Oracle® Communications
Diameter Signaling Router

Policy and Charging Application Configuration

Release 7.3

E67989, Revision 02

August 2016

ORACLE®

Oracle Communications Diameter Signaling Router Policy and Charging Application Configuration Release 7.3

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

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

Table of Contents

List of Tables

List of Figures

List of Procedures

1.0 INTRODUCTION

1.1 PURPOSE AND SCOPE

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

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

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

The audience for this document includes these Oracle CGBU Groups:

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

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

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

1.2 REFERENCES

[1] DSR 7.3 Hardware and Software Installation Procedure 1/2, E53488-03

[2] DSR 7.3 Software Installation and Configuration Part 2/2, E69409-02

[3] IP Front End (IPFE) User's Guide, E73317-01

[4] Policy Charging Application User's Guide, E73186-01

[5] IDIH User's Guide, E69819-01

[6] DSR Software Upgrade Guide, Release 7.3, E73343-01

[7] Diameter User's Guide Release 7.3, E73184-01

[8] DSR GLA Feature Activation Procedure, Release 7.3, E58659-04

1.3 GLOSSARY

Table 1. Acronyms

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

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

Table 2. Terminology

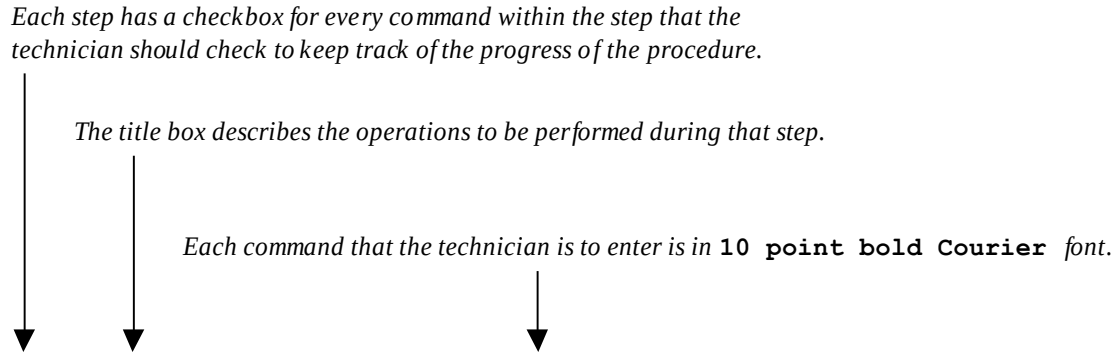
Term	Definition
PCA Application	The Policy and Charging Application hosts the Policy DRA and Online Charging DRA functionality for intelligent routing of policy and charging Diameter signaling. The PCA application is activated and deactivated using the PCA feature activation and deactivation scripts.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

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

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

1.4 GENERAL PROCEDURE STEP FORMAT

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



5 ☐	**ServerX:** Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. `$ cu -l /dev/ttyS7`

Figure 1: Example of a procedure step

2.0 PCA CONFIGURATION OVERVIEW

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

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

2.1 REQUIRED CONFIGURATION DATA

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

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

A. A 3-tier DSR system installed using [1] and [2]

B. Following Diameter configuration material

1. List of supported Application Ids
2. CEX Parameters
3. Local and Peer Node(s) configuration parameters
4. Diameter Connection parameters
5. Routing configuration parameters
   - *Route Groups*
   - *Route Lists*
   - *Peer Route Tables*
   - *Application Route Tables*
6. IDIH Configuration Parameters (Optional)

C. Following PCA configuration material:

1. Server Group configuration parameters
2. Place configuration parameters
3. Place Association configuration parameters
4. Resource Domain configuration parameters
5. SBR Databases
6. Default Audit Options
7. Access Point Names and the "Stale Session Timeout" for the APN
8. Alarm Settings
9. Congestion Settings

D. Depending upon the PCA function, following configuration items

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

2.2 PCA CONFIGURATION SUMMARY

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

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

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

3.0 PCA CONFIGURATION PREPARATION

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

3.1 HARDWARE PREPARATION

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

3.2 REQUIRED MATERIALS CHECK

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

Procedure 1: Required Materials Check

S T E P #	This procedure verifies that all required materials are present. Please refer to the Diameter User's Guide[7] for details of paremeters required for configuring Diameter Please refer to the Policy Charging Application User's Guide[4] for details of parameters required for configuration PCA Functions (Policy DRA, Online Charging DRA) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.	
1 ☐	Verify that the configuration data has been collected	Required Information is listed in Section 2.1. Conduct a system survey to 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 7.3 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 that all DAMP servers that will be running the PCA application and all SBR MP Servers have a Site Place configured. 4. Save the report and/or print the report. Keep these copies for future reference.
4 ☐	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 that all Server Group(s) that have been identified to host the SBR Database(s) have the function “Policy and Charging SBR”. 8. Save the report and/or print the report. Keep these copies for future reference.
5 ☐	Analyze and plan DA-MP restart sequence	If the DSR system is running traffic other than PCA then all the DAMP servers must not be restarted/rebooted simultaneously. Doing so will cause a network/site wide outage. Instead a groups of DAMP servers must be selected and restarted one group at a time such that the servers that are operational when some are down can handle the additional traffic. Analyze system topology and plan for any DA-MPs which will be out-of-service during the PCA configuration sequence. 1. Analyze system topology gathered in Step 1 and 2. 2. Determine exact sequence which DA-MP servers will be restarted (with the expected out-of-service periods). This sequence needs to be followed while executing APPENDIX-B
6 ☐	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. The following diagram depicts an example of a 2 site Mated-Pair PCA system. The topology configuration will depend on the customer's choice of deployment options: standalone (no site-redundancy), mated pair (2 site-redundancy) or mated triplet (3 site-redundancy).

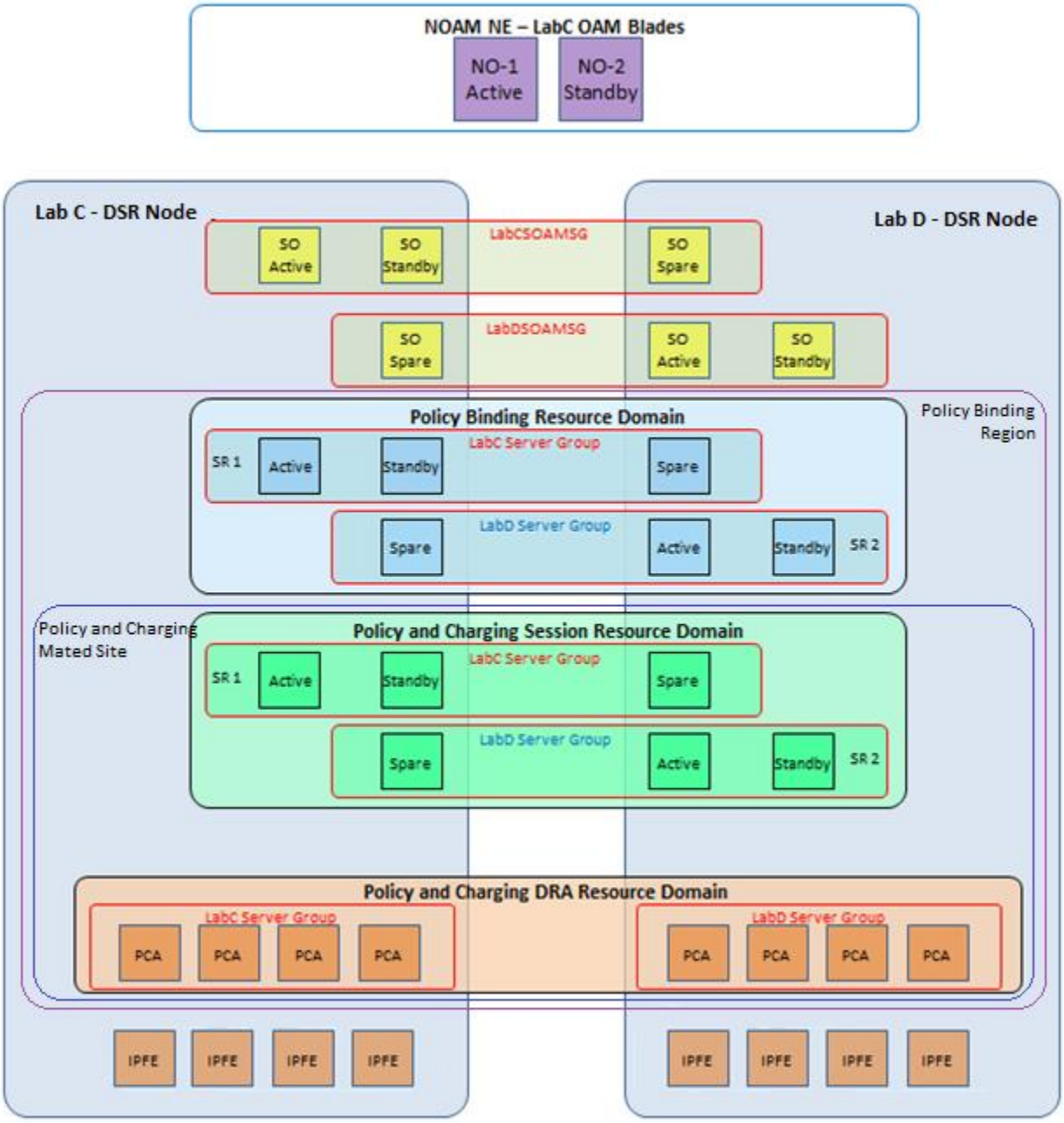


Figure 2: Example – Mated Pair PCA / Policy and Charging SBR Topology

Notes of Figure 2:

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

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

Procedure 3: Record Required Configuration Information

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

		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:** **Use additional space for recording more Mated Sites type Place Associations.**

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. **NOTE: Depending on the redundancy-model chosen there can be up to 3 Server Groups in one Policy and Charging DRA Resource Domain.** **DRA RD1 - LabCDRASG** **DRA RD2 - LabDDRASG** **DRA RD3 -** **DRA RD4 -** **DRA RD5 -** **DRA RD6 -** **DRA RD7 -** **Use additional space for recording more Resource Domains.** 2. Identify and log the '**Policy Binding**' resource domain and its Server Groups. **Note 1: This step is required for Policy DRA functionality only.** **Note 2: Depending on the capacity chosen there can be up to 8 Server Groups in one Policy Binding Resource Domain.** **Policy Binding RD1 – LabCBindingSR1SG** 3. Identify and log the number of '**Policy Session**' resource domains and their Server Groups. **Note: Depending on the capacity chosen there can be up to 8 Server Groups in one Policy Session Resource Domain.** **Policy Session RD1 – LabCSessionSR1SG** **Policy Session RD2 – LabDSessionSR2SG** **Policy Session RD3 – LabCSessionSR3SG** **Policy Session RD4 – LabDSessionSR4SG** **Policy Session RD5 -** **Policy Session RD6 -** **Policy Session RD7 - Use additional space for recording more Resource Domains.**

3.5 DIAMETER NETWORK CHECK

3.5.1 Diameter Network Check for Policy DRA

NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION

SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY

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

Procedure 4: Record Required P-DRA Diameter Configuration

S T E P #	This procedure gathers and records PCA – Policy DRA function Diameter Configuration. Please refer to the Diameter User's Guide[7] for details of paremeters required for configuring Diameter 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 (PCEFs, BBERFs and AFs) and policy servers (PCRFs) in the network. 3. Identify and log the diameter attributes for all the policy clients and policy servers in the network – FQDN, Realm, IP address. 4. Identify and log the type of diameter Transport Protocol needed for all the policy clients and policy Servers - TCP/SCTP 5. Identify and log the type of diameter connection mode needed for all the policy clients and policy server- Responder/Initiator/Responder-Initiator 6. Identify and log the 'Peer Node 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 and Policy Clients. Routing configuration is required for Policy Clients if the Policy Servers send Diameter request messages to be routed to the Policy Clients. 8. Identify and log the Policy Server configuration needed – Both Gx and Rx on same Policy Server or are they on different servers. 9. Identify and log the number of peer route tables needed for the diameter configuration – e.g. one for Rx Policy Servers and One for Gx Policy Servers . 10. Identify and log the number of Application Route Table entries – one for Gx Application and one for Rx Application message processing. 11. Identify and log the TSA used for local nodes if IPFE is used.
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. Note that PCRF Sub Pool Selection Rules are optional. 4. Identify and log the **General Options** parameters for the Policy DRA network – Default Stale Session Timeout Binding Audit Session Query Rate Audit Operation Rate 5. Identify and log the **Network Wide Options** parameters for the Policy DRA network – Early Binding Options Topology Hiding Options Suspect Binding Removal Options Session Integrity Options 6. Identify and log the Alarm Settings for "**DSR Application ingress Message Rate**". 7. Identify and log the Congestion Alarm Thresholds and Message Throttling Rules
3 ☐	Policy DRA Site Configuration (SO scoped)	1.Identify and log the all the PCRFs handling the Policy Traffic for this site. 2.Identify and log the **Binding Key Priority** settings, i.e. the order in which subscriber keys (IMSI, MSISDN, IPv4, IPv6) will be used to correlate binding dependent session creation

		messages and route them to final bound PCRFs. 3. Identify and log the Policy Clients for which the topology hiding is needed. 4. Identify and log the PCRF Pool to PRT mapping configuration. 5. Identify and log the error code configuration for each of the 'Error Condition' in the table per the policy client team request/ inteoperability requirements for Policy Client Vendor. 6. Identify and log the Suspect Binding Removal Rules. 7. Identify and log the Site Options parameters.for this site.

3.5.2 Diameter Network Check for Online Charging DRA

NOTE: EXECUTE THIS PROCEDURE FOR ONLINE CHARGING DRA FUNCTION

SKIP THIS PROCEDURE IF POLICY DRA FUNCTION ONLY

Procedure 5: Record Required OC-DRA Diameter Configuration

S T E P #	This procedure gathers and records 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 (CTFs) and Online Charging servers (OCSs) in the network. 3. Identify and log the diameter attributes for all the Online Charging clients and Online Charging servers in the network – FQDN, Realm, IP address. 4. Identify and log the type of diameter Transport Protocol needed for all the Online Charging clients and Online Charging servers - TCP/SCTP 5. Identify and log the type of diameter connection mode needed for all the Online Charging clients and Online Charging servers - Responder/Initiator/Responder-Initiator 6. Identify and log the 'Peer Node 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 **General Options** parameters for the Online Charging DRA network – Default Stale Session Timeout Audit Operation Rate 4. Identify and log the Online Charging Network Realms to be configured for Session State maintenance. 5. Identify and log the **Network Wide Options** for the Online Charging DRA network – Session State Options OCS Selection Options 6. Identify and log the Alarm Settings for "**DSR Application ingress Message Rate**". 7. Identify and log the Congestion Alarm Thresholds and Message Throttling Rules
3 ☐	Online Charging 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 for the Gy/Ro interface.

3.6 PERFORM HEALTH CHECK

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

Procedure 6: Perform Health Check (PCA configuration Preparation)

S T E P #	This procedure performs a Health Check. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	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 Oracle Support for assistance as necessary.
2 ☐	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 before proceeding with the configuration in below sections.

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

4.1 PLACE ASSOCIATIONS CONFIGURATION

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

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

- Policy and Charging Mated Sites

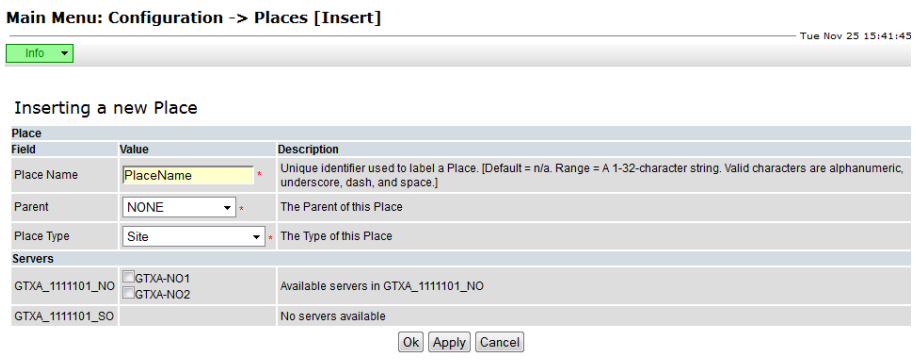
The following type of Place Association is required for Policy DRA function ONLY:

- Policy Binding Region

4.1.1 Policy and Charging Places

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

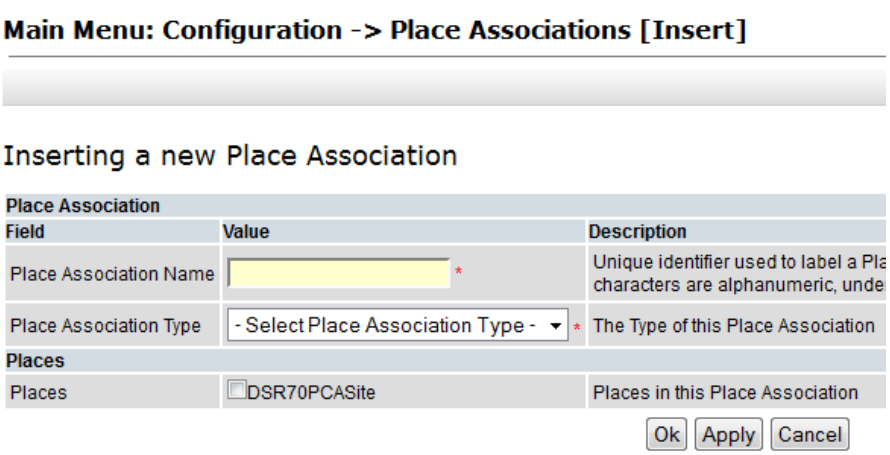
Procedure 7: Policy and Charging Places configuration

S T E P #		
	This procedure configures the Places. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR 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 all DAMP servers (running PCA) and all SBR servers that belong to this Place (DSR Site). 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 8: Policy and Charging Mated Sites Place Associations configuration

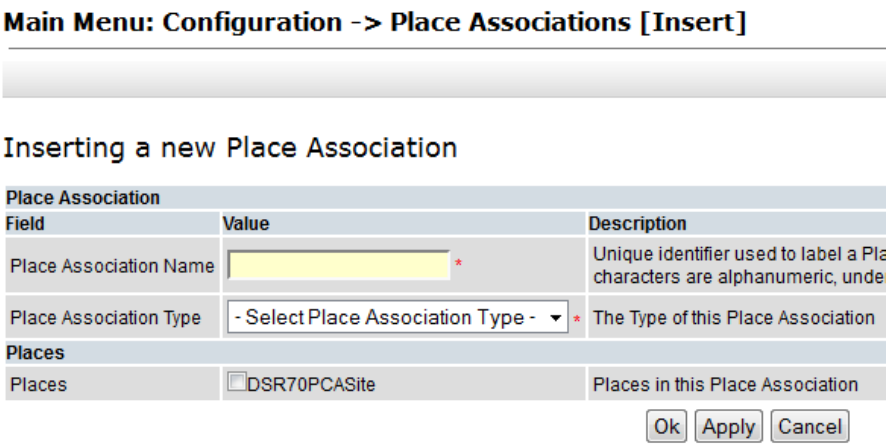
S T E P #	This procedure configures Place Association Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**. **ASSUMPTION: PCA FEATURE IS ALREADY ACTIVATED 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. Please use the data recorded in Section 3.4. 4. Click **Ok**.
4 ☐	**NOAM VIP:** Add other Policy and Charging Mated Sites Place Associations.	Repeat Step 3 for all other Policy and Charging Mated Sites Place Associations that are to be added

4.1.3 Policy Binding Region Place Associations

NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION

SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY

Procedure 9: Policy Binding Region Place Associations configuration

S T E P #	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 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 Binding Region 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:

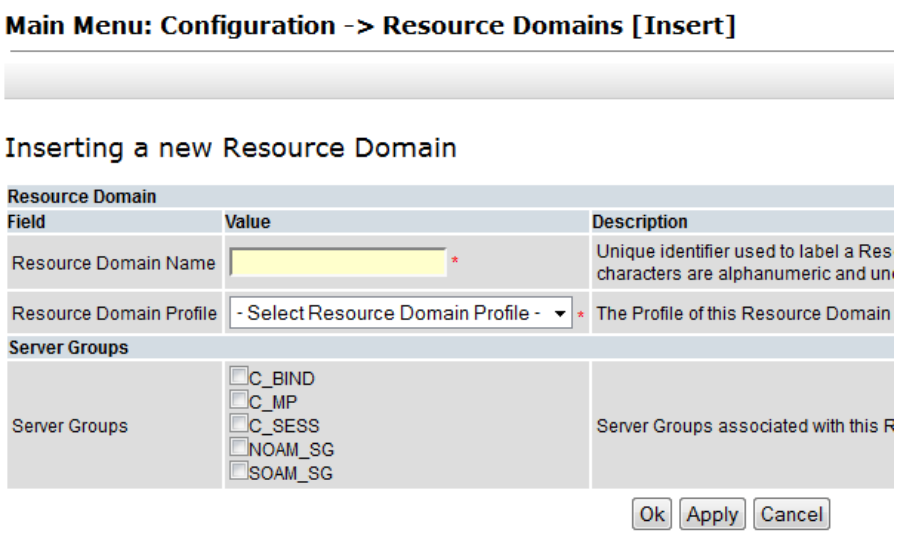
- Policy and Charging DRA
- Policy Session

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

- Policy Binding

4.2.1 Policy and Charging DRA Resource Domain Configuration

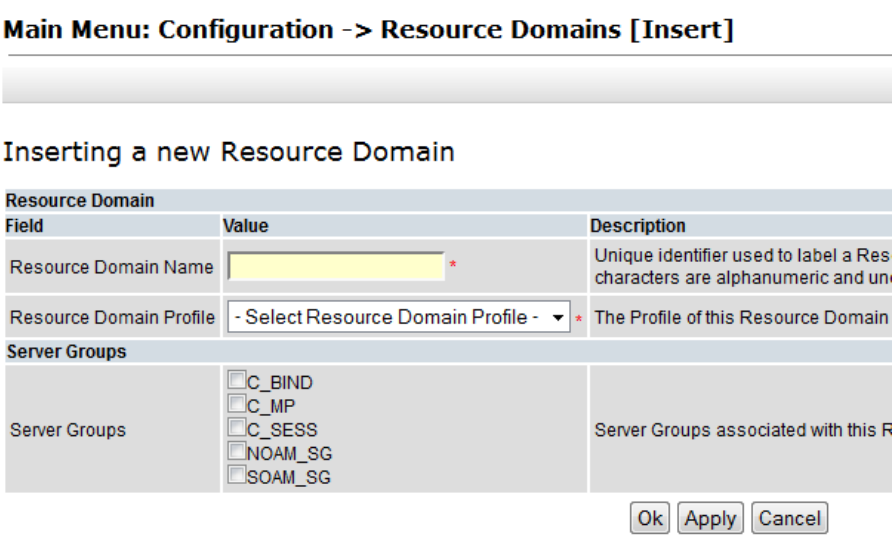
Procedure 10: Policy and Charging DRA Resource Domain configuration

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 Mated DSR Triplets, create one Policy and Charging DRA Resource Domain and add the DA-MP Server Groups from three sites into this Policy and Charging DRA Resource Domain.** **For non-mated pair DSRs and standalone DSR: Configure a Policy and Charging DRA Resource Domain per Site.**
4 ☐	**NOAM VIP:** Add other Policy and Charging DRA Resource Domains.	Repeat Step 3 for all other Policy and Charging DRA Resource Domains that are to be added.
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.

