Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Policy Management Network Impact Report

Release 12.5

E94253-01

December 2018

Oracle Communication Policy Management Network Impact Report

Table of Contents

Figures

Tables

1. INTRODUCTION

1.1 Purpose and Scope

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

1.1 Disclaimers

This document summarizes Oracle Communication Policy Management Release 12.5 new and enhancement features as compared to previous release of 12.3.x/12.4.x and the operations impacts of these features, at a high level.

NOTE: Feature implementations may change slightly during product test.

1.2 Glossary

This section lists terms and acronyms specific to this document.

Table 1: Acronyms

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

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

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

2. OVERVIEW OF POLICY MANAGEMENT RELEASE 12.5 FEATURES

This section provides an overview list of the Policy Management Release 12.5 new features.

1.1 Policy Management release 12.5 New Features Support

Feature Number	Feature Name
26641840	S8HR Support
26557079	PLMN_CHANGE event trigger support for Rx (3GPP Rls 14)
27013746	PCRF picking up event triggers from last executed policy
27433899	9.102 LTE 5G Interworking Call Flows
27433979	9.114 PCRF Invocation for Option 3X (Presence Reporting Area AVP Support)
27175916	9.101 Maintain Session Uniqueness and avoid Stale MP
27177007	9.109 CSG Mobility Event Support
27176622	9.113 Network Services Header Support
27434131	Support for External-ID on Gx/Sh for MSISDN-less devices
27434084	eMPS Conference Call
27176660	9.110 Sy support for OCS initiated termination and invalid PC
25866138	Retry of PCRF-Originated Messages: Gx/Rx RAR
23214881	Match Multiple Table Rows Feature Request
27918667	Hotspot Event Trigger

2.1 Policy Management Hardware Requirements

2.1.1 Supported Hardware

The Policy Management Release 12.5 software can be deployed on the hardware that was previously supported under Release 12.3.x/12.4.x:

- Oracle NETRA Server X5-2.
- Oracle Server X5-2 on Rack Mount Server (RMS).
- Oracle hardware (including X6-2 and X7-2 servers) can be leveraged for virtualized deployments of release OCPM R12.5.
- Compatible with HP Gen-8 and Gen-9 Rack Mount Server (RMS) and C-class Servers
- HP 6120XG and HP 6125XLG enclosure switches.

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

2.2 Policy Management Software Changes

2.2.1 Software Components

Components	Releases
Policy Management	12.5.0.0.0_63.1.0
TPD 64 Bit	7.6.0
COMCOL	6.5
PM&C	6.6.0
TVoE	3.5.0
HP Firmware FUP	2.2.11 (Minimum) 2.2.12 (Current)
Oracle Firmware	3.1.5 (Minimum) 3.1.6 (Current)

2.2.2 UDR and SPR Product Compatibility

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

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

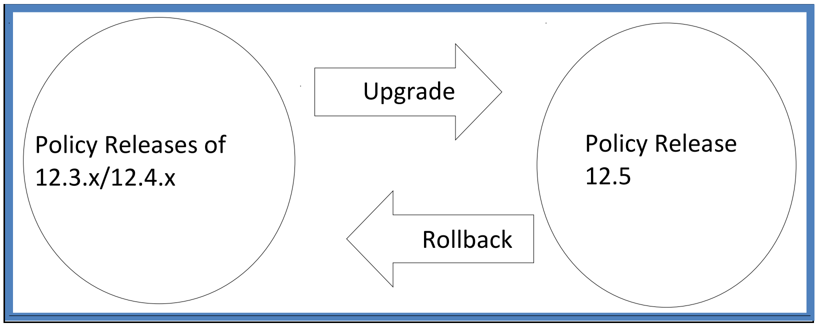
2.3 Policy Management Software Upgrade/Backout Overview

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

2.3.1 Supported Software Upgrade/Rollback (Backout) Paths for Release 12.5

Figure 1shows the supported upgrade Path for Release 12.5

Figure 1 Supportd Upgrade Path

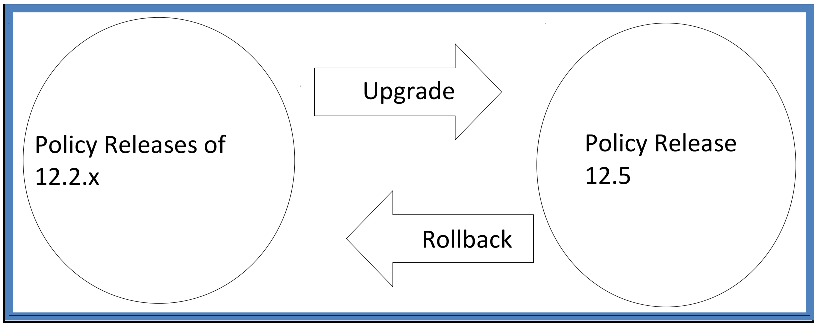


As with the past releases, both Georedundant and Non-georedundant Policy deployments have separate Policy software upgrade/rollback (backout) procedures.

The system must be on release 12.3.x or 12.4.x prior to upgrading to this release (12.5). This applies to wireless and fixed line.

Figure 2 shows the supported upgrade Path for Release 12.5

Figure 2 Upgrade Path for Cable Customer only



The system must be on release 12.2.x prior to upgrading to this release (12.5). This applies to cable.

2.3.2 Mixed Version Policy Management System Expectations

The system that is running Release 12.2.x(Cable)/12.3.x/12.4.x mixed configuration supports the performance and capacity of Release 12.2.x(Cable)/12.3.x/12.4.x respectively. The mixed version Policy Management configuration supports Release 12.2.x(Cable)/12.3.x/12.4.x features respectively.

In the mixed version Policy Management configuration, Release 12.5 CMP has these general limitations:

- New features must not be enabled until the upgrades of all servers managed by that CMP are completed. This also applies to using policy rules that include new conditions and actions introduced in the release.
- Policy rules should not be changed while running in a mixed version environment. If it is necessary to make changes to the policy rules while running in a mixed version environment, changes that do not utilize new conditions and actions for the release can be installed. However, these rules should be reviewed by you and Oracle before deployment to verify that the policies do not use new conditions or actions.
- The support for configuration of MPE and MRA servers is limited to parameters that are available in the previous version. Specifically:
  - Network Elements can be added.
  - Advanced Configuration settings that were valid for 12.2.x(Cable)/12.3.x/12.4.x may be changed.

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP from Release 12.2.x(Cable)/12.3.x/12.4.x to Release 12.5. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to Release 12.5.

Policy Management Components	CMP Release 12.5	MRA Release 12.5	MPE Release 12.5
CMP release 12.2.x(Cable)/12.3.x/12.4.x	No	No	No
MRA release 12.3.x/12.4.x	Yes	Yes	Yes
MPE release 12.3.x/12.4.x	Yes	Yes	N/A
MPE release 12.2.x (Cable)	Yes	N/A	N/A

2.3.3 Supported Software Releases Rollback (Backout) Support and Limitation

- After the entire Policy Management system is upgraded to Release 12.5, you may decide that a backout to the previous release is required. In that case, each individual server/cluster must be backed out.
- If it is necessary to backout multiple servers, it is required that the systems be rolled back in the reverse order in which they were upgraded. This implies that all the related component servers are rolled back first before the active CMP/NW-CMP and DR-CMP/NW-CMP can be rolled back to the previous version.
- After all the servers in the system are backed out to the previous release, the servers could be upgraded to another supported minor or major release for example, if all of the servers in the Policy Management system were backed out from Release 12.5 to Release 12.2.x(Cable)/12.3.x/12.4.x, these servers could subsequently be upgraded to Release 12.5-Build_A.
- Backout may be performed at any time after the upgrade, with these general limitations:
  - If a new features has been enabled, it must be disabled prior to any backout.
  - If there is an unexpected problem that requires backout after a feature has been enabled, it is possible that transient subscriber data, which is changed by the new feature, may be impacted by the unexpected problem. In this situation, those sessions cannot be guaranteed to be unaffected for any subsequent actions (this includes any activity after the feature is disabled). This may prevent data restoration by the SSDP feature during the backout. The impact of any unexpected problem must be analyzed when it occurs to determine the best path forward (or backward).

    NOTE: Although backout after feature activation is allowed, due to the number of possible permutations under which new features may be activated, the only testing that is performed is based on backout without new feature activation.
  - Backout can only be used to go back one release. This restriction applies to all types of releases including any major, minor, maintenance, or incremental release including minor releases of Release 12.5.

2.3.3.1 Rollback (Backout) Sequence

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

NOTE: See the related upgrade/rollback upgrade paths for more detail procedures. These procedures are not documented in this document. See the Policy management 12.5 documentation page.

Release 12.5 to Release 12.3.x/12.4.x (Wireless mode only)

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

Release 12.5 to Release 12.2.x (Cable mode only)

1. MPE clusters, including spare server if geo-redundancy is deployed.
2. Standalone Primary CMP clusters.

2.4 Migration of Policies and Supporting Policy Data

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

3. CHANGES BY FEATURE

3.1 S8HR Support (BUG 26641840)

3.1.1 Introduction

With this enhancement, AF can request the PCRF to provide EPC identities as part of the establishment of an IMS emergency session. This makes IMS emergency registration successful in S8HR scenario.

3.1.2 Feature Activation

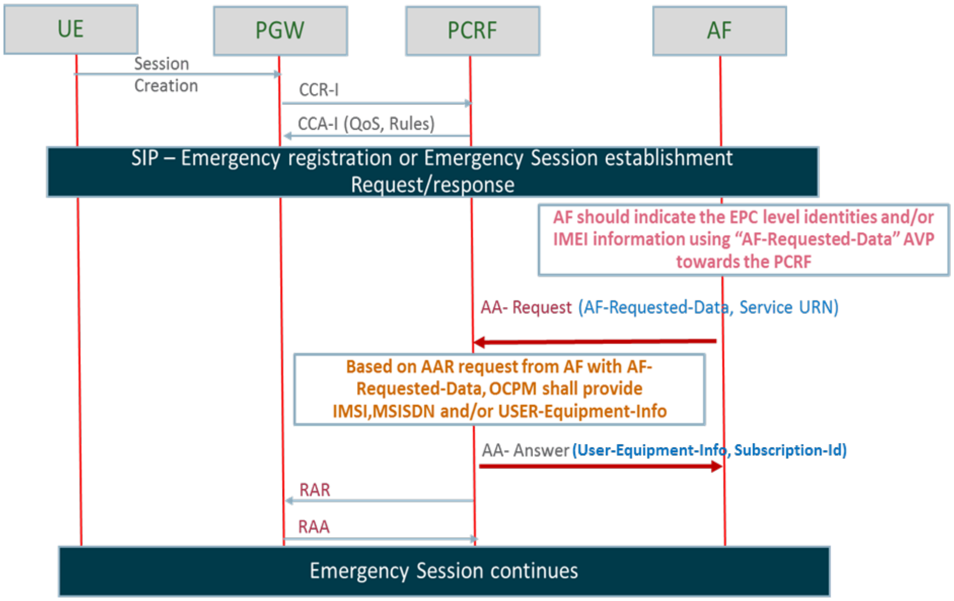
This feature is automatically activated if the AAR from AF containing AF-Requested-Data AVP that indicates "EPC-level Identities required" (bit 0 is set): AF-Requested-Data (551,V,v=10415,l=16) = 1.

3.1.3 Detailed Description

3.1.3.1 Call Flows

If the AF-Requested-Data AVP is provided in the AA-Request command indicating "EPC-level Identities required", the PCRF shall provide the available user information for the IP-CAN session within the Subscription-Id AVP (s) and/or User-Equipment-Info AVP. The call flow is:

Figure 3 Call Flow of AF-Requested-Data for S8HR


UE
PGW
PCRF
AF
Session Creation
CCR-I
CCA-I (QoS, Rules)
SIP – Emergency registration or Emergency Session establishment Request/response
AF should indicate the EPC level identities and/or IMEI information using "AF-Requested-Data" AVP towards the PCRF
AA- Request (AF-Requested-Data, Service URN)
Based on AAR request from AF with AF-Requested-Data, OCPM shall provide IMSI,MSISDN and/or USER-Equipment-Info
AA- Answer (User-Equipment-Info, Subscription-Id)
RAR
RAA
Emergency Session continues

The Rx AA-Request contains AF-Requested-Data indicating "EPC-level Identities required":

The sample AAR with AF-Requested-Data set to 0:

```
Diameter Message: AAR
..............
Session-Id (263,M,l=23) = rx_session_id_1
 Origin-Host (264,M,l=21) = pgw1.test.com
 Origin-Realm (296,M,l=16) = test.com
 Auth-Application-Id (258,M,l=12) = 16777236
 Destination-Realm (283,M,l=18) = oracle.com
Framed-IP-Address (8,M,l=12) = 10.0.11.6
 Specific-Action (513,VM,v=10415,l=16) = INDICATION_OF_LOSS_OF_BEARER  (2)
 Specific-Action (513,VM,v=10415,l=16) = INDICATION_OF_RELEASE_OF_BEARER  (4)
 Specific-Action (513,VM,v=10415,l=16) = INDICATION_OF_ESTABLISHMENT_OF_BEARER  (5)
 Specific-Action (513,VM,v=10415,l=16) = INDICATION_OF_IP_CAN_CHANGE  (6)
 Service-URN (525,VM,v=10415,l=15) = sos
 AF-Requested-Data (551,V,v=10415,l=16) = 1
```

The Rx AA-Answer returns Subscription-Id AVP (s) and/or User-Equipment-Info AVP:

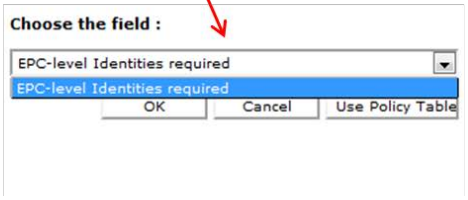
The sample AAA with EPC-level identities:

```
Diameter Message: AAA
.....................
 Session-Id (263,M,l=23) = rx_session_id_1
 Result-Code (268,M,l=12) = DIAMETER_SUCCESS  (2001)
 Subscription-Id (443,M,l=80) =
   Subscription-Id-Type (450,M,l=12) = END_USER_NAI  (3)
   Subscription-Id-Data (444,M,l=57) = 311480000032192@ims.mnc480.mcc311.3gppnetwork.org
 Subscription-Id (443,M,l=40) =
   Subscription-Id-Type (450,M,l=12) = END_USER_E164  (0)
   Subscription-Id-Data (444,M,l=19) = 15084869996
 Subscription-Id (443,M,l=44) =
   Subscription-Id-Type (450,M,l=12) = END_USER_IMSI  (1)
   Subscription-Id-Data (444,M,l=23) = 311480000032192
 User-Equipment-Info (458,,l=44) =
   User-Equipment-Info-Type (459,,l=12) = IMEISV (0)
   User-Equipment-Info-Value (460,,l=24) = 3520990017614823
```

3.1.3.2 Policy Changes

To support the AF-Requested-Data AVP from the policy, a new policy condition is added to check whether AF-Requested-Data AVP exists and indicates selected type(s).:

Policy Condition Group	Policy Condition or Action	Description
"Request" Conditions	where the AF-Requested-Data AVP exists and indicates select type(s)	Check whether AF-Requested-Data AVP indicates selected type. select type: one of: ➢ EPC-level Identities required



3.2 PLMN_CHANGE event trigger support for Rx (3GPP Rls 14) (BUG 26557079)

3.2.1 Introduction

This feature allows application function to subscribe and be updated with Traffic Plane Event of PLMN information through the PCRF using the Rx interface.

If AF subscribes to the notifications of PLMN ID change, OCPM shall provide the PLMN identifier to AF when receiving a change of PLMN from PCEF. In this case OCPM shall send a Diameter RAR command to the AF which include the Specific-Action AVP set to PLMN_CHANGE and include the 3GPP-SGSN-MCC-MNC AVP for the PLMN where the UE is located.

During the Rx session establishment or modification, the OCPM shall respond the AA-Answer message including the PLMN identifier within 3GPP-SGSN-MCC-MNC AVP if the OCPM has previously requested to be updated with this information in the PCEF.

3.2.2 Feature Activation

This PLMN_CHANGE subscription and reporting feature is activated if the supported feature of PLMNInfo is sucessfully negotiated in Rx AAR/AAA.

3.2.3 Detailed Description

OCPM shall support the "PLMNInfo" feature during Rx session establishment.

