

Oracle® Communications
Diameter Signaling Router 7.1

PCA Configuration

E63560 Revision 01

August 2015

ORACLE®

Oracle Communications Diameter Signaling Router Software Installation Procedure, Release 7.1

Copyright © 2012,2015 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

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	6
LIST OF FIGURES.....	6
LIST OF PROCEDURES.....	6
1.0 INTRODUCTION	8
1.1 PURPOSE AND SCOPE	8
1.2 REFERENCES	8
1.3 ACRONYMS.....	8
TABLE 1. ACRONYMS	8
1.4 GENERAL PROCEDURE STEP FORMAT.....	9
2.0 PCA CONFIGURATION OVERVIEW	10
2.1 REQUIRED MATERIALS	10
3.0 PCA CONFIGURATION PREPARATION	12
3.1 HARDWARE PREPARATION.....	12
3.2 REQUIRED MATERIALS CHECK	12
PROCEDURE 1: REQUIRED MATERIALS CHECK.....	12
3.3 SYSTEM TOPOLOGY CHECK	13
PROCEDURE 2: SYSTEM TOPOLOGY CHECK	14
3.4 PCA / POLICY AND CHARGING SBR TOPOLOGY CHECK.....	15
FIGURE 2: EXAMPLE - PCA / POLICY AND CHARGING SBR TOPOLOGY	15
3.5 DIAMETER NETWORK CHECK.....	18
3.5.1 <i>Diameter Network Check for Policy DRA.....</i>	<i>18</i>
NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION	18
SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY	18
3.5.2 <i>Diameter Network Check for Online Charging DRA</i>	<i>21</i>
NOTE: EXECUTE THIS PROCEDURE FOR ONLINE CHARGING DRA FUNCTION	21
SKIP THIS PROCEDURE IF POLICY DRA FUNCTION ONLY	21
3.6 PERFORM HEALTH CHECK.....	22
PROCEDURE 3: PERFORM HEALTH CHECK (PCA CONFIGURATION PREPARATION)	22
4.0 PCA CONFIGURATION.....	23
4.1 PLACE ASSOCIATIONS CONFIGURATION	24
4.1.1 <i>Policy and Charging Places</i>	<i>24</i>
PROCEDURE 4: POLICY AND CHARGING PLACES CONFIGURATION.....	24
4.1.2 <i>Policy and Charging Mated Sites Place Associations</i>	<i>25</i>

PROCEDURE 5: POLICY AND CHARGING MATED SITES PLACE ASSOCIATIONS CONFIGURATION	25
4.1.3 <i>Policy Binding Region Place Associations.....</i>	25
NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION	25
SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY	25
PROCEDURE 6: POLICY BINDING REGION PLACE ASSOCIATIONS CONFIGURATION	25
4.2 RESOURCE DOMAINS CONFIGURATION	27
4.2.1 <i>Policy and Charging DRA Resource Domain Configuration.....</i>	27
PROCEDURE 7: POLICY AND CHARGING DRA RESOURCE DOMAIN CONFIGURATION	27
4.2.2 <i>Policy Session Resource Domain Configuration</i>	28
PROCEDURE 8: POLICY SESSION RESOURCE DOMAIN CONFIGURATION	28
4.2.3 <i>Policy Binding Resource Domain Configuration.....</i>	29
PROCEDURE 9: POLICY BINDING RESOURCE DOMAIN CONFIGURATION.....	29
4.3 DIAMETER CONFIGURATION PROCEDURES	31
4.3.1 <i>Diameter Configuration for Policy DRA.....</i>	31
PROCEDURE 10: DIAMETER CONFIGURATION FOR POLICY DRA.....	31
NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION	31
SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY	31
4.3.2 <i>Diameter Configuration for Online Charging DRA</i>	48
PROCEDURE 11: DIAMETER CONFIGURATION FOR ONLINE CHARGING DRA.....	48
NOTE: EXECUTE THIS PROCEDURE FOR ONLINE CHARGING DRA FUNCTION	48
SKIP THIS PROCEDURE IF POLICY DRA FUNCTION ONLY	48
4.4 PCA FUNCTION CONFIGURATION PROCEDURES.....	61
4.4.1 <i>Policy DRA Configuration</i>	62
PROCEDURE 12: POLICY DRA CONFIGURATION	62
4.4.2 <i>Online Charging DRA Configuration.....</i>	72
PROCEDURE 13: ONLINE CHARGING DRA CONFIGURATION.....	72
4.5 CONFIGURING ONLINE CHARGING FUNCTION ON A RUNNING DSR PCA SYSTEM	78
4.5.1 <i>Configuring new Online Charging DRA Sites.....</i>	78
PROCEDURE 14: NEW ONLINE CHARGING DRA SITE CONFIGURATION.....	78
4.5.2 <i>Configuring Online Charging DRA in existing Sites</i>	78
PROCEDURE 15: ONLINE CHARGING DRA CONFIGURATION ON A RUNNING DSR PCA SYSTEM	78
4.5.3 <i>Configuring Online Charging DRA in existing Sites with scaling</i>	78
PROCEDURE 16: ONLINE CHARGING DRA CONFIGURATION WITH SCALING ON A RUNNING DSR PCA SYSTEM	78
4.6 CONFIGURING POLICY FUNCTION ON A RUNNING DSR PCA SYSTEM	79
4.6.1 <i>Configuring Policy DRA</i>	79
PROCEDURE 17: POLICY DRA CONFIGURATION WITH SCALING ON A RUNNING DSR PCA SYSTEM	79
4.7 UN-CONFIGURING POLICY FUNCTION FROM A RUNNING DSR PCA SYSTEM	80

PROCEDURE 18: UN-CONFIGURING POLICY DRA	80
4.8 UN-CONFIGURING ONLINE CHARGING FUNCTION FROM A RUNNING DSR PCA SYSTEM	82
PROCEDURE 19: UN-CONFIGURING ONLINE CHARGING DRA	82
4.9 POST-CONFIGURATION PROCEDURES	83
4.9.1 <i>Enable Application</i>	83
PROCEDURE 20: ENABLE APPLICATION	83
4.9.2 <i>Enable SBR Databases</i>	85
PROCEDURE 21: ENABLE SBR DATABASES	85
4.9.3 <i>Restart Process</i>	86
PROCEDURE 22: RESTART SERVER	86
4.9.4 <i>Enable Connections</i>	86
PROCEDURE 23: ENABLE CONNECTIONS	86
4.9.5 <i>Perform Health Check</i>	87
PROCEDURE 24: PERFORM HEALTH CHECK	88
5.0 CAVEATS	89
6.0 CUSTOMER SERVICE SIGN OFF	90
DISCREPANCY LIST	90
7.0 REVIEW MEETING MINUTES	91
THE INITIAL FORMAL REVIEW FOR THIS DOCUMENT IS ARCHIVED IN THE DOCUMENT REVIEW TOOL, UNDER REVIEW ID 1	91
8.0 APPENDIX-A	92
8.1 PCA FEATURE ACTIVATION PROCEDURE.....	92
8.1.1 <i>PCA Activation on a freshly installed system</i>	92
PROCEDURE 25: PCA ACTIVATION	92
8.1.2 <i>PCA Activation on a newly added site</i>	93
NOTE:- THIS PROCEDURE NEEDS TO BE EXECUTED ONLY IF A NEW SITE IS ADDED IN EXISTING CONFIGURED SYSTEM	93
PROCEDURE 26: PCA ACTIVATION ON NEWLY ADDED SITE	93
8.1.3 <i>Restart Process</i>	93
PROCEDURE 27: RESTART PROCESS	93
8.1.4 <i>Post PCA Activation System Health Check</i>	94
PROCEDURE 28: VERIFICATION OF APPLICATION ACTIVATION ON NOAM SERVER	94
PROCEDURE 29: VERIFICATION OF APPLICATION ACTIVATION ON SOAM SERVERS	96
8.2 PCA FEATURE DE-ACTIVATION PROCEDURE.....	97
8.2.1 <i>Pre PCA De-Activation Steps</i>	97
PROCEDURE 30: VERIFY AND DEACTIVATE GLA APPLICATION	97
PROCEDURE 31: DISABLE PCA FUNCTIONS (PDRA AND OCDRA)	97

PROCEDURE 32: DISABLE DIAMETER CONNECTIONS.....	98
PROCEDURE 33: DISABLE APPLICATION	99
PROCEDURE 34: STOP SERVER PROCESS	100
PROCEDURE 35: REMOVE PCA CONFIGURATION DATA.....	100
PROCEDURE 36: REMOVE DSR CONFIGURATION DATA	102
8.2.2 <i>PCA De-Activation Procedure.....</i>	103
PROCEDURE 37: PCA APPLICATION DE-ACTIVATION	103
8.2.3 <i>Site Specific PCA De-Activation Procedure.....</i>	104
THIS SECTION ONLY REQUIRED WHEN A PARTICULAR SITE NEEDS TO BE DEACTIVATED FOR PCA APPLICATION.	104
PROCEDURE 38: PCA APPLICATION DE-ACTIVATION ON A PARTICULAR SITE.	104
8.2.4 <i>Post PCA De-Activation Steps.....</i>	105
PROCEDURE 39: MOVE POLICY AND CHARGING SBR SERVERS TO OOS STATE	105
PROCEDURE 40: REMOVE POLICY AND CHARGING SBR SERVERS FROM SERVER GROUPS	105
PROCEDURE 41: DELETE SERVER GROUPS RELATED TO POLICY AND CHARGING SBR.....	106
PROCEDURE 42: REMOVE PLACE CONFIGURATION DATA	106
PROCEDURE 43: REBOOT THE SERVERS.....	106
8.2.5 <i>Post PCA De-Activation System Health Check.....</i>	107
PROCEDURE 44: VERIFICATION OF APPLICATION DE-ACTIVATION ON NOAM SERVER.....	107
PROCEDURE 45: VERIFICATION OF APPLICATION DE-ACTIVATION ON SOAM SERVERS.....	108

List of Tables

Table 1. Acronyms	8
-------------------------	---

List of Figures

Figure 1. Example of a procedure step	9
Figure 2: Example - PCA / Policy and Charging SBR Topology.....	15

List of Procedures

Procedure 1: Required Materials Check	12
Procedure 2: System Topology Check	14
Procedure 3: Perform Health Check (PCA configuration Preparation).....	22
Procedure 4: Policy and Charging Places configuration.....	24
Procedure 5: Policy and Charging Mated Sites Place Associations configuration	25
Procedure 6: Policy Binding Region Place Associations configuration	25
Procedure 7: Policy and Charging DRA Resource Domain configuration	27
Procedure 8: Policy Session Resource Domain configuration	28
Procedure 9: Policy Binding Resource Domain configuration	29
Procedure 10: Diameter configuration for Policy DRA.....	31

Procedure 11: Diameter configuration for Online Charging DRA	48
Procedure 12: Policy DRA configuration.....	62
Procedure 13: Online Charging DRA configuration	72
Procedure 14: New Online Charging DRA Site Configuration.....	78
Procedure 15: Online Charging DRA Configuration on a running DSR PCA System.....	78
Procedure 16: Online Charging DRA Configuration with scaling on a running DSR PCA System	78
Procedure 17: Policy DRA Configuration with scaling on a running DSR PCA System.....	79
Procedure 18: Un-configuring Policy DRA.....	80
Procedure 19: Un-configuring Online Charging DRA	82
Procedure 20: Enable Application.....	83
Procedure 21: Enable SBR Databases.....	85
Procedure 22: Restart Server	86
Procedure 23: Enable connections	86
Procedure 24: Perform Health Check	88
Procedure 25: PCA Activation	92
Procedure 26: PCA Activation on newly added site	93
Procedure 27: Restart Process.....	93
Procedure 28: Verification of application activation on NOAM Server	94
Procedure 29: Verification of application activation on SOAM Servers.....	96
Procedure 30: Verify and Deactivate GLA application.....	97
Procedure 31: Disable PCA Functions (PDRA and OCDRA).....	97
Procedure 32: Disable Diameter Connections.....	98
Procedure 33: Disable application	99
Procedure 34: Stop Server Process	100
Procedure 35: Remove PCA configuration data	100
Procedure 36: Remove DSR configuration data.....	102
Procedure 37: PCA Application De-Activation	103
Procedure 38: PCA Application De-Activation on a particular site.	104
Procedure 39: Move Policy and Charging SBR Servers to OOS State	105
Procedure 40: Remove Policy and Charging SBR Servers from Server Groups	105
Procedure 41: Delete Server Groups related to Policy and Charging SBR.....	106
Procedure 42: Remove Place configuration data	106
Procedure 43: Reboot the Servers	106
Procedure 44: Verification of application de-activation on NOAM Server	107
Procedure 45: Verification of application de-activation on SOAM Servers.....	108

1.0 INTRODUCTION

1.1 PURPOSE AND SCOPE

This document defines the procedures required to configure PCA on a DSR system. This document contains information that is needed to configure PCA which includes configuring the Resource Domains and Diameter Stack (DPI).

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].

1.2 REFERENCES

[1] *DSR 7.1 Base Hardware and Software Installation, E53488-01*

[2] *DSR 7.0/7.1 Software Installation and Configuration Procedure Part 2/2, E58954-02*

[3] *IP Front End (IPFE) User's Guide, E53473-01*

1.3 ACRONYMS

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 Session 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

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.

The title box describes the operations to be performed during that step.

Each command that the technician is to enter is in 10 point bold Courier font.

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. <pre>\$ cu -l /dev/ttyS7</pre>
---	---	--

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 Diameter and PCA specific configurations.

2.1 REQUIRED MATERIALS

- 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
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.

3.0 PCA CONFIGURATION PREPARATION

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

3.1 HARDWARE PREPARATION

There are no hardware changes necessary.

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.	
	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 all required materials are present	Information is listed in Section 2.1: Required information. Gather required information.

3.3 SYSTEM TOPOLOGY CHECK

This procedure is part of PCA configuration preparation and is used to verify the system topology of the DSR 7.1 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 the configuration data is correct for your network. 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 the configuration data is correct for your network. 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>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).
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, see diagram for 2 site system.

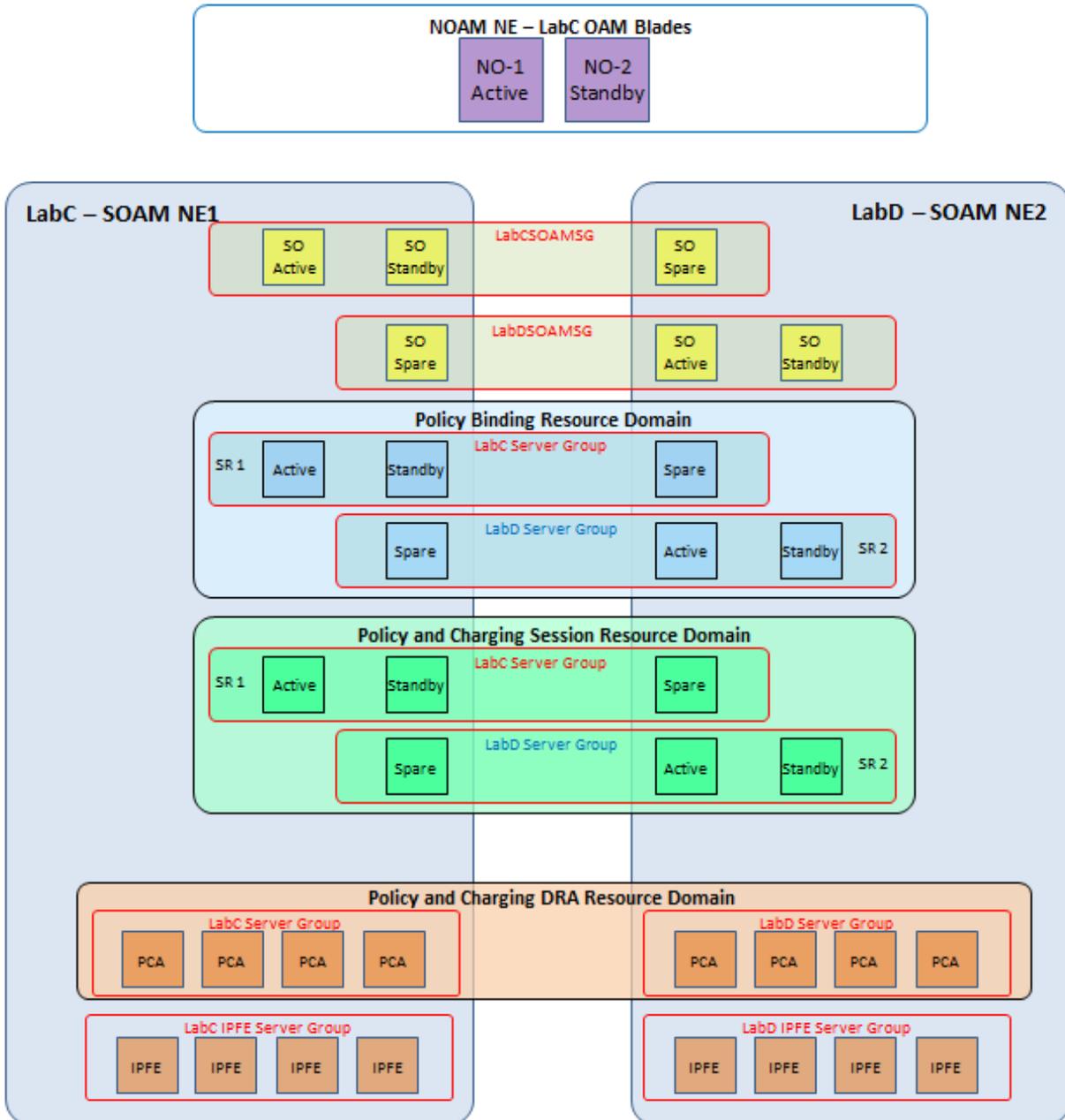


Figure 2: Example - PCA / Policy and Charging SBR Topology

S T E P #	<p>This procedure verifies and logs PCA Topology for the setup. This information must be gathered before configuring the PCA system.</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>	
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 12 places.</p> <div data-bbox="553 422 1052 522" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Number of Places:</p> <p>Place Names:</p> </div> <p>2. Identify and note the number of PCA mated pairs – LabC and Lab D in example.</p> <div data-bbox="553 583 1052 644" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Number of PCA Mated Pairs:</p> </div> <p>3. If Policy DRA function is being configured, then identify and note the Binding Region place associations</p> <p>Note: This step is required for Policy DRA functionality only.</p> <p>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 data-bbox="553 856 1052 917" 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 other required place associations</p> <p>PCA Mated Sites – Identify and Log the mated sites – Lab C and Lab D in example (since this is the only mated pair here, there can be more mated pairs)</p> <div data-bbox="553 1043 1052 1346" style="border: 1px solid black; padding: 5px;"> <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> </div>
2 <input type="checkbox"/>	<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.</p>

PCA RD1 - LabCPCASG

PCA RD2 - LabDPCASG

PCA RD3 -

PCA RD4 -

PCA RD5 -

PCA RD6 -

PCA RD7 -

...

