Oracle® Communications Policy Management

Network Impact Report

Release 12.1

E78679-01

August 2016

ORACLE

Oracle Communications Policy Management Network Impact Report, Release 12.1

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 PURPOSE AND SCOPE

This document highlights the change(s) in this Release 12.1.1 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 ACRONYMS AND TERMINOLOGY

AAR	Authentication Authorization Request
AVP	Attribute Value Pair
CALEA	Communications Assistance for Law Enforcement Act.
CMP	Configuration Management Platform
CMP	Configuration Management Platform
DC	Designated Coordinator
DRA	Diameter Routing Agent
DSR	Diameter Signaling Router
DTMF	Dual Tone Multi Frequency
FRS	Feature Requirements Specification
Gen6, Gen7, Gen8	Refers to the generation of HP server hardware.
HA	High Availability
H-PCRF	Home PCRF or Home MPE
HSS	Home Subscriber Server
HW	Hardware
IMS	IP Multimedia Subsystem

IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Network
LI	Lawful Intercept
LIMF	Lawful Intercept Mediation Function
LVM	Logical Volume Manager
MP	Message Processor
MPE	Oracle Multimedia Policy Engine
MRA	Multiprotocol Routing Agent
NOAM	Network OAM
NW-CMP	Network Configuration management platform
OAM	Operations, Administration, Maintenance
ORACLE COMMUNICATIONS POLICY MANAGEMENT	Oracle Communications Policy Management
OCUDR	Oracle Communications User Data Repository
OCS	On Line Charging System
PC	Policy Counter
PCC	Policy & Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function – Oracle MPE
PTT	Push To Talk
PDN	Packet Data Network
PGW	Packet Gateway
RMS	Rack Mount Server
S-CMP	System-level Configuration Management Platform
SDP	Session Description Protocol

SLA	Spending-Limit-Answer
SLDB	Sliced Database
SLR	Spending-Limit-Request
SNA	Spending-Status-Notification-Answer
SNR	Spending-Status-Notification-Request
SOAM	System-level OAM
SPR	Subscriber Profile Repository
SSDP	Subscriber State Data Preservation
STA	Session-Termination-Answer
STR	Session-Termination-Request
Sy	3GPP Diameter based protocol interface between PCRF and OCS
TPD	Tekelec Platform Distribution
UE	User Equipment
VLAN	Virtual Local Area Network
V-PCRF	Visited PCRF or Visited MPE
WAN	Wide Area Network

2.0 GENERAL DESCRIPTION

2.1 OVERVIEW OF PCRF RELEASE 12.1.1

Here are the new supported features and enhancements -

PR/ Feature	Feature Name
19604262	Policy Support for Platform R7.0.1
19526105	Merge Policy R12.0 and Policy R11.5 into Policy R12.1.1
19526151	X5-2 Server RMS Support
238263/19526129	HP Gen 9 Server Compatibility
20416820	Update 3rd Party Software in Policy R12.1.1
20416896	Remove any 3rd Party non-standard Oracle SW in Policy R12.1.1
20416936	Update Oracle Software to Most Recent SW Versions in Policy R12.1.1.
19108339	Default passwords are not allowed
19116595	[241663][SEC] RHSA-2014-0625: openssl security update
19105229	[217641][SEC] HTTP Server Prone To Slow Denial Of Service Attack
18982430	CVE-2014-0224 ETC, MULTIPLE SECURITY BUGS - UPGRADE OPENSSL
21028386	IPv4 to IPv6 Migration Procedures from R12.0
19525928	R12.1.1 Upgrade FRS for ROW
19671551	3GPP Recommended Updates for Policy R12.1.1
19117050	Policy VM benchmarking/scaling w OVM/ OVM-M on Sun X5-2
19112895	Policy OVM/OVM-M support on Multiple HW Platforms
19112897	Policy VMWare/vCloud Director support on Multiple HW Platforms
20372474	Policy Software Lab and PoC Support for KVM/Openstack
19525974	R12.1.1 Verizon Wireless Reference Architecture
19359794	Entry Level Policy Solution on RMS
19481792	6.118 AN_GW FAILED Reporting to PCRF and P-CSCF
19526026	R12.1.1 ROW Reference Architecture
19481773	6.105 Maintain Session Uniqueness and Avoid Stale Message Processing
19481824	6.102 Diameter Overload Indication Conveyance (DOIC/DOCME) Phase 1

19867237	6.103 Prevent Message Storm Caused by DST
19867204	6.109 Support Rx Interface for 4G PTT Plus
19229408	Recapture of IPv4 Addresses
19982653	Generic Notification for Policy System
19117512	Checksum to verify import/export operations
19117516	Policy Implementation Standardization Using Templates and XML Consolidation
19153045	Bulk import/export
19482447	Sy reconciliation
19525912	R12.1.1 Upgrade FRS for VzW from R12.0
19959369	Split Platform Management Subnet Support for Platform R7.0.x
20386371	Incompatibility between ML OAM and Check Pointing
19117544	Reevaluate auto-generated rules on CCR-U/ Gp Identification of Default Bearer
19117519	Traffic Profile “Advanced Set” Enhancements
19117734	Retry Profile Enhancement
19117508	Enhance 'Validate' button for policy table
19493618	Message sending option for all members of pool
20631688	Generic Notification from Policy System
19530064	Policy R12.1.1 3GPP SoC Documents Update
20078837	PCRF 3GPP S9 Support
19623928	Sh Retry After Sh Timeout(Synchronous)
19720453	eMPS SPR-Triggered Cases
19720586	Binding updates for Emergency APN
19720493	3GPP R11.14 and R12 NetLoc Changes
19118083	Add support for ADC over Gx
19117477	Binding on IP-Domain-Id
19720631	Trusted WLAN Access
19867434	New NetLoc Procedures for Trusted WLAN
20352083	Support of Host Based Diameter Routing in the PCRF
20416995	Policy End User Installation, Upgrade, Rollback documents for Policy R12.1.1

20366861	Policy End User Installation and Backout Documentation for Policy R12.1.1 for the different Hypervisors and Cloud Management Systems Supported in Policy R12.1.1
20482571	R12.1.1 Early Access Software Availability for Verizon Wireless for Performance Demo and Production Testing/IOT
20482680	R12.1.1 Early Access Software Availability for OVM installation and support at one wireless Carrier for production testing
20482728	R12.1.1 Early Access Software Availability for VMWare installation and support at one wireless Carrier for production testing
20482786	R12.1.1 Early Access Software Availability for KVM/Openstack installation and support at one wireless Carrier for lab demonstration
20222796	Metering method of EVENT is missing from traffic profile and charging rule
20883677	Support vSRVCC
19867575	3GPP P-CSCF Restoration Procedures (3GPP R12)
20611122	Support for Policy R12.1.1 On Line Help
19958628	Non-Netra Haswell-based Sun Product Support
239642 / 19117005	Harvest IPV4 Addresses After Migration to IPv6
239461	IPv6 Serviceability Features
235915/19112161	Platform Virtualization Support for OVM-S
226808/19100514	Platform Virtualization Support for VMWare ESXi
219854/19108339	Customer Changeable default account passwords
217641	[SEC] HTTP Server prone to slow Denial of Service Attack
238699	Notification to Application Once Split Brain Resolved

2.1.1 Merge Policy R12.0 and Policy R11.5 Software into Policy R12.1.1 (BUG 19526105)

Policy R12.1.1 has all of the features and functions of Policy R 11.5 and Policy R12.0 regression tested and the features and functions of Policy R12.1.1 tested.

2.2 PCRF HARDWARE CHANGES

2.2.1 Hardware Support

- Oracle X5-2 SUN non-Netra servers on Rack Mount Servers (RMS).
- HP G9 server
- PP-5160 servers will not be supported in thisRelease.

2.2.2 Entry level Policy Solution on Rack Mount Servers (RMS) (BUG 19359794)

PR 19359794 - Policy in a box Solution for OVM/KVM on a RMS - benchmarked only w/ OVM/Enterprise Manager x5-2 (CMP, MPE, PFE)

This feature is intended to meet several goals:

- Provide a product deployment architecture in support of small fixed/wireless customers
- Provide small scale fixed/wireless Policy system that could be used for trials in a customer's lab
- Provide small scale Cable Policy system (outside the scope of this document) that could be used for trials in a customer's lab

The proposed deployment would result in installing an entire Policy system, CMP, MRA, and 2 MPEs, on a single RMS server with another set of policy components running on another RMS serving as a standby component, Thus, the minimum basic Policy system configuration would require only a single RMS and a HA Policy system would require 2 RMS.

2.2.3 Hardware Upgrade

The Policy Release 12.1.1 software upgrade can be applied on any server that previously had Policy Release 11.5 or Release 12.0

2.3 PCRF SOFTWARE CHANGES

2.3.1 Software Components

Platform Release 7.0.2 inherits all functionalities of Release 6.7. Platform 7.0.2 only supports Internet Explorer browser version 8 and newer.

Component	7.0.2 Release	Compatibility
TPD 64 Bit	7.0.2	FC
COMCOL	6.4.1	FC
PM&C	6.0.1	FC
Networking	6.0.1	FC
HP Firmware FUP	2.2.8 (Minimum1)	FC
Oracle X3-2 Firmware	3.1.2 (Minimum2)	FC
Oracle X5-2 Firmware	Latest X5-2 firmware	FC
TVOE	3.0.0.0.0-86.14.0	FC

FC-Fully Compatible; PC-Partially Comptible

2.4 PCRF UPGRADE/BACKOUT OVERVIEW (PR 233969)

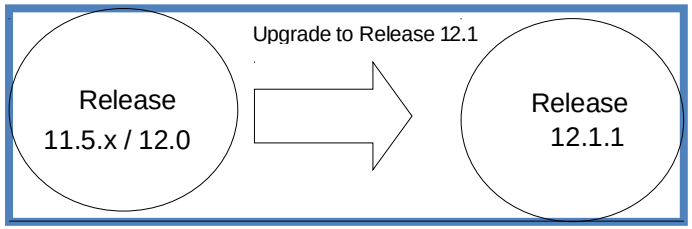
During the Policy Solution upgrade that does not require replacement of the existing hardware, a number of issues were encountered in past versions related to mixed version configuration. The mixed-version PCRF system is a system that includes a CMP and PCRF servers (MRAs and MPEs) that are running different software versions.

In Release 11.5, both Cable and Fixed/Mobile customers/deployments are using the same software release for the first time, though in distinct "modes". Upgrade requirements are generally treated as applying to either deployment mode, while details specific to a given mode (unique features or components) will be called out below (e.g. component upgrade orders). It is expected that upgrade testing will be performed only in Fixed/Mobile mode in Release 11.5->12.1.1 upgrade, as Release 12.1.1 is not planned to support Cable mode deployments.

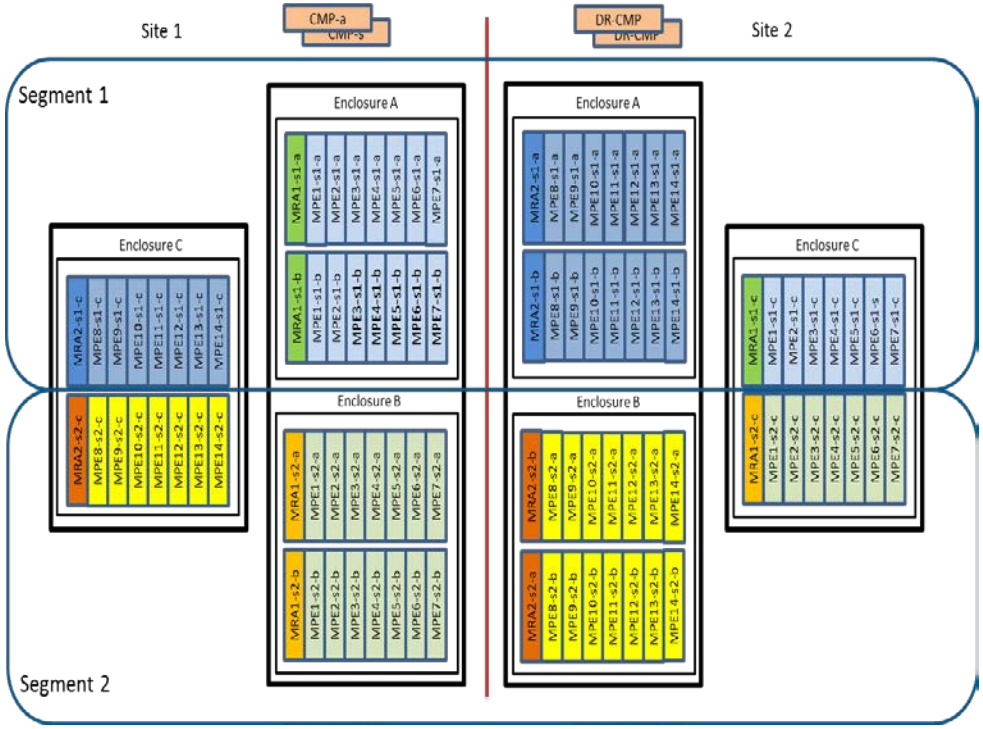
2.4.1 Supported Software Upgrade Path for Release 12.1.1

PCRF upgrade/backout overview (PR 233969)

Figure below shows the supported upgarde Path for Release 12.1.1



The Geo-Redundancy implemented in the MPE and the MRA is using the 2+1 server cluster scheme. The 2 refers to the current 'Active & Standby' servers and the +1 refers to the third 'Spare' server. This 'Spare' server added into the same cluster such that any server can assume the Active role if necessary. 'Spare' server is located in a separate geographical location such that if the two servers at one site were to be unavailable due to site-wide failure, it would likely be unaffected by those same circumstances and be able to continue to provide service as an 'Active' server, as generally illustrated



2.4.2 PCRF System Upgrade Sequence

When considering the approach to changing a mixed-version system, there are two ways that a segment can be upgraded, depending on whether it is part of the initial software evaluation (the FOA) or whether it is part of the upgrade after the FOA period. The goal of the FOA upgrade procedure is to provide time to prove the new version of the software works without unexpected issues.

The goal of the "regular" upgrade procedure is to upgrade the PCRF system to the latest version of the software after it has been proven as efficiently and quickly as possible.

2.4.2.1 Upgrade sequence for an FOA segment

In Fixed/Wireless mode, the upgrade of PCRF system from Release N to Release N+1 shall be executed in the following sequence:

1. Upgrade active CMP
2. Upgrade DR-CMP if present
3. Select an MRA and group of associated MPEs for initial upgrade (up to 4 servers simultaneously)
   A. Upgrade one of the MPEs, if desired
   B. Upgrade the remaining MPEs

C. Upgrade the MRA
4. Upgrade additional MRAs and associated MPEs by repeating steps 3.a. to 3.c.
5. Accept Upgrade

The geo-redundant CMP clusters (active CMP and DR-CMP) shall be upgraded from Release N to Release N+1 prior to executing upgrade on any other server of the system.

In the case that component-level upgrades are backed out due to an issue with the Release N+1 software, the reverse of the above order must be applied.

Note: This upgrade sequence assumes that SPR has been previously upgraded to the latest supported version of SDM/SPR Release 9.3 or OCUDR Release 10.0 or 10.2.

Note: This sequence may be spread through multiple maintenance windows over an extended time period, with periods of "normal" operation in mixed-mode between windows. An upgrade process during FOA in particular may involve "soak test" timing between process steps.

2.4.2.2 Mixed Version PCRF system expectations

The system that is running Release 11.5 / Release 12.0 and Release 12.1.1 mixed configuration supports the performance and capacity of Release 11.5 / Release 12.0 respectively. The mixed version PCRF configuration supports Release 11.5 / Release 12.0 features respectively.

In the mixed version PCRF configuration Release 12.1.1 CMP has the following 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.

- As a general guideline, 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 could be installed, but should be jointly reviewed by the customer and Oracle before deployment to verify that these policies indeed 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:
  i) Network Elements can be added.
  ii) Advanced Configuration settings that were valid for 11.5 may be changed.

- *Note: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP from Release 11.5 / Release 12.0 to Release 12.1.1. The replication is automatically enabled once both active CMP and DR-CMP are upgraded to Release 12.1.1*

PCRF Components	CMP R12.1.1	MRA R12.1.1	MPE R12.1.1
CMP R11.5 / R12.0	No	No	No
MRA R11.5 / R12.0	Yes	Yes	Yes
MPE R11.5 / R12.0	Yes	Yes	N/A

2.4.3 Release 11.5 / Release 12.0 Backout Support & Limitations

- Once MPE, MRA, and CMP servers are upgraded to Release 12.1.1, customer(s) may decide that a backout to the previous release is required. In that case, each individual server has to 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 MRA or MPE servers are rolled back first before the active CMP and DR-CMP can be rolled back to the previous version.

- Once 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. E.g. if all of the servers in the PCRF system were backed out from Release 12.1.1-Build_A to Release 11.5 / Release 12.0, these servers could subsequently be upgraded to Release 12.1.1-Build_B.

Backout may be performed at any time after the upgrade, with the following limitations:

- As stated earlier, once the "**Accept Upgrade**" operation has been performed then backout to the previous release is no longer supported.
- If any new features have been enabled, they 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) for the customer.
- Note: Although backout after new feature activation is allowed, due to the number of possible permutations under which new features may be activated, the only testing that will be performed will be based on backout without new feature activation.
- One additional restriction of backout is that it 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 a re-build of Release 12.1.1.

2.4.4 Upgrade Director

Since the Release 12.1.1 CMP will include the "Upgrade Director" functionality, it should be possible to initially upgrade the CMP using pre-Upgrade Director methods, but then manage the upgrade of all other components using the Release 12.1.1 Upgrade Director in the updated CMP. Whether and how this methodology is used, and how it should be tested, is left for description in the related Feature Description (FD) and Test Plan (TP) documents for 11.5->12.1.1 Upgrade. Ideally, the same techniques would be used for 11.5->12.1.1 as are earlier used for 11.1->12.0.

As for Upgrade path from Release 12.0 to Release 12.1.1, the Upgrade Director functionality already existed in both releases, so just strictly following Upgrade/Rollback prcodecure outlined in the Feature description (FD).

2.5 MIGRATION OF POLICIES AND SUPPORTING POLICY DATA

As in prior releases, the existing Policies configuration and Subscriber Session information will be conserved during the upgrade.

3.0 CHANGES BY FEATURE

3.1 EMPS SPR-TRIGGERED CASES (BUG 19720453)

3.1.1 Introduction

Handling of eMPS is expected generally to depend on both Application/Rx and Subscriber Profile/Sh data. While handling of Rx-triggered cases was implemented in an earlier release, the assumption was that any required SPR/Profile data was present before the Rx session was initiated. Since it is also possible for an Sh Notification to occur while an Application/Rx session already exists, specific testing should be performed to make sure eMPS prioritization is applied or removed accordingly.

3.1.2 Detailed Description

The MPE shall support application & removal of eMPS priority controls based on the occurrence of an SPR notification (Sh PNR) which changes Profile data relevant to eMPS.

Testing shall be performed to check application & removal of eMPS priority controls based on the occurrence of an SPR notification (i.e. even if no code change is required compared to previous releases).

The MPE and CMP shall support statistics regarding the usage of eMPS (number of active eMPS calls, etc).

3.2 BINDING UPDATES FOR EMERGENCY APN (BUG 19720586)

3.2.1 Introduction

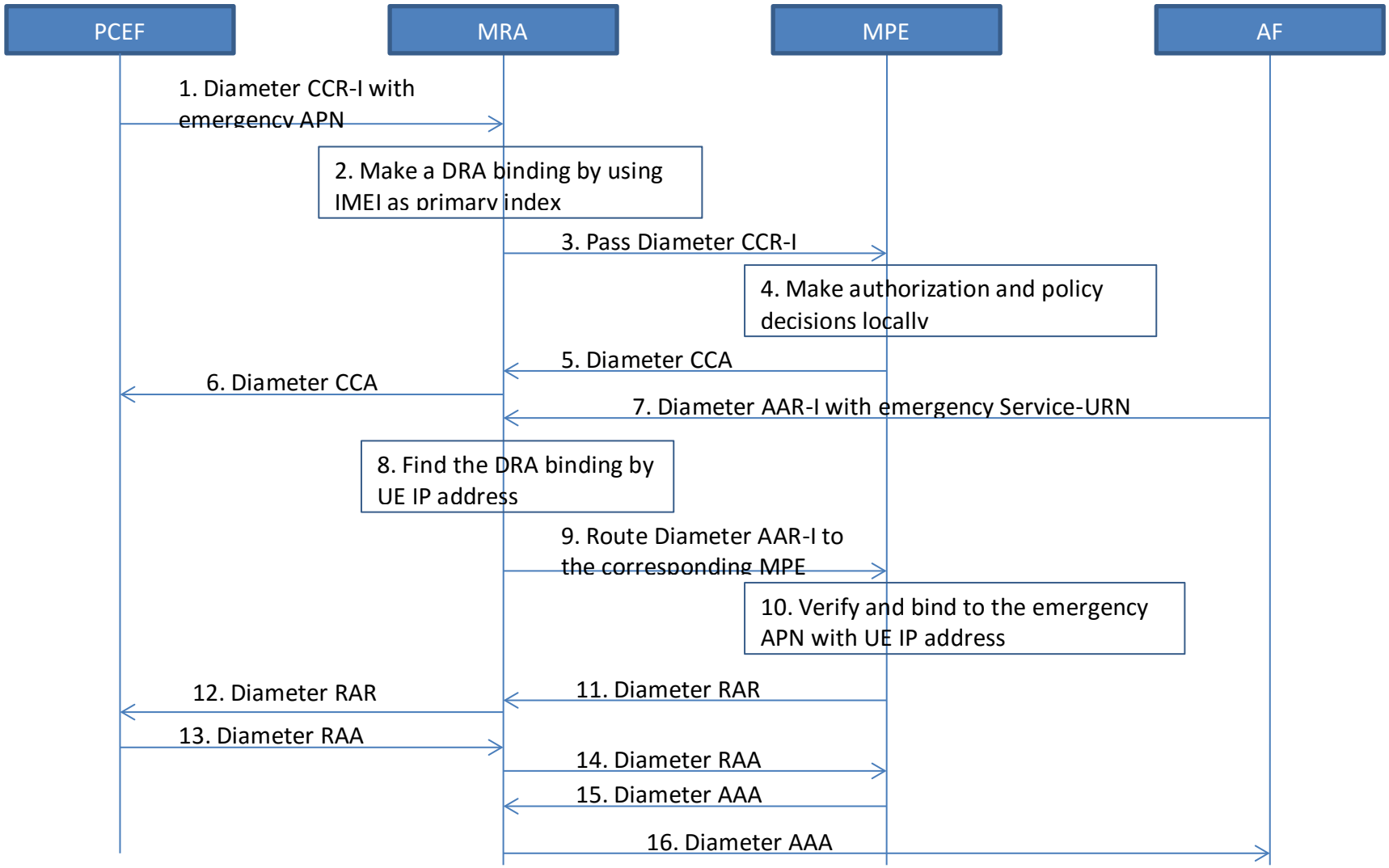
The PCRF shall determine based on the PDN-id if an IP-CAN Session concerns an IMS emergency session. The PCRF shall store a configurable list of Emergency APNs that are valid for the operator to which the PCRF belongs to. For emergency APNs, the IMSI may not be present. The PCRF shall support request for PCC/QoS Rules that do not include an IMSI.

The PCRF shall verify the Service-URN if the IMS service information is associated with a UE IP address belonging to an emergency APN. The PCEF shall store a configurable list of Service-URNs designated for emergency services. If the IMS service information does not contain an emergency related indication and the UE IP address is associated with an emergency APN, the PCRF shall reject the IMS service information provided by the AF.

This feature is available with "Wireless: Diameter 3GPP" mode.

3.2.2 Detailed Description

A setup call flow for emergency APN is depicted as follows:



1. The PCEF sends a CCR command with CC-Request-Type AVP set to value "INITIAL_REQUEST" and the Called-Station-Id AVP including the emergency APN to MRA. The IMSI within Subscription-Id AVP may be included or if not available, the IMEI shall be included within the User-Equipment-Info AVP.

2. The MRA detects the emergency APN by the configurable list and makes a DRA binding by using IMEI as primary index. The IP address will be added as alt key as the same as non-emergency APN if it configured as index in the MRA page.

Note: Here we should not automatically add session Id indexes for DRA binding of emergency session, so if some vendors don't support to send the User-Equipment-Info in the Gx CCR-T message for emergency APN, they will have to configure APN overrides for session Id indexing in the MRA page.

For n-site MRA, the IMEI will be treated as a subscribe indexing for emergency session.

3. The MRA passes the CCR command with emergency APN to MPE.

4. The MPE detects the emergency APN by the configurable list and makes authorization and policy decisions locally, that is the Sp reference point does not apply.

Note: Emergency services are handled locally in the serving network, so the S9 reference point does not apply. And the Sy reference point does not apply either.

5. The MPE sends a CCA command to MRA for emergency service with provisioning PCC rules, DEBQ, APN AMBR(optional), and so on.

6. The MRA sends the CCA command from MPE to PCEF.

7. The AF sends a AAR command with the Service-URN AVP in order to indicate that the new AF session relates to emergency traffic.

8. The MRA finds the DRA binding by UE IP address.

Note: For emergency call, the Rx AAR command will not include any Subscription-Id AVPs, so the Rx shall bind based on IP address which shall be as index in the MRA page.

9. The MRA routes the AAR command to the corresponding MPE.

10. The MPE verifies the Service-URN by the configurable list and binds the Rx session to the emergency APN with UE IP address. If a non-emergency Rx session binding to an emergency APN, the PCRF shall reject the Rx request with experimental result code UNAUTHORIZED_NON_EMERGENCY_SESSION (5066) to AF.

11. The MPE sends a RAR command for the IP-CAN session serving the Rx session to MRA to provide PCC rules.

12. The MRA sends the RAR command from MPE to PCEF.

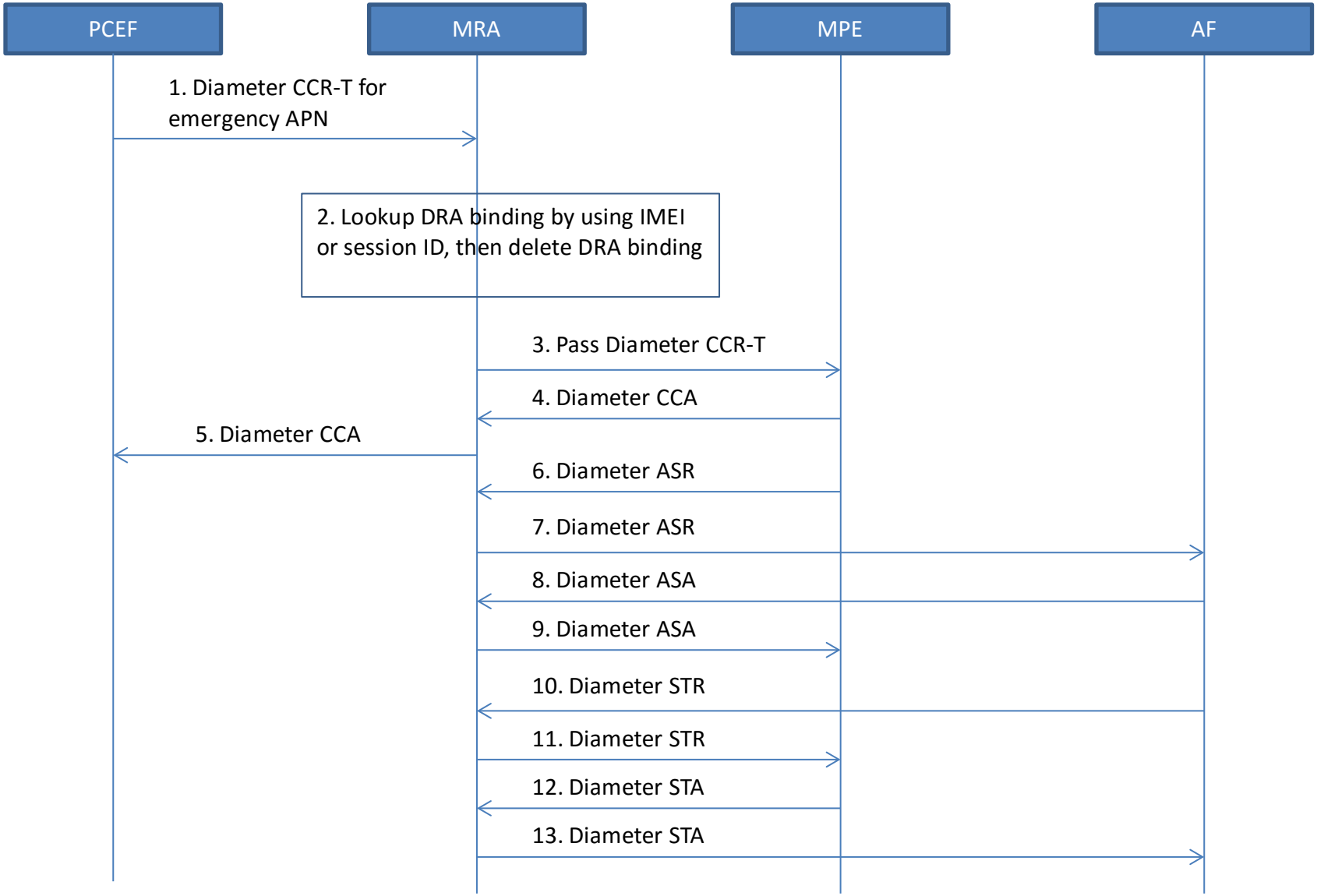
13. The PCEF sends a RAA command to MRA.

14. The MRA sends the RAA command to MPE.

15. The MPE sends a AAA command to AF for the emergency service.

16. The MRA send the AAA command from MPE to AF.

A teardown call flow for emergency APN is depicted as shown in the next page:



1. The PCEF sends a CCR command with CC-Request-Type AVP set to value "TERMINATION _REQUEST" to MRA for emergency APN. The IMEI in User-Equipment-Info AVP may not be within the CCR-T command for some vendors.

2. The MRA lookups the corresponding DRA binding by IMEI if available in the request or by session ID if only session ID found in the request. The DRA binding will be deleted if there isn't any session else related to it.

Note: For n-site MRA, it shall support to lookup the DRA binding by IMEI as index for emergency APN.

3. The MRA passes the CCR command to MPE.

4. The MPE sends a CCA command to MRA.

5. The MRA sends the CCA command from MPE to PCEF.

6. The MPE sends a ASR command to MRA to abort the Rx session.

7. The MRA sends the ASR command from MPE to AF.

8. The AF responds a ASA command to MRA.

9. The MRA sends the ASA command to MPE.

10. The AF sends a STR command to MRA to terminate the Rx session.

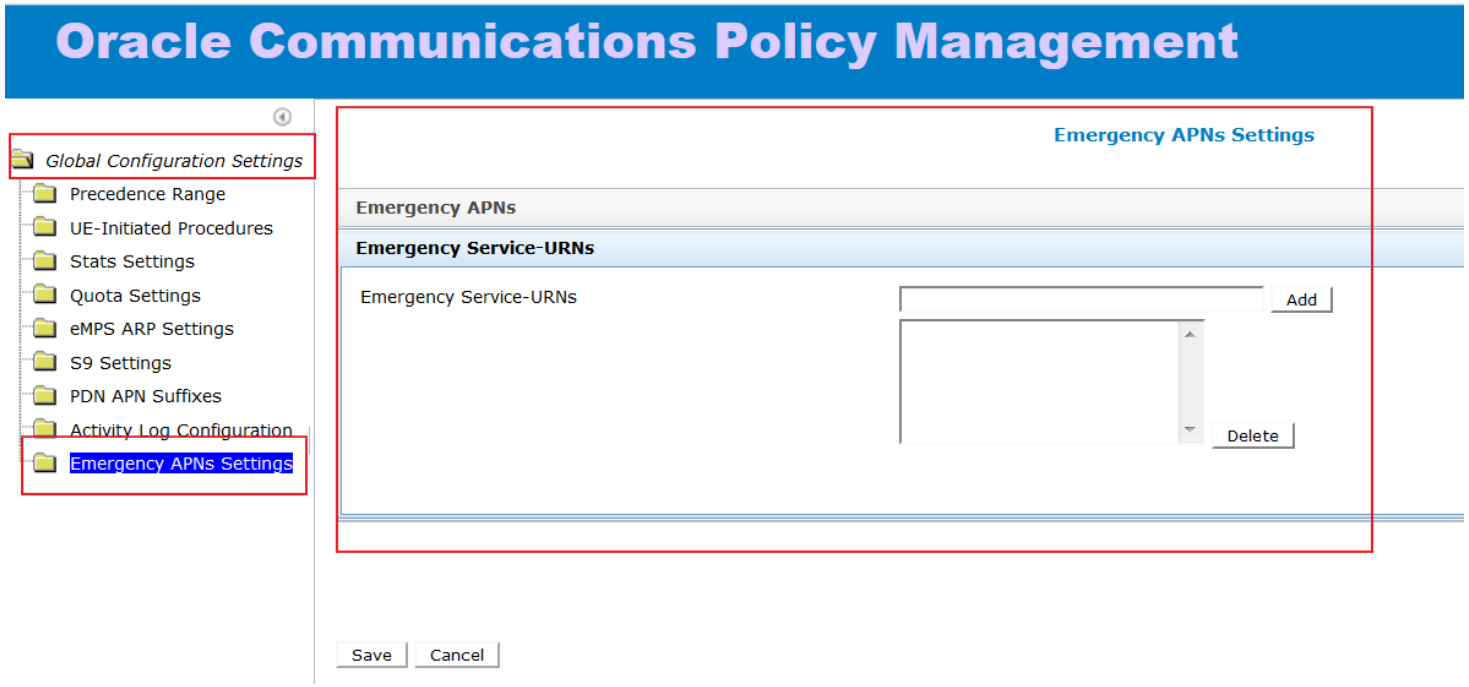
11. The MRA sends the STR command to MPE.

12. The MPE responds a STA command to MRA.

13. The MRA sends the STA command to AF.

3.2.2.1 User Interface Changes

There is a global configuration settings for emergency APN on CMP as follows(the snapshot below is a demo and pay attention to the rectangular selection):



Emergency APNs and Emergency Service-URNs are the lists of APNs and Service-URNs designated for emergency calls/services.

3.3 CUSTOMER CHANGEABLE DEFAULT ACCOUNT PASSWORDS (PR 217641)

Oracle Platform components shall allow the user (customer) to change the password for all built-in, User-Accessible accounts. Changed passwords shall take effect immediately, without requiring the server or services to be restarted. This applies to both operating system accounts and GUI accounts.

Applies To:	TPD	TVOE	AW	PM&C	CC	NET	FWM

- TPD-provided accounts: root, syscheck, platcfg, netbackup, admusr
- TVOE-provided accounts: tvoeadmin, tvoexfer
- PM&C-provided accounts: pmacadmin, pmacop, pmacftpuser, pmacuser
- AppWorks-provided accounts: awadmin, guiadmin, sftpuser

Switch Accounts:

- Switch accounts: HP 6120, HP 6125G, Cisco 3020, Cisco 4948 user accounts. Note that these accounts have user names/passwords that are specified by the user at installation time.

Firmware Management accounts:

- OA: Administrator, root, pmacadmin
- iLO: Administrator, root

Any reliance on fixed passwords by Platform and Application software has been removed. For example, hard-coded passwords used for authentication on machine-to-machine communication using Platform built-in accounts will have to be refactored to remove the dependency on static passwords.

TPD will enforce the same complexity constraints on the root user as those that are configured to be enforced for non-root TPD users. This enforcement will include both compositional and behavioral password constraints.