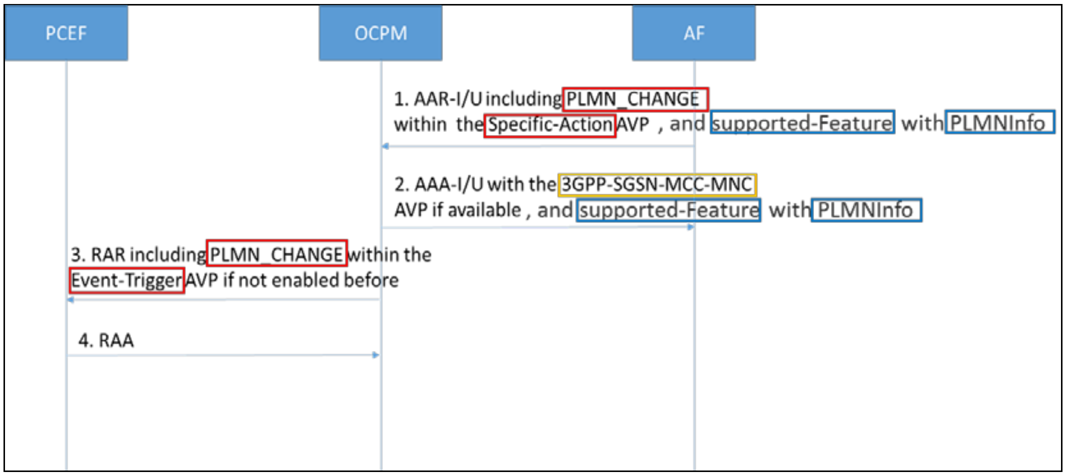
```
Supported-Features (628,V,v=10415,l=56) =
  Vendor-Id (266,M,l=12) = 10415
  Feature-List-ID (629,V,v=10415,l=16) = 1
  Feature-List (630,V,v=10415,l=16) = 524288
```

And the supported feature can be checked by the existing policy condition when evaluating AAR request from AF:

where the request supports feature PLMNInfo

3.2.3.1 Call Flows

Figure 4 Call Flow of PLMN_CHANGE event trigger subscription for Rx


PCEF
OCPM
AF
1. AAR-I/U including PLMN_CHANGE within the Specific-Action AVP , and supported-Feature with PLMNInfo
2. AAA-I/U with the 3GPP-SGSN-MCC-MNC AVP if available , and supported-Feature with PLMNInfo
3. RAR including PLMN_CHANGE within the Event-Trigger AVP if not enabled before
4. RAA

1. AF sends a Diameter AAR to the OCPM for Rx session establishment or update. The Diameter AAR includes the PLMN_CHANGE within the Specific-Action AVP.

Note: The "PLMNInfo" feature shall be supported during Rx session establishment, otherwise OCPM will not perform any specific functions as listed in the 3GPP reference pertaining to this feature.

2. Step2. OCPM responds a Diameter AAA to AF with the 3GPP-SGSN-MCC-MNC AVP if available from corresponding Gx session.

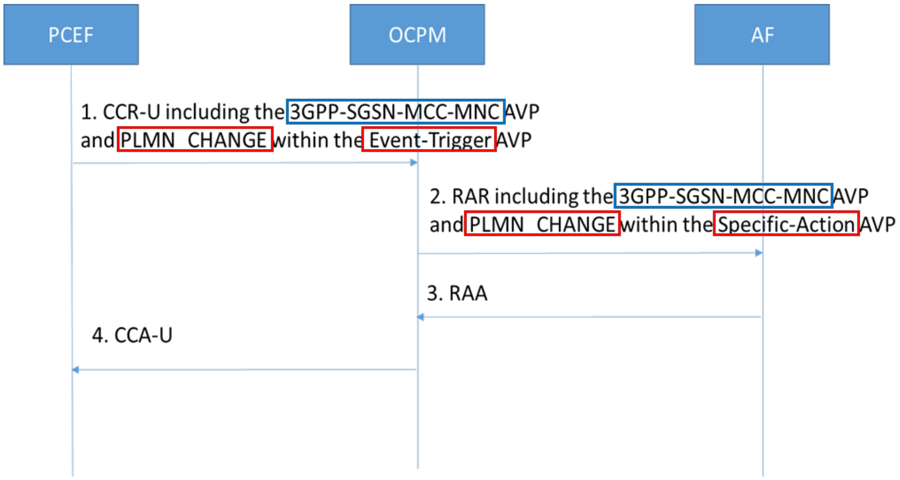
   Note: For the case of Diameter AAR not including the PLMN_CHANGE within the Specific-Action AVP in step 1, OCPM also responds a Diameter AAA to AF with the 3GPP-SGSN-MCC-MNC AVP if available.

3. Step3. OCPM sends a Diameter RAR to request the PCEF to report the change of PLMN.

   Note: The Diameter RAR shall include the PLMN_CHANGE within the Event-Trigger AVP if not enabled already. And in this case, OCPM shall add all existing event triggers into the Diameter RAR also.

4. PCEF responds a Diameter RAA.

Figure 5 Call Flow of PLMN_CHANGE event trigger reporting for Rx


PCEF
OCPM
AF
1. CCR-U including the 3GPP-SGSN-MCC-MNC AVP and PLMN_CHANGE within the Event-Trigger AVP
2. RAR including the 3GPP-SGSN-MCC-MNC AVP and PLMN_CHANGE within the Specific-Action AVP
3. RAA
4. CCA-U

1. PCEF sends a Diameter CCR-U including the 3GPP-SGSN-MCC-MNC AVP and the PLMN_CHANGE within the Event-Trigger AVP.

2. OCPM sends a Diameter RAR including the 3GPP-SGSN-MCC-MNC AVP and the PLMN_CHANGE within Specific-Action AVP.

   Note: OCPM will not report the change of PLMN if AF not request to subscription to the PLMN_CHANGE notification before.

3. AF responds a Diameter RAA.

4. OCPM responds a Diameter CCA-U. And this response may be sent back to PCEF prior to step 2.

3.3 PCRF picking up event triggers from all executed policy (BUG 27013746)

3.3.1 Introduction

Currently, event triggers will be overwritten by last executed policy if multiple policies are triggered.

With this enhancement, a new advanced setting is introduced to support picking up all event triggers from multiple executed policies.

3.3.2 Feature Activation

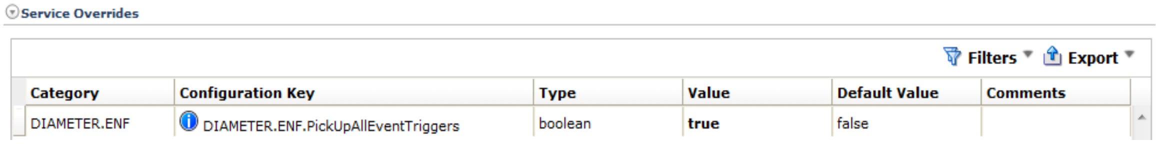
Set advance setting of DIAMETER.ENF.PickUpAllEventTriggers to True and apply to MPE, the event triggers will be merged from multiple executed policies.

3.3.3 Detailed Description

A new advance setting is introduced:

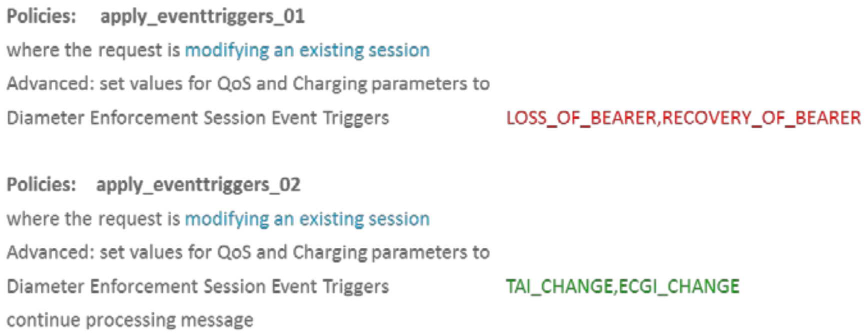
DIAMETER.ENF.PickUpAllEventTriggers, default value false, which is same as legacy behavior, the event triggers are overwritten by last executed policy.

If set this advance setting to true, the event triggers will be merged from multiple executed policies. For example:



Category	Configuration Key	Type	Value	Default Value	Comments
DIAMETER.ENF	DIAMETER.ENF.PickUpAllEventTriggers	boolean	**true**	false	

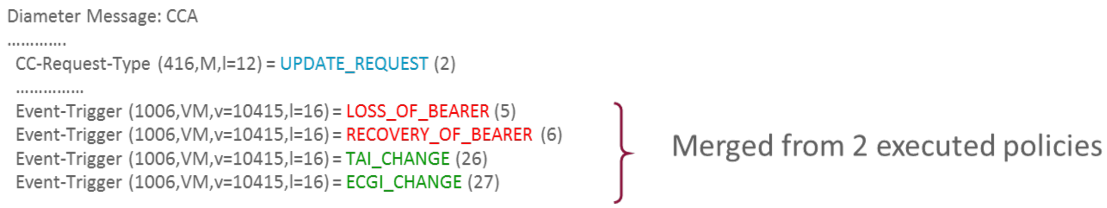
With below 2 sample policies executed,



Policies: **apply_eventtriggers_01**
where the request is modifying an existing session
Advanced: set values for QoS and Charging parameters to
Diameter Enforcement Session Event Triggers LOSS_OF_BEARER,RECOVERY_OF_BEARER

Policies: **apply_eventtriggers_02**
where the request is modifying an existing session
Advanced: set values for QoS and Charging parameters to
Diameter Enforcement Session Event Triggers TAI_CHANGE,ECGI_CHANGE
continue processing message

The result of event triggers armed will be:



```
Diameter Message: CCA
............
 CC-Request-Type (416,M,l=12) = UPDATE_REQUEST (2)
 ..............
 Event-Trigger (1006,VM,v=10415,l=16) = LOSS_OF_BEARER (5)
 Event-Trigger (1006,VM,v=10415,l=16) = RECOVERY_OF_BEARER  (6)
 Event-Trigger (1006,VM,v=10415,l=16) = TAI_CHANGE (26)
 Event-Trigger (1006,VM,v=10415,l=16) = ECGI_CHANGE (27)
```

Merged from 2 executed policies

3.4 LTE 5G Interworking Call Flows (BUG 27433899)

3.4.1 Introduction

Currently QoS specific data over PCC interfaces are defined as Unsigned32 type values indicating the bitrate of bps (bit per second). The maximum bandwidth value is about 4.3 Gbps (2^32 -1= 4,294,967,295 bits per second).

With this enhancement, the extended bandwidth AVPs are supported. These AVPs are also of type Unsigned32 but indicate kbit per second. The maximum supported bandwidth value is about 4,3 Tbps ((2^32 -1)*1000= 4,294,967,295,000 bits per second).

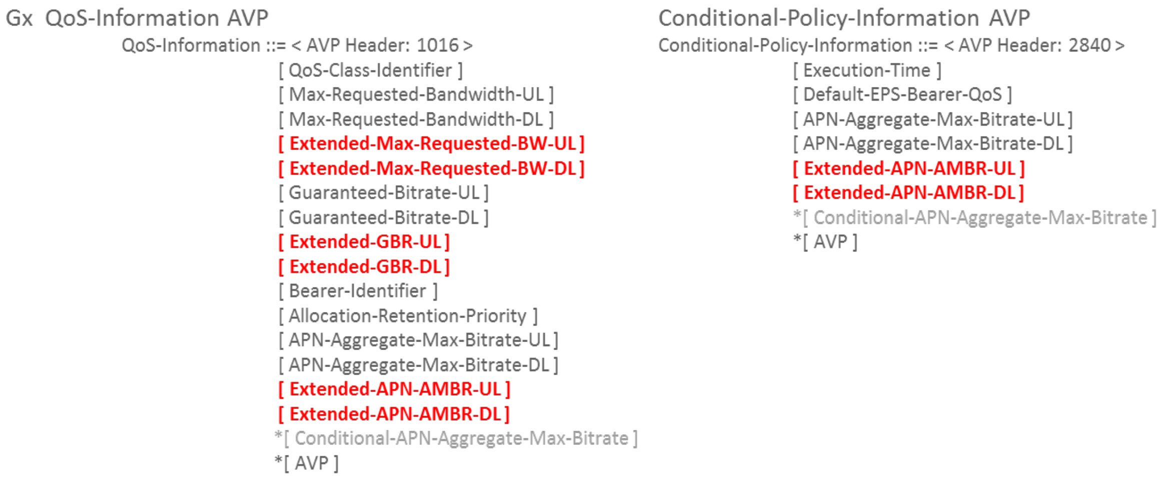
3.4.2 Feature Activation

This feature is automatically activated if the supported features of Extended-BW-NR, Extended-Max-Requested-BW-NR, or Extended-Min-Requested-BW-NR are successfully negotiated during Gx/Rx session establishment.

3.4.3 Detailed Description

3.4.3.1 Gx Interface

When the Extended-BW-NR feature is supported, extended bandwidth AVPs representing bitrates in kbps shall be used to support bandwidth values higher than 2^32-1 bps instead of the bandwidth AVPs representing bitrates in bps.



```
Gx QoS-Information AVP
        QoS-Information ::= < AVP Header: 1016 >
                        [ QoS-Class-Identifier ]
                        [ Max-Requested-Bandwidth-UL ]
                        [ Max-Requested-Bandwidth-DL ]
                        [ Extended-Max-Requested-BW-UL ]
                        [ Extended-Max-Requested-BW-DL ]
                        [ Guaranteed-Bitrate-UL ]
                        [ Guaranteed-Bitrate-DL ]
                        [ Extended-GBR-UL ]
                        [ Extended-GBR-DL ]
                        [ Bearer-Identifier ]
                        [ Allocation-Retention-Priority ]
                        [ APN-Aggregate-Max-Bitrate-UL ]
                        [ APN-Aggregate-Max-Bitrate-DL ]
                        [ Extended-APN-AMBR-UL ]
                        [ Extended-APN-AMBR-DL ]
                       *[ Conditional-APN-Aggregate-Max-Bitrate ]
                       *[ AVP ]
```

```
Conditional-Policy-Information AVP
Conditional-Policy-Information ::= < AVP Header: 2840 >
                        [ Execution-Time ]
                        [ Default-EPS-Bearer-QoS ]
                        [ APN-Aggregate-Max-Bitrate-UL ]
                        [ APN-Aggregate-Max-Bitrate-DL ]
                        [ Extended-APN-AMBR-UL ]
                        [ Extended-APN-AMBR-DL ]
                       *[ Conditional-APN-Aggregate-Max-Bitrate ]
                       *[ AVP ]
```

When the IP-CAN session is being established, if the PCEF supports the Extended-BW-NR feature and for bandwidth values higher than 2^32-1 bps, AVPs should include both:

- AVPs representing bitrate in bps = 2^32-1 bps (non Extended AVPs, just in case peer PCRF does not support Extented-BW-NR, then best effort bps is provided)
- AVPs representing bitrate in kbps = actual required bandwidth (Extended AVPs)

3.4.3.2 Rx Interface

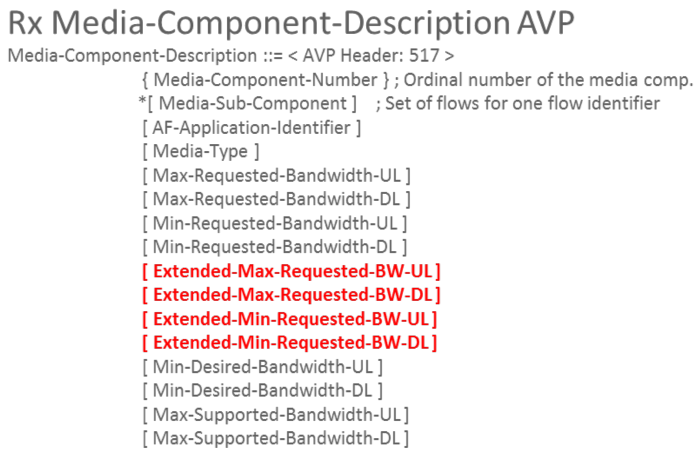
When the Extended-Max-Requested-BW-NR feature, the Extended-Min-Requested-BW-NR feature are supported, extended bandwidth AVPs representing bitrates in kbps shall be used to represent bandwidth values higher than 2^32-1 bps instead of the bandwidth AVPs with a maximum value of 2^32-1 bps that represent bitrates in bps.

For the Extended-Max-Requested-BW-NR feature:

- Extended-Max-Requested-BW-DL/UL AVPs shall be used instead of Max-Requested-Bandwidth-DL/UL AVPs.

For the Extended-Min-Requested-BW-NR feature:

- Extended-Min-Requested-BW-DL/UL AVPs shall be used instead of Min-Requested-Bandwidth-DL/UL AVPs.



