

Oracle® Communications Policy and Charging Rules Function PCRF Network Impact Report

11.5

E61658-02

March 2016

PCRF Network Impact Report

Oracle® Communications Policy and Charging Rules Function, Network Impact Report, Release 11.5

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

MOS (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration. Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>.

TABLE OF CONTENTS

1	INTRODUCTION	4
1.1	PURPOSE/SCOPE	4
1.2	DISCLAIMERS	4
2	REFERENCES.....	4
2.1	ACRONYMS	4
3	ARCHITECTURAL CHANGES (PR232964).....	5
3.1	SUPPORT FOR OCUDR	5
3.2	HARDWARE CHANGES	6
3.3	SOFTWARE CHANGES	6
3.3.1	PLATFORM 6.7.....	6
3.4	FIRMWARE CHANGES	7
3.5	UPGRADE OVERVIEW	8
3.5.1	Upgrade Path	8
3.5.2	Order of Upgrade	8
3.6	MIGRATION OF POLICIES AND SUPPORTING POLICY DATA	8
4	POLICY 11.0 AND 11.1 FEATURES THAT ARE NEEDED FOR 11.5 ROW RELEASE (PR232929)	9
4.1	POLICY ROLLBACK ENHANCEMENTS (PR 219580).....	9
4.2	PCRF COMPLIANCE WITH 3GPP-R11 SPECIFICATION (PR 221797).....	9
4.3	CODEC SUPPORT CHANGES (PR 221799).....	10
4.4	EXPORT SESSION/BINDING DATABASES FOR OFFLINE EXTERNAL PROCESSING (PR 221799)	10
4.5	SUPPORT OF Rx SUBSCRIPTION EXPIRY	10
4.6	SPLIT PDN COUNT BY APN NAME (221817).....	11
4.7	PCRF PERFORMANCE IMPROVEMENTS FOR 2013 (221818)	13
4.8	MULTI-STREAM WAN REPLICATION FOR GEO-REDUNDANCY(PRs 221989 & 222399).....	14
4.9	POLICY SUPPORT FOR SEPARATING TRAFFIC ON DIFFERENT VLANs)PLATFORM PR 211237, POLICY PR 222399)	15
4.10	MRA AGGREGATED COUNTS DISPLAYED ON THE KPI DASHBOARD (PR 222746).....	16
4.11	SPLIT AF SESSION BY RAT TYPE (PR 223393).....	17
4.12	ENHANCEMENT TO AVOID OSCILLATIONS IN SYSTEM RESPONSE DURING OVERLOAD IN GEN8 CONFIGURATION (PR 223504)	18
4.13	ENHANCEMENT TO PCRF LOAD SHEDDING TO TAKE INTO ACCOUNT Rx TRAFFIC (PR 223505).....	19
4.14	ENHANCEMENT TO MRA TO MPE LOAD BALANCING TPS AND SESSION BASED (PR 223519)	21
4.15	CMP BULK OPERATIONS (PR 228704)	23
5	FEATURES-SPECIFIC CHANGES	24
5.1	SUBSCRIBER ACTIVITY LOG (PR 218508)	25
5.2	EXTEND QUOTA POOL TO AT LEAST 20 (PR 232934).....	27
5.3	SUPPORT PRO-RATING ON A PER QUOTA BASIS (PR 235626).....	27
5.4	OPTION TO TRIGGER RAR ON QUOTA CHANGE BY PROVISIONING INTERFACE (PR 232936).....	28
5.5	DYNAMIC QUOTA FOR POOLS (PR 218524).....	32
5.6	SUPPORT DYNAMIC GRANTING ALGORITHM FOR PASSES (PR 234669)	34
5.7	CHARGING CORRELATION (PR 236692, 234002)	36
5.8	SUPPORT FOR NETWORK LOCATION (PR236676, 235934)	38
5.9	TABLE DRIVEN POLICY WITH MULTIPLE-VALUED DATA (PR 221127).....	40
5.10	ALLOW ANY AVP IN THE DICTIONARY TO BE INSERTED IN A MESSAGE (PR 234026).....	42
5.11	SPONSORED DATA CONNECTIVITY (PR 234958).....	43
5.12	PS TO CS HANDOVER FEATURE FOR VoLTE (PR 234003).....	47
5.13	FLOW-DESCRIPTION AVP DOESN'T COMPLY WITH 3GPP RELEASE 9 (PR 232575).....	51
5.14	CORRECT HANDLING OF DUPLICATE Gx DIAMETER REQUESTS (PR 235168 & 235168).....	52
5.15	N-SITE MRA OPTIMIZATIONS AND ENHANCEMENTS (PR 229472).....	53
5.16	TOPOLOGY HIDING IN MRA FOR Rx APPLICATION (PR 239238).....	58

1 Introduction

1.1 Purpose/Scope

Purpose of this Feature Guide document is to highlight the changes in this release of the product that may have impact on the customer network, and should be considered by the customer during planning for this release.

1.2 Disclaimers

This document summarizes Release 11.5 new and enhancement features, and the impacts of these features, at a high level. The Feature Requirements (FRS) documents remain the defining source for the expected behavior of these features.

Note that feature implementations may change slightly during product test.

2 References

- [1] *Formal Peer Review Process*, PD001866, v 2.1, Payne, Sept 2000.
 - [2] *Signaling Transfer Point Generic Requirements, GR-82-CORE, issue 1, (Bellcore), June 1994.*
 - [3] *910-6724-001 Revision B, August 2013*
 - [4] *E56664 Revision 01*
-

2.1 Acronyms

ACL	Access Control List
AVP	Attribute Value Pair
CLI	Command Line Interface
DNS	Domain Name Server
GUI	Graphical User Interface
HSS	Home Subscriber Server
iLO	Integrated Lights Out
IMI	Internal Management Interface
IOT	Interoperability Tests
KPI	Key Performance Indicator
LTE	Long Term Evolution
MEAL.....	Measurements, Events, Alarms, and Logging
MME	Mobility Management Entity
MP.....	Message Processor
MPS	Messages per Second
NE	Network Element
NMS	Network Management System
OAM.....	Operations, Administration, Maintenance
OAM&P	Operations, Administration, Maintenance and Provisioning
OCF	On-line Charging Function
OFCE	Off-line Charging Function
PCRF	Policy Control and Charging Rules Function
P-CSCF.....	Proxy-Call Session Control Function

PDU	Protocol Data Unit
PM&C	Platform, Management and Control
S-CSCF	Session Call Session Control Function
SLF	Subscriber Locator Function
SPR	Subscriber Profile Repository
TPD	ORACLE Platform Distribution
VIP	Virtual IP Address
XMI.....	External Management Interface
XSI.....	External Signaling Interface

3 Architectural Changes (PR232964)

3.1 Support for OCUDR

The Release 11.5 will be supporting OCUDR as part of the overall Policy Solution. The OCUDR release leverages Oracle's internal platform for messaging and database to meet customers performance needs and to align on a common software architecture. The first release of OCUDR will be the OCUDR Release 10.0k. Migration from SDM 9.3 to OCUDR will be supported in subsequent releases.

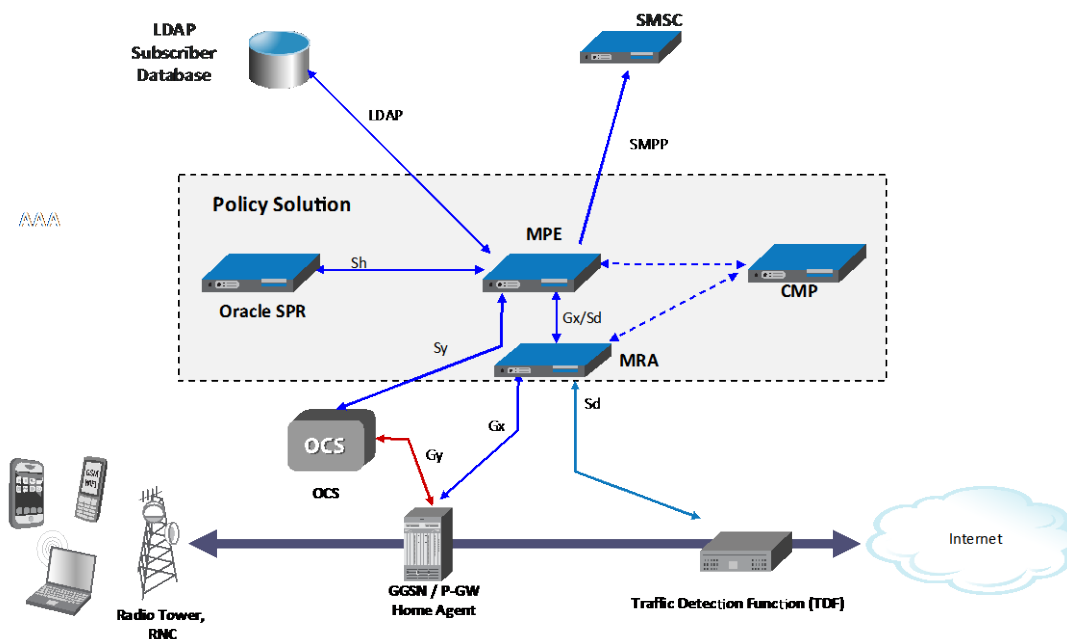


Fig 01: Reference Architecture for Wireless Policy solution

Table below summarizes the performance targets in networks similar to the one presented in Figure-01 above, with OCUDR 10.0 deployed :

Component	Performance Target (per instance)	System TPS capability	System TPS requirement
-----------	-----------------------------------	-----------------------	------------------------

MRA (Statefull, Dynamic)	50,000 TPS 1024 PCRf Client connections	50,000 (100% rated, no failures) /	40,000 TPS@80%
MPE	6,000 TPS for Gen 8 4,500 TPS for Gen 6 6.5M Concurrent Sessions Gen 8/ Gen 6 4 SPR connections.	37,500 TPS@100% • 4 Gen 8 & 3 Gen 6 Clusters 41 M Concurrent Sessions@100% • 4 Gen 8 & 3 Gen 6 Clusters	30,000 TPS@80% • 4 Gen 8 & 3 Gen 6 Clusters 32.8M Concurrent Sessions@80% • 4 Gen 8 & 3 Gen 6 Clusters
SPR	15,000 TPS 60M@100% (2.0K Profile size with overhead) using 96GB Storage	15,000 TPS@100% 60M@100% (2.0K Profile size with overhead) using 96GB Storage	12,000 TPS@80% 48M@80% (2.0K Profile size with overhead) using 96GB Storage
OCUDR R10.0	30,000 TPS 100M@100%(2.0K Profile size with overhead)	30,000 TPS 100M@100%(2.0K Profile size with overhead)	24,000 TPS 80M@80%(2.0K Profile size with overhead)

3.2 Hardware Changes

Hardware	Supported for Customer or Engineering	Comment
HP BL460Gen6	Customer	c-Class
HP BL620Gen7	Customer	c-Class
HP BL460cGen8	Customer	c-Class
X3-2 RMS	Customer	SUN NETRA

Please also note that:

- The PP-5160 servers will not be supported in Release 11.5.
- Release 11.5 shall support mixed deployments of HP G6 and Gen8 blades within a C-Class enclosure.
- Release 11.5 shall support mixed deployments of HP G6 and Gen8 RMS systems.
- Release 11.5 shall not support a mix of Sun Netra RMS systems with Policy application running on either HP G6 blades or RMS or HP Gen8 blades or RMS.
- Release 11.5 shall support Sun Netra RMS system deployed in mixed configuration with other application on HP G6 blades and RMS or HP gen8 blades on RMS.

3.3 Software Changes

3.3.1 Platform 6.7

Supported platform component versions are:

Component	Release
TPD	6.7
Comcol	6.3
PM&C	5.7
TVOE	2.7
Oracle SDM SPR	9.3
OCUDR	10.0

3.4 Firmware Changes

Firmware	Current (Policy Release 10.5)	Current (Policy Release 11.5) - FUP 2.2.7
G8 Blades	System : ProLiant BL460c Gen8 Baseline FW: 2.2.4 Current: 2.2.4 ROM version : 2012.12.14 iLO Driver name: iLO4 Firmware Revision = 1.20	System : ProLiant BL460c Gen8 ROM version w/ TPD builds 82.29 and lower: 2013.09.08 ¹ ROM version w/ TPD builds 82.30 and above: 2014.02.10 iLO Driver name: iLO4 FW Revision=1.51
Onboard Administrator	3.71	4.22
PM&C Server	System : ProLiant DL380p Gen8 ROM version : 2012.12.14 iLO Driver name: iLO4 Firmware Revision = 1.20 TVOE host minimum: 82.37.0 Current baseline is 2.2.5 System : ProLiant DL380 Gen6 ROM version : 2011.05.05 iLO Driver name: iLO2 Firmware Revision = 2.15 TVOE host minimum: 82.37.0 Current baseline is 2.2.5	System : ProLiant DL380p Gen8 ROM version : 2012.12.14 iLO Driver name: iLO4 FW Revision=1.51 TVOE host minimum: TVOE-2.7.0.0.0_84.20.0-x86_64 Current baseline is 2.2.5 System : ProLiant DL380 Gen6 ROM version : 2011.05.05 iLO Driver name: iLO2 Firmware Revision = 2.25 TVOE host minimum: TVOE-2.7.0.0.0_84.20.0-x86_64 Current baseline is 2.2.5
RMS CMP Server	System : ProLiant DL380p Gen8 Baseline FW: 2.2.4 Current: 2.2.4 ROM version : 2012.12.14 iLO Driver name: iLO4 Firmware Revision = 1.20	System : ProLiant DL380p Gen8 Baseline FW: 2.2.7 Current: 2.2.7 ROM version w/ TPD builds 82.29 and lower: 2013.09.08 ² ROM version w/ TPD builds 82.30 and above: 2014.02.10 iLO Driver name: iLO4 FW Revision=1.51
G7 Blades	System : ProLiant BL460c Gen7 Baseline FW: 2.2.4 Current: 2.2.4 ROM version, Current : 2012.12.03 iLO Driver name: iLO3 Firmware Revision = 1.28	System : ProLiant BL460c Gen7 N/A
G6 Blades	System : ProLiant BL460c Gen6 Baseline FW: 2.2.4 Current: 2.2.4 ROM version, Current : 2011.12.02	System : ProLiant BL460c Gen6 Baseline FW: 2.2.7 Current: 2.2.7 ROM version, Current : 2013.10.01 iLO Driver name: iLO2 FW Revision w/

¹ This firmware version requires the installation of Firmware Errata ID CP021603.

² This firmware version requires the installation of Firmware Errata ID CP021628.

	iLO Driver name:iLO2 Firmware Revision = 2.15	TPD 4.x and greater = 2.25

For complete list of changes in FW for different hardware components, please refer to reference [3] & [4] of this document.

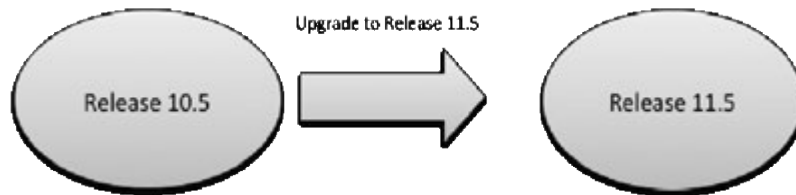
3.5 Upgrade Overview

This section provides an overview of the Upgrade activities for Policy Release 11.5.