Platform components shall require users to change the initial password for all newly-created user accounts upon the first login. This requirement applies to GUI-administered accounts only.

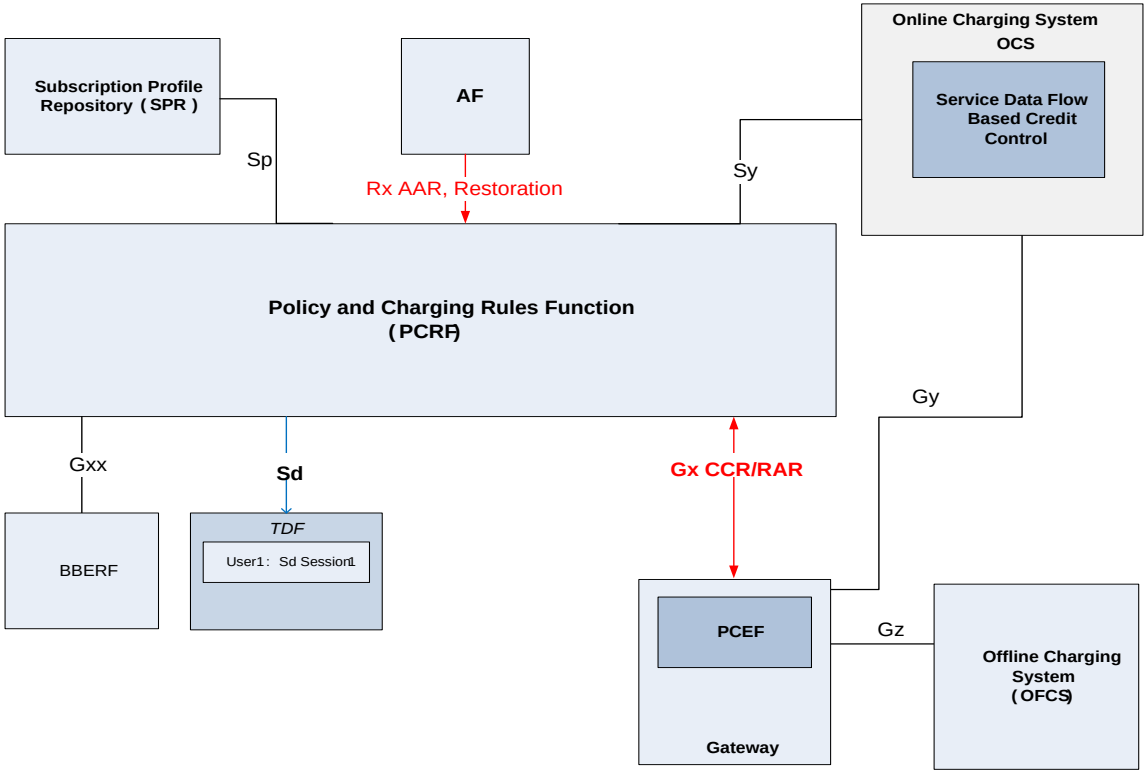
Platform components shall require users to change the password for all user-created, non-operating system accounts when that password has been reset by an administrator. This requirement applies to GUI-administered accounts.

The user shall be required to enter the previous password once and the new password twice when changing the password. This requirement applies for all GUI accounts and operating system accounts that have a login shell.

3.4 3GPP P-CSCF RESTORATION PROCEDURES (3GPP R12) (PR 19867575)

3.4.1 Introduction

This feature describes the support of the IMS-Restoration and the P-CSCF-Restoration procedures of 3GPP TS 23.380 on Gx and Rx. The restoration procedure is initiated in the case of the P-CSCF failure. This describes enhancements to the PCRF to support restoration procedures. The diagram below demonstrates reference of the policy server implementation and the participating components.



3.4.2 Detailed Description

3.4.2.1 3GPP IMS Restoration Procedures PCRF Enhancement

The MRA and MPE support 3GPP IMS Restoration procedures as defined in 3GPP TS 23.380, TS 29.214 Sections 4.4.5a, and TS 29.212 Section 4.5.18. To support IMS restoration procedures first PCRF must support AF signaling flow functionality as described below.

To support IMS restoration procedures Gx PCEF session must negotiate ProvAFsignalFlow supported feature as described in TS 29.212 Section 4.5.18.

Supported Features of Feature-List-ID 1 used in Gx

Feature bit	Feature	M/O	Description
2	ProvAFsignalFlow	O	This feature indicates support for the feature of IMS Restoration as described in TS 29.212 Section 4.5.18. If PCEF supports this feature the PCRF may provision AF signalling IP flow information.

To support IMS restoration procedures Rx request negotiates supported feature ProvAFsignalFlow as described in TS 29.214 Sections 5.4.1.

Supported Features of Feature-List-ID 1 used in Rx

Feature bit	Feature	M/O	Description
2	ProvAFsignalFlow	O	This indicates support for the feature of provisioning of AF signalling flow information as described in TS 29.214 Section 4.4.5a. If the PCRF supports this feature the AF may provision AF signalling flow information. NOTE: This feature is used by the IMS Restoration Procedures to provide to the PDN-Gateway the address of the P-CSCF selected by the UE, refer to 3GPP TS 23.380.

An AF may provision information about the AF signaling IP flows between the UE and the AF. To do so, the AF makes use of an Rx Diameter session already opened with the PCRF if an Rx Diameter session related to the AF signaling is already established. The AF can modify an already open Rx Diameter session related to the AF signaling (e.g. an Rx Diameter session established for the purpose of subscription to notification of signaling path status as described in TS 29.214 4.4.5) or it may open a new Rx Diameter session related to the AF signaling if none exists.

To provision the AF signaling flow information the AF provides the UE's IP address using either Framed-IP-Address AVP or Framed-Ipv6-Prefix AVP. The AF additionally provides a Media-Component-Description AVP including one or more Media-Sub-Component AVP(s) representing the AF signaling IP flows. The Media-Component-Description AVP contains the Media-Component-Number AVP set to "0". Each Media-Sub-Component AVP representing an AF signaling IP flow also contains the Flow-Number AVP and one or two Flow-Description AVP(s) set to the IP flows of the AF signaling. Additionally, the Media-Sub-Component AVP includes the Flow-Usage AVP set to the value "**AF_SIGNALLING**", the Flow-Status AVP set to "ENABLED" and the AF-Signaling-Protocol AVP set to the value corresponding to the signaling protocol used between the UE and the AF.

When the PCRF receives from the AF an AAR message with the signaling flow information, the PCRF performs session binding and acknowledges the AAR command by sending an AAA reply command to the AF.

Note: To support signaling flow release PCRF 12.1.1 extends support for the Flow-Usage AVP by adding a new value AF_SIGNALLING (2). This value is used to indicate that the IP flow is used to transport AF Signaling Protocols.

A new AVP is also supported by PCRF to extend Media-Sub-Component AVP.

The AF-Signalling-Protocol AVP (AVP code 529) is of type Enumerated, and indicates the protocol used for signalling between the UE and the AF.

- NO_INFORMATION (0), this value is used to indicate that no information about the AF signalling protocol is being provided.
- SIP (1), this value is used to indicate that the signalling protocol is Session Initiation Protocol.

Note: If the AF-Signalling-Protocol AVP is not provided in the AA-Request, the value NO_INFORMATION shall be assumed.

The Media-Sub-Component AVP is also extended to comply with the signaling flow type.

AVP format:
Media-Sub-Component ::= < AVP Header: 519 >
{ Flow-Number } ; Ordinal number of the IP flow
0*2[Flow-Description] ; UL and/or DL
[Flow-Status]
[Flow-Usage]
[Max-Requested-Bandwidth-UL]
[Max-Requested-Bandwidth-DL]
[AF-Signalling-Protocol]
*[AVP]

Note: The AF-Signalling-Protocol AVP may be included only if the Flow-Usage AVP has a value of ‘AF_SIGNALLING’.

Example of the Rx AAR message provisioning signaling flow:

Diameter Message: AAR
Version: 1
Msg Length: 484
Cmd Flags: REQ,PXY
Cmd Code: 265
App-Id: 16777236
Hop-By-Hop-Id: 1734614049
End-To-End-Id: 3001180673
Session-Id (263,M,l=36) = pgw.group4.com;1424208550;38

Origin-Host (264,M,l=22) = pgw.group4.com
Origin-Realm (296,M,l=18) = group4.com
Auth-Application-Id (258,M,l=12) = 16777236
Destination-Realm (283,M,l=18) = group4.com
Media-Component-Description (517,VM,v=10415,l=244) =
Media-Component-Number (518,VM,v=10415,l=16) = 0
Media-Sub-Component (519,VM,v=10415,l=152) =
Flow-Number (509,VM,v=10415,l=16) = 0
Flow-Description (507,VM,v=10415,l=51) = permit out ip from 99.2.1.2 6060 to any
Flow-Description (507,VM,v=10415,l=40) = permit in ip from any to any
Flow-Usage (512,VM,v=10415,l=16) = AF_SIGNALLING (2)
AF-Signalling-Protocol (529,VM,v=10415,l=16) = SIP (1)
Flow-Status (511,VM,v=10415,l=16) = ENABLED (2)
Framed-IP-Address (8,M,l=12) = 10.0.0.88
AF-Charging-Identifier (505,VM,v=10415,l=24) = IMS_CHARGING
Specific-Action (513,VM,v=10415,l=16) = INDICATION_OF_FAILED_RESOURCES_ALLOCATION (9)
Supported-Features (628,VM,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) = 4

When the MPE receives an AAR from the P-CSCF which provisions or de-provisions information about signaling flows as defined in TS 29.214 section 4.4.5a, the PCRF installs or removes corresponding Charging-Rule-Definitions by using a Gx RAR on the appropriate enforcement session, as per TS 29.212 section 4.5.18.

In order to support IMS Restoration procedures (refer to 3GPP TS 23.380), PCRF conveys the AF address to the PCEF. In order to do so, in case AF provisions information about the AF signaling flows between the UE and the AF, as defined in 3GPP TS 29.214 Section 4.4.5a, the PCRF installs the corresponding dynamic PCC rules by triggering a Gx RAR message. The PCRF provides the Charging-Rule-Install AVP including the Charging-Rule-Definition AVP(s). The Charging-Rule-Definition AVP includes in the Flow-Information AVP the signaling flows between UE and the AF. The Charging-Rule-Definition AVP also includes the AF-Signalling-Protocol AVP set to the value corresponding to the signaling protocol used between the UE and the AF (SIP for example).

The PCEF acknowledges the command by sending a Gx RAA command to the PCRF and initiates the corresponding bearer procedure if required. In case AF de-provisions information about the AF signaling flows between the UE and the AF, as defined in 3GPP TS 29.214 Section 4.4.5a, the PCRF remove the corresponding dynamic PCC rules by triggering a Gx RAR message. The PCRF provides the Charging-Rule-Remove AVP including the corresponding Charging-Rule-Name AVP(s). The PCEF acknowledges the command by sending a Gx RAA command to the PCRF.

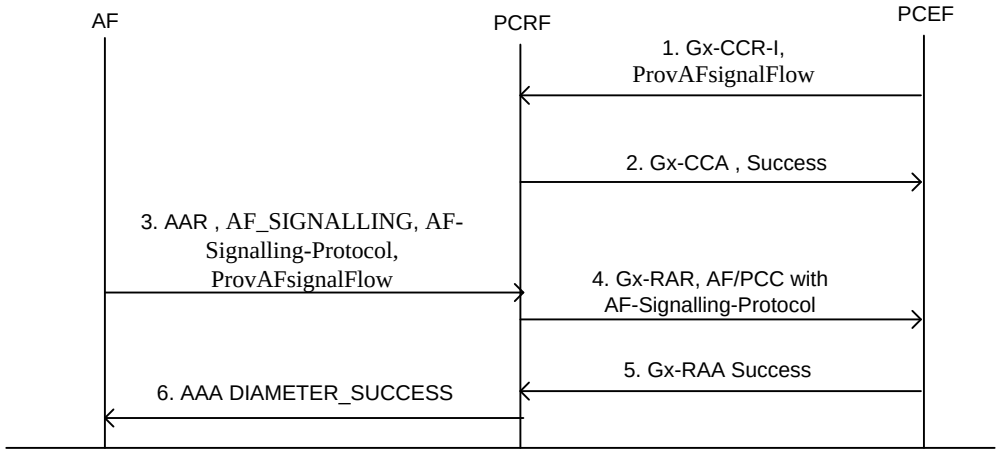
Charging-Rule-Definition AVP extended Format:
Charging-Rule-Definition ::= < AVP Header: 1003 >
{ Charging-Rule-Name }
[Service-Identifier]
[Rating-Group]
*[Flow-Information]
[TDF-Application-Identifier]

[Flow-Status]
[QoS-Information]
[PS-to-CS-Session-Continuity]
[Reporting-Level]
[Online]
[Offline]
[Metering-Method]
[Precedence]
[AF-Charging-Identifier]
*[Flows]
[Monitoring-Key]
[Redirect-Information]
[Mute-Notification]
[AF-Signalling-Protocol]
[Sponsor-Identity]
[Application-Service-Provider-Identity]
*[Required-Access-Info]
*[AVP]

Example of the Gx RAR provisioning signaling AF rule.

```
Diameter Message: RAR
Version: 1
Msg Length: 508
Cmd Flags: REQ,PXY
Cmd Code: 258
App-Id: 16777238
Hop-By-Hop-Id: 448673075
End-To-End-Id: 2254452502
  Session-Id (263,M,l=36) = pgw.group4.com;1424208550;37
  Origin-Host (264,M,l=24) = mpe01.group4.com
  Origin-Realm (296,M,l=18) = group4.com
  Destination-Realm (283,M,l=18) = group4.com
  Destination-Host (293,M,l=22) = pgw.group4.com
  Auth-Application-Id (258,M,l=12) = 16777238
  Re-Auth-Request-Type (285,M,l=12) = AUTHORIZE_ONLY (0)
  Charging-Rule-Install (1001,VM,v=10415,l=340) =
    Charging-Rule-Definition (1003,VM,v=10415,l=328) =
      Charging-Rule-Name (1005,VM,v=10415,l=15) = 0_1
      Flow-Description (507,VM,v=10415,l=51) = permit out ip from 99.2.1.2 6060 to any
      Flow-Description (507,VM,v=10415,l=40) = permit in ip from any to any
      Flow-Status (511,VM,v=10415,l=16) = ENABLED (2)
```

Precedence (1010,VM,v=10415,l=16) = 400
AF-Charging-Identifier (505,VM,v=10415,l=24) = IMS_CHARGING
Flows (510,VM,v=10415,l=44) =
Media-Component-Number (518,VM,v=10415,l=16) = 0
Flow-Number (509,VM,v=10415,l=16) = 0
AF-Signaling-Protocol (529,VM,v=10415,l=16) = SIP (1)



IMS Restoration diagram

1. PCEF Sends Gx CCR-I with the ProvAFsignalFlow supported feature.
2. PCRF replies DIAMETR_SUCCESS
3. AF sends Rx AAR with restoration request as specified in the AF flow and AF-Signalling-Protocol AVP
4. The existing Gx session is locate and a Gx RAR restoration request sent to PCEF with the AF-Signaling-Protocol AVP as a part of the provisioned rule.
5. PCEF replies Gx RAA with DIAMETER_SUCCESS result code.
6. PCRF replies Rx AAA with DIAMETER_SUCCESS result code.

Since the valid lifetime of registration-related Rx sessions may be significantly longer than the expected validity of call-related Rx sessions, the MPE supports a distinct value for stale session cleanup of registration-related sessions for the Rx sessions containing signaling flow. A new configuration value has been introduced in the PCRF release 12.1.1 which is available via CMP expert settings.

DIAMETER.AF.SignallingSessionAuthLifetime

Which is set to the default value 259200 or 3 days as opposed to one day for the regular Rx sessions.

3.4.2.2 3GPP P-CSCF Restoration Procedure PCRF Enhancement

The MPE supports 3GPP P-CSCF Restoration Procedures as defined in 3GPP TS 23.380, TS 29.214 Section 4.4.7, and TS 29.212 Section 4.5.18a. The PCRF-based P-CSCF Restoration Enhancement, as defined in 3GPP TS 23.380, is supported by both P-CSCF and PCRF. The P-CSCF acting as AF sends an AAR command with a P-CSCF Restoration Indication (Rx-Request-Type AVP set to PCSCF_RESTORATION_REQUEST (2)) to the PCRF in the case P-CSCF Restoration needs to be performed. This AAR shall include the following information required by the PCRF to find the corresponding IP-CAN session:

- The UE's IP address as applicable in the Framed-IP-Address AVP or in the Framed-Ipv6-Prefix AVP. If the IP address is not unique (e.g. private IPv4 case), the P-CSCF also includes the IP-Domain-ID AVP if available.
- If the IP address is not available or if the IP address is not unique and the IP-Domain-ID is not available, the P-CSCF includes the IMSI in the Subscription-Id AVP and the APN in the Called-Station-Id AVP.
- AF also sends supported feature PCSCF-Restoration-Enhancement

Features of Feature-List-ID 2 used in Rx

Feature bit	Feature	M/O	Description
0	PCSCF-Restoration-Enhancement	O	This feature indicates support of P-CSCF Restoration Enhancement. It is used for the PCRF and the P-CSCF to indicate if they support P-CSCF Restoration Enhancement.

The AF also includes the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1) in the AAR command, as described in IETF RFC 3588. As a consequence, the PCRF does not create Rx session.

The PCRF acknowledges the AAR command by sending an AAA command to the P-CSCF acting as AF and includes the Auth-Session-State AVP set to NO_STATE_MAINTAINED (1).

Examples of the AAR and AA messages with PCSCF restoration requests:

Diameter Message: AAR
Version: 1
Msg Length: 252
Cmd Flags: REQ,PXY
Cmd Code: 265
App-Id: 16777236
Hop-By-Hop-Id: 570095865
End-To-End-Id: 1762010517
  Session-Id (263,M,l=35) = pgw.group4.com;1424361981;4
  Origin-Host (264,M,l=22) = pgw.group4.com
  Origin-Realm (296,M,l=18) = group4.com
  Auth-Application-Id (258,M,l=12) = 16777236
  Destination-Realm (283,M,l=18) = group4.com
  Framed-IP-Address (8,M,l=12) = 10.0.0.88

AF-Charging-Identifier (505,VM,v=10415,l=24) = IMS_CHARGING
Supported-Features (628,V,v=10415,l=56) =
Vendor-Id (266,M,l=12) = 10415
Feature-List-ID (629,V,v=10415,l=16) = 2
Feature-List (630,V,v=10415,l=16) = 1
Rx-Request-Type (533,V,v=10415,l=16) = PCSCF_RESTORATION_REQUEST (2)
Auth-Session-State (277,M,l=12) = NO_STATE_MAINTAINED (1)

received a reply :
Diameter Message: AAA
Version: 1
Msg Length: 224
Cmd Flags: PXY
Cmd Code: 265
App-Id: 16777236
Hop-By-Hop-Id: 570095865
End-To-End-Id: 1762010517
Session-Id (263,M,l=35) = pgw.group4.com;1424361981;4
Result-Code (268,M,l=12) = DIAMETER_SUCCESS (2001)
Origin-Host (264,M,l=24) = mpe01.group4.com
Origin-Realm (296,M,l=18) = group4.com
Auth-Application-Id (258,M,l=12) = 16777236
Supported-Features (628,V,v=10415,l=56) =
Vendor-Id (266,M,l=12) = 10415
Feature-List-ID (629,V,v=10415,l=16) = 2
Feature-List (630,V,v=10415,l=16) = 1
IP-CAN-Type (1027,VM,v=10415,l=16) = THREEGPP_EPS (5)
RAT-Type-3GPP (21,VM,v=10415,l=13) = EUTRAN(6)
Auth-Session-State (277,M,l=12) = NO_STATE_MAINTAINED (1)

If PCRF negotiated PCSCF-Restoration-Enhancement then PCRF sends a RAR request for P-CSCF Restoration to the PCEF for the corresponding IP-CAN session.

- PCRF also sends supported Gx feature PCSCF-Restoration-Enhancement

Features of Feature-List-ID 1 used in Gx

Feature Bit	Name	M/O	Description
24	PCSCF-Restoration-Enhancement	O	This feature indicates support of P-CSCF Restoration Enhancement. It is used for the PCRF to indicate support of the P-CSCF Restoration Enhancement.

- PCRF also sends PCSCF-Restoration-Indication AVP in Gx RAR to indicate restoration request

PCSCF-Restoration-Indication AVP

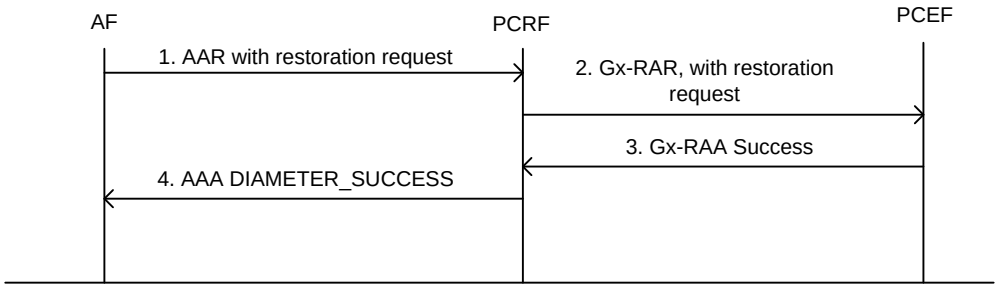
Name	Code	Type							Supported Feature
PCSCF-Restoration-Indication	2826	Unsigned32	V	P		M	Y	All	PCSCF-Restoration-Enhancement

Example of the Gx RAR restoration request:

Diameter Message: RAR
Version: 1
Msg Length: 184
Cmd Flags: REQ,PXY
Cmd Code: 258
App-Id: 16777238
Hop-By-Hop-Id: 4162120445
End-To-End-Id: 2837389268
Session-Id (263,M,l=36) = pgw.group4.com;1424288428;16
Origin-Host (264,M,l=24) = mpe01.group4.com
Origin-Realm (296,M,l=18) = group4.com
Destination-Realm (283,M,l=18) = group4.com
Destination-Host (293,M,l=22) = pgw.group4.com
Auth-Application-Id (258,M,l=12) = 16777238
Re-Auth-Request-Type (285,M,l=12) = AUTHORIZE_ONLY (0)
PCSCF-Restoration-Indication (2826,V,v=10415,l=16) = 0

Upon receipt of an AA-Request from the P-CSCF with a P-CSCF Restoration Indication, the MPE:

- responds to the P-CSCF with an AA-Answer including the Auth-Session-State AVP with a value of NO_STATE_MAINTAINED (1), presuming that the same Auth-Session-State value was in the AA-Request
- determine the IP-CAN session corresponding to the request, using either the provided IP address (Framed-IP-Address or Framed-Ipv6-Prefix AVPs) and IP-Domain-ID AVP (if present), or the IMSI and APN (in Subscription-Id and Called-Station-Id AVPs), and
- Sends a RAR request for P-CSCF Restoration to the corresponding PCEF.



P-CSCF Restoration diagram

1. The stateless Rx AAR with restoration request is received by PCRF
2. The existing Gx session is locate and a Gx RAR restoration request sent to PCEF
3. PCEF replies Gx RAA with DIAMETER_SUCCESS result code.
4. PCRF replies Rx AAA with DIAMETER_SUCCESS result code.

Note: To implement this requirement PCRF release 12.1.1 supports notation of the stateless Rx request, a stateless Rx request create a transient Rx session which is not persisted in the database and purged upon sending AAA response. A stateless Rx request is identified by the presence of the Auth-Session-State AVP with a value of NO_STATE_MAINTAINED (1).

Note: In this particular implementation the stateless Rx request is only serving purpose of the PCSCF restoration procedure.

The main reason this is needed is to support migration from the ext3 file system to the ext4 file system in R12.0. Although TPD supports this even in the versions of TPD we have used for earlier releases (11.x) the customer did not want to migrate to ext4 unless we could provide an ability to back out to ext3 if something went wrong. This can be supported using LVM snapshots.

Thus in R12.0 we would like to support this and have the file system automatically migrated to ext4 during the 12.0 upgrade, but if something goes wrong, we want the ability to return to the prior 11.x release running ext3.

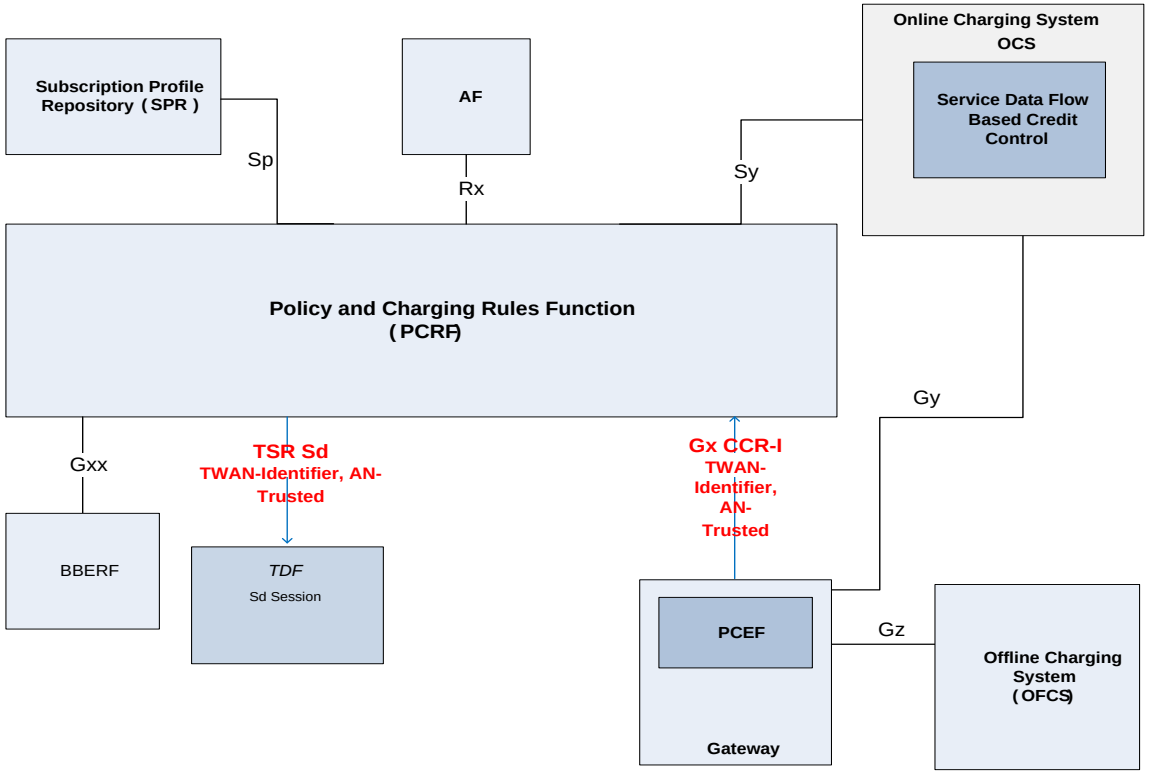
3.5 TRUSTED WLAN ACCESS (BUG 19720631)

3.5.1 Introduction

The feature introduces the support of the Trusted-WLAN Supported Feature indication, TWAN-Identifier and AN-Trusted AVPs as defined in 3GPP TS 29.212 [**Error! Bookmark not defined.**] and 23.402 [1**Error! Bookmark not defined.**] to the policy server release 12.1.1.

This document describes a new feature capability of the PCRF to receive TWAN-Identifier and AN-Trusted AVPs via Gx interface and send these AVPs in the Sd TSR/RAR message to TDF network element. This feature also adds a new capability to the PCRF to detect and decode TWAN-Identifier in the incoming Gx

request by a policy conditions. The combined information present in the TWAN-Identifier like SSID and BSSID and physical address can uniquely identify WLAN access point.



Policy Server reference infrastructure

3.5.2 Detailed Description

In the case of the RAT Type WLAN access technology PCEF can provide PCRF with the information that identifies WLAN access point by sending the Trusted-WLAN access supported feature AVP in combination with the TWAN-Identifier and AN-Trusted AVPs. If such an operation condition discovered by PCRF, a new QoS rules can be pushed down to PCEF or other associated operation performed. In addition to the detection functionality the TWAN-Identifier and AN-Trusted AVPs will be pushed to any Sd session associated with this Gx session in TSR/RAR message to TDF. The following information describes format and gives examples of the Trusted-WLAN supported features for Gx and Sd protocols as well as format of the TWAN-Identifier and AN-Trusted AVPs.

Trusted-WLAN Supported Feature for Gx Protocol

Feature bit	Feature	M/O	Description
13	Trusted-WLAN	O	This feature indicates the support for the Trusted WLAN access as defined in 3GPP TS 23.402

Gx Trusted-WLAN

Trusted-WLAN Supported Feature for Sd Protocol

Feature bit	Feature	M/O	Description
1	Trusted-WLAN	O	This feature indicates the support for the Trusted WLAN access as defined in 3GPP TS 23.402

Sd Trusted-WLAN

Note that Gx and Sd are codding Trusted-WLAN supported feature AVP differently.

TWAN-Identifier

The TWAN-Identifier AVP is used for reporting UE location in a Trusted WLAN Access Network (TWAN). For details see 3GPP TS 23.402 [**Error! Bookmark not defined.**].

The TWAN Identifier value is coded as shown below.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 169 (decimal)							
2 to 3	Length = n							
4	Spare				Instance			
5	Spare			LAII	OPNAI	PLMNI	CIVAI	BSSIDI
6	SSID Length							
7 to k	SSID							
(k+1) to (k+6)	BSSID							
q	Civic Address Length							
(q+1) to (q+r)	Civic Address Information							
s to (s+3)	TWAN PLMN-ID							
t	TWAN Operator Name Length							
(t+1) to (t+u)	TWAN Operator Name							
v	Relay Identity Type							
(v+1)	Relay Identity Length							
(v+2) to (v+w)	Relay Identity							
X	Circuit-ID Length							
(x+1) to (x+y)	Circuit-ID							
p to (n+4)	These octet(s) is/are present only if explicitly specified							

TWAN Identifier format

The BSSID and SSID are encoded as described in IEEE Std 802.11-2012.

The TWAN identifier contains the SSID and, unless otherwise determined by the TWAN operator’s policies, it also contains at least the BSSID, the civic address of the access point to which the UE is attached or the Circuit-ID with the identity of the relay which has allocated it. It may also contain the identifier of the TWAN operator, i.e. either the TWAN PLMN-ID if the TWAN is operated by a mobile operator or the TWAN Operator Name otherwise.

The SSID Length in octet '6' indicates the length of the SSID field. The SSID has a maximum length of 32 octets (see IEEE Std 802.11 [**Error! Bookmark not defined.**]).

The BSSIDI flag in octet 5 indicates whether the BSSID in octets 'k+1' to 'k+6' shall be present. If BSSIDI is set to '1', then the BSSID is present. If BSSIDI is set to '0', then the BSSID is not present.

The CIVAI flag in octet 5 indicates whether the Civic Address Length and Civic Address Information in octets 'q' and 'q+1' to 'q+r' shall be present. If the Civic Address Length and Information is present if and only if the CIVAI flag is set to 1. When present, the Civic Address Information contains the civic address of the Access Point to which the UE is attached and it is encoded as defined in sub-clause 3.1 of IETF RFC 4776 excluding the first 3 octets.

The PLMNI flag in octet 5 indicates whether the TWAN PLMN-ID in octets’s’ to 's+3' is present. The TWAN PLMN-ID is present if and only if the PLMNI flag is set to 1. The TWAN PLMN-ID is encoded as octets 5 to 7 of the Serving Network.

Serving Network is coded as depicted in the table below.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 83 (decimal)							
2 to 3	Length = n							
4	Spare				Instance			
5	MCC digit 2				MCC digit 1			
6	MNC digit 3				MCC digit 3			
7	MNC digit 2				MNC digit 1			
8 to (n+4)	These octet(s) is/are present only if explicitly specified							

Serving Network

If an Administration decides to include only two digits in the MNC, then bits 5 to 8 of octet 6 are coded as "1111".

Unless specified otherwise in the specification, this IE contains the serving core network operator ID provided by the MME, S4-SGSN or ePDG, or the PLMN identity of the selected PLMN used for 3GPP-based access authentication provided by the TWAN. When present, the TWAN PLMN-ID indicates the PLMN-ID of the TWAN operator.

NOTE: the PLMN ID contained in the TWAN PLMN-ID can differ from the PLMN ID in the Serving Network IE.

The OPNAI flag in octet 5 indicates whether the TWAN Operator Name Length and TWAN Operator Name in octets 't' and 't+1' to 't+u' is present. The TWAN Operator Name Length and TWAN Operator Name are present if and only if the OPNAI flag is set to 1. The TWAN Operator Name is encoded as specified in sub-clause 19.8 of 3GPP TS 23.003. The TWAN Operator Name identifies the TWAN operator when the TWAN is not operated by a mobile operator. The TWAN Operator Name is encoded as a realm in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19].

NOTE: The TWAN Operator Name is encoded as a dotted string.

When present, the TWAN Operator Name indicates the identifier of the TWAN operator.

The LAII flag in octet 5 indicates whether the Logical Access ID information is present in the TWAN Identifier IE. The Logical Access ID is encoded by the Relay Identity information in octets 'v' to 'v+w' and the Circuit-ID information in octets 'x' to 'x+y'. The Relay Identity information and the Circuit-ID information are present if the LAII flag is set to '1'. The Relay Identity Type indicates the type of identity as described in Table below. The Relay Identity Length indicates the length of the Identity. In case the Relay Identity Type indicates an IP address, the length indicates if it is IPv4 or IPv6 address of the Relay. The length is 4 octets for IPv4 and 16 octets for IPv6. If the Relay Identity type is set to 1 (i.e. an FQDN), it is encoded as described in section 3.1 of IETF RFC 1035 but excluding the trailing zero byte. The Circuit-ID length indicates the length of the Circuit-ID. The Circuit-ID is as defined in IETF RFC 3046, it is encoded as an Octet string and provided by the Relay.

Relay Identity Type	Values (Decimal)
IPv4 or IPv6 Address	0
FQDN	1

Relay Identity Type

AN-Trusted

The support of the Trusted WLAN access feature adds a new AVP AN-Trusted to identify if current RAT Type is trusted or not. The AN-Trusted AVP (AVP Code 1503) is of type Enumerated. The AN-Trusted AVP sent from the 3GPP AAA Server to the Non-3GPP access network conveys the decision about the access network being trusted or untrusted by the HPLMN.

The following values are defined:

TRUSTED (0) - This value is used when the non-3GPP access network is to be handled as trusted.

UNTRUSTED (1) - This value is used when the non-3GPP access network is to be handled as untrusted.

				AVP Flag rules			
Attribute Name	**AVP Code**	**Vendor ID**	**Value Type**	**Must**	**May**	**Should not**	**Must not**
AN-Trusted	1503	10415	Enumerated	M,V			P

AN-Trusted AVP details

In this feature AN-Trusted AVP is received in the Gx CCR request and forwarded to the TDF via Sd -TSR message or Sd – RAR as a part of the Event-Report-Indication AVP.

The PCRF release 12.1.1 supports receipt of the Trusted-WLAN Supported Feature indication and the TWAN-Identifier and AN-Trusted AVPs in Gx CC-Request and the Trusted-WLAN Supported Feature indication in Sd TDF-Session-Request messages as described in 3GPP TS 29.212 [**Error! Bookmark not defined.**].

