

# Oracle Communications Policy Management

Concepts for Wireless Networks  
Release 12.1

ORACLE WHITE PAPER | NOVEMBER 2015

## **TABLE OF CONTENTS**

<b>INTRODUCTION</b> .....	<b>1</b>
<b>USE CASES</b> .....	<b>2</b>
<b>OCPM COMPONENTS</b> .....	<b>2</b>
SERVER REDUNDANCY .....	3
<b>UNDERSTANDING POLICY MANAGEMENT</b> .....	<b>5</b>
POLICY TRIGGERS .....	5
POLICY CONDITIONS .....	5
POLICY ACTIONS.....	6
POLICY EXAMPLE.....	6
<b>OCPM FUNCTIONAL OVERVIEW</b> .....	<b>8</b>
POWERFUL POLICY SUPPORT.....	8
SCALABILITY AND RELIABILITY .....	9
FLEXIBLE NETWORK DEFINITION .....	9
ADDITIONAL FUNCTIONS .....	10
OPERATIONAL SUPPORT.....	11
<b>OPERATING YOUR SYSTEM</b> .....	<b>13</b>
INITIAL SYSTEM SETUP .....	14
POLICY CREATION AND DEPLOYMENT .....	17
MONITORING AND MANAGEMENT .....	20
<b>PLANNING CONSIDERATIONS</b> .....	<b>29</b>
HARDWARE SELECTION .....	29
NETWORK TOPOLOGIES .....	29
CAPACITY CONSIDERATIONS .....	32
MULTI-LEVEL OAM.....	33
<b>APPENDIX A: NETWORKING AND SECURITY OVERVIEW</b> .....	<b>35</b>
SECURITY .....	35
NETWORKING .....	35
<b>APPENDIX B: WIRELESS SOLUTIONS</b> .....	<b>37</b>
3GPP SUPPORT.....	37
RELATED ORACLE PRODUCTS.....	38
ORACLE SOLUTIONS.....	39
<b>APPENDIX C: REFERENCE DOCUMENTS</b> .....	<b>40</b>

## LIST OF FIGURES

FIGURE 1: SAMPLE PACKET FLOW THROUGH OCPM .....	3
FIGURE 2: OCPM CLUSTER RESILIENCY .....	4
FIGURE 3: CMP NAVIGATION BAR.....	13
FIGURE 4: USER ADMINISTRATION SCREEN.....	14
FIGURE 5: TOPOLOGY SETTINGS SCREEN.....	15
FIGURE 6: SNMP SETTINGS SCREEN.....	15
FIGURE 7: SUBSCRIBER PROFILE PAGE .....	16
FIGURE 8: SELECTING POLICY CONDITIONS .....	19
FIGURE 9: SAMPLE POLICY.....	20
FIGURE 10: SYSTEM-WIDE REPORTS .....	21
FIGURE 11: KPI DASHBOARD .....	22
FIGURE 12: ACTIVE ALARM REPORT.....	23
FIGURE 13: ALARM HISTORY REPORT .....	23
FIGURE 14: TRENDING REPORT EXAMPLE.....	24
FIGURE 15: POLICY SERVER (MPE) ADMINISTRATION SCREEN .....	25
FIGURE 16: STATISTICS SETTINGS .....	26
FIGURE 17: MPE REPORTS .....	27
FIGURE 18: CMP BULK OPERATIONS .....	28
FIGURE 19: STANDALONE PCRF NODE TOPOLOGY (SERVER A IS ACTIVE FOR ALL CLUSTERS).....	30
FIGURE 20: STANDALONE PCRF NODE TOPOLOGY (SERVER B IS ACTIVE FOR SOME CLUSTERS).....	30
FIGURE 21: INTERCONNECTED PCRF NODES (GEODIVERSE) TOPOLOGY .....	31
FIGURE 22: GEOREDUNDANT DESIGN TOPOLOGY .....	31
FIGURE 23: GEOREDUNDANT DESIGN WITH SITE FAILURE .....	32
FIGURE 24: THREE-SITE GEOREDUNDANT DESIGN (SIMPLIFIED VIEW).....	32
FIGURE 25: TWO CMPs MANAGING TWO SEPARATE NETWORKS .....	34
FIGURE 26: MULTI-LEVEL OAM FOR CENTRALIZED PROVISIONING AND ALARM MONITORING .....	34
FIGURE 27: ORACLE CONVERGED WIRELESS ARCHITECTURE.....	37
FIGURE 28: DIAMETER PHYSICAL CONNECTIVITY .....	39

## LIST OF TABLES

TABLE 1: SAMPLE POLICY TABLE .....	8
TABLE 2: VALIDATED HARDWARE FAMILIES .....	29
TABLE 3: OCPM CAPACITY M ETRICS .....	32
TABLE 4: OCPM SIGNALING INTERFACES .....	37
TABLE 5: REFERENCE DOCUMENTATION .....	40

## List of Terms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AAR	Authorization Authentication Request (Diameter message)
CCR	Credit Control Request (Diameter message)
CMP	Configuration Management Platform
COMCOL	Oracle database application used by OCPM
DPI	Deep Packet Inspection
DRA	Diameter Routing Agent
DRMA	Distributed Routing Management Application
GGSN	Gateway GPRS Support Node (system)
Gx	3GPP reference point between PCEF and PCRF
Gy	3GPP reference point between PCEF and OCS
HSS	Home Subscriber Service (system)
IP-CAN	Internet Protocol Connectivity Access Network
KPI	Key Performance Indicator
MCC	Mobile Country Code
MNC	Mobile Network Code
MPE	Multimedia Policy Engine
MRA	Multiprotocol Routing Agent (also referred to as the Policy Front End (PFE))
NE	Network Element
NFV	Network Functions Virtualization
OCPM	Oracle Communications Policy Management (product)
OCS	Online Charging System (system)
OCDM	Oracle Communications Data Model (product)
OCSG	Oracle Communications Services Gateway (product)

Acronym	Meaning
OFCS	Offline Charging System (system)
OSSI	Operations Support Systems Interface
OTT	Over The Top
PCC	Policy Charging and Control
PCEF	Policy and Charging Enforcement Point (system)
PCRF	Policy and Charging Rules Function
QoS	Quality of Service
RADIUS	Remote Access Dial-In Authentication Service
RAR	Re-Auth Request (Diameter message)
PFE	Policy Front End
PGW	PDN Gateway
RAT	Radio Access Type
RMA	Rack Mount Server
Rx	3GPP reference point between the PCRF and Application Function (AF) such as a P-CSCF
Sh	3GPP reference point between the PCRF and Subscriber Profile Repository (SPR) or Home Subscriber Server (HSS)
Sd	3GPP reference point between the PCRF and Traffic Detection Function (TDF)
SNMP	Simple Network Management Protocol
SPR	Subscriber Profile Repository (system)
Sy	3GPP reference point between the PCRF and On-Line Charging System (OCS)
TDF	Traffic Detection Function
TPS	Transactions Per Second
UDR	User Data Repository (system)
VoLTE	Voice over LTE
XML	Extensible Markup Language

# Oracle Communications Policy Management

## Release 12.1 Overview (Wireless & Fixed Networks)

### Introduction

Network Service Providers have an ever increasing need to exert more sophisticated control over their network resources. In addition to optimizing the network for speed, efficiency, security, and cost reduction, there are new challenges in capturing, maintaining, and growing subscriber revenue. Smart phones and other “smart” devices, coupled with the growing availability of data bandwidth, have allowed subscribers to cultivate direct relationships with Over-The-Top (OTT) content providers. Subscribers have also come to expect more sophistication and granularity in personalization of the services they consume from both content and service providers. Further complicating the picture, content providers have begun to seek guaranteed bandwidth from service providers in order to offer their customers more options and a better experience.

The service provider’s secret weapon in harnessing and capitalizing on the full capabilities of their network resources lies in a robust and sophisticated policy management system. For wireless networks, this function is provided by a Policy Charging and Rules Function (PCRF) device, as defined by the 3GPP organization. For cable networks, this function is provided by Packet Cable Multimedia (PCMM), defined by CableLabs. Oracle Communications Policy Management (OCPM) provides both of these functions. This document focuses on the OCPM support for wireless networks.

Oracle Communications Policy Management provides the flexible and resilient network policy system needed to meet the demanding requirements of today’s network service providers. This market-leading independent policy management system provides standards-based, multi-vendor interoperability with a wide range of third party network functions, including 3G/LTE/cable gateways, charging systems, subscriber databases, content filters, and content optimization systems. Its GUI-driven, natural language policy creation wizard provides an intuitive and flexible environment for easy and efficient creation of complex network policies. Its high scalability and resiliency provide a dependable backbone for the largest and most demanding 3G/LTE, wireline, and cable networks.

OCPM is a powerful, flexible scalable PCRF which is in production in over 60 operators in 39 countries in support of a broad range of use cases including LTE services and VoLTE. In addition to providing you with feature-rich ability to control your network, it allows you to implement marketing strategies by allowing rapid deployment of new use cases. The highly scalable and resilient architecture provides the telco-grade reliability required to support the current explosive growth in subscribers and services.

OCPM’s wide range of capabilities enables you to rapidly roll out converged services across multiple access networks including wireless 2G/3G/4G networks with or without VoLTE, fixed line networks and wireless LANs. Strengths include:

- Extensive 3GPP support: OCPM supports a wide range of 3GPP-defined parameters (AVPs), procedures and functionality. In addition, OCPM provides tremendous flexibility by allowing you to dynamically define new 3GPP and operator-specific AVPs, custom codec support, storing received information for later use, and providing the ability to build policies using a library of over 150 conditions which can be checked.
- Advanced VoLTE functionality: In addition to retaining information across site failures to ensure session continuity, OCPM provides leading-edge functionality in support of VoLTE including support for emergency calling and network location.
- Integrated Wireline (RADIUS CoA) support: OCPM can interface with BRAS using the RADIUS CoA support, allowing the same policy solution to support converged wireless and fixed line deployments.

- Integrated quota management: OCPM integrates with numerous quota repositories including Oracle's SPR, industry standard Online Charging Systems (OCS) as well as selected proprietary third party systems.
- Wide range of interfaces: In addition to supporting standard 3GPP Diameter interfaces including S9, OCPM can send notifications using SMS or HTML, and can interface with Oracle Communications Services Gateway to support non-Diameter interfaces.

This document is written as a guide to educate the user on the capabilities of the Policy Management solution and summarize the top considerations for planning your deployment.

## Use Cases

Some of the use cases enabled by OCPM, typically for either individual subscribers or established pools of users, include:

- Limit download speeds during peak times in order to avoid network congestion, while allowing higher data rates during off-peak times
- Control network access and charging for access to specific services
- Offer tiered service levels which provide different performance parameters (e.g., gold level service has higher throughput and provides higher monthly data allowance)
- Establish guaranteed bandwidth paths to ensure good quality service for high revenue applications (e.g., gaming)
- Set aggregate usage thresholds to notify subscribers (e.g., when they exceed 80% of quota) or enforce limits (e.g., throttle when reach 110% of quota or redirect to a self-service portal)
- Limit the number of simultaneous application sessions (per subscriber or per application)
- Pre-paid access, either for a specified period of time (e.g., per day) or usage (e.g., per GB)
- Immediate on-demand bandwidth increase to support heavy volume (turbo button)
- Loyalty programs which provide free or reduced-cost access to services
- Subscriber / parental controls to block/allow access to specific sites at specified times
- Access specific other subscribers ("family and friends calling circle"), to specific websites ("free music streaming"), or during off-peak hours (e.g., "free nights and weekends") without reducing monthly allowances
- Prioritize specific traffic types including emergency calls, medical devices or VPN services

## OCPM Components

OCPM consists of the following components:

- MPE: The Multimedia Policy Engine (MPE) implements the majority of the PCRF functionality provided by OCPM. When a request is received, the MPE contacts external data sources to find additional data related to the request and execute policies based on all known information and then processes the operator-defined policies.

- MRA: The Multi-Protocol Routing Agent (MRA) is a stateful load balancer that selects which MPE will support each initial subscriber requests, based on how loaded each MPE is. Subsequent requests for the same subscriber are then forwarded to the MPE assigned for that subscriber. The MRA also correlates traffic between different sessions. The MRA is also referred to as the Policy Front End (PFE) to highlight that this is not a general-purpose Diameter router.
- CMP: The Configuration Management Platform (CMP) provides system configuration and provisioning policies. It also provides a consolidated view of system alarms and logs for managing/monitoring MPEs and MRAs. CMP also provides an OSSI XML API for exporting/importing information to/from external systems. For large installations, CMP functionality can be distributed between two tiers: A centralized Network CMP (NW-CMP) for provisioning and centralized monitoring, and multiple System CMPs (S-CMP) for managing independent systems.

Each server can run on a dedicated server or as a virtualized application. PCRF node scaling is achieved by adding MPEs. Once MRA capacity is reached, additional MRA clusters may be added with additional MPEs.