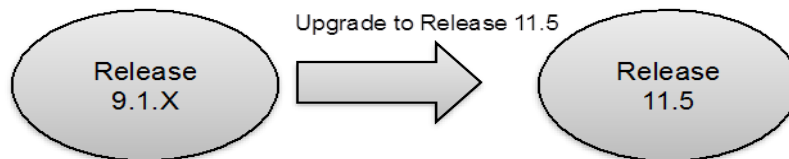
3.5.1 Upgrade Path

Following are the supported upgrade paths to R11.5:

1. PM&C Release 5.x³ to 5.7
2. Policy Release 10.5.x to 11.5



3. Policy Release 9.1.x to 11.5



3.5.2 Order of Upgrade

- 1) Firmware Upgrade: FW upgrades need be carried out first thing according to the section 3.4.
- 2) TVOE upgrade from 2.5 → 2.7 and PM&C upgrade from 5.5 → 5.7
- 3) Policy upgrade in the following sequence:
 - a. CMPs
 - b. MPEs
 - c. MRAs
- 4) Configure for new Policy features

3.6 Migration of Policies and Supporting Policy Data

As in prior releases, the existing policies and supporting data will be conserved during the upgrade. In addition, it will be possible to import Policies and supporting data that was exported from Rel 10.5 or 9.1.x as the case may be.

³ Where x<7

4 Policy 11.0 and 11.1 features that are needed for 11.5 ROW release (PR232929)

4.1 Policy Rollback enhancements (PR 219580)

The enhancement adds new columns to the schema.

When user saves a new Checkpoint, CMP will save Match lists, Retry profiles, Application and Policy Counter Ids into the Checkpoint along with Policies.

New columns in Policy Checkpoints schema

Name	Data type	Desc
rawmatchlist	longblob	The xml format data of match list in CMP system.
rawretryprofile	longblob	The xml format data of retry profile in CMP system.
rawapplication	longblob	The xml format data of application in CMP system.
rawpolicycounter	longblob	The xml format data of policy counter id in CMP system.

4.2 PCRF compliance with 3GPP-R11 specification (PR 221797)

The following requirements have been implemented for these features:

- Added support for Rx-Request-Type AVP in AAR message. The PCRF only stores the value received in this AVP and does not process the value.
- Added support for Min/Max-Requested-Bandwidth-UL/DL AVP's inside the Media-Component-Description AVP
- The PCRF maps between the Min/Max-Requested-Bandwidth-UL/DL and the Guaranteed Bitrate (GBR)

And the following 3GPP specs have been referred for compliance-

3GPP TS 29.212 R11 Sept 2012 - (Gx/Sd) Specification

3GPP TS 29.214 R11 Sept 2012 - (Rx) Specification

3GPP TS 29.213 R11 Sept 2012 - Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping

4.3 Codec Support changes (PR 221799)

The feature supports bandwidth calculation for H.264, VP8 video codecs as well as for T.38 (Fax) codec based on RTP and TCP transport protocol.

The feature enhances MPE to process Codec-Data AVP received over Rx requests and derive bandwidth from the Codec-Data AVP.

The feature provides updated policy rules to set pre-defined bandwidth for received Codec-Data AVP.

4.4 Export Session/Binding Databases for Offline external Processing (PR 221799)

Users can create and extract a subset of an MPE session state database. A command line is used to query the database.

The query produces an XML output file that is stored as a compressed file.

4.4.1.1 Resource Manager

There is no GUI for this. There is a script here with location and syntax found here:

Help text command:

```
$ /opt/camiant/rc/bin/udq.sh -help
```

4.4.1.2 Dependency

None

4.5 Support of Rx Subscription Expiry










The MPE device can be configured to use the Authorization-Lifetime and Auth-Grace-Period AVPs to determine whether an Rx session is stale. A grace period that controls how aggressively the stale Rx sessions are purged can also be configured.

If a message contains the Authorization-Lifetime AVP, and the associated value within the AVP is between the configured minimum and maximum values, then the value in the AVP is used to determine the lifetime of the Rx session. If the value within the AVP is greater than the configured maximum value, then the configured value is used. If the value within the AVP is less than the configured minimum value, then the functionality is disabled, and the value within the AVP is used.

4.5.1 Manager GUI Form

CMP GUI->POLICY SERVER->Configuration->Policy Servers-> Select MPE-> Policy Server->Advanced->add

Other Advanced Configuration Settings

 Add	 Clone	 Edit	 Delete	 Up	 Down
Configuration Key	Value	Default Value	Change Log		
 DIAMETER.Gx.RaceModeratorEnabled	true	false			
 DIAMETER.Gx.RaceRARRetryTimeout	100	100			
 DIAMETER.Gx.RaceRARRetryAttempts	1	1			

Load Shedding Configuration

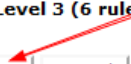
Enabled



► Level 1 (3 rules)

► Level 2 (4 rules)

► Level 3 (6 rules)

 Save Cancel

1. cfg DIAMETER.Gx.RaceRARRetryAttempts to 1 (1=default)
2. cfg DIAMETER.Gx.RaceRARRetryTimeout to 100 (100=default)
3. cfg DIAMETER.Gx.RaceModeratorEnabled to true (false=default)

4.5.2 Dependency

None

4.6 Split PDN Count by APN Name (221817)

Packet data network (PDN) connections can be organized and viewed by access point name (APN).

The PDN connections count can be tracked on up to 25 provisioned, unique APN suffixes.

If the APN of a PDN connection does not match any of the provisioned APN suffixes, that PDN connection is tracked under the Other APNs counter.

A new PDN APN Suffix report is added on the CMP system to display the current and maximum PDN connection counts by APN suffix.

4.6.1 Manager GUI Form

CMP GUI-> POLICY SERVER->Global Configuration Settings->PDN APN Suffixes

Global Configuration Settings

- Precedence Range
- UE-Initiated Procedures
- Stats Settings
- Quota Settings
- eMPS ARP Settings
- Sh Connection Operations
- PDN APN Suffixes**

PDN APN Suffix Administration

Create PDN APN Suffix

PDN APN Suffixes:

apn1. .com	apn1. .com	
apn2. .com		
qq. .com		

PDN APN Suffix configuration

CMP PDN APN Suffix Report page:

CMP GUI->SYSTEM WIDE REPORTS->Sessions->Select PDN APN Suffix Report

The report displays Current and Maximum PDN Connection counts for each APN suffix that has been matched on each MPE server.

Report also displays Aggregation counts for each APN on all MPE servers.

Those PDN connections which do not match any of the APN suffixes are tracked under the OTHER APNs label.

PDN APN Suffix Connection Report (Stats Reset: Manual / Last Refresh :06/05/2013 11:32:49)

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

APN	Server Name	Server Type	Current	Max
TOTAL	TOTAL	TOTAL	0	4
apn1. .com	---	---	0	3
apn1. .com	MPE 35	MPE	0	3
apn2. .com	---	---	0	1
apn2. .com	MPE 35	MPE	0	1

4.6.2 Dependency

None

4.7 PCRF Performance Improvements for 2013 (221818)

Under this PR, PCRF performance improvements are largely carried out by 'Subscriber Indexing Split', in which subscriber indexing is split into indexing by IPv4 address and IPv6 address for both the MRA database and the MPE device. IPv4 and/or IPv6 indexing can be enabled or disabled per APN.

4.7.1 Manager GUI Form

In CMP GUI, Default values for IPv4 and IPv6 can be edited as checkboxes under Subscriber indexing section.

These Defaults can be overridden per APN to either add or remove indexing by IPv4 or IPv6.

Figure 1 – Configure Subscriber indexing

CMP GUI->POLICY SERVER->Configuration->Policy Servers-> Select MPE-> Policy Server->Modify to configure Subscriber indexing

Subscriber Indexing

Index by Username: ☐

Index by NAI: ☐

Index by E.164 (MSISDN): ☐

Index by IMSI: ☐

Index by IP Address

Defaults

Index by IPv4 Address: ☒

Index by IPv6 Address: ☒

Override by APN

APN	IPv4	IPv6
foo	true	false
bar	false	true
baz	false	false
quuz	true	true

4.7.2 Dependency

None

4.8 Multi-Stream WAN replication for Geo-Redundancy(PRs 221989 & 222399)

Only PCRF-GeoRedundant MPE/MRA clusters use this feature. The Replication Stream Count sets up redundant TCP/IP socket connections (“streams”) between the MPE/MRA servers at different sites. It improves the robustness of DB replication traffic over a WAN link that connects the two sites.

The MPE/MRA DB Replication over LAN is unaffected by still using a single stream.

4.8.1 Manager GUI Form

Platform Setting → Topology Setting → (MPE/MRA Cluster name) → Modify Cluster Setting → Replication Stream Count

Topology Configuration

Cluster Settings

Cluster Settings

Name

Appl Type

Site Preference

DSCP Marking

Replication Stream Count

Replication & Heartbeat

Backup Heartbeat

None☐

OAM☐

There is a new Replication statistics report on CMP GUI:
System Wide Reports → Others → MPE/MRA Rep Stats

MPE/MRA Rep Stats (Stats Reset: Manual / Last Refresh: 12/18/2013 13:42:52)

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

Servers	Cluster Name	App Type	Total Sent KB	Peak Sent KB/s	Avg Sent KB/s	Total Recv KB	Peak Recv KB/s	Avg Recv KB/s	Description
mpe-1b->	-mpe-1	MPE	5	0	0	10	1	0	LAN
l-mpe-1a			10	1	0	5	0	0	LAN
mpe-1a->			0	0	0	11	1	0	LAN
mra-1a->	-mra-1	MRA	0	0	0	0	0	0	WAN
l-mra-1b			0	0	0	0	0	0	WAN
mra-1c->			0	0	0	0	0	0	WAN
mra-1c->	-mra-1	MRA	0	0	0	0	0	0	WAN
l-mra-1a			5	0	0	11	1	0	WAN
mra-1b->			11	1	0	5	0	0	LAN
mra-1b->	-mra-1	MRA	11	1	0	5	0	0	WAN
l-mra-1c			5	0	0	11	1	0	LAN
mpe-2a->			5	0	0	11	1	0	LAN
l-mpe-2b	-mpe-2	MPE	11	1	0	5	0	0	LAN
mpe-2a->			5	0	0	10	1	0	WAN
l-mpe-3a			0	0	0	0	0	0	WAN
mpe-3b->	-mpe-3	MPE	5	0	0	10	1	0	LAN
l-mpe-3a			0	0	0	0	0	0	WAN
mpe-3b->			0	0	0	0	0	0	WAN
l-mpe-4a	-mpe-4	MPE	10	1	0	5	0	0	LAN
mpe-4a->			10	1	0	5	0	0	WAN

4.8.2 Dependency

Geo-Redundancy mode enabled running Release 11.5.

4.9 Policy Support for separating traffic on different VLANs)Platform PR 211237, Policy PR 222399)

MPE/MRA replication traffic and secondary high availability (HA) heartbeat traffic can be sent between Geo-Redundant sites on specific networks. MPE/MRA replication traffic can also be marked with Differentiated Services Control Point (DSCP).

These features impact the Firewall properties. Replication traffic requires TCP 17398 and TCP 17400. Primary or Secondary Heartbeat requires TCP 17401, UDP 17401 and TCP 17402.

4.9.1 Manager GUI Form

Platform Setting → Topology Setting → (MPE/MRA Cluster name) → Modify Cluster Setting → DSCP Marking

Cluster Settings	
Name	mpe-1
Appl Type	MPE
Site Preference	Normal

Topology Configuration	
DSCP Marking	CS1
Replication Stream Count	AF11
Replication & Heartbeat	AF12
Backup Heartbeat	AF21

The CMP GUI is used to configure the Replication & Heartbeat Traffic:

Platform Setting → Topology Setting → (MPE/MRA Cluster name) → Modify Cluster Setting → Replication&Heartbeat

Cluster Settings	
Name	mpe-1
Appl Type	MPE
Site Preference	Normal

Topology Configuration	
DSCP Marking	CS1
Replication Stream Count	1
Replication & Heartbeat	OAM
Backup Heartbeat	

The CMP GUI is used to configure the Backup Heartbeat Traffic:

Platform Setting → Topology Setting → (MPE/MRA Cluster name) → Modify Cluster Setting → Backup Heartbeat

Cluster Settings	
Name	mpe-1
Appl Type	MPE
Site Preference	Normal

Topology Configuration	
DSCP Marking	CS1
Replication Stream Count	1
Replication & Heartbeat	
Backup Heartbeat	SIG-A

4.9.2 Dependency

Geo-Redundancy mode enabled running Release 11.5.

4.10 MRA Aggregated Counts Displayed on the KPI Dashboard (PR 222746)

Two rows are added to the KPI Dashboard :

- MRAs Selected — Displays the aggregation count for user-selected MRA databases.
- MPEs Selected — Displays the aggregation counts for the MPE devices that belong to the user-selected MRA databases.

The following counts are aggregated for selected MRA databases and the associated MPE devices :

- TPS (no percentage)
- PDNs (no percentage)
- Active Subscribers (no percentage)
- Critical Alarm Count
- Major Alarm Count
- Minor Alarm Count
- Protocol Errors Sent
- Protocol Errors Received

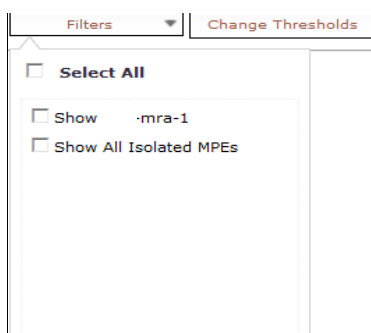
Note: Isolated MPE devices are not included in the aggregation counts.

4.10.1 Manager GUI Form

With this enhancement, CMP can show the aggregation of the KPI related counts for the user selected MRAs and the MPEs associated with these MRAs.

CMP GUI->SYSTEM WIDE REPORTS->KPI Dashboard->Select Filter to view the aggregated counts

Filters available to view the aggregated counts:



The screenshot shows a web interface for the CMP GUI. At the top, there is a 'Filters' dropdown menu and a 'Change Thresholds' button. Below these, there is a section with three checkboxes: 'Select All', 'Show -mra-1', and 'Show All Isolated MPEs'. The 'Select All' checkbox is currently selected.

MRA Aggregated Counts are displayed in the first two rows:

- The first row is named 'MRAs Selected', it shows the aggregation count of all MRAs.
- The second row is named 'MPEs Selected', it shows the aggregation count for the associated MPEs which belong to the selected MRA.