Rx Media-Component-Description AVP

```
Media-Component-Description ::= < AVP Header: 517 >
                  { Media-Component-Number } ; Ordinal number of the media comp.
                 *[ Media-Sub-Component ]    ; Set of flows for one flow identifier
                  [ AF-Application-Identifier ]
                  [ Media-Type ]
                  [ Max-Requested-Bandwidth-UL ]
                  [ Max-Requested-Bandwidth-DL ]
                  [ Min-Requested-Bandwidth-UL ]
                  [ Min-Requested-Bandwidth-DL ]
                  [ Extended-Max-Requested-BW-UL ]
                  [ Extended-Max-Requested-BW-DL ]
                  [ Extended-Min-Requested-BW-UL ]
                  [ Extended-Min-Requested-BW-DL ]
                  [ Min-Desired-Bandwidth-UL ]
                  [ Min-Desired-Bandwidth-DL ]
                  [ Max-Supported-Bandwidth-UL ]
                  [ Max-Supported-Bandwidth-DL ]
```

NOTE: When the Rx session is being established, if the AF supports the Extended-Max-Requested-BW-NR or Extended-Min-Requested-BW-NR feature and needs to indicate bandwidth values higher than 2^32-1 bps, AVPs should include both:

- AVPs representing bitrate in bps = 2^32-1 bps (non-Extended AVPs, just in case peer PCRF does not support Extended-Max-Requested-BW-NR or Extended-Min-Requested-BW-NR, then best effort bps is provided)
- AVPs representing bitrate in kbps = actual required bandwidth (Extended AVPs)

NOTE: Extended-BW-E2EQOSMTSI-NR is not in the scope of this implementation because the dependent E2EQOSMTSI is not supported.

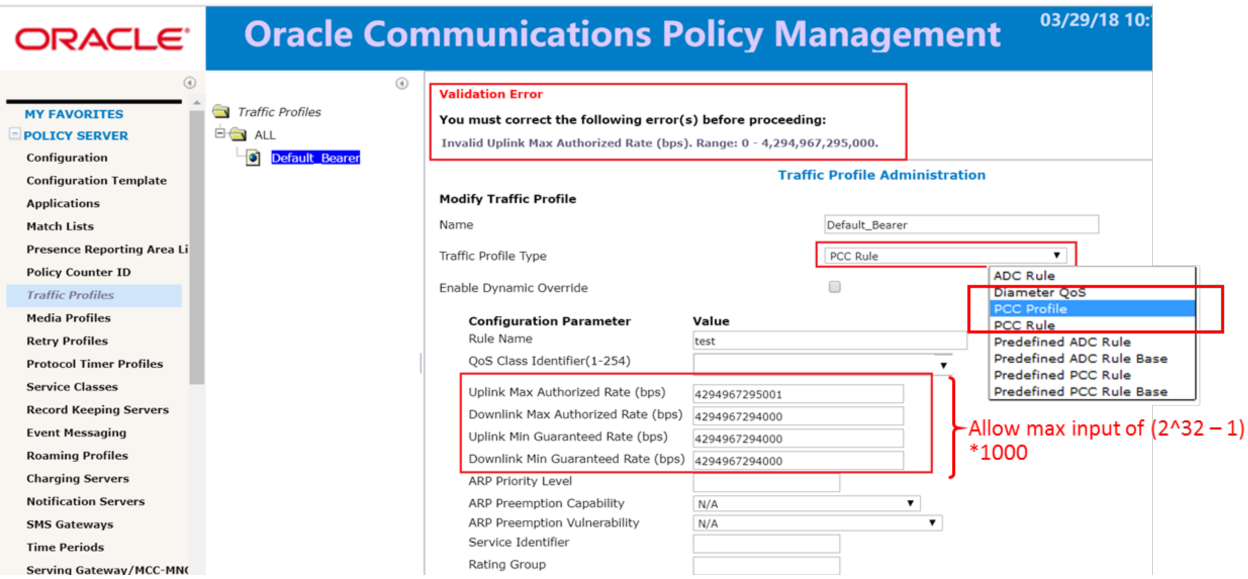
3.4.3.3 User Interface

The bandwidth fields on GUI are enhanced to support bandwidth values > (2^32-1) bps and <= (2^32 – 1)*1000 bps.

- Traffic Profile
- Policy Condition/Action/Table
- Import/Export
- Session Viewer
- RcMgr

For example:

Figure 6 CMP enhancement for Extended QoS



Validation Error

You must correct the following error(s) before proceeding:

Invalid Uplink Max Authorized Rate (bps). Range: 0 - 4,294,967,295,000.

Traffic Profile Administration

Modify Traffic Profile

Name	Default_Bearer
Traffic Profile Type	PCC Rule
Enable Dynamic Override	□

Configuration Parameter	Value
Rule Name	test
QoS Class Identifier(1-254)	
Uplink Max Authorized Rate (bps)	4294967295001
Downlink Max Authorized Rate (bps)	4294967294000
Uplink Min Guaranteed Rate (bps)	4294967294000
Downlink Min Guaranteed Rate (bps)	4294967294000
ARP Priority Level	
ARP Preemption Capability	N/A
ARP Preemption Vulnerability	N/A
Service Identifier	
Rating Group	

Allow max input of (2^32 – 1) *1000

3.5 PCRF Invocation for Option 3X (Presence Reporting Area AVP Support) (BUG 27433979)

3.5.1 Introduction

Currently, only single PRA is supported under Wireless-C mode.

With this enhancement, both multiple PRA and single PRA are supported in Wireless mode for PRA (Presence Reporting area) subscription, reporting and handling.

3.5.2 Feature Activation

This feature is enabled in default and could be disabled by DIAMETER.PRA.PRAEnabled.

The IP-CAN Type(s) which support PRA feature should be added into advance setting of DIAMETER.PRA. PRASupportedAccesses and delimited by comma, e. g. “THREEGPP_GPRS, THREEGPP_EPS”.

3.5.3 Detailed Description

As part of this feature, PCRF shall be enhanced to support Presence Reporting Area (PRA) feature. Feature shall support both single PRA (CNO-ULI) and Multiple PRA (Multi-PRA).

Feature shall also allow Operator to write policies to subscribe or unsubscribe to the PRA event trigger value: CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) anytime during the life time of the IP-CAN session.

For PRA subscription based on Single-PRA, the MPE will send the subscribed Presence-Reporting-Area-Information AVP to PCEF. For Multi-PRA, the PCRF will send the PRA-Install and PRA-Remove information to PCEF for installing or removing the related subscribed PRA.

PCRF will also install the configured PCC rules to PCEF which reports the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) event trigger with Presence-Reporting-Area-Status and Presence Reporting Area Identifier(s).

Both Core Network predefined and UE-dedicated PRA are supported by PCRF. For Core Network predefined PRA, only Presence Reporting Area Identifier(s) is/are necessary for subscribing, and for UE-dedicated PRA, both Presence Reporting Area Identifier(s) and the Presence-Reporting-Area-Elements-List are required.

The difference of single PRA and multiple PRA are listed below:

Use Case	Single PRA	Multiple PRA(s)
Supported Feature	(CCR-I,CCA-I) Feature-List-ID 1: Bit 23: CNO-ULI	(CCR-I,CCA-I) Feature-List-ID 2: Bit 3: **Multi-PRA**
Subscribe	(CCA-I, CCA-U, RAR) Event trigger with value CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48)	
Install (core network predefined)	(CCA-I, CCA-U, RAR) Presence-Reporting-Area-Information (2822,V,v=10415,l=28) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x01A2AC	**PRA-Install** (2845,V,v=10415,l=xx) Presence-Reporting-Area-Information (2822,V,v=10415,l=28) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x01A2AC Presence-Reporting-Area-Information (2822,V,v=10415,l=28) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x01BD9A
Install (UE dedicated)	Presence-Reporting-Area-Information (2822,V,v=10415,l=140) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x000367 Presence-Reporting-Area-Elements-List (2820,V,v=10415,l=110) = 0x22020202020274F880010F74F88000AB64F8820006B164F8820006B064F083000006B364F083000006B264F084000006B564F084000006B464F881006B06AF64F881006B06AE648050001100136480500011001264806100110015648061001100 14	**PRA-Install** (2845,V,v=10415,l=xx) **Presence-Reporting-Area-Information** (2822,V,v=10415,l=140) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x000367 Presence-Reporting-Area-Elements-List (2820,V,v=10415,l=110) = 0x22020202020274F880010........... **Presence-Reporting-Area-Information** (2822,V,v=10415,l=140) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x000367 Presence-Reporting-Area-Elements-List (2820,V,v=10415,l=110) = 0x22020202020274F39D724...........
Remove	**(not support, unsubscribe instead)**	(CCA-U, RAR) **PRA-Remove (2846,V,v=10415,l=xx)** **Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x01A2AC** **Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x01BD9A**
Report	(CCR-U) Event-Trigger (1006,VM,v=10415,l=16) = CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) Presence-Reporting-Area-Information (2822,V,v=10415,l=44) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x01A2AC Presence-Reporting-Area-Status (2823,V,v=10415,l=16) = IN (0)	Event-Trigger (1006,VM,v=10415,l=16) = CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) **Presence-Reporting-Area-Information** (2822,V,v=10415,l=44) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x01A2AC Presence-Reporting-Area-Status (2823,V,v=10415,l=16) = IN (0) **Presence-Reporting-Area-Information** (2822,V,v=10415,l=44) = Presence-Reporting-Area-Identifier (2821,V,v=10415,l=15) = 0x01BD9A Presence-Reporting-Area-Status (2823,V,v=10415,l=16) = OUT (1)
Limitation	Maximum 1 PRA Info.	The maximum number of PRAs may be configured in the PCRF. The PCRF may have independent configuration of the **maximum number** for Core Network pre-configured PRAs and UE-dedicated PRAs. (Implementation gap: a global configure item instead of independent)
Unsubscribe	(CCA-U, RAR) Event trigger without value CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48)	

3.5.3.1 Call Flows

Figure 7 Call Flow of PRA Subscription during Gx session establishment

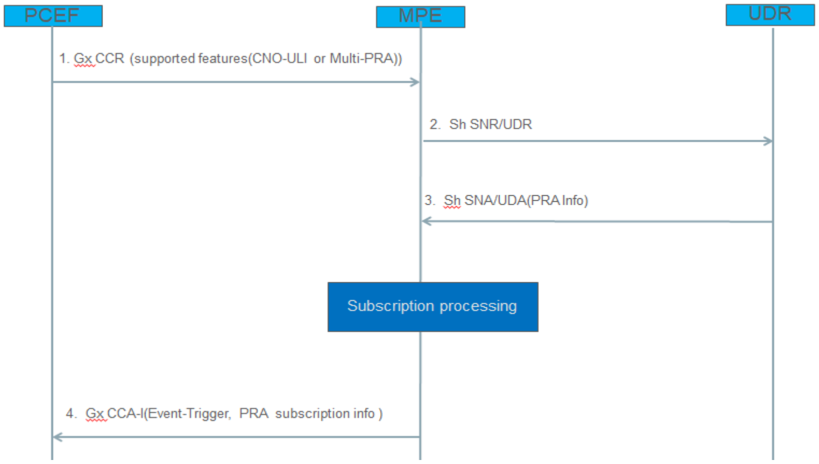

PCEF
MPE
UDR
1. Gx CCR (supported features(CNO-ULI or Multi-PRA))
2. Sh SNR/UDR
3. Sh SNA/UDA(PRA Info)
Subscription processing
4. Gx CCA-I(Event-Trigger, PRA subscription info)

Figure 8 Call Flow of PRA Report and Subscription/Unsubscription during Gx session update

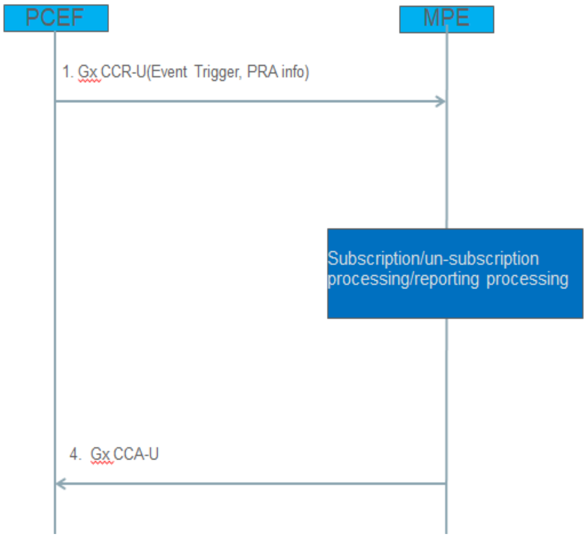
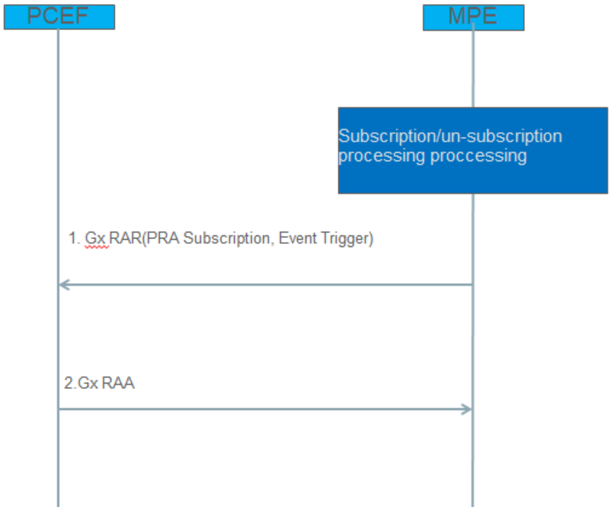
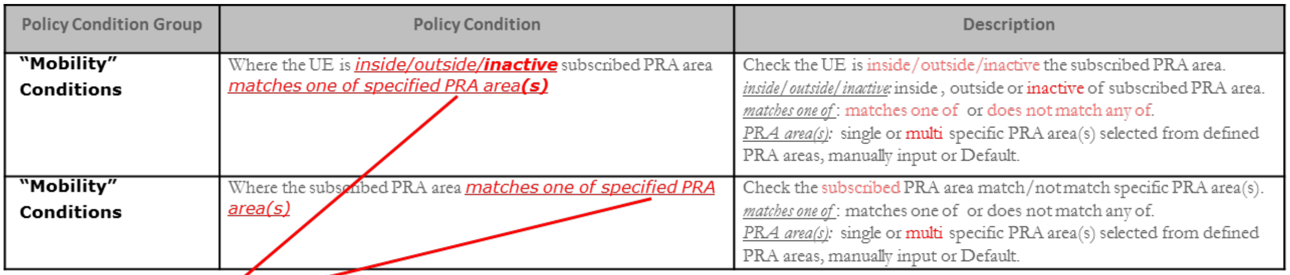

PCEF
MPE
1. Gx CCR-U(Event Trigger, PRA info)
Subscription/un-subscription processing/reporting processing
4. Gx CCA-U

Figure 9 Call Flow of PRA Subscription and Unsubscription during Gx session revalidation

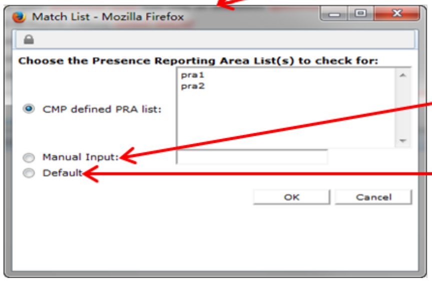

PCEF
MPE
Subscription/un-subscription processing proccessing
1. Gx RAR(PRA Subscription, Event Trigger)
2.Gx RAA

3.5.3.2 Policy Changes

Policy condition:



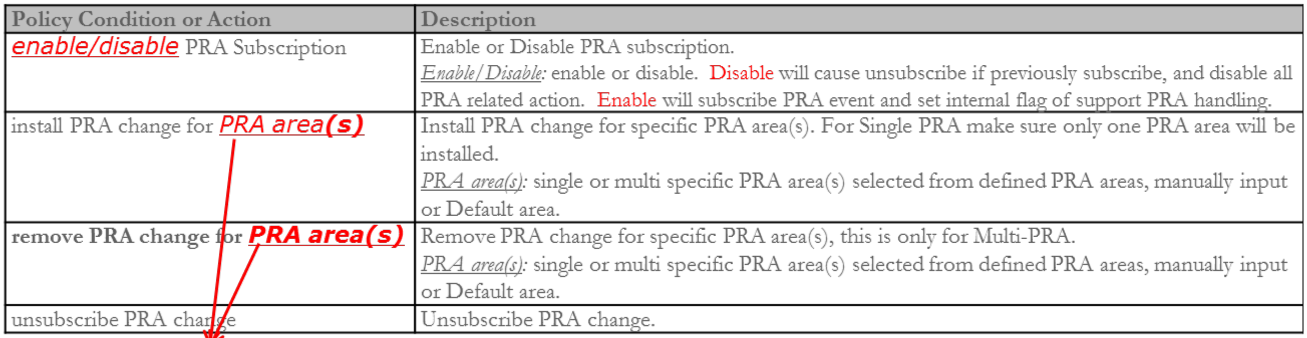
Policy Condition Group	Policy Condition	Description
"Mobility" Conditions	Where the UE is *inside/outside/inactive* subscribed PRA area *matches one of specified PRA area(s)*	Check the UE is inside/outside/inactive the subscribed PRA area. *inside/outside/inactive*: inside , outside or inactive of subscribed PRA area. *matches one of* : matches one of or does not match any of. *PRA area(s)*: single or multi specific PRA area(s) selected from defined PRA areas, manually input or Default.
"Mobility" Conditions	Where the subscribed PRA area *matches one of specified PRA area(s)*	Check the subscribed PRA area match/not match specific PRA area(s). *matches one of* : matches one of or does not match any of. *PRA area(s)*: single or multi specific PRA area(s) selected from defined PRA areas, manually input or Default.


