Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Policy Management
Network Impact Report

Release 12.4

E89546-01

May 2018

Oracle Communication Policy Management Network Impact Report

Table of Contents

Figures

Tables

1. INTRODUCTION

1.1 Purpose and Scope

This document highlights the changes in Oracle Communication Policy Management Release 12.4 that may have an impact on your network, and must be considered during our implementation planning for this release.

1.1 Disclaimers

This document summarizes Oracle Communication Policy Management Release 12.4 feature enhancements as compared to previous release of 12.2.x/12.3.x and the operations impacts of these features, at a high level.

NOTE: Feature implementations may change slightly during product test.

1.2 Glossary

This section lists terms and acronyms specific to this document.

Table 1: Acronyms

Acronym	Definitions
3GPP	Third-Generation Partnership Project
AAA	Authorize-Authenticate-Answer
AAR	Authorize-Authenticate-Request
ADC	Application Detection and Control
AF	Application Function
AMBR	Aggregate Maximum Bit Rate
ARP	Allocation Retention Priority
AVP	Attribute Value Pair
BSS	Business Support System
CALEA	Communications Assistance for Law Enforcement Act.
CCA	Credit-Control-Answer (CC-Answer)
CCR	Credit-Control-Request (CC-Request)
CMP	Configuration Management Platform
CSCF	Call Session Control Function
DCC	Diameter Credit Control
DPI	Deep Packet Inspection
DRA	Diameter Routing Agent
DSR	Diameter Signaling Router
FRS	Feature Requirements Specification
GBR	Guaranteed Bit Rate
G8, G9	Refers to the generation of HP server hardware.
GUI	Graphical User Interface
HA	High Availability

Acronym	Definitions
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HW	Hardware
IE	Internet Explorer
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LI	Lawful Intercept
LIMF	Lawful Intercept Mediation Function
LVM	Logical Volume Manager
MA	Management Agent
MCD	Media Component Description
MP	Message Processor
MPE	Oracle Multimedia Policy Engine
MPE-R	Oracle Multimedia Policy Engine – Routing Mode
MPE-S	Oracle Multimedia Policy Engine – Serving Mode
MRA	Oracle Multiprotocol Routing Agent
MS	Mediation Server
NFV-MANO	Network Function Virtualization Management and Orchestration
NFVO	Network Functions Virtualization Orchestrator
NOAM	Network OAM
NW-CMP	Network-Level Configuration Management Platform
OAM	Operations Administration Maintenance
OCS	Online Charging Service
OM	Operational Measurement
OSSI	Operation Support System Interface
PCC	Policy and Charging Control
PCD	Policy Connection Director
PCEF	Policy and Charging Enforcement Function (GGSN, PGW, DPI)
PCRF	Policy Control Resource Function (Oracle MPE)

Acronym	Definitions
P-CSCF	Proxy CSCF
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PNR	Push-Notification-Request
PUR	Profile-Update-Request
QCI	QoS Class Identifier
QoS	Quality of Service
RAR	Re-Auth-Request (RA-Request) SUPL
REST	Representational State Transfer
ROB	Release of Bearer
S-CMP	Site-Level Configuration Management Platform
S-CSCF	Serving CSCF
SGW	Serving Gateway
Sh	Diameter Sh Interface
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SNR	Subscribe-Notification-Request
SPR	Subscriber Profile Repository
STA	Session-Termination-Answer
STR	Session-Termination-Request
SRA	Successful Resource Allocation
TDF	Traffic Detection Function
TPS	Transactions Per Second
UD	Upgrade Director
UDR	User Data Repository
UE	User Equipment
UM	Upgrade Manager
UMCH	Usage Monitoring Congestion Handling
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
VO	Verification Office
XML	Extensible Markup Language

2. OVERVIEW OF POLICY MANAGEMENT RELEASE 12.4 FEATURES

This section provides an overview list of the Policy Management Release 12.4 features.

1.1 Policy Management Release 12.4 Features

Feature Number	Feature Name
25405538	APN Based Counters Measurement
25943867	APN based data source lookup
25902148	Delivery SMS to two destinations based on policy
25902163	Send SMS Notification frequency based on policy per use case
25455923	Variable to access Max-Requested-Bandwidth
22935518	Extending Oracle Communications Policy Management Session and Binding Information to External Systems

2.1 Policy Management Hardware Requirements

2.1.1 Supported Hardware

The Policy Management Release 12.4 software can be deployed on the hardware that was previously supported under Release 12.2.x/12.3.x:

- Oracle NETRA Server X5-2.
- Oracle Server X5-2 on rack mount server (RMS).
- Oracle hardware (including X6-2 and X7-2 servers) can be leveraged for virtualized deployments of release Oracle Communications Policy Management R12.4.
- Compatible with HP Gen-8 and Gen-9 rack mount server (RMS) and C-class servers
- HP 6120XG and HP 6125XLG enclosure switches.

NOTE: HP Gen-6 and Gen-7 servers is not supported

2.2 Policy Management Software Changes

2.2.1 Software Components

Components	Releases
Policy Management	12.4.0.0.0_51.1.0
TPD 64 Bit	7.5.0
COMCOL	6.5
PM&C	6.0.3
TVoE	3.0.3
AppWorks	6.0.1
Networking	6.0.3
HP Firmware FUP	2.2.9 (Minimum) 2.2.12 (Current)
Oracle Firmware	3.1.5 (Minimum) 3.1.6 (Current)

2.2.2 UDR and SPR Product Compatibility

Products	Releases	Compatibility
Oracle Communication UDR*	12.1 or higher	MPE via Sh interface and CMP via RESTful API. Use of Profile V2, Profile V3, and Profile V4 schemas.

***NOTE:** Policy R12.4 does not support Oracle SDM SPR Release 9.3.1

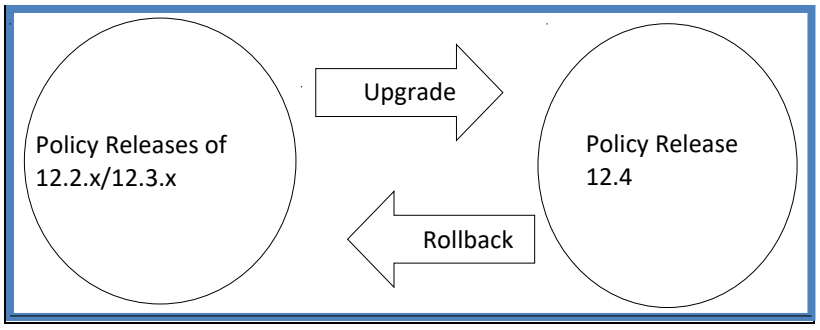
2.3 Policy Management Software Upgrade/Backout Overview

While performing the Policy software upgrade/rollback (backout) procedures, it is expected that the CMP clusters, MRA clusters, and MPE clusters are running different software releases.

2.3.1 Supported Software Upgrade/Rollback (Backout) Paths for Release 12.4

Figure 1shows the supported upgrade Path for Release 12.4

Figure 1 Supportd Upgrade Path



As with the past releases, both Georedundant and Non-georedundant Policy deployments have separate Policy software upgrade/rollback (backout) procedures.

The system must be on release 12.2.x or 12.3.x before upgrading to this release (12.4). This applies to wireless and fixed line.

2.3.2 Mixed Version Policy Management System Expectations

The system that is running Release 12.2.x/12.3.x mixed configuration supports the performance and capacity of Release 12.2.x/12.3.x respectively. The mixed version Policy Management configuration supports Release 12.2.x/12.3.x features respectively.

In the mixed version Policy Management configuration, Release 12.4 CMP has these general limitations:

- New features must not be enabled until the upgrades of all servers managed by that CMP are completed. This also applies to using policy rules that include new conditions and actions introduced in the release.
- Policy rules must not be changed while running in a mixed version environment. If it is necessary to make changes to the policy rules while running in a mixed version environment, changes that do not utilize new conditions and actions for the release can be installed. However, these rules must be reviewed by you and Oracle before deployment to verify that the policies do not use new conditions or actions.
- The support for configuration of MPE and MRA servers is limited to parameters that are available in the previous version. Specifically:
  - Network Elements can be added.
  - Advanced Configuration settings that were valid for 12.2.x/12.3.x may be changed.

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP from Release 12.2.x/12.3.x to Release 12.4. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to Release 12.4.

Policy Management Components	CMP Release 12.4	MRA Release 12.4	MPE Release 12.4
CMP release 12.2.x/12.3.x	No	No	No
MRA release 12.2.x/12.3.x	Yes	Yes	Yes
MPE release 12.2.x/12.3.x	Yes	Yes	N/A

2.3.3 Supported Software Releases Rollback (Backout) Support and Limitation

- After the Policy Management system is completely upgraded to Release 12.4, you may decide that a backout to the previous release is required. In that case, each individual server/cluster must be backed out.
- If it is necessary to backout multiple servers, it is required that the systems be rolled back in the reverse order in which they were upgraded. This implies that all the related component servers are rolled back first before the s CMP/NW-CMP and DR-CMP/NW-CMP can be rolled back to the previous version.
- After all the servers in the system are backed out to the previous release, the servers could be upgraded to another supported minor or major release for example, if all of the servers in the Policy Management system were backed out from Release 12.4 to Release 12.2.x/12.3.x, these servers could subsequently be upgraded to Release 12.4-Build_A.
- Backout may be performed at any time after the upgrade, with these general limitations:
  - If a new feature is enabled, it must be disabled before starting any backout process.
  - If there is an unexpected problem that requires backout after a feature has been enabled, it is possible that transient subscriber data, which is changed by the new feature, may be impacted by

the unexpected problem. In this situation, those sessions cannot be guaranteed to be unaffected for any subsequent actions (this includes any activity after the feature is disabled). This may prevent data restoration by the SSDP feature during the backout. The impact of any unexpected problem must be analyzed when it occurs to determine the best path forward (or backward).

NOTE: Although backout after feature activation is allowed, due to the number of possible permutations under which new features may be activated, the only testing that is performed is based on a backout without new feature activation.

- Backout can only be used to go back one release. This restriction applies to all releases including any major, minor, maintenance, or incremental release including minor releases of Release 12.4.

2.3.3.1 Rollback (Backout) Sequence

The Rollback of Policy Management system from Release N+1 to Release N is generally performed in this order (reverse of the upgrade sequence):

NOTE: See the related upgrade/rollback paths for more detailed procedures. These procedures are not documented in this document. See the Policy Management Release 12.4 documentation.