09/30/13 10:50 AM | [Home](#) | [Logout](#)

KPI Dashboard | [Status: Normal](#) | [Last Refresh: 09/30/2013 10:04:37](#)

[Filter](#) | [Change Thresholds](#)

- [Rating Profile](#)
- [Charging Servers](#)
- [Time Periods](#)
- [Serving Gateway \(MCG\) MNC](#)
- [Custom APP Definitions](#)
- [Global Configuration Settings](#)

POLICY MANAGEMENT

- [Policy Library](#)
- [Template Library](#)
- [Policy Table Library](#)
- [Policy Import / Export](#)
- [Policy Checkpoint / Restore](#)

NETWORK

MRA

SYSTEM WIDE REPORTS

- [KPI Dashboard](#)
- [Trending Reports](#)
- [Alarms](#)
- [Active Alarms](#)
- [Alarm History Report](#)
- [Sessions](#)
- [AF Session Report](#)
- [PDR Connection Report](#)
- [PDR AFN Buffs Report](#)
- [Others](#)
- [Connection Status](#)
- [Protocol Errors](#)
- [Policy Statistics Report](#)

PLATFORM SETTING

UPGRADE MANAGER

	Performance				Alarms			Protocol Errors	
	TPS	PDR	Active Subscribers	Critical	Major	Minor	Sent	Received	
MRA selected	0	0	0	0	0	0	45570	0	
MPEs selected	0	0	0	0	0	1	127961	0	

wall-warp-1		Performance				Connections			Alarms			Protocol Errors		
MRA	State	TPS	PDR	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
stra-1(Server-A)	Standby	0 (0%)	0 (0%)	0 (0%)	1	7	1 of 1	0 of 0	0 of 0	0	0	0	45570	0
stra-2(Server-B)	Active	0 (0%)	0 (0%)	0 (0%)	1	7	1 of 1	0 of 0	0 of 0	0	0	0	45570	0
stra-3(Server-C)	Standby	0 (0%)	0 (0%)	0 (0%)	1	7	1 of 1	0 of 0	0 of 0	0	0	0	45570	0

MPE	State	TPS	PDR	Active Subscribers	CPU %	Memory %	MRA	Data Sources	Critical	Major	Minor	Sent	Received
mpa-1(Server-A)	Active	0 (0%)	0 (0%)	0 (0%)	1	8	1 of 1	1 of 1	0	0	0	127961	0
mpa-2(Server-B)	Standby	0 (0%)	0 (0%)	0 (0%)	1	7	1 of 1	1 of 1	0	0	0	127961	0
mpa-3(Server-C)	Standby	0 (0%)	0 (0%)	0 (0%)	1	7	1 of 1	1 of 1	0	0	0	127961	0

4.10.2 Dependency

None.

4.11 Split AF Session by RAT Type (PR 223393)

Application function (AF) sessions can be tracked by RAT type. A new statistics object is added to the MPE device to track the sessions. The sessions can be viewed on a new AF session report.

4.11.1 Manager GUI Form

This feature in CMP GUI displays MRA stats as an aggregation of the associated MPEs for each RAT type.

CMP GUI->SYSTEM WIDE REPORTS->Sessions->Select AF Session Report

AF Session Report displays MRA stats as an aggregation of the associated MPEs:

The first row displays the total count of RAT types such as WLAN,EUTRAN,HRPD.

Tekelec AF Real Time Connection Count (Stats Reset: Manual / Last Refresh: 10/02/2013 15:11:01)

Display results per page: 50
[First/Prev] [Next/Last] Total 3 pages

Associated MRA	Server Name	Server Type	WLAN - Current	WLAN - Max	EUTRAN - Current	EUTRAN - Max	HSPD - Current	HSPD - Max
TOTAL	TOTAL	TOTAL	0	0	1	1	0	0
mra-1	mra-1	MRA	0	0	1	1	0	0
mpe-1	mpe-1	MPE	0	0	1	1	0	0
mpe-2	mpe-2	MPE	0	0	0	0	0	0

4.11.2 Dependency

None

4.12 Enhancement to avoid oscillations in system response during overload in Gen8 configuration (PR 223504)

MPE and MRA processing improved to reduce large shifts in the rate of responses when the overall system (MRA and associated MPEs) is overloaded:

- When only one MPE is busy but the overall system (MRA + MPEs) are not overloaded, subscriber attachments are not rejected.
- When multiple MPEs are busy, this enhancement results in a portion of the attachments being rejected when the overall system is overloaded.

Communication of the busy status between MPE and MRA by advertising changes to the busy status using the DRMA LNR request:

The busy status is conveyed in a new AVP called Busy-Status within the LNR request.

The Busy-Status AVP (AVP code 3108) is a vendor specific AVP (Vendor-Id=21274(Camiant)) of type Unsigned32. It indicates whether a node is busy or not. A value of 0 means the node is not busy. A value strictly higher than 0 means the node is busy. The default value for this AVP is 0. When present in a DRMA LNR request, the provided value updates the last received value for the node identified in the Origin-Host of the LNR. A node compliant with this document shall include the Busy-Status AVP in every LNR request.

Below are the AVP's flags:

Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not	May Encr.
Busy-Status	3108	Unsigned32	V	P		M	Y

Updated DRMA LNR's ABNF(Augmented Backus-Naur Form):

<LNR> ::= < Diameter Header: 996, REQ >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

{Load-Factor}

[Busy-Status]

*[Supported-Features]

* [AVP]

4.13 Enhancement to PCRF load shedding to take into account Rx traffic (PR 223505)

The load shedding infrastructure is enhanced to include all Diameter applications and the request types when performing admission control on the corresponding requests.

A new load shedding interface is added to the CMP GUI. This interface is used to configure load shedding criteria, including the settings for entering busyness and the action to take when messages arrive after the busyness level has been reached. Up to 3 levels of busyness (from Level 1 as the least busy to Level 3 as the most busy) for an MPE device can be configured. The current busy level of a system is added to the KPI statistics.

4.13.1 Manager GUI Form

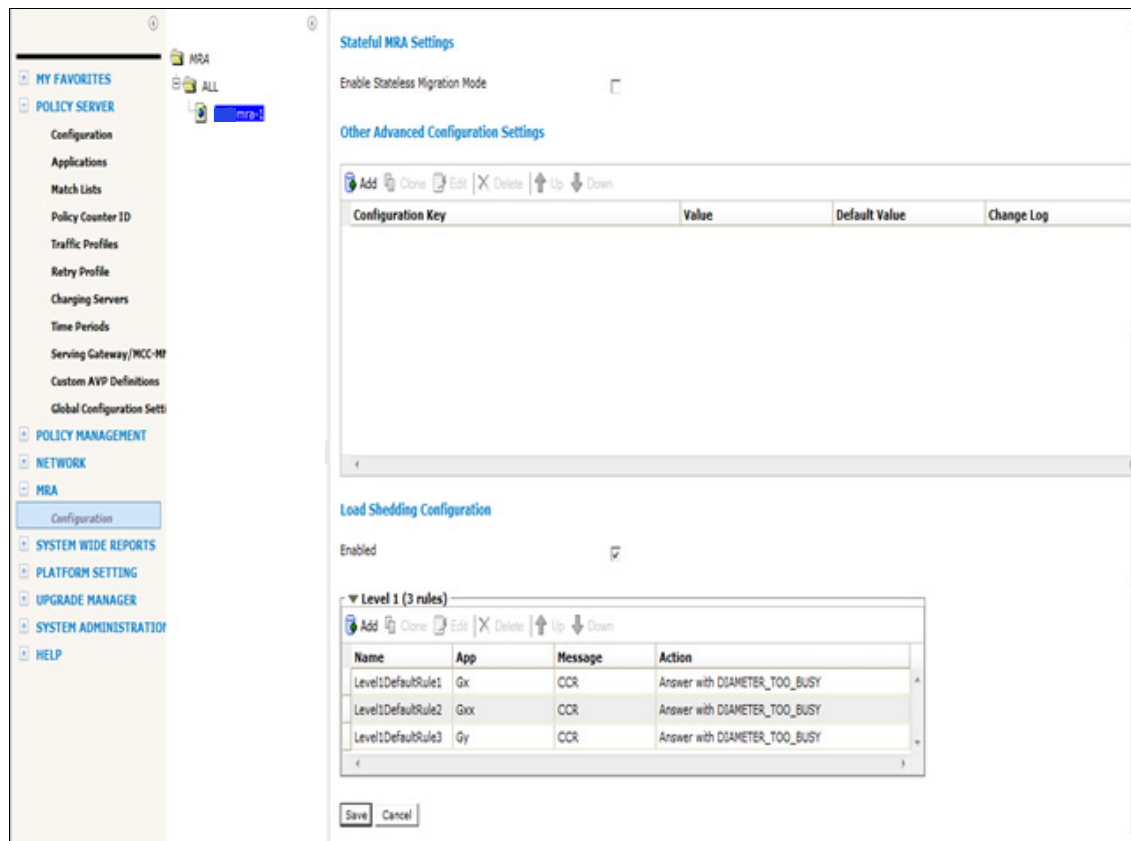
When the user opens the Advanced Configuration view of MPE or MRA, the Load Shedding section displays a collapsed view of the levels including a total count of the rules/actions in each level.

MRA Load Shedding Configuration:

In the left most pane navigate to MRA >>> Configuration.

In the middle pane navigate to any MRA.

In the right most pane select the MRA tab and click Advanced to view the Load Shedding Configuration with collapsed view of levels and default rules/actions.

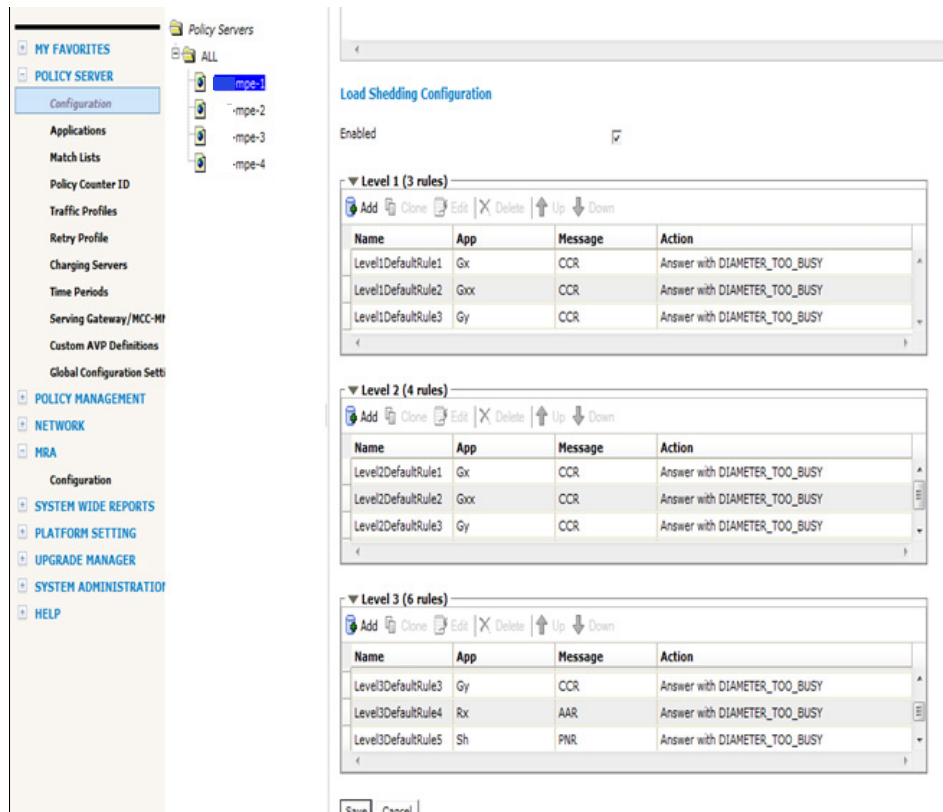


MPE Load Shedding Configuration:

In the left most pane navigate to Policy Server >>> Configuration.

In the middle pane navigate to Policy Servers >>> any MPE.

In the right most pane select the Policy Server tab and select Advanced to view the Load Shedding Configuration with collapsed view of levels and default rules/actions.



4.13.2 Dependency

None.

4.14 Enhancement to MRA to MPE load Balancing TPS and Session based (PR 223519)

Load balancing enhancements are added to the MPE device and the MRA database.

For the MPE device:

- The CPU is included when calculating the current load factor.
- The MPE device publishes the load factor to the MRA database when the load factor changes by .05 or more. The load factor is published at least once per minute but not more frequently than once per second.

For the MRA database:

- The MRA database uses the load factor published by the MPE device when calculating the MPE selection distribution. The load factor is rounded down to the closest hundredth decimal place, allowing for a more even distribution of the load.
- The selection frequency formula is enhanced to reduce the selection frequency of a loaded MPE device while ensuring that the MPE device is never starved of new selections as long as it has not become busy.

4.14.1 Resource Manager

New MPE KPI Stat- CurrentLoadFactor, viewed in Resource Manager:

MPEs current load factor is stored in 'CurrentLoadFactor' KPI Stat and it is a 2 decimal number between 0 and 1. This KPI Stat assists debugging and is not be exposed in CMP GUI KPI dashboard.

On the MPE, start /opt/camiant/rc/bin/rcmgr and view 'CurrentLoadFactor' KPI Stat using 'show counters kpi'.

```
[root@mpe-1a bin]# ./rcmgr
RcMgr> show counters kpi
KPI Stats:

CurrentLoadFactor:                0.00
```

Load factor publishing frequency updated with two config parameters, viewed in Resource Manager:

The combination of the two parameters ensures the MRA is kept up to date as to the MPEs' load and is performing optimal load distribution.

The update to the default change percentage for sending load updates is handled by this advanced configuration:

Name	Description	Type	Old Default	New Default
RCDRMA.Load.PercentChange	Used to determine when the MPE should notify the MRA about changes in current load via an LNR message. If the current load has passed the Notify Threshold, but not yet passed the Clear Threshold, notifications are sent to the MRA about changes in load whenever the load has changed by a percent equal to this value.	int	10	5

The maximum time between load factor updates is handled by this advanced configuration:

Name	Description	Type	Default
RCDRMA.Load.MaxNotifyInterval	The maximum amount of time (in milliseconds) allowed between load factor updates to the MRA. If a load update has not been sent for any reason for more time than this value, a load update are sent regardless of whether or not the value changed.	int	60000

On the MPE, start /opt/camiant/rc/bin/rcmgr and view Config Parameter defaults in Resource Manager –

> 'show cfg RCDRMA.Load.PercentChange -v'

```
RcMgr> show cfg RCDRMA.Load.PercentChange -v
RCDRMA.Load.PercentChange
  Description:    Used to determine when the MPE should notify the MRA about
                  changes in current load via an LNR message. If the current
                  load has passed the NotifyThreshold, but not yet passed the
                  ClearThreshold, notifications will be sent to the MRA about
                  changes in load whenever the load has changed by a percent
                  greater than or equal to this value.
  Default Value: 5
```

> 'show cfg RCDRMA.Load.MaxNotifyInterval -v'

```
RcMgr> show cfg RCDRMA.Load.MaxNotifyInterval -v
RCDRMA.Load.MaxNotifyInterval
  Description:    TThe maximum amount of time (in milliseconds) allowed
                  between load factor updates to the MRA. If a load update has
                  not been sent for any reason for more time than this value,
                  a load update will be sent regardless of whether or not the
                  value changed.
  Default Value: 60000
```

4.14.2 *Dependency*

None

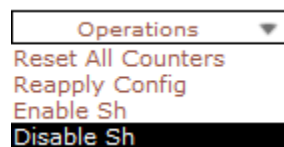
4.15 CMP Bulk Operations (PR 228704)

A single command entry can be provisioned on the CMP system and applied to all of the MPE devices or MRA databases in a specified group.