Match List - Mozilla Firefox
Choose the Presence Reporting Area List(s) to check for:
pra1
pra2
CMP defined PRA list:
Manual Input:
Default
OK
Cancel

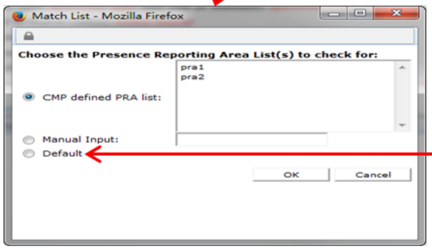
- PRA identifier1[;PRA element list1],PRA identifier2[;PRA element list2],……
  PRA element list using the Hex representation as defined in section 8.108 of TS 29.274[9].
  The manual input is typically used for operator to input a temporally PRA area.
- Also allow get PRA area from Custom field of subscriber, e.g. {User.Custom4} for home, {User.Custom5} for office.

Default option means to check whether the UE has subscribed to a PRA area but don't care what the PRA area is.

Policy actions:



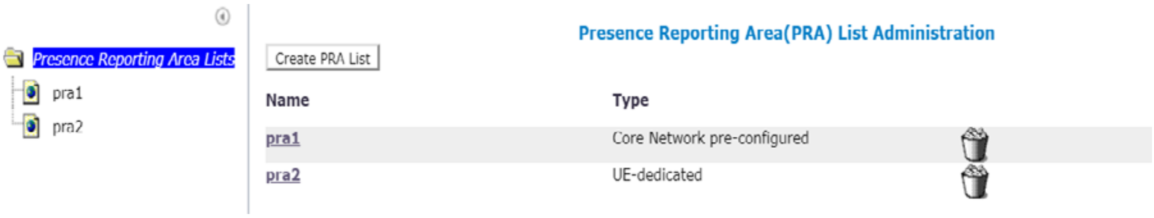
Policy Condition or Action	Description
enable/disable PRA Subscription	Enable or Disable PRA subscription. *Enable/Disable*: enable or disable. Disable will cause unsubscribe if previously subscribe, and disable all PRA related action. Enable will subscribe PRA event and set internal flag of support PRA handling.
install PRA change for *PRA area(s)*	Install PRA change for specific PRA area(s). For Single PRA make sure only one PRA area will be installed. *PRA area(s)*: single or multi specific PRA area(s) selected from defined PRA areas, manually input or Default area.
remove PRA change for *PRA area(s)*	Remove PRA change for specific PRA area(s), this is only for Multi-PRA. *PRA area(s)*: single or multi specific PRA area(s) selected from defined PRA areas, manually input or Default area.
unsubscribe PRA change	Unsubscribe PRA change.


Match List - Mozilla Firefox
Choose the Presence Reporting Area List(s) to check for:
pra1
pra2
CMP defined PRA list:
Manual Input:
Default
OK
Cancel

For subscription and Install action:
CCR-I: use the subscribe profile PRA info
CCR-U: PRA feature will be activated to PGW if it' unsubscribed before

3.5.3.3 User Interface Changes

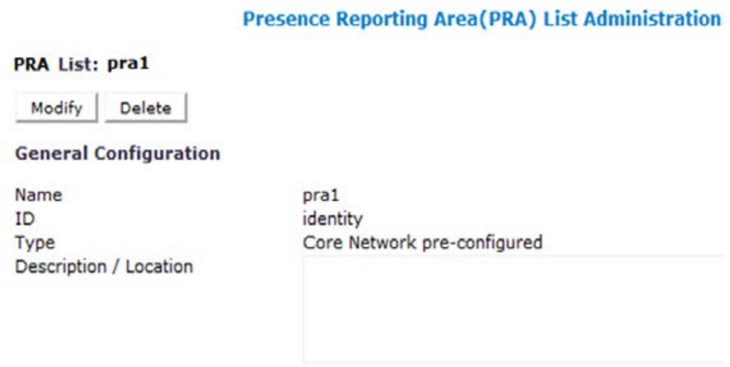
Figure 10 CMP: PRA Administration



Presence Reporting Area(PRA) List Administration

Name	Type
pra1	Core Network pre-configured
pra2	UE-dedicated

Figure 11 CMP: PRA - Core Network Pre-configured



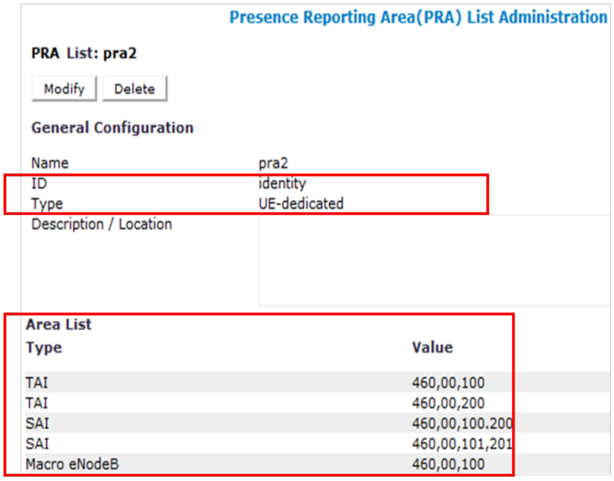
Presence Reporting Area(PRA) List Administration

PRA List: pra1

General Configuration

Name	pra1
ID	identity
Type	Core Network pre-configured
Description / Location	

Figure 12 CMP: PRA - UE-dedicated



Presence Reporting Area(PRA) List Administration

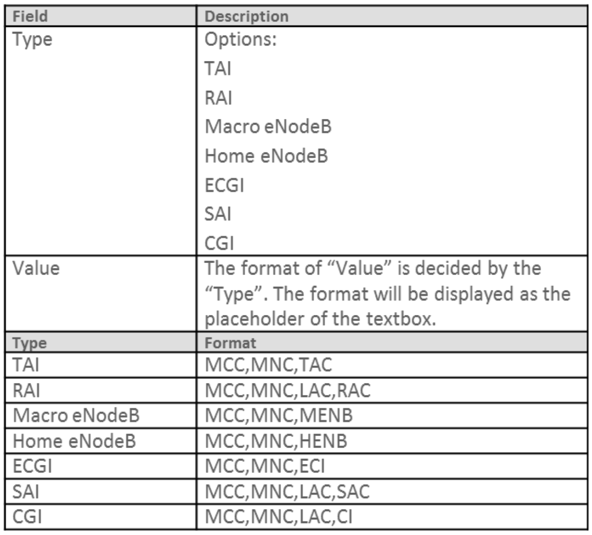
PRA List: pra2

General Configuration

Name	pra2
ID	identity
Type	UE-dedicated
Description / Location	

Area List

Type	Value
TAI	460,00,100
TAI	460,00,200
SAI	460,00,100.200
SAI	460,00,101,201
Macro eNodeB	460,00,100



Field	Description
Type	Options: TAI RAI Macro eNodeB Home eNodeB ECGI SAI CGI
Value	The format of "Value" is decided by the "Type". The format will be displayed as the placeholder of the textbox.

Type	Format
TAI	MCC,MNC,TAC
RAI	MCC,MNC,LAC,RAC
Macro eNodeB	MCC,MNC,MENB
Home eNodeB	MCC,MNC,HENB
ECGI	MCC,MNC,ECI
SAI	MCC,MNC,LAC,SAC
CGI	MCC,MNC,LAC,CI

3.5.3.4 Limitations

Upgrade the single PRA feature from R12.2~12.4 single PRA under Wireless-C mode to R12.5 PRA feature is not supported.

3.6 Maintain Session Uniqueness and avoid Stale MP (BUG 27175916)

3.6.1 Introduction

- Detection and handling of avoid requests collide with an existing session context according Origination-Time-Stamp AVP in CC-Request initial.
- Detection and handling of requests which have timed out at the originating entity.

3.6.2 Detailed Description

Solution for avoid requests collide is to follow TS 29.212 subclause 4.5.26.2 for the IP-CAN session establishment, the CC-Request Initial includes Origination-Time-Stamp AVP. For the CCR-I with same UE (i.e. the same Subscription-Id AVP), same APN (i.e. the same Called-Station-Id AVP) but from a different PCEF (i.e. different Origin-Host AVP),

- accept the new CC-Request only if it contains a more recent timestamp

- reject the new CC-Request by setting the Experimental-Result-Code to DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST if the timestamp is less recent.
- accept a new CC-Request if the origination timestamp is not provided for at least one of the IP-CAN sessions for the same UE and the same APN.

Solution for sender has timed out on the message is to follow TS 29.212 subclause 4.5.26.3 for the IP-CAN session establishment. CC-Request Initial includes Origination-Time-Stamp AVP and Maximum-Wait-Time AVP.

- Accept the request which has not already timed out at the originating node (Origination-Time-Stamp + Maximum-Wait-Time > current time)
- Reject the CC-Request that has timed out by setting the Experimental-Result-Code to DIAMETER_ERROR_TIMED_OUT_REQUEST
- PCRF perform additional similar check before sending the answer.

3.6.2.1 Call Flows

Figure 13 Call flow of handling collide requrest

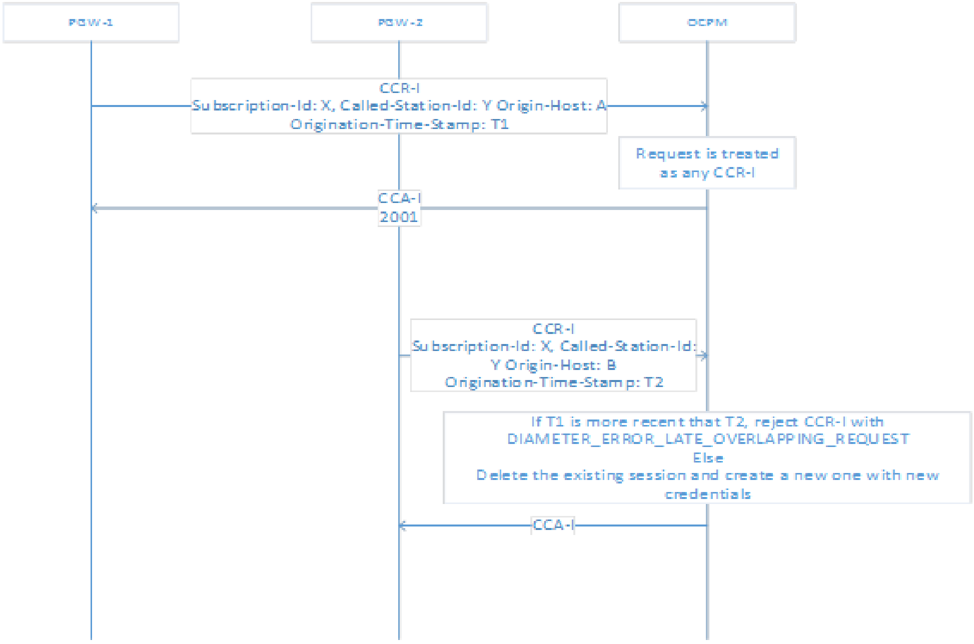
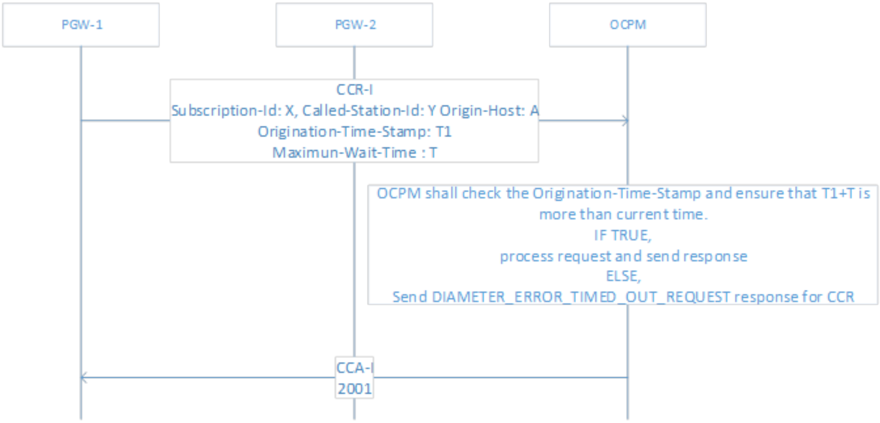

PGW-1
PGW-2
OCPM
CCR-I
Subscription-Id: X, Called-Station-Id: Y Origin-Host: A
Origination-Time-Stamp: T1
Request is treated as any CCR-I
CCA-I
2001
CCR-I
Subscription-Id: X, Called-Station-Id: Y Origin-Host: B
Origination-Time-Stamp: T2
If T1 is more recent that T2, reject CCR-I with DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST
Else
Delete the existing session and create a new one with new credentials
CCA-I

Figure 14 Call flow of handling time out requests


PGW-1
PGW-2
OCPM
CCR-I
Subscription-Id: X, Called-Station-Id: Y Origin-Host: A
Origination-Time-Stamp: T1
Maximun-Wait-Time : T
OCPM shall check the Origination-Time-Stamp and ensure that T1+T is more than current time.
IF TRUE,
process request and send response
ELSE,
Send DIAMETER_ERROR_TIMED_OUT_REQUEST response for CCR
CCA-I
2001

3.6.2.2 *Upgrade Considerations*

This feature will affect upgrade procedures of VzW. As in previous release, VzW is using proprietary AVPs to handle similar case.

With the AVPs changed to be comply with 3GPP spec in OCPM R12.5, after OCPM upgrade to R12.5, PCEF should also be upgraded to support the new AVPs and the Experimental-Result-Code for this feature to take effect.

3.7 CSG Mobility Event Support (BUG 27177007)

3.7.1 Introduction

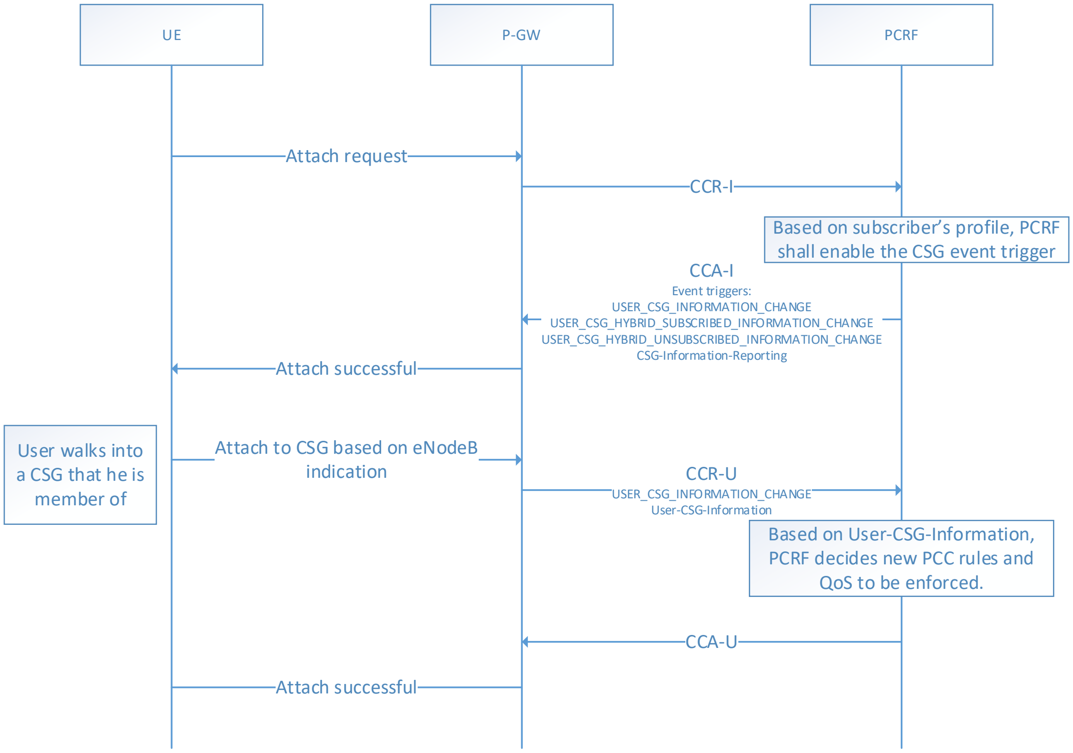
Currently, PCRF supports the CSG related event triggers and “User-CSG-Information” AVP in Gx interface.