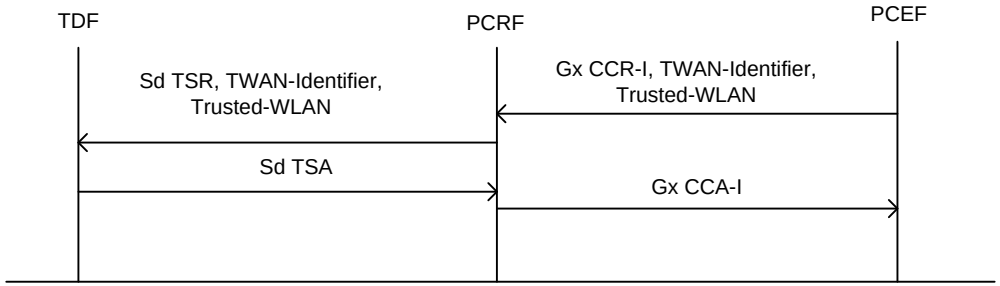
This is an example of the Gx CCR message that includes TWN-Identifier and AN-Trusted AVPs. Note that TWN-Identifier is shown as a fully parsed string value.

Diameter Message: CCR

Version: 1
Msg Length: 668
Cmd Flags: REQ,PXY
Cmd Code: 272
App-Id: 16777238
Hop-By-Hop-Id: 670198006
End-To-End-Id: 3198908018
  Session-Id (263,M,l=35) = pgw.group4.com;1423092427;9
  Origin-Host (264,M,l=22) = pgw.group4.com
  Origin-Realm (296,M,l=18) = group4.com
  Auth-Application-Id (258,M,l=12) = 16777238
  Destination-Realm (283,M,l=18) = group4.com
  CC-Request-Type (416,M,l=12) = INITIAL_REQUEST (1)
  CC-Request-Number (415,M,l=12) = 0
  Subscription-Id (443,M,l=48) =
    Subscription-Id-Type (450,M,l=12) = END_USER_NAI (3)
    Subscription-Id-Data (444,M,l=28) = afatykhov@oracle.com
  Subscription-Id (443,M,l=40) =
    Subscription-Id-Type (450,M,l=12) = END_USER_E164 (0)
    Subscription-Id-Data (444,M,l=18) = 5089981996
  Subscription-Id (443,M,l=44) =
    Subscription-Id-Type (450,M,l=12) = END_USER_IMSI (1)
    Subscription-Id-Data (444,M,l=23) = 123456789123456
  RAT-Type (1032,V,v=10415,l=16) = -1
  Framed-IP-Address (8,M,l=12) = 10.0.0.88
  Network-Request-Support (1024,VM,v=10415,l=16) = NETWORK_REQUEST_SUPPORTED (1)
  IP-CAN-Type (1027,VM,v=10415,l=16) = THREEGPP_EPS (5)
  QoS-Information (1016,VM,v=10415,l=60) =
    QoS-Class-Identifier (1028,VM,v=10415,l=16) = 8
    Max-Requested-Bandwidth-UL (516,VM,v=10415,l=16) = 12800
    Max-Requested-Bandwidth-DL (515,VM,v=10415,l=16) = 51200
  Called-Station-Id (30,M,l=16) = apn1.com
  TFT-Packet-Filter-Information (1013,VM,v=10415,l=96) =
    Precedence (1010,VM,v=10415,l=16) = 7
    TFT-Filter (1012,VM,v=10415,l=51) = permit out 17 from 10.0.0.1 to assigned
    ToS-Traffic-Class (1014,VM,v=10415,l=13) = 0x10
  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) = 8192
  AN-Trusted (1503,VM,v=10415,l=16) = UNTRUSTED (1)
  Bearer-Identifier (1020,VM,v=10415,l=15) = 101
  Bearer-Operation (1021,VM,v=10415,l=16) = ESTABLISHMENT (1)

TWAN-Identifier (29,VM,v=10415,l=59) = ONE, 00:14:22:01:23:45, Home, 123456, Oracle, oracle.com, 123

The PCRF release 12.1.1 supports sending of the TWAN-Identifier AVP in Sd messages as described in 3GPP TS 29.212 [**Error! Bookmark not defined.**]. When TWAN-Identifier is received by MPE in the Gx CCR and Trusted-WLAN supported feature flag is present this value is propagated to the TDF by Sd TSR message. Note that Sd Trusted-WLAN supported feature flag will be also set in this TSR.



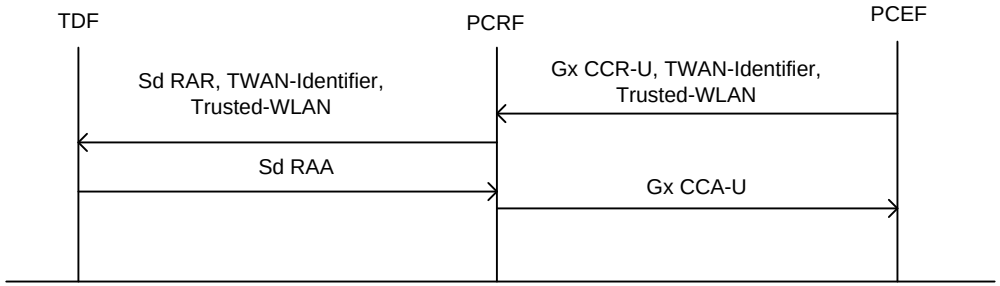
TWAN-Identifier propagation to TDF

This is an example of the Sd TSR message that includes TWN-Identifier AVP. Note that TWN-Identifier is shown as a fully parsed string value.

Diameter Message: TSR
Version: 1
Msg Length: 568
Cmd Flags: REQ,PXY
Cmd Code: 8388637
App-Id: 16777303
Hop-By-Hop-Id: 270248257
End-To-End-Id: 3274213534
  Session-Id (263,M,l=37) = mpe01.group4.com;1423166875;1
  Origin-Host (264,M,l=24) = mpe01.group4.com
  Origin-Realm (296,M,l=18) = group4.com
  Vendor-Specific-Application-Id (260,M,l=32) =

```
    Vendor-Id (266,M,l=12) = 10415
    Auth-Application-Id (258,M,l=12) = 16777303
  Destination-Realm (283,M,l=18) = group4.com
  Destination-Host (293,M,l=22) = tdf.group4.com
  Framed-IP-Address (8,M,l=12) = 10.0.0.88
  IP-CAN-Type (1027,VM,v=10415,l=16) = THREEGPP_EPS (5)
  Called-Station-Id (30,M,l=16) = apn1.com
  Subscription-Id (443,M,l=48) =
    Subscription-Id-Type (450,M,l=12) = END_USER_NAI (3)
    Subscription-Id-Data (444,M,l=28) = afatykhov@oracle.com
  Subscription-Id (443,M,l=40) =
    Subscription-Id-Type (450,M,l=12) = END_USER_E164 (0)
    Subscription-Id-Data (444,M,l=18) = 5089981996
  Subscription-Id (443,M,l=44) =
    Subscription-Id-Type (450,M,l=12) = END_USER_IMSI (1)
    Subscription-Id-Data (444,M,l=23) = 123456789123456
  Event-Trigger (1006,VM,v=10415,l=16) = APPLICATION_START (39)
  Event-Trigger (1006,VM,v=10415,l=16) = APPLICATION_STOP (40)
  Explicit-Route (3000,V,v=21274,l=64) =
    Route-Action (3002,V,v=21274,l=16) = ROUTE (1)
    Explicit-Route-Record (3001,V,v=21274,l=36) =
      Proxy-Host (280,M,l=24) = mra02.group4.com
  TWAN-Identifier (29,VM,v=10415,l=59) = ONE, 00:14:22:01:23:45, Home, 123456, Oracle, oracle.com, 123
  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) = 2
```

In the case when TWAN Identifier is updated by Gx CCR-U



TWAN-Identifier propagation to TDF by RAR

Diameter Message: CCR
Version: 1
Msg Length: 720
Cmd Flags: REQ,PXY
Cmd Code: 272
App-Id: 16777238
Hop-By-Hop-Id: 3754539034
End-To-End-Id: 3670358087
  Session-Id (263,M,l=35) = pgw.group4.com;1424722324;9
  Origin-Host (264,M,l=22) = pgw.group4.com
  Origin-Realm (296,M,l=18) = group4.com
  Auth-Application-Id (258,M,l=12) = 16777238
  Destination-Realm (283,M,l=18) = group4.com
  CC-Request-Type (416,M,l=12) = UPDATE_REQUEST (2)
  CC-Request-Number (415,M,l=12) = 1
  Destination-Host (293,M,l=24) = mpe01.group4.com
  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) = 123456789123456
  Framed-IP-Address (8,M,l=12) = 10.0.0.88
  Network-Request-Support (1024,VM,v=10415,l=16) = NETWORK_REQUEST_SUPPORTED (1)
  IP-CAN-Type (1027,VM,v=10415,l=16) = WIMAX (3)
  QoS-Information (1016,VM,v=10415,l=60) =
    QoS-Class-Identifier (1028,VM,v=10415,l=16) = 8
    Max-Requested-Bandwidth-UL (516,VM,v=10415,l=16) = 12800
    Max-Requested-Bandwidth-DL (515,VM,v=10415,l=16) = 51200
  Called-Station-Id (30,M,l=17) = apn01.com
  TFT-Packet-Filter-Information (1013,VM,v=10415,l=96) =
    Precedence (1010,VM,v=10415,l=16) = 7
    TFT-Filter (1012,VM,v=10415,l=51) = permit out 17 from 10.0.0.1 to assigned
    ToS-Traffic-Class (1014,VM,v=10415,l=13) = 0x10
  Event-Trigger (1006,VM,v=10415,l=16) = IP_CAN_CHANGE (7)
  Event-Trigger (1006,VM,v=10415,l=16) = USER_LOCATION_CHANGE (13)
  Supported-Features (628,V,v=10415,l=56) =
    Vendor-Id (266,M,l=12) = 12951
    Feature-List-ID (629,V,v=10415,l=16) = 1
    Feature-List (630,V,v=10415,l=16) = 1

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) = 8192
Bearer-Identifier (1020,VM,v=10415,l=15) = 101
Bearer-Operation (1021,VM,v=10415,l=16) = ESTABLISHMENT (1)
TWAN-Identifier (29,VM,v=10415,l=59) = ONE, 00:14:22:01:23:45, Home, 123456, Oracle, oracle.com, 123

The PCRF will send an RAR to the TDF with the TWAN Identifier included into Event-Report-Indication AVP with an appropriate event type if TDF subscribed for this event.

Diameter Message: RAR
Version: 1
Msg Length: 348
Cmd Flags: REQ,PXY
Cmd Code: 258
App-Id: 16777303
Hop-By-Hop-Id: 2928937459
End-To-End-Id: 1943973963
Session-Id (263,M,l=37) = mpe01.group4.com;1424722737;7
Origin-Host (264,M,l=24) = mpe01.group4.com
Origin-Realm (296,M,l=18) = group4.com
Destination-Realm (283,M,l=18) = group4.com
Destination-Host (293,M,l=22) = tdf.group4.com
Auth-Application-Id (258,M,l=12) = 16777303
Re-Auth-Request-Type (285,M,l=12) = AUTHORIZE_ONLY (0)
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) = 2
Event-Report-Indication (1033,V,v=10415,l=120) =
Event-Trigger (1006,VM,v=10415,l=16) = USER_LOCATION_CHANGE (13)
Event-Trigger (1006,VM,v=10415,l=16) = IP_CAN_CHANGE (7)
IP-CAN-Type (1027,VM,v=10415,l=16) = WIMAX (3)
TWAN-Identifier (29,VM,v=10415,l=59) = ONE, 00:14:22:01:23:45, Home, 123456, Oracle, oracle.com, 123

When the Trusted-WLAN Supported Feature is indicated and the TWAN-Identifier AVP is present in CC-Request messages, the TWAN-Identifier information can be used to identify WLAN the UE location information. Policy server extends match list policy condition to identify following UE location attributes.

where the TWAN_SSID is contained in Match List(s) TWAN_SSIDs

where the TWAN_BSSID is contained in Match List(s) TWAN_BSSIDs

where the TWAN_PLMNId is contained in Match List(s) TWAN_ PLMNIds

where the TWAN_OperatorName is contained in Match List(s) TWAN_BSSIDs

where the TWAN_RelayIdentity is contained in Match List(s) TWAN_BSSIDs

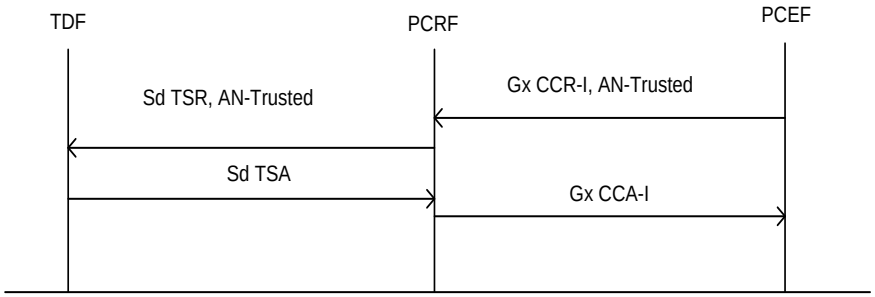
where the TWAN_CircuitId is contained in Match List(s) TWAN_BSSIDs

Each of the value lists contains ASCII formatted string.

When the Trusted-WLAN Supported Feature is indicated and the TWAN-Identifier AVP is present in CC-Request messages, the TWAN-Identifier information is made available in a Policy Rule condition. The conditions can include support for comparing TWAN-Identifier components to Match Lists.

An extended policy conditions can parse TWAN-Identifier value as a separate elements which gives us access to the elements like SSID, BSSID, PLMN, Operator Name, Relay Identity and Circuit ID. Note that SSID is an ASCII string. The BSSID value has a MAC address format and PLMN identity has the same format as MCC-MNC. The Relay Identity can represent an IP address or a fully qualified FQDN name. All of these policy conditions can be applied to the Gx and as well as Sd requests. In the case when policy conditions are used against Gx/Sd RAR request the TWAN-Identifier value will be taken from the associated session.

The PCRF release 12.1.1 supports sending of the AN-Trusted AVP in Sd messages as described in 3GPP TS 29.212 [**Error! Bookmark not defined.**]. When AN-Trusted AVP is received by MPE in the Gx CCR-I the value is propagated to the TDF by Sd TSR message. When AN-Trusted AVP is received by MPE in the Gx CCR-U the value is propagated to the TDF by Sd RAR message as a part of the Event-Report-Indication AVP.



AN-Trusted propagation to TDF by TSR

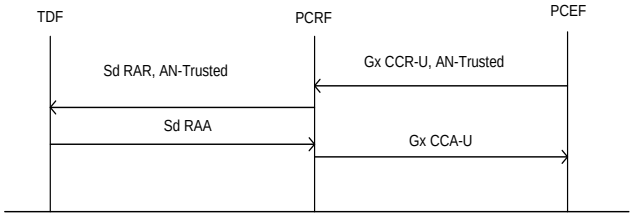
Diameter Message: CCR
Version: 1
Msg Length: 684
Cmd Flags: REQ,PXY
Cmd Code: 272

App-Id: 16777238
Hop-By-Hop-Id: 241680859
End-To-End-Id: 3655755319
  Session-Id (263,M,l=35) = pgw.group4.com;1426862472;1
  Origin-Host (264,M,l=22) = pgw.group4.com
  Origin-Realm (296,M,l=18) = group4.com
  Auth-Application-Id (258,M,l=12) = 16777238
  Destination-Realm (283,M,l=18) = group4.com
  CC-Request-Type (416,M,l=12) = INITIAL_REQUEST (1)
  CC-Request-Number (415,M,l=12) = 0
  Subscription-Id (443,M,l=48) =
    Subscription-Id-Type (450,M,l=12) = END_USER_NAI (3)
    Subscription-Id-Data (444,M,l=28) = afatykhov@oracle.com
  Subscription-Id (443,M,l=40) =
    Subscription-Id-Type (450,M,l=12) = END_USER_E164 (0)
    Subscription-Id-Data (444,M,l=18) = 5089981996
  Subscription-Id (443,M,l=44) =
    Subscription-Id-Type (450,M,l=12) = END_USER_IMSI (1)
    Subscription-Id-Data (444,M,l=23) = 123456789123456
  RAT-Type (1032,V,v=10415,l=16) = -1
  Framed-IP-Address (8,M,l=12) = 10.0.0.88
  Network-Request-Support (1024,VM,v=10415,l=16) = NETWORK_REQUEST_SUPPORTED (1)
  IP-CAN-Type (1027,VM,v=10415,l=16) = THREEGPP_EPS (5)
  QoS-Information (1016,VM,v=10415,l=60) =
    QoS-Class-Identifier (1028,VM,v=10415,l=16) = 8
    Max-Requested-Bandwidth-UL (516,VM,v=10415,l=16) = 12800
    Max-Requested-Bandwidth-DL (515,VM,v=10415,l=16) = 51200
  Called-Station-Id (30,M,l=16) = apn1.com
  TFT-Packet-Filter-Information (1013,VM,v=10415,l=96) =
    Precedence (1010,VM,v=10415,l=16) = 7
    TFT-Filter (1012,VM,v=10415,l=51) = permit out 17 from 10.0.0.1 to assigned
    ToS-Traffic-Class (1014,VM,v=10415,l=13) = 0x10
  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) = 8192
  AN-Trusted (1503,VM,v=10415,l=16) = TRUSTED (0)
  Bearer-Identifier (1020,VM,v=10415,l=15) = 101
  Bearer-Operation (1021,VM,v=10415,l=16) = ESTABLISHMENT (1)
  TWAN-Identifier (29,VM,v=10415,l=59) = ONE, 00:14:22:01:23:45, Home, 123456, Oracle, oracle.com, 123

Sd TSR message:

Diameter Message: TSR
Version: 1
Msg Length: 520
Cmd Flags: REQ,PXY
Cmd Code: 8388637
App-Id: 16777303
Hop-By-Hop-Id: 2739294404
End-To-End-Id: 3804733707
  Session-Id (263,M,l=37) = mpe01.group4.com;1426862414;1
  Origin-Host (264,M,l=24) = mpe01.group4.com
  Origin-Realm (296,M,l=18) = group4.com
  Vendor-Specific-Application-Id (260,M,l=32) =
    Vendor-Id (266,M,l=12) = 10415
    Auth-Application-Id (258,M,l=12) = 16777303
  Destination-Realm (283,M,l=18) = group4.com
  Destination-Host (293,M,l=22) = tdf.group4.com
  Framed-IP-Address (8,M,l=12) = 10.0.0.88
  IP-CAN-Type (1027,VM,v=10415,l=16) = THREEGPP_EPS (5)
  Called-Station-Id (30,M,l=16) = apn1.com
  Subscription-Id (443,M,l=48) =
    Subscription-Id-Type (450,M,l=12) = END_USER_NAI (3)
    Subscription-Id-Data (444,M,l=28) = afatykhov@oracle.com
  Subscription-Id (443,M,l=40) =
    Subscription-Id-Type (450,M,l=12) = END_USER_E164 (0)
    Subscription-Id-Data (444,M,l=18) = 5089981996
  Subscription-Id (443,M,l=44) =
    Subscription-Id-Type (450,M,l=12) = END_USER_IMSI (1)
    Subscription-Id-Data (444,M,l=23) = 123456789123456
  Event-Trigger (1006,VM,v=10415,l=16) = APPLICATION_START (39)
  Event-Trigger (1006,VM,v=10415,l=16) = APPLICATION_STOP (40)
  TWAN-Identifier (29,VM,v=10415,l=59) = ONE, 00:14:22:01:23:45, Home, 123456, Oracle, oracle.com, 123,
  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) = 2
  AN-Trusted (1503,VM,v=10415,l=16) = TRUSTED (0)

The AN-Trusted AVP also can be accepted in the Gx CCR-U message and propagated to TDF in the Sd RAR.



AN-Trusted propagation to TDF by RAR

Example of the Sd RAR message with the TWAN-Identifier and AN-Trusted AVPs:

Diameter Message: RAR
Version: 1
Msg Length: 308
Cmd Flags: REQ,PXY
Cmd Code: 258
App-Id: 16777303
Hop-By-Hop-Id: 3604861396
End-To-End-Id: 3804733765
  Session-Id (263,M,l=38) = mpe01.group4.com;1426862414;11
  Origin-Host (264,M,l=24) = mpe01.group4.com
  Origin-Realm (296,M,l=18) = group4.com
  Destination-Realm (283,M,l=18) = group4.com
  Destination-Host (293,M,l=22) = tdf.group4.com
  Auth-Application-Id (258,M,l=12) = 16777303
  Re-Auth-Request-Type (285,M,l=12) = AUTHORIZE_ONLY (0)
  Event-Report-Indication (1033,V,v=10415,l=136) =
    Event-Trigger (1006,VM,v=10415,l=16) = USER_LOCATION_CHANGE (13)
    Event-Trigger (1006,VM,v=10415,l=16) = IP_CAN_CHANGE (7)
    IP-CAN-Type (1027,VM,v=10415,l=16) = WIMAX (3)
    TWAN-Identifier (29,VM,v=10415,l=59) = ONE, 00:14:22:01:23:45, Home, 123456, Oracle, oracle.com, 123,
    AN-Trusted (1503,VM,v=10415,l=16) = UNTRUSTED (1)

Policy Changes

Policy conditions “where the [field] is contained in Match List(s) [match lists]” and “where the [field] is not contained in Match List(s) [match lists]” are extended to incorporate TWAN data fields

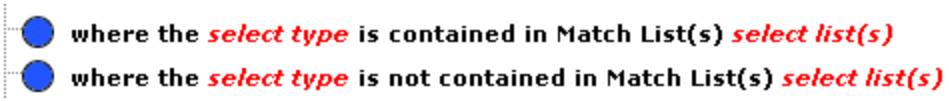
Policy Changes

Policy Condition	Policy Condition or Action	Description

Group		
SSID	where the **TWAN_SSID** is contained in Match List(s) ***[match lists]***	Check whether TWAN-Identifiers SSID field matches value from the specified match lists. The result of the compare is negative if SSID does not match predefined value or TWAN-Identifier is not present in the request or session.
BSSID	where the **TWAN_BSSID** is contained in Match List(s) ***[match lists]***	Check whether TWAN-Identifiers BSSID field matches value from the specified match lists. The result of the compare is negative if BSSID does not match predefined value or TWAN-Identifier is not present in the request or session. BSSID is formatted as MAC address.
PLMN ID	where the **TWAN_PLMNId** is contained in Match List(s) ***[match lists]***	Check whether TWAN-Identifiers PLMN ID field matches value from the specified match lists. The result of the compare is negative if PLMN ID does not match predefined value or TWAN-Identifier is not present in the request or session. PLMN ID is formatted as MCC-MNC address.
Operator Name	where the **TWAN_OperatorName** is contained in Match List(s) ***[match lists]***	Check whether TWAN-Identifiers Operator Name field matches value from the specified match lists. The result of the compare is negative if Operator Name does not match predefined value or TWAN-Identifier is not present in the request or session.
Relay Identity	where the **TWAN_RelayIdentity** is contained in Match List(s) ***[match lists]***	Check whether TWAN-Identifiers Relay Identity field matches value from the specified match lists. The result of the compare is negative if Relay Identity does not match predefined value or TWAN-Identifier is not present in the request or session.
Circuit Id	where the **TWAN_CircuitId** is contained in Match List(s) ***[match lists]***	Check whether TWAN-Identifiers Circuit Id field matches value from the specified match lists. The result of the compare is negative if Circuit Id does not match predefined value or TWAN-Identifier is not present in the request or session.

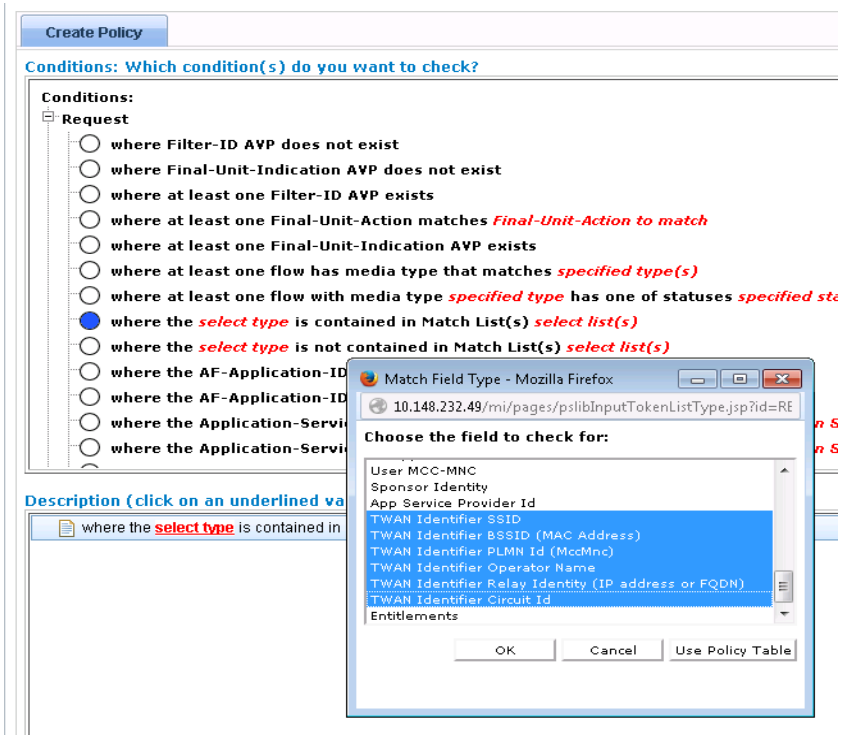
User Interface Changes

This Trusted WLAN access feature defines new field types for the following policy conditions:



Policy Conditions

The match type selection dialog has six new types to select TWAN Identifier components.



TWAN field types

3.6 BINDING ON IP DOMAIN ID (PR 19117477)

3.6.1 Introduction

The Binding on IP-Domain-ID feature try to resolve the problem there are same IP addresses assigned for different end users in multi-network environment on one MPE/MRA. And this feature is only suitable for framed IPv4 address on the wireless mode.

The IP-Domain-ID is an AVP for Rx message to indicate the framed IP address will belong to which network element. And for the network element, an IP-Domain-ID should be provided as well for finding the right network element. Multiple network elements can belong to one IP-domain-Domain-ID, but one network element only has one IP-Domain-Id.

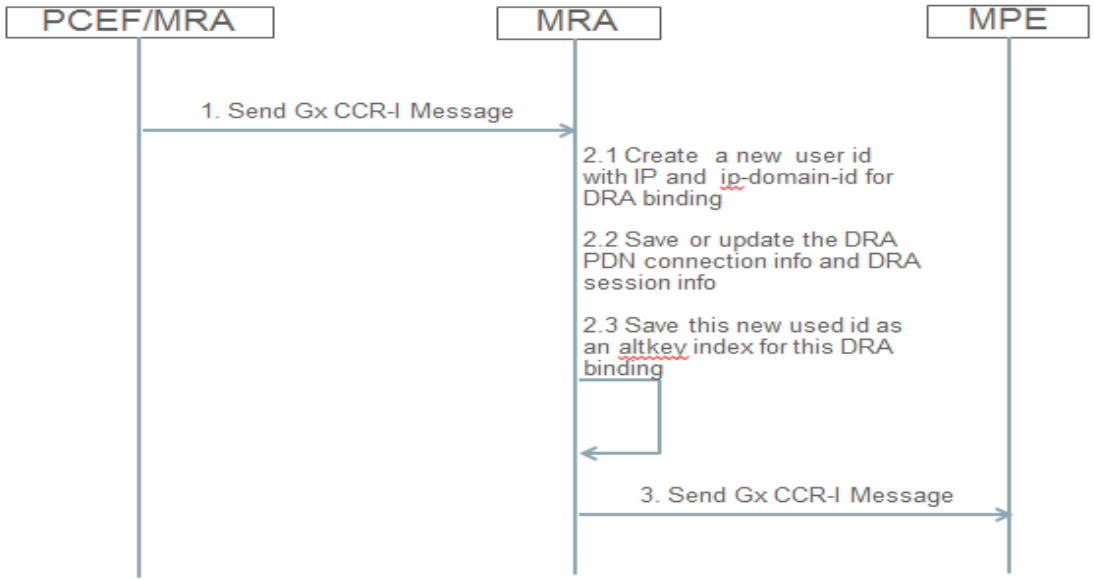
The combination of framed IP address and the mapping of IP-Domain-ID will be one of user Ids for a Diameter message request (Rx, Gx).This IP address with IP-Domain-ID (IPD) user id will be the identity to find the right MPE binding on MRA and Gx session on MPE. The IPD user id is only available when the related network element enables this feature and the IPD index is checked for subscriber indexing.

The IP-Domain-ID is case insensitive, which will be low case for message processing and binding in MRA/MPE.

3.6.2 Detailed Description

The scenario for binding on IP-Domain-Id feature should include two parts: DRA binding on MRA and Session correlations on MPE. And the message involved this feature is Gx CCR-I, Gx CCR-T and Rx AAR message, the detail description about this two messages flow on MRA/MPE will be depicted as following:

- **DRA binding on MRA**
  - Gx CCR-I message



Gx CCR-I message on MRA

The steps on MRA are as following:

1. A new user id for framed IPv4 address with IP-Domain-ID will be created for a Gx DRA binding when related PCEF enables IPD feature and IPD index is checked for subscriber on MRA/MPE.
2. A new alt-key IPWithDomain index will be saved in comcol table DRABinding_Key_Other for this DRA binding.
3. If index by IPD is enabled, the IP with domain user id will be created in MRA. This IPD index should be work along with IPv4 index, otherwise, the Rx message without the IP-Domain-Id AVP will not find the related Gx session.
4. If only index by IPD is enabled, the related network element for this MRA should be configured with IP-domain-Id, otherwise the IPD user id cannot be created properly for this created DRA binding.
5. The IP domain id will be saved in the DRA PDN connection info in the DRA binding for checking if there are existed PDN connection in DRA binding for adding the session info when IPD index or IPD index Overrides by APN are enabled, the processing is:

- When there are different PDN connections with different APNs in the DRA binding, if there is not a PDN connection which has the same APN with new pending PDN connection, this new pending connection will be inserted to DRA binding DB.

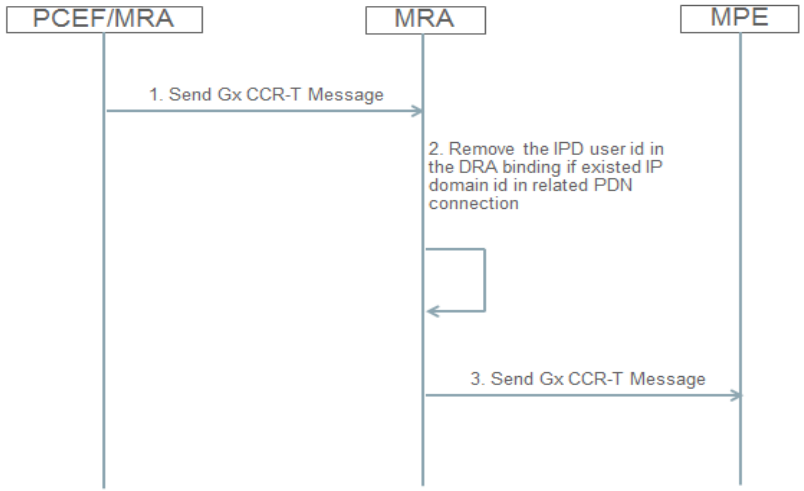
-When there are more than one PDN connections in the same APN which the new pending PDN connection belongs to, two situations should be considered as below:

1). If new pending PDN connection does not have the IP domain id and an existed PDN connection which does not have the IP domain id contains the same IP address as the new PDN connection in DRA binding DB, this PDN connection will be the found PDN connection for adding session info.

2). If new pending PDN connection have the IP domain id and an existed PDN connection which have the same IP domain id and IP address as this new PDN connection in DRA binding DB, this PDN connection will be responsible for this session info processing.

- For other situation, this new pending connection will be inserted to DRA binding DB.

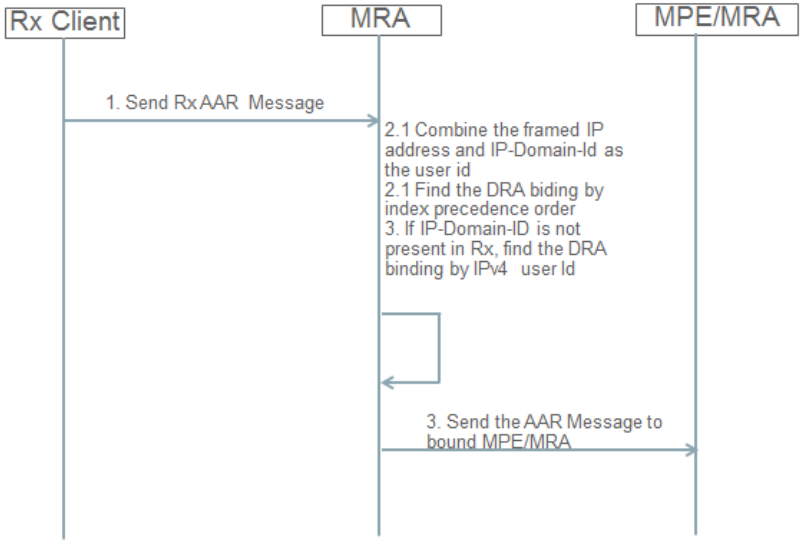
- Gx CCR-T message



Gx CCR-T message on MRA

The steps on MRA are as following:

1. If the IP domain id is existed in this DRA PDN connection, the IPD user id should be removed from DRA binding and index table when removing this session info and check if this IPv4 address is overlapped in other PDN connection, if overlapped, remove the IPv4 user id from binding and index table as well if this IP user id exists when IPv4 indexing is enabled either globally or for this APN.
2. If the IP domain id is not existed in this DRA PDN connection, check if this IPv4 address is overlapped, if overlapped removes the IP user id when this IP user id exists when IPv4 indexing is enabled either globally or for this APN.
    - Rx AAR message



Rx AAR message on MRA

The steps on MRA are as following:

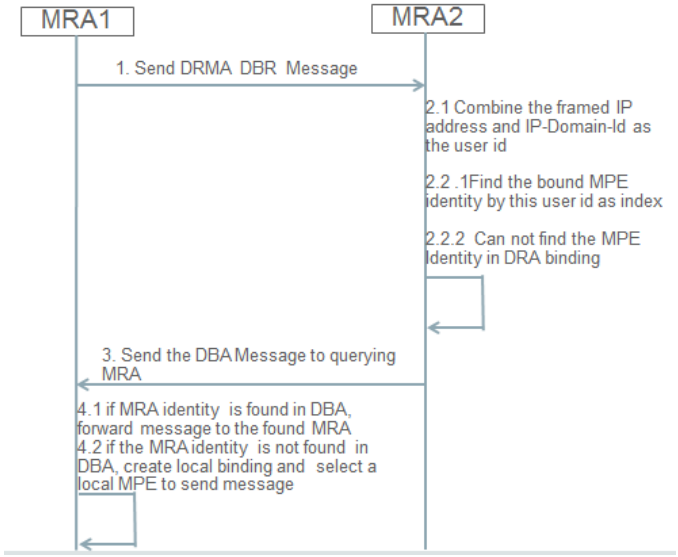
1. The two AVPs of framed IP address and IP-Domain-ID will be used as the IP with IP-Domain-ID index to find the right DRA Binding if the IP-Domain-ID is present.
2. The DRA binding finding process will follow the index precedence, the detail steps are as below:

- A cfg item DB.KeysPrecedence need to be set for designating the order of user id. Ordered comma separated list of keys are used for index precedence processing. The user id index will be preceded by this order. The default value is IMSI, Ipv6, IPD, IPv4, E164, NAI, NAME, SESSID.

-If there are multi indices in the Rx message, the index precedence will follow the order in the DB.KeysPrecedence. For example, if the IPD and IP user ids are in Rx message and the DB.KeysPrecedence is IPD IPv4, the IPD index will be firstly picked up for finding the DRA binding, if not found, the IPv4 index will be used.