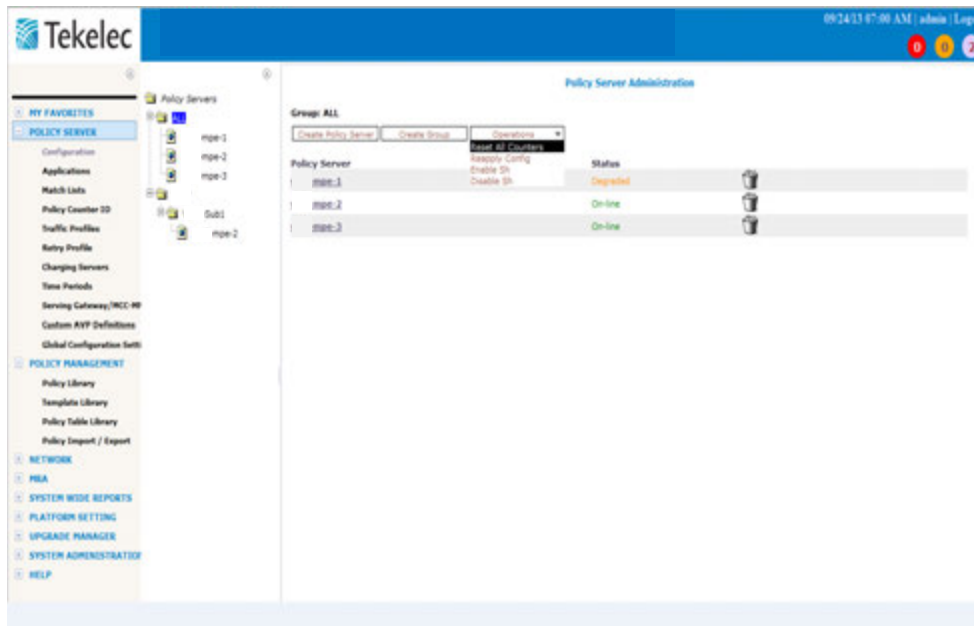
4.15.1 *Manager GUI Form*

To address the need to run one operation across multiple MPE or MRA instances under a specified group, a drop down Operations menu is provided :

Bulk Operations menu:



CMP GUI->Policy Server->Configuration->Policy Servers->Select a group eg. ALL or a sub-group:



The following bulk operations can be applied to all MPE devices in a group :

- Reapply Config
- Reset Counters (when Stats Reset Configuration is set to Interval as CMP GUI-> Policy Server->Global Configuration Settings->Stats Settings-> Stats Reset Configuration=Interval)
- Reset All Counters (when Stats Reset Configuration is set to Manual as CMP GUI-> Policy Server->Global Configuration Settings->Stats Settings-> Stats Reset Configuration=Manual)
- Enable/Disable Sh interface

The following bulk operations can be applied to all MRA databases in a group :

- Reapply Config
- Reset Counters (when Stats Reset Configuration is set to Interval as CMP GUI-> Policy Server->Global Configuration Settings->Stats Settings-> Stats Reset Configuration=Interval)
- Reset All Counters (when Stats Reset Configuration is set to Manual as CMP GUI-> Policy Server->Global Configuration Settings->Stats Settings-> Stats Reset Configuration=Manual)

4.15.2 Dependency

CMP bulk operations functionality is supported only once the entire PCRF system (all CMPs, MPEs and MRAs) is upgraded to PCRF Release 11.5.

5 Features-specific Changes

This Chapter introduces the new features and features' changes that we received in Policy release 11.5, as compared with Policy release 10.5.x.

5.1 Subscriber Activity Log (PR 218508)

Description:

This feature aimed at providing a detailed record of subscriber activity in the system. This will provided insight into the system at a fine grained level that will be useful for both support purposes and for customers interested in subscriber specific tracking. Subscriber activity will include diameter protocol level messaging, user profile retrieval, and policy engine execution. Together this information allows a user to monitor a particular subscriber request(s) through the entire system.

This feature has an automatic override to disable functionality when the system moves into a state of distress. The Subscriber Activity logging feature will register as a listener and receive notifications that the state of the system has changed.

CMP UI changes:

The Subscriber Activity configuration screen layout will be updated to include the following changes:

- 1) The screen will be divided into sections separating different groups of configuration elements for Global Configuration, Log Backup and Subscribers.
- 2) The Backup task configuration will be included on a separate page.
- 3) Under configuration, checkboxes will provide a way to enable/disable log types for inclusion in Subscriber Activities.
- 4) A checkbox will be added to include the MRA in subscriber tracing checks.
- 5) The Subscriber identifier list will be modified to be consistent with other tables in the UI.
- 6) The Target Exporting Folder will be changed to be a non-editable field.

Subscriber Activity Log

Configuration Log Backup

Modify Activity Log History

Configuration

Trace Enable:	true	Activity Type
Include MRA:	false	Protocol: true
Severity:	NOTIFY	Policy: true

Subscriber Identifier List

Identifier Type	Identifier Value	Enable	Realtime Log
IMSI	630002610000001	true	View
IMSI	310410000000016	true	View
IMSI	310410000000017	true	View

Configuration Log Backup

Modify

Configuration

Enabled Subscriber Activity log Backup	true
First Running Time	07/16/2014 11:33
Run Interval(hours)	1
Max Keep Days	1
Folder Max Size(MB)	30
Backup Destination Folder	/var/camiant/subtracing

The Subscriber Activity configuration Modify screen will be updated to include the following changes:

- 1) In the Subscribers section, Add, Edit, Clone and Delete buttons will be added to the table to provide the same functionality as was previously in a separate section of the screen.

Subscriber Activity Log

Configuration Log Backup

Configuration

Trace Enable: ☒ Activity Type

Include MRA: ☐ Protocol: ☒

Severity: NOTIFY Policy: ☒

Subscriber Identifier List

Add Clone Edit Delete

Identifier Type	Identifier Value	Enable
IMSI	630002610000001	true
IMSI	310410000000016	true
IMSI	310410000000017	true

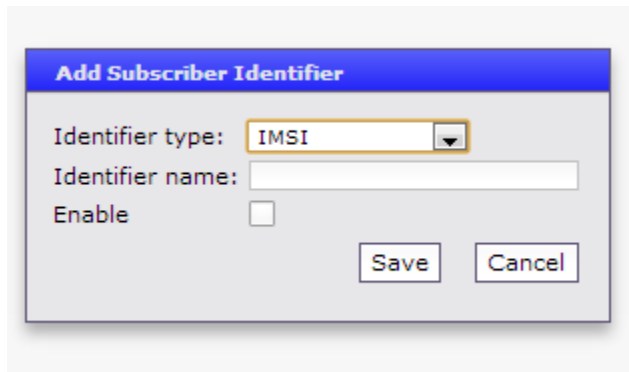
Subscriber Activity Log

Configuration Log Backup

Configuration

Enabled Subscriber Activity log Backup	<input checked="" type="checkbox"/>
First Running Time	07/16/2014 11:33
Run Interval(hours)	1
Max Keep Days	1
Folder Max Size(MB)	30
Backup Destination Folder	/var/camiant/subtracing

Save Cancel



5.2 Extend Quota pool to at least 20 (PR 232934)

Description:

MPE documents the current support for number of subscribers in a pool to a maximum of 10 due to performance considerations. This feature enhancement documents the performance impact of increasing the number of subscribers in a pool to 20. No code changes were performed. The performance impact is a result of notifications being sent for all subscribers in a pool, whenever the pool information is modified. If notifications are enabled for pool profile, pool quota, pool state and pool dynamic quota, each MPE will receive notifications for each subscriber in that pool that is currently connected.

CMP UI changes:

No CMP UI changes have been carried out for this feature.

5.3 Support pro-rating on a per quota basis (PR 235626)

Description:

The Oracle Communications Policy Management supports the proration, but when the proration configuration is used, the proration is applied to all Monthly quota existing for a subscriber, not just new quota plan configured for the given month. Thus, in a scenario where a subscriber has a base quota plan and purchases another monthly plan at, say, 15th of the month and if proration is activated, the base offer that is associated with the subscriber will be prorated as well and the new plan. This is because the proration parameter is not quota specific, but a subscriber specific and is applied to all quota plans even previously existing once.

This feature gives Oracle Communications Policy Management the capability to configure and support separate proration dates for several (up to 30) monthly plans for each subscriber. Thus, when a new plan is added for a subscriber, the proration date entered for a plan would apply only for the new plan and not to all the plans associated with the subscriber.

CMP UI changes:

This feature adds a new configuration field to a plan, called the “Billing Date Effective Name” (This field already exists on a global level on the Policy Server tab). By adding this field to a plan, each individual quota can now be associated with a different configured pro-ration date. This field will work the same as before, by pointing to a custom field in the subscriber’s profile. The value for this field in the subscriber’s profile will expect a date and time to be entered in the format “YYYY-MM-DDThh:mm:ss” for local times, or in the format “YYYY-MM-DDThh:mm:ssZ” to specify the time zone. This new field will apply to both subscriber and pool quota plans.

The screenshot shows the 'New Plan Configuration' form in the 'Plan Administration' section. The form is divided into several sections: 'Name', 'Description / Location', 'Quota Profile Type', 'Max Leakage Threshold (MB)', 'Enable Dynamic Grant', 'Max Sessions Used For Dynamic Grant', 'Minimum Grant Size', 'Reset Frequency', 'Reset Time Variable', 'Report Offset Limit (minutes)', 'Billing Date Effective Name' (highlighted with a yellow box and 'New Field' label), 'Initial Total Volume Limit (bytes)', 'Initial Upstream Volume Limit (bytes)', 'Initial Downstream Volume Limit (bytes)', 'Initial Time Limit (seconds)', and 'Quota Convention'. The 'Billing Date Effective Name' field is set to 'Custom1'. The form also has 'Save' and 'Cancel' buttons.

Dependencies

This feature requires SPR support for Camiant.UserData blob.

5.4 Option to trigger RAR on quota change by provisioning interface (PR 232936)

Description:

When the PCRF subscribes for notifications on SPR interface, PNR message can be received for changes of the subscriber data, subscriber state, or quota data. In the ex-11.5 release of the product, only PNRs received due to change to the provisioned subscriber data (user profile, pool, and dynamic quota (this include Passes, rollovers and top-ups)) would trigger execution of the policy engine and re-authorization. The PNR message received due to quota data change or subscriber state change would result in the update of the subscriber records, but would not trigger execution of the policy engine (and so no re-authorization). This means that policy engine would not re-evaluate subscriber state or quota status until PCRF receives another message or event that results in the policy engine evaluation.

The Policy Solution needs to be enhanced to support policy engine evaluation triggered by PNR received due to the following causes: provisioned subscriber data, subscriber state, subscriber quota data, Pooled quota, pool state, and dynamic Pooled quota. Based on the PNR trigger the policy engine could control sending RAR message through appropriate policies. The policy engine evaluations triggered by PNR are not desirable in all customer scenarios as there could be a significant performance impact associated with this. As a result, the triggering of policy engine evaluations should be configurable for each notification event

type, i.e. subscriber data, subscriber state, subscriber quota data, Pooled quota, pool state, and dynamic Pooled quota.

These changes will be made for notifications from Sh, It will be extended later for another datasource (for example, Sy datasource sends notifications which always generates reauths).

Sy notifications (SNRs) in ex-11.5 releases generate RARs when received. This notification will also pass through the policy engine before deciding to send RARs.

Name	Description	Default value	Configurable through Manager	Configurable through rcmgr
SH.Notifications.ReauthViaPolicy	Reauth processing for notifications via policy conditions and actions. By default only provisioning related notifications generate reauth.	False	Yes	Yes
SY.Notifications.ReauthViaPolicy	Reauth processing for notifications via policy conditions and actions. By default only provisioning related notifications generate reauth.	False	Yes	Yes

Configuration Settings for the MPE

CMP UI changes:

DS display window:

Policy Server Administration

System Server: mpe137

System Reports Logs Policy Server Diameter Routing Policies **Data Sources**

Modify Data Sources

Admin State	Name	Role	Type	Primary Host	Secondary Host
Enabled	hss26-155	Primary	Sh	hss26-155.ims.blueslice.c	
Enabled	shservervm137	Primary	Sh	shservervm137.camiant.c	
Disabled	ldap252-30	Primary	LDAP	10.15.252.30	
Disabled	hss26-154	Primary	Sh	hss26-154.ims.blueslice.c	
Disabled	hss244-199	Primary	Sh	hss244-199.ims.blueslice.c	
Disabled	hss251-32	Primary	Sh	hss251-32.ims.blueslice.c	

General Settings

☐ Merge Search Results
☐ Subscription Enabled Via Policy Only
☒ **Notification re-auth via Policy**
☐ Combine Lookup And Subscription

DS modification display:

Policy Server Administration

Policy Server: mpe137

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

Modify Data Sources

Add Clone Edit Delete Up Down					
Admin State	Name	Role	Type	Primary Host	Secondary Host
Enabled	hss26-154	Primary	Sh	hss26-154.ims.blueslice.com	
Disabled	hss26-155	Primary	Sh	hss26-155.ims.blueslice.com	
Disabled	shservervm137	Primary	Sh	shservervm137.camiar	
Disabled	ldap252-30	Primary	LDAP	10.15.252.30	
Disabled	hss244-199	Primary	Sh	hss244-199.ims.blueslice.com	
Disabled	hss251-32	Primary	Sh	hss251-32.ims.blueslice.com	

General Settings

Merge Search Results ☐

Subscription Enabled Via Policy Only ☐

Sh Settings

Combine Lookup And Subscription ☐

Notification re-authorization via policy ☐

Sy Settings

Notification re-authorization via policy ☐

Save Cancel

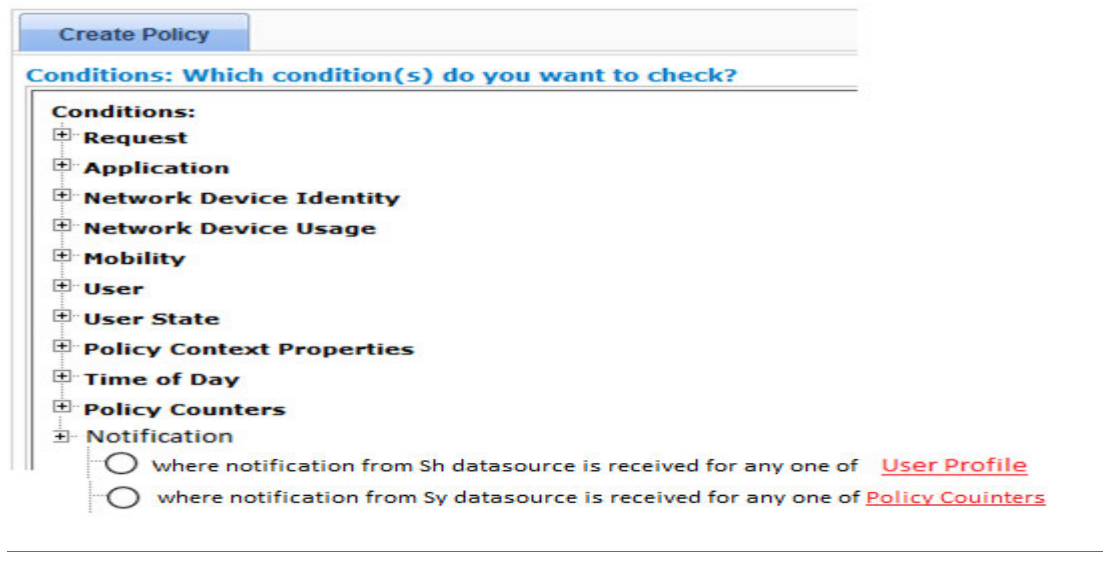
Policy Changes:

Create Policy

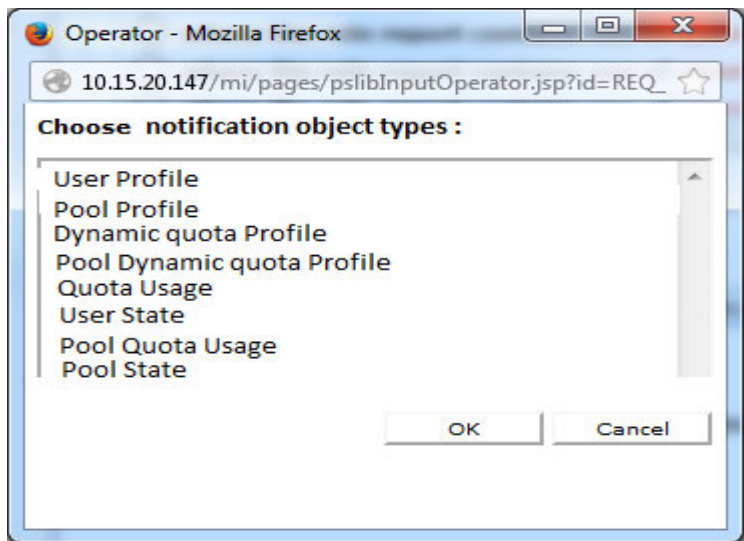
Conditions: Which condition(s) do you want to check?

