> <td>Function</td> <td colspan="2">Application Version</td> </tr> <tr> <td></td> <td>Server Status</td> <td>Appl Max HA Role</td> <td>Network Element</td> <td></td> <td colspan="2">Upgrade ISO</td> </tr> <tr> <td>NOAM01Resize</td> <td>Ready Warn</td> <td>Active N/A</td> <td>Network OAM&P NO_1030101</td> <td>OAM&P</td> <td colspan="2">7.2.0.0-72.17.0</td> </tr> </tbody> </table>	NO_SG	BSBR_SG_SiteA	DAMP_SG_SiteA	DAMP_SG_SiteB	SO_SG_SiteA	SO_SG_SiteB	SSBR_SG_SiteA	Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version			Server Status	Appl Max HA Role	Network Element		Upgrade ISO		NOAM01Resize	Ready Warn	Active N/A	Network OAM&P NO_1030101	OAM&P	7.2.0.0-72.17.0	
NO_SG	BSBR_SG_SiteA	DAMP_SG_SiteA	DAMP_SG_SiteB	SO_SG_SiteA	SO_SG_SiteB	SSBR_SG_SiteA																								
Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version																									
	Server Status	Appl Max HA Role	Network Element		Upgrade ISO																									
NOAM01Resize	Ready Warn	Active N/A	Network OAM&P NO_1030101	OAM&P	7.2.0.0-72.17.0																									
2	<p>NOAM VIP: Check the Upgrade Acceptance status on all servers.</p>	<p>Navigate to Main Menu: Administration -> Software Management -> Upgrade</p> <p>Verify that the Upgrade State column does not show "ACCEPT OR REJECT".</p>																												

NOTE: Upgrade must be accepted on all servers before activating PCA.

NO_SG	BSBR_SG_SiteA	DAMP_SG_SiteA	DAMP_SG_SiteB	SO_SG_SiteA	SO_SG_SiteB	SSBR_SG_Siti
Hostname	Upgrade State	OAM Max HA Role	Server Role	Function	Application Version	
	Server Status	Appl Max HA Role	Network Element			Upgrade ISO
NOAM01Resize	Ready	Active	Network OAM&P	OAM&P	7.2.0.0-72.17.0	
	Warn	N/A	NO_1030101			

If the Upgrade State is "ACCEPT OR REJECT", follow the Installation Guide^[2] or Upgrade Guide^[6] (whichever applies) to accept the upgrade on all servers prior to activating PCA.

Procedure 29: PCA Activation on the entire network

S T E P #	This procedure activates the PCA on complete system. This Procedure does not require a Maintenance Window Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> . NOTE: - PLEASE COMPLETE THE TOPOLOGY CONFIGURATION OF ALL THE REQUIRED SOAM SERVERS BEFORE CONTINUING THIS STEP. SEE [1] AND [2] FOR STEPS.	
	1	Verify configuration of All SOAM servers Before continuing all SOAM servers should be configured in the topology. 1. Log into the NOAM VIP GUI. 2. Navigate Main Menu: Status & Manage -> Server . See all required SOAM servers are configured and Application State is enabled.
	2	Establish a secure shell Session on the active NOAM Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as user "admusr". Use your SSH client to connect to the server (ex. Putty) Note: you must consult your own software client's documentation to learn how to launch a connection. For example: <pre># ssh <active NO XMI VIP Address></pre>
	3	Change to the following directory: <pre># cd /usr/TKLC/dsr/prod/maint/loaders/activate</pre>
	4	PCA Activation: Execute the PCA application activation script <pre># ./load.pcaActivationTopLevel</pre> Note: - This command execution starts Activation on NOAM servers and All Active SOAM servers. Check log file <code>/var/TKLC/log/pcaActivationTopLevel.log</code> to see if there is any execution failure. If the activation fails, then execute the procedure in Section 7.2.2 to restore the system back to state before start of activation.
5	PCA Application Activation Delete all GUI cache files on active SOAM and NOAM for quick view of changes or wait for some time so that new changes can reflect.	

<input type="checkbox"/>	(OPTIONAL): Clear the Web Server cache	# <code>clearCache</code>
--------------------------	--	---------------------------

7.1.2 PCA Activation on a newly added site

Detailed steps are given in the procedure below.

THIS PROCEDURE NEEDS TO BE EXECUTED ONLY IF A NEW SITE IS ADDED TO AN EXISTING CONFIGURED SYSTEM.

This procedure activates the PCA on newly added site only. This section is only valid if system is already configured and a new site is added to the system at a later stage. **Skip this step if system is new for configuration.**

Procedure 30: PCA Activation on newly added site

S T E P #	This procedure activates the PCA on a single site newly added to the DSR topology.	
	This Procedure does not require a Maintenance Window	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.	
1 <input type="checkbox"/>	Verify configuration of All SOAM servers for the newly added site	Before continuing all SOAM servers for the newly added site should be configured in the topology. <ol style="list-style-type: none"> 1. Log into the NOAM VIP GUI. 2. Navigate Main Menu: Status & Manage -> Server. See all required SOAM servers for the newly added site are configured and Application State is enabled.
2 <input type="checkbox"/>	Execute the activation procedure	For PCA activation on new site, the activation procedure needs to be executed from the NOAM. Execute the Procedures in Section 7.1.1.

7.1.3 Restart Process

Detailed steps are given in the procedure below.