3. If the right DRA binding is found, the message will be forwarded to found MPE/MRA server.

- DRMA DBR message –Legacy Mode

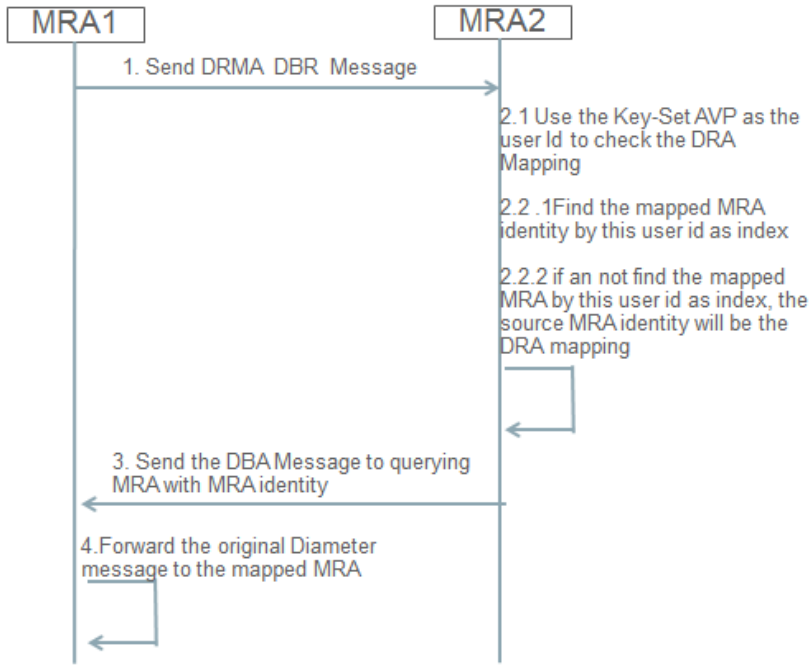


DRMA DBR message for Legacy Mode on MRA

The steps on MRA are as following:

1. The new IP-Domain-Id DBR message AVP should be supported.
2. For Legacy mode, the two AVPs of framed IP address and IP-Domain-Id will be used as the IP with IP-Domain-ID index to find the right Server-Identity.
3. If both IPv4 and IPD indexing are enabled, the MRA receiving the DBR will look for the binding using both keys (according to the precedence configuration).

- DRMA DBR message –Algov1 Mode

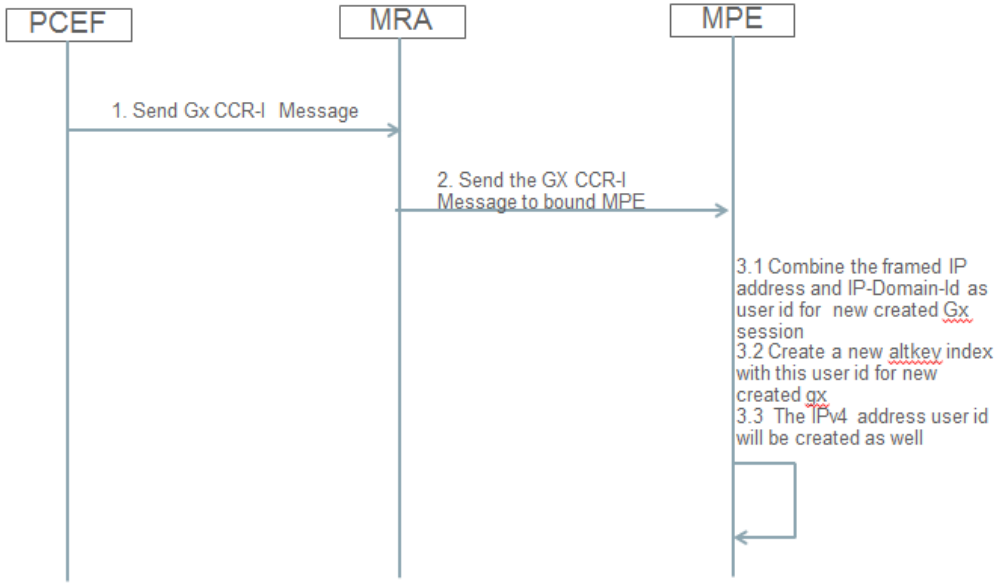


DRMA DBR message for Algov1 mode on MRA

The steps on MRA are as following:

1. For Algov1 mode, the IP address and domain id will be inserted in the Key-Set AVP to find the right Server-Identity.
2. A new IPD AVP value will be added for the Key-Type AVP
3. If both IPv4 and IPD indexing are enabled, the MRA receiving the DBR will look for the binding using both keys (according to the precedence configuration).

- **Session correlations on MPE**
    - Gx CCR-I message

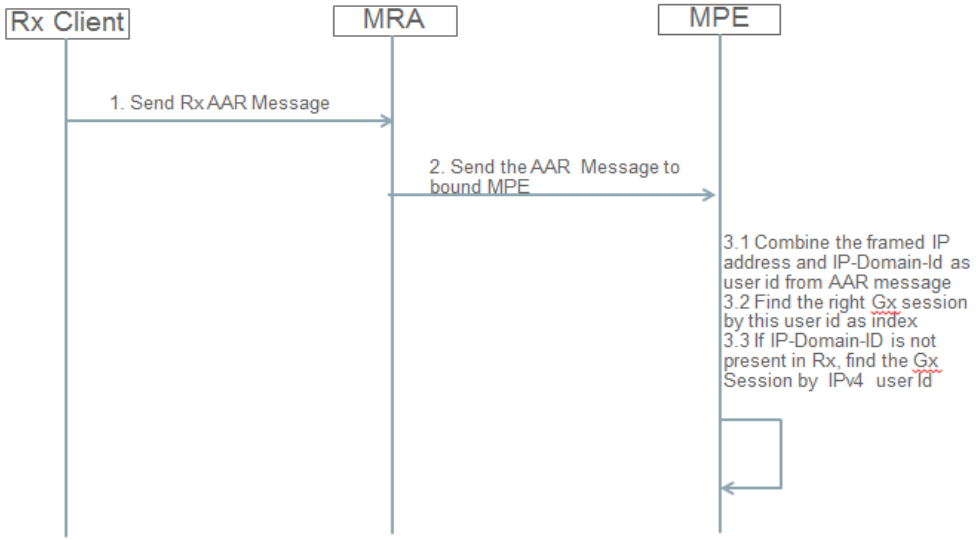


Gx CCR-I message on MPE

The steps on MPE are as following:

1. A new user id for framed IPv4 address with IP-Domain-ID will be created when the IPD indexing is enabled for subscriber indexing on MPE if the IPD index is enabled on the MPE
2. This user id will be as the session correlations key for this Gx session.

- Rx AAR message



Rx AAR message on MPE

The steps on MPE are as following:

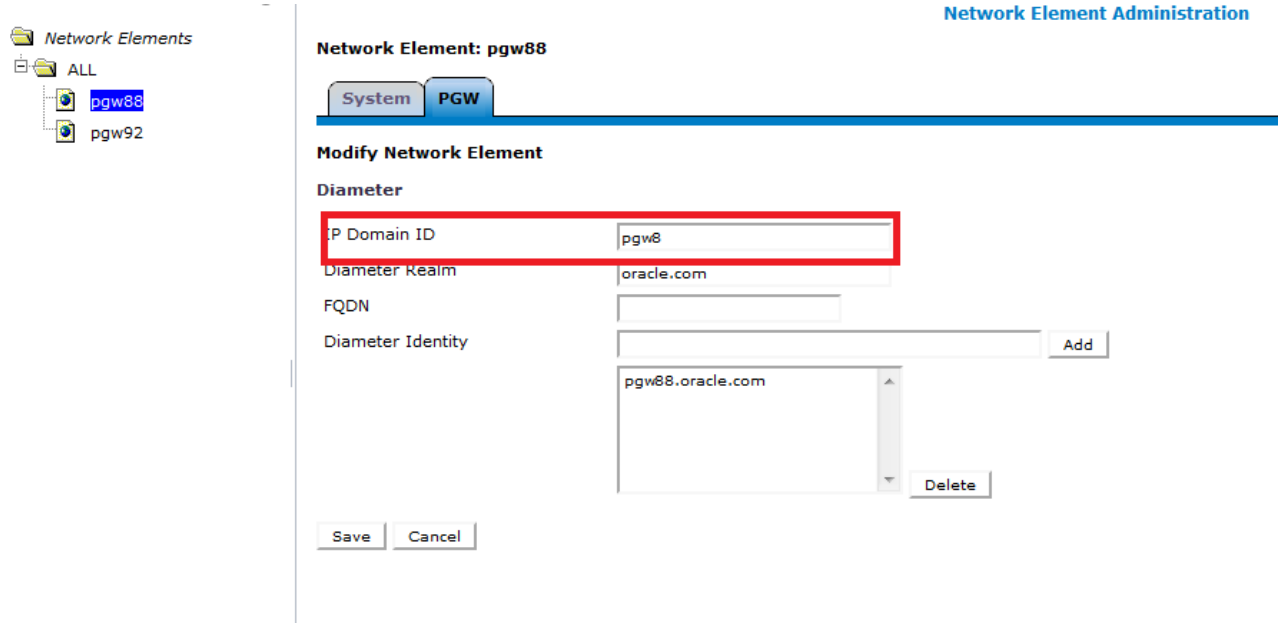
1. The two AVPs of framed IP address and IP-Domain-ID will be used as the IP with IP-Domain-ID user Id to find the right Gx session if IP-Domain-ID is present in Rx and the framed IPv4 address will be used as user id as well.
2. The Gx session will be found according to the user id from Rx and the index enabling on MPE, for example if IPD indexing is disable, the IPD user id will not be used otherwise it will be used.
3. If there are multi indices in the Rx message, the index precedence will follow the order in the index precedence which is mentioned above at the Rx message on MRA.

User Interface Changes

There should be a new input field for the network element information configuration as following:

1. The IP domain id field must be inputted with valid string (only letter and digit, dot , hyphen) of which length is <= 100 or left empty. If the IPD field is empty means this feature is disabled for this network element.
2. This filed should be sent to MRA/MPE as network element information.

The UI is as following:

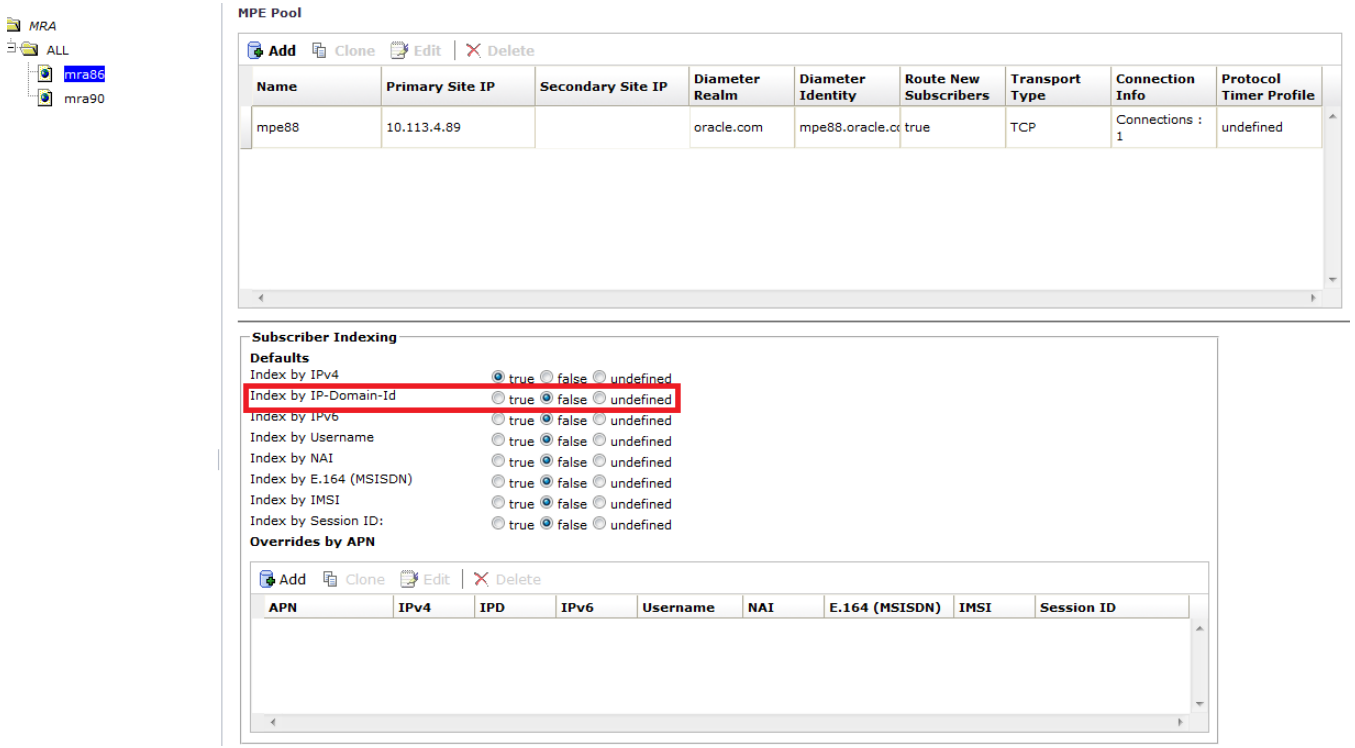


IP Domain ID mapping UI

There should be a new IPD subscriber indexing for MRA configuration as following:

1. A check box group for IPD index indicates this IPD index is checked or not
2. The configuration settings of MRADB.IndexByIpd of which value is set by the above checkbox should be pushed to MRA

The UI is as following:

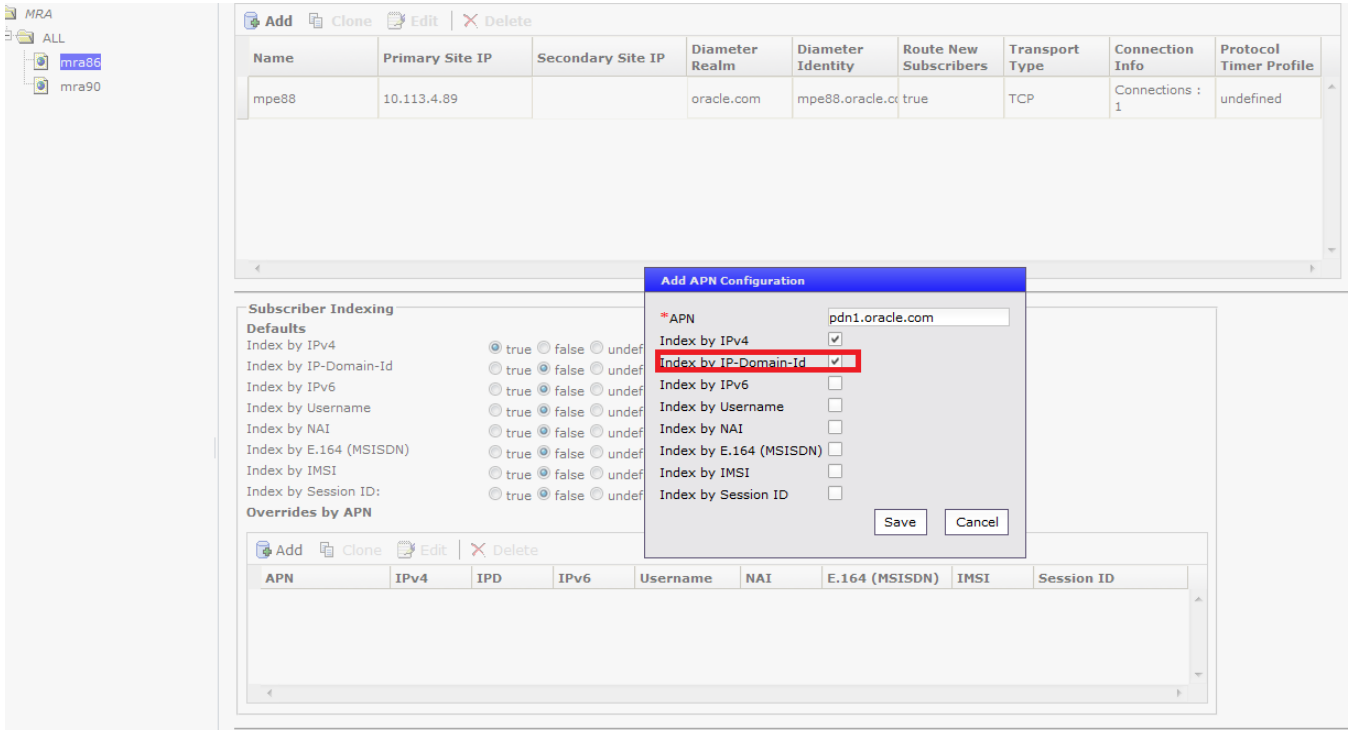


IPD index configuration on MRA

There should be a new IPD subscriber indexing for MRA configuration overrides by APN as following:

1. A check box for IPD index indicates this IPD index is checked or not
2. The configuration settings of DB.INDEXING(n).IndexByIpd of which value is set by the above checkbox should be pushed to MRA. The "n" in DB.INDEXING means it's a list of settings for the related overrides APNs

The UI is as following:

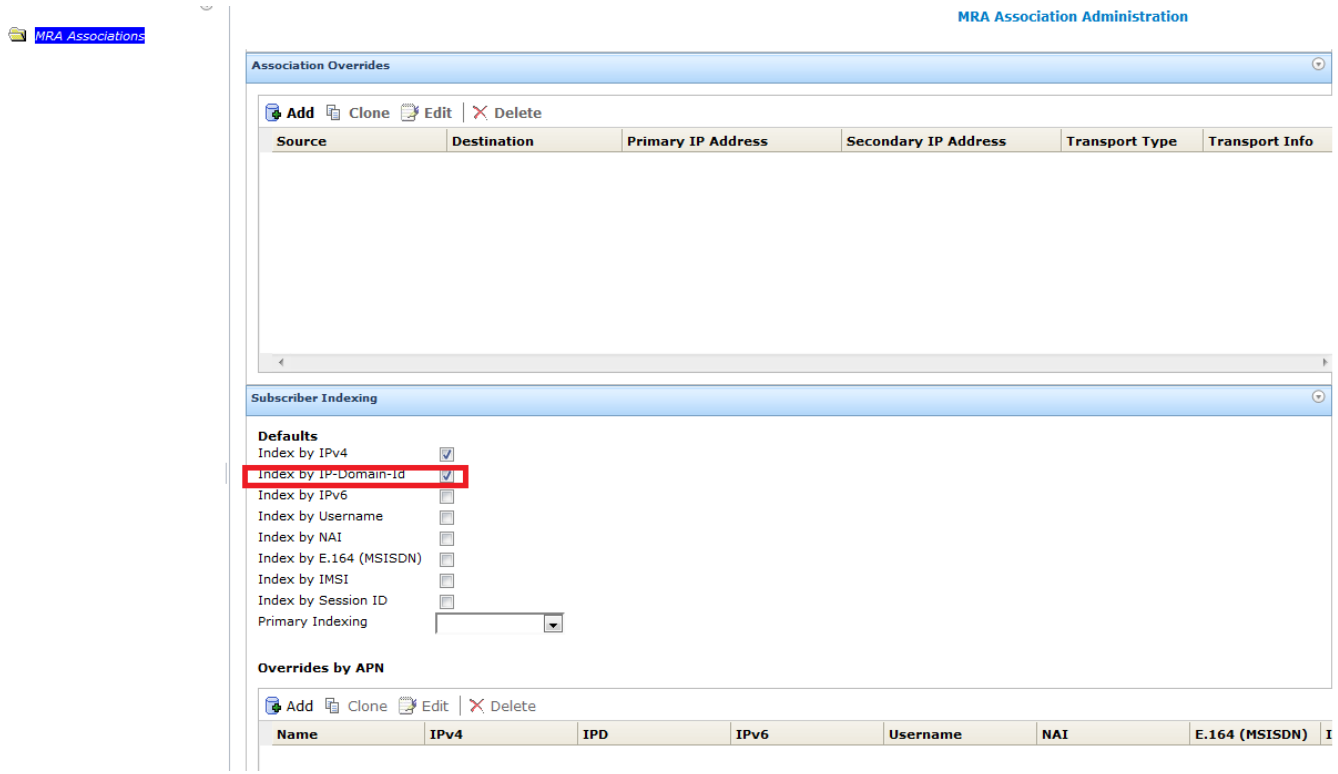


IPD index configuration Overrides By APN on MRA

There should be a new IPD subscriber indexing for MRA association configuration as following:

1. A check box for IPD index indicates this IPD index is checked or not
2. The configuration settings of MRADB.IndexByIpd of which value is set by the above checkbox should be pushed to MRA

The UI is as following:

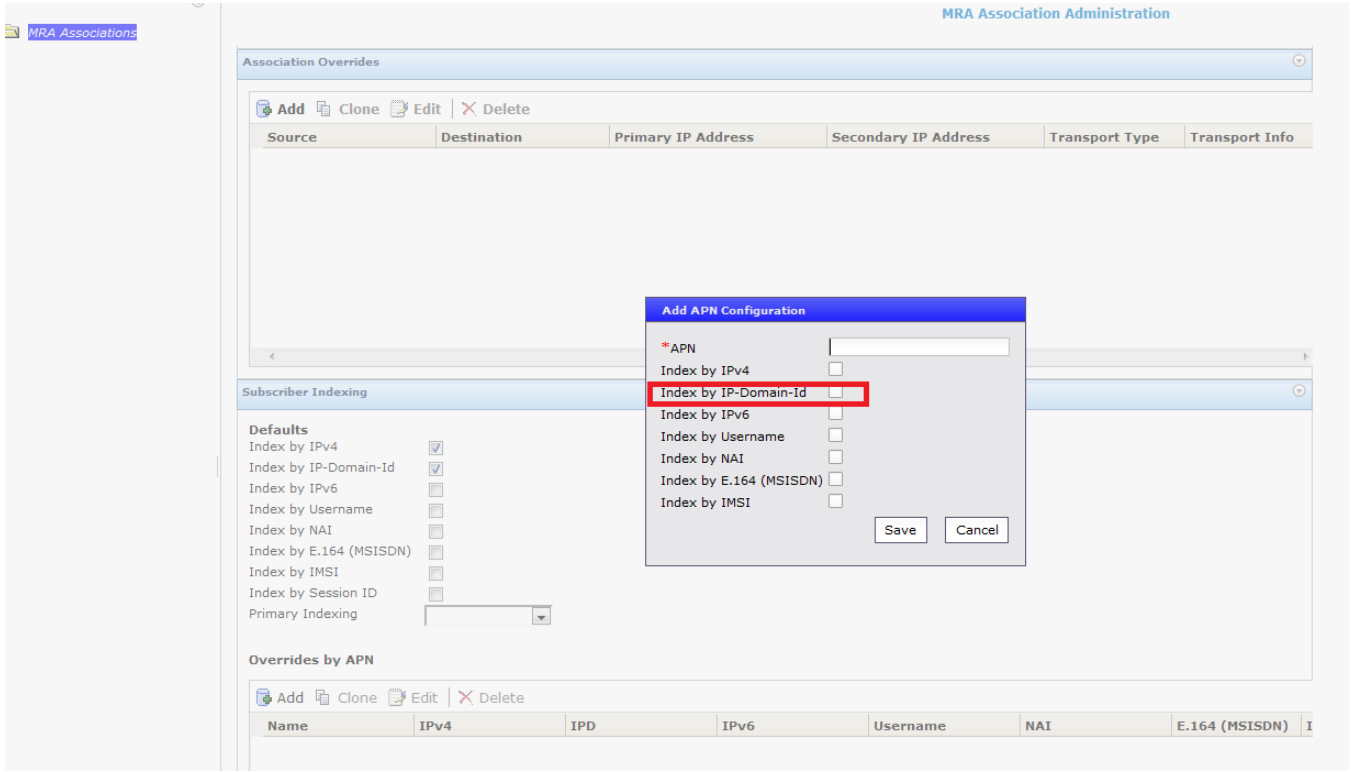


IPD index configuration for MRA association on MRA

There should be a new IPD subscriber indexing for MRA association configuration overrides by APN as following:

1. A check box for IPD index indicates this IPD index is checked or not
2. The configuration settings of DB.INDEXING(n).IndexByIpd of which value is set by the above checkbox should be pushed to MRA. The "n" in DB.INDEXING means it's a list of settings for the related overrides APNs

The UI is as following:

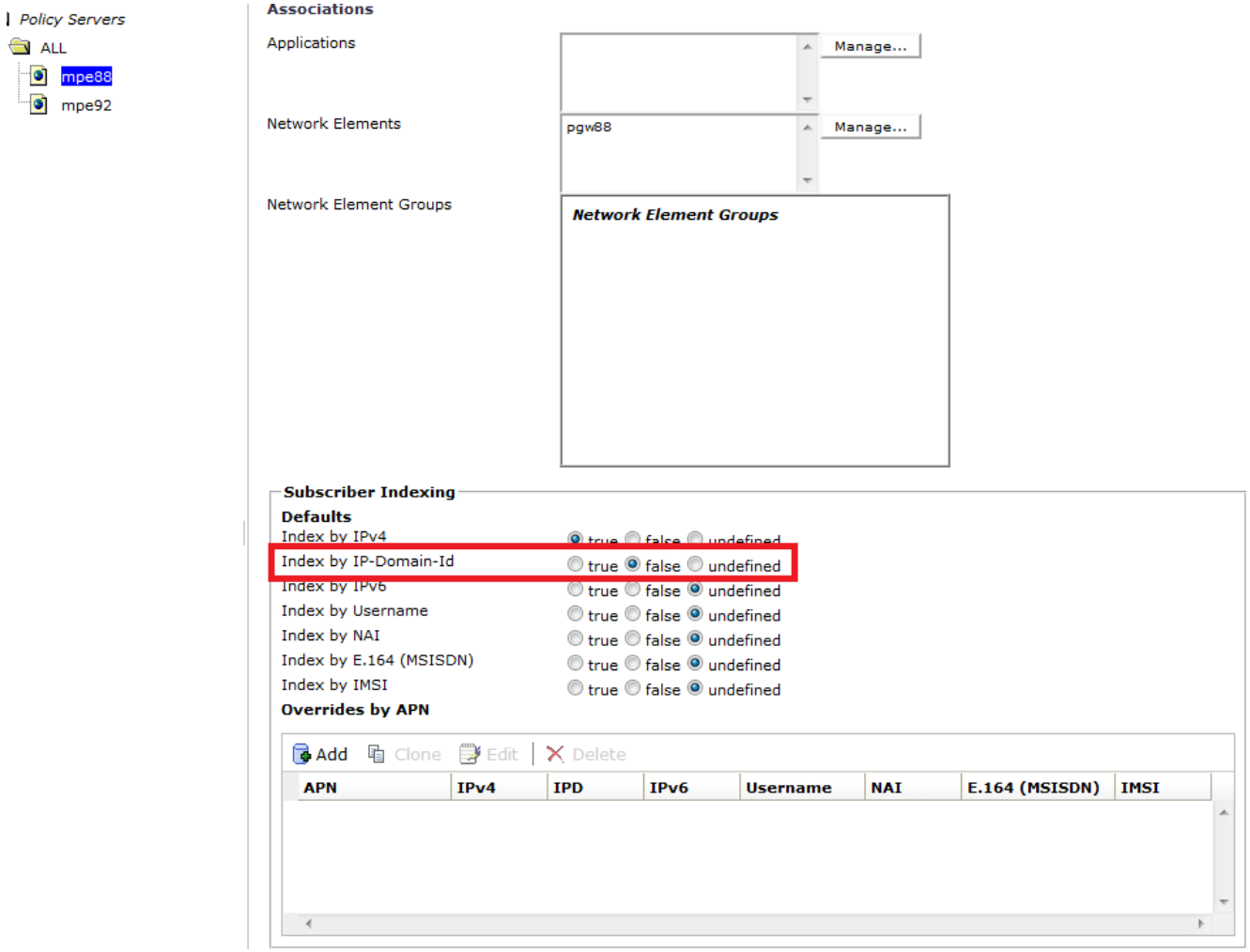


IPD index configuration Overrides By APN for MRA association on MRA

There should be a new IPD subscriber indexing for MPE configuration as following:

1. A check box group for IPD index indicates this IPD index is checked or not
2. The configuration settings of DB.IndexByIpd of which value is set by the above checkbox should be pushed to MPE

The UI is as following:



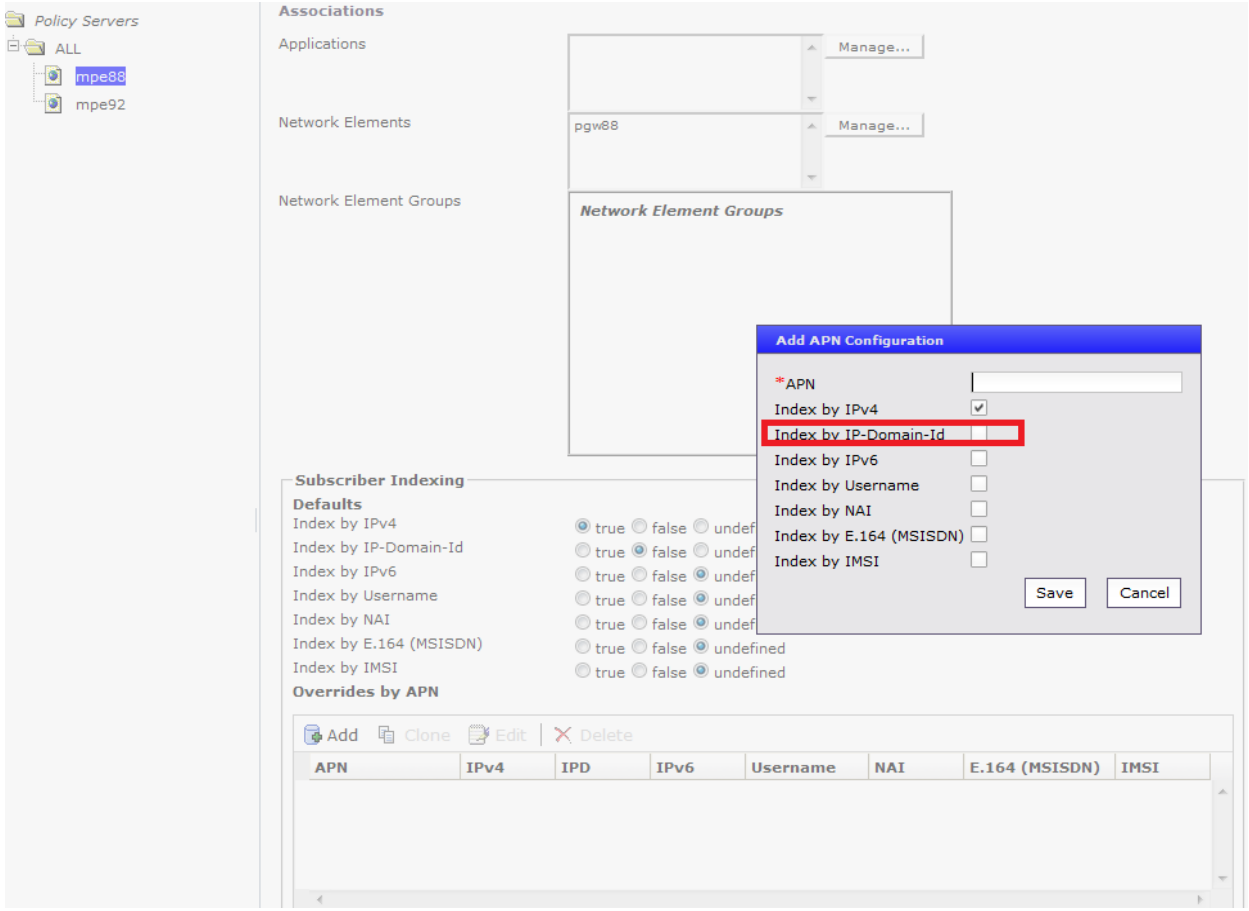
IPD index configuration on MPE

There should be a new IPD subscriber indexing for MPE configuration overrides by APN as following:

1. A check box for IPD index indicates this IPD index is checked or not

2. The configuration settings of DB.INDEXING(n).IndexByIpd of which value is set by the above checkbox should be pushed to MPE. The "n" in DB.INDEXING means it's a list of settings for the related overrides APNs

The UI is as following:



IPD index configuration Overrides By on MPE

3.6.3 Dependency

Currently this feature only supports the GGSN and PGW for IP-Domain-Id binding on the MRA/MPE side.

This feature only support configuring one IP-Domain-ID per Network Element.

IP-Domain-ID can’t be changed without breaking previously established bindings

3.7 SUPPORT FOR HOST BASED ROUTING (BUG 20352083)

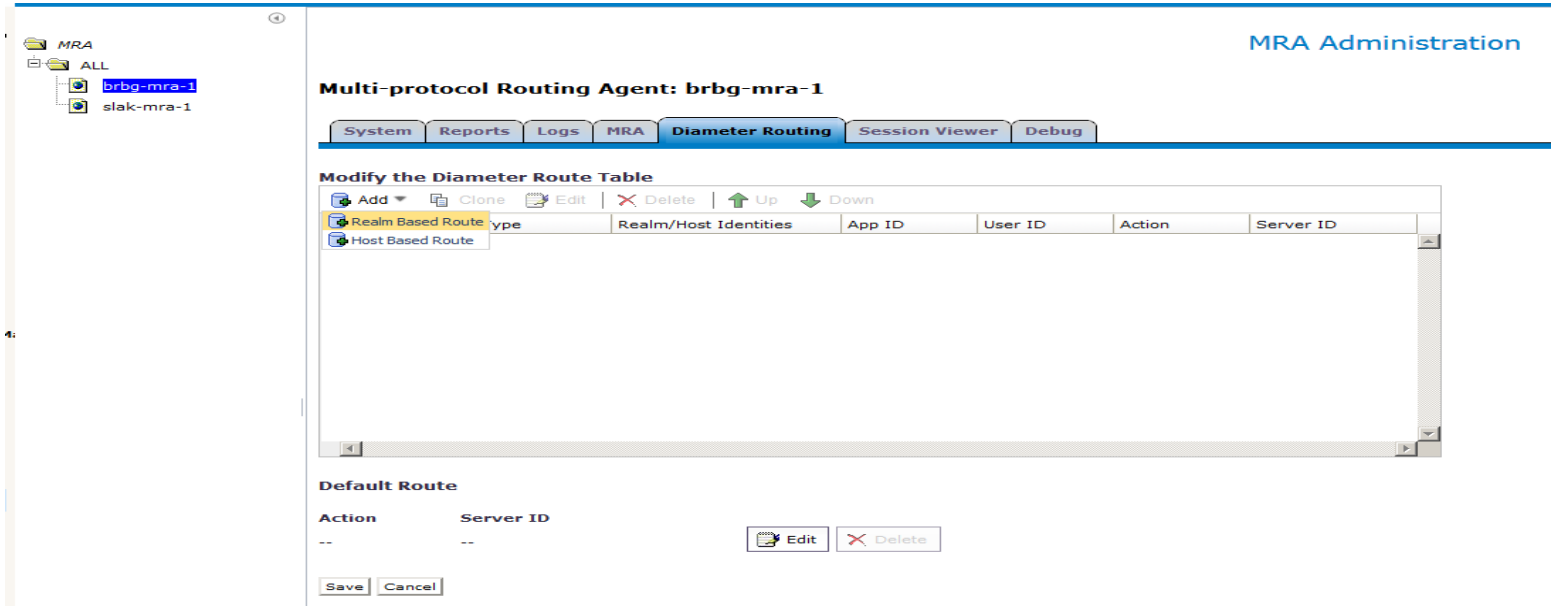
3.7.1 Introduction

This feature enhances the current diameter routing capabilities of the MRA to include host based routing. Host based routing allows a message intended for a specific Destination-Host (which is not directly reachable) to be routed to a specified routing agent or server.