2. Identify and log the number of **'Policy Binding'** resource domains and their Server Groups

Note: This step is required for Policy DRA functionality only.

– In this example it is 2 since there is only one mated pair.

Policy Binding RD1 – LabCBindingSR1SG

Policy Binding RD2 – LabDBindingSR2SG

Policy Binding RD3 – LabCBindingSR3SG

Policy Binding RD4 – LabDBindingSR4SG

Policy Binding RD5 -

Policy Binding RD6 -

Policy Binding RD7 -

...

3. Identify and log the number of **'Policy Session'** resource domains and their Server Groups – In this example it is 2 since there is only one mated pair.

		<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 - ...</p>	
--	--	---	--

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

S T E P #	<p>This procedure verifies PCA – Policy 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 policy clients and policy servers 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. 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.
2 <input type="checkbox"/>	Policy DRA Network configuration (NO scoped)	<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. 4. Identify and log the “Policy and Charging -> Configuration -> Policy DRA-> General Options” for the Policy DRA network – <ul style="list-style-type: none"> Default Stale Session Timeout Maximum Audit Frequency 5. Identify and log the “Policy and Charging -> Configuration -> Policy DRA-> Network Wide Options” for the Policy DRA network – <ul style="list-style-type: none"> Default Stale Session Timeout Origin Host and Origin Realm for Policy DRA generated RAR messages Maximum Audit Frequency Early Binding Polling Interval Maximum Early Binding Lifetime Topology Hinding <ul style="list-style-type: none"> a. Enabled/Disabled b. If Enabled, then identify and log the the Scope – All Messages, All Foreign Realms, Specific Hosts, All Foreign Realms + Specific Hosts c. FQDN and Realm 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 Gx Traffic for this site. 2. Identify and log the “Policy and Charging -> Configuration -> Policy DRA-> Binding Key Priority” settings. 3. Identify and log the 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.
--	--	--

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

S T E P #	This procedure verifies PCA – Online Charging DRA function Diameter Configuration. 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"/>	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 and Online Charging servers 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 “Policy and Charging -> Configuration -> Policy DRA-> General Options” for the Policy DRA network – <ul style="list-style-type: none"> Default Stale Session Timeout Maximum Audit Frequency 4. Identify and log the Online Charging Network Realms to be configured for Session State maintenance. 5. Identify and log the “Policy and Charging -> Configuration -> Online Charging DRA-> Network Wide Options” for the Policy DRA network – <ul style="list-style-type: none"> Request Error Action Session state Scope 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"/>	Policy 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 per the policy client team request/ inteoperability requirements for Policy Client Vendor.

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 3: Perform Health Check (PCA configuration Preparation)

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"/>	Verify DSR Release	<p>DSR Release supports the PCA Application:</p> <ol style="list-style-type: none"> 1. Log into the NOAM VIP GUI. 2. Select Administration > Software Management -> Versions; the DSR Software Versions Report screen is shown. 3. Verify the ORACLE Communications DSR RPM Version shows version 7.0.0 or greater.
2 <input type="checkbox"/>	Verify Server status	<p>Verify Server status:</p> <ol style="list-style-type: none"> 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 Engineering for assistance as necessary.
3 <input type="checkbox"/>	Log all current alarms	<p>Log all current alarms in the system:</p> <ol style="list-style-type: none"> 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 is available before proceeding with the configuration in below sections.

4.1 PLACE ASSOCIATIONS 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 type of Place Associations is required for both functions (Policy DRA and Online Charging DRA) of PCA:

- Policy and Charging Mated Sites

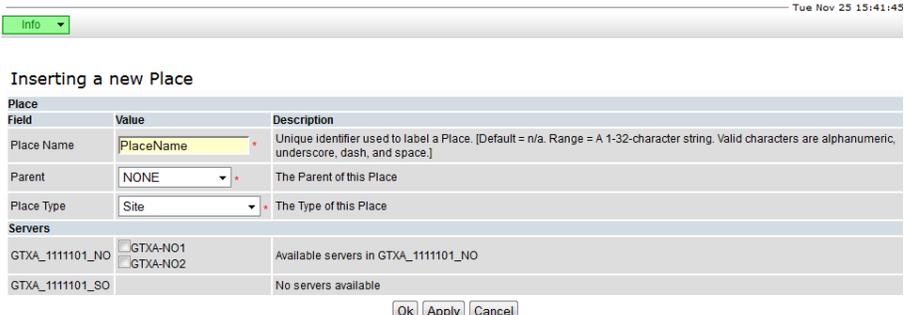
The following type of Place Associations is required for Policy DRA function ONLY:

- 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 4: Policy and Charging Places configuration

S T E P #	<p>This procedure configures the Places.</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: Navigate to Places screen	Navigate to Main Menu -> Configuration -> Places Screen.
3 <input type="checkbox"/>	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>1. Enter the Place Name 2. Select "None" as the Parent 3. Select "Site" as the Place Type 4. Select the Servers. 5. Click Ok.</p>
4 <input type="checkbox"/>	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 5: Policy and Charging Mated Sites Place Associations configuration

S T E P #	<p>This procedure configures Place Association</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	<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 Place Associations screen</p> <p>Navigate to Main Menu -> Configuration -> Place Associations Screen.</p>																	
	3	<p>NOAM VIP: Add Policy and Charging Mated Sites 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> <th colspan="3">Place Association</th> </tr> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Place Association Name</td> <td><input 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 -</td> <td>The Type of this Place Association</td> </tr> <tr> <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 and Charging Mated Sites" as the Place Association Type 3. Select the Places to associate with the Place Association. Select the sites (Places) which need to be configured as mates. 4. Click Ok.</p>	Place Association			Field	Value	Description	Place Association Name	<input type="text" value=""/>	Unique identifier used to label a Pla characters are alphanumeric, unde	Place Association Type	- Select Place Association Type -	The Type of this Place Association	Places			Places	<input type="checkbox"/> DSR70PCASite
Place Association																			
Field	Value	Description																	
Place Association Name	<input type="text" value=""/>	Unique identifier used to label a Pla characters are alphanumeric, unde																	
Place Association Type	- Select Place Association Type -	The Type of this Place Association																	
Places																			
Places	<input type="checkbox"/> DSR70PCASite	Places in this Place Association																	

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 6: 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	<p>Establish GUI Session</p> <p>Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".</p>

1	on the NOAM VIP	
2	NOAM VIP: Navigate to Place Associations screen	Navigate to Main Menu -> Configuration -> Place Associations Screen.
3	NOAM VIP: Add Policy and Charging Mated Sites Place Association	Click on Insert in the lower left corner. You will see a screen similar to:

Main Menu: Configuration -> Place Associations [Insert]

Inserting a new Place Association

Place Association		
Field	Value	Description
Place Association Name	<input type="text"/>	Unique identifier used to label a Pla characters are alphanumeric, unde
Place Association Type	- Select Place Association Type - *	The Type of this Place Association
Places		
Places	<input type="checkbox"/> DSR70PCASite	Places in this Place Association

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](#).

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

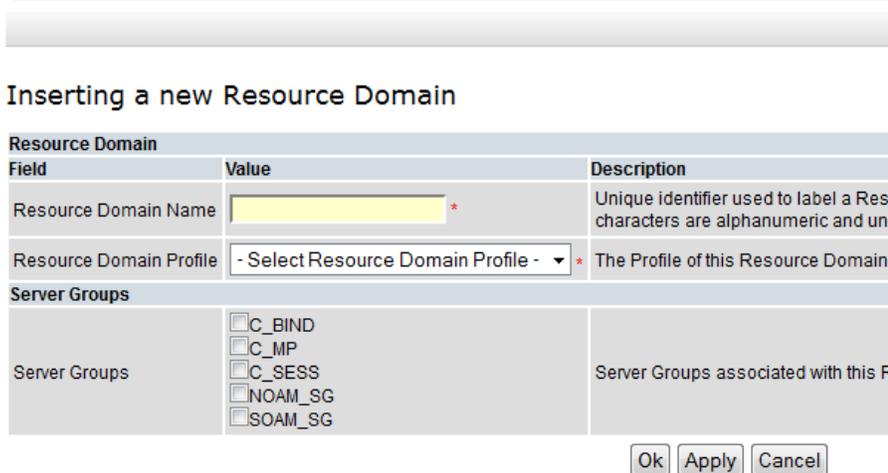
Procedure 7: Policy and Charging DRA Resource Domain configuration

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 ORACLE TAC.</p> <p>ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.</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: Navigate to Resource Domain Screen	Navigate to Main Menu -> Configuration -> Resource Domains Screen.																		
3 <input type="checkbox"/>	NOAM VIP: Add Policy and Charging DRA Resource Domain	<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"> <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 Resource Domain. 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 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 type="text"/>	Unique identifier used to label a Resource Domain. 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
Resource Domain																				
Field	Value	Description																		
Resource Domain Name	<input type="text"/>	Unique identifier used to label a Resource Domain. 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																		

	DA-MP Server Groups from both 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.
4 <input type="checkbox"/>	NOAM VIP: Restart the Servers Navigate to Main Menu -> Status & Manage -> Server screen. Select the Servers just added to the Resource Domain and click 'Restart' button.

4.2.2 Policy Session Resource Domain Configuration

Procedure 8: Policy Session Resource Domain configuration

S T E P #	This procedure configures the Policy Session Resource Domain	
	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 . ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.	
	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 Resource Domain Screen Navigate to Main Menu -> Configuration -> Resource Domains Screen.	
3 <input type="checkbox"/>	NOAM VIP: Add Session Resource Domain Click on Insert in the lower left corner. You will see a screen similar to: Main Menu: Configuration -> Resource Domains [Insert]  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 . NOTE: For Mated DSR sites, create one Policy Session Resource Domain and add all the Policy Session Server Groups from both sites into this Policy Session Resource Domain. For non-mated pair DSRs and standalone DSR: Configure a Policy Session Resource Domain per Site.	
4 <input type="checkbox"/>	NOAM VIP: Add other Repeat Step 4 for all other Policy Session Resource Domains that are to be added.	

<input type="checkbox"/>	Session Resource Domains.	
5	NOAM VIP: Restart the Servers	Navigate to Main Menu -> Status & Manage -> Server screen. Select the Servers just added to the Resource Domain and click 'Restart' button.

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 9: Policy Binding Resource Domain configuration

S T E 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 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="background-color: yellow;" 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 Binding" as the Resource Domain Profile 3. Select the Server Groups to associate with the Resource Domain 4. Click Ok.</p> <p>NOTE: Create only one Policy Binding Resource Domain and add the Policy Binding Server Groups from all the sites in the network into this Policy Binding Resource Domain.</p>	Resource Domain			Field	Value	Description	Resource Domain Name	<input style="background-color: yellow;" 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
	Resource Domain																			
Field	Value	Description																		
Resource Domain Name	<input style="background-color: yellow;" 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																		
4	<p>NOAM VIP: Restart the Servers</p> <p>Navigate to Main Menu -> Status & Manage -> Server screen.</p>																			



Select the Servers just added to the Resource Domain and click 'Restart' button.

4.3 DIAMETER CONFIGURATION PROCEDURES

4.3.1 Diameter Configuration for Policy DRA

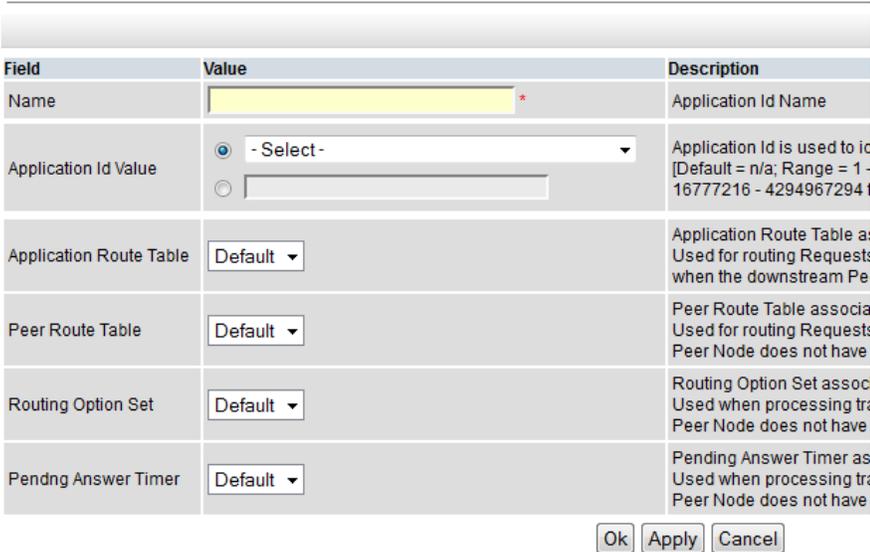
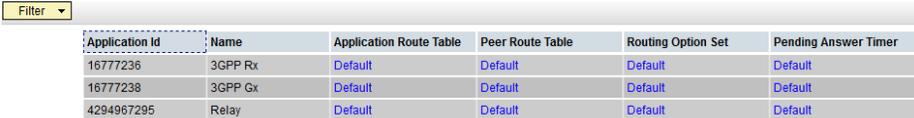
Detailed steps are given in the procedure below.