Procedure 31: Restart Process

S T E P #	This procedure restarts the DSR and SBR application processes.	
	This Procedure needs to be performed in a Maintenance Window	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.	
NOTE: If PCA Activation is being performed on a newly added site, this procedure is limited to the servers belonging to that site only.		
1 <input type="checkbox"/>	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2 <input type="checkbox"/>	NOAM VIP: Restart Process on DA-MP Servers	Navigate to Main Menu -> Status & Manage -> Server Select all the DA-MP servers and press Restart . CAUTION: If the DSR system is processing traffic other than PCA then DO NOT restart all DA-MP servers simultaneously. Doing so will cause a network-wide outage. Please follow the procedure listed in APPENDIX-B to restart the DA-MP servers in a controlled order to minimize traffic loss.
3 <input type="checkbox"/>	NOAM VIP: Restart Process on SBR	Navigate to Main Menu -> Status & Manage -> Server

<input type="checkbox"/>	Servers	Select all the SBR servers and press Restart .
--------------------------	---------	---

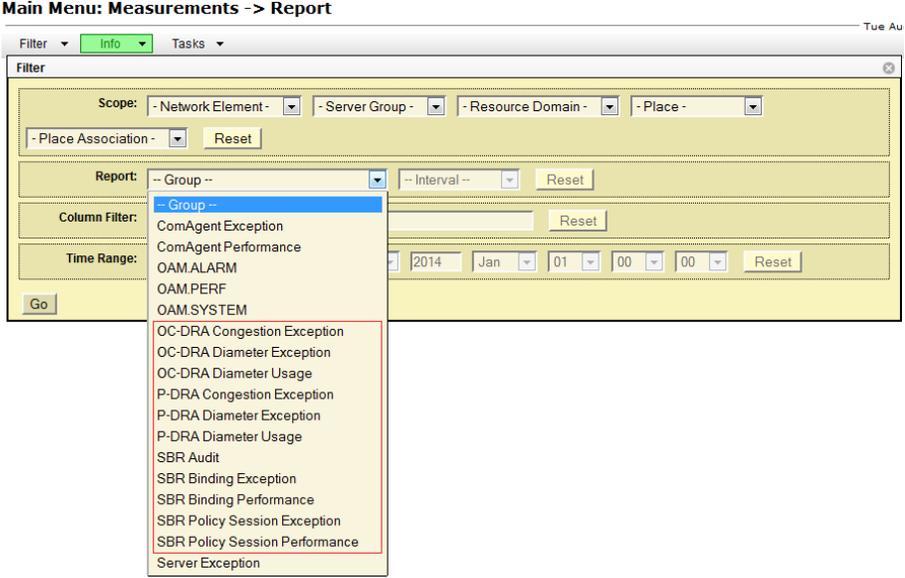
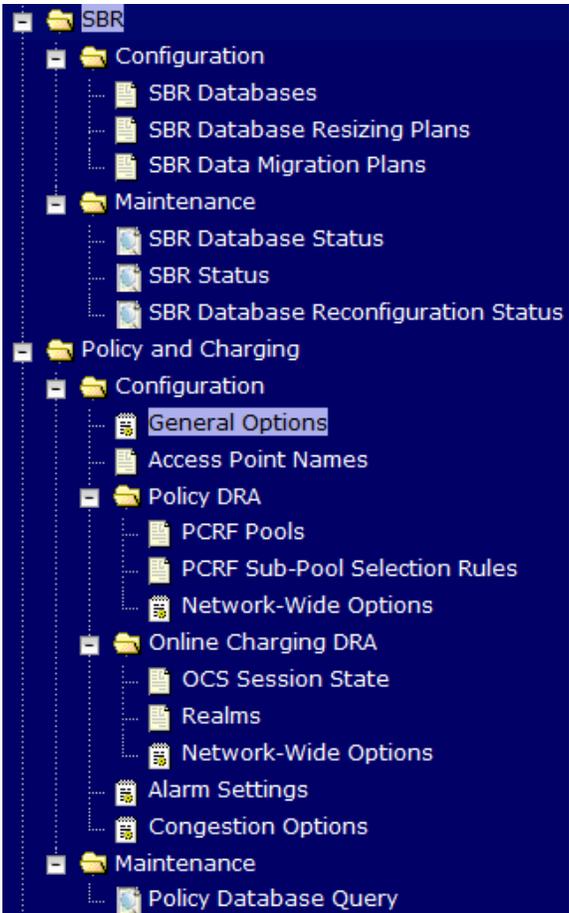
7.1.4 Post PCA Activation System Health Check

7.1.4.1 System health check after Application Activation on NOAM server

Detailed steps are given in the procedure below.