Figure 1 provides an illustrative flow through an OCPM node, such as when an initial subscriber session request is received:

1. A subscriber request is received by the MRA, which determines which MPE should process this message and forwards the packet to that server. Load conditions are shared between MRA and the MPEs using Oracle's Distributed Routing Management Application (DRMA) protocol. In this example, the MRA has selected MPE cluster 2 to support this new subscriber request, and has forwarded the message to the active server in that cluster.
2. The MPE queries external data sources such as subscriber repositories (SPR/UDR/HSS) and/or online charging servers (OCS) to gather information about the subscriber.
3. Once all information is received, the MPE processes the policies to determine the appropriate actions, and forwards the response to the MRA.
4. The MRA performs any required processing and forwards the response to the requester.

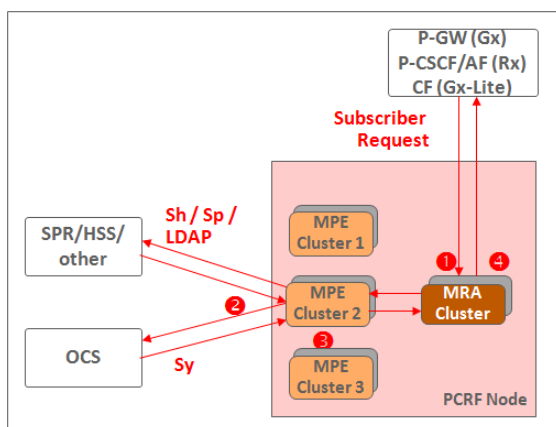


Figure 1: Sample Packet Flow through OCPM

## Server Redundancy

Redundancy is implemented for each component as described below.

### High Availability Cluster (MPE, MRA, CMP)

The basic unit of resiliency within the OCPM is the high availability (HA) cluster, which is a pair of co-located servers which are continually synchronized. These servers may be identified in any of several ways:

- The physical servers are referred to as server A and server B. They are also referred to as *primary* and *standby* servers.
- At any given time, either server may be in the active state, while the other server is in a backup state. The active server processes packets and continually updates the backup server about known sessions so that it can take over if needed.

MRA, MPE and CMP can all be implemented as HA clusters.

Note that each cluster independently determines which server is active. For example, the primary server (server A) may be active for one MPE cluster, while the standby server (server B) is active for another MPE cluster.

### Geographic Redundant Cluster (MPE, MRA)

MRA and MPE clusters may be extended by adding a third server, also called server C or the spare server. This server resides at a different site, but is continually synchronized with the active server. The spare server becomes active if neither server at the primary site is reachable, which may happen if connectivity is lost to that site. When MRA/MPE geo-redundancy is employed, a spare server is typically deployed for every cluster.

Again, each cluster independently determines which server is active. For example, server A may be active for one cluster, server B can be active for a different cluster, and server C can be active for a third cluster. The active server in each cluster continually updates both backup servers.

### Disaster Recovery Cluster (CMP)

Since there can only be one active CMP in the network, an additional level of redundancy is available for this component. You can manually switch to using a separate disaster recovery CMP (DR-CMP) cluster if a power failure occurs at the primary site or a network outage prevents reaching the primary CMP cluster. The DR-CMP is typically located at a backup site.

Figure 2 illustrates the various resiliency schemes. Under normal operation, the primary server at the primary site (site 1) would be the active server, which is shown using a different color.

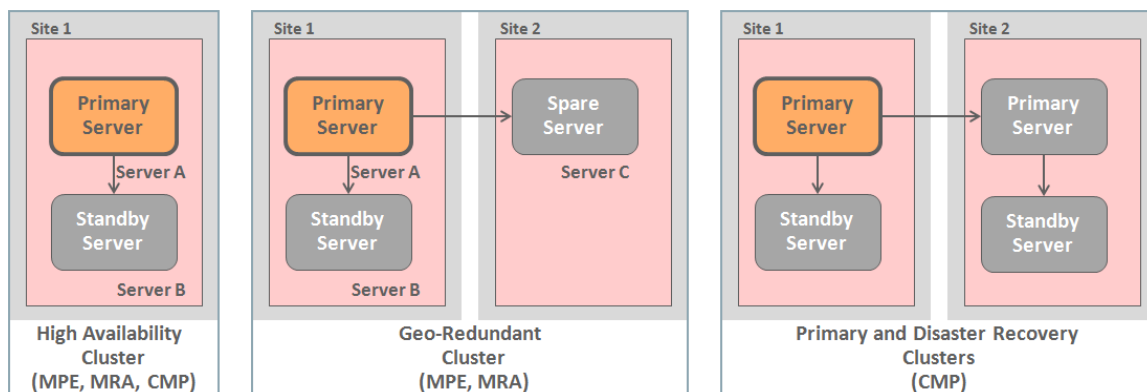


Figure 2: OCPM Cluster Resiliency

### Non-Redundant Servers (for Lab Systems)

For functional lab testing, CMP, MRA and MPE can all operate without any redundancy.



## Understanding Policy Management

A PCRF such as OCPM takes predetermined actions based on received packets and also executes operator-defined *policy rules*. A policy rule is a statement which defines actions which are taken when one or more conditions are met. There are three key components:

- Policy Trigger: An event which causes policies to be *evaluated*
- Policy Condition: The criteria which are evaluated.
- Policy Action: Actions which occur if the condition is met.

### Policy Triggers

OCPM executes operator-defined policies which perform appropriate action(s) based on specified conditions. Policy evaluation is most commonly triggered when a message is received from another device, including PCEF (via Gx interface), AF (via Rx interface), DPI/TDF (via Sd interface), SPR/UDR/HSS (via Sh/Sp/LDAP interfaces), and OCS (via the Sy interface). Policy evaluation can also be triggered based on internally-generated time and day information. This allows you to define time periods and associated actions to be performed when time transitions from one period to another.

Some triggers cause OCPM to contact other data sources to gather additional information. For example, when receiving an initial session request (Gx:CCR-I message), OCPM typically retrieves the subscriber's provisioned information/entitlements and quota related information (from an Oracle SPR/UDR or third party repository) and stores these data elements in its local database. Once the relevant information is in place, OCPM can use the information in the message, information about the subscriber from other systems/components, as well as state information (that is, information previously learned) stored in OCPM to evaluate the policy conditions.


OCPM can limit the number of total (Gx, Gx-Lite and Rx) sessions that a subscriber can have. OCPM correlates the various sessions for each subscriber, or pool of subscribers such as a family plan, if supported by the subscriber repository using either a user identifier such as IMSI or MS-ISDN, or using network session information such as IP address and APN. Policy conditions and actions can utilize all the available information regarding a subscriber when decisions are evaluated. For example:

- Receiving a VoLTE session request across the Rx interface typically results in OCPM sending an updated PCC rule to the PCEF.
- OCPM can determine roaming status via the PCEF Gx information and then push down roaming rules to a DPI device.
- OCPM can use quota-related information gathered over Gx+ with a DPI device to enable different rules on Gx with the PCEF.

OCPM can maintain sessions on multiple Gx interfaces with different PCEFs for a given subscriber session. A single trigger event can cause OCPM to install new policy rules to multiple PCEFs.

### Policy Conditions

The overall policy condition includes one or more conditions which are checked, connected by logical AND, OR, and NOT operators. Many (but not all) conditions check for specific values using the format "if parameter operator value", e.g., "where RAT-Type is equal to WLAN". Policy conditions can also check for the presence of specific information (e.g., if the time zone AVP exists"), ranges ("if the bandwidth is between 100 Mbps and 200 Mbps") and



many other conditions. You can also define (via GUI or importing) match lists of items to be checked in policy conditions. For example, you can check whether the SGSN/SGW address that is included in the Gx:CCR-I trigger message is (or is not) included in an imported SGSN/SGW file. In addition, OCPM can operate using either the subscriber local time zone or the system local time zone.

A policy does not need to have any policy conditions defined. In this case, the policy actions are always applied.

### Policy Actions

OCPM supports over 100 policy actions. The most common policy action specifies how a subscriber should be treated. For example:

- A gold subscriber supports 1 Mbps access uploads and downloads and have unlimited monthly data allowance
- A silver subscriber downloads data at 768 Kbps and uploads data at 384 Kbps
- A bronze subscriber downloads data at 512 Kbps and uploads data at 256 Kbps.

This occurs by setting values and pushing rules to other network devices. This can be a new rule, an update to an existing rule, or an instruction specifying which pre-programmed rule should be used. Of course, rules are removed when a session terminates.

OCPM can instruct the device to redirect traffic to a different port, send SMS notifications to one or multiple subscribers, and generate email messages. Alarm/Trap/Syslog notifications can also be sent to network operations center. In addition, many actions are also available to modify the available quota.

### Policy Example

A pseudo-code example of a complex policy is:


#### **IF (Policy Conditions)**

1. This subscriber is entitled to video AND
2. is connected to a UMTS network AND
3. is in their home network (is not roaming) AND
4. cumulative usage for this billing cycle is less than quota threshold AND
5. the number of sessions currently admitted behind this SGSN/SGW is less than the maximum allowed AND
6. video is allowed during this time period

#### **THEN (Policy Actions)**

7. Admit session
8. Set the minimum guaranteed downstream bandwidth to 1 Mbps
9. Set the maximum allowed downstream bandwidth to 2 Mbps
10. Enable video service (only)

The first line of the policy rule checks against subscriber entitlements which is information retrieved via the UDR. Lines 2 and 3 of the statement checks specific data retrieved from the PCEF. Line 4 involves checks based on



usage information, and Line 5 is a resource threshold check based on OCPM keeping track of resources associated with nodes in the network. Line 6 verifies that the subscriber is entitled to the services during the time of day.

The actions which are executed if these conditions are met appear on the last few lines. In this case the session is allowed for video service only, and the allowable bandwidth is set.

The actual policies are written via a graphical rules creation wizard called Policy Wizard. Available policy conditions and actions are described in the *Policy Wizard Reference Guide*.

## OCPM Functional Overview

This section provides a brief overview of major capabilities provided by Oracle's PCRF implementation. Provisioning of these functions is performed using CMP.

### Powerful Policy Support

#### Policy Wizard

OCPM supports over 250 policy conditions and 150 policy actions. CMP's Policy Wizard walks you through the process of creating policies. Policies can be created from scratch, or an existing policy can be used as the basis for a new policy. You select the desired condition (e.g., "where RAT\_Type is equal to <value>") or action (e.g., "set QCI to <value>") from a list, and then click on the appropriate fields to specify the desired values. Complex policy conditions can be created using AND, OR and NOT modifiers. Policy Wizard is described later in this document.

#### Policy Tables

Policy Tables can reduce the number of policies required when only a few variables change between different policies. Each row in the Policy Table represents a set of policy conditions and actions. Some columns (referred to as key fields and shown in red in Table 1) identify the policy conditions, while other columns define the required policy action. When all key columns are matched within a single row, then the corresponding actions identified in the remaining columns are executed. For example, the following table allows using a single policy to install and remove PCC rules on APNs, instead of requiring four separate policies:

**TABLE 1: SAMPLE POLICY TABLE**

APN	Install PCC Rules	Remove PCC Rules
telco.g1t1	telco rulebase qos t1	modem stop qos
telco.g1t2	telco rulebase qos t2	modem stop qos
telco.g2t1	modem stop qos	telco rulebase qos t1

#### Policy Variables

Policy Variables increase the power of the system by allowing you to store information about activity and use this information later in policies. All variables except pre-defined items are set and removed via Policy Actions, and all can be used in subsequent Policy Conditions. The following types of policy variables are available:

- *Substitution variables* are predefined variables that are available during policy rule execution. A simple example is "{Time}" which would be replaced by the time at which the policy rule that references it is evaluated.
- *Policy Table variables* reference a policy table column.
- *Policy Evaluation variables* last for the lifetime of a policy evaluation cycle (the process of evaluating all the policies for a single request/context).
- *Session State variables* last while the associated session is valid. Once the session is terminated these variables will no longer be available for use in policies.
- *Subscriber Local State variables* last while the associated subscriber has at least one session. Once the last session is terminated these variables will no longer be available for use in policies.

- *Subscriber Remote State variables* persist remotely in an SPR as long as the subscriber exists in the SPR. Using these variables requires that an SPR/HSS be configured that is capable of storing these variables.

## Scalability and Reliability

### Load Balancing and Session Correlation

For initial session requests, the MRA selects which MPE supports the session based upon each MPE's current load. For established sessions, the MRA forwards subsequent messages for this session to the assigned MPE. In addition, the MRA provides session correlation, forwarding requests for the same subscriber to the same MPE.

For initial session requests, the MRA selects which MPE supports the session. Each MPE passes load status information to its MRA, allowing the MRA to intelligently make this decision. For established sessions, the MRA forwards subsequent messages for this session to the assigned MPE. In addition, the MRA provides session correlation, forwarding requests for the same subscriber to the same MPE.

### Pay as You Grow

MPEs can be added dynamically as your network grows, without modifying existing network elements. This approach also reduces the mesh of Diameter connections, allowing the PGW to forward traffic to a small number of MRAs rather than a larger number of MPEs.

PCRF nodes (MRAs with MPEs) can be added to allow additional growth. Up to ten OCPM nodes can be associated together to share information, or each node can support a designated network segment.

### Redundant Design

Each function can run on two (HA) or three (georedundant) servers. The active server is continually updating the other servers to ensure they can take over if a server fails.