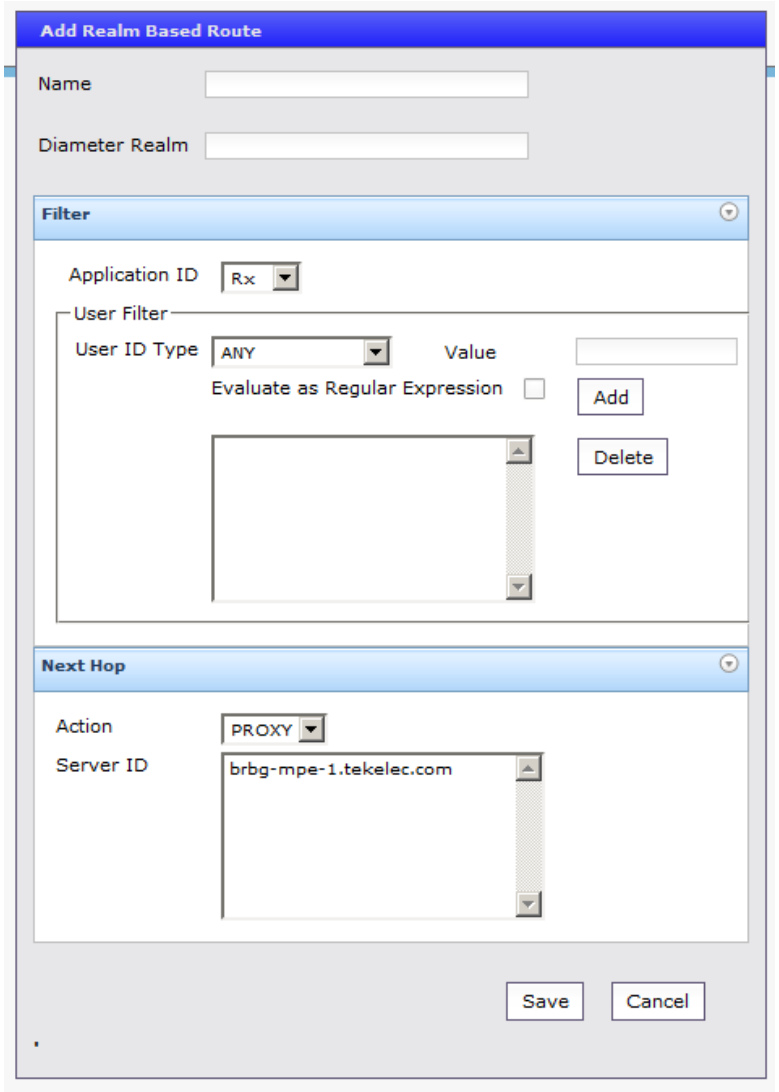
3.7.2 Detailed Description

The host based routing feature enhances the current diameter routing capabilities of the MRA. Currently the diameter routing table allows messages to be routed based on their Destination-Realm and further filters such as UserId(s) and Diameter application (eg. Gx, Rx). However, it may be possible that not all messages for a specific application and realm need to be routed to the same peer. There may be a case where messages intended for a specific Destination-Host or a list of Destination-Hosts needs to be routed to an intermediary peer, since they are not directly reachable. This can now be achieved by creating a Host Based Route in the Diameter Routing table of the MRA

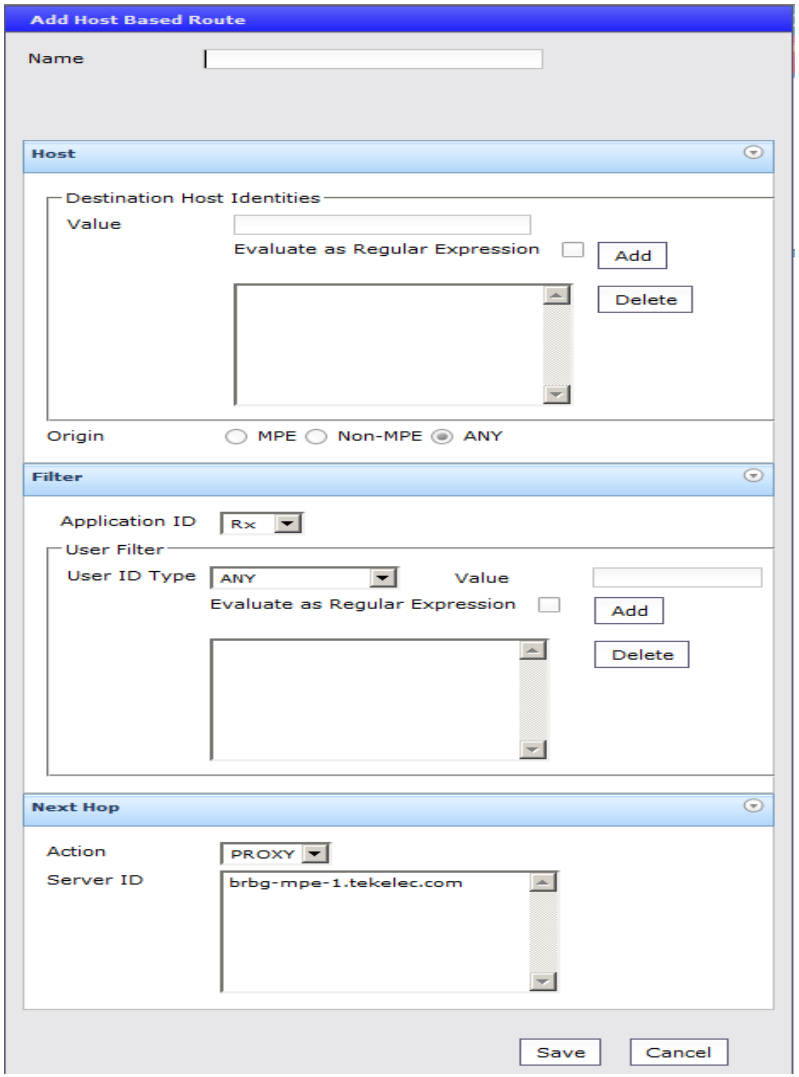
User Interface Changes



The figure above shows the two types of diameter routes to choose from when the "Add" button is clicked. An option to create a Realm or Host Based Route is available. The Realm Based Route is the route type that has been supported in prior releases with just a name change in this release. The Host Based Route is a new type of route that is further described in the following figures.



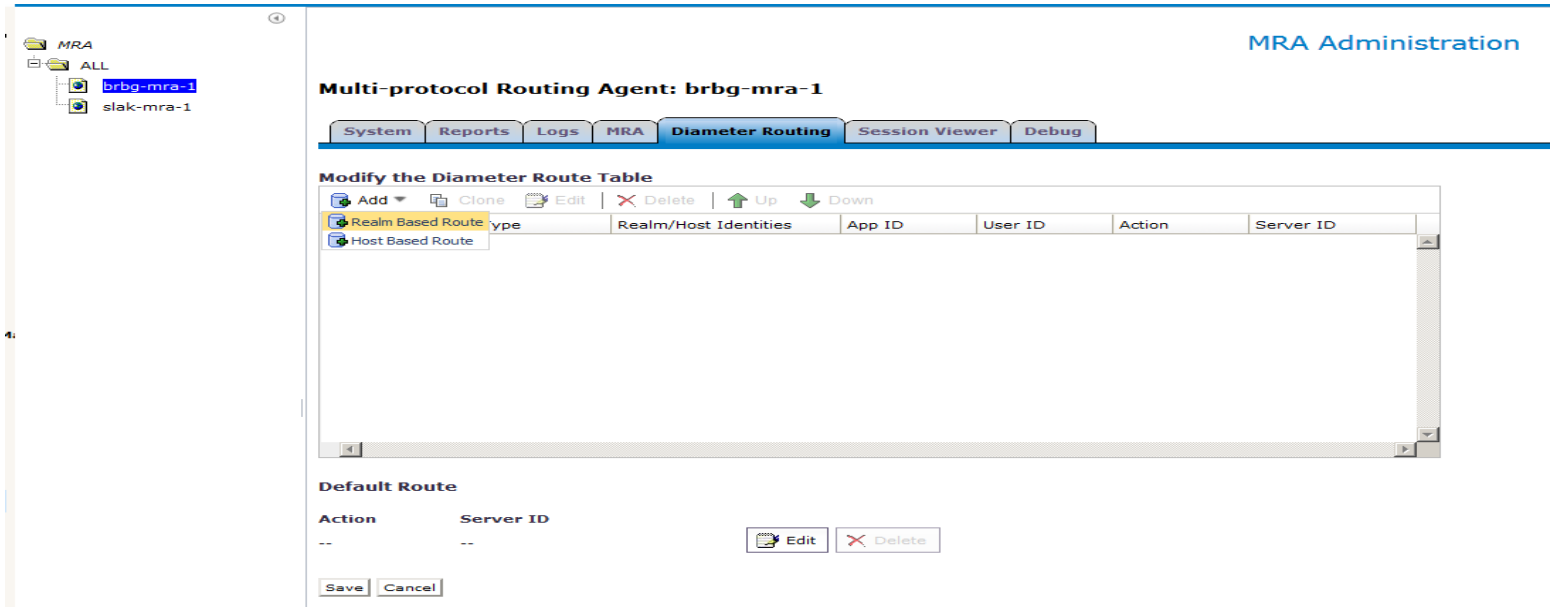
The figure above shows an example of a realm based route. Realm based routes are the original supported type of routes from prior releases. There is no change to their functionality. Previously they were referred to as a "Diameter Route". Also, it is now broken up into sections to organize these settings into a "Filter" and "Next Hop" category.



The figure above shows an example of the new host based route. The first section is called "Host", which contains a few different options, where at least one of these options needs to be selected/configured:

- Option to manually type in any number of host identities, where the values may contain wildcards such as '*' (match any number of characters) and '?' (match only one character). If the "Evaluate as Regular Expression" is checked, then the identity that is added may be evaluated as a regular expression. This field supports a maximum of 255 characters.
- The "Origin" option allows a message to be routed based on its Origin-Host. If the Origin-Host matches an MPE managed by any of the MRA's, then this means it is a MPE originated message. So if this configuration were set to "MPE" then any messages that originated from a managed MPE would apply to this route. By default, this setting is "Any", which means the route applies to any Origin-Host, so the Host Identity may be filled in to narrow this down. If topology hiding is enabled, the message will still be processed based on the original Origin-Host in the routing table. The topology hiding processing takes place after the routing table.

The "Filter" and "Next Hop" sections are carried over from existing functionality that has been supported by the realm based routes. This includes the ability to select 1 or more Server ID's, which allows a primary and backup to be chosen for example. The order of this list is determined by the peer table and thus the first one chosen in the list would become the primary. However, it is recommended to create a separate route for each server if a primary, backup, etc. is desired so the priority can be controlled by the order of the routing table itself.

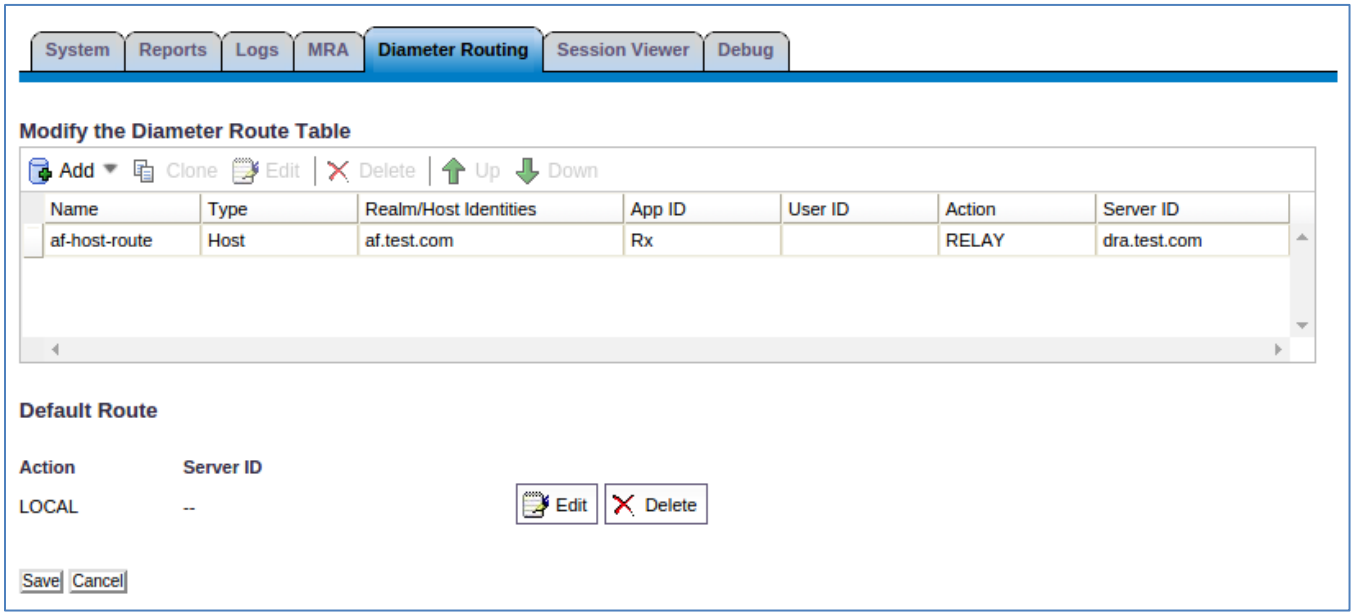


The figure above shows the updated routing table for support for both realm and host based routes. The table will now have additional columns for "Name" and "Type". The "Realm/Host Identities" column will display the realm value for the route if it is a "Realm" type. The "Host" type route will display the Origin setting, as well as the number of Host Identities that have been configured for this route. The remaining columns stay unchanged from prior functionality.

Call Flow Changes

The PCRF will now be able to route messages based on the destination-host or host based routing. If no Destination-Host is provided in a message and a host based route is configured with a host identity, then the route will not be a match. The message will continue to be processed further by the other routes in the table.

3.7.2.1 Host Example with Stateful MRA



Host Route with Stateful MRA

The figure above shows a host route used together with a stateful MRA. The host route is configured to send messages with a Destination-Host of af.test.com for Rx messages to the peer identity dra.test.com.

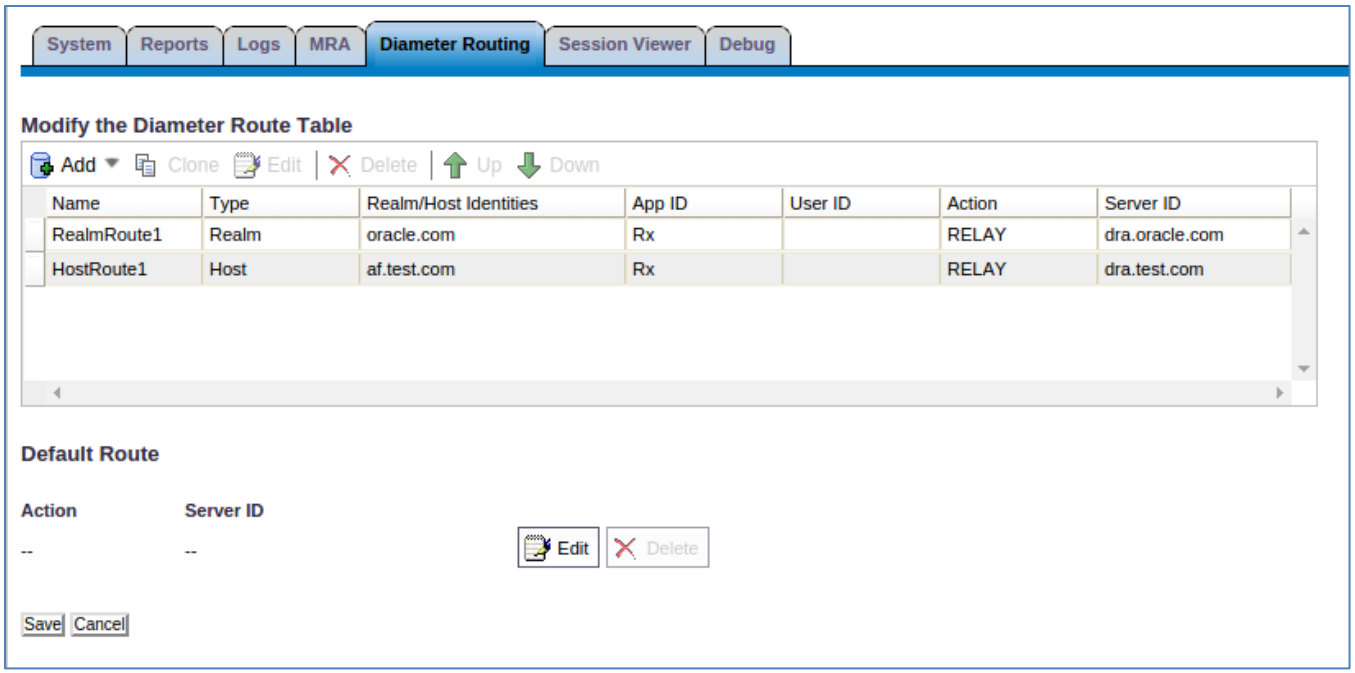
Any other type of message, such as Gx and other Rx messages with a different Destination-Host or no Destination-Host altogether, would get processed locally as indicated by the Default Route of LOCAL.

Any message that is processed locally would then be processed by the stateful MRA, where looking up and creating bindings would take place.

NOTE: Once a route is created in the routing table, there must be a local route created in order for the stateful MRA to be utilized.

3.7.2.2 Realm and Host Example

The following is an example of how the routing table on the PCRF now works with both host based routing and realm based routing.



Host-Based Route Example

Scenario 1:

An Rx message is received by the PCRF with a Destination-Host of af.test.com and Destination-Realm of test.com. The PCRF will check to see if it can send the message directly to af.test.com, however there is no connection to a peer with that identity. The message will then go through the routing table, and the first match that is found finds a host-based route matching that destination-host. The Rx message will be routed to the peer with identity dra.test.com.

Scenario 2:

An Rx message is received by the PCRF with a Destination-Host of af.oracle.com and Destination-Realm of oracle.com. The PCRF will check to see if it can send the message directly to af.oracle.com, however there is no connection to a peer with that identity. The message will then go through the routing table, and the first match that is found finds a realm-based route matching the realm of oracle.com. The Rx message will be routed to the peer with identity dra.oracle.com.

3.8 GENERIC NOTIFICATION FROM POLICY SYSTEM (BUG 19982653)

3.8.1 Introduction

The 'Generic Notifications from Policy System' feature provides a way for operators to generate custom notifications to available web services. Notifications will generated by a new policy action. The destination, content and attributes of the notification will be configurable by the operator and allows for flexible notifications within a HTTP request message

3.8.2 Detailed Description

The 'Generic Notifications from Policy System' feature describes new policy actions that generate an outbound HTTP request targeted to a user configured destination. The intent is to provide a way for customers to generate generic notifications to available web services through policy. By having a general method for doing this, the PCRF provides a client interface to services in place at customer sites. This may avert having to schedule and implement customized solutions into the product for different providers

There are two ways for users to define the 'destination' field of the Send Policy Notification action. The user can define the URL directly into the policy. This allows for cases where the URL itself may be dynamic, based on policy variable substitution. For example: http://10.15.20.190:80/rs/quota/notify/{User.MSISDN}.

The second method for defining a destination will be through configuration. The CMP will have a new section where users will have the option to predefine destinations. For services with URLs that will generally not change, ex http://10.15.20.190:80/rs/quota/notify/setQuotaService,

The MPE shall establish a persistent connection towards 10.15.20.190:80 after splitting the hostname/port from the URL. This will improve performance by eliminating the overhead of having to establish a dynamic connection at the time of each request. Operator can still define dynamic URL based on policy variable substitution.

The persistent connection thus established will be maintained with a keep alive and monitored for problems. The monitor will be responsible for reestablishing lost connections and reporting errors. Connection problems with any of the user defined services will result in Alarms and Warning Trace Logs to alert the user to the problem. The number of connections to establish for a given destination resource will be configurable. It will allow for multiple connections to be available to the threads attempting sending notifications.

Policy Changes

Two new Policy Actions shall be defined to generate flexible HTTP requests: One for sending Notifications via persistent connections and another for sending Notifications via dynamic connections.

Policy Changes – Dynamic destination

Policy Condition Group	Policy Condition or Action	Description
Action	Send http *action* notification to url *URL* with	Send a HTTP request to specified destination. The fields

	headers *headers* and content *content*	'destination', 'headers', 'content' are all free-flowing text fields to be configured by operator.

CMP shall support configuring above Policy Actions as one of actions under Policy Library -> Create Policy -> Actions -> Optional Actions

The 'destination' field is free flowing text field – user can define the 'destination' URL directly into the policy. This allows for cases where the URL itself may be dynamic, based on policy variable substitution. For example: http://10.15.20.190:80/rs/quota/notify/{User.MSISDN}.

The 'action' field shall be a 'drop-down' having values 'GET', 'PUT', 'POST', 'DELETE'. Operator shall be able to choose one of the values in the action field.

The 'headers' field shall be a pop-up box with 2 fields: 'Header Type' and 'Value'. Both fields shall be free-flowing text fields. There shall be no validation whether particular header type is a valid HTTP header. Similarly, there shall be no validation whether the 'value' corresponds to 'header type'. Operator shall be able to add up to 20 such rows of 'header type' and 'values' in a single policy.

The 'content' field is also 'free-flowing' text field which allows for any type of notification like JSON/ XML/ Text message in the body of HTTP request. 'Content' field shall also allow for policy variable substitution. MPE shall not validate whether the 'header' value corresponds to particular 'content'.

Policy Changes – Static destination

Policy Condition Group	Policy Condition or Action	Description
Action	**Send http action notification to select notification destination with headers headers and content content**	Send a HTTP request to pre-defined destination.

For pre-defined destinations, the 'destination' field is a pop-up that will list the pre-defined destination URLs already configured by operator and operator shall select one of them.

The 'action', 'headers' and 'content' field shall be same as described above for dynamic destination.

Note: Policy substitution is still allowed for URLs in pre-defined destinations. Also, it shall be possible that while defining dynamic-destination URL, the IP/port is defined as IP/port of one of the static destination. In that case, the notification message shall be sent through static connections already established.

3.8.2.1 Example New Policy Actions

Below are present some examples of how the policy action can be used by operator:

Example 1: HTTP GET with query params:

send http "GET" notification to "http://10.15.20.190:80/rs/quota/notify?msisdn={User.MSISDN}&quota={User.Quota.Foo.volume}" with "Content-Type: text/plain" and ""

Example 2: JSON POST:

send http "POST" notification to "http://10.15.20.190:80/rs/quota/jsonnotify/{User.MSISDN}" with "Content-Type: application/json" and "{"class":"Subscriber","entitlement":"Extended Service","msisdn":"{User.MSISDN}","name":"{User.name}"}"

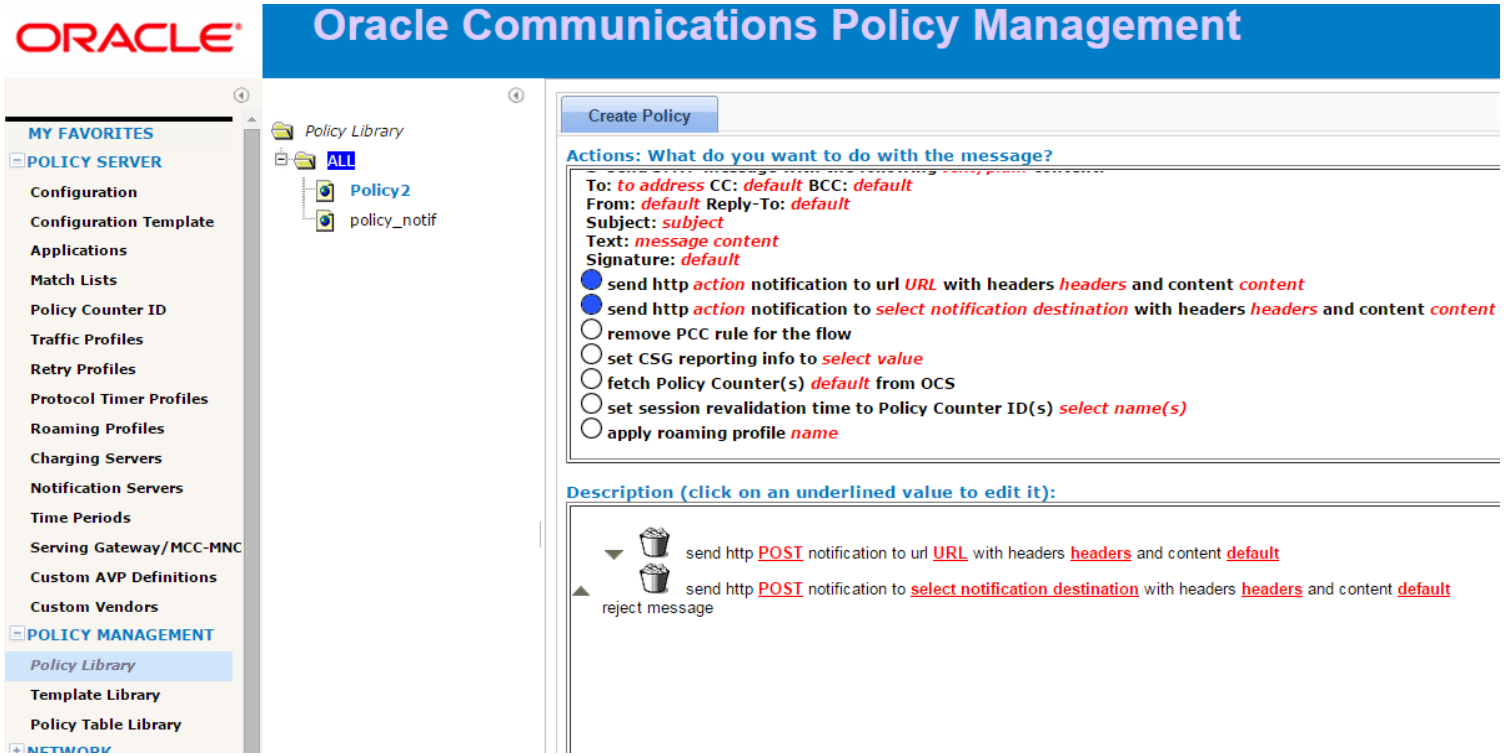
Example 3: XML POST:

send http "POST" notification to "http://10.15.20.190:80/rs/quota/xmlnotify" with "Content-Type: text/xml;charset=UTF-8" and "<?xml version="1.0" encoding="UTF-8"?> <subscriber><msisdn>{User.MSISDN}</msisdn><quota>{User.Quota.Foo.volume}</quota></subscriber>"

User Interface Changes

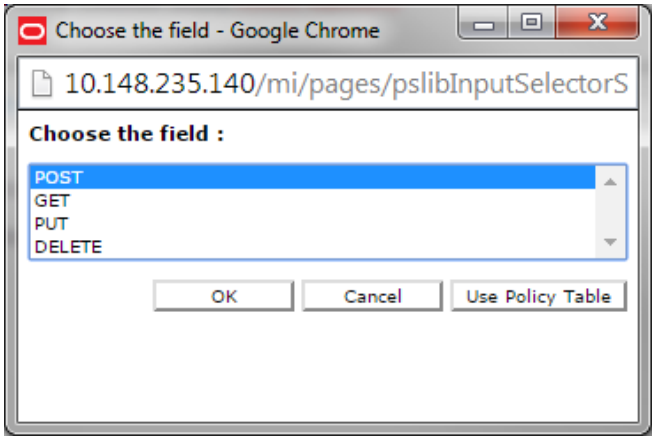
3.8.2.2 Policy Creation – Static and Dynamic Policies in optional Actions

Under POLICY MANAGEMENT -> Policy Library -> Create Policy -> Actions:



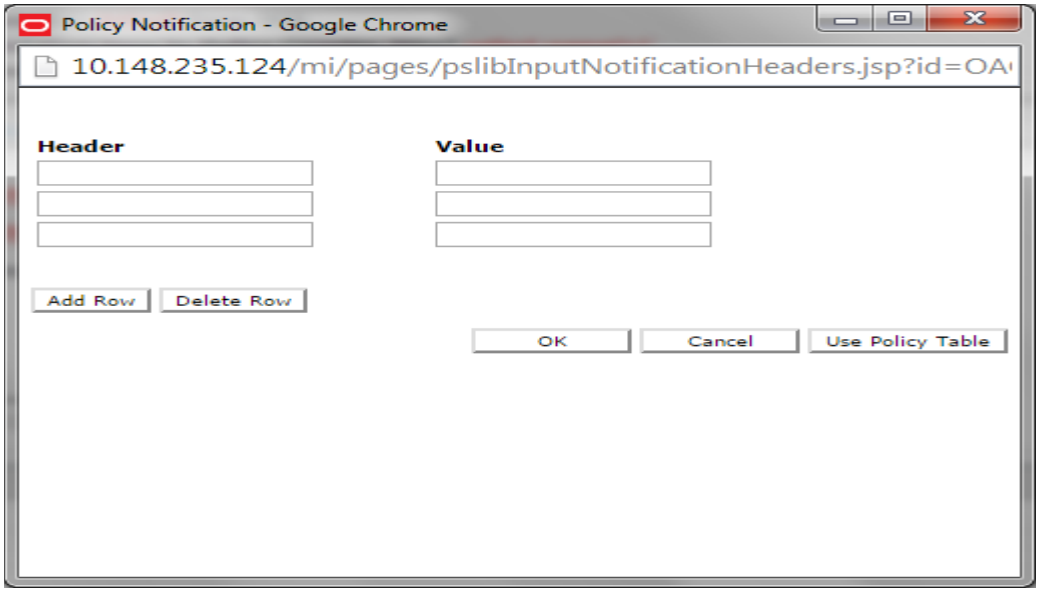
Policy Creation – Static and Dynamic Policies in optional Actions

3.8.2.3 Policy Creation - http Action Selection



Policy Creation - http Action Selection

3.8.2.4 Policy Creation - http Header Selection

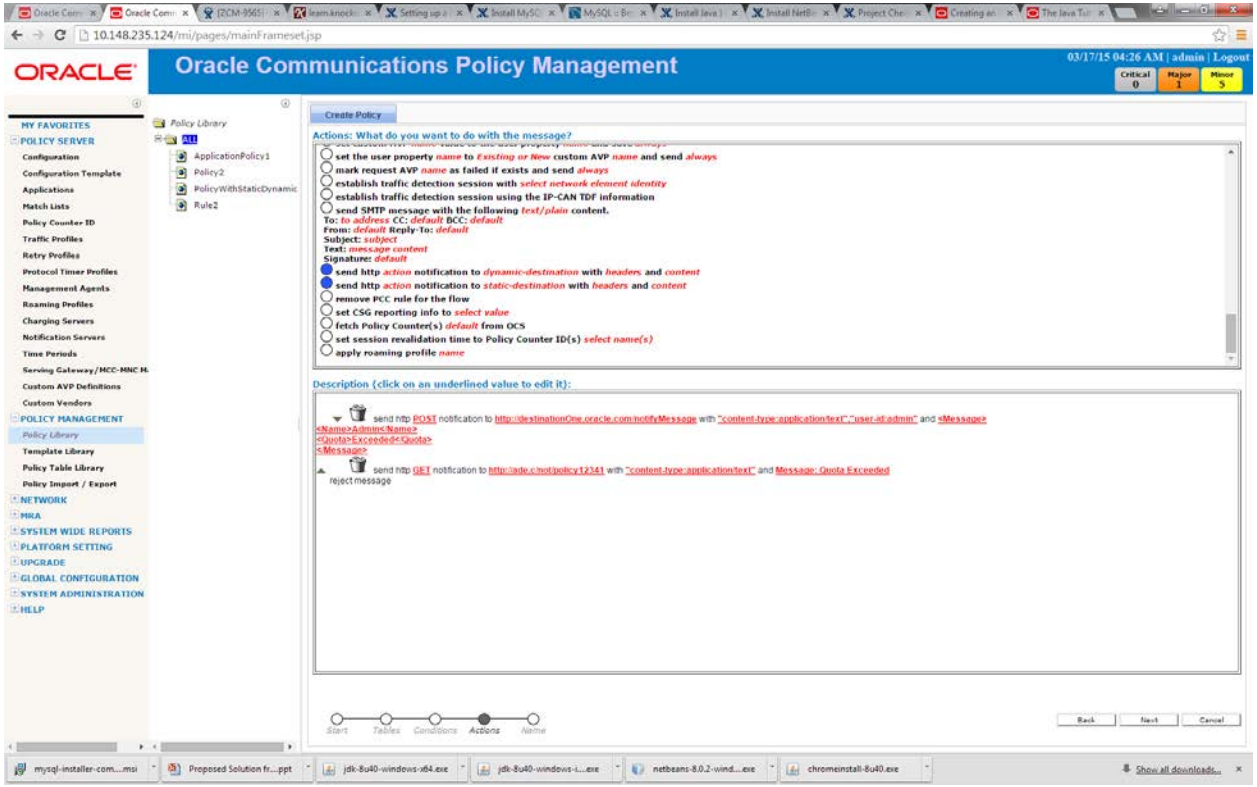


Policy Creation - http Header Selection

3.8.2.5 Policy Creation – Content

Policy Creation - content

3.8.2.6 Policy Creation with values



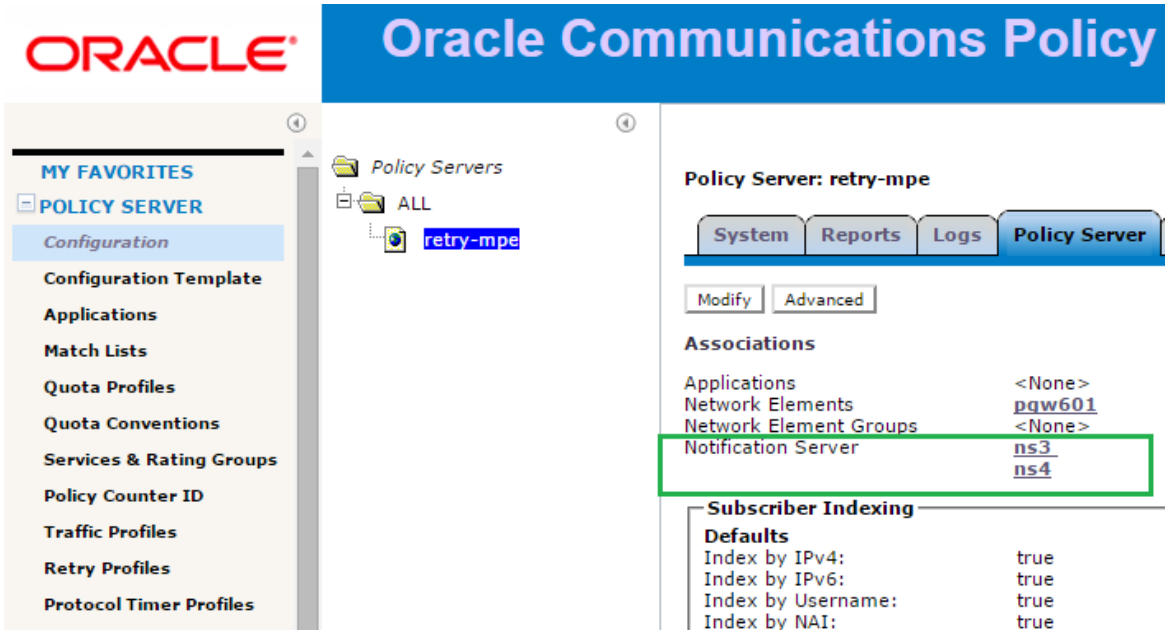
Policy Creation – with Values

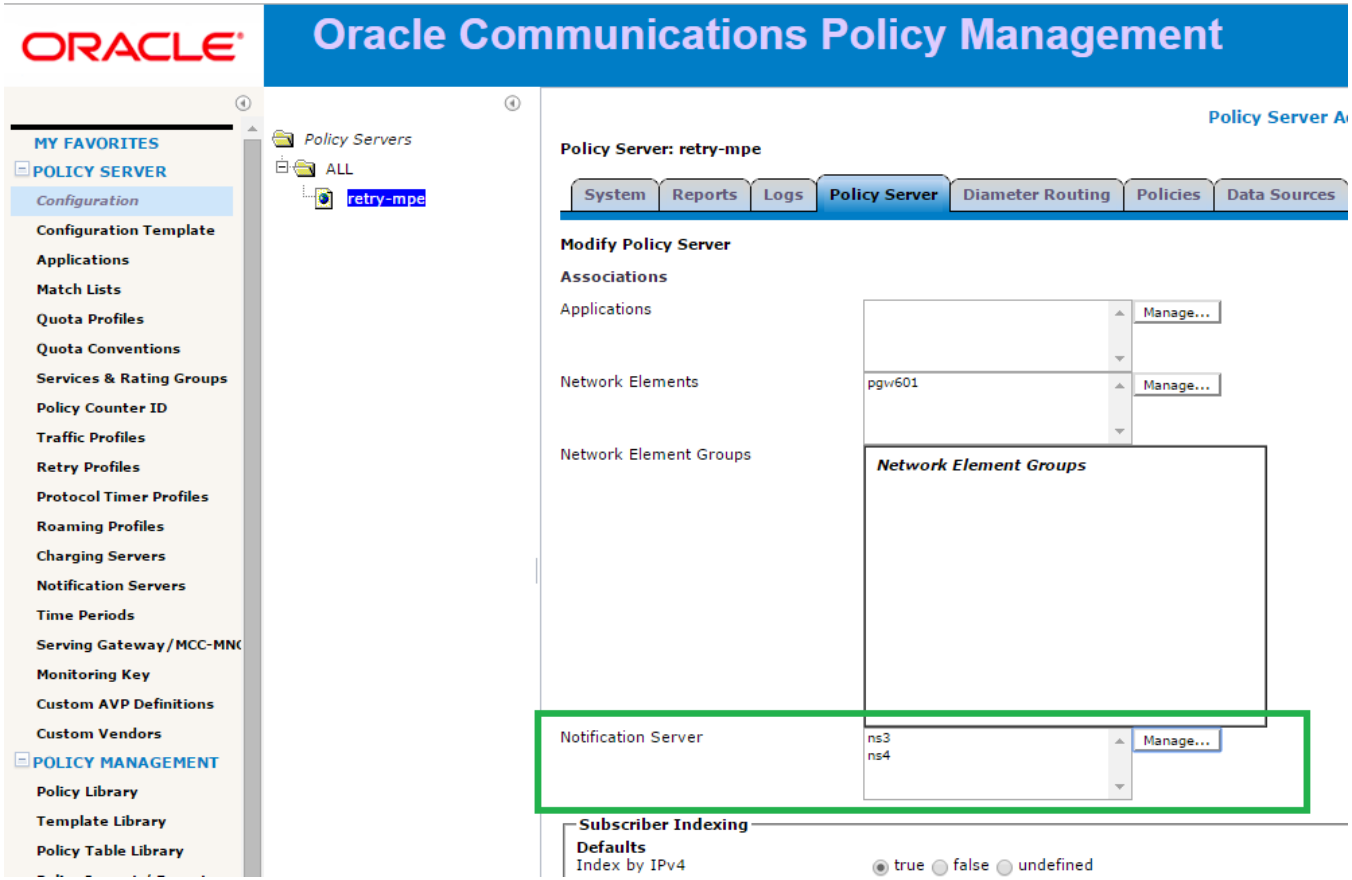
3.8.2.7 Notification Server Administration

Below is screen to configure new Notification Server. While creating the server, it can be associated to a particular MPE as shown.