4.2.2 Policy Session Resource Domain Configuration

Procedure 11: Policy Session Resource Domain configuration

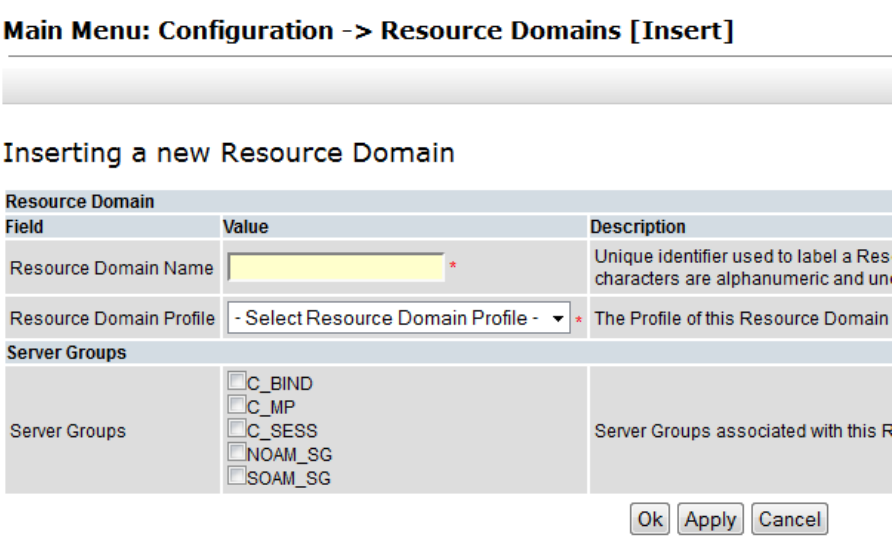
S T E P #	This procedure configures the Policy Session Resource Domain Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**. **ASSUMPTION: PCA FEATURE IS ALREADY 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 and Charging SBR Server Groups from both sites that will be hosting the Session SBR Database for the Mated Pair into this Policy Session Resource Domain. **For Mated DSR triplets, create one Policy Session Resource Domain and add all the Policy and Charging SBR Server Groups from three sites that will be hosting the Session SBR Database for the Mated triplet into this Policy Session Resource Domain.** **For non-mated pair DSRs and standalone DSR: Configure a Policy Session Resource Domain per site and add all the Policy and Charging SBR Server Groups in the site that will be hosting the Session SBR Database.**
4 ☐	**NOAM VIP:** Add other Session Resource Domains.	Repeat Step 3 for all other Policy Session Resource Domains that are to be added.

4.2.3 Policy Binding Resource Domain Configuration

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

Procedure 12: Policy Binding Resource Domain configuration

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 all the Policy and Charging SBR Server Groups from all sites that will be hosting the Binding SBR Database into this Policy Binding Resource Domain.**

4.3 DIAMETER CONFIGURATION PROCEDURES

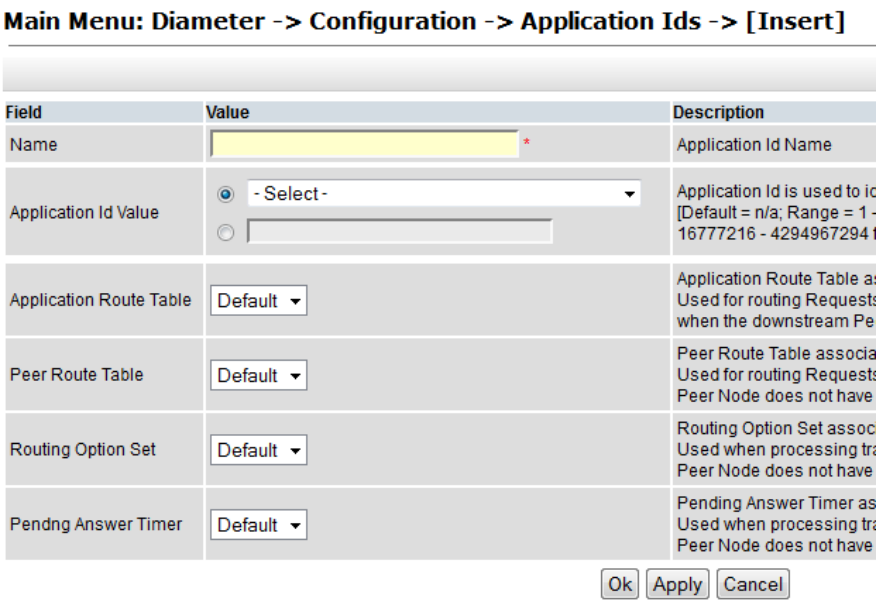
4.3.1 Diameter Configuration for Policy DRA

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

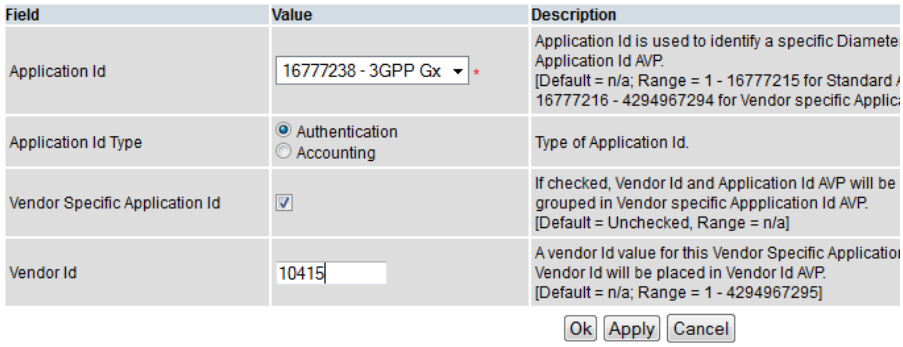
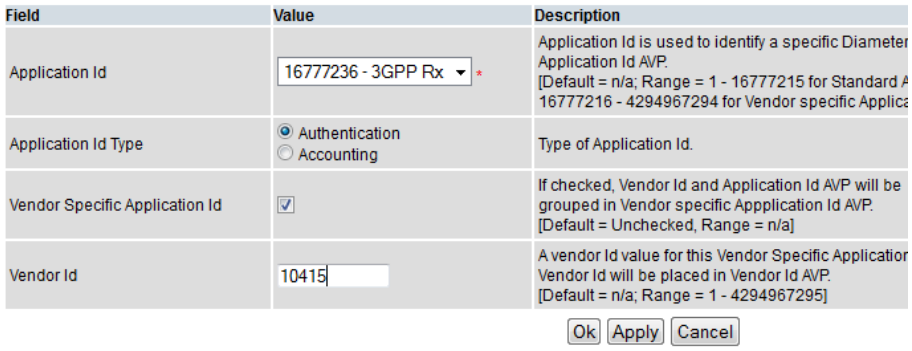
Procedure 13: Diameter configuration for Policy DRA

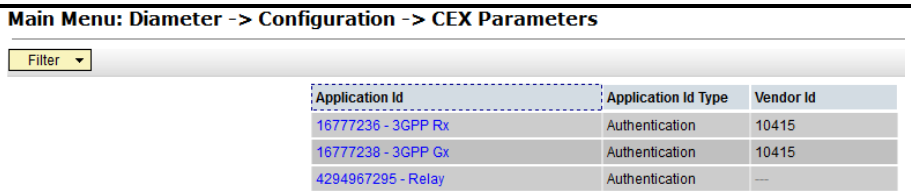
NOTE: EXECUTE THIS PROCEDURE FOR POLICY DRA FUNCTION

SKIP THIS PROCEDURE IF ONLINE CHARGING DRA FUNCTION ONLY

STEP #		
	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 - 3GPP Gx" (This will automatically fill in the "Name" field, please make changes to the name as necessary). 2. Click **Ok**. NOTE: This Application-Id is also used for Gx-Prime interface.

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 f Application Route Table — Default — Application Route Table a: 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 - 3GPP Rx" 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, 16777266 (for 3GPP Gxx) etc.
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]  Field / Value / Description Application Id — 16777238 - 3GPP Gx * — Application Id is used to identify a specific Diameter Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Standard A 16777216 - 4294967294 for Vendor specific Applic Application Id Type — Authentication / Accounting — Type of Application Id. Vendor Specific Application Id — checked — If checked, Vendor Id and Application Id AVP will be grouped in Vendor specific Appplication Id AVP. [Default = Unchecked, Range = n/a] Vendor Id — 10415 — A vendor Id value for this Vendor Specific Applicatio Vendor Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295] Ok Apply Cancel 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]**  Field / Value / Description Application Id — 16777236 - 3GPP Rx * — Application Id is used to identify a specific Diameter Application Id AVP. [Default = n/a; Range = 1 - 16777215 for Standard A 16777216 - 4294967294 for Vendor specific Applic Application Id Type — Authentication / Accounting — Type of Application Id. Vendor Specific Application Id — checked — If checked, Vendor Id and Application Id AVP will be grouped in Vendor specific Appplication Id AVP. [Default = Unchecked, Range = n/a] Vendor Id — 10415 — A vendor Id value for this Vendor Specific Applicatior Vendor Id will be placed in Vendor Id AVP. [Default = n/a; Range = 1 - 4294967295] Ok Apply Cancel 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, 3GPP Gxx, etc.
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.



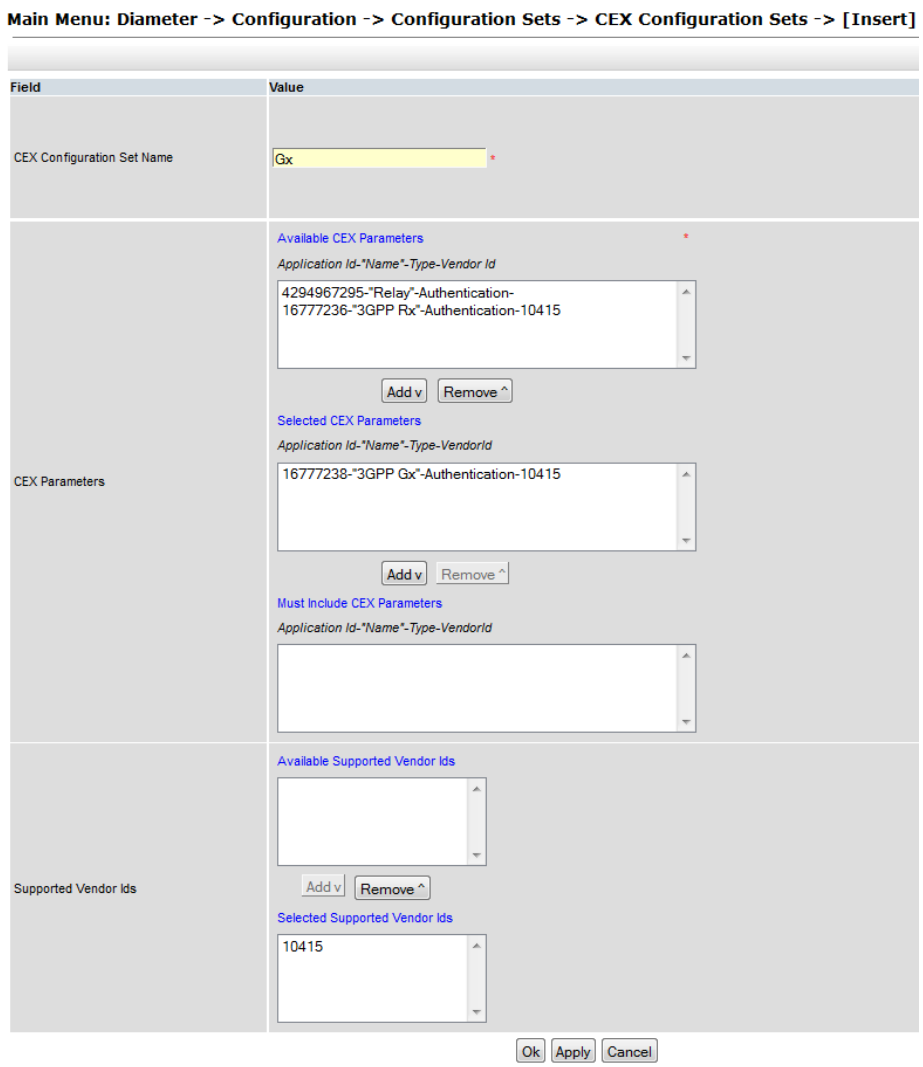
12 **SOAM VIP:** Navigate to CEX Configuration Sets screen

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.

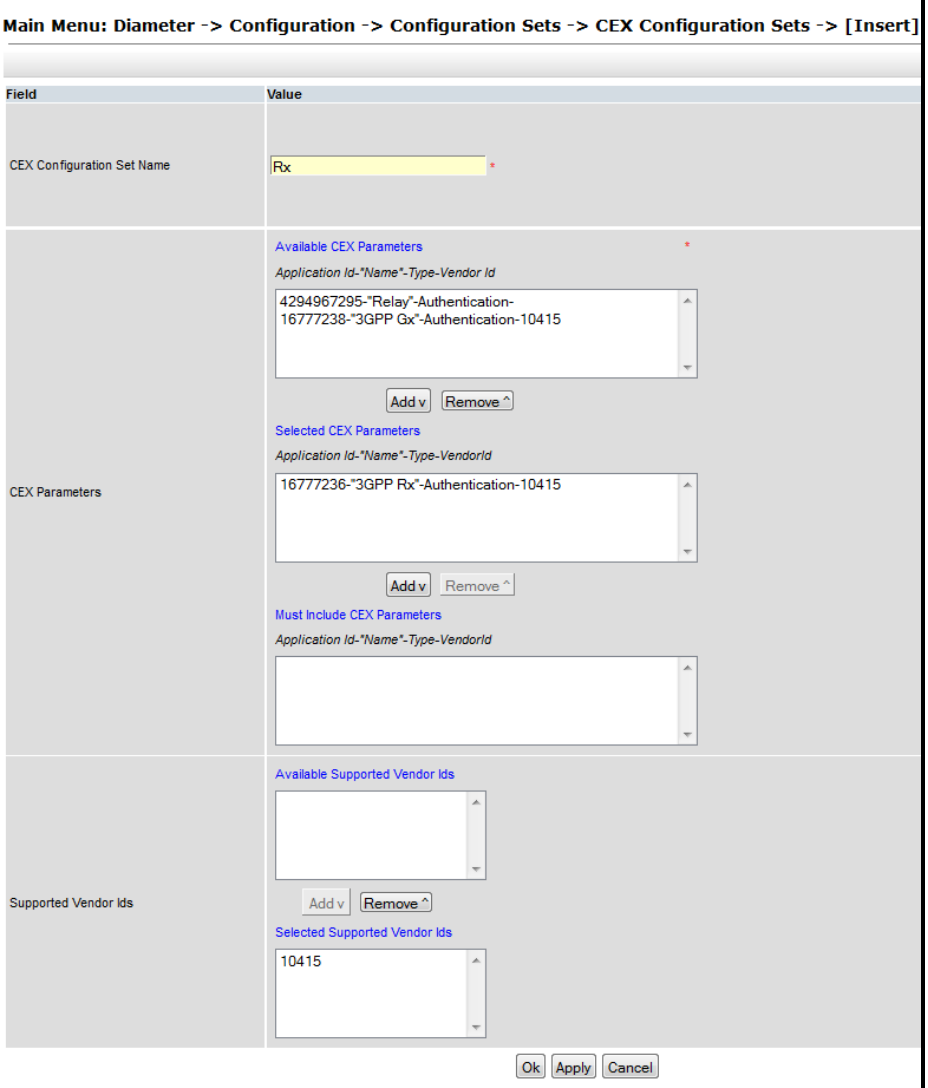
You will see a screen similar to:

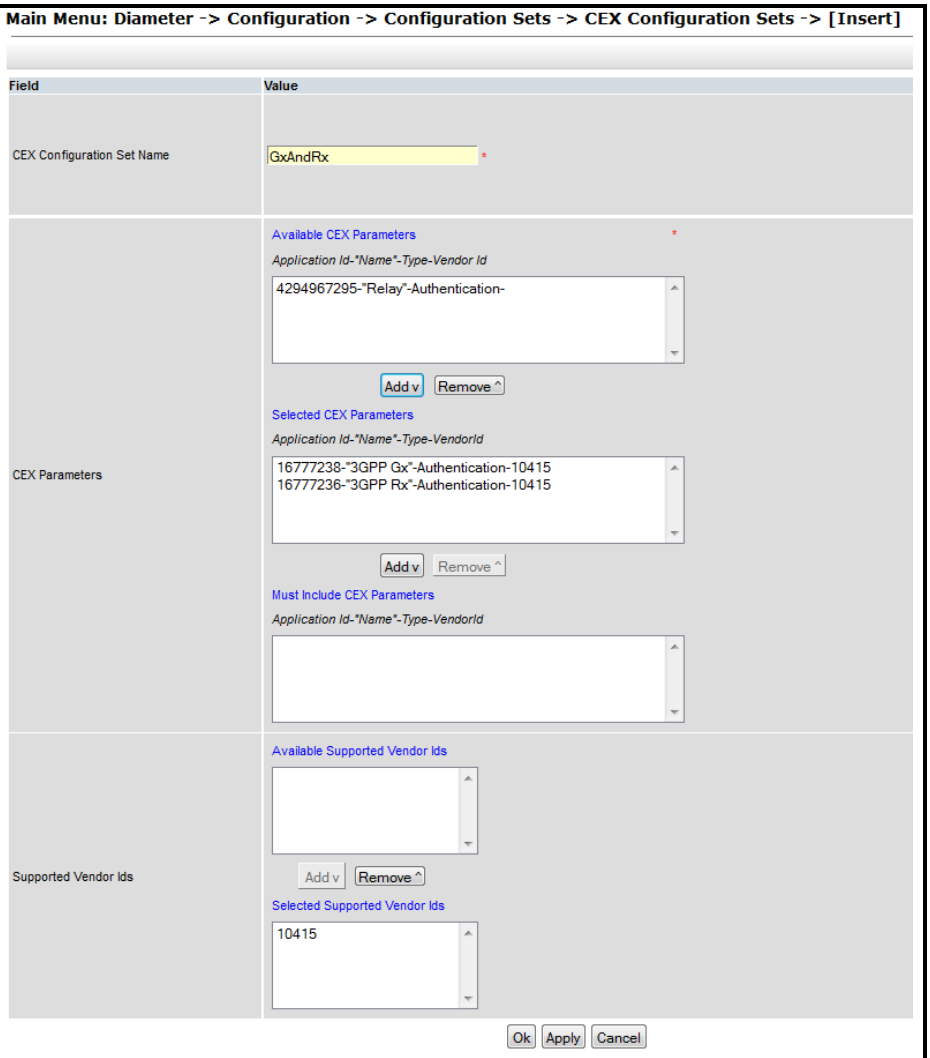


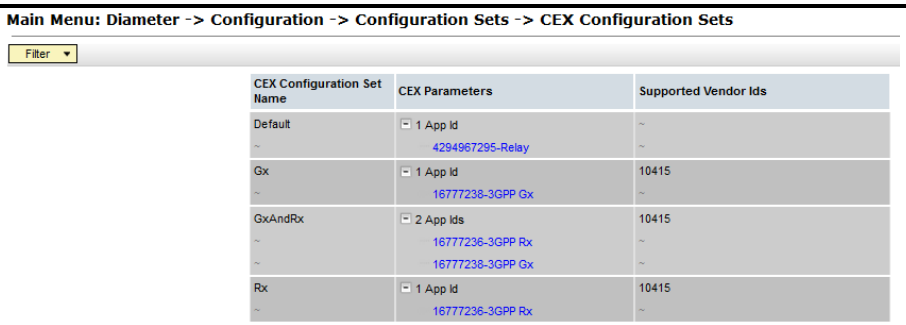
1. Enter the CEX Configuration Set Name “Gx”
2. Select the 3GPP Gx Application Id “16777238” from Available Application Ids
3. Click **Add** just below the list
4. Select the Vendor Id “10415” from Available Supported Vendor Ids
5. Click **Add** just below that list
6. Click **Ok**.