Procedure 32: Verification of application activation on NOAM Server

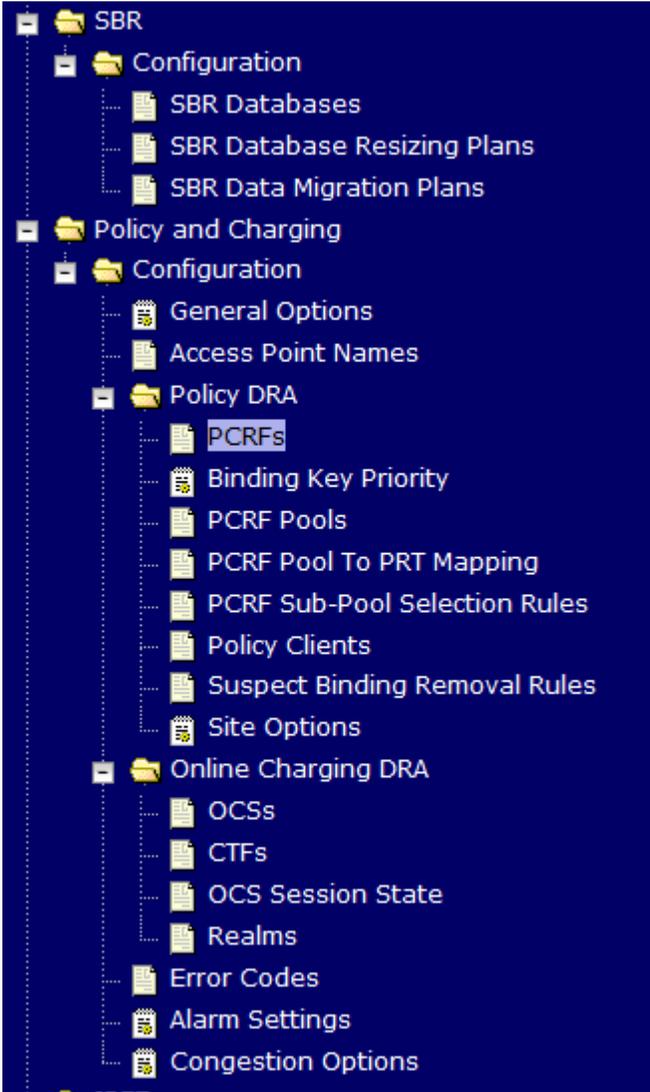
S	This procedure verifies the PCA application activation on NOAM Server.																												
T	This Procedure does not require a Maintenance Window																												
E	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.																												
P	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .																												
#																													
1	Active NOAM VIP: Establish GUI Session on the NOAM VIP	Establish a GUI session on the Active NOAM by using the XMI VIP address. Login as user "guiadmin".																											
2	NOAM VIP: Verify that the Resource Domain Profile show the new profile entries.	<p>Verify that the Resource Domain Profile show the new profile entries.</p> <p>Main Menu: Configuration -> Resource Domains [Insert]</p> <hr/> <p>Inserting a new Resource Domain</p> <table border="1"> <thead> <tr> <th>Resource Domain</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Resource Domain Name</td> <td><input type="text"/></td> <td>Unique identifier used to label a Resource Domain. [Default = n/a. Range = A 1-32 characters are alphanumeric and underscore.]</td> </tr> <tr> <td>Resource Domain Profile</td> <td>- Select Resource Domain Profile -</td> <td>The Profile of this Resource Domain</td> </tr> <tr> <td>Server Groups</td> <td>- Select Resource Domain Profile -</td> <td></td> </tr> <tr> <td></td> <td>NONE</td> <td></td> </tr> <tr> <td></td> <td>Policy Session</td> <td></td> </tr> <tr> <td></td> <td>Policy Binding</td> <td></td> </tr> <tr> <td></td> <td>Policy and Charging DRA</td> <td></td> </tr> <tr> <td></td> <td>Authn/sgs</td> <td></td> </tr> </tbody> </table>	Resource Domain	Value	Description	Resource Domain Name	<input type="text"/>	Unique identifier used to label a Resource Domain. [Default = n/a. Range = A 1-32 characters are alphanumeric and underscore.]	Resource Domain Profile	- Select Resource Domain Profile -	The Profile of this Resource Domain	Server Groups	- Select Resource Domain Profile -			NONE			Policy Session			Policy Binding			Policy and Charging DRA			Authn/sgs	
Resource Domain	Value	Description																											
Resource Domain Name	<input type="text"/>	Unique identifier used to label a Resource Domain. [Default = n/a. Range = A 1-32 characters are alphanumeric and underscore.]																											
Resource Domain Profile	- Select Resource Domain Profile -	The Profile of this Resource Domain																											
Server Groups	- Select Resource Domain Profile -																												
	NONE																												
	Policy Session																												
	Policy Binding																												
	Policy and Charging DRA																												
	Authn/sgs																												
3	NOAM VIP: Verify that the PCA specific KPIs are shown.	<p>Verify that KPIs menu shows the KPI tabs for PCA, SBR, SBR-Binding and SBR-Sessoin.</p> <p>Main Menu: Status & Manage -> KPIs</p> <hr/> <p>Filter ▾ Tasks ▾</p> <table border="1"> <tr> <td>Entire-Network</td> <td>Dsr70PcaBind-a</td> <td>Dsr70PcaBind-b</td> <td>Dsr70PcaDaMP-a</td> </tr> <tr> <td>ComAgent</td> <td style="border: 2px solid red;">PCA</td> <td style="border: 2px solid red;">SBR</td> <td style="border: 2px solid red;">SBR-Binding</td> </tr> <tr> <td></td> <td style="border: 2px solid red;">SBR-Session</td> <td>Server</td> <td></td> </tr> </table>	Entire-Network	Dsr70PcaBind-a	Dsr70PcaBind-b	Dsr70PcaDaMP-a	ComAgent	PCA	SBR	SBR-Binding		SBR-Session	Server																
Entire-Network	Dsr70PcaBind-a	Dsr70PcaBind-b	Dsr70PcaDaMP-a																										
ComAgent	PCA	SBR	SBR-Binding																										
	SBR-Session	Server																											
4	NOAM VIP: Verify that the PCA specific Measurement groups are shown.	Verify that Measurement groups are shown for OC-DRA, P-DRA and PSBR.																											

	
<p>5 NOAM VIP: Verify that the Main Menu shows the Policy and Charging submenu.</p>	<p>Verify that Main Menu on Active NOAM shows the Policy and Charging and SBR submenus with Configuration and Maintenance screens.</p> 

7.1.4.2 System health check after Application Activation on SOAM servers

Detailed steps are given in the procedure below.

Procedure 33: Verification of application activation on SOAM Servers

<p>S T E P #</p>	<p>This procedure verifies the activation of PCA on SOAM Servers.</p> <p>This Procedure does not require a Maintenance Window</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p><u>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</u></p>	
<p>1 <input type="checkbox"/></p>	<p>SOAM VIP: Establish GUI Session using SOAM VIP</p>	<p>Establish a GUI session on the Active SOAM by using the XMI VIP address. Login as user "guiadmin".</p>
<p>2 <input type="checkbox"/></p>	<p>SOAM VIP: Verify that the Policy and Charging folder is visible in the Left Hand Menu</p>	<p>Verify that the Policy and Charging folder appears on the Left Hand Menu:</p> 

7.2 PCA FEATURE DEACTIVATION PROCEDURE

This section provides the detailed steps of the PCA Deactivation procedures.