Procedure 10: Diameter configuration for Policy DRA

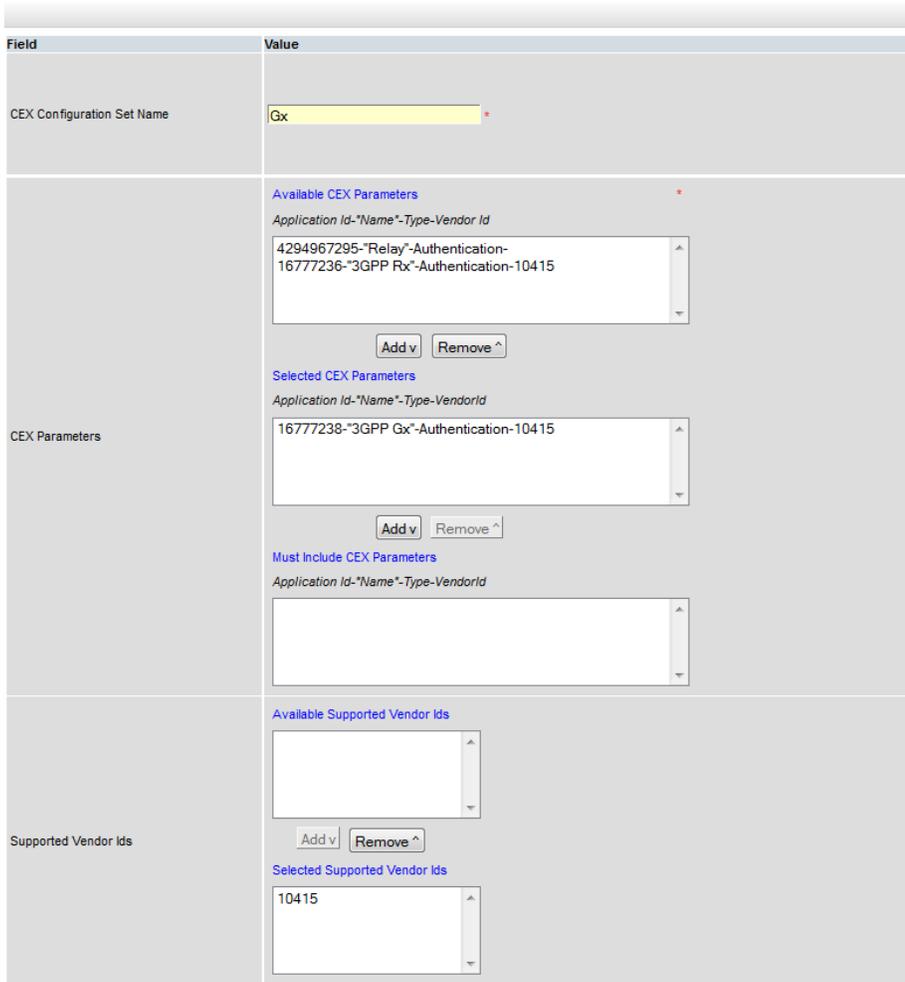
NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION

SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY

S T E P #	<p>This procedure configures the Diameter stack.</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 SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".																					
2 <input type="checkbox"/>	SOAM VIP: Navigate to Application Id Configuration Screen	Navigate to Main Menu -> Diameter -> Configuration -> Application Ids																					
3 <input type="checkbox"/>	SOAM VIP: Add Application Id for Gx Interface	<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" 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" 2. Click Ok.</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 ▾	Pending Answer Timer as Used when processing tr: Peer Node does not have
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																					
4 <input type="checkbox"/>	SOAM VIP: Add Application Id for Rx Interface	<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>  <p>1. Select Application Id for Rx Interface "16777236" 2. Click Ok.</p>																								
5	<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, Gxx and S9 Interfaces.</p>																								
6	<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 Thu Aug 07 16:41</p>  <table border="1" data-bbox="597 1199 1430 1289"> <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																					
7	<p>SOAM VIP: Navigate to CEX Parameters Screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> CEX Parameters</p>																								
8	<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 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 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 AVP. [Default = n/a; Range = 1 - 4294967295]															
<p>9</p> <p>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 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 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 AVP. [Default = n/a; Range = 1 - 4294967295]															
<p>10</p> <p>SOAM VIP: Add CEX Parameters for any other required Interfaces</p>		<p>Repeat Step 9 for all other configured Application Ids. For example, Gxx and S9 Interfaces.</p>															
<p>11</p> <p>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	---												
12	<p>SOAM VIP: Navigate to CEX Configuration Sets screen</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets</p>												
13	<p>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>												
14	<p>SOAM VIP: Configure the CEX Configuration</p>	<p>Click on Insert in the lower left corner.</p>												

Set to be used for Connections with the AF nodes.

You will see a screen similar to:

Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]

Field	Value
CEX Configuration Set Name	Rx *
CEX Parameters	<p>Available CEX Parameters *</p> <p><i>Application Id-Name-Type-Vendor Id</i></p> <p>4294967295-Relay-Authentication-16777238-3GPP Gx-Authentication-10415</p> <p>Add v Remove ^</p> <p>Selected CEX Parameters</p> <p><i>Application Id-Name-Type-Vendor Id</i></p> <p>16777236-3GPP Rx-Authentication-10415</p> <p>Add v Remove ^</p> <p>Must Include CEX Parameters</p> <p><i>Application Id-Name-Type-Vendor Id</i></p> <p></p>
Supported Vendor Ids	<p>Available Supported Vendor Ids</p> <p></p> <p>Add v Remove ^</p> <p>Selected Supported Vendor Ids</p> <p>10415</p>

Ok Apply Cancel

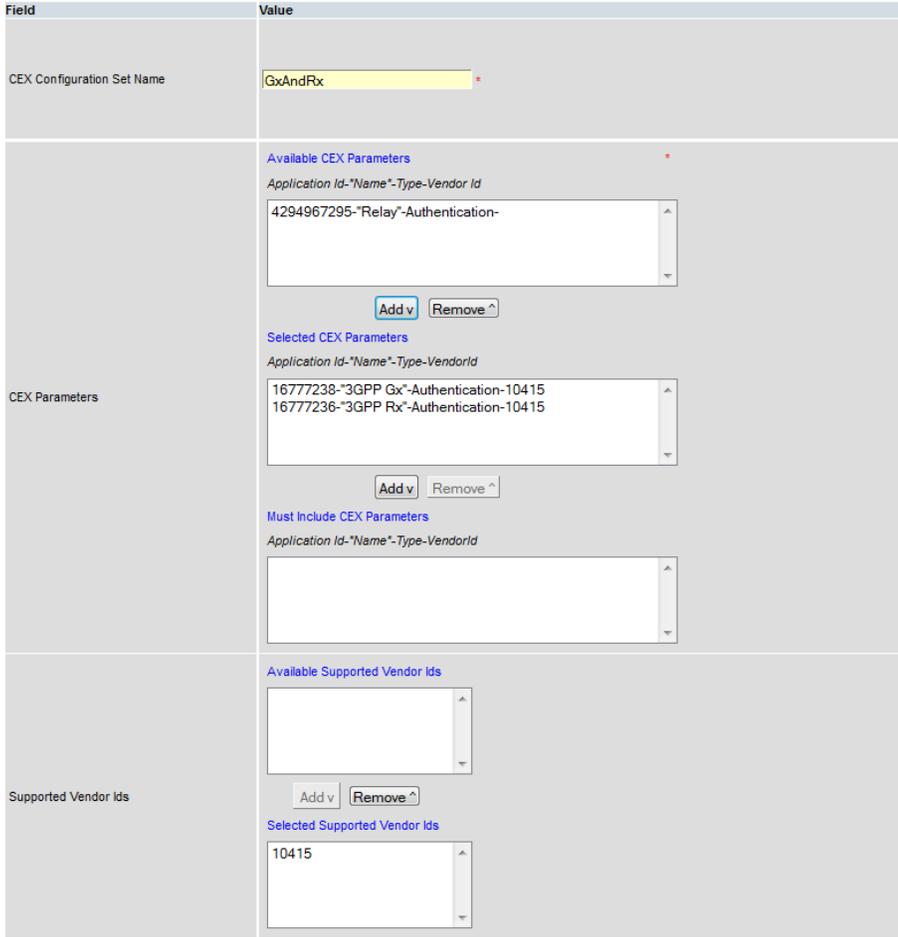
1. Enter the CEX Configuration Set Name "Rx"
2. Select the 3GPP Rx Application Id "16777236" from Available Application Ids
3. Click **Add** just below the list
4. Select the Vendor Id "10415" from Available Supported Vendor Ids
5. Click **Add** just below that list
6. Click **Ok**.

15

SOAM VIP: Configure the CEX Configuration Set to be used for Connections with the PCRF nodes.

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

You will see a screen similar to:

Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]	
	 <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 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 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>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] 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 character 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 (_), but 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. 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 (_), but 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 character 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 (_), but 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. 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 (_), but 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 character 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 (_), but 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. 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 (_), but 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;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 2px;">CEX Configuration Set</td> <td style="padding: 2px;">GxAndRx ▾ *</td> <td style="padding: 2px;">CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]</td> </tr> <tr> <td style="padding: 2px;">IP Addresses</td> <td style="padding: 2px;"> <div style="display: flex; flex-direction: column; gap: 5px;"> <div style="display: flex; align-items: center;">10.240.71.118 ▾ X *</div> <div style="display: flex; align-items: center;">10.240.71.121(TSA) ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> </div> </td> <td style="padding: 2px; vertical-align: top;">The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries]</td> </tr> </table> <div style="text-align: right; margin-top: 5px;"> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div> <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>	CEX Configuration Set	GxAndRx ▾ *	CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]	IP Addresses	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="display: flex; align-items: center;">10.240.71.118 ▾ X *</div> <div style="display: flex; align-items: center;">10.240.71.121(TSA) ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> </div>	The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries]
CEX Configuration Set	GxAndRx ▾ *	CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]						
IP Addresses	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="display: flex; align-items: center;">10.240.71.118 ▾ X *</div> <div style="display: flex; align-items: center;">10.240.71.121(TSA) ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> <div style="display: flex; align-items: center;">- Select - ▾ X</div> </div>	The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries]						
20	<input type="checkbox"/> SOAM VIP: Configure other Local Nodes, if required.	Repeat Step 19 and configure more Local Nodes if required.						
21	<input type="checkbox"/> SOAM VIP: Navigate to Peer Nodes screen	Navigate to Main Menu -> Diameter -> Configuration -> Peer Nodes						
22	<input type="checkbox"/> SOAM VIP: Configure the first PCEF node	Click on Insert in the lower left corner. You will see a screen similar to:						

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. FQDN must contain only digits, dashes ("-") and underscore ("_"). A label must be at most 63 characters long and a FQDN must be [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 an 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

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**.

23 <input type="checkbox"/>	SOAM VIP: Configure other Peer Nodes	Repeat Step 22 to configure other peer nodes (PCEFs, AFs, BBERFs etc.) as required.
24 <input type="checkbox"/>	SOAM VIP: Navigate to Connections screen	Navigate to Main Menu -> Diameter -> Configuration -> Connections
25 <input type="checkbox"/>	SOAM VIP: Configure the connection with PCEF Node	Click on Insert in the lower left corner. You will see a screen similar to:

Main Menu: Diameter -> Configuration -> Connections -> [Insert]

Adding a new connection

Field	Value	Description
Connection Name	<input type="text"/>	A name that uniquely identifies the Connection. [Default = n/a; Range = A 32-character string. Valid characters are
Transport Protocol	<input checked="" type="radio"/> SCTP <input type="radio"/> TCP	The transport protocol used by this Connection. The protocol should be supported by both Local Node and Peer Node
Local Node	PDRA	The Local Node of this Connection.
Connection Mode	Initiator & Responder	Initiator Only Indicates that Local Node will only initiate the connection. Responder Only Indicates that Local Node will only respond to the connection. Initiator & Responder Indicates that Local Node will initiate connection and respond to the connection. [Default = Initiator & Responder; Range = n/a]
Local Initiate Port	<input type="text"/>	The Local Initiate Port of this Connection. [Default = n/a; Range = 1024-65535]
Primary Local IP Address	10.240.10.73 (TSA1-p)	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 unique.
Peer Node	AF1	The Peer Node of this Connection.
Peer Node Identification	<input checked="" type="radio"/> IP Address <input type="radio"/> Transport FQDN <input type="radio"/> Peer Diameter Identity FQDN	Specifies how DSR will derive the peer node's IP address(es) when IP Address Use the remote IP address(es) configured for this Connection when IP Address Use the DNS resolved Transport FQDN address configured for this Connection when Transport FQDN Use the DNS resolved Transport FQDN address configured for this Connection when Peer Diameter Identity FQDN Use the DNS resolved FQDN address configured for the Peer Node when Peer Diameter Identity FQDN
Primary Peer IP Address	10.240.71.85	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 unique.
Transport FQDN	<input type="text"/>	Fully Qualified Domain Name for this connection. FQDN is a case-sensitive, alphanumeric and hyphenated string that must end with a letter or digit. Underscores may be used to separate labels and may only appear at the beginning or following a hyphen. The string must be at least one character long and must not exceed 253 characters. [Default = n/a; Range = A valid FQDN]
Connection Configuration Set	Default	The configuration set of this Connection.
CEX Configuration Set	Gx	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 incoming connections. [Default = Default; Range = A 32-character string. Valid characters are alphanumeric and hyphenated.]
Transport Congestion Abatement Timeout	5	Defines the time period (in seconds) spent by the connection in abatement. [Default = 5; Range = 3 - 60 secs]
Remote Busy Usage	Disabled	Defines which Request messages can be forwarded on this connection. 'Disabled' - The Connection is not considered to be BUSY after receiving a Request message. 'Enabled' - The Connection is considered to be BUSY after receiving a Request message. [Default = Disabled; Range = Disabled, Enabled]
Remote Busy Abatement Timeout	5	Defines the time period (in seconds) that a Connection will be considered BUSY. [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 Read From Request Message - Read Message Priority from incoming Request Message 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 Configuration Set defines the priority of the Request Message.
Egress Message Throttling Configuration Set	- Select -	The Egress Message Throttling 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. [Default = unchecked; Range = n/a]
Test Mode	<input type="checkbox"/>	If checked, indicates that connection is in test mode. [Default = unchecked; Range = n/a]

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

		<p>2. Click Ok.</p> <p>NOTE: Make sure the IPFE configuration matches the protocol which is selected in this step.</p>																		
26	<p>SOAM VIP: Configure all other connection with Peer nodes</p>	<p>Repeat Step 25 to configure all other required DIAMETER connections.</p>																		
27	<p>SOAM VIP: Configure Route Groups</p>	<p>For priority based initial CCR-I routing, there should be N+1 number for Route Groups configured where N is the number of PCRFs in the system. The first N Route Groups shall contain a corresponding PCRF node in them and the last Route Group shall contain ALL PCRFs.</p> <p>The goal is to setup a Routing Configuration such that in case of an initial (binding capable) session request, if there is no route available to the suggested PCRF, Diameter Routing Layer automatically sends the request messages to any other available PCRF.</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Route Groups</p>																		
28	<p>SOAM VIP: Insert a new Route Group and add the first PCRF to it.</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" data-bbox="516 1024 1409 1528"> <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" data-bbox="682 1333 1388 1522"> <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><input type="button" value="Add"/></p> </td> <td>P [C C [C P w T N R N [E</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 Route Group name. 2. Select the Peer Node name (PCRF name). 3. Enter the provisioned capacity as 1. 4. Click Ok.</p>	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" data-bbox="682 1333 1388 1522"> <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><input type="button" value="Add"/></p>	Peer Node	Connection	Provisioned Capacity *	01 pcrf		1 x	P [C C [C P w T N R N [E
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" data-bbox="682 1333 1388 1522"> <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><input type="button" value="Add"/></p>	Peer Node	Connection	Provisioned Capacity *	01 pcrf		1 x	P [C C [C P w T N R N [E												
Peer Node	Connection	Provisioned Capacity *																		
01 pcrf		1 x																		
29	<p>SOAM VIP: Configure more Route Groups corresponding to each PCRF.</p>	<p>Repeat Step 28 for every PCRF that is connected to this DSR.</p>																		
30	<p>SOAM VIP: Configure one Route Group</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																		

containing all PCRF nodes

Adding a new route group

Field	Value	Description
Route Group Name	AllPcrfsRouteGroup	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 (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]
	01 PCRf1	- Select - 1
02 PCRf2	- Select - 1	
03 PCRf3	- Select - 1	
Add		

Ok Apply Cancel

1. Enter the Route Group name.
2. Select the Peer Node name (PCRF name).
3. Enter the provisioned capacity as 1.
4. Click [Add](#).
5. Add another PCRF and so on.
6. Click [Ok](#).

31 SOAM VIP: Configure Route Lists

For priority based initial session binding, there should be N number for Route Lists configured where N is the number of PCRFs in the system. All Route Lists shall contain two Route Groups. The Route Group with a single PCRF will have a higher priority whereas the Route Group with all PCRFs will have a lower priority.

Navigate to [Main Menu -> Diameter -> Configuration -> Route Lists](#)

32 SOAM VIP: Configure the first Route List

Click on [Insert](#) in the lower left corner.