Release 12.4 to Release 12.2.x/12.3.x (Wireless mode only)

1. MRA clusters, including spare server if geo-redundancy is deployed.
2. MPE clusters, including spare server if geo-redundancy is deployed.
3. Standalone Primary CMP/S-CMP and Disaster Recovery (DR) CMP/S-CMP clusters.
4. If multi-level OAM is deployed, Primary NW-CMP primary cluster and Disaster Recovery (DR) NW-CMP cluster.

2.4 Migration of Policies and Supporting Policy Data

The existing Policies configuration and Subscriber Session information is conserved during the upgrade.

3. CHANGES BY FEATURE

3.1 APN Based Counters Measurement (BUG 25405538)

3.1.1 Introduction

Currently, Oracle Communications Policy Management supports the overall counters with mixing the counters generated from different APNs together. This feature inroduces APN based counters for a Gx interface which collects the number of messages for each type of message per APNs.

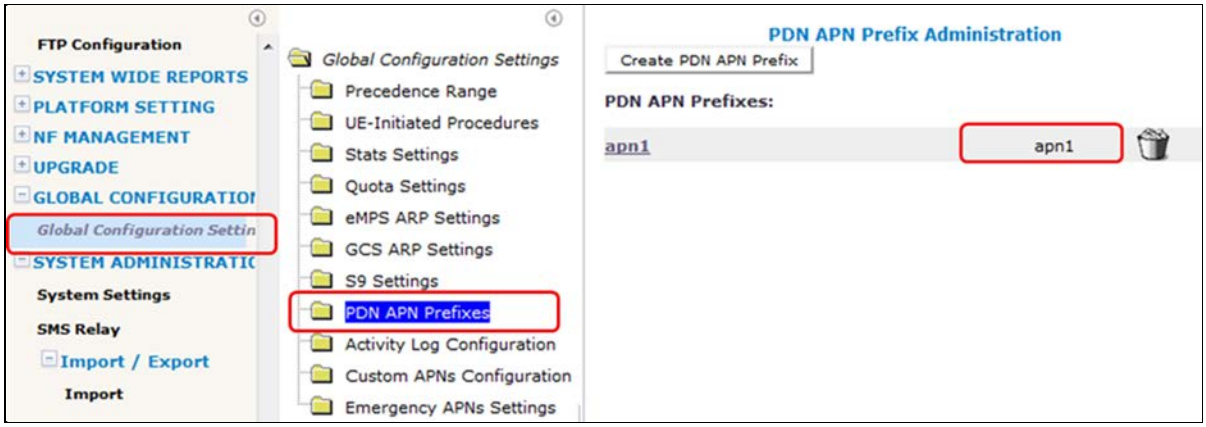
The new APN based counters are generated on MPE servers and merged to the CMP. Some of these counters can be queried and displayed using the CMP GUI (per MPE). These counters can also be queried using the OSSI interface (per MPE).

NOTE: The new APN based counters only have the stats for diameter messages from Gx interface.

3.1.2 Feature Activation

The APN based counters are enabled by configuring APN prefixes from CMP.

Figure 2 PDN APN Prefix Administration



3.1.3 Detailed Description

The feature includes two parts:

1. The generic APN based counters
2. The specific Policy Management profile with APN based counters for Wireless-C mode.

3.1.3.1 Generic APN based counters measurement feature

There are two kinds of stats generated for each matched APN prefixes on the MPE:

1. Counters for the type of diameter messages
2. Counters for result code of diameter error messages.

- DiameterPCEFAPN *xxx* Stats

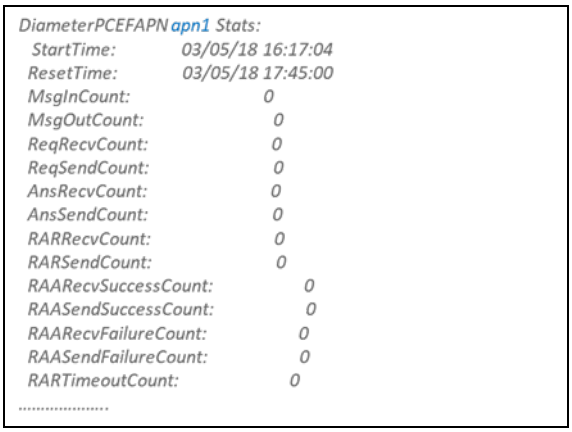
  It is the counters for the type of diameter message and the *xxx* is the matched APN prefix configured on the CMP.

  NOTE: This is the value defined in a PDN APN prefix configuration.

This is an adaptor stats on diameter PCEF and therefore mixes the counters from all connected PCEF peers. It collects information as follows (cmwap is the matched APN prefix):

a. Counters per MPE available on CMP GUI, rcmgr sh counters, OSSI.

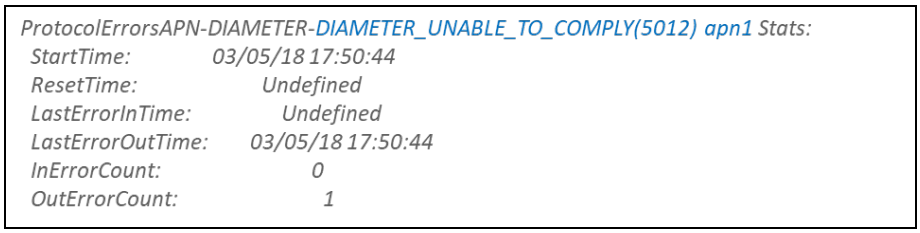
b. Aggregated counters from the MPE servers are partially available in PM file.



- ProtocolErrorsAPN-DIAMETER-<DiameterResultCode> *xxx* Stats

  It is the counters for the result code of diameter error messages and *xxx* is the matched APN prefix configured on the CMP. The DiameterResultCode is the specific diameter result code, such as DIAMETER_UNABLE_TO_COMPLY (5012), DIAMETER_INVALID_AVP_VALUE (5004) and so on. It collects information as follows (cmwap is the matched APN prefix):

  Counters per MPE available on CMP GUI, rcmgr sh counters, OSSI.



3.1.3.2 PM Profile with APN Based Counters in Wireless-C Mode

According to PM requirement introduced from Wireless-C mode, the existing PM Statistics Files support the APN based counters as follows (the new part marked in red):

- **PM file version changed from v2.0 to v2.2 (CMCC mode)**

After upgrade to R12.4, /opt/camiant/mi/pm.xml will be of v2.2.

The NetAct system should also support PM v2.2. Otherwise, need to overwrite /opt/camiant/mi/pm.xml with v2.0 to maintain backward compatible.

Difference between v2.0 and v2.2 highlighted as red below.

```
<Measurements>
<ObjectType>PcrfFunction</ObjectType>
<PmName>
 <N i="1">DIAM.AuthRequest</N>
 <N i="2">DIAM.AuthSucc</N>
 <N i="3">DIAM.ReAuthRequest</N>
 <N i="4">DIAM.ReAuthSucc</N>
 <N i="5">DIAM.SessionTermRequest</N>
 <N i="6">DIAM.SessionTermSucc</N>
 <N i="7">DIAM.AbortSessionRequest</N>
 <N i="8">DIAM.AbortSessionSucc</N>
 <N i="9">SM.RxSessionMean</N>
 <N i="10">SM.RxSessionMax</N>
 <N i="11">SM.SessionNbrMean</N>
 <N i="12">SM.SessionNbrMax</N>
 <N i="13">DIAM.CcInitialRequest._Apn</N>
 <N i="14">DIAM.CcInitialSuccess._Apn</N>
 <N i="15">DIAM.CcInitialFail._Apn</N>
 <N i="16">DIAM.CcInitialFail._Apn._Cause</N>
 <N i="17">DIAM.ReAuthRequest._Apn</N>
 <N i="18">DIAM.ReAuthSuccess._Apn</N>
 <N i="19">DIAM.ReAuthFail._Apn</N>
 <N i="20">DIAM.ReAuthFail._Apn._Cause</N>
 <N i="21">DIAM.ReAuthTimeout._Apn</N>
</PmName>
```

PM files generated on the CMP and pushed to FTP server according scheduled task.

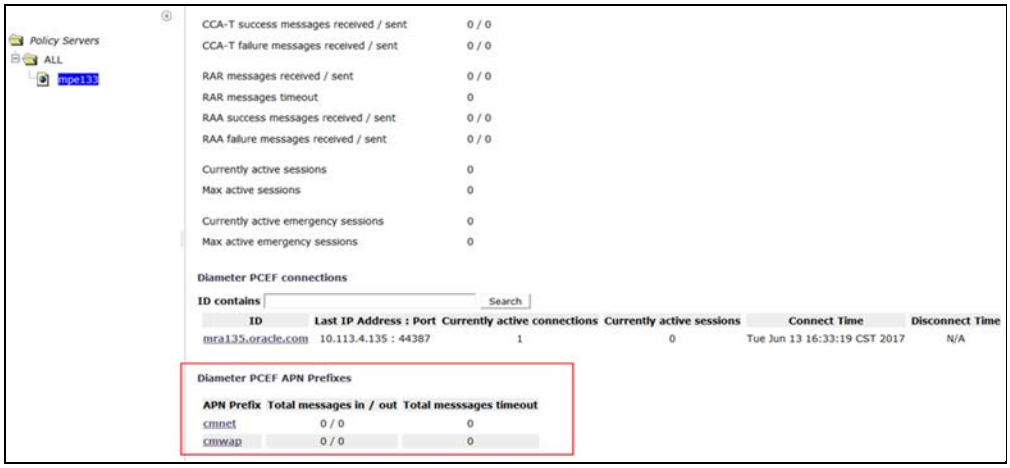
/var/camiant/pm_export/CMCC-PCRF-PM-V2.0.0-20180308-1015.xml

```
<PmData>
 <Pm Dn="SubNetwork=1,ManagedElement=1,PcrfFunction=1" UserLabel="BJMSS01">
  ..................
  <CV i="13">    <SN>DIAM.CcInitialRequest.apn1</SN>    <SV>1</SV>  </CV>
  <CV i="14">    <SN>DIAM.CcInitialSuccess.apn1</SN>    <SV>0</SV>  </CV>
  <CV i="15">    <SN>DIAM.CcInitialFail.apn1</SN>    <SV>1</SV>  </CV>
  <CV i="16">    <SN>DIAM.CcInitialFail.apn1.DIAM.CcInitialFail.-1</SN>    <SV>1</SV>  </CV>
  <CV i="17">    <SN>DIAM.ReAuthRequest.apn1</SN>    <SV>0</SV>  </CV>
  <CV i="18">    <SN>DIAM.ReAuthSuccess.apn1</SN>    <SV>0</SV>  </CV>
  <CV i="19">    <SN>DIAM.ReAuthFail.apn1</SN>    <SV>0</SV>  </CV>
  <CV i="20">    <SN>DIAM.ReAuthFail.apn1.DIAM.ReAuthFail.-1</SN>    <SV>0</SV>  </CV>
  <CV i="21">    <SN>DIAM.ReAuthTimeout.apn1</SN>    <SV>0</SV>  </CV>
 </Pm>
</PmData>
</Measurements>
```