In addition, many network elements and data sources (SPR, OCS) can be dual-homed to OCPM nodes at different sites. This improves reliability by allowing the overall wireless signaling network to route around individual connection failures.

### Congestion Management (Load Shedding)

When congestion occurs, OCPM can notify upstream devices that the packets cannot be processed. In addition, incoming messages are selectively rejected based upon how much congestion exists. For example, at the lowest congestion level, new session requests (CCR-I) are rejected so that the sender can resend them to a different system. Default actions are provided but can be modified by the operator. The load shedding infrastructure takes into account all Diameter applications and the request types when performing admission control on the corresponding requests.


### Stale Session Cleanup

If a subscriber session has existed for longer than its configured maximum validity time without any explicit updates from the corresponding gateway, or if a more recent session exists for the same subscriber and protocol, the session is considered "stale" and will be removed. This cleanup behavior is configurable.

## Flexible Network Definition

### Flexible Data Sources

OCPM can retrieve information from LDAP, SPR and OCS data sources before policies are evaluated. To ensure availability, each data source includes one to four servers which will be checked sequentially to retrieve the requested information. In addition, information retrieved from a data source query can be used as the key for



querying a secondary data source. Queries to OCSs can also be triggered by policy evaluation. Queries can be directed to different data sources based upon the subscriber, and different keys can be used when querying different data sources.

### **Custom AVPs**

OCPM allows you to easily define new AVPs using standard or experimental formats. This allows you to easily support new capabilities without updating your OCPM software. In addition, any known AVP can be inserted into messages, including Diameter applications that they are not originally specified for.

### **Codec SDP Support**

You can create policies which set traffic parameters based upon most codec-data SDP information. In addition, OCPM supports default bandwidth settings for numerous codecs including AMR, AMR-WB and T.38 (fax).

### **Additional Functions**

#### **Advanced Quota Management**

OCPM's quota management features allow you to implement policy control based on subscriber usage, without requiring an OCS. When a subscriber first attaches, OCPM retrieves information about the subscriber's quota/balance from the charging system. When a subscriber detaches, the updated balance information can be pushed back to the charging system. OCPM can also subscribe to be notified of quota changes.

OCPM supports quota management in conjunction with several charging systems, including Oracle's SPR/UDR. OCPM and SPR/UDR exchange quota information using the Sp interface. Oracle pioneered the use of quota management across the Gx interface, and these enhancements have now been adopted by 3GPP.


Based on information about subscriber usage, policy decisions can be made and policy rules can be pushed to the PCEF or TDF to change enforcement. This OCPM can use quota information in policy conditions to take actions such as:

- Set or modify the quota available to this subscriber.
- Grant the user a quota (e.g., volume/time) and set a volume/time threshold for when the PCEF needs to re-authorize with OCPM (acting as Quota Manager) for additional units.
- Query the PCEF to determine the amount of usage (at any point in time mid-session) and potentially grant more.
- Redirect the user session to a top-up portal where they can recharge units, Advice of Charge portal to notify and/or for the user to explicitly accept charges, or a to a Customer Care portal.
- Terminate the credit control session (normally in the case where the user runs out of granted units) or particular service.
- Install dynamic subscriber rules, such as throttling the user once a quota threshold is exceeded.

Specific controls and capabilities vary depending on the signaling interface and parameters provided. Subscriber pools (e.g., family plan) as well as individual subscribers are supported.

OCPM can also receive quota information from the PCEF when the quota has been deleted (quota breach) or updated (quota reallocation) and use this information in policies. The billing day can be changed within the current billing cycle if the user has no usage recorded, the next billing cycle, or when starting a new session.

### **Subscriber Notifications**



You can create policies to send SMS notifications to subscribers for identified events, such as exceeding quota or reaching a pre-defined threshold. In addition, the can create a policy to send a “generic” HTML notification. This function allows you to specify all the information in the policy, including the destination IP address and complete message.

### **Integrated RADIUS Change of Authorization (CoA)**

OCPM has a flexible mechanism to support sending RADIUS CoA messages to Broadband Access Remote Servers (BRAS) to set service capabilities. Typically this is used for subscribers using fixed wireline access networks such as DSL or PON. Sending of these messages is determined by policy evaluation. The CoA messages can be sent when the wireline subscriber initiates a session or based upon information received from the Sy or Sd interface. In addition to supporting standard IETF RADIUS Type-Length-Value (TLV) attributes, OCPM includes pre-defined dictionaries of Vendor-Specific Attributes (VSA) for some common BRAS equipment and allows you to add new dictionaries or add entries into the supplied dictionaries.

### **S9 Interface**

OCPM supports the S9 interface for roaming. OCPM can function as both a Home PCRF (H-PCRF) and a Visiting PCRF (V-PCRF).

### **Second Level Authentication (2AS)**

New session requests for some users can be forwarded to a separate server to authenticate the subscriber. For instance, this may be an enterprise-controlled server which asks the subscriber for a password. The server then notifies OCPM via Rx that the session is allowed, and OCPM notifies the PCEF that this subscriber may access the network.

### **Topology Hiding**

The MRA supports optional topology hiding for Gx and Rx applications. These network elements do not see any information about individual MPEs, only the MRA.

### **Operational Support**


#### **Export/Import**

Existing policies and other information can be exported via the CMP GUI and later imported via the GUI if the operator wishes to “rollback” to a previous set of policies and/or traffic profiles/groups.

The import/export solution also provides several import options to indicate how data collisions/conflicts are handled. These include:

- **Delete all before importing:** All policies, policy groups, and templates currently on the CMP and all MPEs are deleted. You must manually deploy the policies to MPE after the import is complete.
- **Overwrite with imported version:** Existing items are overwritten with the imported versions. Any modified policies are automatically re-deployed to MPEs after the import.
- **Reject any that already exist:** All items are imported except for those which have the same name as existing objects. You must manually deploy the policies after the import is complete.
- **Any collisions prevent all importing:** No items are imported if any of the imported versions has the same name as any existing object. This is the default.

### **Policy Checkpoint**



CMP provides the ability to take a snapshot (“checkpoint”) of the deployed policies. If modifications result in unexpected behavior, you can re-apply this previously saved configuration. The data saved within this snapshot consists of all the data currently contained within the export file that is currently available from the CMP navigation pane, which includes all policies, policy groups, templates, traffic profiles, and traffic profile groups.

You can also delete a specific checkpoint from the saved list. This provides flexibility in pruning the number of saved checkpoints rather than simply deleting the oldest saved version.

### **Statistics Export**

OCPM statistics can be accessed by authorized servers. CMP can push statistics periodically or they can be pulled upon request. Information can be sent using XML or csv formats.



## Operating Your System

OCPM system configuration, policy provisioning and monitoring are performed via CMP. The primary operator interface is the graphical user interface, which is illustrated in Figure 3. Using the GUI, the operator can define servers and clusters, provision policies, monitor the system, upgrade software and perform administrative functions. This section focuses on the tasks required to get the system operational. Within the GUI, functions are selected from the menu in the left-hand frame, and parameters are configured and viewed in the main work area.

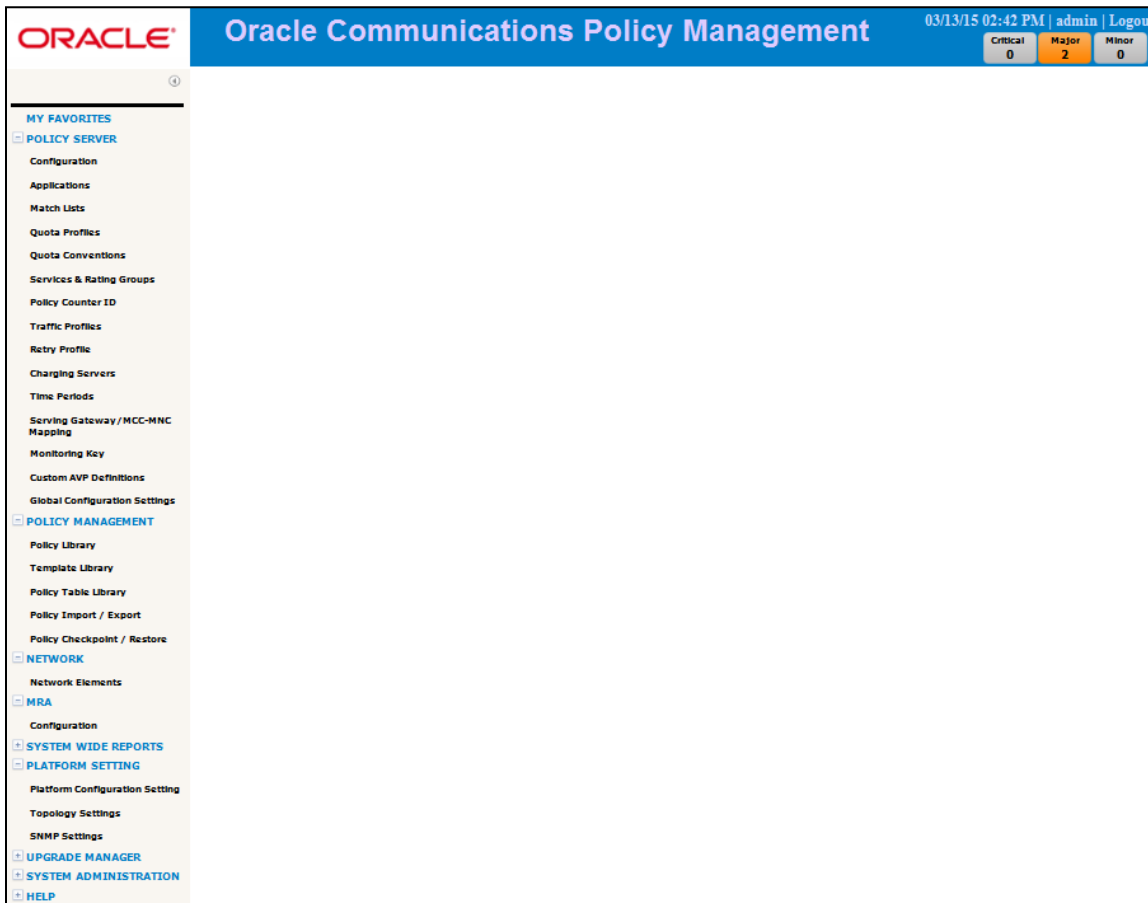


Figure 3: CMP Navigation Bar

Additionally, CMP supports an OSSI interface which allows bulk configuration data to be provisioned into, and queried from, the system. This interface uses XML documents snippets posted or retrieved over HTTP(s).

The user interface exposes a subset of the information available in use for evaluating policy conditions. The information that the operator sees can be customized by modifying an XML file.

The major steps to implement OCPM are:

- Initial system setup
- Policy creation and deployment
- Monitoring and management

## Initial System Setup

Initial system setup includes the following:

1. System Administration: Create an account for each authorized operator
2. Topology Definition: Define how servers are interconnected into clusters
3. Network Definition: Define the other devices (Network Elements, Data Sources, Online Charging Servers) which communicate with OCPM. At this point you can also include any one-time definitions, such as any custom AVPs which are used on your network.

## System Administration

The first step is to authorize operators to perform the various tasks. There are three default *roles*: Administrator, Operator and Viewer. The Administrator has all permissions, an Operator cannot access the User Management functions, and the Viewer can look but not change settings. New roles can be created, and the permissions of each role can be modified. Individual *user* accounts can point to the desired role. In addition, the *scope* of resources which can be modified by each user can also be defined. These functions are performed using the User Management screen under System Administration, which is shown in Figure 4.

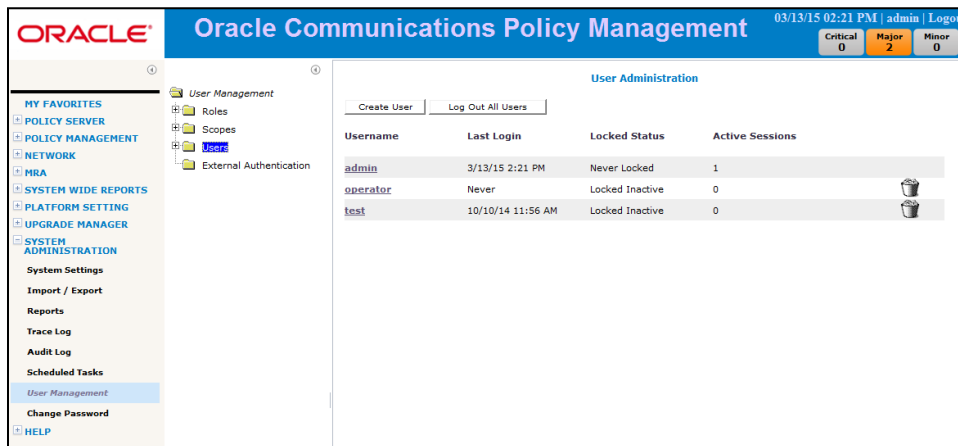


Figure 4: User Administration Screen

## Topology Definition

After installing the hardware, servers are assigned to clusters. Key decisions to be made in conjunction with Oracle include:

- Number of MPEs and MRAs required per site. This is based on the volume of traffic expected.
- Whether geo-redundancy is used, including locations of georedundant servers.