Notification Server Admin

3.8.2.8 Notification Server Mapping – under Policy Server



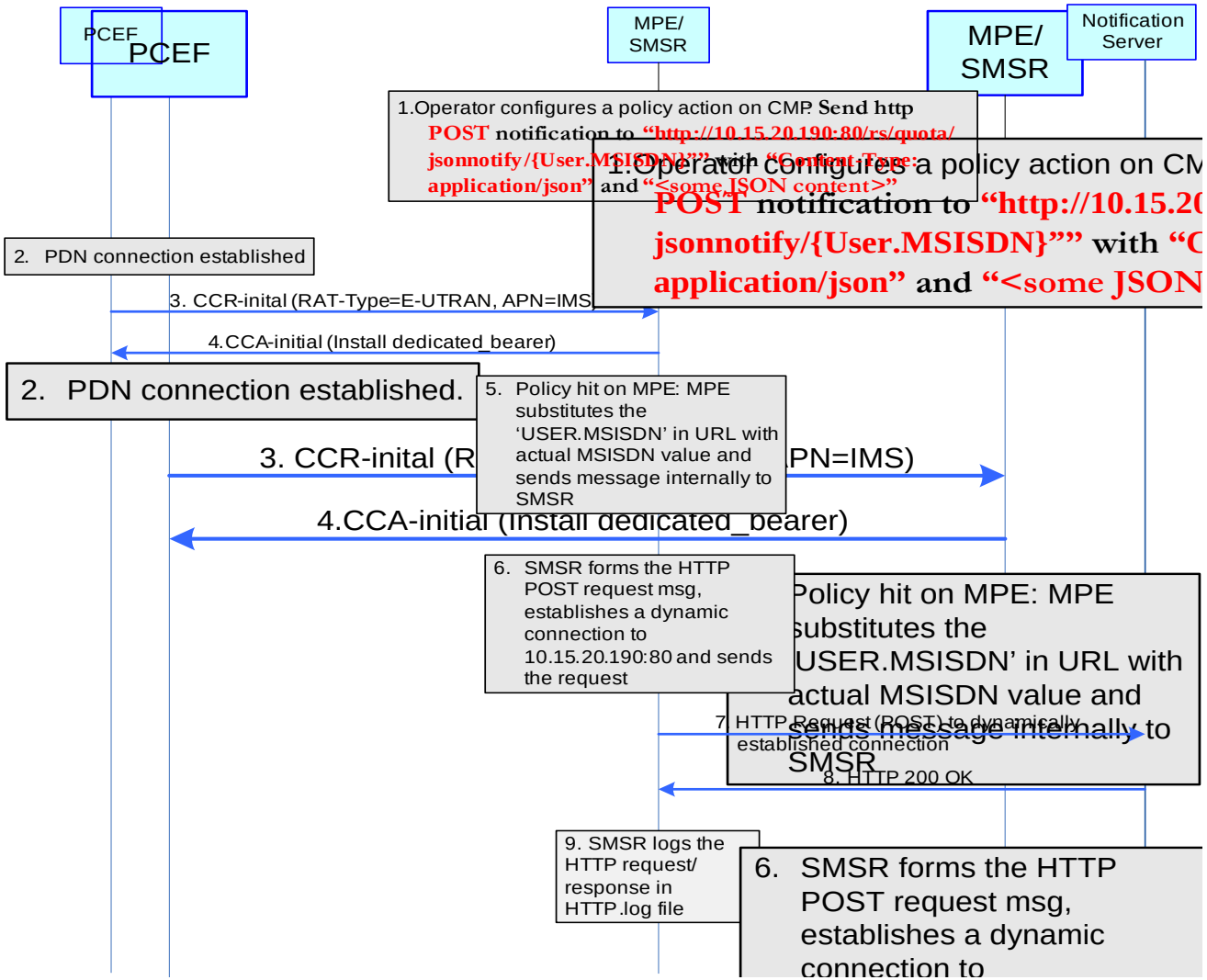


Notification Server Mapping- Under Policy Server

Call Flow Changes

The HTTP response status codes will be processed but no action shall be taken based on response code. Any response within the 200 range indicates the request was received and accepted. DEBUG level Trace Logs will be generated can be used to track successful requests. Responses with status ranges of 400 and 500 signify error and will result in WARNING level Trace Log messages for alerting the user. Trace Log messages will provide details of both the request and response. For error cases (HTTP 500 range) the body of the response may provide details for the error. No message retries shall be done for error response codes.

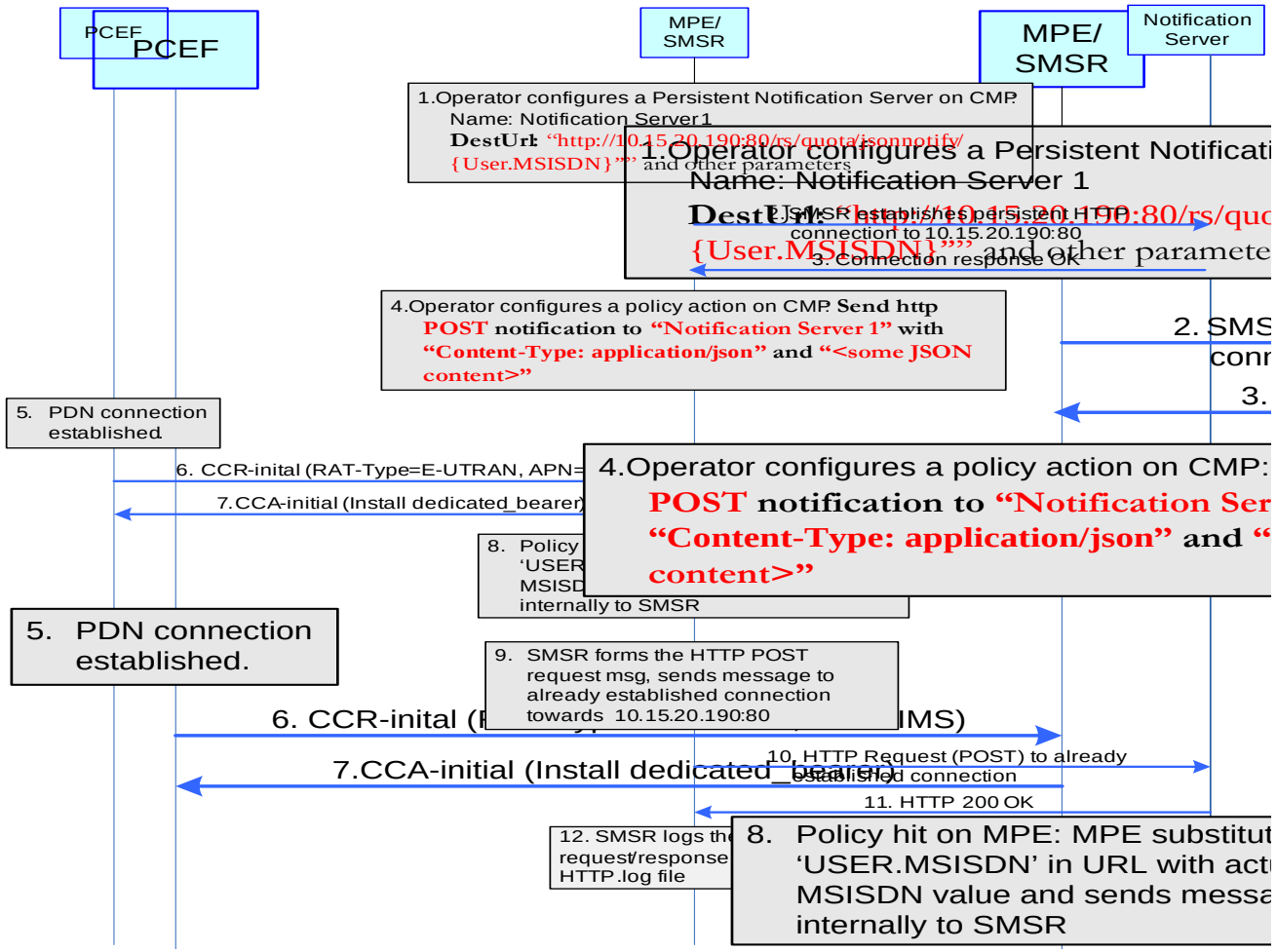
3.8.2.9 HTTP notification to dynamic connection



3.8.2.10 HTTP notification to static connection

When the operator configures a Persistent Notification server, the SMSR shall establish connections to any newly defined destinations and close and re-establish to any modified connections. Should a connection attempt fail it will be retried at constant intervals as per the configured connection retry value. **TODO**: When

to stop retrying and mark connection as closed?. At the time of policy execution if a policy notification is triggered with a target destination for which a connection does not exist, the notification message shall be dropped generating a Warning Trace Log.



3.9 NETLOC PROCEDURES FOR TRUSTED WLAN (PR 19867434)

3.9.1 Introduction

The PCEF provides the PCRF with the access network information, with the user location information that, if available, is included in the TWAN-Identifier AVP if the NetLoc-Trusted-WLAN is supported. And the PCRF shall forward this info to the AF if requested.

3.9.2 Detailed Description

The intention of this feature is to allow support of TWAN connected to EPC as IPCAN, to make the TWAN ID location which consists of SSID, BSSID, Civic Address Info, PLMN ID, Operator Name, Relay identity, circuit ID that the UE is camped on available to the IMS nodes when the mobile operator needs to record this information either to fulfill legal obligations or for charging purposes, especially at the set-up and release of an IMS communication over a TWAN.

3.10 NETLOC UPDATES (3GPP R12) (PR 19720493)

3.10.1 General Description

The current 3GPP Specification includes updates to the NetLoc behavior not included in previous releases. This feature is designed to comply with current 3GPP specification regarding NetLoc-Access-Support and NetLoc-RAN-NAS-Cause capabilities.

3.10.1.1 Feature Abstract

The PCRF will have the capability to run policy conditions on all SDP attributes/descriptors, check their existence and values and act accordingly. One of many actions that the PCRF can take is, setting proper bandwidth values on related PCC rules.

3.10.2 Detailed Description

- NetLoc-Access-Support Feature with a new AVP "AN-Trusted"

Current NetLoc procedures are ambiguous and incomplete with regards to the handling of following two cases:

1) IP-CAN type does not support access network information retrieval

2) IP-CAN type supports access network information retrieval but information isn't provided to the PCEF.

So added a new feature NetLoc-Access-Support to explicitly indicate to the PCRF why the requested access network information wasn't provided and the PCRF can notify AF about the indication for further processing.

- NetLoc-RAN-NAS-Cause Feature

When IP-Can session release/Bearer release, an operator may need to get, beyond the ULI information, detailed RAN and/or NAS release cause codes information from the access network to be included in the S-GW and PDN GW CDRs for call performance analysis, User QoE analysis and proper billing reconciliation. Also, for IMS sessions, the operator may need to get the above information available at the P-CSCF. The "RAN/NAS Release Cause" is transparently transmitted by the SGW to the PGW and from the PDN GW to the PCRF if available.

Policy Changes

Policy Condition Group	Policy Condition or Action	Description
"Request" **Conditions**	Where the RAN-NAS-Release-Cause is ***Protocol Type*** and ***Cause Type***	Check the value of RAN-NAS-Release-Cause in request. *is: matches the value selected.* *value : 2 lists , one is Protocol type, one is Cause type. Protocol type and Cause type compose a value.*

"Request" **Conditions**	where the rule report contains RAN-NAS-Release-Cause and is ***Protocol Type*** and ***Cause Type***	Check the value of RAN-NAS-Release-Cause in Charging-Rule-Report. *is: matches the value selected.* *value : 2 lists , one is Protocol type, one is Cause type. Protocol type and Cause type compose a value.*

3.11 SINGLE RADIO VOICE CALL CONTINUITY (vSRVCC) (PR 20883677)

3.11.1 Introduction

This feature is to support a new AVP Rule, PS-to-CS-Session-Continuity to the Charging-Rule-Definition AVP in the PCC rule via Gx interface. This value will be used to indicate that the service data flow carries video and is a candidate for PS to CS session continuity.

3.11.2 Detailed Description

The Charging-Rule-Definition AVP (AVP code 1003) is of type Grouped, and it defines the PCC rule sent by the PCRF to the PCEF. The Charging-Rule-Name AVP uniquely identifies the PCC rule and it is used to reference to a PCC rule in communication between the PCEF and the PCRF within one IP CAN session as defined in **3GPP TS 29.212 section 5.3.4**.

In Charging-Rule-Definition AVP, **PS-to-CS session continuity** AVP is added to Charging-Rule-Definition AVP to support this feature [3GPP TS 29.212 V12.4.0 section 5.3.84]. PCRF shall support this AVP.

Note: Versions 12.0 and earlier do not support this AVP. This rule is being added to be in compliance with 3GPP.

AVP Format:

The PS-to-CS-Session-Continuity AVP indicates if a service data flow is a candidate for PS to CS session continuity.

Charging-Rule-Definition ::= < AVP Header: 1003 >
{ Charging-Rule-Name }
[Service-Identifier]
[Rating-Group]
*[Flow-Information]
[TDF-Application-Identifier]
[Flow-Status]
[QoS-Information]
[PS-to-CS-Session-Continuity]
[Reporting-Level]
[Online]
[Offline]
[Metering-Method]
[Precedence]
[AF-Charging-Identifier]
*[Flows]
[Monitoring-Key]
[Redirect-Information]
[Mute-Notification]
[AF-Signalling-Protocol]
[Sponsor-Identity]

[Application-Service-Provider-Identity]
*[Required-Access-Info]
[Sharing-Key-DL]
[Sharing-Key-UL]
*[AVP]

The PS-to-CS-Session-Continuity AVP (AVP code 1099) is of type Enumerated, and indicates whether the service data flow is a candidate for PS to CS session continuity as specified in 3GPP TS 23.216 [9].

The following values are defined:

VIDEO_PS2CS_CONT_CANDIDATE (0)

This value is used to indicate that the service data flow carries video and is a candidate for PS to CS session continuity. The provider can define this rule on "Traffic Profiles" page on CMP.

Attribute Name	AVP Code	Clause defined	Value Type (NOTE 2)	AVP Flag rules (NOTE 1)					Acc. Type	Applicability (notes 3, 9)
				Must	May	Should not	Must not	May Encr.		
PS-to-CS-Session-Continuity	1099	5.3.84	Enumerated	V	P			Y	3GPP-EPS	Both vSRVCC

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see RFC 3588 [5].
NOTE 2: The value types are defined in RFC 3588 [5].
NOTE 3: AVPs marked with "CC" are applicable to charging control, AVPs marked with "PC" are applicable to policy control and AVPs marked with "Both" are applicable to both charging control and policy control. AVPs marked with "ADC" are applicable to application detection and control. AVPs marked with "ABC" are applicable to application based charging.
NOTE 9: AVPs marked with a supported feature (e.g. "Rel8", "Rel9", "IFOM" or "EPC-routed") are applicable as described in subclause 5.4.1.

AVP description as defined in TS 29.212 (Table 5.3.1)

The following diagram, from 3GPP TS 23.203, shows the basic network architecture.

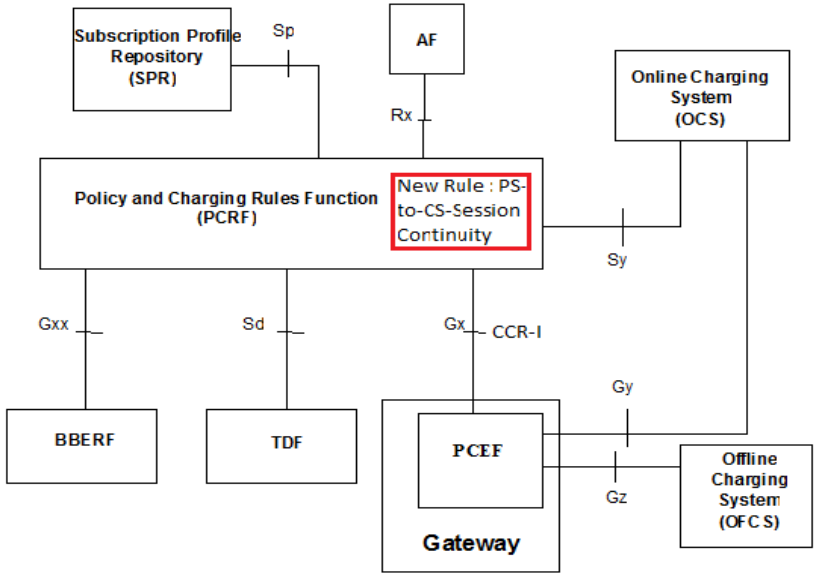


Figure 1 - Basic Network Architecture

PCC Procedures over Gx interface

There are 2 procedures through which PCRF can communicate PCC rules to PCEF over Gx interface. They are –

- **Pull Procedure**

  In this procedure, the PCEF shall indicate, via the Gx reference point, a request for PCC rules in the following instances.

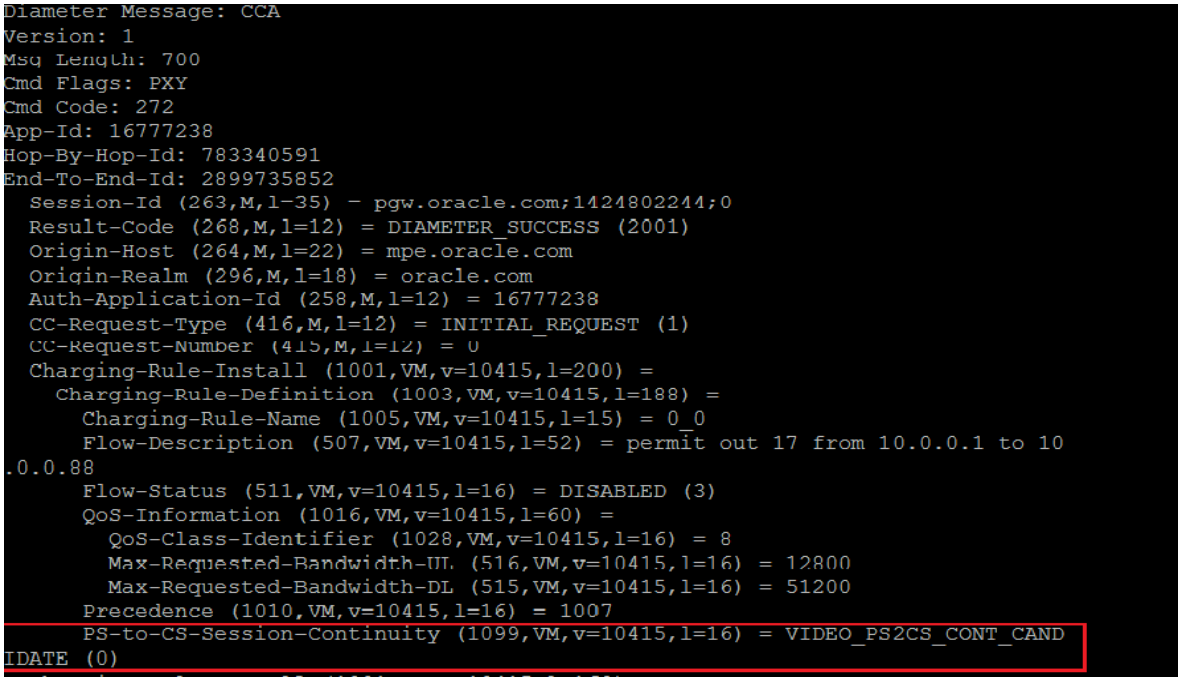
A) **Session Establishment**:

1. PCEF sends a CC-Request with CC-Request Type AVP set to the value “Initial Request” along with user Identification and other attributes to PCRF.
   Example of CCR –

ccr gx -request=initial -userimsi=123456789123456 -framedip=10.0.0.88 -ratt=eutran -ipcantype=5 -user164=15084869996 -operation=1 -bearerid=101 -set tft1.precedence=7 -set tft1.filter="permit out 17 from 10.0.0.1 to assigned" -set tft1.class=0x10 -set qos.class=8 -set qos.upmax=12800 -set qos.downmax=51200 -calledstationid=apn2.com -nrs=1 -usernai=someone@oracle.com

2. In response to the request made by PCEF, PCRF provisions the new dynamic rule containing a value for PS-to-

   CS-Session-Continuity via Gx reference point in the CC-Answer (See Figure Below)

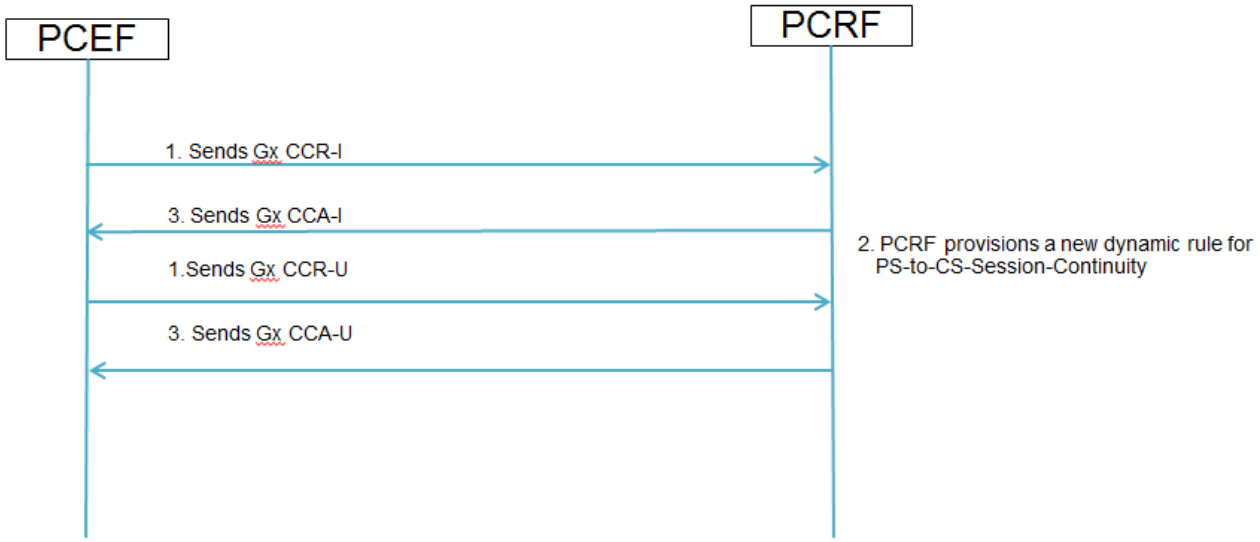


Diameter Message with the new provisioned rule

B) **Session Update**:

1. The PCEF sends a CC-Request (CCR-U) with CC-Request-Type AVP set to the value

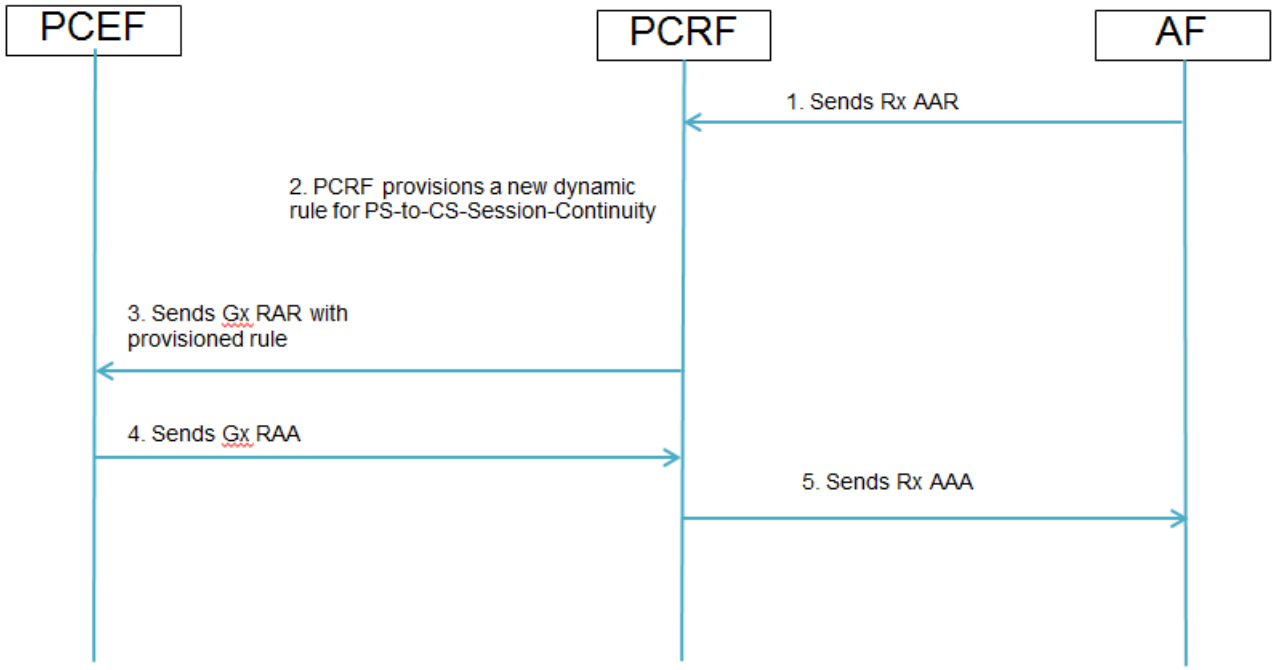
   "UPDATE_REQUEST".
2. PCRF provisions the new dynamic rule containing the value, VIDEO_PS2CS_CONT_CANDIDATE (0) for PS-to-CS-Session-Continuity via Gx reference point in the CC-Answer -UPDATE (CCA-U)



Session Establishment, Session Update (Pull Procedure)

- **Push Procedure**

  In this procedure, the PCRF may decide to provision PCC rules without obtaining any request from the PCEF. This could be in response to information provided by AF over Rx interface, or internal trigger within the PCRF. The PCRF sends these PCC rules in ***Re-Auth Request (RAR) message***. The PCEF sends ***Re-Auth Answer (RAA) message*** in response to the RAR message.



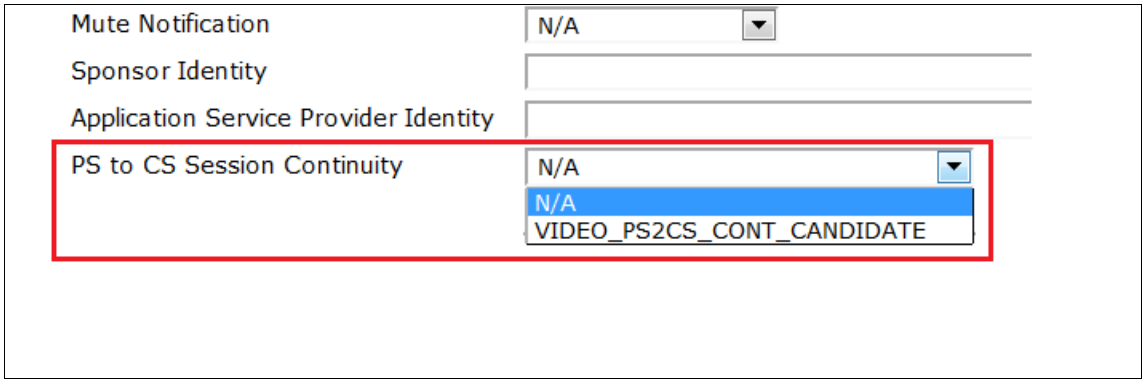
Session Re-Auth Request (Push Procedure)

User Interface Changes

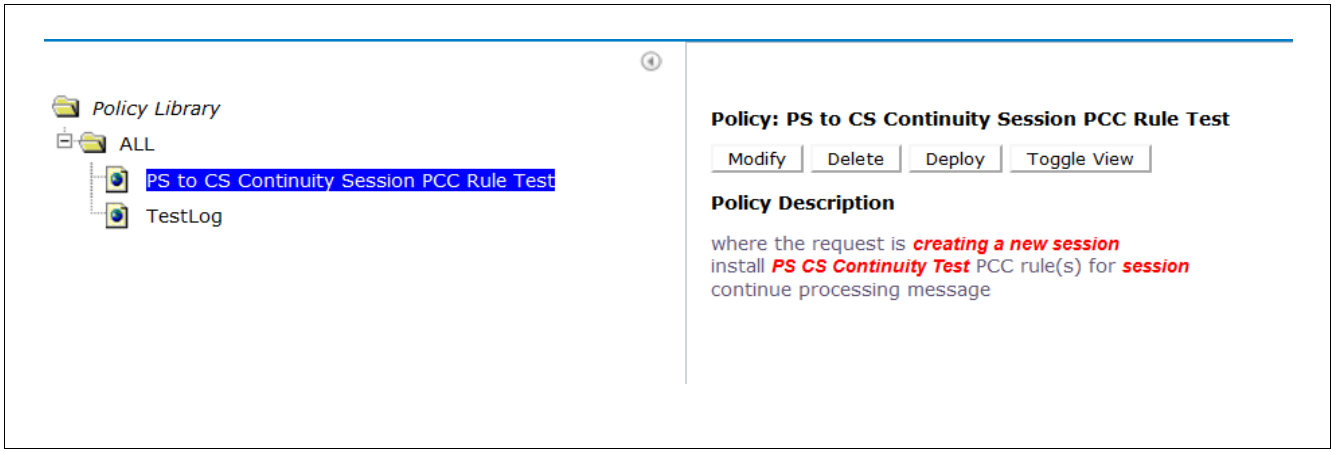
A new field, PS-to-CS-Session Continuity is added to the Traffic Profile on CMP which will have one value in the dropdown i.e., VIDEO_PS2CS_CONT_CANDIDATE (0).

This value indicates that the service data flow carries video and a candidate for PS to CS session Continuity.

If the value is configured to N/A, this AVP should not be included and has no impact to current behavior.



A new field on the Traffic Profile page



Installing the new rule

3.12 CHARGING: METERING METHOD=EVENT (PR 20222796)

3.12.1 Introduction

This feature is required to support new value 'EVENT' in Metering-Method AVP within Charging Rule Definition

3.12.2 Detailed Description

The Metering-Method AVP (AVP code 1007) is of type Enumerated, and it defines what parameters shall be metered for offline charging. The AVP is sent within Charging-Rule-Definition AVP on Gx interface. Currently, PCRF supports following values of this AVP:

DURATION (0)

This value shall be used to indicate that the duration of the service data flow traffic shall be metered.

VOLUME (1)

This value shall be used to indicate that volume of the service data flow traffic shall be metered.

DURATION_VOLUME (2)

This value shall be used to indicate that the duration and the volume of the service data flow traffic shall be metered.

As part of this feature, PCRF shall also support the value 'EVENT' for this Metering method AVP as defined in 3GPP TS 29.212 v 12.2.0:

PCRF shall support sending the Metering-Method AVP within Charging-Rule-Definition AVP with this new value on Gx interface.

pisukapa: I am just wondering the Detailed Description may need the following information on the EVENT(3) AVP

EVENT (3)

This value shall be used to indicate that events of the service data flow traffic shall be metered.