The procedures in this section need to be executed in the following order:

- For PCA deactivation on the entire network
 - Section 7.2.1 Pre PCA Deactivation Steps
 - Section 7.2.2 PCA Deactivation Procedure
 - Section 7.2.4 Post PCA Deactivation Steps
 - Section 7.2.5 Post PCA Deactivation System Health Check
- For PCA deactivation on a site (in the case when the site is being decommissioned)
 - Section 7.2.3 Site Specific PCA Deactivation Procedure
 - Section 7.2.4 Post PCA Deactivation Steps
 - Section 7.2.5.2 System health check after Application Deactivation on SOAM servers

7.2.1 Pre PCA Deactivation Steps

7.2.1.1 Verify and Deactivate the GLA application

Detailed steps are given in the procedure below.

Procedure 34: Verify and Deactivate GLA application

S T E P #	This procedure verifies that GLA is activated and then deactivates the GLA application.	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
	NOTE: - PLEASE VERIFY FIRST THAT GLA IS ACTIVATED IN STEPS 1-2 AND THEN EXECUTE THE STEPS 4-5 TO DEACTIVATE THE GLA APPLICATION.	
	1 <input type="checkbox"/>	Establish GUI Session on the SOAM VIP
2 <input type="checkbox"/>	SOAM VIP: Navigate to Applications screen	Navigate to Main Menu -> Diameter -> Maintenance -> Applications
3 <input type="checkbox"/>	SOAM VIP: Verify the GLA application is present.	Check the presence of GLA application. If GLA application record is present. It means GLA is activated on this system. NOTE: - IF GLA RECORD IS NOT PRESENT ON THIS SCREEN, THEN SKIP THE REMAINING STEPS IN THIS PROCEDURE.
4 <input type="checkbox"/>	SOAM VIP: Deactivate the GLA application.	If GLA record is present in the Applications screen. Then execute the steps to deactivate the GLA application as per deactivation procedures defined in [8] .
5 <input type="checkbox"/>	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Step 1-4 on All Active SOAM servers.

7.2.1.2 Unconfigure PCA Functions

Detailed steps are given in the procedure below.

Procedure 35: Unconfigure PCA Functions (PDRA and OCDRA)

S T E P #	This procedure unconfigures the PCA Functions – Policy DRA and Online Charging DRA. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES.	
	1 <input type="checkbox"/>	Unconfigure Policy DRA Navigate to Main Menu: Policy and Charging -> Configuration -> General Options If Policy DRA is enabled, Execute the steps in Section 4.7 to unconfigure Policy DRA
2 <input type="checkbox"/>	Unconfigure Online Charging DRA Navigate to Main Menu: Policy and Charging -> Configuration -> General Options If Online Charging DRA is enabled, Execute the steps in Section 4.8 to unconfigure Online Charging DRA	

7.2.1.3 Disable Diameter Connections

Detailed steps are given in the procedure below.

Procedure 36: Disable Diameter Connections

S T E P #	This procedure disables the Diameter connections. This Procedure does not require a Maintenance Window Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND <u>ASK FOR ORACLE TAC.</u>																											
	1 <input type="checkbox"/>	Establish GUI Session on the SOAM VIP Establish a GUI session on all the Active SOAM by using the XMI VIP address. Login as user "guiadmin".																										
	2 <input type="checkbox"/>	SOAM VIP: Disable DSR connections. Navigate to Main Menu: Diameter -> Maintenance -> Connections Select all the PCA specific diameter connections and click disable or click Disable All (if applicable). The Admin State of connections should be shown as Disabled. Main Menu: Diameter -> Maintenance -> Connections He Tue Jun 12 11:26:40 2012 UT <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Filter ▾ <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>Connection Name</th> <th>MP Server Hostname</th> <th>Admin State</th> <th>Operational Status</th> <th>Operational Reason</th> <th>Connection Mode</th> <th>Local Node</th> <th>Peer Node</th> <th>Remote IP Addresses</th> </tr> </thead> <tbody> <tr> <td>conn_af</td> <td>blade12</td> <td style="border: 2px solid red;">Disabled</td> <td>Unavailable</td> <td>Disabled</td> <td>Responder Only</td> <td>PDRA</td> <td>AF1</td> <td>---</td> </tr> <tr> <td>conn_pcef</td> <td>blade12</td> <td style="border: 2px solid red;">Disabled</td> <td>Unavailable</td> <td>Disabled</td> <td>Responder Only</td> <td>PDRA</td> <td>PCEF1</td> <td>---</td> </tr> </tbody> </table> </div>	Connection Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Connection Mode	Local Node	Peer Node	Remote IP Addresses	conn_af	blade12	Disabled	Unavailable	Disabled	Responder Only	PDRA	AF1	---	conn_pcef	blade12	Disabled	Unavailable	Disabled	Responder Only	PDRA	PCEF1
Connection Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Connection Mode	Local Node	Peer Node	Remote IP Addresses																				
conn_af	blade12	Disabled	Unavailable	Disabled	Responder Only	PDRA	AF1	---																				
conn_pcef	blade12	Disabled	Unavailable	Disabled	Responder Only	PDRA	PCEF1	---																				
3 <input type="checkbox"/>	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Steps 1 to 2 on All Active SOAM servers.																										

7.2.1.4 **Disable Application**

Detailed steps are given in the procedure below.