3.1.4 User Interface Changes

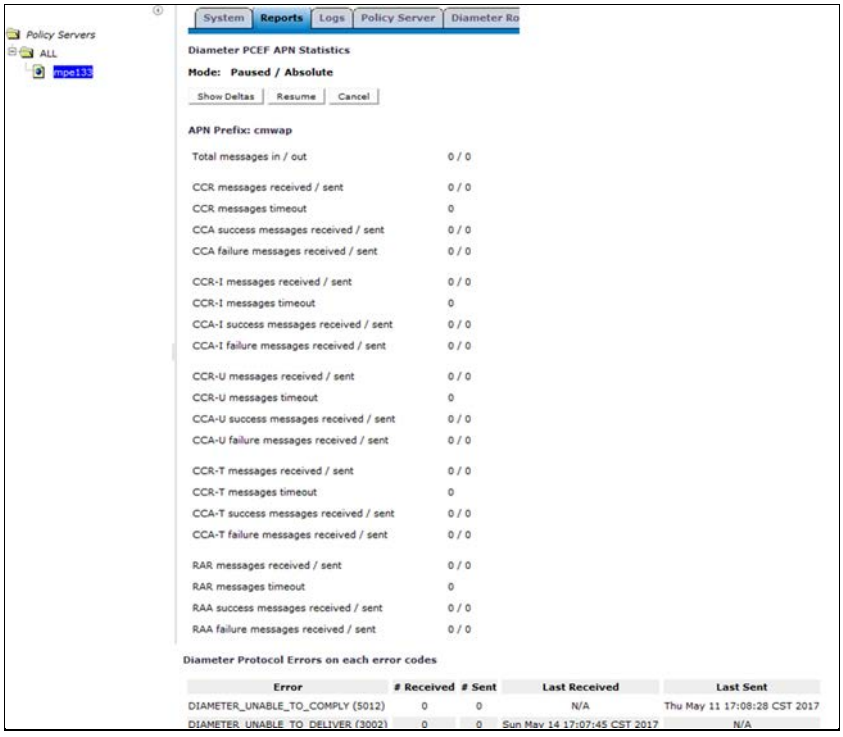
To display the generic APN based counters for the Gx interface on the CMP, use the new diameter PCEF APN statistics that is added to the Diameter PCEF Statistics in the protocol statistics section on the Policy Server reports page (Figure 3).

Figure 3 CMP GUI→MPE→Reports→Diameter PCEF Statistics (Brief View)



The detailed view of the diameter PCEF APN statistics displays message counters (DiameterPCEFAPN xxx Stats) and protocol errors (ProtocolErrorsAPN-DIAMETER-<DiameterResultCode> xxx Stats) as shown in Figure 4.

Figure 4 CMP GUI: Detail View for DiameterPCEFAPN, ProtocolErrorsAPN



3.1.5 Programmatic Interface Changes

CMP supports OSSI query for the new APN based statistics

- DiameterPCEFAPN xxx Stats: Figure 5 shows the OSSI query request/response

Figure 5 Sample OSSI Query Request/Response for DiameterPCEFAPN

Request:

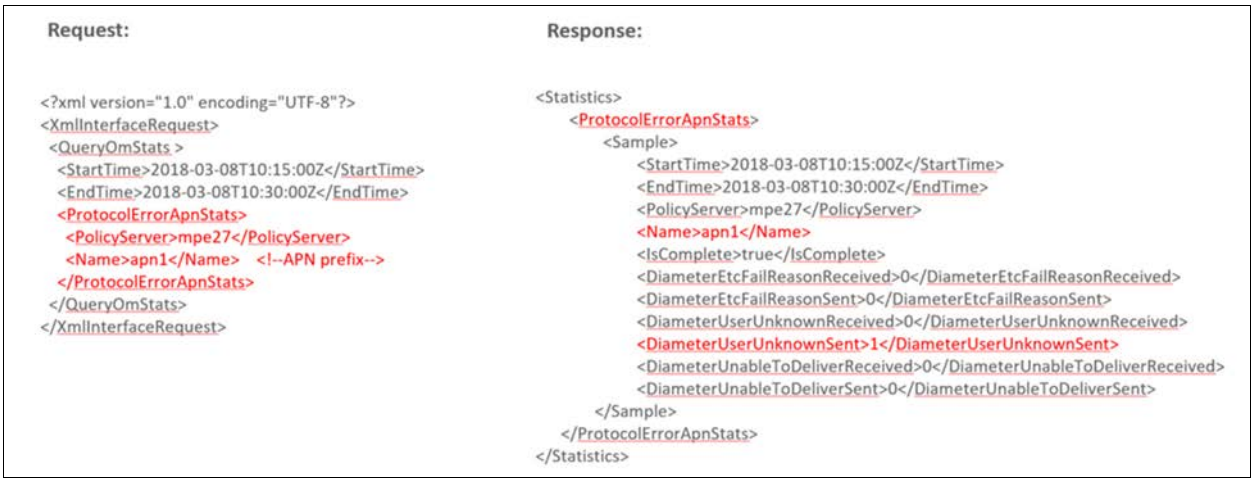
```
<XmlInterfaceRequest>
 <QueryOmStats>
  <StartTime>2018-03-08T10:15:00Z</StartTime>
  <EndTime>2018-03-08T10:30:00Z</EndTime>
  <DiameterPcefApnStats>
   <PolicyServer>mpe27</PolicyServer> <!—MPE hostname -->
   <Name>apn1</Name>  <!--APN prefix-->
  </DiameterPcefApnStats>
 </QueryOmStats>
</XmlInterfaceRequest>
```

Response:

```
<Statistics>
    <DiameterPcefApnStats>
        <Sample>
            <StartTime>2018-03-08T10:15:00Z</StartTime>
            <EndTime>2018-03-08T10:30:00Z</EndTime>
            <PolicyServer>mpe27</PolicyServer>
            <Name>apn1</Name>
            <IsComplete>true</IsComplete>
            <MessagesInCount>1</MessagesInCount>
            <MessagesOutCount>1</MessagesOutCount>
            <CCRMessagesReceivedCount>0</CCRMessagesReceivedCount>
            <CCRMessagesSentCount>0</CCRMessagesSentCount>
            <CCRMessagesTimeoutCount>0</CCRMessagesTimeoutCount>
            <CCASuccessMessagesReceivedCount>0</CCASuccessMessagesReceivedCount>
            <CCASuccessMessagesSentCount>0</CCASuccessMessagesSentCount>
            <CCAFailureMessagesReceivedCount>0</CCAFailureMessagesReceivedCount>
            <CCAFailureMessagesSentCount>0</CCAFailureMessagesSentCount>
            <CCRIMessagesReceivedCount>1</CCRIMessagesReceivedCount>
            <CCRIMessagesSentCount>0</CCRIMessagesSentCount>
            <CCRIMessagesTimeoutCount>0</CCRIMessagesTimeoutCount>
            <CCAISuccessMessagesReceivedCount>0</CCAISuccessMessagesReceivedCount>
            <CCAISuccessMessagesSentCount>0</CCAISuccessMessagesSentCount>
            <CCAIFailureMessagesReceivedCount>0</CCAIFailureMessagesReceivedCount>
            <CCAIFailureMessagesSentCount>1</CCAIFailureMessagesSentCount>
            .....
        </Sample>
    </DiameterPcefApnStats>
</Statistics>
```

- ProtocolErrorsAPN-DIAMETER-<DiameterResultCode> xxx Stats: Figure 6 shows the OSSI query request/response

Figure 6 Sample OSSI Query Request/Response for ProtocolErrorsAPN-DIAMETER



Request:

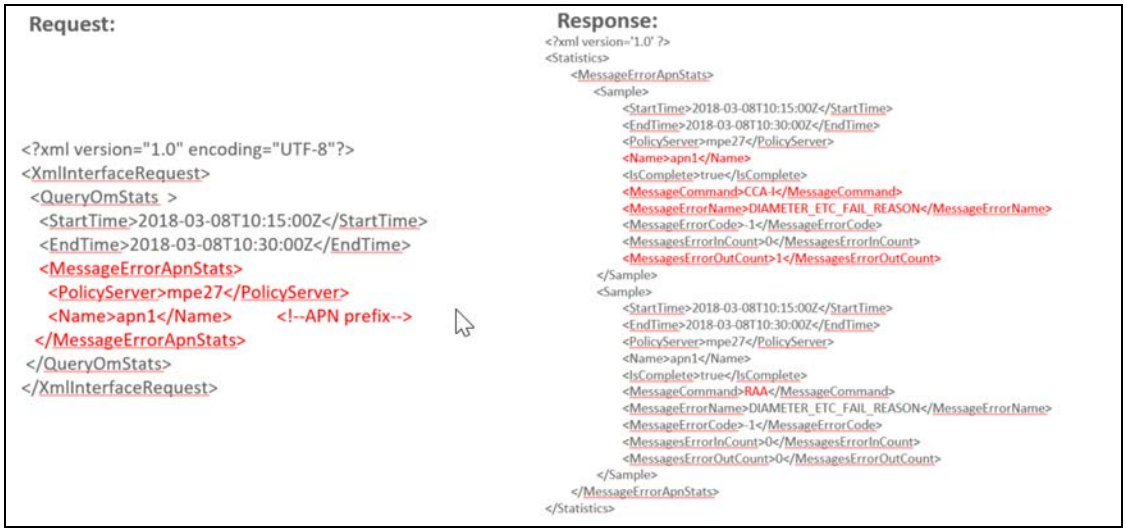
```
<?xml version="1.0" encoding="UTF-8"?>
<XmlInterfaceRequest>
 <QueryOmStats >
  <StartTime>2018-03-08T10:15:00Z</StartTime>
  <EndTime>2018-03-08T10:30:00Z</EndTime>
  <ProtocolErrorApnStats>
   <PolicyServer>mpe27</PolicyServer>
   <Name>apn1</Name>   <!--APN prefix-->
  </ProtocolErrorApnStats>
 </QueryOmStats>
</XmlInterfaceRequest>
```