Conditions:

- ☐ Request
- ☐ Application
- ☐ Network Device Identity
- ☐ Network Device Usage
- ☐ Mobility
- ☐ User
- ☐ User State
- ☐ Policy Context Properties
- ☐ Time of Day
- ☐ Policy Counters
- ☐ Notification
 - ☐ where notification from Sh datasource is received for User Profile



The options available for multi-select for the Sh notification condition are listed in following screenshot. Multi-selection of these options results in OR operation on the notification types. AND operation of notification types currently is not applicable, because the SPR does not send combined PNRs. However, the MPE will support AND operation if the policy condition for each type is written under the policy AND tree.



Notification object types in the CMP

Dependencies

None.

5.5 Dynamic quota for pools (PR 218524)

Description:

This feature includes the support of Passes, Top-ups and Rollovers for Pooled Quotas. The SPR currently supports this for Pools, so no change in SPR is identified. The MPE supports all these for Subscriber Quotas. This is enhanced to include pool quotas as well. This will be disabled by default and a configuration / Manager UI setting will allow this to be enabled. This will also include an enhancement to the Sh data messages in terms of adding a service-indication. The following areas are identified to incorporate changes:

- MPE to SPR Sh interface. No Sh Profiles will be added, only Sh Profile ProfileV4 will support this feature.
- CMP UI for configuring and controlling this feature.
- MPE configuration settings
- Diamcli test support.

Name	Description	Default value	Configurable through Manager	Configurable through rcmgr
DB.DynQuota.PoolDynQuotaEnable	Indicates whether or not to support pool dynamic quota. This is a global configuration for the MPE	False	Yes	Yes
DB.SubscribePoolDynamicQuota	Indicates whether MPE subscribes for Pool dynamic quota. If pool dynamic quota is enabled, then subscription is enabled by default.	True	No	Yes

Configuration settings

Name	Description	Default value	Configurable through Manager	Configurable through rcmgr
SH.QuotaUsage.PoolDynamicQuotaEnabled	Indicates per datasource, if pool dynamic quota is enabled. SH<n> for each datasource.	True	No	Yes

Configuration settings per Sh DS

CMP UI changes:

The global configuration settings at the CMP will allow the user to enable/disable support for pool dynamic quota data. This is disabled by default to maintain backward compatibility and to reduce objects that the MPE needs to lookup by default. This will have to be enabled before the feature can be supported at the MPE.

Global Configuration Settings

- Precedence Range
- UE-Initiated Procedures
- Stats Settings
- Quota Settings**
- eMPS ARP Settings
- PDN APN Suffixes

Modify

Quota Settings

Pooled Quota

Enable subscriber pools	true
Enable pooled quota usage tracking	true
Enable pooled entity state	true
Enable pool dynamic quota	true
Enable Pass Expiration Extension	true

Global Configuration Settings

Quota Profiles

- Plans
 - PoolQuota1
 - PoolTimeQuota
 - Quota1
 - Quota2
 - Rollovertest1
 - SubsQuota1
 - TimeQuota1
 - plan1
 - qprg11
 - quotaProfile_dailyVol
 - quotaProfile_weeklyTim
 - topupplan
- Passes
 - ALL
 - Passtest1**
 - dayPass
 - pass-2
 - pass1
 - Gp1
 - Gp2

Pass Administration

Pass: Passtest1

Modify Delete

Configuration

Name	Passtest1
Description / Location	
Quota Profile Type	Pool
Active Time Period	<None>
Priority	0
Initial Total Volume Limit (bytes)	2000000
Initial Upstream Volume Limit (bytes)	None
Initial Downstream Volume Limit (bytes)	None
Initial Time Limit (seconds)	None
Initial Service Specific Limit (events)	None
Interim Reporting Interval (seconds)	None
Duration	0 Hours
Group	<None>
Expiration Date Extension Method	Name
Quota Exhaustion Action	N/A

New fields for Passes

DIAMETER Sh Protocol support dynamic quota

There will be a new service indication added for exchanging data between the MPE and SPR. Pool dynamic quota service indication is available only with Sh datasource when Sh Profile ProfileV4 being selected. The global configuration for pool dynamic quota should be enabled manually before Pool dynamic quota lookup is performed.

Service Indication	Data type	Description	Existing or New
CamiantUserData	Subscriber	User profile information	Existing
CamiantQuotaData	Subscriber	Quota usage information	Existing
CamiantStateData	Subscriber	State data	Existing
CamiantDyanmicQuotaData	Subscriber	Passes,top-ups and roll-over	Existing
CamiantPoolData	Pool	Pool profile information	Existing
CamiantPoolQuotaData	Pool	Pool Quota usage information	Existing
CamiantPoolStateData	Pool	Pool State data	Existing
<i>CamiantPoolDynamicQuotaData</i>	<i>Pool</i>	<i>Passes,top-ups and roll-over</i>	<i>NEW</i>

Sh Service Indications

Dependencies:

None.

5.6 Support Dynamic Granting algorithm for Passes (PR 234669)

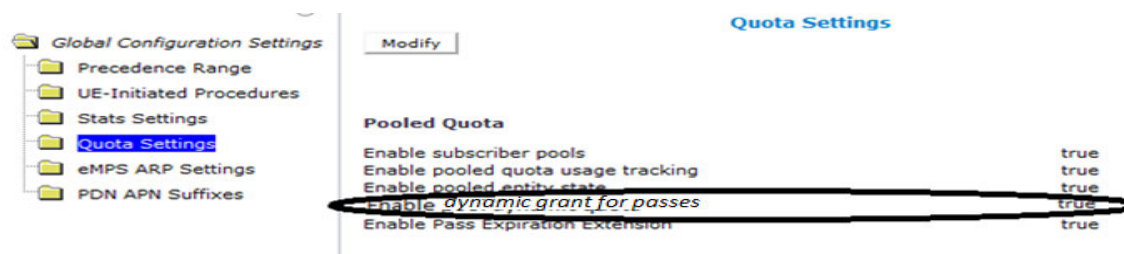
Description:

The Dynamic Granting behavior has previously worked only for Subscriber Plans, but now has been extended to be available for Passes also (for either Subscriber or Pools). Dynamic granting can be enabled when it is desired that the subscriber does not exceed the maximum quota allowed when multiple sessions for the subscriber connect across multiple MPEs. The dynamic grant takes into account what has already been granted to user sessions.

Name	Description	Default value	Configurable through Manager	Configurable through rcmgr
Quota.Passes.AllowDynamic Grant	Enable dynamic granting algorithm for passes.	False	Yes	Yes

Global Configuration Settings for the MPE

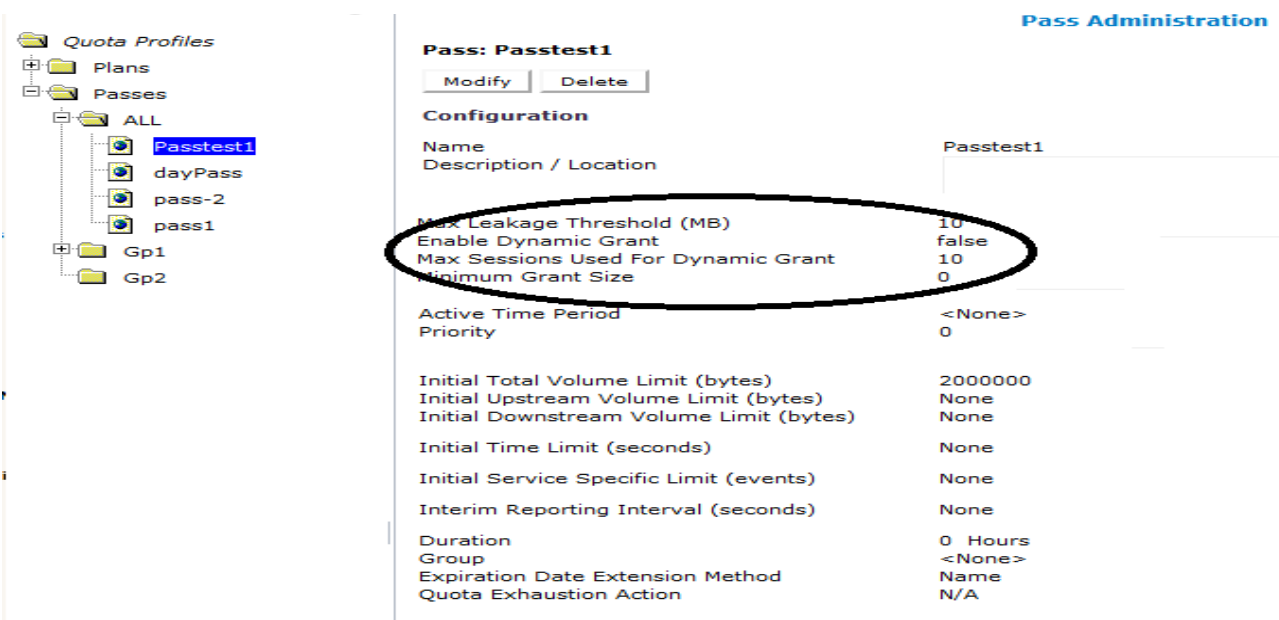
CMP UI changes:



Global Configuration view from CMP GUI

Name	Description	Default Value
Maximum Leakage MB	Maximum amount by which usage can exceed	0
Max active sessions	Number of sessions expected from a subscriber/member of a pool to be used in dynamic grant calculations	20
Use Dynamic Grant	Specifies whether to track grant dynamically for subscriber. This will cause the granted values to be updated by the MPE to the SPR.	False
Maximum sessions used for dynamic grant	Number of simultaneous sessions used in the dynamic grant algorithm for granting quota.	10

Fields added to a Pass Profile for dynamic grant



CMP GUI excerpt showing new fields added to a Pass Profile for dynamic grant

The decision to do the dynamic quota grant is defined in a pass profile, similar to a quota profile:

The granted value for the subscriber = Minimum of ((Max quota leakage – (Known usage + Already granted usage) / Max expected active pooled sessions), (Quota limit – Known usage))

Dependencies:

None.

5.7 Charging Correlation (PR 236692, 234002)

Description:

The Policy release 11.5 support charging correlation exchange procedures on Gx and Rx interface per 3GPP TS 29.214 v11.11.0 section 4.4.6.5 Access Network Charging Information Notification:

“If the AF has subscribed to a notification about Access Network Charging Information, the PCRF shall provide the Access Network Charging Information in the response, if already known by the PCRF. If not available, the PCRF shall provide the Access Network Charging Information by sending a Re-Authorization-Request (RAR) command when the Access Network Charging Information is received from the PCEF. If different Access Network Charging Information is applicable to the IP-CAN session, the PCRF shall notify the AF about the Access Network Charging Information that applies to each authorized flow. The RAR shall include the Specific-Action AVP set to the value "CHARGING_CORRELATION_EXCHANGE" and shall include the assigned Access-Network-Charging-Identifier(s) and may include the Access-Network-Charging-Address AVP.”

MPE shall support *Specific-Action AVP* as **CHARGING_CORRELATION_EXCHANGE** in AAR to indicate that the AF requests the server to provide the access network charging identifier to the AF for each authorized flow, when the access network charging identifier becomes known at the PCRF.

If the AF has subscribed to a notification about Access Network Charging Information, the PCRF shall provide the Access Network Charging Information in the response (AAA) directly, if already known by the PCRF.

AVP Format:

Access-Network-Charging-Identifier ::= < AVP Header: 502 >
{ Access-Network-Charging-Identifier-Value}
*[Flows]

If the AF has subscribed to a notification about Access Network Charging Information, when the access network charging identifier becomes known from PCEF, the PCRF shall send RAR to reports the access network charging identifier to the AF. The RAR shall include the Specific-Action AVP set to the value **CHARGING_CORRELATION_EXCHANGE**, and the assigned Access-Network-Charging-Identifier(s), and may include the Access-Network-Charging-Address AVP if PCEF reports.

The MPE shall support CHARGING_CORRELATION_EXCHANGE in Event-Trigger AVP for the PCEF to provide the ANCID associated to dynamic PCC rules.