Procedure 37: Disable application

S T E P #	<p>This procedure disables the PCA application.</p> <p>This Procedure does not require a Maintenance Window</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>																
	1 <input type="checkbox"/>	<p>Establish GUI Session on the SOAM VIP</p> <p>Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".</p>															
	2 <input type="checkbox"/>	<p>SOAM VIP: Navigate to Applications screen</p> <p>Navigate to Main Menu -> Diameter -> Maintenance -> Applications</p>															
	3 <input type="checkbox"/>	<p>SOAM VIP: Disable the PCA application</p> <p>Select the PCA row and press Disable.</p> <p>If there are multiple DA-MPs under this SOAM then there will be multiple entries of PCA in this screen. Select all the entries and click Disable.</p>															
	4 <input type="checkbox"/>	<p>SOAM VIP: Verify that the PCA application has been Disabled.</p> <p>Navigate to Main Menu -> Diameter -> Maintenance -> Applications</p> <p>Verify that the Application status has changed to Disabled.</p> <p>Main Menu: Diameter -> Maintenance -> Applications Help</p> <p style="text-align: right;">Tue Jun 12 06:33:59 2012 UTC</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #d3d3d3;">Filter</th> <th style="background-color: #d3d3d3;">DSR Application Name</th> <th style="background-color: #d3d3d3;">MP Server Hostname</th> <th style="background-color: #d3d3d3;">Admin State</th> <th style="background-color: #d3d3d3;">Operational State</th> <th style="background-color: #d3d3d3;">Operational Reason</th> <th style="background-color: #d3d3d3;">Congestion Level</th> <th style="background-color: #d3d3d3;">Time of Last Update</th> </tr> </thead> <tbody> <tr> <td></td> <td>PCA</td> <td>blade12</td> <td style="border: 1px solid red;">Disabled</td> <td>Unavailable</td> <td style="background-color: orange;">Not Initialized</td> <td>Normal</td> <td>2012-Jun-12 06:33:43 UTC</td> </tr> </tbody> </table>	Filter	DSR Application Name	MP Server Hostname	Admin State	Operational State	Operational Reason	Congestion Level	Time of Last Update		PCA	blade12	Disabled	Unavailable	Not Initialized	Normal
Filter	DSR Application Name	MP Server Hostname	Admin State	Operational State	Operational Reason	Congestion Level	Time of Last Update										
	PCA	blade12	Disabled	Unavailable	Not Initialized	Normal	2012-Jun-12 06:33:43 UTC										
5 <input type="checkbox"/>	<p>SOAM VIP: Perform steps on All Active SOAM Servers</p> <p>Repeat Steps 1 to 4 on All Active SOAM servers.</p>																

7.2.1.5 Remove DSR Configuration Data

Detailed steps are given in the procedure below.

Procedure 38: Remove DSR configuration data

S T E P #	<p>This procedure removes the DSR configuration data.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p> <p>NOTE:-</p> <p style="text-align: center;">A.) PLEASE DON'T EXECUTE THIS STEP IF YOU ARE GOING TO ACTIVATE PCA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE CONFIGURATION DATA AFTER RE-ACTIVATION.</p>	
	1	<p>Establish GUI Session on the SOAM VIP</p> <p>Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".</p>
	2	<p>SOAM VIP: Remove Application Routing Rules.</p> <p>Main Menu: Diameter -> Configuration -> Application Routing Rules</p> <p>Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.</p>
	3	<p>SOAM VIP: Remove Peer Routing Rules.</p> <p>Main Menu: Diameter -> Configuration -> Peer Routing Rules</p> <p>Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.</p>
	4	<p>SOAM VIP: Remove Route Lists</p> <p>Main Menu: Diameter -> Configuration -> Route Lists</p> <p>Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.</p>
	5	<p>SOAM VIP: Remove Route Groups</p> <p>Main Menu: Diameter -> Configuration -> Route Groups</p> <p>Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.</p>
	6	<p>SOAM VIP: Remove Connections.</p> <p>Main Menu: Diameter -> Configuration -> Connections</p> <p>Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.</p>
	7	<p>SOAM VIP: Remove Peer Nodes.</p> <p>Main Menu: Diameter -> Configuration -> Peer Nodes</p> <p>Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.</p>
	8	<p>SOAM VIP: Remove Local Nodes.</p> <p>Main Menu: Diameter -> Configuration -> Local Nodes</p> <p>Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.</p>
	9	<p>SOAM VIP: Remove CEX Configuration Sets</p> <p>Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets</p> <p>Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.</p>
10	<p>SOAM VIP: Remove CEX Parameters.</p> <p>Main Menu: Diameter -> Configuration -> CEX Parameters.</p>	

<input type="checkbox"/>		Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.
<input type="checkbox"/>	11 SOAM VIP: Remove Application IDs	Main Menu: Diameter -> Configuration -> Application Ids Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.
<input type="checkbox"/>	12 SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Steps 1 to 11 on All Active SOAM servers.

7.2.2 PCA Deactivation Procedure

Detailed steps are given in the procedure below.

Procedure 39: PCA Application Deactivation

S T E P #	This procedure deactivates the PCA application.	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC .	
	1	<p>Establish a secure shell Session on the active NOAM</p> <p>Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as user "admusr".</p> <p>Use your SSH client to connect to the server (ex. putty)</p> <p>Note: you must consult your own software client's documentation to learn how to launch a connection. For example:</p> <pre style="text-align: center;"># ssh <active NO XMI IP Address></pre>
	2	<p>PCA Deactivation: Change directory</p> <p>Change to the following directory:</p> <pre style="text-align: center;"># cd /usr/TKLC/dsr/prod/maint/loaders/deactivate</pre>
3	<p>PCA Deactivation: Execute the PCA application deactivation script</p> <pre style="text-align: center;"># ./load.pcaDeactivationTopLevel</pre> <p>Note: - This command execution will starts Deactivation on Active NOAM and All Active SOAM servers.</p> <p>Check log file <code>/var/TKLC/log/pcaDeactivationTopLevel.log</code> to see if there is any execution failure.</p>	
4	<p>PCA Deactivation [OPTIONAL]: Clear the Web Server cache</p> <pre style="text-align: center;"># clearCache</pre> <p>Delete all GUI cache files on active SOAM and NOAM for quick view of changes or wait for some time so that new changes can reflect.</p>	

7.2.3 Site Specific PCA Deactivation Procedure

THIS SECTION NEEDS TO BE EXECUTED WHEN PCA NEEDS TO BE DEACTIVATED FROM A PARTICULAR SITE.