14 **SOAM VIP:** Configure the CEX Configuration

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

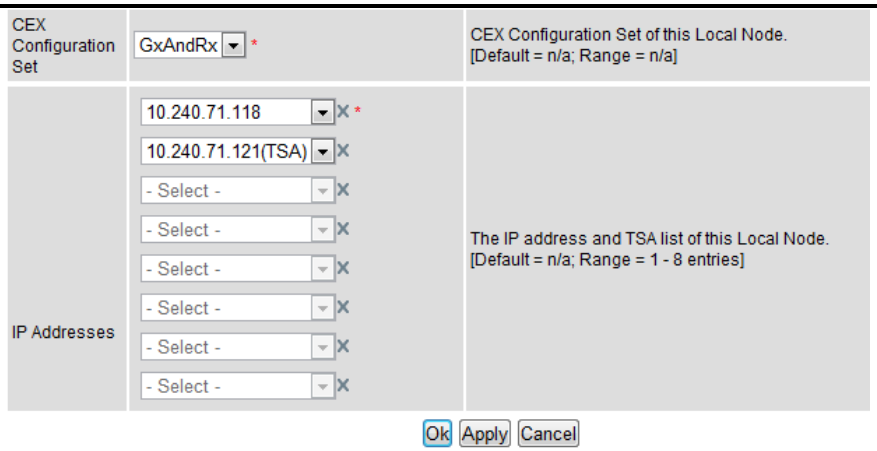
	Set to be used for Connections with the AF nodes.	You will see a screen similar to:  **Main Menu: Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets -> [Insert]** Field / Value CEX Configuration Set Name: Rx * CEX Parameters: Available CEX Parameters * *Application Id-"Name"-Type-Vendor Id* 4294967295-"Relay"-Authentication- 16777238-"3GPP Gx"-Authentication-10415 Add v Remove ^ Selected CEX Parameters *Application Id-"Name"-Type-VendorId* 16777236-"3GPP Rx"-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 "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:

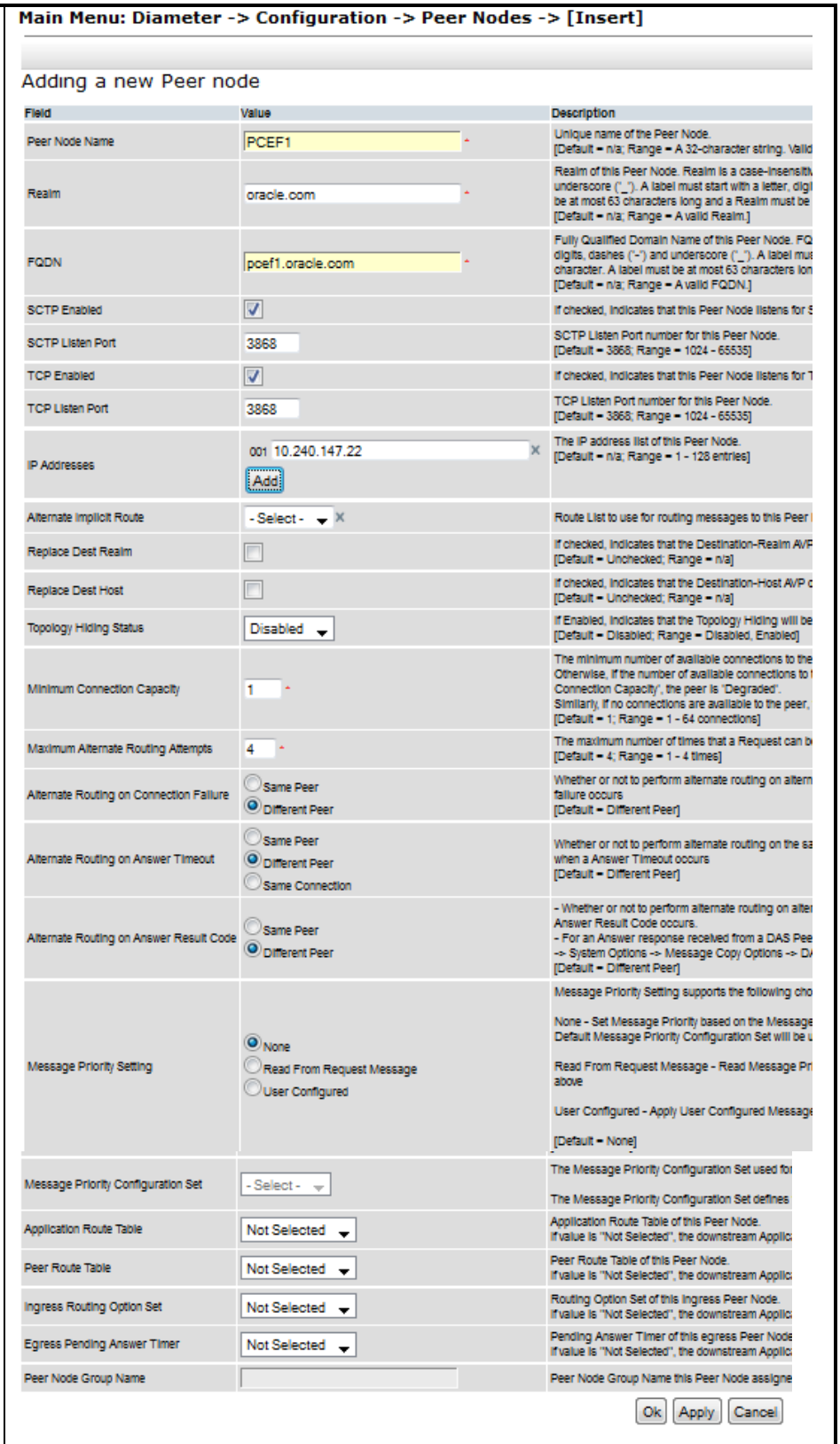
		 1. Enter the CEX Configuration Set Name "GxAndRx" 2. Select the 3GPP Gx Application Id "16777238" and 3GPP Rx Application Id "16777236" from Available Application Ids 3. Click **Add** just below the list 4. Select the Vendor Id "10415" from Available Supported Vendor Ids 5. Click **Add** just below that 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]

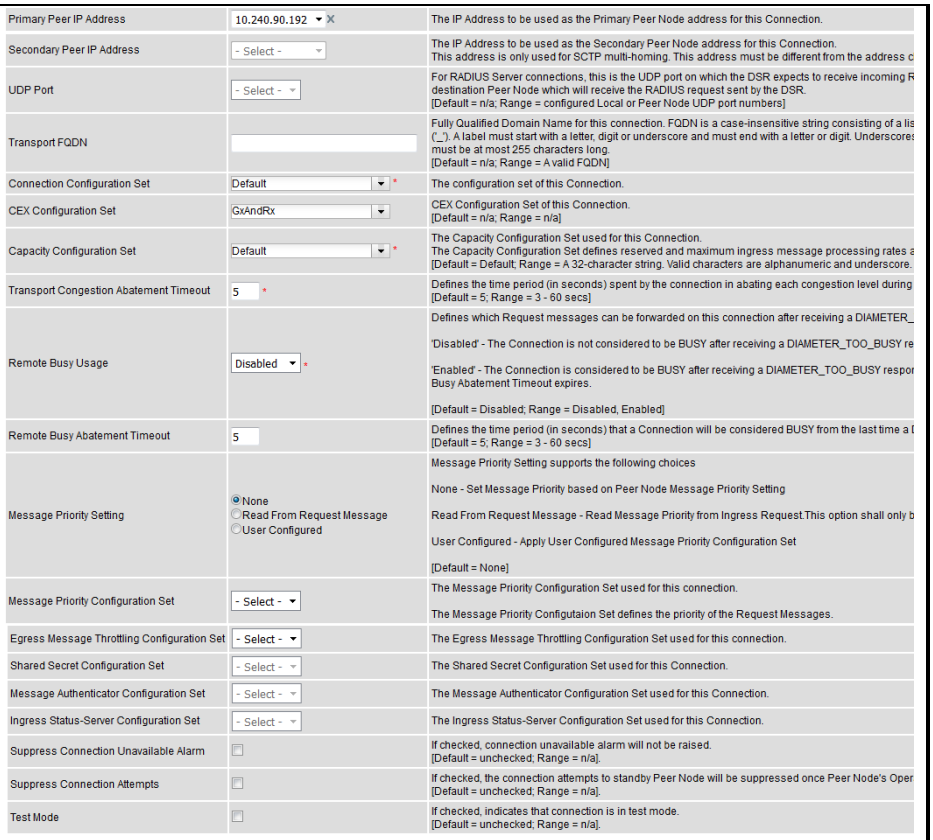
		 1. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values) 2. Click **Ok**. **NOTE:** The drop down list of IP address should contain the XSI addresses configured on DSR MP Servers. If not found then Installation may be incomplete/incorrect, 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:

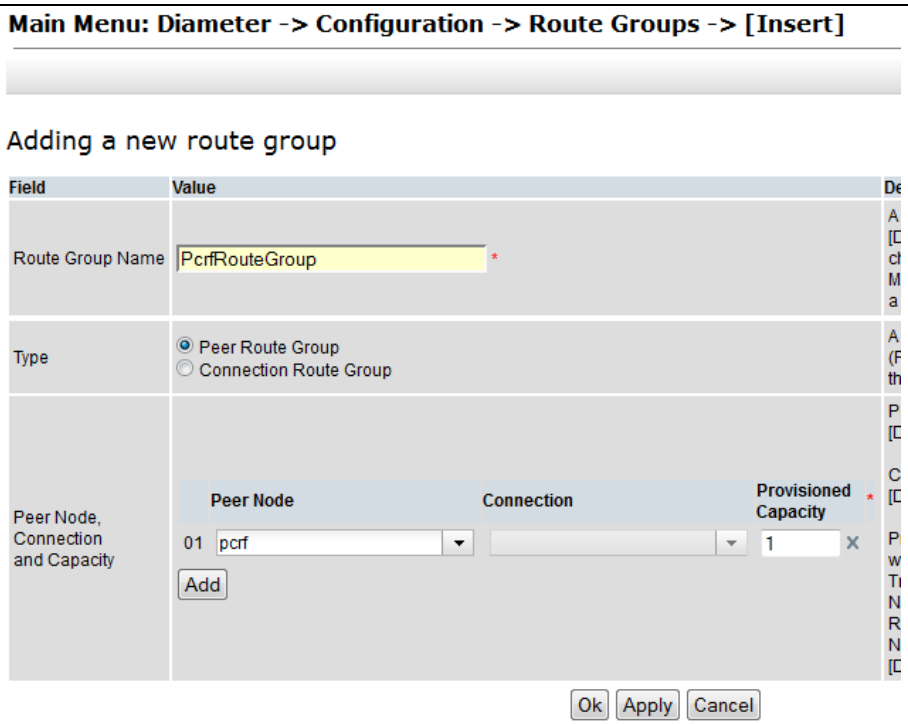


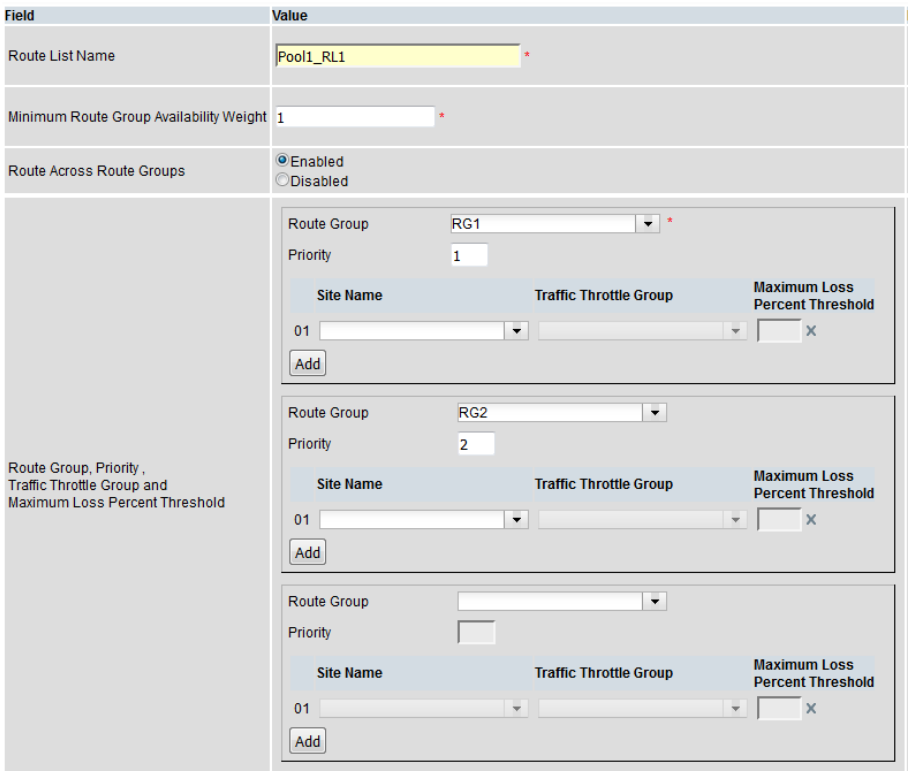
3. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values)

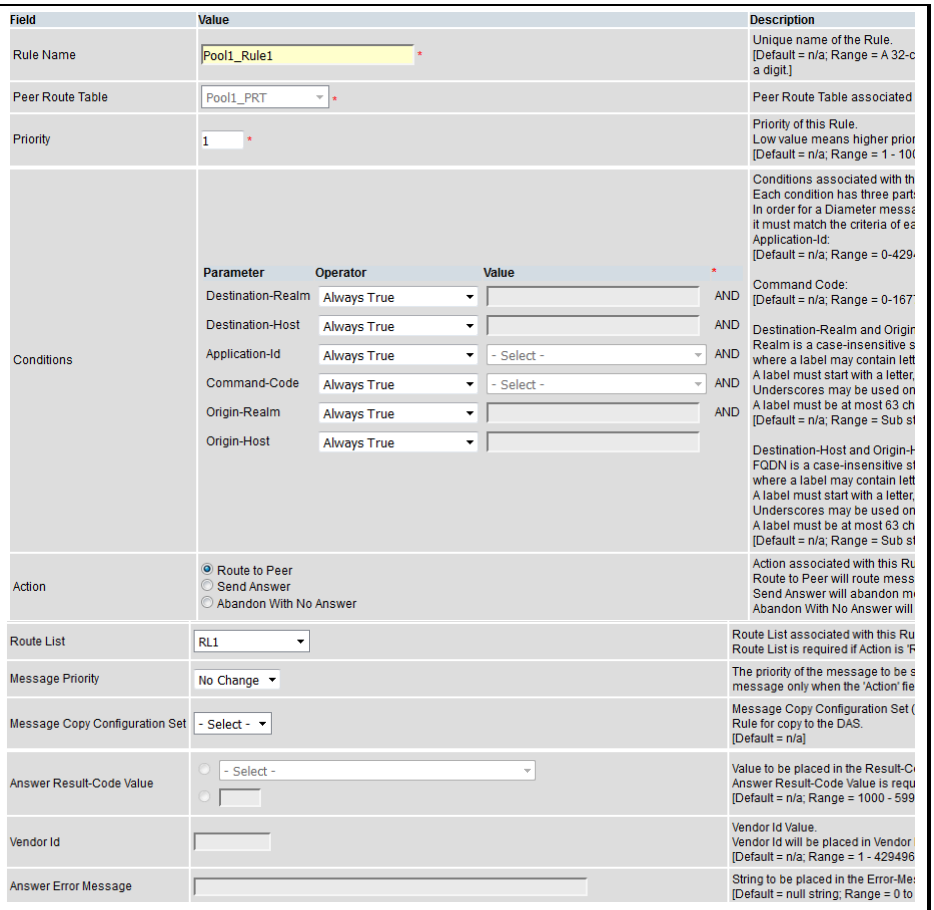
Note:

		- For Peer Nodes that are PCRFs, the “Replace Dest Host” and “Replace Dest Realm” check boxes MUST be checked. - “Topology Hiding Status” field is not applicable for PCA and should remain disabled. - The “Application Route Table” may apply for Peer Nodes that are Policy Clients. - The “Peer Route Table” field may be populated to route to Shared State PCRFs. - For mode details on the fields and routing configuration please consult the Diameter User’s Guide [7] 2. Click **Ok**.
23	**SOAM VIP:** Configure other Peer Nodes	Repeat Step 22 to configure other peer nodes (PCEFs, AFs, BBERFs, PCRFs 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: **Field** / **Value** / **Description** Connection Name: PCRF1_Connection1 * — A name that uniquely identifies the Connection. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric AAA Protocol: Diameter * — The AAA protocol for this Connection, which defines the Connection as Diameter [Default = N/A; Range = Diameter or RADIUS] Transport Protocol: SCTP / TCP / TLS/TCP / DTLS/SCTP / UDP — The Transport Protocol used by this Connection. The protocol should be supported by both Local Node and Peer Node. Note: IPSEC should not be enabled if Connection is configured with TLS/TCP or significant performance impact. Connection Mode: Initiator Only * — Initiator Only indicates that Local Node will only initiate the connection to the Pee Responder Only indicates that Local Node will only respond to the connection in Initiator & Responder indicates that Local Node will initiate connection in additio RADIUS Server indicates that the Local Node receives incoming RADIUS reques RADIUS Client indicates that the Local Node sends RADIUS requests to a Peer [Default = Initiator & Responder; Range = n/a] Local Node: PCA * — The Local Node of this Connection. Local Initiate Port: — The Local Initiator Port of this Connection. [Default = n/a; Range = 1024 - 49151] Primary Local IP Address: 10.240.71.108 (PDRAB3SiteA) * — The IP Address to be used as the Primary Local Node address for this Connecti Secondary Local IP Address: - Select - — The IP Address to be used as the Secondary Local Node address for this Conne This address is only used for SCTP multi-homing. This address must be differe IPFE Initiator DAMP: - Select - — The DA-MP that will be used to initiate connections using the IPFE TSA address. Peer Node: PCRF1 * — The Peer Node of this Connection. Peer Node Identification: None / IP Address / Transport FQDN / Peer Diameter Identity FQDN — Specifies how Node will derive the peer node's IP address(es) when initiating a connection from the peer. None - Use option None for this connection when responding to a connection fr IP Address - Use the remote IP address(es) configured for this Connection whe the peer. Transport FQDN - Use the DNS resolved Transport FQDN address configured f responding to a connection from the peer. Peer Node FQDN - Use the DNS resolved FQDN address configured for the Pee address(es) when responding to a connection from the peer.

		 4. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). Note: Please refer to the Diameter User's Guide [7] for details on fields in this screen. 5. Click **Ok**. **NOTE:** Make sure the IPFE configuration matches the protocol which is selected in this step.
26	**SOAM VIP:** Configure all other connections with Peer nodes	Repeat Step 25 to configure all other required DIAMETER connections.
27	**SOAM VIP:** Configure Route Groups	PCRF Pooling allows the user to set up routing to PCRFs in groups. APNs can be mapped to such groups of PCRFs (called PCRF Pools). Each PCRF Pool can be mapped to a PRT that points to a Route List that points to prioritized Route Groups. Primary and Alternate Route Groups can be set up within each PCRF Pool by creating separate Route Groups and assigning appropriate priority when configuring the Route List. Please refer to the Diameter User's Guide [7] for more information on Diameter Routing.
28	**SOAM VIP:** Create a primary Route Group for the first PCRF Pool	Navigate to **Main Menu -> Diameter -> Configuration -> Route Groups** Click on **Insert** in the lower left corner. You will see a screen similar to:

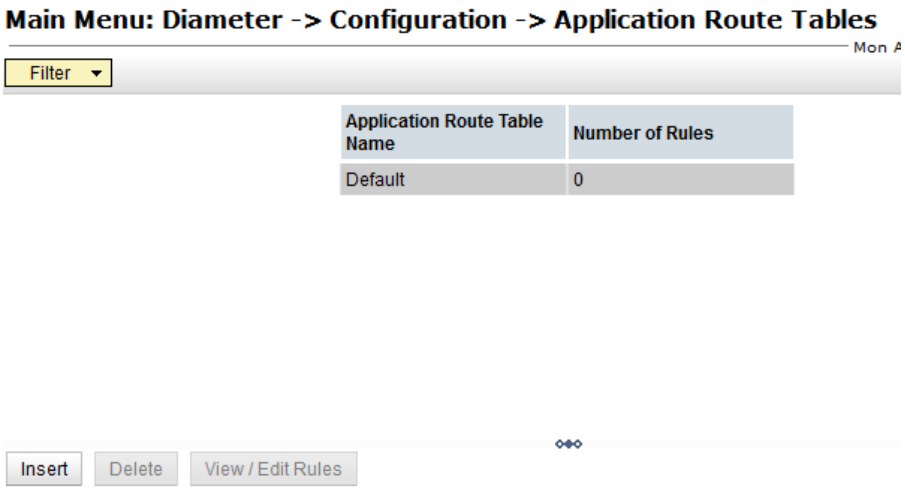
		 1. Enter the Route Group name. 2. Select the Peer Node name (PCRF name). 3. If more PCRFs need to be added, click on "Add" and repeat step 2. 3. Enter the provisioned capacity as required. 4. Click Ok.
29	**SOAM VIP:** Configure alternate Route Group(s) for the **same** PCRF Pool.	**OPTIONAL** If alternate Route Group(s) are planned, repeat step 28 for all such Route Groups.
30	**SOAM VIP:** Configure Route List for the first PCRF Pool.	Navigate to **Main Menu -> Diameter -> Configuration -> Route Lists** Click on **Insert** in the lower left corner. You will see a screen similar to:

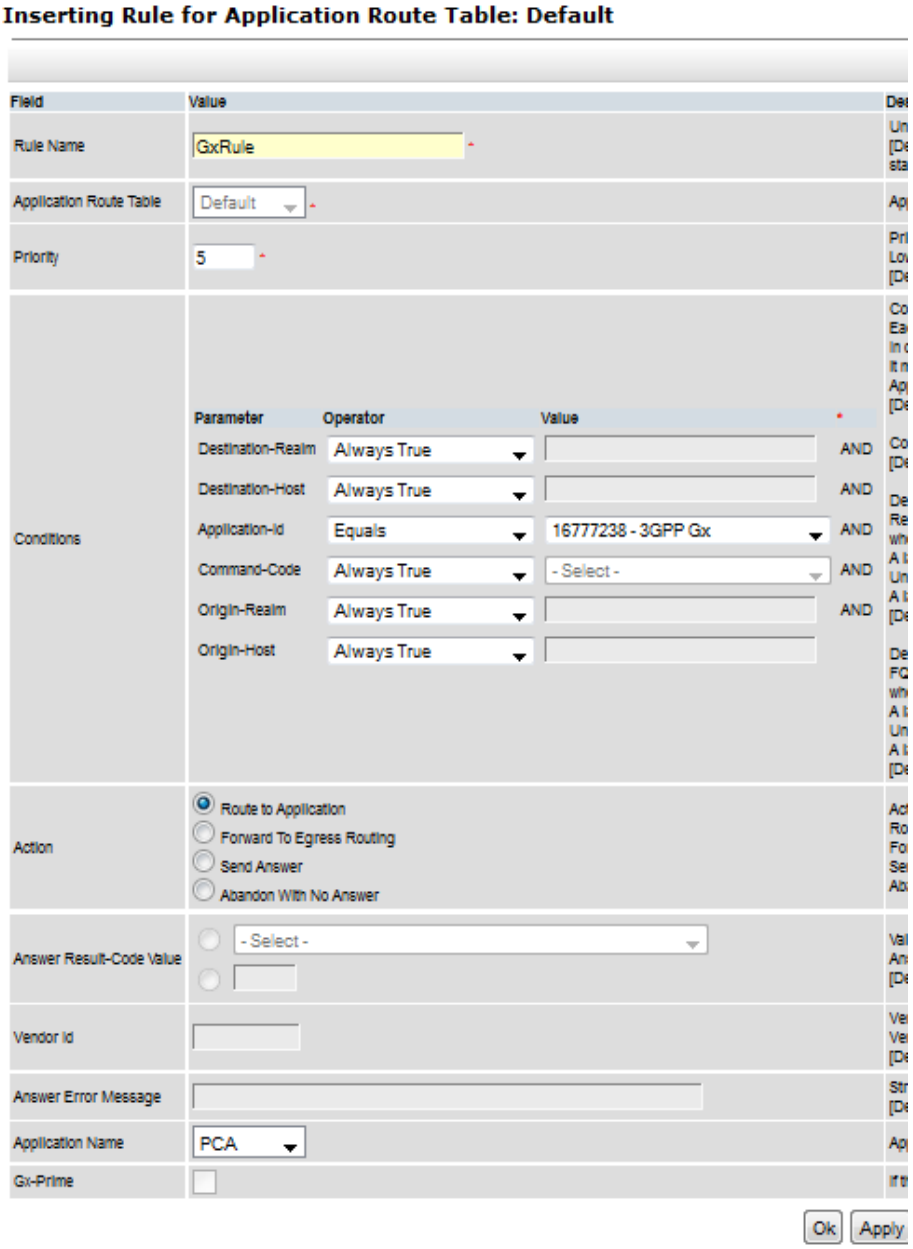
		 1. Enter the Route List name. 2. Set the Minimum Route Group Availability Weight as needed. 3. Select the Route Group(s) configured in the previous two steps and set their desired priorities. 4. Set any other parameters desired (for e.g. Maximum Loss Percent Threshold etc.) 5. Click Ok.
31	**SOAM VIP:** Configure the Peer Routing Rules for the first PCRF Pool.	Configure the PRT such that DSR forwards messages based on the PCRF Pool selected by PCA. Navigate to **Main Menu -> Diameter -> Configuration -> Peer Route Table** Click on **Insert** in the lower left corner. You will see a screen similar to:  1. Enter the Peer Route Table name. 2. Click Ok.
32	**SOAM VIP:** Configure Routing Rules for the first PCRF Pool	Click on **Insert** in the lower left corner. You will see a screen similar to:



1. Enter the Rule name.
2. Set the Priority of the Rule as needed (preferably 1).
3. Select “Always True” for all Condition Parameters. You may base the PCRF Pool routing on some condition parameter in special use cases for example Origin-based routing.
3. Select the Route List configured in step 30.
4. Click `Ok`.