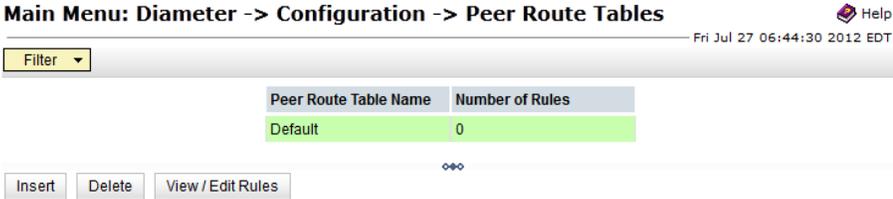
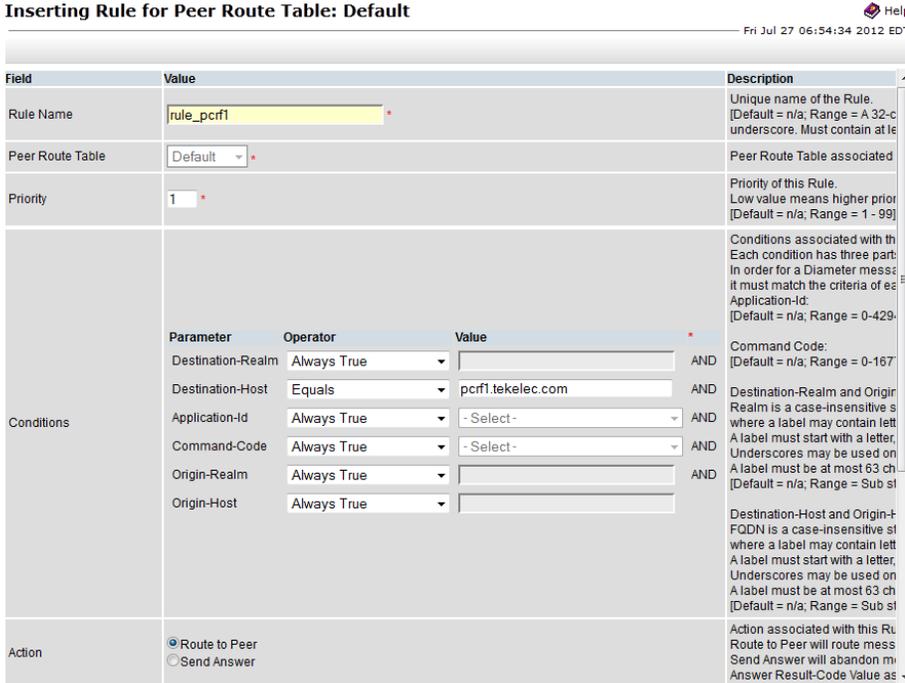
You will see a screen similar to:

Adding a new route list

Field	Value	Description
Route List Name	Pcrf1RouteList	A name that uniquely identifies the Route List. [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]
Minimum Route Group Availability Weight	1	Minimum Route Group Availability Weight of this Route List. Minimum Route Group Availability Weight is used to determine a Route Group availability status within a Route List. [Default = n/a; Range = 1 - 1024000]
Route Group and Priority	Route Group	Route Groups associated with this Route List. [Default = n/a; Range = 1 - 3 entries]
	Priority	Priority of Route Group within this Route List. Low value means high priority. [Default = n/a; Range = 1 - 3]
	Pcrf1RouteGroup	1
AllPcrfsRouteGroup	2	
- Select -		

Ok Apply Cancel

1. Enter the Route List name.
2. Minimum Route Group Availability Weight should be 1.
3. Assign priority 1 to the Route Group containing the intended PCRF, assign priority 2 to the Route Group containing all the PCRFs.

		4. Click Ok .
33	SOAM VIP: Configure all other Route Lists	Repeat step 32 for all other PCRFs connected to this DSR.
34	SOAM VIP: Configure the Peer Routing Rules.	<p>Finally, configure the PRT such that DSR forwards messages based on the PCRF preference.</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Peer Route Table</p>
35	SOAM VIP: Add PRT rules to Default PRT	<p>Navigate to Main Menu -> Diameter -> Configuration -> Peer Route Table</p> <p>You will see a screen similar to:</p>  <p>1. Select the Default Peer Route Table Name to which rules are to be added. 2. Click on View/Edit Rules button.</p>
36	SOAM VIP: Configure PRT rules for the first PCRF	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> 

		<div data-bbox="509 197 1404 478"> </div> <ol style="list-style-type: none"> 1. Enter the Rule name and priority values. 2. Select Destination host "Equals" the configured FQDN of PCRF1. 3. Select "Always True" for other conditions. 4. Select the Route List "Pcrf1RouteList". 5. Click Ok. 				
37	SOAM VIP: Configure PRT rules for all other PCRFs	Repeat from step 36 for all other PCRFs connected to this DSR. This Routing configuration will ensure that whenever PCA requests DSR to route to a particular PCRF based on PRT, DSR will route to it if the PCRF is available, however, if not, it will route the message to any other available PCRF.				
38	SOAM VIP: Navigate to the Application Routing Rules screen	<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> <div data-bbox="509 898 1404 1346"> <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> </div> <ol style="list-style-type: none"> 1. Select the Default Application Route Table Name to which rules are to be added. 2. Click on View/Edit Rules button. 	Application Route Table Name	Number of Rules	Default	0
Application Route Table Name	Number of Rules					
Default	0					
39	SOAM VIP: Configure the ART for Gx 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	Default																												
Rule Name	GxRule	Un [D] sta																												
Application Route Table	Default	Ap																												
Priority	5	Pri Lov [D]																												
Conditions	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> <th>AND</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>16777238 - 3GPP Gx</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>AND</td> </tr> </tbody> </table>	Parameter	Operator	Value	AND	Destination-Realm	Always True		AND	Destination-Host	Always True		AND	Application-Id	Equals	16777238 - 3GPP Gx	AND	Command-Code	Always True	- Select -	AND	Origin-Realm	Always True		AND	Origin-Host	Always True		AND	Co Ea In t It n Ap [D]
	Parameter	Operator	Value	AND																										
	Destination-Realm	Always True		AND																										
	Destination-Host	Always True		AND																										
	Application-Id	Equals	16777238 - 3GPP Gx	AND																										
	Command-Code	Always True	- Select -	AND																										
	Origin-Realm	Always True		AND																										
Origin-Host	Always True		AND																											
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 [D]																												
Vendor Id		Ve Ve [D]																												
Answer Error Message		Str [D]																												
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**.

40

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"> <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**.

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

Repeat Step 40 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

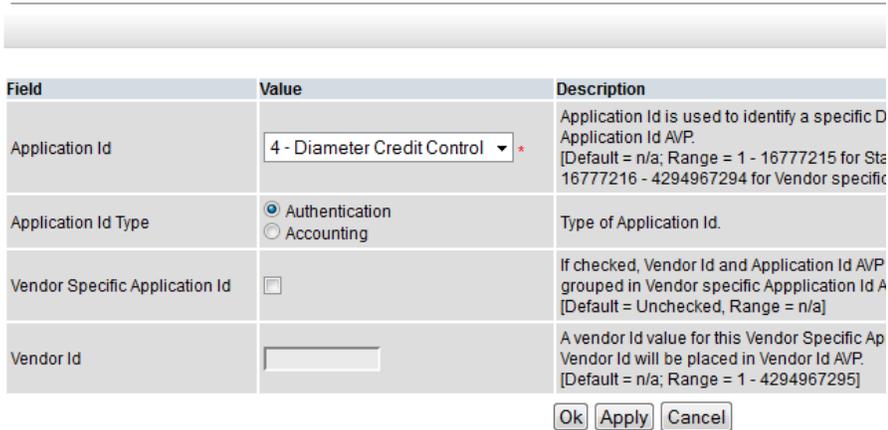
Detailed steps are given in the procedure below.

Procedure 11: 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 #	<p>This procedure configures the Diameter stack.</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>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 Application Id Configuration Screen</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Application Ids</p>																					
	3	<p>SOAM VIP: Add Application Id for GyRo 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" 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: 150px;" type="text"/> </td> <td>Application Id is used to identify the Application Id. [Default = n/a; Range = 1 - 16777216 - 4294967294 for Peer Node does not have a 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 Relay.</td> </tr> <tr> <td>Peer Route Table</td> <td>Default ▾</td> <td>Peer Route Table associated with the Application Id. Used for routing Requests when the downstream Peer Node does not have a Relay.</td> </tr> <tr> <td>Routing Option Set</td> <td>Default ▾</td> <td>Routing Option Set associated with the Application Id. Used when processing traffic when the downstream Peer Node does not have a Relay.</td> </tr> <tr> <td>Pending Answer Timer</td> <td>Default ▾</td> <td>Pending Answer Timer associated with the Application Id. Used when processing traffic when the downstream Peer Node does not have a Relay.</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 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: 150px;" type="text"/>	Application Id is used to identify the Application Id. [Default = n/a; Range = 1 - 16777216 - 4294967294 for Peer Node does not have a Relay]	Application Route Table	Default ▾	Application Route Table as Used for routing Requests when the downstream Peer Node does not have a Relay.	Peer Route Table	Default ▾	Peer Route Table associated with the Application Id. Used for routing Requests when the downstream Peer Node does not have a Relay.	Routing Option Set	Default ▾	Routing Option Set associated with the Application Id. Used when processing traffic when the downstream Peer Node does not have a Relay.	Pending Answer Timer	Default ▾	Pending Answer Timer associated with the Application Id. Used when processing traffic when the downstream Peer Node does not have a Relay.
	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: 150px;" type="text"/>	Application Id is used to identify the Application Id. [Default = n/a; Range = 1 - 16777216 - 4294967294 for Peer Node does not have a Relay]																					
Application Route Table	Default ▾	Application Route Table as Used for routing Requests when the downstream Peer Node does not have a Relay.																					
Peer Route Table	Default ▾	Peer Route Table associated with the Application Id. Used for routing Requests when the downstream Peer Node does not have a Relay.																					
Routing Option Set	Default ▾	Routing Option Set associated with the Application Id. Used when processing traffic when the downstream Peer Node does not have a Relay.																					
Pending Answer Timer	Default ▾	Pending Answer Timer associated with the Application Id. Used when processing traffic when the downstream Peer Node does not have a Relay.																					
4	<p>SOAM VIP: Navigate to CEX Parameters Screen</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> CEX Parameters</p>																						
5	<p>SOAM VIP: Add CEX Parameter for GyRo 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>  <p>1. Select Application Id "4 - Diameter Credit Control". 2. Click Ok.</p>
<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>

Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]

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**.

8

SOAM VIP: Configure the CEX Configuration Set for any other combination of Application Ids.

Repeat step 17 for any other combination of Application Ids that need to be shared in a CEX exchange with some other node, for example, BBERF etc.

9

SOAM VIP: Verify that all the required CEX Configuration Sets have been configured successfully.

Navigate to **Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets**

You should see a screen containing all the configured CEX Configuration Sets.

Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets

Mon Aug 11

Filter ▾

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	~

10	SOAM VIP: Navigate to Local Nodes screen	Navigate to Main Menu -> Diameter -> Configuration -> Local Nodes																																	
11	SOAM VIP: Configure the first Local Node (OC-DRA)	<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>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 underscores (_). A 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. 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 each label may contain letters, digits, dashes (-) and underscores (_). 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> <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 10.240.71.121(TSA) - Select - - Select - </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> <p>1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values).</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</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 underscores (_). A 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. 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 each label may contain letters, digits, dashes (-) and underscores (_). 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]	CEX Configuration Set	GyRo	CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]	IP Addresses	10.240.71.118 10.240.71.121(TSA) - Select - - Select - - Select - - Select - - Select - - Select -	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 underscores (_). A 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. 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 each label may contain letters, digits, dashes (-) and underscores (_). 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]																																	
CEX Configuration Set	GyRo	CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a]																																	
IP Addresses	10.240.71.118 10.240.71.121(TSA) - Select - - Select - - Select - - Select - - Select - - Select -	The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries]																																	

12	SOAM VIP: Configure other Local Nodes, if required.	Customer Service for further assistance. Repeat Step 11 and configure more Local Nodes if required.																																	
13	SOAM VIP: Navigate to Peer Nodes screen	Navigate to Main Menu -> Diameter -> Configuration -> Peer Nodes																																	
14	SOAM VIP: Configure the first CTF node	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p> <p>Main Menu: Diameter -> Configuration -> Peer Nodes -> [Insert] Help Wed Jul 04 06:42:01 2012 UTC</p> <p>Adding a new Peer node</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>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 underscores ('_'). Must contain at least one alpha and must not start with a dash or underscore.]</td> </tr> <tr> <td>Realm</td> <td>oracle.com *</td> <td>Realm of this Peer Node. Realm is a case-insensitive string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), and underscores ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. A label must be at most 63 characters long. [Default = n/a; Range = A valid Realm.]</td> </tr> <tr> <td>FQDN</td> <td>ctf.oracle.com *</td> <td>Fully Qualified Domain Name of this Peer Node. FQDN is a case-insensitive string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), and underscores ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. A label 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 Peer Node listens for SCTP.</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.</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 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 messages sent to this Peer Node is replaced with this Peer Node Realm. [Default = Unchecked; Range = n/a]</td> </tr> </tbody> </table>	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 underscores ('_'). Must contain at least one alpha and must not start with a dash or underscore.]	Realm	oracle.com *	Realm of this Peer Node. Realm is a case-insensitive string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), and underscores ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. A label must be at most 63 characters long. [Default = n/a; Range = A valid Realm.]	FQDN	ctf.oracle.com *	Fully Qualified Domain Name of this Peer Node. FQDN is a case-insensitive string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), and underscores ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. A label 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 Peer Node listens for SCTP.	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.	TCP Listen Port	3868	TCP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]	IP Addresses	01 10.250.53.53 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 messages sent to this Peer Node is replaced with this Peer Node Realm. [Default = Unchecked; Range = n/a]
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 underscores ('_'). Must contain at least one alpha and must not start with a dash or underscore.]																																	
Realm	oracle.com *	Realm of this Peer Node. Realm is a case-insensitive string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), and underscores ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. A label must be at most 63 characters long. [Default = n/a; Range = A valid Realm.]																																	
FQDN	ctf.oracle.com *	Fully Qualified Domain Name of this Peer Node. FQDN is a case-insensitive string of labels separated by dots, where a label may contain letters, digits, dashes ('-'), and underscores ('_'). A label must start with a letter, digit or underscore and must end with a letter or digit. A label 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 Peer Node listens for SCTP.																																	
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.																																	
TCP Listen Port	3868	TCP Listen Port number for this Peer Node. [Default = 3868; Range = 1024 - 65535]																																	
IP Addresses	01 10.250.53.53 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 messages sent to this Peer Node 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 ou this Peer Node Fully Qualified Domain Name. [Default = Unchecked; Range = n/a]
Minimum Connection Capacity	1 *	The minimum number of connections that must be avail Otherwise, the Peer is 'Degraded' if connections less th 'Available' or 'Unavailable' if no connections are available [Default = 1; Range = 1 - 64 connections]
Maximum Alternate Routing Attempts	4 *	The maximum number of times that a Request can be r 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 selecting the next eligible peer of a Peer Route Group w [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 the same same peer before selecting the next eligible peer of a P 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 selecting the next eligible peer of a Peer Route Group w - For an Answer response received from a DAS Peer (M Answer Result Code is determined by the Diameter -> C Copy Options -> DAS Answer Result Code parameter. [Default = Different Peer]
Peer Route Table	Default ▾	The Peer Route Table to be associated with this Peer N
Routing Option Set	Default ▾	The Routing Option Set to be associated with this Peer I
Pending Answer Timer	Default ▾	The Pending Answer Timer to be associated with this P

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**.

15 **SOAM VIP:** Configure other Peer Nodes

Repeat Step 14 to configure other CTF and OCS peer nodes as required.

16 **SOAM VIP:** Navigate to Connections screen

Navigate to **Main Menu -> Diameter -> Configuration -> Connections**

17 **SOAM VIP:** Configure the connection with CTF Node

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

You will see a screen similar to:

Main Menu: Diameter -> Configuration -> Connections -> [Insert] Help
Mon Feb 20 04:54:25 2012 EST

Adding a new connection

Field	Value	Description
Connection Name	conn_ctf *	A name that uniquely identifies the Connection. [Default = n/a; Range = A 32-character string. Valid characters not start with a digit.]
Transport Protocol	<input type="radio"/> SCTP <input checked="" type="radio"/> TCP	The transport protocol used by this Connection. The protocol should be supported by both Local Node and Peer Node.
Local Node	pca ▾ *	The Local Node of this Connection.
Connection Mode	Responder Only ▾ *	Initiator Only indicates that Local Node will only initiate the con Responder Only indicates that Local Node will only respond to Initiator & Responder indicates that Local Node will initiate con Node. [Default = Initiator & Responder; Range = n/a]
Local Initiate Port		The Local Initiate Port of this Connection. [Default = n/a; Range = 1024-65535]
Primary Local IP Address	10.240.71.121(TSA) ▾ *	The IP Address to be used as the Primary Local Node address.
Secondary Local IP Address	- Select - ▾	The IP Address to be used as the Secondary Local Node address. This address is only used for SCTP multi-homing.
Peer Node	CTF ▾ *	The Peer Node of this Connection.
Peer Node Identification	<input checked="" type="radio"/> IP Address <input type="radio"/> Transport FQDN <input type="radio"/> Peer Diameter Identity FQDN	Specifies whether the Peer Node is identified by IP address(es) been selected and no Transport FQDN has been specified, the Peer Diameter Identity FQDN has been selected.
Primary Peer IP Address	10.250.53.51 ▾ X	The IP Address to be used as the Primary Peer Node address.
Secondary Peer IP Address	- Select - ▾	The IP Address to be used as the Secondary Peer Node address. This address is only used for SCTP multi-homing. This address is only used for SCTP multi-homing. This address is only used for SCTP multi-homing.