Detailed steps are given below.

Procedure 40: PCA Application Deactivation on a particular site.

S T E P #	<p>This procedure deactivates the PCA application on a particular site.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>	
1 <input type="checkbox"/>	<p>Establish a secure shell Session on the active SOAM or on which deactivation is required.</p>	<p>Establish a secure shell session on the active SOAM by using the XMI VIP address. Login as user "admusr".</p> <p>Use your SSH client to connect to the server (ex. putty)</p> <p>Note: you must consult your own software client's documentation to learn how to launch a connection. For example:</p> <pre style="text-align: center;"># ssh <active SO XMI IP Address></pre>
2 <input type="checkbox"/>	<p>PCA Deactivation: Change directory</p>	<p>Change to the following directory:</p> <pre style="text-align: center;"># cd /usr/TKLC/dsr/prod/maint/loaders/deactivate</pre>
3 <input type="checkbox"/>	<p>PCA Deactivation: Execute the PCA application deactivation script</p>	<pre style="text-align: center;"># ./load.pcaDeactivateBscoped</pre> <p>Note: - This command execution will start Deactivation on selected active SOAM server.</p> <p>Check log file <code>/var/TKLC/log/pcaDeactivateBscoped.log</code> to see if there is any execution failure.</p>
4 <input type="checkbox"/>	<p>PCA Deactivation [OPTIONAL]: Clear the Web Server cache</p>	<p>Delete all GUI cache files on active SOAM and NOAM for quick view of changes or wait for some time so that new changes can reflect.</p> <pre style="text-align: center;"># clearCache</pre>

7.2.4 Post PCA Deactivation Steps

IF PCA DEACTIVATION IS BEING PERFORMED ON A SINGLE SITE, THE PROCEDURES IN THIS SECTION APPLY TO THE SERVERS BELONGING TO THAT SITE ONLY.

7.2.4.1 Move Policy and Charging SBR Servers to OOS State

Detailed steps are given in the procedure below.

Procedure 41: Move Policy and Charging SBR Servers to OOS State

S T E P #	This procedure puts all the MP Servers in Policy and Charging SBR Server Groups in OOS.	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
	NOTE: - PLEASE DON'T EXECUTE THIS STEP IF YOU ARE GOING TO ACTIVATE PCA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE CONFIGURATION DATA AFTER RE-ACTIVATION.	
	1 <input type="checkbox"/>	Establish GUI Session on the NOAM VIP
2 <input type="checkbox"/>	NOAM VIP: Navigate to Server Groups screen	Navigate to Main Menu: Configuration -> Server Groups
3 <input type="checkbox"/>	NOAM VIP: Find the Server List	Find the Servers with Function as "Policy and Charging SBR".
4 <input type="checkbox"/>	NOAM VIP: Navigate to HA screen	Navigate to Main Menu: Status & Manage -> HA Edit the Servers from list created in Step 3. Change the value of "Max Allowed HA Role" to OOS.

7.2.4.2 Remove Policy and Charging SBR Servers from Server Groups

Detailed steps are given in the procedure below.

Procedure 42: Remove Policy and Charging SBR Servers from Server Groups

S T E P #	This procedure removes all the MP Servers in Policy and Charging SBR Server Groups from their respective Server Groups.	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
	PREREQUISITE: PREVIOUS PROCEDURE HAS BEEN EXECUTED.	
	1 <input type="checkbox"/>	Establish GUI Session on the NOAM VIP
2 <input type="checkbox"/>	NOAM VIP: Navigate to Server Groups screen	Navigate to Main Menu: Configuration -> Server Groups
3 <input type="checkbox"/>	NOAM VIP: Find the Server List	Find the Servers with Function as "Policy and Charging SBR".
4 <input type="checkbox"/>	NOAM VIP: Edit the Server Groups.	Navigate to Main Menu: Configuration -> Server Groups

<input type="checkbox"/>	Edit the Server Group with "Policy and Charging SBR" function and remove the servers from it. Repeat the steps with all server groups with "Policy and Charging SBR" function.
--------------------------	---

7.2.4.3 Delete Server Groups related to Policy and Charging SBR

Detailed steps are given in the procedure below.

Procedure 43: Delete Server Groups related to Policy and Charging SBR

S	This procedure removes the Server Groups related to Policy and Charging SBR.	
T	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
P	# PREREQUISITE: PREVIOUS PROCEDURE HAS BEEN EXECUTED.	
1	<input type="checkbox"/>	Establish GUI Session on the NOAM VIP
		Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2	<input type="checkbox"/>	NOAM VIP: Navigate to Server Groups Screen
		Navigate to Main Menu: Configuration -> Server Groups
3	<input type="checkbox"/>	NOAM VIP: Remove Server Groups Resource Domains
		Remove the Server Groups which has Function value "Policy and Charging SBR".

7.2.4.4 Remove Place Configuration Data

Detailed steps are given in the procedure below.

Procedure 44: Remove Place configuration data

S	This procedure removes the Place configuration data.	
T	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
P	# NOTE: - PLEASE DON'T EXECUTE THIS STEP IF YOU ARE GOING TO ACTIVATE PCA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE CONFIGURATION DATA AFTER RE-ACTIVATION.	
1	<input type="checkbox"/>	Establish GUI Session on the NOAM VIP
		Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2	<input type="checkbox"/>	NOAM VIP: Remove all the data from Place screen as mentioned.
		Main Menu: Configuration -> Places Edit the Places and Remove Servers from it.