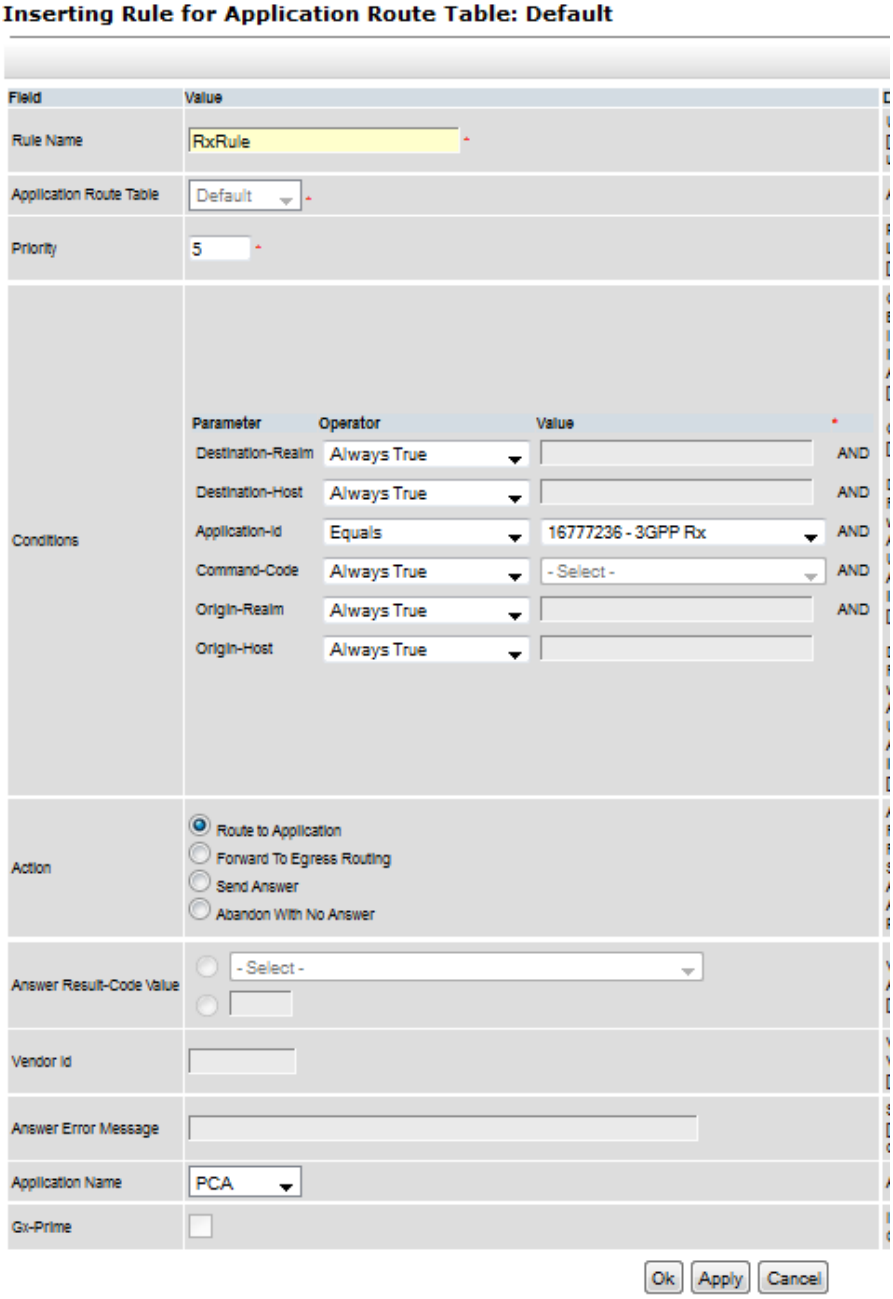
33	**SOAM VIP:** Configure Routing for other PCRF Pools.	`If more, PCRF Pools are planned in the Diameter network, r`epeat steps 28 through 32 for other PCRF Pools' Routing
34	**SOAM VIP:** Configure Routing for in-session Diameter messages	**OPTIONAL** If required, configure the routing for messages where Destination Host is present in the Diameter messages (typically in-session messages). **CAUTION** In-session messages or session creation messages that follow a final subscriber binding, destined for a particular Destination Host (PCRF) can be routed to alternate PCRFs only when such PCRFs share state information. Doing so for PCRFs that do not share state information may result in call failures or split-bindings.
35	**SOAM VIP:** Configure inter DSR Routing	**OPTIONAL** If Diameter messages need to be routed in between DSR sites (nodes), set up the routing as needed. This is likely in 3-site redundancy deployments because many PCEFs likely only support primary and secondary connections. In such deployments routing can be set up between the three sites.

36	**SOAM VIP:** Configure Routing for Gx RAR messages	**OPTIONAL** Configure the Routing Rules to route a Gx RAR message generated at one site that is destined for a PCEF connected to another site. This is likely in 3-site redundancy deployments because many PCEFs likely only support primary and secondary connections. In such deployments routing can be set up between the three sites. TIP: Destination-Host based routing can be set up to route the Gx RAR messages to the appropriate site's DSR.
37	**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.
38	**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**.

39	**SOAM VIP:** Configure the ART for Rx Interface messages	Click on **Insert** in the lower left corner. You will see a screen similar to:



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

40	**SOAM VIP:** Configure the ART for all other Interfaces	Repeat Step 38 for any other Application Id that needs to be routed to the PCA Application by Diameter Routing Layer.

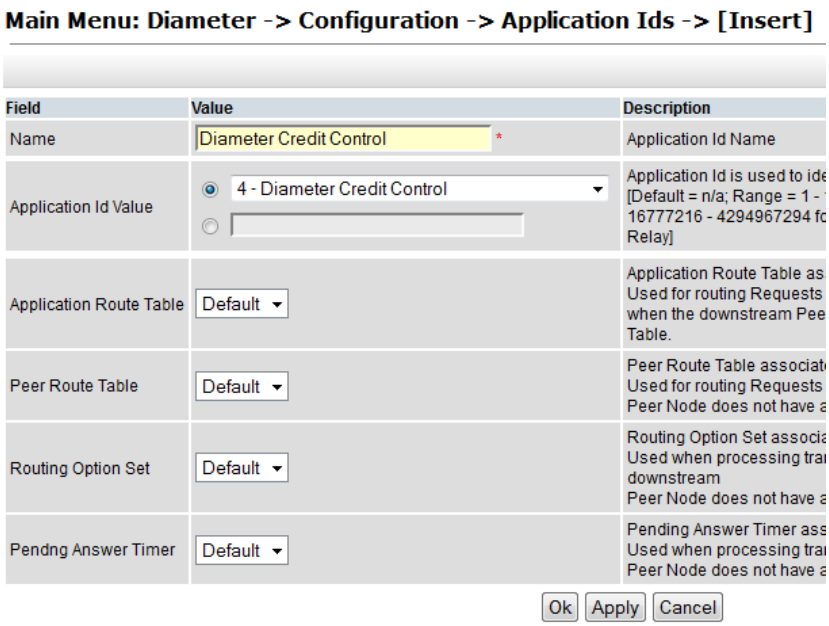
4.3.2 Diameter Configuration for Online Charging DRA

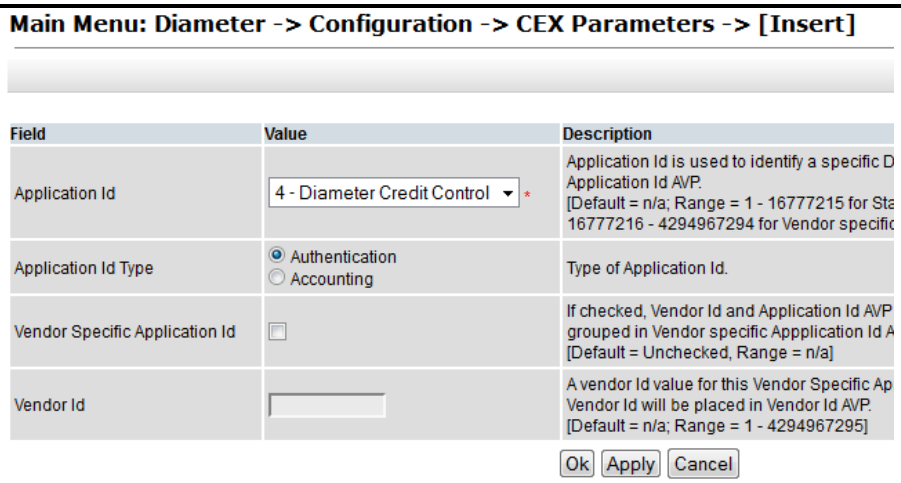
Detailed steps are given in the procedure below.

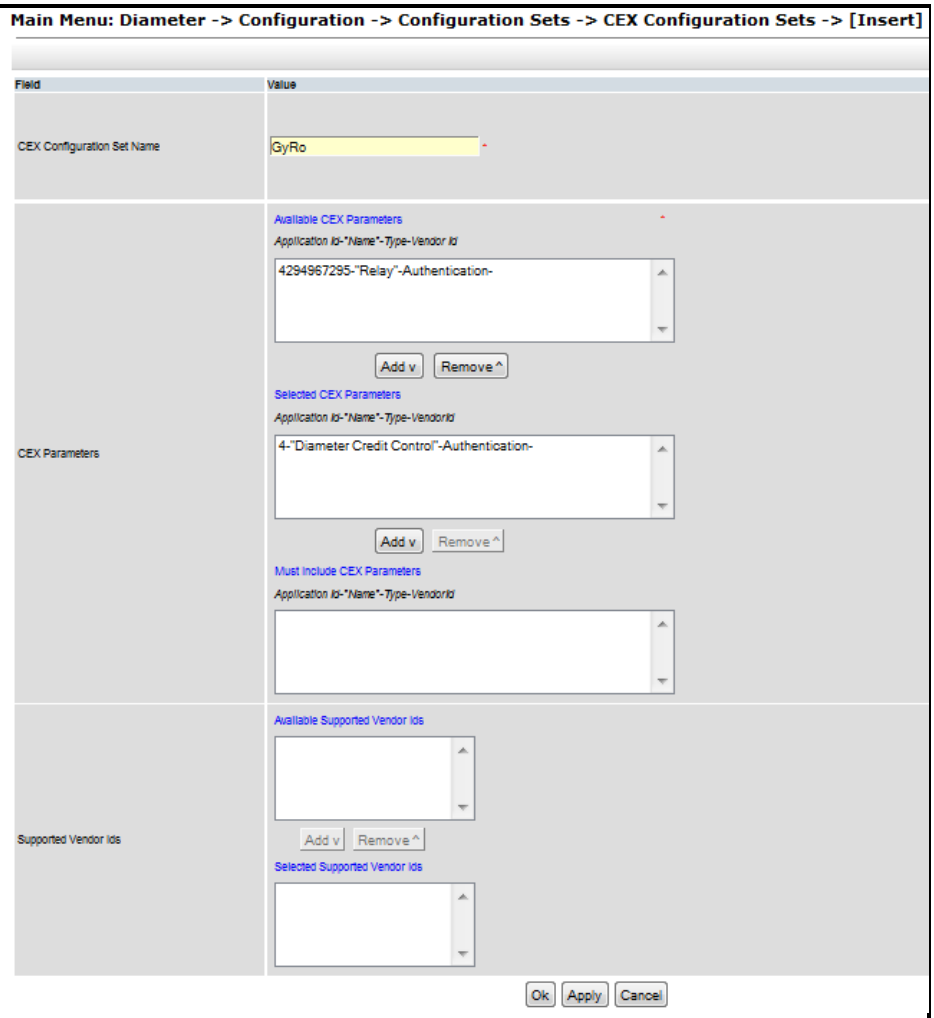
Procedure 14: Diameter configuration for Online Charging DRA

NOTE: EXECUTE THIS PROCEDURE FOR ONLINE CHARGING DRA FUNCTION

SKIP THIS PROCEDURE IF POLICY DRA FUNCTION ONLY

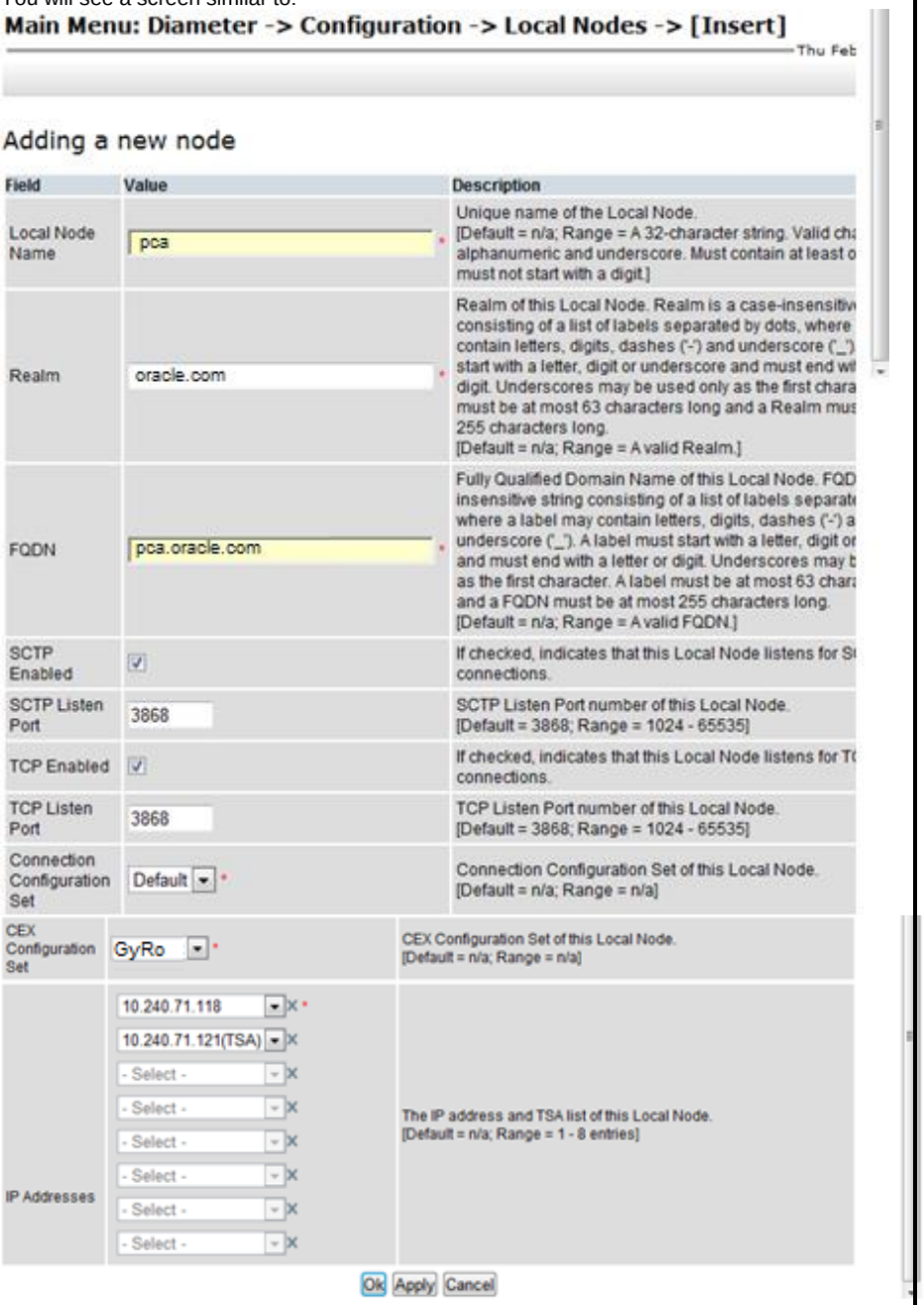
S T E P #	This procedure configures the Diameter stack. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	Establish GUI Session on the SOAM VIP	Establish 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:

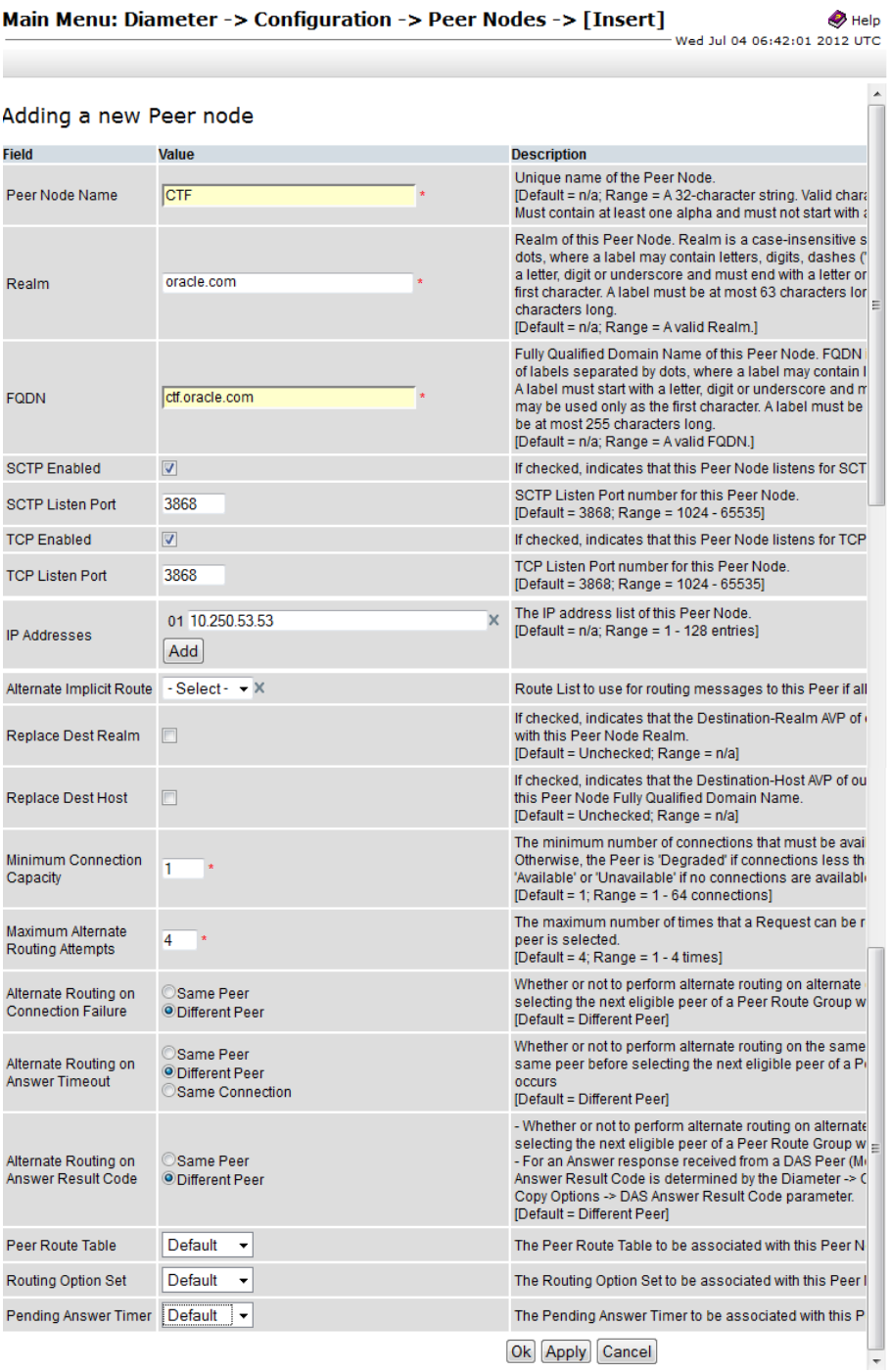
		 1. Select Application Id "4 – Diameter Credit Control". 2. Click **Ok**.
6	**SOAM VIP:** Navigate to CEX Configuration Sets screen	Navigate to **Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets**
7	**SOAM VIP:** Configure the CEX Configuration set to be used for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



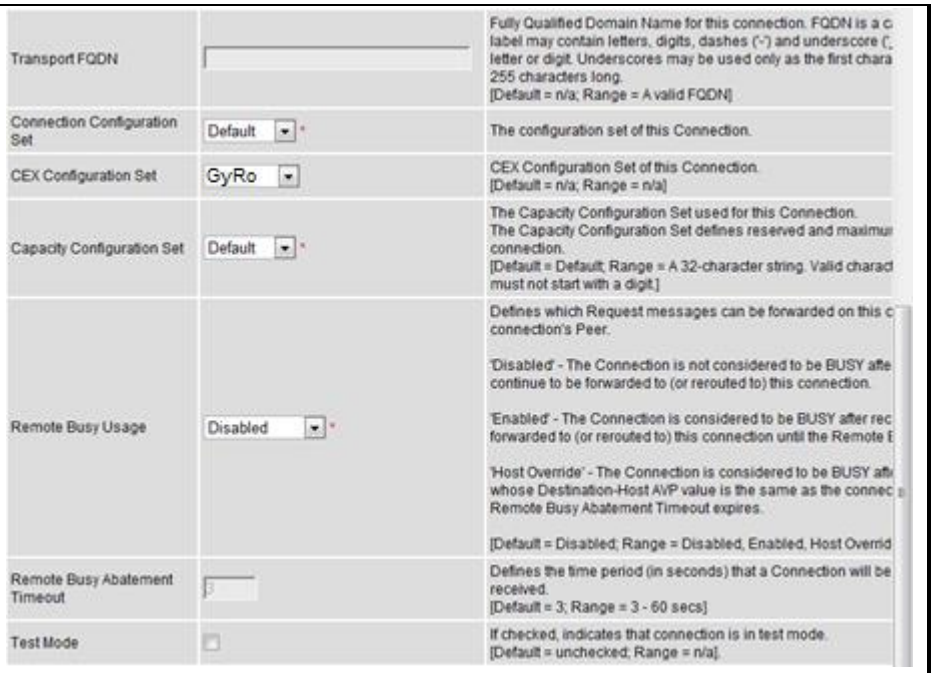
1. Enter the CEX Configuration Set Name “GyRo”.
2. Select the Diameter Credit Control Application Id from Available CEX Parameters box
3. Click **Add** just below the list.
4. Click **Ok**.