After the hardware is installed and configured, the following steps are required:

- Define each cluster. Individual servers are grouped into clusters using CMP.
- Assign MPE clusters to MRA clusters.

Figure 5 shows the Topology Settings screen which is used to define clusters.

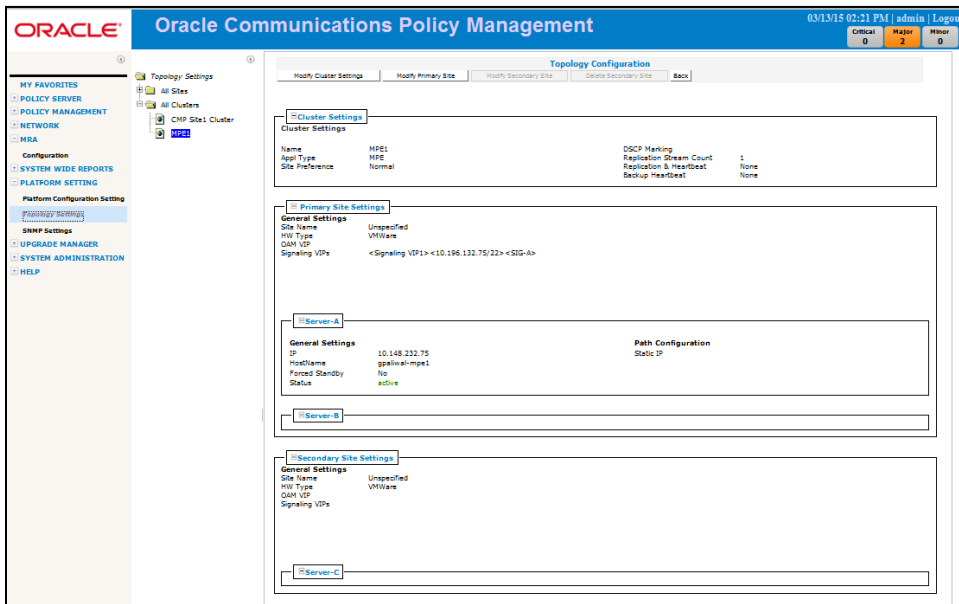


Figure 5: Topology Settings Screen

CMP is also used to define SNMP settings, as shown in Figure 6. OCPM can be configured so that CMP is the source of all traps. Alternatively, each server can generate its own traps. SNMP traps are listed in the *SNMP User's Guide*.

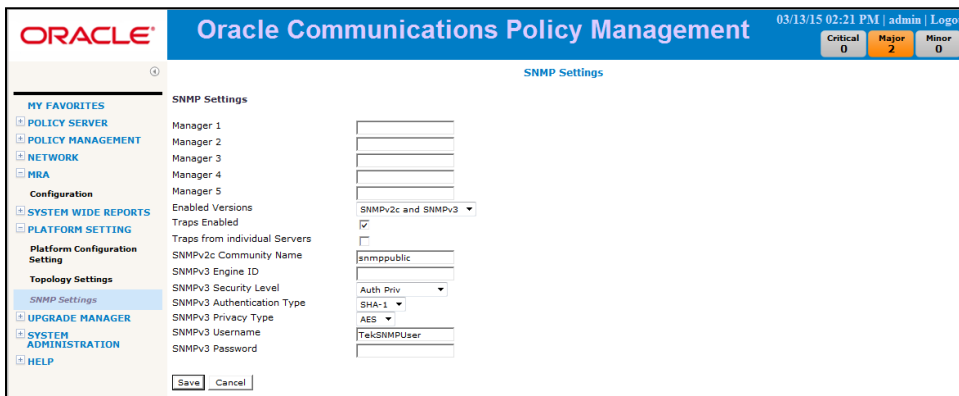


Figure 6: SNMP Settings Screen

When the time comes to upgrade to a later version of OCPM software, *Upgrade Manager* provides step by step guidance through the software upgrade. Multiple MRA/MPE servers can be upgraded simultaneously. If any issues arise, Upgrade Manager guides the operator through the backout procedure.

### Network Definition

Using CMP, you define the other devices with which OCPM communicates. By selecting from the navigation bar, you can configure:

- Network Elements, which are devices that can initiate connections (required). These include PGWs, GGSNs and TDFs.

- Serving Gateways (if needed). An SGSN/SGW may not provide a GGSN/PGW with mobile country code (MCC)/mobile network code (MNC) information, reducing OCPM's ability to detect specific roaming scenarios. This mapping table converts an SGSN IP address to the proper MCC/MNC value. Once the MCC/MNC values are determined, they can be used in policies to differentiate subscriber treatment based on the specific roaming scenario.
- Third Party AVPs (if needed): Most information is transmitted using Attribute Value Pairs (AVPs). Some network elements may support non-standard AVPs, or AVPs which were standardized after OCPM was installed in your network. In addition to the built-in support for standard AVPs, you can define additional AVPs which can then be used in policies. A policy condition can evaluate an AVP in Diameter messages, set an AVP using a user value in the UDR system or set a user value in the UDR using an AVP. A policy action can set or remove the AVP.

When using an OCS, the following parameters should be defined using CMP:

- Online Charging Servers: When an OCS is defined, OCPM requests quota information when establishing or updating subscriber sessions.
- Policy Counter Identifiers (if desired): OCPM communicates with OCS using 3GPP-defined policy counters. You can provision a name for each policy counter, which can then be used in policies. This optional ease-of-use capability is *not* required to communicate with an OCS.

To support quota management using an SPR/UDR, the following can also be defined using CMP:

- Subscriber Profile Repositories: CMP allows you to define subscriber profile repositories; find/create/modify/delete subscriber records using a variety of APIs; add subscribers to pools; and create/modify/delete quota profiles for subscribers/pools. These functions are supported using an Oracle RESTful API interface or a Diameter Sh interface.

**Subscriber Profile**

Subscriber Profile Configuration

Subscriber Key Fields	
NAI	361110420000001@nal.epc.mnc20.mcc208.3gpp.network.org
E.164 (MSISDN)	3611000001
IMSI	361110420000001

Subscriber Information	
Account ID	userA000001
Billing Day	30
Tier	Gold
Entitlements	VQIP
Custom 1	5085551212
Custom 2	
Custom 3	
Custom 4	
Custom 5	
Custom 6	
Custom 7	

Figure 7: Subscriber Profile Page

- Services and Rating Groups: A service identifies a class of traffic such as voice, peer-to-peer, or multimedia. For organizational purposes, you can associate services into rating groups.

- **Quotas:** This limits the amount of data, active session time, or service-specific events that a subscriber can consume. Quotas can be applied to individual services or to rating groups, and can be associated with a time period. A quota profile specifies default values for quotas and defines how quotas are implemented. There are two types of quota profiles: A plan describes a subscriber's basic, recurring service and may include time and volume limits which are computed automatically or through policy rules. A pass is a one-time override that temporarily replaces or augments a subscriber's default plan or service. Passes are common options for pre-paid subscribers, who frequently have limited or no data access via their basic plan, and may purchase passes to gain access to such services. While a pass is in effect, it may modify the Quality of Service (QoS) controls, charging parameters, or other configurable rules associated with a subscriber service. They can also be used to allow casual use and/or promotional plans for pre- or post-paid subscribers to purchase services on an occasional basis, for which they would not otherwise subscribe on an ongoing basis. A pass may be valid for a restricted interval or continuously available.
- **Quota Conventions:** These control rollovers and top-ups, which can override the basic quota. A *rollover* allows a subscriber to carry forward unused units from one billing cycle to another. A *top-up* allows a subscriber to obtain additional units for an existing plan.
- **Monitoring Keys:** This unique operator-defined string identifies the quota profile to be used by a policy and charging control (PCC) rule and application detection control (ADC) rule for usage tracking. The monitoring key is associated with the quota profile by selecting a policy action that grants usage to a selected number of quota profiles. Monitoring keys are a simplified way of communicating quota information between OCPM and other network elements to perform quota tracking.

## Policy Creation and Deployment

After the system has been created, you are ready to create policies. This includes the following steps:

- Create supporting objects which are referenced in policies
- Create the policies which are evaluated. Policies can also be collected into groups, which is simply a list of policies which are typically executed together. You can also create groups of groups.
- Deploy the policies to the MPEs. Different policies can be deployed to different MPEs, allowing you to test a set of policies on a test or FOA system before being deployed into the production network.

### Create Supporting Objects

To simplify policy creation, common information can be stored in separate supporting objects which are referenced by policies. There are several types of supporting objects:

- **Match Lists**, which are a list of possible values of a specified type (e.g., IPv4 addresses, or simple csv). For example, you can create a list of MCC/MNC values which represent operators with whom you have reciprocal roaming agreements.
- **Applications**, which are a list of IP addresses or Diameter identities which should be treated similarly, e.g., multiple servers performing the same function.
- **Traffic Profiles**, which is a set of pre-defined traffic parameters which are assigned to a subscriber. For example, one traffic profile can define the bandwidth and priority parameters for gold tier customers on an LTE network. Additional traffic profiles would be created for other customer tiers and network types. The appropriate traffic profile is applied via policy when a customer initially connects or moves to another type of network.

- Retry Profiles, which specify the circumstances under which installation of a policy and charging control (PCC) rule is retried if the rule is reported to have failed.
- Time of Day profiles, which define time periods which can be used when evaluating policies.

### Policy Provisioning

Policies are typically initially created using the Policy Wizard function within CMP, which walks the user through policy creation as follows:

1. Create a new policy from scratch, create a copy of an existing policy, or modify an existing policy.
2. Select the policy tables which are used as part of this policy
3. Select the desired policy condition(s), and fill in the appropriate values. Policy Wizard provides the valid choices, or performs validity checking on inputted data (e.g., ensure that the entered text is a valid IP address). Policy conditions can include any of the following:
  - The type of message which triggered policy evaluation (e.g., Gx:CCR-I)
  - Information included in that message (e.g., RAT-Type=WLAN)
  - Information included in messages in response to queries by OCPM (e.g., entitlement information included in the subscriber profile, received from the SPR)
  - Information previously stored by OCPM. OCPM keeps track of all session states, enabling it to perform the appropriate binding (and removal) of resources to subscribers and applications.

By default, all policy conditions need to be met for the policy actions to be applied. However, policies can also include logical OR and NOT operators to create complex policy conditions. Policies can be created which do not include policies conditions. Figure 8 shows a typical Policy Wizard screen for selecting policy conditions.

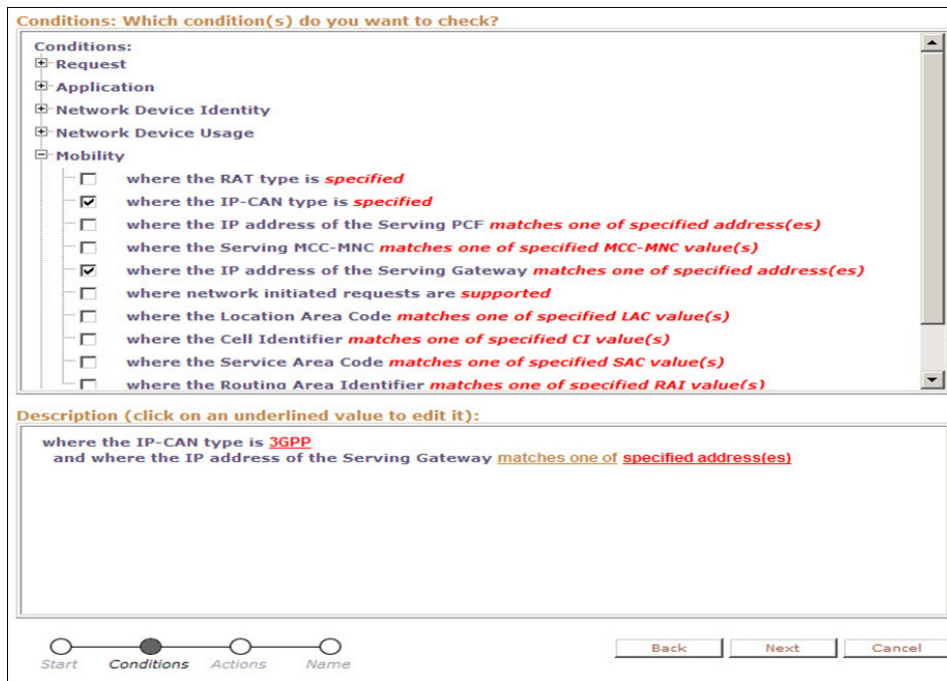


Figure 8: Selecting Policy Conditions

4. Select the appropriate policy action(s), again specifying values if needed. Policies can include a policy action which evaluates another policy (or Policy Group).

All policies must contain exactly one mandatory action from the following list:

- Accept message: After executing the current policy rule, OCPM continues with the normal processing of the protocol message but no further policy rules are evaluated.
- Break from policy level: Stop evaluating the current policy and continue policy evaluation with the next policy at the parent's level. This is applicable only when using *policy nesting*.
- Continue processing message: After executing the current policy rule, OCPM continues with the next policy rule.
- Reject message: After executing the current policy rule, OCPM terminates all policy-rule processing and rejects the current protocol message. For most application-level requests this translates into some type of error being sent back to the application.
- Skip to next device: Stop evaluating policies for the current device and continue policy evaluation with the next device. If there is no next device, policy execution ends.
- Skip to next flow: Stop evaluating policies for the current flow and continue policy evaluation with the next flow. If there is no next flow, evaluation continues with the next device; if there is no next device, policy execution ends.