Response:

```
<Statistics>
    <ProtocolErrorApnStats>
        <Sample>
            <StartTime>2018-03-08T10:15:00Z</StartTime>
            <EndTime>2018-03-08T10:30:00Z</EndTime>
            <PolicyServer>mpe27</PolicyServer>
            <Name>apn1</Name>
            <IsComplete>true</IsComplete>
            <DiameterEtcFailReasonReceived>0</DiameterEtcFailReasonReceived>
            <DiameterEtcFailReasonSent>0</DiameterEtcFailReasonSent>
            <DiameterUserUnknownReceived>0</DiameterUserUnknownReceived>
            <DiameterUserUnknownSent>1</DiameterUserUnknownSent>
            <DiameterUnableToDeliverReceived>0</DiameterUnableToDeliverReceived>
            <DiameterUnableToDeliverSent>0</DiameterUnableToDeliverSent>
        </Sample>
    </ProtocolErrorApnStats>
</Statistics>
```

- MessageErrorsAPN-DIAMETER-<DiameterResultCode>(MessageCmd) xxx Stats (enabled in Wireless-C mode): Figure 7 shows the sample OSSI query request/response

Figure 7 Sample OSSI Query Request/Response for MessageErrorsAPN-DIAMETER



3.2 APN Based Data Source Lookup (BUG 25943867)

3.2.1 Introduction

Currently Oracle Communications Policy Management implementation provides flexibility in selecting data source based on IMSI/MSISDN/NAI. This feature allows the data source (Sh, Sy, LDAP) to be selected based on APN name and combined with existing subscription ID filters. The APN filter support regular expression matching. This feature helps you support multiple services and avoids unnecessary transactions thereby reducing load on nodes in the ecosystem.

3.2.2 Detailed Description

Currently, the data source selection only supports the subscription ID filters. In this implementation, an APN filter is added to the data source selection, which supports regular expression matching. For example if data comes to the MPE with:

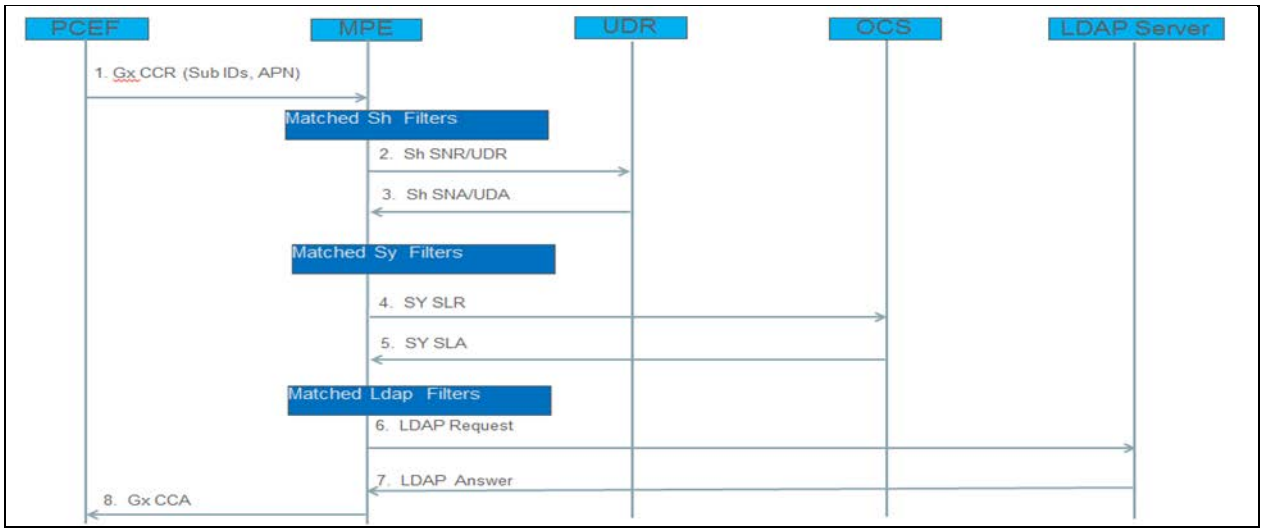
- An APN filter configured for IMS as a prefix match.
- A subscription ID configured for 138 as a prefix on the Sy data source as a Gx CCR-I message with:
  - APN is set to IMS
  - E164 is set to 13800000001.

In this case, an Sy SLR is sent to this Sy data source. Otherwise, if the APN in this message is not set as an IMS prefix, there is one SLR message sent. And for the Sy data source as the secondary data source, this APN filter rules is applied when the primary data source is matched and selected. Table 2 shows examples for these filter matching rules. In this example, only E164 is used, however all sub IDs (IMSI, MSISDN and NAI) are suitable.

Table 2 Filter Matching Rules Examples

Filter Description	Filter Configuration		APN and Subscription IDs	Is matched?
	Sub IDs Filter	APN filter		
Only Subscription IDs configured as Prefix match	E164 is `138.*`	N/A	`APN=pdn1.xxx.com` `E164=13800000001`	Yes
Only APN filter configured as Prefix match	N/A	APN is `pdn.*`	`APN= pdn1.xxx.com` `E164=13800000001`	Yes
Sub ID as equal match, APN as prefix match	E164 is `138`	APN is `pdn.*`	`APN= pdn2.xxx.com` `E164=13800000001`	No
Sub ID as prefix match, APN as prefix match	E164 is `138.*`	APN is `pdn.*`	`APN= pdn1.xxx.com` `E164=13800000001`	Yes
APN as not equal match	N/A	APN is `apn = ^\(?!.*pdn\).*$`	`APN= pdn1.xxx.com`	No
APN as a Not Equal match and Sub ID as a match	E164 is `138.*`	APN is `apn = ^\(?!.*pdn\).*`$	`APN= pdn1.xxx.com` `E164=13800000001`	Yes
APN as equal match	N/A	APN is `pdn`	`APN= pdn1.xxx.com`	No
APN as an Equal match and SUB ID as a match	E164 is `138.*`	APN is `pdn1.xxx.com`	`APN= pdn1.xxx.com` `E164=13800000001`	yes

Figure 8 General Call Flow with APN Based Data Ssource Selection



1. PCEF sends a Gx CCR message with subscription IDs(E164/IMSI/NAI) and Called-Station-ID AVP.
2. MPE checks if there are filters for current Sh Data source selection, three criteria are supported:
   - Only subscription IDs filters are found.

     In this case, the current Sh data source is selected if at least one subscription ID filter is matched.

- Only APN filters are found.

  In this case, the current Sh data source is selected if at least one APN filter is matched.

- Both subscription IDs and APN are found.

  In this case, the current Sh data source is selected when a subscription ID filter and an APN filter are matched.

An Sh SNR/UDR message is sent if the current Sh data source is selected.

3. Sh SNA/UDA message is received on MPE.
4. MPE checks if there are filters for current Sy Data source selection, three cases are supported:
   - Only subscription IDs filters are found.

     In this case, the current Sy data source is selected if at least one subscription ID filter is matched.

   - Only APN filters are found.

     In this case, the current Sy data source is selected if at least one APN filter is matched.

   - Both subscription IDs and APN are found.

     In this case, the current Sy data source is selected when a subscription ID filter and an APN filter are matched.

   An Sy SLR message is sent if the current Sy data source is selected. For a secondary Sy Data source, this data source filter rule runs if it has a primary data source selected.
5. Sy SLA message is received on MPE.
6. MPE checks if there are filters for the current LDAP data source selection, three criteria are supported:
   - Only subscription IDs filters are found.

     In this case, the current LDAP data source is selected if at least one subscription ID filter is matched.

   - Only APN filters are found.

     In this case, the current LDAP data source is selected if at least one APN filter is matched.

   - Both subscription IDs and APN are found.

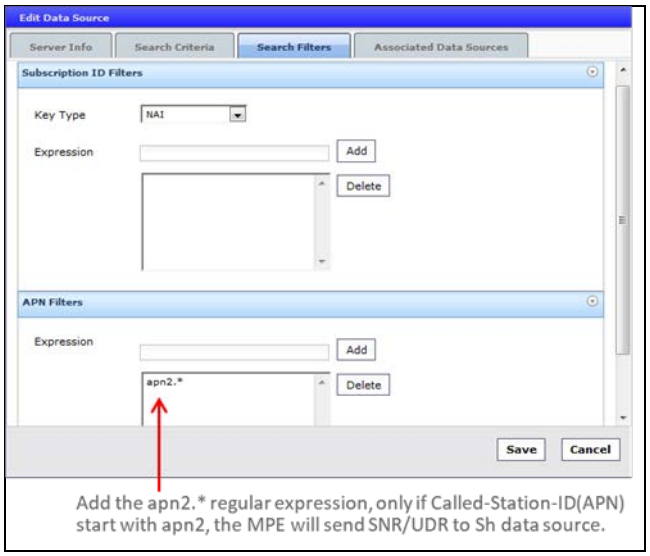
     In this case, the current LDAP data source is selected when a subscription ID filter and an APN filter are matched.

   An LDAP request message is sent if the current LDAP data source is selected
7. LDAP Answer message is received on MPE.
8. MPE sends back CCA Message to PCEF with related user information.

3.2.3 User Interface Changes

There are three filters added for Sh, Sy, and LDAP data source on the CMP GUI. All the APN filter names support regular expression.