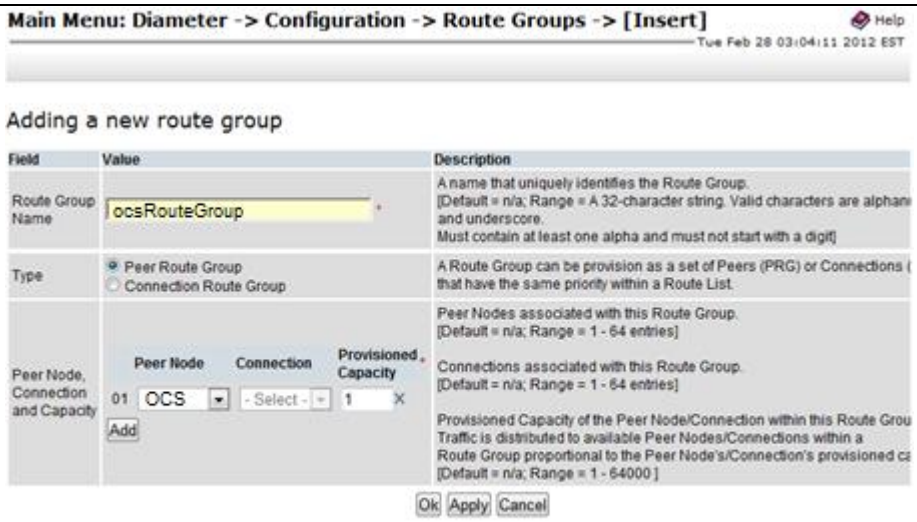
8	**SOAM VIP:** Verify that all the required CEX Configuration Sets have been configured successfully.	Navigate to **Main Menu -> Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets** You should see a screen containing all the configured CEX Configuration Sets. **Main Menu: Diameter -> 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
9	**SOAM VIP:** Navigate to Local Nodes screen	Navigate to **Main Menu -> Diameter -> Configuration -> Local Nodes**
10	**SOAM VIP:** Configure the first Local Node	Click on **Insert** in the lower left corner.

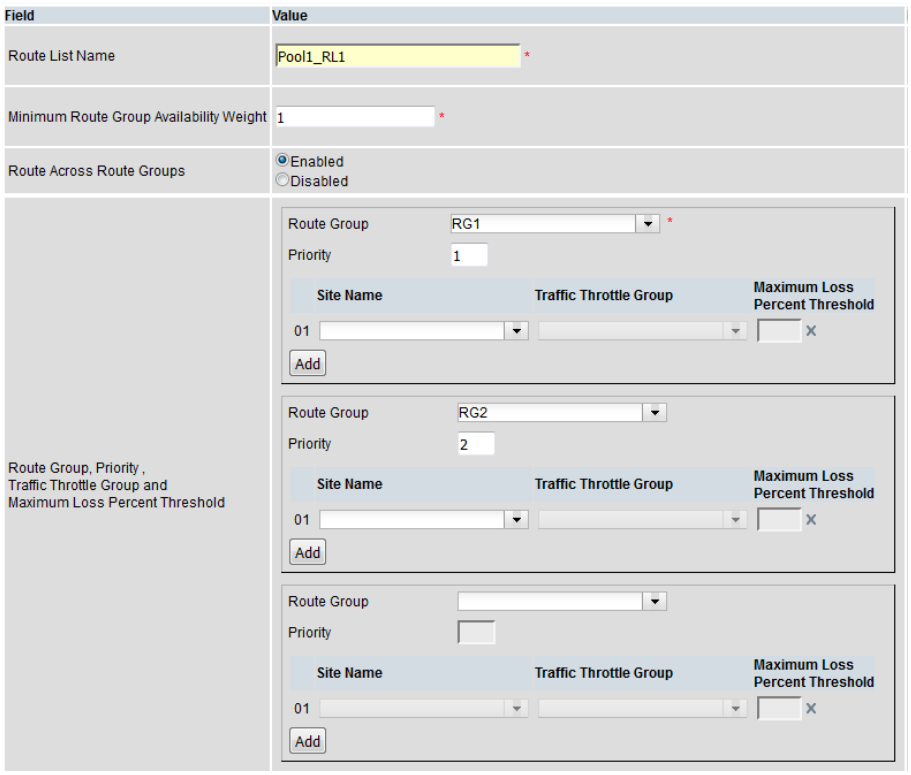
	(OC-DRA)	You will see a screen similar to:  **Main Menu: Diameter -> Configuration -> Local Nodes -> [Insert]** Thu Feb Adding a new node Field / Value / Description Local Node Name: pca — Unique name of the Local Node. [Default = n/a; Range = A 32-character string. Valid cha alphanumeric and underscore. Must contain at least o must not start with a digit.] Realm: oracle.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: pca.oracle.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 char 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] CEX Configuration Set: GyRo — CEX Configuration Set of this Local Node. [Default = n/a; Range = n/a] IP Addresses: 10.240.71.118, 10.240.71.121(TSA), - Select - ... — The IP address and TSA list of this Local Node. [Default = n/a; Range = 1 - 8 entries] Ok Apply Cancel **1.** Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). Please refer to the Diameter User's Guide [7] for details on the fields in this screen. 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.
11	**SOAM VIP:** Configure other Local Nodes, if required.	Repeat Step 10 and configure more Local Nodes if required.

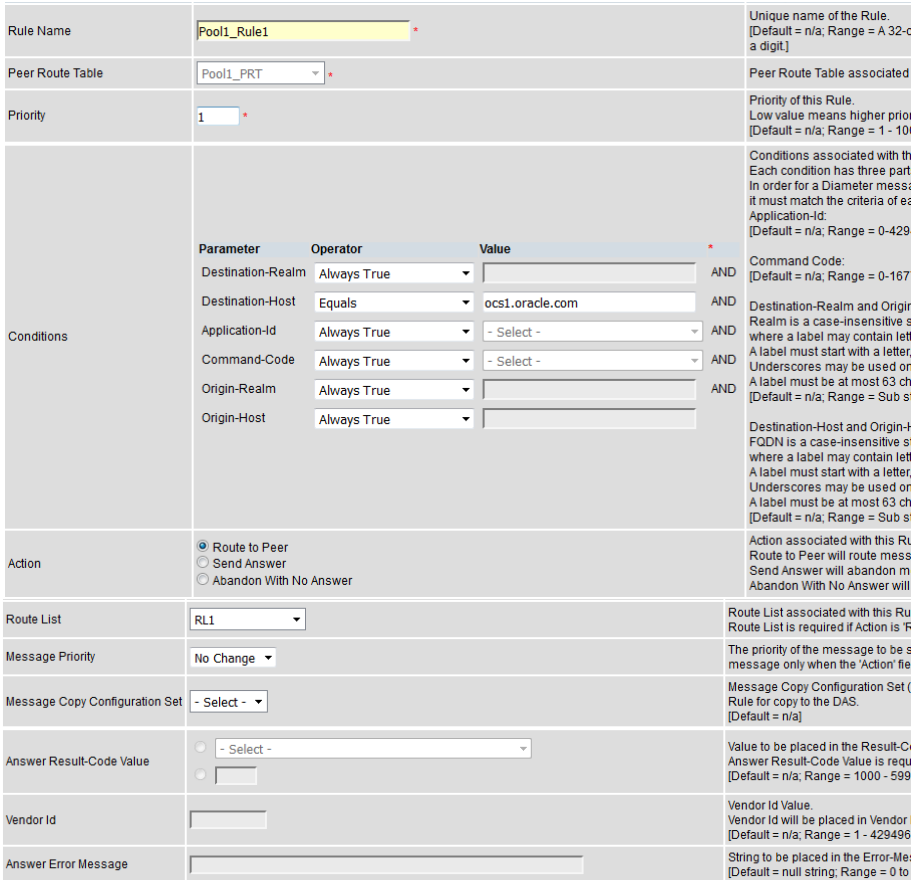
12	**SOAM VIP:** Navigate to Peer Nodes screen	Navigate to **Main Menu -> Diameter -> Configuration -> Peer Nodes**
13	**SOAM VIP:** Configure the first CTF node	Click on **Insert** in the lower left corner. You will see a screen similar to:  6. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). Note: - For Peer Nodes that are OCSs, the “Replace Dest Host” and “Replace Dest Realm”

		check boxes MUST be checked. - "Topology Hiding Status" field is not applicable for PCA and should remain disabled. - The "Application Route Table" may apply for Peer Nodes that are CTFs. - The "Peer Route Table" field may be populated to route to Shared State OCSs. - For mode details on the fields and routing configuration please consult the Diameter User's Guide [7] 7. Click **Ok**.
14	**SOAM VIP:** Configure other Peer Nodes	Repeat Step 13 to configure other CTF and OCS peer nodes as required.
15	**SOAM VIP:** Navigate to Connections screen	Navigate to **Main Menu -> Diameter -> Configuration -> Connections**
16	**SOAM VIP:** Configure the connection with CTF Node	Click on **Insert** in the lower left corner. You will see a screen similar to: **Main Menu: Diameter -> Configuration -> Connections -> [Insert]** Help Mon Feb 20 04:54:25 2012 EST Adding a new connection Field / Value / Description Connection Name: conn_ctf * — A name that uniquely identifies the Connection. [Default = n/a; Range = A 32-character string. Valid characters not start with a digit.] Transport Protocol: SCTP / TCP — The transport protocol used by this Connection. The protocol should be supported by both Local Node and Pe Local Node: pca * — The Local Node of this Connection. Connection Mode: Responder Only * — Initiator Only indicates that Local Node will only initiate the con Responder Only indicates that Local Node will only respond to Initiator & Responder indicates that Local Node will initiate cor Node. [Default = Initiator & Responder; Range = n/a] Local Initiate Port: — The Local Initiate Port of this Connection. [Default = n/a; Range = 1024-65535] Primary Local IP Address: 10.240.71.121(TSA) * — The IP Address to be used as the Primary Local Node address Secondary Local IP Address: - Select - — The IP Address to be used as the Secondary Local Node addr This address is only used for SCTP multi-homing. This addres Peer Node: CTF * — The Peer Node of this Connection. Peer Node Identification: IP Address / Transport FQDN / Peer Diameter Identity FQDN — Specifies whether the Peer Node is identified by IP address(es been selected and no Transport FQDN has been specified, th Primary Peer IP Address: 10.250.53.51 — The IP Address to be used as the Primary Peer Node address Secondary Peer IP Address: - Select - — The IP Address to be used as the Secondary Peer Node addre This address is only used for SCTP multi-homing. This addres

		 8. Enter the field values as shown above (the value given above are examples only and may be replaced by actual values). Note: Please refer to the Diameter User's Guide[7] for details on fields in this screen 9. Click **Ok**. **NOTE:** Make sure the IPFE configuration matches the Transport Protocol which is selected in this step.
17 ☐	**SOAM VIP:** Configure all other connection with Peer nodes	Repeat Step 16 to configure all other required connections.
18 ☐	**SOAM VIP:** Configure Route Groups	If Online Charging DRA is configured to run in Single Pool Mode, Destination Host will not be populated in the CCR-Initiate Diameter message. The user needs to configure Routing Rules based on Origin-Host or route all new session creation messages to a single Pool of OCSs. In either case, primary and alternate routing groups may be configured and prioritized. If Online Charging DRA is configured to run in Multiple Pool Mode, Destination Host will be present in the Diameter CCR-Initiate message. Destination-Host based routing rules may be configured in this case. The Routing configuration shown below takes an example of Multiple Pool Mode OCS Selection.
19 ☐	**SOAM VIP:** Configure the Primary Route Group for the first OCS Pool.	Navigate to **Main Menu -> Diameter -> Configuration -> Route Groups** Click on **Insert** in the lower left corner. You will see a screen similar to:

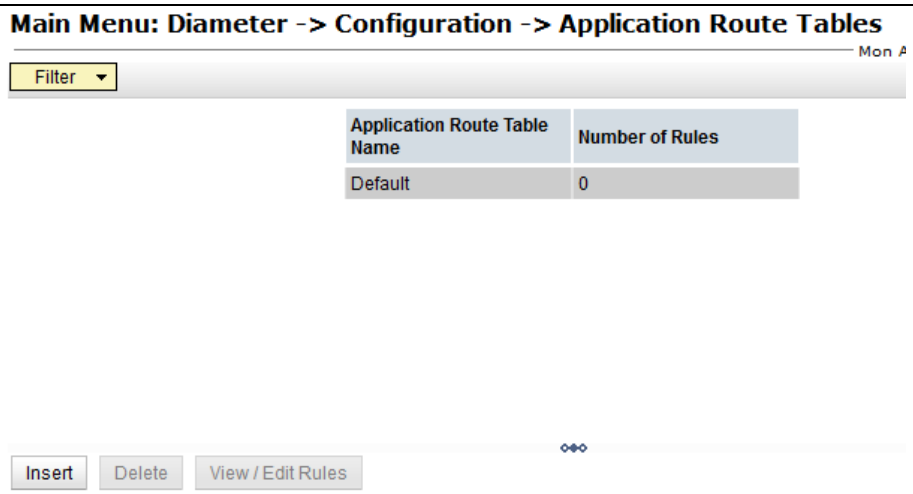
		 1. Enter the Route Group name. 2. Select the Peer Node name (OCS name). 3. If more OCSs need to be added to this Route Group click on Add and repeat step 2. 4. Enter the provisioned capacity as 1. 5. Click `Ok`.
20	**SOAM VIP:** Configure the Alternate Route Group(s) for the **same** OCS Pool.	**OPTIONAL** If alternate Route Group(s) are planned, repeat step 19 for all such Route Groups.
21	**SOAM VIP:** Configure the Route List for the first OCS Pool	Navigate to **`Main Menu -> Diameter -> Configuration -> Route Lists`** Click on **`Insert`** in the lower left corner. You will see a screen similar to:

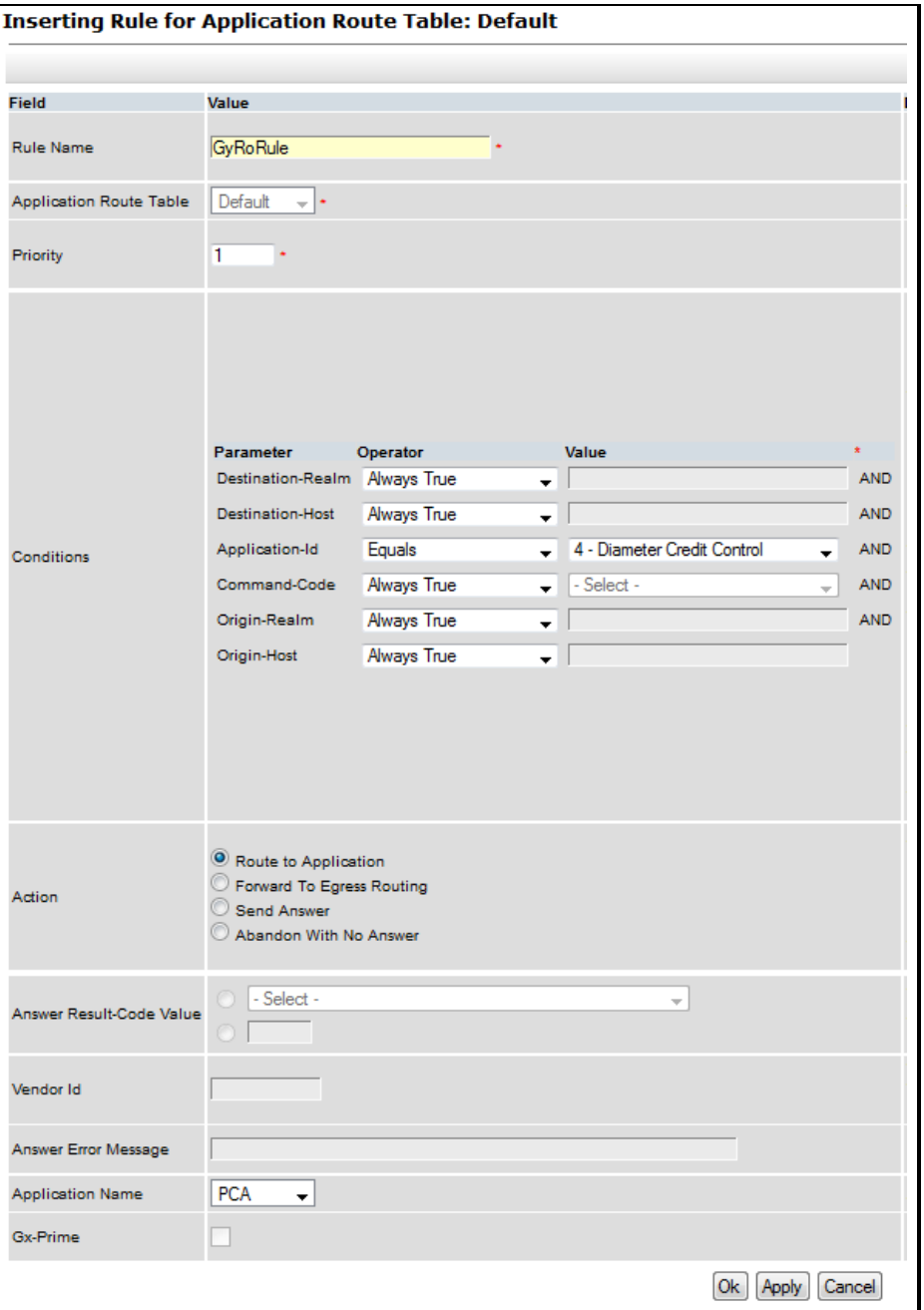
		 1. Enter the Route List name. 2. Set the Minimum Route Group Availability Weight as needed. 3. Select the Route Group(s) configured in the previous two steps and set their desired priorities. 4. Set any other parameters desired (for e.g. Maximum Loss Percent Threshold etc.) 5. Click Ok.
22	**SOAM VIP:** Configure Routing Rules for the first OCS Pool	Configure the Default PRT such that DSR forwards messages based on the OCS Pool selected by PCA. Navigate to **Main Menu -> Diameter -> Configuration -> Peer Route Table** Select the Default Peer Route Table and Click **Edit** You will see a screen similar to:



1. Enter the Rule name.
2. Set the Priority of the Rule as needed (preferably 1).
3. Select the Operator as “Equals” for Destination-Host Condition Parameter and enter the Destination-Host (FQDN) that will be populated by RBAR or any other DSR Application for the first OCS Pool.
3. Select “Always True” for the remaining Condition Parameters. You may base the OCS Pool routing on some condition parameters in special use cases for example Origin-based routing.
3. Select the Route List configured in step 21.
4. Click Ok.

23	**SOAM VIP:** Configure Routing for other OCS Pools.	If more, OCS Pools are planned in the Diameter network, repeat steps 19 through 22 for other OCS Pools’ Routing
24	**SOAM VIP:** Configure inter DSR Routing	**OPTIONAL** If Diameter messages need to be routed in between DSR sites (nodes), set up the routing as needed. This is likely in 3-site redundancy deployments because many CTFs likely only support primary and secondary connections. In such deployments routing can be set up between the three sites.
25	**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.
26	**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.
27	**SOAM VIP:** Configure the ART for GyRo 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**.

28	**SOAM VIP:** Configure the ART for all other Interfaces	Repeat Step 26 for any other Application Id that needs to be routed to the PCA Application by Diameter Routing Layer.

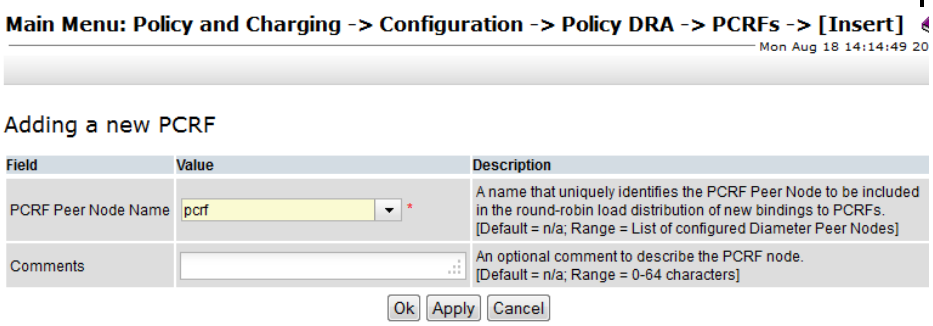
4.4 PCA FUNCTION CONFIGURATION PROCEDURES

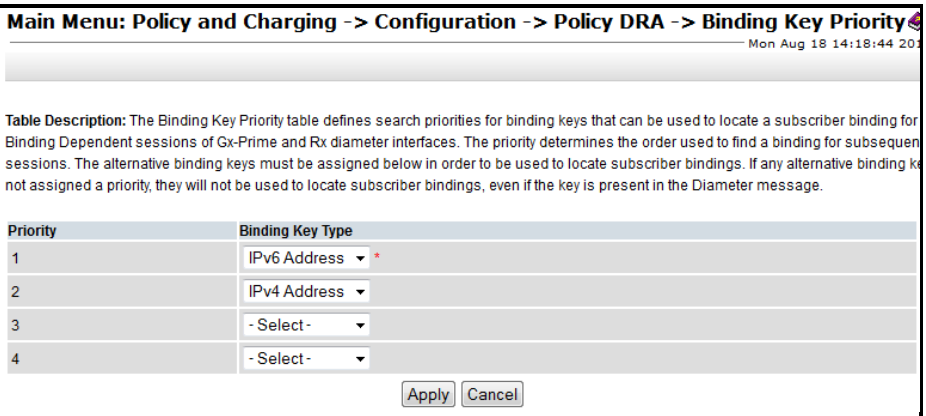
This section provides the detailed procedure steps of the PCA configuration execution.

