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

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 Diameter Network Check for Policy DRA 18

NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION 18

SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY 18

3.5.2 Diameter Network Check for Online Charging DRA 21

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 Policy and Charging Places 24

PROCEDURE 4: POLICY AND CHARGING PLACES CONFIGURATION 24

4.1.2 Policy and Charging Mated Sites Place Associations 25

PROCEDURE 5: POLICY AND CHARGING MATED SITES PLACE ASSOCIATIONS CONFIGURATION 25

4.1.3 Policy Binding Region Place Associations 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 Policy and Charging DRA Resource Domain Configuration 27

PROCEDURE 7: POLICY AND CHARGING DRA RESOURCE DOMAIN CONFIGURATION 27

4.2.2 Policy Session Resource Domain Configuration 28

PROCEDURE 8: POLICY SESSION RESOURCE DOMAIN CONFIGURATION 28

4.2.3 Policy Binding Resource Domain Configuration 29

PROCEDURE 9: POLICY BINDING RESOURCE DOMAIN CONFIGURATION 29

4.3 DIAMETER CONFIGURATION PROCEDURES 31

4.3.1 Diameter Configuration for Policy DRA 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 Diameter Configuration for Online Charging DRA 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 Policy DRA Configuration 62

PROCEDURE 12: POLICY DRA CONFIGURATION 62

4.4.2 Online Charging DRA Configuration 72

PROCEDURE 13: ONLINE CHARGING DRA CONFIGURATION 72

4.5 CONFIGURING ONLINE CHARGING FUNCTION ON A RUNNING DSR PCA SYSTEM 78

4.5.1 Configuring new Online Charging DRA Sites 78

PROCEDURE 14: NEW ONLINE CHARGING DRA SITE CONFIGURATION 78

4.5.2 Configuring Online Charging DRA in existing Sites 78

PROCEDURE 15: ONLINE CHARGING DRA CONFIGURATION ON A RUNNING DSR PCA SYSTEM 78

4.5.3 Configuring Online Charging DRA in existing Sites with scaling 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 Configuring Policy DRA 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 Enable Application 83
PROCEDURE 20: ENABLE APPLICATION 83
4.9.2 Enable SBR Databases 85
PROCEDURE 21: ENABLE SBR DATABASES 85
4.9.3 Restart Process 86
PROCEDURE 22: RESTART SERVER 86
4.9.4 Enable Connections 86
PROCEDURE 23: ENABLE CONNECTIONS 86
4.9.5 Perform Health Check 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 PCA Activation on a freshly installed system 92
PROCEDURE 25: PCA ACTIVATION 92
8.1.2 PCA Activation on a newly added site 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 Restart Process 93
PROCEDURE 27: RESTART PROCESS 93
8.1.4 Post PCA Activation System Health Check 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 Pre PCA De-Activation Steps 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 PCA De-Activation Procedure....103
PROCEDURE 37: PCA APPLICATION DE-ACTIVATION....103
8.2.3 Site Specific PCA De-Activation Procedure....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 Post PCA De-Activation Steps....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 Post PCA De-Activation System Health Check....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).

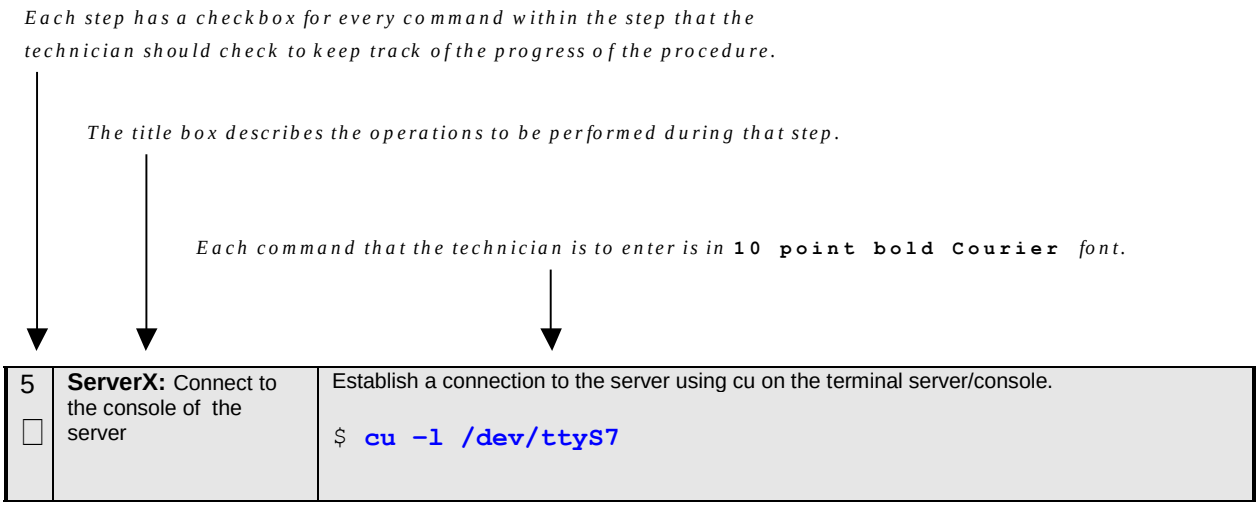


Figure 1. Example of a procedure step

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 requrie 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

STEP #	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 ☐	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 #	This procedure verifies System Topology. 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 ☐	Verify Network Element Configuration data	View the Network Elements configuration data; verify the data; save and print report: 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 ☐	Verify Services Configuration data	View the Services configuration data; verify the data; save and print report: 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 ☐	Verify Place Configuration data	View the Place configuration data; verify the data; save and print report: 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 ☐	Verify Server Group Configuration data	View the Server Group configuration data; verify the data; save and print report: 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 ☐	Analyze and plan DA-MP restart sequence	Analyze system topology and plan for any DA-MPs which will be out-of-service during the PCA configuration sequence. 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 ☐	Verify Network Configuration data	View the Network configuration data; verify the data; save and print report: 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 ☐	Verify Devices Configuration data	View the Devices configuration data; verify the data; save and print report: 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.

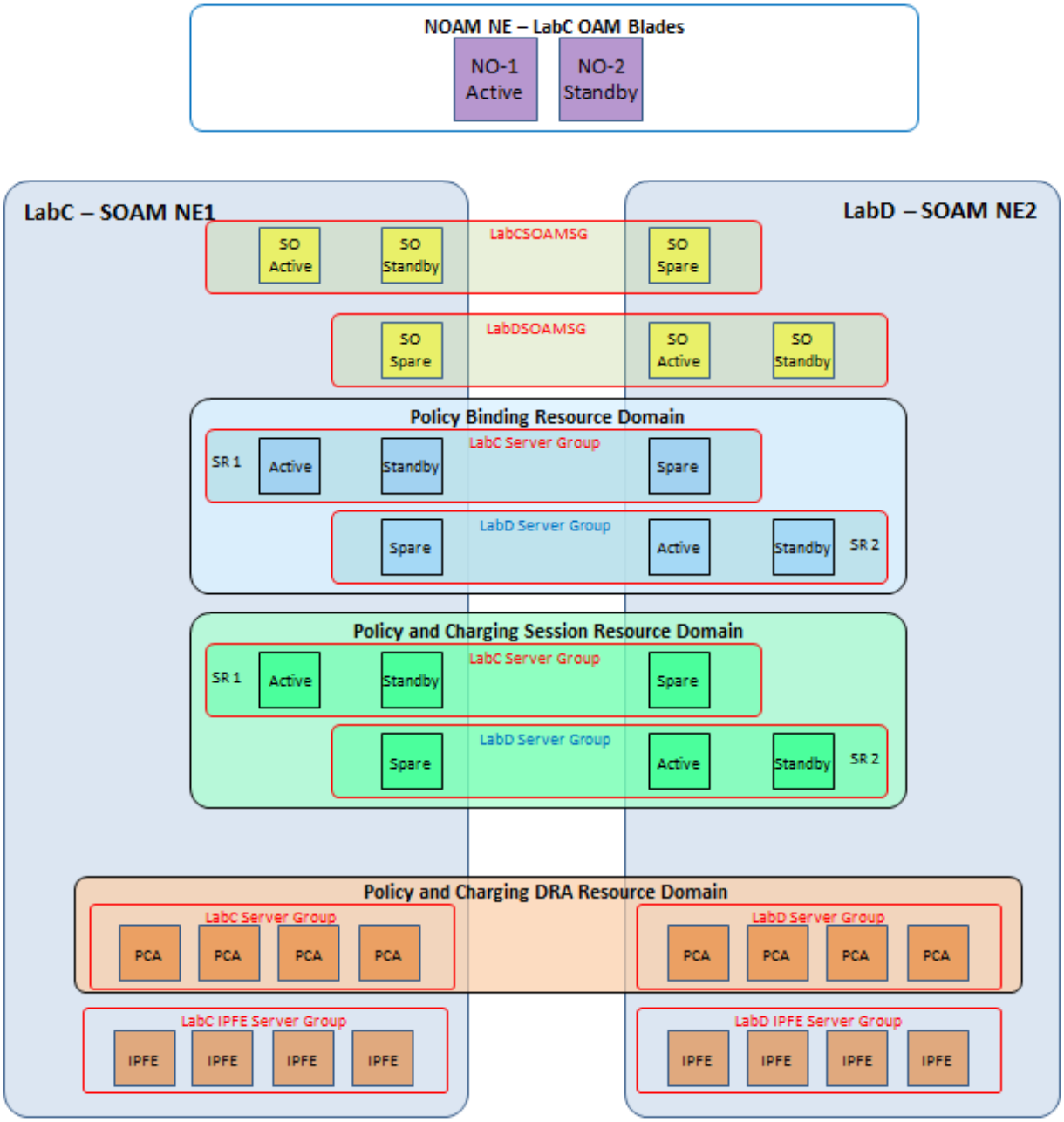


Figure 2: Example - PCA / Policy and Charging SBR Topology

S T E P #	This procedure verifies and logs PCA Topology for the setup. This information must be gathered before configuring the 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 ☐	Identify the Place and Place Association Information.	1. Identify and note the number of places and place names below – 2 in example, there might be upto 12 places. **Number of Places:** **Place Names:** 2. Identify and note the number of PCA mated pairs – LabC and Lab D in example. **Number of PCA Mated Pairs:** 3. If Policy DRA function is being configured, then identify and note the Binding Region place associations **Note: This step is required for Policy DRA functionality only.** 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). **Number of Places in Binding Region:** 4. Identify and note the other required place associations 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) **PCA Mated Site 1: Lab C and Lab D** **PCA Mated Site 2:** **PCA Mated Site 3:** **PCA Mated Site 4:** **PCA Mated Site 5:** **PCA Mated Site 6:** **PCA Mated Site 7:**
2 ☐	Identify and log the Resource Domain information.	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.

		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.

		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 -** **…**

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 #	This procedure verifies PCA – Policy 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 ORACLE TAC.**	
1 ☐	Identify the diameter network and properties.	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 Indentification' 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 ☐	Policy DRA Network configuration (NO scoped)	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 – 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 – 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 Topoligy Hinding 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

3 ☐	Policy DRA Site Configuration (SO scoped)	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 ORACLE TAC.**	
1 ☐	Identify the diameter network and properties.	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 Indentification' 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 ☐	Online Charging DRA Network configuration (NO scoped)	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 – 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 – 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 ☐	Policy DRA Site Configuration (SO scoped)	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 #	This procedure performs a Health Check. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	Verify DSR Release	DSR Release supports the PCA Application: 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 ☐	Verify Server status	Verify Server status: 1. Select **Status & Manage > Server;** the Server Status screen is shown. 2. Verify all Server Status is Normal (Norm) for Application Status (Appl State), Alarms (Alm), Database (DB), Collection (Reporting Status), and Processes (Proc). 3. Do not proceed to PCA configuration if any of the following statuses is not **Norm: DB, Reporting Status, Proc**. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the PCA configuration. Contact Engineering for assistance as necessary. 4. If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the PCA configuration. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the PCA configuration. The activation may be able to proceed in the presence of certain Major or Critical alarms. Contact Engineering for assistance as necessary.
3 ☐	Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active;** the Alarms & Events > View Active view is shown. 2. Click **Report** button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference. Note: the system should be alarm free unless the user is aware of the alarms and understands the impact. 4. Select **Alarms & Events > View History** and repeat steps 2 and 3.

4.0 PCA CONFIGURATION

Before PCA configuration, execute the site survey and the system health check specified in Section3.0.. 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

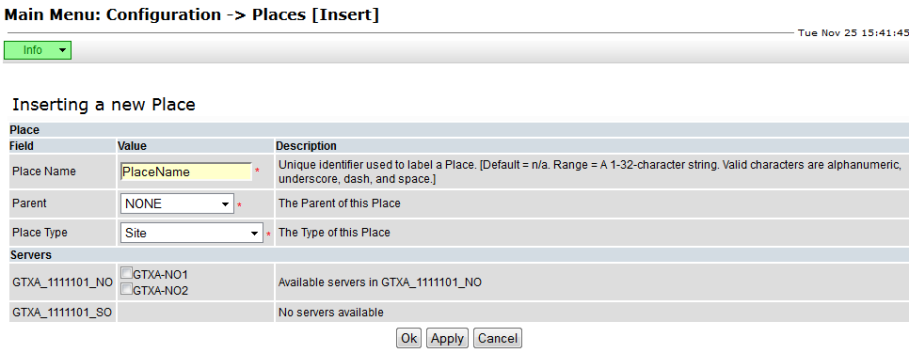
The following type of Place Associations is required for Policy DRA function ONLY:

- Policy Binding Region

4.1.1 Policy and Charging Places

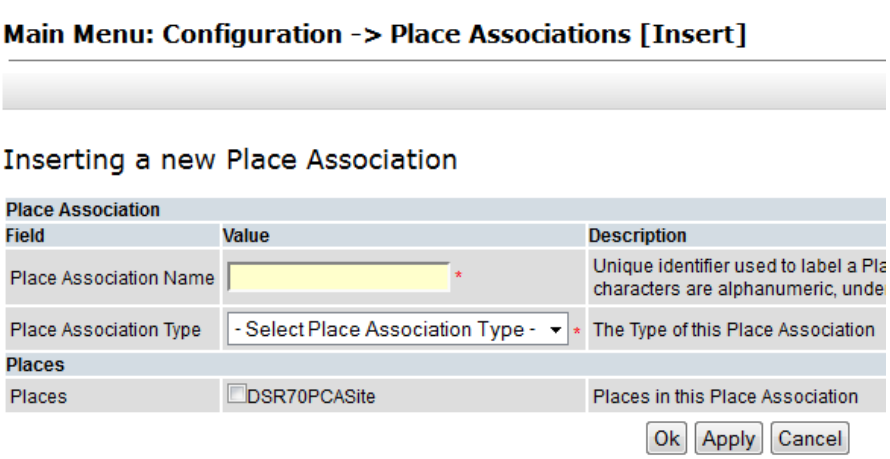
NOTE: EXECUTE THIS PROCEDURE ONLY IF NEW MP SERVERS ARE TO CONFIGURED IN THE TOPOLOGY OTHER THAN THOSE CONFIGURED DURING INSTALLATION PROCEDURE FROM [1]

Procedure 4: Policy and Charging Places configuration

S T E P #	This procedure configures the Places. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**NOAM VIP:** Navigate to Places screen	Navigate to **Main Menu -> Configuration -> Places** Screen.
3 ☐	**NOAM VIP:** Add a new Place	Click on **Insert** in the lower left corner. You will see a screen similar to:  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**.
4 ☐	**NOAM VIP:** Add other Places.	Repeat Step 4 for all other Places that are to be added.

4.1.2 Policy and Charging Mated Sites Place Associations

Procedure 5: Policy and Charging Mated Sites Place Associations configuration

S T E P #	This procedure configures Place Association Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**. **ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.**	
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 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:  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**.

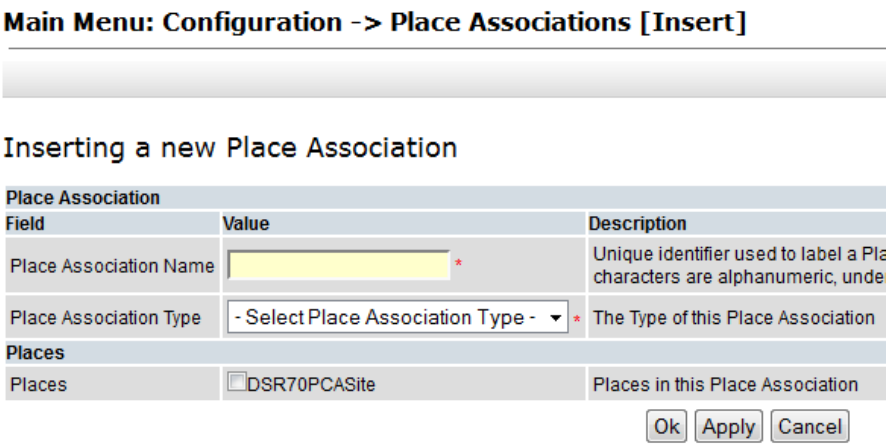
4.1.3 Policy Binding Region Place Associations

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 #	This procedure configures the Policy Binding Region Place Associations 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	Establish GUI Session	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".

	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:  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:

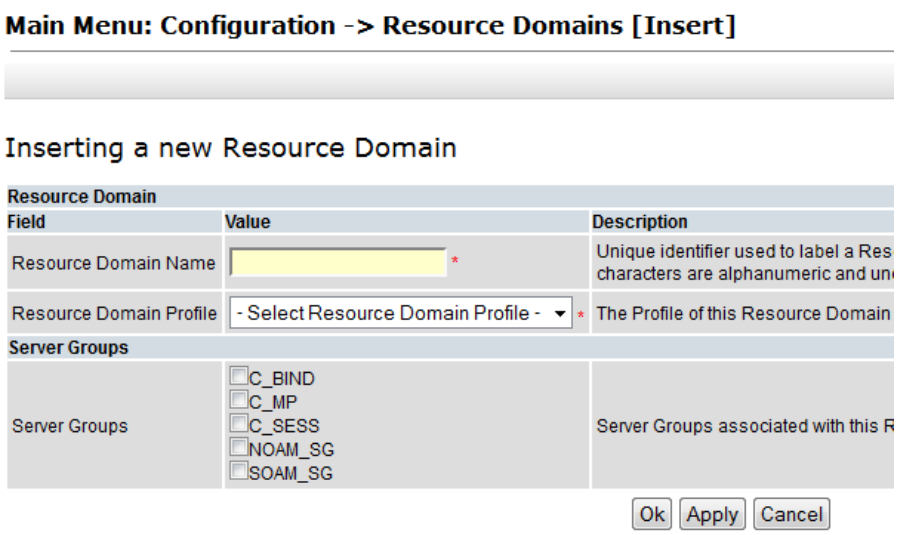
- Policy and Charging DRA
- Policy Session

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

- Policy Binding

4.2.1 Policy and Charging DRA Resource Domain Configuration

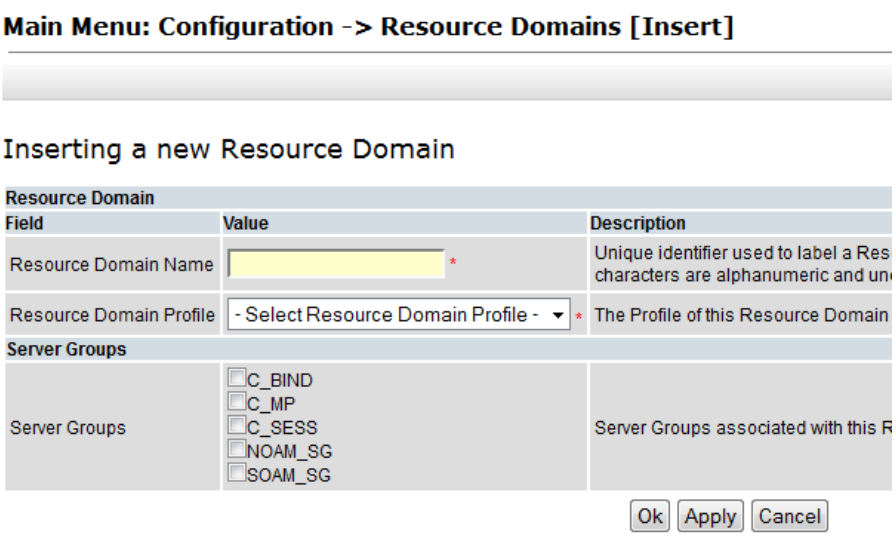
Procedure 7: Policy and Charging DRA Resource Domain configuration

S T E P #	This procedure configures the Policy and Charging 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 ☐	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 Resource Domain Screen	Navigate to **Main Menu -> Configuration -> Resource Domains** Screen.
3 ☐	**NOAM VIP:** Add Policy and Charging DRA Resource Domain	Click on **Insert** in the lower left corner. You will see a screen similar to:  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**. NOTE: **For Mated DSR sites, create one Policy and Charging DRA Resource Domain and add the**

		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	**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

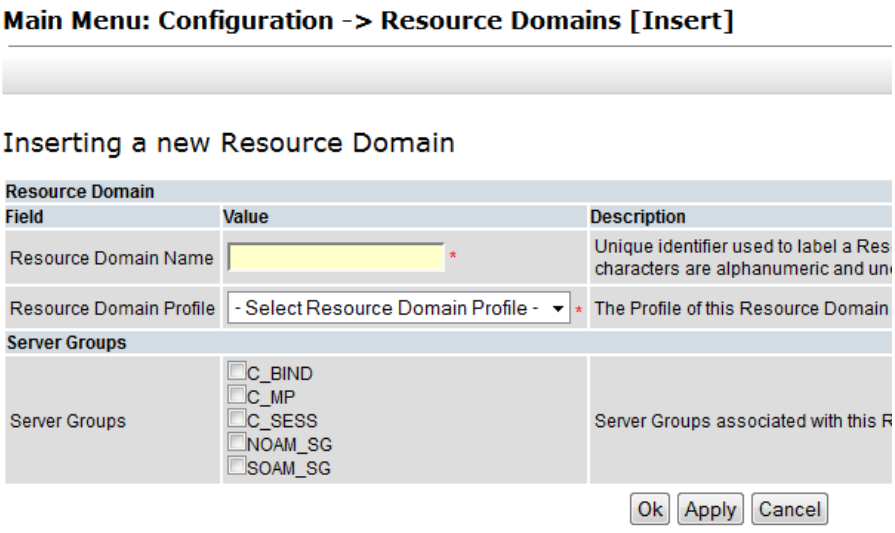
S T E P #	This procedure configures the Policy Session Resource Domain Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**. **ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED USING SECTION 8.1.**
1	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 Resource Domain Screen	Navigate to **Main Menu -> Configuration -> Resource Domains** Screen.
3	**NOAM VIP:** Add Session Resource Domain	Click on **Insert** in the lower left corner. You will see a screen similar to:  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	**NOAM VIP:** Add other	Repeat Step 4 for all other Policy Session Resource Domains that are to be added.