With this enhancement, policy conditions are added to identify the subscriber status when they are in/out CSG Cells or Hybrid Cells.

3.7.2 Detailed Description

3.7.2.1 *Call Flows*

Figure 15 Call flow of CSG subscription and report


UE
P-GW
PCRF
Attach request
CCR-I
Based on subscriber’s profile, PCRF shall enable the CSG event trigger
CCA-I
Event triggers:
USER_CSG_INFORMATION_CHANGE
USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE
USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE
CSG-Information-Reporting
Attach successful
User walks into a CSG that he is member of
Attach to CSG based on eNodeB indication
CCR-U
USER_CSG_INFORMATION_CHANGE
User-CSG-Information
Based on User-CSG-Information, PCRF decides new PCC rules and QoS to be enforced.
CCA-U
Attach successful

3.7.2.2 *Policy Changes*

Policy Condition Group	Policy Condition	Description
“Request” Conditions	Where the select type is contained in Match List(s) select list(s)	Check whether the select type is contained in the specified match list(s). Select type : add a new select type “CSG_ID” Select list(s): select the existing match list(s)

Policy Condition Group	Policy Condition	Description
“Request” Conditions	Where the select type is not contained in Match List(s) select list(s)	Check whether the select type is not contained in the specified match list(s). Select type : add a new select type “CSG_ID” Select list(s): select the existing match list(s)
“Mobility” Conditions	Where the CSG ID is available	Check whether the CSG ID is available. is : is or is not
“Mobility” Conditions	Where the CSG ID matches one of specified CSG ID value(s)	Check whether the CSG ID is one of the listed values. matches one of : matches one of or does not match any of specified CSG ID value(s) : a comma-delimited list of values
“Mobility” Conditions	Where the CSG Access Mode is Closed	Check whether the CSG access mode is Closed. Closed : Closed or Hybrid
“Mobility” Conditions	Where the UE is member of the CSG	Check whether the UE is a member of the CSG. is : is or is not

3.8 Network Services Header Support (BUG 27176622)

3.8.1 Introduction

A VzW specific AVP Enterprise-Service-Path-ID may be included by the PCRF towards the PGW based on a Sh Subscriber profile information.

3.8.2 Feature Activation

The Enterprise-Service-Path-ID is VzW specific AVP, it’s only supported if the capabilities exchange (CER/CEA) includes the Verizon Wireless Vendor ID with value (12951) in a Supported-Vendor-Id AVP.

3.8.3 Detailed Description

This feature enhancement encompasses the protocol and MPE changes necessary to be compliant with Verizon specific feature Network Services Header support.

OCPM support insertion of VzW proprietary Enterprise-Service-Path-ID based on subscriber profile in case of PDP session creation, update or subscriber profile modification (UDR notification). The Enterprise-Service-Path-ID AVP will be included in Gx CCA-I/CCA-U/RAR message if the new policy action is deployed and successfully triggered. It can also be returned by PCRF in session recovery procedure.

3.8.3.1 Policy Changes

Policy Condition Group	Policy Condition or Action	Description
Optional actions	set enterprise service path ID to value for the Gx session	Set enterprise service path ID to a specified value for the Gx session. The value will be stored as the EnterpriseServicePathID attribute of the Gx session. value : specified value

3.9 Support for External-ID on Gx/Sh for MSISDN-less devices (BUG 27434131)

3.9.1 Introduction

Support Subscription-Id of type END_USER_NAI for MTC devices which could be MSISDNless and may not have traditional Subscription-Id type END_USER_E164.

3.9.2 Detailed Description

According VzW Gx spec, MTC devices can be MSISDNless and may not have traditional Subscription-Id type END_USER_E164. External ID will be sent for these devices in Subscription ID instead of MSISDN. END_USER_NAI will be used for Subscription-Id-Type AVP. These devices will have IMSI.

This feature support NAI handling on both Gx and Sh interfaces.

- On Gx interface, NAI can be handled as Subscription-Id type.
- On Sh interface, NAI or IMSI can be translated to User-Identity’s IMS-Public-Id, then send to SPR in SNR/UDR. The translation is compliant with 3GPP TS 23.003.

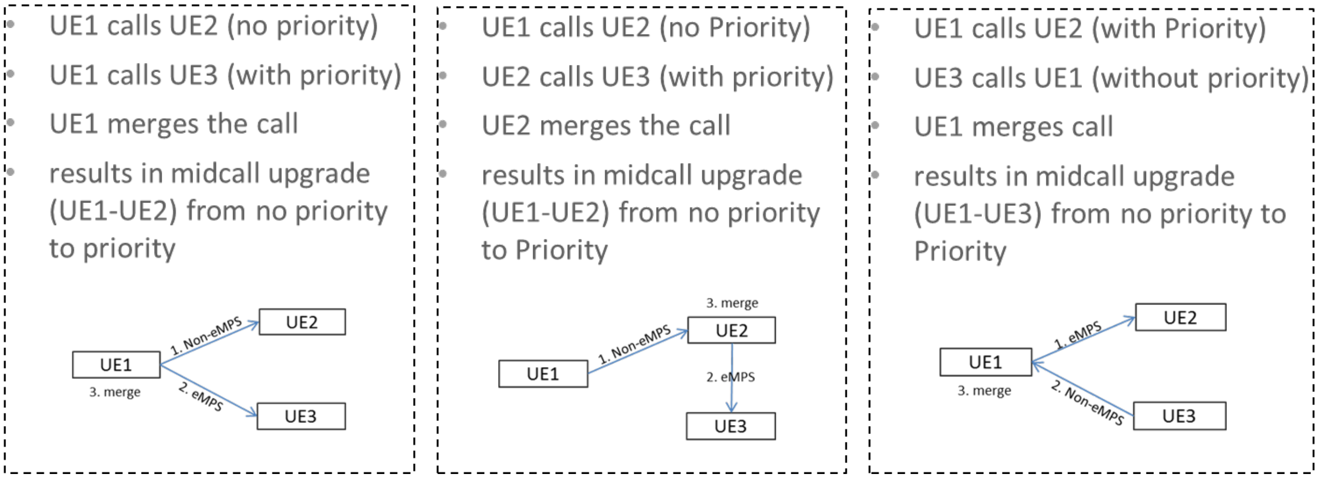
3.10 eMPS Conference Call (BUG 27434084)

3.10.1 Introduction

Extends existing eMPS support by supporting establishment of eMPS conference call. The eMPS related bearer prioritization shall be extended to all the parties involved in the conference.

3.10.2 Detailed Description

There are different kinds of use cases for eMPS conference call. Below is 3 example use cases.



- UE1 calls UE2 (no priority)
- UE1 calls UE3 (with priority)
- UE1 merges the call
- results in midcall upgrade (UE1-UE2) from no priority to priority

- UE1 calls UE2 (no Priority)
- UE2 calls UE3 (with priority)
- UE2 merges the call
- results in midcall upgrade (UE1-UE2) from no priority to Priority

- UE1 calls UE2 (with Priority)
- UE3 calls UE1 (without priority)
- UE1 merges call
- results in midcall upgrade (UE1-UE3) from no priority to Priority

3.10.2.1 Call Flows

Below call flows take above use case 1 as example.

Figure 16 UE1 makes IMS voice call to UE2 without eMPS

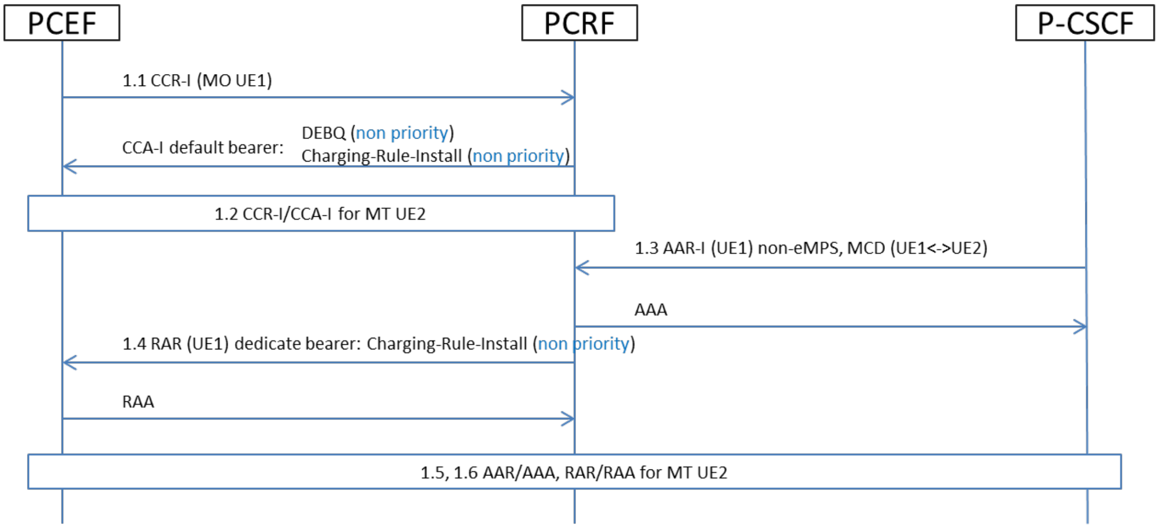

PCEF
PCRF
P-CSCF
1.1 CCR-I (MO UE1)
CCA-I default bearer:
DEBQ (non priority)
Charging-Rule-Install (non priority)
1.2 CCR-I/CCA-I for MT UE2
1.3 AAR-I (UE1) non-eMPS, MCD (UE1<->UE2)
AAA
1.4 RAR (UE1) dedicate bearer: Charging-Rule-Install (non priority)
RAA
1.5, 1.6 AAR/AAA, RAR/RAA for MT UE2

Figure 17 UE1 makes IMS voice call to UE3 with eMPS

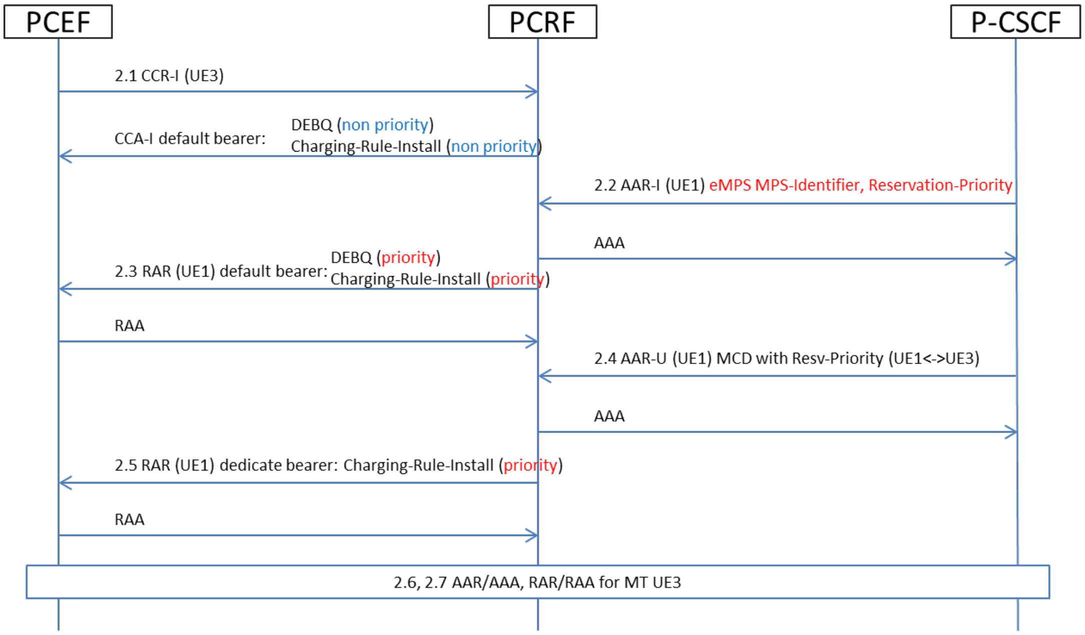

PCEF
PCRF
P-CSCF
2.1 CCR-I (UE3)
CCA-I default bearer:
DEBQ (non priority)
Charging-Rule-Install (non priority)
2.2 AAR-I (UE1) eMPS MPS-Identifier, Reservation-Priority
AAA
2.3 RAR (UE1) default bearer:
DEBQ (priority)
Charging-Rule-Install (priority)
RAA
2.4 AAR-U (UE1) MCD with Resv-Priority (UE1<->UE3)
AAA
2.5 RAR (UE1) dedicate bearer: Charging-Rule-Install (priority)
RAA
2.6, 2.7 AAR/AAA, RAR/RAA for MT UE3

Figure 18 UE1 starts conference call with UE2 and UE3

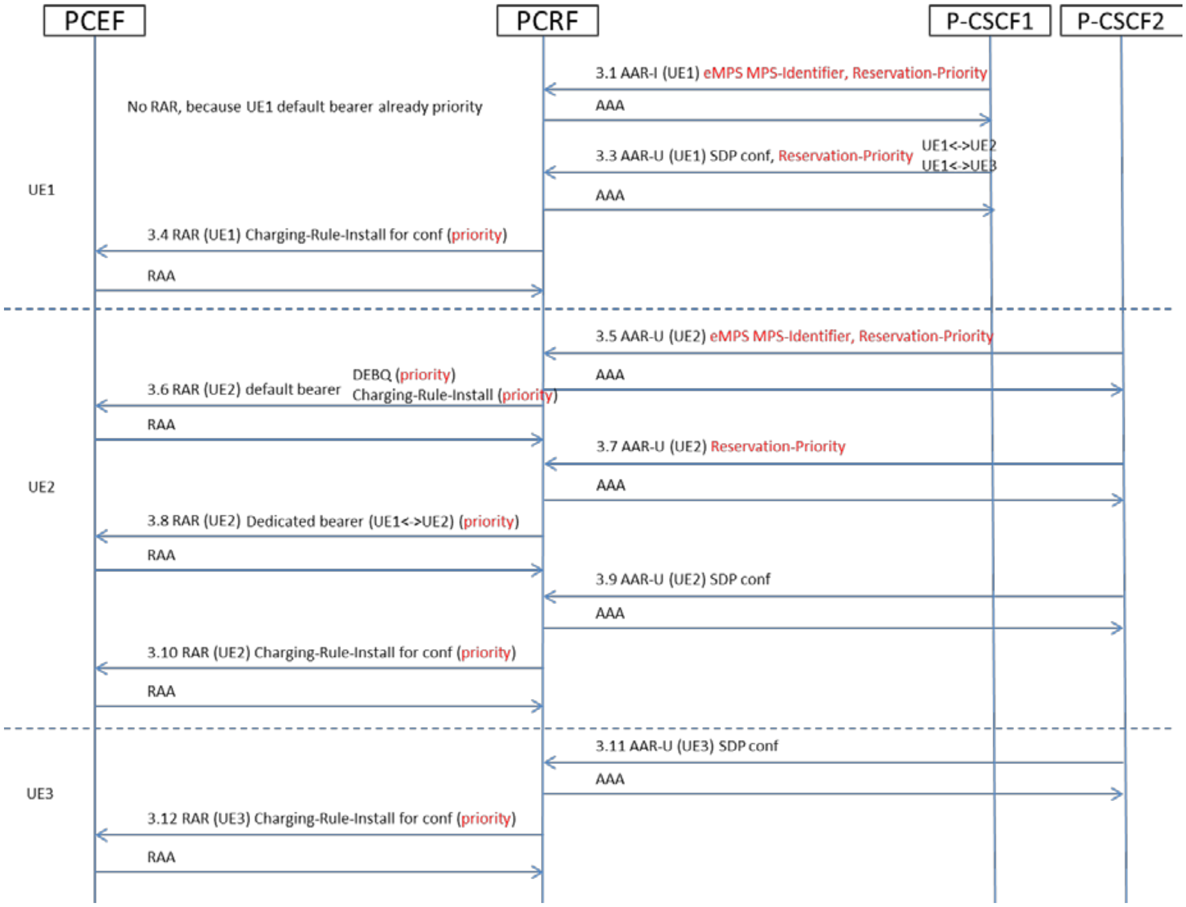
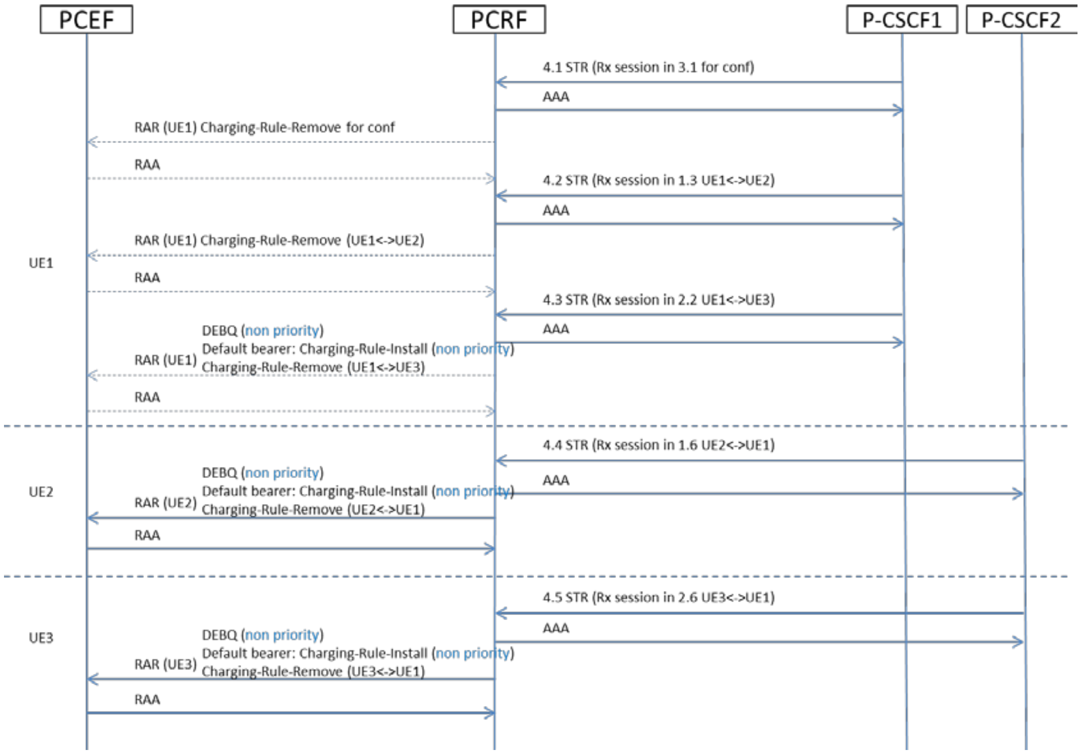