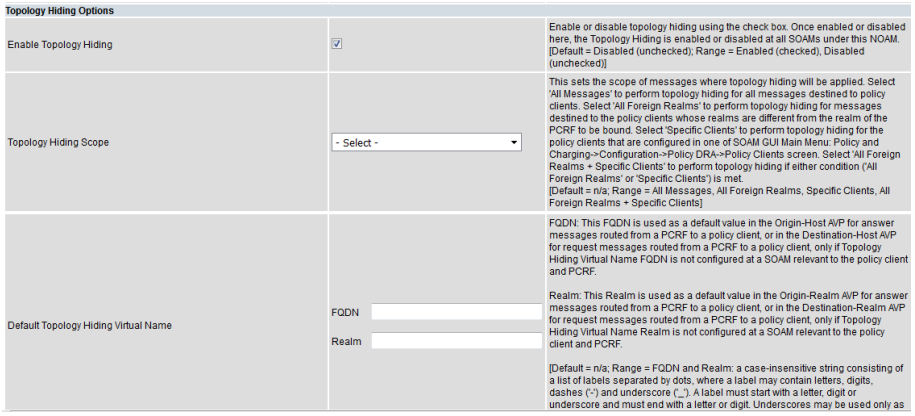
4.4.1 Policy DRA Configuration

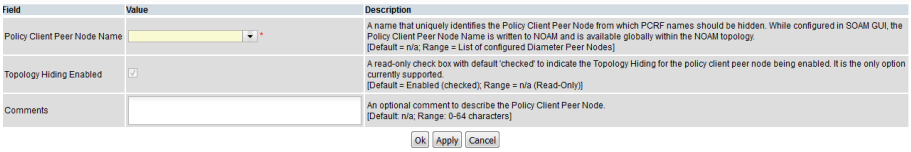
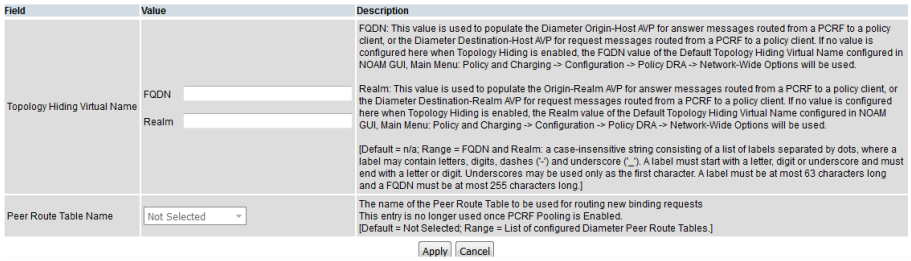
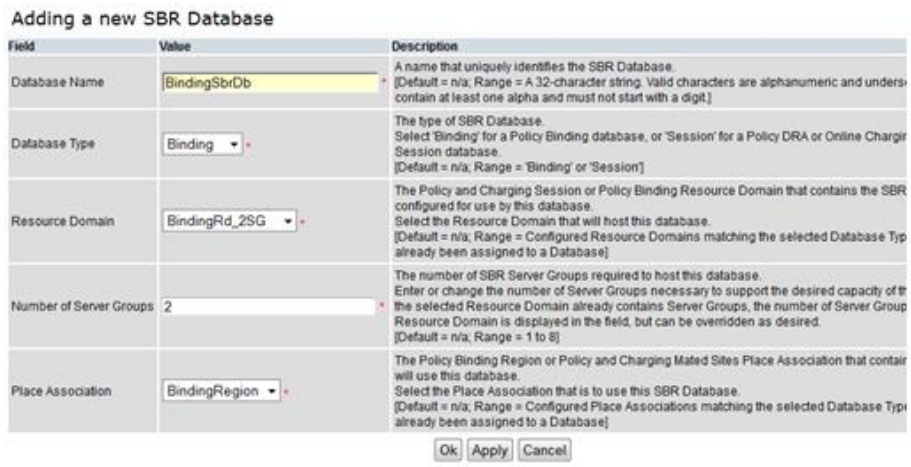
Detailed steps are given in the procedure below.

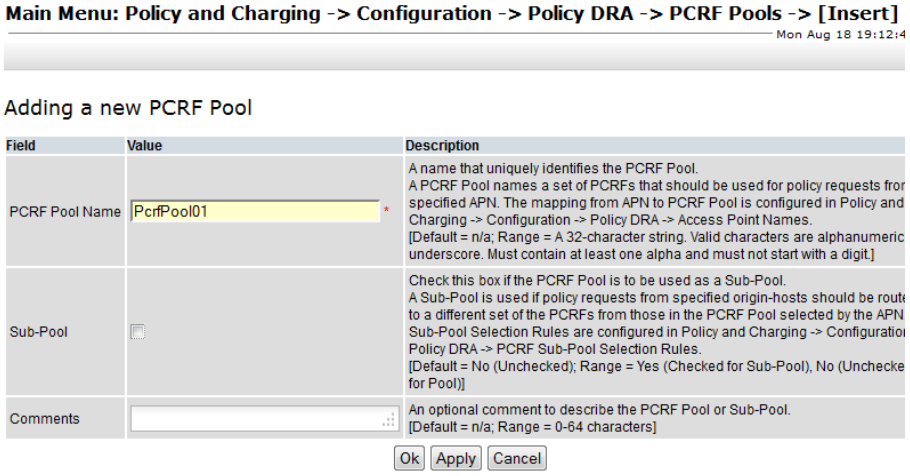
Procedure 15: Policy DRA configuration

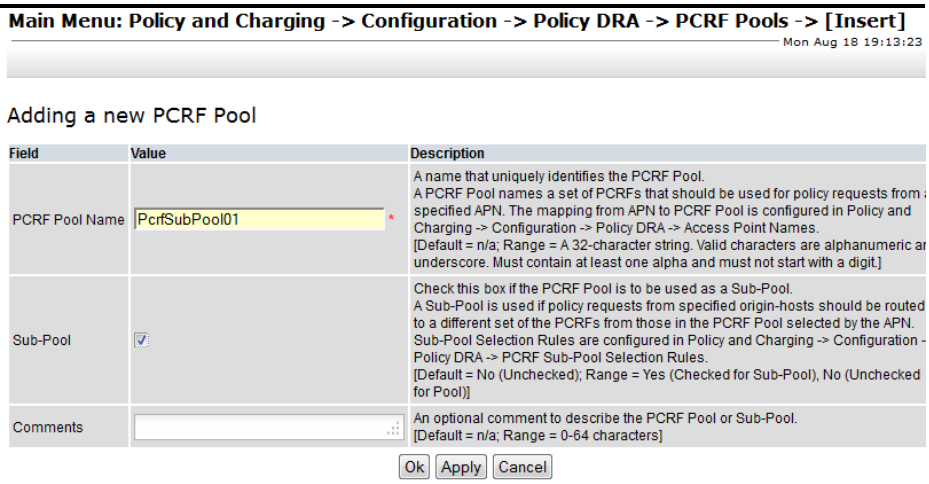
S T E P #		
	This procedure configures the Policy DRA function of PCA application. For details on the fields of various configuration screens please refer to the Policy Charging User's Guide [4]. PRE-REQUISITE: Procedure 13 must be executed before this procedure. Check off (√) each step as it is completed. 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	**NOAM 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 -> Network-Wide Options**  In the Topology Hiding Options section: 1. Check the Enable Topology Hiding checkbox. 2. Select the Topology Hiding Scope from the dropdown. 3. Enter the default Virtual FQDN and Realm to be used in Topology Hidden messages. These are default values that can be overridden by site configuration. 4. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
8	**SOAM VIP:** Configure the Peer node for which PCRF identity needs to be hidden	**OPTIONAL** Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Policy Clients** Click on **Insert** in the lower left corner. You will see a screen similar to:

		Adding a new Policy Client  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	**OPTIONAL** 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 Virtual FQDN and Realm.	**OPTIONAL**  1. Enter the virtual/pseudo host FQDN and Realm to be used for this site. These values override the Virtual FQDN and Realm values configured in Step 7. 2. 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 -> SBR -> 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 -> Policy DRA -> 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	**OPTIONAL** Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> 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.

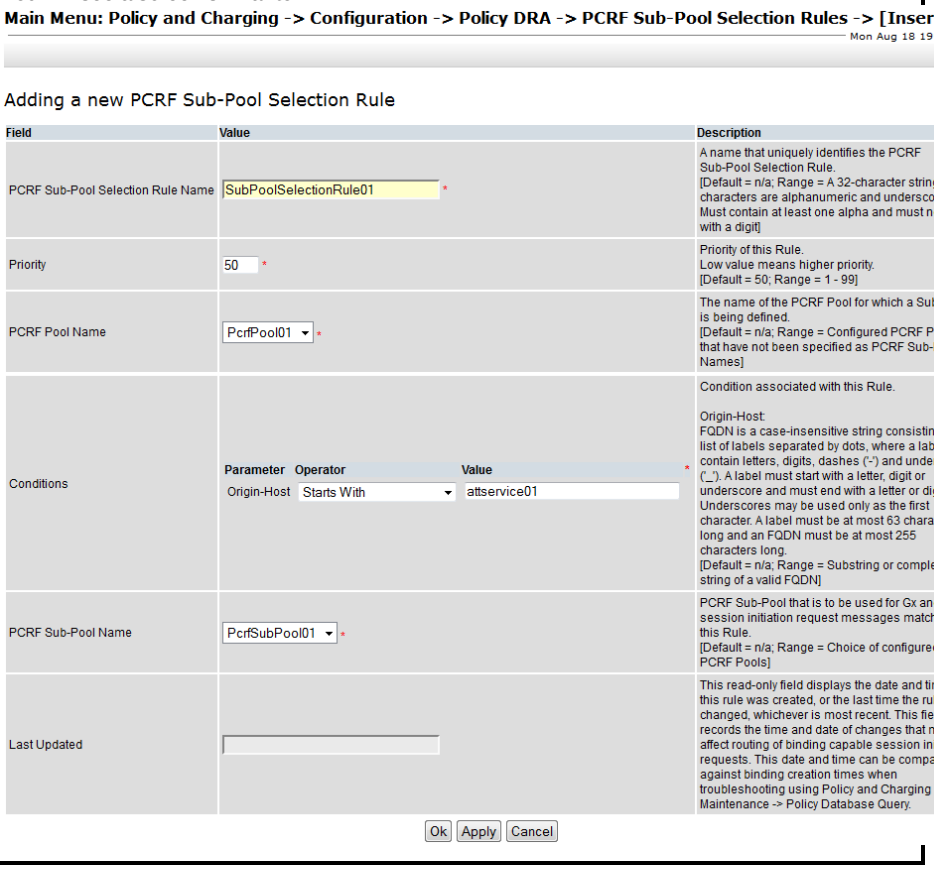
15 **NOAM VIP:** Configure PCRF Sub Pool Selection Rule

OPTIONAL

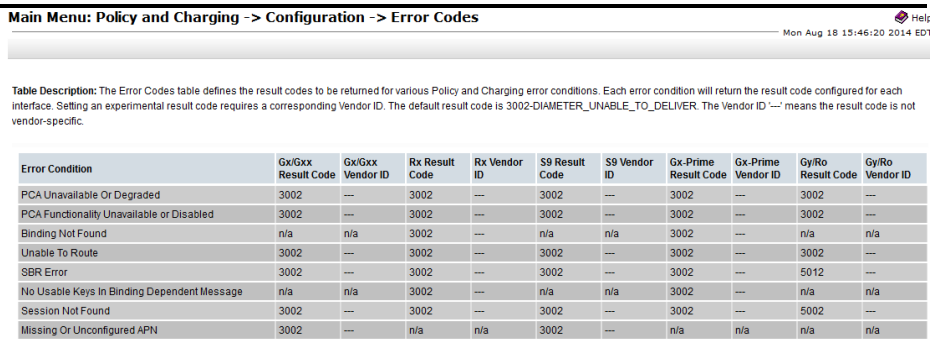
Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pools Selection Rules**

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

You will see a screen similar to:



		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	**SOAM VIP:** Navigate to PCRF Pool To PRT Mapping screen	Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping** You will see a screen similar to: **Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping** Mon Aug 18 15:38: Filter **Table Description:** The PCRF Pool To PRT Mapping table displays the list of PCRF Pools or Sub-Pool configured at the NOAMP a each to be mapped to a Peer Routing Table to be used when a new binding is created for the PCRF Pool. The PCRF Pool or Sub- used for a given subscriber binding attempt is determined based on Access point Name to PCRF Pool mappings, or by rules cor NOAMP in Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules. PCRF Pool Name / Peer Route Table Name Default / Default PcrfPool01 / Not Selected PcrfSubPool01 / Not Selected
17	**SOAM VIP:** Configure the PCRF Pool To PRT Mapping	Select the row with 'Not Selected' under Peer Route Table Name and click 'Edit' You will see a screen similar to: **Main Menu: Policy and Charging -> Configuration -> Policy DRA -> PCRF Pool To PRT Mapping -> [Edit]** Mon Aug 18 15:39:33 20 Field / Value / Description PCRF Pool Name: PcrfPool01 * — A name that uniquely identifies the PCRF Pool. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.] Peer Route Table Name: PcrfPoolPRT — The name of the Peer Route Table that is used to route new bindings for this PCRF Pool. [Default = Not Selected; Range = All Peer Route Tables configured at this site.] Ok Apply Cancel 1. Select appropriate Peer Route Table Name form the drop box. 2. Click **Ok**. NOTE: this is a sample set of configuration data, the actual configuration may differ.
18	**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'.
19	**SOAM VIP:** Navigate to the Error Codes screen	**OPTIONAL** 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.

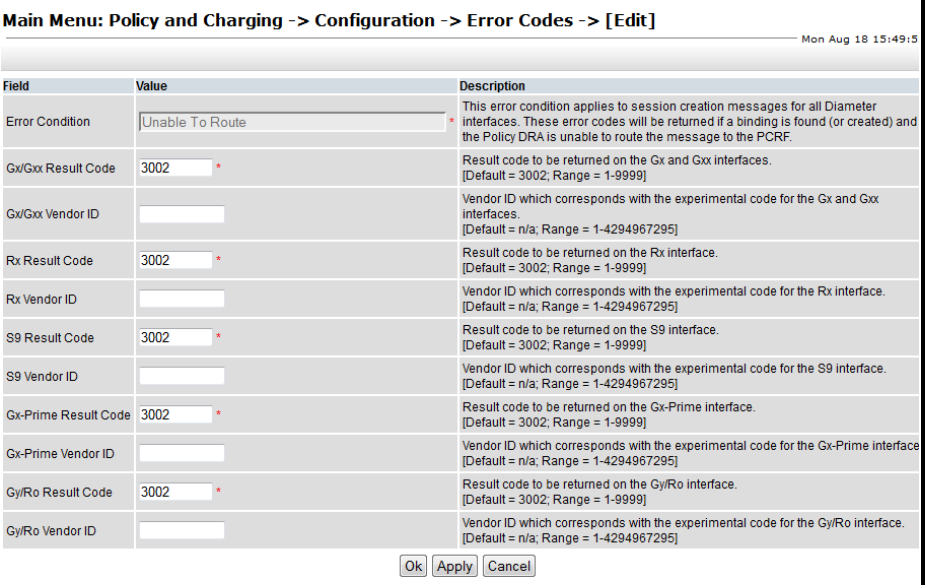
Error Condition	Gx/Gxx Result Code	Gx/Gxx Vendor ID	Rx Result Code	Rx Vendor ID	S9 Result Code	S9 Vendor ID	Gx-Prime Result Code	Gx-Prime Vendor ID	Gy/Ro Result Code	Gy/Ro Vendor ID
PCA Unavailable Or Degraded	3002	---	3002	---	3002	---	3002	---	3002	---
PCA Functionality Unavailable or Disabled	3002	---	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

20 ☐ **SOAM VIP:** Configure the Error Codes

OPTIONAL

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

You will see a screen similar to:



Main Menu: Policy and Charging -> Configuration -> Error Codes -> [Edit]

Mon Aug 18 15:49:5

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

Ok Apply Cancel

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

21 ☐ **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.

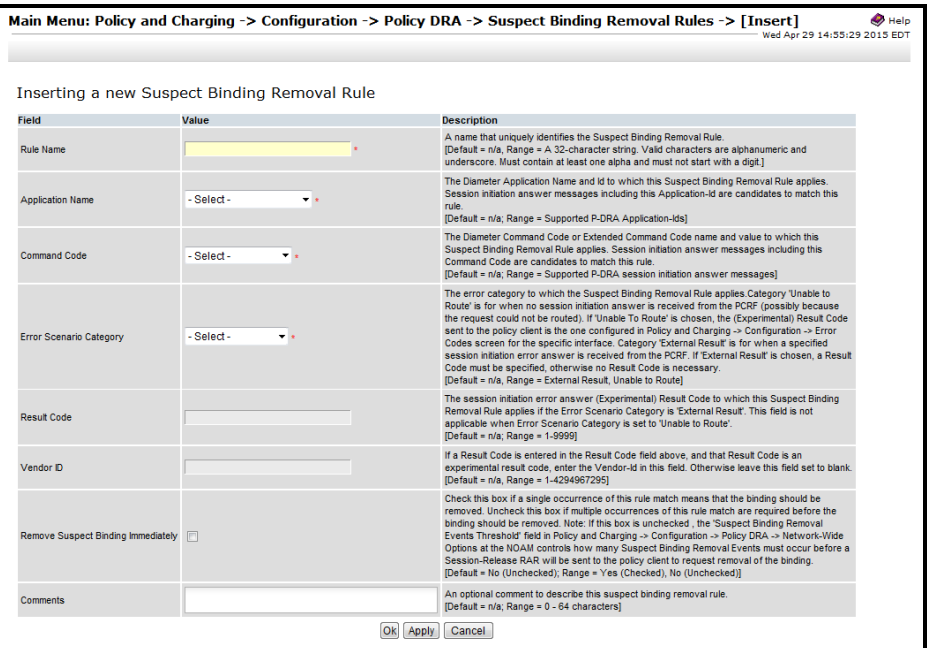
Navigate to **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Suspect Binding Removal Rules**

22 ☐ **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:



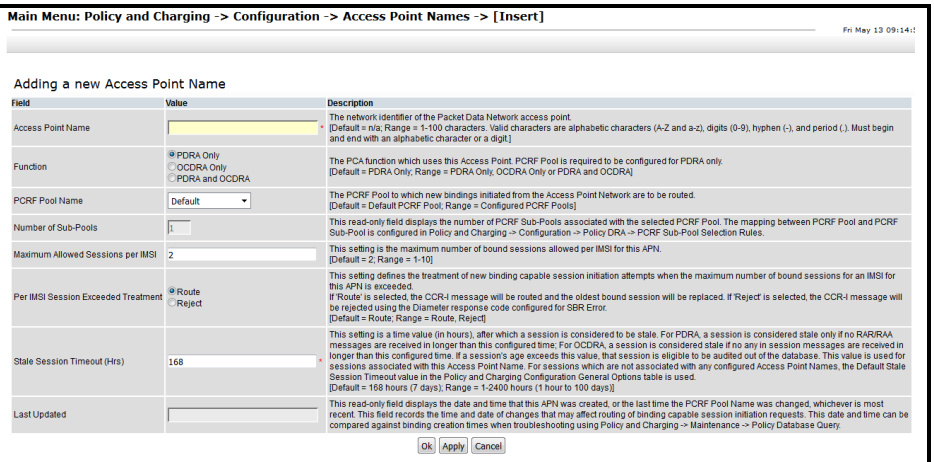
1. Enter the Rule Name
2. Select the Application Name from the drop box
3. Select the Command Code(Message) from the drop box
4. Select the required Error Scenario Category from the drop box
5. If the “External Error” Error Scenario Category was selected,

   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.

23	**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:** 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 required
2. Click **Ok**.

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

24 **NOAM VIP:** Enable the Policy DRA function

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

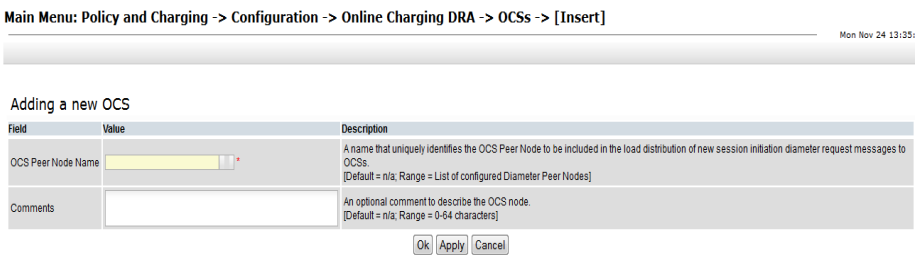
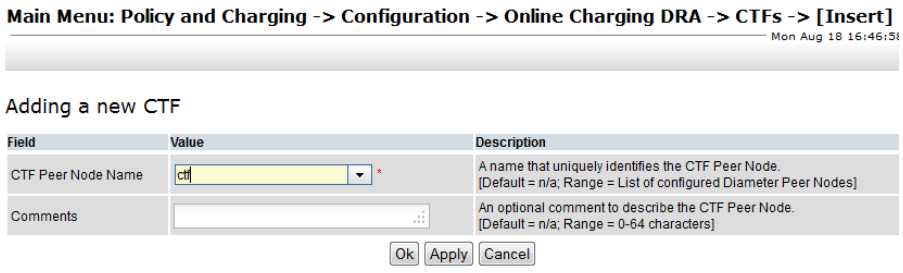
Field	Value	Description
Policy DRA Enabled	☑	Indicate whether the Policy DRA Function of PCA is enabled. [Default = Policy DRA Disabled (Unchecked); Range = Policy DRA Enabled (Checked) or Policy DRA disabled (Unchecked)]
Online Charging DRA Enabled	☐	Indicate whether the Online Charging DRA Function of PCA is enabled. [Default = Online Charging DRA Disabled (Unchecked); Range = Online Charging DRA Enabled (Checked) or Online Charging DRA Disabled (Unchecked)]

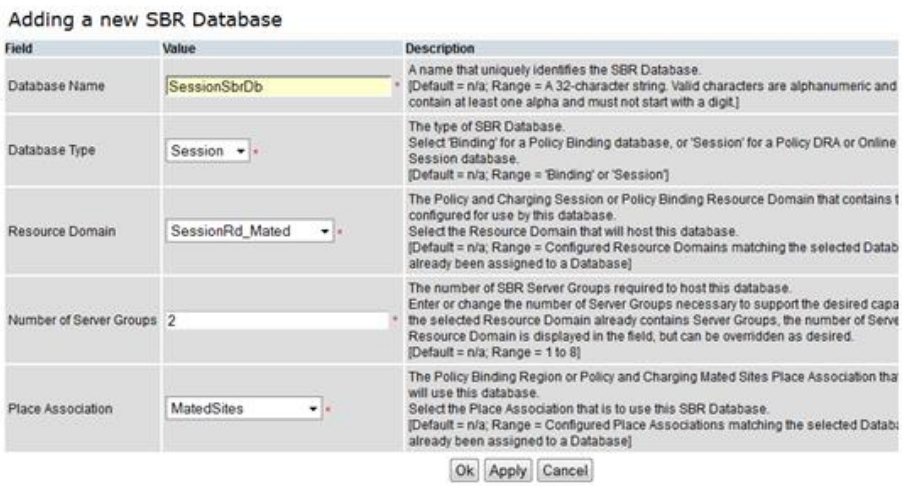
1. Check the Policy DRA Enabled box
2. Click **Apply**.