	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 #	This procedure configures the Policy Binding 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	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 Resource Domain Screen	Navigate to **Main Menu -> Configuration -> Resource Domains** Screen.
3	**NOAM VIP:** Add Policy and Charging DRA Resource Domain	Click on **Insert** in the lower left corner. You will see a screen similar to:  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**. 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.**
4	**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.

4.3 DIAMETER CONFIGURATION PROCEDURES

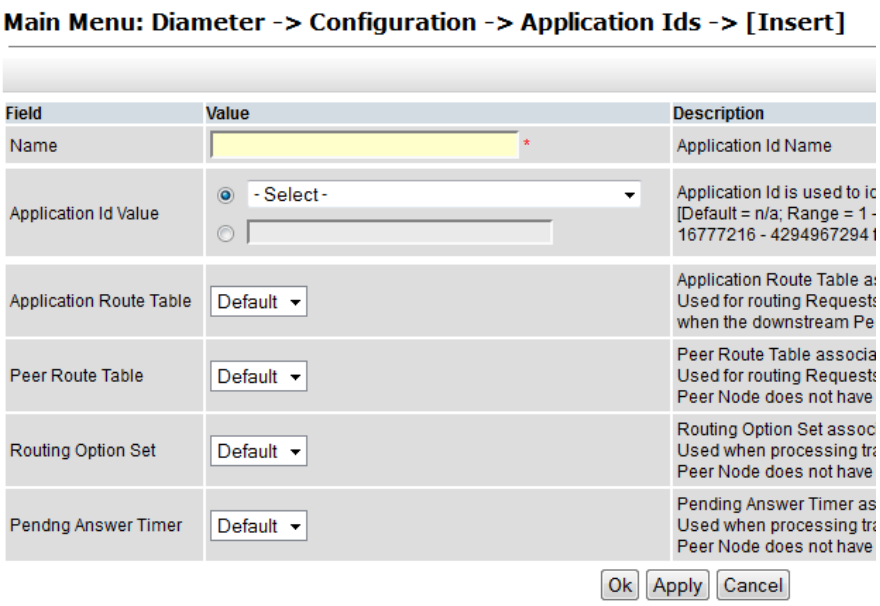
4.3.1 Diameter Configuration for Policy DRA

Detailed steps are given in the procedure below.

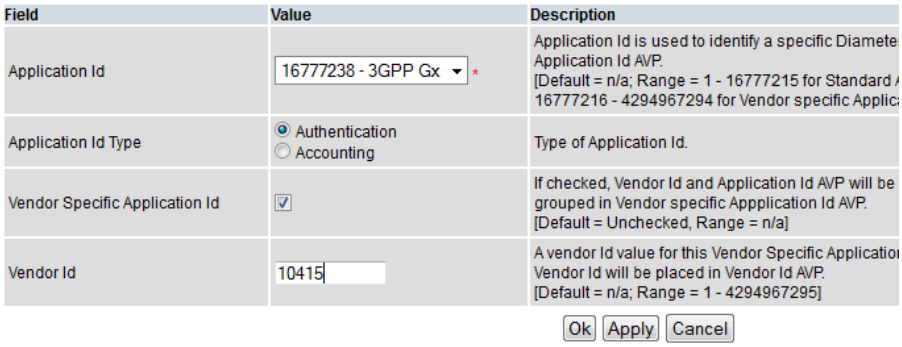
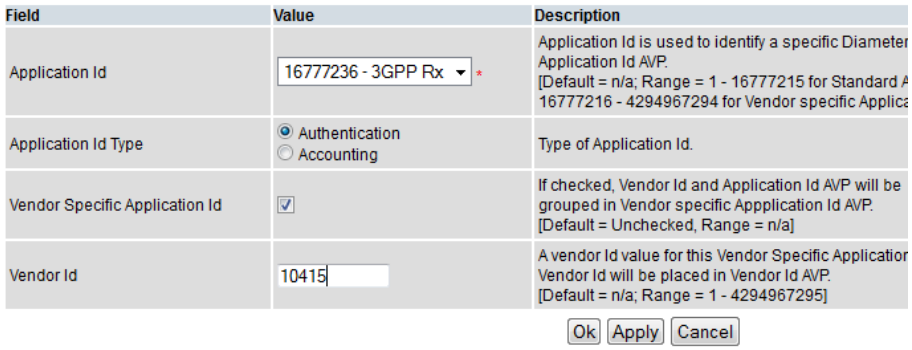
Procedure 10: Diameter configuration for Policy DRA

NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION

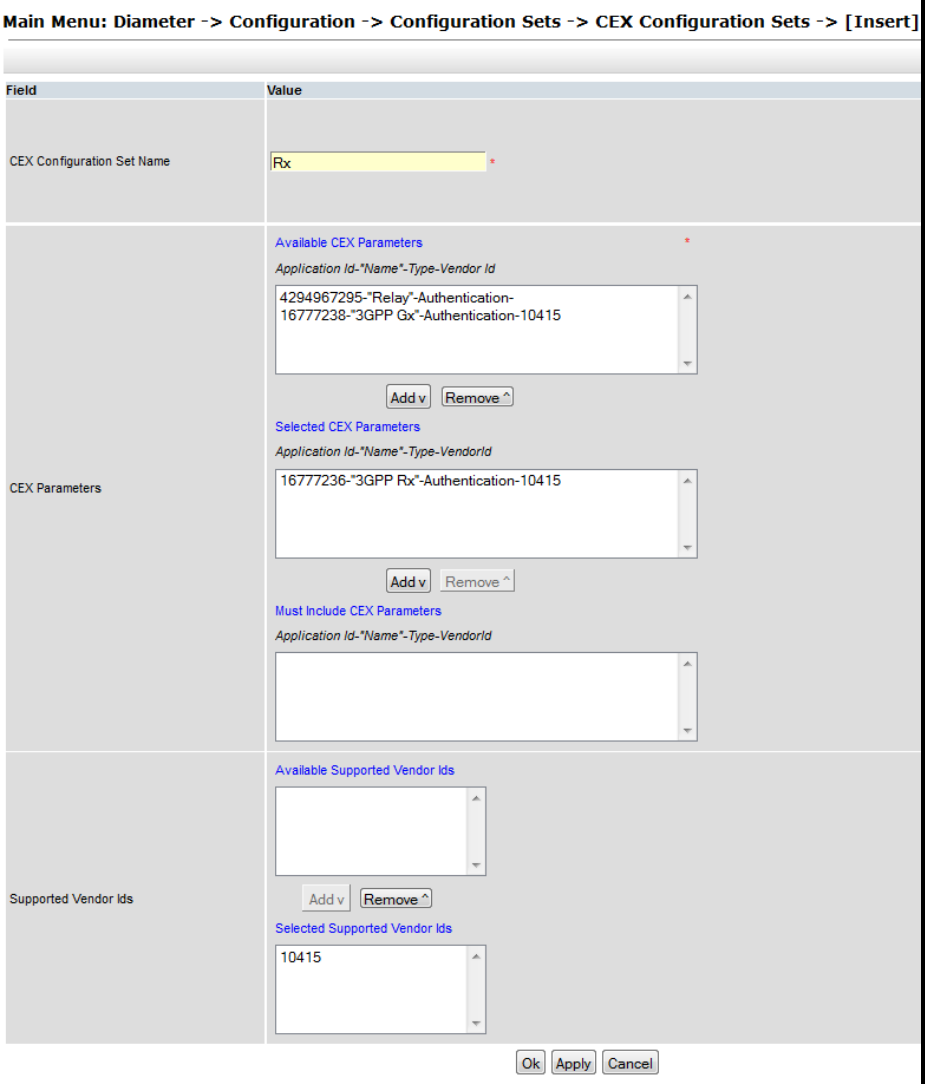
SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY

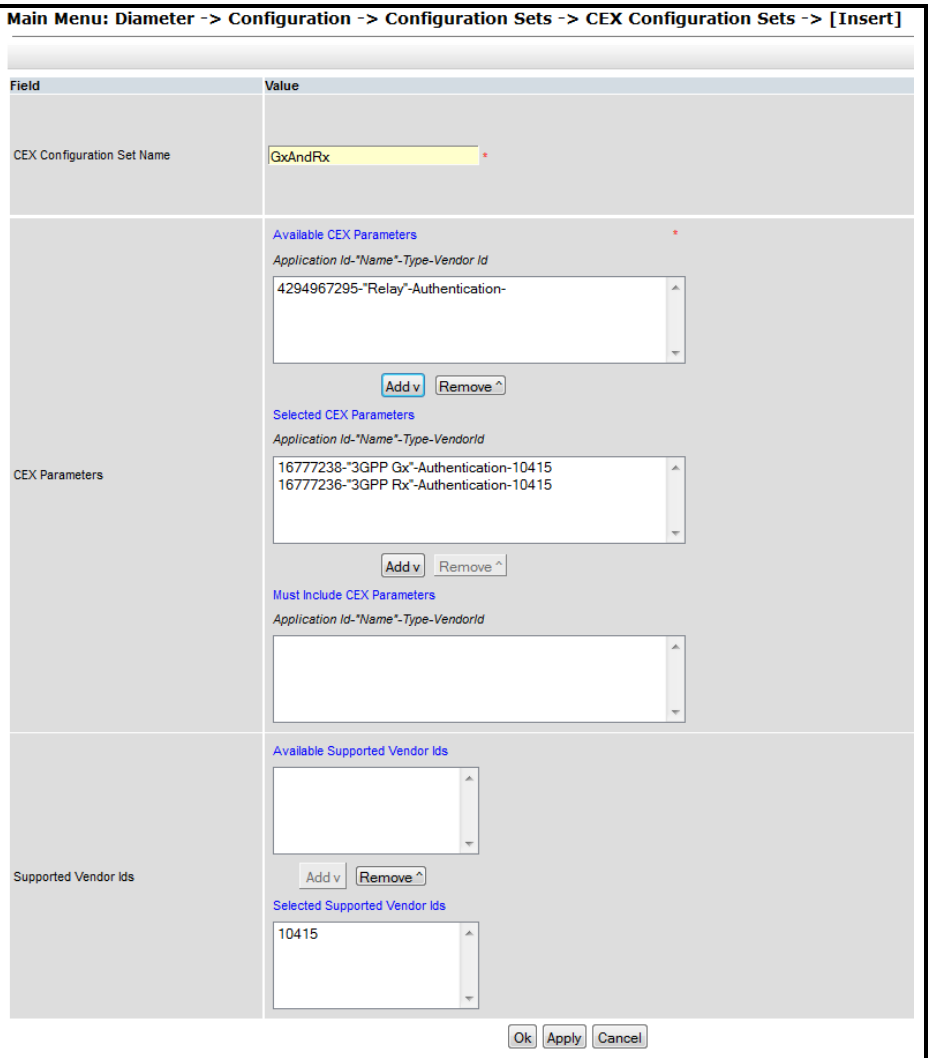
S T E P #	This procedure configures the Diameter stack. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.	
1 ☐	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**SOAM VIP:** Navigate to Application Id Configuration Screen	Navigate to **Main Menu -> Diameter -> Configuration -> Application Ids**
3 ☐	**SOAM VIP:** Add Application Id for Gx Interface	Click on **Insert** in the lower left corner. You will see a screen similar to:  1. Select Application Id for Gx Interface "16777238" 2. Click **Ok**.
4 ☐	**SOAM VIP:** Add Application Id for Rx Interface	Click on **Insert** in the lower left corner. You will see a screen similar to:

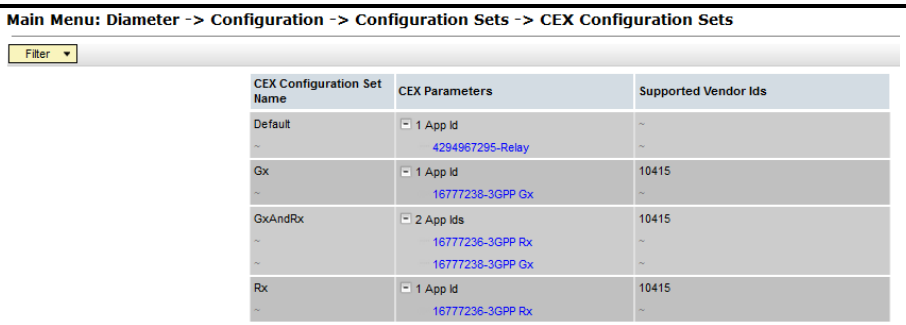
		Main Menu: Diameter -> Configuration -> Application Ids -> [Insert] Field / Value / Description Name — Application Id Name Application Id Value — - Select - — Application Id is used to ic [Default = n/a; Range = 1 - 16777216 - 4294967294 1 Application Route Table — Default — Application Route Table as Used for routing Requests when the downstream Pe Peer Route Table — Default — Peer Route Table associa Used for routing Requests Peer Node does not have Routing Option Set — Default — Routing Option Set assoc Used when processing tra Peer Node does not have Pendng Answer Timer — Default — Pending Answer Timer as Used when processing tra Peer Node does not have Ok Apply Cancel 1. Select Application Id for Rx Interface "16777236" 2. Click **Ok**.
5	**SOAM VIP:** Add Application Ids for any other required Interfaces for Policy DRA	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.
6	**SOAM VIP:** Verify that all Application Ids have been configured successfully.	Navigate to **Main Menu -> Diameter -> Configuration -> Application Ids** You should see a screen containing all the configured Application Ids. **Main Menu: Diameter -> Configuration -> Application Ids** Thu Aug 07 16:41 Filter 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	**SOAM VIP:** Navigate to CEX Parameters Screen	Navigate to **Main Menu -> Diameter -> Configuration -> CEX Parameters**
8	**SOAM VIP:** Add CEX Parameter for Gx Interface	Click on **Insert** in the lower left corner. You will see a screen similar to:

		Main Menu: Diameter -> Configuration -> CEX Parameters -> [Insert]  1. Select Application Id Gx Interface “16777238” 2. Check the Vendor Specific Application Id button 3. Enter the Vendor Id “10415” 4. Click **Ok**.
9	**SOAM VIP:** Add CEX Parameter for Rx Interface	Click on **Insert** in the lower left corner. You will see a screen similar to: **Main Menu: Diameter -> Configuration -> CEX Parameters -> [Insert]**  1. Select Application Id Rx Interface “16777236” 2. Check the Vendor Specific Application Id button 3. Enter the Vendor Id “10415” 4. Click **Ok**.
10	**SOAM VIP:** Add CEX Parameters for any other required Interfaces	Repeat Step 9 for all other configured Application Ids. For example, Gxx and S9 Interfaces.
11	**SOAM VIP:** Verify that all CEX Parameters have been configured successfully.	Navigate to **Main Menu -> Diameter -> Configuration -> CEX Parameters** You should see a screen containing all the configured CEX parameters.

		Main Menu: Diameter -> Configuration -> CEX Parameters Filter Application Id | Application Id Type | Vendor Id 16777236 - 3GPP Rx | Authentication | 10415 16777238 - 3GPP Gx | Authentication | 10415 4294967295 - Relay | Authentication | ---
12	**SOAM VIP:** Navigate to CEX Configuration Sets screen	Navigate to **Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets**
13	**SOAM VIP:** Configure the CEX Configuration set to be used for Connections with the PCEF 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]** Field | Value CEX Configuration Set Name: Gx * CEX Parameters: Available CEX Parameters * *Application Id-"Name"-Type-Vendor Id* 4294967295-"Relay"-Authentication- 16777236-"3GPP Rx"-Authentication-10415 Add v Remove ^ Selected CEX Parameters *Application Id-"Name"-Type-VendorId* 16777238-"3GPP Gx"-Authentication-10415 Add v Remove ^ Must Include CEX Parameters *Application Id-"Name"-Type-VendorId* Supported Vendor Ids: Available Supported Vendor Ids Add v Remove ^ Selected Supported Vendor Ids 10415 Ok Apply Cancel 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**.
14	**SOAM VIP:** Configure the CEX Configuration	Click on **Insert** in the lower left corner.

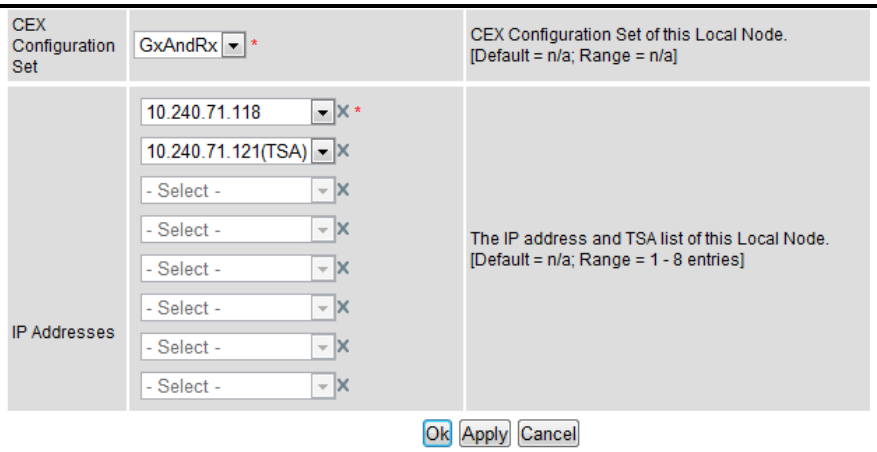
	Set to be used for Connections with the AF nodes.	You will see a screen similar to:  1. Enter the CEX Configuration Set Name “Rx” 2. Select the 3GPP Rx Application Id “16777236” from Available Application Ids 3. Click **Add** just below the list 4. Select the Vendor Id “10415” from Available Supported 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:

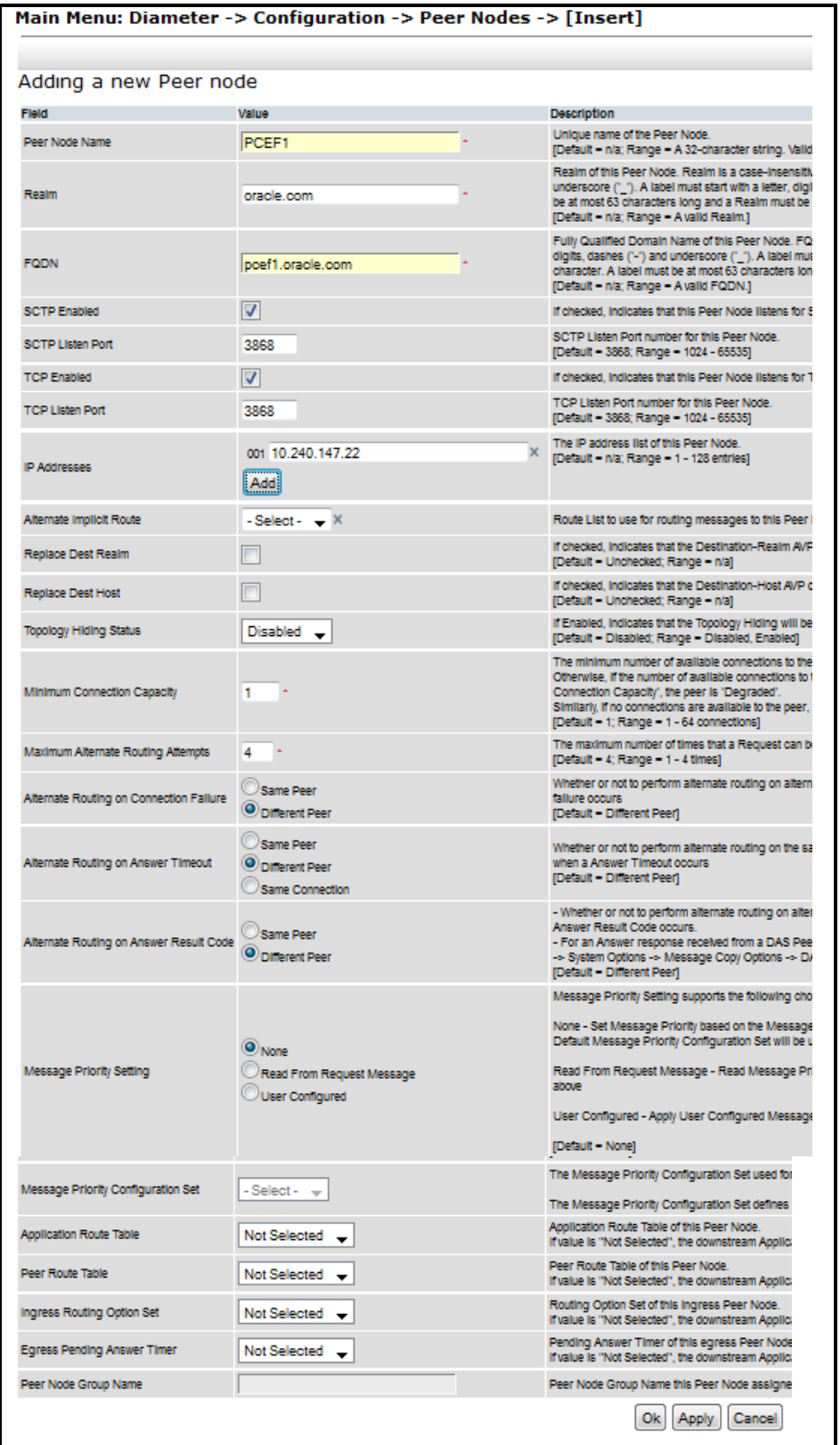
		 1. Enter the CEX Configuration Set Name "GxAndRx" 2. Select the 3GPP Gx Application Id "16777238" and 3GPP Rx Application Id "16777236" from Available Application Ids 3. Click **Add** just below the list 4. Select the Vendor Id "10415" from Available Supported Vendor Ids 5. Click **Add** just below that list 6. Click **Ok**.
16 ☐	**SOAM VIP:** Configure the CEX Configuration Set for any other combination of Application Ids.	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.
17 ☐	**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.