	<table border="1"> <tr> <td>Transport FQDN</td> <td><input type="text"/></td> <td>Fully Qualified Domain Name for this connection. FQDN is a character label may contain letters, digits, dashes ("-") and underscore ("_"), letter or digit. Underscores may be used only as the first character. 255 characters long. [Default = n/a; Range = A valid FQDN]</td> </tr> <tr> <td>Connection Configuration Set</td> <td>Default <input type="button" value="v"/> *</td> <td>The configuration set of this Connection.</td> </tr> <tr> <td>CEX Configuration Set</td> <td>GxOnly <input type="button" value="v"/></td> <td>CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]</td> </tr> <tr> <td>Capacity Configuration Set</td> <td>Default <input type="button" value="v"/> *</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 characters must not start with a digit.]</td> </tr> <tr> <td>Remote Busy Usage</td> <td>Disabled <input type="button" value="v"/> *</td> <td>Defines which Request messages can be forwarded on this 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 received forwarded to (or rerouted to) this connection until the Remote Busy Abatement Timeout expires. 'Host Override' - The Connection is considered to be BUSY after whose Destination-Host AVP value is the same as the connection's Remote Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled, Host Override]</td> </tr> <tr> <td>Remote Busy Abatement Timeout</td> <td><input type="text" value="3"/></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> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>	Transport FQDN	<input type="text"/>	Fully Qualified Domain Name for this connection. FQDN is a character label may contain letters, digits, dashes ("-") and underscore ("_"), letter or digit. Underscores may be used only as the first character. 255 characters long. [Default = n/a; Range = A valid FQDN]	Connection Configuration Set	Default <input type="button" value="v"/> *	The configuration set of this Connection.	CEX Configuration Set	GxOnly <input type="button" value="v"/>	CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]	Capacity Configuration Set	Default <input type="button" value="v"/> *	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 characters must not start with a digit.]	Remote Busy Usage	Disabled <input type="button" value="v"/> *	Defines which Request messages can be forwarded on this 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 received forwarded to (or rerouted to) this connection until the Remote Busy Abatement Timeout expires. 'Host Override' - The Connection is considered to be BUSY after whose Destination-Host AVP value is the same as the connection's Remote Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled, Host Override]	Remote Busy Abatement Timeout	<input type="text" value="3"/>	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 character label may contain letters, digits, dashes ("-") and underscore ("_"), letter or digit. Underscores may be used only as the first character. 255 characters long. [Default = n/a; Range = A valid FQDN]																				
Connection Configuration Set	Default <input type="button" value="v"/> *	The configuration set of this Connection.																				
CEX Configuration Set	GxOnly <input type="button" value="v"/>	CEX Configuration Set of this Connection. [Default = n/a; Range = n/a]																				
Capacity Configuration Set	Default <input type="button" value="v"/> *	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 characters must not start with a digit.]																				
Remote Busy Usage	Disabled <input type="button" value="v"/> *	Defines which Request messages can be forwarded on this 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 received forwarded to (or rerouted to) this connection until the Remote Busy Abatement Timeout expires. 'Host Override' - The Connection is considered to be BUSY after whose Destination-Host AVP value is the same as the connection's Remote Busy Abatement Timeout expires. [Default = Disabled; Range = Disabled, Enabled, Host Override]																				
Remote Busy Abatement Timeout	<input type="text" value="3"/>	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>1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values).</p> <p>2. Click Ok.</p> <p>NOTE:</p> <p>Make sure the IPFE configuration matches the Transport Protocol which is selected in this step.</p>																					
<p>18 <input type="checkbox"/> SOAM VIP: Configure all other connection with Peer nodes</p>	<p>Repeat Step 17 to configure all other required connections.</p>																					
<p>19 <input type="checkbox"/> SOAM VIP: Configure Route Groups</p>	<p>For priority based initial CCR-I routing, there should be N+1 number for Route Groups configured where N is the number of OCSs in the system. The first N Route Groups shall contain a corresponding OCS node in them and the last Route Group shall contain ALL OCSs.</p> <p>The goal is to setup a Routing Configuration such that in case of an initial session request, Diameter Routing Layer sends the request messages to any available OCS.</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Route Groups</p>																					
<p>20 <input type="checkbox"/> SOAM VIP: Insert a new Route Group and add the first OCS to it.</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>																					

Main Menu: Diameter -> Configuration -> Route Groups -> [Insert] Help
Tue Feb 28 03:04:11 2012 EST

Adding a new route group

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 alpha 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 provision 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]
	01 OCS - Select - 1 X	
	<input type="button" value="Add"/>	
<input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

1. Enter the Route Group name.
2. Select the Peer Node name (OCS name).
3. Enter the provisioned capacity as 1.
4. Click [Ok](#).

21 **SOAM VIP:** Configure more Route Groups corresponding to each OCS.

Repeat Step 20 for every OCS that is connected to this DSR.

22 **SOAM VIP:** Configure one Route Group containing all OCS nodes

Click on [Insert](#) in the lower left corner.

You will see a screen similar to:

Main Menu: Diameter -> Configuration -> Route Groups -> [Insert] Help
Tue Feb 28 03:04:11 2012 EST

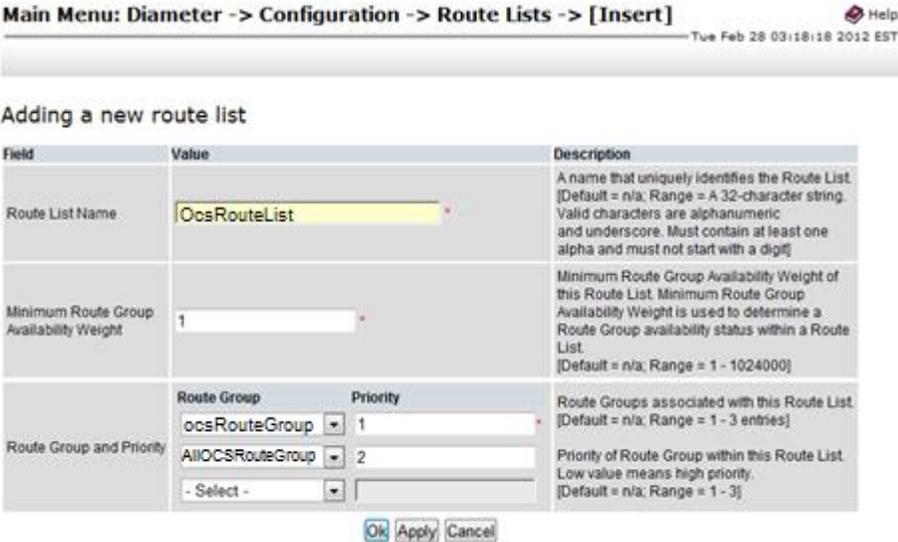
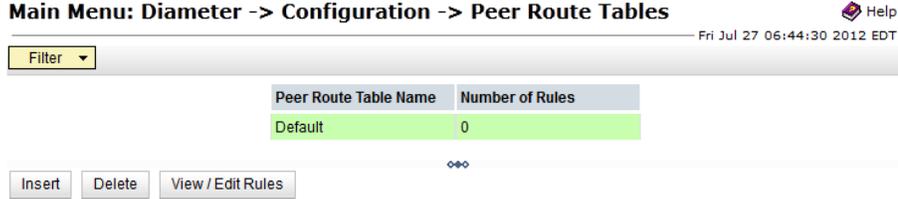
Adding a new route group

Field	Value	Description
Route Group Name	AllOCSRouteGroup	A name that uniquely identifies the Route Group. [Default = n/a; Range = A 32-character string. Valid characters are alpha 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 provision 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]
	01 OCS - Select - 1 X	
	02 OCS1 - Select - 1 X	
	03 OCS2 - Select - 1 X	
	<input type="button" value="Add"/>	
<input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

1. Enter the Route Group name
2. Select Type as 'Peer Route Group'
3. Select the Peer Node name (OCS name).
4. Enter the provisioned capacity as 1.
5. Click [Add](#) and add another OCS and so on.
6. Click [Ok](#).

23 **SOAM VIP:** Configure Route Lists

For priority based initial session binding, there should be N number for Route Lists configured where N is the number of OCSs in the system. All Route Lists shall contain two Route Groups.

		<p>The Route Group with a single OCS will have a higher priority whereas the Route Group with all OCSs will have a lower priority.</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Route Lists</p>
24	<p>SOAM VIP: Configure the first Route List</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>  <p>1. Enter the Route List name. 2. Minimum Route Group Availability Weight should be 1. 3. Assign priority 1 to the Route Group containing the intended OCS, assign priority 2 to the Route Group containing all the OCSs. 4. Click Ok.</p>
25	<p>SOAM VIP: Configure all other Route Lists</p>	<p>Repeat step 24 for all other OCSs connected to this DSR.</p>
26	<p>SOAM VIP: Configure the Peer Routing Rules.</p>	<p>Configure the PRT such that DSR forwards messages based on the OCS preference.</p> <p>Navigate to Main Menu -> Diameter -> Configuration -> Peer Route Table</p>
27	<p>SOAM VIP: Add PRT rules to Default PRT</p>	<p>Navigate to Main Menu -> Diameter -> Configuration -> Peer Route Table</p> <p>You will see a screen similar to:</p>  <p>Select the Default Peer Route Table Name to which rules are to be added and click on View/Edit Rules button.</p>
28	<p>SOAM VIP: Configure PRT rules for the first OCS</p>	<p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>

Inserting Rule for Peer Route Table: Default

Fri Jul 27 06:54:34 2012 EDT

Field	Value	Description																												
Rule Name	rule_ocs1 *	Unique name of the Rule. [Default = n/a; Range = A 32-character string, no spaces, no underscore. Must contain at least one letter.]																												
Peer Route Table	Default *	Peer Route Table associated with this Rule.																												
Priority	1 *	Priority of this Rule. Low value means higher priority. [Default = n/a; Range = 1 - 99]																												
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>ocs.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	ocs.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: Parameter, Operator, and Value. In order for a Diameter message to match the criteria of each condition, it must match the criteria of each condition.</p> <p>Application-Id: [Default = n/a; Range = 0-429]</p> <p>Command Code: [Default = n/a; Range = 0-167]</p> <p>Destination-Realm and Origin-Host: A label must start with a letter, Underscores may be used on a label, A label must be at most 63 characters long. [Default = n/a; Range = Sub string]</p> <p>Destination-Host and Origin-Host: Destination-Host and Origin-Host FQDN is a case-insensitive string where a label may contain letters, Underscores may be used on a label, A label must start with a letter, Underscores may be used on a label, 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	ocs.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	Action associated with this Rule. Route to Peer will route message to Peer. Send Answer will abandon message. Answer Result-Code Value as follows:																												
Route List	OcsRouteList	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. The Message Field value is set to 'Route to Peer'.																												
Answer Result-Code Value	<input type="radio"/> 3002 UNABLE_TO_DELIVER <input type="radio"/>	Value to be placed in the Answer Result-Code Value field. [Default = n/a; Range = 1000 - 4869]																												
Vendor Id		Vendor Id Value. Vendor Id will be placed in the Vendor-Id field. [Default = n/a; Range = 1 - 4294967295]																												
Answer Error Message		String to be placed in the Answer-Error-Message field. [Default = null string, no Error-Message]																												

Ok Apply Cancel

1. Enter the Rule name and priority values.
2. Select Destination host "Equals" the configured FQDN of OCS.
3. Select "Always True" for other conditions.
4. Select the Route List "OcsRouteList".
5. Click **Ok**.

NOTE: the above are sample configuration values, the actual configurations may differ.

29 **SOAM VIP:** Configure PRT rules for all other OCSs

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.

30 **SOAM VIP:** Navigate to the Application Routing Rules screen

Navigate to **Main Menu -> Diameter -> Configuration -> Application Routing Rules**

You will see a screen similar to:

Main Menu: Diameter -> Configuration -> Application Route Tables

Mon 4

Filter ▾

Application Route Table Name	Number of Rules
Default	0



1. Select the Default Application Route Table Name to which rules are to be added.
2. Click on [View/Edit Rules](#) button.

31

SOAM VIP: Configure the ART for GyRo 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	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"/>																												

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**.

32

SOAM VIP: Configure the ART for all other Interfaces

Repeat Step 31 for any other Application Id that needs to be routed to the PCA Application by Diameter Routing Layer.

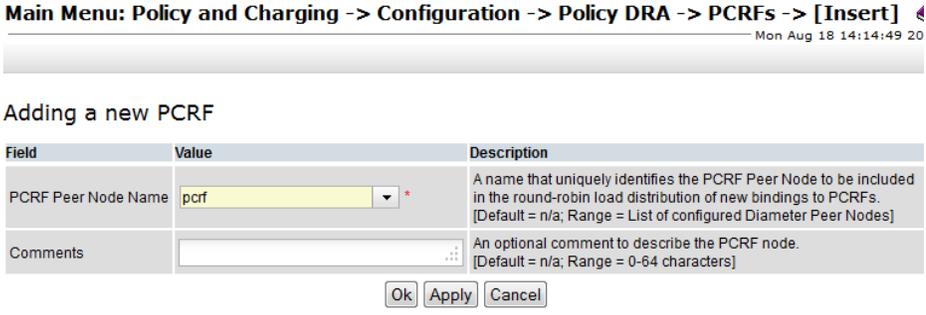
4.4 PCA FUNCTION CONFIGURATION PROCEDURES

This section provides the detailed procedure steps of the PCA configuration execution. These procedures are executed inside a maintenance window.

4.4.1 Policy DRA Configuration

Detailed steps are given in the procedure below.

Procedure 12: Policy DRA configuration

S T E P #	<p>This procedure configures the Policy DRA function of PCA application.</p> <p>PRE-REQUISITE: Procedure 10 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><u>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</u></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>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>
	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> <hr/> <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" data-bbox="516 409 1425 556"> <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;"><input type="button" value="Apply"/> <input type="button" value="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 - ▾											
6	<p>SOAM VIP: Configure the Binding Key Priorities</p>	<p>1. Select the Binding Keys priority as appropriate</p> <p>2. Click Apply.</p>										
7	<p>SOAM 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 -> Topology Hiding</p>										
8	<p>SOAM VIP: Configure the Peer node for which PCRF identity needs to be hidden</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 -> Topology Hiding -> [Insert] </p> <p style="text-align: right;">Mon Aug 18 14:22:53 2014</p> <hr/> <p>Adding a new Policy Client</p> <table border="1" data-bbox="516 1123 1425 1249"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Policy Client Peer Node Name</td> <td>pcrf ▾ *</td> <td>A name that uniquely identifies the Policy Client Peer Node from which PCRF names should be hidden. [Default = n/a; Range = List of configured Diameter Peer Nodes]</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	pcrf ▾ *	A name that uniquely identifies the Policy Client Peer Node from which PCRF names should be hidden. [Default = n/a; Range = List of configured Diameter Peer Nodes]	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	pcrf ▾ *	A name that uniquely identifies the Policy Client Peer Node from which PCRF names should be hidden. [Default = n/a; Range = List of configured Diameter Peer Nodes]										
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>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

SOAM VIP: Configure the Topology Hiding FQDN

Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Site Options

Mon Aug 18 14:35:4

Field	Value	Description
Topology Hiding Options	Enabled <input checked="" type="checkbox"/> Scope: Specific Hosts FQDN local.oracle.com Realm oracle.com	Settings for Topology Hiding Options: Enable (checked) or disable (unchecked) topology hiding using the checkbox. If Enabled, select the Scope, FQDN and Realm to apply for topology hiding. Scope: This sets the scope of messages where topology hiding will be applied. Select 'All Messages' to perform topology hiding for all messages destined for policy clients. Select 'All Foreign Realms' to perform topology hiding if the realm of the policy client is different from the realm of the PCRF that originated the message. Select 'Specific Hosts' to perform topology hiding only if the policy client is configured the Policy and Charging -> Configuration -> Policy DRA -> Topology Hiding screen. Select 'All Foreign Realms + Specific Hosts' to perform topology hiding if either condition ('All Foreign Realms' or 'Specific Hosts') is met. FQDN and Realm: These values are used to populate the Diameter Origin-Host and Origin-Realm AVP for answer messages routed from PCRF to a policy client, or the Diameter Destination-Host and Destination-Realm AVP for request messages routed from a PCRF to policy client. [Default = Disabled: No (unchecked), Scope: n/a, FQDN: n/a, Realm: n/a, Range = Enabled: Yes (checked) or No (unchecked), Scope: All Messages, All Foreign Realms, Specific Hosts, All Foreign Realms + Specific Hosts; 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	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.]

Apply Cancel

If required,

1. Check the Enabled box
2. Select the appropriate value of Scope from the dropdown
3. Enter the virtual/pseudo host FQDN and Realm
4. Click **Apply**.

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

12

NOAM VIP: Configure SBR Databases

Navigate to **Main Menu -> Policy and Charging -> Configuration -> SBR Databases**

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

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> SBR Databases -> [Insert]

Adding a new SBR Database

Field	Value	Description
Database Name	BindingSbrDb *	A name that uniquely identifies the SBR Database. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric contain at least one alpha and must not start with a digit]
Database Type	Binding *	The type of SBR Database. Select 'Binding' for a Policy Binding database, or 'Session' for a Policy DRA or Session database. [Default = n/a; Range = 'Binding' or 'Session']
Resource Domain	BindingRd_2SG *	The Policy and Charging Session or Policy Binding Resource Domain that 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 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 the selected Resource Domain already contains Server Groups, the number of Resource Domain is displayed in the field, but can be overridden as desired. [Default = n/a; Range = 1 to 8]
Place Association	BindingRegion *	The Policy Binding Region or Policy and Charging Mated Sites Place Association 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 already been assigned to a Database]

Ok Apply Cancel

1. Enter Database Name
2. Select Database Type.
3. Select Resource Domain. *This will populate Number of Server Groups field with the number of server groups currently present in the selected Resource Domain.*
4. If needed, update Number of Server Groups value. *Note that Resource Domain will then have to be updated to match this count.*
5. Select Place Association.
6. Click **Ok**

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

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.