5. Specify the name of the policy.

An example of a fully defined policy is shown in Figure 9:

**Name:** Apply\_QoS\_on\_Handoff

**Conditions:**

where the flow is [an application flow](#)  
and where the request is [modifying an existing session](#)  
and where the APN matches one of [ims\\*](#)  
and where the RAT type is [WLAN](#)  
and where the flow media type is one of [Video](#)  
and where the event trigger is one of [RAT\\_CHANGE](#)  
and where the AF-Application-ID matches one of [voip1](#)

**Actions:**

evaluate policy Apply\_QoS\_Parameters\_On\_Handoff  
evaluate policy WLAN\_IMS\_Audio  
accept message

Figure 9: Sample Policy

Policies can also be exported and imported using the OSSI/XML interface. This allows policies and supporting objects created on one system to be ported to other OCPM systems.

### Deploying Policies

After policies are defined, they are deployed to one or more MPEs. Different MPEs can execute different policies. Several tools are available to control how policies are executed:

- Policy Groups allow you to create a list of policies which are executed sequentially. These are useful when a set of policies are always executed together, and are also used with policy nesting. A policy group can also be a “group of groups” which contains other policy groups.
- Policy Nesting provides additional control over whether policies are evaluated, which also reduces processing requirements. For example, given the following policies and policy groups:

1. Policy1: Action=evaluate GroupA (which includes Policy2, Policy3)
2. Policy4

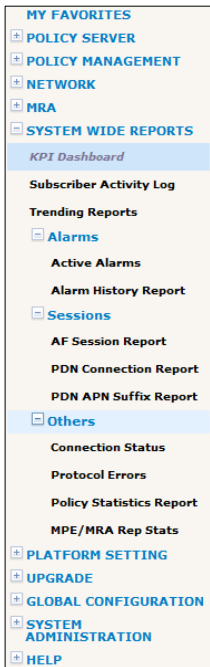
If any policy in GroupA evaluates to true *and* includes the “break from policy level” mandatory action, then subsequent policies in the same Policy Group are skipped. In this example, if Policy1 and Policy2 are true and Policy2 includes this action, then the order of policy evaluation is Policy1 > Policy2 > Policy4.

- Policy Ordering: In complex scenarios, the outcome of the policy execution depends on the order in which the policies are executed. OCPM allows you to specify the order in which policies are executed.
- MPE Groups: MPEs can be grouped together, simplifying the process of deploying the same policies to multiple MPEs. For instance, new policies can be tested on a single MPE, and then deployed to the MPE group which includes the remaining MPEs.

### Monitoring and Management



CMP provides detailed system management functions allowing the display of events or alarms received by the system and user management. Additionally the system audits all operations performed via the GUI as well as the OSS-I interface allowing configuration changes to be tracked by time and operator.



Monitoring functions include the following:

- KPI dashboard
- Alarms
- System-wide trending (graphical) reports
- System-wide tabular reports
- Server (MRA/MPE) reports

Most information is collected by individual servers and forwarded to CMP. Server (MRA/MPE) reports are found under the “Reports” tab in the “Policy Server (MPE) → Configuration” or “MRA → Configuration” sections. All other functions are available via system-wide reports, as shown in Figure 10. All system-wide reports refresh every 10 seconds unless disabled. Many system-wide reports are customizable to view individual servers, all MPE, all MRAs, or all servers. They can also be printed or exported using csv.

Figure 10: System-Wide Reports

### KPI Dashboard

The Key Performance Indicator (KPI) dashboard is the overall system monitoring screen which provides real-time monitoring of the aggregated error and alarm counters. The KPI dashboard tracks alarms and protocol errors as they are happening, which allows better monitoring to prevent events such as system overloads and outages.

The KPI dashboard displays each severity as a column. Each severity column contains the alarm counters of unacknowledged alarms. Alarm signaling is supported by the existing Oracle COMCOL alarm functionality. Figure 11 shows a sample KPI dashboard.

KPI Dashboard (Stats Reset: Interval / Last Refresh:12/27/2013 11:35:43)

Filters ▼ Change Thresholds

Performance				Alarms			Protocol Errors	
	TPS	PDN	Active Subscribers	Critical	Major	Minor	Sent	Received
<b>MRAs selected</b>	40	6000	6000	0	0	2	0	0
<b>MPEs selected</b>	41	6001	6003	0	0	2	0	0

Performance				Connections			Alarms			Protocol Errors				
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra17-118(Server-A)	Active	20 (0%)	3000	3000 (0%)	4	45	4 of 4	2 of 2	1 of 4	0	0	2	0	0
mra17-118(Server-B)	Standby				3	34								
MPE	State	TPS	PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
mpe17-111(Server-A)	Active	9 (0%)	1531	1532 (0%)	4	57	2 of 2	0 of 0		0	0	2	0	0
mpe17-111(Server-B)	Standby				3	37								
mpe17-115(Server-A)	Active	11 (0%)	1469	1469 (0%)	3	56	2 of 2	0 of 0		0	0	0	0	0

Performance				Connections			Alarms			Protocol Errors				
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra17-122(Server-A)	Active	20 (0%)	3000	3000 (0%)	4	45	4 of 4	2 of 2	1 of 4	0	0	0	0	0
mra17-122(Server-B)	Standby				4	34								
MPE	State	TPS	PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
mpe17-116(Server-A)	Active	14 (0%)	1519	1521 (0%)	3	57	2 of 2	0 of 0		0	0	0	0	0
mpe17-117(Server-A)	Active	7 (0%)	1482	1481 (0%)	4	56	2 of 2	0 of 0		0	0	0	0	0
mpe17-117(Server-B)	Standby				3	37								

Figure 11: KPI Dashboard

The KPI dashboard displays system wide alarms and errors reports with hyperlinks to device-specific reports. On the KPI dashboard, each name of a MPE or MRA is a hyperlink to its associated Reports tab. Each value in the Connections column is a hyperlink to the connection type sub-screen under the Reports tab. Each alarm or error count value is a link to its respective device-specific report screen.

### Alarm Reports

Every CMP screen displays an alarm summary in the upper right-hand corner of the screen, as shown in Figure 12. OCPM alarms have three severity levels:

- Critical: Service is being interrupted
- Major: Service may be interrupted if the issue is not corrected
- Minor: Alarm is not a service-affecting fault

Oracle Communications Policy Management
04/22/15 12:40 PM | admin | Logout

Critical  
0

Major  
0

Minor  
3

Figure 20: Alarm Summary in Top Banner

There are two alarm reports: the Active Alarm Report and the Alarm History Report. The *Active Alarm Report*, shown in Figure 12, provides the list of active alarms for CMP, MPE, and MRA servers. The columns in the report include Server identity, Server type (CMP, MPE, or MRA), Severity, Alarm ID, Age, Description, Time, and Operation.



Oracle Communications Policy Management							04/22/15 12:40 PM   admin   Logout		
Active Alarms (Stats Reset: Manual / Last Refresh:04/23/2015 14:31:25)							Critical 0	Major 0	Minor 3
Pause		Save Layout		Columns	Filters	Printable Format	Save as CSV	Export PDF	
Display results per page: 50 [First/Prev] 1 [Next/Last] Total 1 pages									
Server	Server Type	Severity	Alarm ID	Age/Auto Clear	Description	Time	Operation		
gpaliwal-cmp-12-0 10.148.232.70	CMP	Minor	31100	25s / 5m 0s	The DB replication process is impaired by a s/w fault	04/23/2015 14:20:07 EDT	🗑️		
gpaliwal-cmp-12-0 10.148.232.70	CMP	Minor	32509	2h 8m 52s / ---	Server NTP Daemon Not Synchronized	04/23/2015 12:11:40 EDT	🗑️		
gpaliwal-mpe-12-0 10.148.232.75	MPE	Minor	32509	21h 36m 47s / ---	Server NTP Daemon Not Synchronized	04/22/2015 16:43:54 EDT	🗑️		

Figure 12: Active Alarm Report

The *Alarm History Report*, shown in Figure 13, provides the alarm history for each CMP, MPE, and MRA server.

Alarm History Report						
Start Date	End Date	Severity	Cluster or Server	Active Alarms	Aggregate	Filter Close
171 Alarms found, displaying 1 to 25. [First/Prev] 1, 2, 3, 4, 5, 6, 7 [Next/Last]						
Occurrence	Severity	Alarm ID	Text		OAM VIP	Server
Dec 27, 2013 11:09 AM EST	Info	86100	CMP User login.		10.15.17.110	mat-110-cmp02 10.15.16.91
Dec 27, 2013 07:41 AM EST	Minor	32508	Server Core File Detected		10.15.17.111	mat-110-mpe02 10.15.16.93
Dec 27, 2013 07:41 AM EST	Minor	32508	Server Core File Detected		10.15.17.118	mat-110-mra02 10.15.16.96
Dec 27, 2013 07:37 AM EST	Minor	32508	Server Core File Detected		10.15.17.118	mat-110-mra01 10.15.16.95
Dec 27, 2013 07:36 AM EST	Minor	32508	Server Core File Detected		10.15.17.111	mat-110-mpe01 10.15.16.92
Dec 27, 2013 07:35 AM EST	Minor	32508	Server Core File Detected		10.15.17.110	mat-110-cmp01 10.15.16.90
Dec 26, 2013 08:05 AM EST	Info	86102	CMP User logout.		10.15.17.110	mat-110-cmp02 10.15.16.91
Dec 26, 2013 08:04 AM EST	Info	86100	CMP User login.		10.15.17.110	mat-110-cmp02 10.15.16.91
Dec 26, 2013 07:49 AM EST	Info	86001	Application is ready for service.		10.15.17.110	mat-110-cmp01 10.15.16.90
Dec 26, 2013 07:49 AM EST	Clear	70021	The MySQL slave is not connected to the master		10.15.17.110	mat-110-cmp01 10.15.16.90

Figure 13: Alarm History Report

**System-Wide Trending Reports**

CMP provides a graphical display of MRA and MPE key statistics. The statistics that can be graphed include:

- MRA Binding Count
- PDN Connection Count
- Session Count
- Transactions Per Second

As shown in Figure 14, you can also use the search filter to select which devices to graph, or display an aggregated view. The default interval time of 15 minutes can be changed via the Settings button. The information can also be displayed in tabular format using the “View Summary” button.

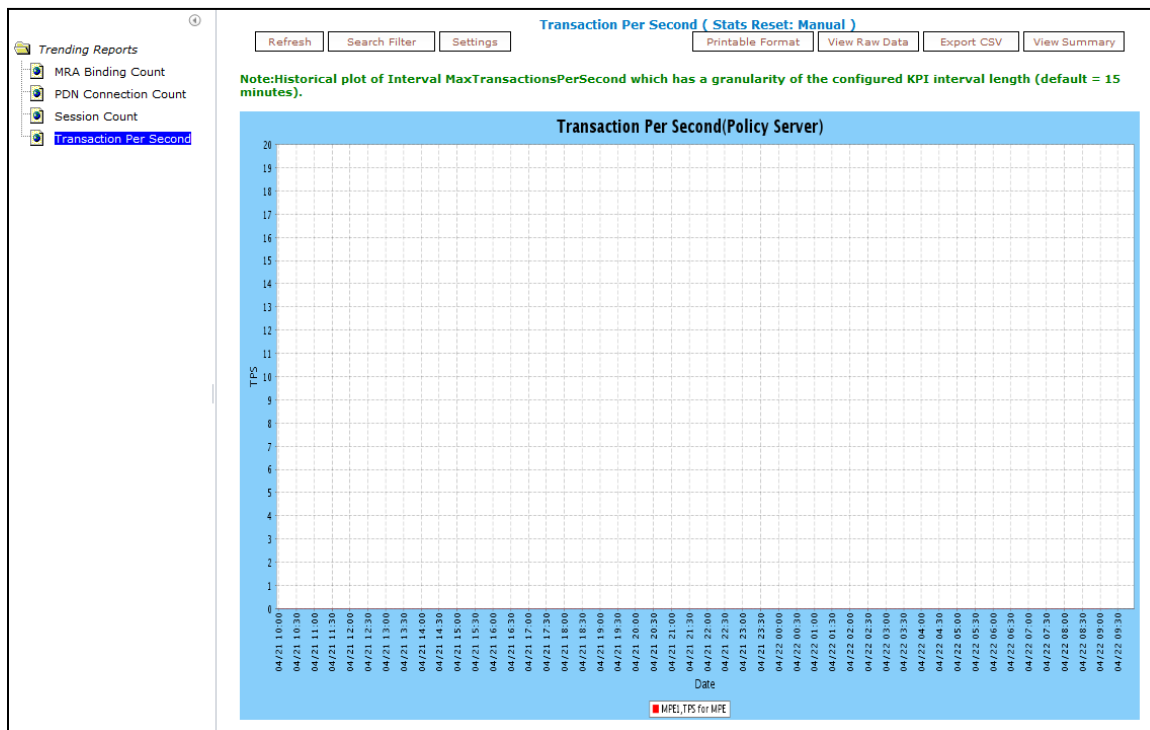


Figure 14: Trending Report Example

### System-Wide Tabular Reports

CMP provides a variety of other reports which summarize activity across multiple servers:

- **AF Session Report:** This report contains current and maximum AF session count (i.e., Rx session) for each MPE and associated MRA per RAT-Type. The operator can choose (customize) the RAT-Types (all RAT-Types defined by 3GPP are supported) to be included in the report. The AF session count for MRA is the aggregate of session counts for all MPEs in the MRA's pool.
- **PDN Connection Report:** This report contains current and maximum PDN connection counts (i.e., Gx session) for each MPE and associated MRA per RAT-Type. The operator can choose (customize) the RAT-Types (all RAT-Types defined by 3GPP are supported) to be included in the report. The PDN connection count for MRA is the aggregate of session counts for all MPEs in the MRA's pool.
- **PDN APN Suffix Report:** This report contains current and maximum PDN connection count (i.e., Gx session) per APN. The operator can choose all or set of specific APNs (filter) to be included in the report.
- **Connection Status Report:** This report contains all Home Subscriber Server (HSS) and gateway connections. The report provides filters (by server, status, site, and error) and report-management actions such as print, save, and export. The data in the connection report is derived from the statistics or counters, which are also used as the basis for the Reports tab for the MPE or MRA.
- **Protocol Errors Report:** This report contains all protocol error statistics retrieved from the system, allows filtering of data, and has print, save, and export functions.
- **Policy Statistics Report:** CMP can display statistics on policy execution for each policy on each MPE.