18	**SOAM VIP:** Navigate to Local Nodes screen	Navigate to **Main Menu -> Diameter -> Configuration -> Local Nodes**
19	**SOAM VIP:** Configure the first Local Node (P-DRA)	Click on **Insert** in the lower left corner. You will see a screen similar to: **Main Menu: Diameter -> Configuration -> Local Nodes -> [Insert]** Thu Feb Adding a new node

Field	Value	Description
Local Node Name	PDRA *	Unique name of the Local Node. [Default = n/a; Range = A 32-character string. Valid cha alphanumeric and underscore. Must contain at least o must not start with a digit.]
Realm	tekelec.com *	Realm of this Local Node. Realm is a case-insensitiv consisting of a list of labels separated by dots, where contain letters, digits, dashes ('-') and underscore ('_') start with a letter, digit or underscore and must end wi digit. Underscores may be used only as the first chara must be at most 63 characters long and a Realm mus 255 characters long. [Default = n/a; Range = A valid Realm.]
FQDN	pdra.tekelec.com *	Fully Qualified Domain Name of this Local Node. FQD insensitive string consisting of a list of labels separat where a label may contain letters, digits, dashes ('-') a underscore ('_'). A label must start with a letter, digit or and must end with a letter or digit. Underscores may b as the first character. A label must be at most 63 chara and a FQDN must be at most 255 characters long. [Default = n/a; Range = A valid FQDN.]
SCTP Enabled	☑	If checked, indicates that this Local Node listens for S connections.
SCTP Listen Port	3868	SCTP Listen Port number of this Local Node. [Default = 3868; Range = 1024 - 65535]
TCP Enabled	☑	If checked, indicates that this Local Node listens for T 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]

		 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:** 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.
20 ☐	**SOAM VIP:** Configure other Local Nodes, if required.	Repeat Step 19 and configure more Local Nodes if required.
21 ☐	**SOAM VIP:** Navigate to Peer Nodes screen	Navigate to **Main Menu -> Diameter -> Configuration -> Peer Nodes**
22 ☐	**SOAM VIP:** Configure the first PCEF node	Click on **Insert** in the lower left corner. You will see a screen similar to:



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

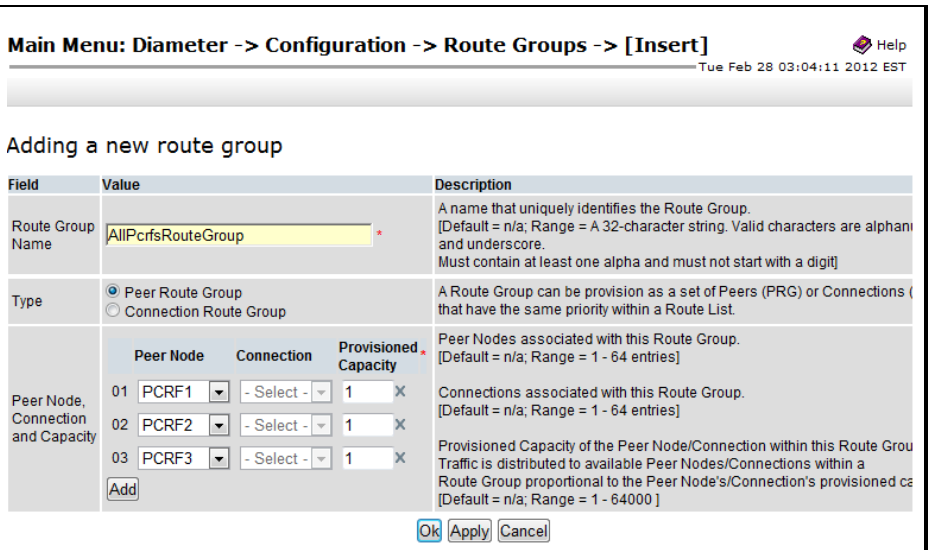
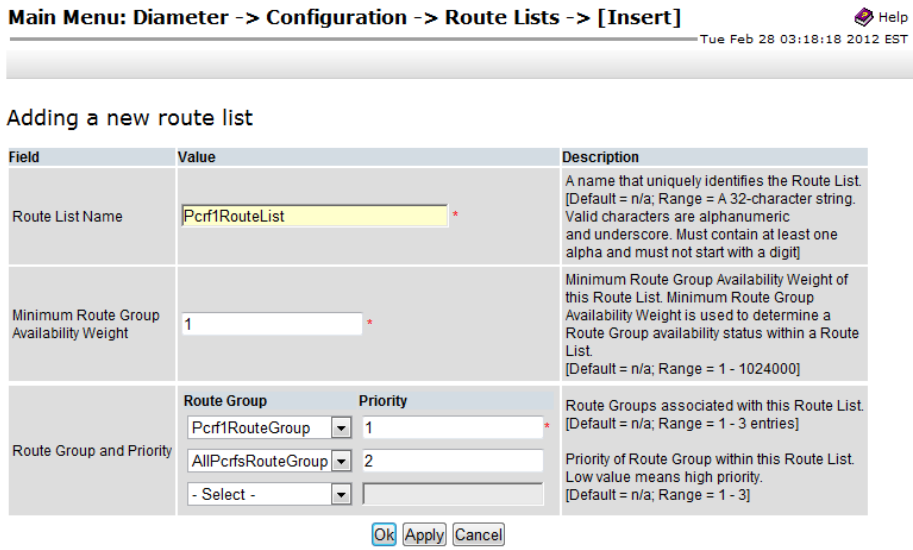
Main Menu: Diameter -> Configuration -> Connections -> [Insert]

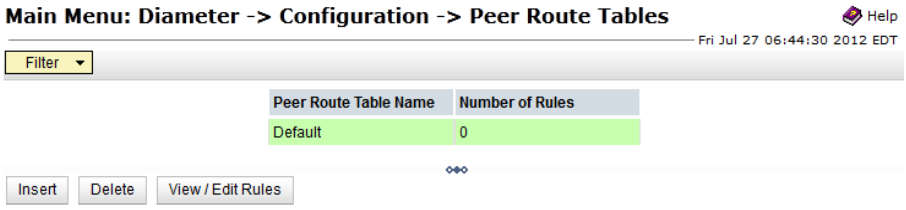
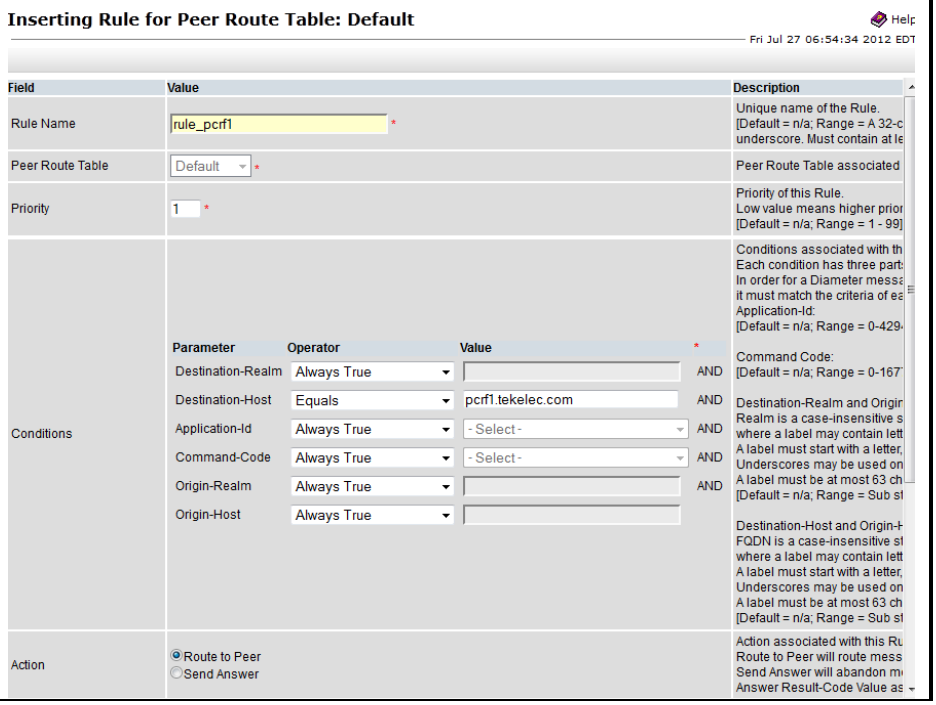
Adding a new connection

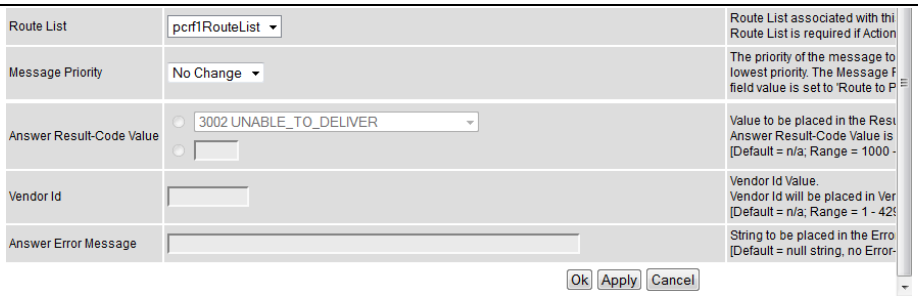
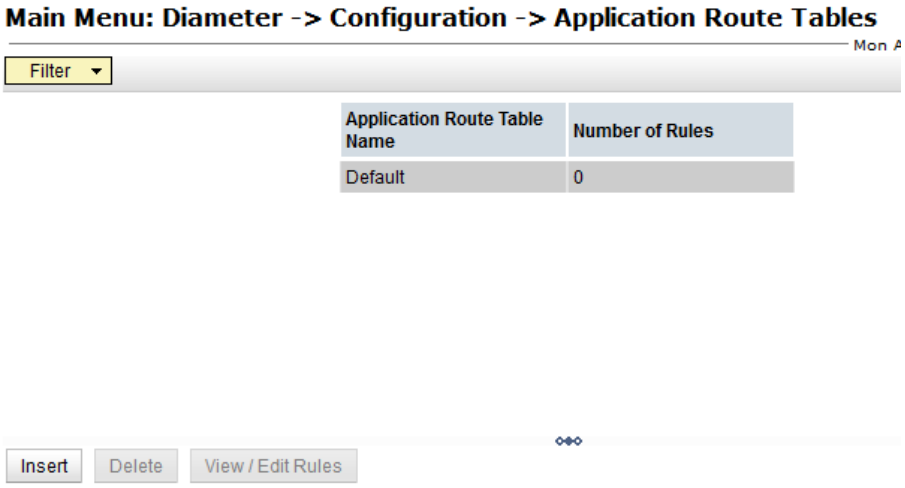
Field	Value	Description
Connection Name		A name that uniquely identifies the Connection. [Default = n/a; Range = A 32-character string. Valid characters are
Transport Protocol	(•) SCTP ( ) TCP	The transport protocol used by this Connection. The protocol should be supported by both Local Node and Peer Nod
Local Node	PDRA	The Local Node of this Connection.
Connection Mode	Initiator & Responder	Initiator Only indicates that Local Node will only initiate the connecti Responder Only indicates that Local Node will only respond to the c Initiator & Responder indicates that Local Node will initiate connect [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	10.240.10.73 (TSA1-p)	The IP Address to be used as the Primary Local Node address for t
Secondary Local IP Address	- Select -	The IP Address to be used as the Secondary Local Node address fo This address is only used for SCTP multi-homing. This address mu
Peer Node	AF1	The Peer Node of this Connection.
Peer Node Identification	(•) IP Address ( ) Transport FQDN ( ) 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 Transport FQDN Use the DNS resolved Transport FQDN address configured for thi Peer Node FQDN Use the DNS resolved FQDN address configured for the Peer Nod
Primary Peer IP Address	10.240.71.85 X	The IP Address to be used as the Primary Peer Node address for th
Secondary Peer IP Address	- Select -	The IP Address to be used as the Secondary Peer Node address fo This address is only used for SCTP multi-homing. This address mu
Transport FQDN		Fully Qualified Domain Name for this connection. FQDN is a case- underscore and must end with a letter or digit. Underscores may be [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 ingr [Default = Default; Range = A 32-character string. Valid characters
Transport Congestion Abatement Timeout	5	Defines the time period (in seconds) spent by the connection in abat [Default = 5; Range = 3 - 60 secs]
Remote Busy Usage	Disabled	Defines which Request messages can be forwarded on this connec 'Disabled' - The Connection is not considered to be BUSY after rec 'Enabled' - The Connection is considered to be BUSY after receivin [Default = Disabled; Range = Disabled, Enabled]
Remote Busy Abatement Timeout	5	Defines the time period (in seconds) that a Connection will be consi [Default = 5; Range = 3 - 60 secs]
Message Priority Setting	(•) None ( ) Read From Request Message ( ) User Configured	Message Priority Setting supports the following choices None - Set Message Priority based on Peer Node Message Priorit Read From Request Message - Read Message Priority from Ingre User Configured - Apply User Configured Message Priority Config [Default = None]
Message Priority Configuration Set	- Select -	The Message Priority Configuration Set used for this connection. The Message Priority Configutaion Set defines the priority of the R
Egress Message Throttling Configuration Set	- Select -	The Egress Message Throttling Configuration Set used for this co
Suppress Connection Unavailable Alarm	☐	If checked, connection unavailable alarm will not be raised. [Default = unchecked; Range = n/a].
Suppress Connection Attempts	☐	If checked, the connection attempts to standby Peer Node will be sup [Default = unchecked; Range = n/a].
Test Mode	☐	If checked, indicates that connection is in test mode. [Default = unchecked; Range = n/a].

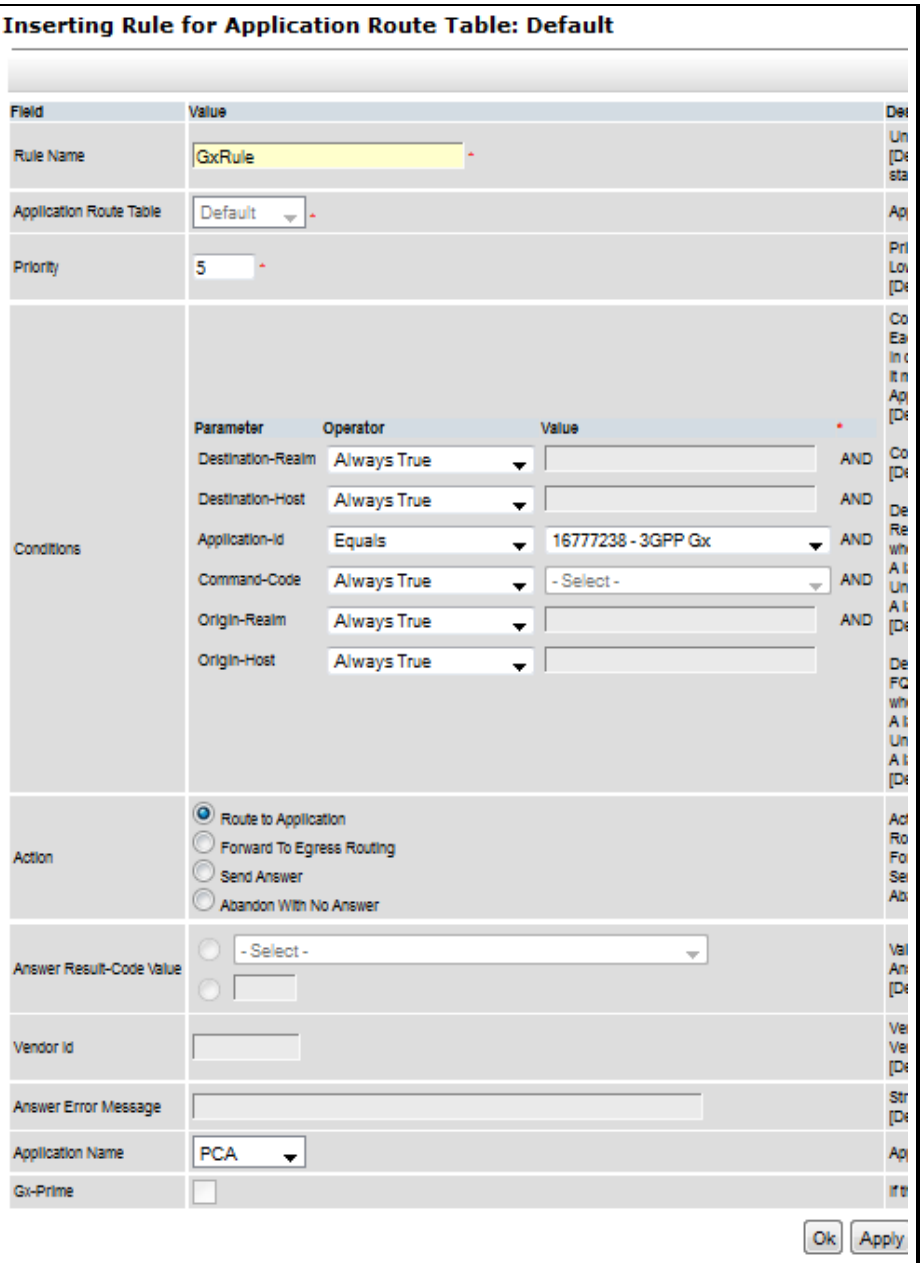
1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values).

		2. Click **Ok**. **NOTE:** Make sure the IPFE configuration matches the protocol which is selected in this step.
26	**SOAM VIP:** Configure all other connection with Peer nodes	Repeat Step 25 to configure all other required DIAMETER connections.
27	**SOAM VIP:** Configure Route Groups	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. 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. Navigate to **Main Menu -> Diameter -> Configuration -> Route Groups**
28	**SOAM VIP:** Insert a new Route Group and add the first PCRF to it.	Click on **Insert** in the lower left corner. You will see a screen similar to: **Main Menu: Diameter -> Configuration -> Route Groups -> [Insert]** Adding a new route group Field / Value Route Group Name: PcrfRouteGroup * Type: Peer Route Group / Connection Route Group Peer Node, Connection and Capacity: Peer Node / Connection / Provisioned Capacity * 01 pcrf — 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 **Ok**.
29	**SOAM VIP:** Configure more Route Groups corresponding to each PCRF.	Repeat Step 28 for every PCRF that is connected to this DSR.
30	**SOAM VIP:** Configure one Route Group	Click on **Insert** in the lower left corner. You will see a screen similar to:

	containing all PCRF nodes	 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:  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.