Figure 9 Sh Data Source Filter



The data source search criteria

- `And` relation between APN filter and Subscription ID filter
- `Or` relationship among same kind of filters

Figure 10 Sy Data Source Filter

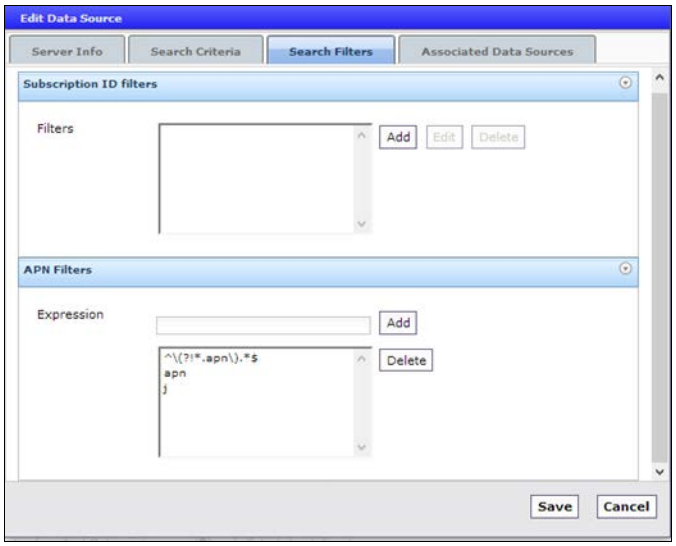
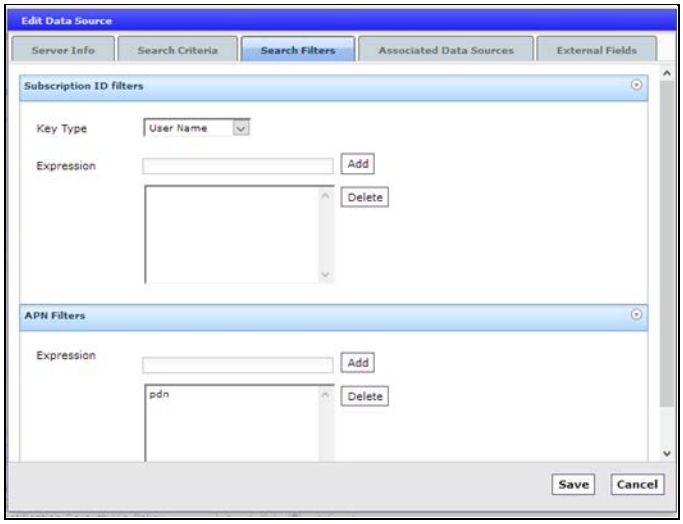


Figure 11 LDAP Data Source Filter



3.3 SMS Notification Enhancement-Delivery SMS to different destinations based on policy actions (BUG 25902148)

3.3.1 Introduction

Currently, PCRF only supports sending SMS via one default SMS gateway for all use cases which require policy action of sending SMS notifications. With this enhancement, the send SMS related policy action is enhanced to allow select a destination SMS gateway.

In R12.4, the PCRF is enhanced to send SMS notifications to different SMS destination hosts based on different use cases using:

- SMPP protocol
- CMPP protocol

3.3.2 Detailed Description

3.3.2.1 Policy Changes

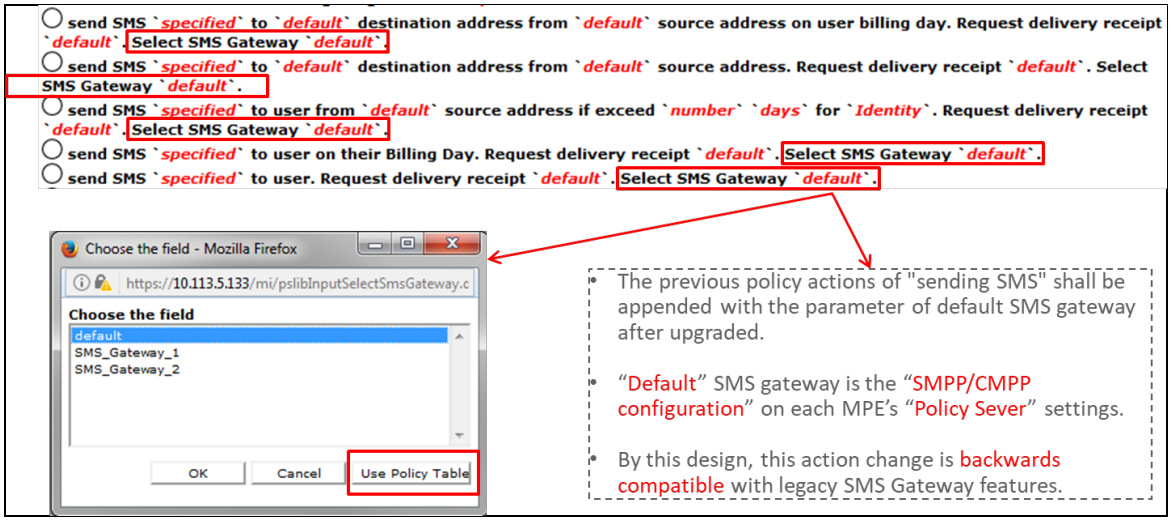
To support this feature, the sending SMS policy actions are appended with a new parameter.

```
Select SMS Gateway `default`
```

When the default parameter link is selected, a window opens as shown in Figure 12. The window lists the SMS gateways. The SMS gateways in the list are configured using the CMP SMS Gateways page. Only one gateway can be selected for the policy action. Selecting default in the gateway list indicates that SMS messages are sent to the default SMS gateway. The default SMS gateway is configured in the CMP using **Policy Server → CMPP/SMPP Configuration**.

In CMPP/SMPP mode, there are 5 sending SMS policy actions that are changed.

Figure 12 Sending SMS Policy Actions in CMPP or SMPP mode



3.3.2.2 User Interface Changes

The CMP added a level 2 menu called MS Gateways under the POLICY SERVER menu. The menu is displayed when either SMPP or CMPP mode is enabled. The CMP is used to configure SMS Gateways lists.

Figure 13 SMS Gateways Menu

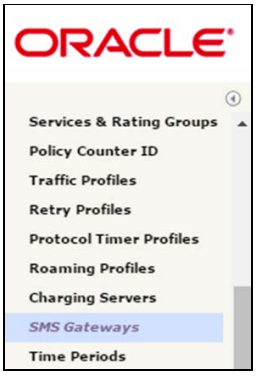


Figure 14 SMS Gateways (CMPP mode)

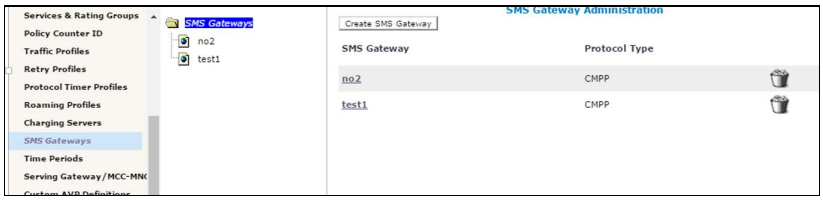
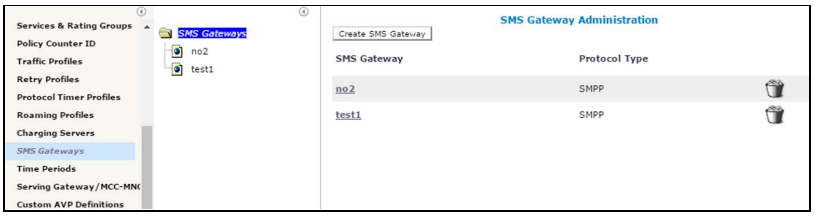
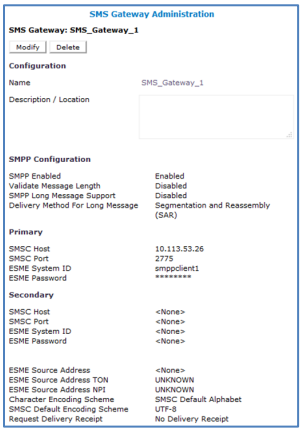


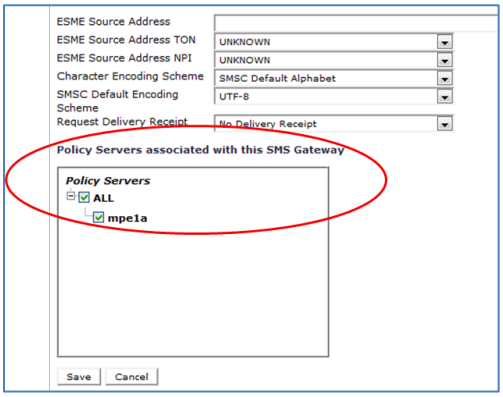
Figure 15 SMS Gateways (SMPP mode)

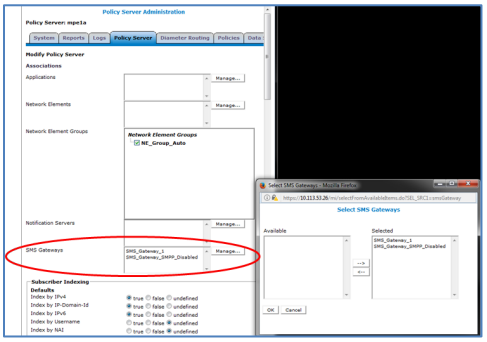


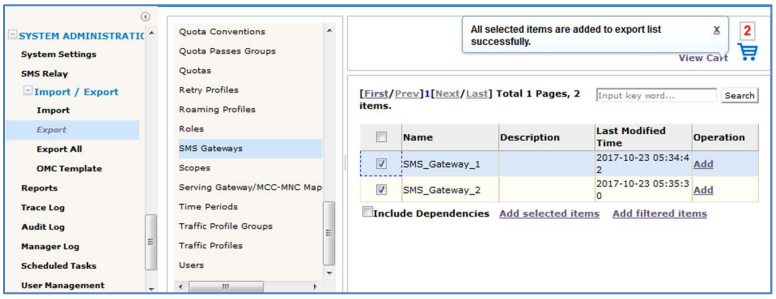
CMP: Manage SMS Gateways (sample screenshots):

- SMPP Enabled must be enabled to use SMS Gateway.
- Associate to MPE when add/edit SMS Gateway.
- Associate the SMS Gateway with the MPE server using the modify option on the **Policy Server** tab.
- Import/Export SMS Gateway.