- Replication Statistics Report: This report shows the number of sent and received packets (total, peak and average) for each MPE/MRA along with the link type (LAN for local server and WAN for remote spare server).

## Server Reports

CMP also provides monitoring of individual MRA and MPE servers, as shown in Figure 15. The numerous tabs allow you to see basic system information, create reports for individual clusters, view logs and routing information, see what policies are deployed to this MPE cluster, see which data sources (SPR/UDR and OCS) this MPE communicates with, and view detailed information about specific sessions.

The screenshot displays the Oracle Communications Policy Management web interface. The top navigation bar includes the Oracle logo, the product name, the current date and time (03/13/15 04:44 PM), the user name (admin), and a Logout link. On the right side of the top bar, there are three status indicators: Critical (0), Major (2), and Minor (0). The main content area is titled "Policy Server Administration" and is for "Policy Server: MPE1". It features several tabs: System, Reports, Logs, Policy Server, Diameter Routing, Policies, Data Sources, and Session Viewer. Below the tabs are buttons for "Modify", "Delete", and "Reapply Configuration". The "Configuration" section shows the following details:

Name	MPE1
Status	On-line
Version	11.1.2
Description / Location	
Secure Connection	No
Legacy	No
Type	Oracle
System Time	Mar 13, 2015 04:44 PM EDT

The left sidebar contains a navigation menu with categories like MY FAVORITES, POLICY SERVER, POLICY MANAGEMENT, NETWORK, MRA, SYSTEM WIDE REPORTS, PLATFORM SETTING, UPGRADE MANAGER, SYSTEM ADMINISTRATION, and HELP.

Figure 15: Policy Server (MPE) Administration Screen

In addition to the system wide reports, information about each MPE and MRA can be displayed using the "Reports" tab. As shown in Figure 16, these statistics are collected periodically at user-defined intervals, and can be reset automatically at specific intervals or manually.

The screenshot displays the Oracle Communications Policy Management web interface for "Stats Settings". The top navigation bar is similar to Figure 15, but the status indicators show Critical (0), Major (0), and Minor (3). The main content area is titled "Stats Settings" and has a "Modify" button. It shows the following configuration:

Stats Reset Configuration	Manual
Stats Collection Period	15 minutes

The left sidebar is also visible, showing the "Global Configuration Settings" section expanded. The URL at the bottom of the page is [http://10.148.232.70/mi/globalConfigurationFolderSelect.do?SEL\\_SRC1=19811025](http://10.148.232.70/mi/globalConfigurationFolderSelect.do?SEL_SRC1=19811025).

Figure 16: Statistics Settings

A statistics file generator scheduled task periodically queries the OSSI interface for statistics and stores the results in a local repository. Statistics can also be:

- Pushed to up to four remote repositories in csv format, using rsynch over SSH.
- Pulled by an external interface using OSSI. Using the OSSI interface, reporting systems can query all or portions of the performance data filtering by time, network element and resource. XML schema documents are provided allowing easy parsing and integration of the data.

Figure 17 shows the full statistics screen for an MPE server. The appropriate corresponding information is also available for MRAs. You can select the provided hyperlinks to see additional information about most categories.

Policy Server: MPE

System Reports Logs Policy Server Diameter Routing Policies Data Sources Session Viewer Debug

Stats Reset: Manual

Cluster Information Report

Mode: Active

Reset All Counters Rediscover Cluster Pause

Cluster: MPE

Cluster Status On-line

Blades

	State	Blade Failures	Overall		Utilization			Actions	
			Uptime	Disk	CPU	Memory			
10.148.230.113 (Server-A)	Active	21	42 days 59 mins 53 secs	2.57 %	6 %	66 %	Restart	Reboot	

Time Period

Current Time Period <None>  
Transition Status N/A Cancel

Policy Statistics (details...)

Name	Evaluated	Executed	Ignored
No policies deployed			

Quota Profile Statistics (details...)

Name	Activated	Volume Threshold Reached	Time Threshold Reached	Event Threshold Reached
No Quota profile deployed				

Traffic Profile Statistics (details...)

Name	Install Attempts	Removed by PCRF	Failed or Removed by Gateway
No Traffic profile deployed			

Session Cleanup Statistics

Session	Ready for Cleanup	Removed on unknown session id	Reauthorized	Reauthorization Timeout	Removed for Expiration
Peg Count	10	0	0	0	2

Protocol Statistics

Name	Connections	Total client messages in / out	Total messages timeout
<b>Diameter</b>			
Diameter AF Statistics	1	0 / 0	0
Diameter PCRF Statistics	1	10 / 10	0
Diameter BBF Statistics	1	0 / 0	0
Diameter IDF Statistics	1	0 / 0	0
Diameter Sh Statistics	0	0 / 0	0
Diameter DRMA Statistics	1	2 / 2	0

#### Latency Statistics

Name	Connections
<b>Diameter</b>	
Diameter AF Statistics	1
Diameter PCEF Statistics	1
Diameter BBERF Statistics	1
Diameter TDF Statistics	1
Diameter Sh Statistics	0
Diameter DRMA Statistics	1

#### Event Trigger Statistics

Name	Peg Count
Event Trigger By Code	
Event Trigger By Application	

#### Error Statistics

Error	Total errors received / sent
<b>Diameter</b>	
Errors By Code	10 / 0
Errors By Remote Identity	10 / 0

#### Data Source Statistics

Name
LDAP Data Source Statistics
Sh Data Source Statistics

#### KPI Interval Statistics

Name
KPI Interval Statistics

Figure 17: MPE Reports

The available information includes:

- Hardware status.
- Policy statistics: Number evaluated, executed (policy conditions evaluate to TRUE so the policy actions are executed) and ignored (policy conditions evaluate to FALSE).
- Quota and traffic profile statistics.
- Session cleanup statistics: If a subscriber session has existed for longer than its configured maximum validity time without any explicit updates from the corresponding gateway, or if a more recent session exists for the same subscriber and protocol, the session is considered "stale" and can be removed via the configurable *stale session cleanup* procedure.
- Protocol statistics: Summarizes the connections to various other network elements.
- Latency statistics: This information is given per network element, per MPE, and per MRA.
- Event trigger statistics: These counters are tracked per network element and per MPE.
- Error statistics: Displays error sent/received by error code and by device.
- Data source statistics: Statistics are shown for LDAP and Sh data sources.
- KPI interval statistics: Shows information about the configured collection interval.

#### Additional Monitoring/Management Functions

CMP provides other tools to assist in operating your network, including:

- Management, Audit and Trace Logs: These track the various system activities. They are available under "System Administration".
- Subscriber Activity Log: MPEs can provide a detailed trace for up to 20 subscribers. This debugging tool simplifies problem determination, including for testing new functionality. This is available under "System Wide Reports".

- **Hardware Management Report:** This report summarizes the available servers, displays disk/CPU/memory utilization, tracks the number of server failures, and allows the user to restart a server. This is available under “System Administration”.
- **Session Viewer:** This displays current session and binding data for a subscriber. It is available for each server via the “Session Viewer tab in the “Policy Server→Configuration” section. The user provides a subscriber identifier such as IMSI, MS-ISDN, IP, and NAI. CMP then displays the current session and binding data for that subscriber from the MRA or MPE that manages the session. If users get the binding data from the MRA, the operator can click the binding MPE hyperlink to go directly to the MPE Session Viewer tab and look up the subscriber data.
- **CMP Bulk Operations:** You can execute a specific subset of an operation on a group of servers. The user selects a server group instance instead of an individual server, and any operations performed are applied to all servers within the group. The supported MPE operations are shown in Figure 18. For MRAs, the Reset Counters and Reapply Configuration commands may be applied to groups.

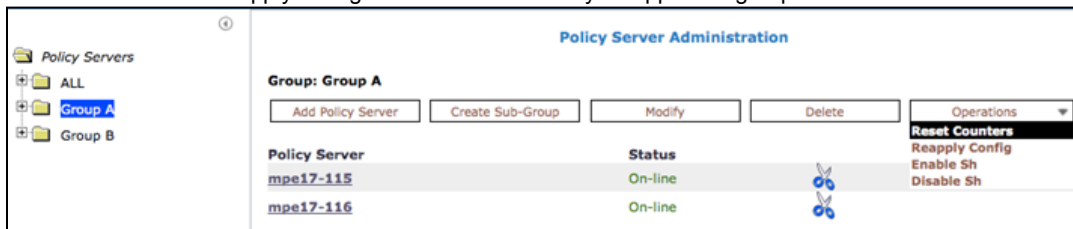


Figure 18: CMP Bulk Operations

- **CMP Online Help:** OCPM includes online help to look up descriptions of alarms or trace log items. While displaying the Active Alarm page, the Alarm History Report, or the Trace Log Viewer you can click on an alarm or trace log item to open the help and display reference documentation for that alarm or trace log item. CMP also includes online help for Policy Wizard conditions and actions while defining policies. For each policy condition or action, the help section contains a general description, a list of applicable parameters, and an example if available.



## Planning Considerations

This section discusses the primary design considerations for a single OCPM system. Of course, you may choose to break your overall network into separate regional networks. The key decisions are:

1. **Hardware selection:** Decide on the hardware (or virtualized infrastructure) on which the OCPM software will operate.
2. **Topology selection:** Decide whether to deploy a standalone, geodiverse or georedundant system.
3. **Capacity:** Determine the total required TPS, Concurrent Sessions and Subscriber Bindings (for each segment).
4. **Multi-Level OAM:** Decide whether Multi-Level OAM is desired.
5. **Optional Software:** Determine which incremental software features you will use.

### Hardware Selection

OCPM components (MPE, MRA, CMP) can operate as follows:

- As a complete system running on a single Oracle X5-2 server running Oracle Linux with a KVM hypervisor. This implementation supports two MPEs, one MRA/PFE and one CMP. This is appropriate for small installations as well as lab systems.
- As virtual machine guests under KVM, OVM or VMware. Oracle provides a reference model with expected performance.
- On dedicated servers. Oracle validates operation and provides performance benchmarks on the following hardware families:

Table 2: Validated Hardware Families

Server	Supported Server Hardware
<b>CMP</b>	HP BL460C G6/G8/G9 Blade Server (in c7000 enclosure) HP DL380 G6/G8 Rack Mount Server Oracle Netra x3-2 (DC, NEBS) Oracle x5-2 (AC, non-NEBS)
<b>MPE, MRA/PFE</b>	HP BL460C G6/G7/G8/G8+/G9 Blade Server (in c7000 enclosure) HP DL380 G6/G7/G8/G8+/G9 Rack Mount Server Oracle Netra x3-2 (DC, NEBS) Oracle x5-2 (AC, non-NEBS)
<b>Management Server (required when using HP c7000 enclosure)</b>	HP DL380 G6/G7/G8/G8+/G9 Rack Mount Server (DC) HP DL360 G6 Rack Mount Server (AC)

All servers in the same cluster must run on the same hardware family. In addition, the DR-CMP cluster must run on the same hardware as the primary CMP cluster.

### Network Topologies

This chapter describes three topologies supported by OCPM. They range from a simple solution with only cluster redundancy to a highly available solution with extreme scalability and multiple redundancy levels. The topologies are:

- Standalone PCRF Node
- PCRF Segments (Geodiverse)
- Georedundant Design

### Standalone PCRF Node

The simplest policy system is a single PCRF node, which consists of one high-availability (two server) MRA cluster and one/more associated MPE clusters. All of these elements are managed by one CMP cluster. This topology is illustrated in Figure 19. In each cluster, the colored servers are active and the gray servers are in standby mode. This example includes three MPE HA clusters. The entire PCRF node must be located at the same site, while the CMP may reside at a different location.