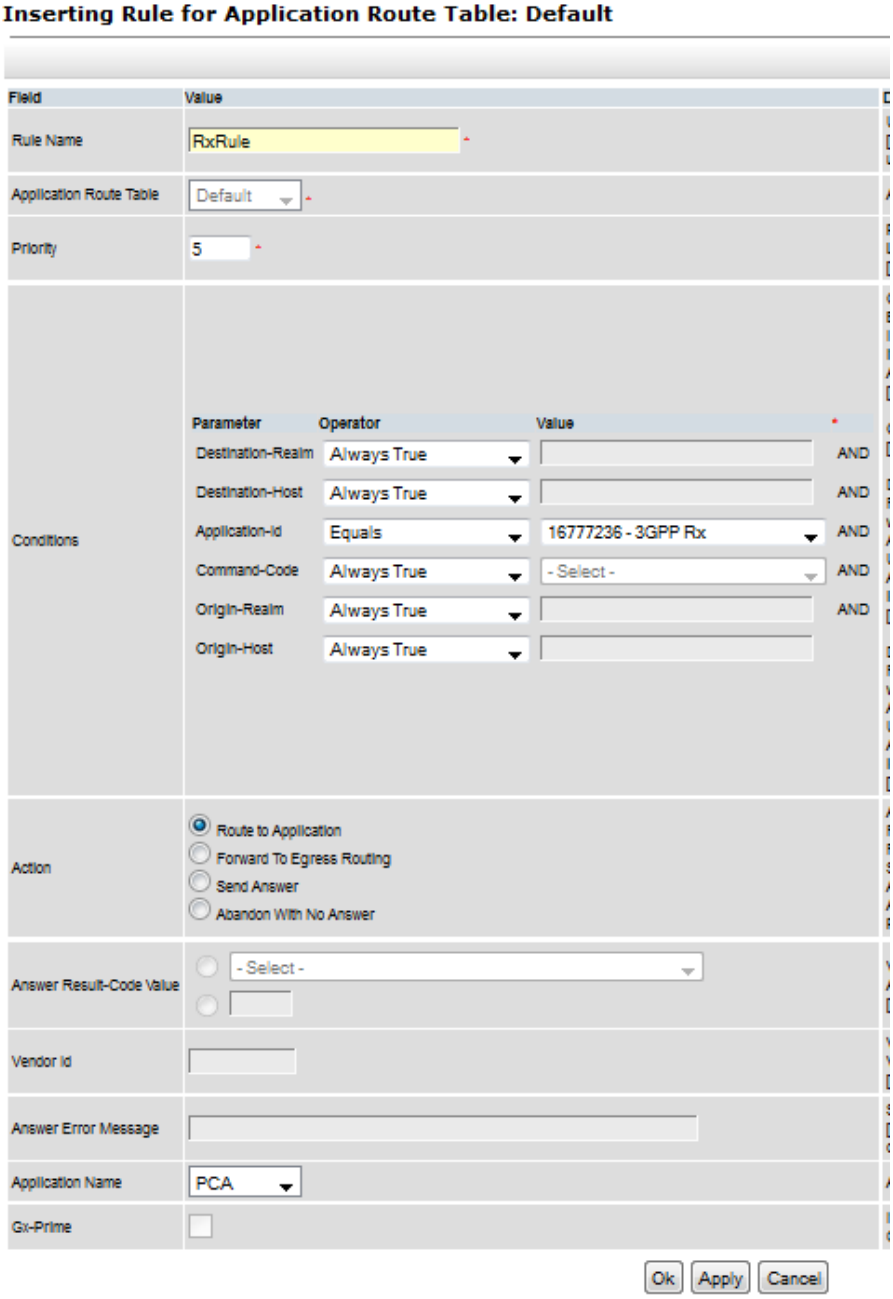
		4. Click **Ok**.
33	**SOAM VIP:** Configure all other Route Lists	Repeat step 32 for all other PCRFs connected to this DSR.
34	**SOAM VIP:** Configure the Peer Routing Rules.	Finally, configure the PRT such that DSR forwards messages based on the PCRF preference. Navigate to **Main Menu -> Diameter ->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

		 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	Navigate to **Main Menu -> Diameter -> Configuration -> Application Routing Rules** You will see a screen similar to:  1. Select the Default Application Route Table Name to which rules are to be added. 2. Click on View/Edit Rules button.
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:



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:

		 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 Interface s	Repeat Step 40 for any other Application Id that needs to be routed to the PCA Application by Diameter Routing Layer.

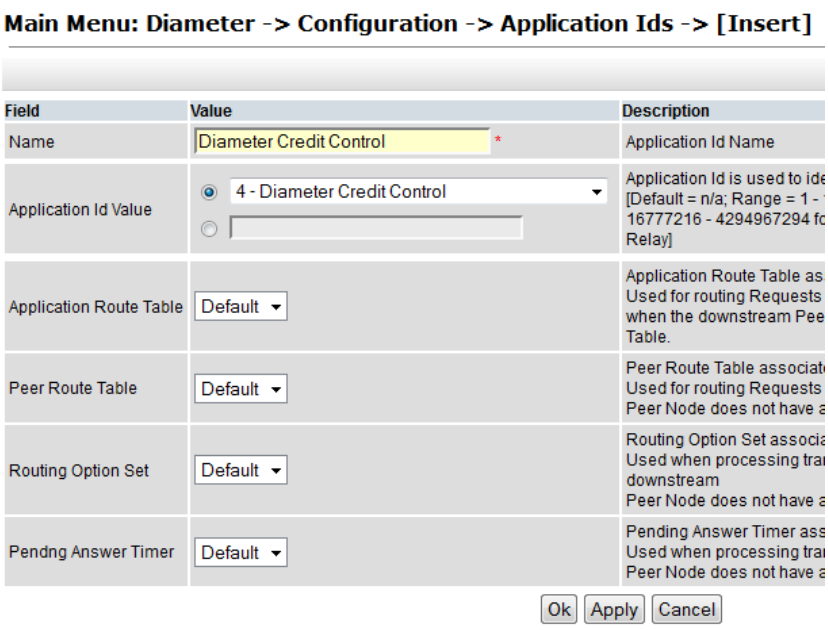
4.3.2 Diameter Configuration for Online Charging DRA

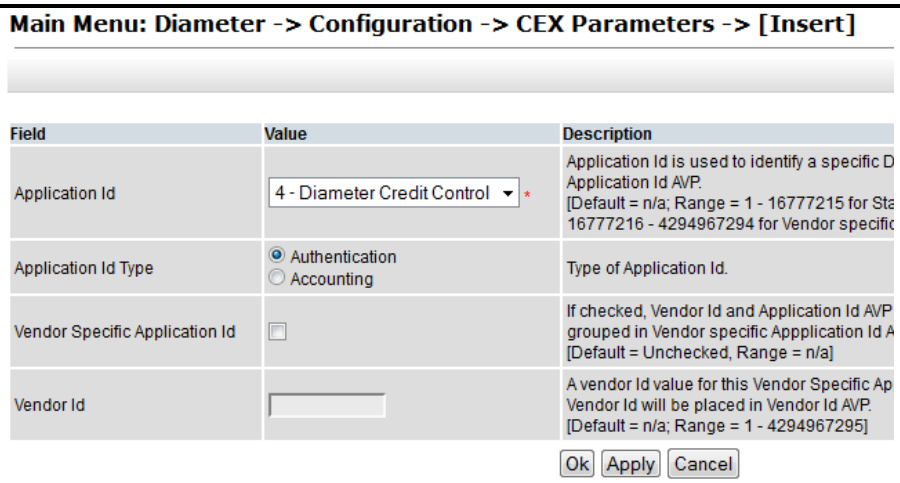
Detailed steps are given in the procedure below.

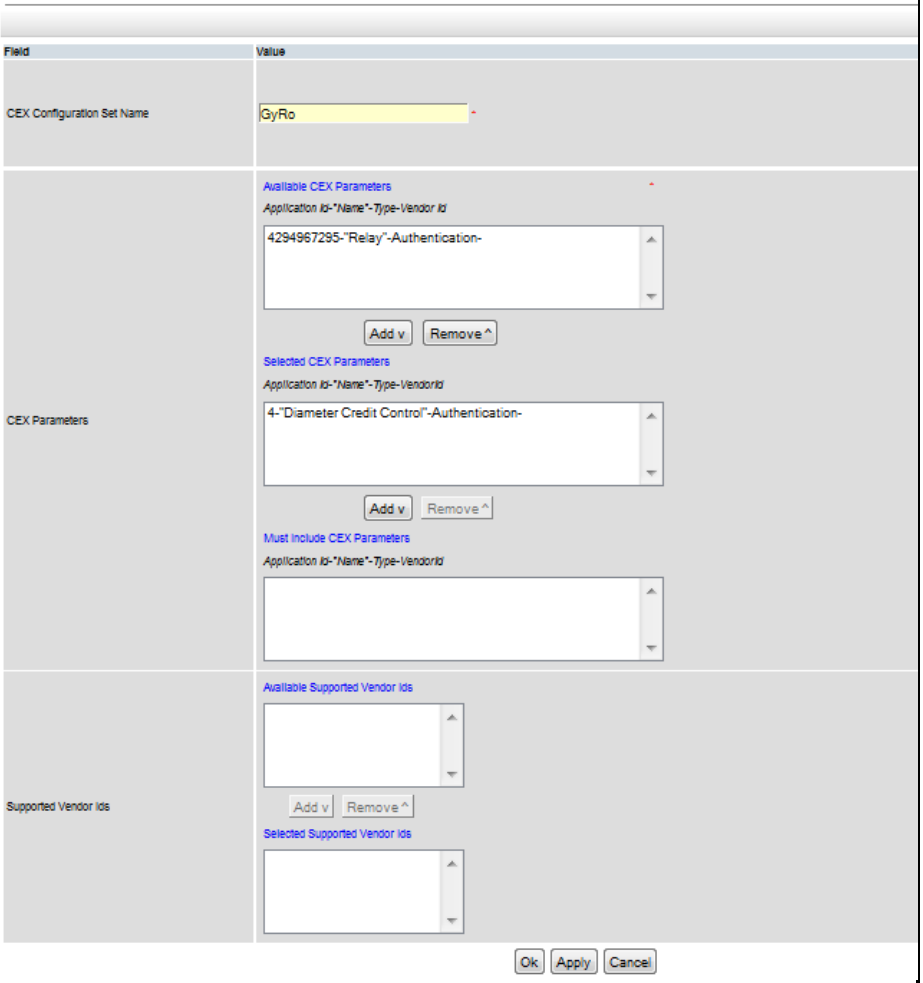
Procedure 11: Diameter configuration for Online Charging DRA

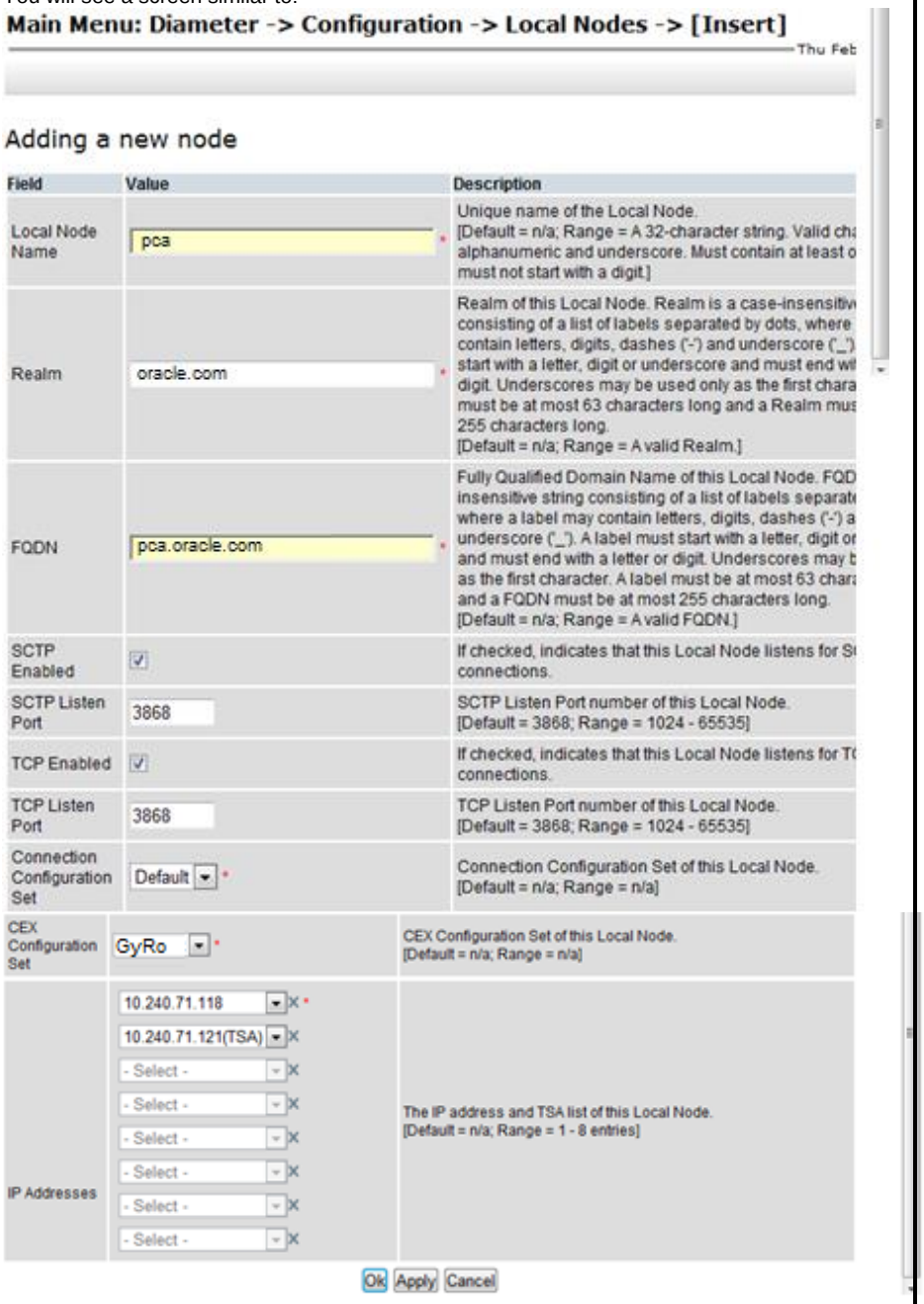
NOTE: EXECUTE THIS PROCEDURE FOR ONLINE CHARGING DRA FUNCTION

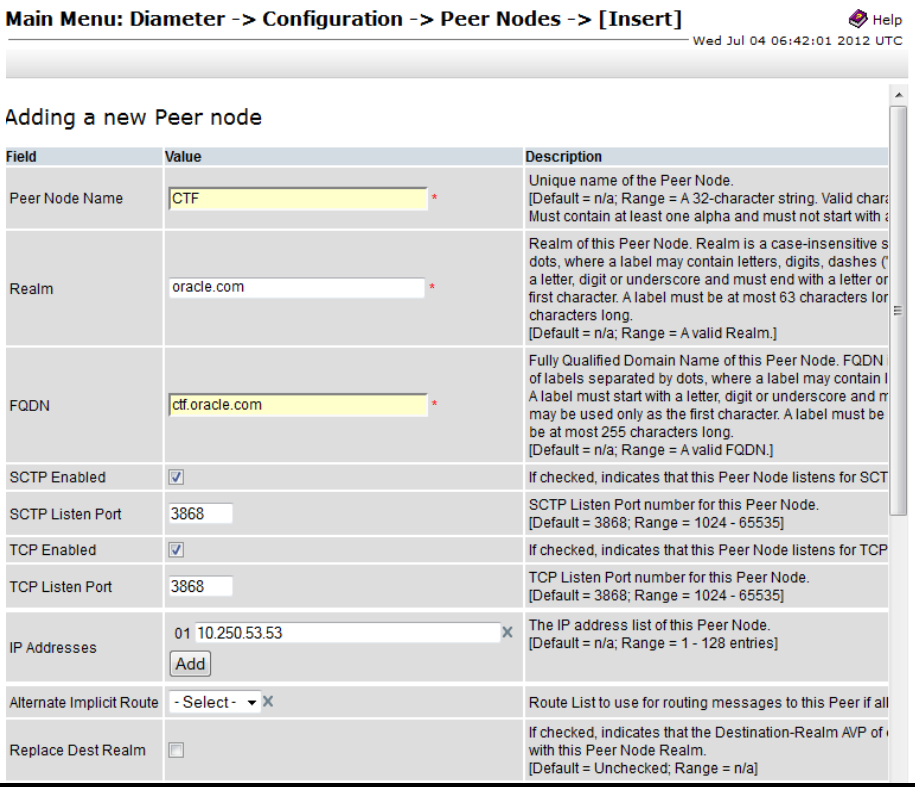
SKIP THIS PROCEDURE IF POLICY DRA FUNCTION ONLY

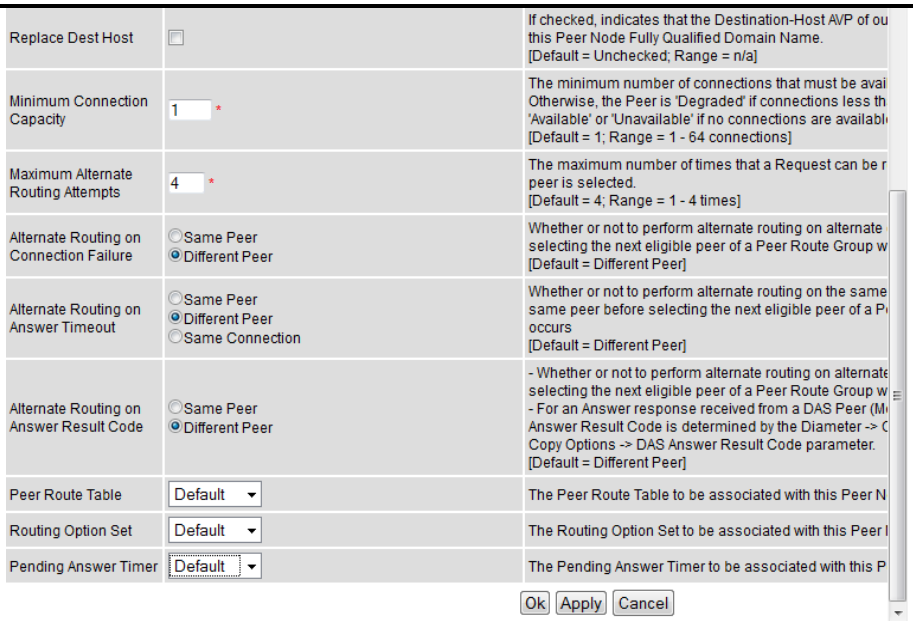
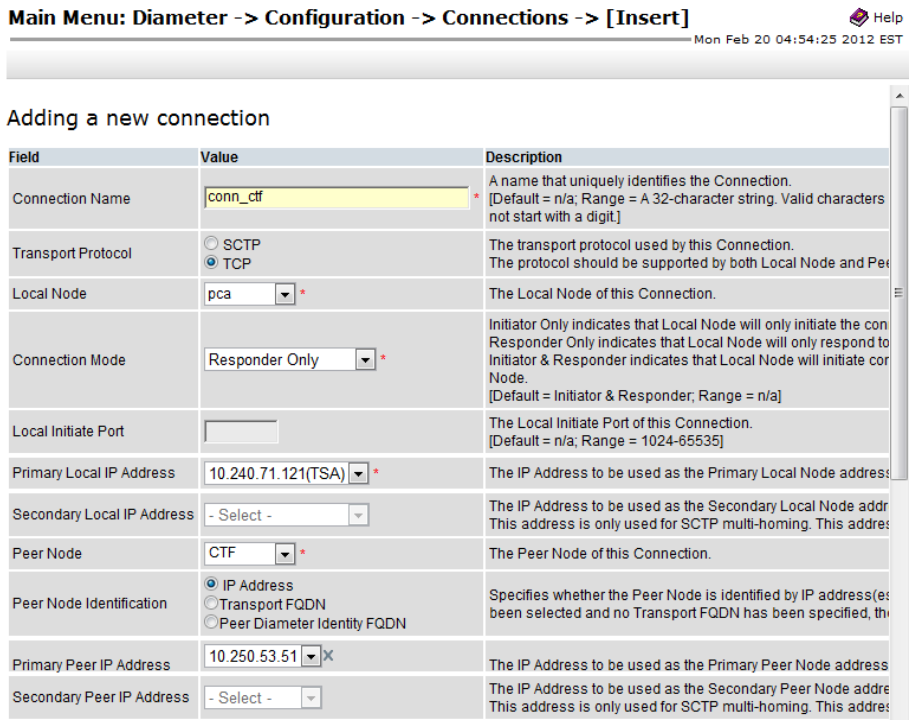
S T E P #	This procedure configures the Diameter stack. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.	
1	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2	**SOAM VIP:** Navigate to Application Id Configuration Screen	Navigate to **Main Menu -> Diameter -> Configuration -> Application Ids**
3	**SOAM VIP:** Add Application Id for GyRo Interface	Click on **Insert** in the lower left corner. You will see a screen similar to:  1. Select Application Id for Diameter Credit Control "4". 2. Click **Ok**.
4	**SOAM VIP:** Navigate to CEX Parameters Screen	Navigate to **Main Menu -> Diameter -> Configuration -> CEX Parameters**
5	**SOAM VIP:** Add CEX Parameter for GyRo Interface	Click on **Insert** in the lower left corner. You will see a screen similar to:

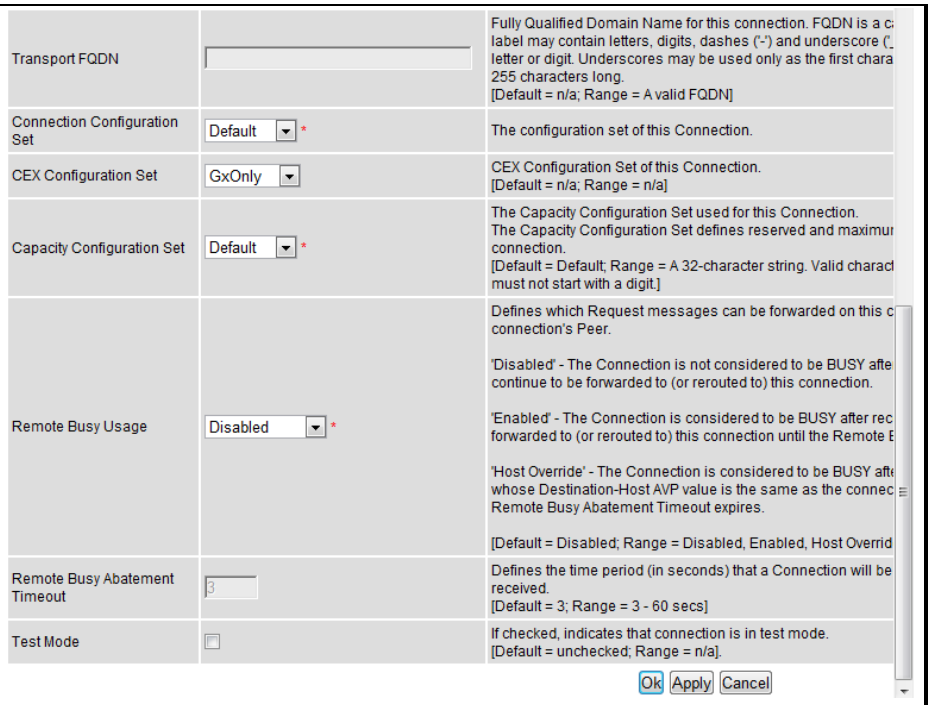
		 1. Select Application Id "4 - Diameter Credit Control". 2. Click **Ok**.
6	**SOAM VIP:** Navigate to CEX Configuration Sets screen	Navigate to **Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets**
7	**SOAM VIP:** Configure the CEX Configuration set to be used for Connections with the CTF and OCS nodes.	Click on **Insert** in the lower left corner. You will see a screen similar to:

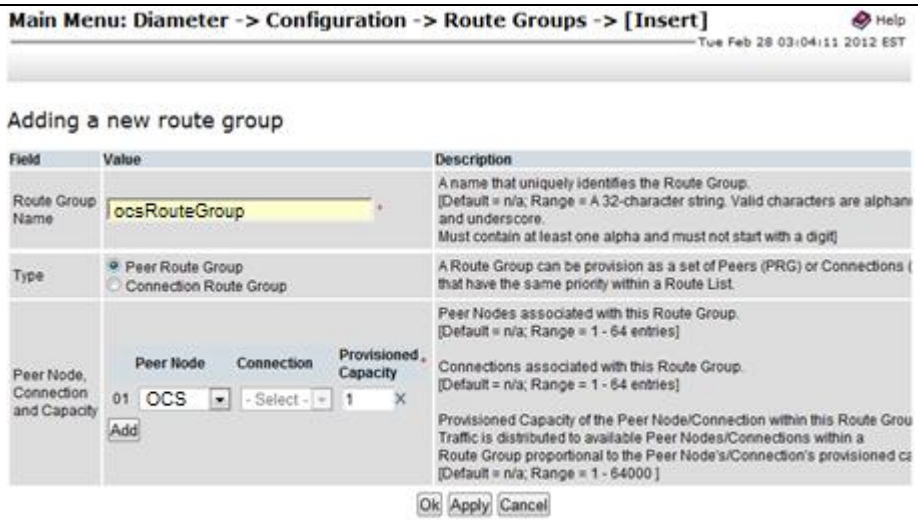
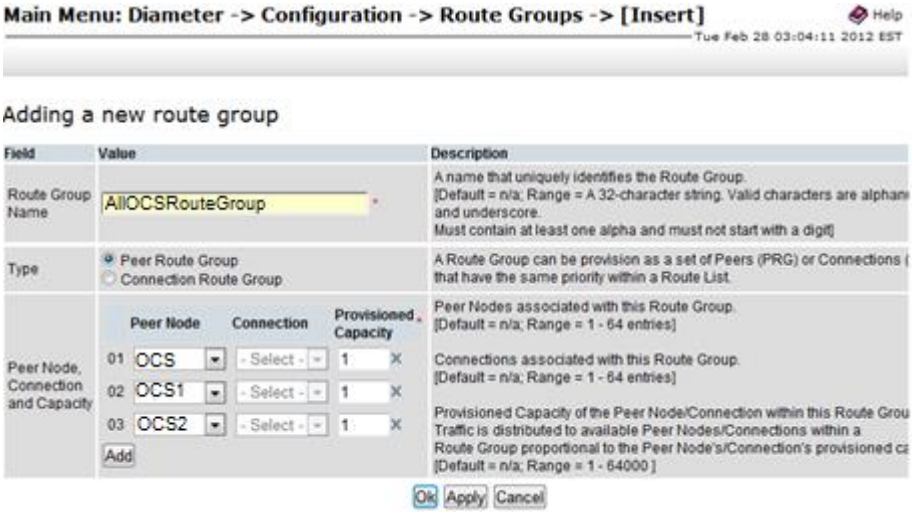
		Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]  1. Enter the CEX Configuration Set Name "GyRo". 2. Select the Diameter Credit Control Application Id from Available CEX Parameters box 3. Click **Add** just below the list. 4. Click **Ok**.
8	**SOAM VIP:** 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 — 1 App Id — 4294967295-Relay GyRo — 1 App Id — 4-Diameter Credit Control

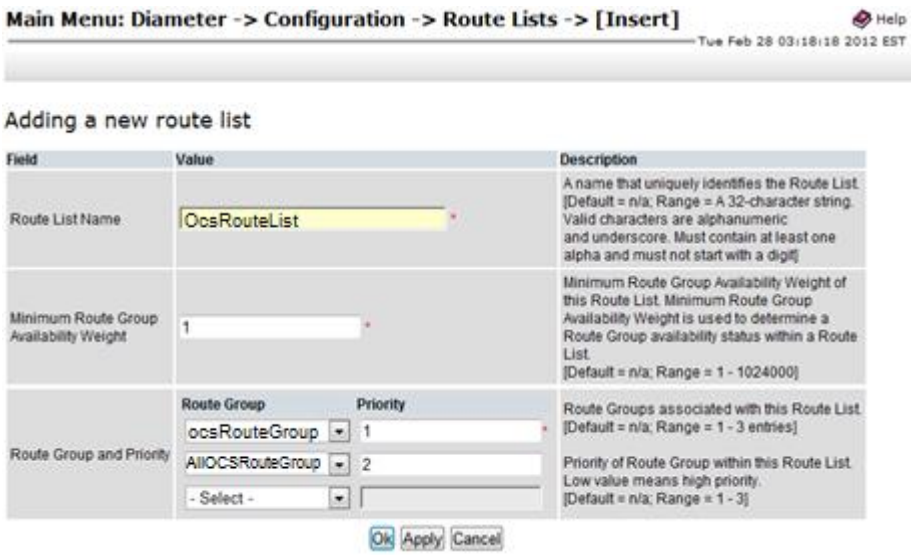
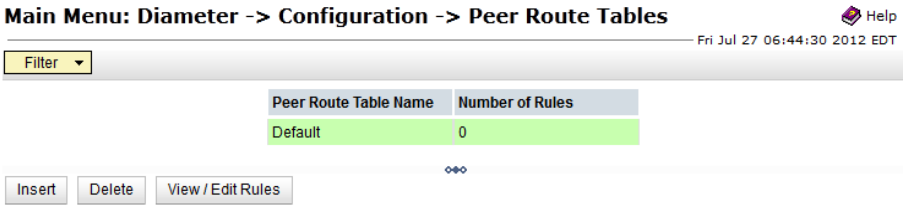
10	**SOAM VIP:** Navigate to Local Nodes screen	Navigate to **Main Menu -> Diameter -> Configuration -> Local Nodes**
11	**SOAM VIP:** Configure the first Local Node (OC-DRA)	Click on **Insert** in the lower left corner. You will see a screen similar to:  1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). 2. Click **Ok**. **NOTE:** 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

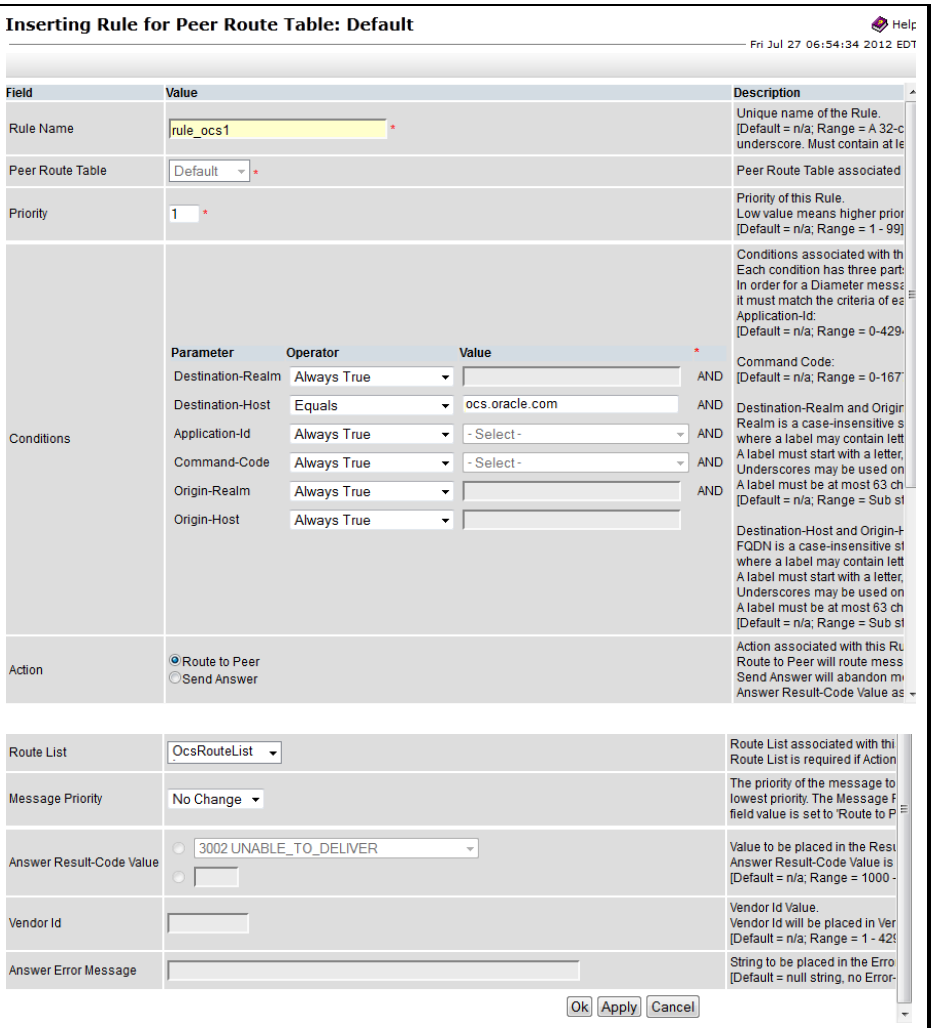
		Customer Service for further assistance.
12	**SOAM VIP:** Configure other Local Nodes, if required.	Repeat Step 11 and configure more Local Nodes if required.
13	**SOAM VIP:** Navigate to Peer Nodes screen	Navigate to **Main Menu -> Diameter -> Configuration -> Peer Nodes**
14	**SOAM VIP:** Configure the first CTF node	Click on **Insert** in the lower left corner. You will see a screen similar to: 

		 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: 

		 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:** Make sure the IPFE configuration matches the Transport Protocol which is selected in this step.
18 ☐	**SOAM VIP:** Configure all other connection with Peer nodes	Repeat Step 17 to configure all other required connections.
19 ☐	**SOAM VIP:** Configure Route Groups	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. 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. Navigate to **Main Menu -> Diameter -> Configuration -> Route Groups**
20 ☐	**SOAM VIP:** Insert a new Route Group and add the first OCS to it.	Click on **Insert** in the lower left corner. You will see a screen similar to:

		 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:  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.

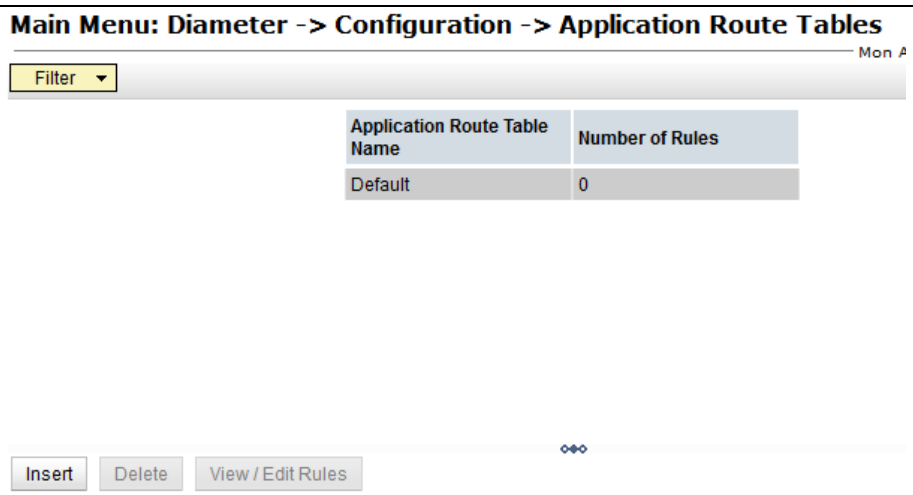
		The Route Group with a single OCS will have a higher priority whereas the Route Group with all OCSs will have a lower priority. Navigate to **Main Menu -> Diameter -> Configuration -> Route Lists**
24	**SOAM VIP:** Configure the first Route List	Click on **Insert** in the lower left corner. You will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

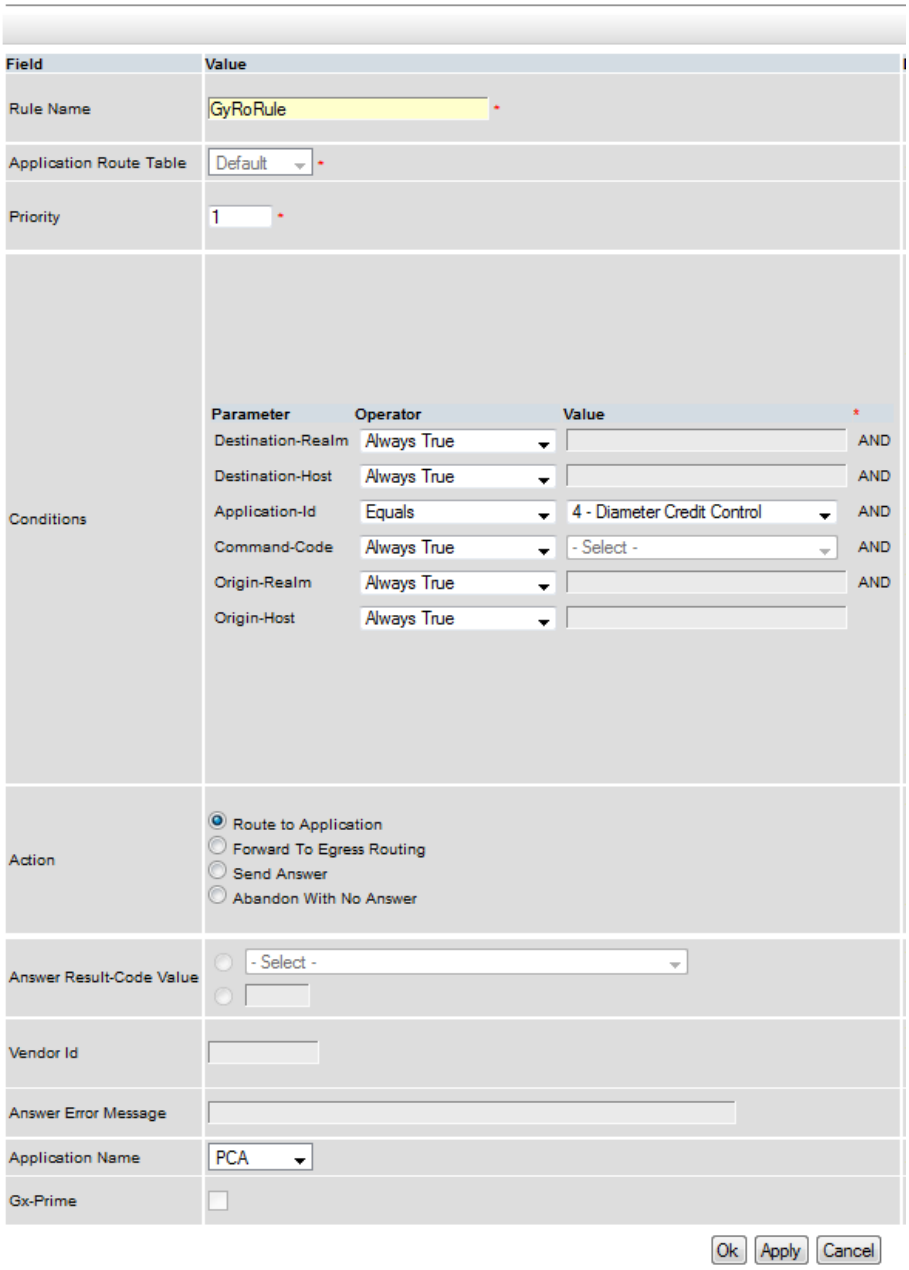


1. Enter the Rule name and priority values.
2. Select Destination host "Equals" the configured FQDN of OCS.
3. Select "Always True" for other conditions.
4. Select the Route List "OcsRouteList".
5. Click Ok.

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:

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

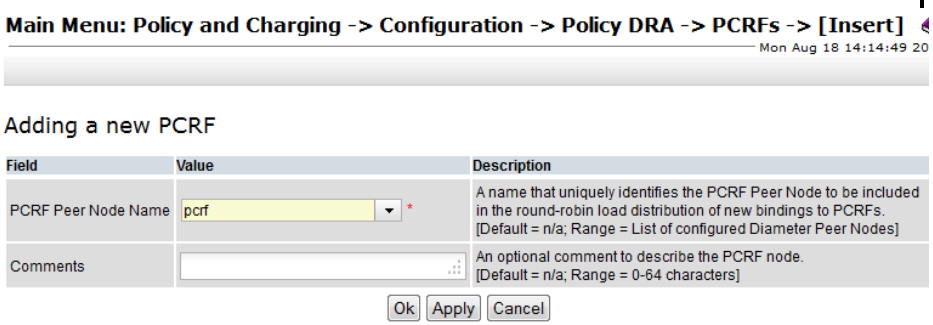
4.4 PCA FUNCTION CONFIGURATION PROCEDURES

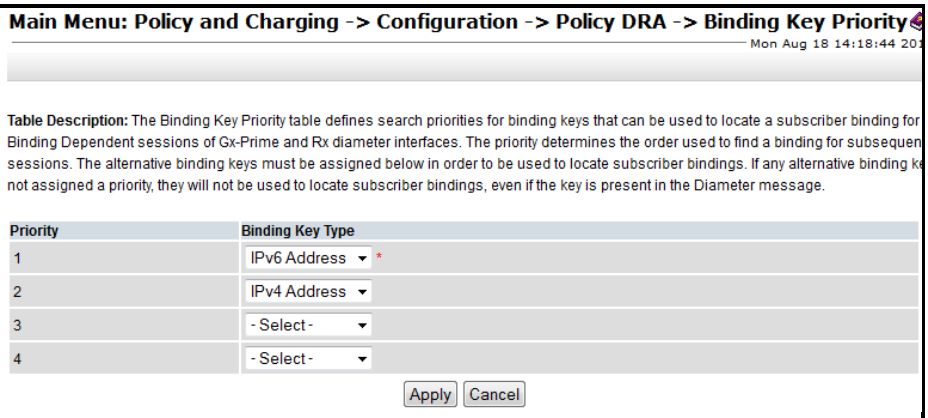
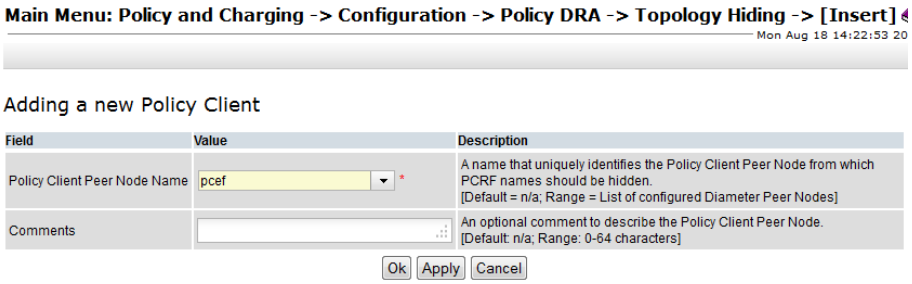
This section provides the detailed procedure steps of the PCA configuration execution. These procedures are executed inside a maintenance window.