7.2.4.5 Reboot the Servers

Detailed steps are given in the procedure below.

Procedure 45: Reboot the Servers

S	This procedure removes the merge data from Servers by rebooting them.	
T	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E		

P #	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .	
1 <input type="checkbox"/>	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2 <input type="checkbox"/>	NOAM VIP: Navigate to Server Groups Screen	Navigate to Main Menu: Status & Manage -> Server
3 <input type="checkbox"/>	NOAM VIP: Reboot the Servers.	<p>Reboots all the relevant servers.</p> <p>Select all the MP servers having Function "Policy and Charging SBR" and click Reboot.</p> <p>Select all the DA-MP servers running PCA and click Reboot.</p> <p>CAUTION:</p> <p>If the DSR system is processing traffic other than PCA then DO NOT reboot all DA-MP servers simultaneously. Doing so will cause a network-wide outage. Please follow the procedure listed in APPENDIX-B to reboot the DA-MP servers in a controlled order to minimize traffic loss.</p> <p>Select all the SOAM Servers belonging to sites running PCA and click reboot.</p> <p>Select all NOAM servers except the Active NOAM and click reboot.</p> <p>Select the Active NOAM server and click Reboot.</p> <p>After rebooting the Active NOAM Server the GUI will go away. Please Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin" after some time.</p>

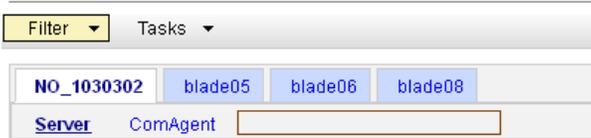
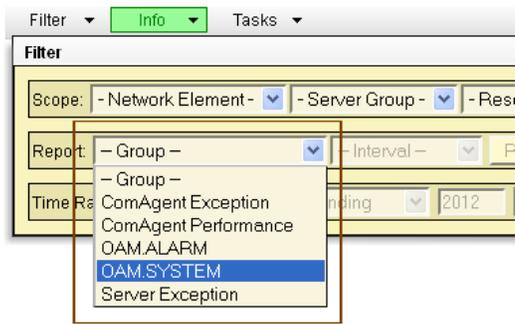
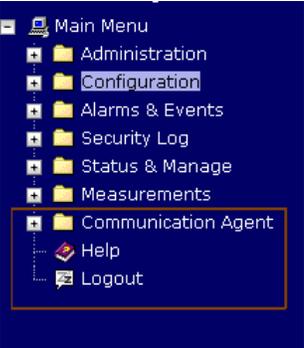
7.2.5 Post PCA Deactivation System Health Check

7.2.5.1 System health check after PCA Deactivation on NOAM server

Detailed steps are given in the procedure below.

Procedure 46: Verification of application deactivation on NOAM Server

S T E P #	<p>This procedure verifies the PCA application deactivation on NOAM Server.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>													
1 <input type="checkbox"/>	Active NOAM VIP: Establish GUI Session on the NOAM VIP	Establish a GUI session on the Active NOAM by using the XMI VIP address. Login as user "guiadmin".												
2 <input type="checkbox"/>	NOAM VIP: Verify that the Resource Domain Profile doesn't show the profile entries of Binding and Session Profiles.	<p>Verify that the Resource Domain Profile drop down doesn't show the profile entries of "Policy Session" and "Policy Binding".</p> <p>Main Menu: Configuration -> Resource Domains [Insert]</p> <hr/> <p>Inserting a new Resource Domain</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3">Resource Domain</th> </tr> <tr> <th style="width: 20%;">Field</th> <th style="width: 40%;">Value</th> <th style="width: 40%;">Description</th> </tr> </thead> <tbody> <tr> <td>Resource Domain Name</td> <td><input style="width: 80%;" type="text" value=""/></td> <td>Unique identifier used to label a Resource Domain. [Default string. Valid characters are alphanumeric and underscore.]</td> </tr> <tr> <td>Resource Domain Profile</td> <td>- Select Resource Domain Profile - <input type="button" value="v"/></td> <td>The Profile of this Resource Domain</td> </tr> </tbody> </table>	Resource Domain			Field	Value	Description	Resource Domain Name	<input style="width: 80%;" type="text" value=""/>	Unique identifier used to label a Resource Domain. [Default string. Valid characters are alphanumeric and underscore.]	Resource Domain Profile	- Select Resource Domain Profile - <input type="button" value="v"/>	The Profile of this Resource Domain
Resource Domain														
Field	Value	Description												
Resource Domain Name	<input style="width: 80%;" type="text" value=""/>	Unique identifier used to label a Resource Domain. [Default string. Valid characters are alphanumeric and underscore.]												
Resource Domain Profile	- Select Resource Domain Profile - <input type="button" value="v"/>	The Profile of this Resource Domain												
3 <input type="checkbox"/>	NOAM VIP: Verify that	Verify that KPIs menu don't show the KPI tabs for PCA, SBR, SBR-Binding and SBR-Session.												

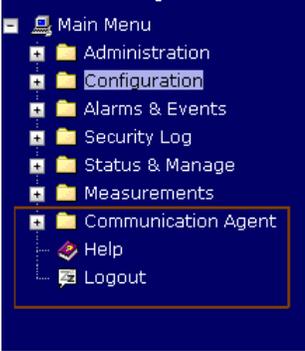
	<p>the KPIs are not shown for PCA, SBR, SBR-Binding and SBR-Session.</p>	<p>Main Menu: Status & Manage -> KPIs</p> 
<p>4</p>	<p>NOAM VIP: Verify that the Measurement groups are not shown for OC-DRA, P-DRA and SBR.</p>	<p>Verify that Measurement groups are not shown for OC-DRA, P-DRA and SBR.</p> <p>Main Menu: Measurements -> Report</p> 
<p>5</p>	<p>NOAM VIP: Verify that the Main Menu don't show the Policy and Charging submenu.</p>	<p>Verify that Main Menu on Active NOAM doesn't show the Policy and Charging submenu.</p> 

7.2.5.2 System health check after Application Deactivation on SOAM servers

Detailed steps are given in the procedure below.