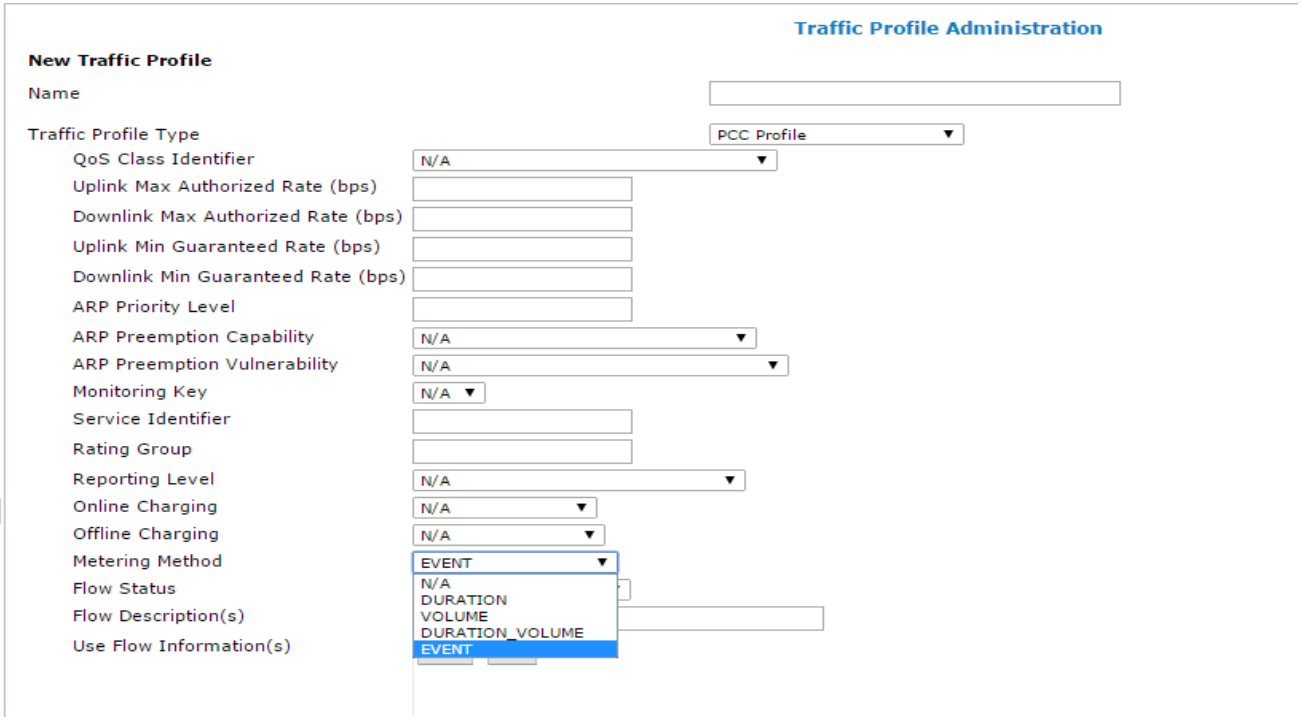
NOTE:

Event based charging is only applicable to predefined PCC rule using a service data flow filter and any PCC rule (predefined and dynamic) using an application detection filter (i.e. with an application identifier)

User Interface Changes

3.12.2.1 Create Traffic Profile screen

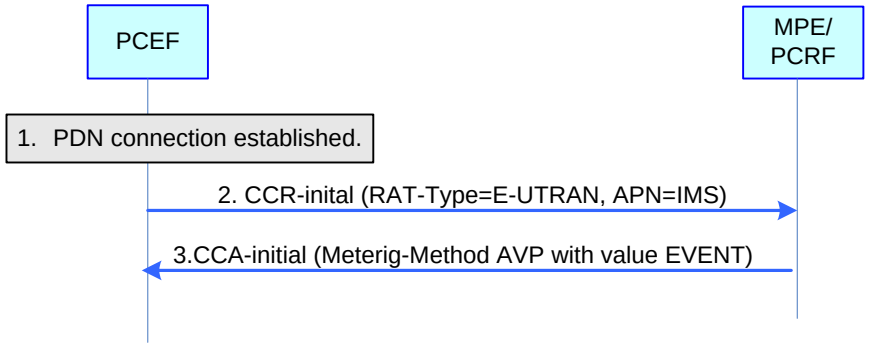
While creating/modifying a Traffic Profile of type PCC Rule/ PCC Profile, a new drop-down value 'EVENT' will be available to be configured for field metering Method' as shown below:



Creation of Traffic Profile

Call Flow Changes

There is no change in call flows. A reference call flow of receiving CCR-I and sending CCA is presented along with message capture to highlight the value 'EVENT' being sent in Metering-Method AVP within Charging-Rule-Definition AVP in CCA message.



Call Flow Changes

Diameter Message: CCA
Version: 1
Msg Length: 624
Cmd Flags: PXY
Cmd Code: 272
App-Id: 16777238
Hop-By-Hop-Id: 2154809487
End-To-End-Id: 374253691
…
Auth-Application-Id (258,M,l=12) = 16777238
CC-Request-Type (416,M,l=12) = INITIAL_REQUEST (1)
CC-Request-Number (415,M,l=12) = 0
Charging-Rule-Install (1001,VM,v=10415,l=72) =
Charging-Rule-Definition (1003,VM,v=10415,l=60) =
Charging-Rule-Name (1005,VM,v=10415,l=16) = pcc1
Precedence (1010,VM,v=10415,l=16) = 0
Metering-Method (1007,VM,v=10415,l=16) = EVENT (3)
Event-Trigger (1006,VM,v=10415,l=16) = QOS_CHANGE (1)
…
Usage-Monitoring-Level (1068,V,v=10415,l=16) = SESSION_LEVEL (0)

3.13 POLICY RELEASE 12.1.1 REFERENCE ARCHITECTURE DESCRIPTION AND REQUIREMENTS

3.13.1 Introduction

This FRS documents the reference architectures and performance requirements for validation of the Policy Release 12.1.1. There will be Gx, Sd, Rx, Sy, Sh, S9, and Fixed Line Radius call flow testing performed on the following hardware configurations:

A. 2 Site GeoRedundant Configuration with C Class Servers
B. 1 Site Configuration with C Class Servers
C. 1 Site Configuration with Rackmount Servers

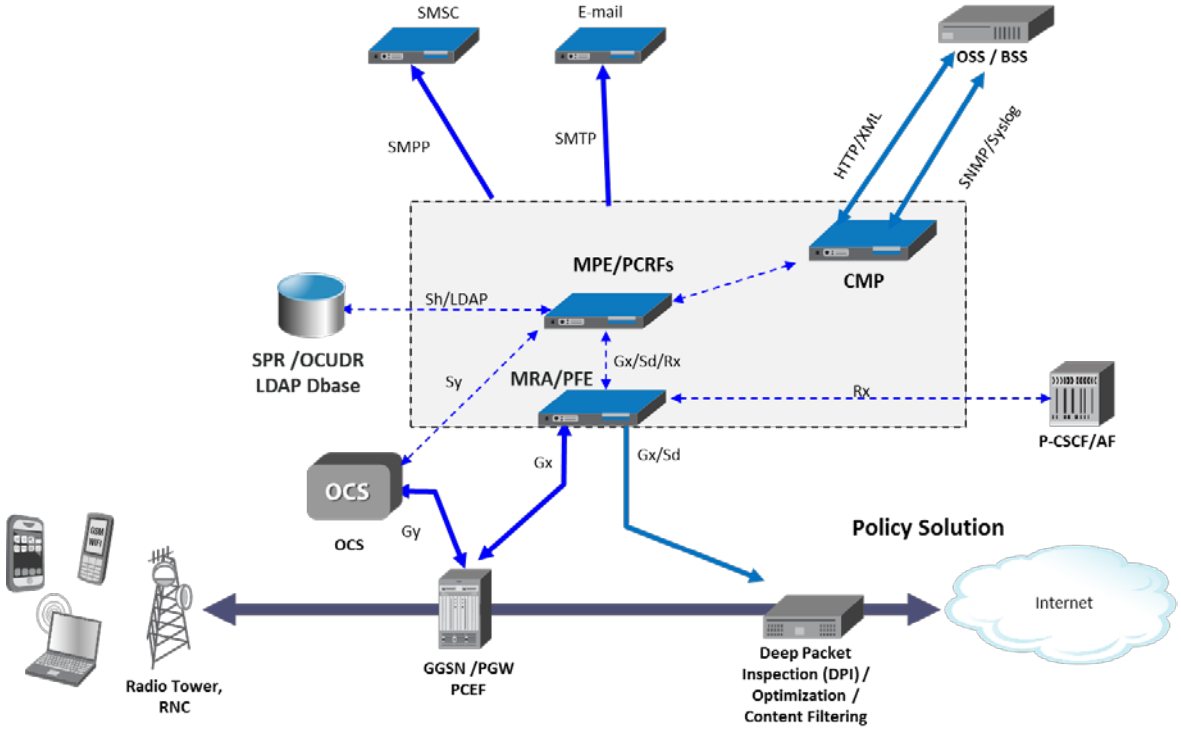
Policy Release 12.1.1 will be support OCUDR 10.0 and SPR R9.3 as part of the overall Oracle Policy Solution. Details of the OCUDR and SPR configurations can be found in Section 2.5 SPR/OCUDR Configurations.

- Testing of the Sh interface will use the SPR/OCUDR versions stated in the document for PCRF system performance validation. The SPR/OCUDR performance number listed below is only the reference for testing team to use SPR/OCUDR with different version to generate the Sh traffic if it has to.
- In no way is there comprehensive solution testing to validate the complete PCRF and SPR/OCUDR solution as this would have to be done in an external solution test which is outside the scope of this document and would have to be a cross product funded activity. The SPR/OCUDR is being used for basic interoperability confirmation and as a tool for PCRF Sh performance testing
- SPR/OCUDR performance will not be validated. That will be done by the SPR/OCUDR team.

Reference Architectures System View

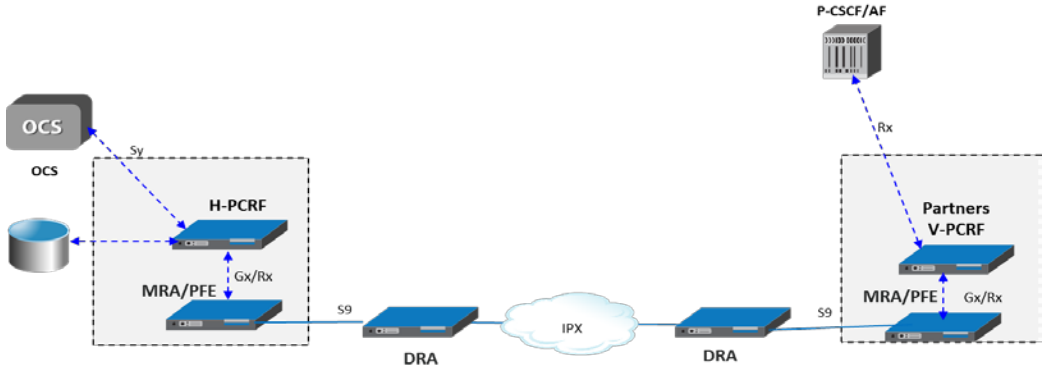
This section includes the Wireless, S9 Outbound Roaming, S9 InBound Roaming, Wireless and Fixed, and Wireless DRA Reference System Architectures that will be used for Policy R12.1.1 Reference Architecture testing with various hardware configurations and call flows as defined in this document.

3.13.2 Wireless Reference System Architecture

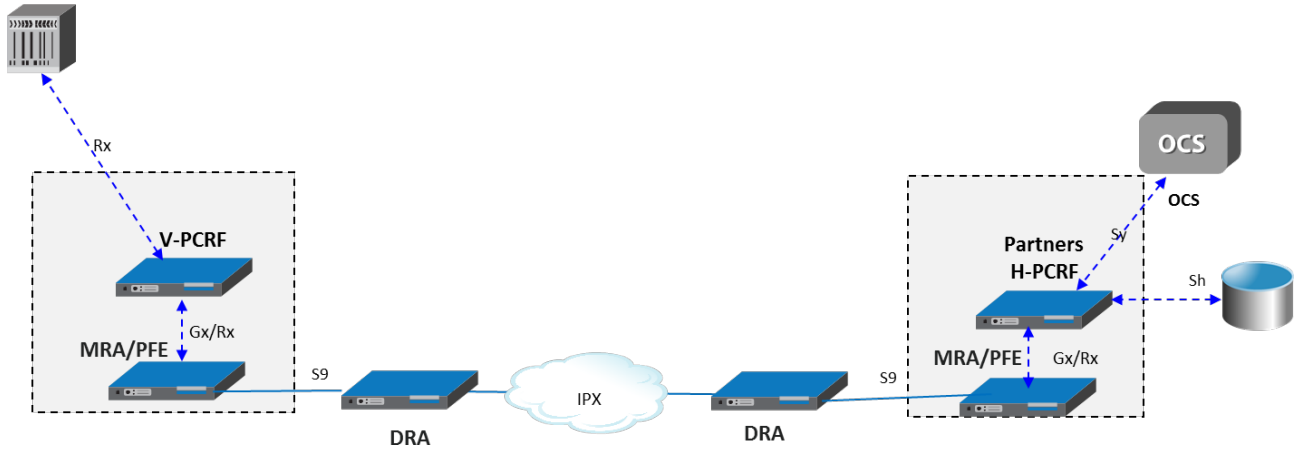


Wireless Reference System Architecture

3.13.3 Wireless S9 Outbound Roaming Reference System Architecture

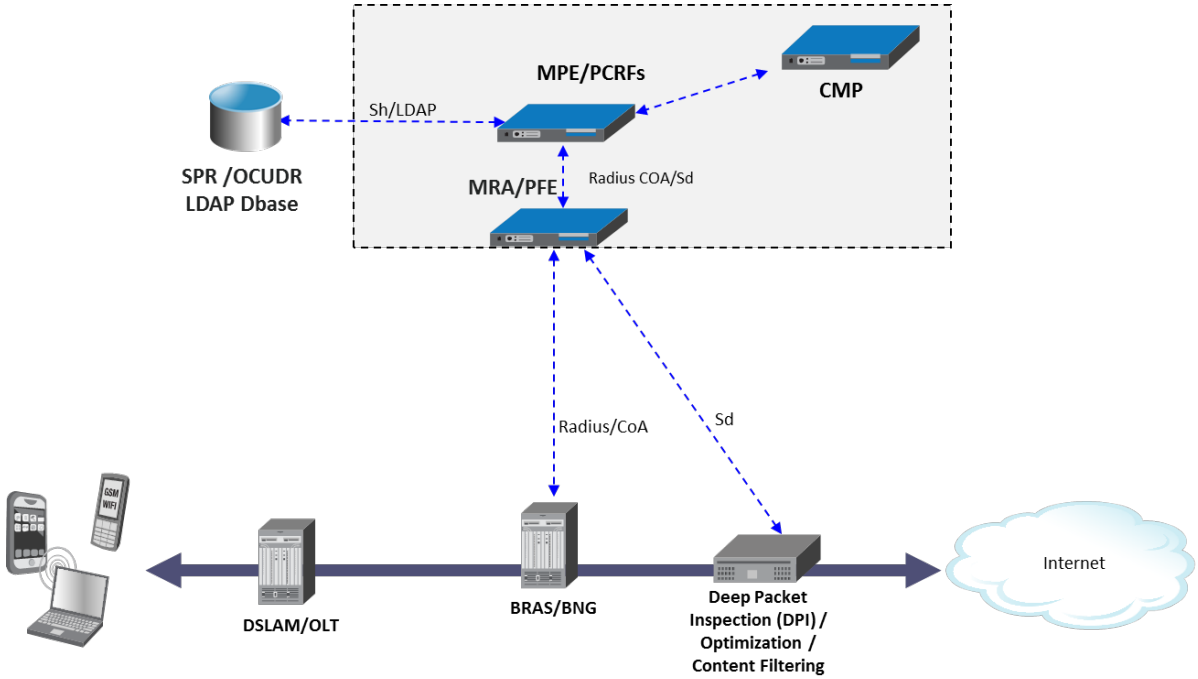


Wireless S9 Outbound Roaming Reference System Architecture



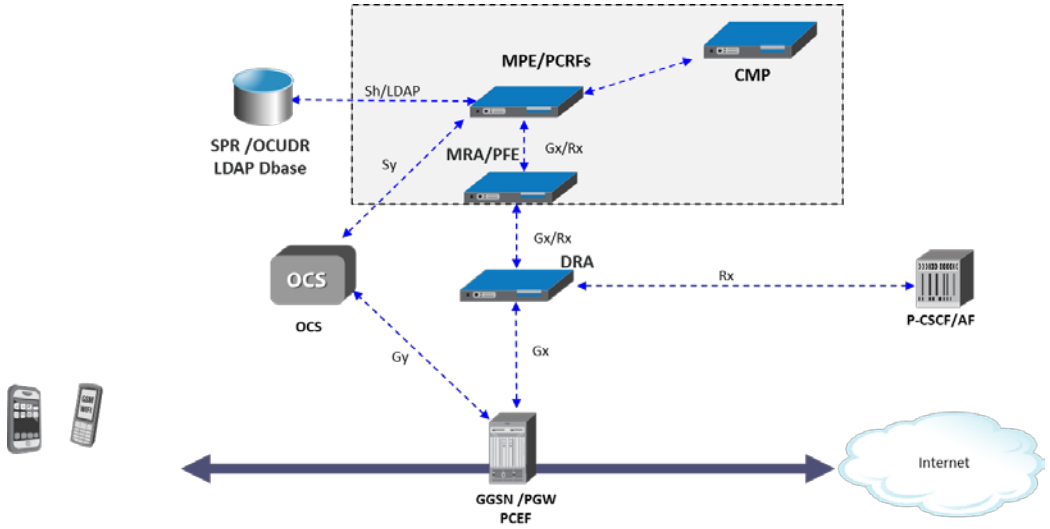
Wireless S9 Inbound Roaming Reference System Architecture

3.13.4 Wireless and Fixed Radius Reference System Architecture



Wireless and Fixed Radius Reference System Architecture

3.13.5 Wireless DRA Reference System Architecture

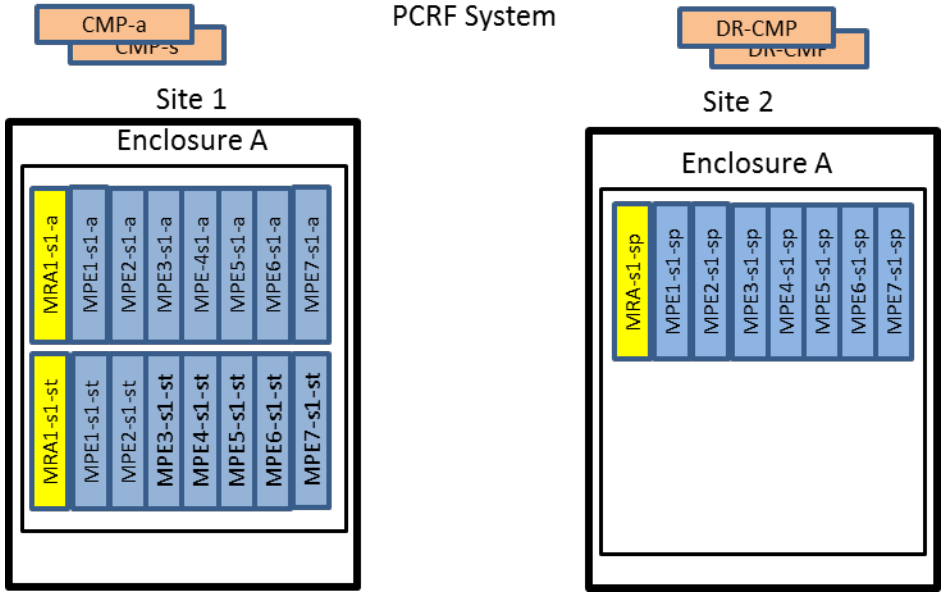


Wireless DRA Reference System Architecture Detailed Description

3.14 REF ARCHITECTURE B PERFORMANCE

3.14.1 Introduction

Topology consists of all Geo-Redundant MRA and MPE clusters. All C-Class blades are BL460 G8. The RMS is DL380. Subscriber authentication will be performed by LDAP and/or SPR lookup. Quota and Entity State variables will be managed and stored by the SPR. Both Legacy SPR and R10.0 OCUSR will be used. TDF and OCS functions will be simulated by seagull servers.

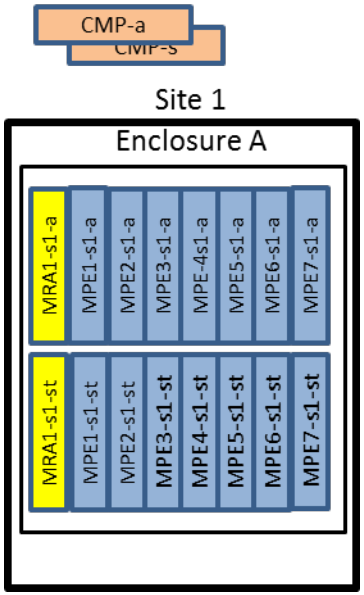


Performance Metrics

Component	Performance Target (per instance)	System TPS capability	System TPS requirement
MRA Per PCRF GeoRedundant Segment- (Statefull, Dynamic)- (1) MRA cluster	52,000 TPS 40M Bindings	52,000 (100% rated, no failures) • HP Gen 9 & HP Gen 8 BL460 Server Clusters	41,600 TPS@80% • HP Gen 9 & HP Gen 8 BL460 Server Clusters

MPE Per PCRF GeoRedundant Segment- (7) MPE Clusters	6,500 TPS for Gen 8 6,500 TPS for Gen 9 15M Concurrent Sessions Gen 9 15M Concurrent Session/Gen 8	45,500 TPS@100% • HP Gen 9 & HP Gen 8 BL460 Server Clusters 105M Concurrent Sessions@100% • HP Gen 9 & HP Gen 8 BL460 Server Clusters	36,400 TPS@80% • HP Gen 9 & HP Gen 8 BL460 Server Clusters 84M Concurrent Sessions@80% • HP Gen 9 & HP Gen 8 BL460 Server Clusters

Topology B-2 consists of a single fully loaded chassis, consisting of an MRA cluster and seven MPE clusters. The chassis is managed by a rack-mount CMP cluster. All C-Class blades are BL460 G8. The RMS is DL380. Just a minimal set of tests will be run in this configuration, since it's a subset of topology B-1 and will inherently be covered by tests run on that topology.

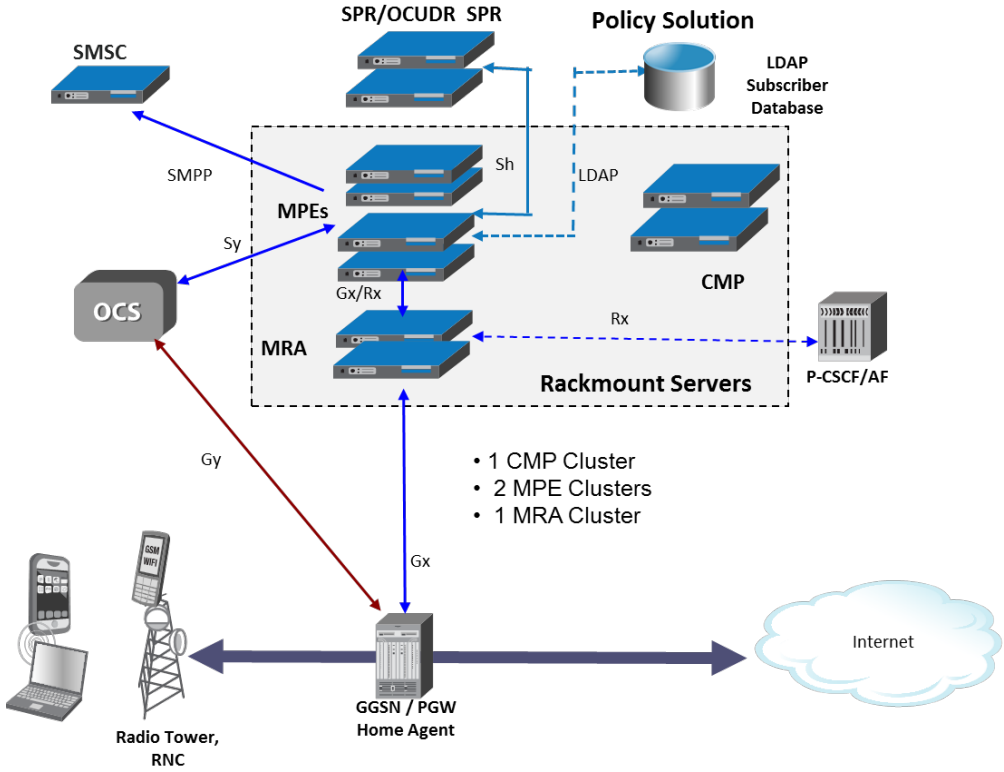


B-2 Performance Metrics

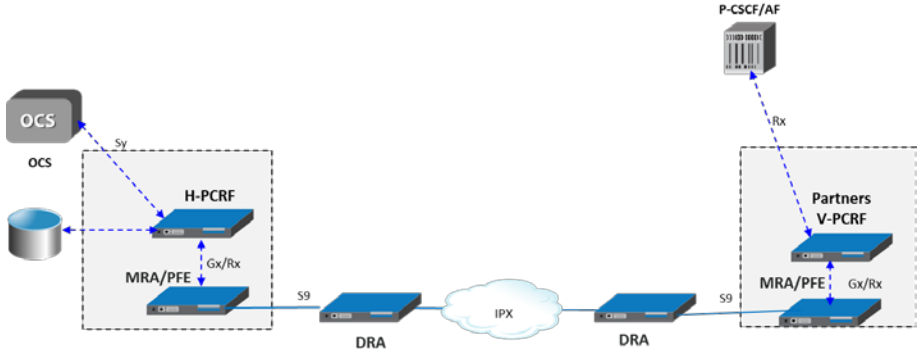
Component	Performance Target (per instance)	System TPS capability	System TPS requirement

(1) MRA Active/Standby Cluster	52,000 TPS 10K PCRF Client connections 40M Bindings	52,000 (100% rated, no failures) • HP Gen 9 & HP Gen 8 BL460 Server Clusters	41,600 TPS@80% • HP Gen 9 & HP Gen 8 BL460 Server Clusters
(7) MPE Active/Standby Clusters	6,500 TPS for Gen 8 6,500 TPS for Gen 9 15M Concurrent Sessions Gen 9 15M Concurrent Session/Gen 8	45,500 TPS@100% • HP Gen 9 & HP Gen 8 BL460 Server Clusters 105M Concurrent Sessions@100% • HP Gen 9 & HP Gen 8 BL460 Server Clusters	36,400 TPS@80% • HP Gen 9 & HP Gen 8 BL460 Server Clusters 84M Concurrent Sessions@80% • HP Gen 9 & HP Gen 8 BL460 Server Clusters

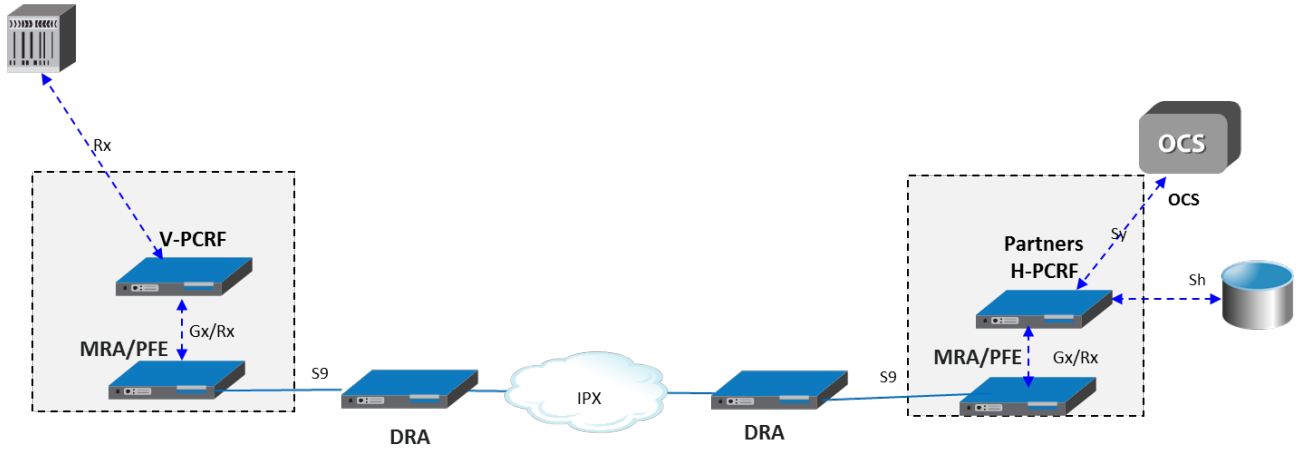
Topology B-3 consists of all rack-mount servers. In this case the servers will be Oracle X5-2 servers. The setup consists of an RMS CMP cluster, and RMS MRA cluster, and 1 or more RMS MPE clusters.



Wireless Outbound Roaming Section of Topology B-3



Wireless inbound Roaming Section of Topology B-3

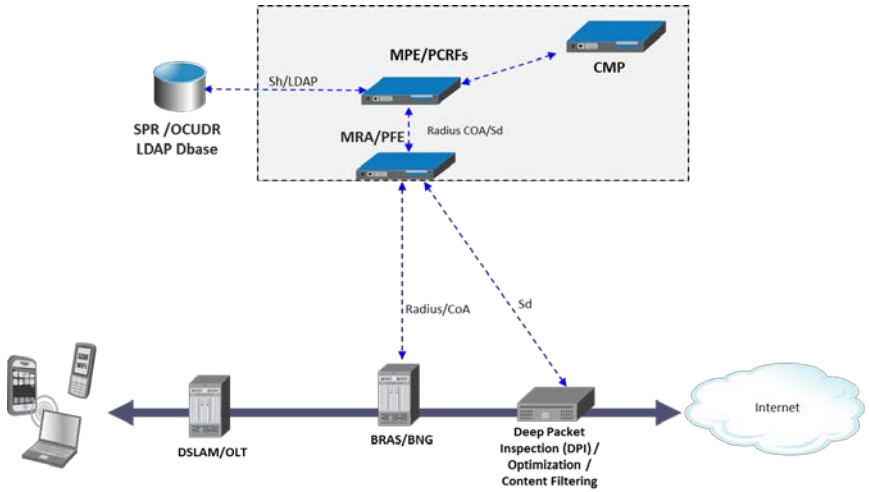


Reference B-3 Performance Metrics

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

(1) MRA Active/Standby Cluster	52,000 TPS 40M Bindings	52,000 (100% rated, no failures)	41,600 TPS@80%
(2) MPE Active/Standby Clusters	6,500 TPS for Gen 8 15M Concurrent Sessions	13,000 TPS@100% 30M Concurrent Sessions@100%	10,400 TPS@80% 44M Concurrent Sessions@80%

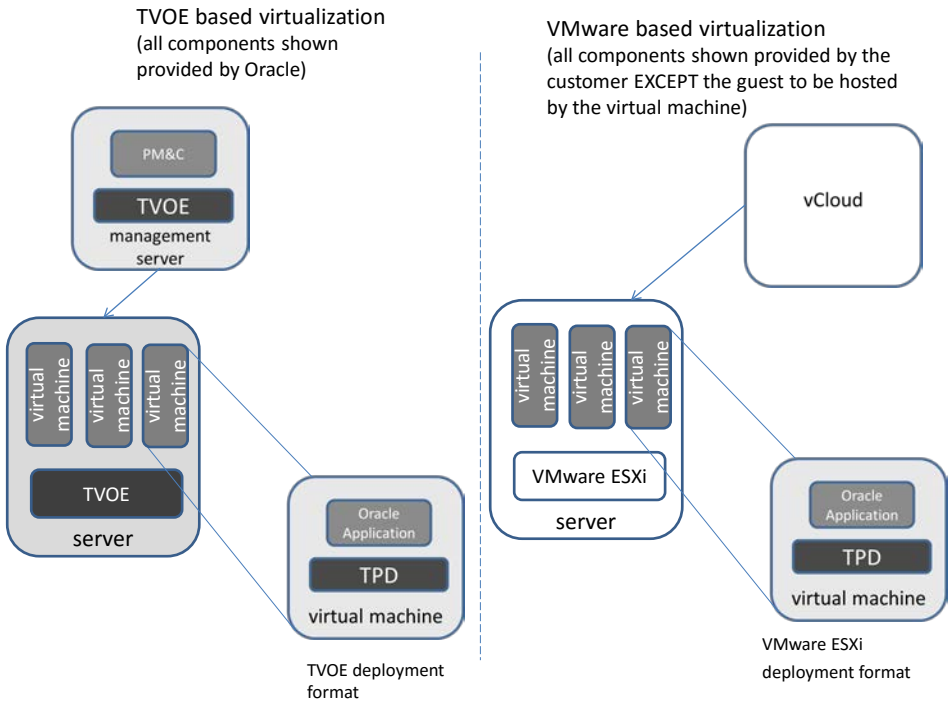
Topology C-3 consists of all rack-mount servers. The same Oracle X5-2 servers that were used in topology B-3 will be used in this setup. The setup consists of an RMS CMP cluster, and RMS MRA cluster, and 1 or more RMS MPE clusters. Topology C-3 will focus on the Fixed Mobile Convergence use case, with a mix of RADIUS and Diameter interfaces.



3.15 PLATFORM VIRTUALIZATION SUPPORT FOR VMWARE ESXI (PR 226808)

This feature supports deployment of legacy Oracle communication applications in a VMware environment. Platform has no control over the hypervisor, cloud manager, hardware, or any options that may be configured at those levels. While applications may have specific performance requirements, there is no performance requirements associated with the ability to deploy or run on ESXi.

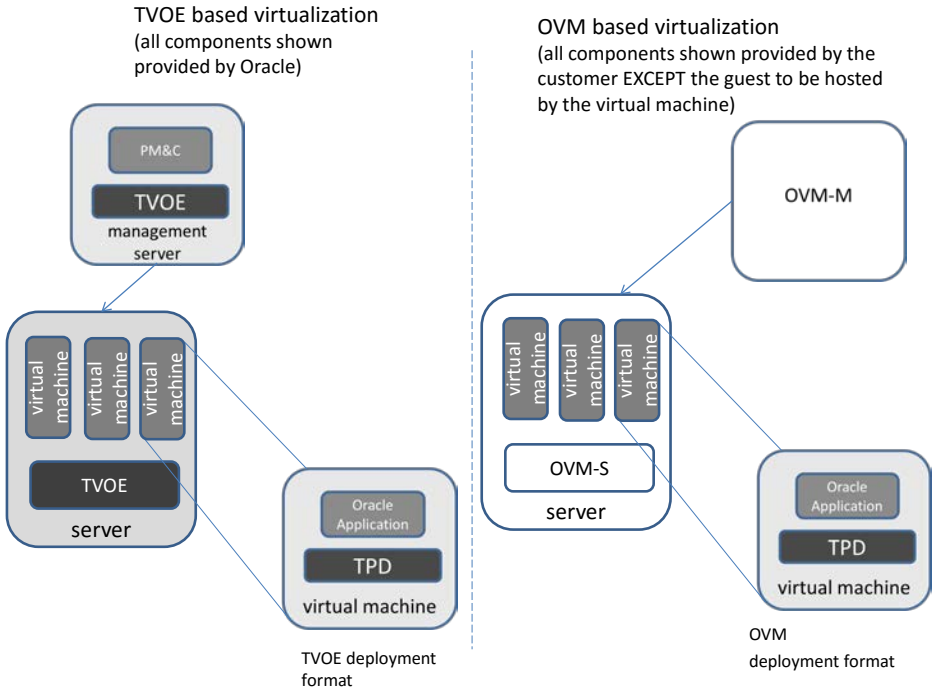
This feature ensures that guests built using TPD are able to run on a customer provided VMware virtualization solution. In this case, Platform is not providing the hypervior, nor the VM manager..