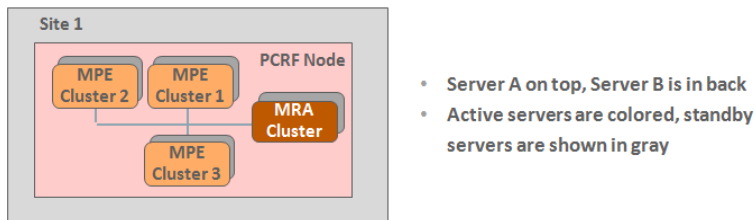


Figure 19: Standalone PCRF Node Topology (Server A is active for all clusters)

Note that each cluster independently determines which server is active. For example, Server A may be active for the MRA cluster, while server B is active for MPE cluster 1. This is depicted in Figure 20.

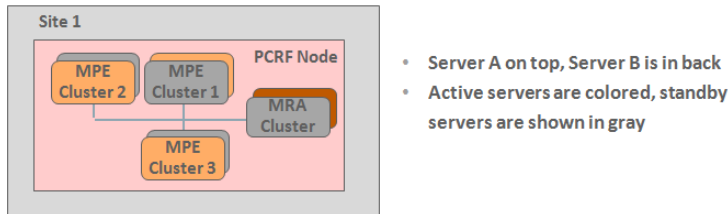


Figure 20: Standalone PCRF Node Topology (Server B is active for some clusters)

An operator can deploy multiple independent PCRF nodes which do not communicate with each other. A single CMP cluster can support multiple PCRF nodes.

### Associated PCRF Nodes (Geodiverse)

This topology interconnects multiple PCRF nodes into a single *policy segment*, which is a collection of PCRF nodes which share session/subscriber binding information. All PCRF nodes within a policy segment are managed by a single CMP cluster.

When an MRA receives a message for a subscriber it does not know about, it first checks whether this is for a subscriber that is known to another PCRF node. If so, the request is handed off to the appropriate PCRF node; otherwise, the original MRA takes ownership of this subscriber and assigns an MPE. The active MRAs share information using DRMA.

Multiple standalone PCRF nodes can be located at the same site to increase overall scaling, or they can be spread across two or more different locations to improve resiliency. For example, a P-GW may be provisioned to send a

request to a preferred MRA, and if a response is not received within a specified time then the request is sent to a different MRA. When the policy segment includes PCRF nodes at multiple sites, it is called a geodiverse deployment. Figure 21 depicts this topology with four PCRF nodes across two sites.

OCPM sites are often deployed in pairs to simplify scaling of the Diameter network. Each Diameter peer provides a primary and secondary Diameter connection to reliably reach the OCPM. If the MPE supporting a subscriber is not local to the MRA which received the message, it routes the message to the appropriate MRA. This approach simplifies the mesh of connections between the MRA and the MPEs.

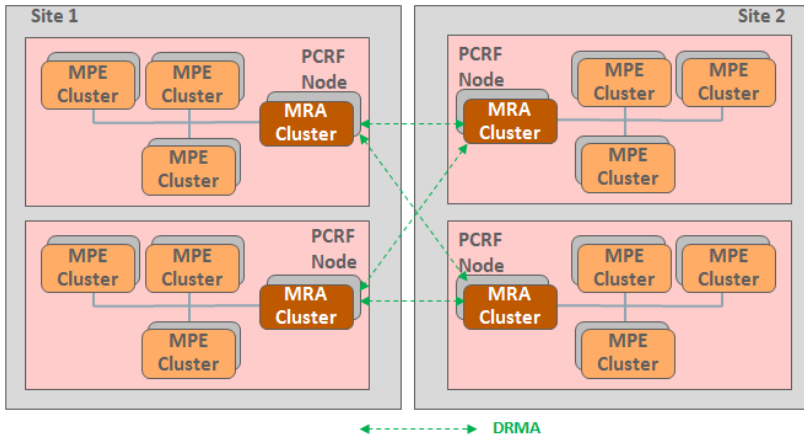


Figure 21: Interconnected PCRF Nodes (Geodiverse) Topology

While the MRAs share information about which subscribers are supported by each, specific binding information is not replicated between MRAs. Therefore, losing all connectivity paths to a PCRF node causes existing sessions established on that PCRF node to fail.

### Georedundant Design

This topology provides an additional level of resiliency by adding a third server to each cluster. Each georedundant cluster has two servers (A and B) at one site and a single server (C) at the other site. Since information about each subscriber is shared between all servers within a cluster, session information is maintained at server C even if both servers at the primary site (servers A & B) fail. Figure 22 illustrates this scenario with two PCRF nodes. For PCRF 1, the primary server (server A) is active for all clusters. For PCRF Node 2, server B has become active for MPE cluster 3, and the server C (the spare server) is active for cluster 5.

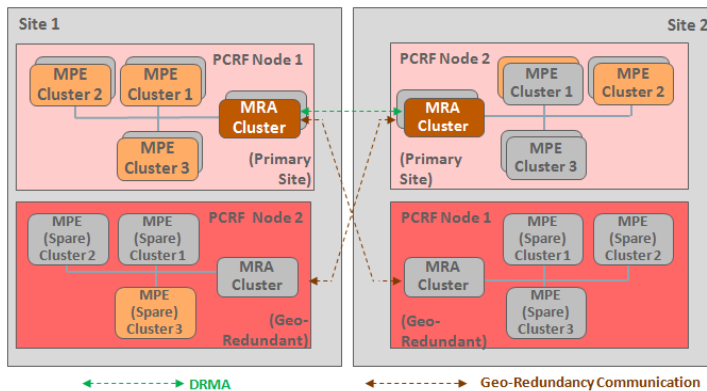


Figure 22: Georedundant Design Topology

If the primary (dual-server) cluster fails, then sessions are routed through an active primary MRA to the georedundant server for that cluster. Figure 23 shows the connections when site 1 fails. In this case, the georedundant server for PCRf Node 1 takes over the load, with communications destined for PCRf Node 1 passing through the active MRA for PCRf Node 2.

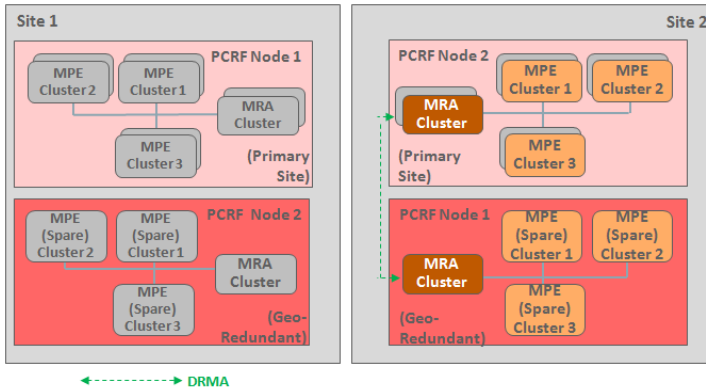


Figure 23: Georedundant Design with Site Failure

While each georedundant PCRf node spans exactly two sites, the overall deployment may encompass additional locations. For example, Figure 24 shows a simplified view of a georedundant design spanning three sites. Each PCRf node can have a connection to every other PCRf node.

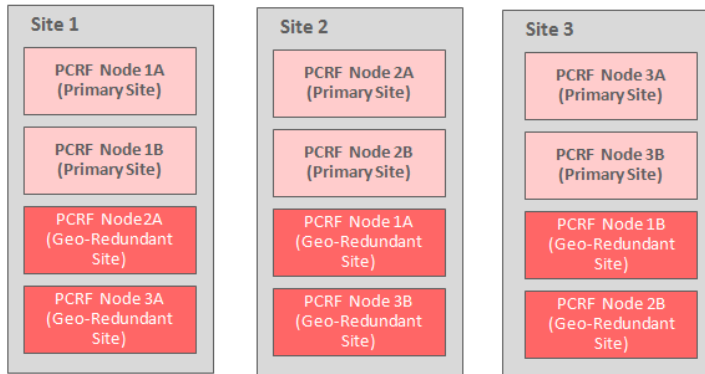


Figure 24: Three-Site Georedundant Design (Simplified View)

### Capacity Considerations

Once the network architecture of the solution is established and optional features are determined, the third step is to determine the capacity requirements. There are three main parameters by which capacity is dimensioned—transactions per second (TPS), concurrent sessions and subscriber bindings. These terms are defined in the table below.

Table 3. OCPM Capacity Metrics

Term	Definition
Transactions Per Second	(PFE and MPE) This is the number of simultaneous transactions per second which can be processed by an OCPM server. A transaction is defined as an incoming or outgoing message (such as a CCR-I or an RAR) and all the associated internal product processing until the

Term	Definition
(TPS)	<p>subsequent message is sent/received. Note that the subsequent message need not be of the same type as the initial message. For example:</p> <ul style="list-style-type: none"> <li>• A common initial session establishment flow consists of two transactions:               <ol style="list-style-type: none"> <li>1. OCPM receives a Gx:CCR-I message and generates a Sh:UDR query to the SPR or other HSS</li> <li>2. OCPM receives the Sh:UDA response message, evaluates policies and generates a Gx:CCA-I response message</li> </ol> </li> <li>• Session updates, such as switching from a cellular to a operator-controlled wi-fi network, often consists of one flow:               <ol style="list-style-type: none"> <li>1. OCPM receives Gx:CCR-U message, evaluates policies and generates a Gx:CCA-U response message</li> </ol> </li> </ul> <p>Transactions between OCPM servers (PFE to MPE, or between PFEs) are not included in this rated capacity.</p>
Concurrent Sessions	<p>(MPE) This is the number of simultaneous sessions and concurrent associations required in the deployment. A session is between the MPE and an external device (e.g. a Gx, Gxa, Gx-Lite, Rx and Sy session). Concurrent associations are between (1) a user endpoint or device and (2) an IP network identified by one IPv4 and/or one IPv6 address.</p>
Subscriber Bindings	<p>(PFE) A binding between a subscriber and an MPE. The PFE maintains bindings, and there is one binding per subscriber even if the subscriber has multiple active sessions.</p>

Determining the target capacity required developing a traffic model. Operations to consider are session establishments, session terminations, and session updates such as quota usage. The traffic model must also specify the average number of sessions per active subscriber per busy hour, the number of new subscribers attaching to the network and the number of subscribers leaving the network during the busy hour.

#### Multi-Level OAM

Multiple OCPM systems can be managed more easily by implementing Multi-Level OAM. In this approach, the CMP functionality is split into two components:

- Network CMP (NW-CMP), which provides a centralized provisioning and alarm monitoring point
- System CMP (S-CMP), which is the primary point for system operation including collecting statistics

Provisioning occurs at the NW-CMP, which pushes the configuration information down to each S-CMP. In addition, each S-CMP forwards its alarms up to the NW-CMP.

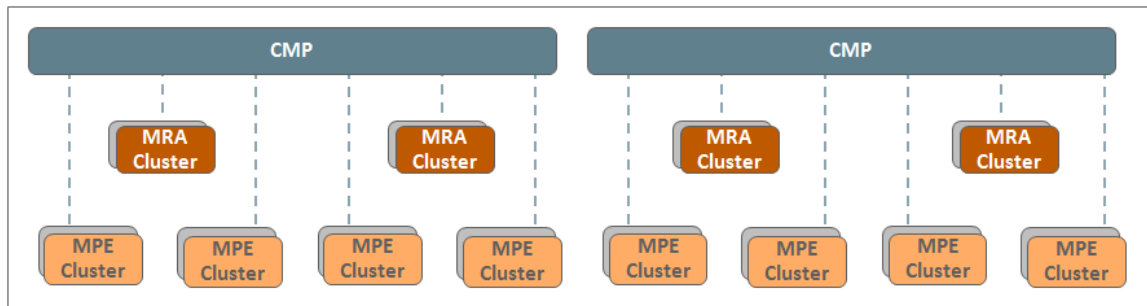


Figure 25: Two CMPs managing two separate networks

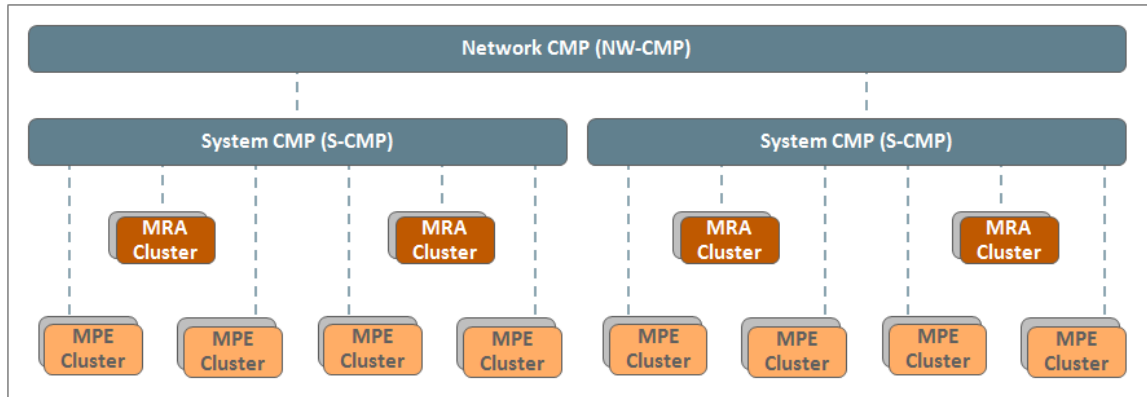


Figure 26: Multi-Level OAM for Centralized Provisioning and Alarm Monitoring

## Appendix A: Networking and Security Overview

All OCPM servers are built on a common platform which provides the common networking and security functionality.