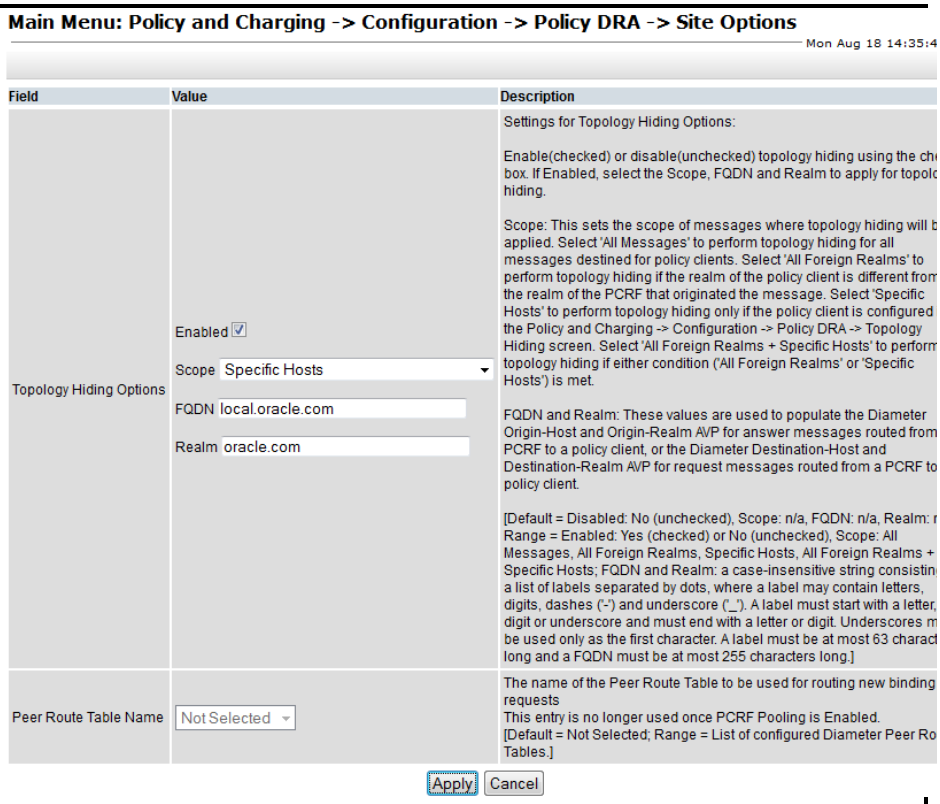
4.4.1 Policy DRA Configuration

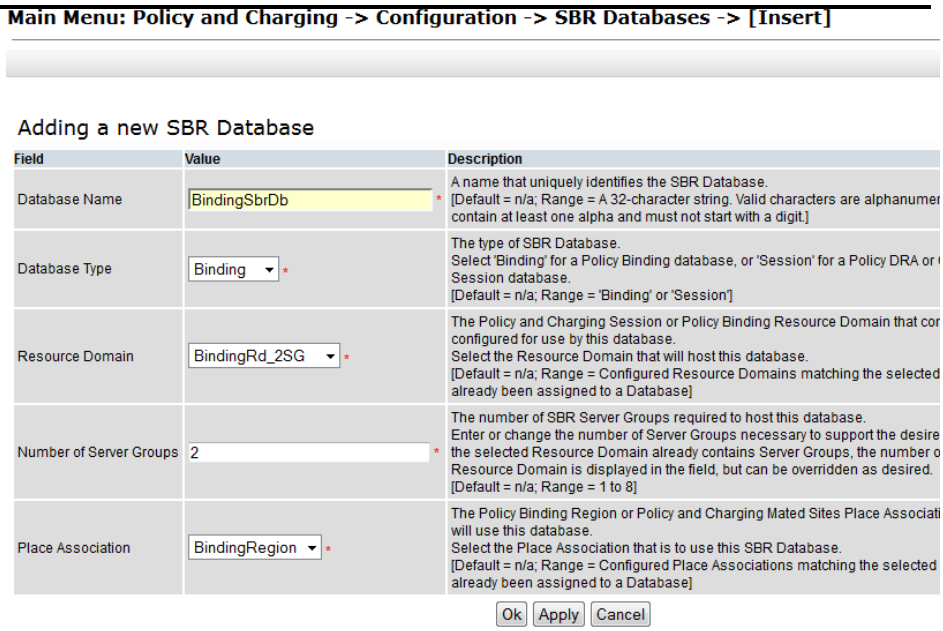
Detailed steps are given in the procedure below.

Procedure 12: Policy DRA configuration

S T E P #	This procedure configures the Policy DRA function of PCA application. PRE-REQUISITE: Procedure 10 must be executed before this procedure. 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 ☐	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**SOAM VIP:** Navigate to PCRFs screen	Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRFs**
3 ☐	**SOAM VIP:** Configure the first PCRF node.	Click on **Insert** in the lower left corner. You will see a screen similar to:  1. Select the PCRF name from the drop down 2. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
4 ☐	**SOAM VIP:** Configure all other PCRF nodes.	Repeat Step 3 to configure all the PCRF nodes.
5 ☐	**SOAM VIP:** Navigate to Binding Key Priority screen	Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Binding Key Priority** You will see a screen similar to:

		
6	**SOAM VIP:** Configure the Binding Key Priorities	1. Select the Binding Keys priority as appropriate 2. Click **Apply**.
7	**SOAM VIP:** Navigate to Topology Hiding screen	**OPTIONAL** If Topology Hiding feature is required execute Steps 7 through 11. Else skip to Step 12 Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Topology Hiding**
8	**SOAM VIP:** Configure the Peer node for which PCRF identity needs to be hidden	Click on **Insert** in the lower left corner. You will see a screen similar to:  1. Select the (policy client) node name from the list for which the PCRF identity needs to be hidden 2. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
9	**SOAM VIP:** Configure other Peer nodes for which PCRF identity needs to be hidden	Repeat Step 8 for all (policy client) nodes for which the PCRF identity needs to be hidden.
10	**SOAM VIP:** Navigate to PCA Site Options screen	**OPTIONAL** Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Site Options**

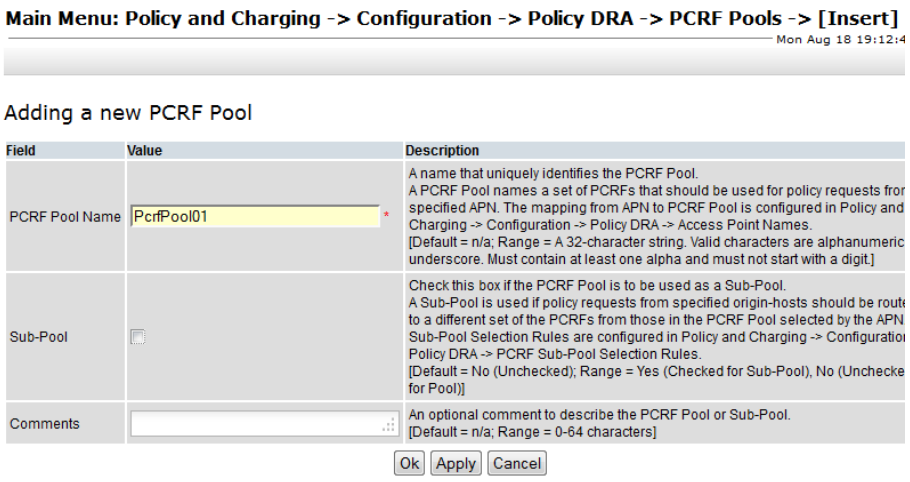
11	**SOAM VIP:** Configure the Topology Hiding FQDN	 If required, 1. Check the Enabled box 2. Select the appropriate value of Scope from the dropbox 3. Enter the virtual/pseudo host FQDN and Realm 4. Click **Apply**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
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:

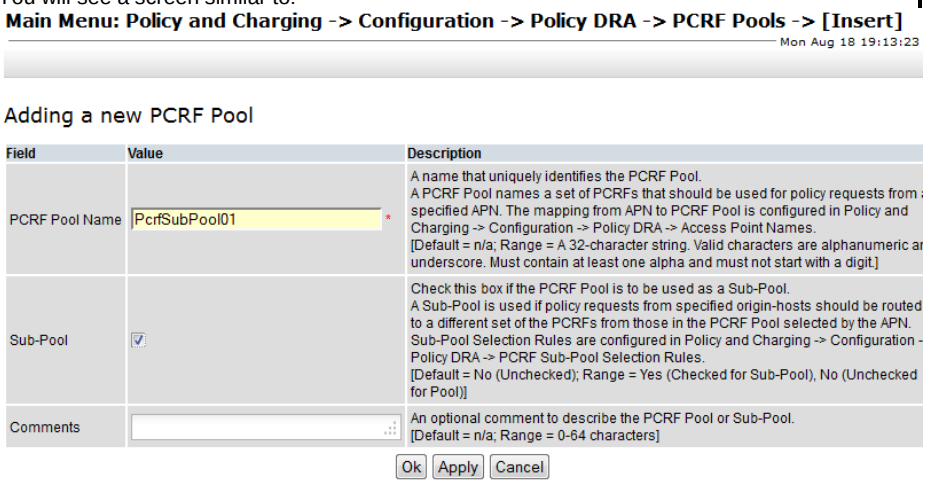


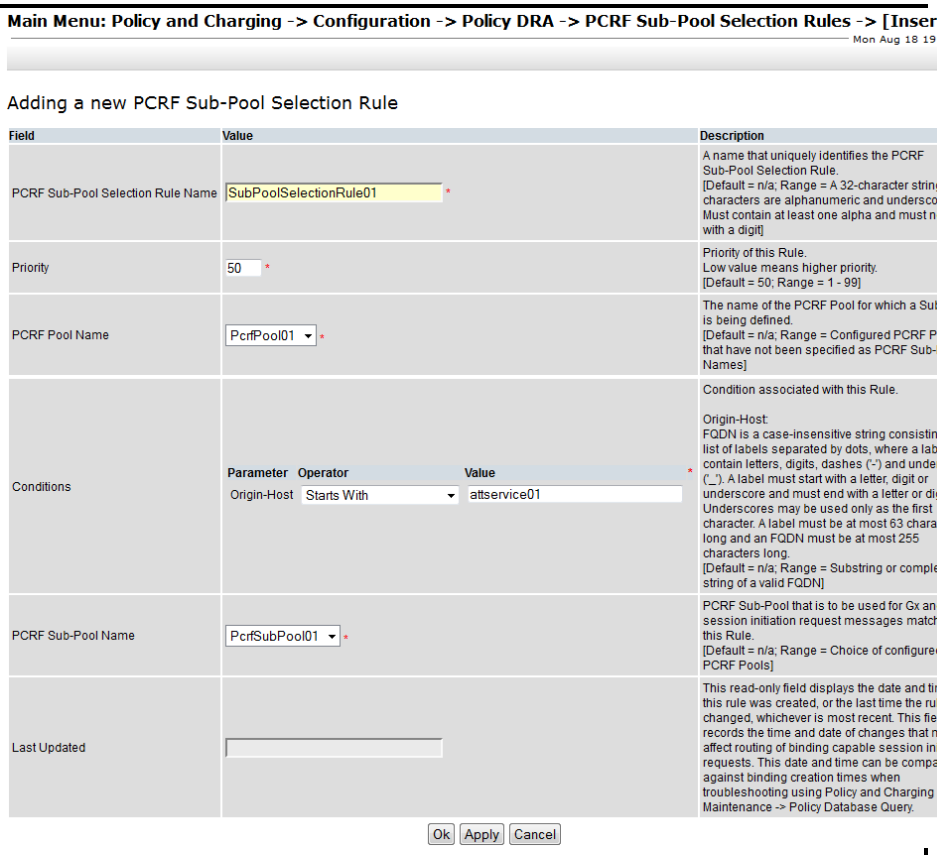
1. Enter Database Name
2. Select Database Type.
3. Select Resource Domain. *This wil populate Number of Server Groups field with the number of server groups currently present in the selected Resource Domain.*
4. If needed, update Number of Server Groups value. *Note that Resource Domain will then have 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: 

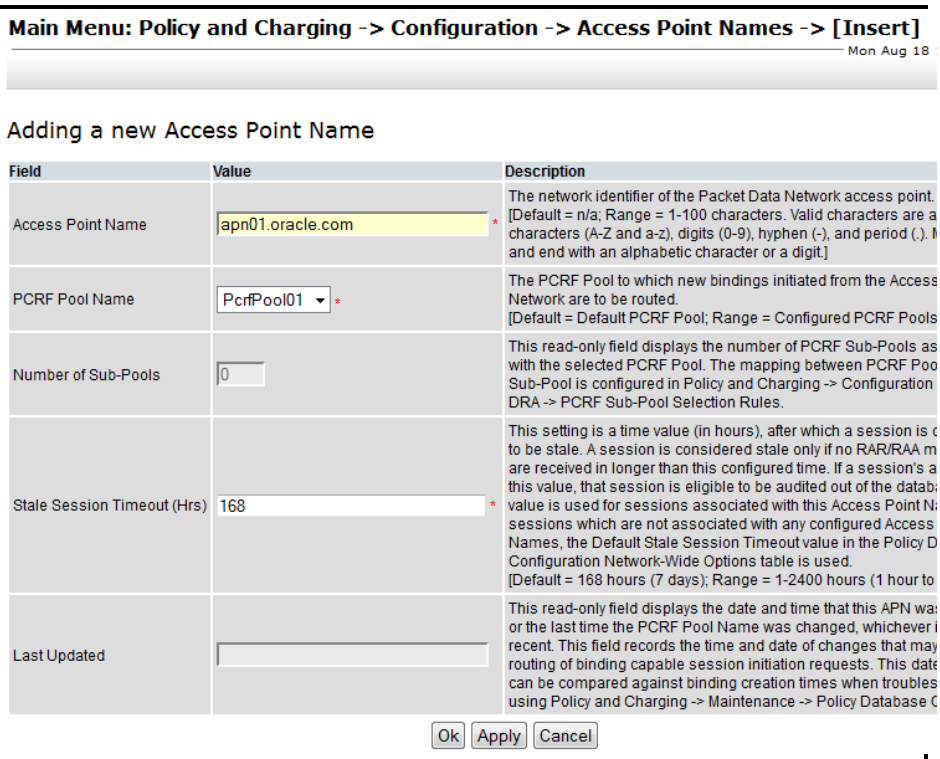
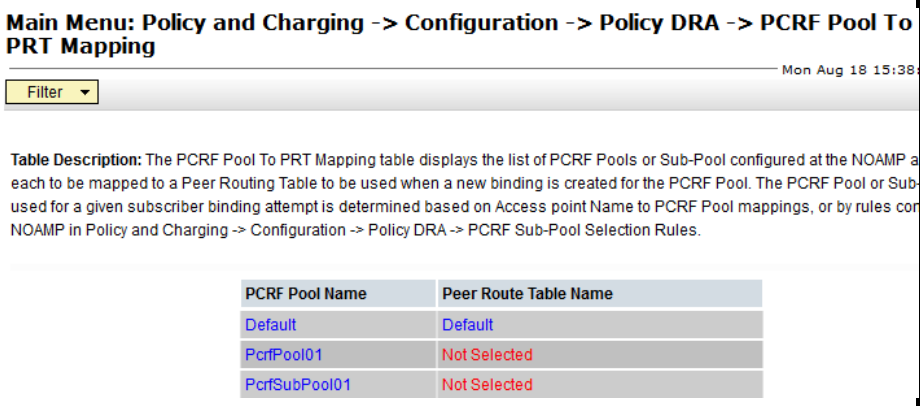
		1. Enter PCRF Pool name 2. Click **Ok** NOTE: this is a sample set of configuration data, the actual configuration may differ.
14	**NOAM VIP:** Configure PCRF Sub Pool	Navigate to **Main Menu -> Policy and Charging -> Configuration -> PCRF Pools** Click on **Insert** in the lower left corner. You will see a screen similar to:  1. Enter PCRF Sub Pool name 2. Check the Sub-Pool box 3. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
15	**NOAM VIP:** Configure PCRF Sub Pool Selection Rule	Navigate to **Main Menu -> Policy and Charging -> Configuration -> PCRF Sub-Pools Selection Rules** Click on **Insert** in the lower left corner. You will see a screen similar to:

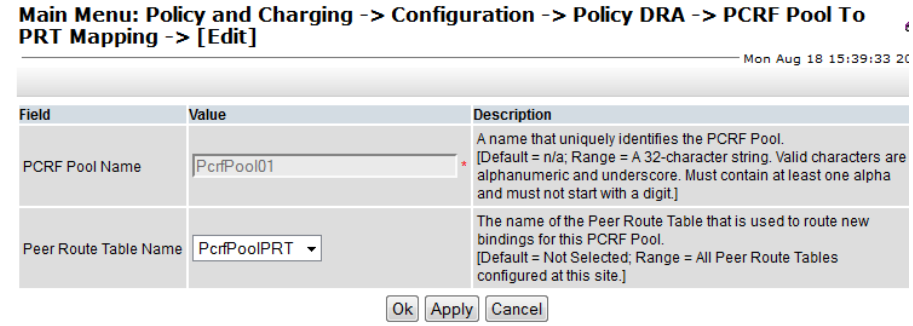


1. Enter the Rule name
2. Select PCRF Pool Name and PCRF Sub-Pool Name
3. Enter the Condition as shown
4. Click **Ok**.

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:

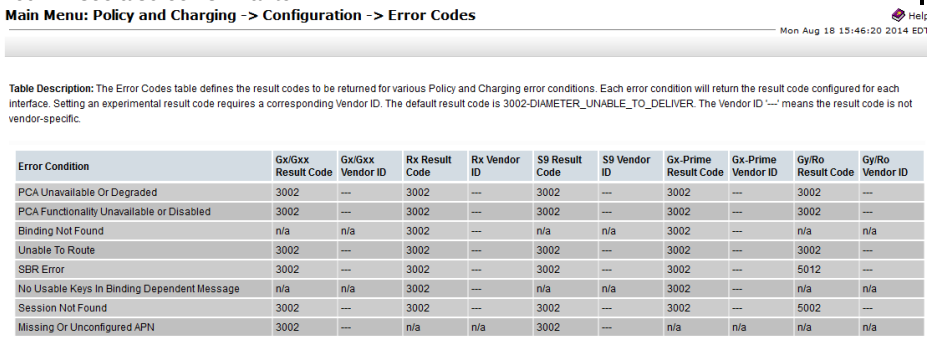
		 1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values) 2. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
17	**SOAM VIP:** Navigate to PCRF Pool To PRT Mapping screen	Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping** You will see a screen similar to: 
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:



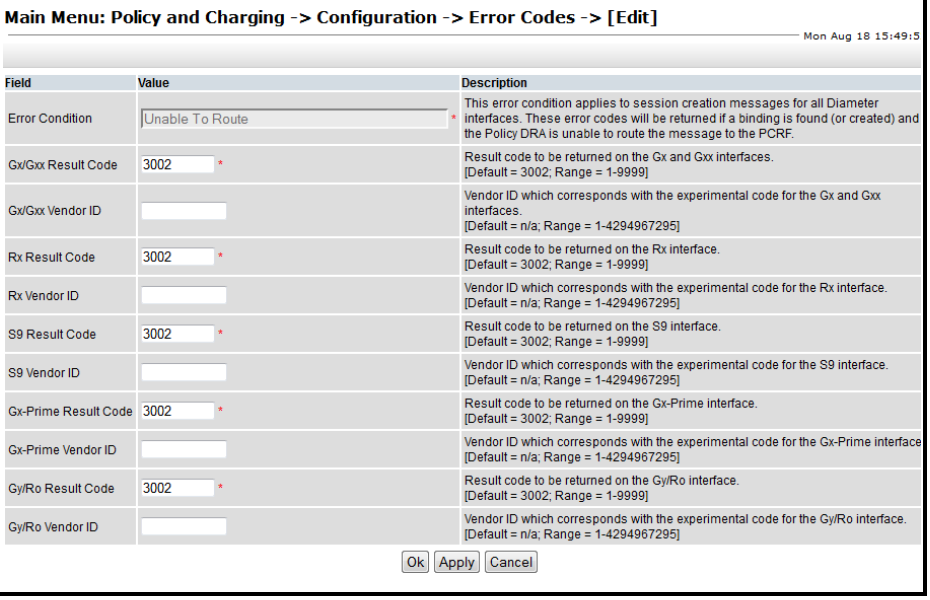
1. Select appropriate Peer Route Table Name form the dropbox.
2. Click **Ok**.