3.3.2.3 OSSI Support for SMS Gateway

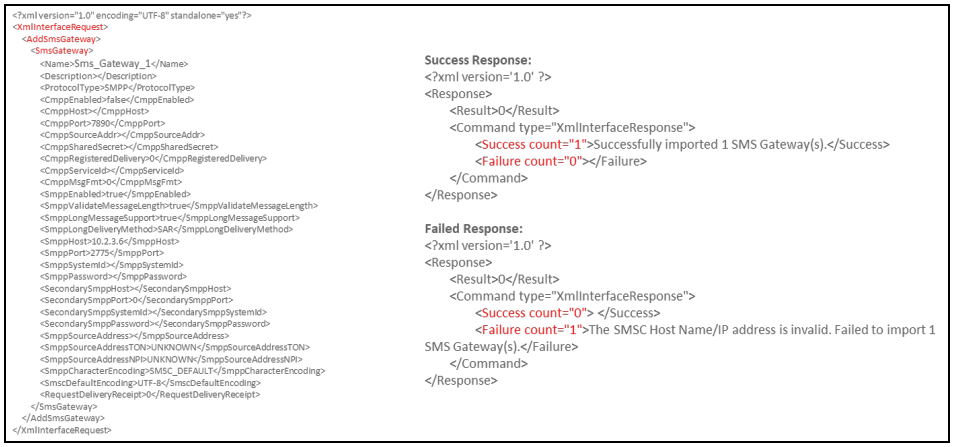
The OSSI supports the SMS Gateway type. Figure 16 through Figure 19 show samples of the SMS Gateway Query, Add, Update, and Delete OSSI requests.

Figure 16 OSSI: Query SMS Gateway

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<XmlInterfaceRequest>
  <QuerySmsGateway>
    <SmsGateway>
      <Name>Sms_Gateway_1</Name>
    </SmsGateway>
  </QuerySmsGateway>
</XmlInterfaceRequest>
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ConfigurationData version="12.4.0.0.0">
  <SmsGateway>
    <Name>Sms_Gateway_1</Name>
    <Description>ss</Description>
    <ProtocolType>CMPP</ProtocolType>
    <CmppEnabled>true</CmppEnabled>
    <CmppHost>1.2.3.4</CmppHost>
    <CmppPort>7890</CmppPort>
    <CmppSourceAddr></CmppSourceAddr>
    <CmppSharedSecret></CmppSharedSecret>
    <CmppRegisteredDelivery>0</CmppRegisteredDelivery>
    <CmppServiceId></CmppServiceId>
    <CmppMsgFmt>0</CmppMsgFmt>
    <SmppEnabled>false</SmppEnabled>
    <SmppValidateMessageLength>true</SmppValidateMessageLength>
    <SmppLongMessageSupport>true</SmppLongMessageSupport>
    <SmppLongDeliveryMethod>SAR</SmppLongDeliveryMethod>
    <SmppHost></SmppHost>
    <SmppPort>2775</SmppPort>
    <SmppSystemId></SmppSystemId>
    <SmppPassword></SmppPassword>
    .....
    <RequestDeliveryReceipt>0</RequestDeliveryReceipt>
  </SmsGateway>
</ConfigurationData>
```

Figure 17 OSSI: Add SMS Gateway



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<XmlInterfaceRequest>
  <AddSmsGateway>
    <SmsGateway>
      <Name>Sms_Gateway_1</Name>
      <Description></Description>
      <ProtocolType>SMPP</ProtocolType>
      <CmppEnabled>false</CmppEnabled>
      <CmppHost></CmppHost>
      <CmppPort>7890</CmppPort>
      <CmppSourceAddr></CmppSourceAddr>
      <CmppSharedSecret></CmppSharedSecret>
      <CmppRegisteredDelivery>0</CmppRegisteredDelivery>
      <CmppServiceId></CmppServiceId>
      <CmppMsgFmt>0</CmppMsgFmt>
      <SmppEnabled>true</SmppEnabled>
      <SmppValidateMessageLength>true</SmppValidateMessageLength>
      <SmppLongMessageSupport>true</SmppLongMessageSupport>
      <SmppLongDeliveryMethod>SAR</SmppLongDeliveryMethod>
      <SmppHost>10.2.3.6</SmppHost>
      <SmppPort>2775</SmppPort>
      <SmppSystemId></SmppSystemId>
      <SmppPassword></SmppPassword>
      <SecondarySmppHost></SecondarySmppHost>
      <SecondarySmppPort>0</SecondarySmppPort>
      <SecondarySmppSystemId></SecondarySmppSystemId>
      <SecondarySmppPassword></SecondarySmppPassword>
      <SmppSourceAddress></SmppSourceAddress>
      <SmppSourceAddressTON>UNKNOWN</SmppSourceAddressTON>
      <SmppSourceAddressNPI>UNKNOWN</SmppSourceAddressNPI>
      <SmppCharacterEncoding>SMSC_DEFAULT</SmppCharacterEncoding>
      <SmscDefaultEncoding>UTF-8</SmscDefaultEncoding>
      <RequestDeliveryReceipt>0</RequestDeliveryReceipt>
    </SmsGateway>
  </AddSmsGateway>
</XmlInterfaceRequest>
```

Success Response:

```
<?xml version='1.0' ?>
<Response>
    <Result>0</Result>
    <Command type="XmlInterfaceResponse">
        <Success count="1">Successfully imported 1 SMS Gateway(s).</Success>
        <Failure count="0"></Failure>
    </Command>
</Response>
```

Failed Response:

```
<?xml version='1.0' ?>
<Response>
    <Result>0</Result>
    <Command type="XmlInterfaceResponse">
        <Success count="0"> </Success>
        <Failure count="1">The SMSC Host Name/IP address is invalid. Failed to import 1
SMS Gateway(s).</Failure>
    </Command>
</Response>
```

Figure 18 OSSI: Update SMS Gateway

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<XmlInterfaceRequest>
  <UpdateSmsGateway>
    <SmsGateway>
      <Name>Sms_Gateway_1</Name>
      <Description></Description>
      <ProtocolType>SMPP</ProtocolType>
      <CmppEnabled>false</CmppEnabled>
      <CmppHost></CmppHost>
      <CmppPort>7890</CmppPort>
      <CmppSourceAddr></CmppSourceAddr>
      <CmppSharedSecret></CmppSharedSecret>
      <CmppRegisteredDelivery>0</CmppRegisteredDelivery>
      <CmppServiceId></CmppServiceId>
      <CmppMsgFmt>0</CmppMsgFmt>
      .....
    </SmsGateway>
  </UpdateSmsGateway>
</XmlInterfaceRequest>
```

Figure 19 OSSI: Delete SMS Gateway

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<XmlInterfaceRequest>
  <DeleteSmsGateway>
    <SmsGateway>
      <Name>Sms_Gateway_1</Name>
    </SmsGateway>
  </DeleteSmsGateway>
</XmlInterfaceRequest>
```

3.3.3 Feature Activation

1. The feature is active only when SMPP/CMPP mode enabled.
2. `Sending SMS via SMS gateway X` is appended to existing send SMS policy action.
3. CMP GUI allows a maximum of 10 different SMS configured gateways.

3.4 Send SMS Notification Enhancement-Send SMS Notification frequency based on policy per use case (BUG 25902163)

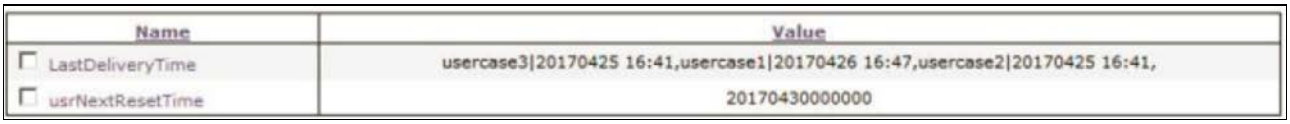
3.4.1 Introduction

This feature is an enhancement for the existing SMS send notification procedure to allow you to reset the last delivery time for specific use cases in the user state field of LastDeliveryTime using the new policy action.

3.4.2 Detailed Description

Currently, the user state field LastDeliveryTime is used to store Last Delivery Time of different use cases to support the send SMS notification frequency based on policy per use case feature.

Figure 20 User State Field of LastDeliveryTime



Name	Value
LastDeliveryTime	usercase3|20170425 16:41,usercase1|20170426 16:47,usercase2|20170425 16:41,
usrNextResetTime	20170430000000

The existing policy action:

```
remove the subscriber state variable name and save always
```

is used to reset the whole value of LastDeliveryTime, but in some cases, you just want to reset the last delivery time of specific use cases and retain the values which do not need to be reset.

This feature introduces a policy action that resets the last delivery time based on a specific use case.

This feature also introduced a policy condition that checks if the last delivery time for a specific use case exists in the Subscriber. State LastDeliveryTime.

3.4.3 Policy Changes

Introduced policy action and condition for this feature.

Policy Condition Group	Policy Condition or Action	Description
Condition Group "State Variables"	where the last delivery time of specific use case exists in the user state variable of LastDeliveryTime	Check whether or not the last delivery time of specific use case exists in the user stat variable of "LastDeliveryTime". specific use case : a string value of a specific use case name exists : "exists" or "does not exist"
New Optional Action	reset the last delivery time of specific use case(s) in the user state variable of LastDeliveryTime	Reset the last delivery time of specific use case(s) in the subscriber state field of "LastDeliveryTime". specific use case(s) : a comma-delimited list of values of specific use case name

3.4.3.1 Sample Use Cases

- Subscriber.State.usrStatus defines the user quota usage status.
- 1: not exceeded 4G quota plan, 2: exceeded 4G quota plan
- In the middle of a billing cycle, BOSS updates userStatus to 2 if the quota plan is exceeded, an SMS is sent to notify user.
- PCRF/Oracle Communications User Data Repository resets userStatus to 1 when next billing cycle starts, and resets the SMS notification LastDeliveryTime.
- If subscriber recharge, the SMS notification LastDeliveryTime is reset.

Sample Policy 1

If subscriber recharges, BOSS updates Subscriber.State.usrStatus to 1, and PCRF resets SMS notification cycle.

```
where notification from Sh datasource is received for any one of User state
    And where the subscriber state variable usrStatus exists
    And where the subscriber state variable usrStatus matches one of `1`
    And where the last delivery time of Exceed4G exists in the user state variable of
LastDeliveryTime
reset the last delivery time of Exceed4G in the user state variable of LastDeliveryTime
re-authorize all PCEF/TDF sessions associated with User
continue processing message
```

Sample Policy 2

Next billing cycle starts (for example, first day of next month), PCRF updates Subscriber.State.usrStatus to 1 and resets the SMS notification cycle.