13 NOAM VIP: Configure PCRF Pools

Navigate to **Main Menu -> Policy and Charging -> Configuration -> PCRF Pools**

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

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pools -> [Insert] Mon Aug 18 19:12:4

Adding a new PCRF Pool

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 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 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		An optional comment to describe the PCRF Pool or Sub-Pool. [Default = n/a; Range = 0-64 characters]

Ok Apply Cancel

		<p>1. Enter PCRF Pool name</p> <p>2. Click Ok</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>												
14	<p>NOAM VIP: Configure PCRF Sub Pool</p>	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> 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]</p> <p style="text-align: right;">Mon Aug 18 19:13:23</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>PrfSubPool01</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 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]</td> </tr> <tr> <td>Sub-Pool</td> <td><input checked="" 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></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> <p>1. Enter PCRF Sub Pool name</p> <p>2. Check the Sub-Pool box</p> <p>3. Click Ok.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>	Field	Value	Description	PCRF Pool Name	PrfSubPool01	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		An optional comment to describe the PCRF Pool or Sub-Pool. [Default = n/a; Range = 0-64 characters]
Field	Value	Description												
PCRF Pool Name	PrfSubPool01	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		An optional comment to describe the PCRF Pool or Sub-Pool. [Default = n/a; Range = 0-64 characters]												
15	<p>NOAM VIP: Configure PCRF Sub Pool Selection Rule</p>	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> PCRF Sub-Pools Selection Rules</p> <p>Click on Insert in the lower left corner.</p> <p>You will see a screen similar to:</p>												

Adding a new PCRF Sub-Pool Selection Rule

Field	Value	Description						
PCRF Sub-Pool Selection Rule Name	SubPoolSelectionRule01 *	A name that uniquely identifies the PCRF Sub-Pool Selection Rule. [Default = n/a; Range = A 32-character string. Characters are alphanumeric and underscores. Must contain at least one alpha and must end with a digit]						
Priority	50 *	Priority of this Rule. Low value means higher priority. [Default = 50; Range = 1 - 99]						
PCRF Pool Name	PcrfPool01 ▾ *	The name of the PCRF Pool for which a Sub-Pool is being defined. [Default = n/a; Range = Configured PCRF Pools that have not been specified as PCRF Sub-Pool Names]						
Conditions	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Operator</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Origin-Host</td> <td>Starts With ▾</td> <td>attservice01</td> </tr> </tbody> </table>	Parameter	Operator	Value	Origin-Host	Starts With ▾	attservice01	Condition associated with this Rule. Origin-Host: FQDN is a case-insensitive string consisting of a list of labels separated by dots, where a label contains letters, digits, dashes (-) and underscores (_). 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 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 ▾	attservice01						
PCRF Sub-Pool Name	PcrfSubPool01 ▾ *	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		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 do not 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.						

Ok Apply Cancel

1. Enter the Rule name
2. Select PCRF Pool Name and PCRF Sub-Pool Name
3. Enter the Condition as shown
4. Click **Ok**.

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

16

NOAM VIP: Configure Access Point Names

Navigate to **Main Menu -> Policy and Charging -> Configuration -> Access Point Names**

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

You will see a screen similar to:

Adding a new Access Point Name

Field	Value	Description
Access Point Name	apn01.oracle.com *	The network identifier of the Packet Data Network access point. [Default = n/a; Range = 1-100 characters. Valid characters are a characters (A-Z and a-z), digits (0-9), hyphen (-), and period (.). It must and end with an alphabetic character or a digit.]
PCRF Pool Name	PcrfPool01 *	The PCRF Pool to which new bindings initiated from the Access 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 as with the selected PCRF Pool. The mapping between PCRF Pool Sub-Pool is configured in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules.
Stale 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 configured time. If a session's age is longer than 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. If no sessions are associated with this Access Point Name, the Default Stale Session Timeout value in the Policy and Charging -> Configuration -> Network-Wide Options table is used. [Default = 168 hours (7 days); Range = 1-2400 hours (1 hour to 2400 hours)]
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 more recent. This field records the time and date of changes that may affect routing of binding capable session initiation requests. This date can be compared against binding creation times when troubleshooting using Policy and Charging -> Maintenance -> Policy Database Configuration.

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.

17

SOAM VIP: Navigate to PCRF Pool To PRT Mapping screen

Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping**

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping

Filter

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 Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules.

PCRF Pool Name	Peer Route Table Name
Default	Default
PcrfPool01	Not Selected
PcrfSubPool01	Not Selected

18

SOAM VIP: Configure the PCRF Pool To PRT Mapping

Select the row with 'Not Selected' under Peer Route Table Name and click 'Edit'

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping -> [Edit] Mon Aug 18 15:39:33 2014

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.]

Ok Apply Cancel

- Select appropriate Peer Route Table Name form the dropdown.
- Click **Ok**.

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

19 SOAM VIP: Configure other PCRF Pool To PRT Mapping

Repeat Step 17 for all other PCRF Pool Names where the Peer Route Table Name is displayed as **'Not Selected'**.

20 SOAM VIP: Navigate to the Error Codes screen

Navigate to **Main Menu -> Policy and Charging -> Configuration -> Error Codes**

You will see a screen similar to:

Main Menu: Policy and Charging -> Configuration -> Error Codes Mon Aug 18 15:46:20 2014 EDT

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

21 SOAM VIP: Configure the Error Codes

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 15:49:53

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.
Gv/Gxx Result Code	3002	Result code to be returned on the Gx and Gxx interfaces. [Default = 3002; Range = 1-9999]
Gv/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]
Gy/Ro Result Code	3002	Result code to be returned on the Gy/Ro interface. [Default = 3002; Range = 1-9999]
Gy/Ro Vendor ID		Vendor ID which corresponds with the experimental code for the Gy/Ro interface. [Default = n/a; Range = 1-4294967295]

Ok Apply Cancel

		<ol style="list-style-type: none"> 1. Enter the Result Code and Vendor ID values as appropriate 2. Click Ok. 																											
22	SOAM VIP: Navigate to Suspect Binding Removal Rules screen OPTIONAL	<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>																											
23	SOAM VIP: Configure the Suspect Binding Removal Rule for Diameter Interfaces and messages that are needed. OPTIONAL	<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" data-bbox="527 640 1364 1144"> <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 NOAM 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> <ol style="list-style-type: none"> 1. Enter the Rule Name 2. Select the Application Name from the dropbox 3. Select the Command Code(Message) from the dropbox 4. Select the required Error Scenario Category from the dropbox 5. If the "External Error" Error Scenario Category was selected, Enter the Result Code 6. If the "External Error" Error Scenario Category was selected, Enter the Vendor ID(Optional) 7. Check the Remove Suspect Binding Immediately checkbox if the Binding is to be removed on the first rule match. If not, leave the checkbox unchecked. 8. Click Ok. <p>NOTE: This is a sample set of configuration data, the actual configuration may differ.</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 NOAM 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 NOAM 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]																											
24	SOAM VIP: Configure additional Suspect Binding Removal Rules. OPTIONAL	<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	NOAM VIP: Enable	Navigate to Main Menu -> Policy and Charging -> Configuration																											

the Policy DRA function

-> **General Options** Screen.

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)]

1. Check the Policy DRA Enabled box
2. Click **Apply**.

4.4.2 Online Charging DRA Configuration

Detailed steps are given in the procedure below.

Procedure 13: Online Charging DRA configuration

<p>S T E P #</p>	<p>This procedure configures the Online Charging DRA function of PCA application.</p> <p>PRE-REQUISITE: Procedure 11 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><u>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</u></p>										
<p>1 <input type="checkbox"/></p>	<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>									
<p>2 <input type="checkbox"/></p>	<p>SOAM VIP: Navigate to OCSs screen</p>	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> OCSs</p>									
<p>3 <input type="checkbox"/></p>	<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] Mon Nov 24 13:35:</p> <hr/> <p>Adding a new OCS</p> <table border="1" data-bbox="516 947 1412 1081"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>OCS Peer Node Name</td> <td><input type="text"/></td> <td>A name that uniquely identifies the OCS Peer Node to be included in the load distribution of new session initiation diameter request messages to OCSs. [Default = n/a; Range = List of configured Diameter Peer Nodes]</td> </tr> <tr> <td>Comments</td> <td><input type="text"/></td> <td>An optional comment to describe the OCS 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 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>	Field	Value	Description	OCS Peer Node Name	<input type="text"/>	A name that uniquely identifies the OCS Peer Node to be included in the load distribution of new session initiation diameter request messages to OCSs. [Default = n/a; Range = List of configured Diameter Peer Nodes]	Comments	<input type="text"/>	An optional comment to describe the OCS node. [Default = n/a; Range = 0-64 characters]
Field	Value	Description									
OCS Peer Node Name	<input type="text"/>	A name that uniquely identifies the OCS Peer Node to be included in the load distribution of new session initiation diameter request messages to OCSs. [Default = n/a; Range = List of configured Diameter Peer Nodes]									
Comments	<input type="text"/>	An optional comment to describe the OCS node. [Default = n/a; Range = 0-64 characters]									
<p>4 <input type="checkbox"/></p>	<p>SOAM VIP: Configure all other OCS nodes.</p>	<p>Repeat Step 3 to configure all the OCS nodes.</p>									
<p>5 <input type="checkbox"/></p>	<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>									
<p>6 <input type="checkbox"/></p>	<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] Mon Aug 18 16:46:51</p> <hr/> <p>Adding a new CTF</p> <table border="1" data-bbox="516 1682 1404 1816"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CTF Peer Node Name</td> <td>ctf <input type="text"/></td> <td>A name that uniquely identifies the CTF Peer Node. [Default = n/a; Range = List of configured Diameter Peer Nodes]</td> </tr> <tr> <td>Comments</td> <td><input type="text"/></td> <td>An optional comment to describe the CTF 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 CTF name from the drop down</p>	Field	Value	Description	CTF Peer Node Name	ctf <input type="text"/>	A name that uniquely identifies the CTF Peer Node. [Default = n/a; Range = List of configured Diameter Peer Nodes]	Comments	<input type="text"/>	An optional comment to describe the CTF Peer Node. [Default = n/a; Range = 0-64 characters]
Field	Value	Description									
CTF Peer Node Name	ctf <input type="text"/>	A name that uniquely identifies the CTF Peer Node. [Default = n/a; Range = List of configured Diameter Peer Nodes]									
Comments	<input type="text"/>	An optional comment to describe the CTF Peer Node. [Default = n/a; Range = 0-64 characters]									

		<p>2. Click Ok.</p> <p>NOTE: this is a sample set of configuration data, the actual configuration may differ.</p>																		
7	<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>																		
8	<p>NOAM VIP: Configure SBR Databases</p>	<p>Navigate to Main Menu -> Policy and Charging -> Configuration -> SBR Databases</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 -> SBR Databases -> [Insert]</p> <hr/> <p>Adding a new SBR Database</p> <table border="1" data-bbox="527 709 1446 1192"> <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 Binding 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 configured for use by this database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching 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 selected Resource Domain already contains Server Groups, Resource Domain is displayed in the field, but can be overridden. [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 Policy Binding Region will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching already been assigned to a Database]</td> </tr> </tbody> </table> <p style="text-align: right;">Ok Apply Cancel</p> <ol style="list-style-type: none"> 7. Enter Database Name 8. Select Database Type (Session). 9. 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> 10. If needed, update Number of Server Groups value. <i>Note that Resource Domain will then have to be updated to match this count.</i> 11. Select Place Association. 12. Click Ok <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 Binding Session database. [Default = n/a; Range = 'Binding' or 'Session']	Resource Domain	SessionRd_Mated *	The Policy and Charging Session or Policy Binding Resource Domain configured for use by this database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching 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 selected Resource Domain already contains Server Groups, Resource Domain is displayed in the field, but can be overridden. [Default = n/a; Range = 1 to 8]	Place Association	MatedSites *	The Policy Binding Region or Policy and Charging Mated Sites Policy Binding Region will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching 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 Binding Session database. [Default = n/a; Range = 'Binding' or 'Session']																		
Resource Domain	SessionRd_Mated *	The Policy and Charging Session or Policy Binding Resource Domain configured for use by this database. Select the Resource Domain that will host this database. [Default = n/a; Range = Configured Resource Domains matching 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 selected Resource Domain already contains Server Groups, Resource Domain is displayed in the field, but can be overridden. [Default = n/a; Range = 1 to 8]																		
Place Association	MatedSites *	The Policy Binding Region or Policy and Charging Mated Sites Policy Binding Region will use this database. Select the Place Association that is to use this SBR Database. [Default = n/a; Range = Configured Place Associations matching already been assigned to a Database]																		
9	<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>																		

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 9, 10, 11 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-gtxa.com	OCS1-GTXA-east-gtxa.com	No

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

OPTIONAL

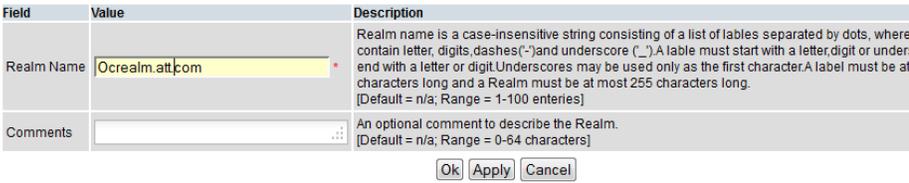
Select an OCS by highlighting the line, click on edit in the lower left corner.

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-gtxa.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-GTXA-east-gtxa.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>									
12	NOAM VIP: Configure the Session State for all other OCSs.	OPTIONAL Repeat Step 10 to configure all the OCSs.									
13	NOAM VIP: Navigate to Realms screen	OPTIONAL Navigate to Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> Realms									
14	NOAM VIP: Configure the first Realm.	OPTIONAL Click on Insert in the lower left corner. You will see a screen similar to: Main Menu: Policy and Charging -> Configuration -> Online Charging DRA -> Realms -> [Insert]  <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>Realms 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	Realms 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									
Realms 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]									
15	NOAM VIP: Configure all other Realm names.	OPTIONAL Repeat Step 3 to configure all the realms.									
16	NOAM VIP: Navigate to Network-Wide Options screen	OPTIONAL Navigate to Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> Network-Wide Options									
17	NOAM VIP: Configure the options										

Main Menu: Policy and Charging -> Configuration -> Online Charging DRA -> Network-Wide Options

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']
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

1. Select the appropriate values for the available options
2. Click **Apply**.

18

SOAM VIP: Navigate to the Error Codes screen

Navigate to **Main Menu -> Policy and Charging -> Configuration -> Error Codes**

You will see a screen similar to:

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

Mon Aug 18 15:46:20 2014 EDT

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

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]

Ok Apply Cancel

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 14: 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 13.

4.5.2 Configuring Online Charging DRA in existing Sites

Detailed steps are given in the procedure below.

Procedure 15: 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 13 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 16: 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 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 17: 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 ORACLE TAC.	
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 FUNCTION FROM A RUNNING DSR PCA SYSTEM

Detailed steps are given in the procedure below.