PCEF
PCRF
P-CSCF1
P-CSCF2
3.1 AAR-I (UE1) eMPS MPS-Identifier, Reservation-Priority
No RAR, because UE1 default bearer already priority
AAA
3.3 AAR-U (UE1) SDP conf, Reservation-Priority
UE1<->UE2
UE1<->UE3
UE1
AAA
3.4 RAR (UE1) Charging-Rule-Install for conf (priority)
RAA
3.5 AAR-U (UE2) eMPS MPS-Identifier, Reservation-Priority
DEBQ (priority)
3.6 RAR (UE2) default bearer
Charging-Rule-Install (priority)
AAA
RAA
3.7 AAR-U (UE2) Reservation-Priority
UE2
AAA
3.8 RAR (UE2) Dedicated bearer (UE1<->UE2) (priority)
RAA
3.9 AAR-U (UE2) SDP conf
AAA
3.10 RAR (UE2) Charging-Rule-Install for conf (priority)
RAA
3.11 AAR-U (UE3) SDP conf
AAA
UE3
3.12 RAR (UE3) Charging-Rule-Install for conf (priority)
RAA

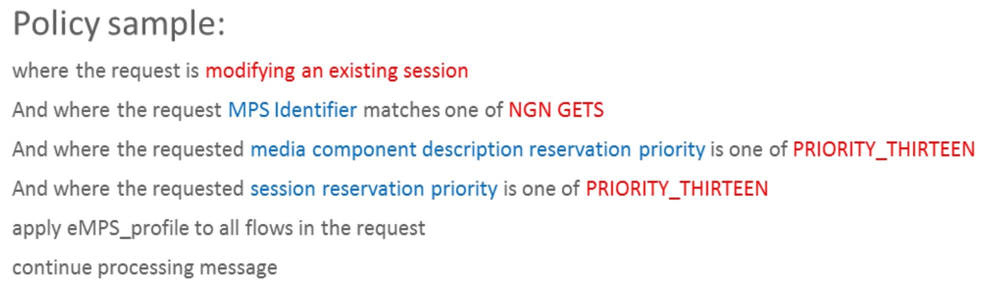
Figure 19 UE says BYE


PCEF
PCRF
P-CSCF1
P-CSCF2
4.1 STR (Rx session in 3.1 for conf)
AAA
RAR (UE1) Charging-Rule-Remove for conf
RAA
4.2 STR (Rx session in 1.3 UE1<->UE2)
AAA
RAR (UE1) Charging-Rule-Remove (UE1<->UE2)
UE1
RAA
4.3 STR (Rx session in 2.2 UE1<->UE3)
DEBQ (non priority)
AAA
RAR (UE1)
Default bearer: Charging-Rule-Install (non priority)
Charging-Rule-Remove (UE1<->UE3)
RAA
4.4 STR (Rx session in 1.6 UE2<->UE1)
DEBQ (non priority)
AAA
UE2
RAR (UE2)
Default bearer: Charging-Rule-Install (non priority)
Charging-Rule-Remove (UE2<->UE1)
RAA
4.5 STR (Rx session in 2.6 UE3<->UE1)
AAA
UE3
DEBQ (non priority)
RAR (UE3)
Default bearer: Charging-Rule-Install (non priority)
Charging-Rule-Remove (UE3<->UE1)
RAA

3.10.2.2 Limitations

In most of the call flows, it’s MPE’s default behavior to automatically upgrade/recover priorities, no policy configuration is needed.

An exception is at step 3.8 of above call flow, the RAR will not automatically trigger dedicated bearer priority upgrade, policy is needed for this step.



Policy sample:

where the request is modifying an existing session

And where the request MPS Identifier matches one of NGN GETS

And where the requested media component description reservation priority is one of PRIORITY_THIRTEEN

And where the requested session reservation priority is one of PRIORITY_THIRTEEN

apply eMPS_profile to all flows in the request

continue processing message

3.11 Sy support for OCS initiated termination and invalid PC (BUG 27176660)

3.11.1 Introduction

Support OCS initiated termination of the Sy session, for use case of customer is removed from the OCS system, or migrated from one OCS system to another OCS system.

3.11.2 Detailed Description

The major enhancements are:

- Sy
  - Supported-Features AVP support new feature ASR (Abort Session Request).
  - Support of SN-Request-Type AVP.
- Policy
  - A new policy condition is added to provide ability to trigger session termination or re-authorization over Gx on receiving OCS initiated session termination request.
- Stats
  - Sy Statistics and Sy peer statistics are added for identifying received OCS initiated session termination request.
  - Support displaying the new stats on CMP page
  - Support querying the new stats from OSSI interface

3.11.2.1 Call Flows

Figure 20 Supported Feature Negotiation of Sy ASR

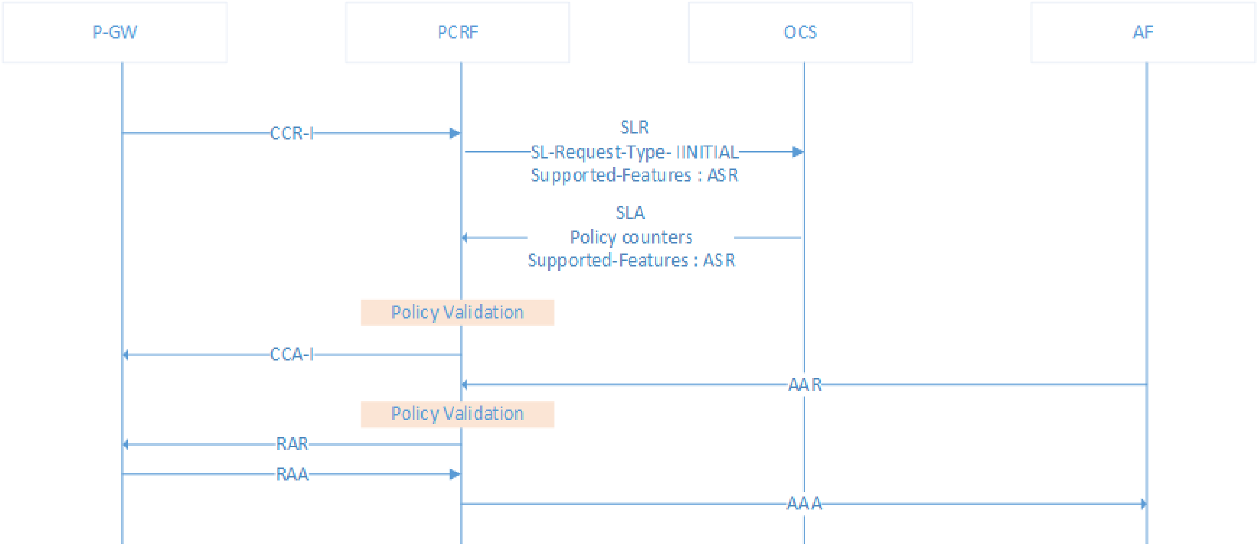
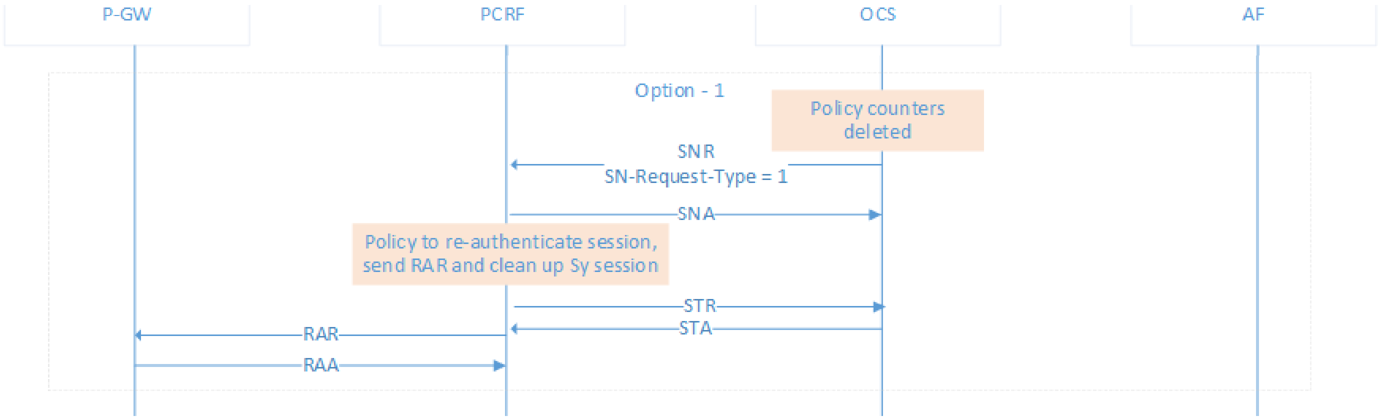


Figure 21 Sy ASR Cause Gx Session Reauthorization



3.11.2.2 Policy Changes

Policy Condition	Description
REASON_SY_SESSION_TERMINATION_BY_OCS	new reason, used when the request is triggered because of the OCS initiated Abort Session Request

3.11.2.3 Stats and OSSI

MPE Stats Name	CMP OSSI Name	CMP	Description
DiameterSyStats.ABORT_SESSION_SNR_RECV_COUNT	<DiameterSyPeerStats> <AbortSessionSNRMessagesReceivedCount/> <DiameterSyPeerStats>	Displayed on the MPE Reports tab, “Diameter Sy Statistics”	Number of Abort Session SNR received by a specific Sy peer connection

MPE Stats Name	CMP OSSI Name	CMP	Description
DiameterSyAdaptorStats.ABORT_SESSION_SNR_RECV_COUNT	<DiameterSyStats> <AbortSessionSNRMessagesReceivedCount/> </DiameterSyStats>	Displayed on the Reports tab, sub page of "Diameter Sy connections".	Number of Abort Session SNR received by PCRF

3.12 Retry of PCRF-Originated Messages: Gx/Rx RAR (BUG 25866138)

3.12.1 Introduction

MRA support re-routing RAR, ASR, TSR to an alternate P-DRA node if the failures are encountered, in case of certain types of error codes (can be configured) in response messages or response timeout.

3.12.2 Feature Activation

This feature is activated if select "Diameter Routing Enh" or "Wireless-C" mode.

3.12.3 Detailed Description

Currently the PCRF does not take any further actions after receiving an error for originated Rx/Gx:RAR messages or if this RAR message times out. This feature will extend MRA routing functionality to support it.

In this feature, MRA will route diameter messages to appropriate destination over configured multiple P-DRAs in active-standby or load-balancing mode and multiple connections in active-standby or load-balancing mode between each P-DRA and MRA.

MRA also shall support PCEF direct connecting to it-self with multiple diameter connections, these direct-connect nodes shall be independent in general, independent means that there is no AS/LB mode to defines their relationship, but the relationship of AS/LB is still applicable in diameter connection level in direct-connect network element scenario.

For MRA initiate diameter request in load-balancing mode, MRA is responsible for the P-DRA selection that based on load balancing arithmetic. Ensuring robustness and reliability of diameter signaling network, MRA should provide its best effort to select an alternate connection or node to route messages when delivering message failure is detected.

MRA is responsible for re-routing requests to an alternate P-DRA connection if the following transport failures are encountered:

- Diameter connection failure
- Diameter connection watchdog failure

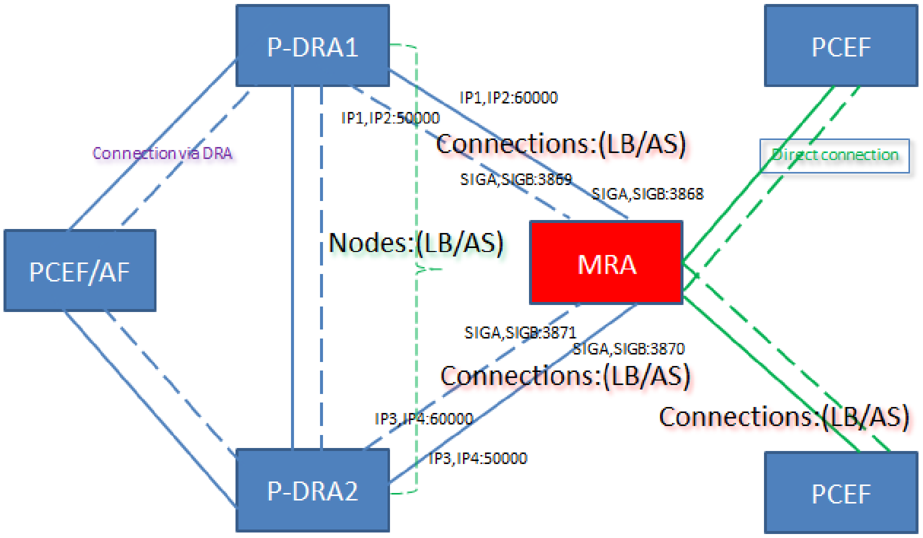
MRA is responsible for re-routing requests to an alternate P-DRA node if the following response failures are encountered:

- Certain types of error codes (can be configured) are received in response messages
- Response timeout

MRA is also enhanced to support Flow Congestion Control Function in order to avoid routing request messages to congested diameter nodes. MRA will control the traffic load to an adjacent P-DRA/PCEF/AF node when receiving a response containing Result-Code AVP with value 3004 (DIAMETER TOO BUSY).