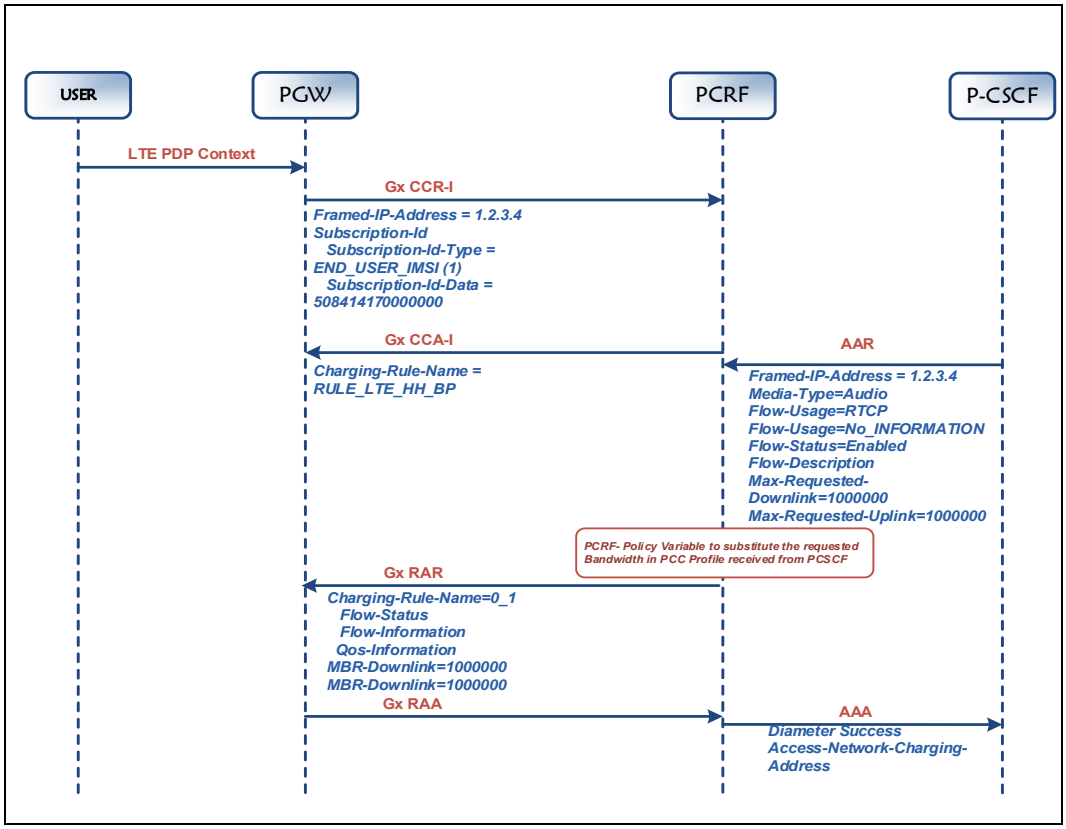
```
where the request is re-authorizing an existing session
    And where the session is an enforcement session
    And where the reauthorization reason is REASON_USER_SCHEDULED_TASK
    And where the reauth request is triggered by scheduled task containing Billing
Day Any with reset action
    And where the last delivery time of Exceed4G exists in the user state variable of
LastDeliveryTime
reset the last delivery time of Exceed4G in the user state variable of LastDeliveryTime
continue processing message
```

3.5 Session variable to access Maximum-Requested-Bandwidth (BUG 25455923)

3.5.1 Introduction

This feature is an enhancement for the existing Oracle Communications Policy Management procedure to add flexibility in supporting VOLTE use cases where you wants to override the adjusted bandwidth values calculated by PCRF, with the requested value provided by AF through the Rx interface. This bandwidth information is made available to the co-related Gx session.

Figure 21 VoLTE General Call flow (Session Variable to Access MRB)



3.5.2 Detailed Description

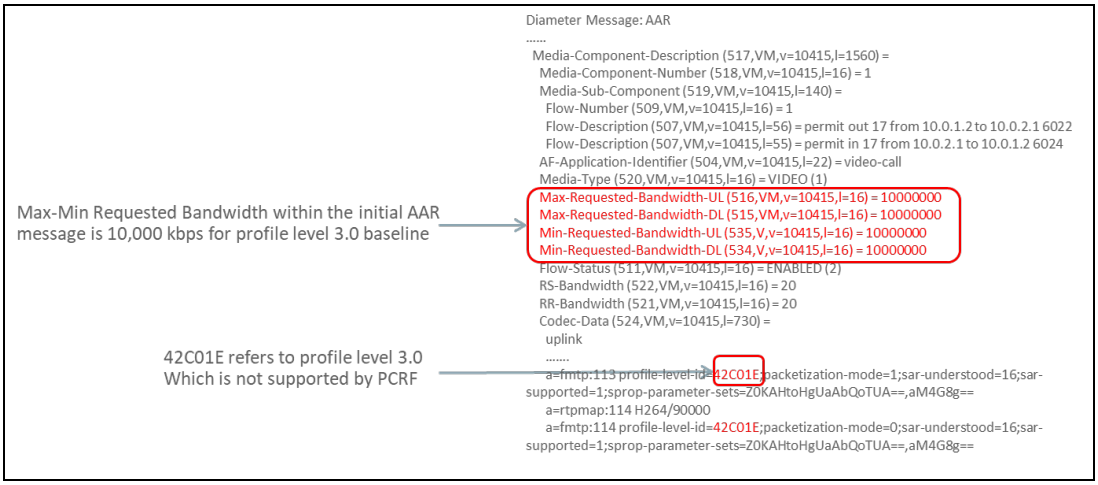
Currently, ORACLE COMMUNICATIONS POLICY MANAGEMENT only supports H264 profile level 1.1, 1.2, 3.1.

If the requested profile level is not supported, the bandwidth is recalculated based on the default H264 profile level 1.1. The default profile is configured using the **sh cfg** command.

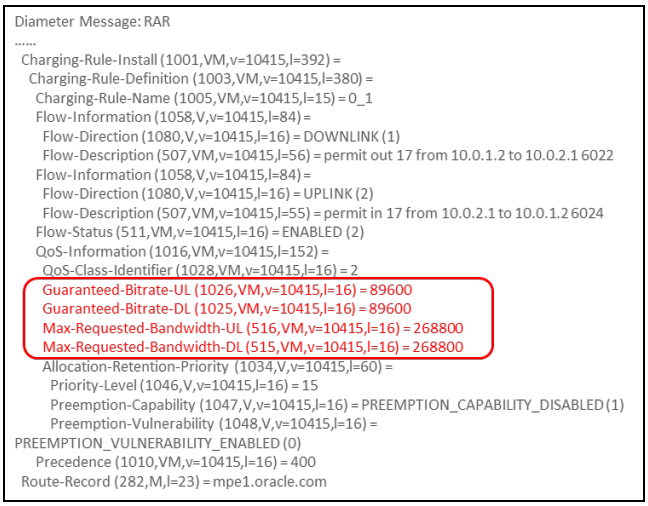
```
RcMgr> sh cfg DIAMETER.AF.RTPAVPFH264ProfileDefaultLevel -v
DIAMETER.AF.RTPAVPFH264ProfileDefaultLevel
  Description:    This is the value of RTP/AVPF H264 Profile default Level
                  .Example:11 means level 1.1,12 means level 1.2,31 means
                  level3.1
  Default Value:  11
```

Then the recalculated bandwidth result may not meet the requested bandwidth.

Figure 22 Example of Problem: AAR with codec Data



- RAR message
- Bandwidth recalculated with default profile level 1.1
- Bandwidth values 268.8 kbps and 89.6 kbps are provided.
- The bandwidth cannot meet the requirement for level 3.0 baseline.



This enhancement introduced 4 variables for the original Max-Min Requested Bandwidth value provided by the AF through the Rx interface.

There are two new variables that can be used as internal substitution variables so that you can configure a policy to utilize the variables to override the unexpected bandwidth values adjusted by PCRF.

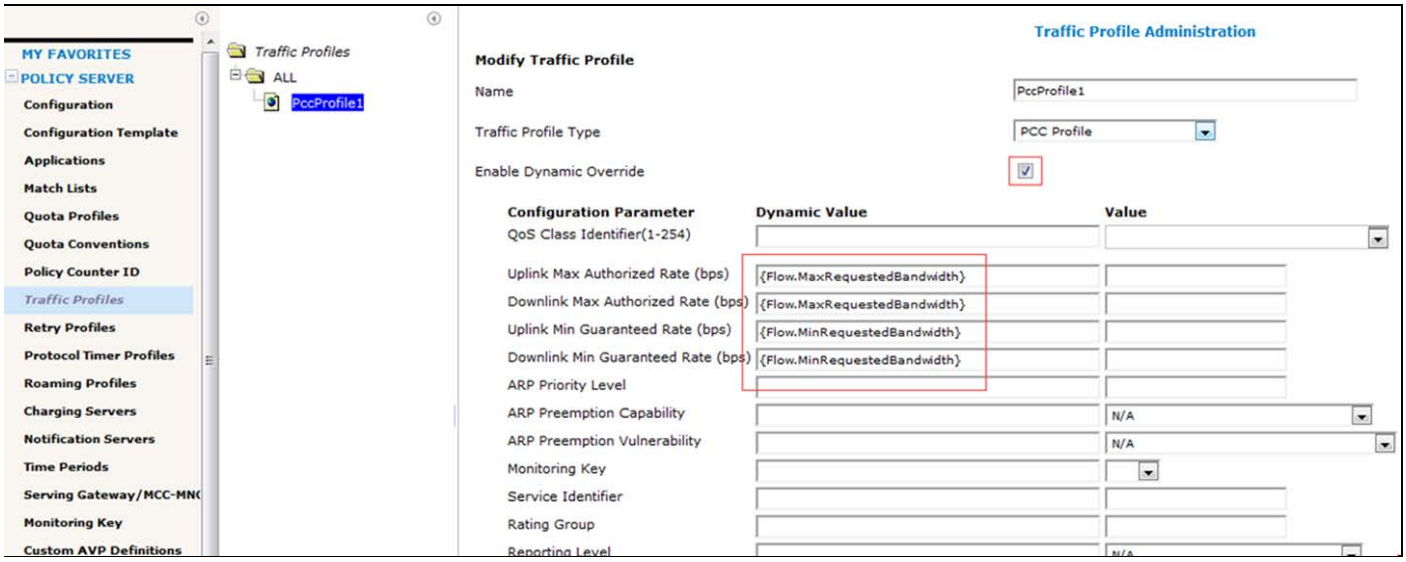
Variable Name	Description
Flow.MaxRequestedBandwidth	The default value is -1, is used to access the original value of the AVP Max-Requested-Bandwidth-UL/Max-Requested-Bandwidth-DL within the MCD/MSC of Rx AAR message.
Flow.MinRequestedBandwidth	The default value is -1, is used to access the original value of the AVP Min-Requested-Bandwidth-UL/Min-Requested-Bandwidth-DL within the MCD/MSC of Rx AAR message.