Procedure 18: 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 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 is Enabled (Checked) or 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 is Enabled (Checked) or 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. 	Field	Value	Description	Policy DRA Enabled	<input type="checkbox"/>	Indicate whether the Policy DRA is Enabled (Checked) or Policy DRA disabled (Unchecked)	Online Charging DRA Enabled	<input type="checkbox"/>	Indicate whether the Online Charging DRA is Enabled (Checked) or 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)									
Online Charging DRA Enabled	<input type="checkbox"/>	Indicate whether the Online Charging DRA is Enabled (Checked) or Online Charging DRA Disabled (Unchecked)									
3 <input type="checkbox"/>	NOAM VIP: Disable the Policy DRA specific SBR Database	<p>Main Menu -> Policy and Charging -> Maintenance -> SBR Database Status</p> <p>Select the SBR Database of type 'Binding' and Disable it.</p>									
4 <input type="checkbox"/>	NOAM VIP: Delete the Policy DRA specific SBR Database	<p>Main Menu -> Policy and Charging -> Configuration -> SBR Databases</p> <p>Delete the SBR Database of type 'Binding' from this screen.</p>									
5 <input type="checkbox"/>	NOAM VIP: Delete the Policy DRA specific APNs	<p>Main Menu -> Policy and Charging -> Configuration -> Access Point Names</p> <p>Delete the Policy DRA specific configuration data from this screen.</p>									
6 <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".									
7 <input type="checkbox"/>	SOAM VIP: De-reference all the PRTs from PCRF Pools	<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>									
8 <input type="checkbox"/>	SOAM VIP: Delete all the PCRFs	<p>Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRFs</p> <p>Delete the complete configuration data from this screen.</p>									
9 <input type="checkbox"/>	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>									
10 <input type="checkbox"/>	SOAM VIP: Un-	Main Menu -> Policy and Charging -> Configuration ->									

<input type="checkbox"/>	configure the Site Options	Policy DRA -> Site Options Uncheck the 'Enabled' box against 'Topology Hiding Options'.
11 <input type="checkbox"/>	SOAM VIP: Restore default values of Error Codes (OPTIONAL)	Main Menu -> Policy and Charging -> Configuration -> Error Codes Edit all Error Conditions and set the Result Code as 3002 for all Policy DRA application interfaces (Gx/Gxx, Rx, S9, Gx-Prime).
12 <input type="checkbox"/>	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Steps 4 to 9 on All Active SOAM servers.
13 <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".
14 <input type="checkbox"/>	NOAM VIP: Delete all the Sub-Pool Selection Rules	Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules Delete the complete configuration data from this screen.
15 <input type="checkbox"/>	NOAM VIP: Delete all the PCRF Pools	Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pools 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 19: Un-configuring Online Charging DRA

STEP #	This procedure un-configures the Online Charging DRA function of 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 <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: Disable the Online Charging DRA function	Navigate to Main Menu -> Policy and Charging -> Configuration -> General Options Screen. <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	NOAM VIP: Delete all configured Realms	Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> Realms Delete the complete configuration data from this screen.									
4	NOAM VIP: Delete the Online Charging specific APNs	Main Menu -> Policy and Charging -> Configuration -> Access Point Names Delete the Online charging specific configuration data from this screen.									
5	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".									
6	SOAM VIP: Delete the Online Charging Servers	Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> OCSs Delete the complete configuration data from this screen.									
7	SOAM VIP: Delete the Online charging Clients	Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> CTFs Delete the complete configuration data from this screen.									
8	SOAM VIP: Restore default values of Error Codes (OPTIONAL)	Main Menu -> Policy and Charging -> Configuration -> Error Codes <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. 									
9	SOAM VIP: Perform	Repeat Steps 5 to 7 on All Active SOAM servers.									

<input type="checkbox"/>	steps on All Active SOAM Servers	
--------------------------	----------------------------------	--

4.9 POST-CONFIGURATION PROCEDURES

4.9.1 Enable Application

Detailed steps are given in the procedure below.

Procedure 20: Enable Application

S T E P #	This procedure enables 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 <u>ORACLE TAC</u> .																						
	NOTE: - PLEASE DO ALL RESOURCE DOMAIN RELATED CONFIGURATION BEFORE CONTINUING THIS STEP.																						
	1 <input type="checkbox"/>	Establish GUI Session on the active SOAM VIP	Establish a GUI session on the all Active SOAM servers by using the XMI VIP address. Login as user "guiadmin".																				
2 <input type="checkbox"/>	SOAM VIP: Navigate to Applications screen	Navigate to Main Menu -> Diameter -> Maintenance -> Applications																					
3 <input type="checkbox"/>	SOAM VIP: Enable the PCA application	Select the PCA row and Click Enable .																					
4 <input type="checkbox"/>	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" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <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 <input type="checkbox"/>	SOAM VIP: Enable PCA application on All Active SOAM servers	Repeat Steps 1 to 4 on All Active SOAM servers from Active Servers List collected from Step 1 of Procedure 4.																					

4.9.2 Enable SBR Databases

Detailed steps are given in the procedure below.

Procedure 21: 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> <p>NOTE: - PLEASE DO ALL RESOURCE DOMAIN RELATED CONFIGURATION BEFORE CONTINUING THIS STEP.</p>																						
1 <input type="checkbox"/>	Establish GUI Session on the active NOAMP VIP	Establish a GUI session on the Active NOAMP servers by using the XMI VIP address. Login as user "guiadmin".																					
2 <input type="checkbox"/>	NOAMP VIP: Navigate to SBR Database Status screen	Navigate to Main Menu -> Policy and Charging -> Maintenance -> SBR Database Status																					
3 <input type="checkbox"/>	NOAMP VIP: Prepare the SBR Database	Select the SBR Database and Click Prepare .																					
4 <input type="checkbox"/>	NOAMP VIP: Verify that the SBR Database has been prepared.	<p>Navigate to Main Menu -> Policy and Charging -> 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>Main Menu: Policy and Charging -> Maintenance -> SBR Database Status</p> <p style="text-align: right;">Thu May 07 07:36:41 2</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 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>Prepare</td> <td>Prepared</td> <td>3 of 3 prepared</td> <td>2 of 2 prepared</td> <td>No</td> <td>Binding</td> </tr> <tr> <td>SessionSbrDb</td> <td>Prepare</td> <td>Prepared</td> <td>3 of 3 prepared</td> <td>2 of 2 prepared</td> <td>No</td> <td>Session</td> </tr> </tbody> </table> </div> <p>NOTE:</p> <p>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	Prepare	Prepared	3 of 3 prepared	2 of 2 prepared	No	Binding	SessionSbrDb	Prepare	Prepared	3 of 3 prepared	2 of 2 prepared	No	Session
Database Name	Administrative State	Operational Status	Resource User Operational Reason	Resource Provider Operational Reason	Reconfiguration In Progress	Database Type																	
BindingSbrDb	Prepare	Prepared	3 of 3 prepared	2 of 2 prepared	No	Binding																	
SessionSbrDb	Prepare	Prepared	3 of 3 prepared	2 of 2 prepared	No	Session																	
5 <input type="checkbox"/>	NOAMP VIP: Enabled the SBR Database	Select the SBR Database and Click Enable .																					
6 <input type="checkbox"/>	NOAMP VIP: Verify that the SBR Database has been enabled.	<p>Navigate to Main Menu -> Policy and Charging -> 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>																					

Main Menu: Policy and Charging -> Maintenance -> SBR Database Status Thu May 07 07:37:4

Filter

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

NOTE:
It may take some time (5-6 seconds) to change state.

7 **NOAMP VIP:** Enable PCA application on All Active SOAM servers

Repeat Steps 1 to 6 for all SBR Databases which are to be enabled.

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.

4.9.3 Restart Process

Detailed steps are given in the procedure below.

Procedure 22: Restart Server

S T E P #	<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 <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 DSR MP and Policy and Charging SBR Servers	Navigate to Main Menu -> Status & Manage -> Server Select all the MP servers with Function "Diameter Signaling Router" and "Policy and Charging SBR" then Click Restart .

4.9.4 Enable Connections

Detailed steps are given in the procedure below.

Procedure 23: Enable connections

S T E P #	<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> <p>SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC.</p>	
1 <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".
2 <input type="checkbox"/>	SOAM VIP: Navigate to Connections screen	Navigate to Main Menu -> Diameter -> Maintenance -> Connections

<p>3</p> <p>SOAM VIP: Enable all connections</p>	<p>Select all Connection rows and Click Enable.</p>																																																								
<p>4</p> <p>SOAM VIP: Verify that the connections have been Enabled.</p>	<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.</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 24: 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 HA Services Status</p> <p>Verify HA Services status:</p> <ol style="list-style-type: none"> 1. Log into the NOAM GUI using the XMI VIP address. 2. Select Main Menu: Communication Agent -> Maintenance -> HA Services Status 3. Verify that the Main Menu: Communication Agent -> Maintenance -> HA Services Status view screen is shown in work area. 4. Verify that the "Resource Routing Status" is shown as "Available" for all the "User/Provider" listed. <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 Automatic Connection Count for all the PCA and Policy SPR servers</p> <p>Verify ComAgent Automatic Connection Status:</p> <ol style="list-style-type: none"> 1. Log into the NOAM GUI using the XMI VIP address. 2. Select Main Menu: Communication Agent -> Maintenance -> Connection Status 3. Verify that the Main Menu: Communication Agent -> Maintenance -> Connection Status view screen is shown in work area. 4. Verify that the "Automatic Connection Count" for each of the servers are shown as "X or Y In Service" Where Y >= X and X=Y indicates successful Automatic Connection setup. <p>If all the verifications are successful, then proceed with next step else STOP! And call ORACLE Customer Service for further assistance.</p>
	3 <input type="checkbox"/>	<p>Verify the Policy and Charging SBR Status</p> <p>Verify Policy and Charging SBR Services status:</p> <ol style="list-style-type: none"> 5. Log into the NOAM GUI using the XMI VIP address. 6. Select Main Menu: Policy and Charging -> Maintenance -> Policy and Charging SBR Status 7. Verify that the Main Menu: Policy and Charging -> Maintenance -> Policy and Charging SBR Status view screen is shown in work area. 8. 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" tables. <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 REVIEW MEETING MINUTES

The initial formal review for this document is archived in the Document Review tool, under Review ID 1.

8.0 APPENDIX-A

8.1 PCA FEATURE ACTIVATION PROCEDURE

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

8.1.1 PCA Activation on a freshly installed system

Detailed steps are given in the procedure below.

Procedure 25: PCA Activation

S T E P #	<p>This procedure activates the PCA on complete system.</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: Navigate to HA screen</p> <p>Navigate to Main Menu: Status & Manage -> HA</p> <p>Find the Active NOAM and Active SOAM Servers list</p>
	2	<p>Verify configuration of All SOAM servers</p> <p>Before continuing all SOAM servers should be configured in the topology.</p> <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 are configured and Application State is enabled.
	3	<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># ssh <active NO XMI VIP Address></pre>
	4	<p>PCA Application Activation: Change directory</p> <p>Change to the following directory:</p> <pre># cd /usr/TKLC/dsr/prod/maint/loaders/activate</pre>
	5	<p>PCA Activation: Execute the PCA application activation script</p> <pre># ./load.pcaActivationTopLevel</pre> <p>Note: - This command execution will starts Activation on NOAM servers and All Active SOAM servers.</p> <p>If the activation fails, then execute the procedure in Section 8.2.2 to restore the system back to state before start of activation.</p>
6	<p>PCA Application Activation (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># clearCache</pre>	

8.1.2 PCA Activation on a newly added site

Detailed steps are given in the procedure below.

NOTE:- This procedure needs to be executed only if a new site is added in 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 26: PCA Activation on newly added site

S T E 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>NOAM VIP: Navigate to HA screen</p>	<p>Navigate to Main Menu: Status & Manage -> HA</p> <p>Find the Active NOAM and Active SOAM Servers list</p>
2 <input type="checkbox"/>	<p>Verify configuration of All SOAM servers</p>	<p>Before continuing all SOAM servers should be configured in the topology.</p> <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 are configured and Application State is enabled.
3 <input type="checkbox"/>	<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># ssh <active NO XMI VIP Address></pre>
4 <input type="checkbox"/>	<p>PCA Activation: Change directory</p>	<p>Change to the following directory:</p> <pre># cd /usr/TKLC/dsr/prod/maint/loaders/activate</pre>
5 <input type="checkbox"/>	<p>PCA Activation: Execute the PCA application activation script</p>	<pre># ./load.pcaActivationTopLevel</pre> <p>Note: - This command execution will start activation on newly added SOAM Servers.</p> <p>If the activation fails, then execute the procedure in Section 8.2.3 to restore the system back to state before start of activation.</p>
6 <input type="checkbox"/>	<p>PCA Activation (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># clearCache</pre>

8.1.3 Restart Process

Detailed steps are given in the procedure below.

Procedure 27: Restart Process

S T E	<p>This procedure restarts the DSR and SBR application processes.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p>
----------------------	--

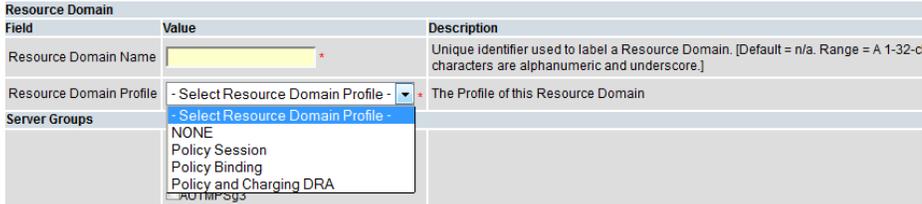
P #	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ORACLE TAC .	
	NOTE: - This STEP is MANDATORY only if DSR MP AND PSBR Servers are newly added in the TOPOLOGY.	
1 □	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2 □	NOAM VIP: Restart Process on DA-MP Servers	Navigate to Main Menu -> Status & Manage -> Server Select all the DA-MP servers and press Restart .
3 □	NOAM VIP: Restart Process on SBR Servers	Navigate to Main Menu -> Status & Manage -> Server Select all the SBR servers and press Restart .

8.1.4 Post PCA Activation System Health Check

8.1.4.1 System health check after Application Activation on NOAM server

Detailed steps are given in the procedure below.

Procedure 28: Verification of application activation on NOAM Server

S T E P #	This procedure verifies the PCA application activation on NOAM Server. 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 □	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.	Verify that the Resource Domain Profile show the new profile entries. Main Menu: Configuration -> Resource Domains [Insert] 
3 □	NOAM VIP: Verify that the PCA specific KPIs are shown.	Verify that KPIs menu shows the KPI tabs for PCA, SBR, SBR-Binding and SBR-Sessoin. Main Menu: Status & Manage -> KPIs 
4 □	NOAM VIP: Verify that the PCA specific Measurement groups	Verify that Measurement groups are shown for OC-DRA, P-DRA and PSBR.

are shown.

Main Menu: Measurements -> Report

Filter

Scope: - Network Element - - Server Group - - Resource Domain - - Place -

- Place Association - Reset

Report: -- Group -- -- Interval -- Reset

Column Filter:

- Group --
- ComAgent Exception
- ComAgent Performance
- OAM ALARM
- OAM PERF
- OAM.SYSTEM
- OC-DRA Congestion Exception
- OC-DRA Diameter Exception
- OC-DRA Diameter Usage
- P-DRA Congestion Exception
- P-DRA Diameter Exception
- P-DRA Diameter Usage
- SBR Audit
- SBR Binding Exception
- SBR Binding Performance
- SBR Policy Session Exception
- SBR Policy Session Performance
- Server Exception

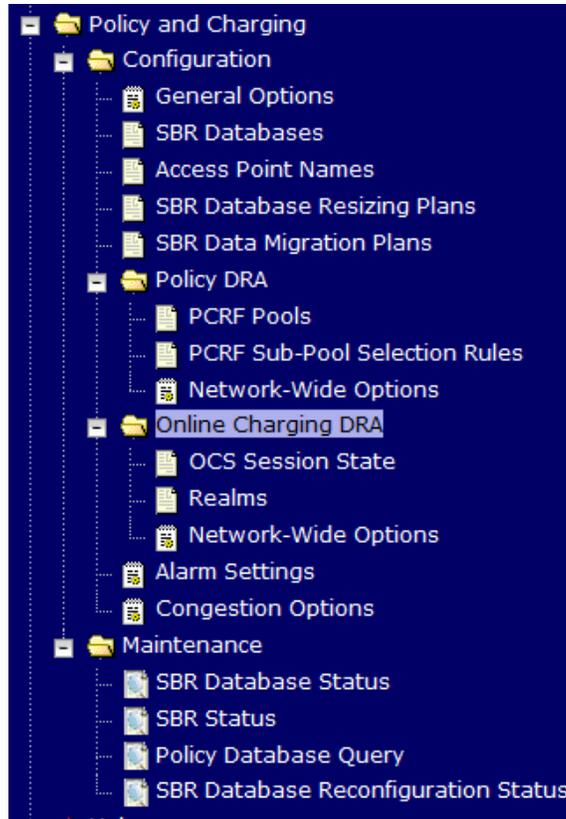
Time Range: 2014 Jan 01 00 00 Reset

Go

5

NOAM VIP: Verify that the Main Menu shows the Policy and Charging submenu.

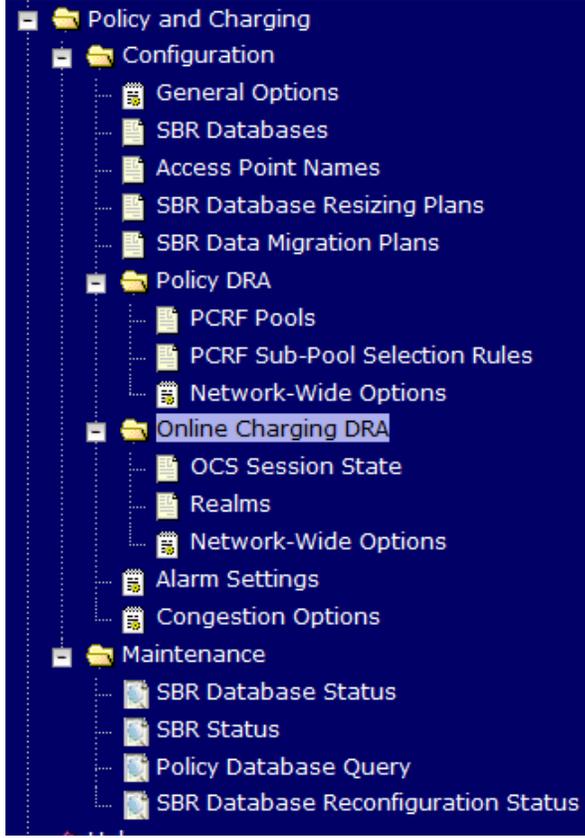
Verify that Main Menu on Active NOAM shows the Policy and Charging submenu with Configuration and Maintenance screens.