### Security

As a global provider of signaling and broadband data management solutions, Oracle is committed to delivering secure solutions. MPE, MRA CMP and UDR are built upon a common telecommunications grade Oracle Linux implementation. As the OS represents the largest portion of the total attack surface in an application, special attention is given by Oracle to ensure continuous efforts are made in hardening of the OS and reduction of its overall attack surface. This includes, in part, regular security updates, custom security patching from upstream providers, kernel hardening, restrictive user access and permissions, log management and removal of unnecessary services, ports and software. By utilizing this common infrastructure all components take advantage of the common carrier grade platform that supports a broad range of security features.

Each component provides several levels of security to prevent unauthorized access to the system. A username and a password must be provided to access the system through the CLI, web interface, and any remote provisioning interface. Remote computer connections are allowed only using a secure shell (ssh) or secure HTTP connection. All user initiated logins are captured in the audit logs. The logs provide information about the access and duration of the sessions on the system. In addition, terminal activity timeout and password restrictions (minimum length, minimum lifetime, maximum lifetime and warning age) are provided. The system can restrict the number of login warnings before the password is disabled.


All daemons that are not required have been disabled. The "r" commands (rsh, rcp, rexec) are not used, and incoming telnet and ftp connections are not permitted. No passwords are sent across the network in clear text. Public-key encryption is the only supported method for incoming network access. ssh is used for secure network logins, while scp and sftp are used for secure file transfers.

Additional security design choices include:

- Configuration file revision history: Files that provide OS level configuration are revision controlled using RCS.
- Minimal software package content: In order to eliminate unnecessary vulnerabilities, only required software packages are included as part of the distribution package.
- Minimal user accounts: User accounts are kept to an absolute minimum to reduce the risk of unauthorized access to any server.
- Minimal system services: All non-essential system services are disabled.
- Restricted file permissions: All file permissions are restricted utilizing the least access rule, (allow write access only where needed). Restrict elevated authority by finding Set UID root programs and removing the SUID bit if possible, and by removing all access to directories, files, and programs that are not required.
- No DNS or NIS name services: The system can be configured to use only local file lookup by changing the file /etc/nsswitch.conf.

### Networking

To simplify operations, each OCPM server can use multiple logical networks (that is, multiple IP addresses and VLAN identifiers) to support various functions. The following networks are required:

- 
- Operations, Administration and Management (OAM): All PCRF functionality can be performed using the OAM network. However, in most cases incremental functionality is deployed using the optional logical interfaces discussed below, and this network is used for operational control.

The following network is required when using specific hardware:

- Platform Management (PlatMgt): This logical network supports hardware management, including support for HP's iLO (Integrated Lights Out) operation.

The following optional networks can also be configured:

- Signaling (SIG-A, SIG-B): In almost all networks, signaling between network elements occurs on a separate logical interface (SIG-A). Some operators split the signaling across the two available signaling interfaces.
- Replication (REP): Georedundant replication can be done using a separate logical set of replication (REP) addresses. This function can alternatively be performed using the OAM or SIG interfaces.
- Backup (BKUP): A separate set of addresses for backup using Symantec Netbackup.

OCPM also supports the following:

- Separate DSCP markings can be set for signaling traffic and georedundant replication so that switching/routing components can effectively prioritize traffic.
- Different IP versions can be used to each Diameter peer. OCPM's IPv6 implementation complies with the DoD standard for an IPv6 capable (1) Host and Workstations and (2) Advanced Server, as outlined in DoD's IPv6 Standard Profiles for IPv6 Capable Products Version 2.0.
- Connections to Diameter peers use either Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP), including SCTP multi-homing.



## Appendix B: Wireless Solutions

### 3GPP Support

OCPM communicates with other wireless network elements, as shown in Figure 27. These include:

- Policy and Charging Enforcement Functions (PCEF): PDN Gateways (PGW) and Gateway GPRS Support Nodes (GGSN)
- Serving Gateways (SGW) and Serving GPRS support node (SGSN)
- Application Functions (AF) such as P-CSCF
- Traffic Detection Functions (TDF)
- Online Charging Systems (OCS)
- Lawful Intercept Mediation Function (LIMF)

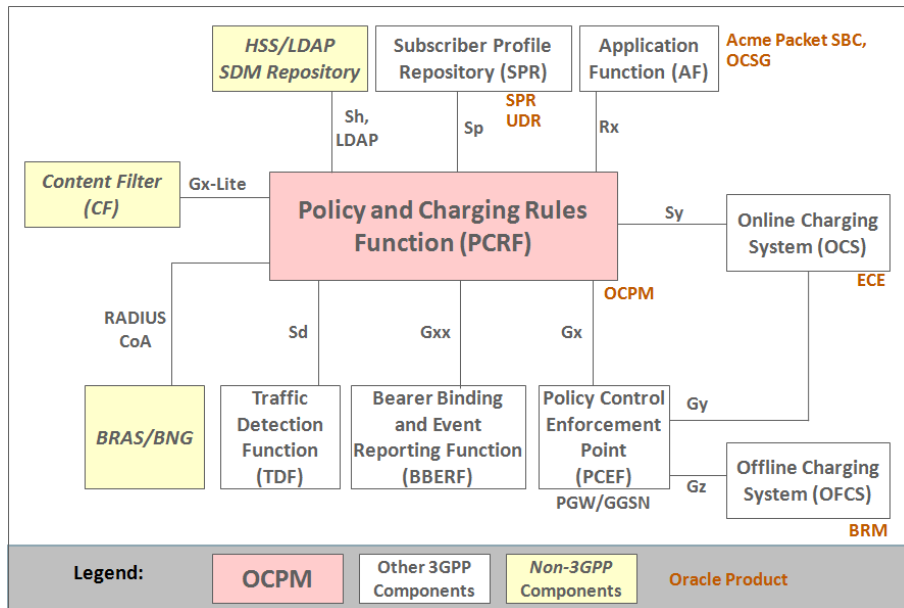


Figure 27: Oracle Converged Wireless Architecture

Supported signaling interfaces are summarized in Table 4:

Table 4: OCPM Signaling Interfaces

Interface	Purpose	Endpoints connected to Policy Management
Gx, Gxx, Gx-Lite	Policy Control (e.g. policy rules)	PCEF, BBERF, DPI, TDF
LDAP	Subscriber information interface	LDAP server
Sd	Traffic detection and enforcement	TDF

Sh	Subscriber information and control	SPR
S9	Exchange information between networks	Visited/home PCRF
Sy	Charging interface	OCS
Rx	Application-initiated service	Application Function (e.g., P-CSCF)
X1/X2	Lawful Intercept	Lawful Intercept Mediation Function (LIMF)
RADIUS CoA	Update services available to wirelinesubscribers	Broadband Network Gateway (BNG)

### Related Oracle Products

Oracle's support for 3GPP includes the following products and product families:

- Oracle Communications Policy Management (OCPM):** OCPM provides PCRF functionality as defined by the 3GPP standards organization. This centralized signaling control point applies operator-defined rules that enforce business needs, such as whether a subscriber is authorized to access a service, whether it can be accessed from the current location and the bandwidth which should be allocated.

OCPM is compliant with 3GPP standards specifications including TS 23.203, TS 29.212, TS 29.213, TS29.214, TS29.219, and TS 29.239 as defined in Oracle's 3GPP Statement of Compliance Documents. OCPM supports all PCRF capabilities for session binding, QoS authorization, and dynamic charging for each application session established via the IMS framework. In addition to supporting 3GPP standards, OCPM has been tested with IMS and Mobile Gateway infrastructures from leading vendors.
- Oracle Communication Subscriber Profile Repository (SPR)/Oracle Communications User Data Repository (UDR):** SPR, and its successor UDR, provide 3GPP SPR functionality. OCPM and SPR/UDR also have been extended to provide quota management, eliminating the need for a separate OCS in some networks.
- Business and Revenue Management (BRM):** BRM serves as the 3GPP offline charging system (OFCS) as well as providing the ability to define new subscribers and what they are allowed to do.
- Elastic Charging Engine (ECE):** ECE, which is part of the BRM product suite, serves as the 3GPP online charging system (OCS).
- Oracle Session Border Controller (SBC):** OCPM is interoperable with Oracle (formerly Acme Packet) Session Border Controllers. These function as a P-CSCF, which is a type of Application Function (AF) in the 3GPP reference architecture.
- Diameter Signaling Router (DSR):** These and other network elements are interconnected using Diameter Routing Agents (DRAs) such as Oracle's DSR. There may be multiple Diameter networks connecting various types of equipment, as shown in Figure 28.

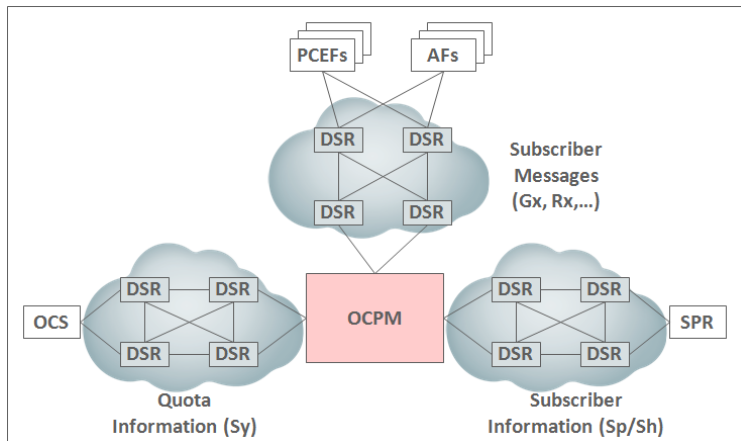


Figure 28: Diameter Physical Connectivity

## Oracle Solutions

The capabilities provided by OCPM can be expanded when used in conjunction with other Oracle products including:

- Network Policy as a Service (NPaaS):** Oracle's NPaaS solution securely exposes and aggregates network policy assets to accelerate innovation and external partner collaboration, enabling the operator to provide compelling new services to grow revenue. Oracle Communications Services Gateway (OCSG) exchanges information with OCPM using the CableLabs PCMM (for cable networks) or 3GPP Rx (for wireless networks) interfaces.
- Oracle Communications Policy Analytics:** OCPM has been integrated with Oracle Communications Data Model (OCDM) into a pre-built analytics solution designed for quick implementation. Policy Analytics provides insight into OCPM value and effectiveness. Analytics systems provide detailed reports on policy usage, quota usage, subscriber behavior, and policy system performance, among other items. OCPM can generate an Analytics Data Stream (ADS) to send information about what is occurring to an external server for analysis.

## Appendix C: Reference Documents

This section lists out any other documents that a user may want to reference for more information.

**TABLE 5: REFERENCE DOCUMENTATION**



Document Number	Document Name
<a href="http://docs.oracle.com/cd/E62448_01/index.htm">http://docs.oracle.com/cd/E62448_01/index.htm</a>	Oracle Communication Policy Management documentation set (Release 12.1)
<a href="http://www.oracle.com/us/products/applications/communications/subscriber-data-management/index.html">http://www.oracle.com/us/products/applications/communications/subscriber-data-management/index.html</a>	Oracle Communications SPR/UDR overview
<a href="http://docs.oracle.com/cd/E48805_01/index.htm">http://docs.oracle.com/cd/E48805_01/index.htm</a>	Oracle Communications SPR documentation set (Release 9.3)
<a href="http://docs.oracle.com/cd/E58598_01/index.htm">http://docs.oracle.com/cd/E58598_01/index.htm</a>	Oracle Communications UDR documentation set (Release 10)
<a href="http://www.oracle.com/us/products/applications/communications/industry-analytics/data-model/overview/index.html">http://www.oracle.com/us/products/applications/communications/industry-analytics/data-model/overview/index.html</a>	Oracle Communications Data Model (OCDM) overview
<a href="http://www.oracle.com/us/products/applications/communications/connected-digital-lifestyle/services-gatekeeper/overview/index.html">http://www.oracle.com/us/products/applications/communications/connected-digital-lifestyle/services-gatekeeper/overview/index.html</a>	Oracle Communications Services Gateway (OCSG) overview



**Oracle Corporation, World Headquarters**  
500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200

CONNECT WITH US

-  [blogs.oracle.com/oracle](http://blogs.oracle.com/oracle)
-  [facebook.com/oracle](http://facebook.com/oracle)
-  [twitter.com/oracle](http://twitter.com/oracle)
-  [oracle.com](http://oracle.com)

**Hardware and Software, Engineered to Work Together**

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 1115



Oracle is committed to developing practices and products that help protect the environment