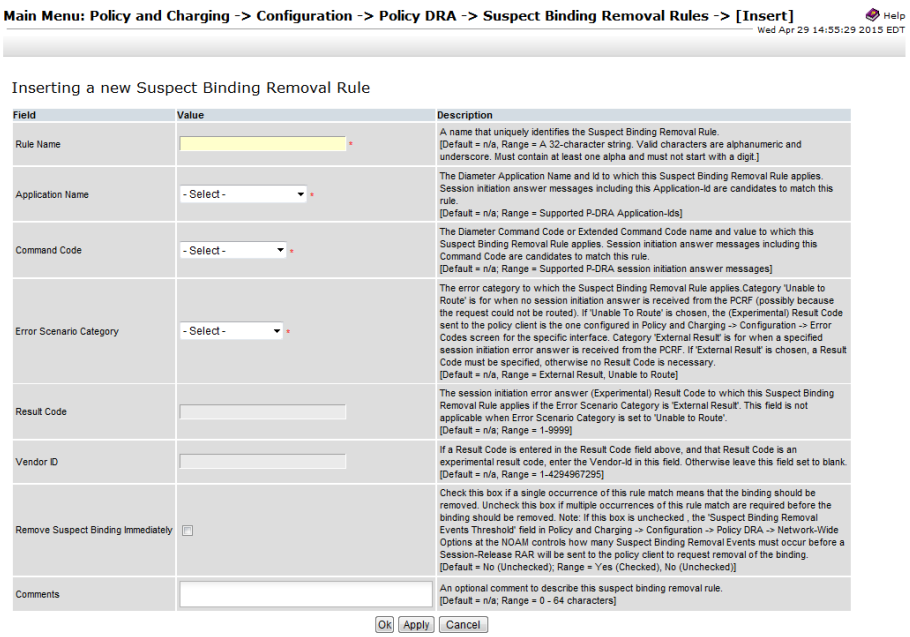
NOTE: this is a sample set of configuration data, the actual configuration may differ.

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:



21	**SOAM VIP:** Configure the Error Codes	Select the row to edit and click on 'Edit' button You will see a screen similar to:



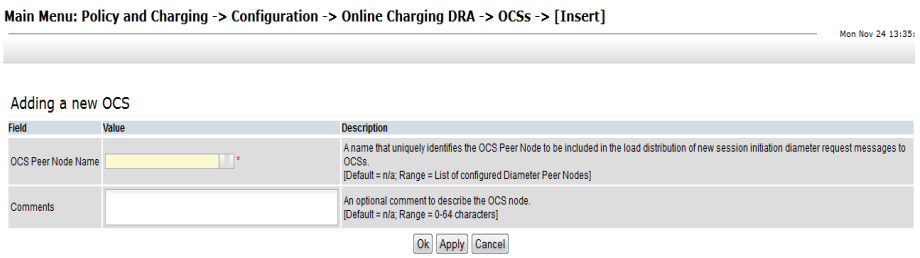
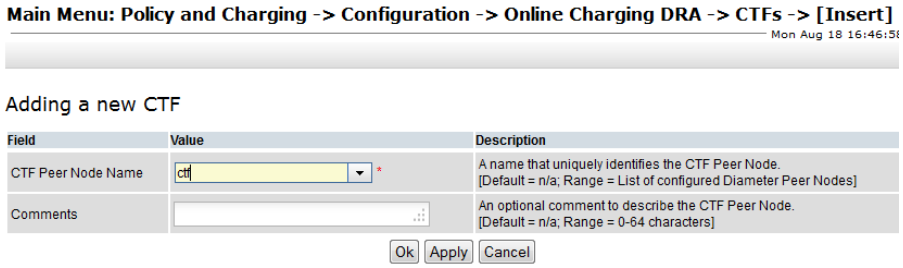
		1. Enter the Result Code and Vendor ID values as appropriate 2. Click **Ok**.
22	**SOAM VIP:** Navigate to Suspect Binding Removal Rules screen **OPTIONAL**	**Execute Steps 21 through 23 if additional Suspect Binding Removal Rules are required.** Note: A default Suspect Binding Removal rule for Gx CCA-I messages is created by default. Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Suspect Binding Removal Rules**
23	**SOAM VIP:** Configure the Suspect Binding Removal Rule for Diameter Interfaces and messages that are needed. **OPTIONAL**	Click on **Insert** in the lower left corner. You will see a screen similar to:  Main Menu: Policy and Charging -> Configuration -> Policy DRA -> Suspect Binding Removal Rules -> [Insert] Help Wed Apr 29 14:55:29 2015 EDT Inserting a new Suspect Binding Removal Rule Field / Value / Description Rule Name — 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 — 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 — 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 — 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 — 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 — 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 — 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 — An optional comment to describe this suspect binding removal rule. [Default = n/a; Range = 0 - 64 characters] Ok Apply Cancel 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**. NOTE: This is a sample set of configuration data, the actual configuration may differ.
24	**SOAM VIP:** Configure additional Suspect Binding Removal Rules. **OPTIONAL**	Repeat Step 22 for all Suspect Binding Rules that are needed. Note: Steps 21 through 23 may need to be repeated for each active SOAM.
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 — 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 — 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**.

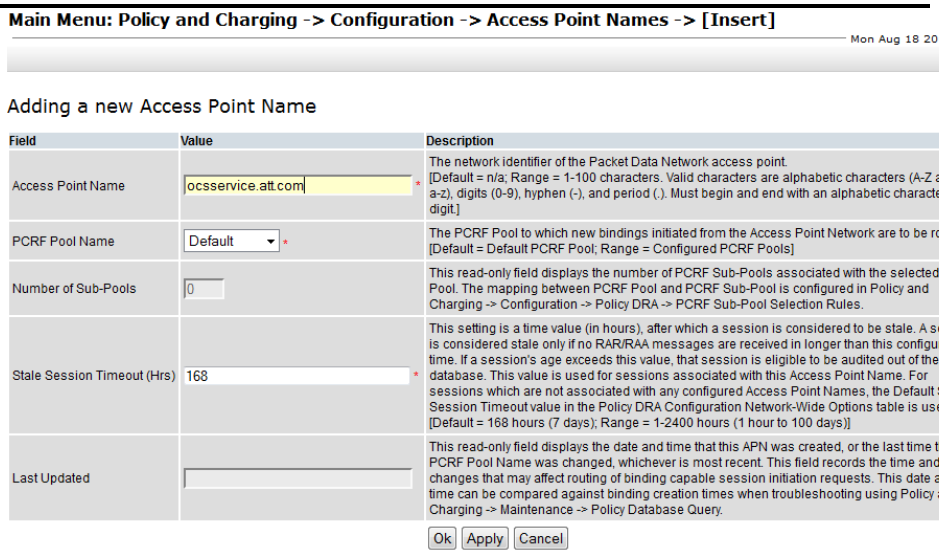
4.4.2 Online Charging DRA Configuration

Detailed steps are given in the procedure below.

Procedure 13: Online Charging DRA configuration

S T E P #	This procedure configures the Online Charging DRA function of PCA application. PRE-REQUISITE: Procedure 11 must be executed before this procedure. 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 ☐	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**SOAM VIP:** Navigate to OCSs screen	Navigate to **Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> OCSs**
3 ☐	**SOAM VIP:** Configure the first OCS node.	Click on **Insert** in the lower left corner. You will see a screen similar to:  1. Select the OCS name from the drop down 2. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
4 ☐	**SOAM VIP:** Configure all other OCS nodes.	Repeat Step 3 to configure all the OCS nodes.
5 ☐	**SOAM VIP: Navigate to CTFs screen**	If Session State needs to be maintained for Online Charging client, then Navigate to **Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> CTFs**
6 ☐	**SOAM VIP: Configure the first CTF node.**	Click on Insert in the lower left corner. You will see a screen similar to:  1. Select the CTF name from the drop down

		2. Click Ok. NOTE: this is a sample set of configuration data, the actual configuration may differ.
7	**SOAM VIP: Configure all other CTF nodes.**	Repeat Step 6 to configure all the CTF nodes for which the Session State needs to be maintained.
8	**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: SessionSbrDb * — A name that uniquely identifies the SBR Database. [Default = n/a; Range = A 32-character string. Valid characters ar… 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 F… Session database. [Default = n/a; Range = 'Binding' or 'Session'] Resource Domain: SessionRd_Mated * — The Policy and Charging Session or Policy Binding Resource Do… 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 databas… Enter or change the number of Server Groups necessary to supp… 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 P… 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] Ok Apply Cancel 7. Enter Database Name 8. Select Database Type (Session). 9. Select Resource Domain. *This wil populate Number of Server Groups field with the number of server groups currently present in the selected Resource Domain.* 10. If needed, update Number of Server Groups value. *Note that Resource Domain will then have to be updated to match this count.* 11. Select Place Association. 12. Click **Ok** NOTE: This is a sample set of configuration data, the actual configuration may differ. For Online Charging DRA Function, Session Type SBR Database per standalone-site/mated-pair/mated-triplet MUST be configured.
9	**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:



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.

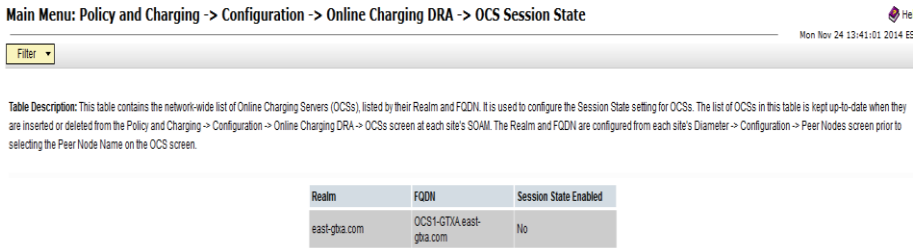
10 **NOAM VIP: Navigate to OCS Session State screen**

OPTIONAL

Execute Step 9, 10, 11 is 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:

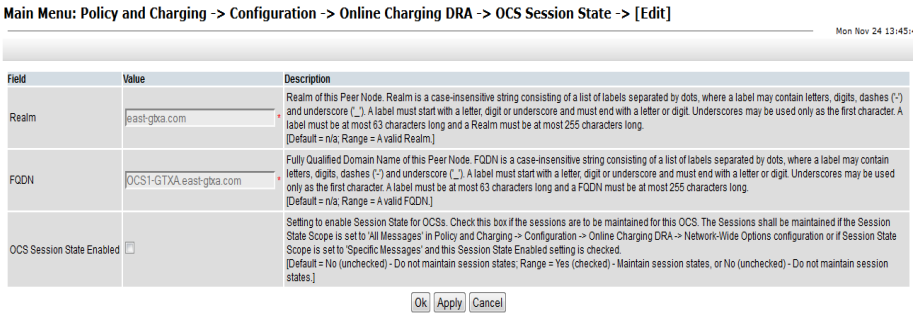


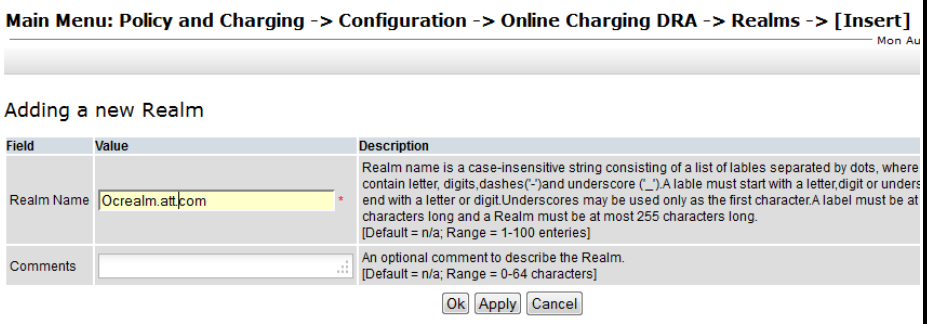
11 **NOAM VIP: Configure the Session State for an OCS.**

OPTIONAL

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

You will see a screen similar to:



		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. 2. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
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:  1. Enter the realm name 2. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
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']

Apply 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

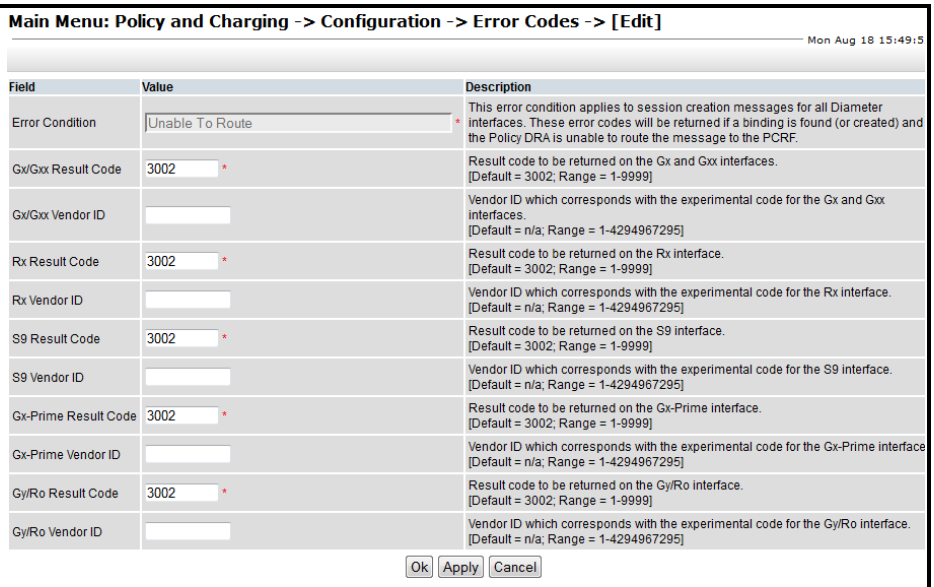
Table Description: The Error Codes table defines the result codes to be returned for various Policy and Charging error conditions. Each error condition will return the result code configured for each interface. Setting an experimental result code requires a corresponding Vendor ID. The default result 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

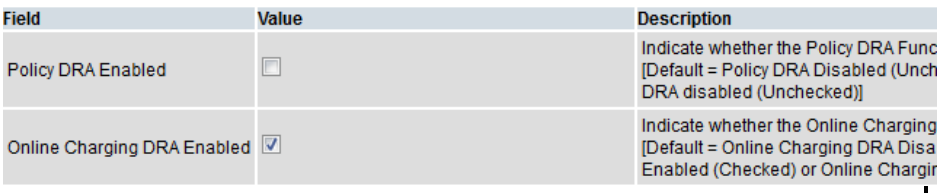
Select the row to edit and click on 'Edit' button

You will see a screen similar to:



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.



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 ORACLE TAC.**	
1 ☐	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 ORACLE TAC.**	
1 ☐	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 ORACLE TAC.**	
1 ☐	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.

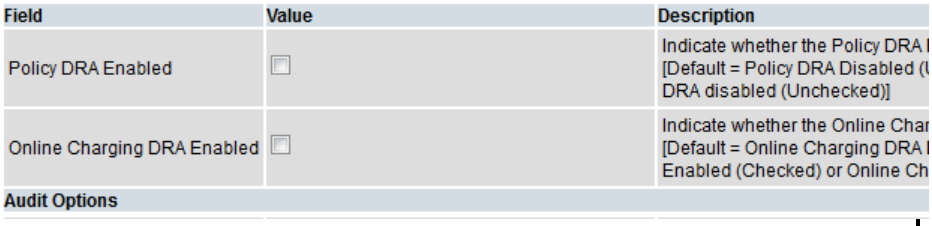
Procedure 17: Policy DRA Configuration with scaling on a running DSR PCA System

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 ☐	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

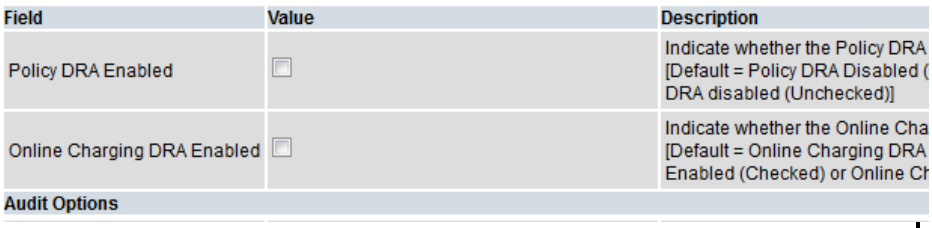
S T E P #	This procedure un-configures the Policy DRA function of PCA application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.	
1	Establish GUI Session 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.  1. Uncheck the Policy DRA Enabled box 2. Click **Apply**.
3	**NOAM VIP:** Disable the Policy DRA specific SBR Database	**Main Menu -> Policy and Charging -> Maintenenace -> SBR Database Status** Select the SBR Database of type 'Binding' and Disable it.
4	**NOAM VIP:** Delete the Policy DRA specific SBR Database	**Main Menu -> Policy and Charging -> Configuration -> SBR Databases** Delete the SBR Database of type 'Binding' from this screen.
5	**NOAM VIP:** Delete the Policy DRA specific APNs	**Main Menu -> Policy and Charging -> Configuration -> Access Point Names** Delete the Policy DRA specific configuration data from this screen.
6	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	**SOAM VIP:** De-reference all the PRTs from PCRF Pools	**Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping** Edit all the PCRF Pool Name entries and set the Peer Route Table Name to 'Not Selected'.
8	**SOAM VIP:** Delete all the PCRFs	**Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRFs** Delete the complete configuration data from this screen.
9	**SOAM VIP:** Delete all the Policy Clients configuration	**Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Policy Clients** Delete the complete configuration data from this screen.
10	**SOAM VIP:** Un-	**Main Menu -> Policy and Charging -> Configuration ->**

☐	configure the Site Options	**Policy DRA -> Site Options** Uncheck the 'Enabled' box against 'Topology Hiding Options'.
11 ☐	**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 ☐	**SOAM VIP:** Perform steps on All Active SOAM Servers	Repeat Steps 4 to 9 on All Active SOAM servers.
13 ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
14 ☐	**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 ☐	**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

S T E P #	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 ORACLE TAC**.	
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.  1. Uncheck the Online Charging DRA Enabled box 2. Click **Apply**.
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** 1. Edit the Error Condition 'SBR Error' and set the Gy/Ro Result Code as 5012. 2. Edit the Error Condition 'Session Not found' and set the Gy/Ro Result Code as 5002. 3. 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.

	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 ORACLE TAC.** **NOTE: - PLEASE DO ALL RESOURCE DOMAIN RELATED CONFIGURATION BEFORE CONTINUING THIS STEP.**	
1 ☐	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 ☐	**SOAM VIP:** Navigate to Applications screen	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**
3 ☐	**SOAM VIP:** Enable the PCA application	Select the PCA row and Click **Enable**.
4 ☐	**SOAM VIP:** Verify that the PCA application has been Enabled.	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications** Verify that the Application status has changed to Enabled-Available-Normal-Normal. **NOTE:** It may take some time (15-30 seconds) to initialize and change state.
5 ☐	**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.

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

4.9.2 Enable SBR Databases

Detailed steps are given in the procedure below.

Procedure 21: Enable SBR Databases

S T E P #		
		This procedure enables the SBR Databases. 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 DO ALL RESOURCE DOMAIN RELATED CONFIGURATION BEFORE CONTINUING THIS STEP.**
1 ☐	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 ☐	**NOAMP VIP:** Navigate to SBR Database Status screen	Navigate to **Main Menu -> Policy and Charging -> Maintenance -> SBR Database Status**
3 ☐	**NOAMP VIP:** Prepare the SBR Database	Select the SBR Database and Click **Prepare**.
4 ☐	**NOAMP VIP:** Verify that the SBR Database has been prepared.	Navigate to **Main Menu -> Policy and Charging -> Maintenance -> SBR Database Status** Verify that the SBR Database status has changed to Prepare – Prepared - N of N prepared - N of N prepared **Main Menu: Policy and Charging -> Maintenance -> SBR Database Status** Thu May 07 07:36:41 2 Filter 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 **NOTE:** It may take some time (5-6 seconds) to change state.
5 ☐	**NOAMP VIP:** Enabled the SBR Database	Select the SBR Database and Click **Enable**.
6 ☐	**NOAMP VIP:** Verify that the SBR Database has been enabled.	Navigate to **Main Menu -> Policy and Charging -> Maintenance -> SBR Database Status** Verify that the SBR Database status has changed to Enable – Normal - N of N available - N of N available

		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 #	This procedure restarts the DSR and Policy and Charging SBR process. 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 ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**NOAM VIP:** Restart Process on DSR MP and Policy and Charging SBR Servers	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 #	This procedure enables the Diameter connection with Peer nodes. 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 ☐	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**SOAM VIP:** Navigate to Connections screen	Navigate to **Main Menu -> Diameter -> Maintenance -> Connections**

3	**SOAM VIP:** Enable all connections	Select all Connection rows and Click **Enable**.
4	**SOAM VIP:** Verify that the connections have been Enabled.	Navigate to **Main Menu -> Diameter -> Maintenance -> Connections** 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. **Main Menu: Diameter -> Maintenance -> Connections** Help Thu Feb 16 09:39:46 2012 EST Filter **NOTE 1:** For connections of type “Responder Only” (client nodes), the Operational Status and Reason will be “Unk” if using TSA. **NOTE 2:** It may take some time (15-30 seconds) to initialize and change state.