8.1.4.2 System health check after Application Activation on SOAM servers

Detailed steps are given in the procedure below.

Procedure 29: Verification of application activation on SOAM Servers

S T E P #	<p>This procedure verifies the activation of PCA 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>	
1 <input type="checkbox"/>	SOAM VIP: Establish GUI Session using SOAM VIP	Establish a GUI session on the Active SOAM by using the XML VIP address. Login as user "guiadmin".
2 <input type="checkbox"/>	SOAM VIP: Verify that the Policy and Charging folder is visible in the Left Hand Menu	Verify that the Policy and Charging folder appears on the Left Hand Menu:
		

8.2 PCA FEATURE DE-ACTIVATION PROCEDURE

This section provides the detailed steps of the PCA De-Activation procedures.

8.2.1 Pre PCA De-Activation Steps

8.2.1.1 Verify and Deactivate the GLA application

Detailed steps are given in the procedure below.

Procedure 30: 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 ORACLE TAC .		
	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	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
	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.	Verify the GLA application is present. 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 De-activation procedures defined in [4].	
5 <input type="checkbox"/>	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Step 1-4 on All Active SOAM servers.	

8.2.1.2 Disable PCA Functions

Detailed steps are given in the procedure below.

Procedure 31: Disable PCA Functions (PDRA and OCDRA)

S T E P #	This procedure disables the DSR connections.	
	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"/>	Establish GUI Session on the NOAM VIP

2 <input type="checkbox"/>	NOAM VIP: Disable PCA Functions.	<p>Navigate to Main Menu: Policy and Charging -> Configuration -> General Options</p> <p>Uncheck 'Policy DRA Enabled' and 'Online Charging DRA Enabled'. Click Apply.</p> <p>Main Menu: Policy and Charging -> Configuration -> General Options Thu Nov 20 14:57:07 2012</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 style="text-align: center;"><input 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 style="text-align: center;"><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>	Field	Value	Description	Policy DRA Enabled	<input 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 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)]									

8.2.1.3 Disable Diameter Connections

Detailed steps are given in the procedure below.

Procedure 32: Disable Diameter Connections

S T E P #	<p>This procedure disables the Diameter connections.</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"/>	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.	<p>Navigate to Main Menu: Diameter -> Maintenance -> Connections</p> <p>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.</p> <p>Main Menu: Diameter -> Maintenance -> Connections Tue Jun 12 11:26:40 2012 UT</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 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>PDR</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>PDR</td> <td>PCEF1</td> <td>---</td> </tr> </tbody> </table>	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	PDR	AF1	---	conn_pcef	blade12	Disabled	Unavailable	Disabled	Responder Only	PDR	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	PDR	AF1	---																					
conn_pcef	blade12	Disabled	Unavailable	Disabled	Responder Only	PDR	PCEF1	---																					
3 <input type="checkbox"/>	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Steps 1 to 2 on All Active SOAM servers.																											

8.2.1.4 Disable Application

Detailed steps are given in the procedure below.

Procedure 33: Disable application

S T E P #	<p>This procedure disables the 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 SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".														
2 <input type="checkbox"/>	SOAM VIP: Navigate to Applications screen	Navigate to Main Menu -> Diameter -> Maintenance -> Applications														
3 <input type="checkbox"/>	SOAM VIP: Disable the PCA application	<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"/>	SOAM VIP: Verify that the PCA application has been Disabled.	<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</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Filter ▾</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">DSR Application Name</th> <th style="text-align: left;">MP Server Hostname</th> <th style="text-align: left;">Admin State</th> <th style="text-align: left;">Operational State</th> <th style="text-align: left;">Operational Reason</th> <th style="text-align: left;">Congestion Level</th> <th style="text-align: left;">Time of Last Update</th> </tr> </thead> <tbody> <tr> <td>PDRA</td> <td>blade12</td> <td style="border: 2px solid #ff00ff;">Disabled</td> <td>Unavailable</td> <td style="background-color: #ffcc00;">Not Initialized</td> <td>Normal</td> <td>2012-Jun-12 06:33:43 U</td> </tr> </tbody> </table> </div>	DSR Application Name	MP Server Hostname	Admin State	Operational State	Operational Reason	Congestion Level	Time of Last Update	PDRA	blade12	Disabled	Unavailable	Not Initialized	Normal	2012-Jun-12 06:33:43 U
DSR Application Name	MP Server Hostname	Admin State	Operational State	Operational Reason	Congestion Level	Time of Last Update										
PDRA	blade12	Disabled	Unavailable	Not Initialized	Normal	2012-Jun-12 06:33:43 U										
5 <input type="checkbox"/>	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Steps 1 to 4 on All Active SOAM servers.														

8.2.1.5 Stop Processes

Detailed steps are given in the procedure below.

Procedure 34: Stop Server Process

S T E P #	<p>This procedure stops the DSR and PSBR processes.</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 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: Stop DSR MP and PSBR MP Server processes.</p>	<p>Find the DA-MP and SBR server hostnames corresponding to the functions "Diameter Signaling Router" and "SBR" from Main Menu: Configuration -> Server Groups</p> <p>Then, navigate to Main Menu -> Status & Manage -> Server</p> <p>Select all the DA-MP and SBR and press Stop.</p>

8.2.1.6 Remove PCA Configuration Data

Detailed steps are given in the procedure below.

Procedure 35: Remove PCA configuration data

S T E P #	<p>This procedure removes the PCA 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>	
	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: Remove all the data from PCA screen as mentioned.</p>	<p>NOTE: THIS STEP #2 IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ACTIVATE PCA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF CONFIGURATION DATA AFTER RE-ACTIVATION. HOWEVER ALL SUBSEQUENT STEPS IN THIS PROCEDURE ARE MANDATORY.</p> <p>Main Menu: Policy DRA -> Configuration -> PCRFs</p> <p>Delete the complete configuration data from this screen.</p>
3 <input type="checkbox"/>	<p>SOAM VIP: Perform steps on All Active SOAM Servers</p>	<p>Repeat Steps 1 and 2 on All Active SOAM servers.</p>
4	<p>Establish GUI Session on the NOAMP VIP</p>	<p>Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user "guiadmin".</p>
5	<p>NOAMP VIP: Complete or Cancel any ongoing Reconfiguration Plans</p>	<p>Main Menu: Policy and Charging -> Maintenance -> SBR Database Reconfiguration Status</p> <p>If any Reconfiguration Plan is in the Prepared or Preparing state, then click Cancel to return to the Planned state.</p> <p>If any Reconfiguration Plan has been started then click Complete and confirm the confirmation dialog by clicking Force Complete to transition to the Complete state.</p>

<p>6 NOAMP VIP: Delete any existing Reconfiguration Plans</p>	<p>Main Menu: Policy and Charging -> Configuration -> SBR Database Resizing Plans</p> <p>Delete all Database Resizing Plans from this screen.</p> <p>Main Menu: Policy and Charging -> Configuration -> SBR Data Migration Plans</p> <p>Delete all Data Migration Plans from this screen.</p>
---	---

8.2.1.7 Remove DSR Configuration Data

Detailed steps are given in the procedure below.

Procedure 36: 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="padding-left: 40px;">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> <p style="padding-left: 40px;">B.) DON'T EXECUTE THIS STEP IF THERE ARE MUTIPLE APPLICATIONS INSTALLED ON THIS SYSTEM.</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 all the data of 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 all the data of 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 all the data of 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 all the data of 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 all the data of 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 all the data of 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 all the data of 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 all the data of 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	SOAM VIP: Remove all the data of CEX Parameters.	Main Menu: Diameter -> Configuration -> CEX Parameters. Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.
11	SOAM VIP: Remove all the data of Application IDs	Main Menu: Diameter -> Configuration -> Application Ids Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.
12	SOAM VIP: Perform steps on All Active SOAM Servers	Repeat Steps 1 to 11 on All Active SOAM servers.

8.2.2 PCA De-Activation Procedure

Detailed steps are given in the procedure below.

Procedure 37: PCA Application De-Activation

S T E P #	This procedure de-activates 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 <u>ORACLE TAC</u> .		
	1	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: # ssh <active NO XMI IP Address>
	2	PCA Deactivation: Change directory	Change to the following directory: # cd /usr/TKLC/dsr/prod/maint/loaders/deactivate
	3	PCA Deactivation: Execute the PCA application de-activation script	# ./load.pcaDeactivationTopLevel Note: - This command execution will starts De-Activation on Active NOAM and All Active SOAM servers.
	4	PCA Deactivation [OPTIONAL]: Clear the Web Server cache	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. # clearCache
5	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".	
6	NOAM VIP: Restart DSR MP Servers	Navigate to Main Menu -> Status & Manage -> Server Select all the DA-MP servers and press Restart .	

8.2.3 Site Specific PCA De-Activation Procedure

THIS SECTION ONLY REQUIRED WHEN A PARTICULAR SITE NEEDS TO BE DEACTIVATED FOR PCA APPLICATION.

Detailed steps are given below.

Procedure 38: PCA Application De-Activation on a particular site.

S T E P #	<p>This procedure de-activates 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 <u>ORACLE TAC</u>.</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> <p style="text-align: center;"># ssh <active SO XMI IP Address></p>
	2 <input type="checkbox"/>	<p>PCA Deactivation: Change directory</p> <p>Change to the following directory:</p> <p># cd /usr/TKLC/dsr/prod/maint/loaders/deactivate</p>
	3 <input type="checkbox"/>	<p>PCA Deactivation: Execute the PCA application de-activation script</p> <p># ./load.pcaDeactivateBscoped</p> <p>Note: - This command execution will start De-Activation on selected active SOAM server.</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> <p># clearCache</p>	

8.2.4 Post PCA De-Activation Steps

8.2.4.1 Move Policy and Charging SBR Servers to OOS State

Detailed steps are given in the procedure below.

Procedure 39: Move Policy and Charging SBR Servers to OOS State

S T E P #	<p>This procedure puts all the MP Servers in Policy and Charging SBR Server Groups in OOS.</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: - 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 <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 Server Groups screen</p> <p>Navigate to Main Menu: Configuration -> Server Groups</p>
	3 <input type="checkbox"/>	<p>NOAM VIP: Find the Server List</p> <p>Find the Servers with Function as "Policy and Charging SBR".</p>
	4 <input type="checkbox"/>	<p>NOAM VIP: Navigate to HA screen</p> <p>Navigate to Main Menu: Status & Manage -> HA</p> <p>Edit the Servers from list created in Step 3. Change the value of "Max Allowed HA Role" to OOS.</p>

8.2.4.2 Remove Policy and Charging SBR Servers from Server Groups

Detailed steps are given in the procedure below.

Procedure 40: Remove Policy and Charging SBR Servers from Server Groups

S T E P #	<p>This procedure removes all the MP Servers in Policy and Charging SBR Server Groups from their respective Server Groups.</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: - 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 <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 Server Groups screen</p> <p>Navigate to Main Menu: Configuration -> Server Groups</p>
	3 <input type="checkbox"/>	<p>NOAM VIP: Find the Server List</p> <p>Find the Servers with Function as "Policy and Charging SBR".</p>
	4 <input type="checkbox"/>	<p>NOAM VIP: Edit the Server Groups.</p> <p>Navigate to Main Menu: Configuration -> Server Groups</p> <p>Edit the Server Group with "Policy and Charging SBR" function and remove the servers from it.</p>

	Repeat the steps with all server groups with "Policy and Charging SBR" function.
--	--

8.2.4.3 Delete Server Groups related to Policy and Charging SBR

Detailed steps are given in the procedure below.

Procedure 41: Delete Server Groups related to Policy and Charging SBR

S T E P #	This procedure removes the Server Groups related to Policy and Charging SBR.	
	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	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".

8.2.4.4 Remove Place Configuration Data

Detailed steps are given in the procedure below.

Procedure 42: Remove Place configuration data

S T E P #	This procedure removes the Place configuration data.	
	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"/>	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.

8.2.4.5 Reboot the Servers

Detailed steps are given in the procedure below.

Procedure 43: Reboot the Servers

S T E P #	This procedure removes the merge data from Servers by rebooting them.	
	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	

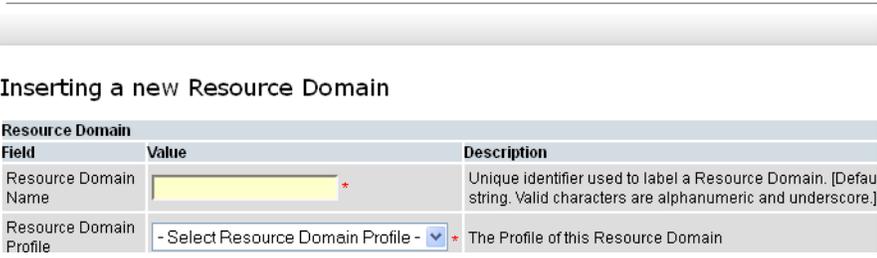
THIS SYSTEM AND YOU WANT TO RE-USE THE CONFIGURATION DATA AFTER RE-ACTIVATION.		
1	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2	NOAM VIP: Navigate to Server Groups Screen	Navigate to Main Menu: Status & Manage -> Server
3	NOAM VIP: Reboot the Servers.	Reboots all the servers. Click each row of server and press Reboot. Keep order from down to top. So that the self-server is rebooted at last. After rebooting the last server (self-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.

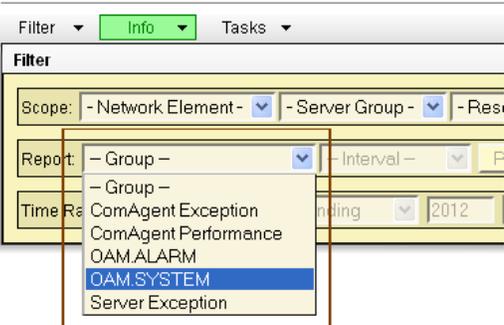
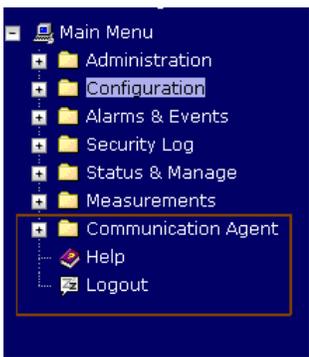
8.2.5 Post PCA De-Activation System Health Check

8.2.5.1 System health check after PCA De-activation on NOAM server

Detailed steps are given in the procedure below.

Procedure 44: Verification of application de-activation on NOAM Server

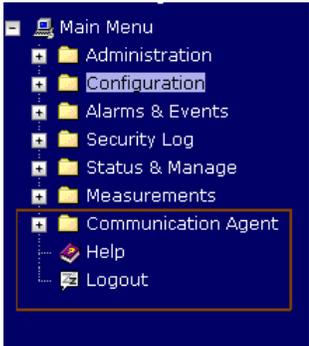
S T E P #	This procedure verifies the PCA application deactivation on NOAM Server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR <u>ORACLE TAC</u> .										
	1	Active 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 doesn't show the profile entries of Binding and Session Profiles. Verify that the Resource Domain Profile drop down doesn't show the profile entries of "Policy Session" and "Policy Binding". Main Menu: Configuration -> Resource Domains [Insert]  Inserting a new Resource Domain <table border="1" data-bbox="516 1367 1393 1507"> <thead> <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 Resource Domain. [Default string. Valid 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> </tbody> </table>	Field	Value	Description	Resource Domain Name	<input type="text"/>	Unique identifier used to label a Resource Domain. [Default string. Valid characters are alphanumeric and underscore.]	Resource Domain Profile	- Select Resource Domain Profile -	The Profile of this Resource Domain
	Field	Value	Description								
	Resource Domain Name	<input type="text"/>	Unique identifier used to label a Resource Domain. [Default string. Valid characters are alphanumeric and underscore.]								
Resource Domain Profile	- Select Resource Domain Profile -	The Profile of this Resource Domain									
3	NOAM VIP: Verify that the KPIs are not shown for PCA, SBR, SBR-Binding and SBR-Session. Verify that KPIs menu don't show the KPI tabs for PCA, SBR, SBR-Binding and SBR-Session. Main Menu: Status & Manage -> KPIs 										
4	NOAM VIP: Verify that the Measurement groups are not shown for OC-DRA, P-DRA and SBR. Verify that Measurement groups are not shown for OC-DRA, P-DRA and SBR.										

	<p>Main Menu: Measurements -> Report</p> 
<p>5 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> 

8.2.5.2 System health check after Application Deactivation on SOAM servers

Detailed steps are given in the procedure below.

Procedure 45: Verification of application de-activation 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 ORACLE TAC.</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><input type="checkbox"/></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><input type="checkbox"/></p>	<p>SOAM VIP: Verify PCA application on All Active SOAM servers</p>	<p>Repeat Steps 1 to 3 on All Active SOAM servers from Active Servers List collected from Step 1 of Procedure 4.</p>							