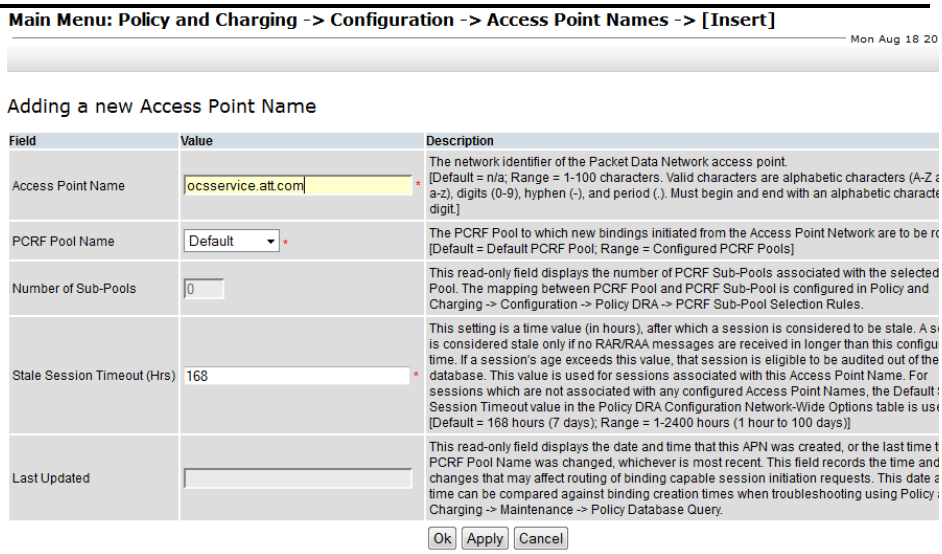
4.4.2 Online Charging DRA Configuration

Detailed steps are given in the procedure below.

Procedure 16: Online Charging DRA configuration

S T E P #	This procedure configures the Online Charging DRA function of PCA application. For details on the fields of various configuration screens please refer to the Policy Charging User's Guide [4]. PREREQUISITE: Procedure 14 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 -> SBR -> 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 (Session). 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 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.

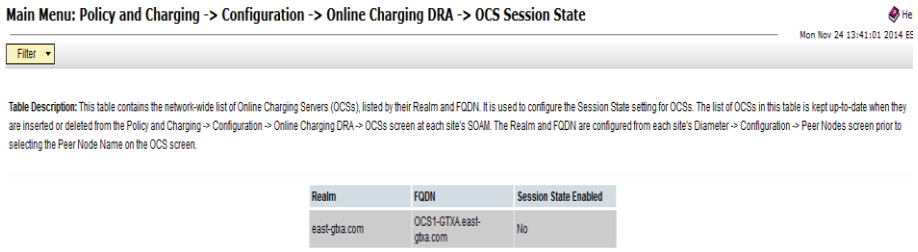
10 **NOAM VIP: Navigate to OCS Session State screen**

OPTIONAL

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

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

You will see a screen similar to:

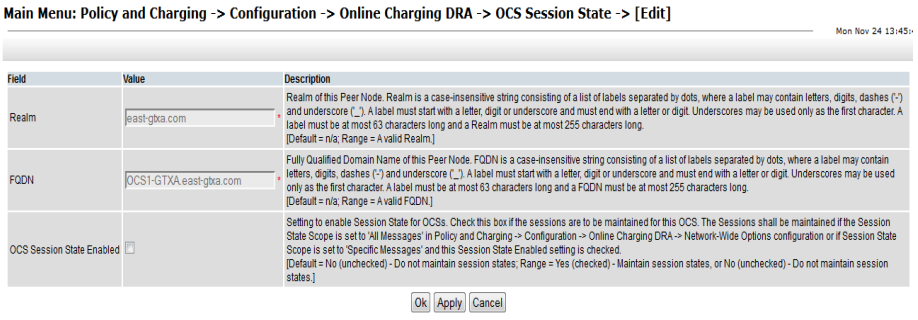


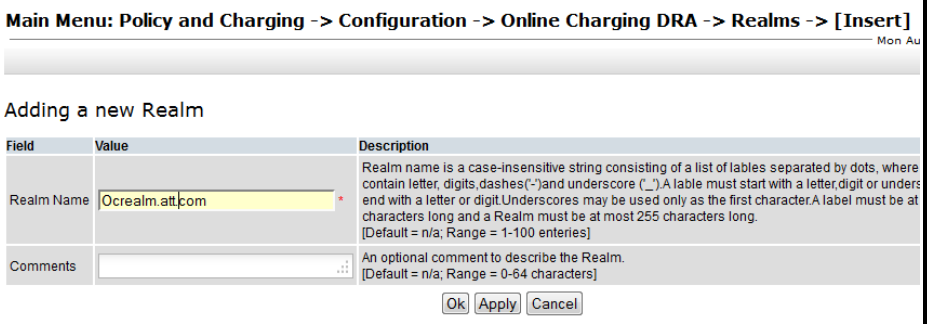
11 **NOAM VIP: Configure the Session State for an OCS.**

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 11 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 14 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. Please refer to the Policy Charging Application User's Guide [4] for details on the fields.

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

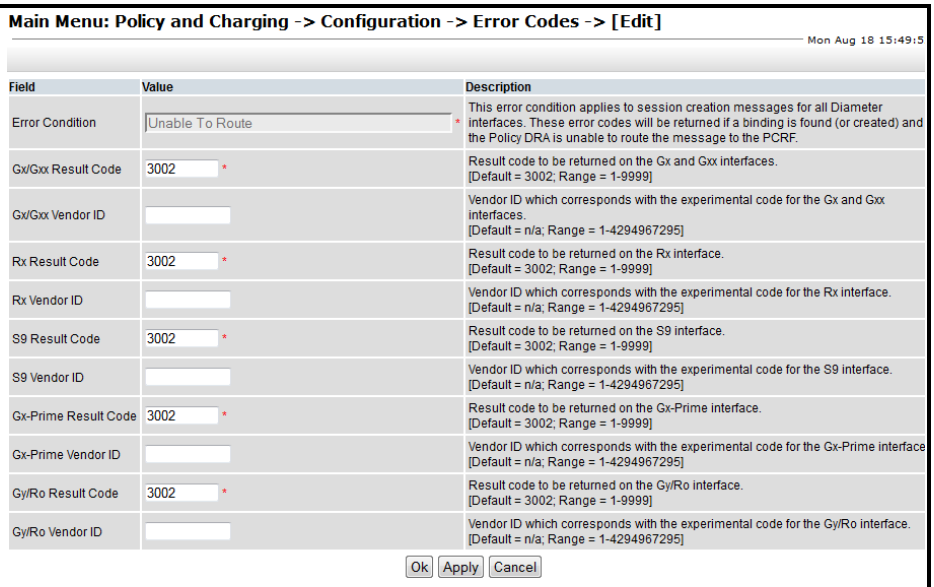
Table Description: The Error Codes table defines the result codes to be returned for various Policy and Charging error conditions. Each error condition will return the result code configured for each interface. Setting an experimental result code requires a corresponding Vendor ID. The default result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

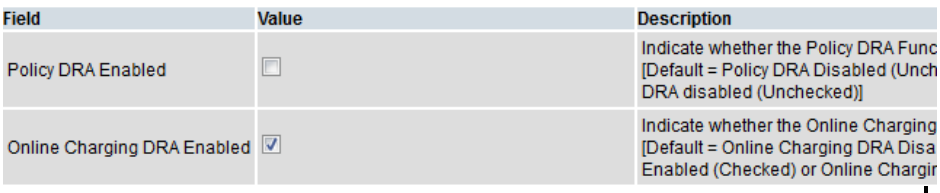
Select the row to edit and click on 'Edit' button

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 17: New Online Charging DRA Site Configuration

S T E P #	This procedure configures a site for OC-DRA function in a DSR PCA network Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR 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 16.

4.5.2 Configuring Online Charging DRA in existing Sites

Detailed steps are given in the procedure below.

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

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

4.5.3 Configuring Online Charging DRA in existing Sites with scaling

Detailed steps are given in the procedure below.

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

S T E P #	This procedure performs scaling of OC-DRA function on a running PCA system Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR 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 DRA FUNCTION ON A RUNNING DSR PCA SYSTEM

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

4.6.1 Configuring Policy DRA

Detailed steps are given in the procedure below.

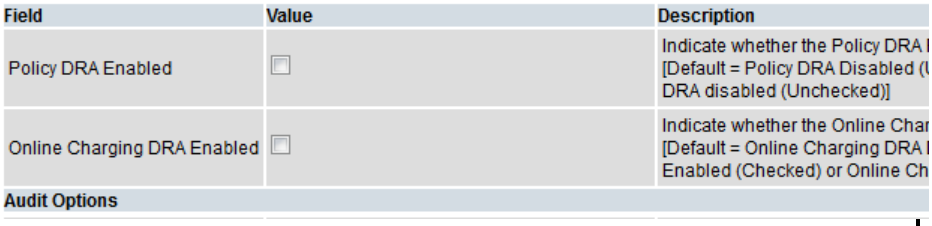
Procedure 20: Policy DRA Configuration with scaling on a running DSR PCA System

S T E P #	This procedure performs scaling of P-DRA function on a running PCA system Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR 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 DRA FUNCTION FROM A RUNNING DSR PCA SYSTEM

Detailed steps are given in the procedure below.

Procedure 21: Un-configuring Policy DRA

S T E P #	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 Policy DRA function	Navigate to **Main Menu -> Policy and Charging -> Configuration -> General Options** Screen.  1. Uncheck the Policy DRA Enabled box 2. Click **Apply**. **CAUTION** Executing this step will irretrievably delete all the subscriber binding and Policy session records from the SBR Databases.
3 ☐	**NOAM VIP:** Disable the Policy DRA specific Binding SBR Database	**Main Menu -> SBR -> Maintenenace -> SBR Database Status** Select the SBR Database of type 'Binding' and Disable it.
4 ☐	**NOAM VIP:** Disable the Policy DRA Session SBR Database	If the Online Charging DRA Function is not enabled, disable all the Session Database(s). Navigate to **Main Menu -> SBR -> Maintenenace -> SBR Database Status** One by one select the SBR Database of type 'Session' and Disable it.
5 ☐	**NOAM VIP:** Delete the Policy DRA specific Binding SBR Database	**Main Menu -> SBR -> Configuration -> SBR Databases** Delete the SBR Database of type 'Binding' from this screen.
6 ☐	**NOAM VIP:** Delete the Policy DRA Session SBR Databases	If the Online Charging DRA Function is not enabled, disable all the Session Database(s). Navigate to **Main Menu -> SBR -> Configuration -> SBR Databases** Delete the SBR Databases of type 'Session' from this screen.
7 ☐	**NOAM VIP:** Delete the Policy DRA specific APNs	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE APN CONFIGURATION DATA AFTER RE-ENABLE.** **Main Menu -> Policy and Charging -> Configuration ->**

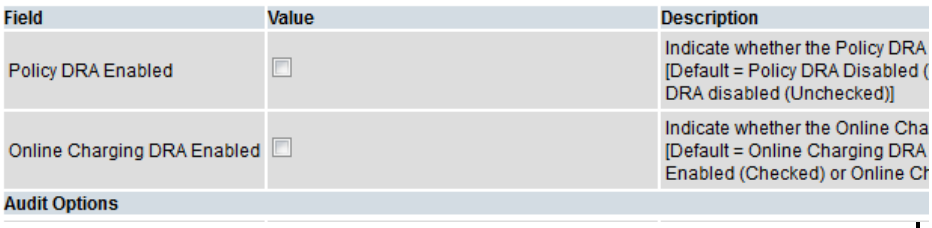
		Access Point Names Delete the Policy DRA specific configuration data from this screen.
8	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
9	**SOAM VIP:** De-reference all the PRTs from PCRF Pools	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF POOL CONFIGURATION DATA AFTER RE-ENABLE.** **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'.
10	**SOAM VIP:** Delete all the PCRFs	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF CONFIGURATION DATA AFTER RE-ENABLE.** **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRFs** Delete the complete configuration data from this screen.
11	**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.
12	**SOAM VIP:** Un-configure the Site Options	**Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> Site Options** Uncheck the 'Enabled' box against 'Topology Hiding Options'.
13	**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 etc.).
14	**SOAM VIP:** Perform steps on All Active SOAM Servers	Repeat Steps 4 to 9 on All Active SOAM servers.
13	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin".
16	**NOAM VIP:** Delete all the Sub-Pool Selection Rules	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF POOL CONFIGURATION DATA AFTER RE-ENABLE.** **Main Menu -> Policy and Charging -> Configuration -> Policy DRA -> PCRF Sub-Pool Selection Rules** Delete the complete configuration data from this screen.
17	**NOAM VIP:** Delete all the PCRF Pools	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE PCRF POOL CONFIGURATION DATA AFTER RE-ENABLE.** **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 22: 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:** Disable the Online Charging DRA Session SBR Database	If the Policy DRA Function is not enabled, disable all the Session Database(s). Navigate to **Main Menu -> SBR -> Maintenenace -> SBR Database Status** One by one select the SBR Database of type 'Session' and Disable it.
4 ☐	**NOAM VIP:** Delete the Online Charging DRA Session SBR Databases	If the Policy DRA Function is not enabled, delete all the Session Database(s). Navigate to **Main Menu -> SBR -> Configuration -> SBR Databases** Delete the SBR Databases of type 'Session' from this screen.
5 ☐	**NOAM VIP:** Delete all configured Realms	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE ONLINE CHARGING REALMS CONFIGURATION DATA AFTER RE-ENABLE.** **Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> Realms** Delete the complete configuration data from this screen.
6 ☐	**NOAM VIP:** Delete the Online Charging specific APNs	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE APN CONFIGURATION DATA AFTER RE-ENABLE.** **Main Menu -> Policy and Charging -> Configuration -> Access Point Names** Delete the Online charging specific configuration data from this screen.

7	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
8	**SOAM VIP:** Delete the Online Charging Servers	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE OCS CONFIGURATION DATA AFTER RE-ENABLE.** **Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> OCSs** Delete the complete configuration data from this screen.
9	**SOAM VIP:** Delete the Online charging Clients	**NOTE: THIS STEP IS OPTIONAL. THIS STEP CAN BE SKIPPED IF YOU ARE GOING TO ENABLE Policy DRA AGAIN ON THIS SYSTEM AND YOU WANT TO RE-USE THE CTF CONFIGURATION DATA AFTER RE-ENABLE.** **Main Menu -> Policy and Charging -> Configuration -> Online Charging DRA -> CTFs** Delete the complete configuration data from this screen.
10	**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.
11	**SOAM VIP:** Perform steps on All Active SOAM Servers	Repeat Steps 5 to 7 on All Active SOAM servers.

4.9 POST-CONFIGURATION PROCEDURES

4.9.1 Enable Application

Detailed steps are given in the procedure below.

Procedure 23: Enable Application

STEP #	This procedure enables the PCA application on the DA-MP 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	Establish GUI Session on the active SOAM VIP	Establish a GUI session on the Active SOAM server by using the XMI VIP address. Login as user "guiadmin".
2	**SOAM VIP:** Navigate to	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**

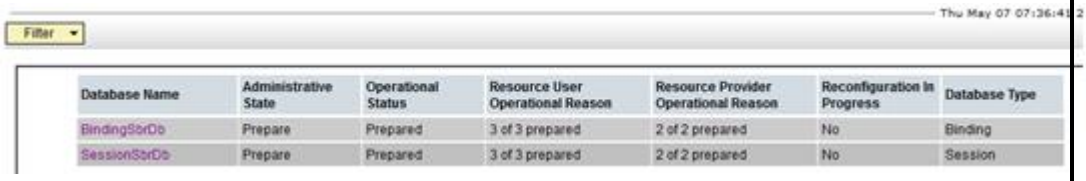
	Applications screen	
3 ☐	**SOAM VIP:** Enable the PCA application	Select the PCA row(s) and Click **Enable**.
4 ☐	**SOAM VIP:** Verify that the PCA application has been Enabled.	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications** Verify that the Application status has changed to Enabled-Available-Normal-Normal. **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.

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 24: 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**.	
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 -> SBR -> Maintenance -> SBR Database Status**
3 ☐	**NOAMP VIP:** Prepare the SBR Database	Select the SBR Database and Click **Prepare**. NOTE: This step enables status monitoring of the database by all servers that will communicate with the database. In the Prepare state, the PCA application is not yet allowed to use the database.
4 ☐	**NOAMP VIP:** Verify that the SBR Database has been prepared.	Navigate to **Main Menu -> SBR -> Maintenance -> SBR Database Status** Verify that the SBR Database status has changed to Prepare – Prepared – N of N prepared – N of N prepared  Filter Thu May 07 07:36:41 2 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. **CAUTION**: If the state does not change to "N of N prepared" it is recommened to fix the problems that are causing part or all of the database resource users and/or providers to not transit to prepared state. If the SBR Database is enabled while it is still in "Preparing" state calls may fail because users of the database do not have access to part or all the it.
5 ☐	**NOAMP VIP:** Enabled the SBR Database	Select the SBR Database and Click **Enable**. NOTE: Enabling the database allows the PCA application to begin reading and writing the database.
6 ☐	**NOAMP VIP:** Verify that the SBR Database has been enabled.	Navigate to **Main Menu -> SBR -> Maintenance -> SBR Database Status** Verify that the SBR Database status has changed to Enable – Normal – N of N available – N of N available

		 **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 25: 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 the MP servers with Function "DSR (multi-active cluster)" that are or will be handling PCA traffic and all MP servers with Function "Policy and Charging SBR" then Click **Restart**. NOTE: The Function of an MP Server is the same as the Function assigned to its Server Group in **Main Menu -> Configuration -> Server Groups** **CAUTION:** **If the DSR system is processing traffic other than PCA then DO NOT restart all DA-MP servers simultaneously. Doing so will cause a network-wide outage. Please follow the procedure listed in** APPENDIX-B **to restart the DA-MP servers in a controlled order to minimize traffic loss.**

4.9.4 Enable Connections

Detailed steps are given in the procedure below.

Procedure 26: Enable connections

S T	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.

E P #	SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	Establish GUI Session on the SOAM VIP	Establish a GUI session on the SOAM by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**SOAM VIP:** Navigate to Connections screen	Navigate to **Main Menu -> Diameter -> Maintenance -> Connections**
3 ☐	**SOAM VIP:** Enable all connections	Select all Connection rows for newly added PCA Peers Nodes and Click **Enable**.
4 ☐	**SOAM VIP:** Verify that the connections have been Enabled.	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. Responder Only connections will remain in Listening Operational Status until the peer node initiates the connection

Connection Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Connection Mode	Local Node	Peer No
conn_af	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	AF
conn_pcef1	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	PCEF1
conn_pcef2	blade14	Enabled	Unavailable	Listening	Responder Only	PDRA	PCEF2
conn_pcrf1	blade14	Enabled	Unavailable	Connecting	Initiator Only	PDRA	PCRF1
conn_pcrf2	blade14	Enabled	Unavailable	Connecting	Initiator Only	PDRA	PCRF2

conn_af1		Enabled	Unk	Unk	Responder Only	PDRA	AF1

4.9.5 Perform Health Check

Execute this Procedure to verify the sanity of the system.

Procedure 27: Perform Health Check

S T E P #	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 SBR Database Status	1. Log into the NOAM GUI using the XMI VIP address. 2. Navigate to **Main Menu: SBR -> Maintenance -> SBR Database Status** 3. Verify that the status for all the SBR Database rows have the following values Administrative State = Enabled Operational Status = Normal Resource User Operational Reason = X of X available Resource Provider Operational Reason = Y of Y available If all the verifications are successful, then proceed with next step else STOP! And call ORACLE Customer Service for further assistance.
2 ☐	Verify the Policy and Charging SBR Status	1. Log into the NOAM GUI using the XMI VIP address. 2. Navigate to **Main Menu: SBR -> Maintenance -> SBR Status** 3. Verify that the server "**Resource HA Role**" is shown as "**Active/Standby/Spare**" and '**Congestion Level**' is '**Normal**' for all the "Binding Region" and 'Mated Site" tabs. The Resource HA Role of Standby applies if there is server level redundancy configured in the DSR system. The Resource HA Role of Spare applies if there is site level redundancy configured in the DSR system. If all the verifications are successful, then proceed with signaling call flow execution else STOP! And call ORACLE Customer Service for further assistance.
3 ☐	Verify there are no PCA Alarms raised	1. Log into the NOAM GUI using the XMI VIP address. 2. Navigate to **Main Menu: Alarms & Events -> View Active** 3. Verify that there are no Alarms raised with Product PCA/SBR. 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 APPENDIX-A

7.1 PCA FEATURE ACTIVATION PROCEDURE

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

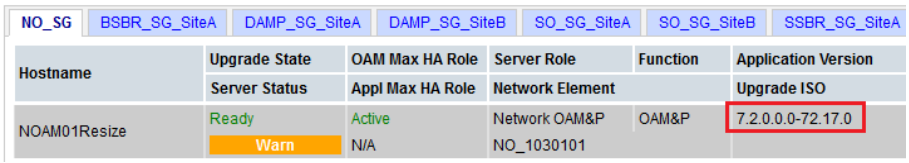
The procedures in this section need to be executed in the following order:

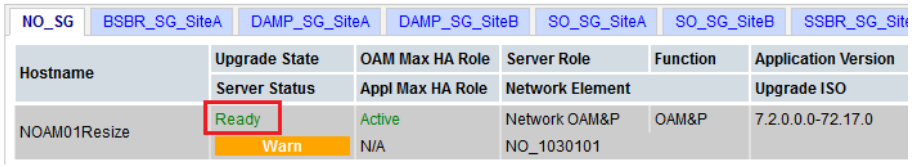
- For PCA activation on the entire network
  - Section 7.1.1 PCA Activation on an installed or upgraded system
  - Section 7.1.3 Restart Process
  - Section 7.1.4 Post PCA Activation System Health Check
- For PCA activation on a newly added site
  - Section 7.1.2 PCA Activation on a newly added site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

7.1.1 PCA Activation on an installed or upgraded system

Detailed steps are given in the procedure below.