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 #	This procedure performs a Health Check. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	Verify HA Services Status	Verify HA Services status: 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. If all the verifications are successful, then proceed with next step else STOP! And call ORACLE Customer Service for further assistance.
2 ☐	Verify the Automatic Connection Count for all the PCA and Policy SPR servers	Verify ComAgent Automatic Connection Status: 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. If all the verifications are successful, then proceed with next step else STOP! And call ORACLE Customer Service for further assistance.
3 ☐	Verify the Policy and Charging SBR Status	Verify Policy and Charging SBR Services status: 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. If all the verifications are successful, then proceed with signaling call flow execution else STOP! And call ORACLE Customer Service for further assistance.

5.0 CAVEATS

6.0 CUSTOMER SERVICE SIGN OFF

Discrepancy List

Date	Test Case	Description of Failures and/or Issues. Any CSR's / RMA's issued during Acceptance. Discrepancy	Resolution and Engineer Responsible	Resolution Date

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 #	This procedure activates the PCA on complete 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.** **NOTE: - PLEASE COMPLETE THE TOPOLOGY CONFIGURATION OF ALL THE REQUIRED SOAM SERVERS BEFORE CONTINUING THIS STEP. SEE [1] AND [2] FOR STEPS.**	
1 ☐	**NOAM VIP:** Navigate to HA screen	Navigate to **`Main Menu: Status & Manage -> HA`** Find the Active NOAM and Active SOAM Servers list
2 ☐	Verify configuration of All SOAM servers	Before continuing all SOAM servers should be configured in the topology. 1. Log into the NOAM VIP GUI. 2. Navigate **Main Menu: Status & Manage -> Server.** See all required SOAM servers are configured and Application State is enabled.
3 ☐	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 VIP Address>`**
4 ☐	**PCA Application Activation:** Change directory	Change to the following directory: **`# cd /usr/TKLC/dsr/prod/maint/loaders/activate`**
5 ☐	**PCA Activation:** Execute the PCA application activation script	**`# ./load.pcaActivationTopLevel`** Note: - This command execution will starts Activation on NOAM servers and All Active SOAM servers. If the activation fails, then execute the procedure in Section 8.2.2 to restore the system back to state before start of activation.
6 ☐	**PCA Application Activation (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`**

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 #	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 ☐	**NOAM VIP:** Navigate to HA screen	Navigate to **Main Menu: Status & Manage -> HA** Find the Active NOAM and Active SOAM Servers list
2 ☐	Verify configuration of All SOAM servers	Before continuing all SOAM servers should be configured in the topology. 1. Log into the NOAM VIP GUI. 2. Navigate **Main Menu: Status & Manage -> Server.** See all required SOAM servers are configured and Application State is enabled.
3 ☐	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 VIP Address>`
4 ☐	**PCA Activation:** Change directory	Change to the following directory: `# cd /usr/TKLC/dsr/prod/maint/loaders/activate`
5 ☐	**PCA Activation:** Execute the PCA application activation script	`# ./load.pcaActivationTopLevel` Note: - This command execution will start activation on newly added SOAM Servers. If the activation fails, then execute the procedure in Section 8.2.3 to restore the system back to state before start of activation.
6 ☐	**PCA Activation (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`

8.1.3 Restart Process

Detailed steps are given in the procedure below.

Procedure 27: Restart Process

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

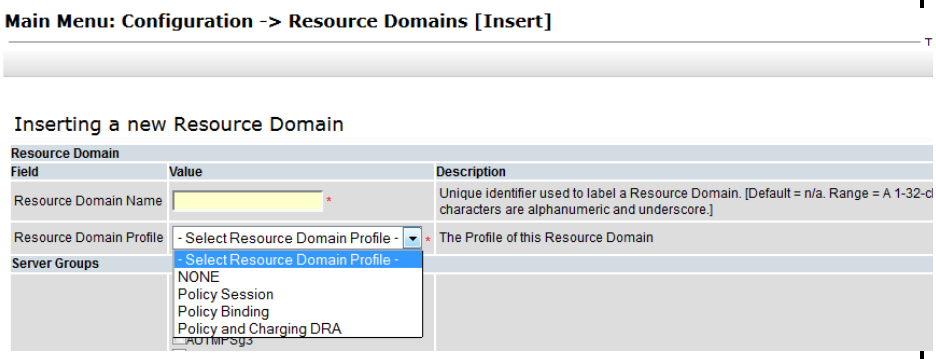
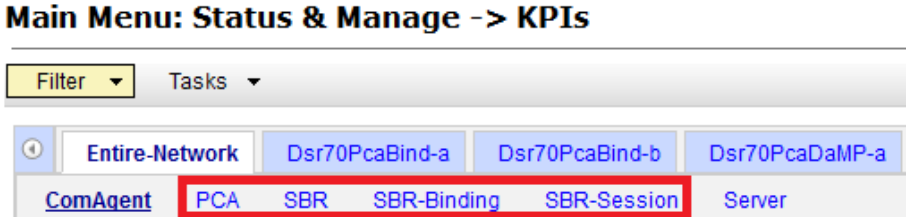
P #	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**. **NOTE: - This STEP is MANDATORY only if DSR MP AND PSBR Servers are newly added in the TOPOLOGY.**	
1 ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. 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**.

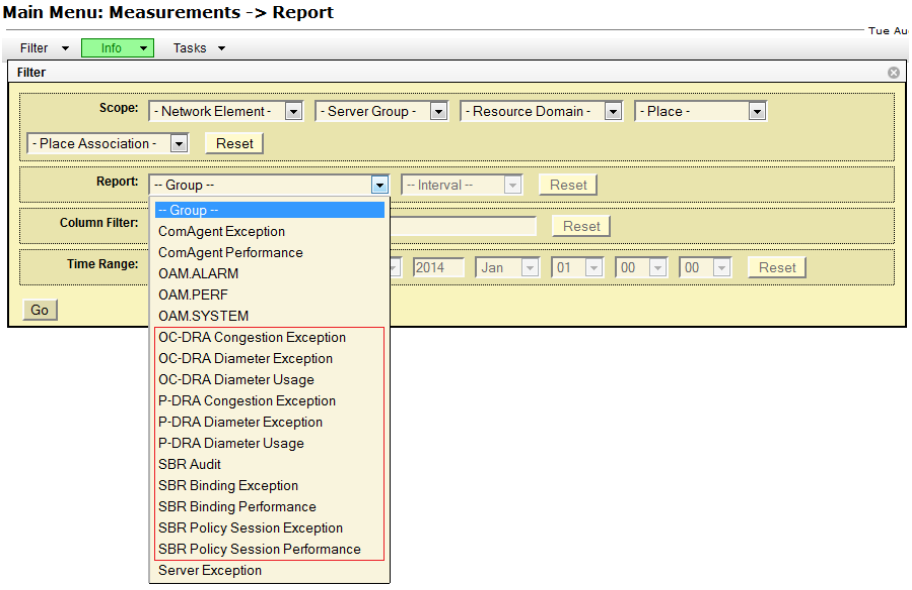
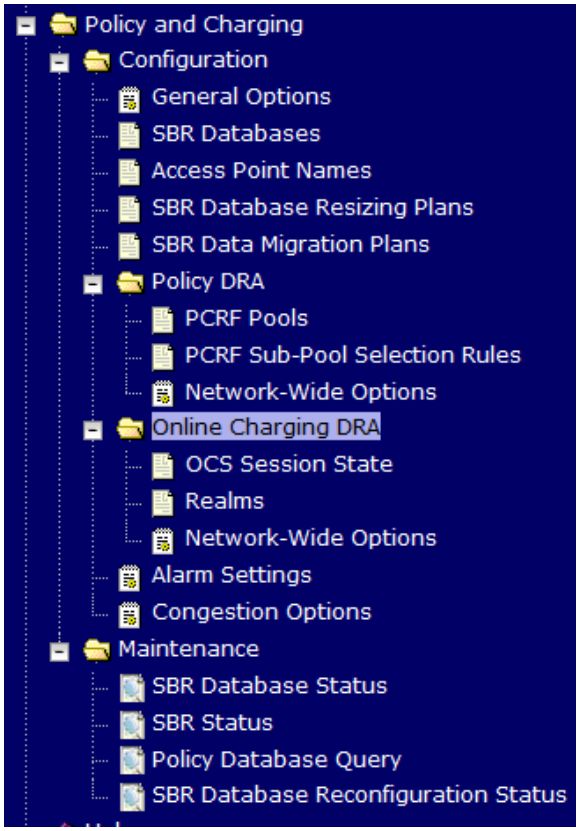
8.1.4 Post PCA Activation System Health Check

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

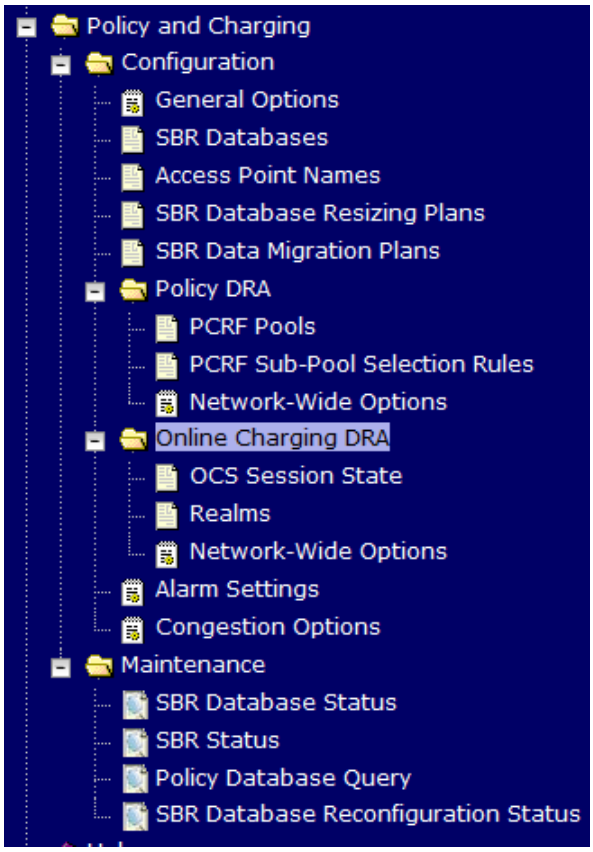
S T E P #	This procedure verifies the PCA application activation on NOAM Server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.	
1 ☐	**Active NOAM VIP:** 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. 
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. 
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.	
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 #	This procedure verifies the activation of PCA on SOAM Servers. 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 ☐	**SOAM VIP:** Establish GUI Session using SOAM VIP	Establish a GUI session on the Active SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**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

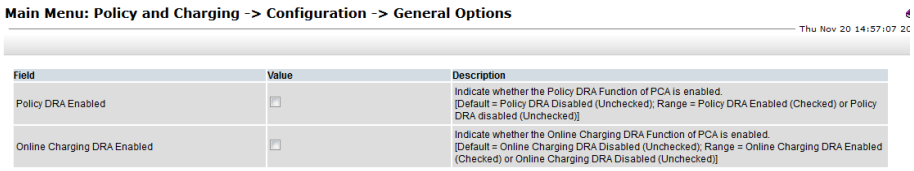
S T E P #	This procedure verifies that GLA is activated and then deactivates the GLA application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**. **NOTE: - PLEASE VERIFY FIRST THAT GLA IS ACTIVATED IN STEPS 1-2 AND THEN EXECUTE THE STEPS 4-5 TO DEACTIVATE THE GLA APPLICATION.**	
1 ☐	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**SOAM VIP:** Navigate to Applications screen	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**
3 ☐	**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 ☐	**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 ☐	**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)

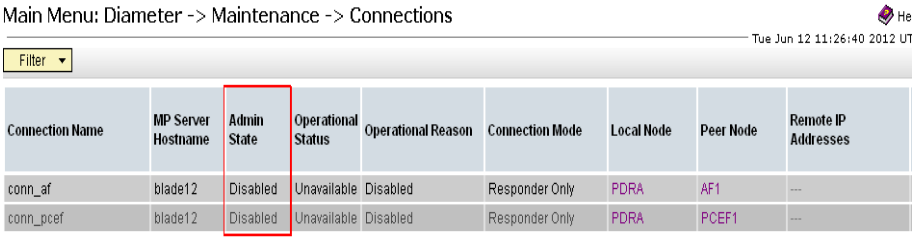
S T E P #	This procedure disables the DSR connections. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES.	
1 ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the Active NOAM by using the XMI VIP address. Login as user "guiadmin".

2	**NOAM VIP:** Disable PCA Functions.	Navigate to **Main Menu: Policy and Charging -> Configuration -> General Options** Uncheck 'Policy DRA Enabled' and 'Online Charging DRA Enabled'. Click Apply. 

8.2.1.3 Disable Diameter Connections

Detailed steps are given in the procedure below.

Procedure 32: Disable Diameter Connections

S T E P #	This procedure disables the Diameter 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 AND **ASK FOR ORACLE TAC**.
1	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	**SOAM VIP:** Disable DSR connections.	Navigate to **Main Menu: Diameter -> Maintenance -> Connections** Select all the PCA specific diameter connections and click disable or click Disable All (if applicable). The Admin State of connections should be shown as Disabled. 
3	**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 #	This procedure disables the PCA application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**SOAM VIP:** Navigate to Applications screen	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**
3 ☐	**SOAM VIP:** Disable the PCA application	Select the PCA row and press **Disable**. 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.
4 ☐	**SOAM VIP:** Verify that the PCA application has been Disabled.	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications** Verify that the Application status has changed to Disabled. Main Menu: Diameter -> Maintenance -> Applications Tue Jun 12 Filter 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 ☐	**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 #	This procedure stops the DSR and PSBR processes. 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	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:** Stop DSR MP and PSBR MP Server processes.	Find the DA-MP and SBR server hostnames corresponding to the functions "Diameter Signaling Router" and "SBR" from **Main Menu: Configuration -> Server Groups** Then, navigate to **Main Menu -> Status & Manage -> Server** Select all the DA-MP and SBR and press **Stop**.

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 #	This procedure removes the PCA 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 ORACLE TAC.**	
1	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2	**SOAM VIP:** Remove all the data from PCA screen as mentioned.	**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.** **Main Menu: Policy DRA -> Configuration -> PCRFs** Delete the complete configuration data from this screen.
3	**SOAM VIP:** Perform steps on All Active SOAM Servers	Repeat Steps 1 and 2 on All Active SOAM servers.
4	Establish GUI Session on the NOAMP VIP	Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user "guiadmin".
5	**NOAMP VIP:** Complete or Cancel any ongoing Reconfiguration Plans	**Main Menu: Policy and Charging -> Maintenance -> SBR Database Reconfiguration Status** If any Reconfiguration Plan is in the Prepared or Preparing state, then click Cancel to return to the Planned state. 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.

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

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 #	This procedure removes the DSR 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 ORACLE TAC**. **NOTE:-** **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.** **B.) DON'T EXECUTE THIS STEP IF THERE ARE MUTIPLE APPLICATIONS INSTALLED ON THIS SYSTEM.**	
1 ☐	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	***SOAM VIP:*** *Remove all the data of Application Routing Rules.*	***Main Menu: Diameter -> Configuration -> Application Routing Rules*** *Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.*
3 ☐	***SOAM VIP:*** *Remove all the data of Peer Routing Rules.*	***Main Menu: Diameter -> Configuration -> Peer Routing Rules*** *Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.*
4 ☐	***SOAM VIP:*** *Remove all the data of Route Lists*	***Main Menu: Diameter -> Configuration -> Route Lists*** *Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.*
5 ☐	***SOAM VIP:*** *Remove all the data of Route Groups*	***Main Menu: Diameter -> Configuration -> Route Groups*** *Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.*
6 ☐	***SOAM VIP:*** *Remove all the data of Connections.*	***Main Menu: Diameter -> Configuration -> Connections*** *Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.*
7 ☐	***SOAM VIP:*** *Remove all the data of Peer Nodes.*	***Main Menu: Diameter -> Configuration -> Peer Nodes*** *Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.*
8 ☐	***SOAM VIP:*** *Remove all the data of Local Nodes.*	***Main Menu: Diameter -> Configuration -> Local Nodes*** *Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.*
9 ☐	***SOAM VIP:*** *Remove all the data of CEX Configuration Sets*	***Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets*** *Select and delete the PCA specific or the complete configuration data (as applicable) from this screen.*

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 ORACLE TAC**.
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 #	This procedure de-activates the PCA application on a particular site. 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 ☐	Establish a secure shell Session on the active SOAM or on which deactivation is required.	Establish a secure shell session on the active SOAM 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 SO 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.pcaDeactivateBscoped` Note: - This command execution will start De-Activation on selected active SOAM server.
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`

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 #	This procedure puts all the MP Servers in Policy and Charging SBR Server Groups in OOS. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**. **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: Configuration -> Server Groups**
3 ☐	**NOAM VIP:** Find the Server List	Find the Servers with Function as "Policy and Charging SBR".
4 ☐	**NOAM VIP:** Navigate to HA screen	Navigate to **Main Menu: Status & Manage -> HA** Edit the Servers from list created in Step 3. Change the value of "Max Allowed HA Role" to OOS.

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 #	This procedure removes all the MP Servers in Policy and Charging SBR Server Groups from their respective Server Groups. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**. **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: Configuration -> Server Groups**
3 ☐	**NOAM VIP:** Find the Server List	Find the Servers with Function as "Policy and Charging SBR".
4 ☐	**NOAM VIP:** Edit the Server Groups.	Navigate to **Main Menu: Configuration -> Server Groups** Edit the Server Group with "Policy and Charging SBR" function and remove the servers from it.

		Repeat the steps with all server groups with “Policy and Charging SBR” function.

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 ORACLE TAC.** **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: Configuration -> Server Groups`**
3	**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 ORACLE TAC.**	
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:** 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 ORACLE TAC.** **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.

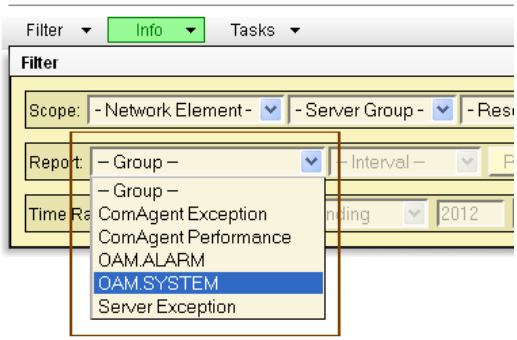
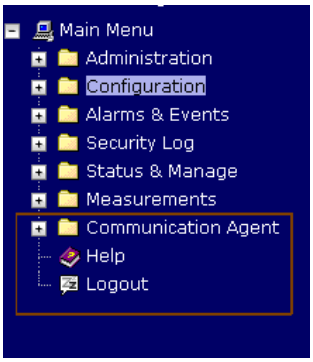
8.2.5 Post PCA De-Activation System Health Check

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

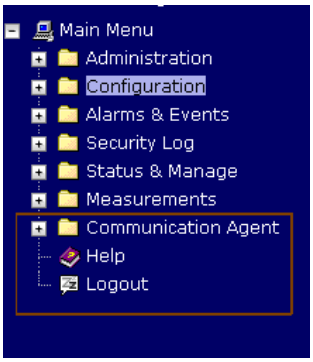
S T E P #	This procedure verifies the PCA application deactivation on NOAM Server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.	
1 ☐	**Active NOAM 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 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 Resource Domain Field / Value / Description Resource Domain Name * — Unique identifier used to label a Resource Domain. [Defau 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 Filter Tasks NO_1030302 blade05 blade06 blade08 Server ComAgent
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.

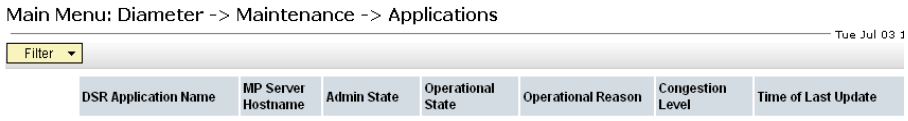
		Main Menu: Measurements -> Report 
5	**NOAM VIP:** Verify that the Main Menu don't show the Policy and Charging submenu.	Verify that Main Menu on Active NOAM doesn't show the Policy and Charging submenu. 

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

S T E P #	This procedure verifies the PCA application deactivation on SOAM Servers. 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	**SOAM VIP:** Establish GUI Session on the SOAM VIP	Establish a GUI session on the Active SOAM by using the XMI VIP address. Login as user "guiadmin".
2	**SOAM VIP:** Verify that the Policy and Charging folder is not visible in the Left Hand Menu	Verify that the Policy and Charging folder does not appear on the Left Hand Menu: 

3 ☐	**SOAM VIP:** Verify that the Diameter maintenance application menu do not show the entry of PCA application	Verify that the Diameter maintenance application menu do not show the entry of PCA application 
4 ☐	**SOAM VIP:** Verify PCA application on All Active SOAM servers	Repeat Steps 1 to 3 on All Active SOAM servers from Active Servers List collected from Step 1 of Procedure 4.