Procedure 47: Verification of application deactivation on SOAM Servers

<p>S T E P #</p>	<p>This procedure verifies the PCA application deactivation on SOAM Servers.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>	
<p>1</p>	<p>SOAM VIP: Establish GUI Session on the SOAM VIP</p>	<p>Establish a GUI session on the Active SOAM by using the XMI VIP address. Login as user "guiadmin".</p>
<p>2</p>	<p>SOAM VIP: Verify that the Policy and Charging folder is not visible in the Left Hand Menu</p>	<p>Verify that the Policy and Charging folder does not appear on the Left Hand Menu:</p>

									
<p>3</p>	<p>SOAM VIP: Verify that the Diameter maintenance application menu do not show the entry of PCA application</p>	<p>Verify that the Diameter maintenance application menu do not show the entry of PCA application</p> <p>Main Menu: Diameter -> Maintenance -> Applications</p> <p style="text-align: right;">Tue Jul 03 1</p> <p>Filter ▾</p> <table border="1"> <thead> <tr> <th>DSR Application Name</th> <th>MP Server Hostname</th> <th>Admin State</th> <th>Operational State</th> <th>Operational Reason</th> <th>Congestion Level</th> <th>Time of Last Update</th> </tr> </thead> </table>	DSR Application Name	MP Server Hostname	Admin State	Operational State	Operational Reason	Congestion Level	Time of Last Update
DSR Application Name	MP Server Hostname	Admin State	Operational State	Operational Reason	Congestion Level	Time of Last Update			
<p>4</p>	<p>SOAM VIP: Verify PCA application on All Active SOAM servers</p>	<p>Repeat Steps 1 to 3 on All Active SOAM servers.</p>							

8.0 APPENDIX-B

This section has the procedure to restart DA-MP servers on a running DSR system such that the traffic loss is confined.

Procedure 48: Restarting DA-MP servers on a running DSR system

S T E P #	<p>This procedure restarts the DA-MP servers in a specific order so that the traffic loss is minimized.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>		
	1	<p>NOAM VIP: Establish GUI Session on the NOAM VIP</p>	<p>Establish a GUI session on the Active NOAM by using the XMI VIP address. Login as user "guiadmin".</p>
	2	<p>Select a DSR site</p>	<p>Chose a DSR site where the DA-MP servers will be restarted.</p>
	3	<p>SOAM VIP: Identify the DA-MP Leader</p>	<p>Establish a GUI session on the Active SOAM of the site chosen in Step 2 by using the XMI VIP address. Login as user "guiadmin".</p> <p>Navigate to Main Menu: Diameter -> Maintenance -> DA-MPs</p> <p>Locate and note the MP Server hostname for which the value in the "MP Leader" column is set to yes.</p>
	4	<p>NOAM VIP: Restart a set of DA-MP servers</p>	<p>Navigate to Main Menu: Status & Manage -> Server</p> <p>Select a set of DA-MP servers in the site chosen in Step 2 such that the remaining DA-MP servers in the site are able to handle the additional traffic when the selected DA-MP servers are restarted.</p> <p>Click Restart.</p> <p>NOTE: The DA-MP Leader located in step 3 must be included in the last set of DA-MP servers to be restarted to minimize DA-MP Leader switches.</p>
	5	<p>NOAM VIP: Restart next set of DA-MP servers</p>	<p>Repeat Step 4 for the next set of DA-MP servers until all DA-MP servers in the site chosen in step 2 have been restarted.</p>
	6	<p>NOAM VIP: Repeat for all DSR Sites</p>	<p>Repeat Steps 2 to 5 for all DSR sites.</p>

Procedure 49: Rebooting DA-MP servers on a running DSR system

S T E P #	<p>This procedure reboots the DA-MP servers in a specific order so that the traffic loss is minimized.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u>.</p>		
	1	<p>NOAM VIP: Establish GUI Session on the NOAM VIP</p>	<p>Establish a GUI session on the Active NOAM by using the XMI VIP address. Login as user "guiadmin".</p>
	2	<p>NOAM VIP: Select a DSR site</p>	<p>Chose a DSR site where the DA-MP servers will be rebooted.</p>

<input type="checkbox"/>		
3 <input type="checkbox"/>	SOAM VIP: Identify the DA-MP Leader	Establish a GUI session on the Active SOAM of the site chosen in Step 2 by using the XMI VIP address. Login as user "guiadmin". Navigate to Main Menu: Diameter -> Maintenance -> DA-MPs Locate and note the MP Server hostname for which the value in the "MP Leader" column is set to yes.
4 <input type="checkbox"/>	NOAM VIP: Restart a set of DA-MP servers	Navigate to Main Menu: Status & Manage -> Server Select a set of DA-MP servers in the site chosen in Step 2 such that the remaining DA-MP servers in the site are able to handle the additional traffic when the selected DA-MP servers are restarted. Click Reboot . NOTE: The DA-MP Leader located in step 3 must be included in the last set of DA-MP servers to be rebooted to minimize DA-MP Leader switches.
5 <input type="checkbox"/>	NOAM VIP: Restart next set of DA-MP servers	Repeat Step 4 for the next set of DA-MP servers until all DA-MP servers in the site chosen in step 2 have been restarted.
6 <input type="checkbox"/>	NOAM VIP: Repeat for all DSR Sites	Repeat Steps 2 to 5 for all DSR sites.