Policies enhancement

Rx reference point enhancement

Policy condition:

where the specific action is one of specified action(s)

We can use this policy condition to check Specific-Action for Rx session.
For example:

where the specific action is one of **CHARGING_CORRELATION_EXCHANGE,INDICATION_OF_LOSS_OF_BEARER**

Policy action:

Advanced: set values for QoS and Charging parameters to specified value
Support Diameter AF Specific Actions

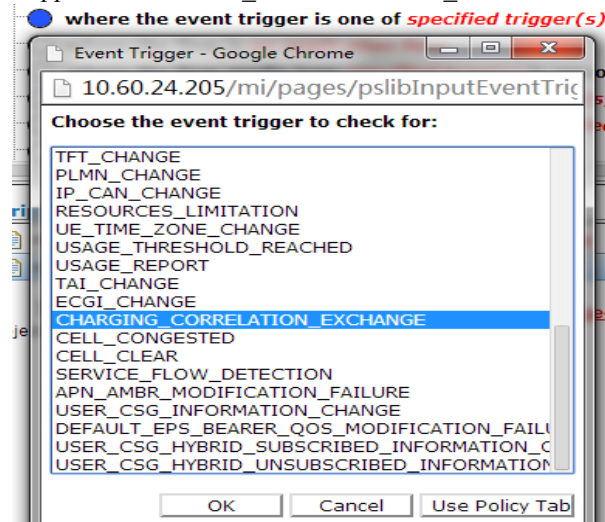
For example:

Advanced: set values for QoS and Charging parameters to
Diameter AF Specific Actions **CHARGING_CORRELATION_EXCHANGE,INDICATION_OF_RECOVERY_OF_BEARER**

Gx reference point enhancement

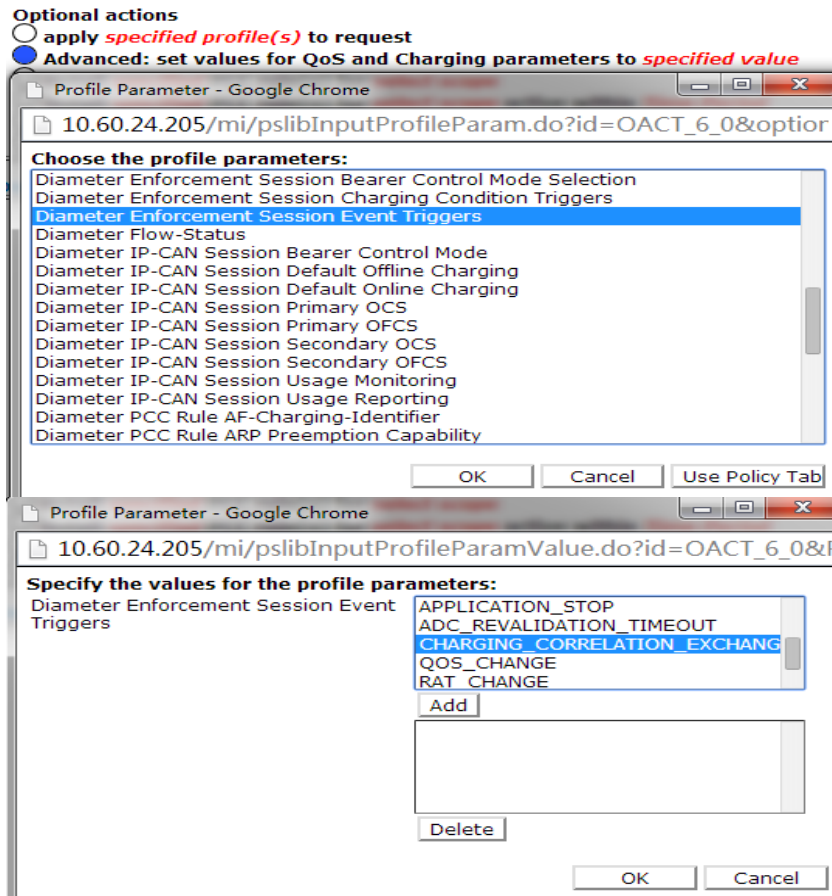
Policy condition:

where the event trigger is one of specified trigger(s)
Support CHARGING_CORRELATION_EXCHANGE



Policy action:

Advanced: set values for QoS and Charging parameters to specified value
Diameter Enforcement Session Event Triggers Support CHARGING_CORRELATION_EXCHANGE



Dependencies:

The offering of these features will depend on the functionality being available on AF. Validation of interoperability with AF vendor will be required.

5.8 Support for Network Location (PR236676, 235934)

Description:

An important capability required by VoLTE is the ability to provide a subscriber's location across the IP network. Oracle PCRF didn't support the 3GPP-standardized (*TS 29.212 V11.11.0*, *29.214 V11.11.0* and *29.213 V11.9.0*) procedure in previous Policy releases, but does in Policy release 11.5.

If the AF requests the PCRF to report the access network information (e.g. user location and/or user time zone information), the AF shall subscribe to the "ACCESS_NETWORK_INFO_REPORT" within the Specific-Action AVP and shall include the required access network information within the Required-Access-Info AVP.

The AF may also request the PCRF to report the access network information at Rx session termination. To do so, the AF shall include the required access network information within the Required-Access-Info AVP in the corresponding ST-Request.

When the PCRF receives a request to report the access network information from the AF, it shall **immediately** configure the PCEF or BBERF to provide such access network information. When the PCRF then receives the requested access network information from the PCEF/BBERF, the PCRF shall provide the corresponding access network information to the AF within the 3GPP-User-Location-Info AVP (if available), User-Location-Info-Time AVP (if available), 3GPP-SGSN-MCC-MNC AVP (if location info is not available) and/or 3GPP-MS-TimeZone AVP. If the information is requested as part of an AA-Request command, PCRF shall also provide the ACCESS_NETWORK_INFO_REPORT within Specific-Action AVP. If the PCRF receives the serving PLMN identifier from the PCEF/BBERF instead of the requested access network information, the PCRF shall provide the serving PLMN identifier within 3GPP-SGSN-MCCMNC AVP to the AF.

The PCRF shall not report any subsequently received access network information to the AF, unless the AF sends a new request for access network information.

Policy Support:

PCRF shall be able to use policy wizard to authorize and change the request from AF.

Policy Conditions:

- The operator shall be able to create policy conditions based on the value of the Specific-Action AVP field within the ACCESS_NETWORK_INFO_REPORT received across the Rx interface.

where the Specific-Action is one of **specified value(s)**

- The operator shall be able to create policy conditions based on the presence or absence of the Required-Access-Info AVP received across the Rx interface.

where the Required-Access-Info **matches one of value(s)**

- The operator shall be able to create policy conditions based on the value of the Required-Access-Info AVP field received across the Rx interface.

where the Required-Access-Info matches one of value(s)

- The operator shall be able to create policy conditions based on the presence or absence of the ACCESS_NETWORK_INFO_REPORT in the Event-Trigger AVP received across the Gx interface.

where the event trigger is one of **specified trigger(s)**

NOTE: it is an already existing condition.

Policy Actions:

- The operator shall be able to trigger sending the ACCESS_NETWORK_INFO_REPORT to the PCEF, with or without receiving any message across the Rx interface.

Advanced: set values for QoS and Charging parameters to specified value

And select “Diameter Enforcement Session Event Triggers”

Traffic Profiles for PCC rules and PCC profiles

Required-Access-Info shall be added to the traffic profile (PCC Profile and PCC Rule) as an option selection field. The value could be USER_LOCATION or/and MS_TIME_NONE.

If Required-Access-Info is not set, PCRF shall use the value(s) sent in AF requests, otherwise PCRF shall overwrite using the selected value(s).

Dependencies:

None.

5.9 Table Driven Policy with Multiple-Valued Data (PR 221127)

Description:

This new Policy 11.5 feature extends the functionality of table driven policies in the MPE to provide support for key matching with multi valued fields. Fields such as Entitlements can be retrieved as part of the subscriber profile with multiple values. The previous implementation of policy driven tables is unable to support flexible matching of these values. This feature will provide the configuration such that multiple values can be compared as a whole or subset to values provided in the defined policy table.

Matching Operations:

The available matching operations are shown below:

Matching Operation 1: Set Contains All Multiple Valued Context

A multiple valued policy context data set, CTX, is compared to a multiple value key column set, KC. If the intersection of CTX and KC equals KC: $KC \subseteq CTX$, in other words CTX is a subset of KC then this is a match. (The entire set of CTX must be included in KC).

Matching Operation 2: Set Contains All Multiple Valued Key Column

A multiple valued policy context data set, CTX, is compared to a multiple value key column set, KC. If the intersection of CTX and KC equals CTX: $CTX \subseteq KC$, in other words KC is a subset of CTX then this is a match. (The entire set of KC must be included in CTX)

Matching Operation 3: Set Contains Any Multiple Valued Context (intersect)

A multiple valued policy context data set, CTX, is compared to a multiple value key column set, KC. If the intersection of CTX and KC exists then this is a match.

Matching Operation 4: Set Equivalence

A multiple valued policy context data set, CTX, is compared to a multiple value key column set, KC. If the sets $CTX = KC$ then this is a match.

Matching Operation 5: Multiple Key Column Set Contains Single Valued Context

A SINGLE valued policy context data set, CTX, is compared to a multiple value key column set, KC. If CTX is a subset of KC then this is a match. (The CTX will be evaluated as a string and must be included in KC).

Matching Operation 6: Multiple Context Set Contains Single Valued Key Column

A multiple valued policy context data set, CTX, is compared to a SINGLE value key column set, KC. If KC is a subset of CTX then this is a match. (The KC will be evaluated as a string and must be included in CTX)

Matching Operation 7: Wildcard

A wildcard match is a set of delimited wildcards in the key column cell. The context, CTX, is then compared value by value to the wildcards specified in the KC. If there is any match between the two, that row will be considered matched.

Matching Operation 8: Matchlist

This is the same type of match as the wildcard, intersect, however this match can only be initiated by a matchlist.

CMP UI Changes:

The screenshot displays the Oracle Communications Policy Manager (CMP) web interface. The top header features the Oracle logo and the title "Oracle Communications Policy Manager". On the left, a navigation menu lists various configuration areas, with "POLICY MANAGEMENT" expanded to show "Policy Table Library" selected. The main content area is titled "Policy Table:" and contains a form for configuring a policy table. The "Name" field is populated with "test123". Below the form are buttons for "Add Row", "Add Column", and "Operations". A modal dialog titled "Policy Table Column" is open, showing fields for "Column Name" (test321), "Column Type", "Key" (checkbox), "Delimiter" (checkbox), and "Matching Operation". The dialog includes "Save" and "Cancel" buttons.

Policy Table Column Configuration

Select Matching Operation and selecting delimiter

The Policy Table Column creation panel is shown in **Error! Reference source not found.**. This is used when defining a Table Driven Policy and creating a column. **Error! Reference source not found.** includes all types of matches; the same figure also adds a delimiter section to place an ascii character, and adds a check box to enable or disable it for the specific column. In the case that either the policy context or key column does not contain that delimiter, then they will be compared as a single item.

Dependencies:

This feature is an extension of the Table Driven Policy feature introduced in Release 8.0

5.10 Allow any AVP in the dictionary to be inserted in a message (PR 234026)

Description:

This new Policy 11.5 feature promotes interoperability with a P-GW feature, which requires 3GPP-Charging-Characteristics (a Gy AVP) to be included in Gx CCA messages from the PCRF; the AVP is defined in the DIAMETER dictionary, but it is not part of Gx protocol standard. By allowing the AVPs defined in the DIAMETER dictionary to be used by 3rd Party AVP feature conditions and actions, will allow the PCRF to implement these kinds of scenarios.

CMP UI Changes:

Following is an example, in which a Base AVP is inserted in a nonstandard application message (Charging-Characteristics-3GPP in Gx message

```
<avp name="Charging-Characteristics-3GPP" code="13" mandatory="must" may-encrypt="yes" vendor="must"
vendor-id="10415" min-length="4" max-length="4">
  <type type-name="utf8String" />
</avp>
```

AVP Name	Charging-Characteristics-3GPP
Description	
AVP Code	13
Vendor Id	10415
Protect Flag	<input type="checkbox"/>
May Encrypt Flag	<input checked="" type="checkbox"/>
Vendor Specific Flag	<input checked="" type="checkbox"/>
AVP Type	Utf8String
Parent AVP	QoS-Information

Dependencies:

None

5.11 Sponsored Data Connectivity (PR 234958)

Description:

The sponsored data connectivity has been introduced as a capability in 3GPP Release 10. It allows for subscriber's application traffic to be sponsored by application service provider. The sponsor would have to establish a business agreement with the service provider and reimburses for user's specific application usage.

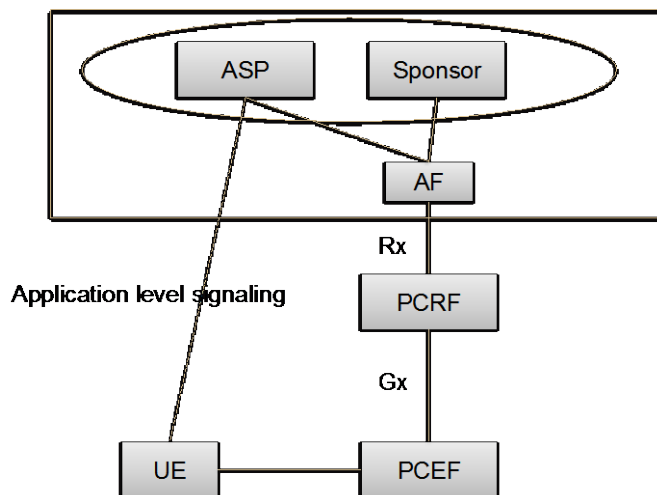
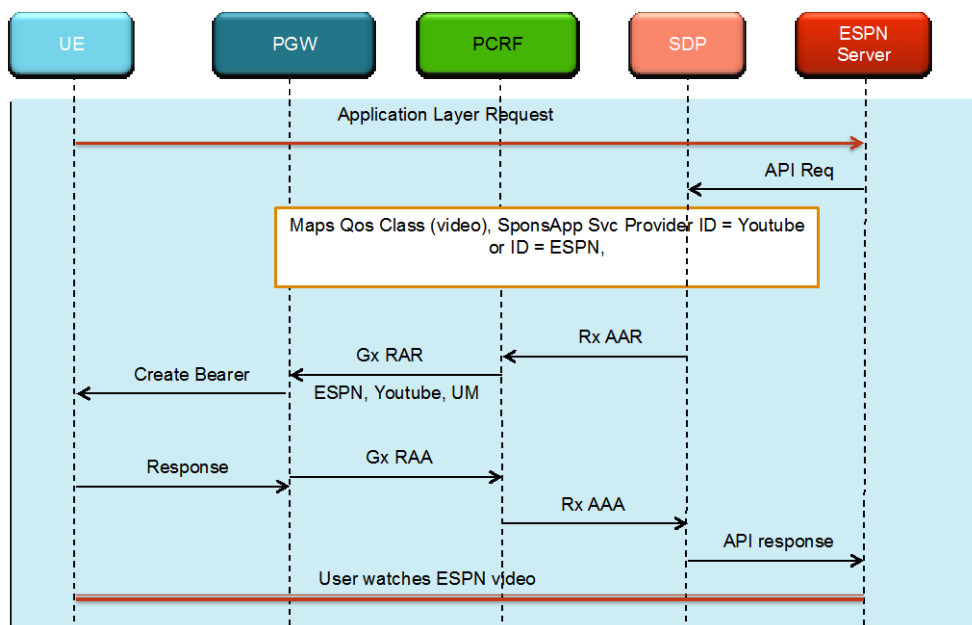


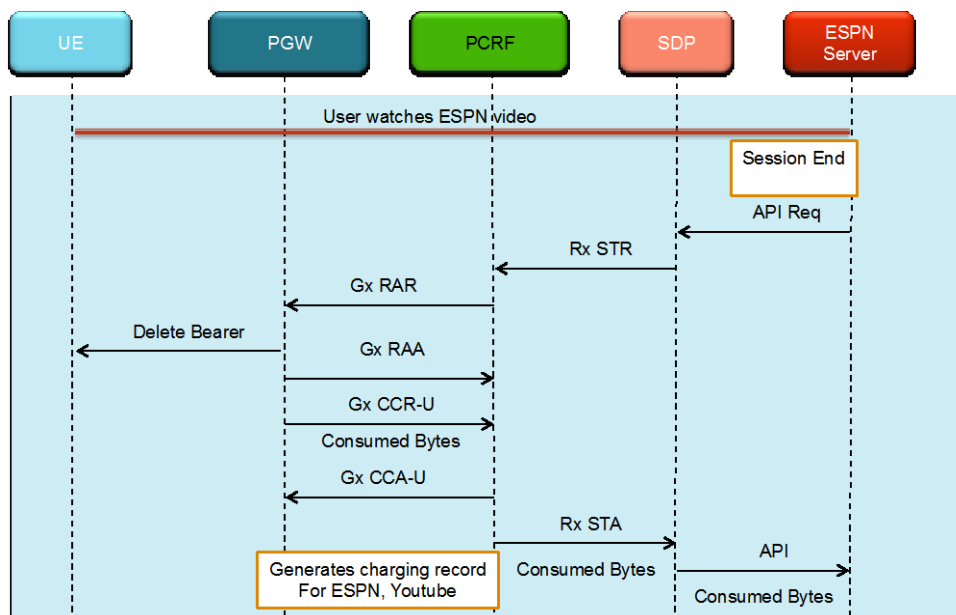
Figure 1: Sponsored Data connectivity interfaces

The sponsored data connectivity defines standard method for AF to provide usage threshold information and request usage report for sponsored data used by the subscriber. As a result, PCRF has to allocate usage monitoring keys, grant PCEF usage quota and deliver to AF usage report received by PCEF when the threshold is reached or the session is terminated.