3.16 PLATFORM VIRTUALIZATION SUPPORT FOR OVM-S (PR 235915)

This feature supports deployment of legacy Oracle communication applications in an OVM environment. Platform has no control over the deployed hardware, or any options that may be configured at hypervisor or cloud manager levels. While applications may have specific performance requirements, there is no performance requirements associated with the ability to deploy or run on OVM-S.

This feature ensures that guests built using TPD are able to run on an OVM-S hypervisor.



3.17 [SEC] HTTP SERVER PRONE TO SLOW DENIAL OF SERVICE ATTACK (PR 217641)

A slow denial of service attack is when a user attempts to disable network resources by slowly sending partial requests to a server. This is mitigated by decreasing the Timeout value in apache's configuration.

3.18 NOTIFICATION TO APPLICATION ONCE SPLIT BRAIN RESOLVED (PR 238699)

This feature was requested by PCRF, but is available for any application to use.

- The active (winning) application to know when an actual multi-active event has been resolved and how long the multi-active event lasted. (eg. one or more active instances have been demoted).
- Each active application to know if the cluster is or is not intact
- The application can either be notified of the above events (similar to the way an application is notified to "go active") or have an API it can use to poll / query for the state

3.19 NON-NETRA HASWELL-BASED SUN PRODUCT SUPPORT (PR 238745)

The Oracle Server X5-2 server is to simply take the place of all DL360 and DL380 Gen8 servers in the existing HP enterprise, and Wrightline cabinets for new customer deployments of HP hardware. Oracle cabinets are not included as they are sold only for DC-powered solutions and this is an AC-powered server.

This means that an Oracle Server shall be installable anywhere that an HP rack-mount server has been installed (with exception of replacing a 1U rack-mount server with a 2U rack-mount server).

3.20 MESSAGE SENDING OPTIONS FOR ALL MEMBERS OF A POOL (BUG 19493618)

Policies can then be written to use that custom field to send SMS. To support MPE automatically sending SMS to all members of a pool.

3.21 PCRF 3GPP S9 SUPPORT (BUG 20078837)

This feature enhancement is for the PCRF to support S9 per the 3GPP TS 29.215. The S9 reference point is used in roaming scenarios involving a HPLMN and a VPLMN. The S9 reference point allows the ORACLE COMMUNICATIONS POLICY MANAGEMENT to support LTE roaming services such as Voice over LTE (VoLTE). This is done by establishing S9 and Rx sessions between the H-PVRF and the V-PCRF.

The ORACLE COMMUNICATIONS POLICY MANAGEMENT will support 'visited access' (aka local breakout) roaming scenario (both PCEF and P-CSCF in VPLMN).

3.22 HARVEST IPV4 ADDRESSES AFTER MIGRATION TO IPV6 (PR 239642)

Platform shall allow a user to delete an IPv4 address from an interface without affecting IPv6 traffic on that interface.

The intent here is to allow users to harvest their IPv4 addresses after they migrate their entire network to IPv6.

It is also the intent to not disrupt existing IPv6 traffic on Highly Available applications while removing IPv4 addresses. PM&C is exempt from the requirement to not disrupt IPv6 traffic. In other words, PM&C may disrupt IPv6 traffic on an interface while removing an IPv4 address on that interface.

3.23 RETRY PROFILE ENHANCEMENT (BUG 19117734)

The enhanced 'Retry Profile' mechanism allows PCRF to retry PCC/ADC rule installation for error scenarios corresponding to either failure to establish dedicated bearers for particular services (like PTT, Business Class Priority Service etc) OR preemption of such dedicated bearers in case customer activates bearer preemption in their network. In case of preemption, the congestion may persist for long time. This feature enhances current Retry Profile mechanism to better handle transient errors as well as longer duration network congestion scenarios

3.24 ENHANCED "VALIDATE BUTTON" FOR POLICY TABLE (BUG 19117508)

When creating or updating a policy table, the user is able to validate the current data in this policy table by clicking the 'validate' button in the GUI. If the user clicks the button, there will a popup displayed with the error message while the table is incorrectly configured, However, if the table is configured correctly, there is not any message or indication of success, hence the user will not have no idea if the operation goes well or not. This is a user experience issue which can be enhanced.

If user clicks the 'validate' button, and if the table is configured correctly, there will be a popup window with a prompt "This policy table is correctly configured." The user can click the "OK" button on the popup to dismiss it.

Normally, when viewing an object in CMP GUI, the user can modify or delete the object as long as they have the according privilege. The 'Modify' button should on the left of 'Delete' button. However, in Policy Table Library, the 'Modify' button is on the right of 'Delete' button. This is inconsistent and will be enhanced. Thus, in this release, CMP will display 'Modify' button on the left of 'Delete' button in the view page of 'Policy Table Library'.

3.25 SH RETRY AFTER SH TIMEOUT (BUG 19623928)

PCRF supports retry to the secondary datasource in case of error responses. This enhancement is to support retry in case of response timeout from the primary server. This is an extension to the current Sh Retry on Error mechanism. The Sh timeout is treated as another type of error which will result in retry.

3.26 TRAFFIC PROFILE "ADVANCED SET" ENHANCEMENT (BUG 19117519)

This feature make Policy Tables much more useful, by allowing them to be used to set fields normally defined in a PCC Rule. VZW requests that the functionality associated to the policy action.
The policy action "Advanced: set values for QoS and Charging parameters to specified value" should be extended so that this policy action can be used with the Diamter PCC Rule profile parameters (e.g., Diameter PCC Rule AF-Charging-Identifier) to modify a Charging-Rule-Definition of a Charging-Rule being installed as the result of a policy action to install a PCC Rule, by adding AVPs (set to a specific value) that are not specified by
the PCC Rule to the Charging-Rule-Definition, and/or modifying the value used for AVPs in the Charging-Rule-Definition that are specified by the PCC Rule.

3.27 GENERIC NOTIFICATION FROM POLICY SYSTEM (BUG 20631688)

The 'Generic Notifications from Policy System' feature provides a way for operators to generate custom notifications to available web services. Notifications will be generated by a new policy action. The destination, content and attributes of the notification will be configurable by the operator and allows for flexible notifications within a HTTP request message

3.28 DIAMETER INTERFACE OVERLOAD CONTROL (BUG 19481824)

The MRA and MPE both currently enter an overloaded state when they are processing more traffic than they can handle. The MRA will proactively reject certain requests destined for an MPE while that MPE is currently busy. The MPE conveys the overload state to the MRA in a DRMA LNR message. Currently, only CCR-Is for subscribers which already have bindings pointing to a busy PCRF are rejected proactively. This feature will extend the MRA's capabilities to reject all messages the MPE would normally reject to reduce the time it takes for an MPE to clear the overloaded state. We'll also attempt to successfully process a message that would currently be rejected, wherever possible. We'll do this in one of two ways:

- **Local Diversion**: Selecting a new MPE in the MRA's MPE pool for a new PDN Connection for a subscriber which was already bound to a busy MPE.
- **Remote Diversion**: Selecting a new MRA to handle a new PDN Connection for a subscriber which was already bound to a busy MPE. The new MRA will then select create a new binding for the subscriber pointing to one of the MPE's in its MPE pool.

Remote diversion will be off by default. The recommendation is for the customer to only enable remote diversion on the MRAs after all MRAs in the association have been upgraded. One they're all upgraded, the feature can safely be enabled by configuring the Expert Setting.

3.29 MAINTAIN SESSION UNIQUENESS AND AVOID STALE MESSAGE PROCESSING (BUG 19481773)

This new feature capability in the PCRF that evaluates the Origination-Timestamp AVP and the Max-Wait-Time AVP over the PCRF Gx interface to minimize race conditions and avoid stale sessions as well as maintain session uniqueness across topology.

If the PCRF receives a Gx CCR-I message after the NTP time of (Origination-Timestamp + Max-Wait-Time), then the PCRF drops the Gx CCR-I message.

This session uniqueness feature can be enabled/disabled on a per MPE cluster basis based on 2 system wide Expert configuration settings from the CMP. The default configuration values for both settings will be set to be disabled (false). When the features are disabled, the PCRF ignores the Origination-Timestamp and/or the Max-Wait Time AVPs.

Name	Default Value	Description
DIAMETER.SessionUniquenessControl	False	Controls Verizon specific validation of the new session creation
DIAMETER.SessionUniquenessControlWaitTime	False	Controls Verizon specific validation of the new session creation, taking Max-Wait-Time AVP into account

When the features are disabled then the PCRF ignores the Origination-Timestamp and/or the Max-Wait Time AVPs.

3.30 PREVENT MESSAGE STORM CAUSED BY DST (BUG 19867237)

To verify the correct operation of "Prevent Message Storms Caused by DST" that is enhanced in 12.1.1. With this feature, the PCRF will eliminate the CCR update message storm by not having the PGW send the CCR update messages upon a DST change in the UE's.

When there is a change in the UEs Daylight Saving Time (DST) a storm of CCR messages between the PGW and PCRF can occur. The goal of this feature is to eliminate the CCR message storm by not having the PGW send the CCR messages upon a DST change in the UEs.

In this solution the PGW will subscribe to time zone changes over the S5 interface from the MME. The PCRF will not subscribe to UE_TIMEZONE_CHANGE event, in order to eliminate the message storm between the PGW and PCRF. Since the PCRF doesn't subscribe to TZ change event, that PGW will not send CCR update requests to the PCRF upon UE DST Time changes, which is the reason for CCR-U storm to the PCRF today...

Since the PCRF does not register for UE_TIMEZONE_CHANGE when the Gx session is established, there will be no CCR-U message storm whenever the DST changes. This is a positive impact on performance.

In order for this feature to work, the event trigger 'UE_TIME_ZONE_CHANGE' is NOT configured for the policies, then the 'message storm' caused by DST change will be avoided.

3.31 CUSTOMER CHANGEABLE DEFAULT ACCOUNT PASSWORDS (PR 219854)

System passwords are changeable, not through GUI.

After SSH keys are properly exchanged, changing root password does not break QP components that use SSH. The components include:

- Cluster File Sync
- rsyncUtil
- Upgrade manager

3.32 RECAPTURE OF IPV4 ADDRESSES (BUG 19229408)

If the topology is running IPv4, it has to be migrated to IPv6 before recapturing IPv4 addresses.

After all servers in a cluster are running IPv4+IPv6 dual stack, and IPv6 has been selected as the preferred IP family on both OAM IP and alternative replication path, the user may decide to remove or harvest IPv4 addresses from this cluster. The operation "Remove IPv4 addresses" is applied to a cluster/site. Consider a geo-redundant MPE cluster with server A and B in site1, and server C in site 2, IPv4 addresses of server A and B are moved in one transaction, server C in another transaction.

The status of harvesting IPv4 addresses is saved in QPInfoPersist.0 with key IPv4HarvestStatus. This is a MS (Merged state) table, so the status all servers can be viewed from the Active CMP. When the key IPv4HarvestStatus does not exist, “Not harvested” is assumed.

A few states are defined for each server:

- State “not_harvested”: This is the default state when the server is installed.
- State “blocked_oam_ipv4”: In this state, IPv4 traffic is blocked on the OAM interface. Alarm 70038 is active.
- State “harvested_oam_only”: In this state, IPv4 address for OAM interface is deleted. Alarm 70038 is cleared.
- State “blocked_all_ipv4”: In this state, IPv4 traffic is blocked on all interfaces. Alarm 70039 is active.
- State “harvested_all”: In this state, IPv4 addresses for all interfaces are deleted. IPv4 VIPs are deleted on all interfaces. All configured IPv4 routes are deleted. COMCOL replication and HA traffic goes through IPv6 addresses. Alarm 70039 is cleared.

3.33 SUPPORT RX INTERFACE FOR 4G PTT (PUSH TO TALK) PLUS (BUG 19867204)

Currently, Push To Talk (PTT), is implemented in such a way that dedicated bearers can only be setup and torn down when a Gx session is created or terminated. With the “Support Rx interface for 4G PTT Plus” feature, using the Rx interface will allow dedicated bearers to be created dynamically on demand.

The PCRF will use mostly existing functionality to support the PTT feature. In order to support installing the appropriate rules for PTT, a policy must be created that looks for the correct AF-Application-Id that the PTT application uses. A simple/basic policy is shown below. Host based routes will have to be created for the PTT Rx messages that are sent from the MRA.

Policy Description

where the AF-Application-ID matches one of ***ptt-application-id***
apply ***PTT*** to all flows in the request
continue processing message

3.34 CHECKSUM TO VERIFY IMPORT/EXPORT OPERATIONS, (BUG 19117512)

CMP will calculate the MD5 checksum for exported zip files and check the MD5 when importing. If there is no MD5 file, CMP will skip the checksum when importing. If the MD5 presents and checksum fails, CMP will prompt user the failure by providing them with options ‘Proceed’ or ‘Cancel’.

When importing, user can check the ‘Skip checksum’ to import and ignore checksum mismatch.

3.35 CONFIGURATION PACKAGE (USING TEMPLATES AND XML CONSOLIDATION (BUG 19117516)

When exporting a configuration template, the system shall allow the operator to include other dependent policy objects which are referenced in the configuration template.

3.36 INCOMPATIBILITY BETWEEN MILT-LEVEL OAM AND CHECKPOINT (BUG 20386371)

Due to the incompatibility, when using the Multi-Level OAM feature (in other words, all the CMP installations are configured to be S-CMPs or NW-CMPs, then the functions for managing checkpoints are disabled (not available in the GUI). This is to prevent the user from relying on the checkpoint function when it will not work as expected. If the customer relies on the Checkpoint functions as a key part
of their processes for managing changes then they should not use the Multi-Level OAM feature.

3.37 BULK IMPORT AND EXPORT (BUG 19153045)

- Import/Export in CMP is a fundamental function. Generally, it allows users to export the current configuration objects in the CMP to xml files, so users can import these files later either to restore the configuration objects or to configure a new CMP system.
- To use the System Administrator > Import/Export action, a user must have a role that includes the System Administrator Privileges with access to Import / Export.
- The export will include the selected configuration template(s) as well as all associated dependent objects that are selected for inclusion
- Bulk export: Export multiple type of configuration objects in a single file.

3.38 SY RECONCILIATION (BUG 19482447)

Solves the issue of out-of-sync Sy sessions after recovery from a Split-brain event in the Geo-Redundant PCRF system.

Split-brain occurs when the two geo-redundant sites of the same MPE cluster (Server at Site-1 and Spare Server-C at remote Site-2) are both in “Active” role and process sessions (existing and new) during that time. Once the network recovers from the Split-brain occurrence , the MPE servers in the cluster will elect one to take on the “Active” role which is designated as the “winner”, and as a result, updates in the “loser” server during the time of split-brain, are lost. This leaves the “winner” Active MPE server with incomplete Session information by the 2 scenarios below –

1. The ”winner” server knows about the Gx and Sy sessions. However, some updates from the OCS may have been sent to the “loser” server. In this case the “winner” server has the outdated Policy Counter Status information.
2. The “winner” server does not know about the Gx and/or Sy sessions. In this case the “winner” server must recover the Gx session and then, if necessary, get the current Sy Policy Counter Status from OCS.
3. The following Expert Setting table contains the **new Sy Reconciliation configuration keys** –

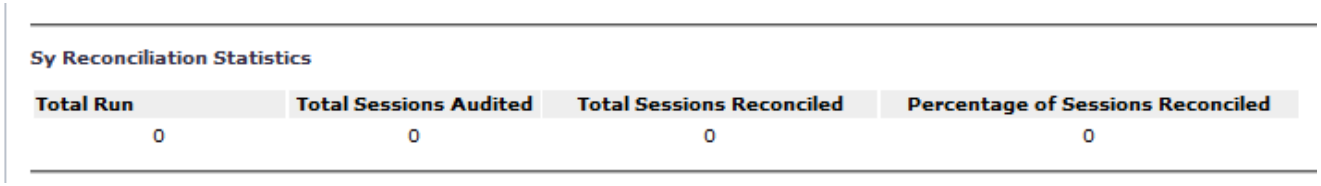
Name	Default Value	Description
SY.Reconciliation.Enabled	false	Determines whether the Sy Reconcilliation is activated and an audit of Sy sessions will be executed on a recovery from the Split-brain scenario.
SY.Reconciliation.HoldTimer	180	The time in seconds after receipt of a notification of recovery from the Split-brain scenario the Sy Reconcilliationt task will wait before starting.

Name	Default Value	Description
SY.Reconciliation.MaxSessionReconcileRate	50	The rate (in sessions/sec) at which the task will attempt to send Sy SLR Messages to reconcile Sy sessions.

4. The following table shows the **new and updated Trace Logs** –

ID	Description
10128	This relays the current status of the Sy Reconciliation task, as the following - • RUNNING – A notification of split-brain resolution was received and either the hold-down timer has expired or the hold-down timer was set to 0. The task is currently processing Sy sessions. The next state reported by the task should be STOPPED or COMPLETED. • HOLD – A notification of split-brain resolution was received. The task has been triggered, but is currently not running due to the configured hold-down timer. The next state reported by the task should be RUNNING. • STOPPED – The task was running, but was stopped probably due to a notification of resolution of another split-brain scenario. Statistics will be recorded up to the point the task was stopped. This is an end-state for the task. • COMPLETE – The task has finished processing. Statistics will be recorded for this execution of the task. This is an end-state for the task.
10129	This relays the statistics about the most recent pass of the Sy Reconciliation task. This will only be displayed if the status is STOPPED or COMPLETE.
10132	Notification of split-brain recovery was received by the MPE from the QP with the timestamp the QP believes the split-brain event began.

5. A **new Stats counter** for the feature as shown –



Sy Reconciliation Statistics

Total Run	Total Sessions Audited	Total Sessions Reconciled	Percentage of Sessions Reconciled
0	0	0	0

6. A **new Policy condition** added –

Policy Condition Group	Policy Condition or Action	Description
"Network Devices" Conditions	*For example:* where the remote MPE is unavailable	Check whether the remote site in a Geo-Redundant configuration is *unavailable or available*

3.39 SPLIT PLATFORM MANAGEMENT SUBNET SUPPORT FOR PLATFORM R7.0.X (BUG 19959369)

Expand the PCRF footprint by adding a third enclosure to a PM&C domain that already includes two enclosures. The third enclosure to be in a separate Platform Management Subnet due to unavailability of IP addresses in existing subnet.

The technology to support multiple subnets already exists within our product. This feature is anticipated to primarily be a documentation and test exercise.

3.40 6.118 AN_GW FAILED REPORTING TO PCRF AND P-CSCF (BUG 19481792)

In case of SGW failure, all Rx requests will be rejected.

The PCRF will not enforce new or updated policies to the PGW by either RAR or CCA, as long as the SGW is unavailable except if they have PCC rules to be removed.

If rule installation was triggered by an Rx request from an application function, and the rules cannot be updated or installed on the PCEF because of Serving Gateway failure, the PCRF will notify the Application Function of the Specific Action INDICATION_OF_FAILED_RESOURCE_ALLOCATION or INDICATION_OF_RELEASE_OF_BEARER if the Application function had registered for it.

There are three cases in which we consider the S-GW as unavailable:

1) PCRF sends RAR to P-GW and RAA is received with experimental result code DIAMETER_AN_GW_FAILED.
2) P-GW replies with RAA or sends CCR-U to the PCRF, including rule report(S) with rule failure code set to AN_GW_FAILED.
3) P-GW replies with RAA or sends CCR-U with An-Gw-Status AVP set to AN_GW_FAILED(0).

In all three cases, we set the enforcement session field ‘anGwStatus’ to ‘AN_GW_FAILED’ (enumeration) and store the current time. The ‘anGwStatus’ is set back to ‘UNKNOWN’ only when the PCRF receives AN_GW_CHANGE event trigger or when the PCRF sends RAR to the P-GW since the maximum time for the S-GW to be unavailable without getting a notification from the P-GW for S-GW restoration was reached, and RAA returns DIAMETER_SUCCESS.

When any indication about S-GW failure is received from the P-GW, the PCRF stores the current timestamp in the session. If there is any internal change in the PCRF that triggers RAR to the P-GW while the S-GW is still unavailable, the PCRF will add maximum amount of time (configured) to the stored timestamp. In case the result exceeds the current time, the PCRF will send the RAR to the P-GW even if the status of the S-GW is still unavailable. This is done to avoid a scenario in which the PCRF did not receive an indication of S-GW restoration although the S-GW became available.

3.41 IPV6 SERVICEABILITY FEATURES (PR 239641)

Platform shall provide a mechanism to bulk import IP addresses and IP routes for Platform software IP interfaces.

- Platform shall support adding IPv6 addresses via this mechanism.
- Platform shall support adding IPv4 addresses via this mechanism.
- Ability to modify IP addresses via bulk import is not a requirement.
- This requirement Applies to all Platform IP interfaces except IP interfaces on PM&C and third-party devices.

For an external device, if an IPv4 address is the only address that has been configured within Platform, Platform shall allow adding a new IPv6 address for that device without impacting any IPv4 traffic that may already be running between Platform and that device.The intent here is to allow a customer to create a file with all IP address assignments and to upload the file to the system as opposed to entering one address at a time via an interactive GUI.

3.42 REEVALUATE AUTO-GENERATED RULES ON CCR-U/ GP IDENTIFICATION OF DEFAULT BEARER (BUG 19117544)

3.42.1 Introduction

On Gx session establishment, in case the operator does not install a Charging Rule using policies, the Oracle PCRF generates a default rule for the session and sends it to the gateway in the CCA message. This rule is called a *generated default rule* in the document to follow.

3.42.1 Details Description

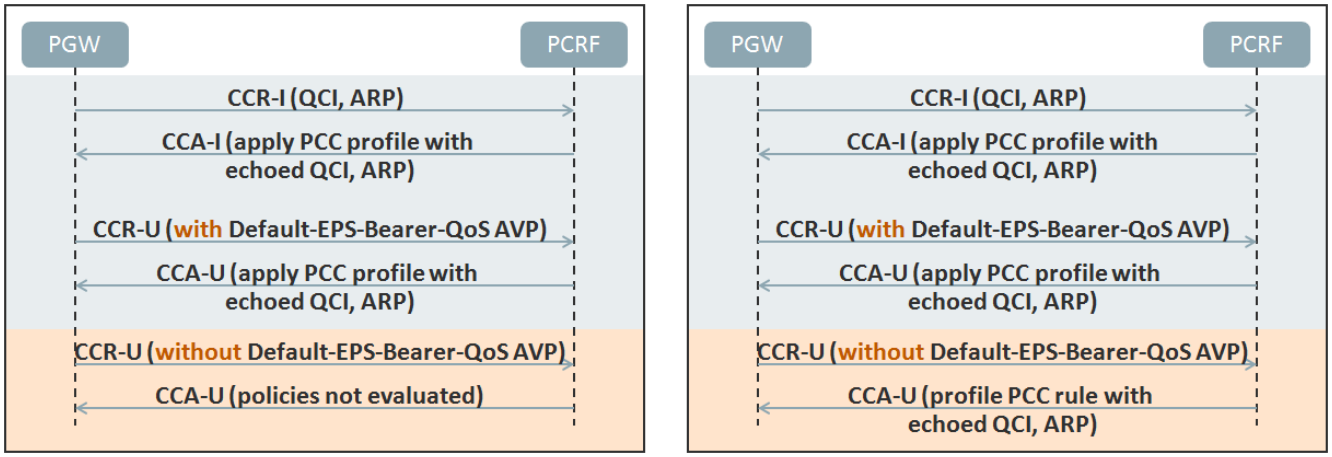
Some situations (e.g., outbound Gp-based roaming) require that the PCRF to install a-generated default rule in which QoS values (e.g. QCI and ARP values) are echoed back. This rule also needs to specify other parameters such as Rating Group, Online Charging method and Offline Charging method. This information in turn is based on the subscriber's APN and SPR/HSS profile.

Currently, a generated default rule (based on a provisioned PCC profile) may be installed by the PCRF when it receives a CCR-I. The policy action *apply traffic profile* works on CCR-I for both UTRAN/GERAN and EUTRAN radio access type. When this action is used, the generated default rule is modified as per the parameters from the applied profile and sent back to the PGW. If the QCI/ARP parameters are absent in the applied profile, the value received in the Default-EPS-Bearer-QOS in the incoming CCR-I is used to formulate the QCI and ARP values in the rule sent out in the CCA.

On CCR-U, this policy action works *only* if the CCR-U also contains the Default-EPS-Bearer-QOS (DEBQ) AVP. The PCRF does not re-evaluate the generated default rule on an update message if the default EPS bearer QoS does not change. If the Default-EPS-Bearer-QoS is not provided in a CCR-U, the flow which includes the default auto-generated rule (e.g., 0_0) is not evaluated through the policy engine. As a result, there is nothing to apply a PCC profile to. Given that the PGW (in some networks) only provides the Default-EPS-Bearer-QoS when it changes, the operator cannot rely on using an a*pply profile* policy to always set the contents of the generated default rule.

However, if Default-EPS-Bearer-QOS is provided in a CCR-U, the PCRF will automatically copy the values from the Default-EPS-Bearer-QoS to the generated default rule and provision this rule in the corresponding CCA-U. The CCA-U will include the default auto generated rule with the values from applied profile.

This enhancement allows the generated default rule to be updated when a CCR-U is received, regardless of whether the Default-EPS-Bearer-QoS AVP is present.



Current (left) and updated (right) flows

Functionality

The policy system shall allow the re-evaluation and installation of the generated default rule when a CCR-U is received, even if the Default-EPS-Bearer-QoS is not present.

4.0 **OSSI XML/ SNMP MIB DELTA**

In the following table, the Added & changed MIBs are listed, for the Delta of TPD 6.7.0.0.1_84.20.0 to TPD 7.0.2.0.0_86.25.0

Change Type	MIB Module	OID	OID Name	Event Description	ALARM Event-ID	Default Severity Level
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.49	tpdFipsSubsystemProblem	The FIPS subsystem needs intervention		
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.3.38	tpdFipsSubsystemWarning	The FIPS subsystem needs intervention		
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.38	tpdFlashProgramFailure	Flash device failed to update	32337	Major
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.2	tpdHidsBaselineCreated	HIDS baseline created	32701	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.3	tpdHidsBaselineDeleted	HIDS baseline deleted	32702	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.8	tpdHidsBaselineUpdated	HIDS baseline has been updated	32707	Info

Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.5	tpdHidsDisabled	HIDS monitoring has been disabled	32704	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.4	tpdHidsEnabled	HIDS monitoring has been enabled	32703	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.50	tpdHidsFileTampering	HIDS file tampering detected	32349	Major
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.7	tpdHidsResumed	HIDS monitoring has been resumed	32706	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.6	tpdHidsSuspended	HIDS monitoring has been suspended	32705	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.51	tpdSecurityProcessDown	HIDS detected security process is down	32350	Major
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.39	tpdSerialMezzUnseated	Serial Mezzanine card is not seated properly	32338	Major

Changed	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.3.14	tpdDeviceIfWarn	Device Interface Warning	32513	Minor

In the following table, the Added & changed MIBs are listed, for the Delta of TPD 7.0.0.0.0_86.12.0 to TPD 7.0.2.0.0_86.25.0

Change Type	MIB Module	OID	OID Name	Event Description	ALARM Event-ID	Default Severity Level
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.38	tpdFlashProgramFailure	Flash device failed to update	32337	Major
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.2	tpdHidsBaselineCreated	HIDS baseline created	32701	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.3	tpdHidsBaselineDeleted	HIDS baseline deleted	32702	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.8	tpdHidsBaselineUpdated	HIDS baseline has been updated	32707	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.5	tpdHidsDisabled	HIDS monitoring has been disabled	32704	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.4	tpdHidsEnabled	HIDS monitoring has been enabled	32703	Info

Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.50	tpdHidsFileTampering	HIDS file tampering detected	32349	Major
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.7	tpdHidsResumed	HIDS monitoring has been resumed	32706	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.4.6	tpdHidsSuspended	HIDS monitoring has been suspended	32705	Info
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.51	tpdSecurityProcessDown	HIDS detected security process is down	32350	Major
Added	TEKELEC-TPD-ALARMS-MIB	1.3.6.1.4.1.323.5.3.18.3.1.2.39	tpdSerialMezzUnseated	Serial Mezzanine card is not seated properly	32338	Major

In the following table, the Added, changed and Deleted MIBs are listed, for the Delta of Policy Release 11.5.0.0.0_38.1.0 to 12.1.1.1

Change Type	MIB Module	OID	OID Name	Event Description	ALARM Event-ID	Default Severity Level
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.31301	comcolHaTopologyNotify	HA Topology Events	31301	Info
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.32347	comcolTpdHWMGMTCLIProblemNotify	Oracle hwmgmtcliStatus Problem	32347	Major
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.32346	comcolTpdOEMHardwareProblemNotify	Server Hardware Problem	32346	Major
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.86306	pcrfMIBNotificationsCMPApplyFailedNotify	CMP Failed to apply settings.	86306	Major
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70501	pcrfMIBNotificationsClusterMixedVersionNotify	The Cluster is running different versions of software	70501	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70502	pcrfMIBNotificationsClusterReplicationInhibitedNotify	Replication is inhibited in the cluster	70502	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71403	pcrfMIBNotificationsConnectivityDegradedNotify	Diameter Connectivity Degraded	71403	Minor

ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71402	pcrfMIBNotificationsConnectivityLostNotify	Diameter Connectivity Lost	71402	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70505	pcrfMIBNotificationsISOMismatchNotify	The server's ISO is not the expected version	70505	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.86308	pcrfMIBNotificationsNCMPReferdObjMissNotify	The top level object is missing in NW-CMP but is referred by S-CMP	86308	Major
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.86303	pcrfMIBNotificationsNWCMPApplyFailedNotify	NW-CMP failed to apply settings to S-CMP.	86303	Major
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71003	pcrfMIBNotificationsOmStatsExceptionErrorNotify	OM stats task could not genarate a perticular stats due to Exception	71003	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71002	pcrfMIBNotificationsOmStatsParseErrorNotify	OM stats task could not parse stats info	71002	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71005	pcrfMIBNotificationsOmStatsValueExceedErrorNotify	OM stats value has been truncated to fit the data size	71005	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70041	pcrfMIBNotificationsQPFailedToExecuteRecaptureIpv4 Notify	QP failed to execute recapture of IPv4 addresses	70041	Minor

ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70040	pcrfMIBNotificationsQPFailedToPrepareRecaptureIpv4Notify	QP failed to prepare recapture of IPv4 addresses	70040	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70042	pcrfMIBNotificationsQPFailedToRollbackRecaptureIpv4Notify	QP failed to rollback recapture of IPv4 addresses	70042	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70039	pcrfMIBNotificationsQPHasBlockedIPv4Notify	QP has blocked IPv4 traffic	70039	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71001	pcrfMIBNotificationsRemoteDiversionNotPossibleNotify	Remote diversion is not possible	71001	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.86307	pcrfMIBNotificationsSCMPSYNCFAILSNotify	S-CMP fails sync the reference with NW-CMP.	86307	Major
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.86305	pcrfMIBNotificationsSCMPSplitBrainNotify	S-CMP is in split brain.	86305	Major
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.86304	pcrfMIBNotificationsSCMPUNREACHABLENotify	S-CMP is unreachable.	86304	Major
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.72575	pcrfMIBNotificationsSMSRHTTPConnectionClosedNotify	The connection to a configured Policy Notification destination was lost	72575	Minor

ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70503	pcrfMIBNotificationsServerForcedStandbyNotify	The server is in forced standby	70503	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70508	pcrfMIBNotificationsServerIsZombieNotify	A server has become a zombie	70508	Critical
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70500	pcrfMIBNotificationsSystemMixedVersionNotify	The system is running different versions of software	70500	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70507	pcrfMIBNotificationsUpgradeInProgressNotify	An upgrade/backout action on a server is in progress	70507	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70506	pcrfMIBNotificationsUpgradeOperationFailedNotify	An upgrade action on a server failed	70506	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.79995	pcrfMIBNotificationsX1ConnectionLostNotify	X1 Connection between the Mediation Function and Policy Server is Lost	79995	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.79996	pcrfMIBNotificationsX2ConnectionLostNotify	X2 Connection between the Policy Server and Mediation Function is Lost	79996	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.31301	comcolHaTopologyNotify	HA Topology Events	31301	Info

CHANGED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.31223	comcolHaHbTransmitFailureNotify	The high availability monitor failed to send heartbeat	31223	Major
CHANGED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.31222	comcolHaNotConfiguredNotify	High availability is disabled due to system configuration	31222	Minor
CHANGED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.31225	comcolHaSvcStartFailureNotify	The required high availability resource failed to start	31225	Major
DELETED	~~PCRF-ALARM-MIB~~	~~1.3.6.1.4.1.323.5.3.29.1.2.71402~~	~~pcrfMIBNotificationsTransportClosedNotify~~	~~Diameter Transport Closed~~		
DELETED	~~PCRF-ALARM-MIB~~	~~1.3.6.1.4.1.323.5.3.29.1.2.71403~~	~~pcrfMIBNotificationsTransportDisconnectedNotify~~	~~Diameter Transport Disconnected~~		

In the following table, the Added, changed and Deleted MIBs are listed, for the Delta of Policy Release 12.0.0.0.0_23.3.0 to 12.1.1.1

Change Type	MIB Module	OID	OID Name	Event Description	ALARM Event-ID	Default Severity Level
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.31301	comcolHaTopologyNotify	HA Topology Events	31301	Info
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70501	pcrfMIBNotificationsClusterMixedVersionNotify	The Cluster is running different versions of software	70501	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70502	pcrfMIBNotificationsClusterReplicationInhibitedNotify	Replication is inhibited in the cluster	70502	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70505	pcrfMIBNotificationsISOMismatchNotify	The server's ISO is not the expected version	70505	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71003	pcrfMIBNotificationsOmStatsExceptionErrorNotify	OM stats task could not genarate a perticular stats due to Exception	71003	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71002	pcrfMIBNotificationsOmStatsParseErrorNotify	OM stats task could not parse stats info	71004	Minor

ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71005	pcrfMIBNotificationsOmStatsValueExceedErrorNotify	OM stats value has been truncated to fit the data size	71005	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70041	pcrfMIBNotificationsQPFailedToExecuteRecaptureIpv4Notify	QP failed to execute recapture of IPv4 addresses	70041	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70040	pcrfMIBNotificationsQPFailedToPrepareRecaptureIpv4Notify	QP failed to prepare recapture of IPv4 addresses	70040	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70042	pcrfMIBNotificationsQPFailedToRollbackRecaptureIpv4Notify	QP failed to rollback recapture of IPv4 addresses	70042	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70039	pcrfMIBNotificationsQPHasBlockedIPv4Notify	QP has blocked IPv4 traffic	70039	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.71001	pcrfMIBNotificationsRemoteDiversionNotPossibleNotify	Remote diversion is not possible	71001	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.72575	pcrfMIBNotificationsSMSRHTTPConnectionClosedNotify	The connection to a configured Policy Notification destination was lost	72575	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70503	pcrfMIBNotificationsServerForcedStandbyNotify	The server is in forced standby	70503	Minor

ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70508	pcrfMIBNotificationsServerIsZombieNotify	A server has become a zombie	70508	Critical
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70500	pcrfMIBNotificationsSystemMixedVersionNotify	The system is running different versions of software	70500	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70507	pcrfMIBNotificationsUpgradeInProgressNotify	An upgrade/backout action on a server is in progress	70507	Minor
ADDED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70506	pcrfMIBNotificationsUpgradeOperationFailedNotify	An upgrade action on a server failed	70506	Minor
CHANGED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.86308	pcrfMIBNotificationsNCMPReferdObjMissNotify	The top level object is missing in NW-CMP but is referred by S-CMP	86308	Major
CHANGED	PCRF-ALARM-MIB	1.3.6.1.4.1.323.5.3.29.1.2.70050	pcrfMIBNotificationsQPTimezonechangedetectedNotify	Timezone change detected.Application needs to be rebooted	70050	Minor