NOTE: Max requested Bandwidth information provided within the MSC takes precedence over information within the encapsulating MCD.

3.5.3 User Interface Changes

The first step in overriding the unexpected bandwidth adjusted by PCRF is to create a PCC profile. The below figure depicts the sample PCC profile to override bandwidth.

Figure 23 Sample PCC Profile to Override Bandwidth



3.5.4 Sample Policy to Apply the PCC Profile and Override Bandwidth

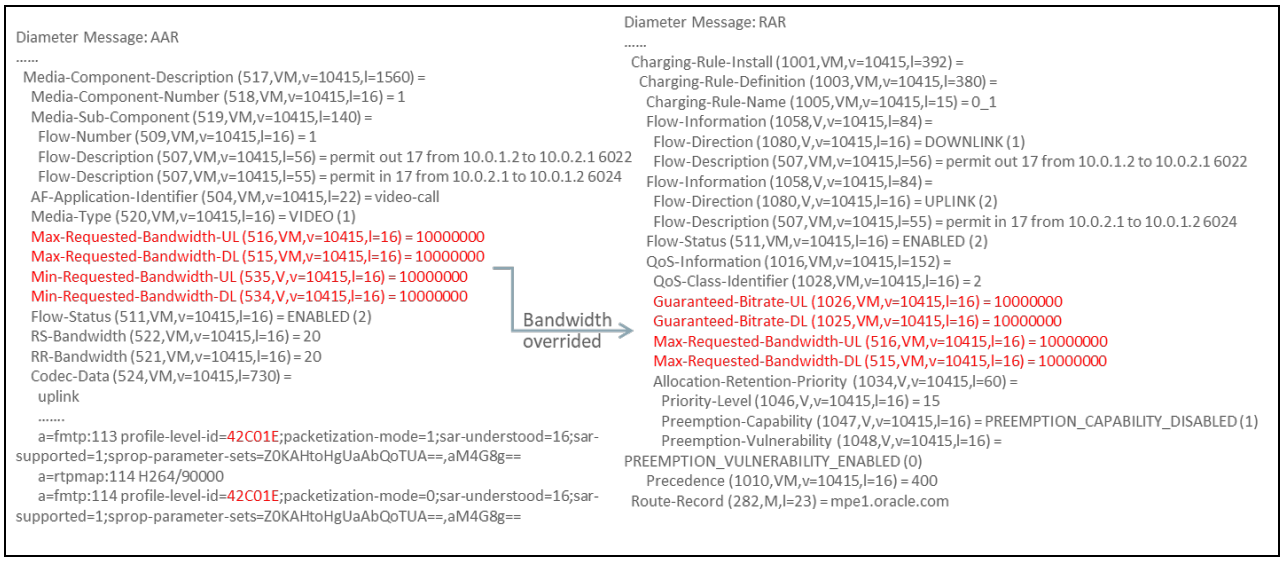
The following figure shows a sample example:

Policy Description

where the request is *creating a new flow,modifying an existing flow*
And where the session is *an application session*
And where the flow media type is one of *Video*
And where the *common sdp.[codec-name(H264).fmtp.profile-level-id] exists*
And where the *common sdp.[codec-name(H264).fmtp.profile-level-id] does not match any of 42E00B,42E00C,42E01F*
apply *PccProfile1* to flow
skip to next flow

After the deployment of the policy is complete, the previous test can be performed again to demonstrate the effects. The message stack is shown in Figure 24:

Figure 24 Sample AAR and RAR Message Stack



3.6 Extending Oracle Communications Policy Management Session and Binding Information to External Systems/Subscriber Session Information Interface (BUG 22935518)

3.6.1 Introduction

Currently, the CMP Session Viewer GUI for the MRA or MPE displays binding data for a specific subscriber from the specific MRA or MPE.

With this enhancement, CMP provides an OSSI interface for external systems that allows you to conveniently query the subscriber binding and session information, without knowing which MRA and MPE supports the target sessions.

3.6.2 Detailed Description

CMP query MRAs until find the binding, then query target MPE for session data, the following diagram shows the steps of how Oracle Communications Policy Management processes the request.

Figure 25 General Call Flow of Oracle Communications Policy Management Processes the Request

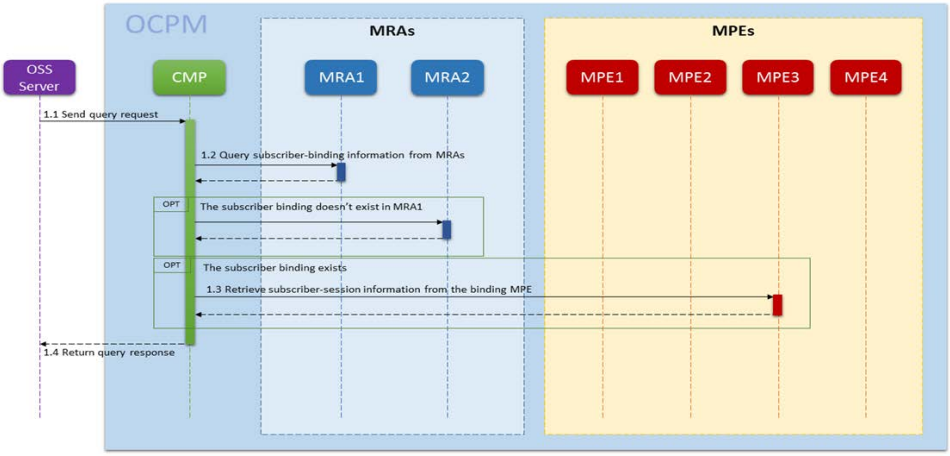
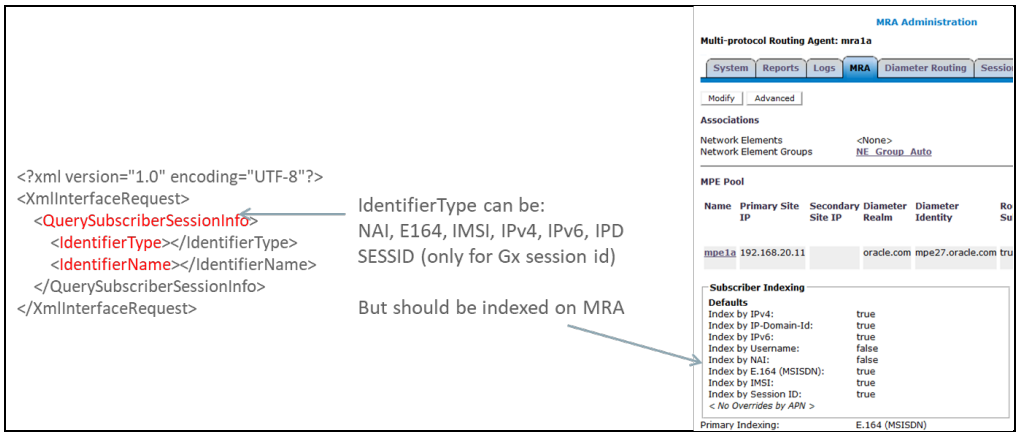


Figure 26 OSSI Request Query Subscriber Session Info: Request Format



3.6.3 Limitations

1. At least one MRA cluster must be deployed.
2. If querying by SESSID, only Gx session id support.
3. N-CMP not verified by PV.

3.6.4 Performance

BL460G8: 710 TPS (Transaction per Second)

4. PROTOCOL FLOW/PORT CHANGE

No Changes

5. MEAL INSERTS

This section summarizes the changes to alarms, measurements, KPIs, and MIBs. In the following inserts pertain to Oracle Communications Policy Management Release 12.4.0.0.0_51.1.0 MEAL snapshot and deltas to earlier releases 12.2.x/12.3.x to 12.4

The Policy Management GA Release is 12.4.0.0.0_51.1.0

Note:

- Policy Product Release: 12.4.0.0.0_51.1.0
- Base Distro Product: TPD
- Base Distro Release: 7.5.0.0.0_88.46.0

  12.2.0.0.0_65.1.0 is TPD: 7.0.3.0.0_86.46.0

  12.2.1.0.0_6.1.0 is TPD: 7.0.3.0.0_86.46.0

  12.3.0.0.0_29.1.0 is TPD: 7.0.3.0.0_86.46.0

The MEAL spreasheets can be found on the Policy Mangement Release 12.4 documentation page. All the files are contained in a downloadable .zip file.

- MEAL Snapshot: Policy-12.2.0.0.0_65.1.0 to Policy-12.4.0.0.0_51.1.0

  Filename: MEAL_Policy-12.2.0.0.0_65.1.0-Policy-12.4.0.0.0_51.1.0.xslx
- MEAL Deltas (Policy-12.2.1.0.0_6.1.0 to Policy-12.4.0.0.0_51.1.0)

  Filename: MEAL_Policy-12.2.1.0.0_6.1.0-Policy-12.4.0.0.0_51.1.0.xslx
- MEAL Deltas (Policy-12.3.0.0.0_29.1.0 to Policy-12.4.0.0.0_51.1.0)

  Filename: MEAL_Policy-12.3.0.0.0_29.1.0-Policy-12.4.0.0.0_51.1.0.xslx
- MEAL Snapshot: Policy-12.4.0.0.0_51.1.0

  Filename: MEAL_Policy-12.4.0.0.0_51.1.0.xslx
- DELTA of TPD Changes from Policy 12.2.x/12.3.x to 12.4.x

  Filename: MEAL_tpd-7.0.3.0.0_86.46.0-tpd-7.5.0.0.0_88.46.0.xslx

  Filename: MEAL_tpd-7.5.0.0.0_88.46.0.xslx