Procedure 28: Verify PCA Activation Pre-Requisites

S T E P #		
	This procedure ensures that pre-requisites for activating PCA on an installed or upgraded system have been fulfilled. This Procedure does not require a Maintenance Window Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.** **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:** Check the software version on all servers.	Navigate to **Main Menu: Administration -> Software Management -> Upgrade** Verify that the Upgrade ISO column shows the correct release number for all servers in the DSR network. NOTE: All servers in the network must be on the same DSR release when activating PCA. 
2	**NOAM VIP:** Check the Upgrade Acceptance status on all servers.	Navigate to **Main Menu: Administration -> Software Management -> Upgrade** Verify that the Upgrade State column does not show ”ACCEPT OR REJECT”.

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

Procedure 29: PCA Activation on the entire network

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

☐	**(OPTIONAL):** Clear the Web Server cache	`# clearCache`

7.1.2 PCA Activation on a newly added site

Detailed steps are given in the procedure below.

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

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

Procedure 30: PCA Activation on newly added site

S T E P #		
	This procedure activates the PCA on a single site newly added to the DSR topology. This Procedure does not require a Maintenance Window Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.	
1 ☐	Verify configuration of All SOAM servers for the newly added site	Before continuing all SOAM servers for the newly added site should be configured in the topology. 1. Log into the NOAM VIP GUI. 2. Navigate **Main Menu: Status & Manage -> Server.** See all required SOAM servers for the newly added site are configured and Application State is enabled.
2 ☐	Execute the activation procedure	For PCA activation on new site, the activation procedure needs to be executed from the NOAM. Execute the Procedures in Section 7.1.1.

7.1.3 Restart Process

Detailed steps are given in the procedure below.

Procedure 31: Restart Process

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

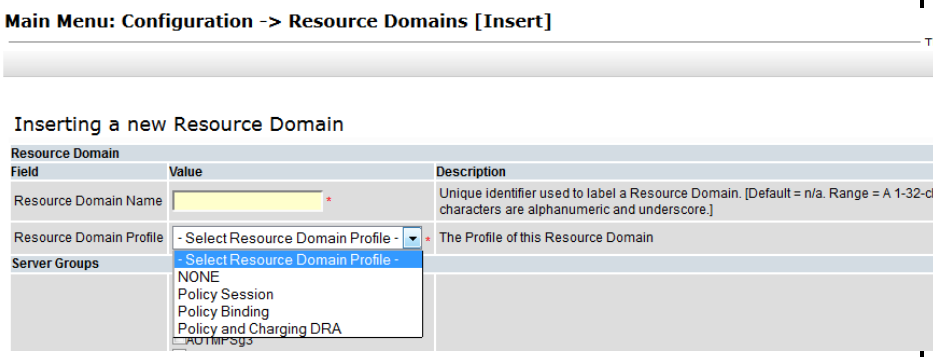
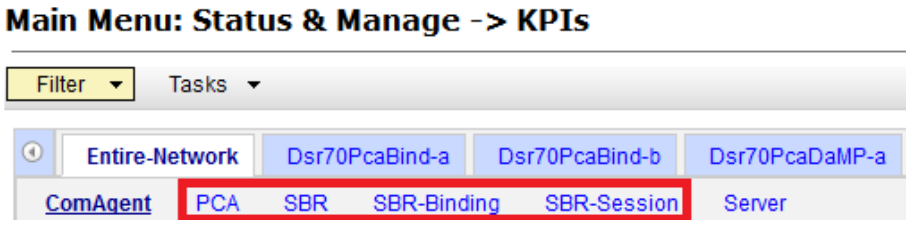
☐	Servers	Select all the SBR servers and press **Restart**.

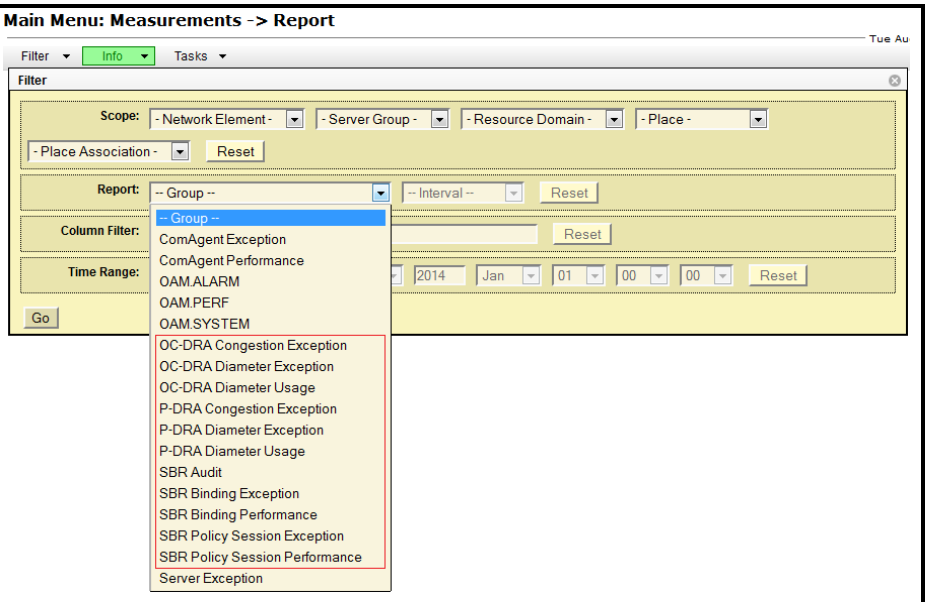
7.1.4 Post PCA Activation System Health Check

7.1.4.1 System health check after Application Activation on NOAM server

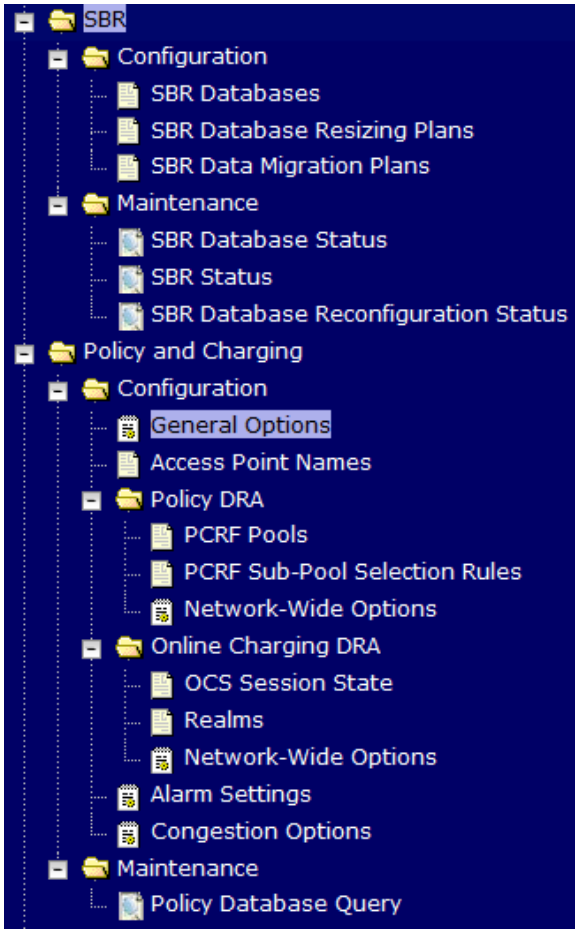
Detailed steps are given in the procedure below.

Procedure 32: Verification of application activation on NOAM Server

S T E P #		
	This procedure verifies the PCA application activation on NOAM Server. This Procedure does not require a Maintenance Window Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	**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 are shown.	Verify that Measurement groups are shown for OC-DRA, P-DRA and PSBR.



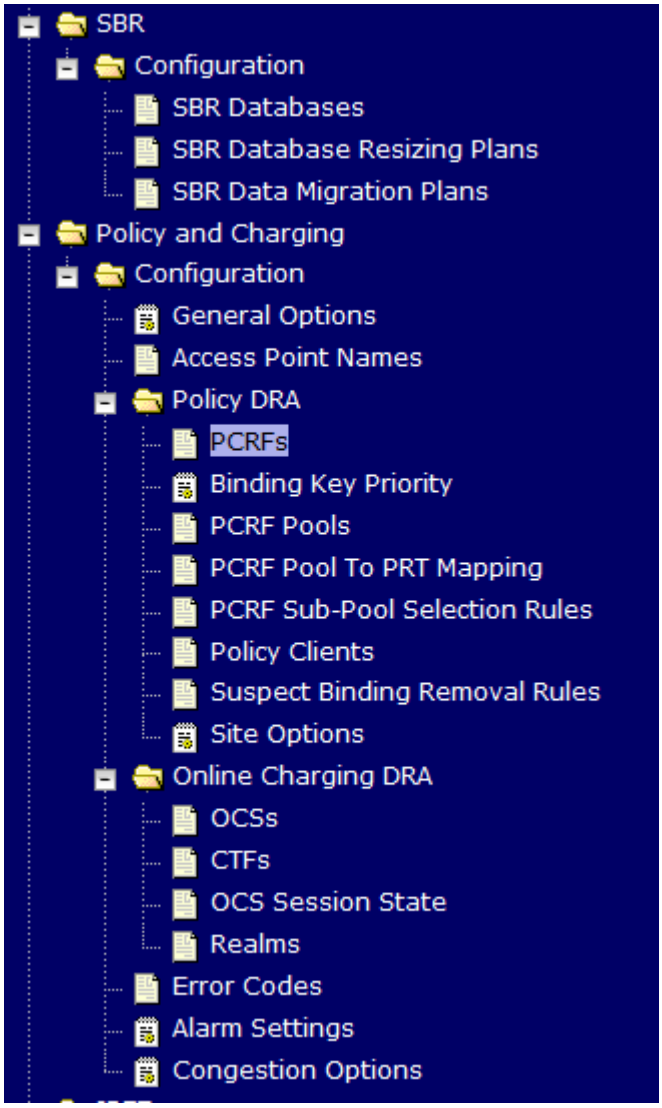
5	**NOAM VIP:** Verify that the Main Menu shows the Policy and Charging submenu.	Verify that Main Menu on Active NOAM shows the Policy and Charging and SBR submenus with Configuration and Maintenance screens.



7.1.4.2 System health check after Application Activation on SOAM servers

Detailed steps are given in the procedure below.

Procedure 33: Verification of application activation on SOAM Servers

S T E P #	This procedure verifies the activation of PCA on SOAM Servers. This Procedure does not require a Maintenance Window Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.**	
1 ☐	**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: 

7.2 PCA FEATURE DEACTIVATION PROCEDURE

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

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

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

7.2.1 Pre PCA Deactivation Steps

7.2.1.1 Verify and Deactivate the GLA application

Detailed steps are given in the procedure below.

Procedure 34: Verify and Deactivate GLA application

S T E P #	This procedure verifies that GLA is activated and then deactivates the GLA application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR 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.	Check the presence of GLA application. If GLA application record is present. It means GLA is activated on this system. **NOTE: - IF GLA RECORD IS NOT PRESENT ON THIS SCREEN, THEN SKIP THE REMAINING STEPS IN THIS PROCEDURE.**
4 ☐	**SOAM VIP:** Deactivate the GLA application.	If GLA record is present in the Applications screen. Then execute the steps to deactivate the GLA application as per deactivation procedures defined in [8] .
5 ☐	**SOAM VIP:** Perform steps on All Active SOAM Servers	Repeat Step 1-4 on All Active SOAM servers.

7.2.1.2 Unconfigure PCA Functions

Detailed steps are given in the procedure below.

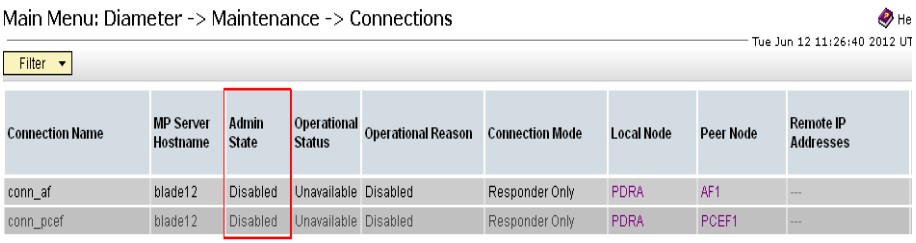
Procedure 35: Unconfigure PCA Functions (PDRA and OCDRA)

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

7.2.1.3 Disable Diameter Connections

Detailed steps are given in the procedure below.

Procedure 36: Disable Diameter Connections

S T E P #	This procedure disables the Diameter connections. This Procedure does not require a Maintenance Window Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **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.  Main Menu: Diameter -> Maintenance -> Connections Tue Jun 12 11:26:40 2012 UT Filter Connection Name / MP Server Hostname / Admin State / Operational Status / Operational Reason / Connection Mode / Local Node / Peer Node / Remote IP Addresses conn_af / blade12 / Disabled / Unavailable / Disabled / Responder Only / PDRA / AF1 / --- conn_pcef / blade12 / Disabled / Unavailable / Disabled / Responder Only / PDRA / PCEF1 / ---
3 ☐	**SOAM VIP:** Perform steps on All Active SOAM Servers	Repeat Steps 1 to 2 on All Active SOAM servers.

7.2.1.4 Disable Application

Detailed steps are given in the procedure below.

Procedure 37: Disable application

S T E P #		
	This procedure disables the PCA application. This Procedure does not require a Maintenance Window Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.	
1	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 Help Tue Jun 12 06:33:59 2012 UTC Filter DSR Application Name | MP Server Hostname | Admin State | Operational State | Operational Reason | Congestion Level | Time of Last Update PCA | blade12 | Disabled | Unavailable | Not Initialized | Normal | 2012-Jun-12 06:33:43 UTC
5	**SOAM VIP:** Perform steps on All Active SOAM Servers	Repeat Steps 1 to 4 on All Active SOAM servers.

7.2.1.5 Remove DSR Configuration Data

Detailed steps are given in the procedure below.

Procedure 38: Remove DSR configuration data

S T E P #	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.	
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 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 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 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 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 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 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 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 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 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 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.

7.2.2 PCA Deactivation Procedure

Detailed steps are given in the procedure below.

Procedure 39: PCA Application Deactivation

S T E P #	This procedure deactivates the PCA application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC**.
1 ☐	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 deactivation script	**# ./load.pcaDeactivationTopLevel** Note: - This command execution will starts Deactivation on Active NOAM and All Active SOAM servers. Check log file ***/var/TKLC/log/pcaDeactivationTopLevel.log*** to see if there is any execution failure.
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**

7.2.3 Site Specific PCA Deactivation Procedure

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

Detailed steps are given below.

Procedure 40: PCA Application Deactivation on a particular site.

S T E P #	This procedure deactivates 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 deactivation script	`# ./load.pcaDeactivateBscoped` Note: - This command execution will start Deactivation on selected active SOAM server. Check log file ***/var/TKLC/log/pcaDeactivateBscoped.log*** to see if there is any execution failure.
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`

7.2.4 Post PCA Deactivation Steps

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

7.2.4.1 Move Policy and Charging SBR Servers to OOS State

Detailed steps are given in the procedure below.

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

S T E P #	This procedure puts all the MP Servers in Policy and Charging SBR Server Groups in OOS. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR 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.

7.2.4.2 Remove Policy and Charging SBR Servers from Server Groups

Detailed steps are given in the procedure below.

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

S T E P #	This procedure removes all the MP Servers in Policy and Charging SBR Server Groups from their respective Server Groups. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT ORACLE TECHNICAL SERVICES AND **ASK FOR ORACLE TAC.** **PREREQUISITE: PREVIOUS PROCEDURE HAS BEEN EXECUTED.**	
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.

7.2.4.3 Delete Server Groups related to Policy and Charging SBR

Detailed steps are given in the procedure below.

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

S 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**. **PREREQUISITE: PREVIOUS PROCEDURE HAS BEEN EXECUTED.**	
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”.

7.2.4.4 Remove Place Configuration Data

Detailed steps are given in the procedure below.

Procedure 44: 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**. **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:** Remove all the data from Place screen as mentioned.	**Main Menu: Configuration -> Places** Edit the Places and Remove Servers from it.

7.2.4.5 Reboot the Servers

Detailed steps are given in the procedure below.

Procedure 45: Reboot the Servers

S T E	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.

P #	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 Server Groups Screen	Navigate to **`Main Menu: Status & Manage -> Server`**
3 ☐	**NOAM VIP:** Reboot the Servers.	Reboots all the relevant servers. Select all the MP servers having Function "Policy and Charging SBR" and click Reboot. Select all the DA-MP servers running PCA and click Reboot. **CAUTION:** **If the DSR system is processing traffic other than PCA then DO NOT reboot all DA-MP servers simultaneously. Doing so will cause a network-wide outage. Please follow the procedure listed in** APPENDIX-B **to reboot the DA-MP servers in a controlled order to minimize traffic loss.** Select all the SOAM Servers belonging to sites running PCA and click reboot. Select all NOAM servers except the Active NOAM and click reboot. Select the Active NOAM server and click Reboot. After rebooting the Active NOAM Server the GUI will go away. Please Establish a GUI session on the NOAM by using the XMI VIP address. Login as user "guiadmin" after some time.

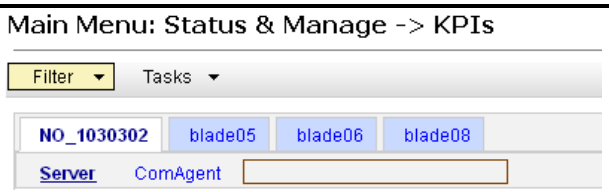
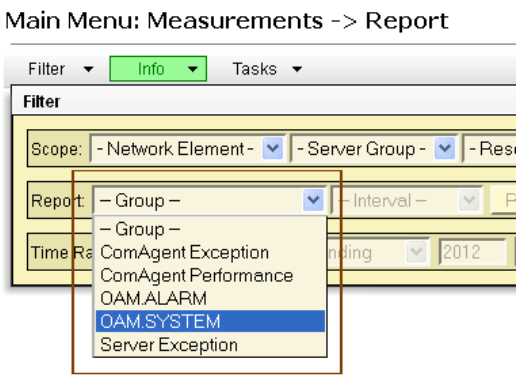
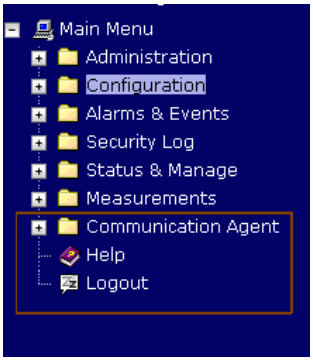
7.2.5 Post PCA Deactivation System Health Check

7.2.5.1 System health check after PCA Deactivation on NOAM server

Detailed steps are given in the procedure below.

Procedure 46: Verification of application deactivation on NOAM Server

S T E P #	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	Verify that KPIs menu don't show the KPI tabs for PCA, SBR, SBR-Binding and SBR-Session.

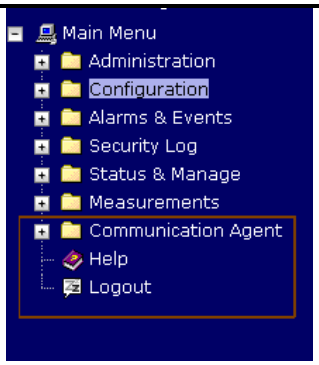
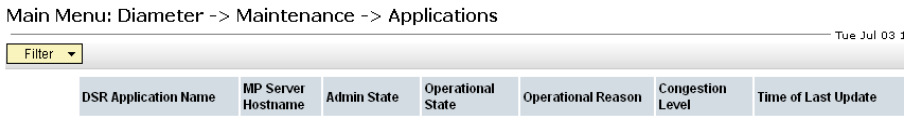
	the KPIs are not shown for PCA, SBR, SBR-Binding and SBR-Session.	
4	**NOAM VIP:** Verify that the Measurement groups are not shown for OC-DRA, P-DRA and SBR.	Verify that Measurement groups are not shown for OC-DRA, P-DRA and SBR. 
5	**NOAM VIP:** Verify that the Main Menu don't show the Policy and Charging submenu.	Verify that Main Menu on Active NOAM doesn't show the Policy and Charging submenu. 

7.2.5.2 System health check after Application Deactivation on SOAM servers

Detailed steps are given in the procedure below.

Procedure 47: Verification of application deactivation on SOAM Servers

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.

8.0 APPENDIX-B

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

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

S T E P #	This procedure restarts the DA-MP servers in a specific order so that the traffic loss is minimized. 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:** 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 ☐	Select a DSR site	Chose a DSR site where the DA-MP servers will be restarted.
3 ☐	**SOAM VIP:** Identify the DA-MP Leader	Establish a GUI session on the Active SOAM of the site chosen in Step 2 by using the XMI VIP address. Login as user "guiadmin". Navigate to **Main Menu: Diameter -> Maintenance -> DA-MPs** Locate and note the MP Server hostname for which the value in the "MP Leader" column is set to yes.
4 ☐	**NOAM VIP:** Restart a set of DA-MP servers	Navigate to **Main Menu: Status & Manage -> Server** Select a set of DA-MP servers in the site chosen in Step 2 such that the remaining DA-MP servers in the site are able to handle the additional traffic when the selected DA-MP servers are restarted. Click **Restart**. **NOTE**: The DA-MP Leader loacted in step 3 must be included in the last set of DA-MP servers to be restarted to minimize DA-MP Leader switches.
5 ☐	**NOAM VIP:** Restart next set of DA-MP servers	Repeat Step 4 for the next set of DA-MP servers until all DA-MP servers in the site chosen in step 2 have been restarted.
6 ☐	**NOAM VIP:** Repeat for all DSR Sites	Repeat Steps 2 to 5 for all DSR sites.

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

S T E P #	This procedure reboots the DA-MP servers in a specific order so that the traffic loss is minimized. 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:** 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:** Select a DSR site	Chose a DSR site where the DA-MP servers will be rebooted.

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