The PCRF accomplishes this by installing PCC Rules on the Gateway that would track usage and provide a report when the usage threshold has been reached or when a session has been terminated. As a result, a service provider is able to offer “sponsored” value-added application services to subscribers using a standard based mechanism that allows to associate data flows with a particular sponsor and limit that sponsored data usage.



Sponsored Data Connectivity - Call setup



Sponsored Data Connectivity - Teardown call flow

The following actors are involved in a scenario of sponsored connectivity:

Sponsor: the one willing to take the operator's charge for connectivity.

Application Service provider: the one providing the sponsored service. May coincide with the sponsor.

Operator: the one providing connectivity. May also be service provider.

End user: the one using the sponsored service. Is a subscriber at the operator.

Policy Enhancement

Below are new policies conditions defined that can evaluate the Sponsor Identity and Provider Identity in Sponsored-Identity and Application-Services-Provider-Identity AVPs.

*where the Sponsored-Identity matches one of **specified Sponsored id(s)***

For example:

Where the Sponsored-Identity matches one of **ESPN, NBA**

*where the Application-Services-Provider-Identity matches one of **specified application services provider id(s)***

For example:

Where the Application-Services-Provider-Identity matches one of **Youtube, Facebook**

The new types of Sponsor Identity and Provider Identity are supported when choosing the field to check for in the following match-list based policy conditions:

*where the **select type** is contained in Match List(s) **select list(s)***

*where the **select type** is not contained in Match List(s) **select list(s)***

Here **select type** is a name of specified AVP that you can select from a dropped list. **select list(s)** is a string list that you can configure it from CMP UI(POLICY SERVER → Mach lists)

For example:

Where the **Sponsor Identity** is contained in Match List(s) **sponsor lists**

Where the **Application Services Provider Identity** is not contained in Match List(s) **provider lists**

The new mandatory policy action for reject message with experimental result code is defined as follows:

*reject message with Experimental-Result-Code **number** and Vendor-ID **number***

For example:

reject message with Experimental-Result-Code **5067** and Vendor-ID **10415**

Traffic profile enhancement

The policy traffic profiles, PCC Profile and PCC Rule, have been updated to include sponsored connectivity configuration including Sponsored Identity and Application Service Provider Identity. The Reporting Level has been updated to include the value SPONSORED_CONNECTIVITY_LEVEL. The traffic profile in CMP is depicted as follows:

The screenshot displays the 'Traffic Profiles' configuration window. On the left, a sidebar shows 'Traffic Profiles' and a folder icon labeled 'ALL'. The main area contains a list of configuration fields. The 'Reporting Level' dropdown is highlighted with a red box, and its expanded menu shows 'SPONSORED_CONNECTIVITY_LEVEL' selected. The 'Sponsor Identity' and 'Application Service Provider Identity' fields are also highlighted with a red box. Other fields include 'Downlink Max Authorized Rate (bps)', 'Uplink Min Guaranteed Rate (bps)', 'Downlink Min Guaranteed Rate (bps)', 'ARP Priority Level', 'ARP Preemption Capability', 'ARP Preemption Vulnerability', 'Service Identifier', 'Rating Group', 'Monitoring Key', 'Online Charging', 'Offline Charging', 'Metering Method', 'Flow Status', 'Flow Description(s)', 'Use Flow Information(s)', 'Precedence', 'Resource Allocation Notification', 'TDF Application Identifier', 'TDF Redirect Support', 'TDF Redirect Address Type', 'TDF Redirect Server Address', and 'Save' and 'Cancel' buttons at the bottom.

Field	Value
Downlink Max Authorized Rate (bps)	
Uplink Min Guaranteed Rate (bps)	
Downlink Min Guaranteed Rate (bps)	
ARP Priority Level	
ARP Preemption Capability	N/A
ARP Preemption Vulnerability	N/A
Service Identifier	
Rating Group	
Monitoring Key	N/A
Reporting Level	SPONSORED_CONNECTIVITY_LEVEL
Online Charging	N/A
Offline Charging	
Metering Method	N/A
Flow Status	N/A
Flow Description(s)	
Use Flow Information(s)	
Precedence	
Resource Allocation Notification	N/A
TDF Application Identifier	
TDF Redirect Support	N/A
TDF Redirect Address Type	N/A
TDF Redirect Server Address	
Sponsor Identity	
Application Service Provider Identity	

Statistics Enhancement

The Diameter AF statistics have been enhanced by including the following additional counters:

- Current number of active sponsored sessions
- Max sponsored active sessions
- Current number of active sponsors
- Max number of sponsors
- Current number of active service providers
- Max number of service providers

Current number of active sponsored sessions	0
Max sponsored active sessions	0
Current number of active sponsors	0
Max number of sponsors	0
Current number of active service providers	0
Max number of service providers	0
<hr/>	
Current Sponsored Sessions	0
Max Sponsored Sessions	0
Current Number of Service Providers	0
Max Number of Service Providers	0
Current Number of Sponsors	0
Max Number of Sponsors	0
Max Sponsored Session	0
Current Number of Service Providers	0
Max Number of Service Providers	0
Current Number of Sponsors	0
Max Number of Sponsors	0

Dependencies:

The offering of this feature will depend on the functionality being available on AF and PCEF. Validation of interoperability with AF and PCEF vendors will be required.

5.12 PS to CS Handover Feature For VoLTE (PR 234003)

Description:

In this new Policy 11.5 feature, when the IP-CAN bearer is terminated by PS to CS handover, the PCEF reports related PCC rule for this IP-CAN bearer by including the Rule-Failure-Code AVP set to the value PS_TO_CS_HANDOVER and Rule-Status set to inactive within the Charging-Rule-Report AVP as part of the IP-CAN session modification procedure. And then the PCRF shall inform the AF by sending an RAR command with the Abort-Cause AVP set to the value PS_TO_CS_HANDOVER if not all the service data flows within the AF session are affected or sending an ASR command with the Abort-Cause AVP set to PS_TO_CS_HANDOVER if all the service data flows within the AF session are affected.

New stats of handover on Rx counters

This feature extends the current statistics to provide some new counters of Rx messages in handover scenario. There could be new counters introduced as followings:

- Initial/update AAA successful/failed response to AAR on peer/pcrf level

- Handover triggered ASR number on peer/pcrf level
- The number of ASR sent/timeout messages triggered by PS_TO_CS_HANDOVER within Diameter AF Adaptor and peer stats (ASRHOSendCount / ASRHOTimeoutCount)
- The number of RAR sent/timeout messages triggered by PS_TO_CS_HANDOVER within Diameter AF Adaptor and peer stats (RARHOSendCount / RARHOTimeoutCount)

It needs to display the four new counters on GUI of diameter AF adaptor page & AF Peer page both on MPE & MRA.

It needs to provide ossi query interface to get the four new counters on each of MPE & AF peer Diameter AF adapter page on MPE.

Diameter AF adapter page on MRA

ASR messages received / sent	0 / 0
ASR messages timeout	0
ASR HO messages received / sent	0 / 0
ASR HO timeout	0
ASA success messages received / sent	0 / 0
ASA failure messages received / sent	0 / 0
RAR messages received / sent	0 / 0
RAR messages timeout	0
RAR HO messages received / sent	0 / 0
RAR HO messages Timeout	0
RAA success messages received / sent	0 / 0
RAA failure messages received / sent	0 / 0

Diameter AF peer page on MPE

ASR messages received / sent	0 / 0
ASR messages timeout	0
ASR HO messages received / sent	0 / 0
ASR HO timeout	0
ASA success messages received / sent	0 / 0
ASA failure messages received / sent	0 / 0
RAR messages received / sent	0 / 0
RAR messages timeout	0
RAR HO messages received / sent	0 / 0
RAR HO messages Timeout	0
RAA success messages received / sent	0 / 0
RAA failure messages received / sent	0 / 0

Diameter AF peer page on MRA

ASR messages received / sent	0 / 0
ASR messages timeout	0
ASR HO messages received / sent	0 / 0
ASR HO timeout	0
ASA success messages received / sent	0 / 0
ASA failure messages received / sent	0 / 0
RAR messages received / sent	0 / 0
RAR messages timeout	0
RAR HO messages received / sent	0 / 0
RAR HO messages Timeout	0
RAA success messages received / sent	0 / 0
RAA failure messages received / sent	0 / 0

OSSI request sample of Diameter AF

```
<?xml version="1.0" encoding="UTF-8" ?>
<XmlInterfaceRequest>
  <QueryOmStats DeltaCount="true">
    <StartTime>2014-09-01T16:25:00</StartTime>
    <EndTime>2014-09-01T16:30:00</EndTime>
    <DiameterAfStats></DiameterAfStats>
  </QueryOmStats>
```

OSSI response sample of Diameter AF

```
<Statistics>
  <DiameterAfStats>
    <Sample>
      ...
      <ASRHoSendCount>0</ASRHoSendCount>
      <ASRHoReceivedCount>0</ASRHoReceivedCount>
      <ASRHoTimeoutCount>0</ASRHoTimeoutCount>
      <RARHoSendCount>0</RARHoSendCount>
      <RARHoReceivedCount>0</RARHoReceivedCount>
      <RARHoTimeoutCount>0</RARHoTimeoutCount>
      ...
    </Sample>
  </DiameterAfStats>
</Statistics>
```

OSSI request sample of DiameterAfPeerStats:

```
<?xml version="1.0" encoding="UTF-8" ?>
<XmlInterfaceRequest>
  <QueryOmStats DeltaCount="true">
    <StartTime>2014-09-01T16:25:00</StartTime>
    <EndTime>2014-09-01T16:30:00</EndTime>
    <DiameterAfPeerStats></DiameterAfPeerStats>
  </QueryOmStats>
</XmlInterfaceRequest>
```

OSSI response sample of DiameterAfPeerStats:

```
<Statistics>
  <DiameterAfPeerStats>
    <Sample>
      ...
      <ASRHoSendCount>1</ASRHoSendCount>
      <ASRHoReceivedCount>0</ASRHoReceivedCount>
      <ASRHoTimeoutCount>1</ASRHoTimeoutCount>
      <RARHoSendCount>0</RARHoSendCount>
      <RARHoReceivedCount>0</RARHoReceivedCount>
      <RARHoTimeoutCount>0</RARHoTimeoutCount>
      ...
    </Sample>
  </DiameterAfPeerStats>
</Statistics>
```

OSSI request sample of DiameterMraAfStats:

```
<XmlInterfaceRequest>
  <QueryOmStats DeltaCount="true">
    <StartTime>2014-09-01T16:25:00</StartTime>
    <EndTime>2014-09-01T16:30:00</EndTime>
    <DiameterMraAfStats></DiameterMraAfStats>
  </QueryOmStats>
</XmlInterfaceRequest>
```

OSSI response sample of DiameterMraAfStats:

```
<Statistics>
  <DiameterMraAfStats>
    <Sample>
      ...
      <ASRHoSendCount>0</ASRHoSendCount>
      <ASRHoReceivedCount>0</ASRHoReceivedCount>
      <ASRHoTimeoutCount>0</ASRHoTimeoutCount>
      <RARHoSendCount>0</RARHoSendCount>
      <RARHoReceivedCount>0</RARHoReceivedCount>
      <RARHoTimeoutCount>0</RARHoTimeoutCount>
      ...
    </Sample>
  </DiameterMraAfStats>
</Statistics>
```

OSSI request sample of DiameterMraAfPeerStats:

```
<?xml version="1.0" encoding="UTF-8" ?>
<XmlInterfaceRequest>
  <QueryOmStats DeltaCount="true">
    <StartTime>2014-09-01T16:25:00</StartTime>
    <EndTime>2014-09-01T16:30:00</EndTime>
    <DiameterMraAfPeerStats></DiameterMraAfPeerStats>
  </QueryOmStats>
</XmlInterfaceRequest>
```

OSSI response sample of DiameterMraAfPeerStats:

```
<Statistics>
  <DiameterMraAfPeerStats>
    <Sample>
      ...
      <ASRHoSendCount>0</ASRHoSendCount>
      <ASRHoReceivedCount>0</ASRHoReceivedCount>
```

```
<ASRHoTimeoutCount>0</ASRHoTimeoutCount>
<RARHoSendCount>0</RARHoSendCount>
<RARHoReceivedCount>0</RARHoReceivedCount>
<RARHoTimeoutCount>0</RARHoTimeoutCount>
...
</Sample>
</DiameterMraAfPeerStats>
</Statistics>
```

Dependencies:

None.

5.13 Flow-Description AVP doesn't comply with 3GPP Release 9 (PR 232575)

Description:

This new Policy 11.5 feature realizes 3GPP TS 29.214 v9.15.0 and 3GPP TS 29.212 v9.16.0.

3GPP TS 29.214 v9.15.0 section 5.3.8:

The Flow-Description AVP (AVP code 507) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:

- Direction (in or out). The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.
- Source and destination IP address (possibly masked).
- Protocol.

3GPP TS 29.212 v9.16.0 section 5.4:

Attribute Name	Reference	Description	Acc. type	Applicability (notes 1, 4)
----------------	-----------	-------------	-----------	-------------------------------

Attribute Name	Reference	Description	Acc. type	Applicability (notes 1, 4)
Flow-Description	3GPP TS 29.214 [10]	<p>Defines the service flow filter parameters for a PCC rule. The following rules apply to Gx:</p> <ul style="list-style-type: none"> - Only the Action "permit" shall be used. - The invert modifier "!" for addresses shall not be used. - Direction "out" shall be used. - The keyword "assigned" may be used. - Source and destination port values are optional and, if present, they shall be either single value, list or range. 	All	Both

As shown above, there are more restrictions when Flow-Description AVP re-used in Gx reference point. Especially, direction of Flow-Description AVP shall only be “out” in Gx release 9 or above, but it may be “in” or “out” in Gx release 8 or below. Our PCRF always allow “permit in ...” in Flow-Description AVP, so we need to switch “permit in” to “permit out” in Gx Flow if Gx release version is 9 or above. At the same time, we also need to swap source and destination address/port parameters.