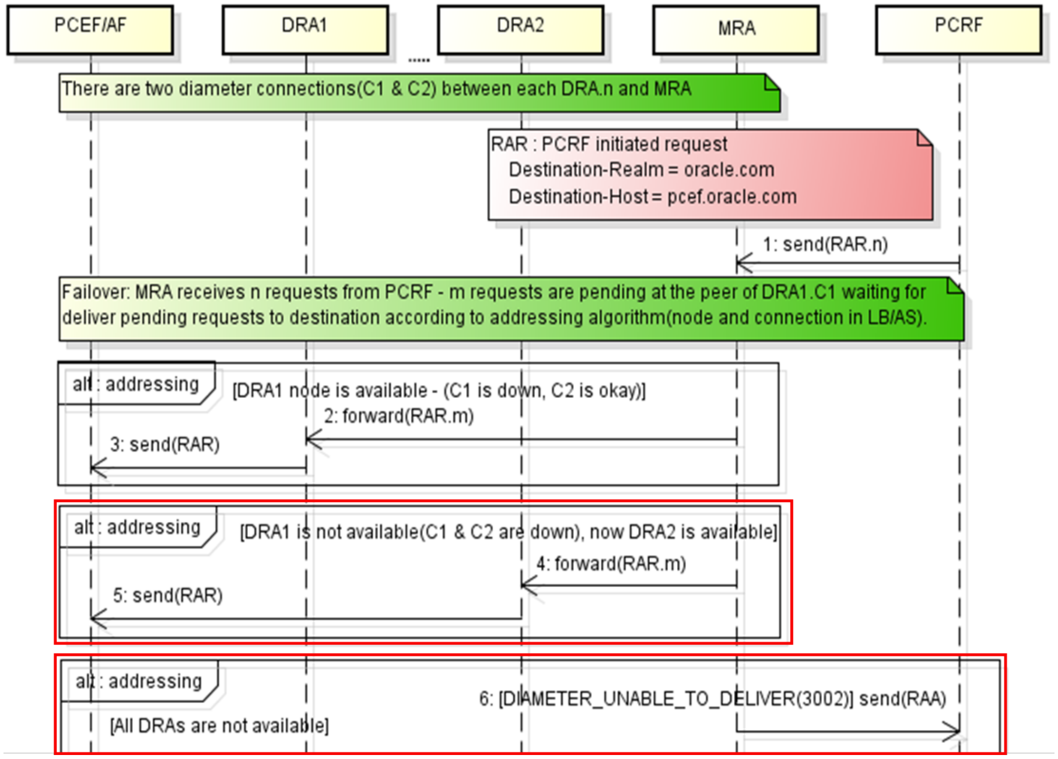
This feature can co-work with existing diameter routing table on MRA. If the selected node in diameter routing table returns preconfigured error codes, the feature will retry the message via other nodes in same peer group.

Figure 22 Diameter routing enhancement for high availability and reliability



3.12.3.1 Call Flows

Figure 23 Routing PCRF originated requests for outbound error handling



There are two diameter connections(C1 & C2) between each DRA.n and MRA

RAR : PCRF initiated request
Destination-Realm = oracle.com
Destination-Host = pcef.oracle.com

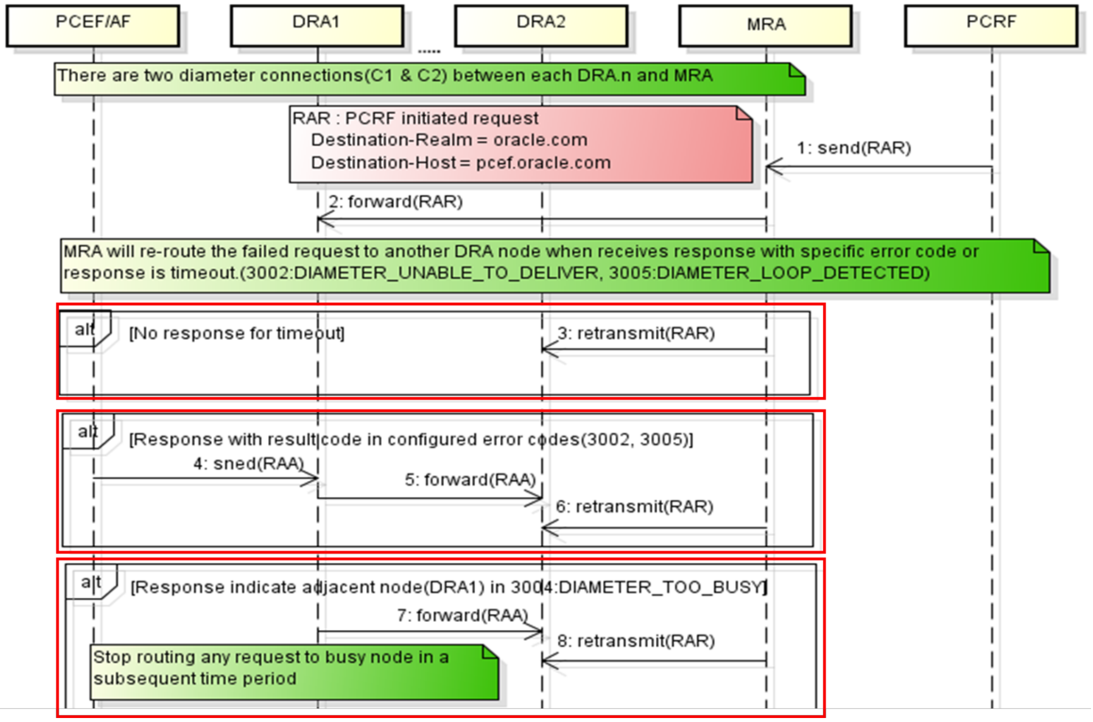
Failover: MRA receives n requests from PCRF - m requests are pending at the peer of DRA1.C1 waiting for deliver pending requests to destination according to addressing algorithm(node and connection in LB/AS).

[DRA1 node is available - (C1 is down, C2 is okay)]

[DRA1 is not available(C1 & C2 are down), now DRA2 is available]

[All DRAs are not available]

Figure 24 Re-routing PCRF originated requests if receiving specific error codes


PCEF/AF
DRA1
.....
DRA2
MRA
PCRF
There are two diameter connections(C1 & C2) between each DRA.n and MRA
RAR : PCRF initiated request
Destination-Realm = oracle.com
Destination-Host = pcef.oracle.com
1: send(RAR)
2: forward(RAR)
MRA will re-route the failed request to another DRA node when receives response with specific error code or response is timeout.(3002:DIAMETER_UNABLE_TO_DELIVER, 3005:DIAMETER_LOOP_DETECTED)
alt
[No response for timeout]
3: retransmit(RAR)
alt
[Response with result code in configured error codes(3002, 3005)]
4: sned(RAA)
5: forward(RAA)
6: retransmit(RAR)
alt
[Response indicate adjacent node(DRA1) in 3004:DIAMETER_TOO_BUSY]
7: forward(RAA)
8: retransmit(RAR)
Stop routing any request to busy node in a subsequent time period

3.12.3.2 User Interface Changes

Figure 25 CMP: Diameter routing enhancement management

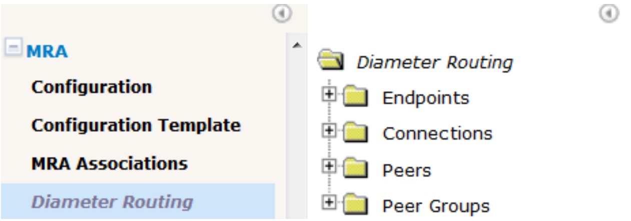
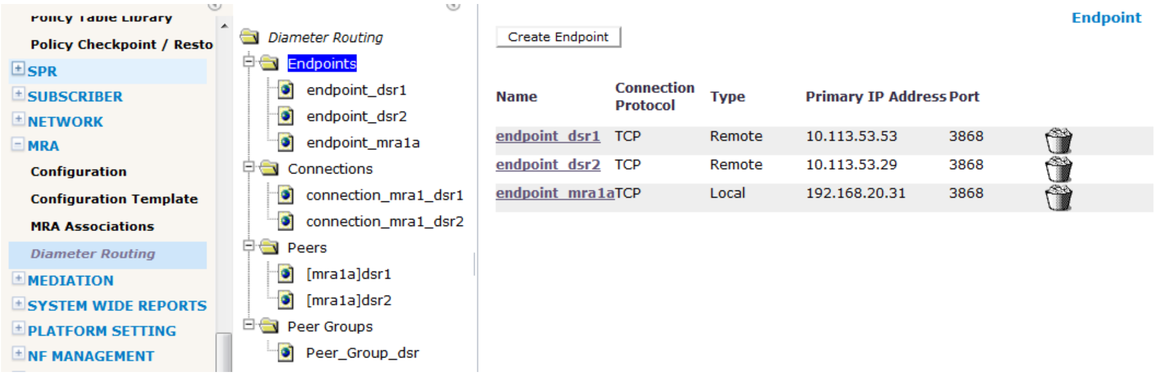
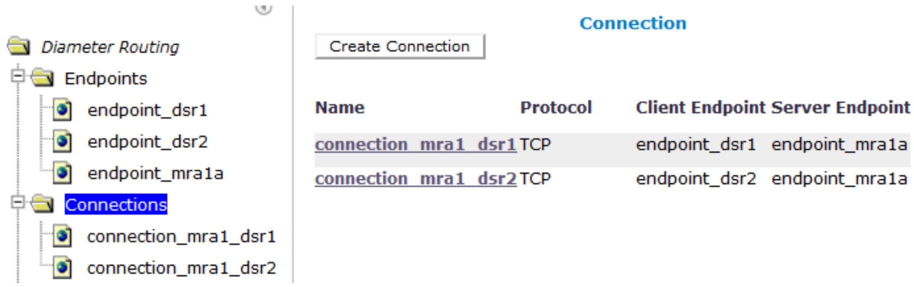


Figure 26 CMP: Diameter routing enhancement: end point management



Name	Connection Protocol	Type	Primary IP Address	Port
endpoint_dsr1	TCP	Remote	10.113.53.53	3868
endpoint_dsr2	TCP	Remote	10.113.53.29	3868
endpoint_mra1a	TCP	Local	192.168.20.31	3868

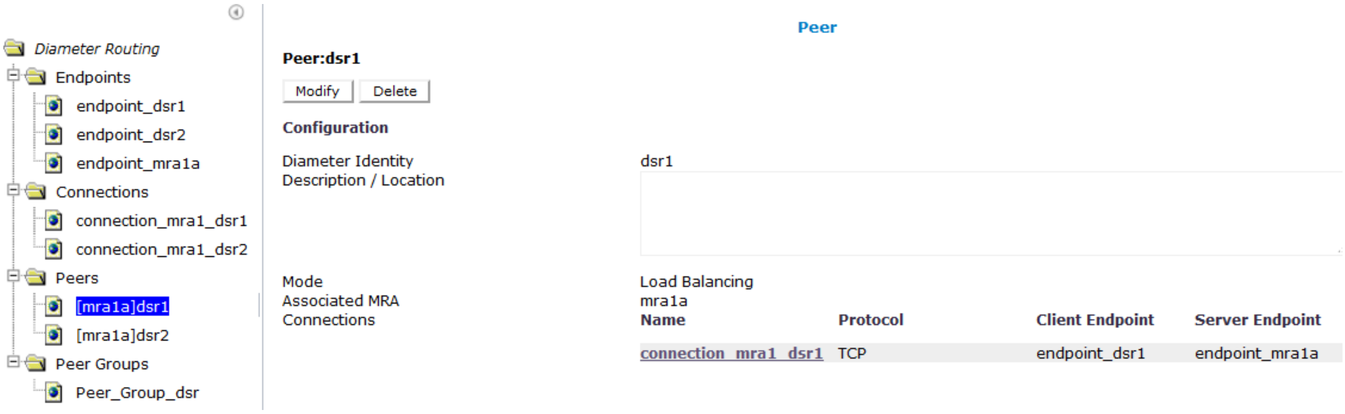
Figure 27 CMP: diameter routing enhancement: connection management



Connection

Name	Protocol	Client Endpoint	Server Endpoint
connection_mra1_dsr1	TCP	endpoint_dsr1	endpoint_mra1a
connection_mra1_dsr2	TCP	endpoint_dsr2	endpoint_mra1a

Figure 28 CMP: diameter routing enhancement: peer management



Peer

Peer:dsr1

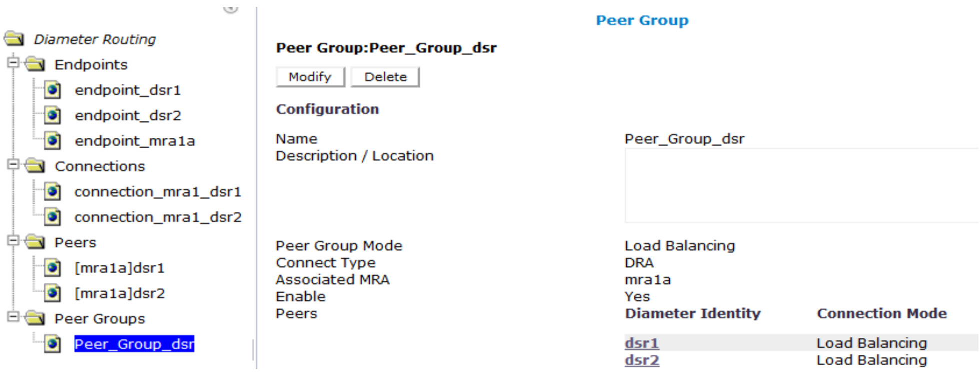
Configuration

Diameter Identity: dsr1
Description / Location:

Mode: Load Balancing
Associated MRA: mra1a
Connections:

Name	Protocol	Client Endpoint	Server Endpoint
connection_mra1_dsr1	TCP	endpoint_dsr1	endpoint_mra1a

Figure 29 CMP: diameter routing enhancement: peer grop management



Peer Group

Peer Group:Peer_Group_dsr

Configuration

Name: Peer_Group_dsr
Description / Location:

Peer Group Mode: Load Balancing
Connect Type: DRA
Associated MRA: mra1a
Enable: Yes
Peers:

Diameter Identity	Connection Mode
dsr1	Load Balancing
dsr2	Load Balancing

3.12.3.3 Trace Logs

Trace Id	Level	Overload Level	Log Message	Example
15152	WARN	INFO	Diameter:Rerouted {0} to {1}({2} attempts) {0}: MessageType [SessionId] {1}: ToPeerId {2}: ReroutingTimes	Diameter:Rerouted RAR [123456789/pcef1.x.com] to dra1.y.com (1 attempts)
15150	WARN		DRA: Rejecting non-authorized {0}, no associate {1} found. {0}: diameter single peer instance	DRA: Rejecting non-authorized DRASinglePeer@6c959674 [identity=pgw1, connection=(SCTP 10.60.56.244:50000 -> 10.60.56.250:3868), dynamic=true,

			{1}: node/connection string	secondary=false, state=R_Open, status=OKAY], no associate node found.

3.13 Match Multiple Table Rows Feature Request (BUG 23214881)

3.13.1 Introduction

Currently Policy Table evaluation results in a single row match.

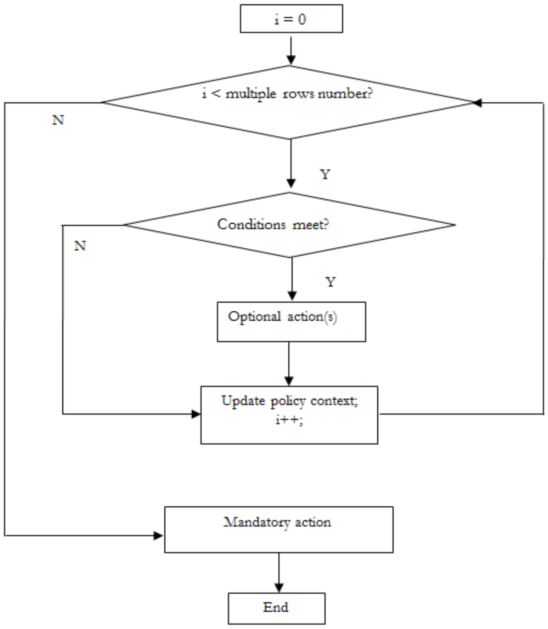
With this enhancement, it allows using a single policy to matching multiple rows in a Policy Table and execute the action associated with each row. This allows the customer to reduce the number of needed policies and reduces the number of rows required in the Policy Table.

3.13.2 Detailed Description

A new policy table association is added to allow select whether return unique row or multiple rows of the policy table.

If multiple policy table rows are matched, the optional actions will be executed for each row. The mandatory action will only be executed once at last.

Figure 30 Work flow: match multiple row



3.13.2.1 Policy Changes

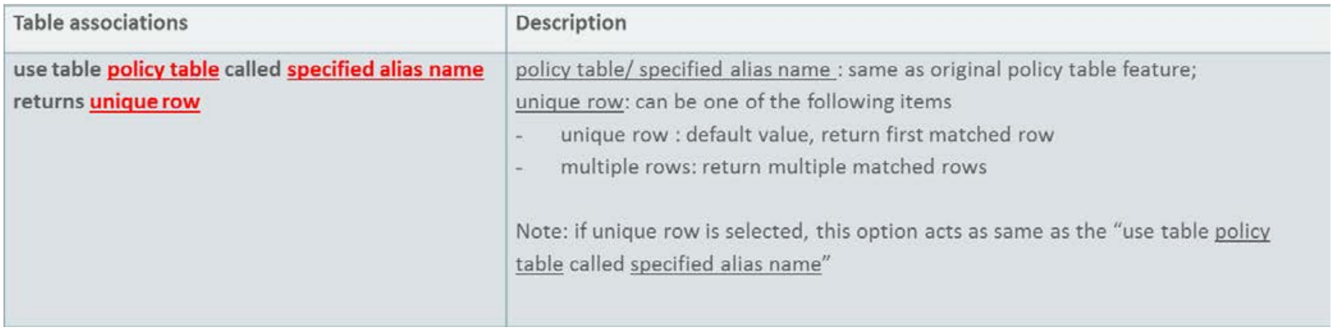
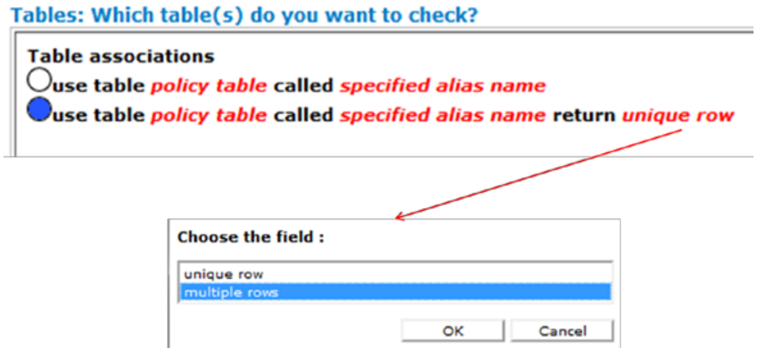


Table associations	Description
use table policy table called specified alias name returns unique row	policy table/ specified alias name : same as original policy table feature; unique row: can be one of the following items - unique row : default value, return first matched row - multiple rows: return multiple matched rows Note: if unique row is selected, this option acts as same as the "use table policy table called specified alias name"

3.13.2.2 User Interface Changes

Figure 31 CMP: policy table association of returning multiple rows



Tables: Which table(s) do you want to check?