The Flow-Description AVP often contained in Flow-Information AVP which is sent from PCRF to PCEF and contains the information from a single IP flow packet filter.

The Flow-Description, ToS-Traffic-Class, Security-Parameter-Index and Flow-Label AVPs specify the parameters to be used for matching payload packets. If any of these AVPs is present, then the Flow-Direction AVP shall also be included.

5.14 Correct Handling of Duplicate Gx Diameter Requests (PR 235168 & 235168)

Description:

With this new Policy 11.5 feature enabled, when a Gx diameter request times out (specifically in the case where the PCRF sends a response but the answer is not received or is received after the timer has expired), it is valid for gateway to retransmit a request with the same Origin-Host ID and end-to-end ID, and PCRF should identify such request and reply the previous response with updated hop-by-hop ID. In previous releases, PCRF simply drops the duplicate request and this behavior would result in a double timeout scenario at gateway side.

Dependencies:

None.

5.15 N-site MRA optimizations and enhancements (PR 229472)

Dependencies:

The scalability of the MRA in the previous architecture is limited to a four site system. The main limitation of the MRA scalability was due to the fact that each MRA has to query all the other MRAs in the system when it doesn't have a binding for a subscriber. As more MRAs are added, the number of queries increases, causing the effective throughput of each MRA to decrease.

The enhancements and optimizations attempt to minimize the number of queries amongst MRAs to determine which instance is handling a subscriber's binding. In addition, these changes ensure that the amount of work an individual MRA instance performs to manage subscribers' bindings does not increase as the number of MRAs in the system changes. This will allow a linear increase in the overall throughput of the system as MRAs are added.

MRA Changes:

In order to support the above described functionality, the following changes will be made on the MRA:

- (1) Support an algorithm to deterministically designate an M-MRA to hold the mapping between a Key and the B-MRA.
- (2) Support querying, updating, and deleting the mapping between a Key and a B-MRA.
- (3) Support for auditing of the mappings for stale mapping cleanup.

DIAMETER DBR message will also be extended with an AVP to indicate whether the query is for binding of mapping data. This is mainly needed for migration mode and for the mapping audit task. It only makes sense for the QUERY and QUERY_CREATE DBR types.

The updated ABNF is shown below with changes in *italic bold*:

```
DRA-Binding-Request (DBR) := < Diameter Header: 999, REQ, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    [ Destination-Host ]
    [ Binding-Request-Type ]
    *[ Key-Set ]
    [ Called-Station-Id ]
    *[ Subscription-Id ]
    *[ Supported-Features ]
    [ Framed-IP-Address ]
    [ Framed-IPv6-Prefix ]
    [ IP-CAN-Type ]
    [ PDN-Connection-ID-AVP ]
    [ User-Equipment-Info ]
    [ Server-Identity ]
    [ Queried-Session-Id ]
```

```

    [ Query-Type ]
    * [ Proxy-Info ]
    * [ Route-Record ]
    * [ AVP ]

```

```

<DBA> ::= < Diameter Header: 999 >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Auth-Application-ID }
    [ Result-Code ]
    [ Experimental-Result ]
    [ Server-Identity ]
    [ Binding-Create-Time ]
    * [ Supported-Features ]
    * [ Key-Destination ]
    * [ AVP ]

```

Configuration Changes:

There is one “advanced” configuration (DRADRMA.MultiSiteOptimization) added to the MRA to determine whether the MRA shall use the procedures and algorithm defined in this document when determining an M-MRA. Its default value is “Algov1” (algorithm version 1). In order to disable this new functionality, this config needs to be set to “Legacy”.

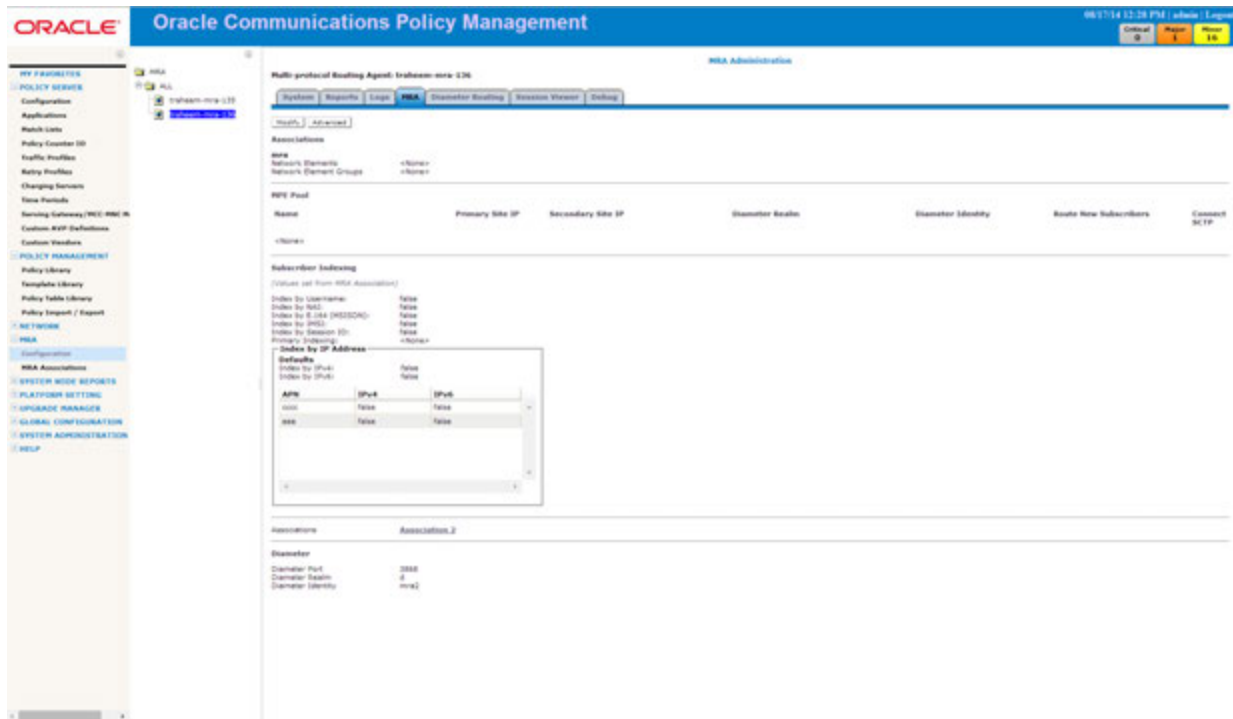
Name	Description	Type	Default	Exposed in CMP
DRADRMA.MultiSiteOptimization	Determines the algorithm used to distribute binding indexes across MRAs in a system. Possible values are: <ul style="list-style-type: none"> - Legacy - Algov1 (default) 	String	Algov1	Yes
DRADRMA.QueryPrimaryKeyOnSecondary	If enabled, the M-MRA will always query the secondary M-MRA for a primary key mapping if the primary M-MRA does not already have a mapping.	Bool	False	No
DRADRMA.Migrating	The CMP sets this cfg automatically when migration starts. It is cleared when the user accepts the migration. This cfg tells the MRA to continue to use the migration behavior described in the migration section.	Bool	False	No
DRADRMA.Sync.StartTime	This setting allows the mapping sync task to be scheduled at a	String	null	No

	certain time. The task will start running at this time and will run to completion. Once the task is done running, the cfg will be reset to null. The expected format is a Unix timestamp in milliseconds.			
DRADRMA.Sync.BundleFactor	The number of keys to bundle in a single DBR-SYNC message. The MRA will not send a DBR until there are at least this many keys ready to send to an MRA unless there are no more keys left to send. Note: This cfg also applies to the migration task.	Int	10	No
DRADRMA.Sync.MaxMappingsEachIterationPass	The maximum number of mappings to load into memory each iteration pass. This cfg is to ensure the MRA doesn't run out of memory by loading the entire contents of the mapping database into the java heap.	Int	100000	No
DRADRMA.Sync.Abort	Aborts the currently executing sync. Once the sync task has been aborted or if there was no sync task currently running, the cfg is reset to false.	Bool	false	No
DRADRMA.Sync.MaxDBRRate	The maximum rate (msgs/sec) at which DBR-SYNC messages are sent during the sync task. Note: This cfg also applies to the migration task.	int	5000	No
DRADRMA.Migration.StartTime	This setting allows the migration from legacy mode to be scheduled at a certain time. The task will start running at this time and run to completion. Once the task is done running, the cfg will be reset to null. The expected format is a Unix timestamp in milliseconds.	String	Null	No
DRADRMA.Migration.MaxBindingsEachIterationPass	The maximum number of bindings to load into memory each iteration pass. This cfg is to ensure the MRA doesn't run out of memory by loading the entire contents of the binding database into the java heap.	int	100000	No
DRADRMA.Migration.Abort	Aborts the currently executing legacy migration. Once the task has been aborted or if there was no task currently running, the cfg is reset to false.	bool	false	No
DIAMETERDRA.Cleanup.MappingValidityTime	The amount of time in seconds after which the mapping needs to be audited for staleness. Default value is 5 days	int	432000	No
DIAMETERDRA.Cleanup.MaxMapping	The maximum amount of time in	int	864000	No

gValidityTime	seconds after which the mapping is cleaned up on any error. Default value is 10 days.			
DIAMETERDRA.Cleanup.MaxMappingsEachIterationPass	The maximum number of mappings to load into memory each iteration pass. This cfg is to ensure the MRA doesn't run out of memory by loading the entire contents of the mapping database into the java heap.	Int	100000	No
DIAMETERDRA.Cleanup.CheckForStaleMappings	Check for stale mappings during the binding cleanup.	Bool	True	No
DIAMETERDRA.Cleanup.MaxMappingCleanupRate	The maximum rate (in mappings per second) mappings will be cleaned up.	Int	5000	No
DRADRMA.Rollback.StartTime	This setting allows the rollback to legacy mode to be scheduled at a certain time. The task will start running at this time and run to completion. Once the task is done running, the cfg will be reset to null. The expected format is a Unix timestamp in milliseconds.	Int	Null	No
DRADRMA.Rollback.MaxMappingRollbackRate	The rate (in bindings/sec) at which the rollback task will attempt to revert bindings from being migrated.	Int	5000	No
DRADRMA.Rollback.Abort	Aborts the currently executing rollback. Once the task has been aborted or if there was no task currently running, the cfg is reset to false.	bool	false	No

CMP Changes

The past releases' CMP screens for adding backup/associated MRAs are cumbersome and require repeating configuration on every single MRA configuration screen. This becomes even more unwieldy as the number of MRAs grows beyond four with this feature. Also the need to edit and save configuration on each MRA separately means the configuration change to the network is not done atomically and there is a large period of time where the configuration on each MRA is inconsistent. The main proposed change to the CMP for this feature is to remove the backup/associated MRA configuration from the MRA page and extract it into a separate top level page. The page will be located under the MRA heading and will be where all MRA Association configuration is done.



The above mockup shows where the new MRA Association configuration page will be located as a top level item. It also shows that the existing Backup/Associated MRA configuration has been removed from the MRA tab and replaced with a hyperlink to the Association which brings the user directly to the view screen for that specific Association. It also shows that the subscriber indexing values of the MRA were set on the MRA Association page.

DRMA statistics

There are new DRMA statistics that will be added to the MRA and MRA peer stats to capture the new DBR types. These are:

- DBR-Q received/sent
- DBR-Q timeouts
- DBA-Q success received/sent
- DBA-Q failure received/sent
- DBR-QC received/sent
- DBR-QC timeouts
- DBA-QC success received/sent
- DBA-QC failure received/sent
- DBR-U received/sent
- DBR-U timeouts
- DBA-U success received/sent
- DBA-U failure received/sent

- DBR-T received/sent
- DBR-T timeouts
- DBA-T success received/sent
- DBA-T failure received/sent
- DBR-S received/sent
- DBR-S timeouts
- DBA-S success received/sent
- DBA-S failure received/sent

There are also new statistics that will be added to the Diameter DRA Statistics screen. These are:

- Currently active mappings
- Max active mappings

Upgrade:

Upon upgrade to release 11.5, the CMP will inspect all the MRA in the system and then determine whether an MRA has a backup and or associated MRAs. If it happens that a given MRA has a backup and/or associated MRAs, the CMP will automatically create an association called “Generated Association {N}” and then include all the associated MRA as well as backups if any exists. {N} – Will start from the number 1.

Dependencies:

None.

5.16 Topology hiding in MRA for Rx application (PR 239238)

Description:

PCRF will hide the topology, and it should just provide the MRA hostname to the other function entities, and hide the detail of the topology.

And the following messages are taken affected:

AAR ASR STR RAR

AAA ASA STA RAA

New binding info added to AAR-I

When the topology hiding is enabled, AAR-U will contain a destination host “MRA.oracle.com”, and this information can’t be used to locate the message to MPE, so this message should be processed locally, and find binding information to locate MPE. AAR-U could only contain “SessionId”, so we should use this USERID to find the binding information.

Pending binding will be created and will be stored in 'PendingMap' when AAR-I has been received, then persist it into DB when the AAA with successful result comes.

When CCR-I comes in:

```
MraMgr> show dra binding -v
```

```
BindingId: 6010127069357277186
UserId: IMSI:450086020000136
UserId: IP:10.0.0.3
UserId: SESSID:pgw-p.tekelec.com;1399259761;20
PdnConnectionInfo: (DRAPdnConnectionInfo):
  APN: lte.ktfwing.com
  IP Address: 10.0.0.3
  ServerIdentity: null
  SessionInfo: (DRASessionInfo):
    SessionId: pgw-p.tekelec.com;1399259761;20
    AppId: 16777238
    Origin: pgw-p.tekelec.com
    OriginRealm: tekelec.com
    CreatedTimestamp: 1399342675172
    ValidityTimestamp: 1399342675172
  ServerIdentity: MPE-XIAMEN.oracle.com
  ModifiedTimestamp: 1399342675183
  CreatedTimestamp: 1399342675172
  IsBindingVisited: false
  IsSuspect: false
```

And then a Rx AAR with the IP "10.0.0.3" comes, and AAA with DIAMETER_SUCCESS returns.

```
MraMgr> show dra binding -v
```

```
BindingId: 6010127069357277186
UserId: IMSI:450086020000136
UserId: IP:10.0.0.3
UserId: SESSID:pgw-p.tekelec.com;1399259761;20
UserId: SESSID:af-p.tekelec.com;1399259800;18
PdnConnectionInfo: (DRAPdnConnectionInfo):
  APN: lte.ktfwing.com
  IP Address: 10.0.0.3
  ServerIdentity: null
  SessionInfo: (DRASessionInfo):
    SessionId: pgw-p.tekelec.com;1399259761;20
    Origin: pgw-p.tekelec.com
    OriginRealm: tekelec.com
    CreatedTimestamp: 1399342675172
    ValidityTimestamp: 1399342675172
SessionInfo: (DRASessionInfo):
SessionId: af-p.tekelec.com;1399259800;18
AppId: 16777236
Origin: af-p.tekelec.com
OriginRealm: tekelec.com
CreatedTimestamp: 1399342702756
ValidityTimestamp: 1399342702756
```

ServerIdentity: MPE-XIAMEN.oracle.com
ModifiedTimestamp: 1399342702790
CreatedTimestamp: 1399342675172
IsBindingVisited: false
IsSuspect: false

Dependencies:

None.