Table associations

○ use table *policy table* called *specified alias name*

● use table *policy table* called *specified alias name* return *unique row*

Choose the field :

unique row
multiple rows

3.14 Hotspot Event Trigger (BUG 27918667)

3.14.1 Introduction

This feature is to support CMCC specific Event-Trigger value HOTSPOT_SHARE_START(500), to enable the business requirement to have the special data package target to the users who are using their devices as hotspot to share the WIFI access to others.

3.14.2 Detailed Description

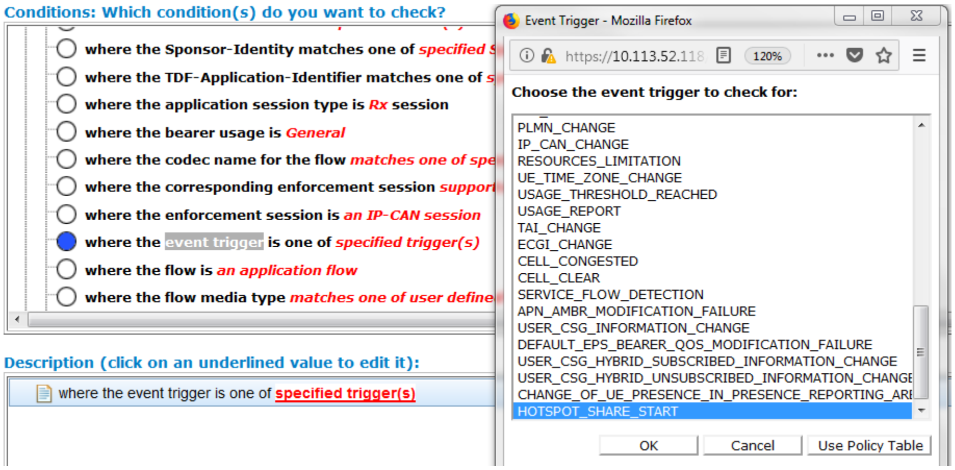
CMCC expect to have the special data package target to the users who are using their devices as hotspot to share the WIFI access to others. A proprietary event trigger is designed HOTSPOT_SHARE_START(500) for Event-Trigger AVP.

HOTSPOT_SHARE_START event trigger can be subscribed by PCRF to PCEF for detecting the users who are using their devices as hotspot to share the WIFI access to others.

HOTSPOT_SHARE_START event trigger can be used to notify from PCEF to PCRF while users are detected to start hotspot sharing for differentiated policy control.

3.14.2.1 User Interface Changes

Figure 32 CMP: policy condition: HOTSPOT_SHARE_EVENT event trigger



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

○ where the Sponsor-Identity matches one of *specified S*

○ where the TDF-Application-Identifier matches one of *s*

○ where the application session type is *Rx* session

○ where the bearer usage is *General*

○ where the codec name for the flow *matches one of spe*

○ where the corresponding enforcement session *support*

○ where the enforcement session is *an IP-CAN session*

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

○ where the flow is *an application flow*

○ where the flow media type *matches one of user define*

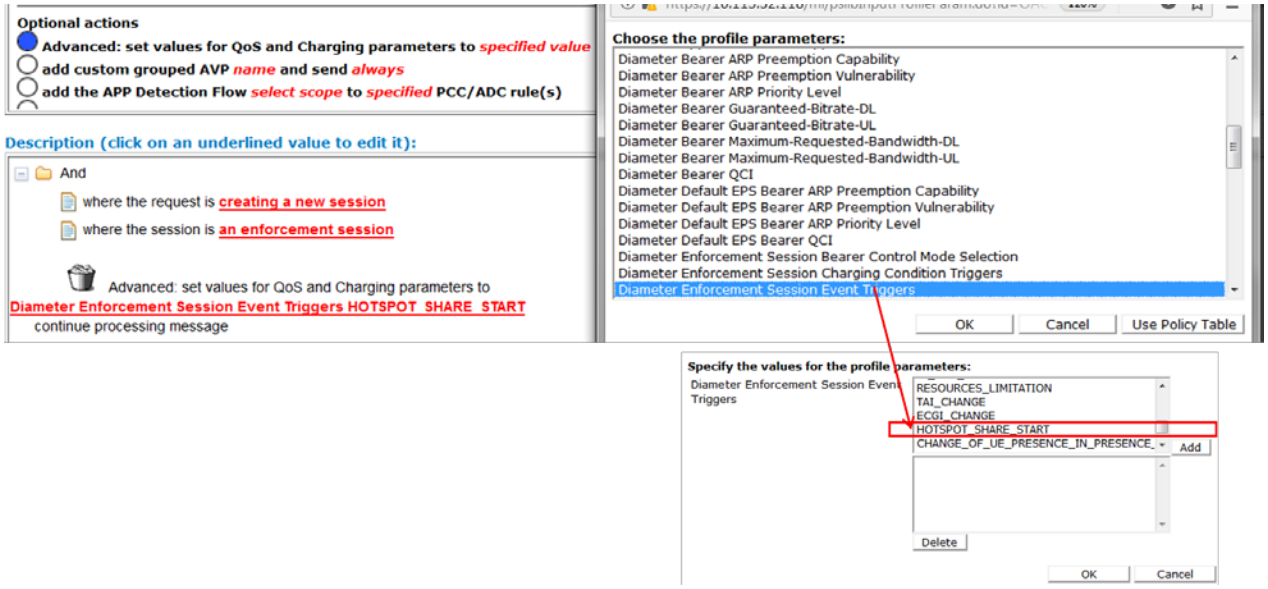
Description (click on an underlined value to edit it):

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

Choose the event trigger to check for:

PLMN_CHANGE
IP_CAN_CHANGE
RESOURCES_LIMITATION
UE_TIME_ZONE_CHANGE
USAGE_THRESHOLD_REACHED
USAGE_REPORT
TAI_CHANGE
ECGI_CHANGE
CELL_CONGESTED
CELL_CLEAR
SERVICE_FLOW_DETECTION
APN_AMBR_MODIFICATION_FAILURE
USER_CSG_INFORMATION_CHANGE
DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE
USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE
USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE
CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_ARE
HOTSPOT_SHARE_START

Figure 33 CMP: policy action: HOTSPOT_SHARE_START event trigger



Optional actions

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

○ add custom grouped AVP *name* and send *always*

○ add the APP Detection Flow *select scope* to *specified* PCC/ADC rule(s)

Description (click on an underlined value to edit it):

And
- where the request is creating a new session
- where the session is an enforcement session

Advanced: set values for QoS and Charging parameters to Diameter Enforcement Session Event Triggers HOTSPOT_SHARE_START
continue processing message

Choose the profile parameters:

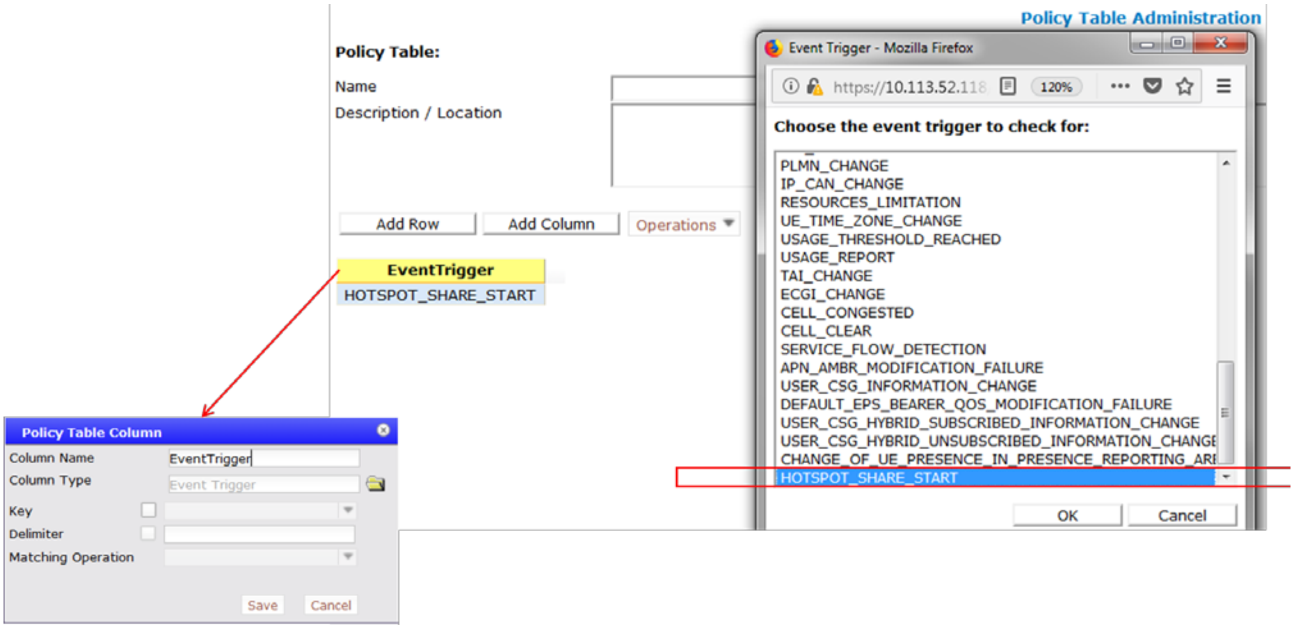
- Diameter Bearer ARP Preemption Capability
- Diameter Bearer ARP Preemption Vulnerability
- Diameter Bearer ARP Priority Level
- Diameter Bearer Guaranteed-Bitrate-DL
- Diameter Bearer Guaranteed-Bitrate-UL
- Diameter Bearer Maximum-Requested-Bandwidth-DL
- Diameter Bearer Maximum-Requested-Bandwidth-UL
- Diameter Bearer QCI
- Diameter Default EPS Bearer ARP Preemption Capability
- Diameter Default EPS Bearer ARP Preemption Vulnerability
- Diameter Default EPS Bearer ARP Priority Level
- Diameter Default EPS Bearer QCI
- Diameter Enforcement Session Bearer Control Mode Selection
- Diameter Enforcement Session Charging Condition Triggers
- Diameter Enforcement Session Event Triggers

Specify the values for the profile parameters:

Diameter Enforcement Session Event Triggers

- RESOURCES_LIMITATION
- TAI_CHANGE
- ECGI_CHANGE
- HOTSPOT_SHARE_START
- CHANGE_OF_UE_PRESENCE_IN_PRESENCE_

Figure 34 CMP: policy table: HOTSPOT_SHARE_START event trigger



Policy Table Administration

Policy Table:

Name

Description / Location

EventTrigger
HOTSPOT_SHARE_START

Policy Table Column

Column Name: EventTrigger

Column Type: Event Trigger

Key □

Delimiter □

Matching Operation

Event Trigger - Mozilla Firefox

https://10.113.52.118 120%

Choose the event trigger to check for:

- PLMN_CHANGE
- IP_CAN_CHANGE
- RESOURCES_LIMITATION
- UE_TIME_ZONE_CHANGE
- USAGE_THRESHOLD_REACHED
- USAGE_REPORT
- TAI_CHANGE
- ECGI_CHANGE
- CELL_CONGESTED
- CELL_CLEAR
- SERVICE_FLOW_DETECTION
- APN_AMBR_MODIFICATION_FAILURE
- USER_CSG_INFORMATION_CHANGE
- DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE
- USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE
- USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE
- CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_ARE
- HOTSPOT_SHARE_START

4. PROTOCOL FLOW/PORT CHANGE

No Changes

5. MEAL INSERTS

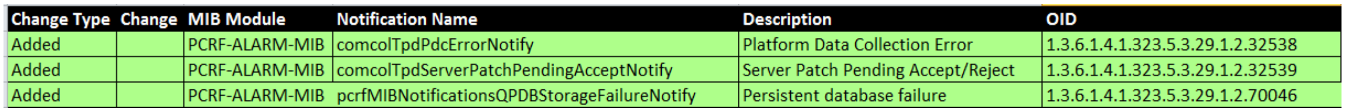
This section will summarize the changes to Alarms, Measurements, KPIs and MIBs. In the following inserts pertain to Oracle Communications Policy Management Release 12.5.0.0.0_63.1.0 MEAL snapshot and deltas to earlier releases 12.3.x/12.4.x to 12.5

The Policy Management GA Release is 12.5.0.0.0_63.1.0

Note: The Policy Product Release: 12.5.0.0.0_63.1.0
Base Distro Product: TPD
Base Distro Release: 7.6.0.0.0_88.54.0

12.3.0.0.0_29.1.0 = TPD: 7.0.3.0.0_86.46.0
12.3.1.0.0_42.1.0 = TPD: 7.0.3.0.0_86.46.0
12.4.0.0.0_51.1.0 = TPD: 7.5.0.0.0_88.46.0
12.4.1.0.0_22.1.0 = TPD: 7.5.0.0.0_88.46.0

5.1 MEAL Deltas (Policy-12.3.0.0.0_29.1.0 to Policy-12.5.0.0.0_63.1.0)

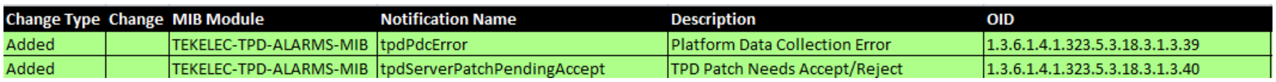


Change Type	Change	MIB Module	Notification Name	Description	OID
Added		PCRF-ALARM-MIB	comcolTpdPdcErrorNotify	Platform Data Collection Error	1.3.6.1.4.1.323.5.3.29.1.2.32538
Added		PCRF-ALARM-MIB	comcolTpdServerPatchPendingAcceptNotify	Server Patch Pending Accept/Reject	1.3.6.1.4.1.323.5.3.29.1.2.32539
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsQPDBStorageFailureNotify	Persistent database failure	1.3.6.1.4.1.323.5.3.29.1.2.70046

The MEAL spreadsheets can be found on the Policy Management Release 12.5 documentation page. All the files are contained in a downloadable .zip file.

- MEAL Deltas (Policy-12.4.0.0.0_51.1.0 to Policy-12.5.0.0.0_63.1.0)
  - File name: MEAL_Policy-12.4.0.0.0_51.1.0-12.5.0.0.0_63.1.0
- MEAL Snapshot: Policy-12.4.0.0.0_51.1.0
  - File name: MEAL_Policy-12.4.0.0.0_51.1.0.xlsx
- MEAL Snapshot: Policy-12.5.0.0.0_63.1.0
  - File name: MEAL_Policy-12.5.0.0.0_63.1.0.xlsx
- DELTA of TPD Changes from Policy 12.3.x/12.4.x to 12.5.x

  MEAL_tpd-7.0.3.0.0_88.46.0-tpd-7.6.0.0.0_88.54.0



Change Type	Change	MIB Module	Notification Name	Description	OID
Added		TEKELEC-TPD-ALARMS-MIB	tpdPdcError	Platform Data Collection Error	1.3.6.1.4.1.323.5.3.18.3.1.3.39
Added		TEKELEC-TPD-ALARMS-MIB	tpdServerPatchPendingAccept	TPD Patch Needs Accept/Reject	1.3.6.1.4.1.323.5.3.18.3.1.3.40

  - File name: MEAL_tpd-7.5.0.0.0.0_88.46.0-tpd-7.6.0.0.0_88.54.0
  - File name: MEAL_tpd-7.5.0.0.0_88.46.0.xlsx
  - File name: MEAL_tpd-7.6.0.0.0_88.54.0.xlsx